Amazon Connect

Administrator Guide

Amazon Connect: Administrator Guide

Table of Contents

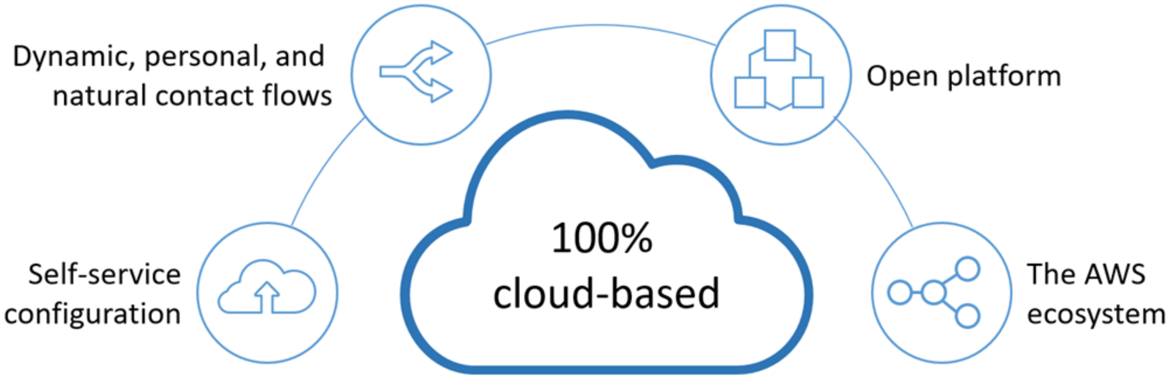
What is Amazon Connect?

Amazon Connect is an omnichannel cloud contact center. You can set up a contact center (p. 9) in a few steps, add agents who are located anywhere, and start engaging with your customers.

You can create personalized experiences for your customers using omnichannel communications. For example, you can dynamically offer chat and voice contact (p. 536), based on such factors as customer preference and estimated wait times. Agents, meanwhile, conveniently handle all customers from just one interface (p. 1135). For example, they can chat with customers, and create or respond to tasks as they are routed to them.

Amazon Connect is an open platform that you can integrate with other enterprise applications, such as Salesforce (p. 294). In addition, you can take advantage of the AWS ecosystem to innovate new experiences for your customers.

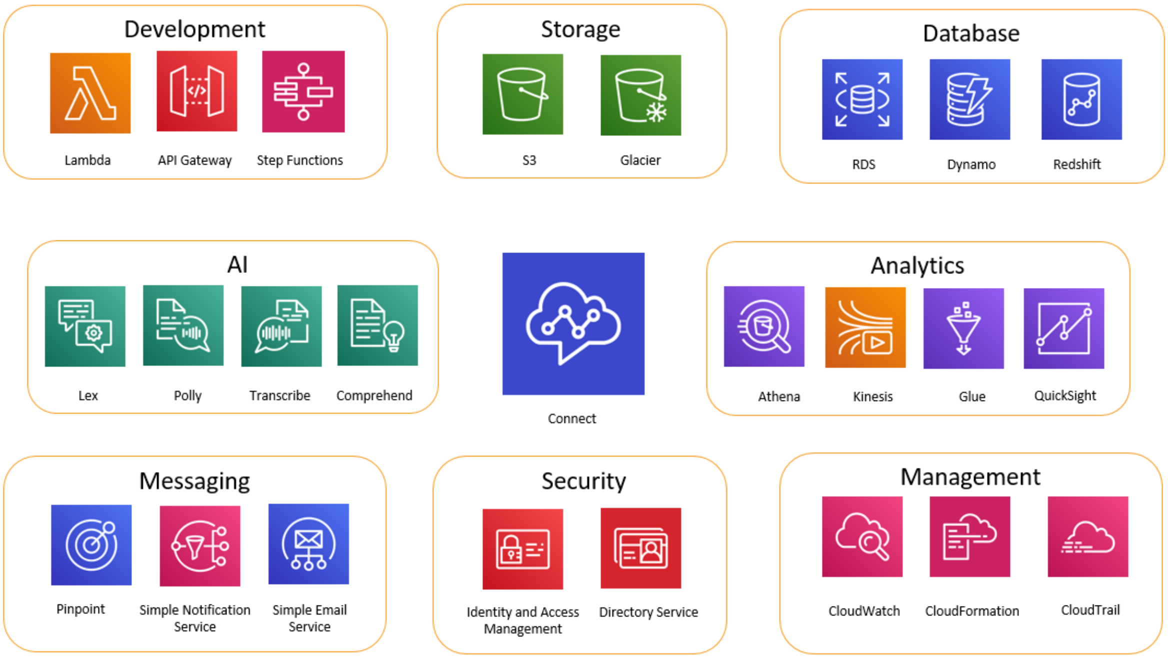
The following diagram shows these key characteristics of Amazon Connect.


Dynamic, personal, and natural contact flows
Open platform
Self-service configuration
100% cloud-based
The AWS ecosystem

Contents

The power of AWS with Amazon Connect

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



Development

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

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

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

For more information, see:

- Invoke AWS Lambda functions (p. 488)

Storage

Amazon Connect uses Amazon Simple Storage Service (Amazon S3) to store recorded conversations and exported reports. When you set up Amazon Connect, it creates default buckets for these requirements, or you can point it to existing Amazon S3 infrastructure. For more information, see Step 4: Data storage (p. 137) in Create an Amazon Connect instance (p. 135).

VPC endpoints are not supported.

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

Database

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

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

For more information, see:

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

Analytics

Amazon Connect tracks all interactions using contact records (p. 1001). Contact records are used for real-time and historical metrics reports. You can also use Amazon Kinesis to stream them to an AWS database like Amazon Redshift or Amazon Athena for BI analysis (Amazon QuickSight, or a third party such as Tableau). There are AWS CloudFormation templates available to set up this functionality for Amazon Redshift and Athena.

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

For more information, see:

- How to access Kinesis Video Streams data (p. 776)
- Blog post: Recovering abandoned calls with Amazon Connect

Machine Learning (ML) and Artificial Intelligence (AI)

Amazon Connect uses the following services for ML/AI:

- Amazon Lex—Lets you create a chatbot to use as Interactive Voice Response (IVR). For more information, see Add an Amazon Lex bot (p. 617).
- Amazon Polly—Provides text-to-speech in all contact flows. For more information, see Add text-to-speech to prompts (p. 456) and SSML tags supported by Amazon Connect (p. 464).
- Amazon Transcribe—Grabs conversation recordings from Amazon S3, and transcribes them to text so you can review them.
- Amazon Comprehend—Takes the transcription of recordings, and applies speech analytics machine learning to the call to identify sentiment, keywords, adherence to company policies, and more.

Messaging

Amazon Connect uses the following services for messaging:

- Amazon Pinpoint—Use as an outbound messaging trigger for events; for example, bulk messaging (such as outbound marketing campaigns). For more information, see this blog post: Using Amazon Pinpoint to send text messages in Amazon Connect.

- Amazon Simple Notification Service (Amazon SNS)—Use to send and receive SMS and other channel notifications. Amazon SNS is particularly useful for sending alerts and validations.
- Amazon Simple Email Service (Amazon SES)—Use to send validation e-mails, such as a password reset bot sending a confirmation of the transaction.

Security

Amazon Connect uses the following services for added security:

- AWS Identity and Access Management (IAM)—Use to manage permissions for users. Amazon Connect users require permission for services. For more information, see Identity and access management for Amazon Connect (p. 1078).
- AWS Directory Service—Amazon Connect supports user federation through the internal directory (created in the Amazon Connect instance), using Active Directory integration (MAD, ADFS) or SAML 2.0.

  For more information, see:
  - Plan your identity management in Amazon Connect (p. 123)
  - Blog post: Enabling federation with AWS Single Sign-On and Amazon Connect

Management

Amazon Connect uses the following services for monitoring usage:

- Amazon CloudWatch—Collects logs, service metrics, performance metrics for Amazon Connect. For more information, see Monitoring your instance using CloudWatch (p. 1014).
- AWS CloudFormation—Amazon Connect does not support this directly for creating instances. However, it does support AWS CloudFormation templates for associated services, like integrations, database export, and so on.
- AWS CloudTrail—Provides a record of Amazon Connect API calls. This is especially useful for tracking who accessed recorded conversations (p. 806).

  For more information about Amazon Connect and AWS CloudTrail, see Logging Amazon Connect API calls with AWS CloudTrail (p. 1025).

Browsers supported by Amazon Connect

Agents use the Contact Control Panel (CCP) (p. 1135) in Amazon Connect to communicate with contacts. The CCP is a website that they access using a web browser.

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

Browser	Version	How to check your version
Google Chrome	Latest three versions	Open Chrome and type chrome://version in your address bar. The version is in the Google Chrome field at the top of the results.
Mozilla Firefox ESR	Versions are supported until their Firefox end-of-life date.	Open Firefox. On the menu, choose the Help icon and

Browser	Version	How to check your version
	For details, see the Firefox ESR release calendar.	then choose **About Firefox**. The version number is listed underneath the Firefox name.
Mozilla Firefox	Latest three versions	Open Firefox. On the menu, choose the Help icon and then choose **About Firefox**. The version number is listed underneath the Firefox name. Please see Issue with Firefox version 86 (p. 5).
Microsoft Edge and Edge Chromium	Not supported	

For more requirements, see Agent headset and workstation requirements for the CCP (p. 292).

Browsers on mobile devices

The Amazon Connect console and Contact Control Panel (CCP) do not work on mobile browsers. However, your agents can forward the audio portion of the call to their mobile device. For instructions, see Forward calls to a mobile device (iPhone, Android) (p. 1144).

Issue with Firefox version 86

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

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

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

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

Supported screen readers

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

- JAWS
- NVDA

- VoiceOver

Languages supported by Amazon Connect

Contact Control Panel

CCP	Supported languages
Contact Control Panel - latest version	• Chinese (Simplified) • Chinese (Traditional) • English • French • German • Italian • Japanese • Korean • Portuguese (Brazilian) • Spanish
Contact Control Panel - earlier version	• English • French • German • Italian • Japanese • Korean • Portuguese (Brazilian) • Spanish

Chat message content

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

Amazon Connect Admin console

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

Contact Lens for Amazon Connect

Post-call analytics	Post-call redaction	Real-time analytics	Real-time redaction	Call summarization
Arabic (Gulf)				
English (Australia)	English (Australia)	English (Australia)	English (Australia)	English (Australia)
English (Great Britain)	English (Great Britain)	English (Great Britain)	English (Great Britain)	English (Great Britain)
English (United States)	English (United States)	English (United States)	English (United States)	English (United States)
English (India)	English (India)			English (India)
English (Ireland)	English (Ireland)			English (Ireland)
English (Scotland)	English (Scotland)			English (Scotland)
English (Wales)	English (Wales)			English (Wales)
French (Canada)		French (Canada)		
French (France)		French (France)		
German (Germany)		German (Germany)		
German (Switzerland)				
Hindi (India)				
Italian (Italy)		Italian (Italy)		
Japanese (Japan)		Japanese (Japan)		
Korean (South Korea)		Korean (South Korea)		
Mandarin (Mainland China)		Mandarin (Mainland China)		
Portuguese (Brazil)		Portuguese (Brazil)		
Portuguese (Portugal)				
Spanish (Spain)				
Spanish (United States)		Spanish (United States)		

Pattern match languages

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

- English (United States)

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

Amazon Connect Wisdom

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

Amazon Lex

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

Amazon Polly

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

Get started with Amazon Connect

Use these steps to set up your contact center.

1. Create an Amazon Connect instance (p. 135). Use an instance to contain all the resources and settings related to your contact center. You specify how you plan to manage user accounts, whether your contact center will accept incoming calls and make outbound calls, and review the location where data will be stored in your Amazon S3 bucket.
2. Set up phone numbers for your contact center (p. 157). 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. 220). Create your queues and routing profiles, and set your hours of operation. In your routing profiles, specify the channels that agents should use: voice, chat, tasks, or all three. You also specify how many chats and tasks an agent can manage at the same time.
4. Create Amazon Connect contact flows (p. 296). Establish a contact flow to define the customer experience with your contact center from start to finish. A single contact flow works for voice, chat, and tasks, which makes your design more efficient. When you build contact flows and configure the blocks, indicate how the flow should work for voice, chat, and tasks.
5. Add users, which are your managers and agents, and configure their settings. Assign a routing profile to each agent, specify whether they are using a softphone or desk phone, and set how long they have for **After contact work**. For instructions, see Add users to Amazon Connect (p. 785) and Set up agents (p. 230).
6. If you're using chat, we provide several tools to help you enable your customer-facing app to engage with Amazon Connect chat. For more information, see Set up your customer's chat experience (p. 243).

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. 479). 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. 798).
2. Add an Amazon Lex bot (p. 617). Use Amazon Lex in your contact center to reduce the load on your agents. For example, a bot can handle the initial interaction before the chat is routed to an agent, and also answer common questions for the customer.

Take a free online class

Check out the following free online classes:

- Introduction to Amazon Connect and the Contact Control Panel (CCP)
- Amazon Connect: Introduction to the Administrative Interface
- Amazon Connect: Creating and Managing Amazon Connect Instances

Concepts

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

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

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

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

Contents

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

Contents

Telephony architecture

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

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

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

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 that 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 make 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 that you are local to their area, and provide a cheaper inbound route than a long-distance call if you don't publish a toll-free number.

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

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

Claiming numbers in Amazon Connect

Amazon Connect provides you the ability to claim both direct dial and toll-free numbers in supported countries from inventories maintained by AWS. To claim a number, log into your Amazon Connect instance and select **Phone numbers**. For instructions, see Claim a phone number in your country (p. 167).

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/regions. In the United States and Canada, the process is regulated and well-defined. In other countries/regions, some have 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. 157) 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 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. 157).

Use cases for different configurations

Starting fresh with Amazon Connect

In this case, simply select new numbers using the claim a number process. For instructions, see Claim a phone number in your country (p. 167).

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. 157) 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 external platform is the primary call handler, you will need to configure that platform to forward calls to a number you claim in Amazon Connect. Choose either a toll-free number, which will give you better redundancy and capacity at an increased cost, or a bank of DID numbers to terminate the call into Amazon Connect.
- For the use case, we recommend that you engage AWS Solution Architecture support to ensure your contact center is well-architected to achieve the best possible outcomes.

Chat

Amazon Connect Chat enables your customers to start chatting with contact center agents from any of your business applications, web or mobile. Interactions are asynchronous, enabling your customers to start a chat with an agent or Amazon Lex bot, step away from it, and then resume the conversation again. They can even switch devices and continue the chat.

Agents have a single user interface to help customers using both voice and chat. This reduces the number of tools that agents have to learn and the number of screens they have to interact with. Chat activities integrate into your existing contact center flows and the automation that you built for voice. You build your flows once and reuse them across multiple channels. Likewise, for metrics collection and the dashboards you built, they automatically benefit from the unified metrics across multiple channels.

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

Getting started with chat

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

- Enable chat at the instance level by creating an Amazon S3 bucket for storing chat transcripts (p. 137).
- Add chat to your agent's routing profile (p. 227).

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

Amazon Connect provides several resources to help you add chat to your website. For more information, see Set up your customer's chat experience (p. 243).

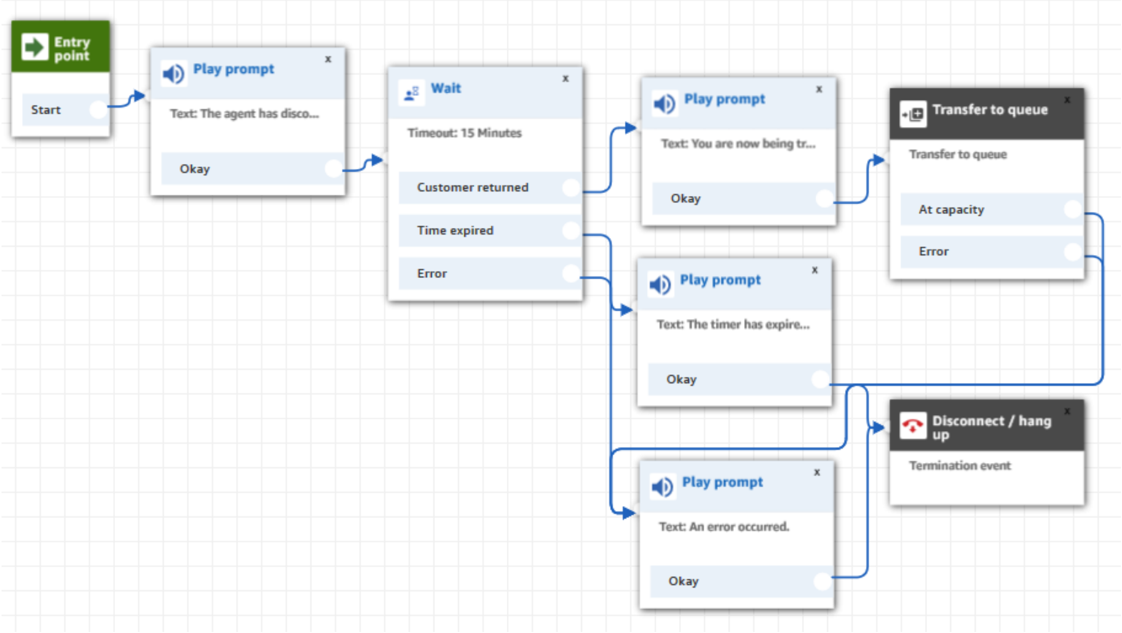
Example chat scenario

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

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

Here's how you build this scenario:

1. Create a disconnect flow. The following image shows the Sample disconnect flow (p. 310).

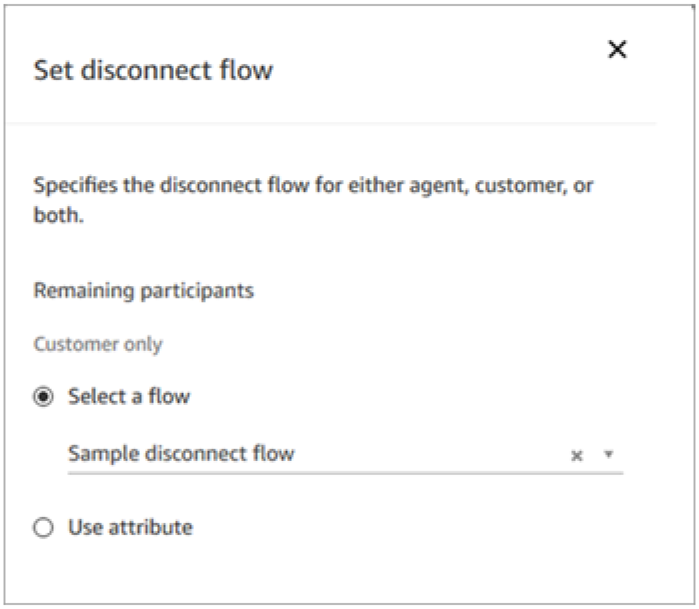


2. In the disconnect flow, add a Wait (p. 441) block. The Wait block has two branches:

   - **Timeout**: Run this branch if the customer hasn't sent a message after a specified amount of time. The total duration of the chat, including multiple **Wait** blocks, cannot exceed 25 hours.

     For example, for this branch you might just want to run a **Disconnect** block and end the chat.
   - **Customer return**: Run this branch when the customer returns and sends a message. With this branch, you can route the customer to the previous agent, previous queue, or set a new working queue or agent.
3. In your inbound contact flow, add the Set Disconnect Flow (p. 403) 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.



Set disconnect flow

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

Remaining participants

Customer only

● Select a flow

Sample disconnect flow

○ Use attribute

For an example that uses the **Set disconnect flow** block, see the Sample inbound flow (p. 309).

When do chats end?

By default, the duration for a chat conversation, including the time spent waiting when the customer isn't active, can't exceed 25 hours.

To configure a custom chat duration, call the StartChatContact API and add the `ChatDurationInMinutes` parameter. Using this parameter, you can configure a chat to last from as little as 1 hour (60 minutes) to up to 7 days (10,080 minutes).

During an ongoing chat session, there's no limit to the number of times a customer can leave and rejoin an existing ongoing chat session. To accomplish this, use the Wait (p. 441) block. For example, you might wait 12 hours for the customer to resume the chat before ending the chat session. If the customer tries to resume the chat after 12 hours, in the flow you can have an Amazon Lex bot ask if they're contacting you about the same issue or a different one.

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

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

More information

For more information about chat, see the following topics:

- Test voice, chat, and task experiences (p. 148)
- How routing works with multiple channels (p. 221)
- Create a routing profile (p. 227)

- Amazon Connect Chat SDK and Sample Implementations

Tasks

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

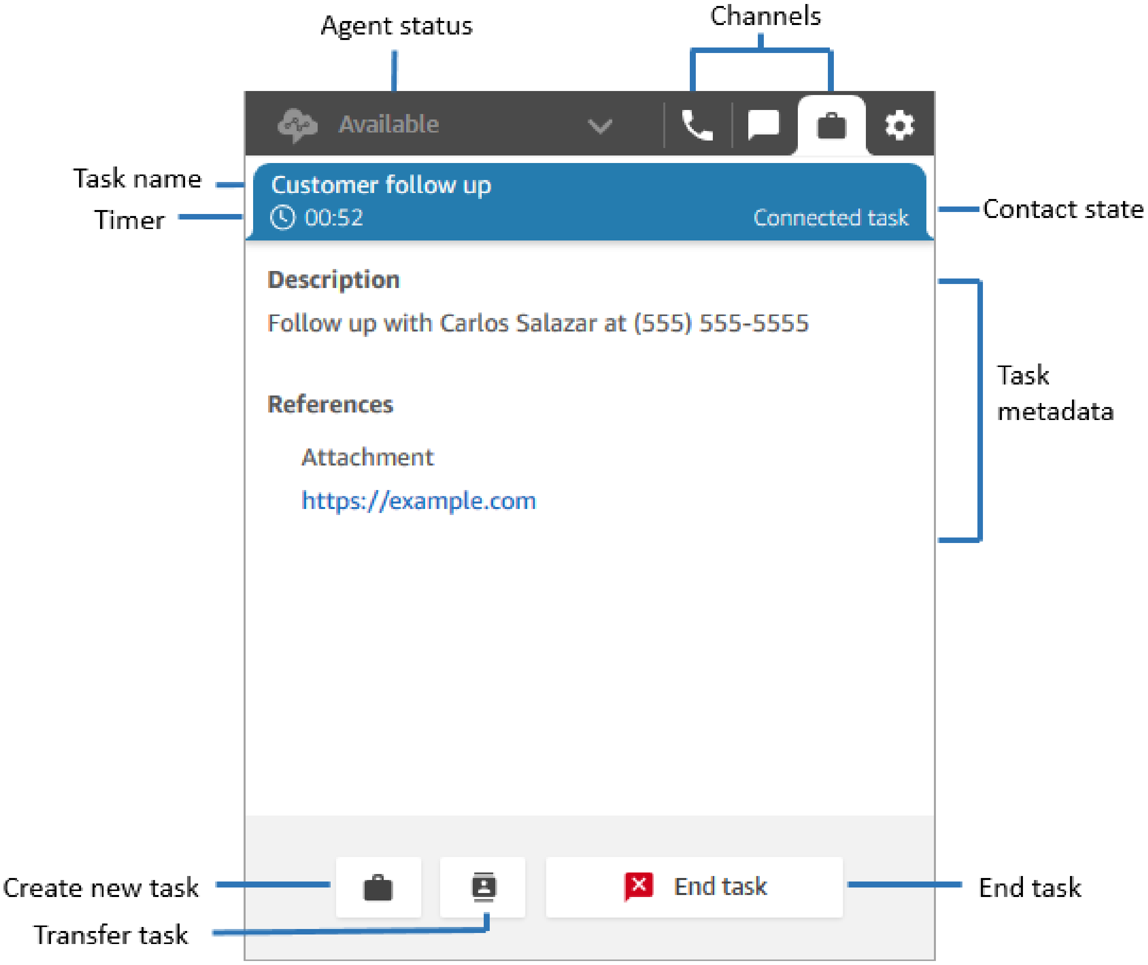
- Follow-up on customer issues recorded in a customer relationship management (CRM) solution such as Salesforce.
- Follow-up with a customer via a call.
- Complete actions in a business-specific system, such as processing a customer claim in an insurance application.

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

What is a task?

A *task* is a unit of work that an agent must complete. This includes work that may have originated in external applications. It's routed, prioritized, assigned, and tracked just like voice and chat.

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



Customer follow up
00:52
Connected task

Description

Follow up with Carlos Salazar at (555) 555-5555

References

Attachment

https://example.com

How to create tasks

Amazon Connect provides different ways for you to create tasks:

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

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

   For more information, see Set up applications for task creation (p. 757) and Create rules that generate tasks for third-party integrations (p. 602).
2. You can integrate with your homegrown or business-specific applications to create tasks using Amazon Connect APIs.

   For more information, see the StartTaskContact API.
3. You can add a Create task (p. 355) block to your contact flows. This block enables you to create and orchestrate tasks directly from flows based on customer input (DTMF input), and contact and tasks information.
4. You can enable your agents to create tasks from the Contact Control Panel (CCP) without you doing any development work.

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

For more information, see Test voice, chat, and task experiences (p. 148).

For more information on getting started with tasks, see Set up tasks (p. 237).

Supported contact flow types

You can use tasks in the following contact flow types:

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

Supported contact blocks

You can use tasks in the following contact blocks:

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

Using IAM? Add Task permissions

If your organization is using custom IAM policies to manage access to the Amazon Connect console, make sure users have the appropriate permissions to set up applications for task creation. For a list of required permissions, see Tasks page (p. 1090).

Note
If your instance was created before October 2018, for information about how to configure your service-linked roles (SLR), see For instances created before October 2018 (p. 1121).

Track tasks in real-time and historical metrics reports

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

- How long agents spent working on each task (Agent on contact time (p. 941)).
- The total time from when a task was created to when it was completed. (Contact handle time (p. 945)).

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

Real-time metrics

- Avg interaction and hold time (p. 921)
- Avg hold time (p. 920)

Historical metrics

- Agent interaction and hold time (p. 940)
- Agent interaction time (p. 940)
- Average agent interaction time (p. 943)
- Average customer hold time (p. 943)

Manage tasks to custom service levels (SL)

While voice and chats may have short service level times based on seconds or minutes, you may have some tasks with service levels that are hours or days. You can create custom service level durations that are appropriate to each of your channels. For more information, see real-time custom service levels (p. 924) and historical custom service levels (p. 951).

When do tasks end?

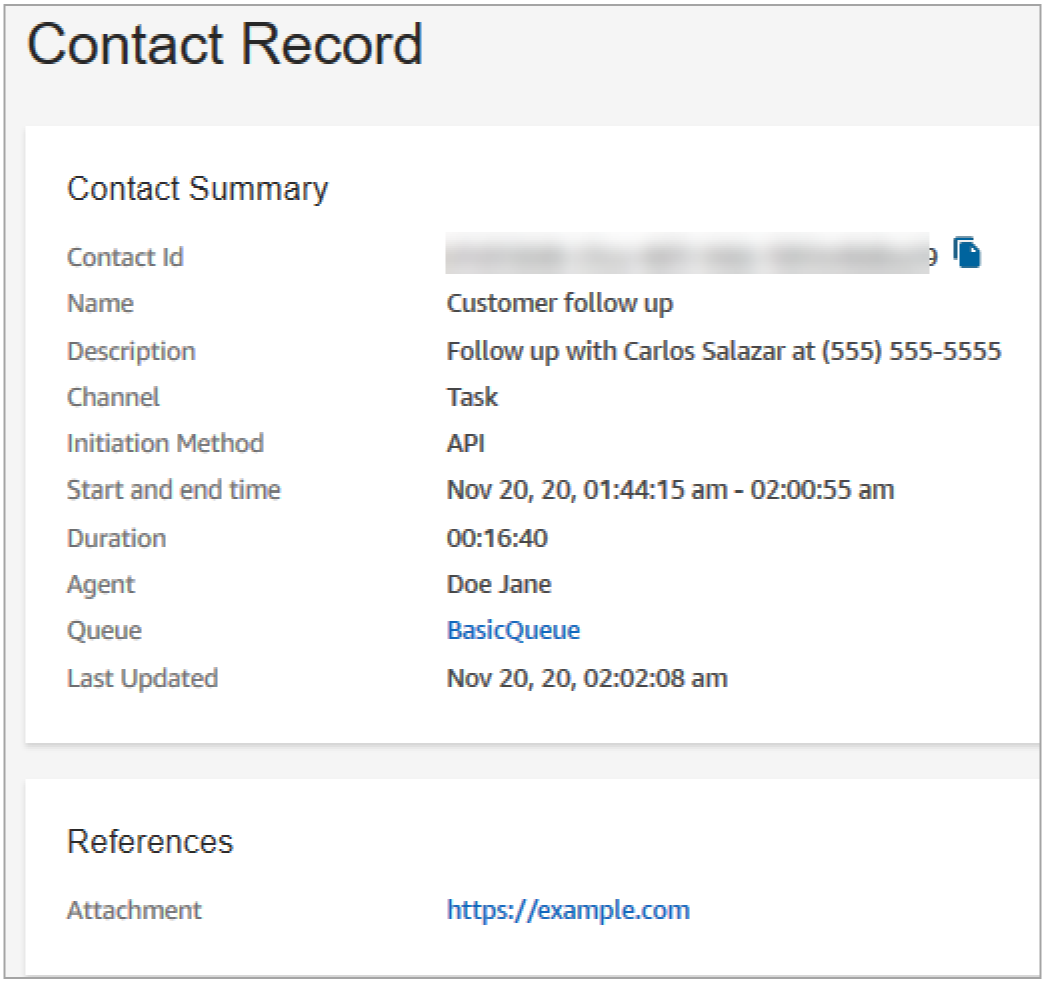
The total duration of a task can be up to 7 days. A task ends when one of the following happens:

- An agent completes the task.
- A contact flow runs a Disconnect / hang up (p. 362) block, which ends the task.
- A task reaches the 7 day limit.
- You end the task using the StopContact API.

Search and review completed tasks

Use the Contact search (p. 907) page to search for and review completed tasks.

The following image is an example of what the **Contact Summary** and **References** look like in a contact record for a task.



Contact Record

Contact Summary

Contact Id	[redacted]
Name	Customer follow up
Description	Follow up with Carlos Salazar at (555) 555-5555
Channel	Task
Initiation Method	API
Start and end time	Nov 20, 20, 01:44:15 am - 02:00:55 am
Duration	00:16:40
Agent	Doe Jane
Queue	BasicQueue
Last Updated	Nov 20, 20, 02:02:08 am

References

Attachment	https://example.com

The following data is appended to the contact record but not stored with it. The data is included in an export.

- Contact flow ID
- Potential attributes:
  - ContactDetails (p. 988)
    - Name: the name of the task
    - Description: the description of the task
  - References (p. 995): any links to forms or other sites

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

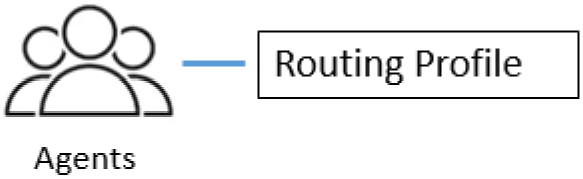
More information

- Feature specifications (p. 1210)
- Accept a task (p. 1172)
- Create a new task (p. 1175)
- Transfer a task (p. 1179)

Routing profiles

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

- Each agent is assigned to one routing profile.
- A routing profile can have multiple agents assigned to it.



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

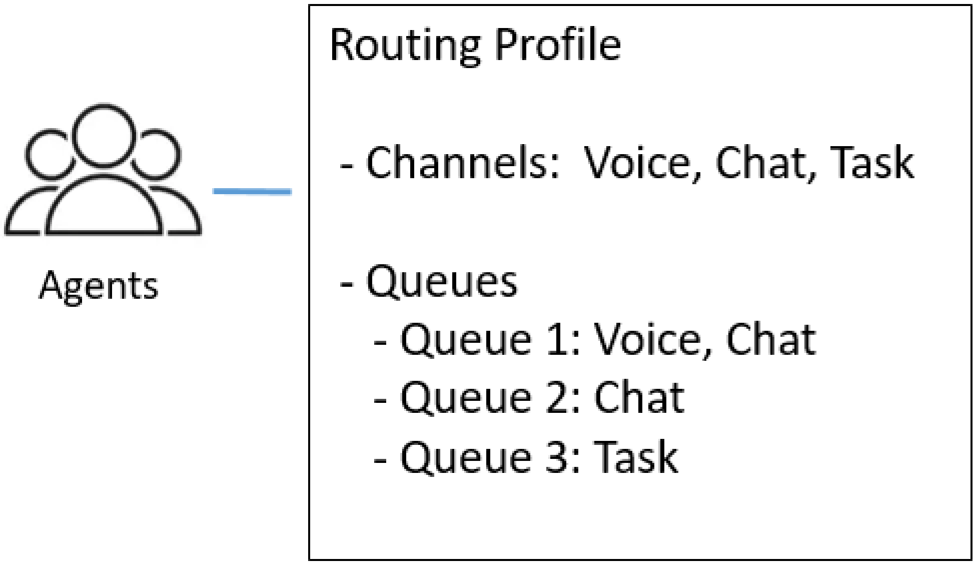
Default routing profile: Basic routing profile

Amazon Connect includes a default routing profile named **Basic routing profile**. Along with the default contact flows (p. 297) and default queue (named **BasicQueue**), it powers your contact center so you don't need to do any customization. This is what enables you to get started quickly.

Routing Profiles Link Queues and Agents

When you create a routing profile, you specify:

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



Queues: standard and agent

There are two types of queues:

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

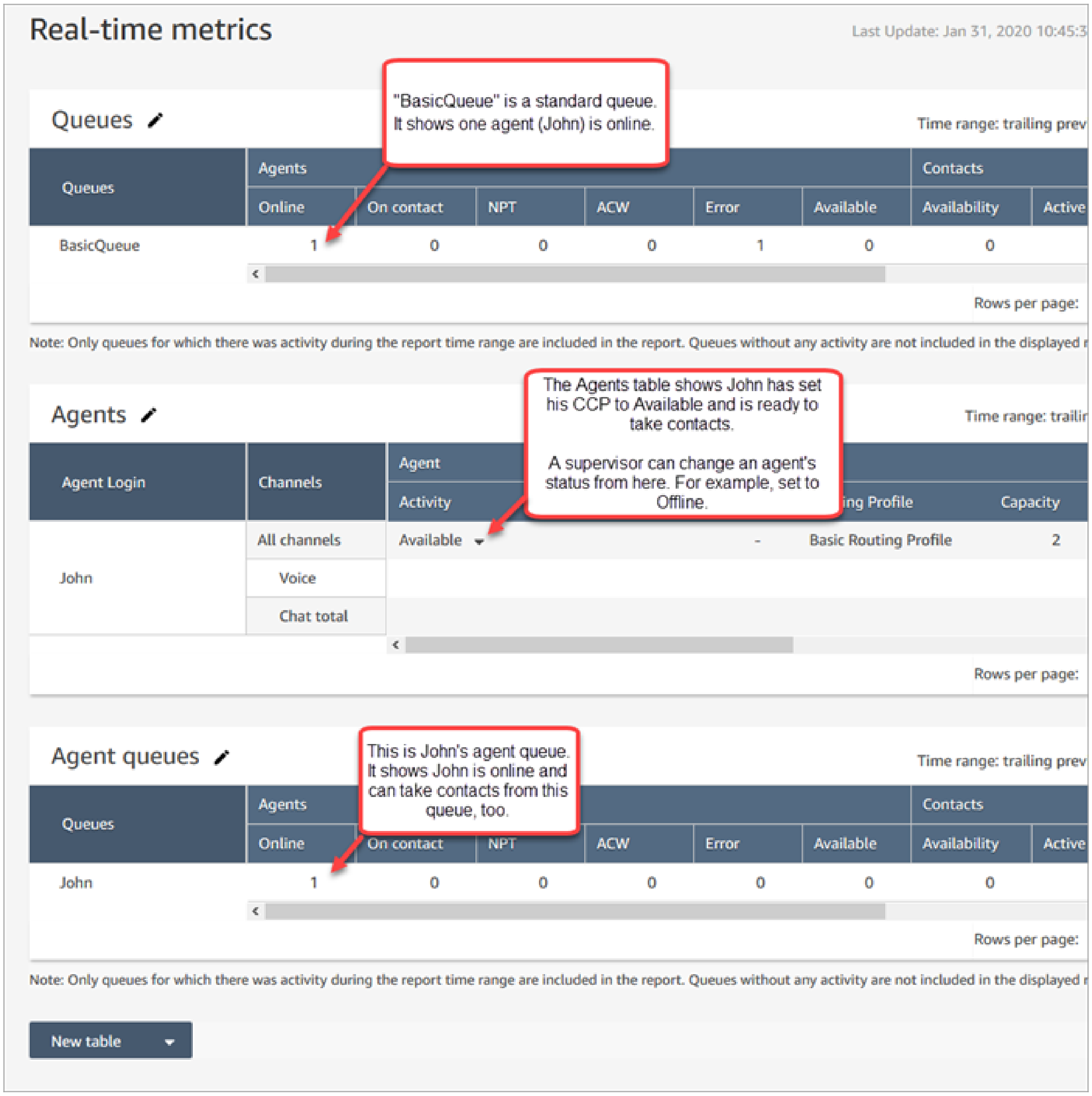
  Contacts are only routed to agent queues when explicitly sent there as part of a contact flow. For example, you might route contacts to a specific agent who's responsible for certain customer issues, such as billing or premium support. Or you might use agent queues to route to an agent's voice-mail.

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

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

Queues in metrics reports

In a real-time metrics report (p. 916), you can monitor how many contacts are in standard queues and agent queues. The following image shows a sample real-time metrics Queues report where an Agents table and Agents queues table have been added.



Real-time metrics

Last Update: Jan 31, 2020 10:45:3

"BasicQueue" is a standard queue. It shows one agent (John) is online.

Queues

Time range: trailing prev

Queues	Agents						Contacts	
	Online	On contact	NPT	ACW	Error	Available	Availability	Active
BasicQueue	1	0	0	0	1	0	0	

Rows per page:

Note: Only queues for which there was activity during the report time range are included in the report. Queues without any activity are not included in the displayed r

The Agents table shows John has set his CCP to Available and is ready to take contacts.

A supervisor can change an agent's status from here. For example, set to Offline.

Agents

Time range: trailir

Agent Login	Channels	Agent				
		Activity			ing Profile	Capacity
John	All channels	Available		-	Basic Routing Profile	2
	Voice					
	Chat total					

Rows per page:

This is John's agent queue. It shows John is online and can take contacts from this queue, too.

Agent queues

Time range: trailing prev

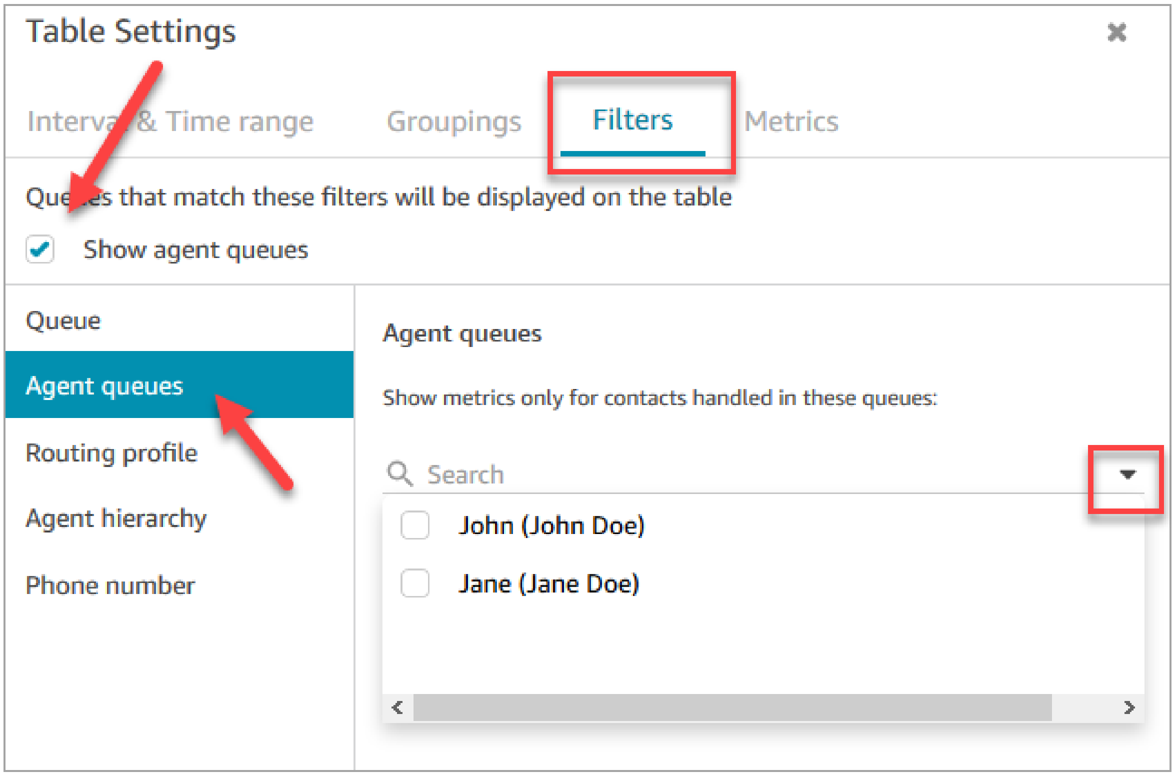
Queues	Agents						Contacts	
	Online	On contact	NPT	ACW	Error	Available	Availability	Active
John	1	0	0	0	0	0	0	

Rows per page:

Note: Only queues for which there was activity during the report time range are included in the report. Queues without any activity are not included in the displayed r

When an agent gets a contact from a standard queue, the contact never appears in the agent queue. It just goes directly to the agent.

In a historical metrics report (p. 938), by default agent queues don't appear in a Queues table. To show them, choose the **Settings** icon, then choose **Show agent queues**.



Queues that match these filters will be displayed on the table

☑ Show agent queues

Agent queues

Show metrics only for contacts handled in these queues:

□ John (John Doe)

□ Jane (Jane Doe)

Tip

The metrics APIs don't support agent queues.

Default queue: BasicQueue

Amazon Connect includes a default queue named **BasicQueue**. Along with the default contact flows (p. 297) and default routing profile (named **Basic routing profile**), it powers your contact center so you don't need to do any customization. This is what enables you to get started quickly.

Queues: priority and delay

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

Example 1: Different priority but same delay

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

Queue	Priority	Delay (in seconds)
Sales	1	0
Support	2	0

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

Example 2: Same priority but different delay

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

Queue	Priority	Delay (in seconds)
Sales	1	0
Support	1	30

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

Example 3: Different Priorities and Delays

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

Queue	Priority	Delay (in seconds)
Tier 1 Support	1	0
Tier 2 Support	1	0
Tier 3 Support	2	20
Tier 4 Support	3	80

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

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

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

Example 4: Same Priority and Delay

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

Queue	Priority	Delay (in seconds)
Sales	1	0

Queue	Priority	Delay (in seconds)
Support	1	0

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

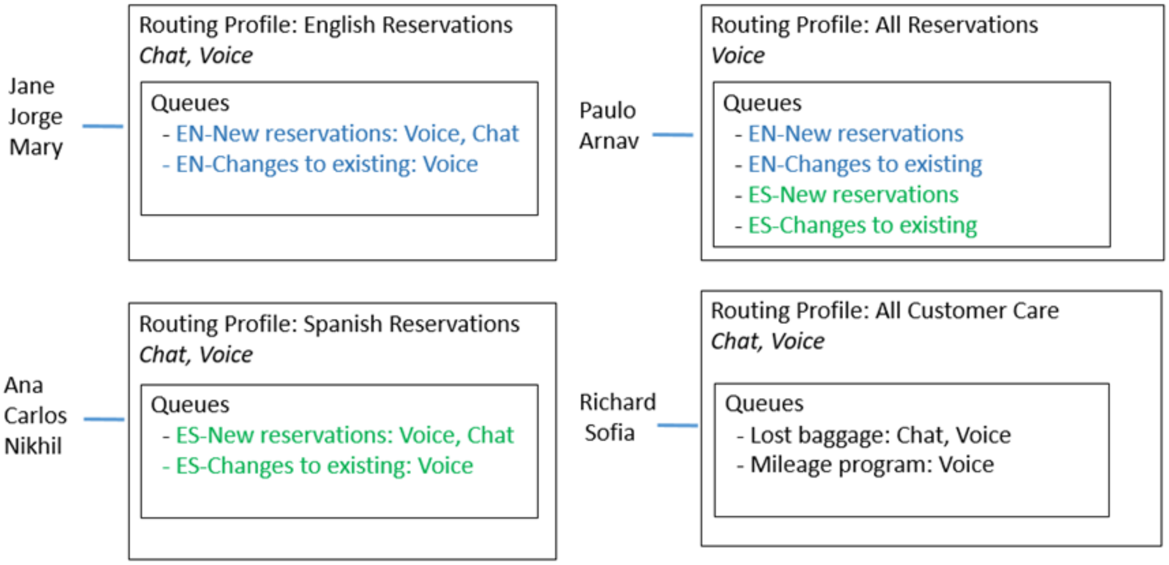
Queue-based routing

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

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

The following illustration shows you can:

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


Jane
Jorge
Mary
Routing Profile: English Reservations
Chat, Voice
Queues
- EN-New reservations: Voice, Chat
- EN-Changes to existing: Voice
Paulo
Arnav
Routing Profile: All Reservations
Voice
Queues
- EN-New reservations
- EN-Changes to existing
- ES-New reservations
- ES-Changes to existing
Ana
Carlos
Nikhil
Routing Profile: Spanish Reservations
Chat, Voice
Queues
- ES-New reservations: Voice, Chat
- ES-Changes to existing: Voice
Richard
Sofia
Routing Profile: All Customer Care
Chat, Voice
Queues
- Lost baggage: Chat, Voice
- Mileage program: Voice

For an overview of the steps to set up queue-based routing, see Set up queue-based routing (p. 230).

Channels and concurrency

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

Suppose an agent is configured in their routing profile for voice, up to 10 chats, and up to 10 tasks. When the agent logs in, they can be routed a chat, task, or voice call. However, once they are on a voice call, no more voice calls, chats, or tasks are routed to them until they finish the call.

If the agent accepts a chat first, up to 10 chats will be routed to them, but no voice calls or tasks. Once they are done with the chats, they're available for the next contact, which can be voice, chat, or tasks. To learn more, see How routing works (p. 221).

To learn more about what the agent experiences in the Contact Control Panel when handling multiple chats, see Chat with contacts (p. 1148).

Contact flows

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

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

Default contact flows

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

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

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

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

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

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

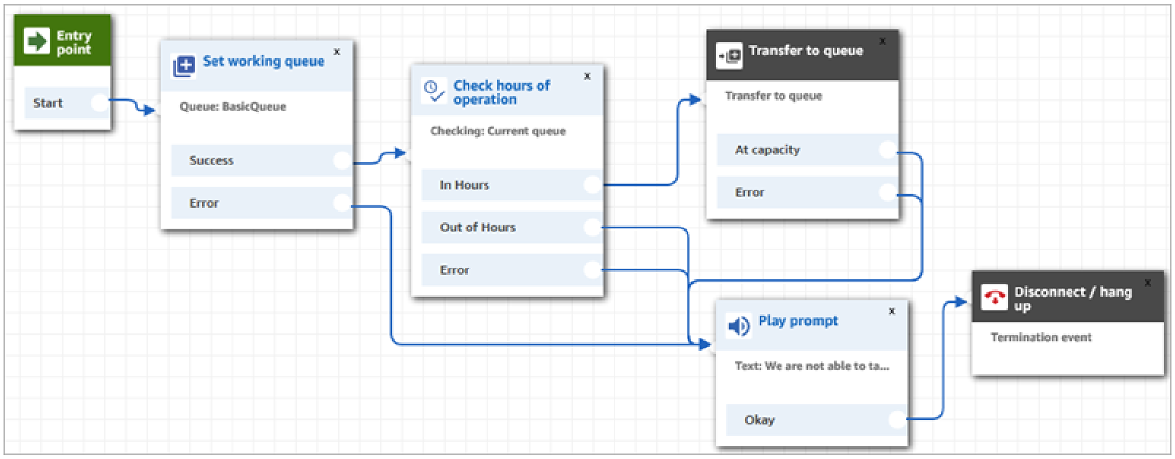
For a list of all the default contact flows and what they do, see Default contact flows (p. 297).

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. 317).

Sample contact flows

To see how to put contact blocks together to create different flows, see Sample contact flows (p. 308).

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, Lambda, chat, Amazon Lex, and the Contact Control Panel (CCP).

We also recommend reviewing Security Best Practices for Amazon Connect (p. 1132).

Contact flows

- Use consistent attribute naming conventions across all AWS services. Use camel case for yourAttributeNames to avoid confusion when passing and referencing variables.
- Use standard naming conventions for attribute names. Don't use spaces or special characters that could impact downstream reporting processes such as AWS Glue crawlers.
- Create modular contact flows. Make the flows as small as possible, and then combine modular flows into an end-to-end contact experience. This helps to keep your flows manageable, and you won't require numerous regression testing cycles.
- When you set **User Defined** or **External** values in dynamic attribute fields, use only alphanumeric characters (A-Z, 0–9) and periods. No other characters are allowed.
- Ensure all error branches are routed to a block that effectively handles the error or terminates the contact.
- Use a **Set logging behavior** block to enable or disable logging for segments of the contact flow where sensitive information is collected and can't be stored in CloudWatch.
- Use **Set recording behavior** block in your contact flow to disable and enable recordings according to your use case. Keep in mind that Amazon Connect records conversations with agents only. It doesn't record IVR interactions.
- Ensure that attributes used in the flow are set and referenced correctly. If there are periods prepended to the attribute names, you are likely using JSONPath ($.) format while also selecting a variable type from the pick list. For example:, using:
  - **Save text as attribute** and value `$.External.variableName` works as expected.
  - `Use attribute` and value `variableName` works as expected.
  - **Use attribute** and `$.External.variableName` results in a prepended period.
- Before transferring a call to agent and putting that call in a queue, ensure that **Check hours of operation** and **Check staffing** blocks are used. They verify that the call is within working hours and that agents are staffed to service.
- Ensure that callbacks are offered before and after queue transfer by using **Check queue status** blocks. Include a condition for **Queue capacity** that is greater than X, where X is a number representing your expected queue capacity.
  - If queue capacity exceeds the expected capacity, use a **Get Customer Input** block to offer a callback. This retains the caller's position in the queue and calls them back when an agent is available.
  - In the **Set callback number** block, choose the number to be used to call the customer back in the CCP. Use **System** and **Customer Number** or a new number, collected by a **Store Customer Input** block, using **System** and **Stored customer input**.
  - Finally, add a **Transfer to queue** block. Configure it to **Transfer to callback queue** and configure the callback options to fit your specific use case.
- Use a **Loop prompts** block in your Customer queue flow to interrupt with a queued callback and external transfer option at regular intervals.
- Ensure that all countries referenced in external transfers or used for outbound dialing are added to the service quota for your account/instance.

- Ensure that all numbers referenced in external transfers are in E.164 format. Drop the national trunk prefix that you use when calling locally. This prefix would be the leading 0 for most of Europe, 1 for the US. The prefix is replaced by the country code. For example, the UK mobile number **07911 123456** in E.164 format is **+44 7911 123456 (tel:+447911123456)**.
- Ensure that there are no infinite loops in the 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.

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. 540).
- For voice, some words are best spelled phonetically to get the correct pronunciation, such as last names. If this is the case with your scenario, include it in the design of your bot. Or, you can keep the voice and chat bots separate.
- Tell agents about the bot. When a contact is connected to the agent, the agent sees the entire transcript in their window. The transcript includes text from both the customer and the bot.

Contact Control Panel

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

  For instructions, see this Google Chrome Help article.

Tutorials: An introduction to Amazon Connect

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

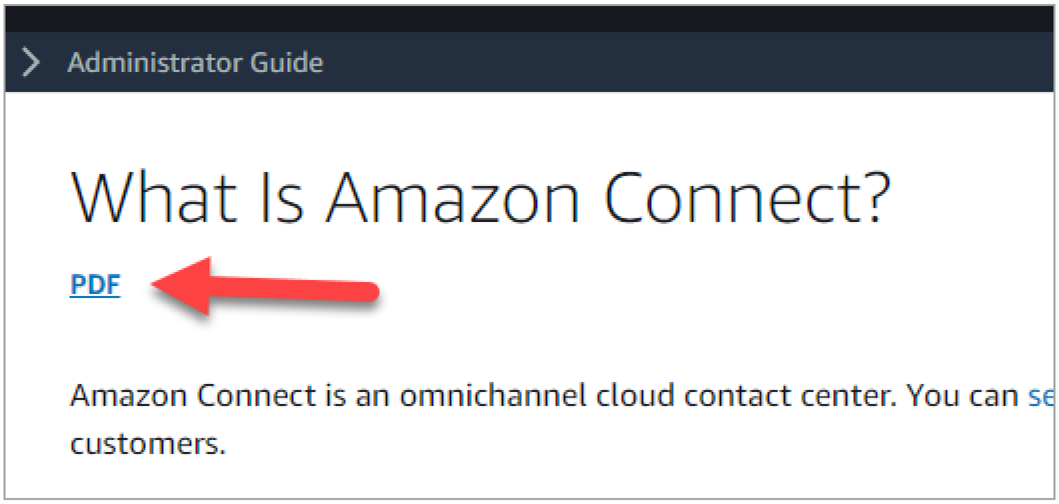
These tutorials are suitable for both knowledge workers and developers.

Prerequisite

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

Print the tutorials

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



What Is Amazon Connect?

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

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

Contents

Tutorial 1: Set up your Amazon Connect instance

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

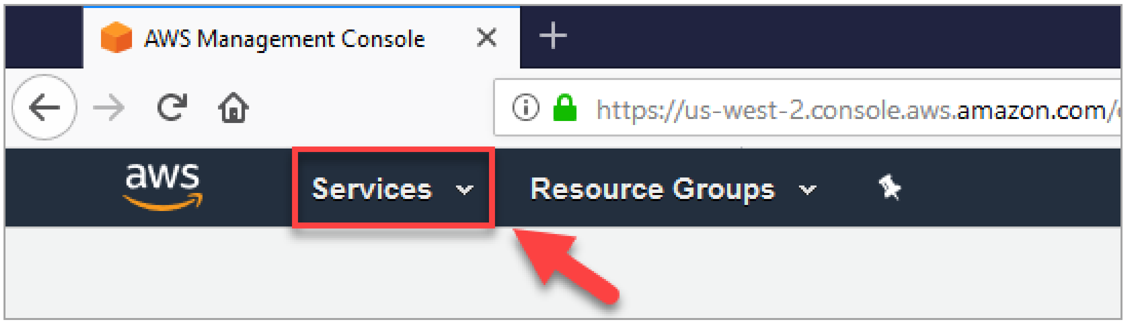
In this tutorial, you open Amazon Connect, create an instance of Amazon Connect, and claim a phone number that you can use for testing.

Contents

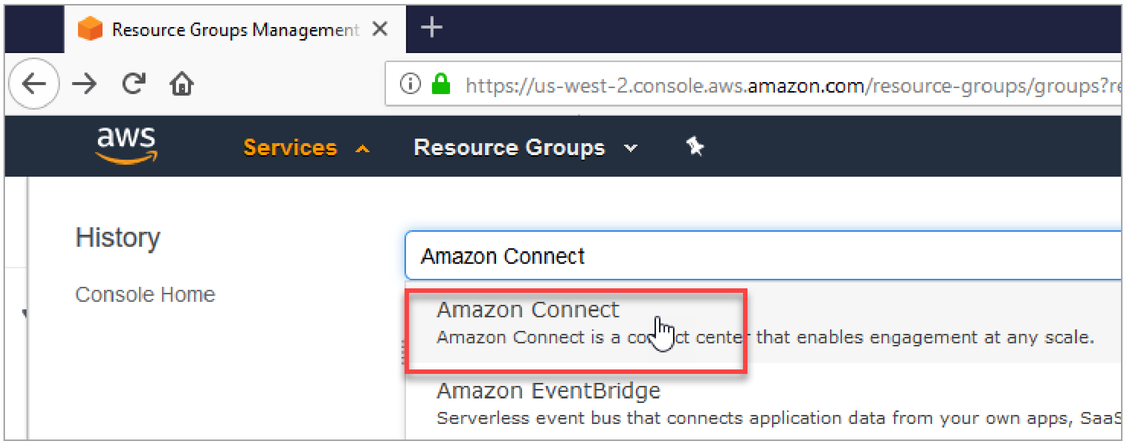
Step 1: Launch Amazon Connect

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

1. Log in to the AWS Management Console (https://console.aws.amazon.com/console) using your AWS account.
2. In the AWS Management Console, at the top of the page, choose the **Services** drop-down menu.

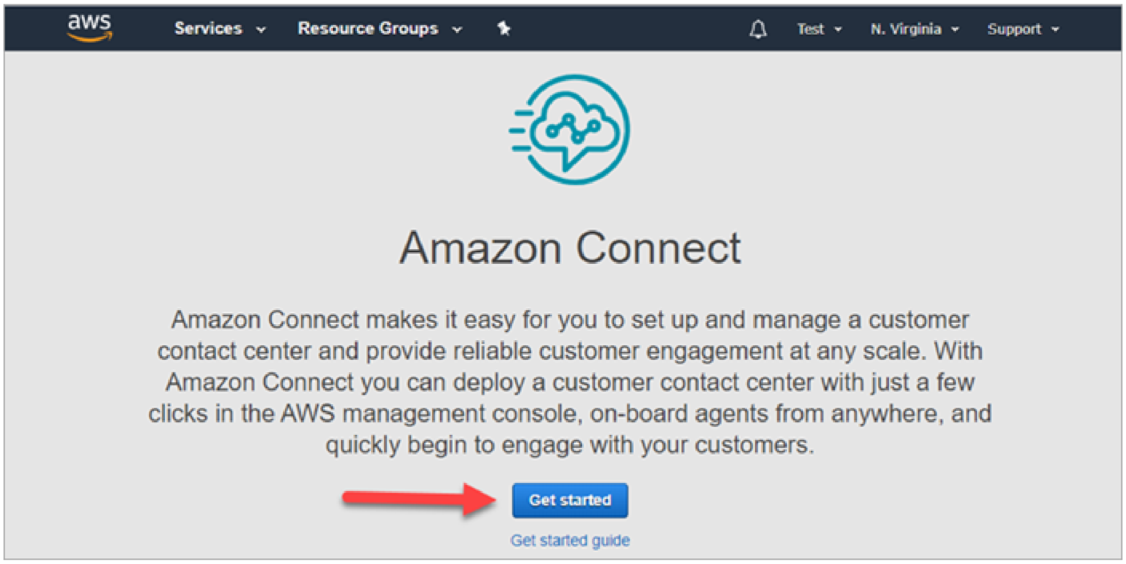


3. In the search box, type **Amazon Connect**.


Resource Groups Management
https://us-west-2.console.aws.amazon.com/resource-groups/groups?r
aws
Services
Resource Groups
History
Console Home
Amazon Connect
Amazon Connect
Amazon Connect is a contact center that enables engagement at any scale.
Amazon EventBridge
Serverless event bus that connects application data from your own apps, SaaS

4. Choose **Amazon Connect**.

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



Amazon Connect

Amazon Connect makes it easy for you to set up and manage a customer contact center and provide reliable customer engagement at any scale. With Amazon Connect you can deploy a customer contact center with just a few clicks in the AWS management console, on-board agents from anywhere, and quickly begin to engage with your customers.

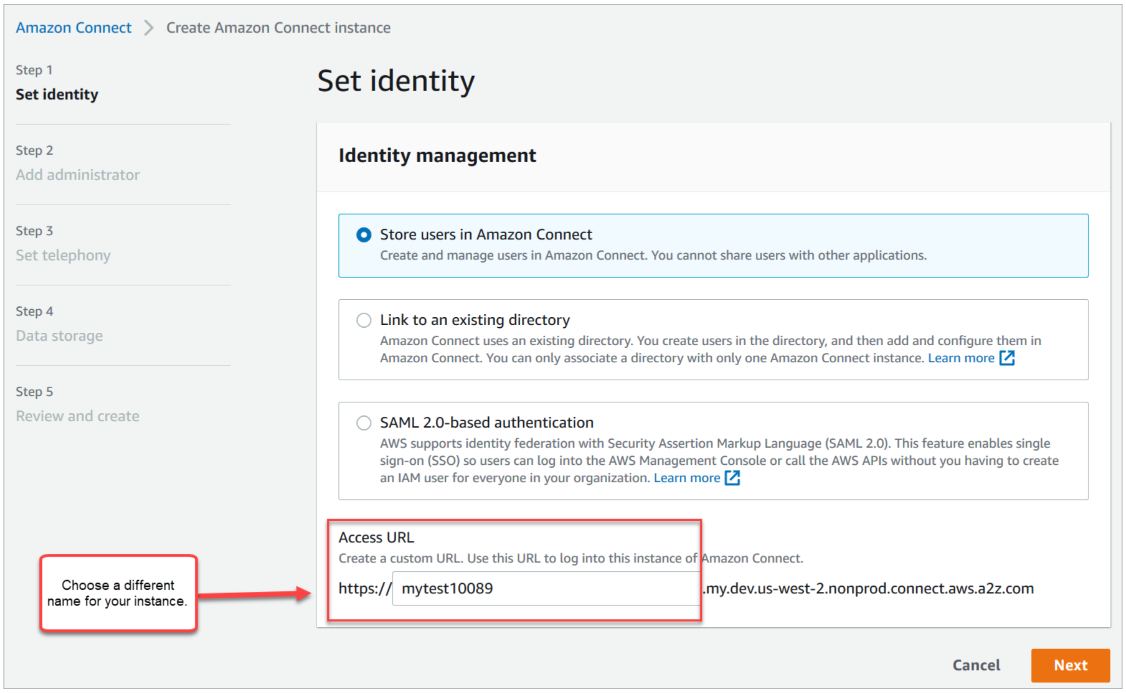
5. Choose **Get started**.

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

Go to Step 2: Create an instance (p. 33).

Step 2: Create an instance

1. On the **Amazon Connect virtual contact center instances** page, choose **Add an instance**.
2. Type a unique name for your instance. For example, the following image shows **mytest10089** as a name. Choose a different name for your instance. Then choose **Next**.



Set identity

Identity management

● Store users in Amazon Connect
Create and manage users in Amazon Connect. You cannot share users with other applications.

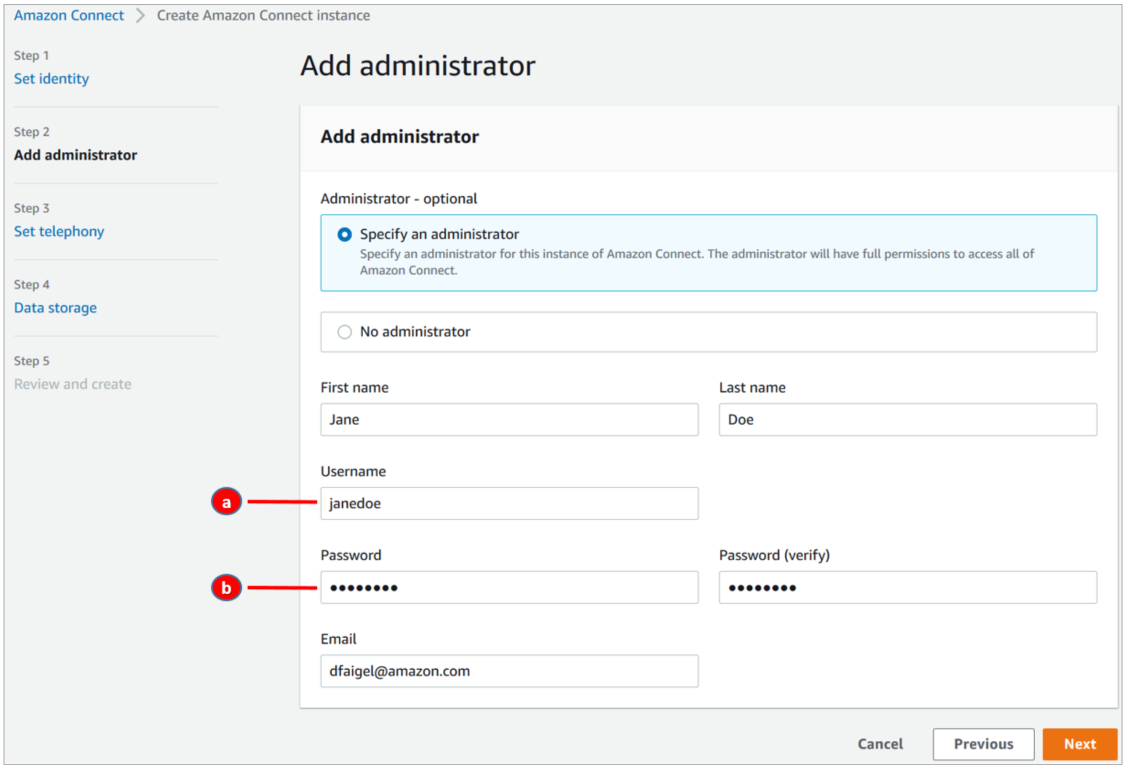
○ Link to an existing directory
Amazon Connect uses an existing directory. You create users in the directory, and then add and configure them in Amazon Connect. You can only associate a directory with only one Amazon Connect instance. Learn more

○ SAML 2.0-based authentication
AWS supports identity federation with Security Assertion Markup Language (SAML 2.0). This feature enables single sign-on (SSO) so users can log into the AWS Management Console or call the AWS APIs without you having to create an IAM user for everyone in your organization. Learn more

Access URL
Create a custom URL. Use this URL to log into this instance of Amazon Connect.
https:// mytest10089 .my.dev.us-west-2.nonprod.connect.aws.a2z.com

Choose a different name for your instance.

3. On the **Add administrator** page, add a new administrator account for Amazon Connect. Use this account to log in to your instance later using the unique access URL. Choose **Next**.



Add administrator

Add administrator

Administrator - optional

● Specify an administrator
Specify an administrator for this instance of Amazon Connect. The administrator will have full permissions to access all of Amazon Connect.

○ No administrator

First name: Jane

Last name: Doe

Username: janedoe

Password: ••••••••

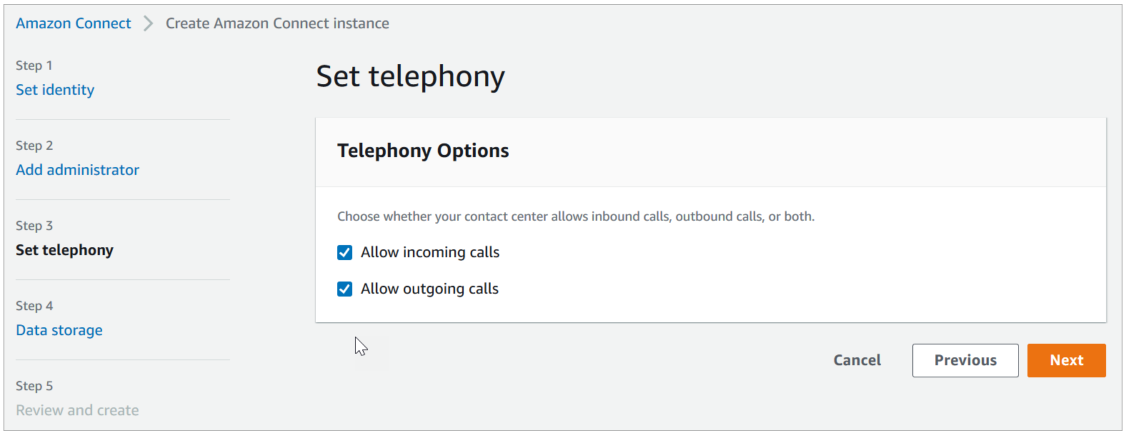
Password (verify): ••••••••

Email: dfaigel@amazon.com

   a. The user name will be your Amazon Connect login. It's case sensitive.

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

4. On the **Telephony Options** page, accept the default settings and choose **Next**.



Set telephony

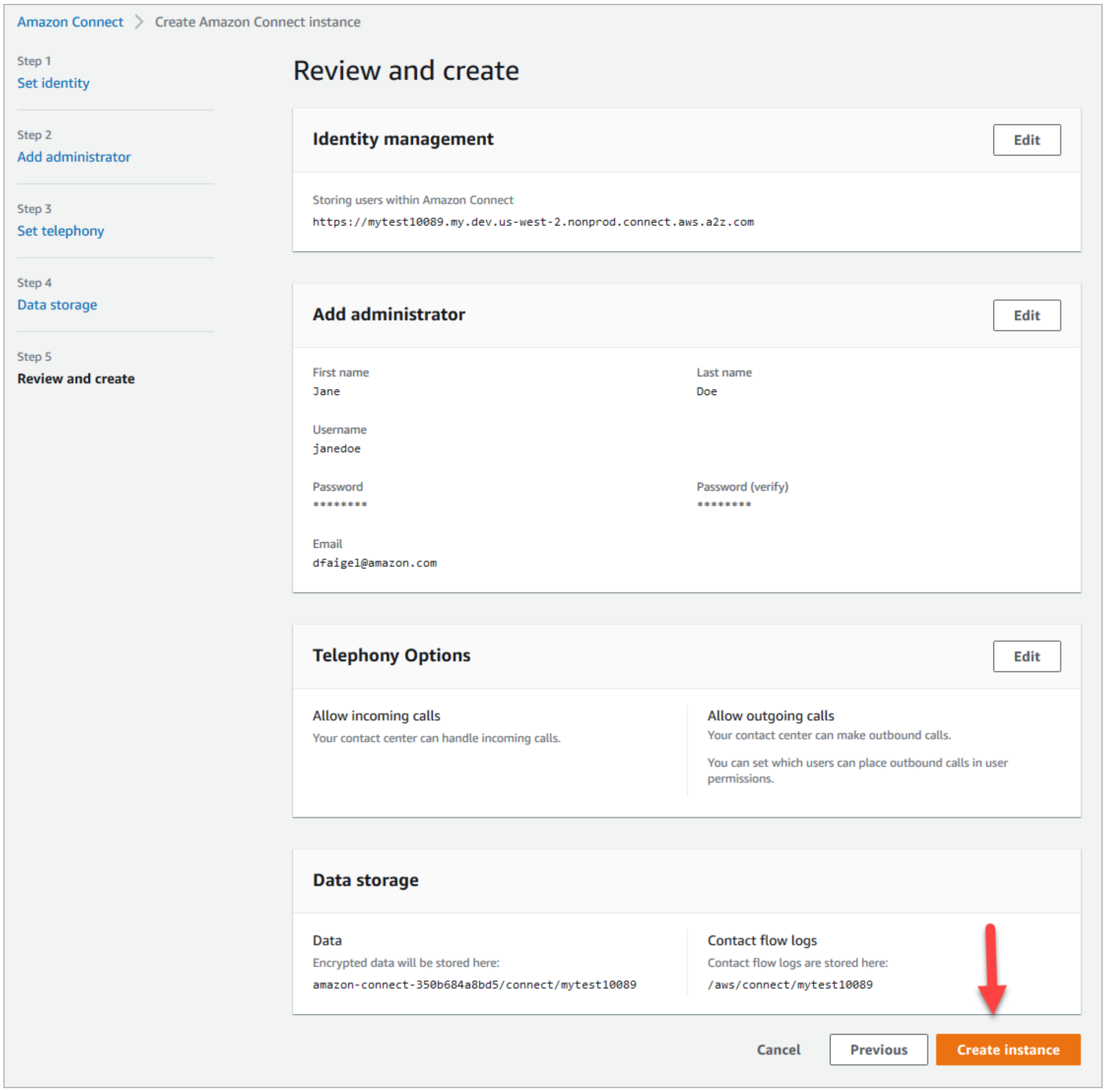
Telephony Options

Choose whether your contact center allows inbound calls, outbound calls, or both.

☑ Allow incoming calls

☑ Allow outgoing calls

5. On the **Review and create** page, choose **Create instance**.



Amazon Connect > Create Amazon Connect instance

Step 1
Set identity

Step 2
Add administrator

Step 3
Set telephony

Step 4
Data storage

Step 5
Review and create

Review and create

Identity management Edit

Storing users within Amazon Connect
`https://mytest10089.my.dev.us-west-2.nonprod.connect.aws.a2z.com`

Add administrator Edit

First name: Jane
Last name: Doe

Username: janedoe

Password: ********
Password (verify): ********

Email: dfaigel@amazon.com

Telephony Options Edit

Allow incoming calls
Your contact center can handle incoming calls.

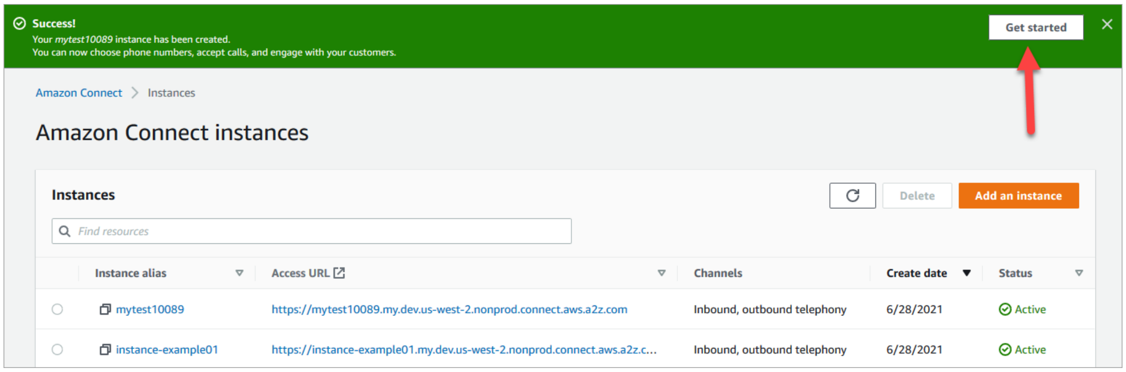
Allow outgoing calls
Your contact center can make outbound calls.
You can set which users can place outbound calls in user permissions.

Data storage

Data
Encrypted data will be stored here:
`amazon-connect-350b684a8bd5/connect/mytest10089`

Contact flow logs
Contact flow logs are stored here:
`/aws/connect/mytest10089`

6. After the instance is created, choose **Get started**.



Success!
Your *mytest10089* instance has been created.
You can now choose phone numbers, accept calls, and engage with your customers.

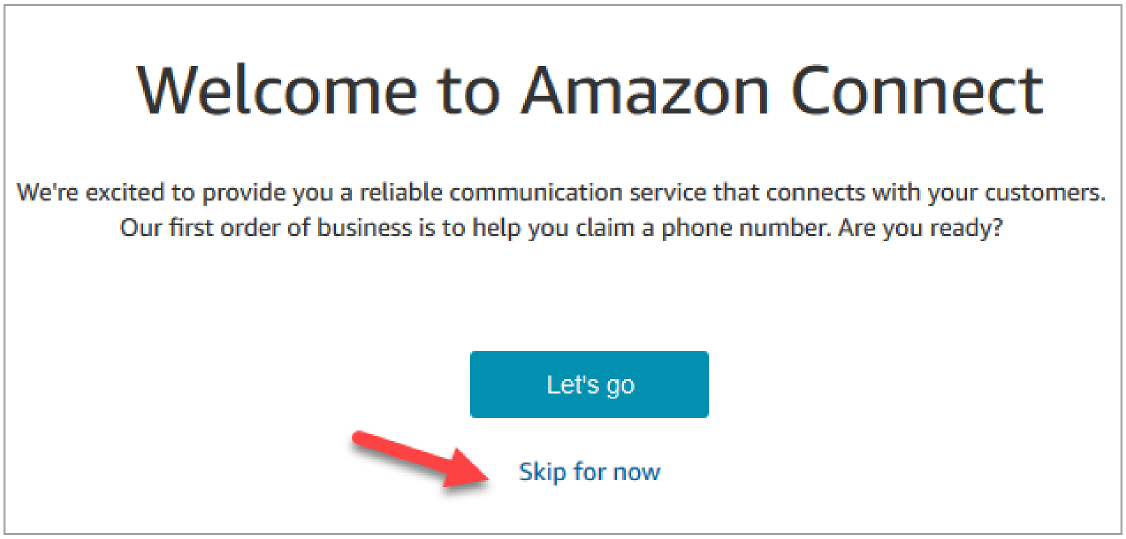
Amazon Connect > Instances

Amazon Connect instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest10089	https://mytest10089.my.dev.us-west-2.nonprod.connect.aws.a2z.com	Inbound, outbound telephony	6/28/2021	✓ Active
○	instance-example01	https://instance-example01.my.dev.us-west-2.nonprod.connect.aws.a2z.c...	Inbound, outbound telephony	6/28/2021	✓ Active

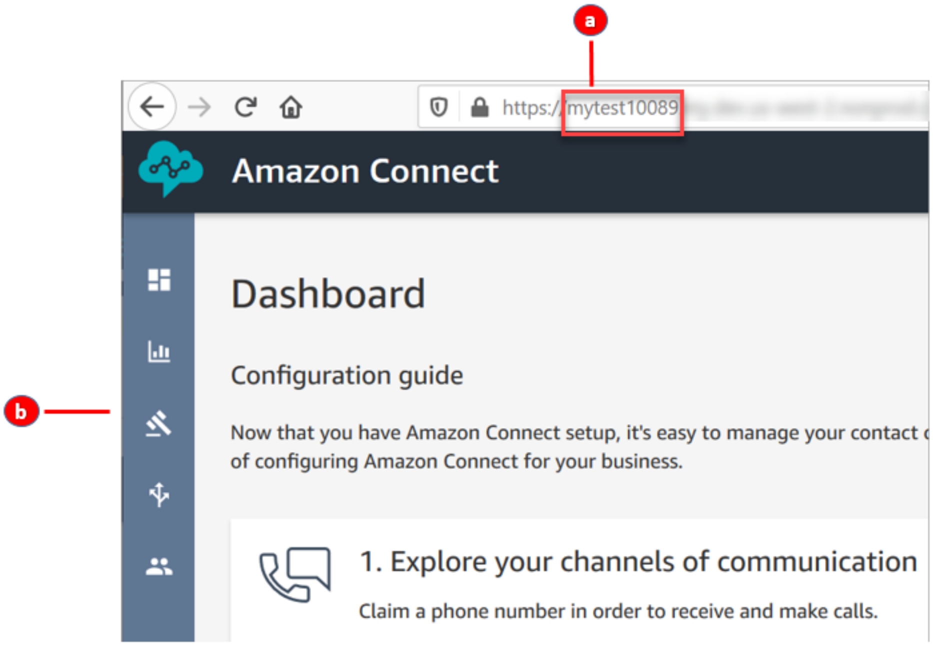
7. On the **Welcome to Amazon Connect** page, choose **Skip for now**.



Welcome to Amazon Connect

We're excited to provide you a reliable communication service that connects with your customers. Our first order of business is to help you claim a phone number. Are you ready?

8. You're now on the Amazon Connect dashboard. On the left is the navigation menu. Your instance name (also called an **alias**) displays in the URL.



Dashboard

Configuration guide

Now that you have Amazon Connect setup, it's easy to manage your contact c
of configuring Amazon Connect for your business.

1. Explore your channels of communication

Claim a phone number in order to receive and make calls.

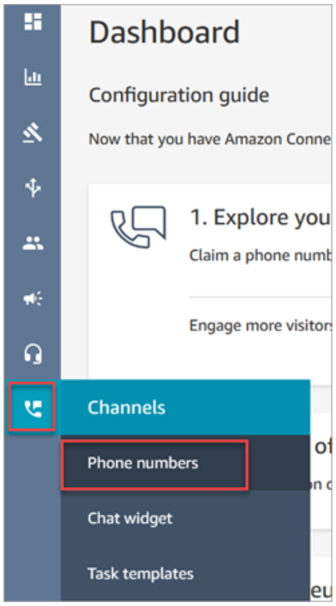
   a. Your instance alias is located in the first part of the URL.
   b. The navigation menu.

Congratulations! You set up your instance and now you're on the Amazon Connect dashboard. Go to Step 3: Claim a phone number (p. 36).

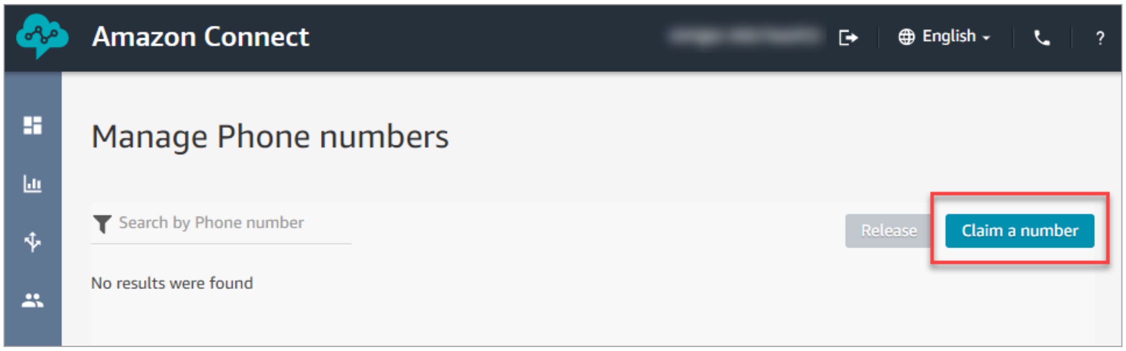
Step 3: Claim a phone number

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

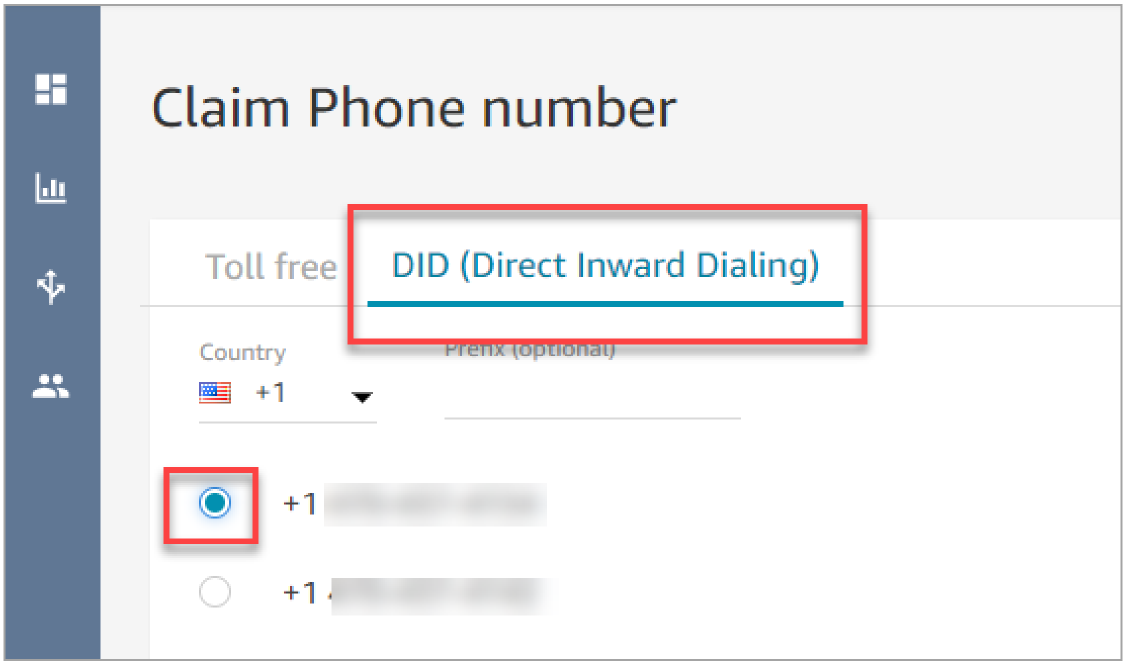
1. On the navigation menu, choose **Channels**, **Phone numbers**.



2. On the right side of the page, choose **Claim a number**.



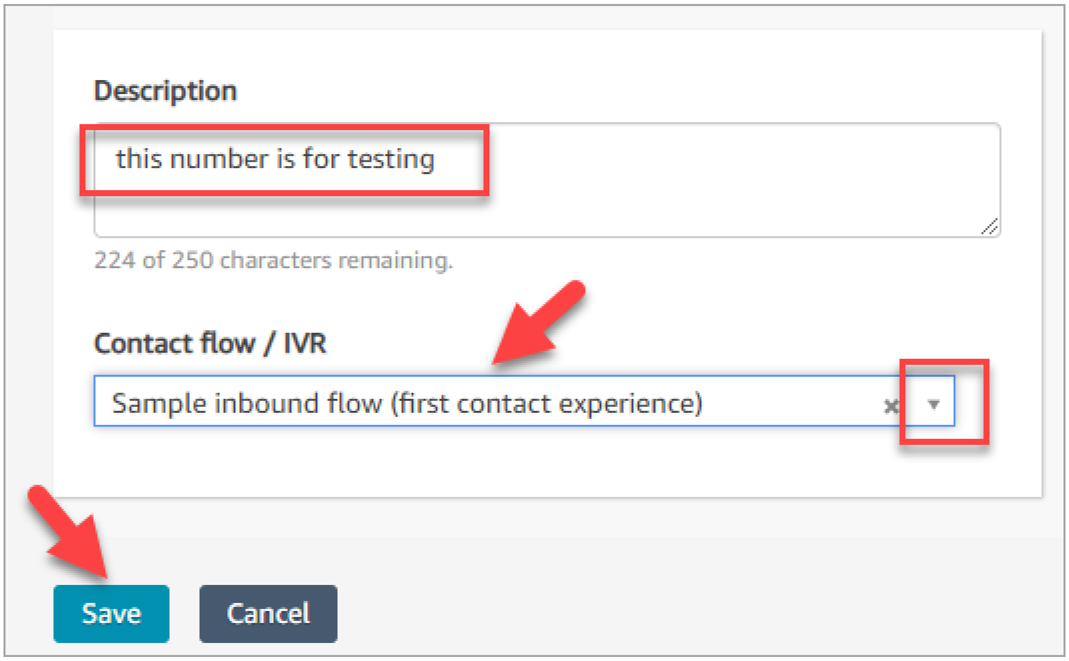
3. Select the **DID (Direct Inward Dialing)** tab. Use the drop-down arrow to choose your country/ region. When numbers are returned, choose one.



● +1 [redacted]

○ +1 [redacted]

4. Write down the phone number. You call it later in this tutorial.
5. In the **Description** box, type this note: **this number is for testing**.



Description: this number is for testing

Contact flow / IVR: Sample inbound flow (first contact experience)

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

Congratulations! You set up your instance and claimed a phone number. Now you're ready to experience how chat and voice work in Amazon Connect. Go to Tutorial 2: Test the sample voice and chat experience (p. 39).

Tutorial 2: Test the sample voice and chat experience

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

This tutorial shows you how to access and use the Contact Control Panel (CCP) (p. 1135). The CCP is a web page that agents use to accept and manage voice and chat contacts.

Prerequisites

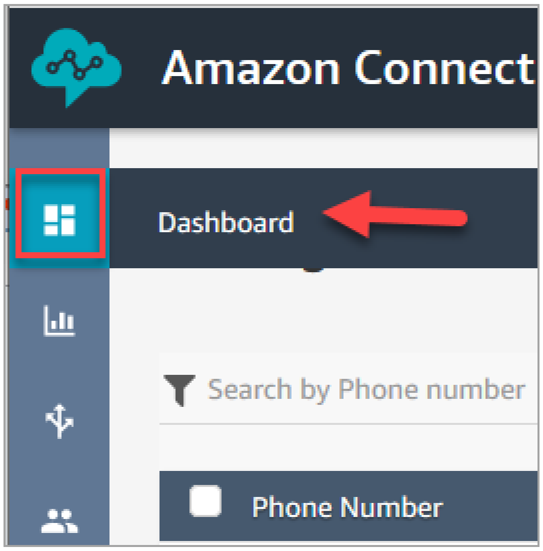
This tutorial is part of a series. If you performed Tutorial 1, you're ready to go. If not, here's what you need:

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

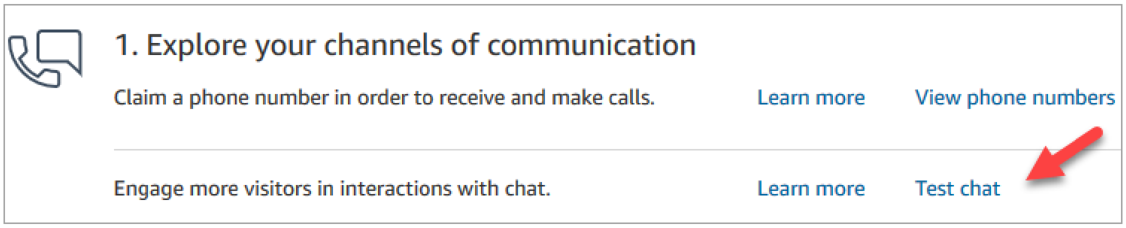
Contents

Step 1: Handle a voice contact

1. On the navigation menu, choose **Dashboard**.



2. On the **Dashboard** page, choose **Test chat**.

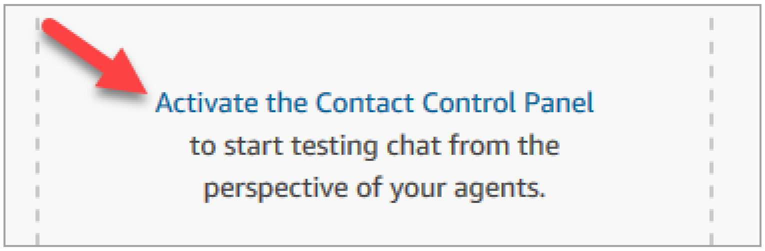


1. Explore your channels of communication

Claim a phone number in order to receive and make calls. Learn more View phone numbers

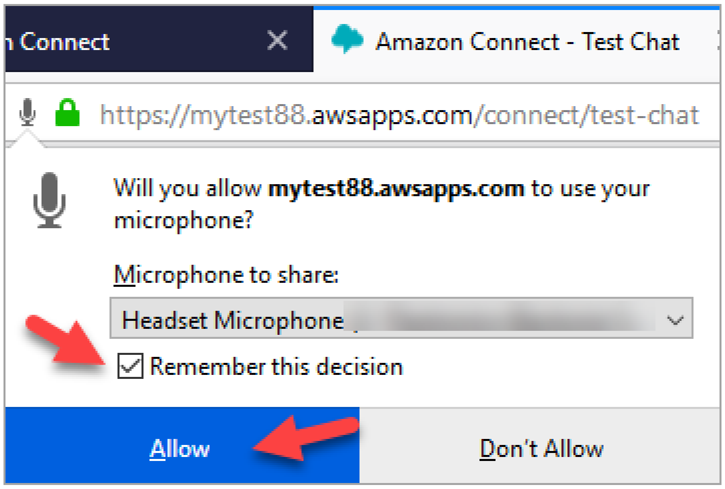
Engage more visitors in interactions with chat. Learn more Test chat

3. Choose **Activate Contact Control Panel**.



Activate the Contact Control Panel to start testing chat from the perspective of your agents.

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



n Connect
Amazon Connect - Test Chat
https://mytest88.awsapps.com/connect/test-chat

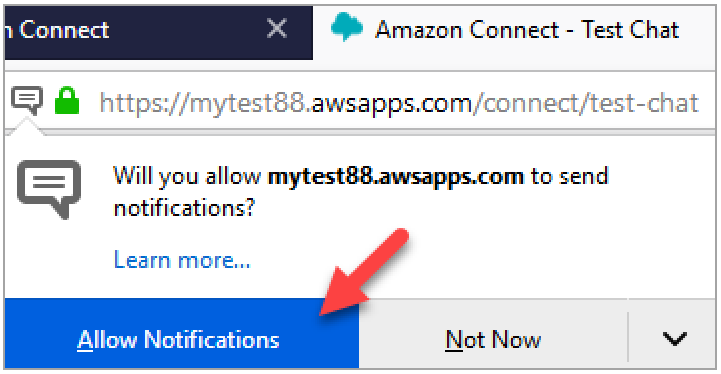
Will you allow **mytest88.awsapps.com** to use your microphone?

Microphone to share:

Headset Microphone

☑ Remember this decision

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

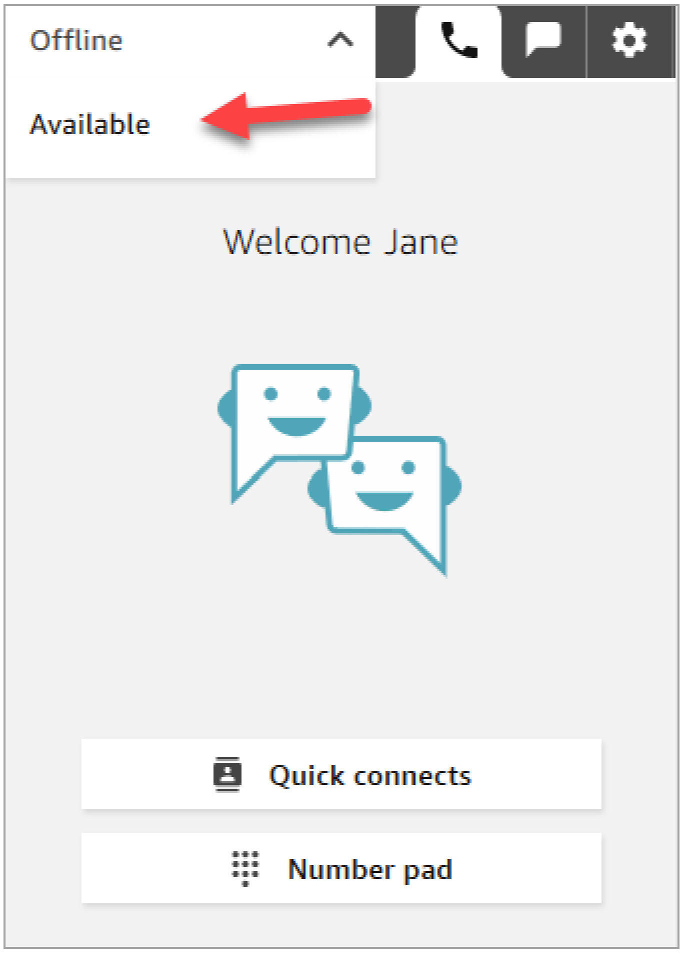


n Connect
Amazon Connect - Test Chat
https://mytest88.awsapps.com/connect/test-chat

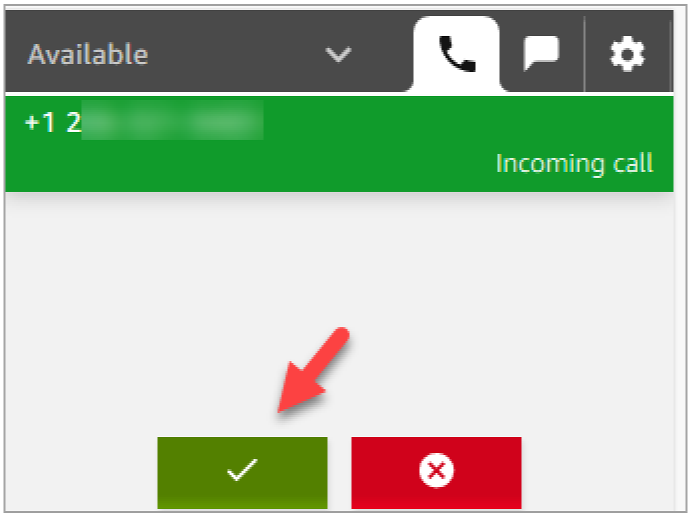
Will you allow **mytest88.awsapps.com** to send notifications?

Learn more...
Allow Notifications
Not Now

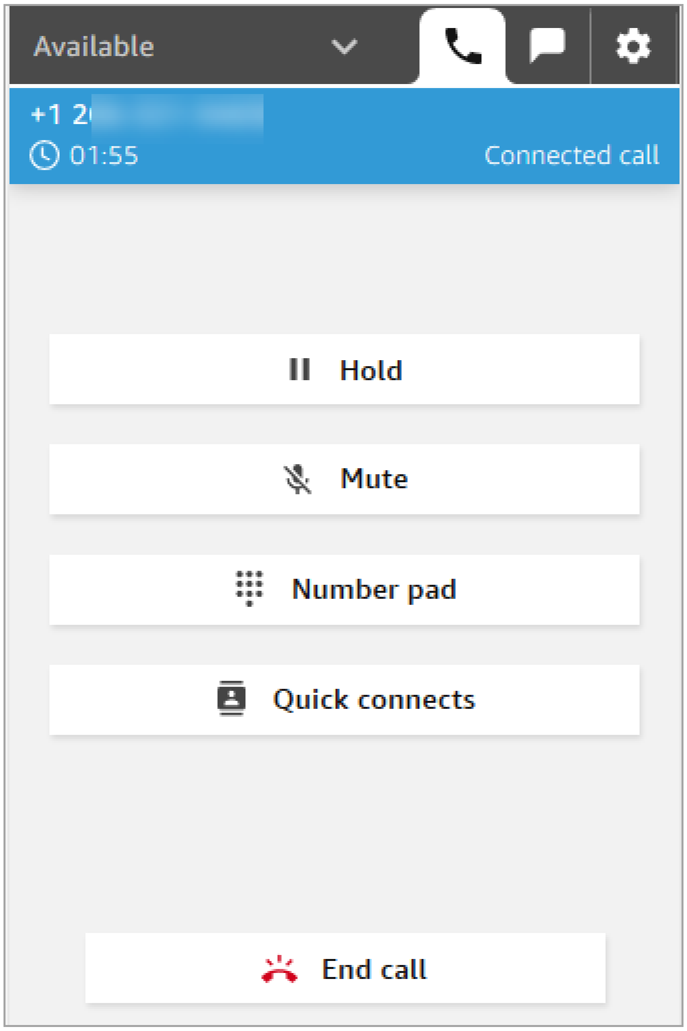
6. In the test CCP, set your status to **Available**.



7. Use your mobile phone to call the phone number that you claimed earlier. If you didn't write down the number, you can find it by going to **Channels**, **Phone numbers**.
8. When your call is joined to Amazon Connect you'll hear "Press 1 to be put in queue for an agent, 2 to ..." This is the Sample inbound flow (p. 309) that Amazon Connect runs by default. You're going to change this later in the tutorial.
9. You can play around with the different options in the Sample inbound contact flow. To connect to an agent, press **1**, **1**, **1**.
10. In the CCP, choose **Accept call**.

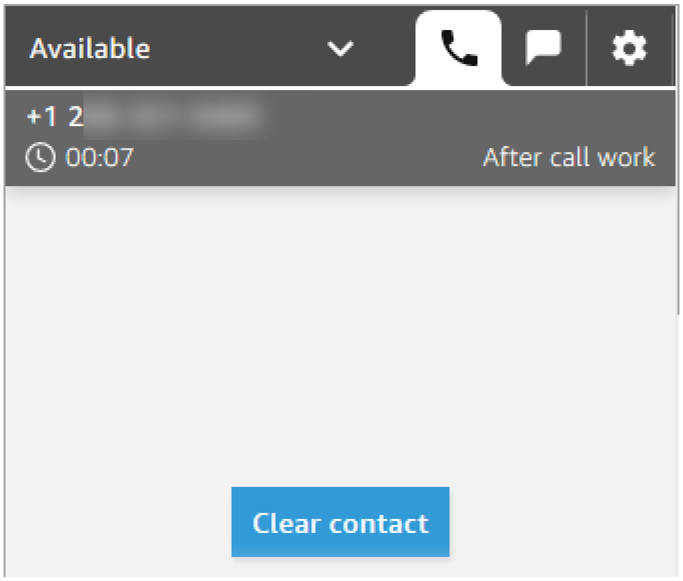


11. You'll see what the CCP looks like when an agent is connected to a customer.



12. Choose **End call**.

Now the contact is in the After Contact Work (ACW) state. This is when the agent might enter some notes about the contact.

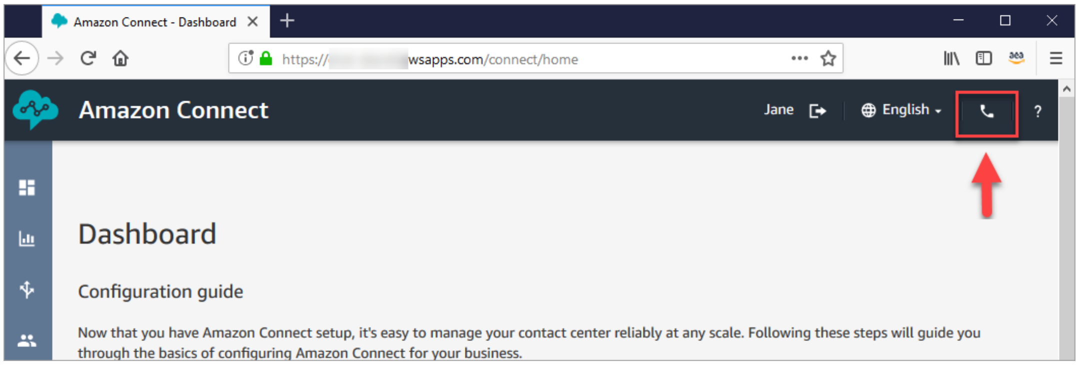


13. Choose **Clear contact**. This frees up the agent to take another incoming contact.

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

Tip

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


Amazon Connect - Dashboard
https://[redacted]wsapps.com/connect/home
Amazon Connect
Jane
English
?

Dashboard

Configuration guide

Now that you have Amazon Connect setup, it's easy to manage your contact center reliably at any scale. Following these steps will guide you through the basics of configuring Amazon Connect for your business.

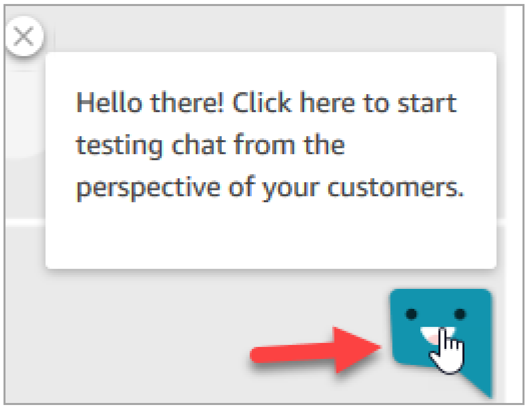
Next step

Go to Step 2: Handle a chat contact (p. 43) to experience how to handle a chat contact.

Step 2: Handle a chat contact

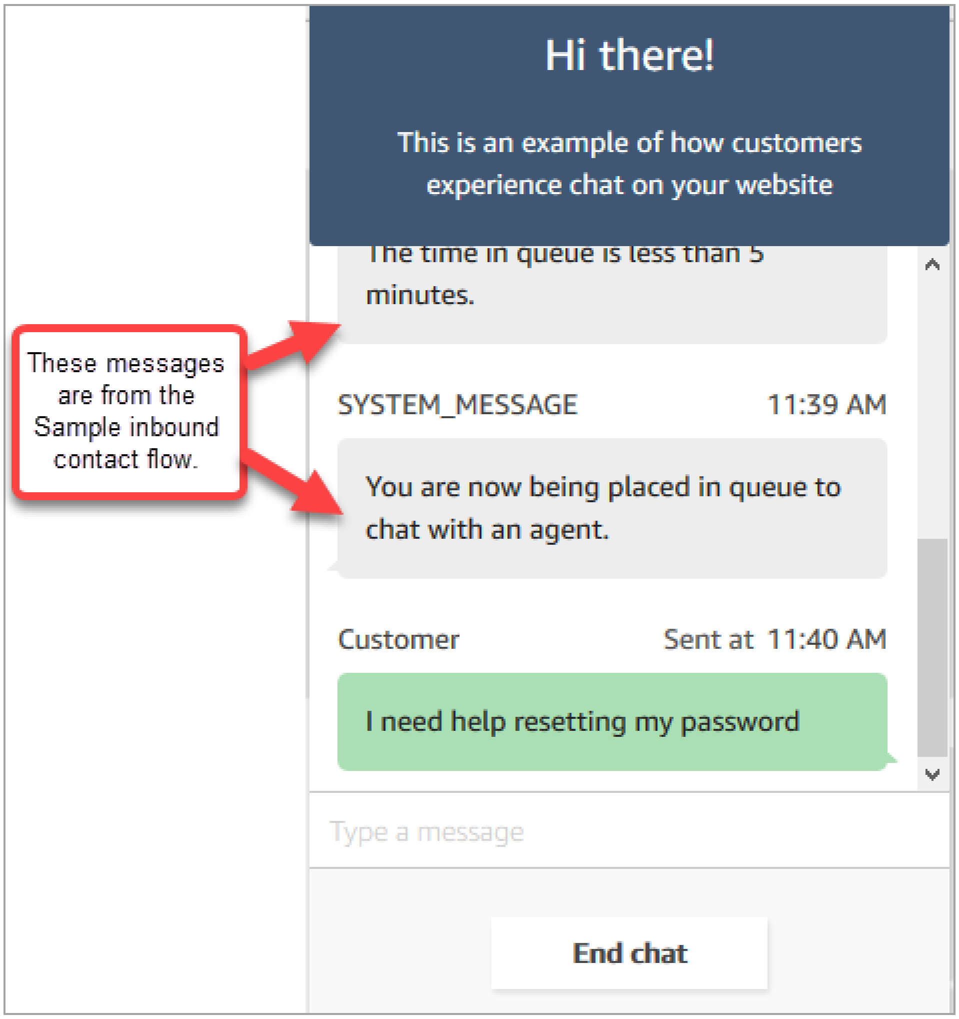
In Step 1, you used the Contact Control Panel (CCP) to manage a voice contact. In this step, you experience how to use the CCP to manage a chat contact.

1. Choose the chat bubble to start a chat.



Hello there! Click here to start testing chat from the perspective of your customers.

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



Hi there!

This is an example of how customers experience chat on your website

The time in queue is less than 5 minutes.

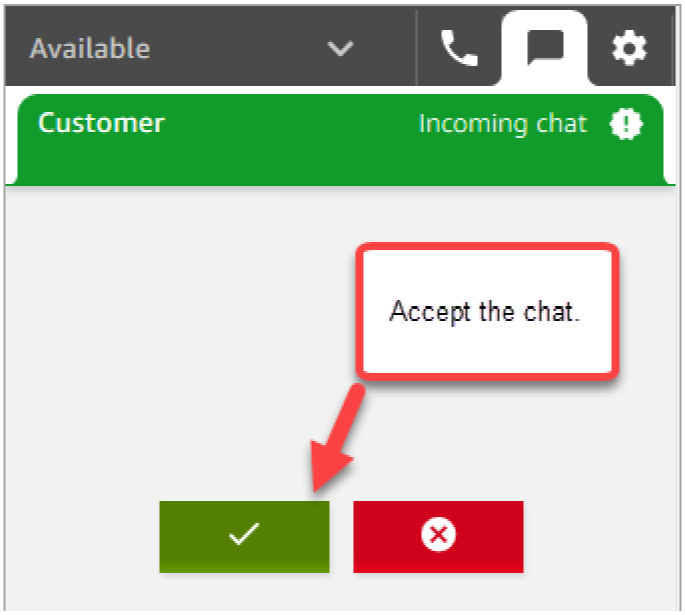
SYSTEM_MESSAGE 11:39 AM

You are now being placed in queue to chat with an agent.

Customer Sent at 11:40 AM

I need help resetting my password

3. In the CCP, accept the incoming chat.



4. Use the CCP to send chat messages to the customer.
5. When you're done chatting, choose **End chat**. Then in the CCP, choose **Close contact**.

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

Next, try Tutorial 3 to set up an IT Help Desk. It shows you how to set up routing, create a contact flow, and then test the custom voice and chat experience. Go to Tutorial 3: Create an IT help desk (p. 45).

Tutorial 3: Create an IT help desk

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

Prerequisite

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

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

Contents

Step 1: Create an Amazon Lex bot

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

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

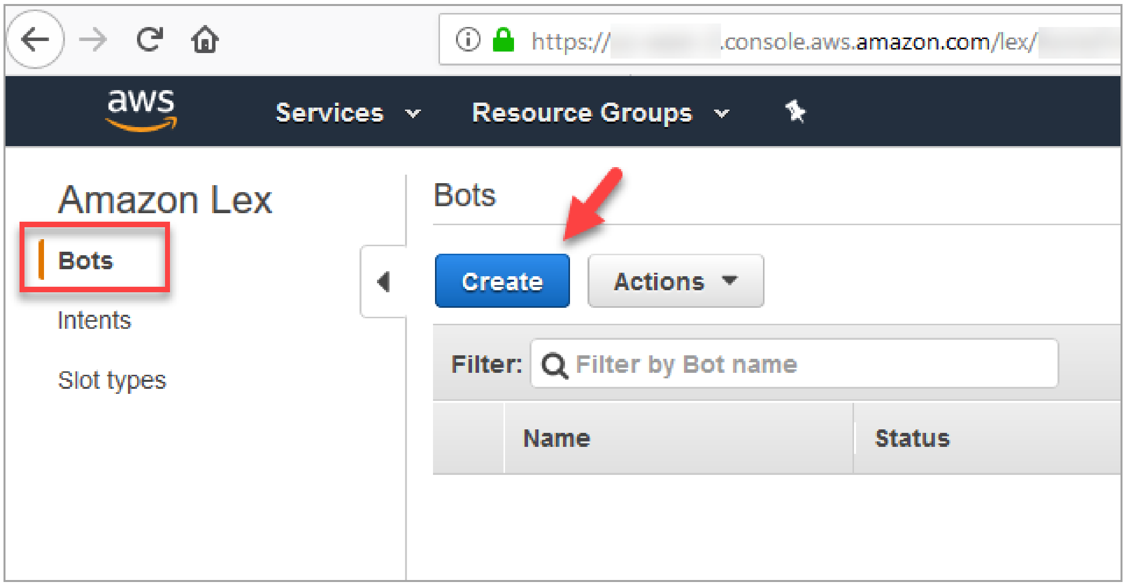
This step has five parts to it.

Contents

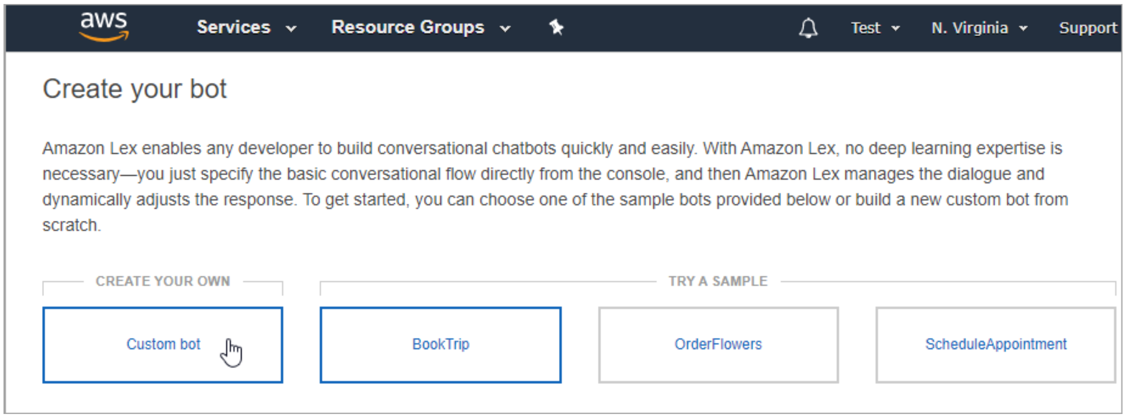
Part 1: Create an Amazon Lex bot

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

1. Choose the following link to open the Amazon Lex console, or enter the URL in your web browser: **https://console.aws.amazon.com/lex/**.
2. If this is the first time you've created Amazon Lex bot, choose **Get Started**. Otherwise, you are already in the Amazon Lex dashboard.



3. Choose **Custom bot**.



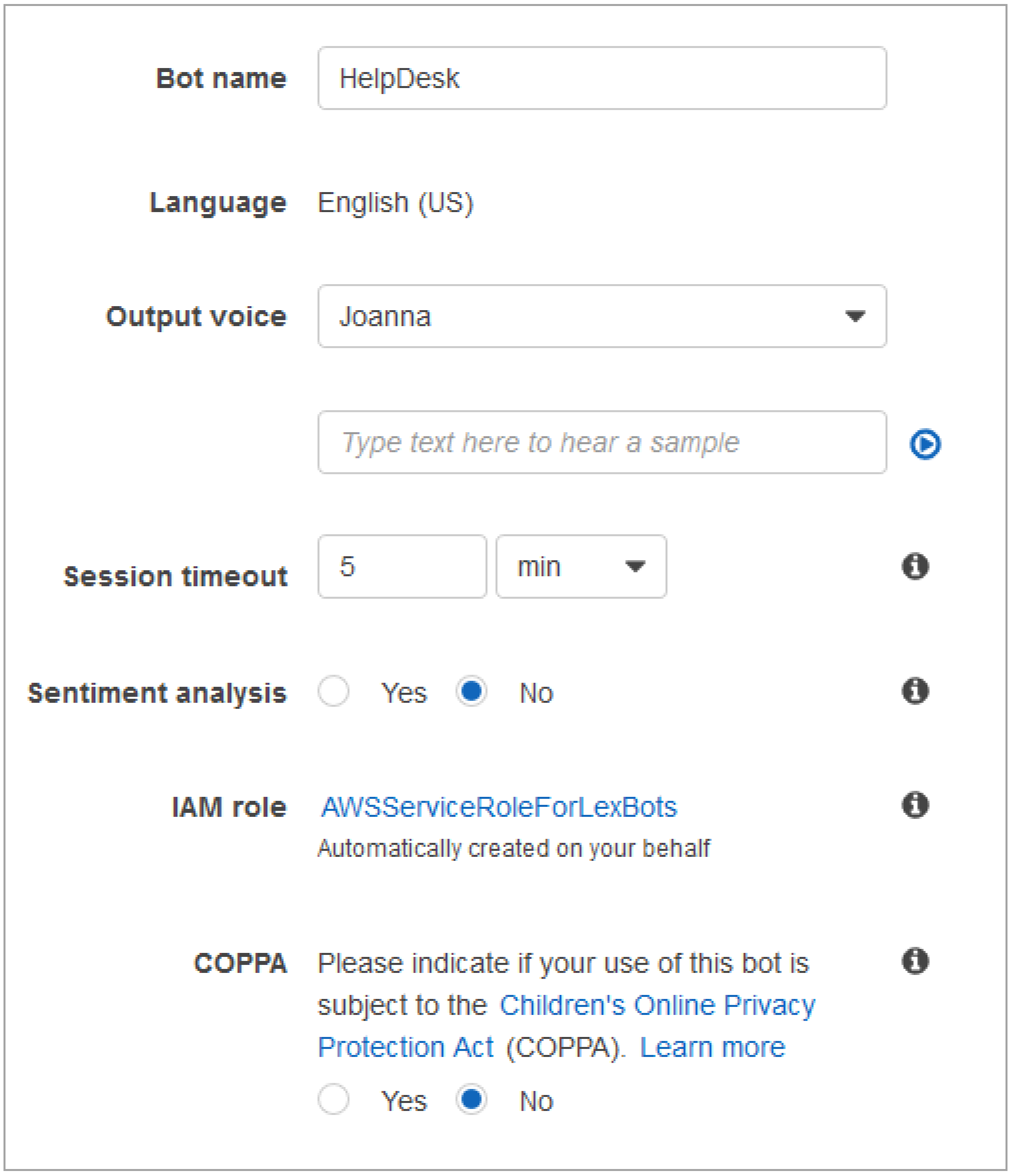
Create your bot

Amazon Lex enables any developer to build conversational chatbots quickly and easily. With Amazon Lex, no deep learning expertise is necessary—you just specify the basic conversational flow directly from the console, and then Amazon Lex manages the dialogue and dynamically adjusts the response. To get started, you can choose one of the sample bots provided below or build a new custom bot from scratch.

4. Enter the following information:

   - **Bot name** — For this tutorial, name the bot **HelpDesk**.
   - **Output voice**— Select the voice for your bot to use when speaking to callers. The default voice for Amazon Connect is Joanna.
   - **Session timeout**— Choose how long the bot should wait to get input from a caller before ending the session.
   - **COPPA**— Choose whether the bot is subject to the Children's Online Privacy Protection Act.

   The completed page looks like the following image.



Bot name	HelpDesk
Language	English (US)
Output voice	Joanna
	Type text here to hear a sample
Session timeout	5 min
Sentiment analysis	○ Yes ● No
IAM role	AWSServiceRoleForLexBots Automatically created on your behalf
COPPA	Please indicate if your use of this bot is subject to the Children's Online Privacy Protection Act (COPPA). Learn more ○ Yes ● No

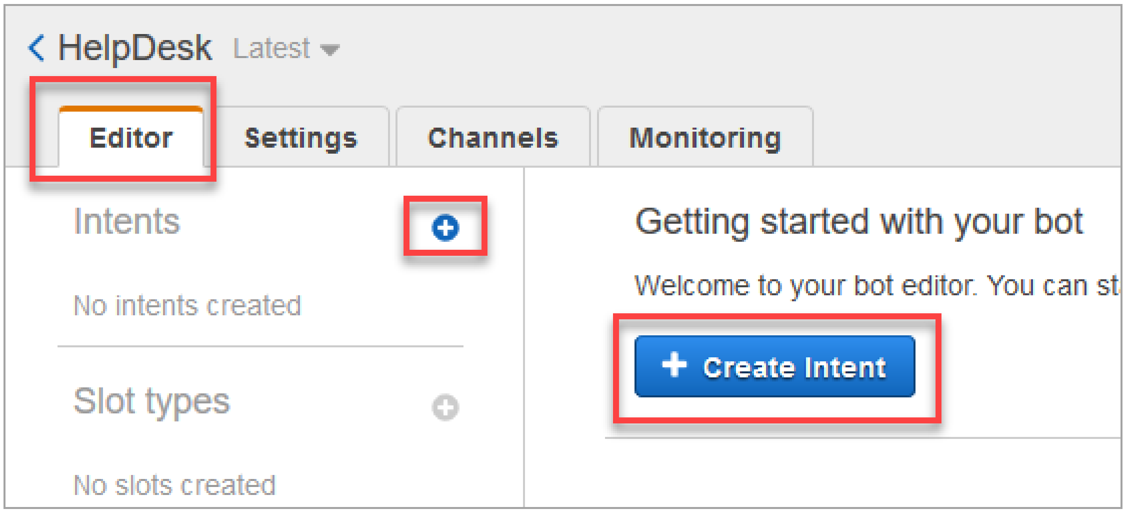
5. Choose **Create**.

Go to Part 2: Add intents to your Amazon Lex bot (p. 48).

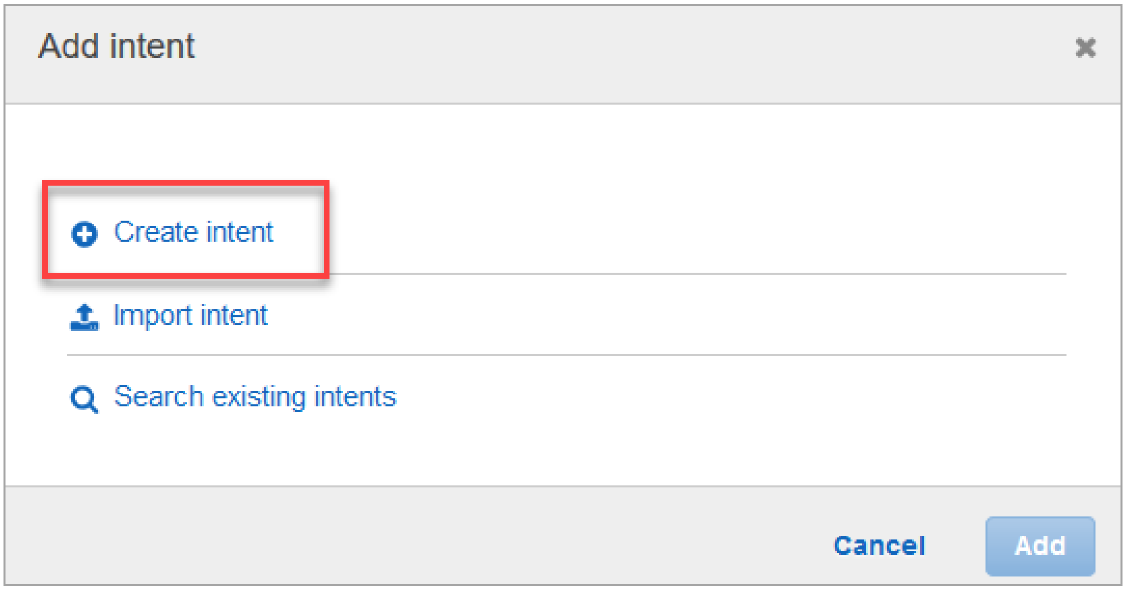
Part 2: Add intents to your Amazon Lex bot

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

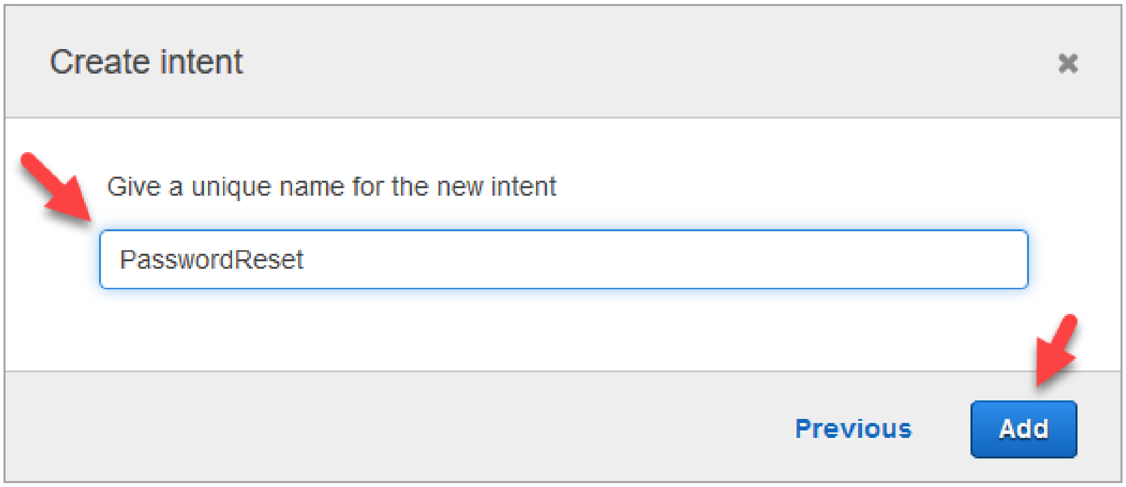
1. In the Amazon Lex console, choose the **Editor** tab.



2. Choose the **+** icon next to **Intents**, and choose **Create new intent**.
3. In the **Add intent** box, choose **+ Create intent**.



4. Name the intent **PasswordReset** and choose **Add**.



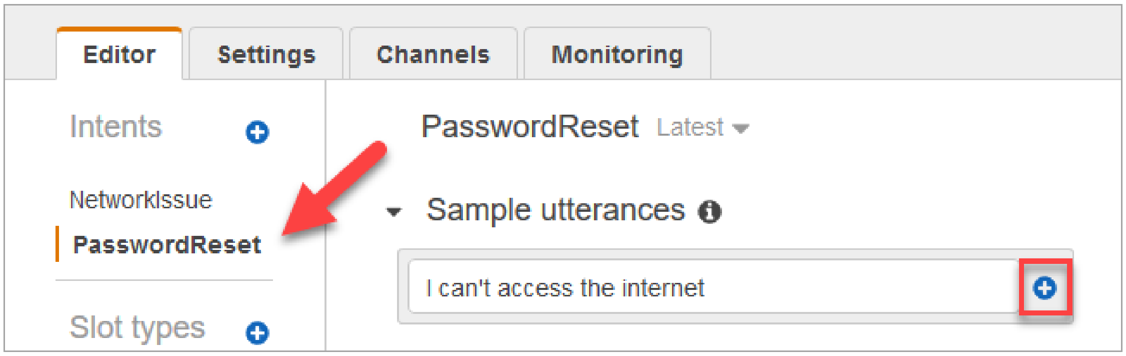
5. Choose the **+** icon next to **Intents** again, and add an intent for **NetworkIssue**.

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

Part 3: Add sample utterances

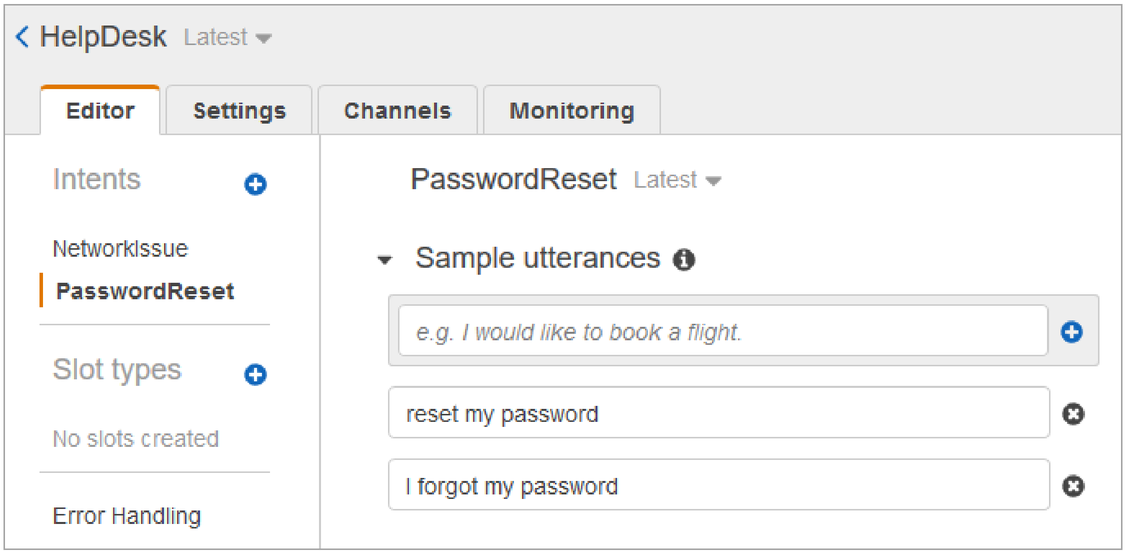
After defining the intents, add some sample utterances. Utterances are what a customer might say or chat to the bot.

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



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

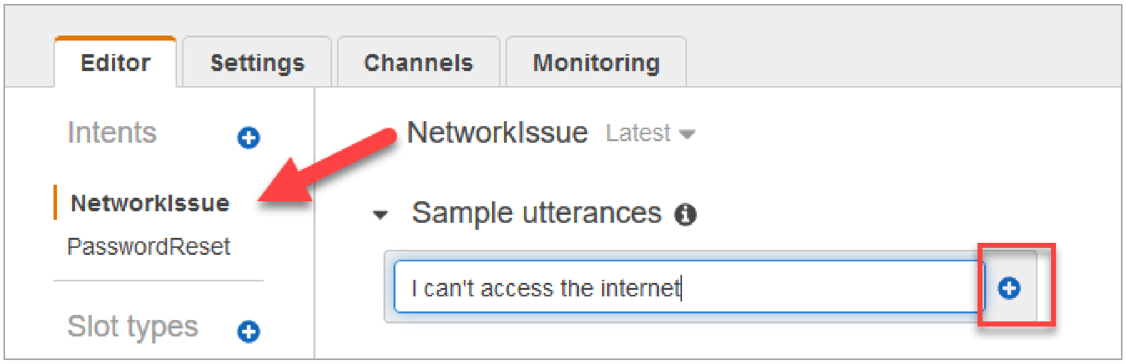
   The sample utterances look like what's shown in the following image.



reset my password

I forgot my password

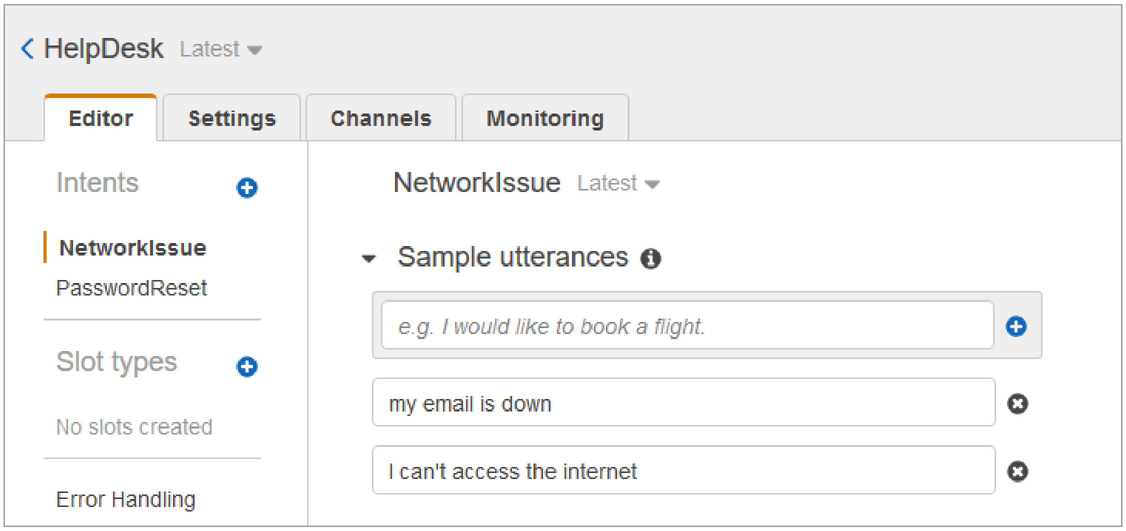
4. Select the **NetworkIssue** intent.



I can't access the internet

5. Add a sample utterance, such as **I can't access the internet**, and choose **+**.
6. Repeat step 5 to add the utterance **my email is down**.

   The sample utterances look like what's shown in the following image.



my email is down

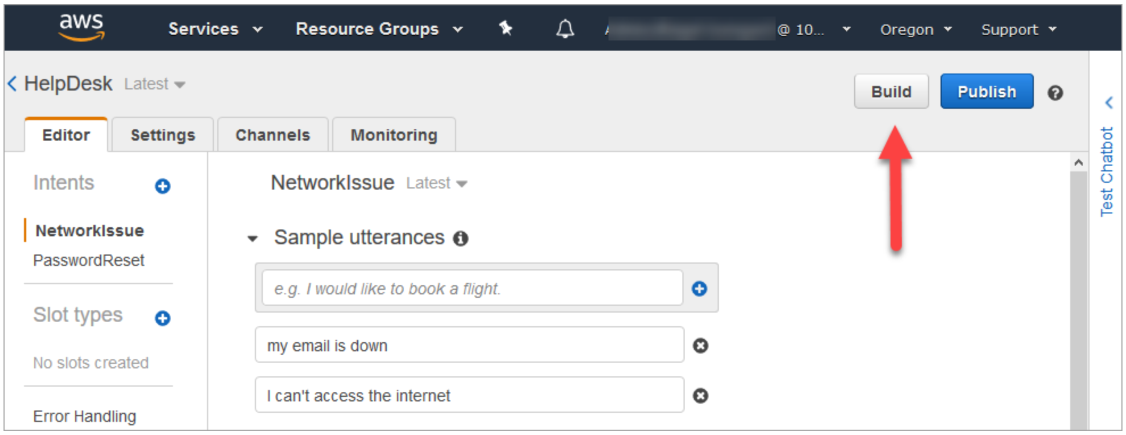
I can't access the internet

Go to Part 4: Build and test the Amazon Lex bot (p. 52).

Part 4: Build and test the Amazon Lex bot

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

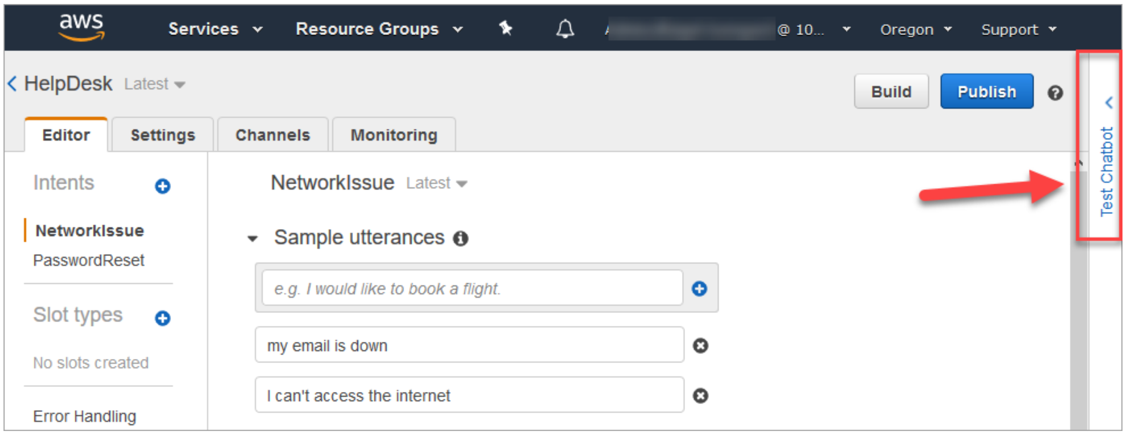
1. In the Amazon Lex console, choose **Build**. The build may take a minute or two.



my email is down

I can't access the internet

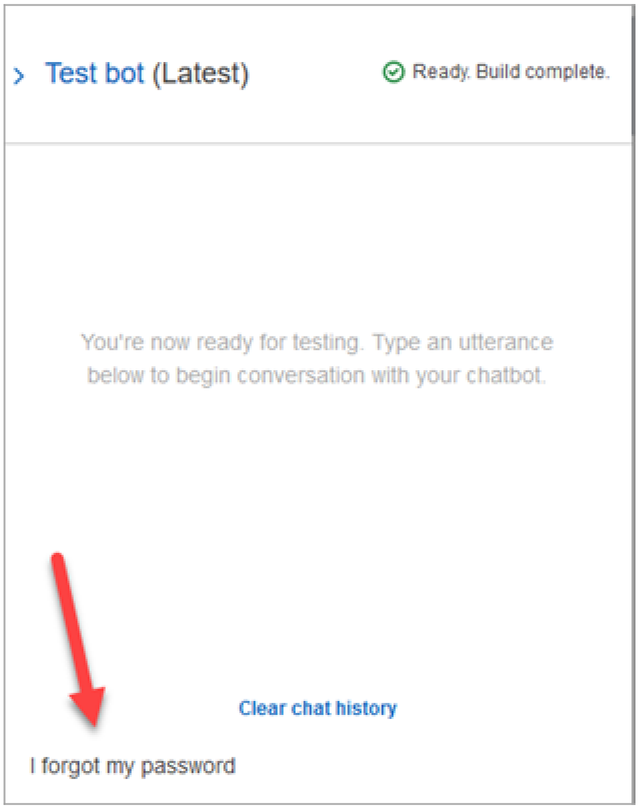
2. When it's finished building, choose **Test Chatbot**.



my email is down

I can't access the internet

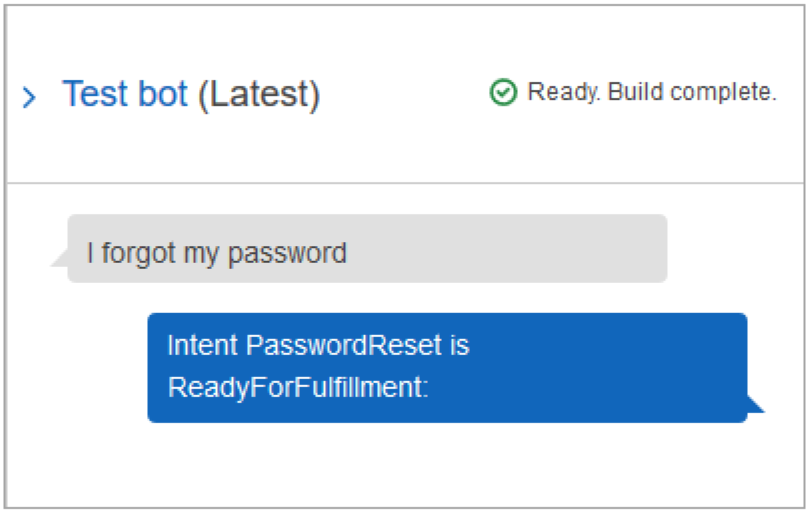
3. Test the **PasswordReset** intent. In the **Test Chatbot** pane, type **I forgot my password**, and press **Enter**.



You're now ready for testing. Type an utterance below to begin conversation with your chatbot.

I forgot my password

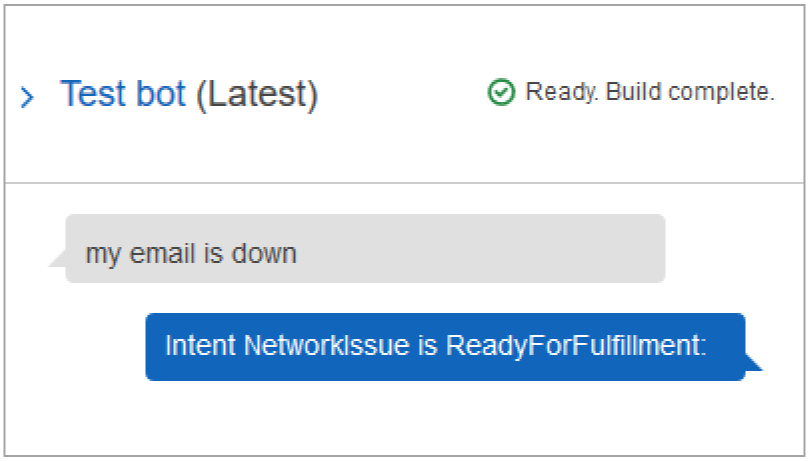
4. The verification looks like what's shown in the following image.



I forgot my password

Intent PasswordReset is ReadyForFulfillment:

5. To confirm that the **NetworkIssue** intent is working, type **my email is down**. The verification looks like what's shown in the following image.



Test bot (Latest)

Ready. Build complete.

my email is down

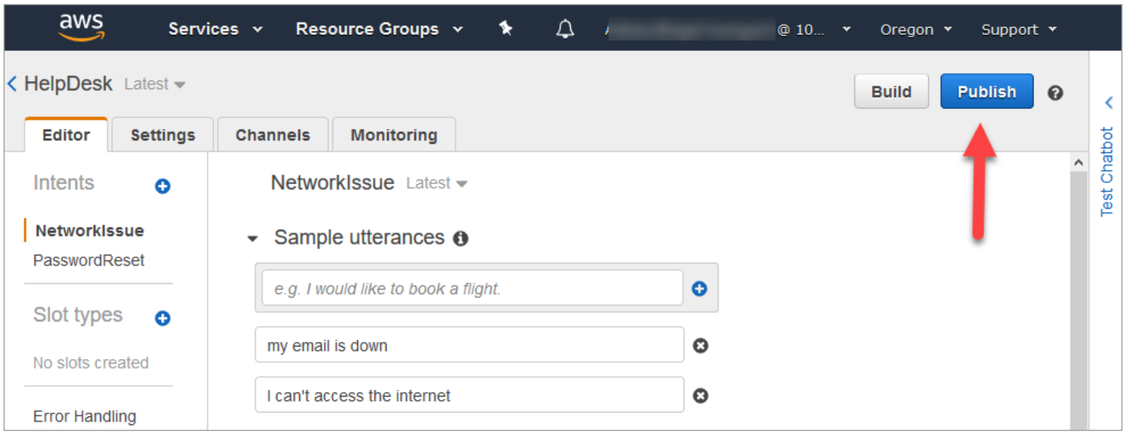
Intent NetworkIssue is ReadyForFulfillment:

Go to Part 5: Publish the Amazon Lex bot and create an alias (p. 54).

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

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

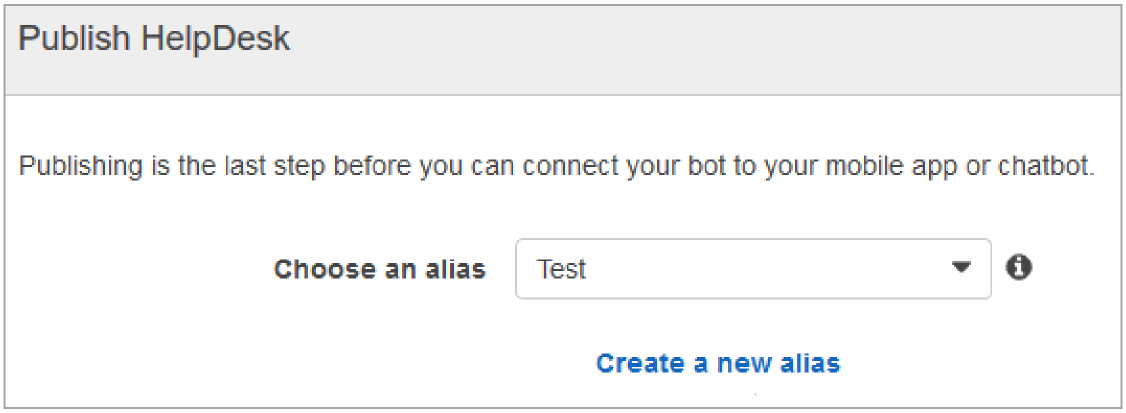
1. In the Amazon Lex console, choose **Publish**.



my email is down

I can't access the internet

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



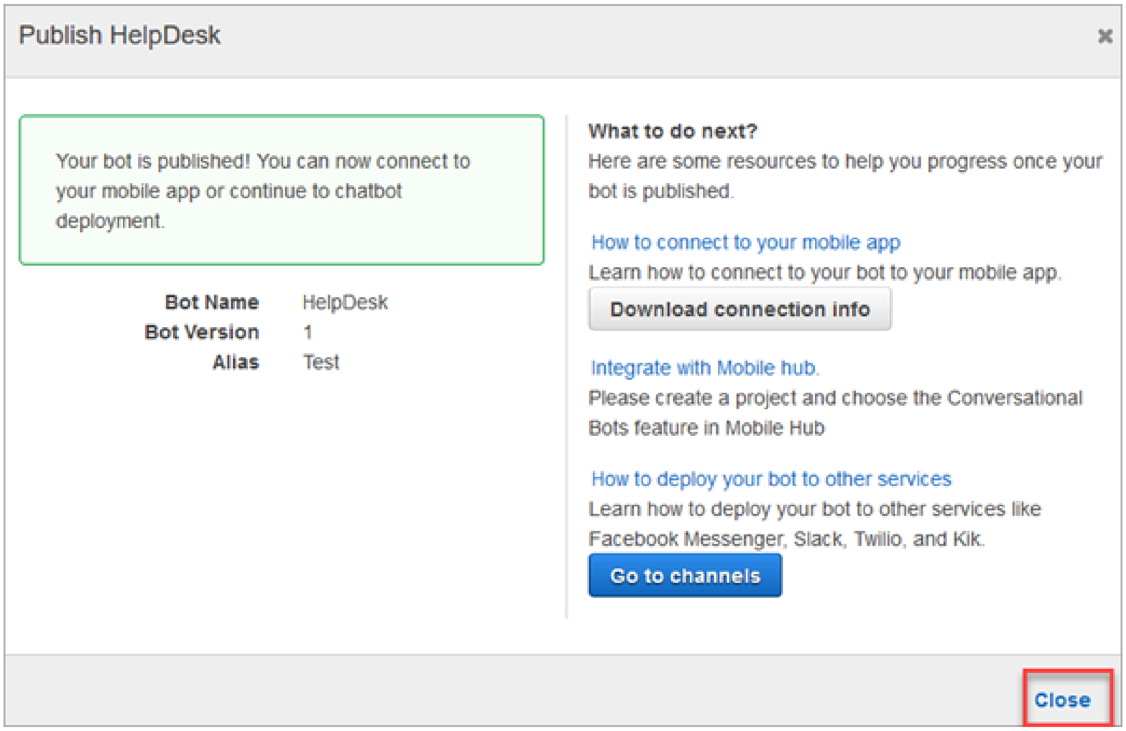
Publish HelpDesk

Publishing is the last step before you can connect your bot to your mobile app or chatbot.

Choose an alias: Test

3. Choose **Publish**. The publishing takes a few minutes.

4. When Amazon Lex finishes publishing, choose **Close**.



Publish HelpDesk

Your bot is published! You can now connect to your mobile app or continue to chatbot deployment.

Bot Name	HelpDesk
Bot Version	1
Alias	Test

What to do next?

Here are some resources to help you progress once your bot is published.

How to connect to your mobile app

Learn how to connect to your bot to your mobile app.

Integrate with Mobile hub.

Please create a project and choose the Conversational Bots feature in Mobile Hub

How to deploy your bot to other services

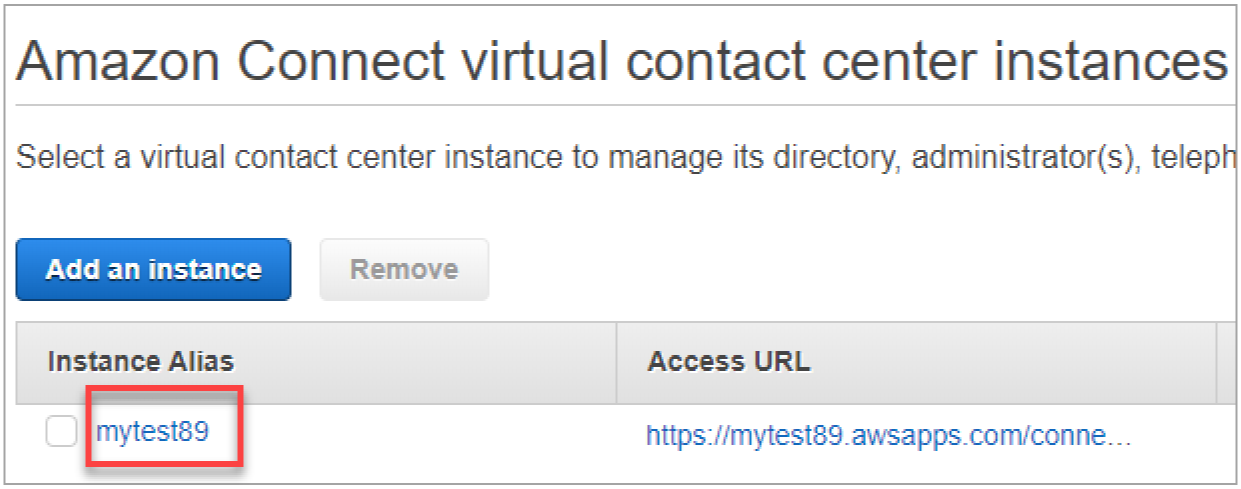
Learn how to deploy your bot to other services like Facebook Messenger, Slack, Twilio, and Kik.

Well done! You created an Amazon Lex bot that has intents and utterances. Now you can add the bot to Amazon Connect. Go to Step 2: Add permissions to Amazon Lex bot (p. 55).

Step 2: Add permissions to Amazon Lex bot

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

1. Open the Amazon Connect console (https://console.aws.amazon.com/connect/).
2. Choose the name of the instance that you created.

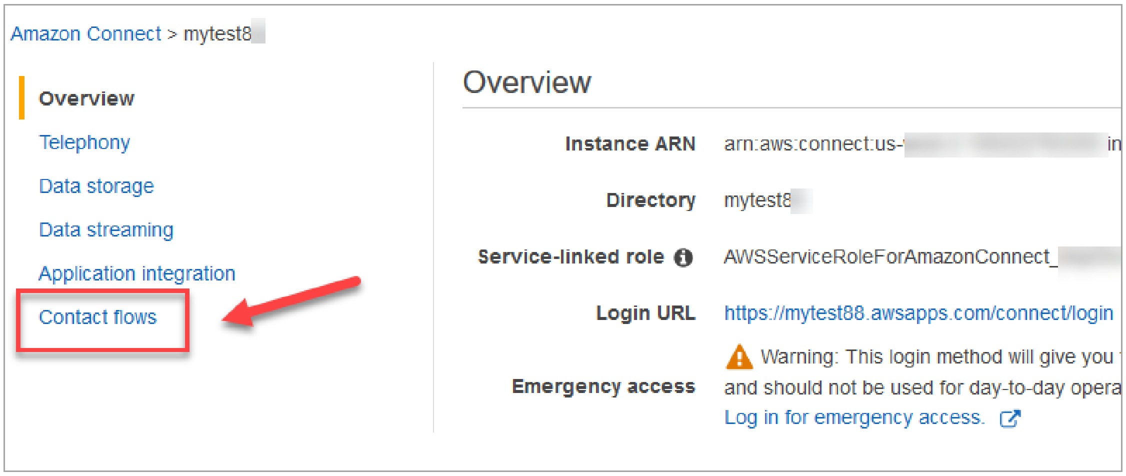


Amazon Connect virtual contact center instances

Select a virtual contact center instance to manage its directory, administrator(s), teleph

	Instance Alias	Access URL
□	mytest89	https://mytest89.awsapps.com/conne...

3. Do not log in on the name page (this method of logging in is for emergency access only). Rather, choose **Contact flows**.



Amazon Connect > mytest8[redacted]

- **Overview**
- Telephony
- Data storage
- Data streaming
- Application integration
- Contact flows

Overview

Instance ARN arn:aws:connect:us-[redacted]in

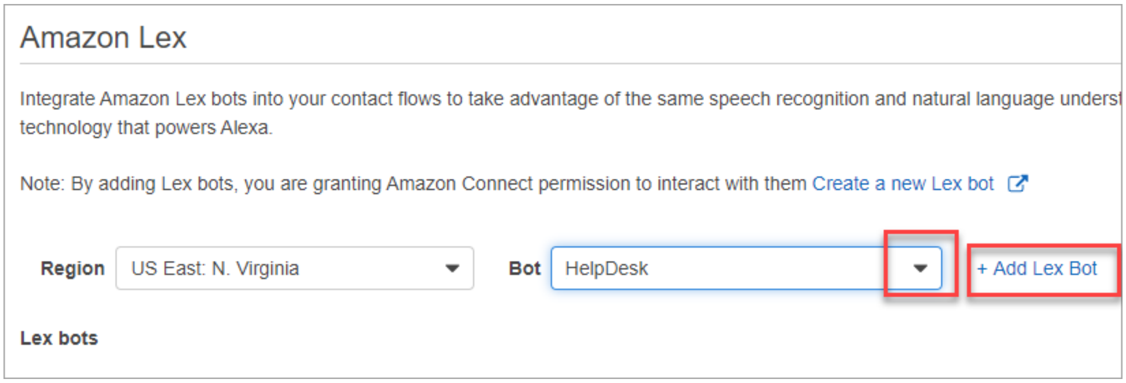
Directory mytest8[redacted]

Service-linked role AWSServiceRoleForAmazonConnect_[redacted]

Login URL https://mytest88.awsapps.com/connect/login

Emergency access Warning: This login method will give you and should not be used for day-to-day opera
Log in for emergency access.

4. Under **Amazon Lex**, use the drop-down arrow to choose **HelpDesk**, and then choose **+ Add Lex Bot**.



Amazon Lex

Integrate Amazon Lex bots into your contact flows to take advantage of the same speech recognition and natural language underst technology that powers Alexa.

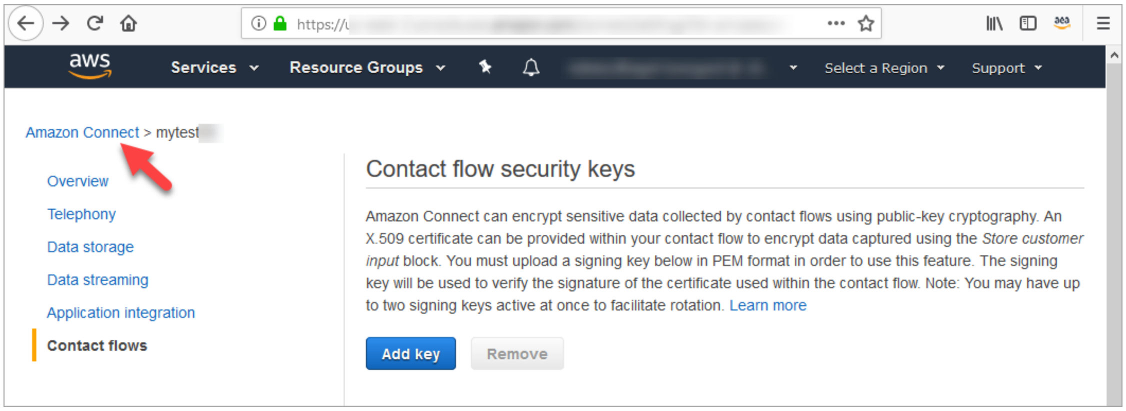
Note: By adding Lex bots, you are granting Amazon Connect permission to interact with them Create a new Lex bot

Region US East: N. Virginia **Bot** HelpDesk + Add Lex Bot

Lex bots

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

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



Amazon Connect > mytest[redacted]

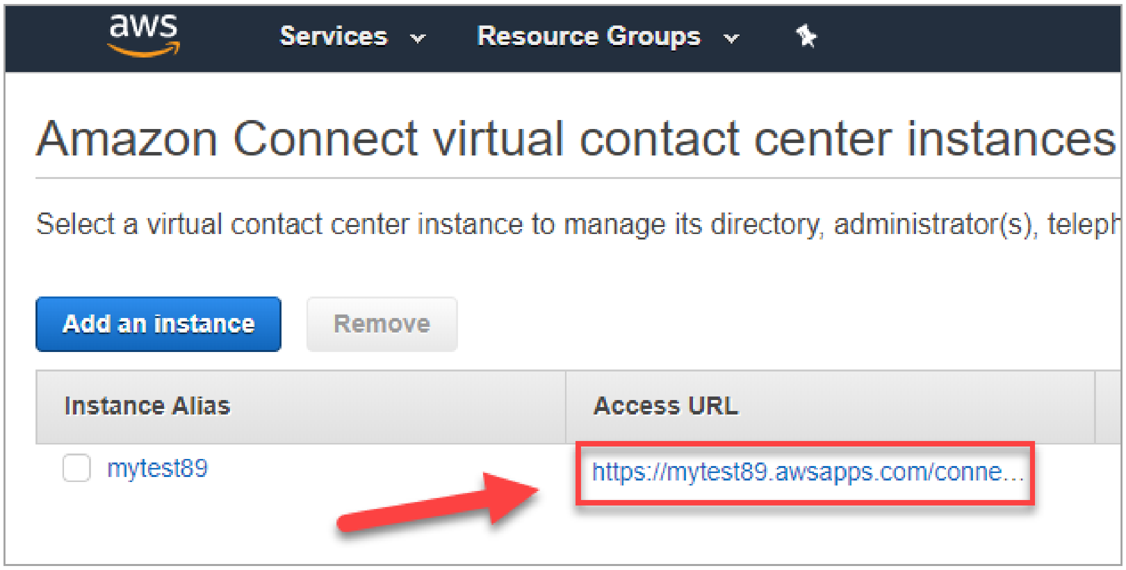
- Overview
- Telephony
- Data storage
- Data streaming
- Application integration
- **Contact flows**

Contact flow security keys

Amazon Connect can encrypt sensitive data collected by contact flows using public-key cryptography. An X.509 certificate can be provided within your contact flow to encrypt data captured using the *Store customer input* block. You must upload a signing key below in PEM format in order to use this feature. The signing key will be used to verify the signature of the certificate used within the contact flow. Note: You may have up to two signing keys active at once to facilitate rotation. Learn more

Add key Remove

6. Choose the access URL of your instance.



Amazon Connect virtual contact center instances

Select a virtual contact center instance to manage its directory, administrator(s), teleph

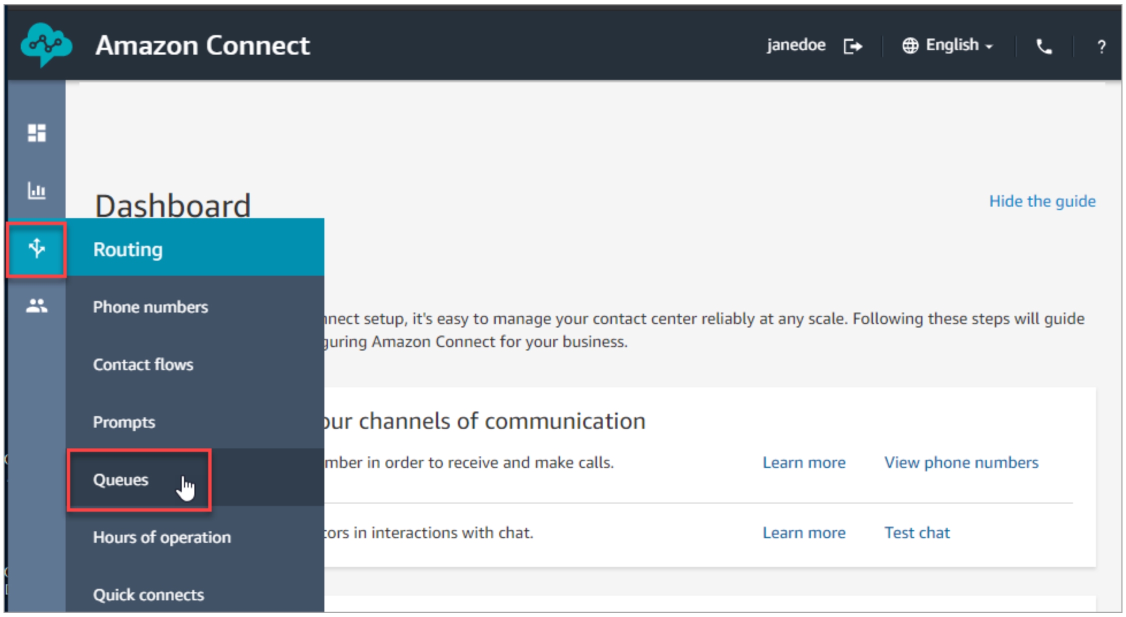
Instance Alias	Access URL
□ mytest89	https://mytest89.awsapps.com/conne…

This takes you back to the Amazon Connect dashboard.

Step 3: Set up routing

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

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



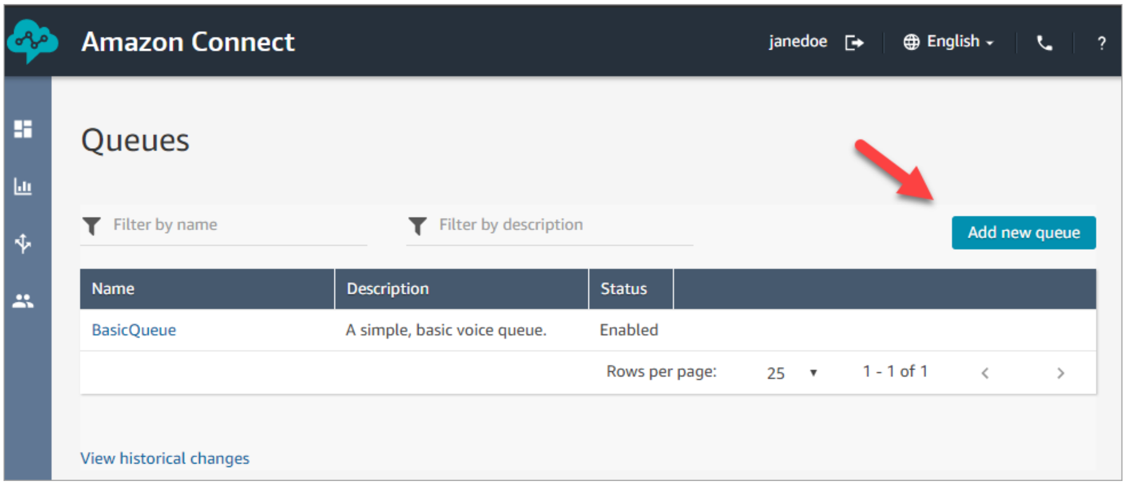
nect setup, it's easy to manage your contact center reliably at any scale. Following these steps will guide
guring Amazon Connect for your business.

our channels of communication

mber in order to receive and make calls.

tors in interactions with chat.

2. Choose **Add new queue**.



Queues

Filter by name

Filter by description

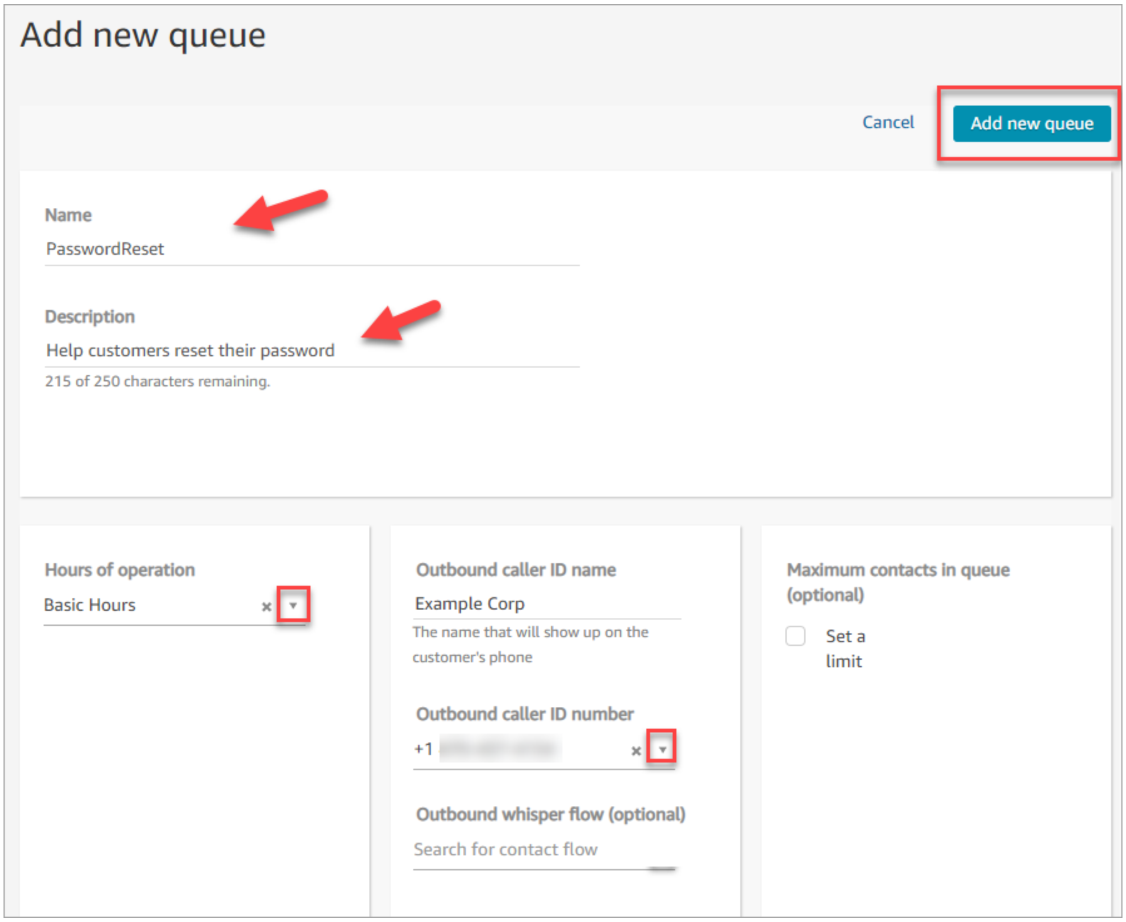
Add new queue

Name	Description	Status
BasicQueue	A simple, basic voice queue.	Enabled

Rows per page: 25 1 - 1 of 1

View historical changes

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



Add new queue

Name
PasswordReset

Description
Help customers reset their password
215 of 250 characters remaining.

Hours of operation
Basic Hours

Outbound caller ID name
Example Corp
The name that will show up on the customer's phone

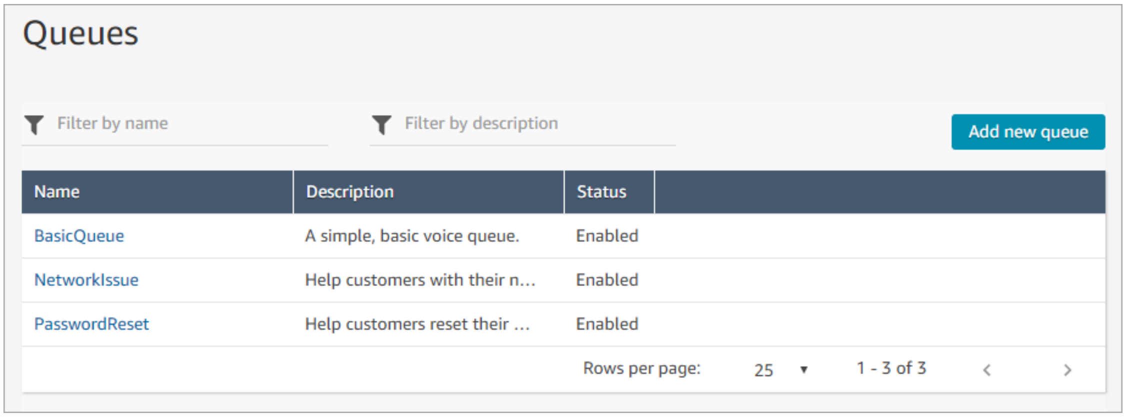
Outbound caller ID number
+1 [redacted]

Outbound whisper flow (optional)
Search for contact flow

Maximum contacts in queue (optional)
□ Set a limit

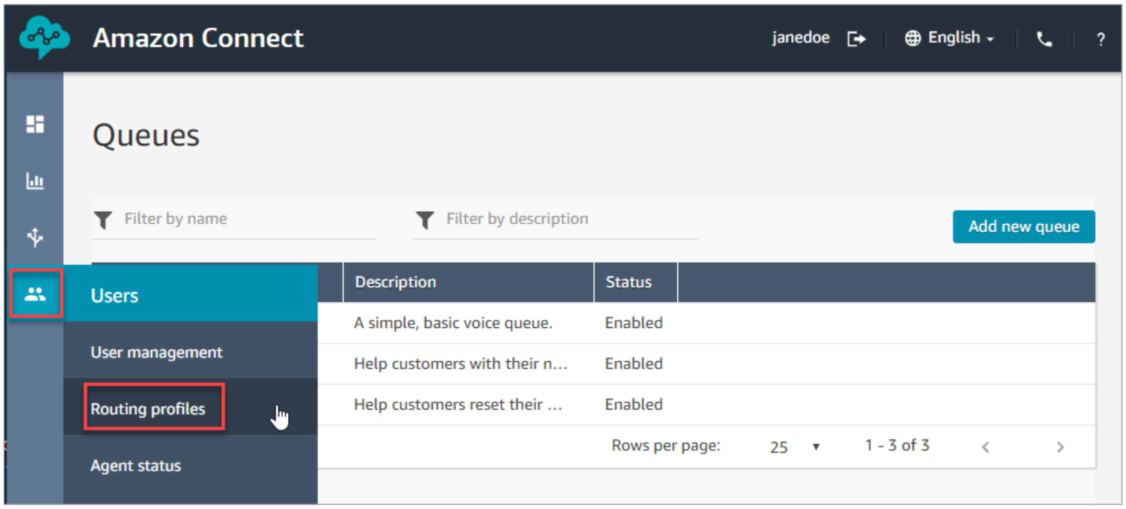
4. Add a queue named **NetworkIssue**. Complete the **Add new queue** page like you did for the **PasswordReset** queue.

   When done, you'll have three queues.



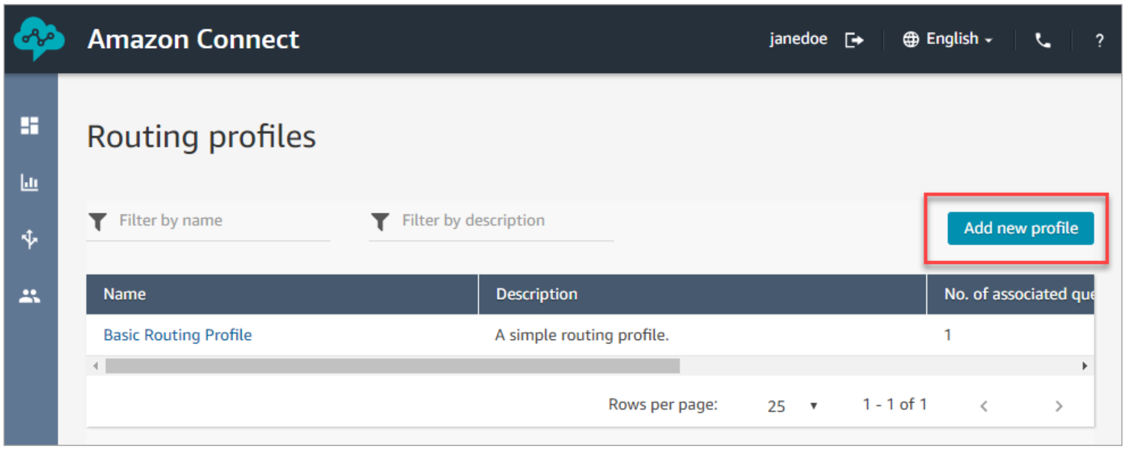
Name	Description	Status
BasicQueue	A simple, basic voice queue.	Enabled
NetworkIssue	Help customers with their n...	Enabled
PasswordReset	Help customers reset their ...	Enabled

5. On the navigation menu, go to **Users**, **Routing Profiles**.



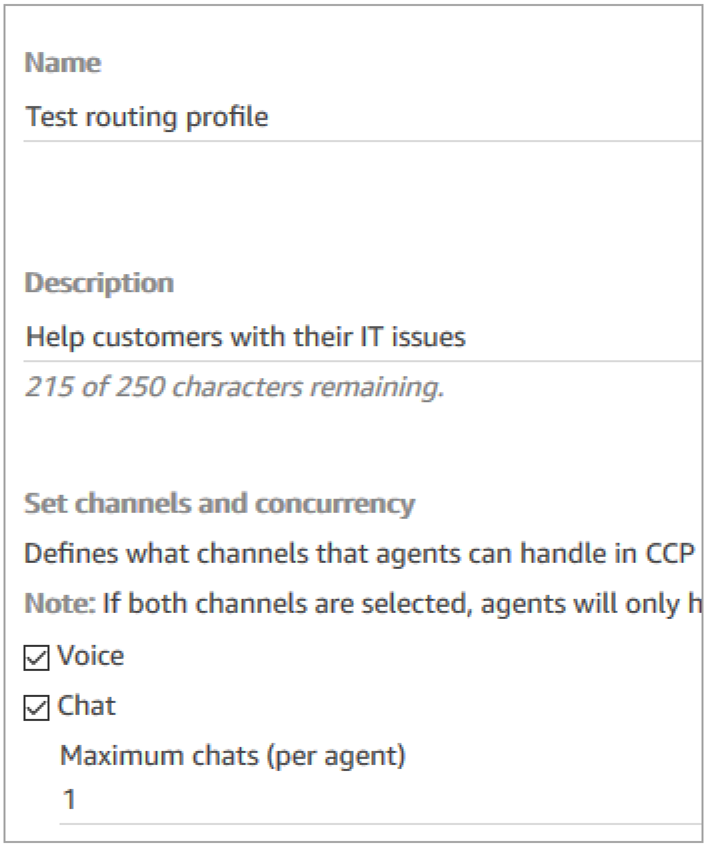
Description	Status
A simple, basic voice queue.	Enabled
Help customers with their n...	Enabled
Help customers reset their ...	Enabled

6. Choose **Add new profile**.



Name	Description	No. of associated que
Basic Routing Profile	A simple routing profile.	1

7. Assign a name to the new profile (for example, **Test routing profile**). Enter a description, select **Voice**, **Chat**, and set **Maximum chats** to **1.**



Name

Test routing profile

Description

Help customers with their IT issues

215 of 250 characters remaining.

Set channels and concurrency

Defines what channels that agents can handle in CCP

Note: If both channels are selected, agents will only h

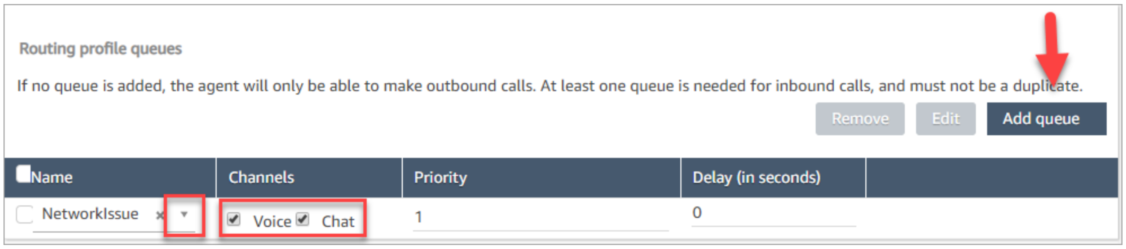
☑ Voice

☑ Chat

Maximum chats (per agent)

1

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

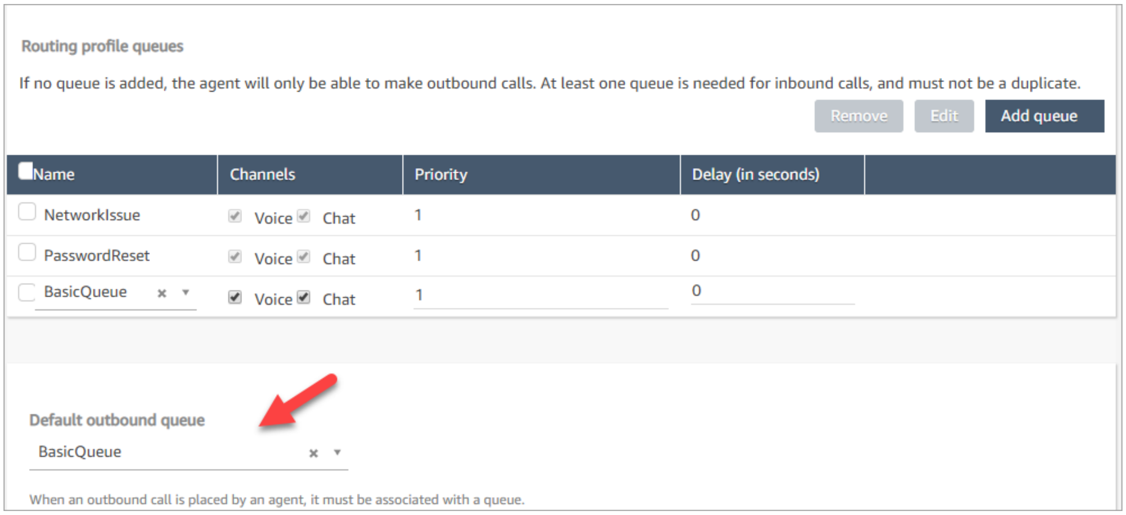


Routing profile queues

If no queue is added, the agent will only be able to make outbound calls. At least one queue is needed for inbound calls, and must not be a duplicate.

□ Name	Channels	Priority	Delay (in seconds)
□ NetworkIssue × ▾	☑ Voice ☑ Chat	1	0

9. Then add the **PasswordReset** queue. Select **Voice** and **Chat**, and then choose **Add queue**.
10. Under **Default outbound queue**, use the drop-down arrow to choose **BasicQueue**.



Routing profile queues

If no queue is added, the agent will only be able to make outbound calls. At least one queue is needed for inbound calls, and must not be a duplicate.

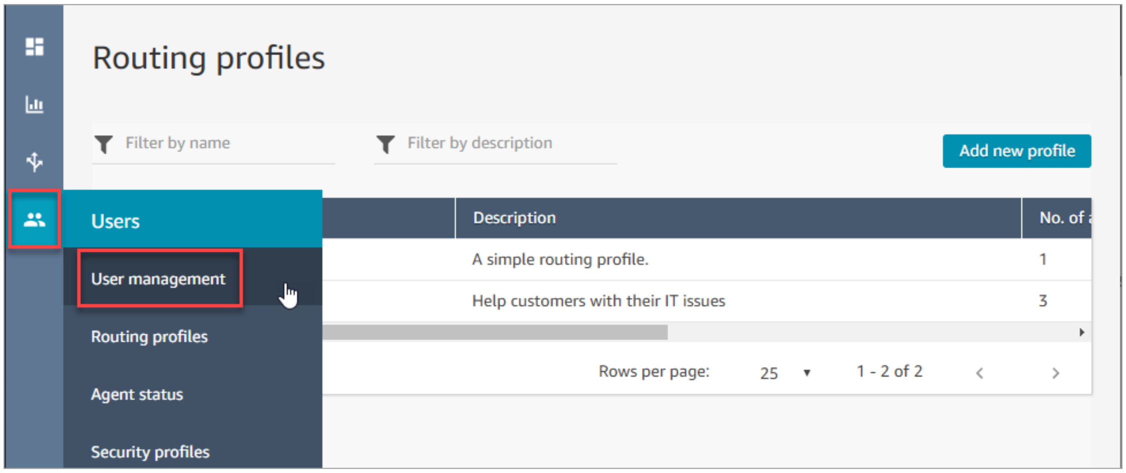
□ Name	Channels	Priority	Delay (in seconds)
□ NetworkIssue	☑ Voice ☑ Chat	1	0
□ PasswordReset	☑ Voice ☑ Chat	1	0
□ BasicQueue × ▾	☑ Voice ☑ Chat	1	0

Default outbound queue

BasicQueue × ▾

When an outbound call is placed by an agent, it must be associated with a queue.

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

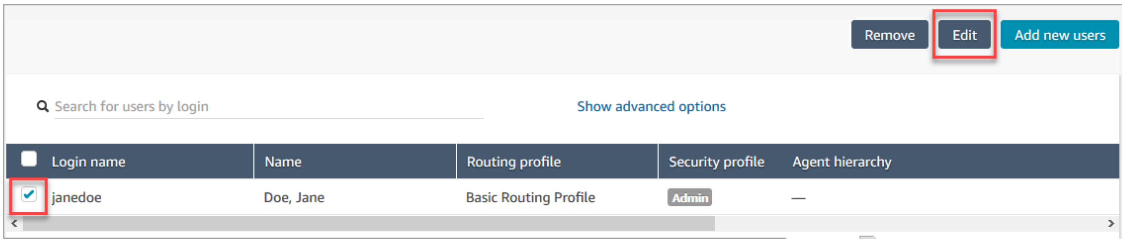


Routing profiles

Description	No. of a
A simple routing profile.	1
Help customers with their IT issues	3

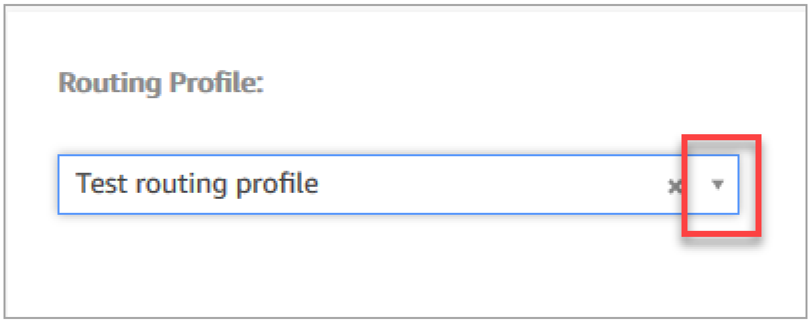
Rows per page: 25 ▾ 1 - 2 of 2 ‹ ›

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



□ Login name	Name	Routing profile	Security profile	Agent hierarchy
☑ janedoe	Doe, Jane	Basic Routing Profile	Admin	—

14. Use the drop-down arrow to choose the routing profile you created, for example, **Test routing profile**. Choose **Save**.



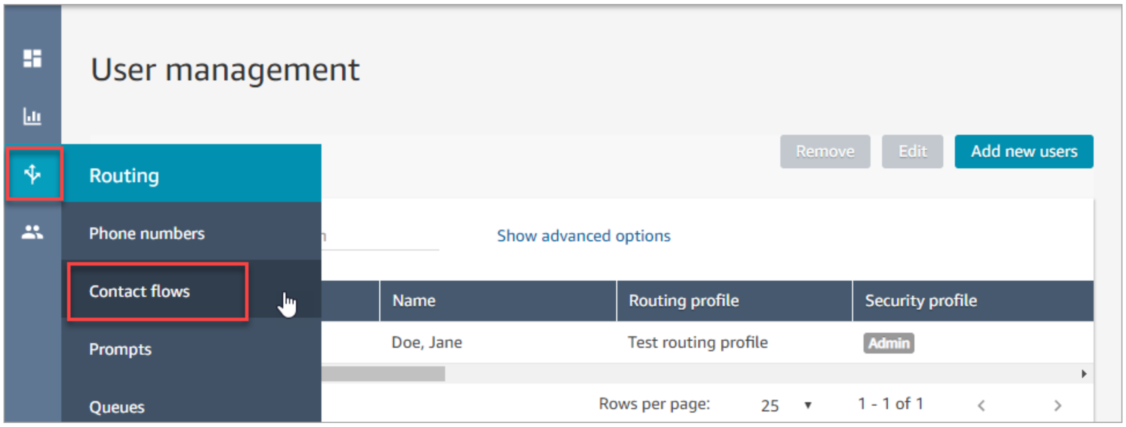
Routing is all set up and ready to go.

Step 4: Create a contact flow

Although Amazon Connect comes with a set of built-in contact flows (p. 297), you can create your own contact flows to determine how a customer experiences your contact center. The contact flows contain the prompts that customers hear or see, and they transfer them to the right queue or agent, among other things.

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

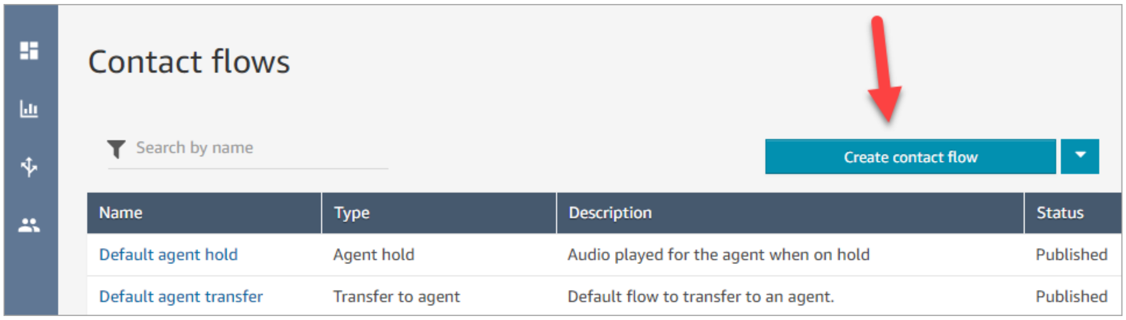
1. On the navigation menu, go to **Routing**, **Contact flows**.



Name	Routing profile	Security profile
Doe, Jane	Test routing profile	Admin

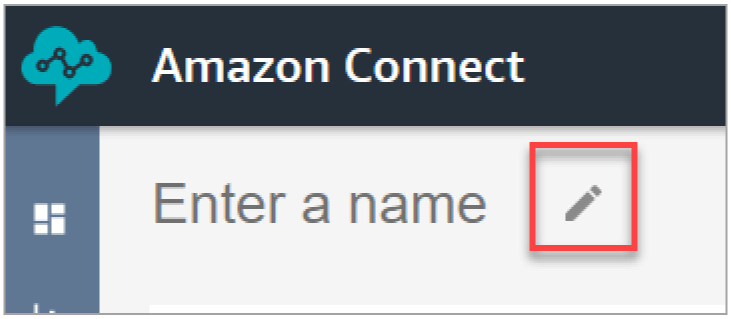
Rows per page: 25 ▾ 1 - 1 of 1

2. Choose **Create contact flow**.

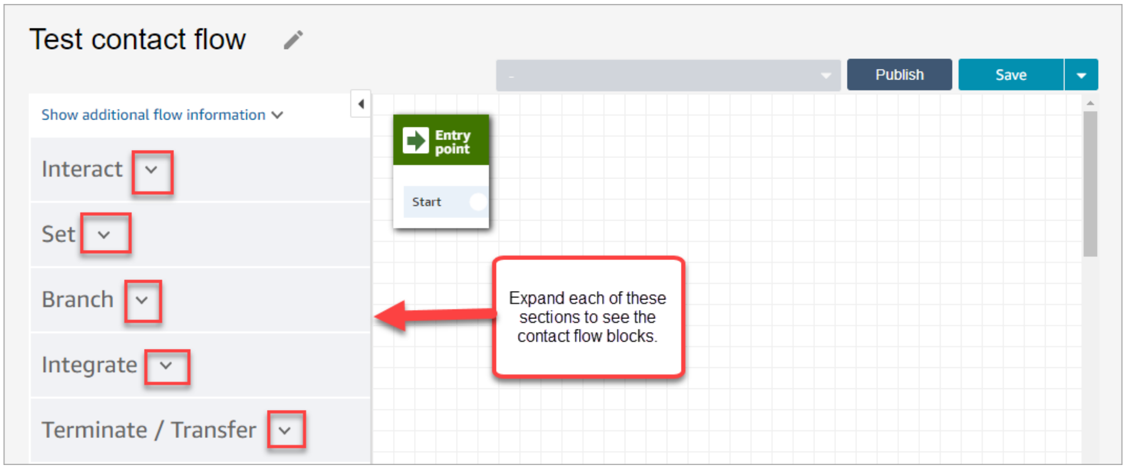


Name	Type	Description	Status
Default agent hold	Agent hold	Audio played for the agent when on hold	Published
Default agent transfer	Transfer to agent	Default flow to transfer to an agent.	Published

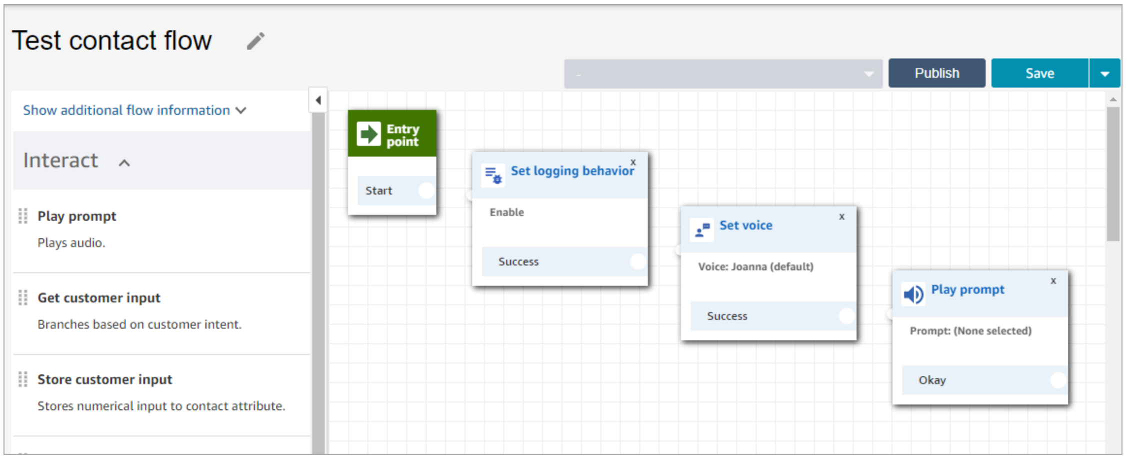
3. The contact flow designer opens. Enter a name for the contact flow, such as **Test contact flow**.



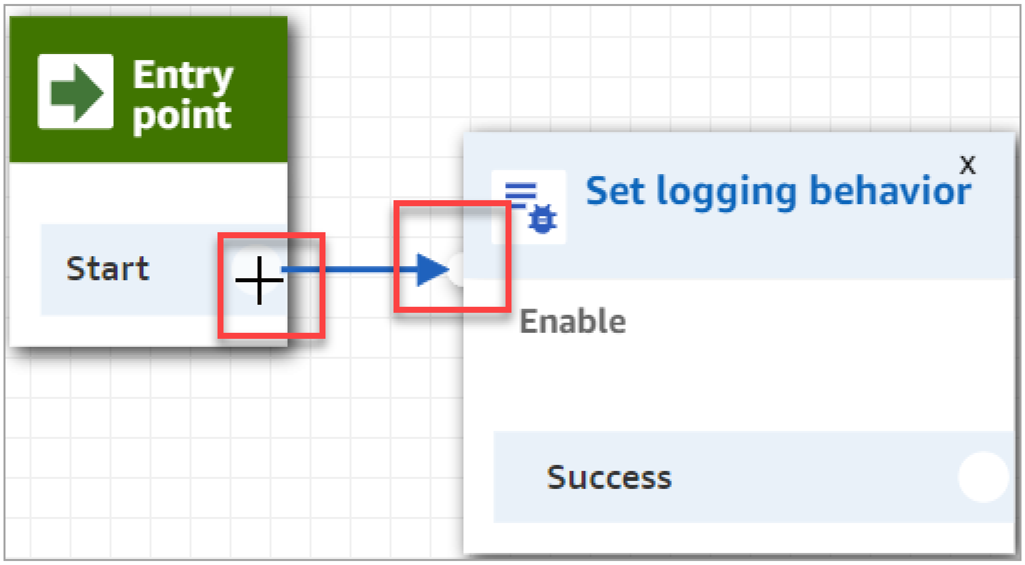
4. Choose the drop-down arrows to expand the sections to access the blocks in them.


Test contact flow
Publish
Save
Show additional flow information
Interact
Set
Branch
Integrate
Terminate / Transfer
Entry point
Start
Expand each of these sections to see the contact flow blocks.

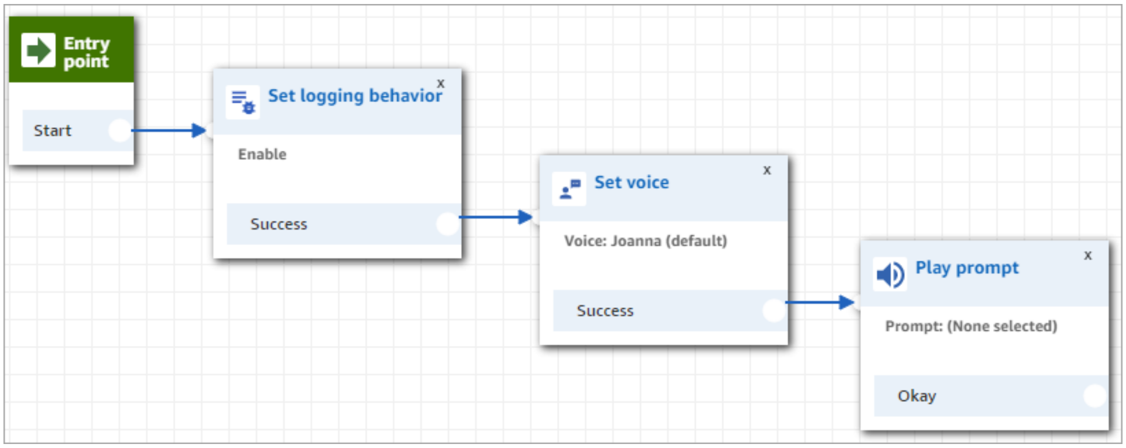
5. Drag the following blocks onto the grid: Set logging behavior (p. 407) (in the **Set** group), Set voice (p. 415) (in the **Set** group), and Play prompt (p. 393) (in the **Interact** group).



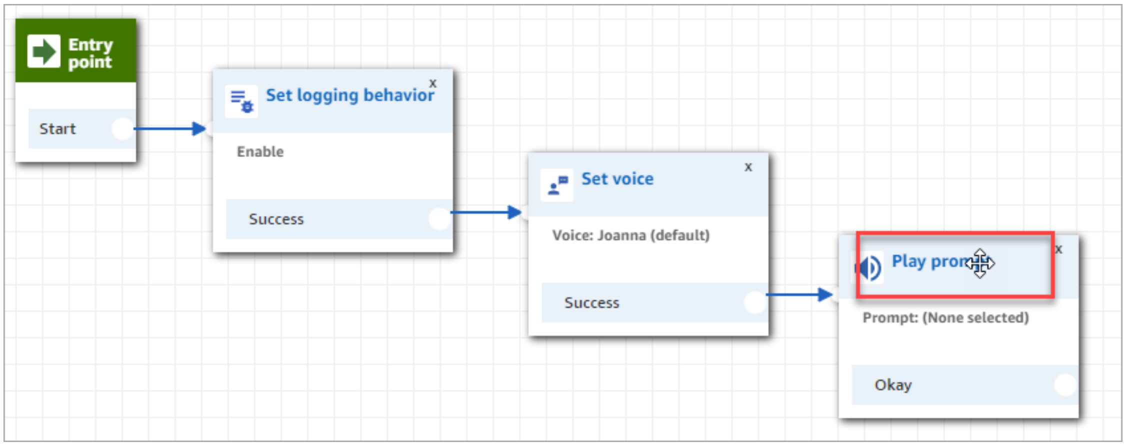
6. Use your mouse to drag an arrow from the **Start** block to the **Set logging behavior** block.



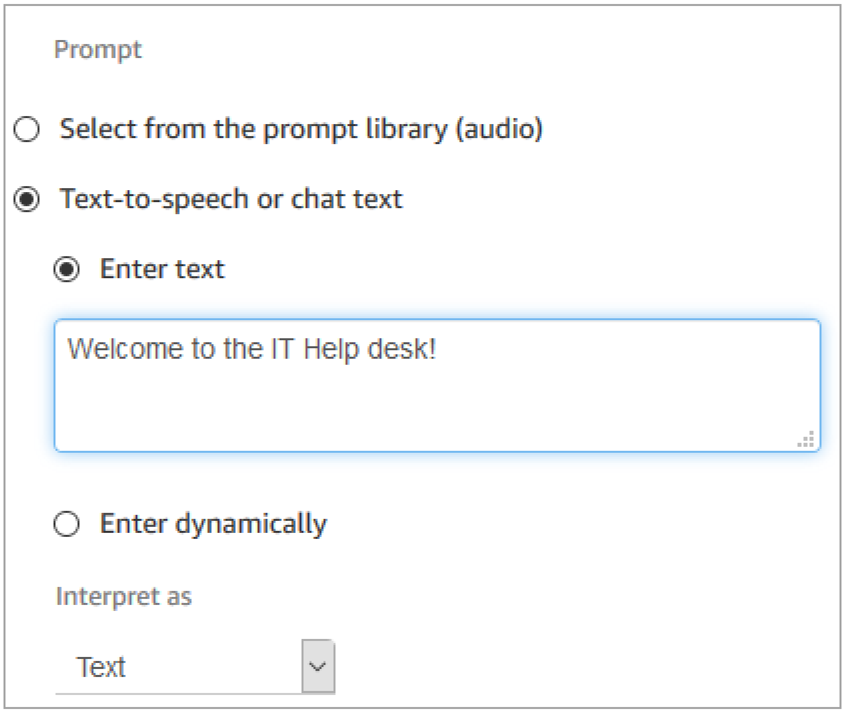
7. Connect the remaining blocks, as shown in the following image.



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



9. Configure the **Play prompt** block, as shown in the following image, and then choose **Save**.



Prompt

○ Select from the prompt library (audio)

● Text-to-speech or chat text

● Enter text

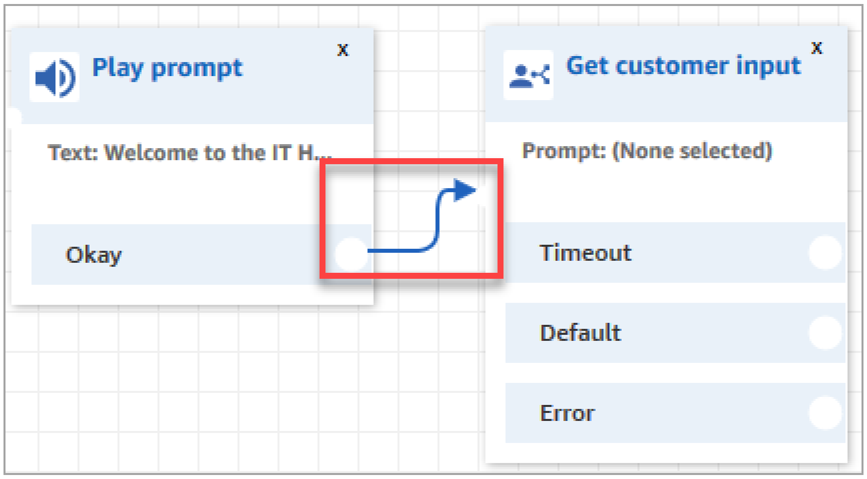
Welcome to the IT Help desk!

○ Enter dynamically

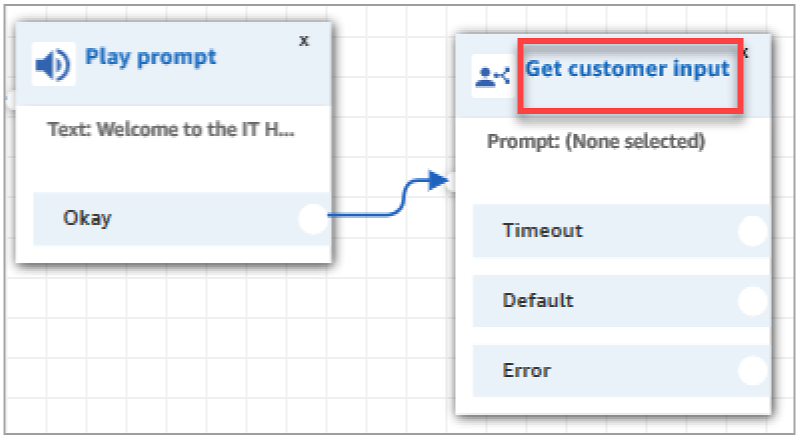
Interpret as

Text

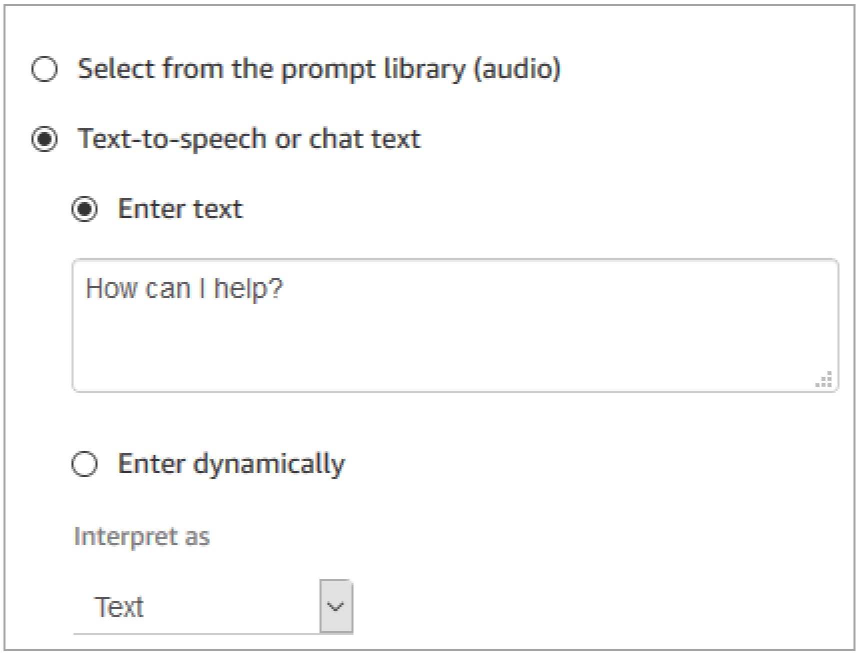
10. Add a Get customer input (p. 366) block and connect to the **Play prompt** block.



11. Choose the title of the Get customer input (p. 366) block to open the properties page.



12. Configure the **Get customer input** block, as shown in the following images.



○ Select from the prompt library (audio)

● Text-to-speech or chat text

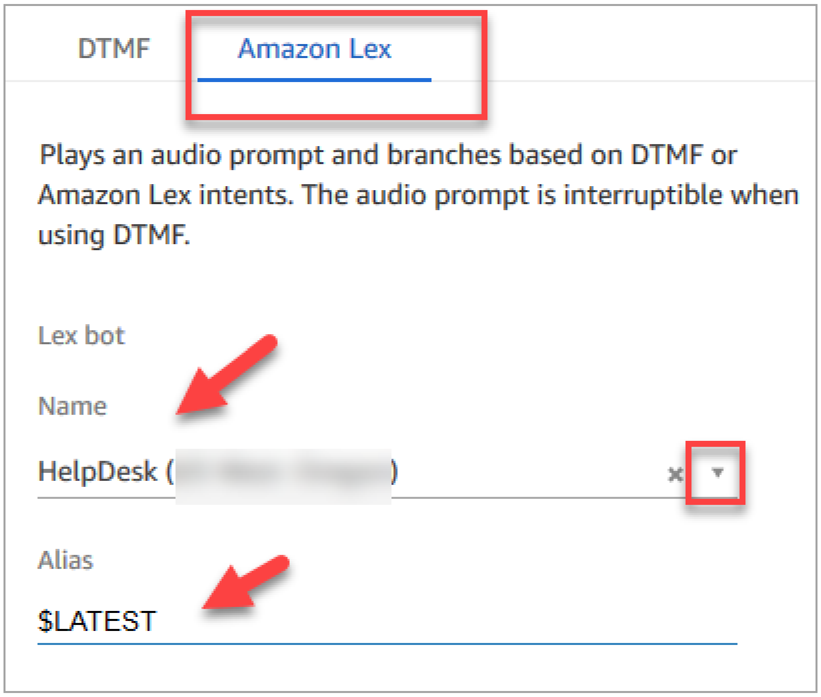
● Enter text

How can I help?

○ Enter dynamically

Interpret as

Text



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

Lex bot

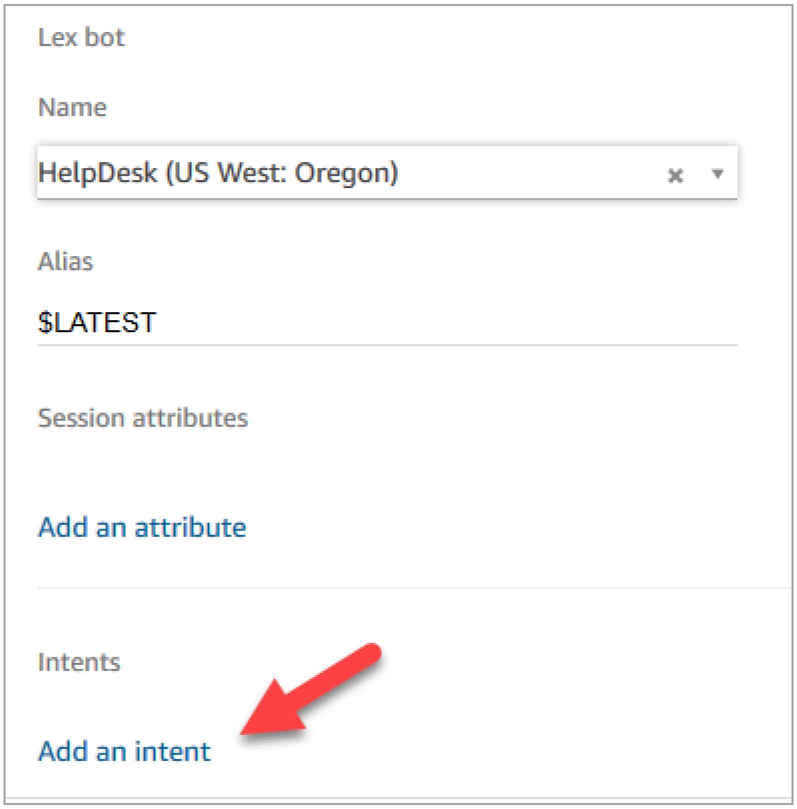
Name

HelpDesk ([redacted])

Alias

$LATEST

13. While still in the **Get customer input** block, choose **Add an intent**.



Lex bot

Name

HelpDesk (US West: Oregon)

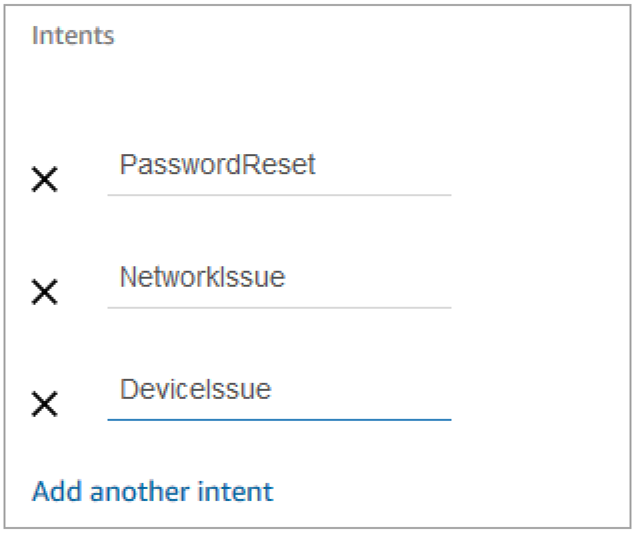
Alias

$LATEST

Session attributes

Intents

14. Enter the names of the intents that you created in the Amazon Lex bot. They are case sensitive!



Intents

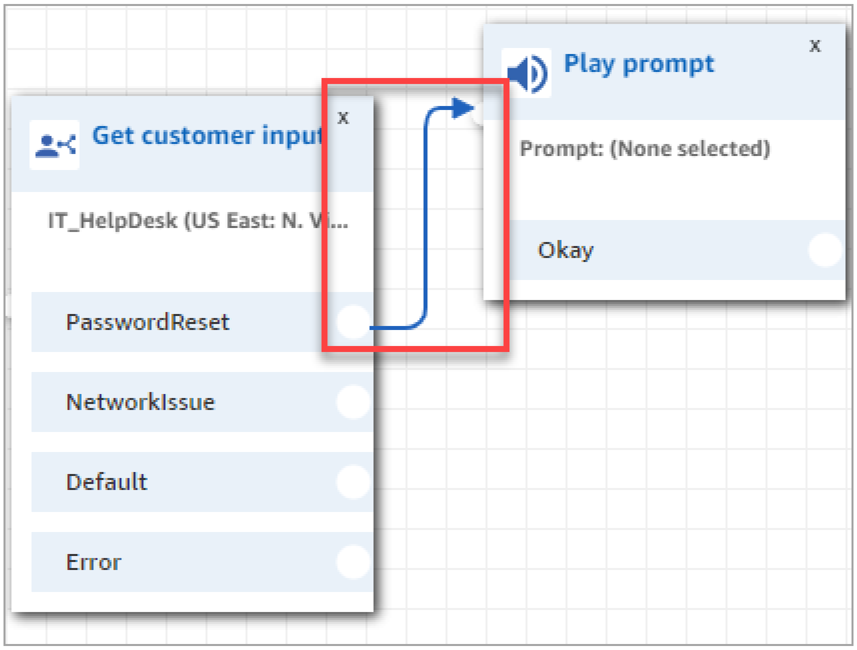
× PasswordReset

× NetworkIssue

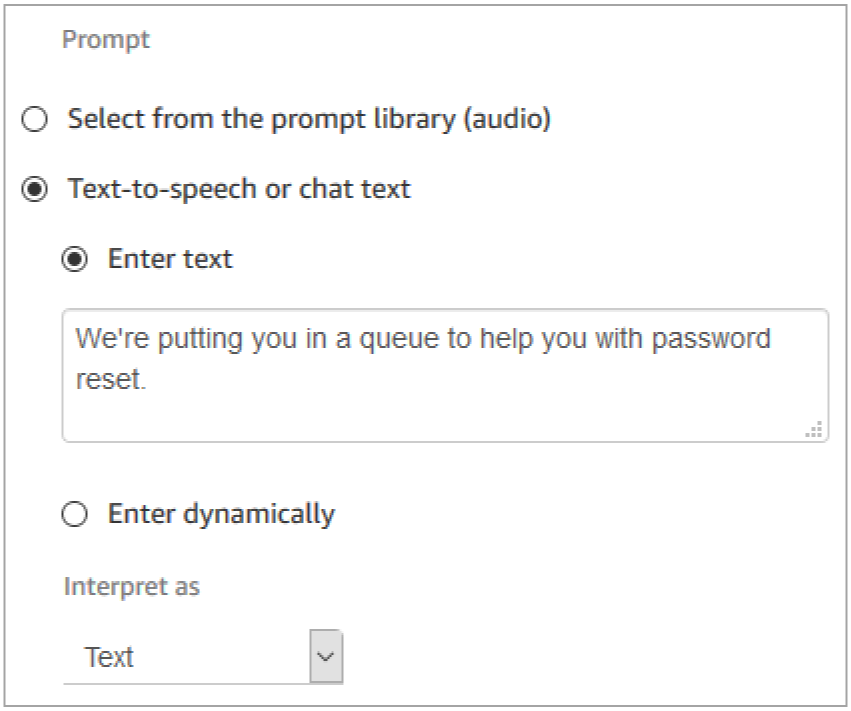
× DeviceIssue

Add another intent

15. Choose **Save**.
16. Add a **Play prompt** block (from the **Interact** group) and connect it to the **PasswordReset** branch.



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



Prompt

○ Select from the prompt library (audio)

● Text-to-speech or chat text

● Enter text

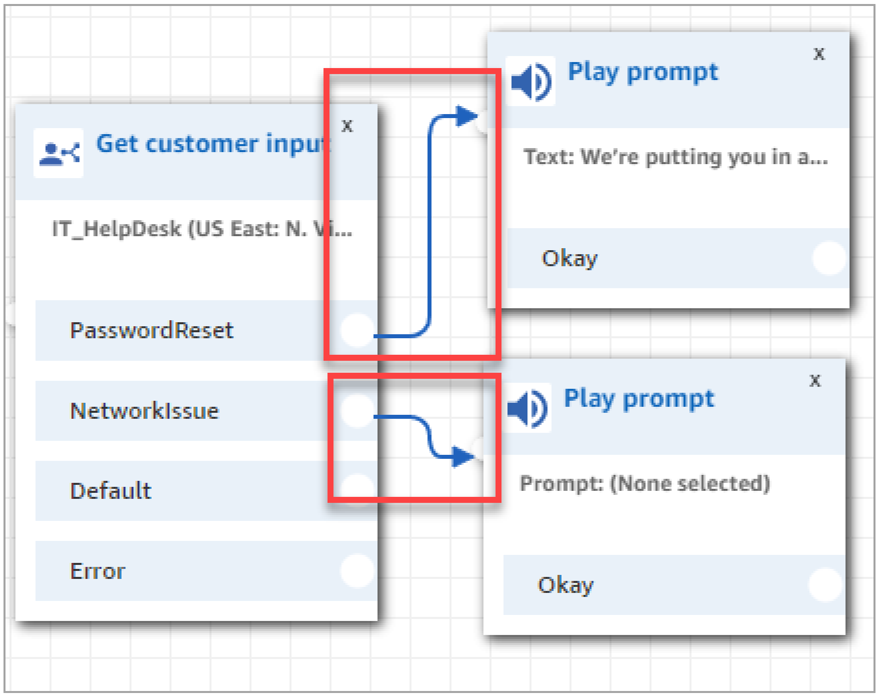
We're putting you in a queue to help you with password reset.

○ Enter dynamically

Interpret as

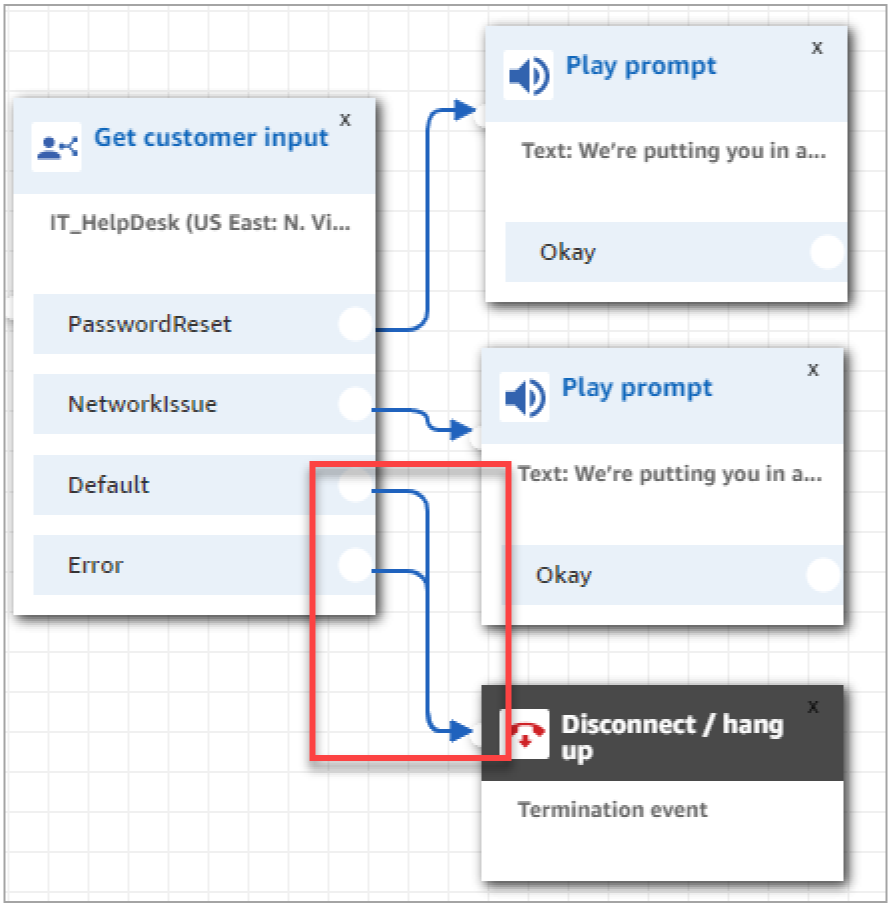
Text

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

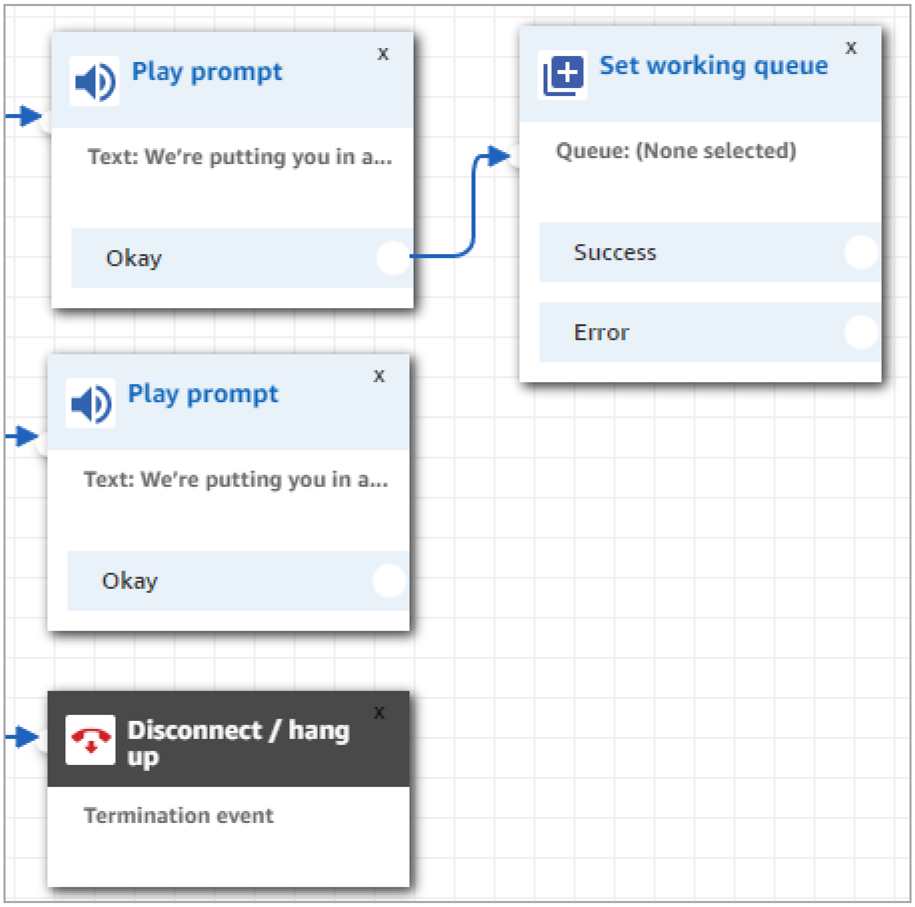


19. Choose the **Play prompt** title to open its properties page. Configure the **Play prompt** block with the message *We're putting you in a queue to help you with your network issues.* Choose **Save**.

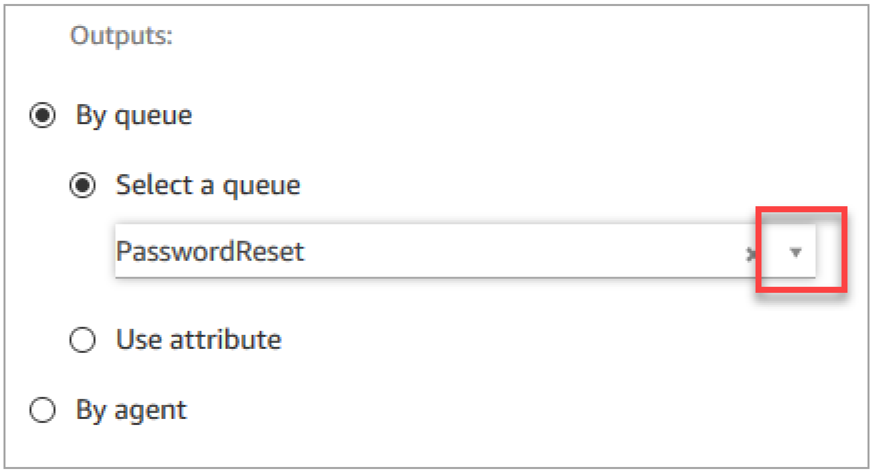
20. Add a Disconnect / hang up (p. 362) block (from the **Terminate/Transfer** group) to the grid. Connect the **Default** and **Error** branches to it.



21. Add a Set working queue (p. 421) block (from the **Set** group) to the grid. Connect the **Play prompt**.



22. Choose the **Set working queue** title to open its properties page. Configure the **Set working queue** block by using the drop-down arrow to choose the **PasswordReset** queue. Choose **Save**



Outputs:

● By queue

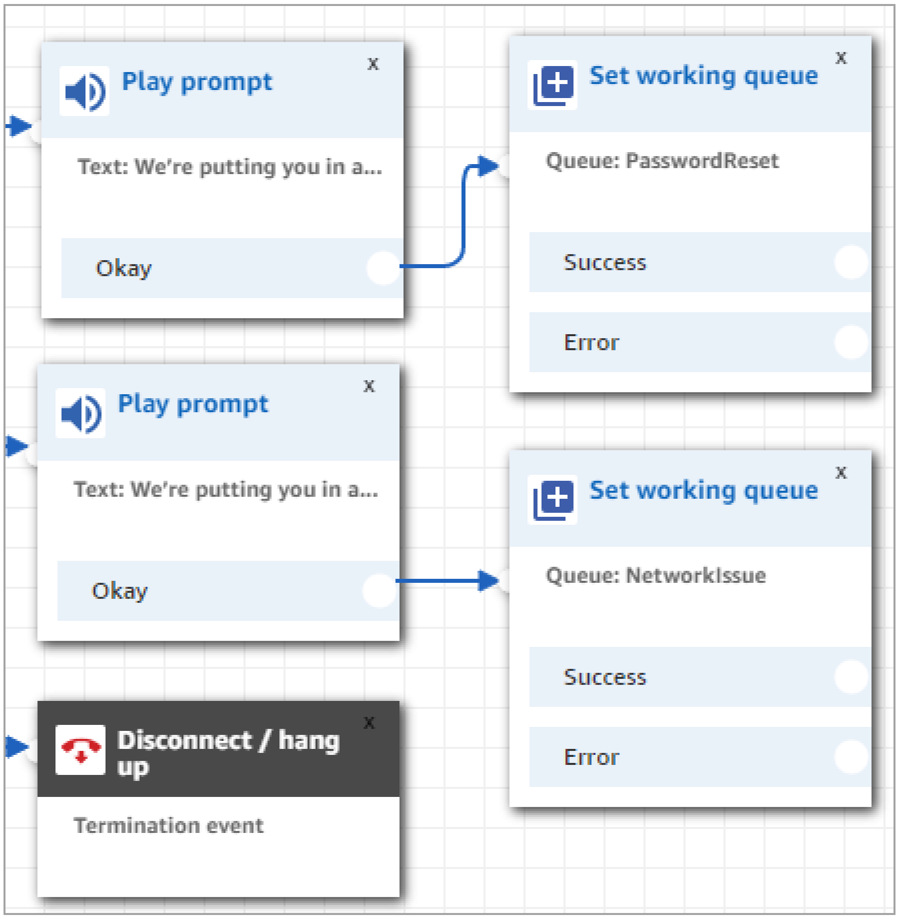
● Select a queue

PasswordReset

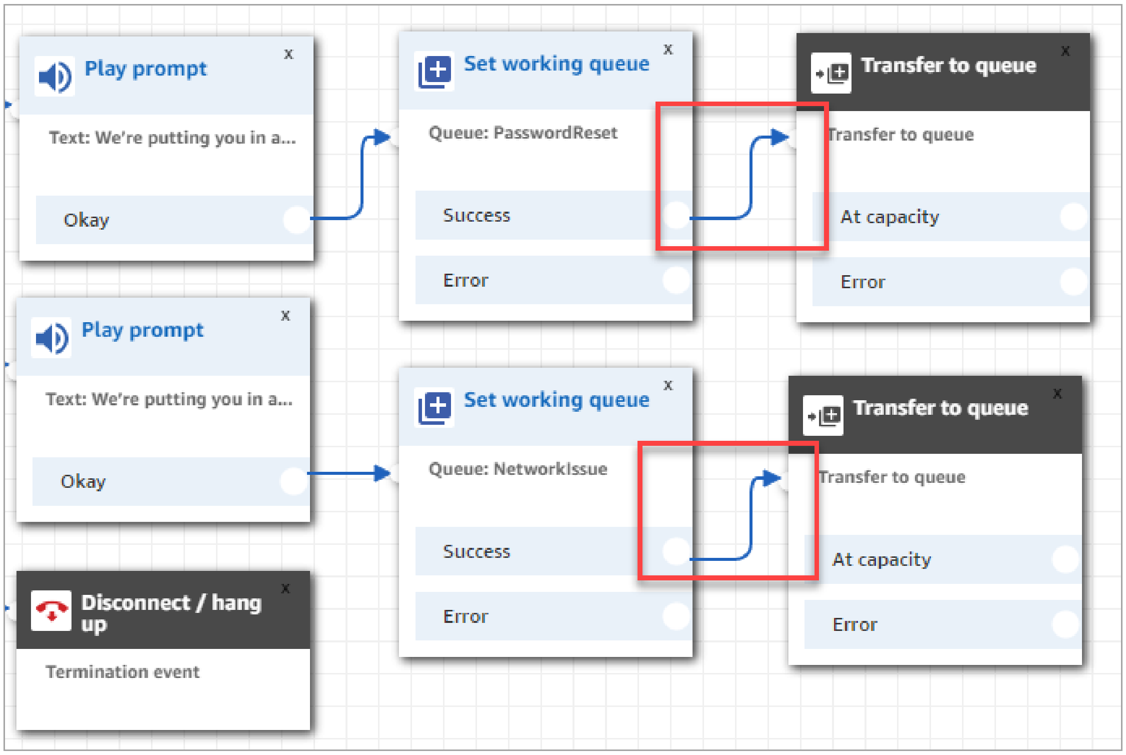
○ Use attribute

○ By agent

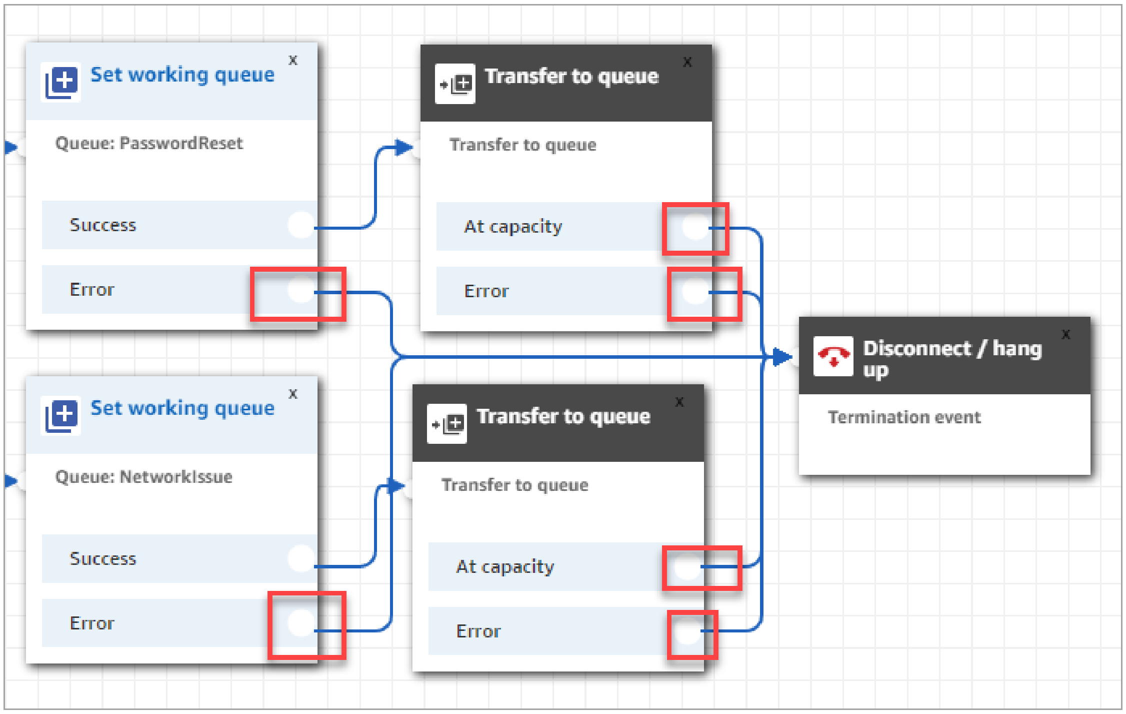
23. Add a **Set working queue** block for NetworkIssue, and configure it with the NetworkIssue queue.



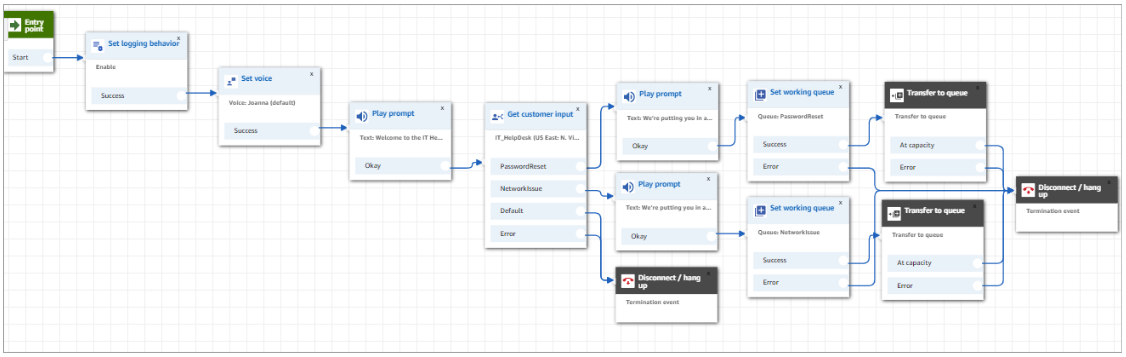
24. Drag two **Transfer to queue** blocks (from the **Terminate/Transfer** group) onto the grid.
25. Connect each of the **Set working queue** blocks to a **Transfer to queue** block, as shown in the following image.



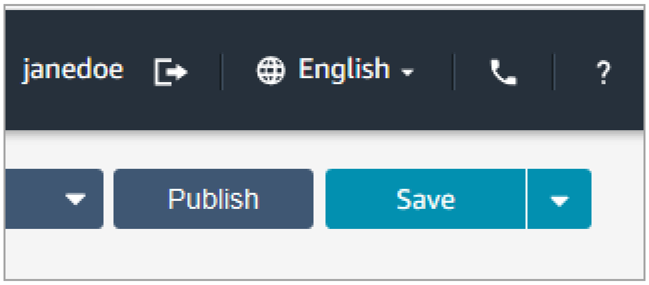
26. Drag another **Disconnect/hang up** block onto the grid. Connect all of the remaining **Error** and **At capacity** branches to it.



27. The completed contact flow looks similar to the following image.

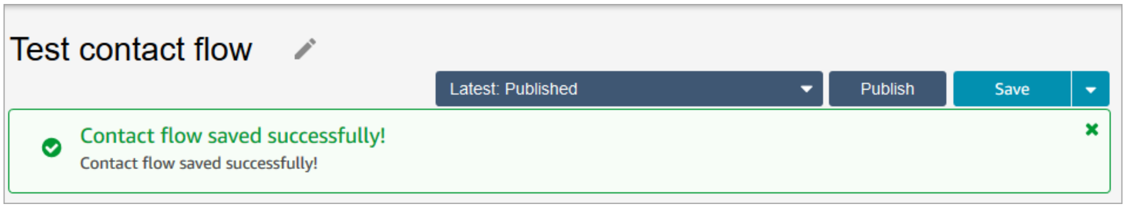


28. Choose **Save**, and then choose **Publish**.



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

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

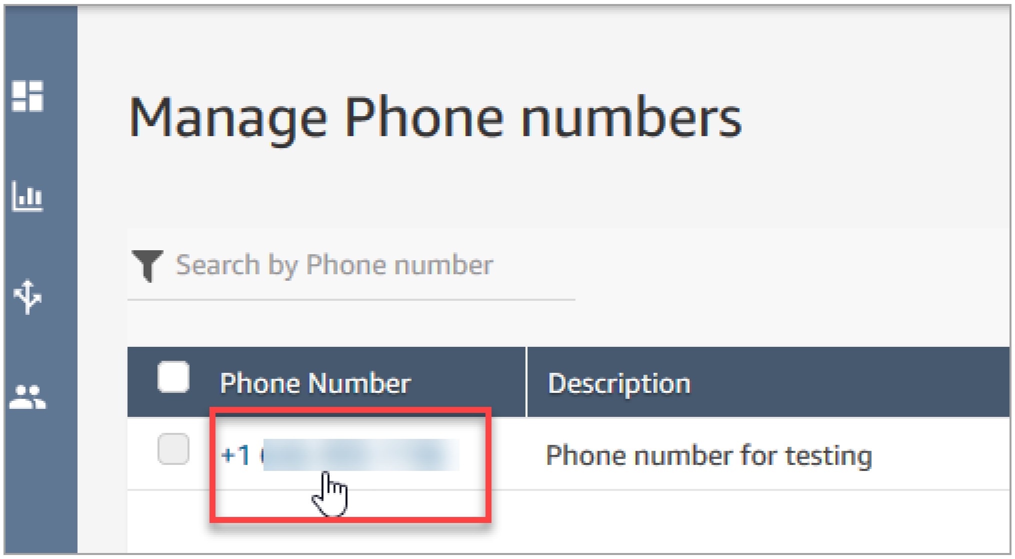


Contact flow saved successfully!
Contact flow saved successfully!

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

Step 5: Assign the contact flow to the phone number

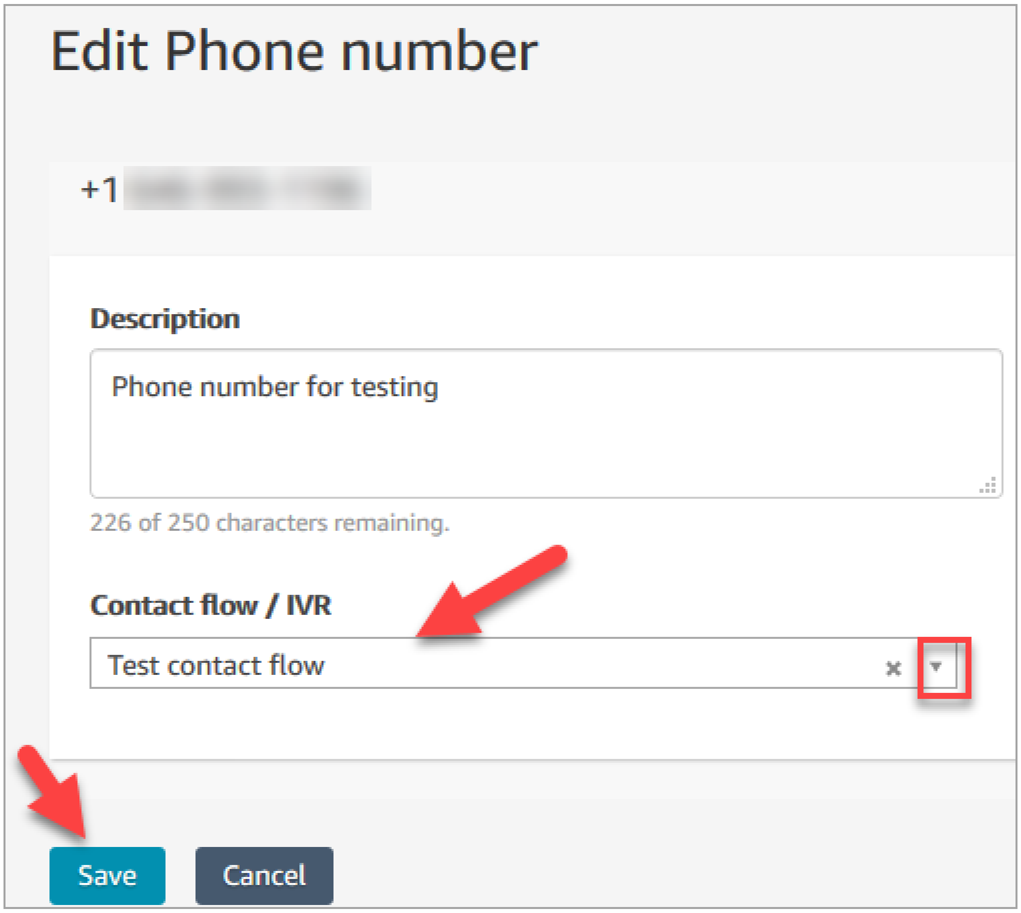
1. On the navigation menu, go to **Channels**, **Phone Numbers**.
2. Choose your phone number.



Manage Phone numbers

□ Phone Number	Description
□ +1 [redacted]	Phone number for testing

3. Use the drop-down box to choose the contact flow you just created, and then choose **Save**.



Edit Phone number

+1 [redacted]

Description

Phone number for testing

226 of 250 characters remaining.

Contact flow / IVR

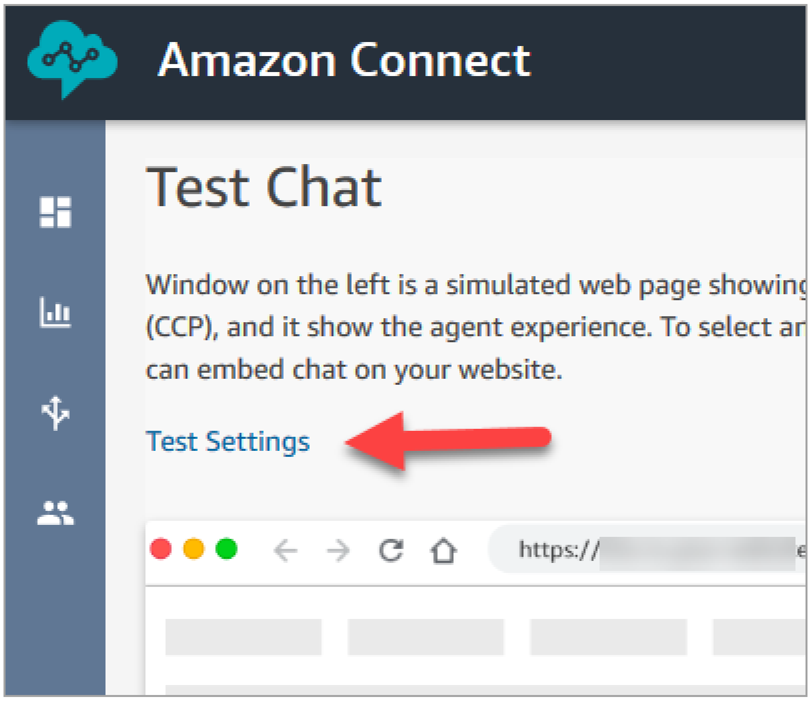
Test contact flow

Everything is all set up! Now you're ready to test your IT Help Desk. Go to Step 6: Test a custom voice and chat experience (p. 76).

Step 6: Test a custom voice and chat experience

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

1. On the navigation menu, go to the **Dashboard** and choose **Test chat**.
2. Choose **Test Settings**.

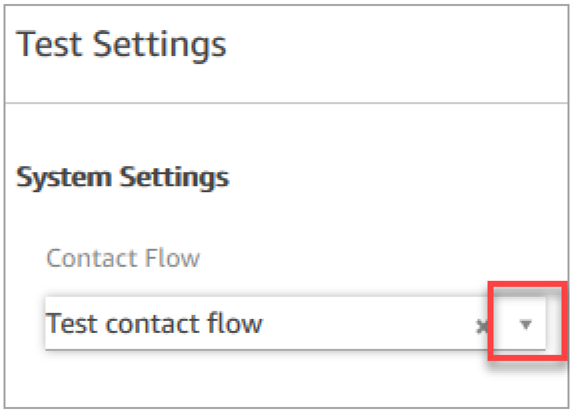


Amazon Connect

Test Chat

Window on the left is a simulated web page showing
(CCP), and it show the agent experience. To select ar
can embed chat on your website.

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



Test Settings

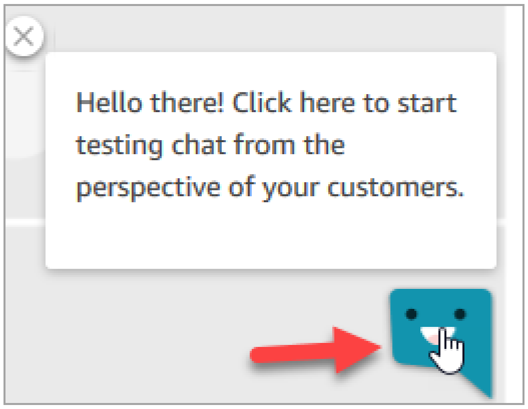
System Settings

Contact Flow

Test contact flow

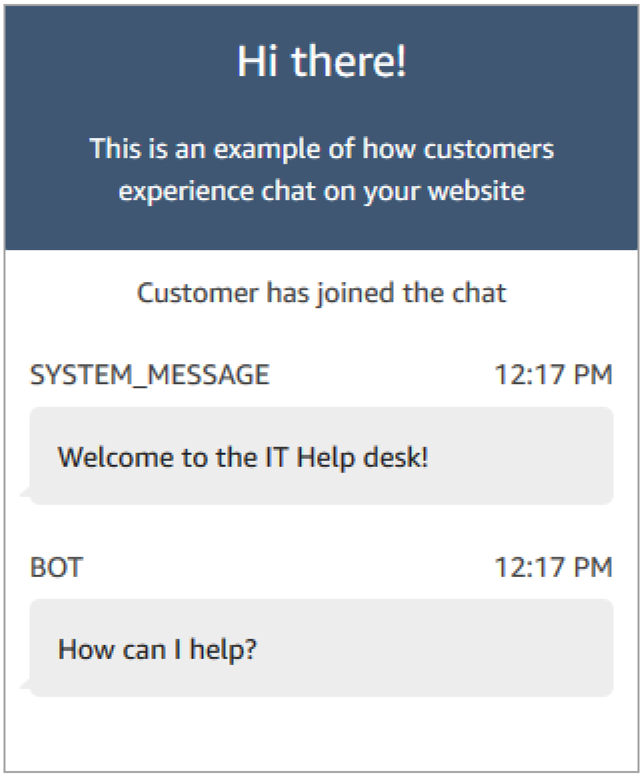
Test a custom chat experience

1. If needed, choose the chat bubble to start a chat.



Hello there! Click here to start testing chat from the perspective of your customers.

2. Amazon Connect automatically detects a contact and runs the contact flow that you created.



Hi there!

This is an example of how customers experience chat on your website

Customer has joined the chat

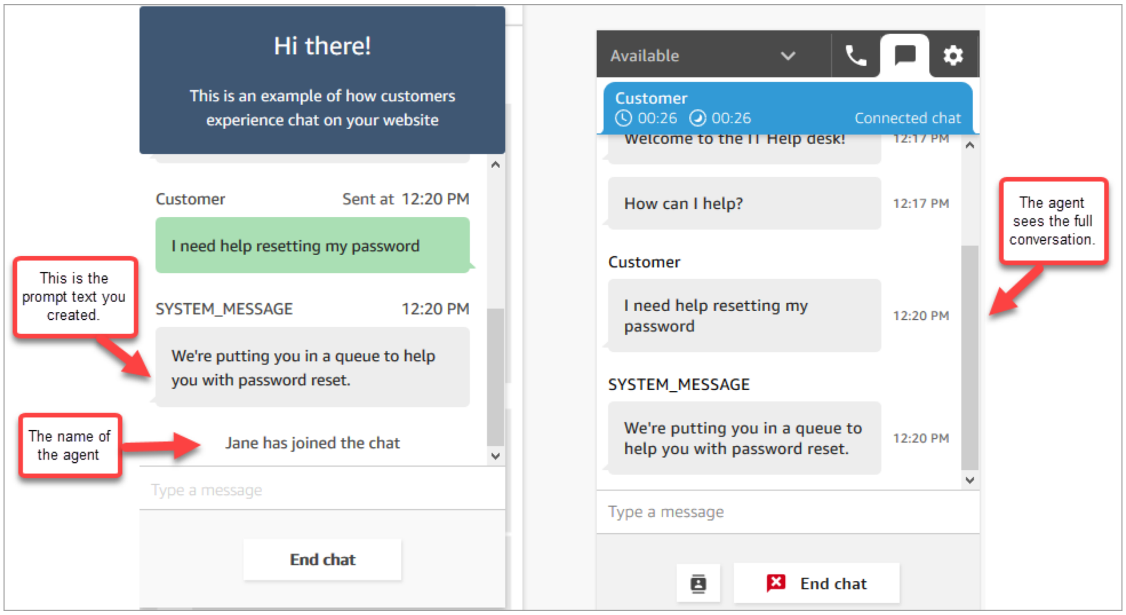
SYSTEM_MESSAGE 12:17 PM

Welcome to the IT Help desk!

BOT 12:17 PM

How can I help?

3. Enter that you need help resetting a password. Then accept the incoming chat. The following image shows you what the chat and agent interfaces look like when you're trying them.



Hi there!

This is an example of how customers experience chat on your website

Customer Sent at 12:20 PM

I need help resetting my password

SYSTEM_MESSAGE 12:20 PM

We're putting you in a queue to help you with password reset.

Jane has joined the chat

Welcome to the IT Help desk! 12:17 PM

How can I help? 12:17 PM

Customer

I need help resetting my password 12:20 PM

SYSTEM_MESSAGE

We're putting you in a queue to help you with password reset. 12:20 PM

This is the prompt text you created.

The name of the agent

The agent sees the full conversation.

4. In the customer pane on the right, choose **End chat** to close the chat window.
5. In the test CCP, choose **Close contact** to end the After Contact Work (ACW).

Test a custom voice experience

1. If the test chat window is still open, choose **End chat** to close it. Then you can try the voice experience.
2. Call your phone number.
3. When prompted, say *I'm having trouble accessing the internet*. You should hear the message that you're being transferred to the NetworkIssue queue.

   Tip
   After you're transferred, you'll hear this message:
   Thank you for calling. Your call is very important to us and will be answered in the order it was received.
   This message is generated by a default contact flow (p. 297) named Default customer queue (p. 303).
4. Go to the test CCP and accept the incoming call.
5. After you accept the call, but before you're connected to the customer, you'll hear an inbound whisper stating what queue the contact is in, for example, NetworkIssue. This helps you know what the customer is calling about.

   The inbound whisper is generated by a default contact flow (p. 297) named Default agent whisper (p. 305).
6. When done, end the call.
7. In the CCP, choose **Clear contact** to end After Contact Work (ACW).

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

> **Tip**
> If you don't want to keep the phone number that you claimed for testing, you can release it back to inventory. For instructions, see Release a phone number (p. 170).

Architectural guidance for Amazon Connect

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

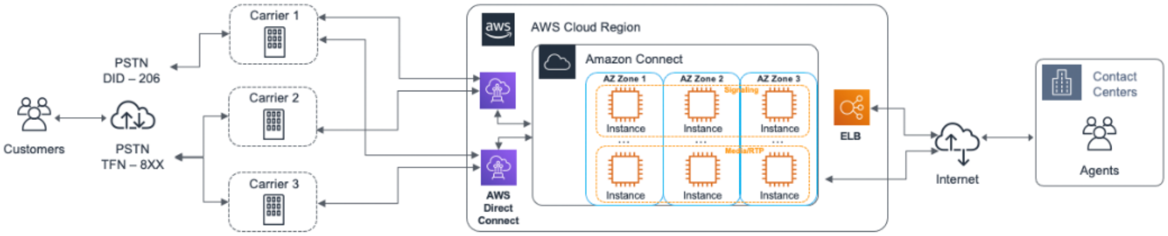
This content is intended for chief technology officers (CTOs), architects, developers, and operations team members.

Contents

Amazon Connect workload layers

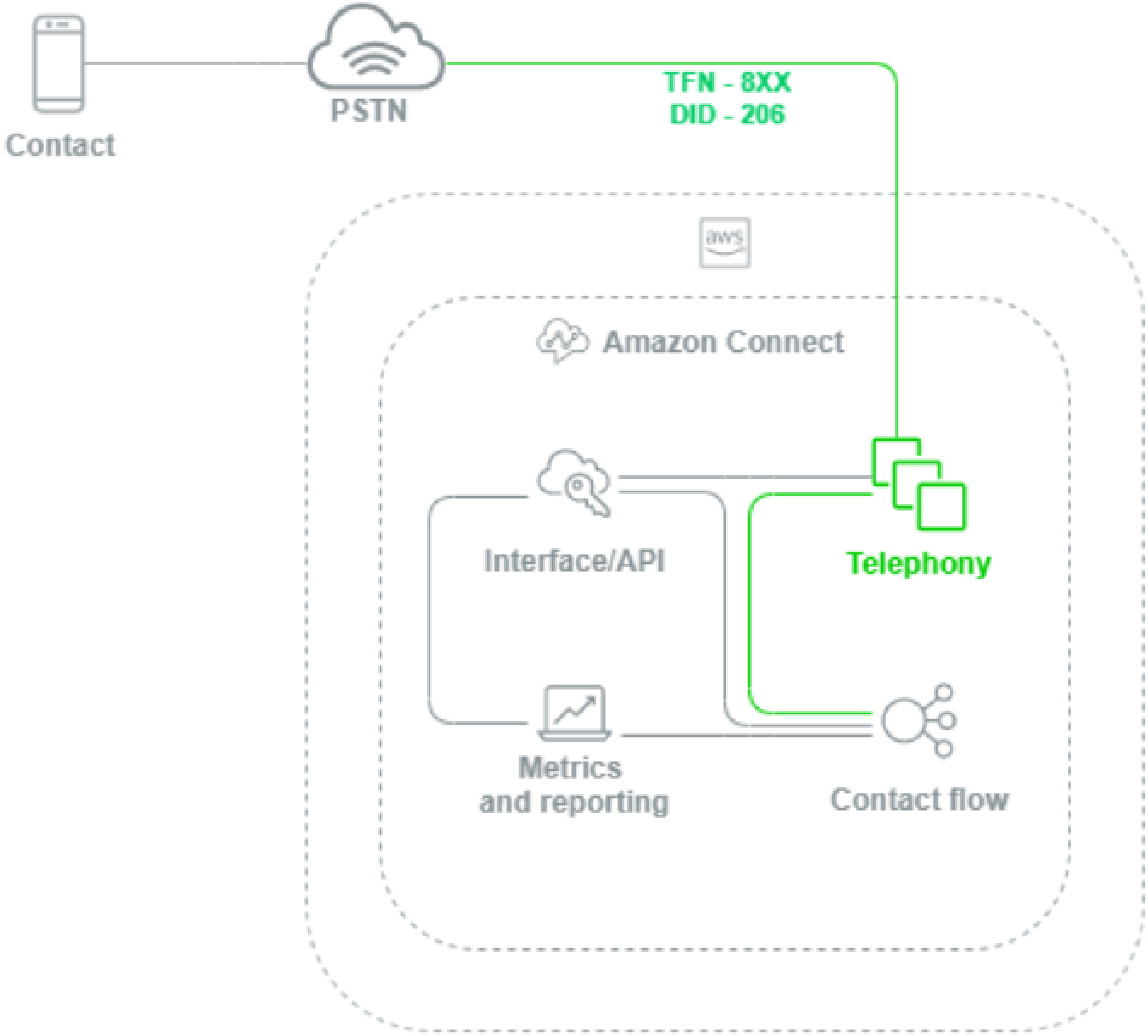
You can separate Amazon Connect workloads into the following layers: telephony, Amazon Connect interface/API, flows/IVR, agent workstation, and metric and reporting.

Telephony



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

Zone experiences failure, the affected endpoint is taken out of rotation, allowing you to continue to provide a consistent quality experience for your customers.



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

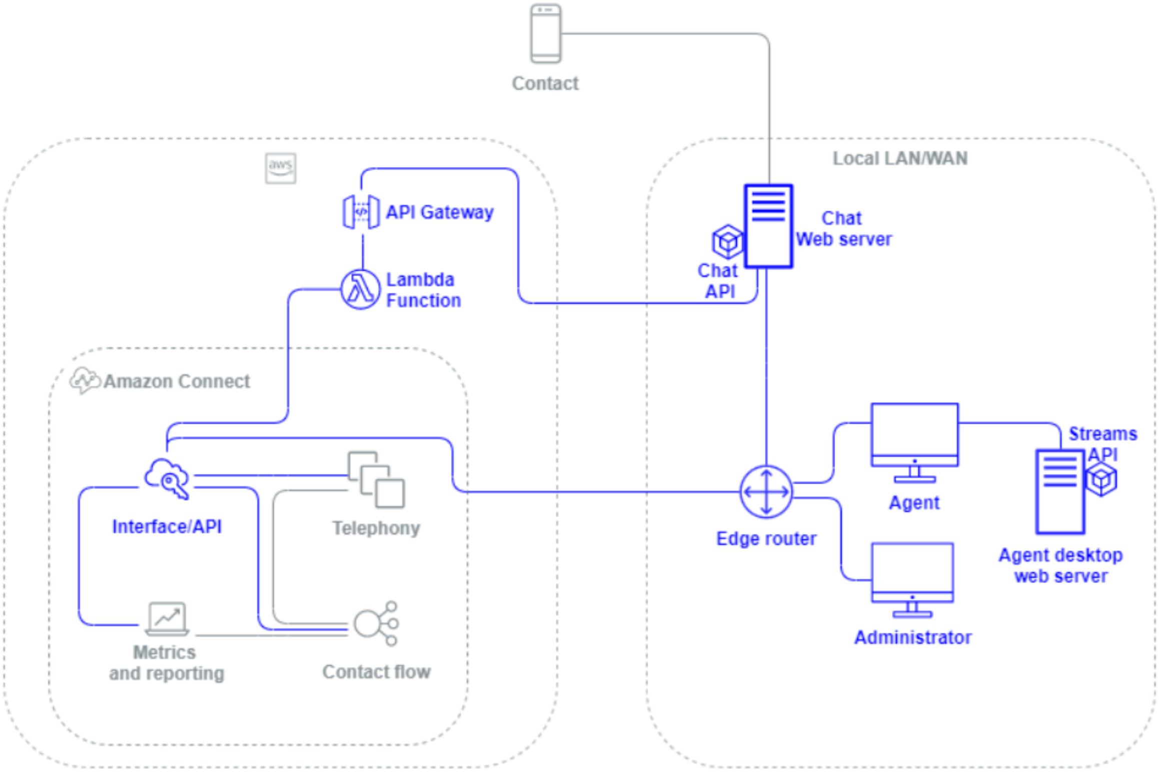
Amazon Connect Interface/API

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

- Single Sign-On (SSO) integration user authentication

- Custom desktop applications created using the Amazon Connect Streams API that may provide additional functionality and/or integrate with existing Customer Relationship Management (CRM) systems including the Amazon Connect Salesforce CTI Adapter (p. 294).
- Amazon Connect contact-facing chat interface
- Chat web server hosting the Amazon Connect Chat API
- Any Amazon API Gateway endpoints and corresponding AWS Lambda functions necessary to route chat contacts to Amazon Connect.

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

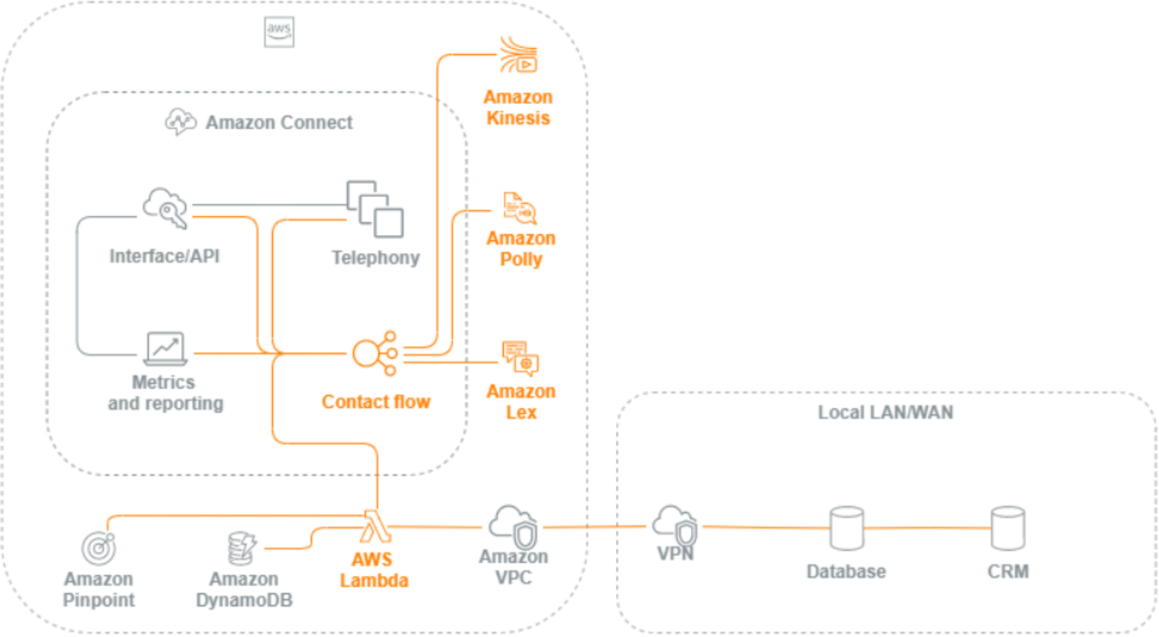


Contact flow / IVR

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

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

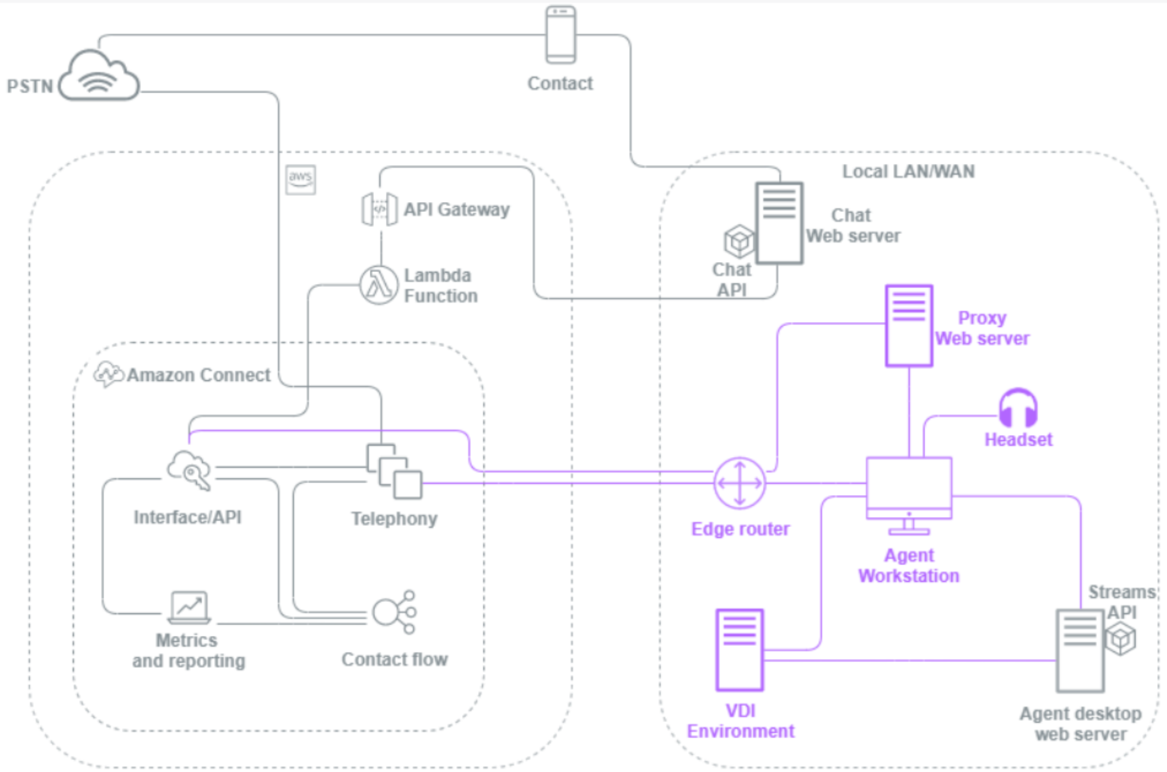
Contact flows enable you to dynamically prompt contacts, collect and store contact attributes, and route appropriately. You can assign a contact flow to multiple phone numbers, and manage and configure it through Amazon Connect.



Agent workstation

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

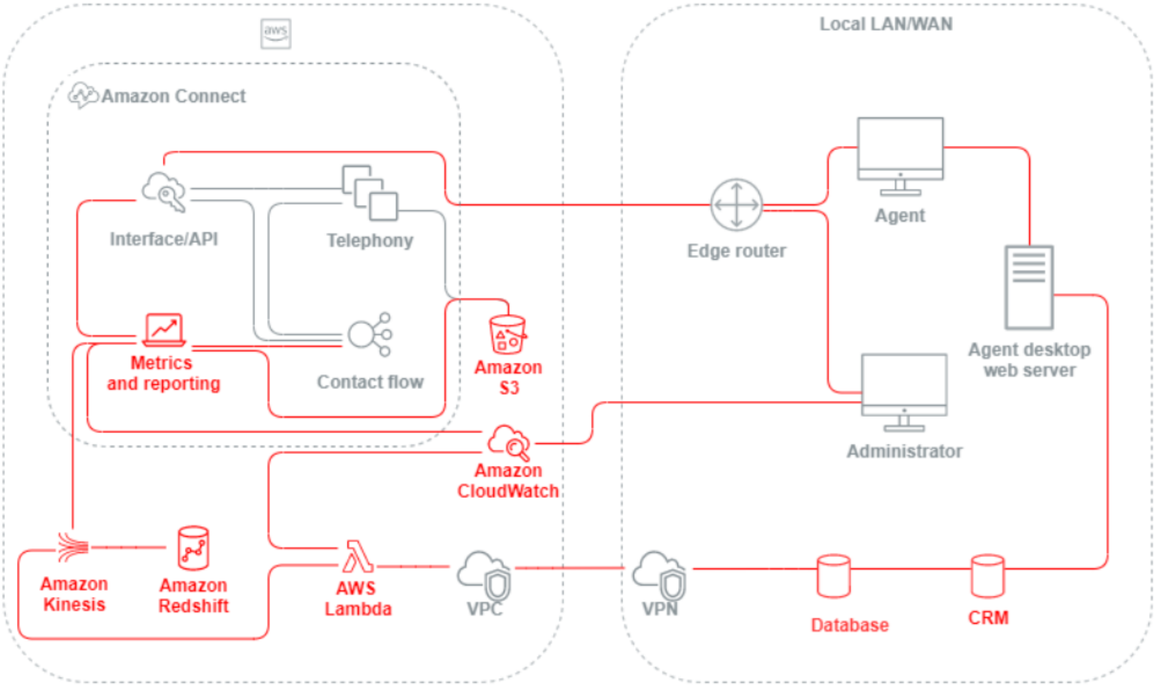
- The Contact Control Panel (CCP) agent hardware
- Network path
- Agent headset or handset
- VDI environment
- Operating system and web browser
- Endpoint security
- All networking components and infrastructure
- Internet Service Provider (ISP) or AWS Direct Connect dedicated network path to AWS.
- All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



Metric and reporting

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

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



Scenario and deployment approaches

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

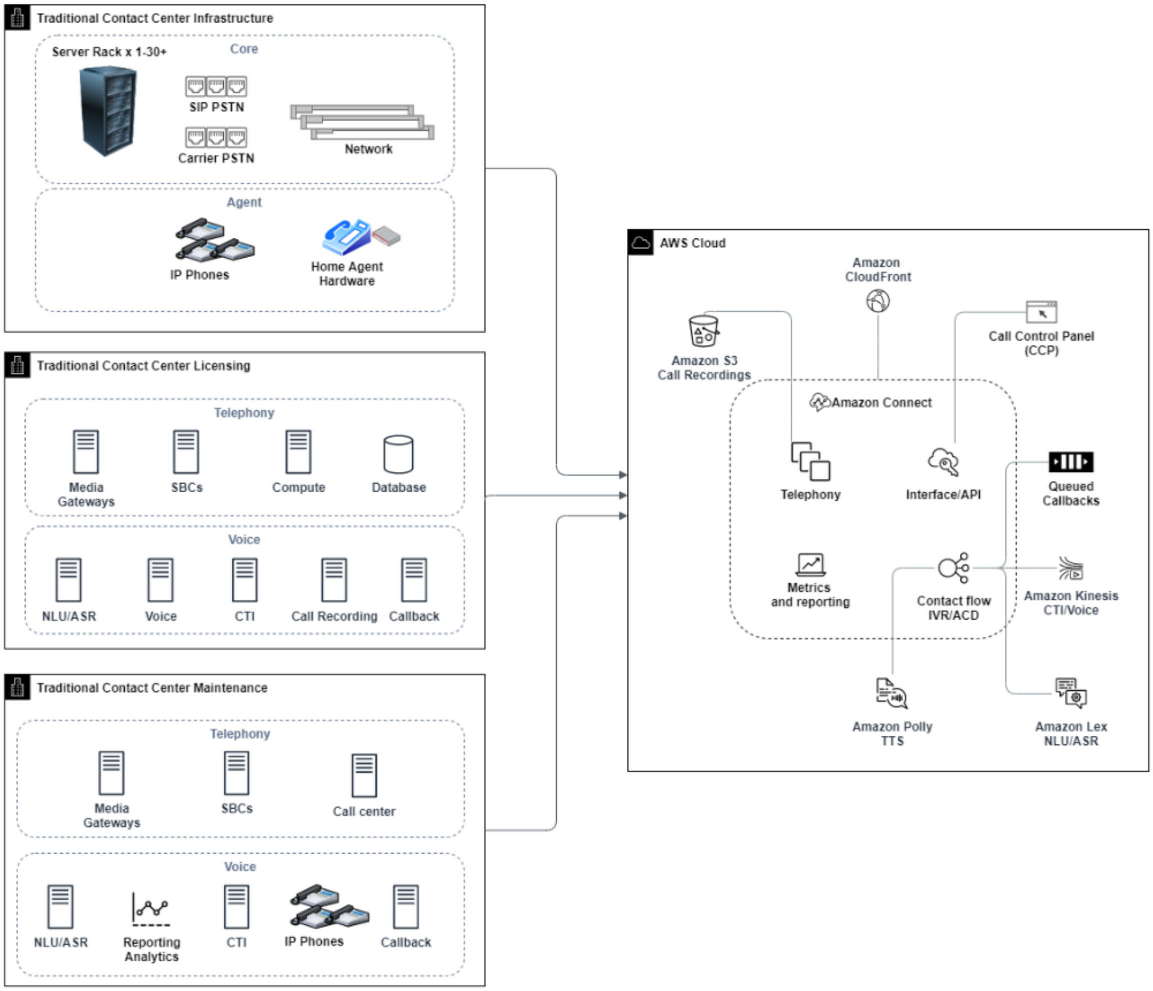
- Traditional contact center
- Inbound
- Outbound
- Hybrid contact center
- Legacy contact center migration
- Virtual desktop infrastructure (VDI)

Traditional contact center

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

It is common to have separate vendors and infrastructure requirements for local and remote agent hardware and VPN connectivity, Text-To-Speech (TTS), Automatic Call Distribution (ACD), Interactive Voice Response (IVR), voice audio and data, physical desk phones, voice recording, voice transcriptions, chat, reporting, database, Computer Telephony Integration (CTI), Automatic Speech Recognition

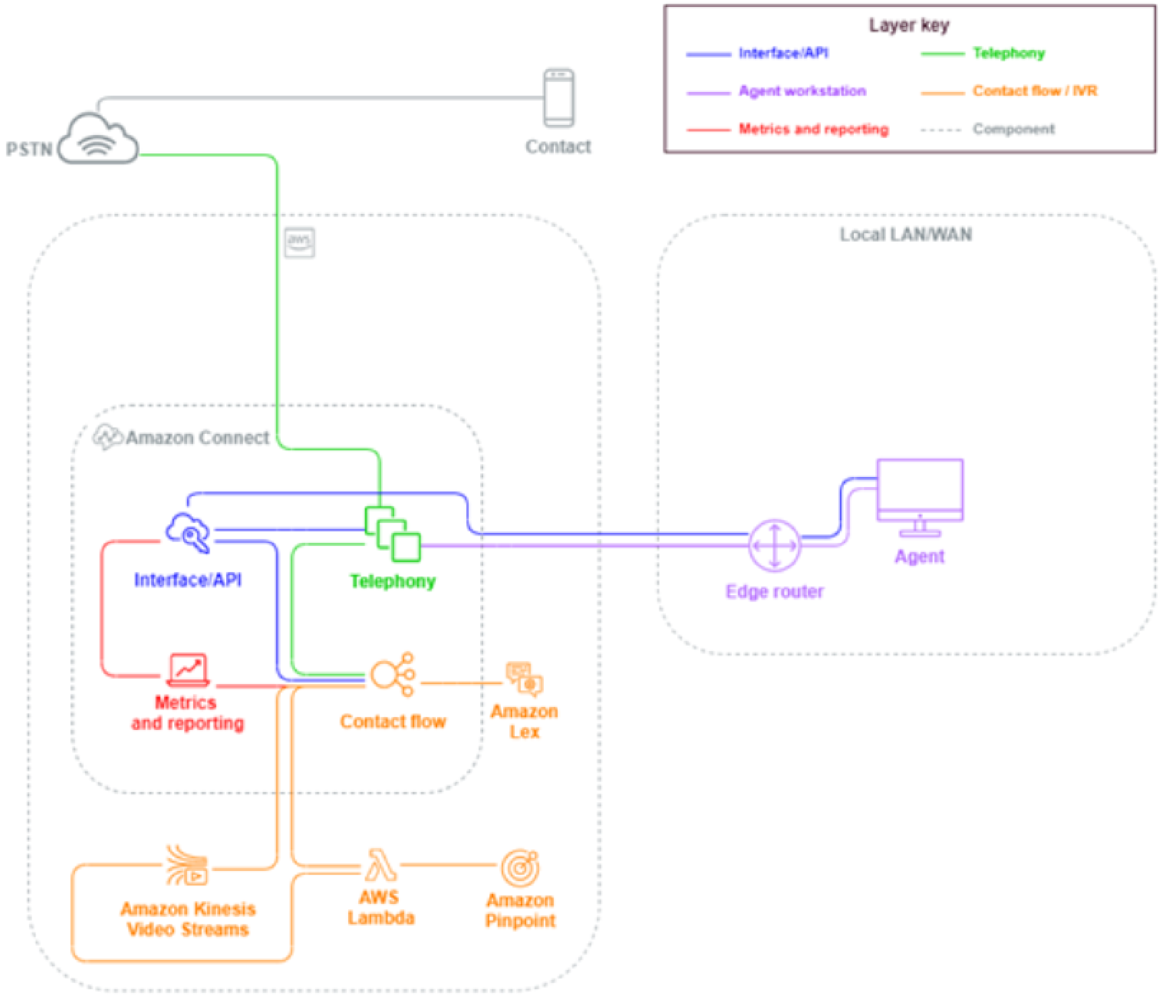
(ASR), and Natural Language Understanding (NLP). Your contact center architecture and infrastructure becomes more complicated when you consider multi-stage development, quality assurance, and test environments.



A typical Amazon Connect deployment solves or reduces many of the challenges associated with versioning, compatibility, licensing, contact center telephony infrastructure, and maintenance. It gives you the flexibility to create instances in new locations in minutes and migrate components individually, or in parallel, to best meet your individual business objectives. You can use contact flows for your IVR/ ACD, have voice and data delivered through a supported web browser to your agent's softphone, port your existing phone numbers, redirect softphone audio to an existing desk phone, invoke an Amazon Lex bot natively within your contact flow for ASR and NLP, and use the same contact flow for chat and voice. You can use Amazon Contact Lens to automatically generate voice transcriptions, perform key word identification and sentiment analysis, and categorize contacts. For agent CTI data and real-time voice streaming, you can use Amazon Connect Agent Event Streams and Kinesis Video Streams. You can also create multi-stage development, quality assurance, and test environments at no additional cost and only pay for what you use.

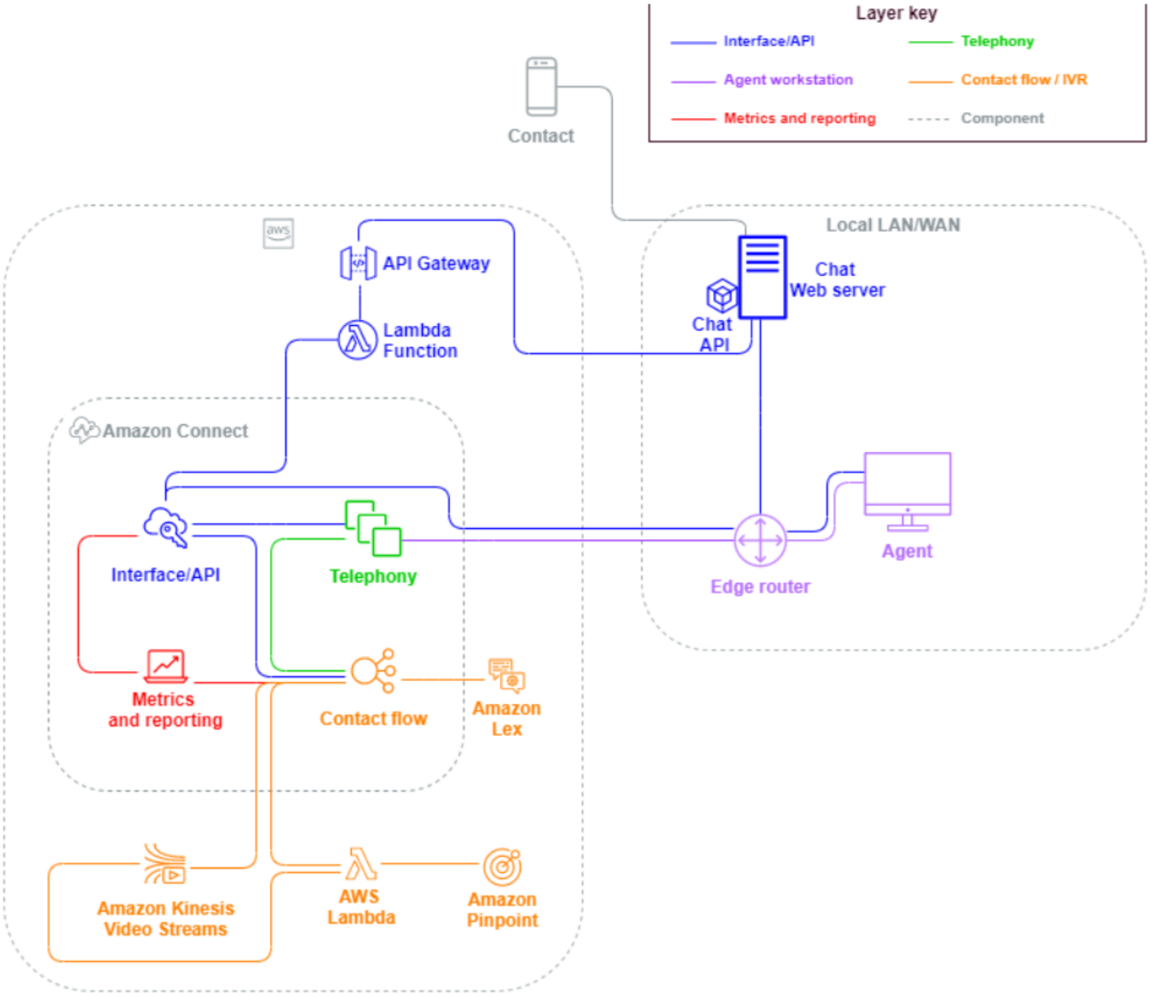
Inbound

Inbound is a contact center term used to describe a communication request initiated by a contact to the center. Contacts can reach your Amazon Connect instance for inbound self-service or to speak with a live agent in a variety of ways, including voice and chat. Voice contacts go through the PSTN and are routed to the Amazon Connect Instance telephony entry point through the phone number claimed in your instance. You can reserve a phone number with Amazon Connect directly, port your existing phone number, or forward voice contacts to Amazon Connect. Amazon Connect can provide local and toll-free numbers in all Regions where the service is supported.



When a phone call is placed to a number claimed in or ported to your Amazon Connect instance, the contact flow associated with the called number will be invoked. You can define the contact flow using contact blocks that can be configured with no coding knowledge required. The contact flow determines how the contact should be processed and routed, optionally prompting the contact for additional information to assist in routing decisions, storing those attributes to the contact details, and, if necessary, routing that contact to an agent with all of the call details and transcripts gathered along the way. Through the contact flow, you can invoke AWS Lambda functions to query customer information, call other AWS services like Amazon Pinpoint to send SMS text messages, and use native AWS service integrations including Amazon Lex for NLU/NLP and Kinesis Video Streams for real-time streaming of voice calls.

If an inbound contact needs to reach an agent, the contact is put into a queue and routed to an agent when they change their status to Available, according to your routing configuration. When the available agent's contact is accepted manually or through auto-accept configuration, Amazon Connect connects the contact with the agent.



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

Outbound

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

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

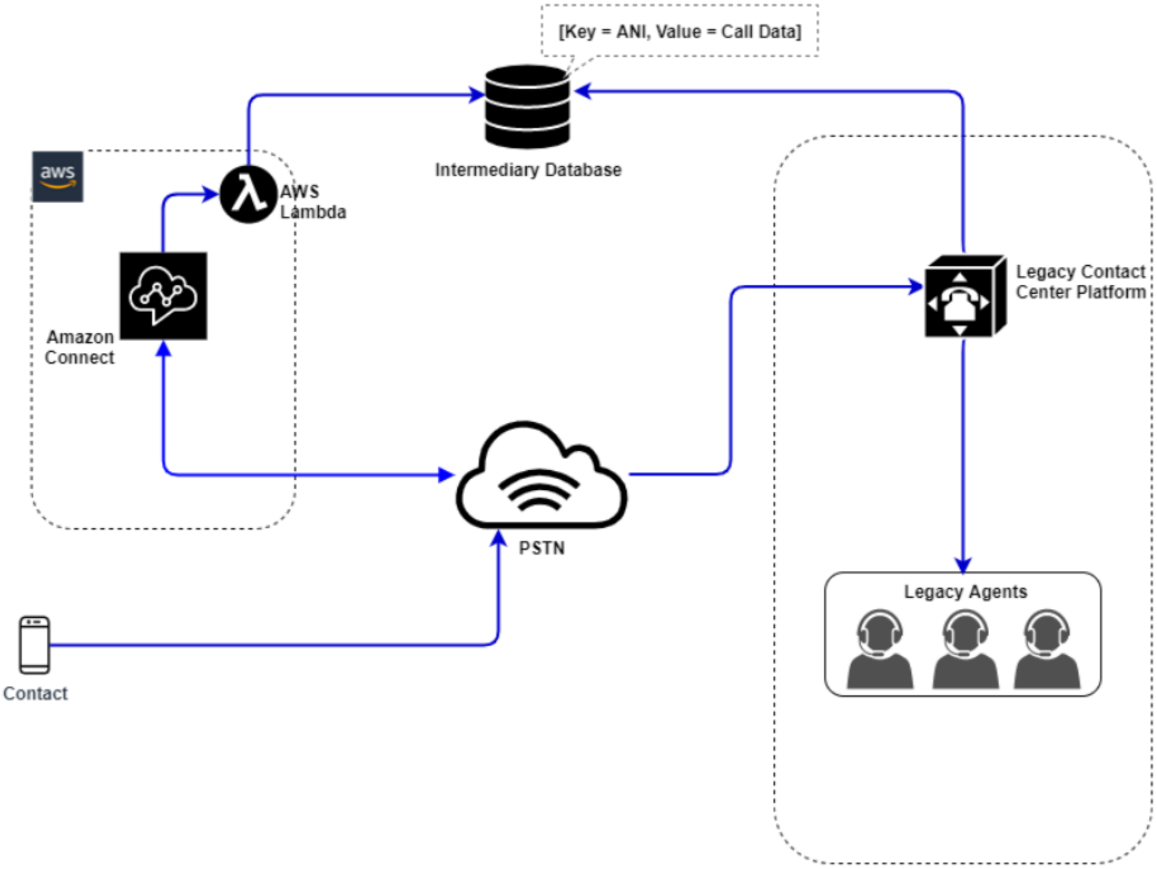
Hybrid

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

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

IVR-only

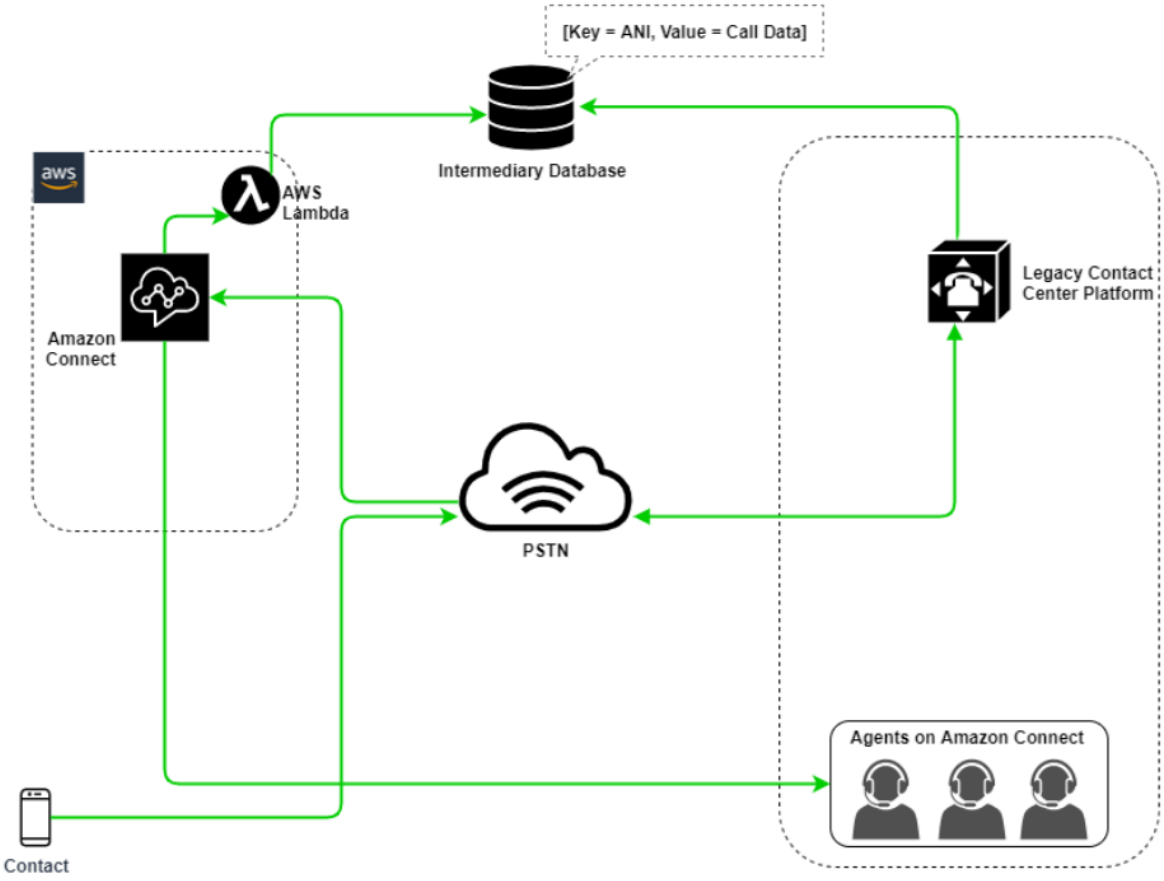
You may choose to use Amazon Connect to drive the contact's IVR experience while your agent population remains on your legacy contact center platform. With this approach, you can use Amazon Connect contact flows to drive self-service and routing logic, and, if necessary, transfer the contact to the target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



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

Agent-only

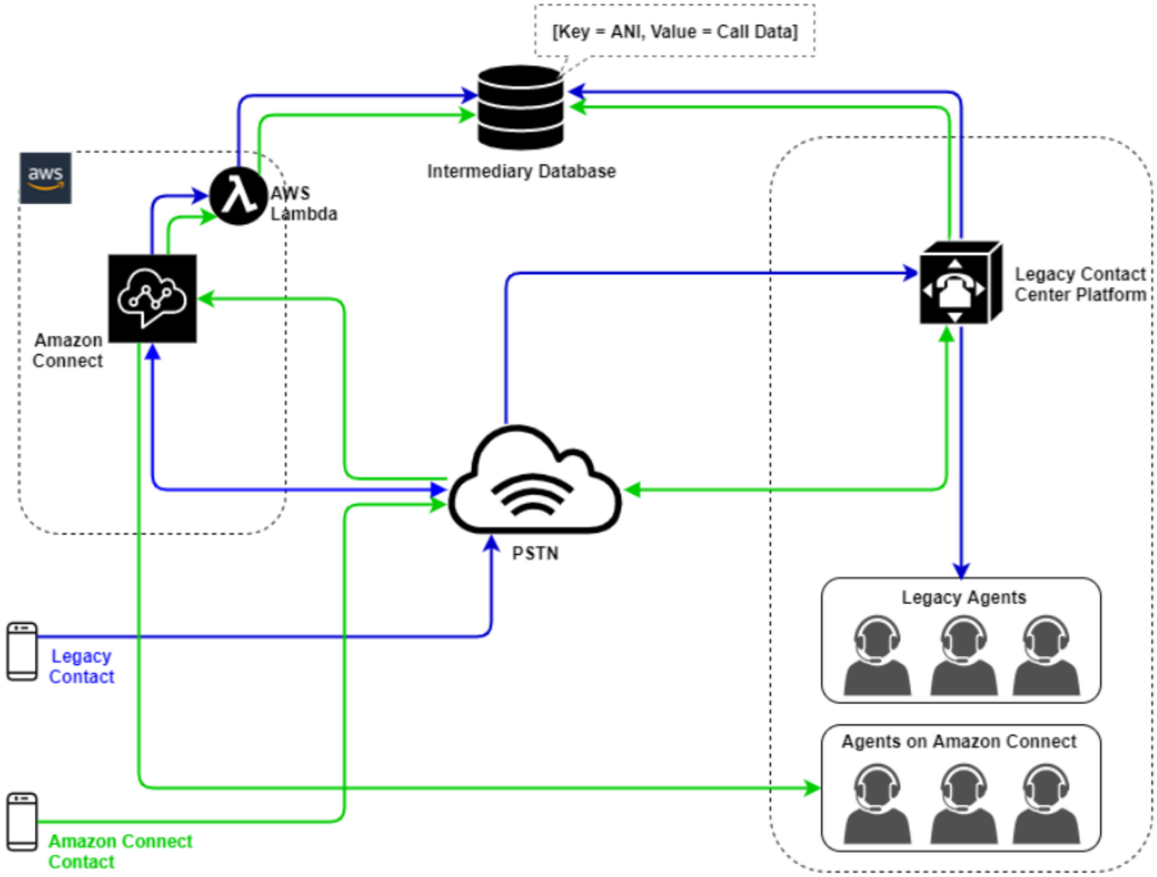
With this approach, your legacy contact center IVR drives the contact's IVR self-serve and routing logic, and, if necessary, transfers the contact to Amazon Connect to route to your agent population.



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

Mixed

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



Legacy contact center migration

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

New workload

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

IVR First

You may choose to use Amazon Connect to drive the contact's IVR experience while your agent population remains on your legacy contact center platform. With this approach, you can use Amazon

Connect Contact flows to drive self-service and routing logic, and, if necessary, transfer the contact to the target agent or agent queue on your legacy contact center platform.

IVR Last

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

Line of business segmentation

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

Site or agent group segmentation

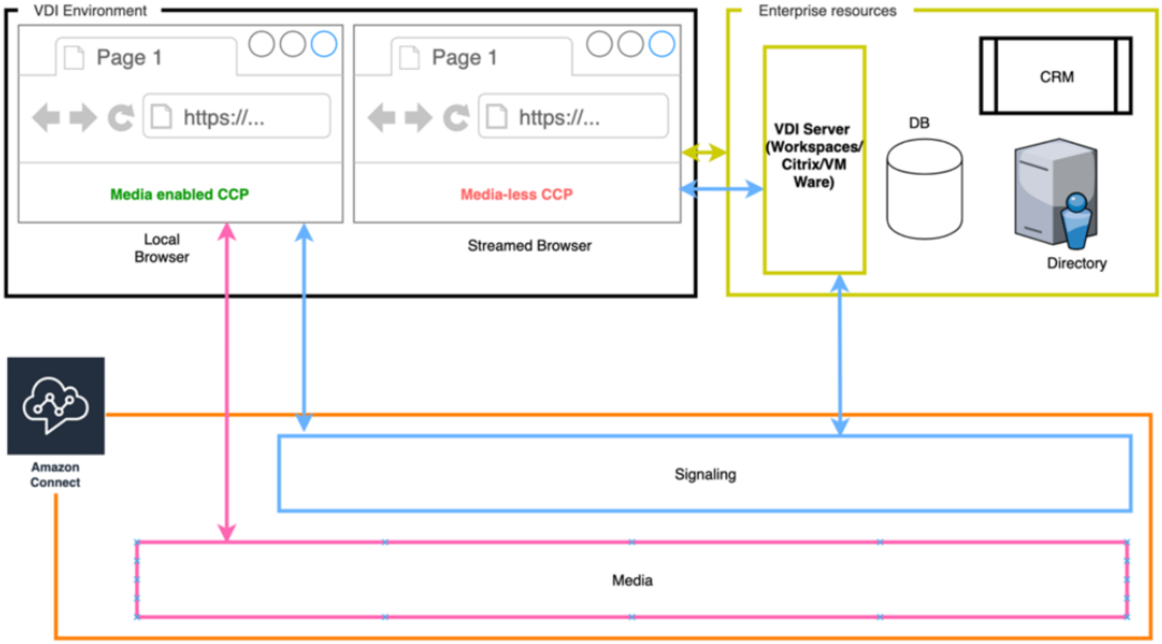
If your contact center has a global footprint, services contacts from multiple countries, or is managed independently by a respective geography or location, you may want to consider a migration approach based on a physical site or geography of agents. Each agent population and/or geography can have its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

Virtual desktop infrastructure (VDI)

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

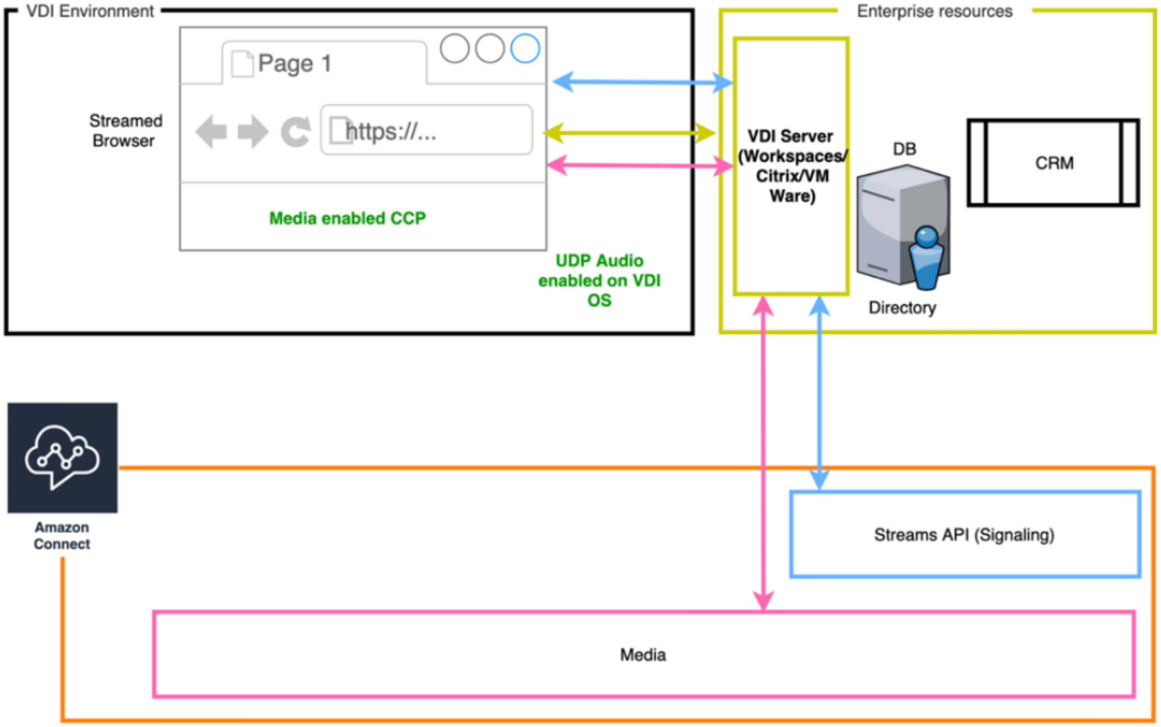
VDI client with local browser access

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



VDI client without local browser access

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



Operational Excellence

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

Prepare

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

AWS account

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

Region selection

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

Telephony

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

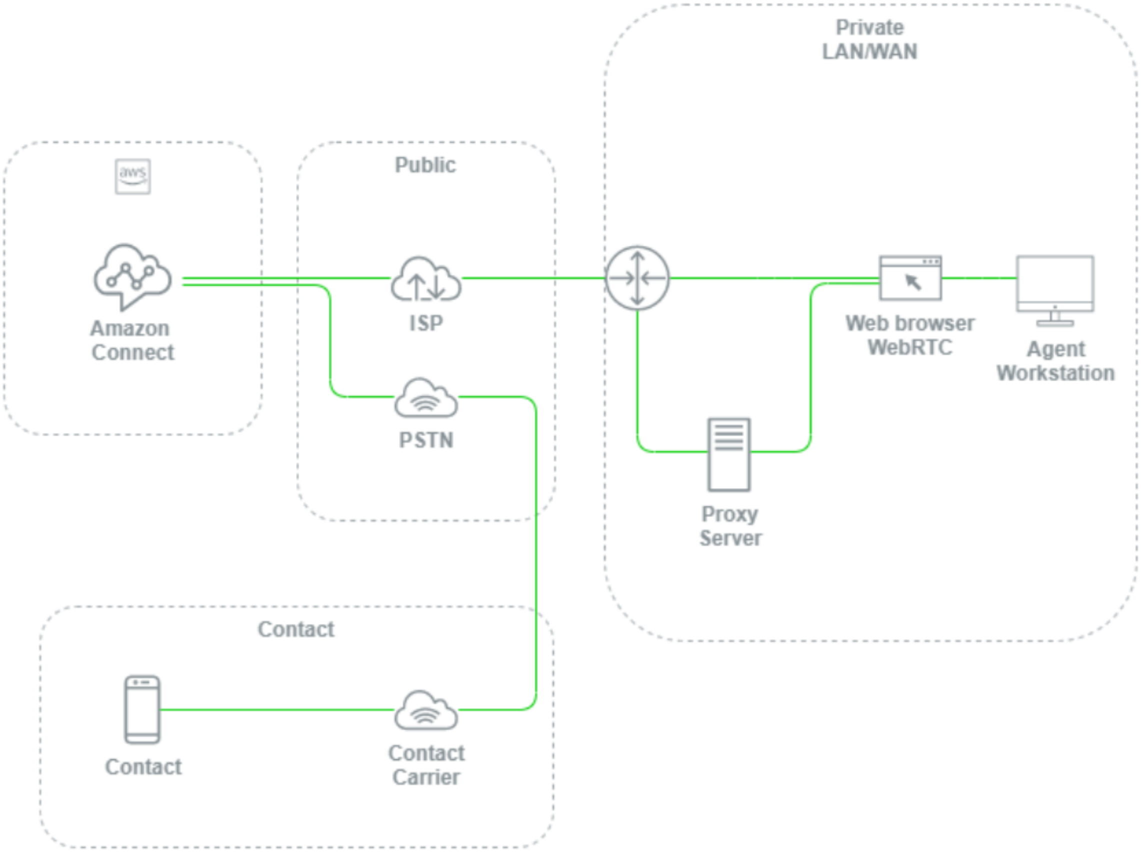
  When porting phone numbers for critical workloads, include all requirements and use case information in your claim/port number several months before the go-live date. This includes requests for live cutover support, communication prior, during, and after cutover, monitoring, and anything else specific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

  For detailed information about porting your numbers, see Port your current phone number (p. 157).
- **Carrier diversity** In the US, you should use Amazon Connect telephony services for US toll-free numbers, allowing you to route toll-free traffic across multiple suppliers in an active-active fashion at no additional charge. In situations where you are forwarding inbound traffic to an Amazon Connect phone number, you should request redundant DID or Toll-Free numbers across multiple telephony providers. If you are claiming or porting multiple DID or Toll-Free numbers outside of the US, you should request that those numbers be claimed or ported to a variety of telephony providers for increased resiliency.
- **International toll-free and high-concurrency DIDs** If you are using an existing toll-free national service to redirect inbound traffic to DIDs, you should request DID phone numbers across multiple telephony providers. A general recommendation for this configuration is 100 sessions per-DID and your AWS Solutions Architect can help with capacity calculations and setup.
- **Testing** Thoroughly test all use case scenarios, preferably using the same or similar environment as your agents and customers. Ensure that you test several inbound and outbound scenarios for quality of experience, Caller ID functionality, and measure latency to ensure it falls within acceptable range for your use case. Any deviations from your target agent and customer environments need to be measured and accounted for. For more information, including use case testing instructions and criteria, see Troubleshooting Issues with the Contact Control Panel (CCP) (p. 1193).

Agent workstation

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

- Set Up Your Network for CCP use and ensure that your agent hardware meets minimum requirements.
- Ensure that you have used the Amazon Connect Check Amazon Connectivity Tool on the same network segment as your agents to verify that your network and environment is configured correctly for CCP use.
- Calculate PSTN latency for use cases that require agents and contacts to be in geographically distant locations
- Review the Troubleshooting Issues with the Contact Control Panel (CCP) (p. 1193) section to create runbooks and playbooks for your agents and supervisors to follow should they encounter issues.
- Set up monitoring for your agent workstations and consider partner solutions for call quality monitoring. Your goal with monitoring your agent workstations should be the ability to identify the source of any potential network and resource contention. For example, consider a typical agent's softphone network connection path to Amazon Connect:



Without setting up monitoring at the local LAN/WAN, path to AWS, and agent workstation levels, it's difficult and often impossible to determine if a voice quality issue is originating from your agent's workstation, their private LAN/WAN, ISP, AWS, or the contact itself. Setting up logging and alerting mechanisms proactively is critical in determining root cause and optimizing your environment for voice quality.

Configure your existing directory

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

Service Quotas

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

AWS Enterprise support

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

AWS well-architected review

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

Operate

Consider the following areas to operate an Amazon Connect workload.

Logging and monitoring

See Monitoring your instance using CloudWatch (p. 1014) and Logging Amazon Connect API calls with AWS CloudTrail (p. 1025).

Contact attributes

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

Note the following considerations:

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

- Data sensitivity – Note if any attributes being set, queried, and referenced are sensitive or fall under any regulatory guidelines and ensure that the data is being treated appropriately for your use case.
- Data persistence – Any attributes set using the Set contact attributes block will be included in the contact record for your contact and available for screen pop to any custom agent desktop using the Streams API. Any time the attribute is referenced within your contact flow and logging is enabled for the flow, the name and value of the attribute will be logged to Amazon CloudWatch.

Best practices

- Monitor usage – As you implement new functionality, onboard new business units, and iterate on existing contact flows, look up your current attribute usage in contact search, copy the attributes to a text editor, add the new attributes, and ensure that you do not exceed the 32KB size limitation. Be sure to account for variable length fields like firstName and lastName and ensure that, even when the maximum space is used in a field, that you are still below the 32KB limitation.
- Clean-up – If data persistence isn't required, you can set an attribute with the same name and a blank value to prevent the data from being stored to the contact record or passed in a screen pop to an agent using the Amazon Connect Streams API while freeing up the bytes that data would have otherwise used in the contact record.
- Sensitive data – Use the **Store customer input** block to collect sensitive DTMF input from your contacts and use envelope encryption to protect both the raw data and the data keys used to encrypt them. Store sensitive data in a separate database where persistence is required, use the **Set logging behavior** contact flow block to disable logging whenever sensitive information is referenced, and remove, clean up, or obfuscate sensitive data using the **Set contact attributes** block Clean-up method outlined previously. For more information, see Compliance validation in Amazon Connect (p. 1126).

Telephony

In the US, use toll-free phone numbers wherever possible to load balance across multiple carriers for additional route and carrier redundancy. This also helps to decrease time to resolution when compared to DID phone numbers, which must be managed by a single carrier. In situations where you use DIDs, load balance across numbers from multiple carriers, when possible, to increase reliability. Make sure that you handle all error paths in your contact flow appropriately, and implement the best practices, requirements, and recommendations located in Troubleshooting Issues with the Contact Control Panel (CCP) (p. 1193).

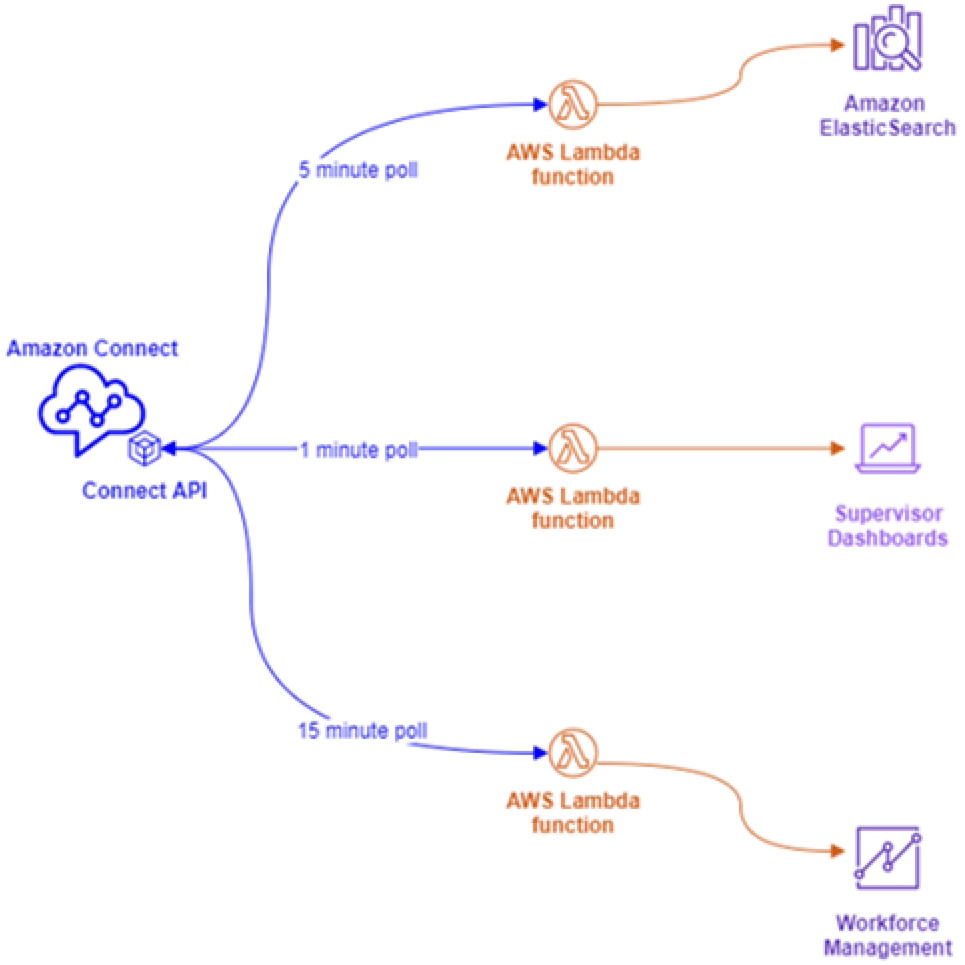
If you're forwarding your existing telephony provider's phone numbers to Amazon Connect, ensure that the process to change the forward destination to an alternative DID/toll-free number or otherwise remove the forward is defined and well-understood by your operations team. Ensure that you have Runbooks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

Amazon Connect APIs

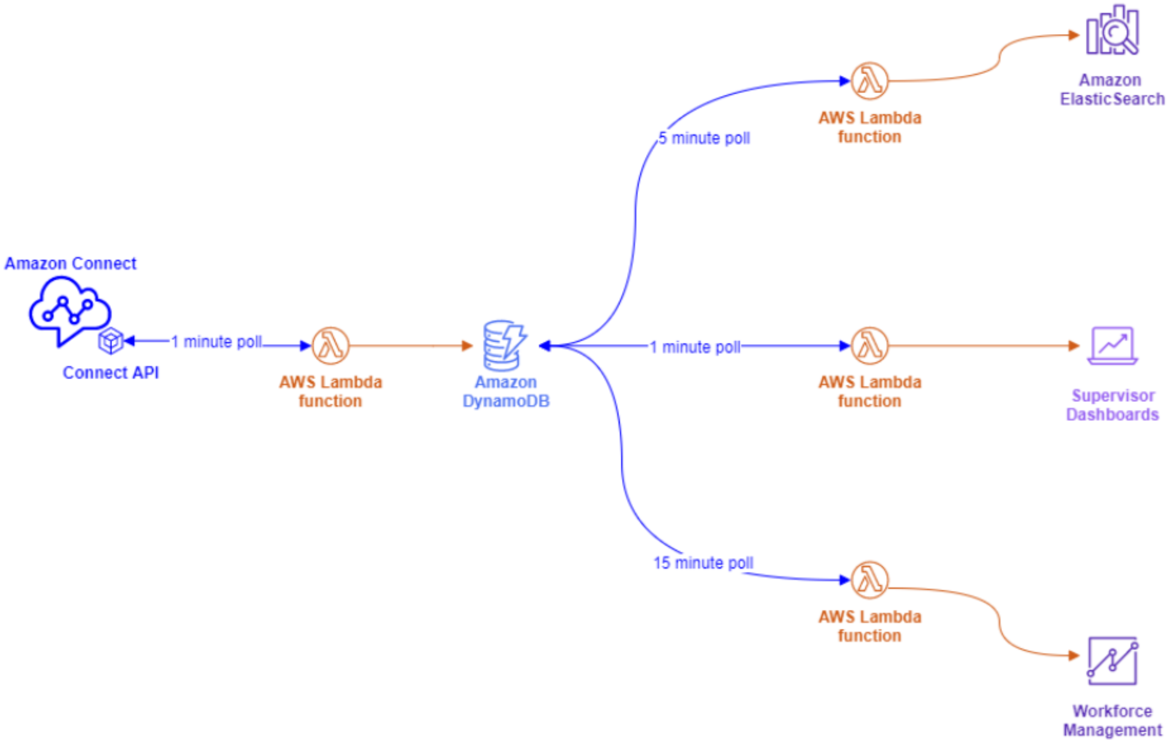
Amazon Connect throttling quotas are by account, and not instance. You should consider the following best practices when working with Amazon Connect APIs:

Implement a caching/queuing solution

To decrease API data query overhead and avoid throttling, you can use an intermediary database like Amazon DynamoDB to store API call results rather than calling the API from all endpoints interested in the API data. For example, the following diagram represents the use of the Amazon Connect metric API from multiple sources that need to consume this information:



Rather than having separate AWS Lambda functions, each with their own polling requirements, you can have a single AWS Lambda function write all interesting data to Amazon DynamoDB. Rather than having each endpoint go to the API directly to retrieve the data, they point to DynamoDB, as illustrated in the following diagram:



This architecture allows you to change polling intervals and add endpoints, as needed, without worrying about exceeding service quotas, giving you the ability to scale to however many concurrent connections your database solution supports. You can use this same concept with querying any real-time data feeds from Amazon Connect. For situations where you need to perform an API action, like an Outbound API call, you can use this same concept in combination with Amazon Simple Queue Service to queue API requests Using AWS Lambda with SQS.

Exponential back off and retry strategies

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

Change management

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

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

- **Distribute by percentage**: To reduce risk encountered during change management and experiment with new experiences for your contacts, you can use the **Distribute by percentage** block to route a subset of your traffic to new contact flows while leaving the other traffic on the original experience.
- **Measuring results**: Data driven decision making is key to successfully driving meaningful changes for your business. Having a key metric to measure your changes against is absolutely necessary. For all changes you're making, you need to plan for how you will measure success. For example, if you're implementing self-service functionality for your contacts, what percentage of contacts do you expect to self-serve to consider the workload successful or what other metrics are you measuring to determine success?
- **Rollbacks**: Ensure that there is a clear, well-defined, and well-understood process to back out any changes to the previous state, specific to the change performed. For example, if you publish a new contact flow version, ensure that the change instructions include documentation on how to roll back to the previous contact flow version.

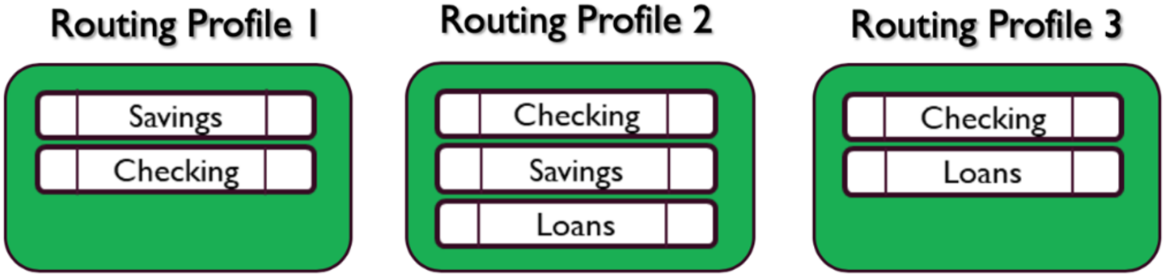
Routing profiles

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

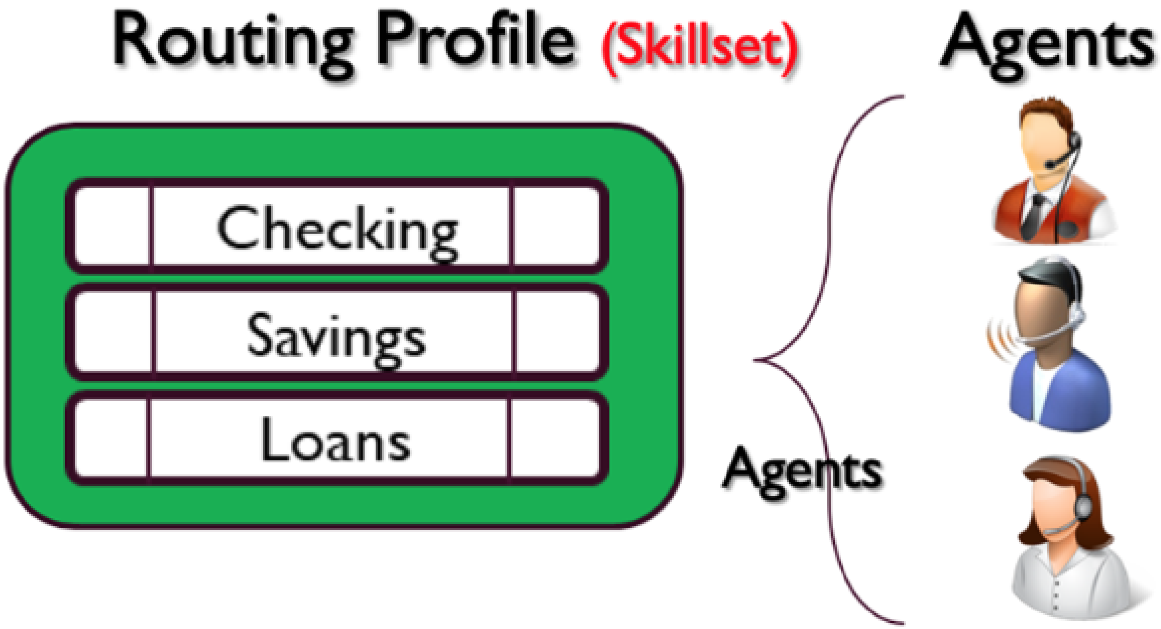
Routing in Amazon Connect

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

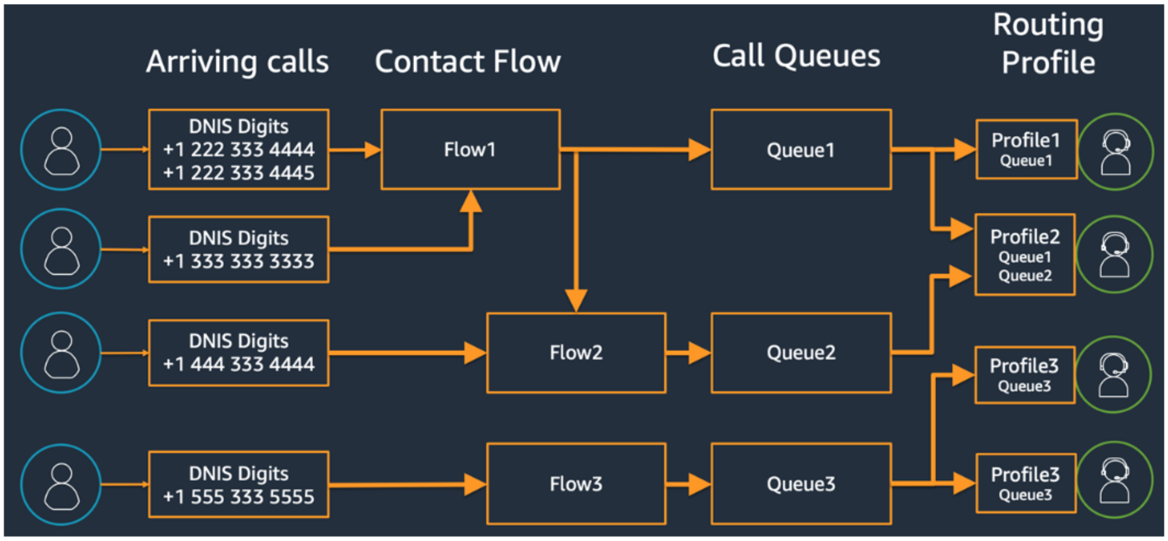
Within your contact flow, you can prompt for additional information and, if they need to reach an agent, you can use the contact flow configuration to place them in the appropriate queue. In the following example, Savings, Checking, and Loans are individual queues or skills and the three routing profiles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



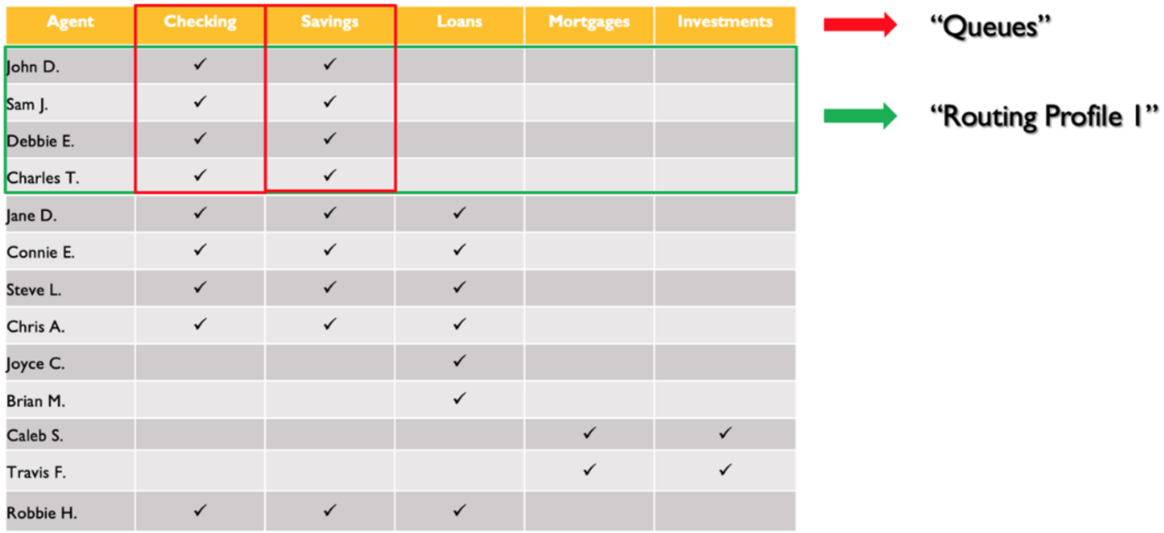
Each agent is assigned to only one routing profile based on their skillset, and many agents with similar skillset can share the same routing profile:



Each phone number or chat endpoint will be associated with one contact flow. The contact flow executes its logic, which may involve prompting the customer for information, to determine the contact's needs, and eventually routes the contact into an appropriate queue. The following diagram depicts how routing profile, queue, and contact flow work together to service a contact:



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

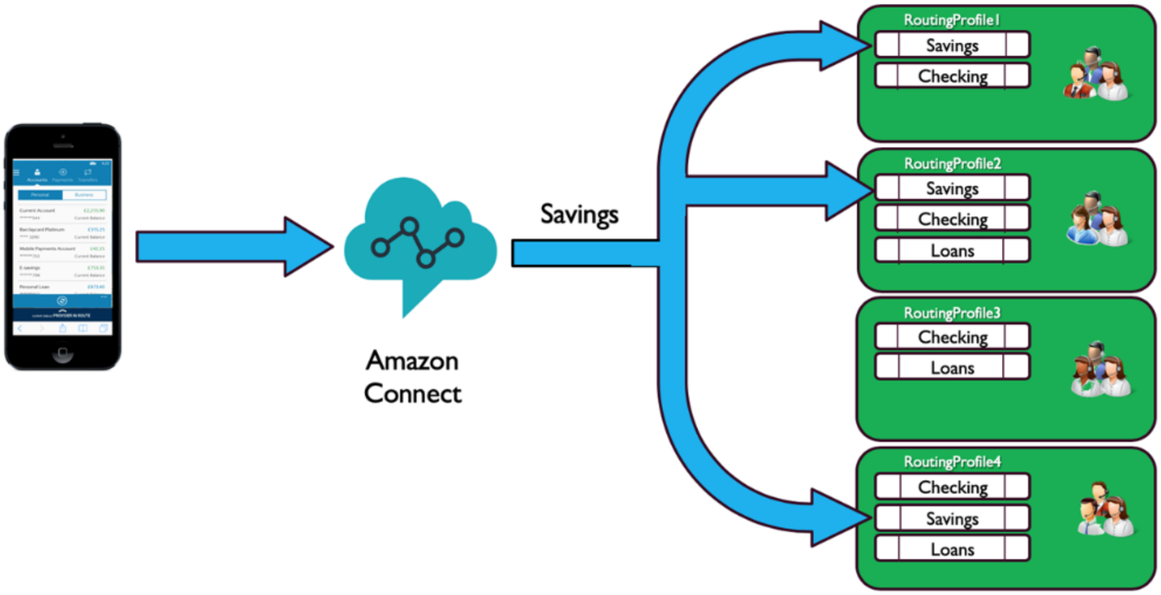


Agent	Checking	Savings	Loans	Mortgages	Investments
John D.	✓	✓			
Sam J.	✓	✓			
Debbie E.	✓	✓			
Charles T.	✓	✓			
Jane D.	✓	✓	✓		
Connie E.	✓	✓	✓		
Steve L.	✓	✓	✓		
Chris A.	✓	✓	✓		
Joyce C.			✓		
Brian M.			✓		
Caleb S.				✓	✓
Travis F.				✓	✓
Robbie H.	✓	✓	✓		

"Queues"
"Routing Profile 1"

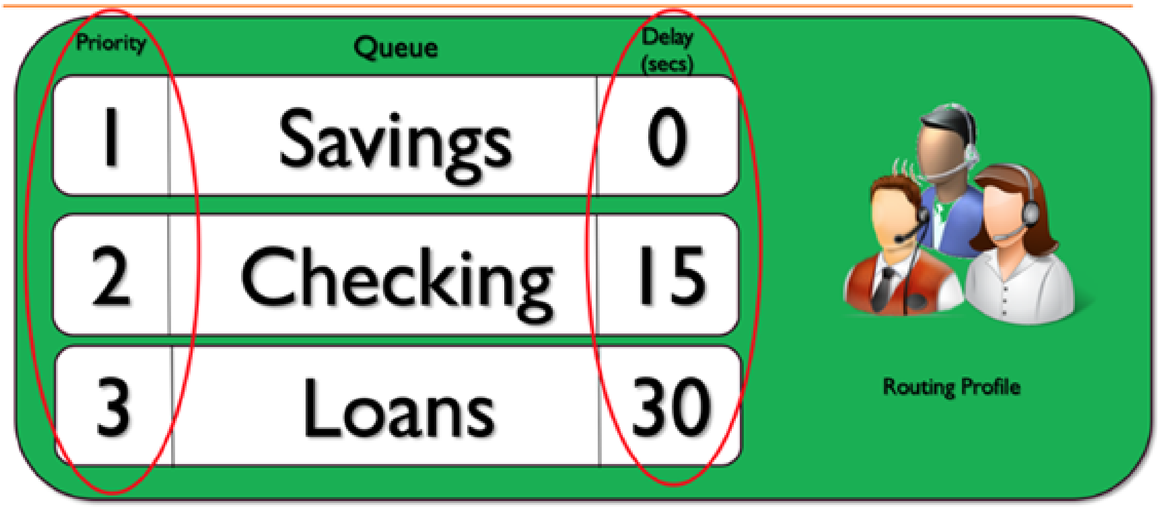
On the top row, you've identified your skills or queues. In the left column, you have your list of agents, and in the middle, you've checked the skills supported by each of the agents. You can sort the matrix grouped by the common set of skill requirements across our agent population. This help sidentify the routing profiles as one marked in the green box (which consists of two queues), which you can assign agents to. As a result of this exercise, you have identified four routing profiles, and assign your 13 agents to them accordingly.

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



Priority and delay

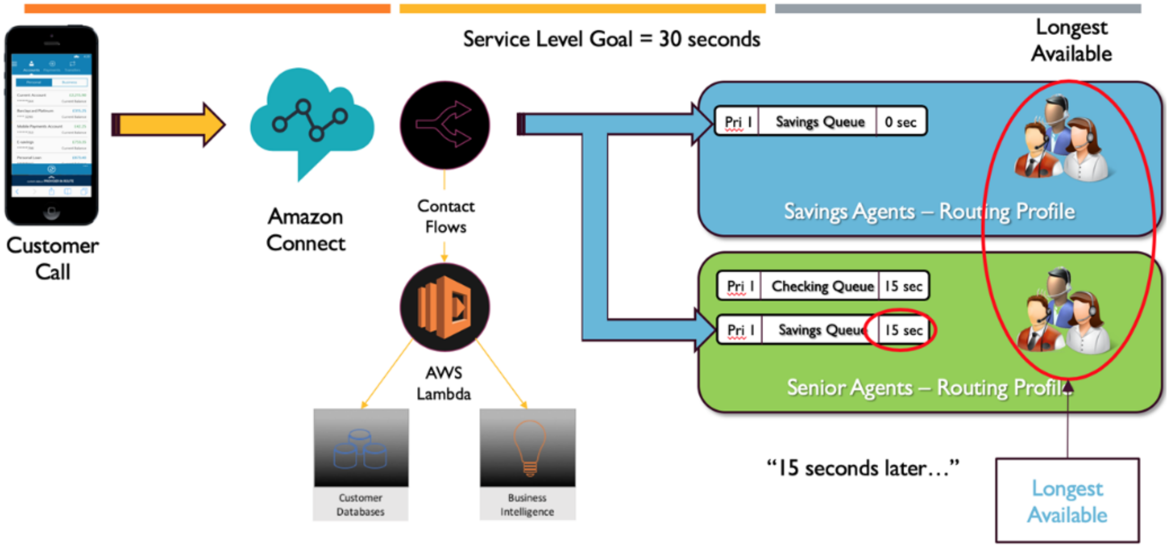
Using the combination of priority and delay in different Routing Profiles, you can create flexible routing strategies.



Priority	Queue	Delay (secs)
1	Savings	0
2	Checking	15
3	Loans	30

The preceding routing profile example shows a set of queues, and their respective priority and delay. The lower the number, the higher the priority. All higher priority calls must be processed before a lower priority call will be processed. This is a difference from systems that will eventually process lower priority of calls based upon a weighting factor.

You can also add a delay to each of the queues within each of the routing profiles. Any call coming into the queue will be held for the specified period of delay assigned to the designated queue. The call will be held for the delay period, even when agents are available. You might use this in situations where you have a group of agents who are reserved to help you meet your Service Level Agreements (SLAs), but are otherwise assigned to other tasks or queues. If a call doesn't get answered within a specified period of time, these agents would become eligible to receive a call from the designated queue. For example, consider the following diagram:

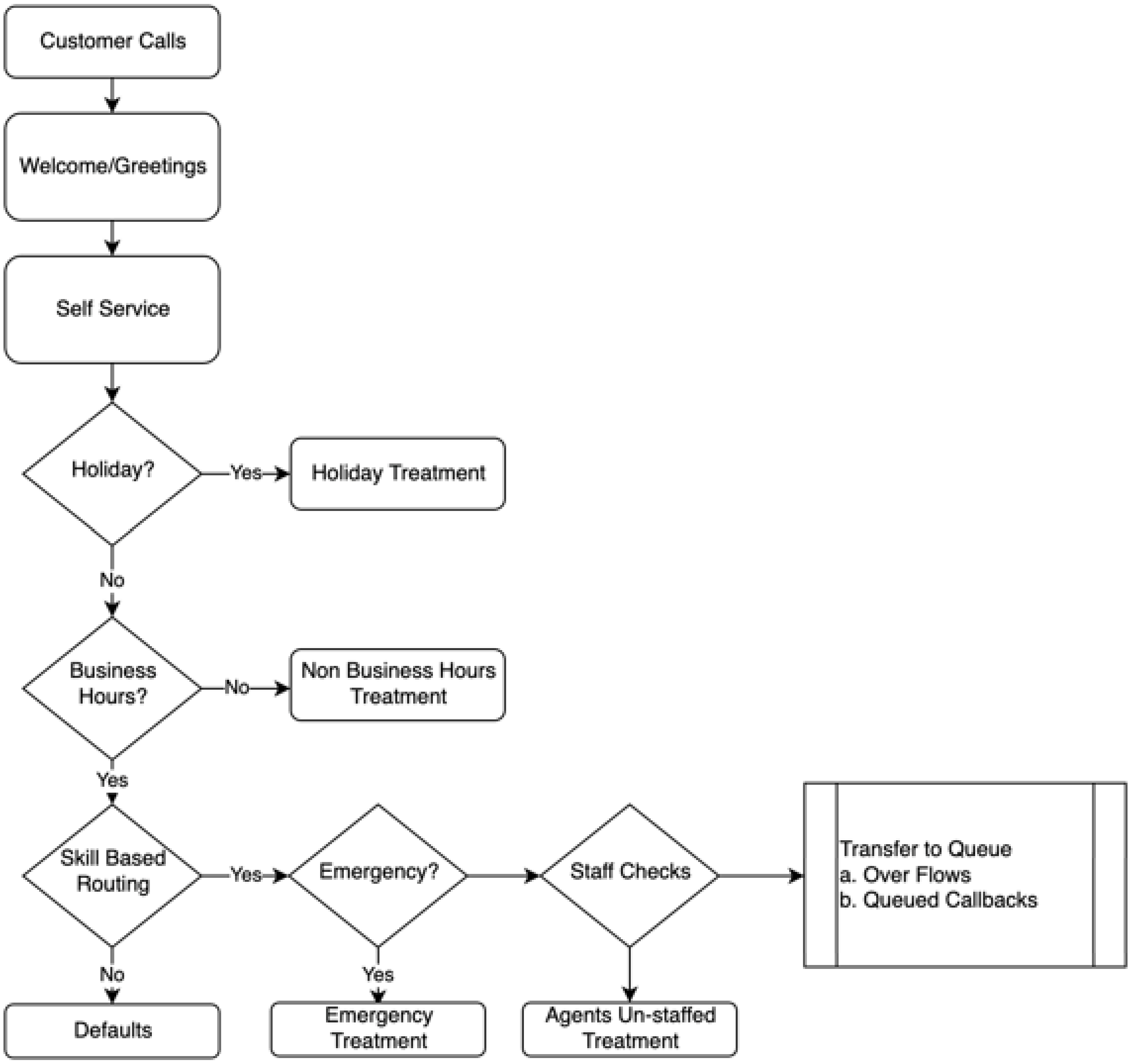


Service Level Goal = 30 seconds
Longest Available
Customer Call
Amazon Connect
Contact Flows
AWS Lambda
Customer Databases
Business Intelligence
Pri 1 | Savings Queue | 0 sec
Savings Agents – Routing Profile
Pri 1 | Checking Queue | 15 sec
Pri 1 | Savings Queue | 15 sec
Senior Agents – Routing Profile
"15 seconds later…"
Longest Available

This diagram shows an SLA of 30 seconds. A call comes in for the Savings queue. The Savings queue immediately looks for an agent in the "Savings" routing profile due to the configuration of 0 delay in the profile for the queue. Because of the configuration of 15 delay for Senior Agents, they will not be eligible to receive the Savings contact for 15 seconds. After 15 seconds elapses, the contact becomes available for a Senior Level agent and Amazon Connect looks for the Longest Available across both routing profiles.

Path to service

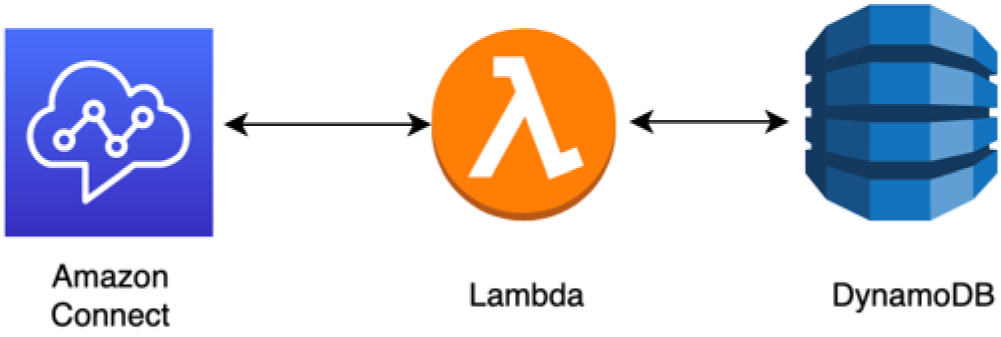
When you are designing customer experiences in Amazon Connect, plan to ensure a path to service. There are many planned and unplanned events that can impact the customer experience as they traverse through Amazon Connect contact flows. The following sample customer experience shows some suggested checks to ensure a consistent quality experience for your contacts:



This sample customer experience takes into account planned events such as Holidays and Business hours as well as unplanned events, like agents not staffed during business hours. With this logic, you can also account for emergency situations, such as contact center closures because of inclement weather or service disruptions. Consider the following concepts as illustrated in the diagram:

- **Self-service**: In a typical IVR, you can include any greetings and disclaimer messages such as call recording announcements upfront, which can be followed by self-service options. Self-service brings cost and performance optimizations for your contact center and enables your organization to serve customers 24x7, regardless of holidays, business hours, or availability of agents. Always include a path to service in case customers are unable to self-serve and need human assistance. For example, if you are using Amazon Lex bots for self-service, you can make use of fallback intents to escalate conversations for human assistance.

- **Holidays**: Many enterprise customers have a central repository that holds corporate holidays. You can use an AWS Lambda function to data dip into that repository and offer holiday treatment to customers. Additionally, you can also store corporate holidays in DynamoDB along with a custom message for each holiday. For example, if your enterprise observes December 25 as Christmas, you could have a holiday prompt or Text to Speech, "We are currently closed for Christmas. Please call back on December 26 when our normal business hours will resume."



- **Business hours**: After holidays have been verified, you can check for business hours and, if outside of business hours, you can change the experience dynamically for your contacts. If the contact occurs during business hours, you can identify customer intent for calls and map to certain queues in your contact center, increasing the likelihood of getting to the correct agent, and decreasing the amount of time it takes your contact to reach service. It is highly recommended to map defaults as customers could be calling for a reason you haven't accounted for yet or may respond in a way you don't expect.
- **Emergency messages**: After you have identified customer intent for call, it is suggested to implement an emergency check treatment. In the event of an emergency situation that impacts your contact center, you can store an emergency True/False flag in an intermediary database like DynamoDB. To allow your supervisors and administrators to set this flag dynamically, with no code, you can build a separate IVR that authenticates your Amazon Connect administrators based upon ANI and PIN number verification for internal use only. In the event of emergency, your supervisors can call into that dedicated line from their phones and after authentication set the Emergency flag to true for scenarios such as contact center closure due to inclement weather or ISP outage at the physical location of contact center.
- **Emergency message API**: You can also consider building an AWS API gateway with AWS Lambda function at the back end to set the Emergency flag to true/false securely in the database. Your supervisors can securely access that API through web to toggle disaster mode or dynamically toggle it in response to an external event. In your Amazon Connect instance, every contact that comes in through the contact flow will use AWS Lambda to check for that emergency flag and, in case of disaster mode, you can dynamically make announcements and provide a customer with a path to service. This will further ensure business continuity and mitigate the impact of situations like these from affecting your customers.
- **Check agent staffing**: Before transferring to the queue in your contact flow, you can check agent staffing to ensure that an agent is logged in to service the contact. For example, you may have an agent busy servicing another contact that might become available in the next five minutes, or you may not have anyone logged into the system at all. During these instances, you will prefer a different customer experience rather than making them wait in the queue for an agent to become available.
- **Route to service**: When you transfer the call to the queue, you can offer queued callbacks, queue overflows, or tiered routing using Amazon Connect routing profiles to offer a consistent, high-quality experience for your callers that meet your Service Level requirements.

Resources

Documentation

- DevOps and AWS
- Amazon Connect Service API Documentation

Blog

- How to handle unexpected contact spikes with Amazon Connect

Whitepaper

- Operational Excellence Pillar

Video

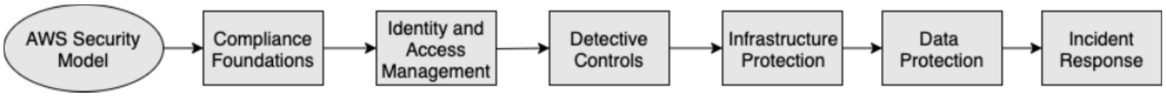
- DevOps at Amazon

Security: Design principles for developing a secure contact center

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

Amazon Connect Security Journey

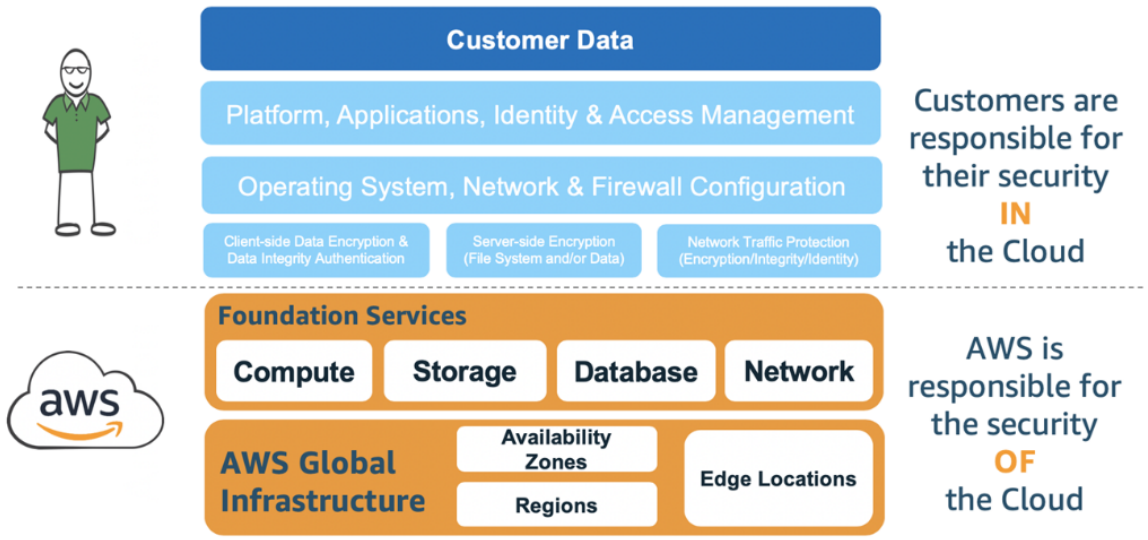
After you've made the decision to move your workload to Amazon Connect, in addition to reviewing Security in Amazon Connect (p. 1063) and Security Best Practices for Amazon Connect (p. 1132), follow these guidelines and steps to understand and implement your security requirements relative to the following core security areas:



Understanding the AWS Security Model

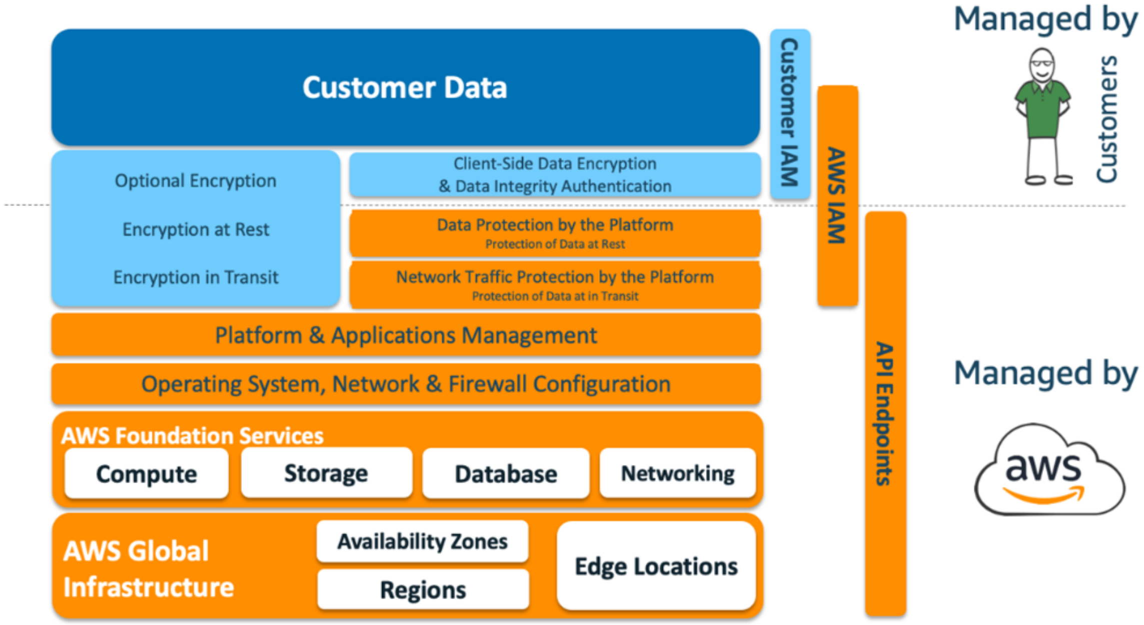
When you move computer systems and data to the cloud, security responsibilities become shared between you and AWS. AWS is responsible for securing the underlying infrastructure that supports the cloud, and you're responsible for anything you put on the cloud or connect to the cloud.

AWS Shared Responsibility Model


Customer Data
Platform, Applications, Identity & Access Management
Operating System, Network & Firewall Configuration
Client-side Data Encryption & Data Integrity Authentication
Server-side Encryption (File System and/or Data)
Network Traffic Protection (Encryption/Integrity/Identity)
Customers are responsible for their security IN the Cloud
Foundation Services
Compute
Storage
Database
Network
AWS Global Infrastructure
Availability Zones
Regions
Edge Locations
aws
AWS is responsible for the security OF the Cloud

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

AWS Shared Responsibility Model for Amazon Connect


Customer Data
Optional Encryption
Encryption at Rest
Encryption in Transit
Client-Side Data Encryption & Data Integrity Authentication
Data Protection by the Platform
Protection of Data at Rest
Network Traffic Protection by the Platform
Protection of Data at in Transit
Platform & Applications Management
Operating System, Network & Firewall Configuration
AWS Foundation Services
Compute
Storage
Database
Networking
AWS Global Infrastructure
Availability Zones
Regions
Edge Locations
Customer IAM
AWS IAM
API Endpoints
Managed by
Customers
Managed by
aws

Compliance Foundations

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

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

Region selection

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

For more information, see Set up your network (p. 605).

AWS services integration

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

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

Data Security in Amazon Connect

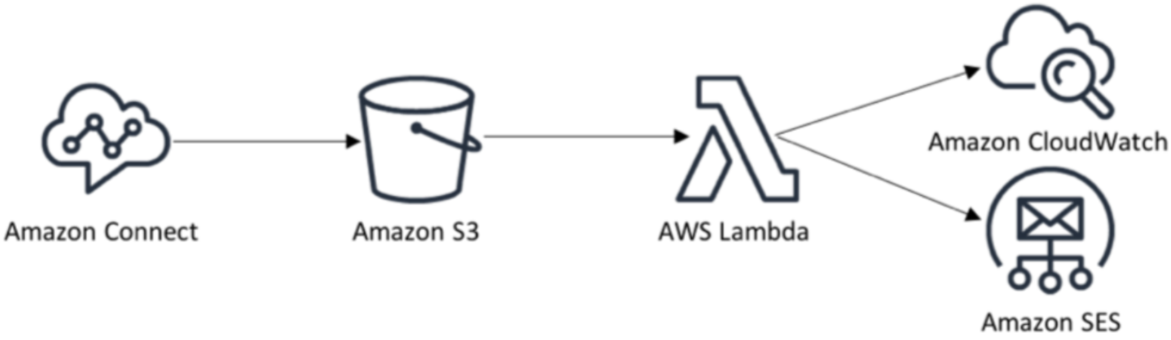
During your security journey, your security teams may require a deeper understanding of how data is handled in Amazon Connect. See the following resources:

- Detailed network paths for Amazon Connect (p. 613)
- Infrastructure security in Amazon Connect (p. 1129)
- Compliance validation in Amazon Connect (p. 1126)

Workload diagram

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

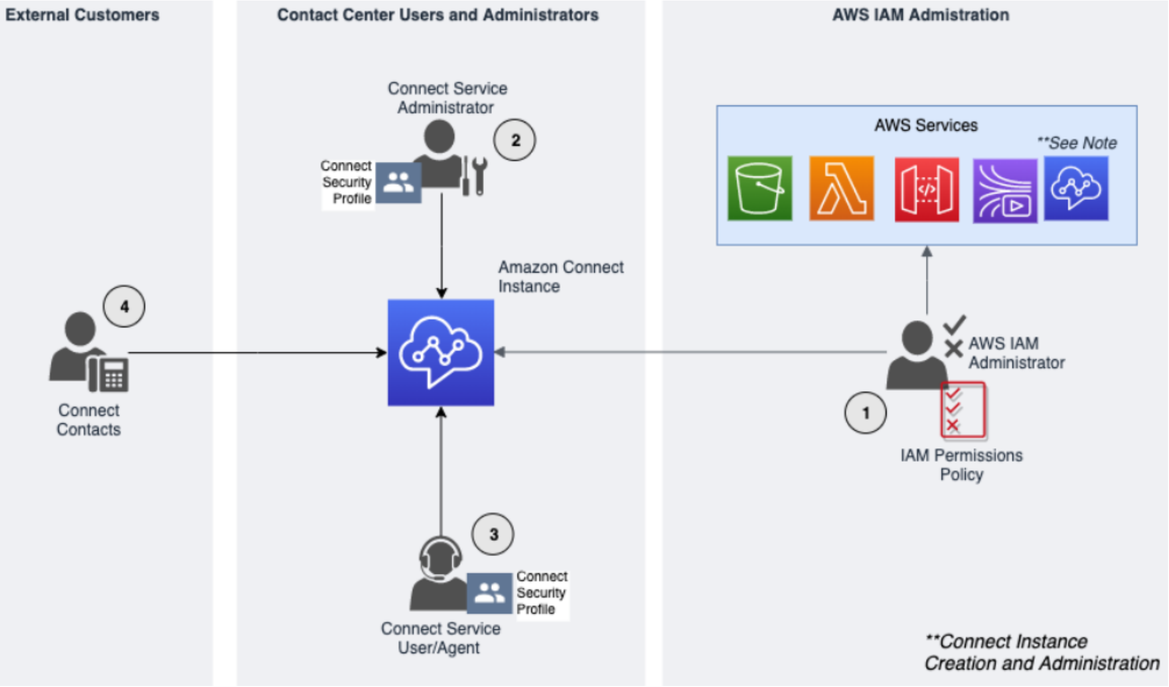
For example, a workload for automatically distributing scheduled reports for Amazon Connect stores the scheduled reports in an S3 bucket. A CloudWatch event initiates an AWS Lambda function when a new report is added to the S3 bucket. It then sends an email with the report attached. The following workload diagram shows Amazon Connect along with AWS Lambda, Amazon S3, Amazon CloudWatch, and Amazon Simple Email Service (Amazon SES).



AWS Identity and Access Management (IAM)

Types of Amazon Connect Personas

There are four types of Amazon Connect personas, based on the activities being performed.



1. IAM administrator – IAM administrators create or modify Amazon Connect resources and may also delegate administrative access to other principals. The scope of this persona is focused on creating and administering your Amazon Connect instance.
2. Amazon Connect administrator – Service administrators determine which Amazon Connect features and resources employees should access within the Amazon Connect console. The service administrator assigns security profiles to determine who can access the Amazon Connect console and what tasks they can perform. The scope of this persona is focused on creating and administering your Amazon Connect contact center.
3. Amazon Connect agent – Agents interact with Amazon Connect to perform their job duties. Service users may be contact center agents or supervisors.
4. Amazon Connect Service contact – The customer who interacts with your Amazon Connect contact center.

IAM Administrator Best Practices

IAM Administrative access should be limited to approved personnel within your organization. IAM administrators should also understand what IAM features are available to use with Amazon Connect. For IAM best practices, see Security best practices in IAM in the *IAM User Guide*. Also see Amazon Connect identity-based policy examples (p. 1101).

Amazon Connect Service Administrator Best Practices

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

Security profiles (p. 789) help you manage who can access the Amazon Connect dashboard and Contact Control Panel, and who can perform specific tasks. Review the granular permissions granted within the default security profiles available natively. Custom security profiles can be set up to meet specific requirements. For example, a power agent who can take calls but also has access to reports. After this is finalized, users should be assigned to the correct security profiles.

Multi-Factor Authentication

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

Identity Federation

In addition to storing users in Amazon Connect, you can enable single sign-on (SSO) to Amazon Connect (p. 124) by using identity federation. Federation is a recommended practice to allow for employee lifecycle events to be reflected in Amazon Connect when they are made in the source identity provider.

Access to Integrated Applications

Steps within your contact flows may need credentials to access information in external applications and systems. To provide credentials to access other AWS services in a secure way, use IAM roles. An IAM role is an entity that has its own set of permissions, but that isn't a user or group. Roles also don't have their own permanent set of credentials and are automatically rotated.

Credentials such as API keys should be stored outside of your contact flow application code, where they can be retrieved programmatically. To accomplish this, you can use AWS Secrets Manager or an existing third-party solution. Secrets Manager enables you to replace hardcoded credentials in your code, including passwords, with an API call to Secrets Manager to retrieve the secret programmatically.

Detective controls

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

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

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

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

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

Infrastructure protection

Although there is no infrastructure to manage in Amazon Connect, there could be scenarios where your Amazon Connect instance needs to interact with other components or applications deployed in infrastructure residing on-premises. Consequently, it is important to ensure that networking boundaries are considered under this assumption. Review and implement specific Amazon Connect infrastructure security considerations. Also, review contact center agent and supervisor desktops or VDI solutions for security considerations.

You can configure a Lambda function to connect to private subnets in a virtual private cloud (VPC) in your account. Use Amazon Virtual Private Cloud to create a private network for resources such as databases, cache instances, or internal services. Amazon Connect your function to the VPC to access private resources during execution.

Data protection

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

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

After analyzing the scope of the data, data classifications should be performed paying attention to identifying sensitive data. Amazon Connect conforms to the AWS shared security model. Data protection in Amazon Connect (p. 1063) includes best practices like using MFA and TLS and the use of other AWS services, including Amazon Macie.

Amazon Connect handles variety of data related to contact centers (p. 1064). This includes phone call media, call recordings, chat transcripts, contact metadata as well as contact flows, routing profiles and queues. Amazon Connect handles data at rest by segregating data by account ID and instance ID. All data exchanged with Amazon Connect is protected in transit between the user's web browser and Amazon Connect using open standard TLS encryption.

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

Protecting Data Using Client-Side Encryption

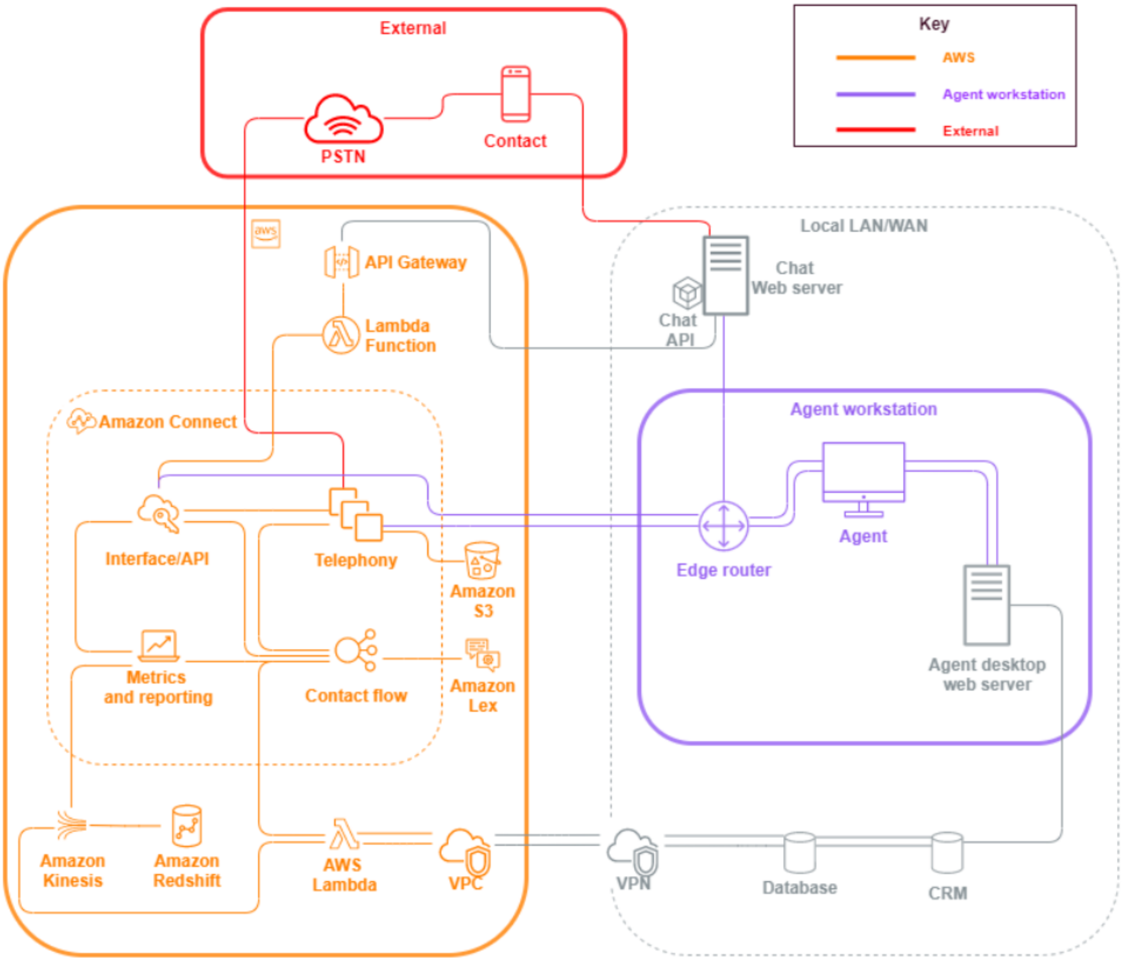
Your use case may require encryption of sensitive data that is collected by contact flows. For example, to gather appropriate personal information to customize the customer experience when they interact with your IVR. To do this you can use public-key cryptography with the AWS Encryption SDK. The AWS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

Input validation

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

Amazon Connect security vectors

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



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

   Follow your security best practices for this layer with special attention to the following:

   - Plan identity management keeping in mind best practices noted in Security Best Practices for Amazon Connect (p. 1132).
   - Mitigate insider threat and compliance risk associated with workloads that handle sensitive information, by creating a secure IVR solution that enables you to bypass agent access to sensitive information. By encrypting contact input in your contact flows, you're able to capture information securely without exposing it to your agents, their workstations, or their operating environments. For more information, see Encrypt customer input (p. 508).
   - You are responsible for maintaining the allow list of AWS IP addresses, ports, and protocols needed to use Amazon Connect.

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

   - Plan identity management, keeping in mind best practices noted in Security Best Practices for Amazon Connect (p. 1132).
   - Integrations with other AWS services: Identify each AWS service in the use case as well as any third-party integration points applicable for this use case.

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

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

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

   - You can create contact filters for repeat and fraudulent contacts using AWS Lambda to write contact details to DynamoDB from within your contact flow, including ANI, IP address for click-to-dial and chat endpoints, and any other identifying information to track how many contact requests occur during a given period of time. This approach allows you to query and add contacts to deny lists, automatically disconnecting them if they exceed reasonable levels.
   - ANI Fraud detection solutions using Amazon Connect telephony metadata (p. 524) and partner solutions can be used to protect against caller ID spoofing.
   - Amazon Connect Voice ID (p. 858) and other voice biometric partner solutions can be used to enhance and streamline the authentication process. Active voice biometric authentication allows contacts the option to speak specific phrases and use those for voice signature authentication. Passive voice biometrics allow contacts to register their unique voiceprint and use their voiceprint to authenticate with any voice input that meets sufficient length requirements for authentication.
   - Maintain the application integration (p. 616) section in the Amazon Connect console for adding any third-party application or integration points to your allow list, and remove unused endpoints.
   - Send only the data necessary to meet minimum requirements to external systems that handle sensitive data. For example, if you have only one business unit using your call recording analytics solution, you can set an AWS Lambda trigger in your S3 bucket to process contact records, check for the business unit's specific queues in the contact record data, and if it is a queue that belongs to the unit, send only that call recording to the external solution. With this approach, you only send the data necessary and avoid the cost and overhead associated with processing unnecessary recordings.

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

Resources

Documentation

- AWS Cloud Security
- Security in Amazon Connect (p. 1063)
- IAM Best Practices
- AWS Compliance
- AWS Security blog

Articles

- Security Pillar
- Introduction to AWS Security
- AWS Security Best Practices

Videos

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

Reliability

Reliability includes the ability of a system to recover from infrastructure or service disruptions, dynamically acquire computing resources to meet demand, and mitigate disruptions such as misconfigurations or transient network issues. As resiliency is handled as part of the service, there are no reliability practices unique to Amazon Connect beyond of what is covered in Operational Excellence (p. 93). You can find prescriptive guidance on implementation in the Reliability Pillar whitepaper.

Resources

Documentation

- AWS Service quotas
- Resilience in Amazon Connect (p. 1128)
- Amazon CloudWatch

Whitepaper

- Reliability Pillar

Video

- Embracing Failure: Fault-Injection and Service Reliability

Product

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

Performance efficiency

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

Architectural design

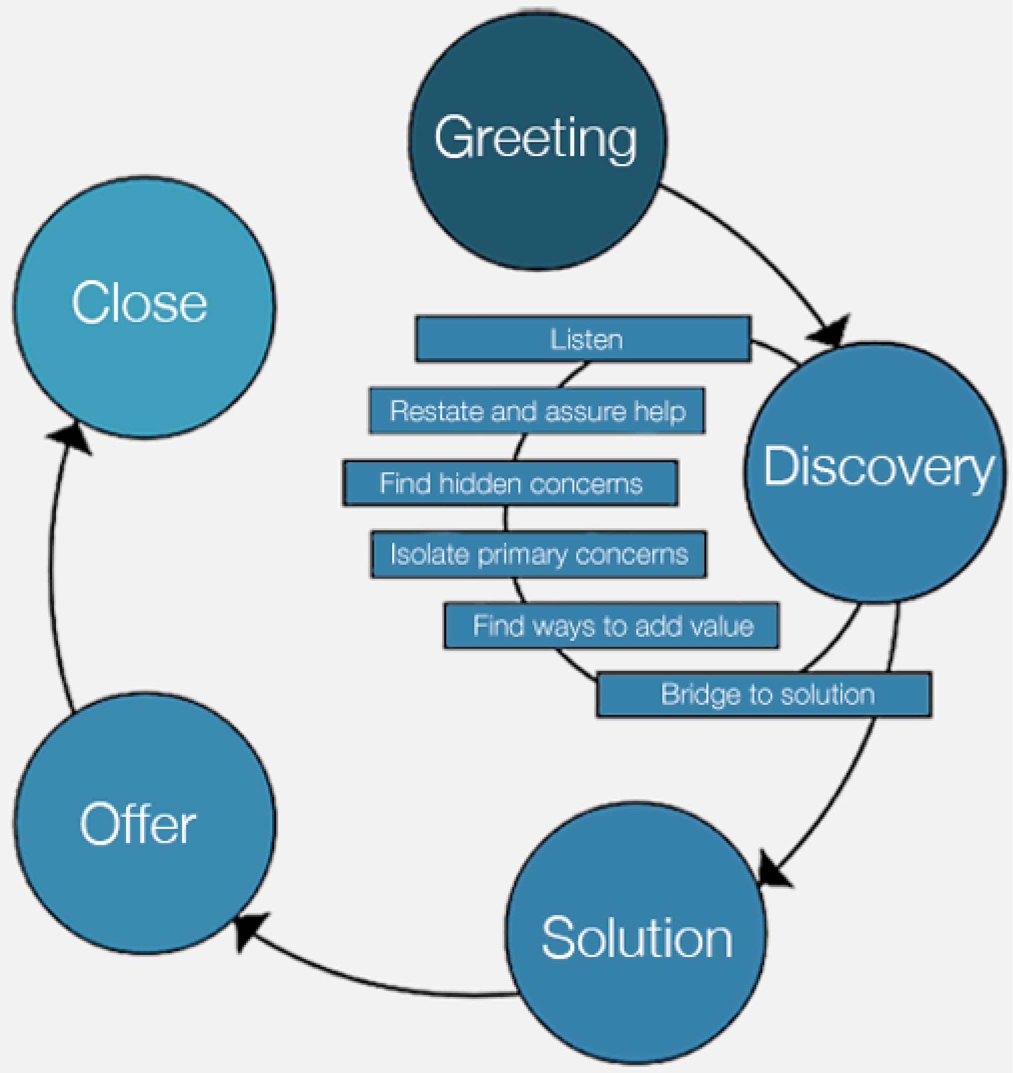
There are two fundamental architectural design principles to consider when designing experiences for the contact center:

- Reductionism is a philosophical tenet stating that by analyzing a system to its ultimate component parts, you can unravel it at deeper levels.

- Holism, in contrast, states that by considering the whole picture one gets a deeper and more complete view of a situation than by analyzing it into its component parts

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

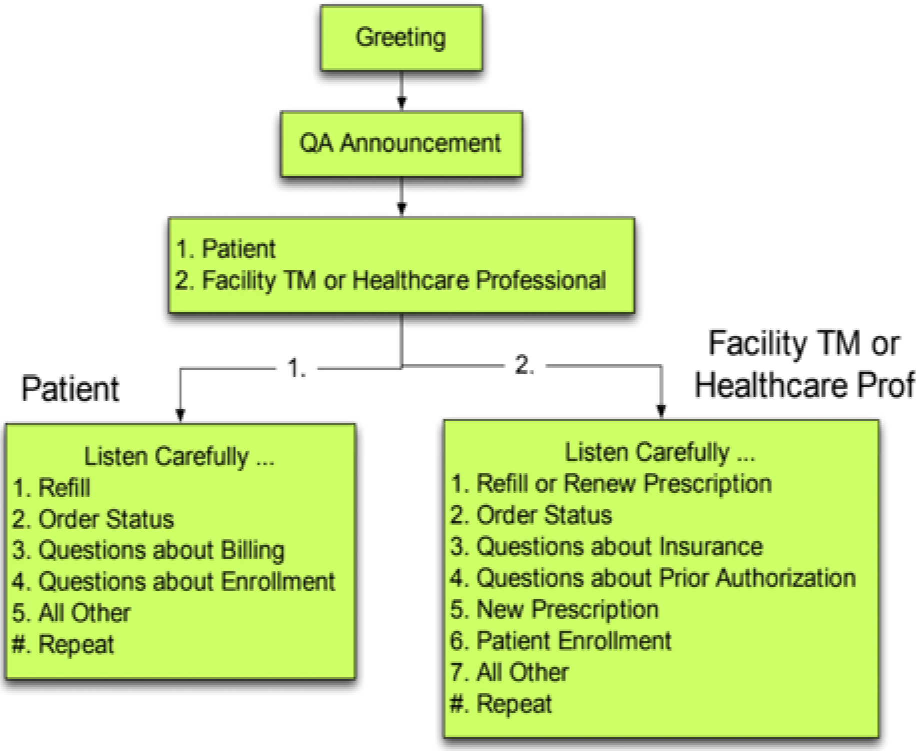
A holistic view of the contact center is shown in the following diagram:



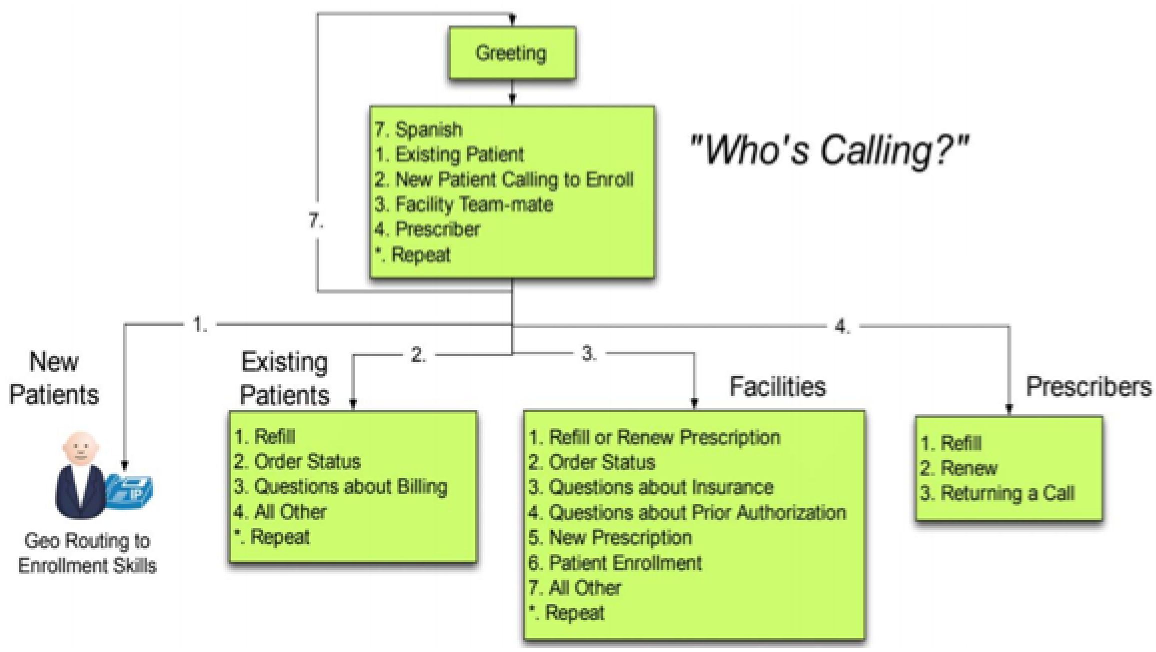
The holistic approach results focus on a more complete and cohesive experience for customers, and not which technology will provide which part of that experience.

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

You can start with the default experience, building out your contact flows, but refactoring your single contact flow into two to enable future segmentation:


Greeting
QA Announcement
1. Patient
2. Facility TM or Healthcare Professional
1.
2.
Patient
Facility TM or Healthcare Prof
Listen Carefully ...
1. Refill
2. Order Status
3. Questions about Billing
4. Questions about Enrollment
5. All Other
#. Repeat
Listen Carefully ...
1. Refill or Renew Prescription
2. Order Status
3. Questions about Insurance
4. Questions about Prior Authorization
5. New Prescription
6. Patient Enrollment
7. All Other
#. Repeat

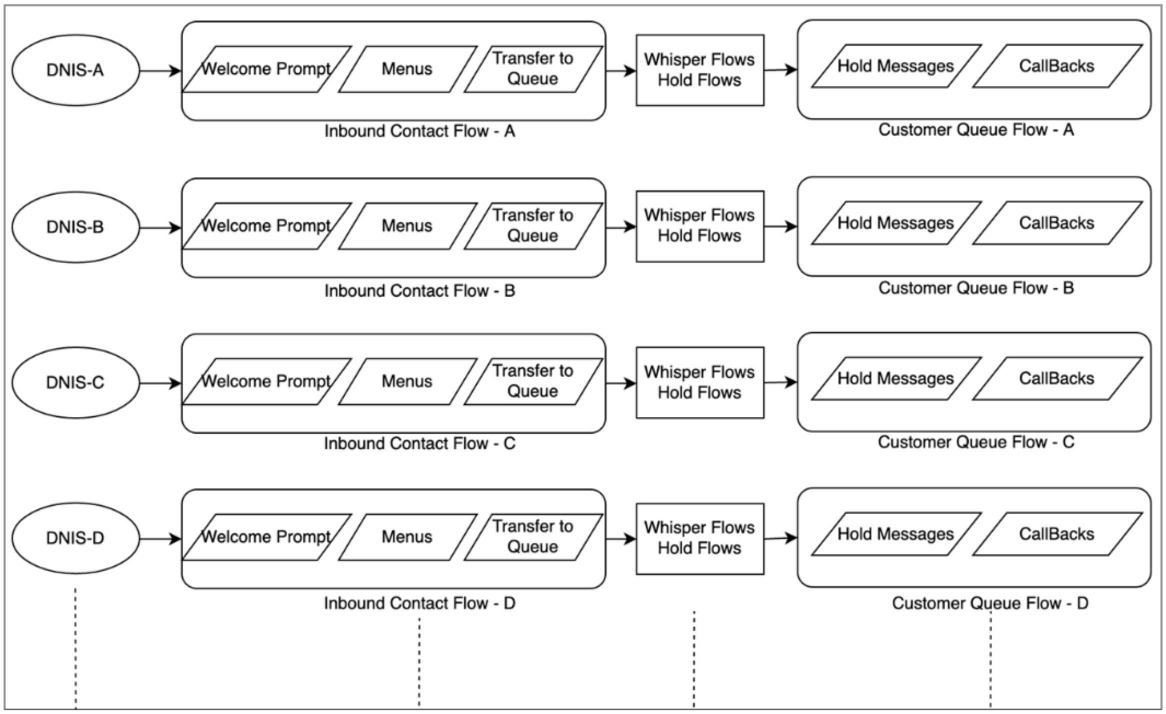
In your next iteration, identify additional experiences that you need to plan for and build routing and, if necessary, contact flows for each. For example, you may want to play different prompts for a contact that is past due on their bill or that may have tried to contact multiple times for the same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



Contact flow design

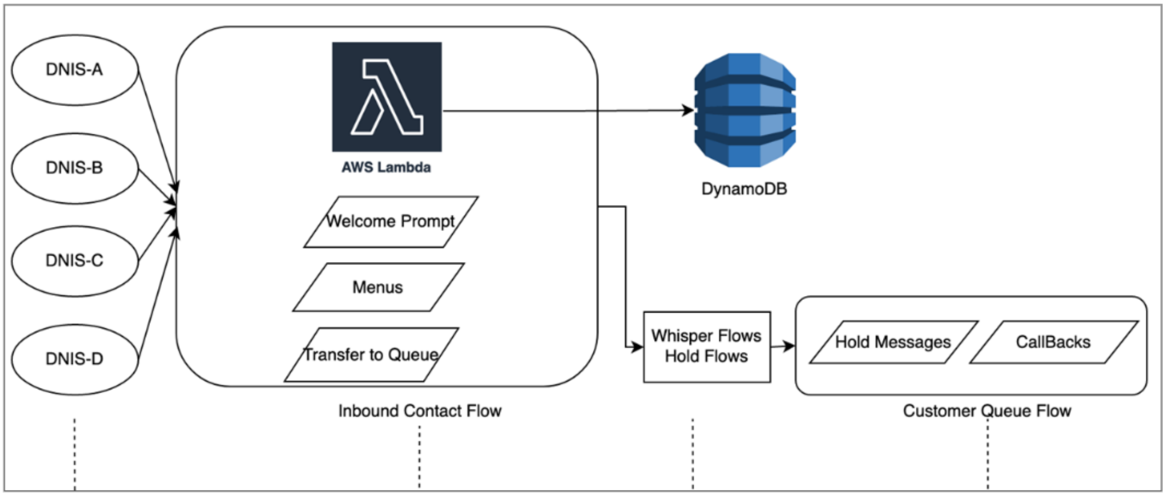
A contact flow defines the customer experience with your contact center from start to finish. Your contact flow configuration can have a direct impact on performance, operational efficiency, and ease of maintenance.

Many Large businesses support multiple phone numbers, business units, prompts, queues, and other Amazon Connect resources. While it is possible to have unique contact flows for each phone number and line of business, it can lead to a one-to-one mapping of phone numbers and contact flows. This results in unnecessary service quota requests and a large number of contact flows to support and maintain. A one-to-one mapping of DNIS and Contact flow implementation is illustrated in the following figure:



Alternatively, you should consider an approach that results in Multiple DNIS to one or few contact flows by using the dynamic nature of Amazon Connect contact flows. With this approach, you can store configuration information like Prompts, Queues, Business Hours, Whisper Prompts/Flows, Queues, Queue Treatments and Hold Messages etc., in NoSQL Database DynamoDB. In Amazon Connect, you can associate multiple phone numbers to the same contact flow and use the Lambda function to look up configurations for that phone number. This allows you to dynamically define the contact's experience based on the attributes returned from DynamoDB.

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



Load testing

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

Agent enablement

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

- CRM integration - The Streams API allows you to embed the CCP in your CRM application, create your own interface, or integrate with other AWS services and partner solutions to provide your agents with the tools and resources they need to service your contacts. With a custom desktop, like the Amazon Connect and Salesforce integration (p. 294), your agents can get a comprehensive view of customer and contact in a single interface without managing multiple screens and interfaces.
- Authentication - You can configure SAML for identity management in Amazon Connect and use AWS SSO (SSO) to allow your agents to use the same credentials they use to access your other systems and avoid the need to enter them multiple times.
- Agent automation - In addition to streamlining your agent experience, you can automate common, repeatable tasks. For example, automatically creating cases or pre-filling webforms and offering a screen pop with relevant information when a contact is offered. This can reduce handle times and improve the quality of experience for your agents and contacts.
- Enhanced capabilities - You can also enhance/extend the CCP functionality to include real-time Transcriptions, Translations, Suggested Actions and Knowledge base integrations. Integrating enhanced capabilities with your agent desktop will allow skilled agents to service contacts more efficiently and unskilled agents to provide service when skilled agents aren’t available. For example, you can use this approach to automatically translate a chat contact for unskilled agent that doesn’t know the language. When your agent replies, you can automatically translate the text to the contact’s language, allowing for real-time bilingual communication.

Using other AWS services

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

AWS Lambda

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

AWS Direct Connect

AWS Direct Connect is a cloud service solution that makes it more efficient to establish a dedicated network connection from your premises to AWS. It provides a durable, consistent connection rather than relying on your ISP to dynamically route requests to AWS resources. It allows you to configure your edge router to redirect AWS traffic across dedicated fiber rather than traversing the public WAN and establish private connectivity between AWS and your data center, office, or colocation environment. In many cases, this can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than Internet-based connections.

While AWS Direct Connect does not solve issues specific to private LAN/WAN traversal to your edge router, it can help solve for latency and connectivity issues between your edge router and AWS resources. It can also solve for latency and poor call quality between your edge router and AWS resources.

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

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

Amazon Polly

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

Amazon Lex

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

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

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

- Monitoring in Amazon Lex
- Building Better bots using Amazon Lex

Amazon Kinesis

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

- Export your contact record data to Amazon Redshift using Amazon Kinesis.
- Use Amazon Kinesis video stream (KVS) and AWS Lambda to transcribe call recordings or voice contacts in real-time using Amazon Transcribe and send the resulting text to Amazon Comprehend for sentiment analysis.
- Leverage the Amazon Connect Agent Event Kinesis Stream (p. 965) for real-time agent CTI and schedule adherence data.

Amazon OpenSearch Service and Kibana

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

Amazon Connect Contact Lens

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

Resources

Documentation

- Best practices design patterns: optimizing Amazon S3 performance
- Amazon EBS volume performance on Linux instances

Whitepaper

- Performance Efficiency Pillar

Video

- AWS re:Invent 2016: Scaling Up to Your First 10 Million Users (ARC201)
- AWS re:Invent 2017: Deep Dive on Amazon EC2 Instances

Cost optimization

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

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

Region selection

Amazon Connect Region selection is one of the first decision customers make when adopting Amazon Connect for their contact center workloads. While latency and voice quality are important aspects to

Region selection, you should evaluate Region selection from a cost perspective as well. Telephony pricing for Claimed Phone Numbers Per Day and Per Minute Inbound Usage can be different for countries depending upon the AWS Region in which you select to instantiate your Amazon Connect Instance. You can find telephony price for each Region at Amazon Connect Pricing page.

Callbacks

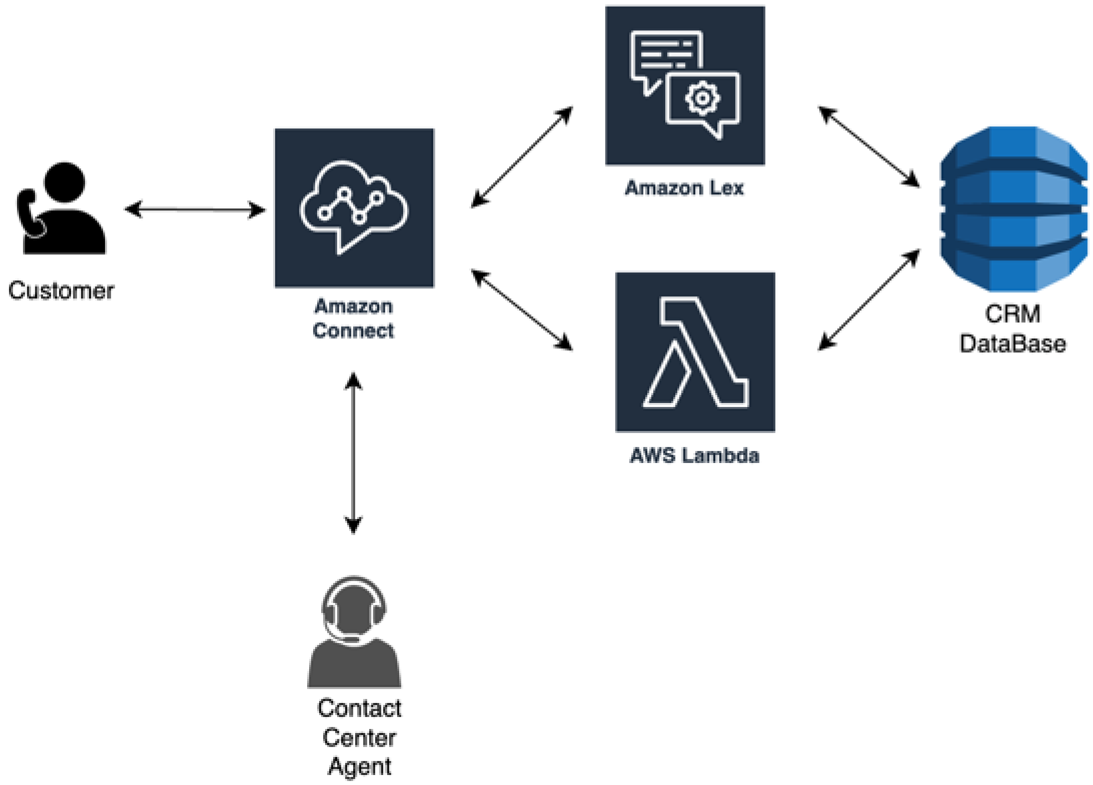
You can provide a callback in your contact flow for callers during high call volume periods or long wait times. You can use callbacks to reduce cost and improve the quality of experience for your contacts. When your contact opts-in for the callback, Amazon Connect will retain the position in the queue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

Storage

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

Self-service

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



Click-to-call

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

Redirect voice contacts to chat

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

Resources

Documentation

- Analyzing Your Costs with Cost Explorer
- AWS Cloud Economics Center
- What are AWS Cost and Usage Reports

Whitepaper

- Cost Optimization Pillar

Plan your identity management in Amazon Connect

Before you set up your Amazon Connect instance (p. 135), 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 an instance. Instead, you must delete the instance and create a new one. However, if you delete an instance, you lose its configuration settings and metrics data.

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

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

  When you manage users in Amazon Connect, the user name and password for each user is specific to Amazon Connect. Users must remember a separate user name and password to log in to Amazon Connect.
- **Link to an existing directory**—Choose this option to use an existing Active Directory. Users will log in to Amazon Connect using their corporate credentials.

  If you choose this option, the directory must be associated with your account, set up in AWS Directory Service, and be active in the same Region in which you create your instance. If you plan to choose this option, you should prepare your directory before you create your Amazon Connect instance. For more information, see Use an existing directory for identity management (p. 123).
- **SAML 2.0-based authentication**—Choose this option if you want to use your existing network identity provider to federate users with Amazon Connect. Users can only log in to Amazon Connect by using the link configured through your identity provider. If you plan to choose this option, you should configure your environment for SAML before you create your Amazon Connect instance. For more information, see Configure SAML with IAM for Amazon Connect (p. 124).

Use an existing directory for identity management

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

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

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

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

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

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

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

Configure SAML with IAM for Amazon Connect

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

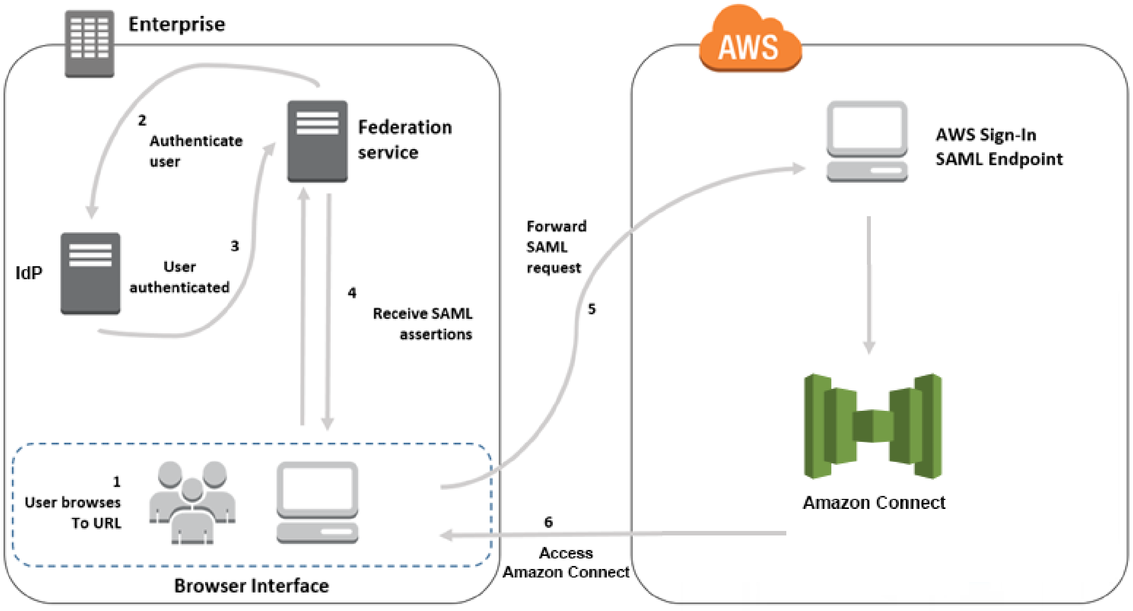
Important notes

Before you begin, note the following:

- Choosing SAML 2.0-based authentication as the identity management method for your Amazon Connect instance requires the configuration of AWS Identity and Access Management federation.
- The user name in Amazon Connect must match the RoleSessionName SAML attribute specified in the SAML response returned by the identity provider.
- An Amazon Connect user can only be associated with a single AWS IAM Role. Changing the AWS IAM Role used for federation will cause previously federated users to fail on login. For more information about Identity and Access Management user and role management, see IAM roles.

Overview of using SAML with Amazon Connect

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



SAML requests go through the following steps:

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

Enabling SAML-based authentication for Amazon Connect

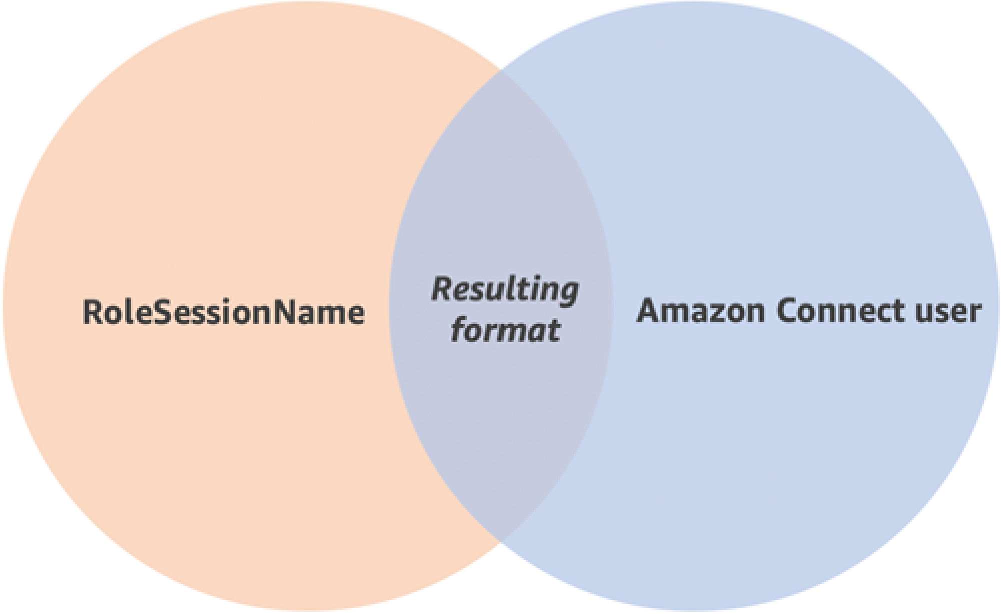
The following steps are required to enable and configure SAML authentication for use with your Amazon Connect instance:

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

Important

Due to the association of an Amazon Connect user and an AWS IAM Role, the user name must match exactly the RoleSessionName as configured with your AWS IAM federation integration, which typically ends up being the user name in your directory.

The format should match the intersection of the format conditions of the RoleSessionName and an Amazon Connect user, as shown in the following diagram:



Format:

- String: Upper- and lower-case alphanumeric characters with no spaces
- Length constraints: Minimum length of 2. Maximum length of 64.
- Special characters: **@ - .**

4. Configure your identity provider for the SAML assertions, authentication response, and relay state. Users log in to your identity provider. When successful, they are redirected to your Amazon Connect instance. The IAM role is used to federate with AWS, which allows access to Amazon Connect.

Select SAML 2.0-based authentication during instance creation

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

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

Enable SAML federation between your identity provider and AWS

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

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

The steps necessary to enable SAML federation with AWS include:

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

   > **Important**
   > Replacing this Role causes previously federated users to fail at login because it breaks existing user logins due to the immutable Amazon Connectuser association with the previous Role.

   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. For Amazon Connect, leave the **Application Start URL** blank.
6. 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.

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

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

  Note
  You can find the instance ID for your instance by choosing the instance alias in the Amazon Connect console. The instance ID is the set of numbers and letters after '/instance' in the **Instance ARN** displayed on the **Overview** page. For example, the instance ID in the following Instance ARN is *178c75e4-b3de-4839-a6aa-e321ab3f3770*.
  arn:aws:connect:us-east-1:450725743157:instance/*178c75e4-b3de-4839-a6aa-e321ab3f3770*

Configurations for regionally isolated SAML sign in

Perform the following steps to use regional SAML endpoints. These steps are IdP agnostic; they work for any SAML IdP (for example, Okta, Ping, OneLogin, Shibboleth, ADFS, AzureAD, and more).

1. Update (or override) the AssertionConsumerService. There are two ways you can do this:

   - **Option 1**: Download the AWS SAML metadata and update the `Location` attribute to the Region of your choice. Load this new version of the AWS SAML metadata into your IdP.

     Following is an example of a revision:

     ```
     <AssertionConsumerService index="1" isDefault="true"
     Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
     Location="https://region-id.signin.aws.amazon.com/saml"/>
     ```
   - **Option 2**: Override the AssertionConsumerService (ACS) URL in your IdP. For IdPs like Okta that provide prebaked AWS integrations, you can override the ACS URL in the AWS admin console. Use the same format to override to a Region of your choice (for example, https://*region-id*.signin.aws.amazon.com/saml).
2. Update the associated role trust policy:

   a. This step needs to be done for every role in every account that trusts the given identity provider.

   b. Edit the trust relationship, and replace the signular `SAML:aud` condition with a multivalued condition. For example:

      - Default: "`SAML:aud`": "https://signin.aws.amazon.com/saml".
      - With modifications: "`SAML:aud`": ["https://signin.aws.amazon.com/saml", "https://*region-id*.signin.aws.amazon.com/saml"]

   c. Make these changes to the trust relationships in advance. They should not be done as part of a plan during an incident.
3. Configure a relay state for the Region-specific console page.

   a. If you don't do this final step, there's no guarantee that the Region-specific SAML sign in process will forward the user to the console sign in page within the same Region. This step is most varied per identity provider, but there are a blogs (for example, How to Use SAML to Automatically Direct Federated Users to a Specific AWS Management Console Page) that show the use of relay state to achieve deep linking.

   b. Using the technique/parameters appropriate for your IdP, set the relay state to the console endpoint that matches (for example, https://*region-id*.console.aws.amazon.com/connect/federate/*instance-id*).

   Note

   - Ensure that STS is not disabled in your additional Regions.

- Ensure no SCPs are preventing STS actions in your additional Regions.

Use a destination in your relay state URL

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

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

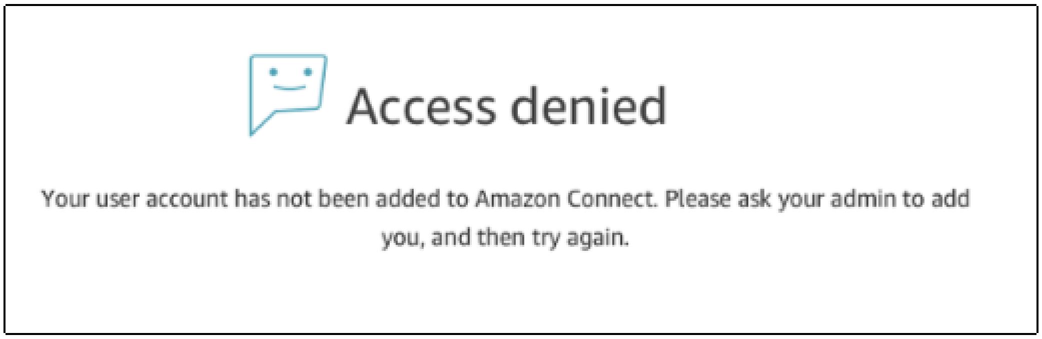
For a GovCloud instance, the URL is **https://console.amazonaws-us-gov.com/**. So the address would be:

- https://console.amazonaws-us-gov.com/connect/federate/instance-id?destination=%2Fconnect%2Fccp-v2

Add users to your Amazon Connect instance

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

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



Access denied

Your user account has not been added to Amazon Connect. Please ask your admin to add you, and then try again.

Bulk upload users with the template

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

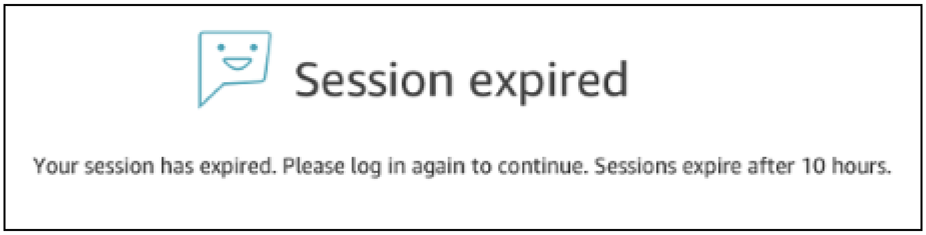
SAML user logging in and session duration

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

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

About session expiration

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



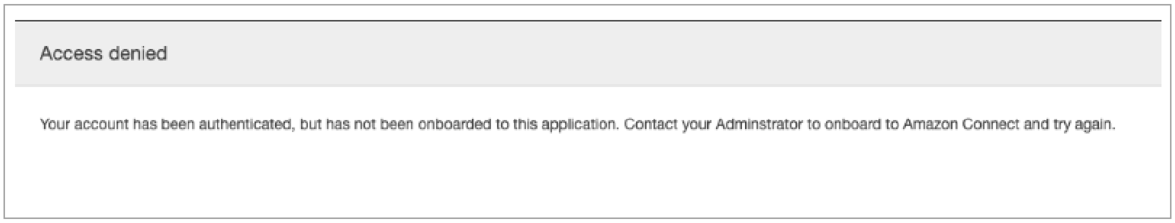
Session expired

Your session has expired. Please log in again to continue. Sessions expire after 10 hours.

Troubleshoot SAML with Amazon Connect

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

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



Access denied

Your account has been authenticated, but has not been onboarded to this application. Contact your Adminstrator to onboard to Amazon Connect and try again.

What does this mean?

This error means that the user has successfully authenticated via SAML into the AWS SAML login endpoint. However, the user could not be matched/found inside Amazon Connect. This usually indicates one of the following:

- The username in Amazon Connect doesn't match the `RoleSessionName` SAML attribute specified in the SAML response returned by the identity provider.

- The user doesn't exist in Amazon Connect.
- The user has two separate profiles assigned to them with SSO.

Resolution

Use the following steps to check the RoleSessionName SAML attribute specified in the SAML response returned by the identity provider, and then retrieve and compare with the login name in Amazon Connect.

1. Perform a HAR capture (**H**TTP **AR**chive) for the end-to-end login process. This captures the network requests from the browser side. Save the HAR file with your preferred file name, for example, **saml.har**.

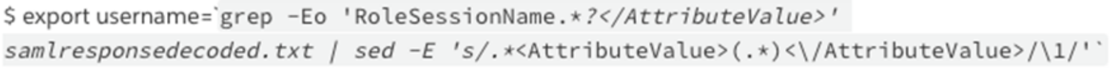
   For instructions, see How do I create a HAR file from my browser for an AWS Support case?
2. Use a text editor to find the SAMLResponse in the HAR file. Or, run the following commands:

   ```
   $ grep -o "SAMLResponse=.*&" azuresaml.har | sed -E 's/SAMLResponse=(.*)&/
   \1/' > samlresponse.txt
   ```

   - This searches for the SAMLresponse in the HAR file and saves it to a **samlresponse.txt** file.
   - The response is URL encoded and the contents are Base64 encoded.
3. Decode the URL response and then decode the Base64 contents using a third-party tool or a simple script. For example:

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

   This script uses a simple python command to decode the SAMLResponse from its original URL encoded format. Then it decodes the response from Base64 and outputs the SAML Response in plain text format.
4. Check the decoded response for the needed attribute. For example, the following image shows how to check `RoleSessionName`:

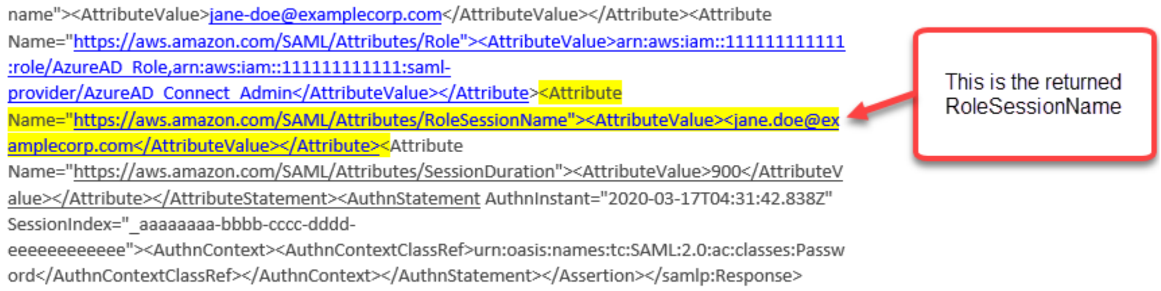
   ```
   $ export username=`grep -Eo 'RoleSessionName.*?</AttributeValue>'
   samlresponsedecoded.txt | sed -E 's/.*<AttributeValue>(.*)<\/AttributeValue>/\1/'`
   ```
5. Check whether the username returned in from the previous step exists as a user in your Amazon Connect instance:

   ```
   $ aws connect list-users --instance-id [INSTANCE_ID] | grep $username
   ```

   - If the final grep does not return a result then this means that the user does not exist in your Amazon Connect instance or it has been created with a different case/capitalization.
   - If your Amazon Connect instance has many users, the response from the ListUsers API call maybe paginated. Use the `NextToken` returned by the API to fetch the rest of the users. For more information, see ListUsers.

Example SAML Response

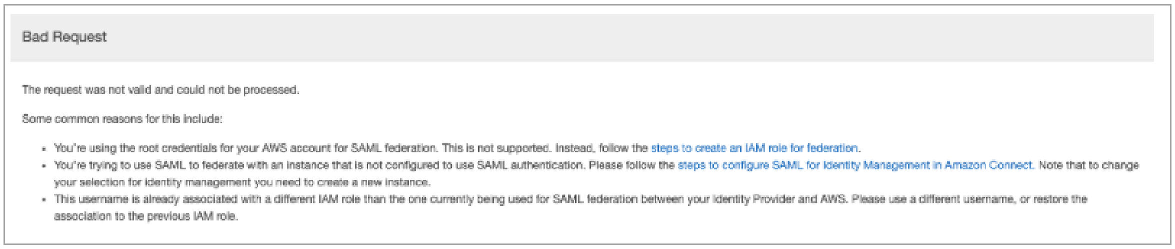
Following is an image from a sample SAML Response. In this case, the identity provider (IdP) is Azure Active Directory (Azure AD).



```
name"><AttributeValue>jane-doe@examplecorp.com</AttributeValue></Attribute><Attribute
Name="https://aws.amazon.com/SAML/Attributes/Role"><AttributeValue>arn:aws:iam::111111111111
:role/AzureAD_Role,arn:aws:iam::111111111111:saml-
provider/AzureAD_Connect_Admin</AttributeValue></Attribute><Attribute
Name="https://aws.amazon.com/SAML/Attributes/RoleSessionName"><AttributeValue><jane.doe@ex
amplecorp.com</AttributeValue></Attribute><Attribute
Name="https://aws.amazon.com/SAML/Attributes/SessionDuration"><AttributeValue>900</AttributeV
alue></Attribute></AttributeStatement><AuthnStatement AuthnInstant="2020-03-17T04:31:42.838Z"
SessionIndex="_aaaaaaaa-bbbb-cccc-dddd-
eeeeeeeeeeee"><AuthnContext><AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Passw
ord</AuthnContextClassRef></AuthnContext></AuthnStatement></Assertion></samlp:Response>
```

This is the returned RoleSessionName

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



Bad Request

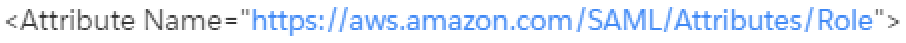
The request was not valid and could not be processed.

Some common reasons for this include:

- You're using the root credentials for your AWS account for SAML federation. This is not supported. Instead, follow the steps to create an IAM role for federation.
- You're trying to use SAML to federate with an instance that is not configured to use SAML authentication. Please follow the steps to configure SAML for Identity Management in Amazon Connect. Note that to change your selection for identity management you need to create a new instance.
- This username is already associated with a different IAM role than the one currently being used for SAML federation between your Identity Provider and AWS. Please use a different username, or restore the association to the previous IAM role.

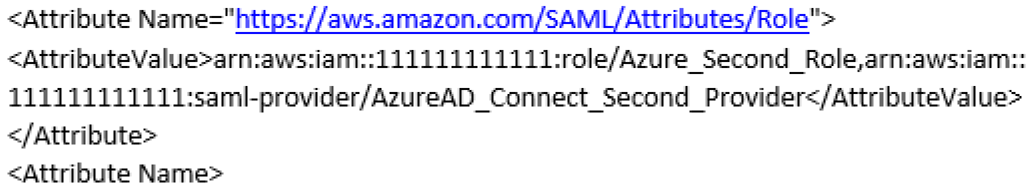
What does this mean?

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



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

Then the same user tried to login but with a different `Role` SAML Attribute, for example:



```
<Attribute Name="https://aws.amazon.com/SAML/Attributes/Role">
<AttributeValue>arn:aws:iam::111111111111:role/Azure_Second_Role,arn:aws:iam::
111111111111:saml-provider/AzureAD_Connect_Second_Provider</AttributeValue>
</Attribute>
<Attribute Name>
```

Resolution

The recommended solution is to reuse the existing Role associated with the Amazon Connect user and edit the trust relationship to reference a new identity provider or service principal to meet your new authentication requirements. If you do need to associate an Amazon Connect user with a new Role, you need to delete and recreate the user in the existing Amazon Connect instance which will result in the loss of data for that user.

For instructions for doing this in the Amazon Connect console, see Manage users in Amazon Connect (p. 785). Or, use these commands for doing this from the AWS CLI:

1. Get the user ID:

```
aws connect list-users --instance-id [INSTANCE_ID]
```

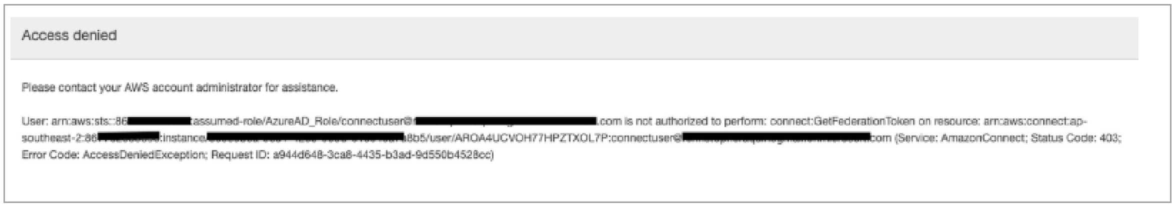
2. Delete the user account:

   ```
   aws connect delete-user --instance-id [INSTANCE_ID] --user-id [USER_ID]
   ```
3. Create the user account:

   ```
   aws create-user --username [USER_ID] --phone-config [PHONE_CONFIG]
   --security-profile-ids [SECURITY_PROFILE_ID] --routing-profile-id
   [ROUTING_PROFILE_ID] --instance-id [INSTANCE_ID]
   ```

You can also complete these actions using the AWS SDKs.

Error Message: Access denied, Please contact your AWS account administrator for assistance.



Access denied

Please contact your AWS account administrator for assistance.

User: arn:aws:sts::86[redacted]:assumed-role/AzureAD_Role/connectuser@[redacted].com is not authorized to perform: connect:GetFederationToken on resource: arn:aws:connect:ap-southeast-2:86[redacted]:instance[redacted]8b5/user/AROA4UCVOH77HPZTXOL7P:connectuser@[redacted]com (Service: AmazonConnect; Status Code: 403; Error Code: AccessDeniedException; Request ID: a944d648-3ca8-4435-b3ad-9d550b4528cc)

What does this mean?

The role that the user has assumed has successfully authenticated via SAML. However, the role doesn't have permission to call the GetFederationToken API for Amazon Connect. This call is required so the user can log in to your Amazon Connect instance using SAML.

Resolution

1. Attach a policy that has the permissions for `connect:GetFederationToken` to the role found in the error message. Following is a sample policy:

   ```
   {
       "Version": "2012-10-17",
       "Statement": [{
           "Sid": "Statement1",
           "Effect": "Allow",
           "Action": "connect:GetFederationToken",
               "Resource": [
               "arn:aws:connect:ap-southeast-2:xxxxxxxxxxxx:instance/aaaaaaaa-bbbb-cccc-
   dddd-eeeeeeeeeeee/user/${aws:userid}"
               ]
           }
       ]
   }
   ```
2. Use the IAM console to attach the policy. Or, use the attach-role-policy API, for example:

   ```
   $ aws iam attach-role-policy —role-name [ASSUMED_ROLE] —policy_arn
   [POLICY_WITH_GETFEDERATIONTOKEN]
   ```

Set up your contact center

Amazon Connect enables you to create a virtual contact center in the AWS cloud. To get started, create a virtual contact center instance. For more information, see Get started with Amazon Connect (p. 9).

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

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

Things to know before you begin

- When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon Connect. You are charged only for the services that you use. To create an AWS account, see How do I create and activate an AWS account?
- To allow an IAM user to create an instance, ensure that they have the permissions granted by the **AmazonConnect_FullAccess** policy.

- For a list of the minimum IAM permissions required to create an instance, see Required permissions for using custom IAM policies to manage access to the Amazon Connect console (p. 1082).
- Amazon Connect is not available to customers in India using Amazon Web Services through Amazon Internet Services Pvt. Ltd (AISPL). You will receive an error message if you try to create an instance in Amazon Connect.
- When you create an instance, you must decide how you want to manage users. **You can't change the identity management option after you create the instance**. For more information, see Plan your identity management in Amazon Connect (p. 123).

Step 1: Set identity

Permissions to access Amazon Connect features and resource are assigned to user accounts within Amazon Connect. When you create an instance, you must decide how you want to manage users. You can't change the identity management option after you create the instance. For more information, see Plan your identity management in Amazon Connect (p. 123).

To configure identity management for your instance

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

Step 2: Add administrator

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

To specify the administrator for your instance

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

Step 3: Set telephony

Use the options in this section to choose whether you want your agents to receive calls from customers, make outbound calls, and hear early media audio.

Early media

When early media audio is enabled, for outbound calls your agents can hear pre-connection audio such as busy signals, failure-to-connect errors, or other informational messages provided by telephony providers.

By default, early media is enabled for you. Note the following exception:

- Your instance was created before April 17, 2020, and you weren't enrolled in the preview program. You need to enable early media audio. For instructions, see Update telephony options (p. 140).

To configure telephony options for your instance

1. To allow inbound calls to your contact center, choose **Allow incoming calls**.
2. To enable outbound calling from your contact center, choose **Allow outgoing calls**.
3. To enable multi-party calls, choose **Enable up to six parties on a call**.
4. Choose **Next**.

Step 4: Data storage

> **Note**
> Amazon Connect does not support Amazon S3 Object Lock in compliance mode to store objects using a write-once-read-many (WORM) model.

When you create an instance, by default we create an Amazon S3 bucket. Data, such as reports and recordings of conversations, is encrypted using AWS Key Management Service, and then stored in the Amazon S3 bucket.

This bucket and key are used for both recordings of conversations and exported reports. Alternatively, you can specify separate buckets and keys for recordings of conversations and exported reports. For instructions, see Update instance settings (p. 140).

By default, Amazon Connect creates buckets for storing call recordings, chat transcripts, exported reports, and contact flow logs.

- When a bucket is created to store call recordings, call recording is enabled at the instance level. The next step for setting up this functionality is to set up recording behavior in a contact flow (p. 479).
- When a bucket is created to store chat transcripts, chat transcription is enabled at the instance level. Now all chat transcripts will be stored. Only if you want to monitor chat conversations do you need to set up recording behavior in a contact flow (p. 479).
- Live media streaming is not enabled by default.

By default, Amazon Connect creates a Customer Profiles domain, which stores profiles that combine customer contact history with customer information such as account number, address, billing address, and birth date. Data is encrypted using AWS Key Management Service. You can configure Customer Profiles to use your own customer managed key after your instance is set up. For more information, see Create a KMS key to be used by Customer Profiles to encrypt data (required) (p. 642).

Review and copy the location of the S3 bucket, contact flow logs, and whether you want to enable Customer Profiles.

1. If desired, copy the location of the S3 bucket where your data encryption is stored, and the location of the contact flow logs in CloudWatch.
2. Choose **Next**.

Step 5: Review and create

To create your instance

1. Review the configuration choices. Remember that you cannot change the identity management options after you create the instance.
2. (Optional) To change any of the configuration options, choose **Edit**.
3. Choose **Create instance**.
4. (Optional) To continue configuring your instance, choose **Get started** and then choose **Let's go**. If you prefer, you can access your instance and configure it later on. For more information, see Next steps (p. 138).

   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. 157).

Create a dev (Sandbox) or test (QA) instance

You might want to create multiple contact center instances, for example, one as a Sandbox for development, another for QA, and a third for Production.

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

> **Important**
> Most entities in Amazon Connect can be (re)created and replicated among instances using the Amazon Connect API. While doing that keep the following limitations in mind:
>
> - Service quotas are specific to each instance.
> - Some supporting services, such as User Directory, can be linked to only one Amazon Connect instance at a time.
> - Any additional external and Region-specific limitations.
>
> For more information, see Can I migrate my Amazon Connect instance from a test environment to a production environment?

To create another instance

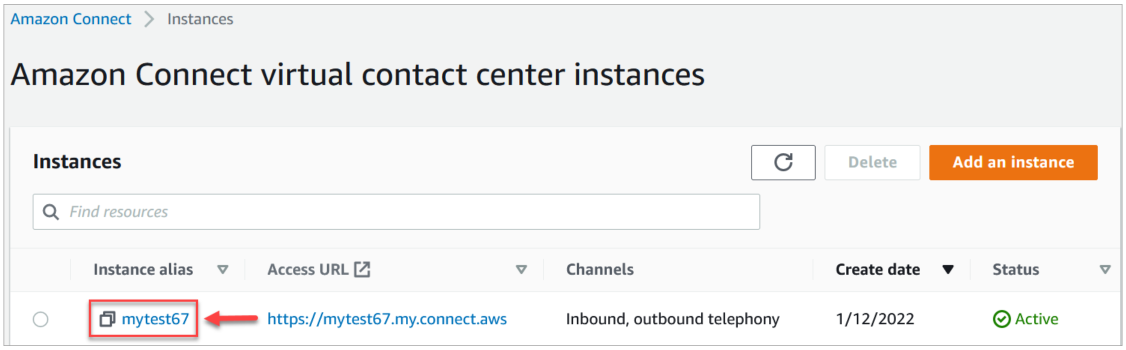
1. In the AWS Management Console, choose **Amazon Connect**.
2. Choose **Add an instance**.

3. Complete the steps on the Amazon Connect resource configuration page. For instructions see Create an Amazon Connect instance (p. 135).

Find your Amazon Connect instance ID/ARN

When you open a support ticket, you may be asked to provide your Amazon Connect instance ID (also called the ARN). Use the following steps to find it.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.

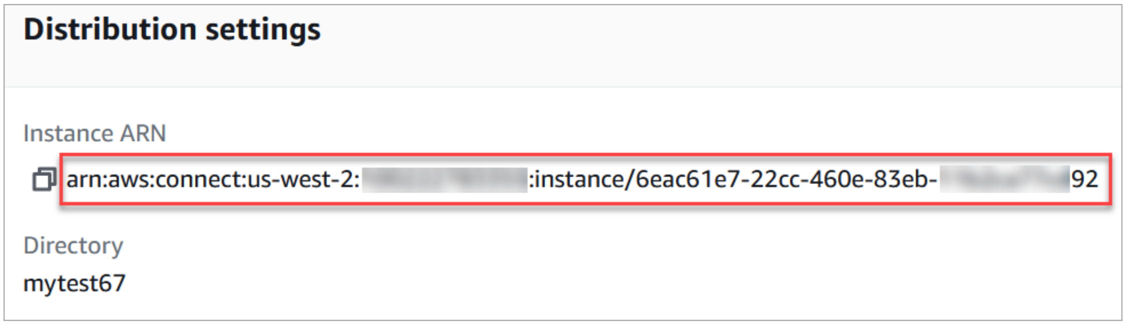


Amazon Connect > Instances

Amazon Connect virtual contact center instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

On the **Account overview** page, in the **Distribution settings** section, you can see the full instance ARN.

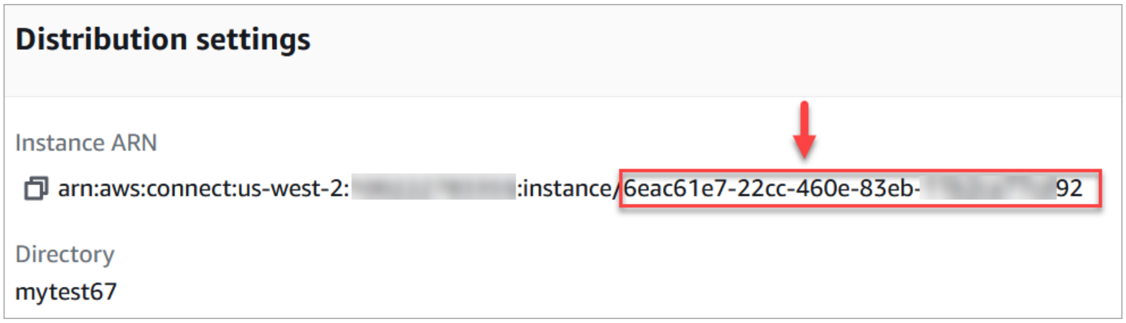


Distribution settings

Instance ARN
arn:aws:connect:us-west-2:[redacted]:instance/6eac61e7-22cc-460e-83eb-[redacted]92

Directory
mytest67

The information after **instance/** is the instance ID.



Distribution settings

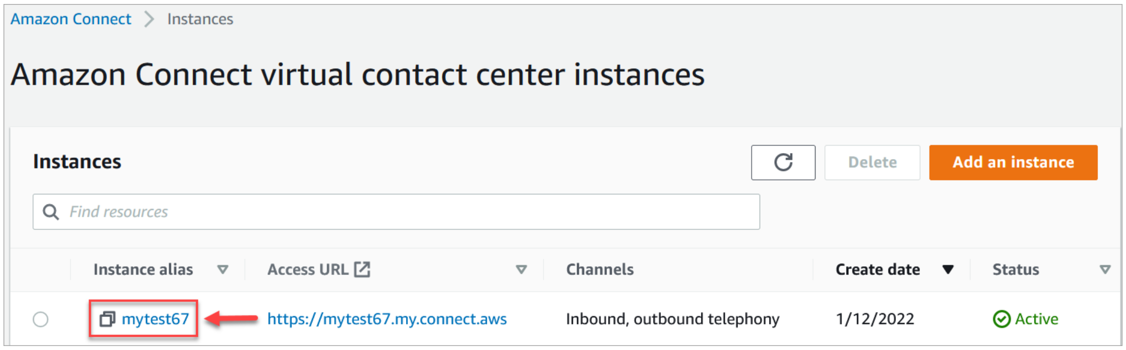
Instance ARN
arn:aws:connect:us-west-2:[redacted]:instance/6eac61e7-22cc-460e-83eb-[redacted]92

Directory
mytest67

Find your Amazon Connect instance name

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

2. On the instances page, the instance name appears in the **Instance Alias** column. This instance name appears in the URL you use to access Amazon Connect.

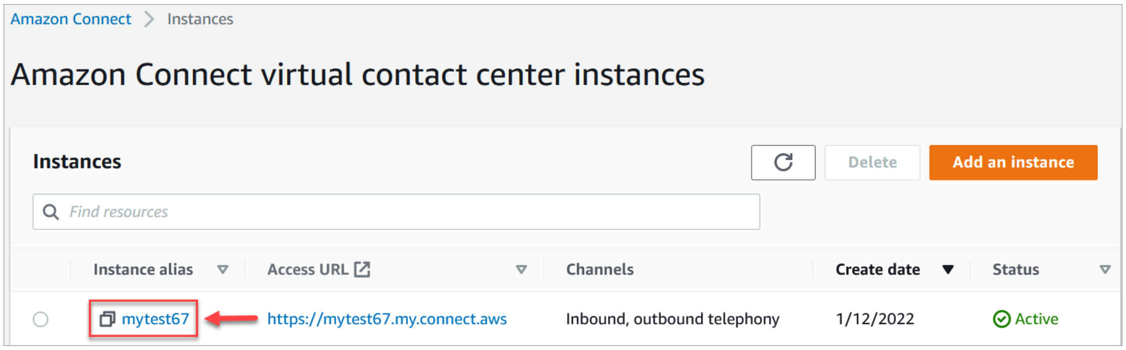

Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

Update instance settings

To update the instance settings:

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.


Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. Complete the following procedures.

Update telephony options

1. In the navigation pane, choose **Telephony**.
2. To enable customers to call into your contact center, choose **Receive inbound calls with Amazon Connect**.
3. To enable outbound calling from your contact center, choose **Make outbound calls with Amazon Connect**.
4. To enable high-volume outbound communications, choose **Enable high-volume outbound communications**.
5. By enabling early media audio, your agents can hear pre-connection audio such as busy signals, failure-to-connect errors, or other informational messages from telephony providers, when making outbound calls. Choose **Enable early media**.
6. By default, you can have three participants on a call (for example, two agents and a customer, or an agent, a customer, and an external party). To enable multi-party calls with more participants, choose **Enable up to six parties on a call**. This feature is only available in CCPv2.
7. Choose **Save**.

Update data storage

1. In the navigation pane, choose **Data storage**.
2. To specify the bucket and KMS key for recordings of voice conversations, choose **Call recordings**, **Edit**, specify the bucket name and prefix, select the KMS key by name, and then choose **Save**.

   When this bucket is created, call recording is enabled at the instance level. The next step for setting up this functionality is to set up recording behavior in a contact flow (p. 479).
3. To specify the bucket and KMS key for recordings (transcripts) of chat conversations, choose **Chat transcripts**, **Edit**, specify the bucket name and prefix, select the KMS key by name, and then choose **Save**.

   When this bucket is created, chat transcripts are enabled at the instance level. Now all chat transcripts will be stored here.
4. To enable live media streaming, choose **Live media streaming**, **Edit**. For more information, see Capture customer audio: live media streaming (p. 775).
5. 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**.
6. To enable file sharing for both agents and customers, next to **Attachments** choose **Edit**, then **Enable Attachments sharing**. For more information about this option and additional steps, see Enable attachments to share files using chat (p. 142).
7. To enable a **Customer Profiles domain**, choose that option.

   A Customer Profiles domain stores profiles that combine customer contact history with customer information such as account number, address, billing address, and birth date. Data is encrypted using AWS Key Management Service. You can configure Customer Profiles to use your own customer managed key after your instance is set up. For more information, see Create a KMS key to be used by Customer Profiles to encrypt data (required) (p. 642).

Update data streaming options

1. In the navigation pane, choose **Data streaming**.
2. Choose **Enable data streaming**. For more information, see Enable data streaming for your instance (p. 145).
3. For **Contact records**, do one of the following:
   - Choose **Kinesis Firehose** and select an existing delivery stream, or choose **Create a new Kinesis Firehose** to open the Kinesis Firehose console and create the delivery stream.
   - Choose **Kinesis Stream** and select an existing stream, or choose **Create a new Kinesis Firehose** to open the Kinesis console and create the stream.
4. For **Agent Events**, select an existing Kinesis stream or choose **Create a new Kinesis Stream** to open the Kinesis console and create the stream.
5. Choose **Save**.

Update analytics tools options

1. In the navigation pane, choose **Analytics tools**.
2. Choose **Enable Contact Lens**. For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 811).
3. Choose **Save**.

Update contact flow settings

1. In the navigation pane, choose **Contact flows**.
2. (Optional) To add a signing key for use in contact flows, choose **Add key**. For more information, see Encrypt customer input (p. 508).
3. (Optional) To integrate with Amazon Lex, select a Lex bot. For more information, see Add an Amazon Lex bot (p. 617).
4. (Optional) To integrate with AWS Lambda, select a Lambda function. For more information, see Invoke AWS Lambda functions (p. 488).
5. (Optional) To enable contact flow logs, choose **Enable Contact flow logs**. For more information, see Track events as customers interact with contact flows (p. 509).
6. (Optional) To use the best available voice from Amazon Polly, choose **Use the best available voice**. For more information, see Amazon Polly best sounding voice (p. 457).
7. (Optional) Use the voices available in Amazon Polly.

Enable attachments to share files using chat

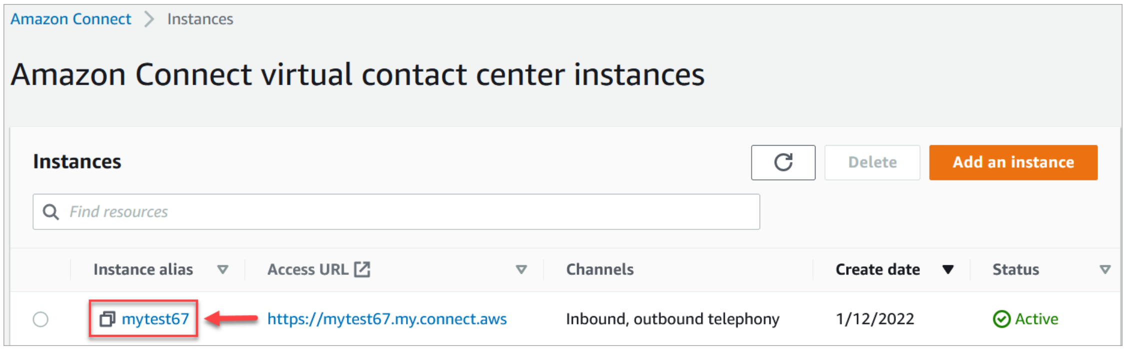
You can allow customers and agents to share files using chat. After you complete the steps in this topic, an attachment icon automatically appears in your agent's Contact Control Panel so they can share attachments on chats.

You will need to update your customer-facing user interface to support attachment sharing.

Using a custom agent application? Check out the APIs we've added to support attachment sharing: StartAttachmentUpload, CompleteAttachmentUpload, and GetAttachment.

Step 1: Enable attachments

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



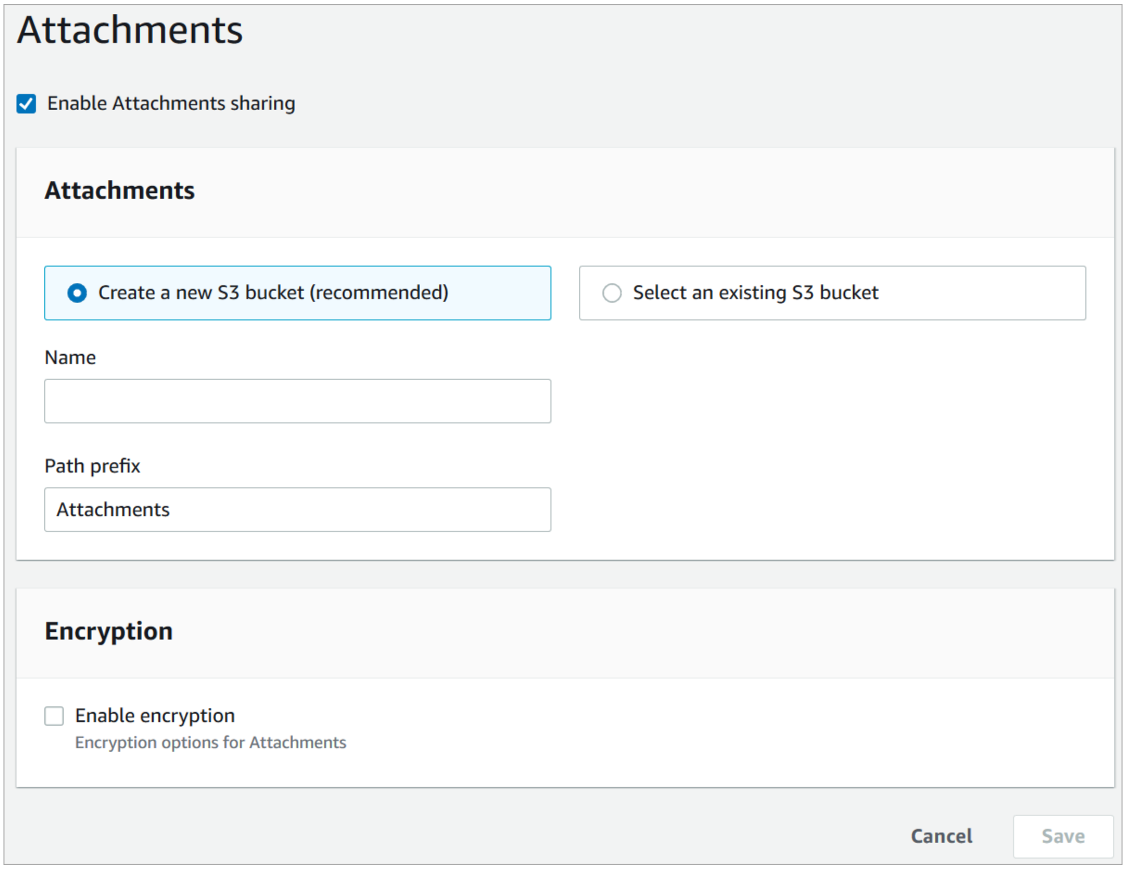
Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. On the **Data storage** page, under the **Attachments**, choose **Edit**, select **Enable Attachments sharing**, and then choose **Save**.

   Storage options appear, similar to the following image.



Attachments

☑ Enable Attachments sharing

Attachments

● Create a new S3 bucket (recommended)

○ Select an existing S3 bucket

Name

Path prefix

Attachments

Encryption

□ Enable encryption
Encryption options for Attachments

4. You can change the Amazon S3 bucket location where attachments are stored. By default, your existing Amazon Connect bucket is used, with a new prefix for attachments.

   Note
   Currently, Amazon Connect doesn’t support S3 buckets with Object Lock enabled.

   The attachments feature leverages two Amazon S3 locations: a staging location and a final location.

   Note the following about the staging location:

   - The staging location is used as part of a business validation flow. Amazon Connect uses it to validate the file size and type before it is shared with the chat participant.
   - The staging prefix is created by Amazon Connect based on the bucket path you have selected. Specifically, it includes the S3 prefix for where you are saving files, with **staging** appended to it.
   - We recommend that you change the data retention policy for the staging prefix to one day. This way you won't be charged for storing the staging files. For instructions, see How do I create a lifecycle rule for an S3 bucket? in the *Amazon S3 User Guide*.

     Warning
     Only change the lifecycle for the **file staging location**. If you accidentally change the lifecycle for the entire Amazon S3 bucket, all transcripts and attachments will be deleted.

Step 2: Configure a CORS policy on your attachments bucket

To allow customers and agents to upload and download files, update your cross-origin resource sharing (CORS) policy to allow `PUT` and `GET` requests for the Amazon S3 bucket you are using for attachments.

This is more secure than enabling public read/write on your Amazon S3 bucket, which we don't recommend.

To configure CORS on the attachments bucket

1. Find the name of the Amazon S3 bucket for storing attachments:

    a. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.

    b. In the Amazon Connect console, choose **Data storage**, and locate the Amazon S3 bucket name.
2. Open the Amazon S3 console at https://console.aws.amazon.com/s3/.
3. In the Amazon S3 console, select your Amazon S3 bucket.
4. Choose the **Permissions** tab, and then scroll down to the **Cross-origin resource sharing (CORS)** section.
5. Add a CORS policy that has one of the following rules on your attachments bucket. For example CORS policies, see Cross-origin resource sharing: Use-case scenarios in the *Amazon S3 Developer Guide*.

    - Option 1: List the endpoints from where attachments will be sent and received, such as the name of your business web site. This rule allows cross-origin PUT and GET requests from your website (for example, http://www.example1.com).

      Your CORS policy might look like the following example:

```
[
    {
        "AllowedMethods": [
            "PUT",
            "GET"
        ],
        "AllowedOrigins": [
            "http://www.example1.com",   //List the endpoints from where attachments
 will be sent and received,
            "http://www.example2.com"    //such as the name of your business web
 site.
       ],
       "AllowedHeaders": [
            "*"
       ]
    }
]
```

    - Option 2: Add the `*` wildcard to `AllowedOrigin`. This rule allows cross-origin PUT and GET requests from all origins, so you don't have to list your endpoints.

      Your CORS policy might look like the following example:

```
[
    {
        "AllowedMethods": [
            "PUT",
            "GET"
        ],
        "AllowedOrigins": [
            "*"
        ],
        "AllowedHeaders": [
            "*"
        ]
    }
]
```

Step 3: Update your chat UI

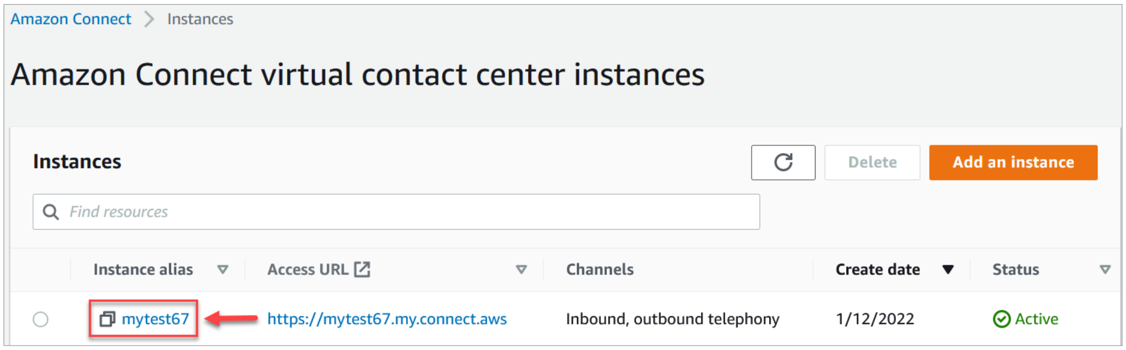
To help you update the chat user interface that your customers use, we've posted an updated version of chat interface JS. It exposes an attachment icon on the UI and supports the backend calls for attachment sharing. See Amazon Connect Chat UI Examples on GitHub.

Enable data streaming for your instance

You can export contact records and agent events from Amazon Connect and perform real-time analysis on contacts. Data streaming sends data to Amazon Kinesis.

To enable data streaming for your instance

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



Amazon Connect > Instances

Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Data streaming**.
4. Choose **Enable data streaming**.
5. For **Contact records**, do one of the following:
   - Choose **Kinesis Firehose** and select an existing delivery stream, or choose **Create a new Kinesis firehose** to open the Kinesis Firehose console and create the delivery stream. For more information, see Creating an Amazon Kinesis Data Firehose Delivery Stream.
   - Choose **Kinesis Stream** and select an existing stream, or choose **Create a Kinesis stream** to open the Kinesis console and create the stream. For more information, see Creating and Managing Streams.
6. For **Agent Events**, select an existing Kinesis stream or choose **Create a new Kinesis stream** to open the Kinesis console and create the stream.
7. Choose **Save**.

Using server-side encryption for the Kinesis stream

If you enable server-side encryption for the Kinesis stream you select, Amazon Connect cannot publish to the stream because it does not have permission to call `kms:GenerateDataKey` so that it can encrypt data sent to Kinesis. To work-around this, do the following steps:

1. Enable encryption for recordings of conversations or scheduled reports.
2. Create a customer managed key to use for encryption.
3. Choose the same customer managed key for the Kinesis data stream that you use for scheduled reports or recordings of conversations.

   For more information, see Creating Keys in the *AWS Key Management Service Developer Guide*.

Emergency admin login

As a best practice, users assigned to the Amazon Connect **Admin** security profile should always use their Amazon Connect instance URL to login:

- Log in to your contact center at https://*instance name*.my.connect.aws/.

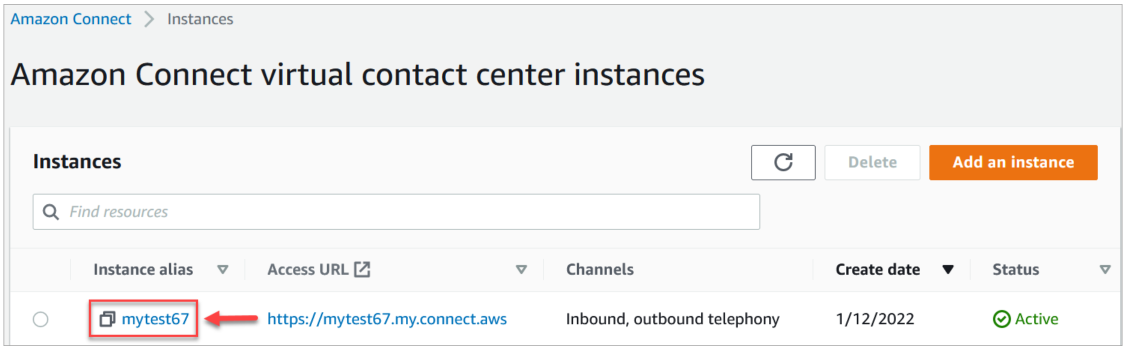
This method ensures the appropriate levels security.

However, if there's an emergency, you can log in from the Amazon Connect console using your AWS account credentials. For example, you may need to login in this way in the following situations:

- You forgot your Amazon Connect administrator password and no other Amazon Connect administrators are around to reset it.
- Someone deleted the Amazon Connect **Admin** security profile by mistake.

To login for emergency access

1. Make sure you have your AWS account credentials at hand and that you have the required permissions (p. 1095).
2. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
3. If prompted to login, enter your AWS account credentials.
4. Choose the name of the instance from the **Instance alias** column.



Amazon Connect > Instances

Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

5. In the navigation pane, choose **Overview**.
6. Choose **Log in for emergency access**.

   You aren't prompted for your credentials because you are federated in from the AWS console.

   Important
   For daily usage, we strongly recommend always using your instance URL to login. The procedure provided in this article should only be used for emergency access when using the instance URL is not an option.

To log out

To log out of your instance, go to the title bar at the top of the screen and select the icon with the arrow (**Log out**) that appears next to your user name.

Delete your Amazon Connect instance

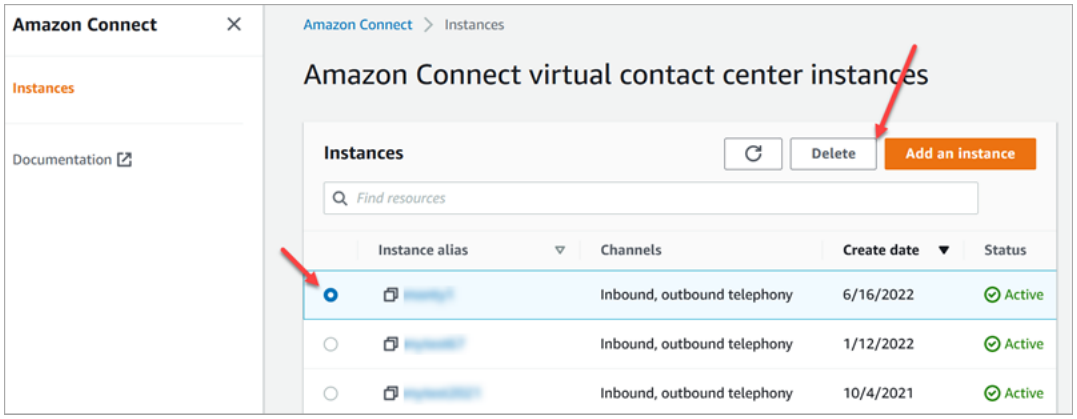
If you no longer need your contact center, you can delete your Amazon Connect instance. When you delete an instance, we release its claimed phone number back to inventory. When customers call the phone number that you've released, they'll get a message that it's not a working phone number.

> **Important**
> You can't restore a deleted instance or access its settings, data, metrics, and reports.

Delete your instance

To delete your Amazon Connect instance

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Select the radio button for the instance.
3. Choose **Delete**. If you don't see the **Delete** button, you don't have permissions to delete instances. Contact your AWS administrator for help.



	Instance alias	Channels	Create date ▼	Status
●	[redacted]	Inbound, outbound telephony	6/16/2022	Active
○	[redacted]	Inbound, outbound telephony	1/12/2022	Active
○	[redacted]	Inbound, outbound telephony	10/4/2021	Active

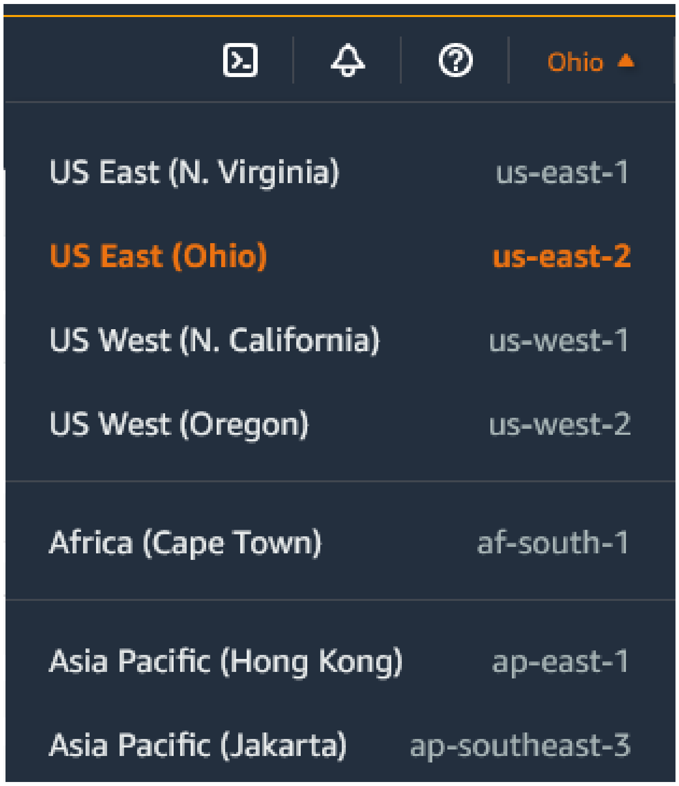
4. When prompted, enter the name of the instance and then choose **Delete**.

Error message: "Region Unsupported. Amazon Connect is not available in [Region]"

If you get this error message, it means that you selected a Region in the AWS Management Console that is not the Region in which you created the Amazon Connect instance, and Amazon Connect isn't available in that Region.

To switch Regions and delete your Amazon Connect instance

1. From the navigation bar, open the Region selector. Select the Region in which you created the Amazon Connect instance.


Ohio
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2
Africa (Cape Town) af-south-1
Asia Pacific (Hong Kong) ap-east-1
Asia Pacific (Jakarta) ap-southeast-3

2. From the navigation bar, choose **Amazon Connect** from the list of services to open the Amazon Connect console. If you don't see the instance, keep selecting from the supported Regions until you find your instance.
3. Select the radio button for the instance.
4. Choose **Delete**. If you don't see the **Delete** button, you don't have permissions to delete instances. Contact your AWS administrator for help.
5. When prompted, enter the name of the instance and then choose **Delete**.

Test voice, chat, and task experiences

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

Test voice

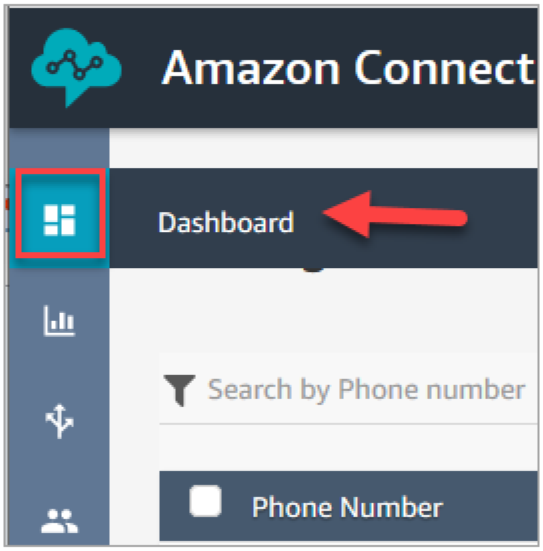
After you claim a number you can immediately call it to hear what the experience will be like for your customers. Amazon Connect uses the default contact flows (p. 297) to power your initial experience.

To test a customized contact flow, assign a phone number (p. 453) to it and then call that number.

Test chat

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

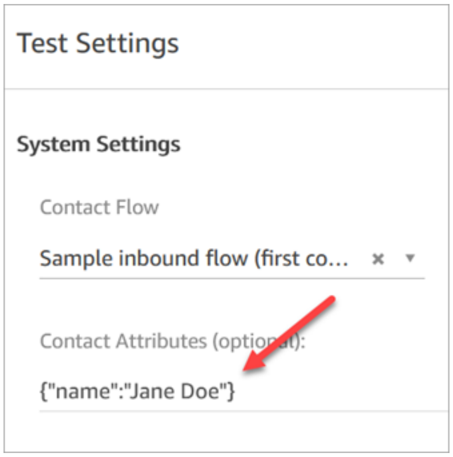
1. On the navigation menu, choose **Dashboard**.



2. Choose **Test chat**.

   If you don't see the option to test chat, click here.
3. On the **Test Chat** page, choose **Test Settings**.
4. Under **System Settings**, choose the contact flow you want to test with chat, and then click **Apply**. By default, it runs the Sample inbound flow (p. 309).

   Tip
   If you want to test a chat and use contact attributes, note that the key and value pair must be enclosed in quotes, as shown in the following image:

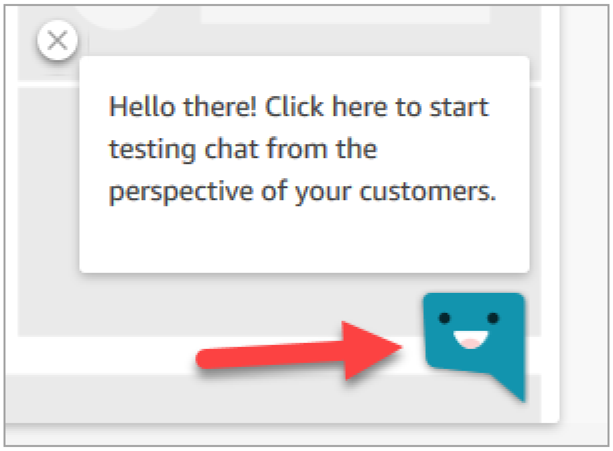
   

   Test Settings

   System Settings

   Contact Flow: Sample inbound flow (first co...

   Contact Attributes (optional): {"name":"Jane Doe"}
5. In the chat window, click the icon as shown below.



Hello there! Click here to start testing chat from the perspective of your customers.

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

   Tip
   The test environment uses the BasicQueue and Basic Routing Profile. The Basic Routing Profile is set up for 2 chats. If you want to test what it's like to have more than two chats, change the Basic Routing Profile to 5 chats. For instructions, see Create a routing profile (p. 227).

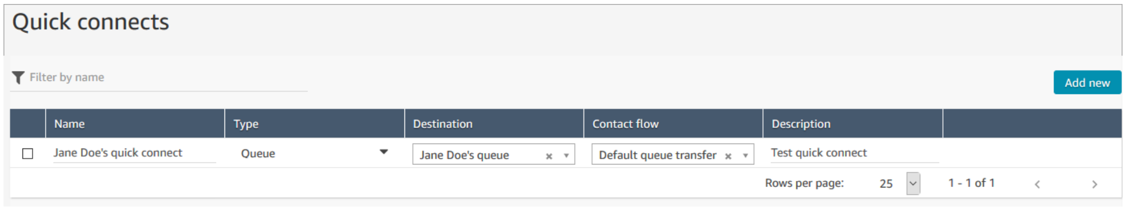
   To learn more about what the agent experiences when managing chat conversations, see Chat with contacts (p. 1148).

Test tasks

The first step in testing the task experience is to create a quick connect for the queue you want to assign the example tasks to.

Step 1: Create a quick connect

1. On the navigation menu, choose **Routing**, **Quick connects**, **Add a new**.
2. Enter a name for the quick connect. For example, if you want to assign the test task to yourself, enter your name (for example, **Jane Doe**).
3. Under **Type**, use the dropdown list to choose **Queue**.
4. Under **Destination**, use the dropdown list to choose a queue you set up for yourself (assuming you want to assign the test task to yourself).
5. Under **Contact flow**, choose **Default queue transfer**.
6. Under **Description**, enter something like **Test quick connect**.
7. Choose **Save**.

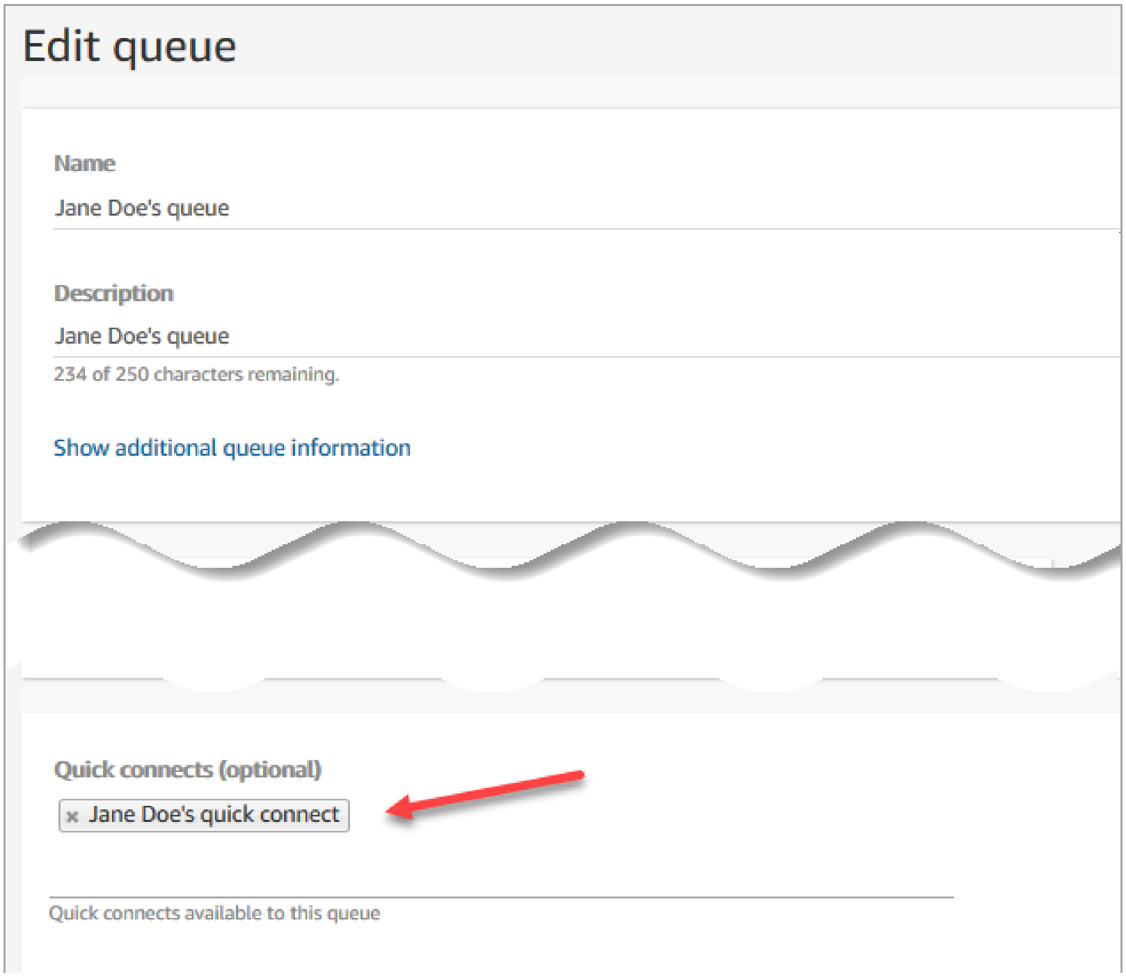


Quick connects

	Name	Type	Destination	Contact flow	Description
□	Jane Doe's quick connect	Queue	Jane Doe's queue	Default queue transfer	Test quick connect

Step 2: Make the quick connect visible in the CCP by assigning it to a queue

1. After you create the quick connect, go to **Routing**, **Queues** and then choose the appropriate queue for the contact to be routed to.
2. On the **Edit queue** page, in the **Quick connects** box, search for the quick connect you created. For example, it might have your name.



Edit queue

Name: Jane Doe's queue

Description: Jane Doe's queue

234 of 250 characters remaining.

Quick connects (optional): Jane Doe's quick connect

Quick connects available to this queue

3. Select the quick connect and then choose **Save**.

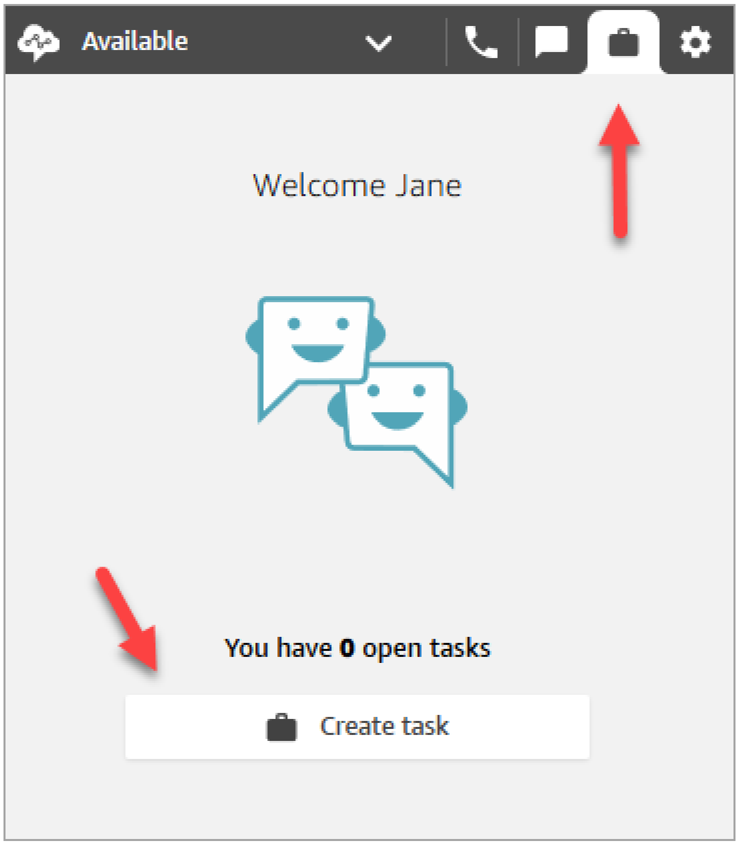
Step 3: Assign the queue to the agent's routing profile

1. Go to **Users**, **Routing profiles** and choose the agent's routing profile.
2. Under **Set channels and concurrency** choose **Tasks**.
3. Add the agent's queue to the routing profile, and choose **Task** for the channel.

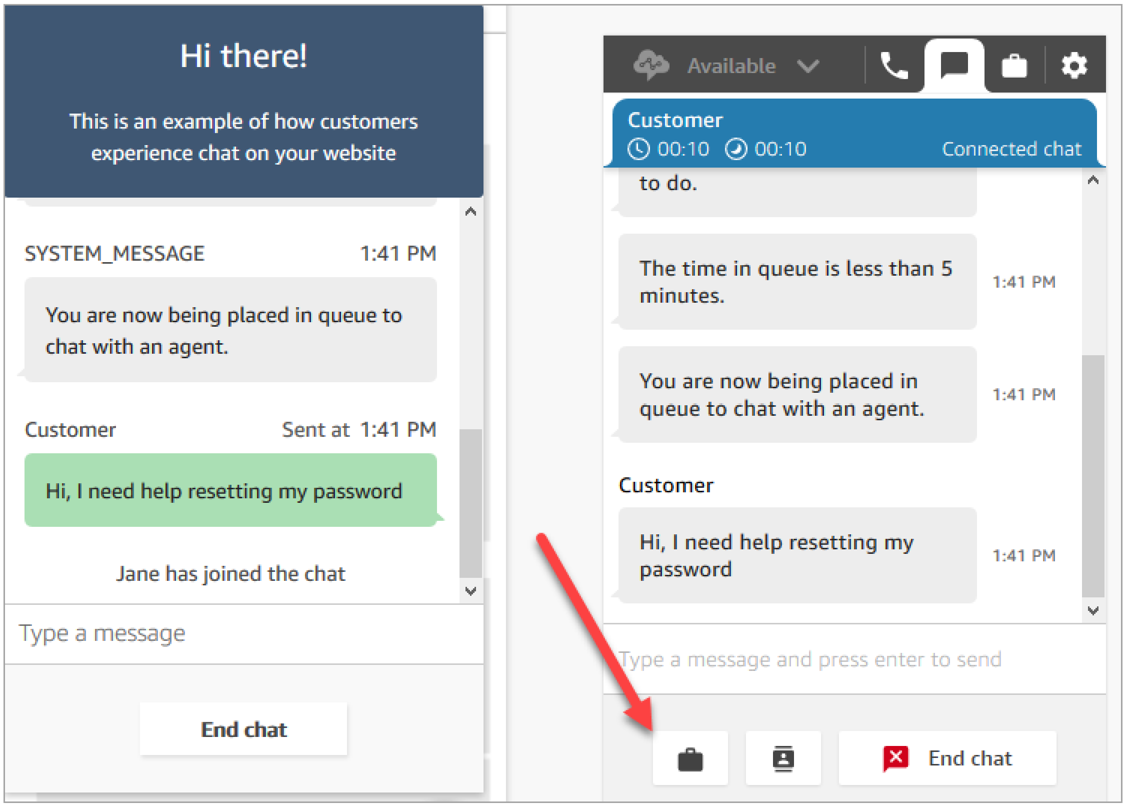
   If the agent can receive transfers through other channels, select them as well.
4. Choose **Save**.

Step 4: Test tasks

1. Open the CCP. Select the **Task** tab, and then choose **Create task**.



Or, if you're testing the chat experience, for example, you can choose the **Task** icon, as shown in the following image.

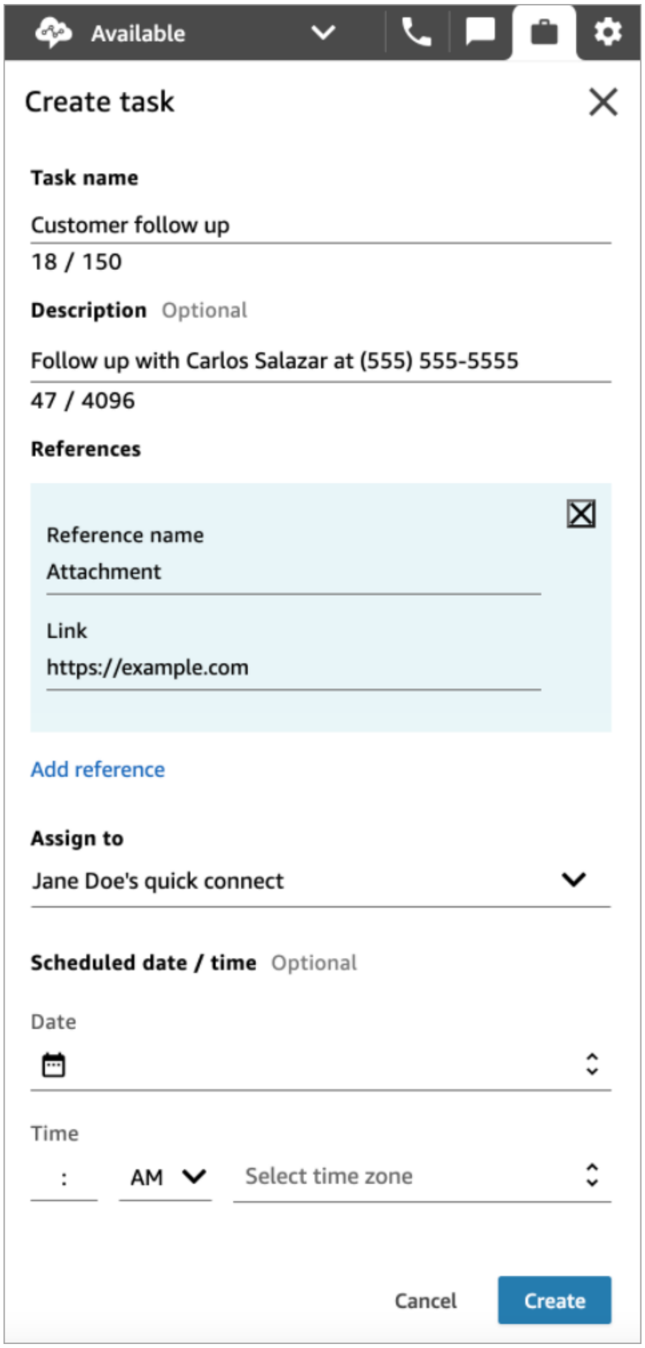


Hi there!
This is an example of how customers experience chat on your website
SYSTEM_MESSAGE 1:41 PM
You are now being placed in queue to chat with an agent.
Customer Sent at 1:41 PM
Hi, I need help resetting my password
Jane has joined the chat
Type a message
End chat
Available
Customer
00:10 00:10 Connected chat
to do.
The time in queue is less than 5 minutes. 1:41 PM
You are now being placed in queue to chat with an agent. 1:41 PM
Customer
Hi, I need help resetting my password 1:41 PM
Type a message and press enter to send
End chat

2. Complete the **Create task** page. When you choose **Assign to**, you can assign only a task to someone or a queue that has quick connect.

   To create a scheduled task for the future, use the **Scheduled date/time** box to choose a future date and time. You can schedule a task up to six days in future.

   Choose **Create**.



Create task

Task name

Customer follow up

18 / 150

Description Optional

Follow up with Carlos Salazar at (555) 555-5555

47 / 4096

References

Reference name

Attachment

Link

https://example.com

Assign to

Jane Doe's quick connect

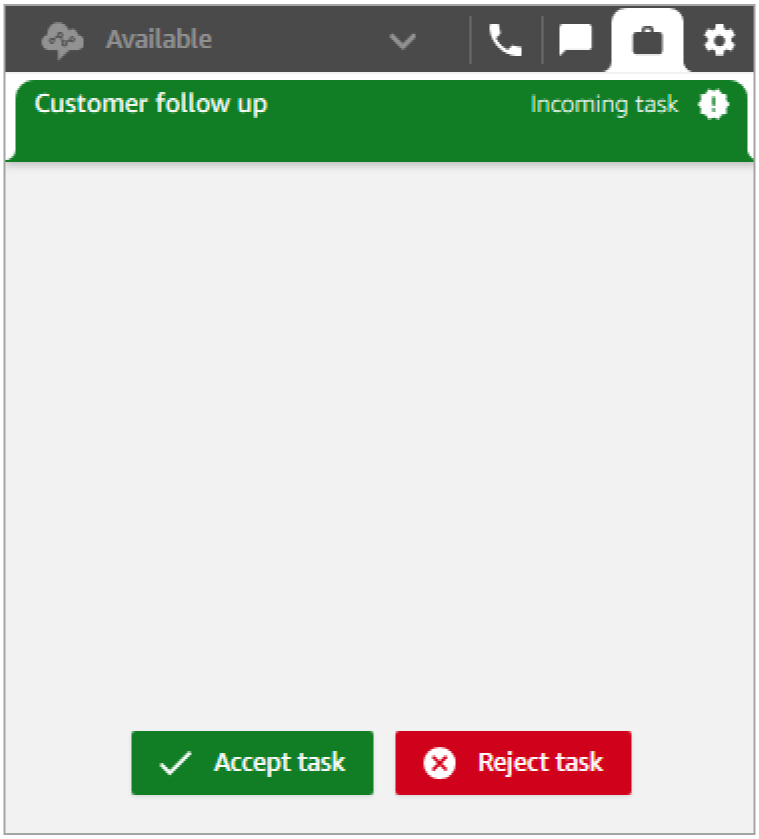
Scheduled date / time Optional

Date

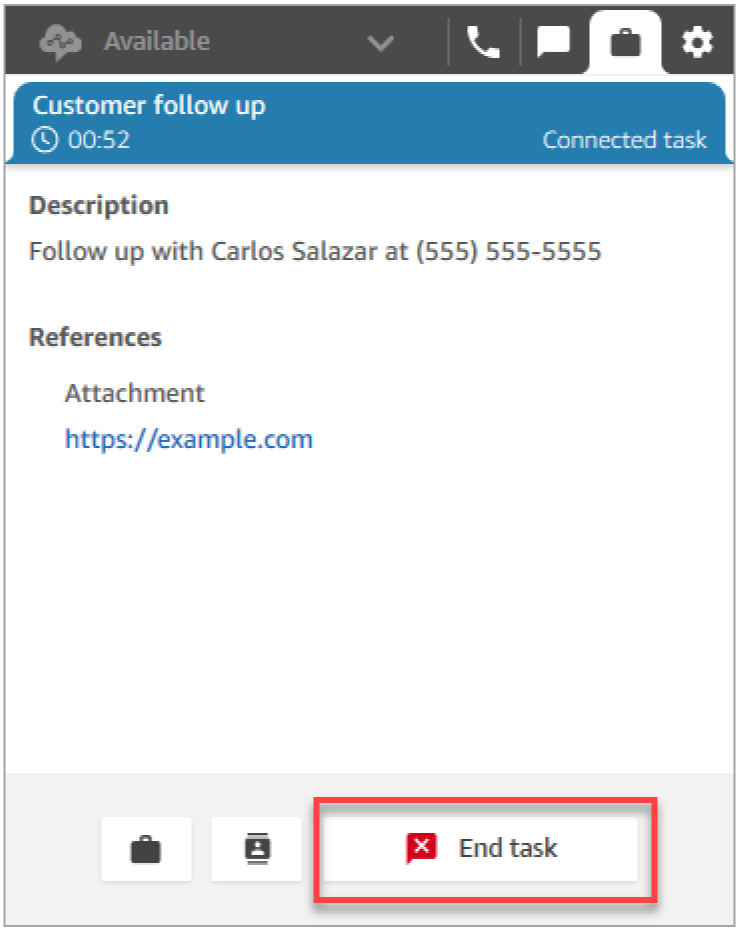
Time

: AM Select time zone

3. If you chose yourself, the task will be routed to you. Choose **Accept task**.



4. Review the task, and choose **End task** when done.



Description

Follow up with Carlos Salazar at (555) 555-5555

References

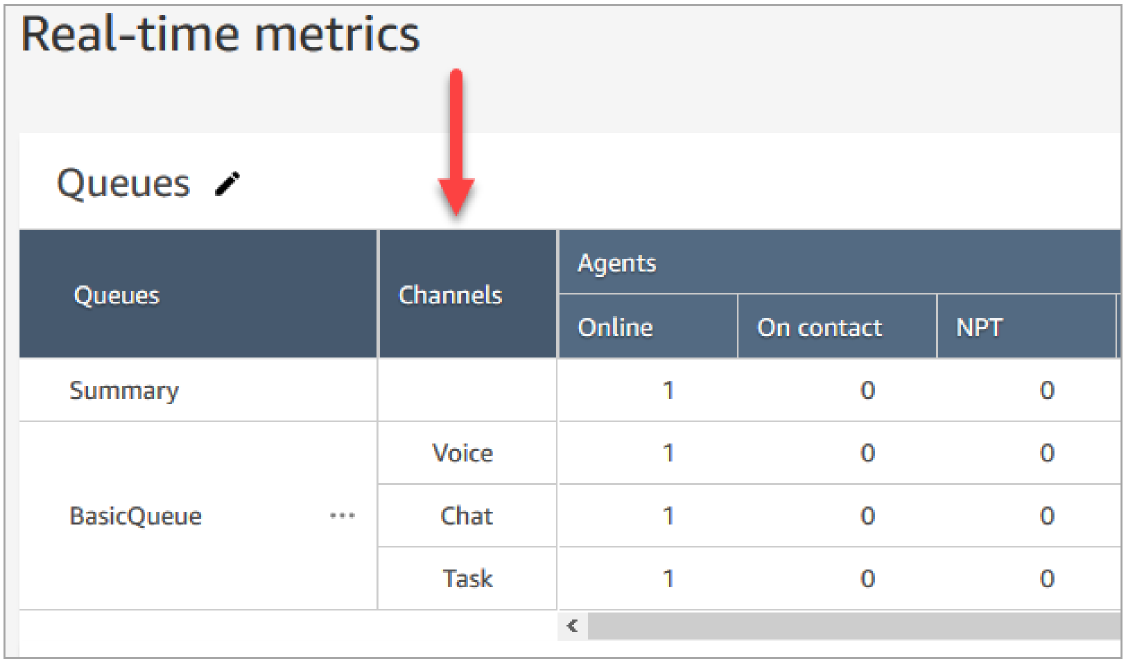
Attachment

https://example.com

View metrics for the test experiences

When you're testing the voice, chat, and task experiences, you may also want to explore metrics.

1. On the left navigation menu, choose **Analytics**, **Real-time metrics**, **Queues**.
2. You can review the real-time metrics as you test the different channels.
3. To view metrics by channel in a real-time metrics report, go to **Settings**, **Groupings**, **Queues grouped by channels**, **Apply**. Your report will look similar to the following image.



Real-time metrics

Queues

Queues	Channels	Agents		
		Online	On contact	NPT
Summary		1	0	0
BasicQueue	Voice	1	0	0
	Chat	1	0	0
	Task	1	0	0

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 claimed phone number costs, see Amazon Connect pricing.
- For a list of the telephony capabilities that Amazon Connect provides, see the Amazon Connect Telecoms Country Coverage Guide.

If you want to keep a phone number you already have, you can port the phone number and use it with Amazon Connect. After a phone number is ported to Amazon Connect, it appears in the list of available phone numbers for you to assign to contact flows.

Contents

Port your current phone number

You can port your existing phone numbers to your Amazon Connect contact center.

Contents

Things to know before porting

The topics in this section explain which numbers can be ported, how long it takes, and what fees you might incur.

Contents

What is phone number porting?

Porting a phone number is the process of moving a phone number from one telephony service provider, or carrier, to another. Many businesses and organizations already have a phone number that is advertised to their customers, and changing this number would be disruptive.

If you port a phone number from your current carrier to Amazon Connect, you can keep using the same phone number for your contact center. This helps to eliminate the need to update your business contact information.

Downtime and service disruption during the porting process

The porting process requires the losing carrier to remove your number from their systems, the winning carrier to add your number to their systems, and for number routing to be updated. Most porting activities complete within 15-30 minutes, with possible call disruptions. To ensure that they have engineers available to troubleshoot issues, most losing carriers complete porting actions only during normal business hours. Carriers typically communicate a two-hour porting window to accommodate for resolving any issues that could arise.

For detailed information about available porting dates and times, see Region requirements for ordering and porting phone numbers (p. 171) for your country or region.

What happens to a number after it is ported

As long as you continue to pay for the phone number, and do not release it from your Amazon Connect instance, it stays assigned to your account, and you are billed accordingly.

To release a phone number, follow the steps in Release a phone number (p. 170).

When a phone number is released from your Amazon Connect instance:

- You will no longer be charged for it.
- You cannot reclaim the phone number.
- Amazon Connect reserves the right to allow it to be claimed by another customer.

If you move your contact center away from Amazon Connect, and want to port your phone number away from Amazon Connect, see Port phone numbers away from Amazon Connect (p. 167).

How much does number porting cost?

Amazon Connect does not charge fees for porting numbers. Your existing carrier may have fees associated with the disconnection and early termination of your service.

After a phone number is ported to Amazon Connect, standard pricing applies for Amazon Connect service usage and associated telephony rates.

Can my number be ported to Amazon Connect?

Not all phone numbers can be ported. The ability to port a specific phone number depends on several factors. For example:

- The regulations in the country of the phone number.
- Agreements between the losing and winning carriers.
- The type of phone number being ported.
- Your service contract with your current service provider.

To find out if a phone number that you currently own—whether local, mobile, or toll-free—can be ported to Amazon Connect:

1. See if your country supports number porting: Region requirements for ordering and porting phone numbers (p. 171).
2. Then get started by submitting an Amazon Connect support ticket for number verification (p. 162).

Porting numbers purchased from other contact center providers

In most cases, you can port numbers that were purchased from other contact center providers. Confirm with your current contact center provider who holds the assignment to the number, and work with them to ensure the correct information is provided on the Letter of Authorization (LOA).

Port short phone numbers

Due to Telecom regulations in various countries, the short phone number will need to be evaluated on a case-by-case basis. To verify if your phone number can be ported to Amazon Connect, submit an Amazon Connect support ticket (p. 162).

Port a number to one EU Region only

The Amazon Connect Regions of EU-CENTRAL-1 and EU-WEST-2 are symmetrical European regions that offer the same carrier coverage for telephony. If a phone number cannot be ported to an instance in one of these Regions, then it cannot be ported to an instance in the other.

If you had a phone number ported into the EU-CENTRAL-1 or EU-WEST-2 Regions, and want to move it to the other Region, submit an Amazon Connect support ticket (p. 162) for assistance.

The same is true for the North America Regions of US-EAST-1 and US-WEST-2.

Port a subset of numbers from a block

If you have a block of numbers, in some instances we can port a subset or portion of your phone numbers. In other cases, it is required by the carrier to port full block of phone numbers.

If you want to port only a subset of the phone numbers you currently own to Amazon Connect, submit an Amazon Connect support ticket (p. 162) to verify whether the phone numbers can be ported. We will verify the actions that can be completed and assist you with next steps.

Note

If you only port a subset of the phone numbers, you will still be liable for the remaining phone numbers with the original carrier and any associated fees.

If your intent to is release the remaining phone numbers not being ported to Amazon Connect, we recommend waiting until the requested porting has been completed to avoid any unwanted disruptions to service.

Letter of compromise

Before porting phone numbers, some customers ask for a letter of compromise stating that they will be allowed to move their phone numbers from Amazon Connect to another service if their contact center moves. Due to Telecom regulations in various countries, the phone number will need to be evaluated on a case-by-case basis. Please submit a ticket to Amazon Connect support (p. 162) to verify if your phone number can be ported to Amazon Connect.

How long does it take to port numbers?

Important

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

The amount of time that it takes to port numbers depends on the country, complexity of the request, the type and quantity of numbers being ported, and your current carrier. Telecom carriers also may implement porting block days because of holidays and network maintenance. Because of this, we require porting requests to be open several months before pending go-live dates.

Inside the US and Canada

Phone numbers in the US or Canada typically take between two to four weeks to port, after phone number portability has been verified, and all required documents are correctly submitted to the carrier.

Outside the US and Canada

Phone numbers outside the US and Canada require between two to six months to complete the full porting process. This includes:

- Time for you to submit all the documents to AWS Support.
- Time for the Amazon Connect service provider to verify whether they can port all of the phone numbers that you have requested.
- Time for the losing provider to verify the provided documents.

After all documents are verified by the losing provider, the losing provider and the Amazon Connect service provider will schedule a mutually agreed date to port the numbers to Amazon Connect.

What affects porting timelines?

Porting timelines can be negatively impacted when incorrect information is provided on the required Letter of Authorization (LOA). This causes the LOA to be rejected and resets the porting timelines.

Port many numbers over multiple countries or carriers

Complex porting requests have their own timelines. The timelines discussed elsewhere in this topic do not apply to complex porting requests.

Complex porting requests for more than 10 distinct number ranges or 10 distinct locations are considered a project and require advanced coordination with your AWS Account team. If you are a Business or Enterprise customer, engage your Amazon Connect Solutions Architect (SA) or Technical Account Manager (TAM) for assistance in planning your number porting.

To help make the process as smooth as possible, gather the following information before submitting a porting request:

- Your most recent telephony bill from the carriers that currently service the numbers to be ported.
- The country specific documentation required; see Region requirements for ordering and porting phone numbers (p. 171).
- The contact information for a central point of contact who can act on behalf of your organization in support of the porting requests.

Can I choose the port date?

Depending on the country and carriers involved, you may be able to choose the porting date and time. In most cases, however, the losing carrier picks the date and time and communicates it to Amazon Connect based on their schedule.

If you have a specific date and time you want to request, provide the information in your support case. We will work with our carrier to determine if they can support the requested date and time.

> **Note**
> Most carriers only support porting activity during their normal business hours. For detailed information about available porting dates and times for your country, see Region requirements for ordering and porting phone numbers (p. 171).

Can I cancel a porting that is already scheduled?

> **Important**
> If you need to cancel or reschedule your porting, let us know immediately.

Depending on the country of service, after a mutually agreed date and time has been provided it can be difficult to cancel.

Because of the coordination required between carriers, Amazon Connect support requires a minimum of 5 business days notice to cancel or reschedule a porting request. If you need to cancel or reschedule your porting, let us know immediately.

If a porting is successfully cancelled, timelines for the port schedule are reset and the carriers will need to identify another mutually agreed date and time. This will impact the overall timeline for porting your numbers.

> **Note**
> Please be advised that sometimes a porting request cannot be cancelled because of process automation, but Amazon Connect support will make every attempt possible to stop the request.

When do I cancel my current telecom service?

Do not cancel your existing telecom service until your phone numbers have been ported and confirmed working in Amazon Connect.

Canceling your existing telecom service before your number is ported releases your phone number assignment, and may result in you losing the number.

Porting your phone numbers

Porting phone numbers from your existing carrier to Amazon Connect is a multi-step process. It's important to get started several months in advance of your scheduled go-live date, and have all of your documentation in order.

Contents

How to port your numbers to Amazon Connect

The following steps are for a typical porting request. This process requires timely communication to make progress. If you take longer than 30 days to respond to requests for information, your porting request may be cancelled, rescheduled, or restarted from the beginning. For a list of country-specific requirements for porting numbers, see Region requirements for ordering and porting phone numbers (p. 171).

Step 1: Submit an Amazon Connect support ticket

Submit an Amazon Connect support ticket to verify if your phone number can be ported to Amazon Connect.

Premium support plan

1. Open AWS Support Center at https://console.aws.amazon.com/support/home and sign in using your AWS account.
2. Choose **Create case**.
3. Choose **Technical support**.
4. For **Case classification**, do the following:
   a. Choose service as **Connect (Contact center)**.
   b. Choose category as **Phone Number Porting**.
   c. Choose the required severity.
   d. For **Contact Center Instance ARN**, enter the instance ARN (also called the instance ID). For instructions on how to find your instance ARN, see Find your Amazon Connect instance ID/ARN (p. 139).
   e. Enter the subject.
   f. Under **Case description**, **Use case description**, include as much information as possible about your request, including phone number(s) to be ported, your current carrier, and the contact information for the person authorized to make changes to your current phone service. If you don't know all of these details, you can leave information out.
5. Expand **Contact options**, and then choose your **Preferred contact language** and **Contact methods**.
6. Choose **Submit**.
7. The Amazon Connect team will review your ticket and gets back to you.

Basic support plan

1. Open AWS Support Center at https://console.aws.amazon.com/support/home and sign in using your AWS account.
2. Choose **Create case**.
3. Choose **Service limit increase**.
4. For **Case details**, do the following:
   a. For **Limit type**, choose **Amazon Connect**.
   b. For **Contact Center Instance ARN - optional**, enter the instance ARN (also called the instance ID). For instructions on how to find your instance ARN, see Find your Amazon Connect instance ID/ARN (p. 139).
5. For **Requests**, **Request 1** do the following:
   a. For **Region**, select the Region in which you created your Amazon Connect instance.
   b. For **Limit**, choose **Phone Number Porting**.
   c. For **New limit value**, enter the number of phone numbers to port.

6. (Optional) To port additional phone numbers, choose **Add another request**, and then repeat step 6 for each additional request.
7. For **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**.
10. The Amazon Connect team will review your request and get back to you.

Step 2: Complete Letter of Authorization (LOA)

If the phone number qualifies for porting, the Amazon Connect team will provide you a Letter of Authorization (LOA) to be completed by you. Complete all mandatory fields and sign the LOA.

Along with the LOA, Telecom regulations in many countries require additional documents to register a number, such as proof of business, proof of address, and proof of ID. For a list of country-specific requirements for porting numbers, see Region requirements for ordering and porting phone numbers (p. 171).

How to complete an LOA

All portings require the completion of a Letter of Authorization (LOA). The LOA authorizes your current carrier to release your number and allow it to be ported.

- If you are porting multiple numbers from different carriers and countries, submit separate tickets for each set of phone numbers to be ported from different carriers and different countries to streamline communications, tracking, and the LOA process.
- A separate LOA is required for numbers from each losing carrier.

To complete an LOA, provide the following information:

- The numbers to port.
- Information about your current carrier, such as their business name and contact information.
- Contact information for the person authorized to make changes to your phone service. The name, address, and information you provide on the LOA must match the information on file with your current carrier exactly. To help ensure the porting process goes smoothly, include a copy of the Customer Service Record (CSR) or latest phone bill from your carrier. This will have your name, address, and related telephone numbers on it. Check that the information on your LOA matches your CSR **exactly**.
- If you have any questions regarding specific details about your current service, consult with your current carrier to ensure the data is accurate. This will minimize the risk that the LOA is rejected.

> **Important**
>
> Your LOA form must meet the following criteria:
>
> - It must be legible: clearly written or typed.
> - It must list your company name, the company address, and contact name. This information must match what is on the current carrier's CSR.
> - It must include a true signature. Most carriers will reject an electronic or printed signature.
> - It must be dated within the last 15 days.
> - It must include any toll-free numbers you want to port. Up to 10 toll-free numbers can be listed on the LOA. If you are requesting more than 10 phone numbers be ported, a

spreadsheet is required to be attached. Specify "See Attached" on the LOA where the phone numbers would be listed.

- It must include only those telephony numbers that belong to the same current carrier and in the same country. If you have multiple current carriers and countries, you will need to submit multiple LOAs.

To further minimize the risk of having your LOA rejected, see Common reasons why carriers reject an LOA (p. 165).

Step 3: The porting request goes to the Amazon Connect carrier

After you have submitted all required documentation, the Amazon Connect team submits the porting request on your behalf to the winning carrier.

- The losing and winning carrier follow an industry standard process to validate the contents of the LOA and submitted documentation.
- If the LOA contains discrepancies, it will be rejected and you will need to fix the discrepancies and submit a new LOA.
- After the carriers successfully validate the LOA, they will either confirm your requested date or provide an available date for the actual porting. This is known as the "mutually agreed date."

> **Note**
> Most carriers require that portings are completed during normal business hours. For country-specific business hours, see Region requirements for ordering and porting phone numbers (p. 171).

Step 4: Assign the phone number to the contact flow, request service quota increases

About 3-4 days before the mutually agreed date and time, the Amazon Connect support team loads the phone number that will be ported into the instance ARN you have provided, and then notifies you. Now it's time for you to perform the following steps:

1. Associate the phone number to the desired contact flow (p. 453) so the phone number will be ready to receive phone calls after the porting is completed. If you require assistance assigning multiple phone numbers to contact flows, let us know in your support request.

   > **Important**
   > If you do not assign the phone number to the contact flow, calls will not arrive successfully to your Amazon Connect contact center.

2. Submit a service quota request (p. 1205) at least five days in advance of the mutually agreed date for any changes to your service quotas required to support your use case. For example, you may need to increase the number of concurrent calls per instance, or enable countries for outbound calling.

Step 5: Checklist of activities on your porting date

The action of porting a number can be disruptive: the process involves updating the routing of phone numbers between carriers across a country or Region, including carriers not involved in the actual porting. In rare cases it can take several hours before all routes across all Telecom carriers are fully updated.

Steps you perform to minimize disruption to your phone services

On the mutually agreed port date, perform the following steps:

- Double-check that the activities listed in Step 4 (p. 164) have been completed:

    1. Verify that you have assigned the number being ported into your Amazon Connect instance to the appropriate contact flow.
    2. Verify that any required service quota increases or changes for your Amazon Connect instance were implemented. For example, increase the number of concurrent calls per instance, or enable countries for outbound calling.
- Monitor call traffic from your existing contact center to confirm that incoming traffic has stopped.
- Place test calls to your Amazon Connect instance to verify calls are being routed to the correct contact flows.
- Ensure agents are logged in to the Contact Control Panel (CCP) and can answer calls as they are received.
- Monitor call traffic to your Amazon Connect instance to confirm that you are receiving the expected levels of traffic.

Steps the Amazon Connect team performs to ensure a smooth transition

1. After the Amazon Connect team receives confirmation that the porting has been completed, we will perform final testing to confirm that the porting was successful and the phone number is receiving calls to Amazon Connect.
2. After we have completed our testing, we will notify you and ask you to verify the successful completion of the porting.

Documentation requirements for porting numbers

The Letter of Authorization (LOA) is an industry standard document type used by carriers to authorize the transfer of a phone number from one carrier to another. In many cases, the LOA is specific to the country or region, carrier, or porting relationship between the losing and winning carriers. If your number can be ported, Amazon Connect support will provide you with an LOA form appropriate for the situation.

For more information, see How to complete an LOA (p. 163).

Additionally, regulations in some countries require a local business address and specific documentation to use a phone number. For country specific requirements, see Region requirements for ordering and porting phone numbers (p. 171). If this is required, we will ask for this information to be submitted with the completed LOA.

Common reasons why carriers reject an LOA

There are four common reasons that an LOA may be initially rejected by the losing carrier:

- Unsatisfactory business relationship

  This usually means that you have an unpaid balance or the carrier charges a port away fee. After you pay the bill or fee to your carrier, we will resubmit the port request.
- Name or address mismatch

  The information you submitted on your Letter of Authorization (LOA) is different from what's on file with your carrier in their Customer Service Record (CSR). To fix this, contact your existing carrier to update your CSR information, obtain the correct CSR information, or both. Let us know when they update your information and we will resubmit the port request. Or, send us a new LOA with the correct information as provided by your existing carrier.
- Number cannot be ported

  We will work with all Amazon Connect carriers in a Region to support the porting of your numbers. In some cases, however, specific numbers may not be portable because of regulatory restrictions or carrier limitations. In these situations, consider claiming a new number from Amazon Connect.

- Missing information

  One or more fields have been left blank on the LOA. This may include a missing signature, phone number, address information, or other requested information. Review all LOAs before submitting them to ensure that you have filled out all requested data. After the LOA is updated with all the required information, we will resubmit the port request.

How to verify flows before numbers are ported

We recommend that you test your call flows before the mutually agreed date and time of porting. If you would like to test your call flows, we recommend that you claim a direct inward dial (DID) or toll-free phone number available within Amazon Connect and assign it to the call flow for testing.

When you are done testing, you can release the number from your instance so you will no longer be charged for it. For instructions, see Release a phone number (p. 170).

Until you release the number, you are charged the daily rate associated with claiming a phone number and the per minute rate for telephony minutes used. For more information see the standard pricing for Amazon Connect service usage and associated telephony rates.

After the porting process completes

After you have ported your numbers to Amazon Connect, use the topics in this section to troubleshoot issues, or to release numbers you no longer need after porting.

Contents

Not receiving calls on the ported number

After the scheduled porting window has completed, if you are not receiving phone calls on the ported phone number, update your support ticket. We will troubleshoot with our carrier to verify the porting status and identify the next steps to resolve issue.

Amazon Connect and our carriers make every effort to ensure number porting occurs with minimal downtime and without issues. In all cases, the losing carrier is responsible for initiating the number porting and releasing your number to the winning carrier.

In rare situations, a number routing issue can occur, resulting in calls not arriving to Amazon Connect from the carrier.

Release ported numbers that you no longer need

You do not have to keep phone numbers assigned to your Amazon Connect instance.

When a phone number is released from your Amazon Connect instance:

- You will no longer be charged for it.
- You cannot reclaim the phone number.
- Amazon Connect reserves the right to allow it to be claimed by another customer.

To release a phone number

1. Log in to your contact center at https://*instance name*.my.connect.aws/. To find the name of your instance, see Find your Amazon Connect instance ID/ARN (p. 139).
2. On the navigation menu, choose **Channels**, **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 have released, they will get a message that it is not a working phone number.

Revert to original carrier after porting

To complete the porting, the losing and gaining carriers both make configuration changes to pass the phone number ownership. After the porting is complete, the gaining carrier has sole control of the phone number.

To move the phone number again, you must complete a new LOA and any required documentation.

Port phone numbers away from Amazon Connect

If you want to port your numbers to a different carrier, open a support case to tell us. Then make arrangements with your new carrier. By letting us know, it will reduce the amount of back and forth between us and your new carrier, and it will help make the process go faster.

1. Create a case.
2. Choose **Service limit increase**.
3. In **Limit type** select **Amazon Connect**.
4. In **Use case description**, let us know that you're porting your number away, and the name of your new carrier.

Claim a phone number in your country

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

To claim a number for your contact center

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. On the navigation menu, choose **Channels**, **Phone numbers**.
3. Choose **Claim a number**. You can choose a toll free number or a Direct Inward Dialing (DID) number.

   Note

   Use the Amazon Connect service quotas increase form for these situations:

   - If you select a country or region, but no numbers display, you can request additional numbers for the country or region.
   - If you want to request a specific area code or prefix that you don't see listed, we'll try to accommodate your request.
4. Enter a description for the number and, if required, attach it to a contact flow in **Contact flow / IVR**.
5. Choose **Save**.
6. Repeat this process until you have claimed all your required phone numbers.

There is a service quota for how many phone numbers you can have in each instance. For the default service quota, see Amazon Connect service quotas (p. 1205). If you reach your quota, but want a different phone number, you can release one of previously claimed numbers. You cannot claim the same phone number after releasing it.

If you need more phone numbers, you can request a service quota increase using the Amazon Connect service quota increase form.

"You've reached the limit of Phone Numbers. To increase the limit, contact support."

Even if it's the first time you've claimed a phone number, it's possible to get this error message when you attempt to claim a number. All the issues that cause this error message require help from AWS Support to resolve.

Contact AWS Support and they will provide assistance.

Claim a phone number you already own in another country

Let's say your business is located in Germany. You also have agents in Japan to serve customers who live there, and you need a Japanese phone number for that contact center. To claim a phone number that you already own in another country, use the following steps to create a support case.

To claim a number that you don’t already own in another country or region, see Request numbers, international numbers, or termination points (p. 169).

1. Go to Create case.
2. Choose **Service limit increase**.
3. In **Limit type** select **Amazon Connect**.
4. In **Use case description**, provide the address of your business that's located in the other country.
5. In **Contact options**, choose whether we should contact you by email or phone.
6. Choose **Submit**.

We'll contact you to help with your request.

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

To claim a phone number for an Amazon Connect instance you create in the Asia Pacific (Tokyo) Region, open an AWS support case and provide documentation that your business is located in Japan.

> **Important**
> You must provide three pieces of required documentation. For a list of acceptable identification, see Japan (JP) (p. 188), in the Region requirements for ordering and porting phone numbers (p. 171) topic.

Numbers can be claimed for business use only, not for personal use.

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

- **Direct Inward Dialing (DID) numbers**—DID numbers are also referred to as local numbers.

- 050 prefix numbers.
- 03 prefix for numbers in Tokyo. Amazon Connect does not offer phone numbers for other cities in Japan at this time.
- **Toll Free numbers**
  - 0120 prefix numbers.
  - 0800 prefix numbers.

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

Request numbers, international numbers, or termination points

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

- A local office address.
- Specific identification documents.

For identification requirements by country, see Region requirements for ordering and porting phone numbers (p. 171).
In most countries it takes 2-6 weeks for us to fulfill your request. In some cases it can take up to 60 days. If you need a number by a certain date, let us know in your AWS Support case.

Note
Amazon does not provide premium rate or higher cost services. If you want these services we recommend you contract with specialist providers to route calls into Amazon Connect DID's following local country regulations.

To request international phone numbers that require documentation, or numbers not available within a specific region, create an AWS Support case. In the support case, you must specify exactly how many numbers you want for each country.

Submit an Amazon Connect support ticket to verify if your phone number can be ported to Amazon Connect.

Premium support plan

1. Open AWS Support Center at https://console.aws.amazon.com/support/home and sign in using your AWS account.
2. Choose **Create case**.
3. Choose **Technical support**.
4. In **Case details**, do the following:

   a. Choose service as **Connect (Contact Center)**.

   b. Choose category as **Phone Number Requests**.

   c. Choose the required severity.

   d. For **Contact Center Instance ARN**, enter the instance ARN (also called the instance ID). For instructions on how to find your instance ARN, see Find your Amazon Connect instance ID/ARN (p. 139).

   e. Enter the subject.

   f. Under **Case description**, **Use case description**, include as much information as possible about your request. If you don't know all of these details, you can leave information out.

5. Expand **Contact options**, and then choose your **Preferred contact language** and **Contact methods**.
6. Choose **Submit**.
7. The Amazon Connect team will review your ticket and gets back to you.

We'll contact you to help with your request.

After your request is approved, the exact number of requested phone numbers appear in your Amazon Connect console for you to claim. You won't have access to all available numbers in that country.

Basic support plan

1. Open AWS Support Center at https://console.aws.amazon.com/support/home and sign in using your AWS account.
2. Choose **Create case**.
3. Choose **Service limit increase**.
4. For **Case details**, **Limit type**, choose **Amazon Connect**.
5. For **Case description**, **Use case description**, enter the number that you want to request or exactly how many numbers you want for each country. If you need the number by a certain date, include that, too.
6. Expand **Contact options**, and then choose your **Preferred contact language** and **Contact methods**.
7. Choose **Submit**.
8. The Amazon Connect team will review your request and get back to you.

We'll contact you to help with your request.

After your request is approved, the exact number of requested phone numbers appear in your Amazon Connect console for you to claim. You won't have access to all available numbers in that country.

Requirements for Custom Termination Points

In the Asia Pacific (Sydney) Region, you can request Custom Termination Points.

The term "Custom Termination Points" means custom Tier 1 telephony destinations for customer calls to Amazon Connect configured as local phone numbers. In using Custom Termination Points, you understand and agree that you:

1. Have a current toll-free national service that allows you to set Custom Termination Points as a destination for customer phone calls.
2. Cannot port or move Custom Termination Points to a different telephony provider once assigned by Amazon Connect.
3. Will be billed at the standard daily rate for claimed Australian phone numbers and DID inbound usage fees.
4. You are responsible for adding the Custom Termination Points in your existing toll-free national service.

Release a phone number

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

When a phone number is released from your Amazon Connect instance:

- You will no longer be charged for it.
- You cannot reclaim the phone number.
- Amazon Connect reserves the right to allow it to be claimed by another customer.

> **Tip**
> If you want to "close" your Amazon Connect account, do these steps for all of your phone numbers. This will ensure you aren't billed if people erroneously call numbers that you've claimed, and initiate your contact flows. You may also want to delete your instances. (p. 147)

To release a phone number

1. Log in to your contact center at https://*instance name*.my.connect.aws/. To find the name of your instance, see Find your Amazon Connect instance ID/ARN (p. 139).
2. On the navigation menu, choose **Channels**, **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 have released, they will get a message that it is not a working phone number.

Telecoms regulations

Contents

Region requirements for ordering and porting phone numbers

Country or region regulations often require a local office address and specific identification documents to purchase and own a phone number. The address that you provide can be the business or personal address where the phone numbers are used.

For a list of the telephony capabilities that Amazon Connect provides, see the Amazon Connect Telecoms Country Coverage Guide.

Following is a list of ID Requirements by country or region. When you request an international number (p. 169), we'll work with you to submit your documents.

> **Note**
> After your numbers are ordered or ported, the exact number of requested phone numbers appear in your Amazon Connect console for you to claim. You won't have access to all available numbers in that country.

Argentina (AR)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	No	
	Toll-free prefixes: +54 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Australia (AU)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Sydney) Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Tokyo)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone. Do not use a PO Box.
	Toll-free prefixes: +61 1300, +61 1800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
Asia Pacific (Sydney) Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Tokyo)	8AM -12 PM AEST Monday-Friday	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Austria (AT)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	Yes	Proof of telecom services at your address, which must match the city code requested.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Canada (Central) EU (Frankfurt) EU (London)			Your business name, address, and registration number, and a copy of the ID or passport of an authorized representative.
	Toll-free prefixes: +43 800	Yes	Your business name, address, a copy of the business registration (global), and a copy of the passport of an authorized representative. A global address is acceptable.
	National prefixes: +43 720	Yes	Your business name, address, a copy of the business registration (global), and a copy of the passport of an authorized representative. A global address is acceptable.

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Belgium (BE)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone.
	Mobile prefixes: +32 46	Yes	

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Toll-free prefixes: +32 800	No	
	National prefixes: +32 78	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Mandatory to provide service address for the numbers 4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Bulgaria (BG)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your residence or business address. Both must be in the relevant geographic zone.
	Toll-free prefixes: +359 800	Yes	Your name and address.

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers Bulgarian Registration Number is mandatory for customers based in Bulgaria

Canada (CA)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London) AWS GovCloud (US-West)	Local telephone numbers:	No	
	Toll-free prefixes:	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West Canada (Central) EU (Frankfurt) EU (London) AWS GovCloud (US-West)	7 AM to 5 PM CST	1. Last invoice 2. Letter of Authorization (LOA)

Cayman Islands (KY)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	No	
	Toll-free prefixes:	Yes	Businesses must provide a copy of business registration containing a proof of address.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
			Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year). The business address must be outside of Cayman Islands.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Chile (CL)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	No	
	Toll-free prefixes:	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Costa Rica (CR)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	Yes	Businesses must provide a copy of business registration containing a proof of address as well

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
			as an ID of an authorised respresentative. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year); the proof of ID is a copy of the national identity ID or passport of an authorized representative. The business address must be outside of Costa Rica.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Croatia (HR)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your residence or business address. Both must be in the relevant geographic zone.
	Mobile prefixes: + 385 95	Yes	Your business name, address, and business registration or VAT number.
	Toll-free prefixes: + 385 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt)	10 AM to 12 PM CET	1. Last invoice

Supported Regions	Porting Windows	Required Documents
EU (London)		2. Letter of Authorization (LOA) 3. Copy of Court Registration 4. Copy of legal representative's photo ID 5. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Cyprus (CY)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	No	
	Toll-free prefixes: + 357 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Copy of **Certificate of Directors and Secretary of the Company** 4. Copy of **Certificate of Incorporation** 5. Copy of legal representative's photo ID

Czech Republic (CZ)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central)	Local telephone numbers:	Yes	Your residence or business address. Both must be in the relevant geographic zone.
	Mobile prefixes: +420 73	Yes	Your business name, address, and business registration or VAT number,

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)			and a copy of the ID or passport of an authorized representative.
	Toll-free prefixes: +420 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	3 PM to 4 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required per Type of Number as listed in the previous table for ordering numbers

Denmark (DK)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your name, address, and business registration or VAT number.
	Mobile prefixes: +45 9x	No	
	Toll-free prefixes: +45 808	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required per Type of Number as listed in the previous table for ordering numbers

El Salvador (SV)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Toll-free prefixes:	Yes	Businesses must provide a copy of business registration containing a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year). The business address must be outside of El Salvador.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Estonia (EE)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Toll-free prefixes: +372 800	No	
	National prefixes: +372	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA)

Supported Regions	Porting Windows	Required Documents
		3. LOA template has to include a local address. 4. If this is a company, a business number is required.

Finland (FI)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your residence or business address. Both must be in the relevant geographic zone.
	Toll-free prefixes: +358 800	No	
	National prefixes: +358 75	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

France (FR)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone as the number. You must provide proof of the address along

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Canada (Central) EU (Frankfurt) EU (London)			with a copy of the business registration.
	Toll-free prefixes: +33 805	No	
	National prefixes: +339	Yes	An address in France is required.

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required per Type of Number as listed in the previous table for ordering numbers 4. It is mandatory to provide RIO code from the losing carrier, or at least the SIRET (if you're a business customers only). You can obtain the SIRET by contacting your existing telecom carrier.

Georgia (GE)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	National prefixes: +995 70	No	
	Local telephone numbers: (Tibilisi)	Yes	Your business address. It must be in the relevant geographic zone as the number.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Germany (DE)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Local address in Germany is required. The address dictates where the geographic number must be sited. Businesses must provide a copy of the business registration document as proof of address.
	Toll-free prefixes: +49 800	Yes	Your residence or business address outside of Germany. You must provide proof of the address. For numbers to be answered inside of Germany, a special process applies. You must obtain the number directly from the local regulator and then port it to Amazon Connect. Details about the process are provided when you make the request.
	National prefixes: +49 32	Yes	Address in Germany is required. Businesses must provide a copy of the business registration document as proof of address.

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. For business ports, end user stamp is mandatory on the LOA. 4. If the number to be ported is an extended line, the main line must be ported.

Supported Regions	Porting Windows	Required Documents
		5. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Greece (GR)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone.
	Toll-free prefixes: +30 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Company registration certificate 4. Copy of LOA signatory's photo ID/ Passport 5. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Hong Kong (HK)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul) Asia Pacific (Singapore)	Local telephone numbers:	Yes	Your address and proof of address. A global address is acceptable.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Sydney) Asia Pacific (Tokyo)	National prefixes: +852 58	Yes	Your address and proof of address. A global address is acceptable.
	Toll-free prefixes: +852 800	Yes	Your business address. A global address is acceptable.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not support	N/A	N/A

Hungary (HU)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone. You must provide proof of the address along with a copy of the business registration. A copy of the ID or passport of an authorized representative.
	Toll-free prefixes: +36 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Indonesia (ID)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	Local telephone numbers:	No	
	Mobile prefixes: +62 855	Yes	Proof of business address, a copy of the ID or passport of an authorized representative, and the business registration. You must also provide a description of how you plan to use the numbers.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Ireland (IE)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone.
	Toll-free prefixes: +353 1800	No	
	National prefixes: +353 76	No	No longer Available - Nomadic numbers (076) are being phased out by the end of 2021.

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East	10 AM to 12 PM CET	1. Last invoice

Supported Regions	Porting Windows	Required Documents
US West EU (Frankfurt) EU (London)		2. Letter of Authorization (LOA) 3. It is mandatory to provide the main telephone number on the account. 4. It is mandatory to provide a Wholesale Account number. 5. Type of the line mandatory on the LOA. 6. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Italy (IT)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business name, address, and VAT number. You must provide proof of the address along with a copy of the business registration. You must provide the following details of an authorized representative: name and address, birth location and data, and nationality and tax code. Also provide proof of the authorized representative's identity, which can be a copy of an ID or passport. Any Italian address is acceptable.
	Toll-free prefixes: +39 800	Yes	Your business name, address, and VAT number. You must provide the following details of an authorized representative: name and address, birth location and data, and nationality and tax code. Also provide proof of the authorized representative's identity, which can be a copy of an ID or passport.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
			A global address is acceptable.

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Migration code of the requested number is mandatory. Obtain this code from the losing carrier. 4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Japan (JP)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	Local telephone numbers:	Yes	Businesses must provide 3 pieces of documentation: • **Company registration documents**. These documents must show: ◦ The business address is in the city corresponding to the requested area code of the number. ◦ The authorized representative of the business. • **A copy of the personal ID or passport of the business's authorized representative**. The person must be registered on the Company Registration Documents. Valid personal ID can be government-issued IDs, passports, drivers license.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
			- **Proof of address for the business**. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 3 months); government documents (issued in the previous year); or IDs listing the submitted address, such as government-issued IDs, passports, drivers licenses, and business registration. Copies of these documents should be made into a single ZIP file.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
	Toll-free prefixes: +81 120, +81 800	Yes	Businesses must provide the following documentation: • **A copy of the personal ID or passport of the business's authorized representative**. The person must be registered on the Company Registration Documents. Valid personal ID can be government-issued IDs, passports, drivers license. • **Proof of address for the business**. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 3 months); government documents (issued in the previous year); or IDs listing the submitted address, such as government-issued IDs, passports, drivers licenses, and business registration. A global address is acceptable. Copies of these documents should be made into a single ZIP file.

For porting numbers

Note

Local telephone numbers cannot be ported. Only toll-free numbers can be ported.

Supported Regions	Porting Windows	Required Documents
Asia Pacific (Tokyo)	Toll-free prefixes: +81 120, +81 800	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required per Type of Number as listed in the previous table for ordering numbers

Latvia (LV)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Mobile prefixes: +371 28	Yes	Businesses must provide proof of address within Latvia. Valid forms of proof: • Business Registration • Third-party issued bank statement or public utility bill showing regular use • Lease Agreement
	Toll-free prefixes: +371 80	Yes	Businesses must provide proof of address within Latvia. Valid forms of proof: • Business Registration • Third-party issued bank statement or public utility bill showing regular use • Lease Agreement
	National prefixes: +371 6	Yes	Businesses must provide proof of address within Latvia. Valid forms of proof: • Business Registration • Third-party issued bank statement or public utility bill showing regular use • Lease Agreement

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA)

Supported Regions	Porting Windows	Required Documents
		3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Lithuania (LT)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	No	
	Mobile prefixes: +370 66	Yes	Your business name, address, and registration number. A global address is acceptable.
	Toll-free prefixes: +370 800	Yes	Proof of business address in the country is required.

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. VAT number and local address is needed on the LOA. 4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Luxembourg (LU)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers: +352 27	Yes	Your residence or business address. It must be in the relevant geographic zone.
	National prefixes:	No	
	Toll-free prefixes: +352 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. You must provide the account number from the Main Losing Carrier to which the requested DID is assigned. 4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Malaysia (MY)

For ordering phone numbers

Inside Malaysia

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	Local telephone numbers (Inbound and Outbound required post 9th July 2021)	Yes	Business Registration Documentation, Letter of Authority naming an authorised business user. Government issued ID such as passport.
	Local telephone numbers (existing Inbound only pre 9th July 2021)	Yes	Business Registration Documentation, Letter of Authority naming an authorised business user. Government issued ID such as passport.
	Toll-free prefixes: +60 1800	Yes	Business Registration Documentation, Letter of Authority naming an authorised business user. Government issued ID such as passport.

Outside Malaysia

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul)	Local telephone numbers (Inbound required post 9th July 2021)	Yes	Non Malaysia Business Registration Documentation

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	Toll-free prefixes: +60 1800	Yes	Non Malaysia Business Registration Documentation

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Malta (MT)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	National prefixes: +356	Yes	Your business name, address, a copy of the business registration (global), and a copy of the ID or passport of an authorized representative. A global address is acceptable.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Mexico (MX)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East	Local telephone numbers:	No	

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US West	Toll-free prefixes: +52 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West	10 AM to 12 PM CET or 2 PM to 4 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Copy of LOA signatory´s photo ID 4. Copy of power of attorney

New Zealand (NZ)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	Local telephone numbers:	No	
	Toll-free prefixes: +64 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	7 AM to 11AM NZST	1. Last invoice 2. Letter of Authorization (LOA) 3. Wholesale account number of the phone number from the current carrier.

Netherlands (NL)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone.
	Mobile prefixes: +31 97	Yes	A global business address. No voice services are supported, only AWS Server Migration Service (AWS SMS).
	Toll-free prefixes: +31 800	Yes	File orders in writing. Use the form that is provided to you when you make the request. Provide the following information: • Your name and address. • A description of the service for which the number will be used. Estimated lead time from order to activation is 6 weeks.
	National prefixes: +31 85	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Nigeria (NG)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Africa (Cape Town)	Local telephone numbers:	Yes	Businesses must provide a copy of business registration containing a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year). The business address must be inside Nigeria.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Norway (NO)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address in Norway, street code, municipality code, and company organization number. Proof of Norwegian business registration.
	Mobile prefixes: +47 59	Yes	Your business name, address, and registration number, and a copy of the ID or passport of an authorized representative.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
			A global address is acceptable.
	Toll-free prefixes: +47 800	Yes	Your business address in Norway, street code, municipality code, and company organization number. Proof of Norwegian business registration.
	National prefixes: +47 81	Yes	Your business address in Norway, street code, municipality code, and company organization number. Proof of Norwegian business registration.

Numbers are available to businesses only, not individuals. The DID type is Landline, instead of Geographic. This is because all formerly geographic numbers are now classified as landline, and do not have a geographic zone.

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Panama (PA)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Toll-free prefixes: +507 800	Yes	Your business address. You can have a maximum of 5 Panama toll-free numbers per business name.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Peru (PE)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	No	
	Toll-free prefixes: +51 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Poland (PL)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address and a copy of a business registration. A global address is acceptable.
	Mobile prefixes: +48 73	Yes	Your business name, address and registration number, and a copy of the ID or passport of an authorized representative. A global address is acceptable.
	Toll-free prefixes: +48 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Portugal (PT)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone. You must also submit the required proof of Telecom services being provided to the address.
	Toll-free prefixes: +35 1800	No	
	National prefixes: +351 30	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Copy of legal representative's photo ID 4. Documents required per Type of Number as listed in the previous table for ordering numbers

Puerto Rico (PR)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central)	Local telephone numbers: +1 787, +1 939	No	
	Toll-free prefixes: +1 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West	10 AM to 12 PM PST	1. Last invoice 2. Letter of Authorization (LOA)

Romania (RO)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your address and proof of address. It must be in the relevant geographic zone.
	Toll-free prefixes: +40 800	No	
	National prefixes: +40 376	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM PST	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Serbia (RS)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Businesses must provide a copy of business registration containing a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year). The business address must be outside Serbia.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Singapore (SG)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	Mobile prefixes: +65 8	Yes	Proof of the business address and proof of ID. A global address is acceptable.
	National prefixes: +65 31 and +65 6	Yes	Address required in country. Documents required for company: Company registration documents
	Toll-free prefixes: +65 800	Yes	Your business address. A global address is acceptable.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Asia Pacific (Singapore)	NA	1. Last invoice 2. Letter of Authorization (LOA) 3. List of Port in Numbers

Slovakia (SK)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone.
	Toll-free prefixes: +421 800	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Slovenia (SI)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone.
	Toll-free prefixes: +386 80	No	

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
	National prefixes: +386 82	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

South Africa (ZA)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Africa (Cape Town)	Local numbers:	Yes	Your business address in South Africa along with your Tax ID.
	Mobile numbers:	Yes	Your business address in South Africa and proof of address such as one of the following documents: • Excerpt from the commercial register showing the South Africa address • Utility bill • Tax notice • Rent receipt • Title deed

South Korea (KR)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Seoul)	Local telephone numbers: +82 2	Yes	Your business address in Seoul.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
			Local customers should provide a copy of their **business (tax office) registration certificate**, which is issued by local tax authorities and shows the company's registered address.
	Toll-free prefixes: +82 308	Yes	Your business address in South Korea.
	National prefixes: +82 70	Yes	Your business address in South Korea.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Spain (ES)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone as the phone number. A copy of the ID/business registration.
	Toll-free prefixes: +34 900	No	
	National prefixes: +34 518, +34 902	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. CIF/NIF (VAT number)

Supported Regions	Porting Windows	Required Documents
EU (London)		4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Sweden (SE)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	Yes	Your business address in Sweden.
	Mobile prefixes: +46 766	No	
	Toll-free prefixes: +46 20	No	
	National prefixes: +46 77 and +46 10	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Your tax number has to be provided. A Swedish organization number usually contains 12 digits, starting with **16** if it is from a company, or **19** or **20** if it's personal. 4. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers

Switzerland (CH)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West	Local telephone numbers:	Yes	Your business address. It must be in the relevant geographic zone.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Canada (Central) EU (Frankfurt) EU (London)			A proof of business registration.
	Toll-free prefixes: +41 800	Yes	Your business address and a copy of business registration. A global address is acceptable.

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA) 3. Documents required for the Type of Number, as listed in the previous table for ordering phone numbers 4. Proof of address 5. Company registration

Thailand (TH)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification	Restrictions
Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo)	Local telephone numbers:	Yes	**For business address inside Thailand**: Business must provide a copy of the ID of a company authorized representative and company certificate. **For business address outside of Thailand**: Proof of business address and proof of ID, such as the business registration. Also, a copy of the ID or passport of an authorized representative.	International caller ID is not guaranteed.

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification	Restrictions
	Toll-free prefixes: +66 1800	Yes	Proof of business address and proof of ID, such as the business registration. Also, a copy of the ID or passport of an authorized representative. The address cannot be in Thailand.	

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Uganda (UG)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Africa (Cape Town)	Local telephone numbers:	Yes	Businesses must provide a copy of business registration containing a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year). The business address must be inside of Uganda.

United Kingdom (UK)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo) Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	No	
	Mobile prefixes: +44	No	
	Toll-free prefixes: +44 800, +44 808	No	
	National prefixes:	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo) EU (Frankfurt) EU (London)	10 AM to 12 PM CET	1. Last invoice 2. Letter of Authorization (LOA)

United States (US)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
US East US West Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo) Canada (Central) EU (Frankfurt) EU (London)	Local telephone numbers:	No	
	Toll-free prefixes:	No	

For porting numbers

Supported Regions	Porting Windows	Required Documents
US East US West Asia Pacific (Seoul) Asia Pacific (Singapore) Asia Pacific (Sydney) Asia Pacific (Tokyo) EU (Frankfurt) EU (London)	7 AM to 5 PM CST	1. Last invoice 2. Letter of Authorization (LOA)

Vietnam (VN)

For ordering phone numbers

Supported Regions	Type of Number	Are there ID requirements?	Acceptable Identification
Asia Pacific (Sydney) Asia Pacific (Singapore) Asia Pacific (Tokyo)	Local telephone numbers:	No	
	Toll-free prefixes:	yes	Businesses must provide a copy of business registration containing a proof of address. Valid proofs of address include: third-party issued bank statements, utility bills (all issued in the previous 6 months); government documents (issued in the previous year). The business address must be outside Vietnam.

Coverage Limitations

- Local : All major networks except minority three networks FPT, CMC and Gtel.
- TFN : National reachability only from: VNPT fixed network, Vinaphone Mobile, and SPT network.

For porting numbers

Supported Regions	Porting Windows	Required Documents
Not supported	N/A	N/A

Set up outbound communications

You can send outbound communications to customers for a variety of reasons, such as appointment reminders, subscription renewals, and debt collection. Amazon Connect provides both normal and high-volume outbound campaign capabilities.

Contents

Set up outbound caller ID

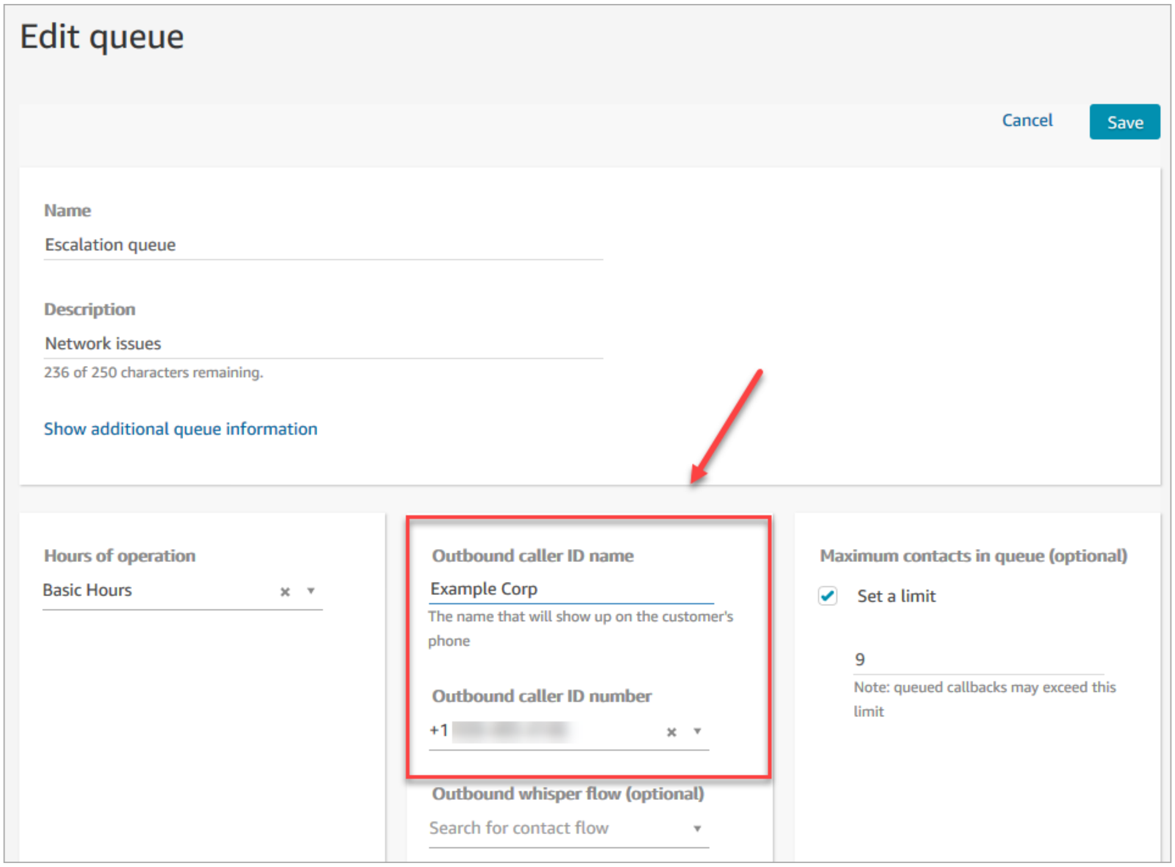
We recommend setting your outbound caller ID. Not doing so may result in some PSTN carriers considering your outbound calls fraudulent activity, and they may drop them.

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

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

Caller ID name: Set in queue

You set the caller ID name, such as the name of your company, in the queue settings. To edit queue settings, on the navigation menu choose **Routing**, **Queues**, and then choose the queue you want to edit.



Name
Escalation queue

Description
Network issues
236 of 250 characters remaining.

Hours of operation
Basic Hours

Outbound caller ID name
Example Corp
The name that will show up on the customer's phone

Outbound caller ID number
+1 [redacted]

Outbound whisper flow (optional)
Search for contact flow

Maximum contacts in queue (optional)
☑ Set a limit
9
Note: queued callbacks may exceed this limit

If your DID/TFN phone number is in the US/CANADA: The name you use should be the same one that's registered in the CNAM (Caller Name) database provided by Amazon Connect; this is a nationwide resource available in the US/CANADA to provide the name of the calling party on incoming calls if recipients subscribe to CNAM services from their telecom carrier.

Open an AWS Support ticket to register your US based phone number with your company name in the CNAM database of the Amazon Connect carrier. We'll handle the registration process for you. **It may take up to 30 days for the caller ID names to propagate through the database.**

If you are using CNAM phoning into CANADA, the end network may support Caller ID lookups, but this functionality is not guaranteed, as not all receiving networks support this feature. We are currently unable to provide support for lookups in other locales.

> **Important**
> CNAM is not supported for custom caller IDs, third-party numbers, or with the use of whisper flow transfers.

> **Tip**
> If you want each agent to have their own caller ID name while dialing out (such as *Example Corp Billing Dept*), create a queue for each agent/caller ID name.

Caller ID number: Set in the queue or Call phone number block

Only phone numbers that you've claimed (p. 167) or ported to Amazon Connect (p. 157) can be used as your caller ID number.

To use an external phone number as your outbound caller ID number, contact AWS Support to see if it's possible. You'll need to provide proof of ownership (p. 171).

You can set the caller ID number as follows:

- **Call phone number (p. 322) block**: Use this block in an outbound whisper flow to initiate an outbound call to a customer and, optionally, specify a custom caller ID number that is displayed to call recipients.

  This block is useful when you have multiple telephone numbers used to make outbound calls, but want to consistently display the same company phone number for the caller ID for calls made from your contact center.

  You can also use this block with the Set contact attributes (p. 399) block to set the callback number dynamically. For example, you can display a certain caller ID number based on the customer's account type.
- **Queue:** If no caller ID number is specified in the Call phone number (p. 322) block, then the caller ID in the queue settings is used.

> **Important**
> **In Australia**: The caller ID must be an Amazon Connect provided DID (Direct Inward Dialing) phone number. If a toll free number or a number not provided by Amazon Connect is used in the caller ID, local telephony suppliers may reject outbound calls due to local anti-fraud requirements.

Setting the caller ID dynamically

Use an attribute in the Call phone number (p. 322) block to set the caller ID number dynamically during the contact flow.

The attribute can be one you define in the Set contact attributes (p. 399) 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 setting the caller ID dynamically, see this AWS Support Knowledge Center article: How can I set my Amazon Connect outbound caller ID dynamically based on country?

Use E.164 format for international phone numbers

Amazon Connect requires phone numbers in E.164 format.

To express a US phone number in E.164 format, add the '+' prefix and the country code in front of the number. For example, for a US number:

- +1-800-555-1212

In the UK and many other countries internationally, local dialing requires the addition of a 0 in front of the subscriber number. However, to use E.164 formatting, this 0 must be removed. A number such as 020 718 xxxxx in the UK would be formatted as +44 20 718 xxxxx.

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

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

How to specify a custom caller ID number using a Call phone number (p. 322) block

1. On the navigation menu, 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 (p. 322) block to the flow, and connect the **Entry point** block to it.

   The Call phone number (p. 322) block must be placed before a **Play prompt** block if one is included in your contact flow.
4. Select the Call phone number (p. 322) 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 (p. 399) 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 (p. 322) block to the next block in the flow.

   There is no error branch for the block. If a call is not successfully initiated, the contact flow ends and the agent is placed in an **AfterContactWork** (ACW) state.

Why your caller ID might not appear correctly to customers

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

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

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

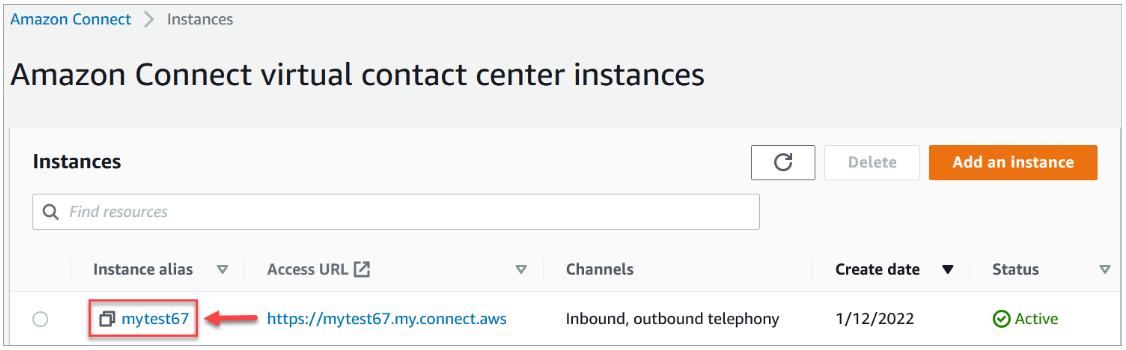
To enroll your numbers with this CNAM services provider, open an AWS Support ticket. Our support team will gather the required information to enroll your numbers. For instructions on how to access AWS Support, see Get administrative support for Amazon Connect (p. 1257).

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

Enable outbound calls

Before your agents can make outbound calls to customers, you need to set up your Amazon Connect instance for outbound communications.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.


Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	✓ Active

3. In the navigation pane, choose **Telephony**.
4. To enable outbound calling from your contact center, choose **Make outbound calls with Amazon Connect**.
5. To enable high-volume outbound communications, choose **Enable high-volume outbound communications**.
6. By enabling early media audio, your agents can hear pre-connection audio such as busy signals, failure-to-connect errors, or other informational messages from telephony providers, when making outbound calls. Choose **Enable early media**.
7. Choose **Save**.

> **Note**
> For a list of countries you can call **by default** based on the Region of your instance, see Countries you can call (p. 1214).
> For a list of all countries available for outbound calls based on the Region of your instance, see Amazon Connect pricing. If a country is not available in your dropdown menu, open a ticket to add it to your allow list.

Enable high-volume outbound communications

Before you begin

There are a few things that you need in place before using high-volume outbound communications:

- Make sure your instance is enabled for outbound calling (p. 215).
- Create a dedicated outbound communications queue to handle any contacts that will be routed to agents as a result of the campaign.
- Assign the queue to the agent's routing profile.
- Create and publish a contact flow that includes a Check call progress (p. 327) block. This block enables you to branch based on whether a person answered the phone, for example, or a voicemail was detected.

> **Note**
> If you plan to call customers in Australia or New Zealand, see *Step 4: Create a new campaign in the Amazon Connect instance* in this blog for instructions: Make predictive and progressive calls using Amazon Connect high-volume outbound communications.

Create a AWS KMS key

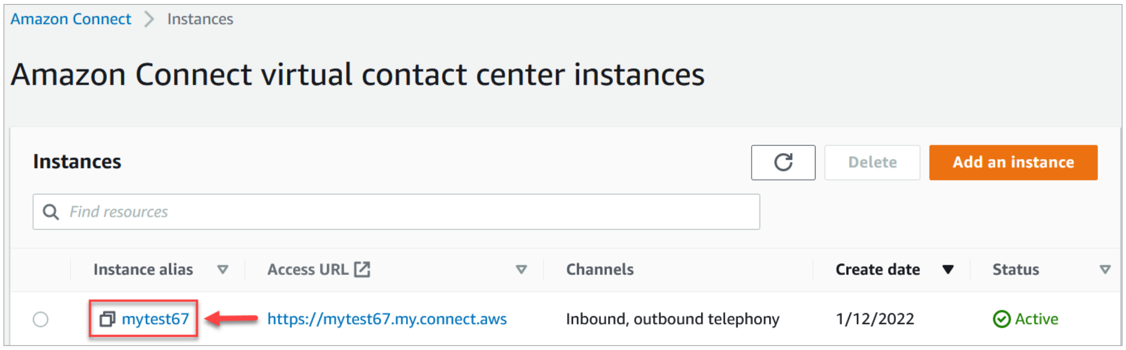
When you enable high-volume outbound communications, you have the option to provide your own AWS KMS key. These keys are created and managed by you (AWS KMS charges apply). You also have the option to use an AWS owned key.

When enabling or disabling high-volume outbound communications using an API, make sure the API user is either the administrator or has the following permissions: `kms:DescribeKey`, `kms:CreateGrant`, and `kms:RetireGrant` for the key.

> **Note**
> To switch the KMS key that is associated with high-volume outbound communications, first you need to disable high-volume outbound communications, and then re-enable it using a different AWS KMS key.

Configure high-volume outbound communications

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.


Amazon Connect > Instances

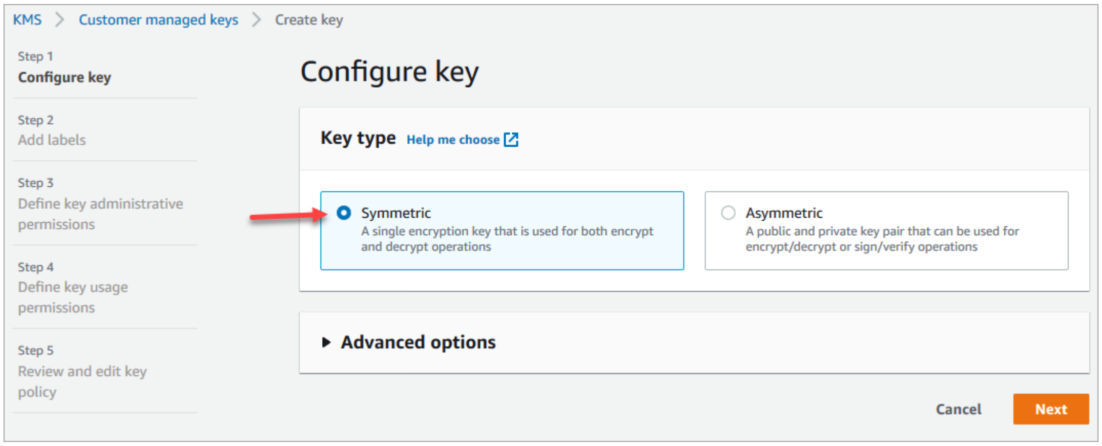
Amazon Connect virtual contact center instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Telephony**.
4. To enable high-volume outbound communications, choose **Enable high-volume outbound communications**.
5. Under **Encryption settings**, enter your own AWS KMS key or choose **Create an AWS KMS key**.

   If you choose **Create an AWS KMS key**:

   - A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review and edit key policy

Configure key

Key type Help me choose

● Symmetric
A single encryption key that is used for both encrypt and decrypt operations

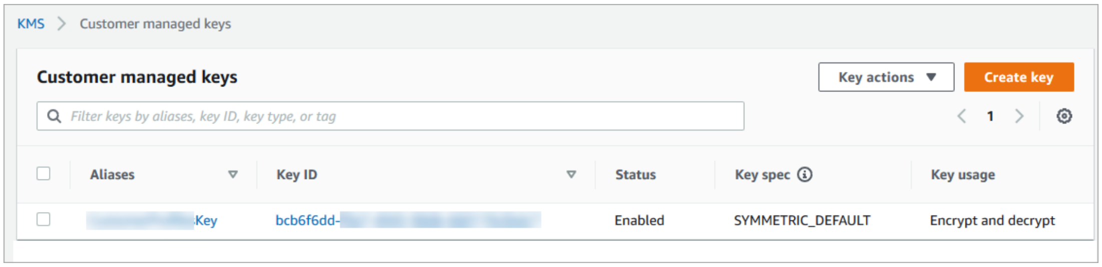
○ Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

▶ Advanced options

Cancel Next

- On the **Add labels** page, add a name and description for the key, and then choose **Next**.
- On the **Define key administrative permissions** page, choose **Next**.
- On the **Define key usage permissions** page, choose **Next**.
- On the **Review and edit key policy** page, choose **Finish**.

  In the following example, the name of the key starts with **bcb6fdd**:



KMS > Customer managed keys

Customer managed keys

Key actions ▼ Create key

Filter keys by aliases, key ID, key type, or tag

□	Aliases	Key ID	Status	Key spec	Key usage
□	[redacted]Key	bcb6f6dd-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

- Return to the tab in your browser for the Amazon Connect console, **Telephony** page. Click or tap in the **AWS KMS key** for the key you created to appear in a dropdown list. Choose the key you created.

6. Choose **Save**.
7. It takes a few minutes for high-volume outbound communications to be enabled. When it's successfully enabled, you can create outbound campaigns in Amazon Connect for voice calls. If it does not enable, verify you have the required IAM permissions (p. 1082).

Create a high-volume outbound campaign

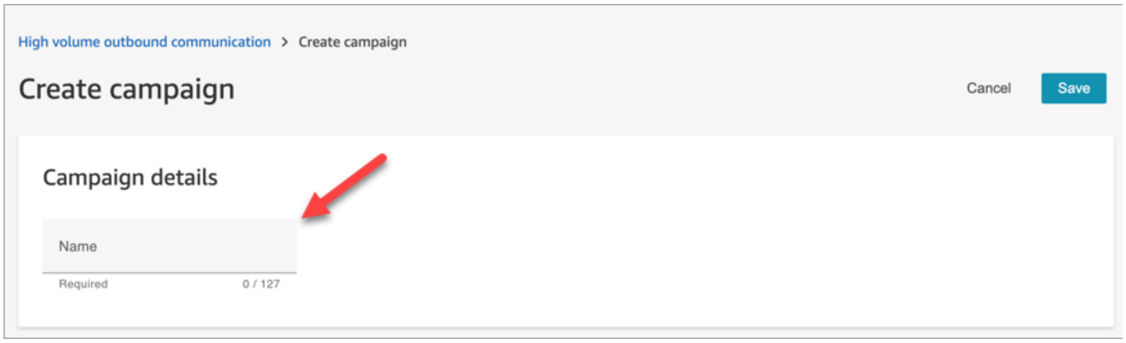
Contact centers send outbound communications to customers for a variety of reasons, such as appointment reminders, telemarketing, subscription renewals, and debt collection. By using Amazon Pinpoint Journeys and Amazon Connect, you can create high-volume outbound campaigns for voice, SMS, and email.

There are two ways you can create a high-volume outbound campaign:

- Use Amazon Connect console and Amazon Pinpoint. This topic provides instructions.
- Use the High-volume outbound communications API. For more information, see Amazon Connect High-Volume Outbound Communications API Reference. Note that you can't update the name of the outbound queue using the API.

How to create a high-volume outbound campaign

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. In the navigation pane, choose **High-volume outbound communication**, and then choose **Create campaign**.
3. In the **Campaign details** section, specify the name.



High volume outbound communication > Create campaign

Create campaign

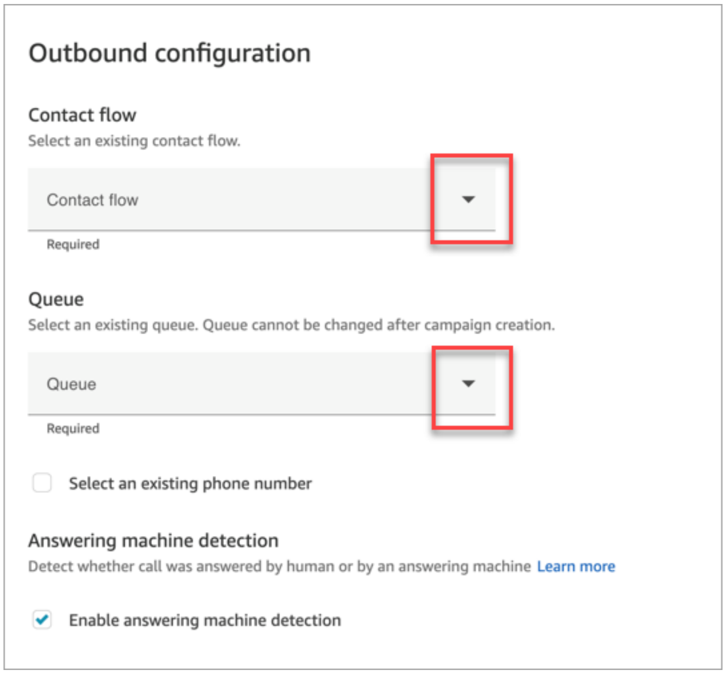
Cancel Save

Campaign details

Name

Required 0 / 127

4. In the **Outbound configuration** section, select the published flow you created for outbound communications (a flow that includes a Check call progress (p. 327) block).



Outbound configuration

Contact flow

Select an existing contact flow.

Contact flow

Required

Queue

Select an existing queue. Queue cannot be changed after campaign creation.

Queue

Required

☐ Select an existing phone number

Answering machine detection

Detect whether call was answered by human or by an answering machine Learn more

☑ Enable answering machine detection

5. Select a queue to associate with this campaign.
6. Answering machine detection is enabled by default. If desired, you can choose to disable it.

   Note

   If you disable answering machine detection, and if your flow includes the Check call progress (p. 327) block, the contact is routed down the Error branch.
7. Choose a phone number to be shown as caller ID when making outbound calls. The outbound phone number is specified for a queue.

   Important

   - You must use a phone number that has been ported to your Amazon Connect instance, or claimed from Amazon Connect.

- Telecom regulations in certain countries dictate use of phone numbers from specific carriers for outbound calling. For more information, see the Amazon Connect Telecoms Country Coverage Guide to learn more.
- If you plan to call customers in Australia or New Zealand, see *Step 4: Create a new campaign in the Amazon Connect instance* in this blog for instructions: Make predictive and progressive calls using Amazon Connect high-volume outbound communications.

8. Choose a dialer type.
9. Choose a bandwidth allocation.
10. Open the Amazon Pinpoint console (https://console.aws.amazon.com/pinpoint/) and Create a journey, using the name of the campaign that you created in Amazon Connect.
11. Associate this campaign to a customer journey on Amazon Pinpoint to start making high-volume outbound calls.

Campaign state

After a campaign is running, you can pause or stop it. You can also delete a campaign at any time.

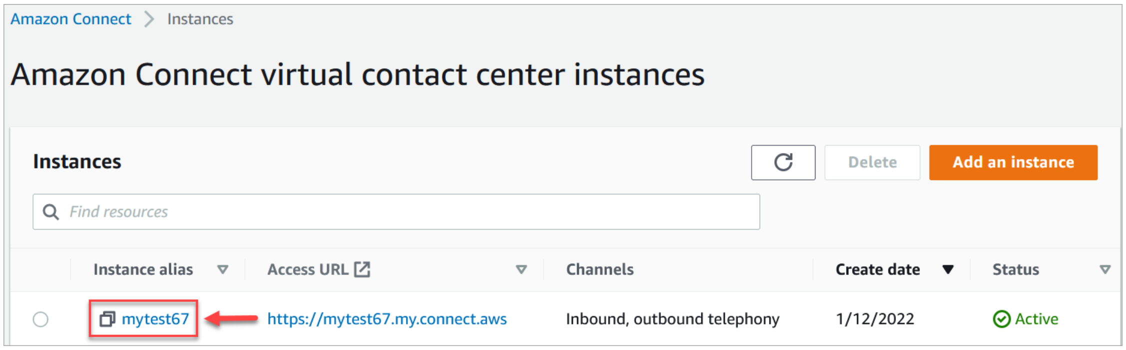
Following is a description of each campaign state:

- **Created** – The campaign is created.
- **Running** – The campaign as running.
- **Paused** – The campaign is paused until it is resumed.
- **Stopped** – The campaign is stopped. You can't resume a campaign that is stopped.
- **Failed** – An error state caused the campaign to fail.

Disable high-volume outbound communications

Important
You must delete all existing campaigns before you can disable high-volume outbound communications.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.


Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

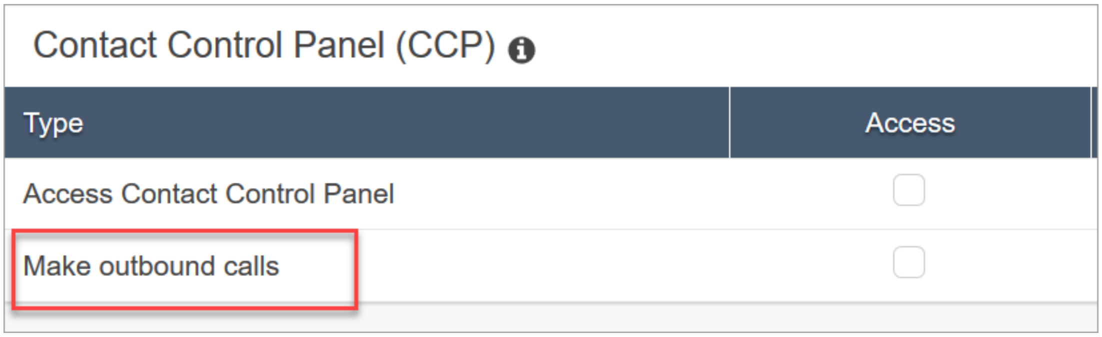
	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	✓ Active

3. In the navigation pane, choose **Telephony**.
4. To disable high-volume outbound communications, uncheck **Enable high-volume outbound communications**.
5. Choose **Save**.

You can no longer create high-volume outbound campaigns.

Security profile permissions for outbound communications

To enable agents to make outbound calls, the following **Make outbound calls** permissions to the agent's security profile:



Contact Control Panel (CCP)

Type	Access
Access Contact Control Panel	☐
Make outbound calls	☐

To enable call center managers to create high-volume outbound campaigns, assign the **high-volume outbound communications** permissions to their security profile.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

By default, the **Admin** security profile already has permissions to perform all activities.

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. 296).

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

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

- Which queues will be in it.
- Whether one queue should be prioritized over another.
- What channels agents will handle in the Contact Control Panel (CCP).
- How many contacts agents can handle simultaneously for each channel.
- Whether individual queues are for all channels or specific ones.

Each agent is assigned to one routing profile.

Contents

How routing works

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 (that is, the agent who has been idle longest).
- Contacts are placed on hold if there are no available agents. The order in which they are serviced is determined by their time in queue, on a first-come, first-served basis.
- If multiple agents are 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 multiple channels, agents must complete the interactions with inbound contacts on one channel before they can receive a contact or a task on the other.

Example: Say a routing profile is configured for voice contacts and for up to 10 chats and up to 10 tasks. Here's how it would work:

- When agents sign on, they can be routed a chat, task, or voice contact.
- After the agents begin interacting with a voice call, no chats, tasks, or additional voice contacts are routed to them until they finish the call.
- When agents accept a chat, up to 10 chats are routed to them, but no voice contacts or tasks. After they're done with the chats, they're available for the next contact, which could be voice, chat, or task.
- When agents accept a task, up to 10 tasks are routed to them, but no voice contacts or chats. After they're done with the tasks, they're available for the next contact, which could be voice, chat, or task.

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. 227).

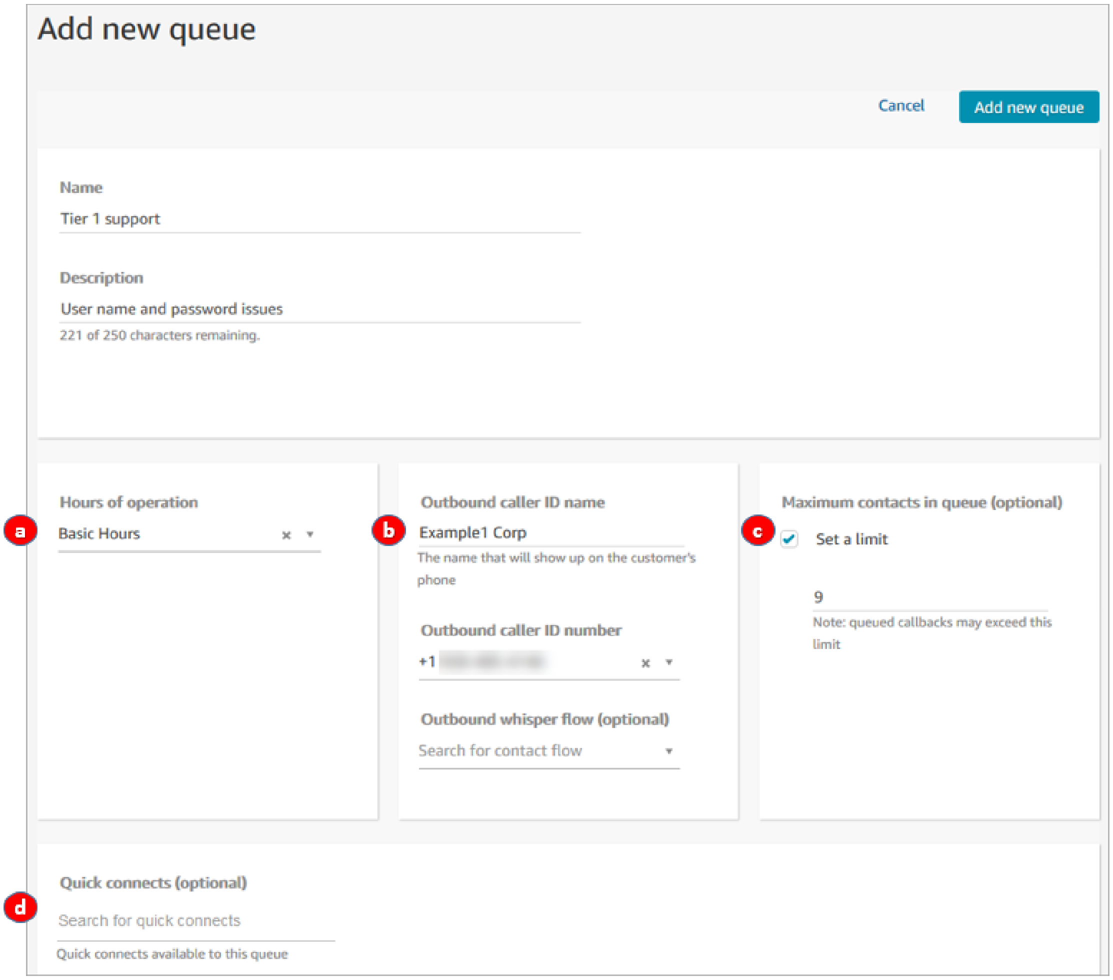
Learn more about routing

See the following topics to learn more about routing:

- Routing profiles (p. 21)
- Queue-based routing (p. 26)
- Set up queue-based routing (p. 230)

Create a queue

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



Add new queue

Name
Tier 1 support

Description
User name and password issues
221 of 250 characters remaining.

Hours of operation
Basic Hours

Outbound caller ID name
Example1 Corp
The name that will show up on the customer's phone

Outbound caller ID number
+1 [redacted]

Outbound whisper flow (optional)
Search for contact flow

Maximum contacts in queue (optional)
☑ Set a limit
9
Note: queued callbacks may exceed this limit

Quick connects (optional)
Search for quick connects
Quick connects available to this queue

See the following topics for detailed information about each of the above areas:

1. Set the hours of operation and timezone for a queue (p. 225)
2. Set up outbound caller ID (p. 212)
3. Set the Maximum contacts in queue limit (p. 224)
4. Create quick connects (p. 466)

The queue is automatically active.

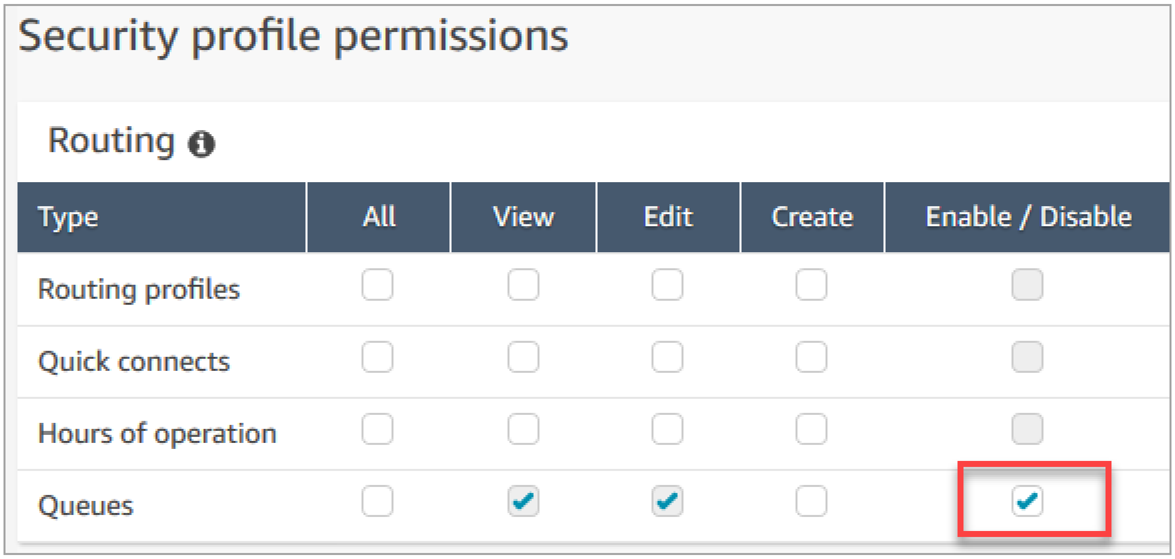
3. Assign the queue to a routing profile; for information, see Create a routing profile (p. 227). The routing profile links the queue and agents together.

To learn how queues work, see Routing profiles (p. 21) and Queue-based routing (p. 26).

Disable a queue

You can quickly control the flow of contacts to queues by temporarily disabling a queue. When a queue is disabled, it's put in an offline mode. No new contacts are routed to the queue, but any existing contacts already in the queue are routed to agents.

Only users who have a security profile with **Queues - Enable/Disable** permissions can disable a queue.



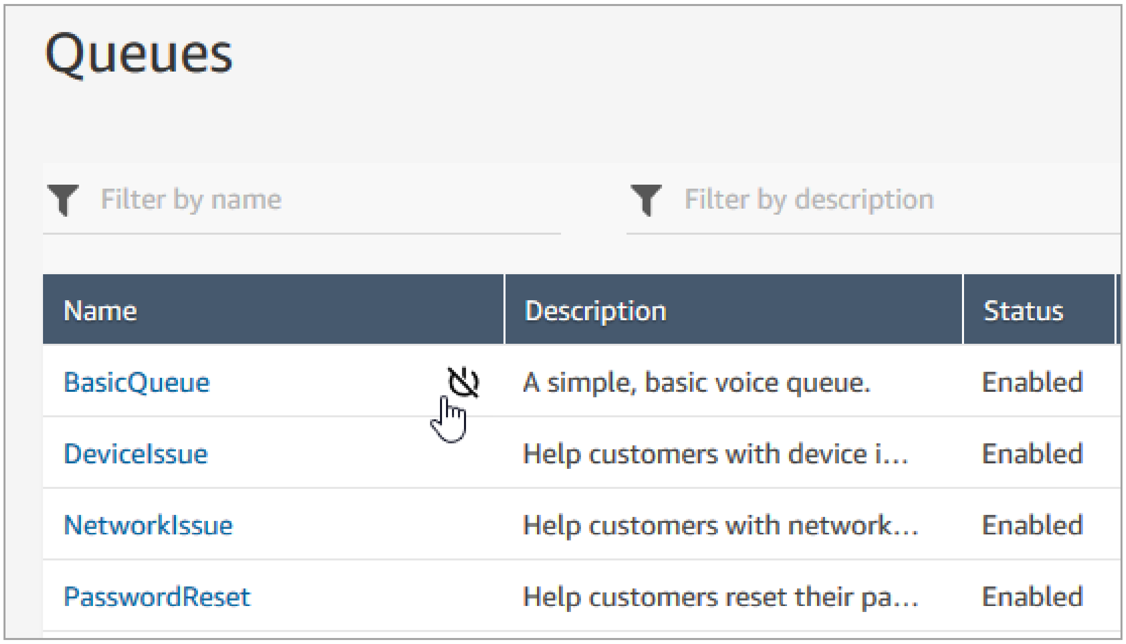
Security profile permissions

Routing

Type	All	View	Edit	Create	Enable / Disable
Routing profiles	☐	☐	☐	☐	☐
Quick connects	☐	☐	☐	☐	☐
Hours of operation	☐	☐	☐	☐	☐
Queues	☐	☑	☑	☐	☑

To disable an active queue

1. On the navigation menu, choose **Routing**, **Queues**.
2. Hover over the name of the queue to edit. Choose the power icon that appears.



Queues

Name	Description	Status
BasicQueue	A simple, basic voice queue.	Enabled
DeviceIssue	Help customers with device i...	Enabled
NetworkIssue	Help customers with network...	Enabled
PasswordReset	Help customers reset their pa...	Enabled

3. Choose **Disable** to confirm you want to disable the queue. You can immediately re-enable the queue if needed by choosing the power button again.

Set the Maximum contacts in queue limit

To determine how many contacts can be in a standard queue (p. 22) at the same time, you set the **Maximum contacts in queue** limit for the standard queue. This setting does not apply to agent queues (p. 22); those are always limited to 10 contacts.

This setting applies to all the contacts that are in the standard queue, across all channels. For example, you set **Maximum contacts in queue** to 100 and configure the queue for calls, chats, and tasks. This means the limit is set to a total of 100 concurrent calls AND chats AND active tasks in the queue.

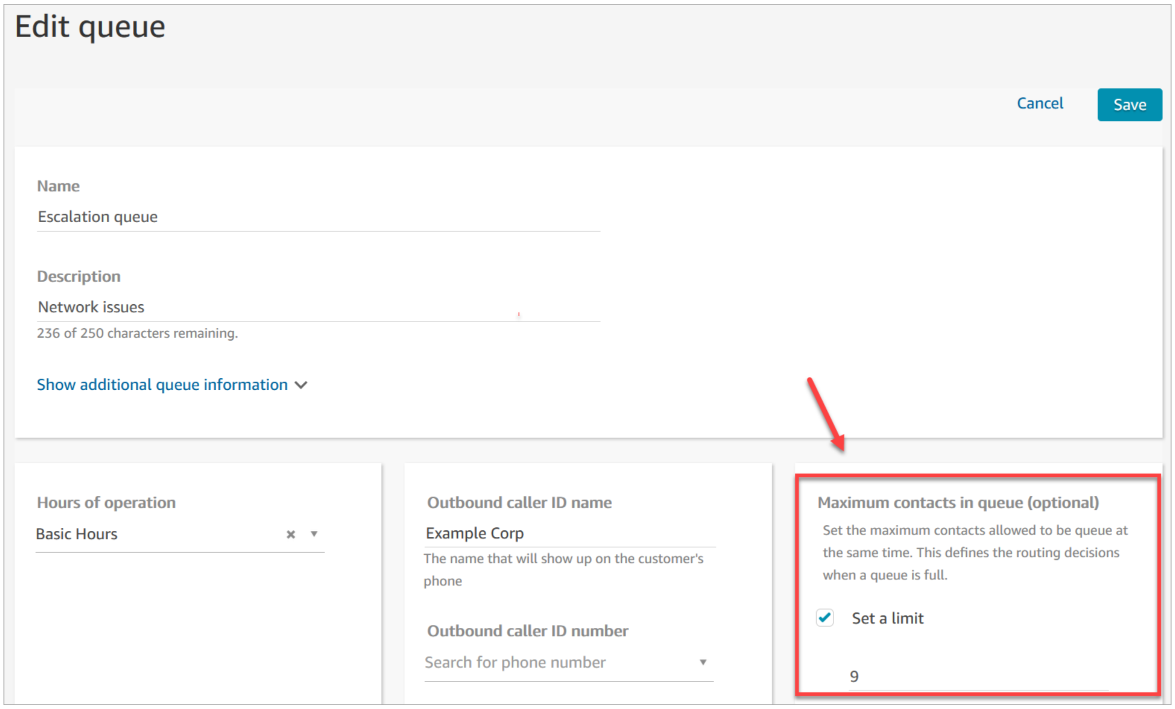
> **Important**
> By default you cannot set **Maximum contacts in queue** to be greater than your **Concurrent calls per instance** service quota.
> For information about default service quotas and how to request an increase, see Amazon Connect service quotas (p. 1205).

To set Maximum contacts in queue

1. On the navigation menu, choose **Routing**, **Queues**, **Add new queue**. Or, edit an existing queue.
2. Under **Maximum contacts in queue** choose **Set limit**.
3. Specify how many contacts can be in the queue before it's considered full.

   Queued callbacks count towards the queue size limit, but they are routed to the error branch. For example, if you have a queue that handles both callbacks and incoming calls, and that queue reaches the size limit:

   - The next callback is routed to the error branch.
   - The next incoming call gets a reorder tone (also known as a fast busy tone), which indicates no transmission path to the called number is available.



Edit queue

Name
Escalation queue

Description
Network issues
236 of 250 characters remaining.

Hours of operation
Basic Hours

Outbound caller ID name
Example Corp
The name that will show up on the customer's phone

Outbound caller ID number
Search for phone number

Maximum contacts in queue (optional)
Set the maximum contacts allowed to be queue at the same time. This defines the routing decisions when a queue is full.

☑ Set a limit

9

Route contacts based on queue capacity

To define routing decisions based on queue capacity, use a Transfer to queue (p. 437) block to check whether a queue is full (Maximum contacts in queue (p. 224)), and then route the contact accordingly.

The Transfer to queue (p. 437) block checks the Maximum contacts in queue (p. 224). If no limit is set, the queue is limited to the number of total concurrent contacts for the following quotas:

- Active tasks per instance
- Concurrent calls per instance
- Concurrent chats per instance

Set the hours of operation and timezone for a queue

The first thing you need to do when you set up a queue is to specify the hours of operation and timezone. The hours may be referenced in contact flows. For example, when routing contacts to agents, you might use the Check hours of operation (p. 333) block first, and then route the contact to the appropriate queue.

To set the hours of operation and timezone for a queue

1. On the navigation menu, choose **Routing**, **Hours of operation**.
2. To create a template, choose **Add new hours** and enter a name and a description.
3. For **Time zone**, select a value.
4. For **Add new**, set new hours.
5. Choose **Save**.
6. Now you can specify these the hours of operation when you create a queue (p. 222), and check them in the Check hours of operation (p. 333) block.

How to specify midnight

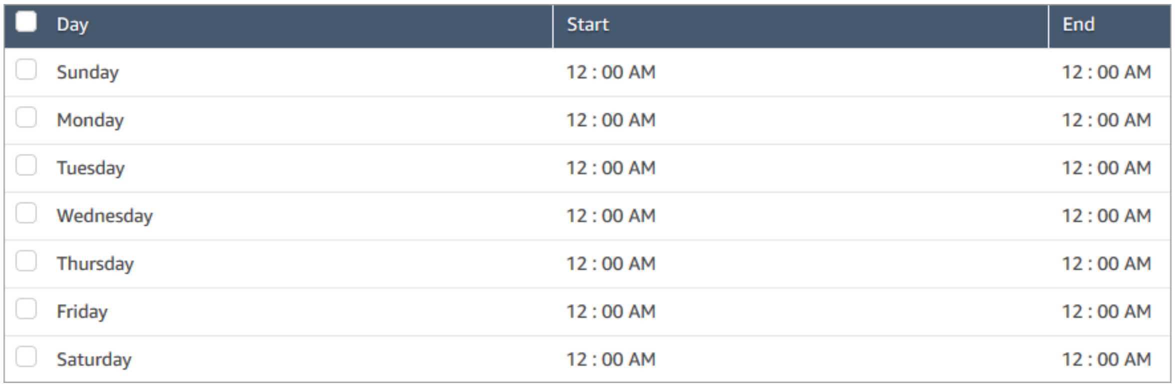
To specify midnight, enter 12:00AM.

For example, if you want to set your hours to 10:00AM to midnight, you would enter: 10:00AM to 12:00AM. Your call center would be open for 14 hours. Here's the math:

- 10:00AM-12:00PM = 2 hours
- 12:00PM-12:00AM = 12 hours
- Total = 14 hours

Examples

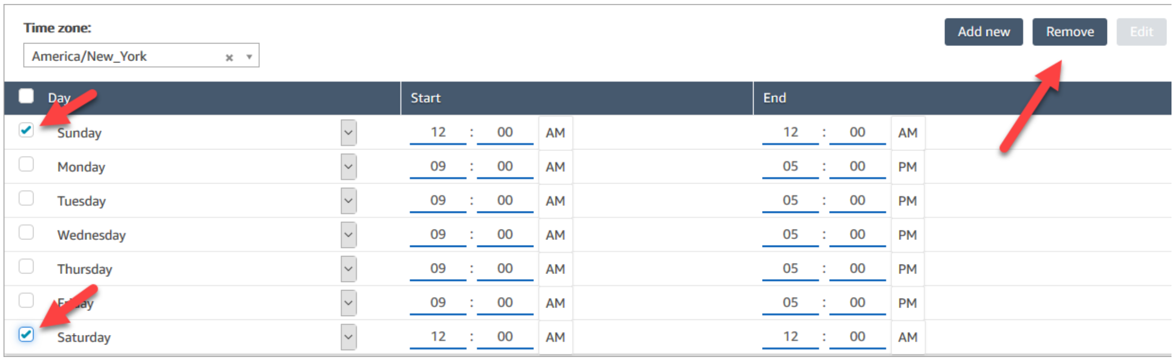
Schedule for 24x7



□ Day	Start	End
□ Sunday	12 : 00 AM	12 : 00 AM
□ Monday	12 : 00 AM	12 : 00 AM
□ Tuesday	12 : 00 AM	12 : 00 AM
□ Wednesday	12 : 00 AM	12 : 00 AM
□ Thursday	12 : 00 AM	12 : 00 AM
□ Friday	12 : 00 AM	12 : 00 AM
□ Saturday	12 : 00 AM	12 : 00 AM

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

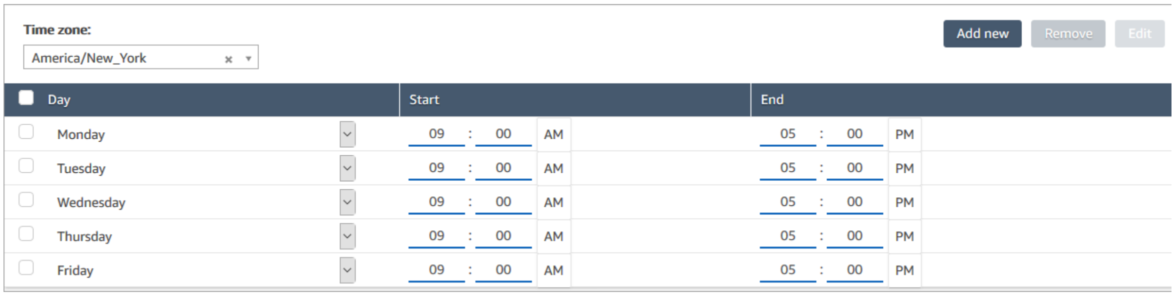
Remove Sunday and Saturday from the schedule.



Time zone: America/New_York

□ Day	Start	End
☑ Sunday	12 : 00 AM	12 : 00 AM
□ Monday	09 : 00 AM	05 : 00 PM
□ Tuesday	09 : 00 AM	05 : 00 PM
□ Wednesday	09 : 00 AM	05 : 00 PM
□ Thursday	09 : 00 AM	05 : 00 PM
□ Friday	09 : 00 AM	05 : 00 PM
☑ Saturday	12 : 00 AM	12 : 00 AM

The final schedule looks like this:

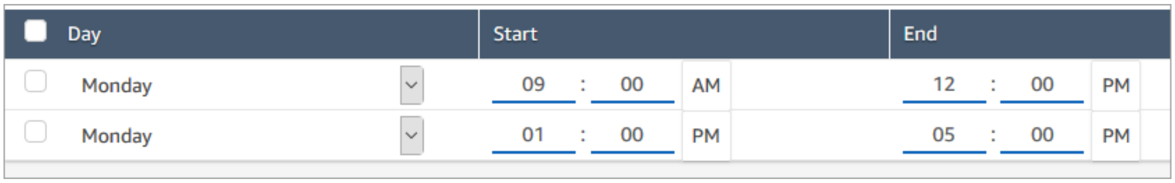


Time zone: America/New_York

□ Day	Start	End
□ Monday	09 : 00 AM	05 : 00 PM
□ Tuesday	09 : 00 AM	05 : 00 PM
□ Wednesday	09 : 00 AM	05 : 00 PM
□ Thursday	09 : 00 AM	05 : 00 PM
□ Friday	09 : 00 AM	05 : 00 PM

Add lunch and other breaks

If your entire contact center were to close for lunch from 12-1, for example, then you'd enter hours to specify that, as in the following image:



□ Day	Start			End		
□ Monday	09	00	AM	12	00	PM
□ Monday	01	00	PM	05	00	PM

In most contact centers breaks are staggered. While some agents are at lunch, for example, others are still available to handle contacts. Instead of specifying this in the hours of operation, you add custom agent statuses (p. 232) that appear in the agent's Contact Control Panel (CCP).

For example, you might create a custom status named **Lunch**. When the agent goes to lunch, they change their status in the CCP from **Available** to **Lunch**. During this time, no contacts are routed to them. When they return from lunch and are ready to take contacts again, they change their status back to **Available**.

Supervisors can change an agent's status using the real-time metrics report.

For more information, see these topics:

- Add custom agent status (p. 232)
- About agent status (p. 998)
- Change the "Agent activity" status in a real-time metrics report (p. 935)

What happens during daylight saving time

Amazon Connect uses the timezone to determine whether daylight saving time is in effect for the queues, and adjusts automatically for all timezones that observe daylight saving time. When a contact comes in, Amazon Connect looks at the hours and timezone to determine whether the contact can be routed to the given queue.

> **Important**
> Eastern Standard Time (EST) is used when observing standard time. It is five hours behind Coordinated Uniserval Time (UTC).
> Eastern Daylight Time (EDT) is used when observing daylight saving time. It is four hours behind Coordinated Uniserval Time (UTC).
> Unlike EST, Central European Time (CET) observes daylight savings time.

Use the Check Hours of Operation block

At the start of your contact flows, use the Check hours of operation (p. 333) block to determine whether your contact center is open, and to branch accordingly.

Create a routing profile

While queues are a 'waiting area' for contacts, a routing profile links queues to agents. When you create a routing profile, you specify 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. For more information about routing profiles and queues, see Routing profiles (p. 21).

To create a routing profile

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

Item	Description	
Name	Enter a searchable display name.	
Description	Describe what the routing profile is for.	
Set channels and concurrency	Choose whether agents assigned to this profile handle contacts using voice, chat, or both. Also specify whether the agent can receive tasks. For **Chat**, specify how many chat conversations that an agent can have simultaneously, up to 10. For **Task**, specify how many tasks an agent can have simultaneously, up to 10. For more on setting this option, see Tips for setting up channels and concurrency (p. 229). For information about how Amazon Connect routes contacts when multiple channels are in use, see How routing works with multiple channels (p. 221).	

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

Item	Description	
Name	Use the dropdown menu to choose a queue you've already set up. You can add multiple queues to a routing profile.	
Channels	Choose whether the queue is for chat, voice, task, or all three. **Important** The channel that you specify here must also be specified under **Set channels and**	

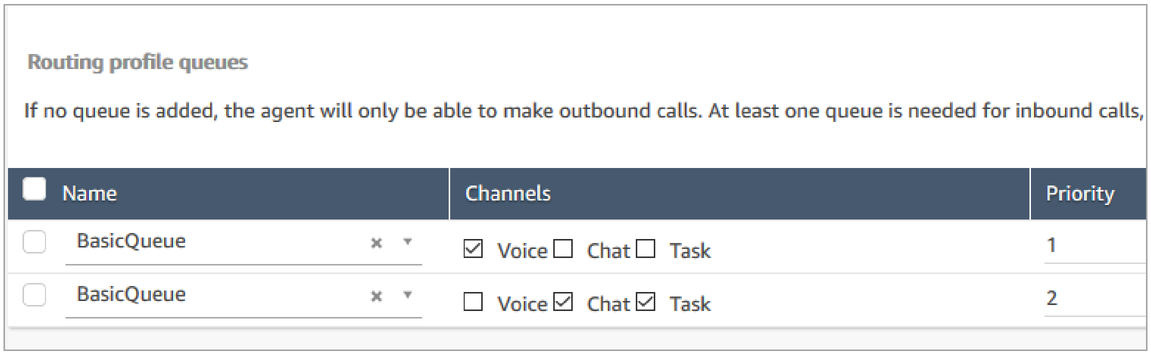
Item	Description	
	concurrency. If it isn't, contacts from that channel won't be routed to agents.	
Priority	Specify the order in which contacts are to be handled for that queue. For example, a contact in a queue with a priority of 2 would be a lower priority than a contact in a queue with a priority of 1.	
Delay (in seconds)	Enter the minimum amount of time a contact should be in the queue before they are routed to an available agent. To learn more about how Priority and Delay work together, see Queues: priority and delay (p. 24).	
Default outbound queue	Choose a queue to be associated with outbound calls placed by the agents.	

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, chat, and task contacts.

  For example, there are 20 queues assigned to a profile. All of the queues are enabled for voice, chat, and task. By removing the **Voice** option at the routing profile level, you can stop all voice calls to these agents, across all queues in the profile. When you want to restart voice contacts for these agents again, select **Voice**.
- For each queue in the profile, choose whether it's for voice, chat, task, or all three.
- If you want a queue to handle voice, chat, and task, but want to assign a different priority to each channel, add the queue twice. For example, in the following image, voice is priority 1 but chat and task are priority 2.



Routing profile queues

If no queue is added, the agent will only be able to make outbound calls. At least one queue is needed for inbound calls,

□ Name	Channels	Priority
□ BasicQueue	☑ Voice □ Chat □ Task	1
□ BasicQueue	□ Voice ☑ Chat ☑ Task	2

Delete a routing profile

Currently it's not possible to delete a routing profile. To take a routing profile out of use, detach it from the agents.

To indicate that the routing profile is no longer in use, we recommend renaming it with a **zz_** prefix, for example, zz_Sales.

Set up queue-based (skills-based) routing

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

- Create the queues (p. 222), for example, one for each skill you want to use for routing.
- Create the routing profiles (p. 227):
  - Specify the channels supported by this routing profile.
  - Specify the queues: the channel, priority, and delay.
- Configure agent settings (p. 233) to assign the routing profiles to them.

When you create your contact flows (p. 445), you'll add the queues to them. If a contact chooses to speak to an agent in Spanish, for example, they will be routed to the Spanish Reservations queue.

For information about how routing works, and queue-based routing, see these topics:

- How routing works with multiple channels (p. 221)
- Queue-based routing (p. 26)

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

Agent hierarchies are a way for you to organize agents into teams and groups for reporting purposes. It's useful to organize them based on their location and their skill sets. For example, you might want to create large groups, such as all agents who work on a specific continent, or smaller groups such as all agents working in a specific department.

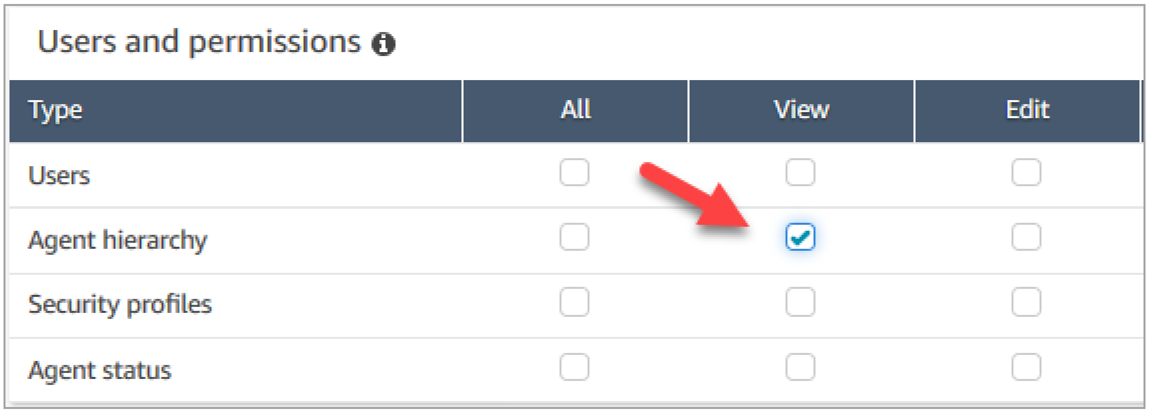
You can also configure hierarchies with up to five levels, and segment agents or teams. Here are a couple of things to note about using hierarchies:

- Removing agents from a level affects historical reporting.
- When you use the **Restrict contact access** permission, you can restrict contact search results based on the agent's hierarchy. For more information, see Manage who can search for contacts and access detailed information (p. 911).

Required permissions

To create agent hierarchies, you need the **View - Agent hierarchy** permission in your security profile.

> **Note**
> Since agent hierarchies may include location and skill set data, you also need this permission to view the agent hierarchy information in a real-time metrics report.



Users and permissions

Type	All	View	Edit
Users	☐	☐	☐
Agent hierarchy	☐	☑	☐
Security profiles	☐	☐	☐
Agent status	☐	☐	☐

Create a new agent hierarchy

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to create agent hierarchies.
2. Choose **Users**, **Agent hierarchy**.
3. Enter a name and choose **+** to create the first level of your hierarchy.
4. Choose **+** to add more levels to your hierarchy.
5. Choose **Save** to apply the changes, or **Cancel** to undo them.

   > **Tip**
   > If the Save button isn't active, you don't have permissions to create or edit the agent hierarchy.

Add groups, teams, and agents to a hierarchy

After you create a hierarchy, you can add groups, teams, and agents from the top down.

1. Select the top level of the hierarchy.
2. Choose **x** to add groupings to each level.
3. Choose the check icon to save the name, choose the pencil icon to edit the name.
4. Choose **Save**.

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

Add custom agent status

Agents are responsible for setting their status in the Contact Control Panel (CCP). In fact, the only time an agent's status changes is when they manually change it in the CCP, or when their supervisor changes it (p. 935) in a real-time metrics report.

Amazon Connect provides two default status values:

- Available
- Offline

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

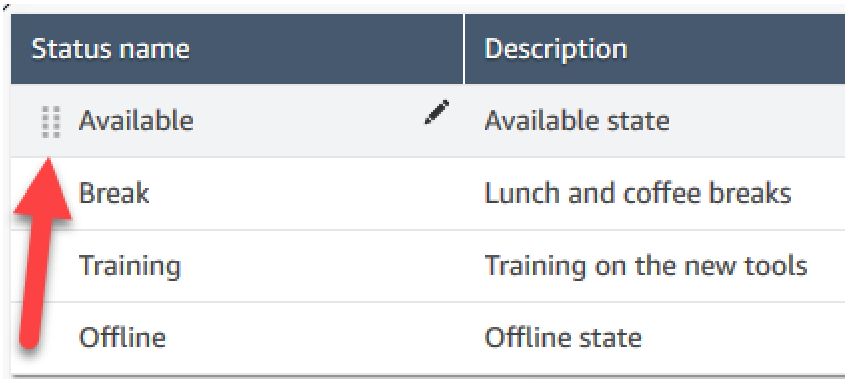
When you add a new status, it will always be **Custom**, not routable.

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

To add a new agent status

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

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



Status name	Description
Available	Available state
Break	Lunch and coffee breaks
Training	Training on the new tools
Offline	Offline state

To edit a status

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

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

Configure agent settings: routing profile, phone type, and auto-accept calls

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

- What is their routing profile? They can only be assigned one.
- Will they have the **Agent** security profile or a custom profile you created?
- Are they going to use a soft phone? If so, will they be connected to contacts automatically, or will they need to press the **Accept** button in their Contact Control Panel (CCP)?
- Or, are they going to use a desk phone? If so, what is their number?
- How many seconds do they have for After contact work (ACW)? There's no way you can turn off ACW time altogether so agents never go to ACW. (A value of **0** means an indefinite amount of time.)
- Are they going to be assigned to an agent hierarchy?

> **Note**
> You can't configure how long an available agent has to connect with a contact before it's missed. Agents have 20 seconds to accept or reject a contact. If no action is taken, the current agent's status will be **Missed** and the contact is routed to the next available agent.

To configure agent settings

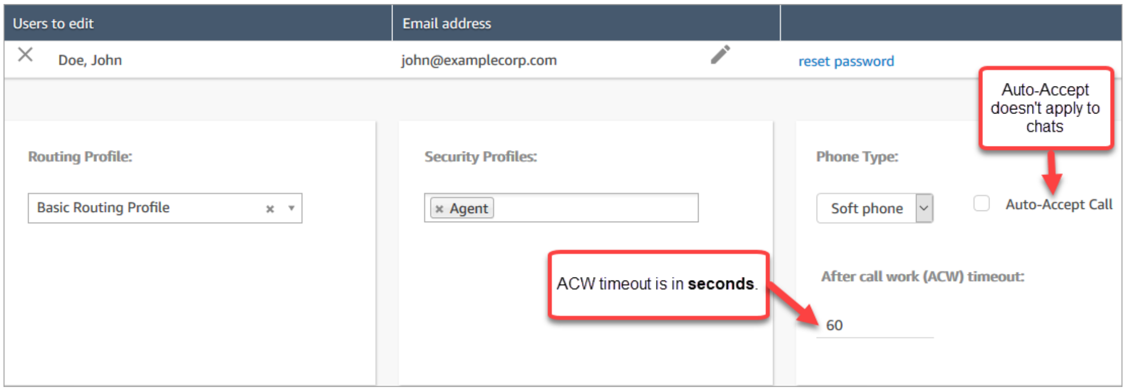
1. In the navigation pane, go to **Users, User management**.
2. Choose the user you want to configure, then choose **Edit**.
3. Assign a routing profile (p. 227) to them. You can only assign one.
4. Assign the **Agent** security profile, unless you've created custom security profiles.
5. Under **Phone Type** choose whether the agent is using a desk phone or soft phone.

   - If you select desk phone, enter their phone number.

     > **Important**
     > Outbound telephony charges occur when using a desk phone to answer inbound calls.

   - If you select soft phone, choose **Auto-Accept Call** if you want agents to be connected to calls automatically. This doesn't apply to chats.
6. In **After call work (ACW) timeout**, type how many seconds agents have for after contact work, such as entering notes about the contact. 1 second is the minimum amount of time you can enter.

   Enter **0** if you don't want to allocate a specific amount of ACW time. It essentially means an indefinite amount of time. When the conversation ends, ACW starts; the agent must choose **Close contact** to end ACW.



Users to edit	Email address	
Doe, John	john@examplecorp.com	reset password

Routing Profile: Basic Routing Profile

Security Profiles: Agent

Phone Type: Soft phone

☐ Auto-Accept Call

After call work (ACW) timeout: 60

Auto-Accept doesn't apply to chats

ACW timeout is in **seconds**.

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.

How long until the call is connected to the agent?

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

There isn't an option for increasing the amount of time before a call is automatically accepted.

Auto-Accept Call doesn't work for callbacks.

Enable auto-accept call for existing agents

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

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

1. Log in to the Amazon Connect console with an Admin account, or an account assigned to a security profile that has permissions to create or edit users.
2. In the left navigation bar, choose **Users**, **User management**.
3. In the list of users, select an agent, and then choose **Edit**.
4. On the Edit users page, under Phone Type, select the **Auto-Accept Call** check box.
5. Choose **Save**.
6. Repeat these steps for each user that you want to edit.

Bulk upload new users with auto-accept call enabled

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

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

10. Under **Verify user details**, verify that the information is correct for the new users, and then choose **Create users**.

(Optional) Verify the change in CCP logs

To confirm that **Auto-Accept Call** is enabled for an agent, download the CCP logs generated for that agent: in the CCP for the agent, choose **Settings**, **Download logs**. The logs are saved to your browser's default download directory.

In the logs, the **autoAccept** attribute is set to **"true"** if this setting is enabled. The logs show something like this:

```
                  "type": "agent",
                  "initial": false,
                  "softphoneMediaInfo": {
                       "callType": "audio_only",
                       "autoAccept": true
```

CCPv1: Log out agents automatically when they close their CCP

Important
This topic only applies to customers who use CCPv1. The URL for CCPv1 ends with **/ccp#**.

When using the default Amazon Connect CCPv1, closing the CCP window or logging out doesn't automatically change an agent's status from **Available** to **Offline**. An agent must change their status manually to **Offline** and then log out.

To change this behavior, you can do one of the following:

- Use CCPv2. When agents log out, their status is automatically switched to **Offline**. However, note that CCPv2 doesn't automatically switch agents to **Offline** if they only close the window. For instructions on upgrading to CCPv2, see My CCP URL ends with /ccp# (p. 278).
- Create a custom CCP. See Amazon Connect Streams API and the Agent API
- Use the following steps in this topic to update your CCP so it switches agents to **Offline** and logs out agents automatically when they close the CCP window.

Step 1: Set up the Streams API

For instructions, see the Amazon Connect Streams Documentation.

Step 2: Update your application code to change the agent state

Integrate the following Streams API calls into your web application:

1. Use connect.agent() to subscribe to agent events and retrieve agent objects.

```
let mAgent;

connect.agent(function(agent) {
  mAgent = agent;
});
```

2. Call agent.setState() in the onbeforeunload event handler to change the agent state.

```
window.addEventListener("beforeunload", function(event) {
    if (mAgent != null) {
        let states = mAgent.getAgentStates();
        // "states" is an array of changeable states. You can filter the desired state
 to change by name.
        let offlineState = states.filter(state => state.name === "Offline")[0];

        // Change agent state
        mAgent.setState(offlineState, {
        success: function() {
            console.log("SetState succeeded");
        },
        failure: function() {
        console.log("SetState failed");
        }
    });
  }
});
```

Step 3: Design for errors

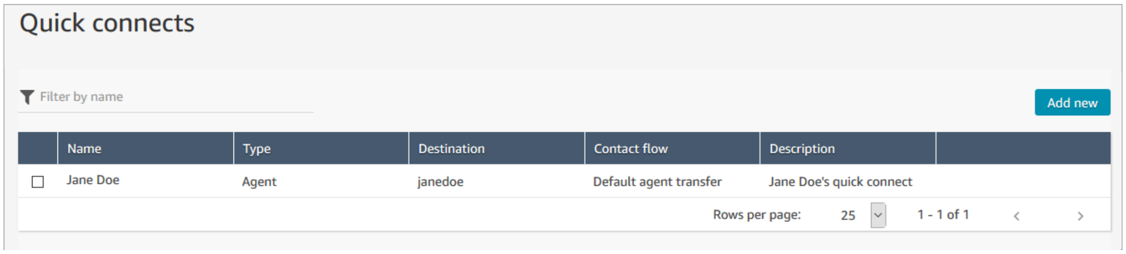
If an API call fails to execute the first time and a contact takes the error branch of your contact flow, there's a chance that an agent's state won't change as expected. Be sure to include logic to account for this possibility. For example, you could delay the page unload while the API call is tried again. Or, you could pop a "Call failed" warning message in a modal dialog before the page unload.

Set up agents to assign tasks to themselves

For an agent to be able receive a task, they need a quick connect created for them. With this quick connect, agents will be able to assign tasks to themselves, and other agents will be able to assign tasks to them.

Step 1: Create a quick connect for the agent

1. On the navigation menu, choose **Routing**, **Quick connects**, **Add a new**.
2. Enter a name for the quick connect, such as the name of the agent. For example, if you want Jane Doe to be able to assign tasks to herself, enter **Jane Doe**.
3. Under **Type**, use the dropdown list to choose **Agent**.
4. Under **Destination**, use the dropdown list to choose the user name for the agent.
5. Under **Contact flow**, choose **Default agent transfer**, or the appropriate contact flow for your contact center.
6. Under **Description**, enter a description, such as **Jane Doe's quick connect**.
7. Choose **Save**.



Quick connects

	Name	Type	Destination	Contact flow	Description
□	Jane Doe	Agent	janedoe	Default agent transfer	Jane Doe's quick connect

Step 2: Create a queue for the agent and associate the quick connect

1. After you create the quick connect, go to **Routing**, **Queues** and add a queue for the agent.
2. On the **Add new queue** page, in the **Quick connects** box, search for the quick connect you created for the agent.
3. Select the quick connect and then choose **Save**.

Step 3: Add the queue to the agent's routing profile

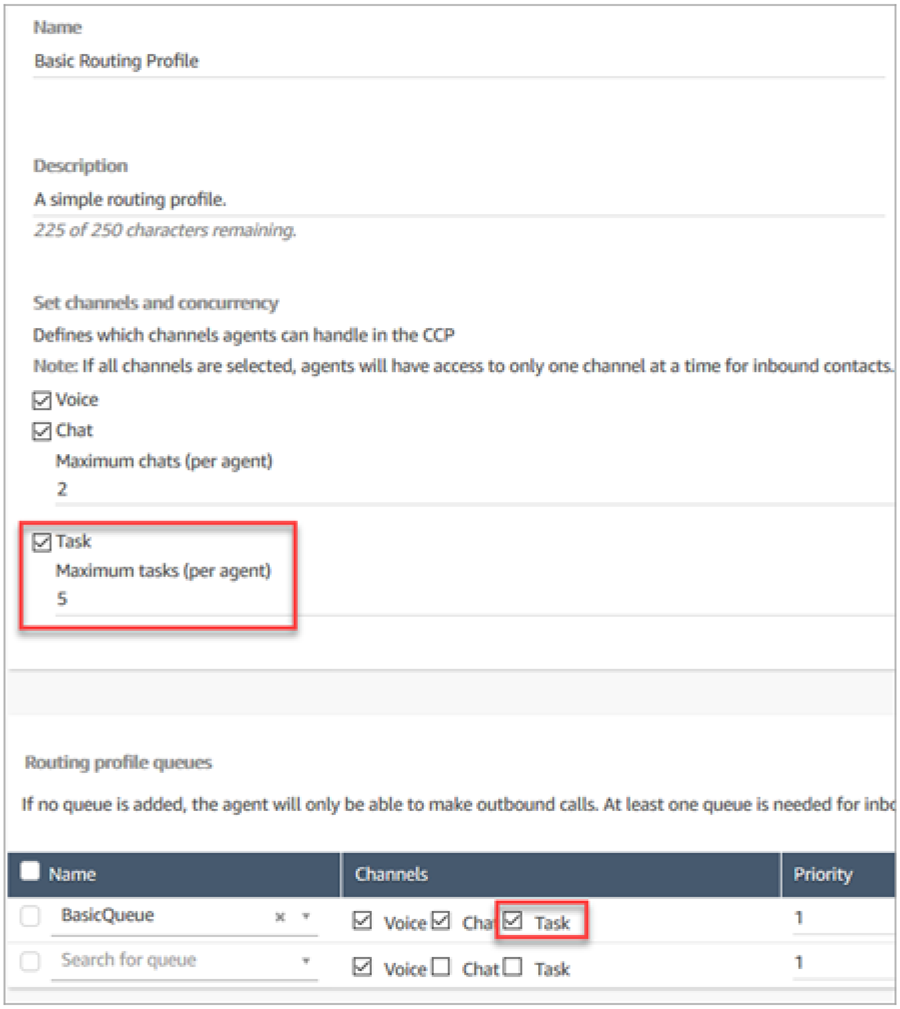
1. Go to **Users**, **Routing profiles** and choose the agent's routing profile.
2. Add the agent's queue to the routing profile, and choose **Task** for the channel.

   If the agent can receive transfers through other channels, select them as well.
3. Choose **Save**.

Set up tasks

1. Update your agent's routing profile (p. 227) so they can manage and create tasks.

   When you add tasks to their routing profile, you can specify that up to 10 tasks be assigned to them at a time.



Name

Basic Routing Profile

Description

A simple routing profile.

225 of 250 characters remaining.

Set channels and concurrency

Defines which channels agents can handle in the CCP

Note: If all channels are selected, agents will have access to only one channel at a time for inbound contacts.

☑ Voice

☑ Chat

Maximum chats (per agent)

2

☑ Task

Maximum tasks (per agent)

5

Routing profile queues

If no queue is added, the agent will only be able to make outbound calls. At least one queue is needed for inbc

□ Name	Channels	Priority
□ BasicQueue × ▾	☑ Voice ☑ Cha ☑ Task	1
□ Search for queue ▾	☑ Voice □ Chat □ Task	1

2. Create quick connects (p. 466) so that agents can create/assign tasks to themselves, or other agents or shared queues.
3. Update your contact flows to route tasks.
4. Optionally, create task templates (p. 238) to make it easy for agents to create tasks. All the fields they need to create a task are defined for them.
5. Optionally, integrate with external applications (p. 757) and set up rules to automatically create tasks (p. 602) based on pre-defined conditions.
6. By default all agents can create tasks. If you want to block permissions (p. 243) for some agents, assign the **Contact Control Panel**, **Restrict task creation permission** in their security profile.

Create task templates

Task templates make it easy for agents to capture the right information to create and complete a task (p. 16). All the fields they need to create given type of task are provided for them.

Important things to know before you create your first template

- When you publish your first template, your agents will be prompted to select a template when they create a new task. Agents must select one of the templates you have published.

- If you want to return to the standard task experience and not require agents to select a template, on the **Task templates** page, use the **Disable/Enable** toggle to disable all templates you published.
- Verify your Amazon Connect account has permissions to create task templates (p. 243).
- Review the list of quotas for task templates, such as the **Task templates per instance** and **Task template customized fields per instance**. See Amazon Connect service quotas (p. 1205).

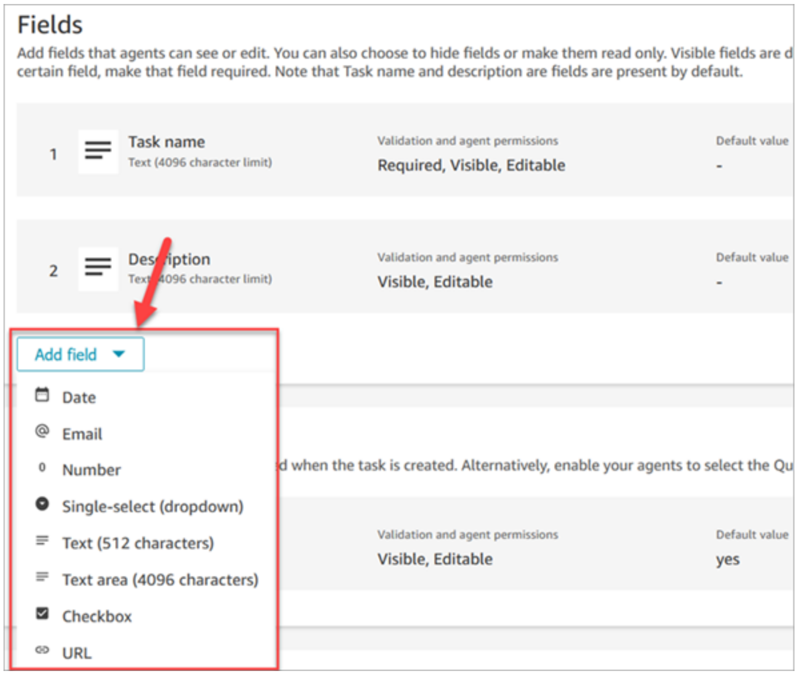
How to create a task template

Step 1: Name the template

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to create task templates (p. 243).
2. In the left navigation bar, choose **Channels**, **Task templates**.
3. On the **Task templates page**, choose **+ New template**.
4. On the **Create new template** page, in the **Template name** box, enter the name that will be displayed your agents.
5. In the **Description** box, describe the purpose of the template. This information is not displayed to agents; it's for your own use.

Step 2: Add fields, task assignment, and schedule

1. In the **Fields** section, choose the **Add field** dropdown, and then select the type of field you want to add to your template.



Fields

Add fields that agents can see or edit. You can also choose to hide fields or make them read only. Visible fields are d
certain field, make that field required. Note that Task name and description are fields are present by default.

1 Task name
Text (4096 character limit)
Validation and agent permissions: Required, Visible, Editable
Default value: -

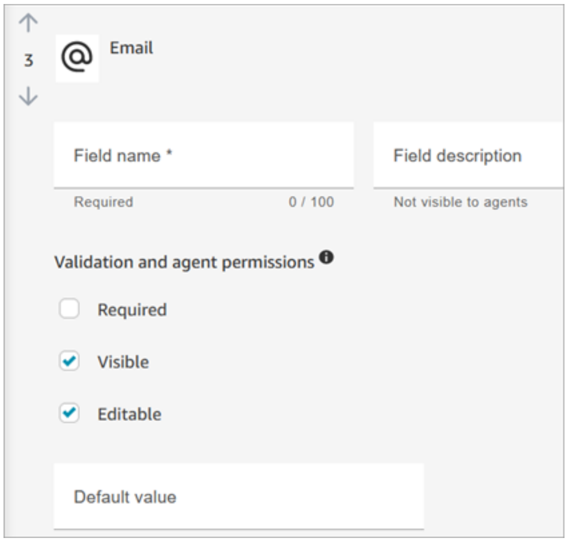
2 Description
Text (4096 character limit)
Validation and agent permissions: Visible, Editable
Default value: -

d when the task is created. Alternatively, enable your agents to select the Qu

Validation and agent permissions: Visible, Editable
Default value: yes

2. Use the up and down arrows as needed to change the order the field appears on the template.
3. In the **Validation and permissions** section, choose whether the field is required to be populated by the agent when they create a task, or add a default value to pre-populate the field when the agent opens the template.

   The following image shows what this section looks like for a field that is type **Email**.



3 Email

Field name *
Required 0 / 100

Field description
Not visible to agents

Validation and agent permissions

□ Required

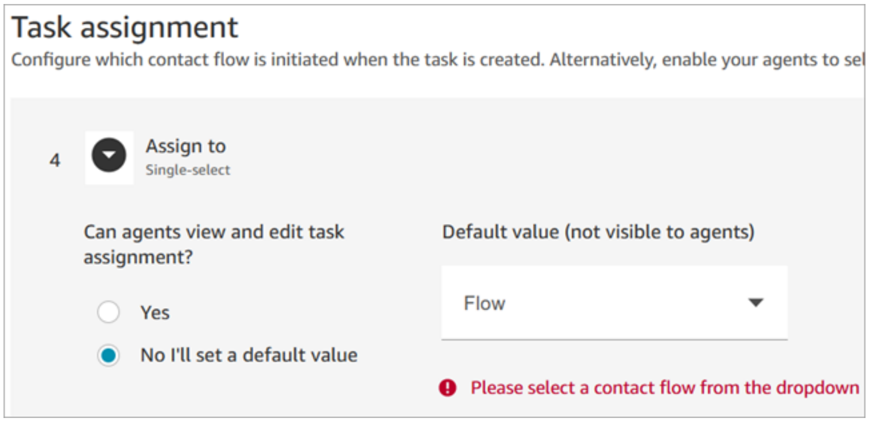
☑ Visible

☑ Editable

Default value

4. In the **Task assignment** section, choose whether agents can view and edit a task assignment when they creating the task. Or, assign a default value, which is a published flow that runs after the agent chooses **Create** to create the task. Agents don't see the name of the flow on the CCP.

   Note
   Only published flows are listed in the **Default value** dropdown.



Task assignment

Configure which contact flow is initiated when the task is created. Alternatively, enable your agents to sel

4 Assign to
Single-select

Can agents view and edit task assignment?

○ Yes

● No I'll set a default value

Default value (not visible to agents)

Flow

Please select a contact flow from the dropdown

5. In the **Task schedule** section, choose whether you want agents to be able to schedule a future start date and time for tasks.

Step 3: Publish

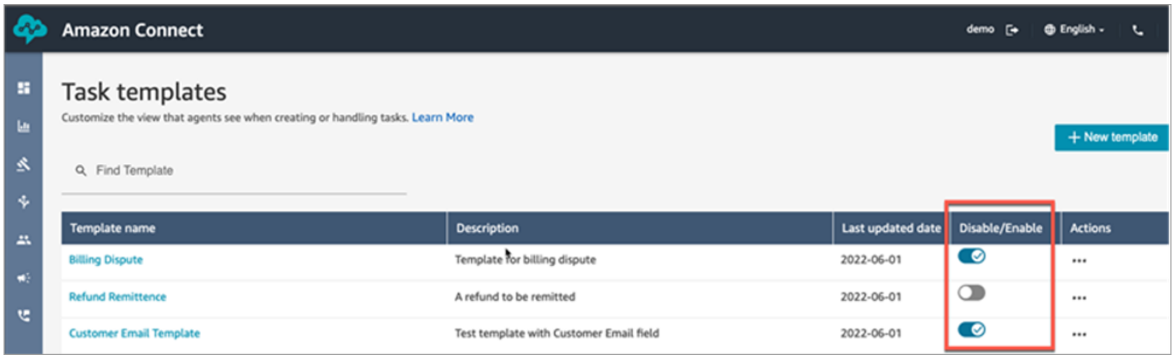
After you configure your template, choose **Publish** to create it and make it visible to your agents.

Important
If this is your first template, when you choose **Publish**, agents are automatically required to select a task template when they create a task.
If you want to maintain the standard task experience without selectable templates, disable all templates.

What your agents experience

After you publish a template, agents are required to select a template to create a task.

For example, the following image shows two templates have published: **Customer Email Template** and **Billing Dispute**.

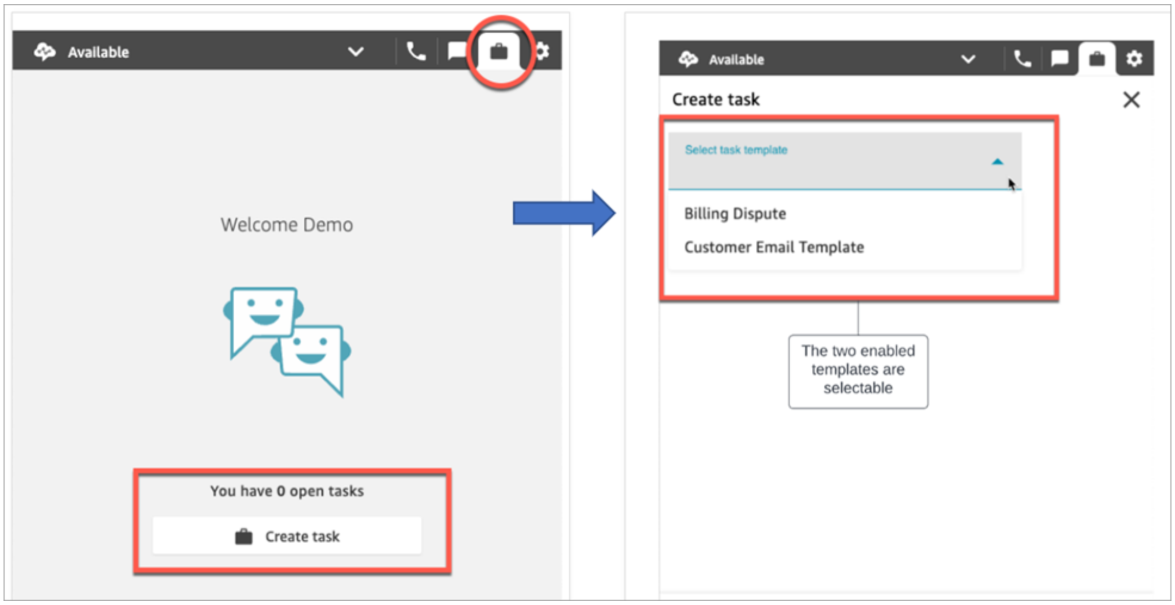


Task templates

Customize the view that agents see when creating or handling tasks. Learn More

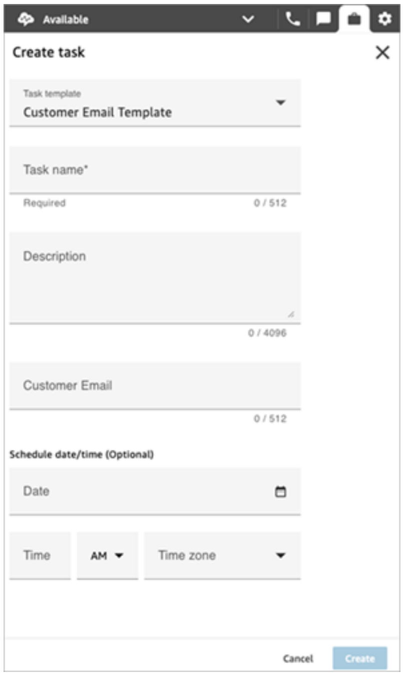
Template name	Description	Last updated date	Disable/Enable	Actions
Billing Dispute	Template for billing dispute	2022-06-01	●	•••
Refund Remittence	A refund to be remitted	2022-06-01	○	•••
Customer Email Template	Test template with Customer Email field	2022-06-01	●	•••

In the Contact Control Panel, when agents choose **Create task**, they must choose one of the templates: **Billing Dispute** or **Customer Email Template**.



The two enabled templates are selectable

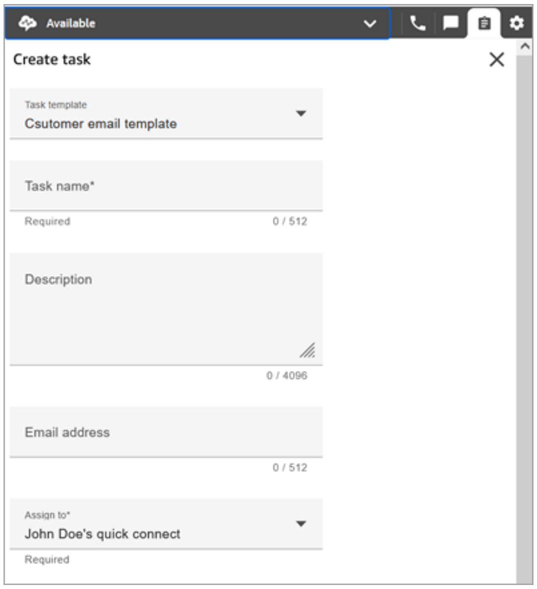
Let's assume the agent chooses **Customer Email Template**. The following image shows the fields the agent must complete in order to create a task. Notice that there is no option for the agent to assign the task; this template has **Task assignment** set to a default value.



Task template
Customer Email Template

"No data" message in the Assign to dropdown

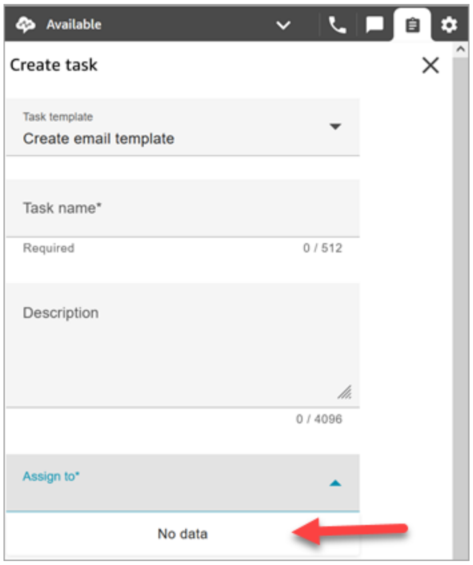
Let's says that in the **Task assignment** section, you choose to allow agents to assign the task to another agent. To set up for this scenario, you must create a quick connect for the destination agent so it appears in the dropdown list of choices, as shown in the following image. For instructions about creating a quick connect for an agent, see Test tasks (p. 150).



Task template
Csutomer email template

Assign to*
John Doe's quick connect

If no quick connects exist, then the message **No data** appears when you choose the **Assign to** dropdown menu, as shown in the following image:



Security profile permissions for task templates

Assign the **Routing**, **Task templates** permissions to enable a user to create task templates.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

By default, the **Admin** security profile already has permissions to perform all task activities.

Block agents from creating tasks

To block agents from being able to create tasks, assign the **Contact Control Panel (CCP)**, **Restrict task creation** permission. By default this permissions is unchecked, which means all agents can create tasks.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

By default, the **Admin** security profile already has permissions to perform all tasks activities.

Set up your customer's chat experience

You can provide a chat experience to your customers by using one of the following methods:

- Add a chat user interface to your website (p. 244).
- Download and customize our open source example (p. 253).
- Customize your solution using Amazon Connect APIs (p. 254). We recommend starting with the Amazon Connect ChatJS open source library when customizing your own chat experiences. For more information, see the Amazon Connect ChatJS repo on Github.

More resources to customize the chat experience

- Interactive messages provide customers with a prompt and pre-configured display options that they can select from. These messages are powered by Amazon Lex and configured through Amazon Lex using a Lambda. For instructions about how to add interactive messages through Amazon Lex, see this blog: Set up interactive messages for your Amazon Connect chatbot.

Amazon Connect supports the following templates: a list picker and a time picker. For more information, see Add interactive messages to chat (p. 633).

- Enable Apple Messages for Business (p. 259)
- Amazon Connect Service API Documentation, especially the StartChatContact API.
- Amazon Connect Participant Service API.
- Amazon Connect Chat SDK and Sample Implementations
- Amazon Connect Streams. Use to integrate your existing apps with Amazon Connect. You can embed the Contact Control Panel (CCP) components into your app.

Add a chat user interface to your website

To support your customers through chat, you can add a chat widget to your website that is hosted by Amazon Connect. You can configure the chat widget in the Amazon Connect console: customize the font and colors, and secure the widget so that it can be launched only from your website. As a result, you will have a short code snippet that you add to your website.

Because Amazon Connect hosts the widget, it ensures that the latest version is always live on your website.

> **Tip**
> Use of the chat widget is subject to default service quotas, such as the number of required characters for each message. Before launching your chat widget into production, make sure that your service quotas are set for your organization's needs. For more information, see Amazon Connect service quotas (p. 1205).

Supported browsers

The pre-built chat widget supports the following browser versions and higher:

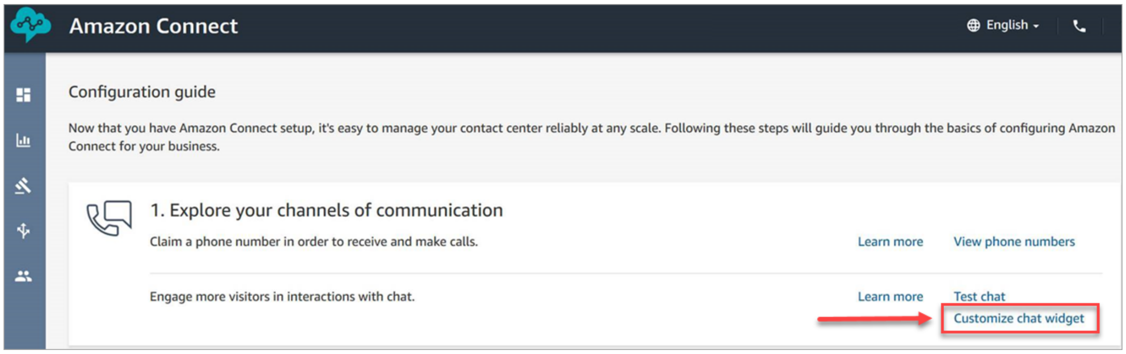
- Google Chrome 85.0
- Safari 13.1
- Microsoft Edge version 85
- Mozilla Firefox 81.0

The chat widget supports browser notifications for desktop devices. For more information, see Browser notifications (p. 254).

Step 1: Customize your chat widget

In this step, you customize the experience of the chat widget for your customers.

1. Log in to your contact center at https://*instance name*.my.connect.aws/.. Choose **Customize chat widget**.



Amazon Connect

Configuration guide

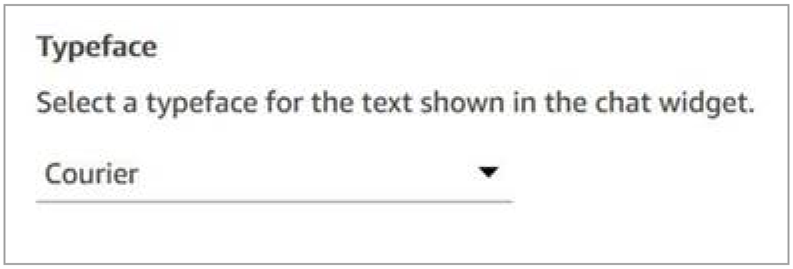
Now that you have Amazon Connect setup, it's easy to manage your contact center reliably at any scale. Following these steps will guide you through the basics of configuring Amazon Connect for your business.

1. Explore your channels of communication

Claim a phone number in order to receive and make calls.

Engage more visitors in interactions with chat.

2. For **Typeface**, use the dropdown to choose the font for the text in the chat widget.



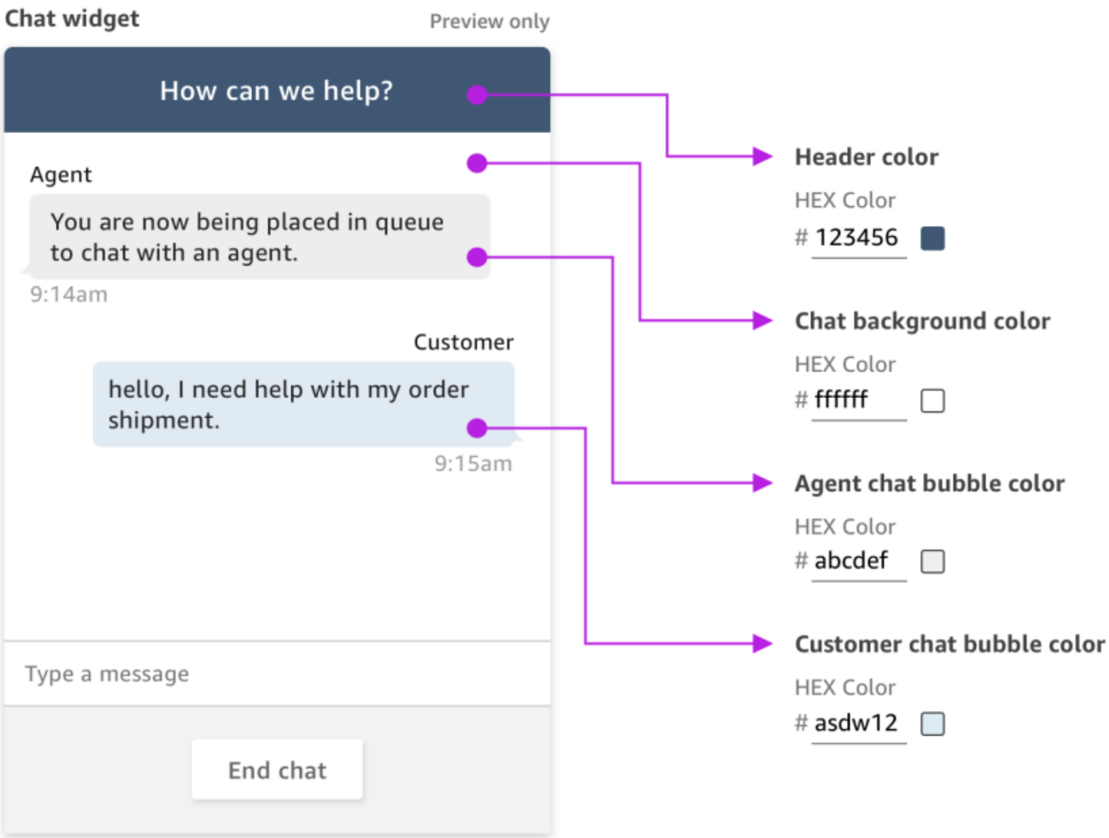
Typeface

Select a typeface for the text shown in the chat widget.

Courier

3. For **Chat widget**, choose the colors for the widget header, chat message bubbles, and launch and minimize icons by entering hex values (HTML color codes) that align the chat widget with your website branding.

   As you choose colors, the chat preview updates automatically so that you can see what your widget will look like.

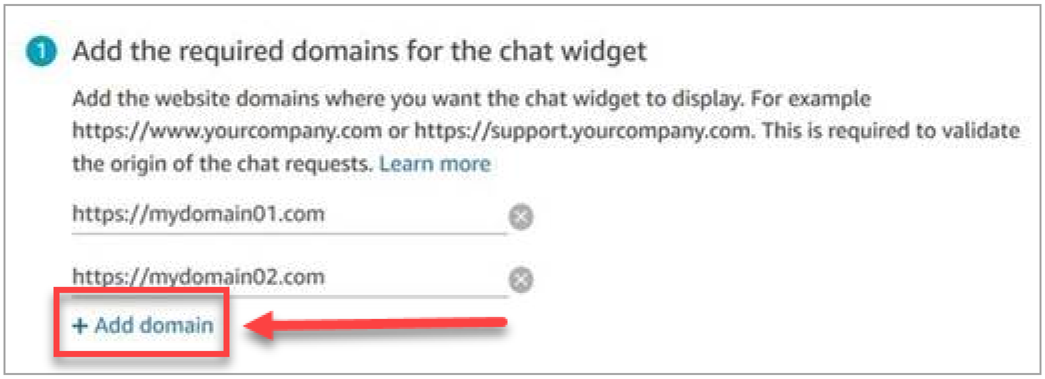


4. For **Minimize chat icon**, select the colors for the icon that customers will choose or tap to minimize the chat widget.
5. For **Open chat icon**, select the colors for the icon that customers will choose or tap to start a chat with your contact center.
6. For **Select contact flow**, choose the inbound flow that initiates when a customer starts a chat.
7. Choose **Next**.

Step 2: Specify the website domains where you expect to display the chat widget

1. Enter the website domains where you want to place the chat widget. Chat loads only on websites that you select in this step.

   Choose **Add domain** to add up to five domains.



1 Add the required domains for the chat widget

Add the website domains where you want the chat widget to display. For example https://www.yourcompany.com or https://support.yourcompany.com. This is required to validate the origin of the chat requests. Learn more

https://mydomain01.com

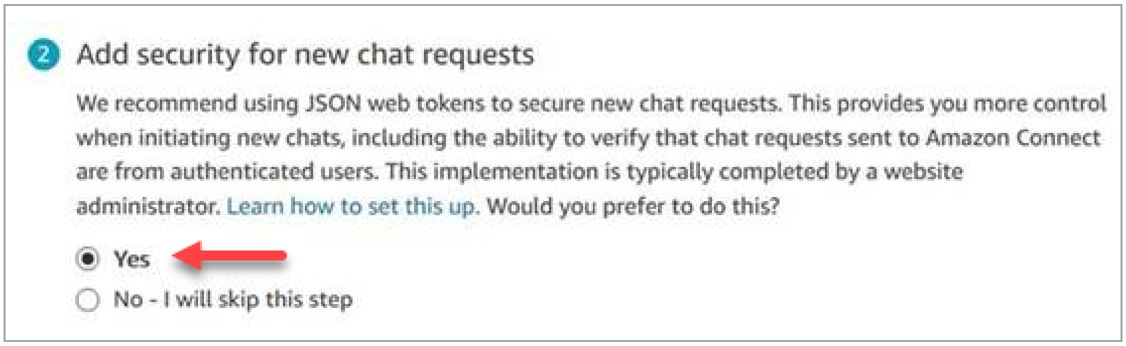
https://mydomain02.com

+ Add domain

Important

- Double-check that your website URLs are valid and does not contain errors. Include the full URL starting with https://.
- We recommend using https:// for your production websites and applications.

2. Under **Add security for your chat widget**, we recommend choosing **Yes**, and working with your website administrator to set up your web servers to issue JSON Web Tokens (JWTs) for new chat requests. This provides you more control when initiating new chats, including the ability to verify that chat requests sent to Amazon Connect are from authenticated users.



2 Add security for new chat requests

We recommend using JSON web tokens to secure new chat requests. This provides you more control when initiating new chats, including the ability to verify that chat requests sent to Amazon Connect are from authenticated users. This implementation is typically completed by a website administrator. Learn how to set this up. Would you prefer to do this?

● Yes

○ No - I will skip this step

Choosing **Yes** results in the following:

- Amazon Connect provides a 44-character security key on the next page that you can use to create JWTs.
- Amazon Connect adds a callback function within the chat widget embed script that checks for a JWT when a chat is initiated.

  You must implement the callback function in the embedded snippet, as shown in the following example.

```
amazon_connect('authenticate', function(callback) {
  window.fetch('/token').then(res => {
    res.json().then(data => {
      callback(data.data);
    });
  });
});
```

If you choose this option, in the next step you'll get a security key for all chat requests initiated on your websites. Ask your website administrator to set up your web servers to issue JWTs using this security key.

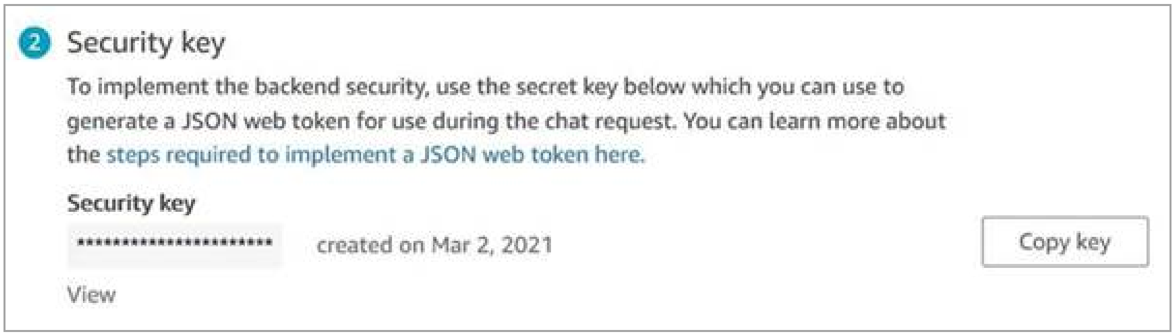
3. Choose **Save**.

Step 3: Confirm and copy chat widget code and security keys

In this step, you confirm your selections and copy the code for the chat widget and embed it in your website. If you chose to use JWTs in Step 2 (p. 246), you can also copy the secret keys for creating them.

Security key

Use this 44-character security key to generate JSON web tokens from your web server. You can also update, or rotate, keys if you need to change them. When you do this, Amazon Connect provides you with a new key and maintains the previous key until you have a chance to replace it. After you have the new key deployed, you can come back to Amazon Connect and delete the previous key.


2 Security key

To implement the backend security, use the secret key below which you can use to generate a JSON web token for use during the chat request. You can learn more about the steps required to implement a JSON web token here.

Security key

********************** created on Mar 2, 2021

When your customers interact with the start chat icon on your website, the chat widget requests your web server for a JWT. When this JWT is provided, the widget will then include it as part of the end customer's chat request to Amazon Connect. Amazon Connect then uses the secret key to decrypt the token. If successful, this confirms that the JWT was issued by your web server and Amazon Connect routes the chat request to your contact center agents.

JSON Web Token specifics

- Algorithm: **HS256**
- Claims:
  - **sub**: *`widgetId`*

    Replace `widgetId` with your own widgetId. To find your widgetId, see the example Chat widget script (p. 249).
  - **iat**: *Issued At Time.
  - **exp**: *Expiration (10 minute maximum).

  * For information about the date format, see the following Internet Engineering Task Force (IETF) document: JSON Web Token (JWT), page 5.

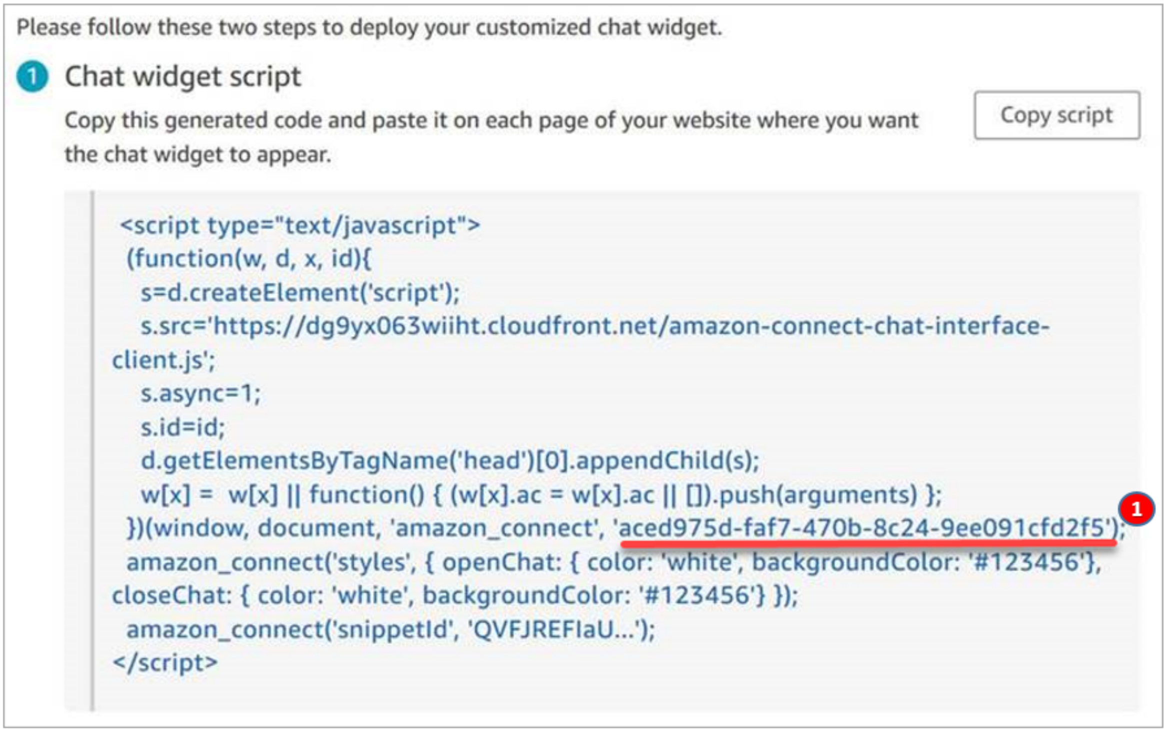
The following code snippet shows an example of how to generate a JWT in Python:

```
payload = {
```

```
'sub': widgetId, // don't add single quotes, such as 'widgetId'
'iat': datetime.utcnow(),
'exp': datetime.utcnow() + timedelta(seconds=JWT_EXP_DELTA_SECONDS)
}

header = {
'typ': "JWT",
'alg': 'HS256'
}

encoded_token = jwt.encode((payload), CONNECT_SECRET, algorithm=JWT_ALGORITHM,
 headers=header) // CONNECT_SECRET is the security key provided by Amazon Connect
```

Chat widget script

The following image shows an example of the JavaScript that you embed on the websites where you want customers to chat with agents. This script displays the widget in the bottom-right corner of your website.



Please follow these two steps to deploy your customized chat widget.

1 Chat widget script

Copy this generated code and paste it on each page of your website where you want the chat widget to appear.

```
 <script type="text/javascript">
  (function(w, d, x, id){
    s=d.createElement('script');
    s.src='https://dg9yx063wiiht.cloudfront.net/amazon-connect-chat-interface-
client.js';
    s.async=1;
    s.id=id;
    d.getElementsByTagName('head')[0].appendChild(s);
    w[x] =  w[x] || function() { (w[x].ac = w[x].ac || []).push(arguments) };
  })(window, document, 'amazon_connect', 'aced975d-faf7-470b-8c24-9ee091cfd2f5');
  amazon_connect('styles', { openChat: { color: 'white', backgroundColor: '#123456'},
closeChat: { color: 'white', backgroundColor: '#123456'} });
  amazon_connect('snippetId', 'QVFJREFIaU...');
</script>
```

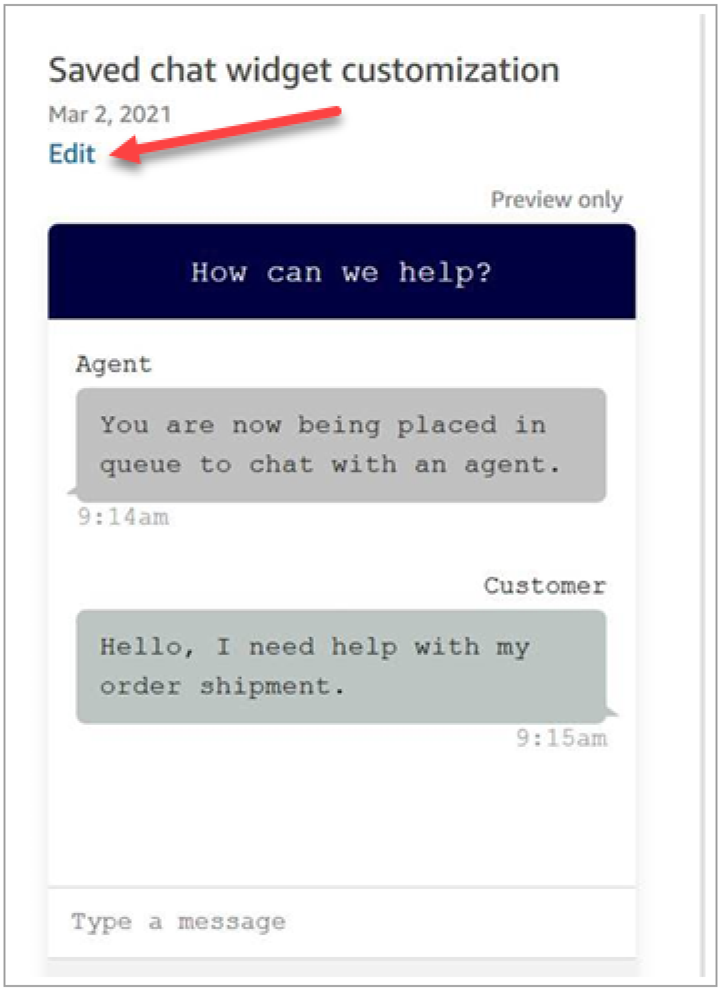
1. An example of where to find your widgetId.

When your website loads, customers first see the **Start Chat** icon. When they choose this icon, the chat widget opens and customers are able to send a message to your agents.

To make changes to the chat widget at any time, choose **Edit**.

Note

Saved changes update the customer experience in a few minutes. Confirm your widget configuration before saving it.



Saved chat widget customization

Mar 2, 2021

Edit

Preview only

How can we help?

Agent

You are now being placed in queue to chat with an agent.

9:14am

Customer

Hello, I need help with my order shipment.

9:15am

Type a message

To make changes to widget icons on the website, you will receive a new code snippet to update your website directly.

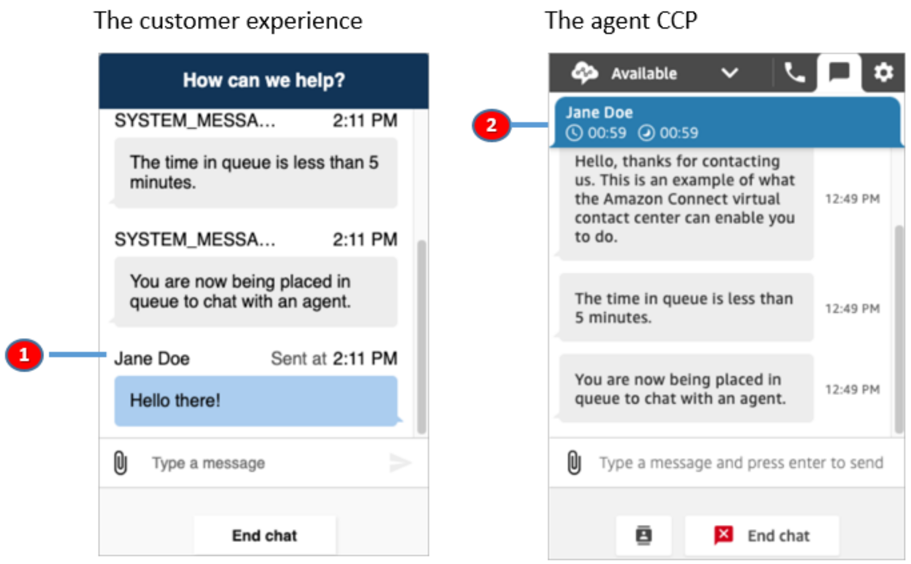
More customizations for your chat widget

See the following topics for more you can do to customize the chat experience:

- Pass the customer display name when a chat initializes (p. 250)
- Pass contact attributes when a chat initializes (p. 252)

Pass the customer display name when a chat initializes

To deliver a more personalized experience for both your customers and agents, you can customize the Amazon Connect chat widget to pass the customer display name during contact initialization. The name is visible to both the customer and agent throughout the chat interaction. This display name is recorded in the chat transcript.


The customer experience

The agent CCP

SYSTEM_MESSA... 2:11 PM

The time in queue is less than 5 minutes.

SYSTEM_MESSA... 2:11 PM

You are now being placed in queue to chat with an agent.

Jane Doe Sent at 2:11 PM

Hello there!

Jane Doe
00:59 00:59

Hello, thanks for contacting us. This is an example of what the Amazon Connect virtual contact center can enable you to do. 12:49 PM

The time in queue is less than 5 minutes. 12:49 PM

You are now being placed in queue to chat with an agent. 12:49 PM

1. How the customer display name may appear to the customer using the chat user interface.
2. How the customer display name may appear to the agent using the CCP.

How to pass a customer display name in the chat widget

To pass a customer display name, implement your callback function in the snippet. Amazon Connect retrieves the display name automatically.

1. Complete the steps in Add a chat user interface to your website (p. 244), if you haven't already.
2. Augment your existing widget snippet to add a `customerDisplayName` callback. It might look something like the following example:

```
amazon_connect('customerDisplayName', function(callback) {
  const displayName = 'Jane Doe';
  callback(displayName);
});
```

   The important thing is that the name is passed to `callback(name)`.

Things you need to know

- Only one `customerDisplayName` function can exist at a time.
- The customer display name must follow the limitations set by the StartChatConnect API. That is, the name must be a string between 1 and 256 characters.
- An empty string, null, or undefined is invalid input for the display name. To protect against accidentally passing of these inputs, the widget logs an error, `Invalid customerDisplayName provided`, in the browser console, and then starts the chat with the default display name, **Customer**.
- Because the snippet is in the front end of your website, do not pass sensitive data as the display name. Be sure to follow the appropriate security practices to keep your data safe and protect against attacks and bad actors.

Pass contact attributes when a chat initializes

You can use contact attributes (p. 515) to capture information about the contact who is using the chat widget. Then, you can display that information to the agent through the Contact Control Panel (CCP), or use it elsewhere in the flow.

For example, you can customize your contact flow to say the name of the customer in your welcome message. Or, you can use attributes specific to your business, such as account/member IDs, customer identifiers like names and emails, or other metadata associated with a contact.

How to pass contact attributes into the chat widget

1. Enable security in the chat widget as described in Add a chat user interface to your website (p. 244), if you haven't already:

   a. In Step 2, under **Add security for your chat widget**, choose **Yes**.

   b. In Step 3, use the security key to generate JSON web tokens.

2. Add the contact attributes to the payload of your JWT as an `attributes` claim.

   Following is an example of how you might generate a JWT with contact attributes in Python:

```
import jwt

CONNECT_SECRET = "your-securely-stored-jwt-secret"

payload = {
  'sub': 'widget-id',
  'iat': datetime.datetime.utcnow(),
  'exp': datetime.datetime.utcnow() + datetime.timedelta(seconds=500),
  'attributes': {"name": "Jane", "memberID": "123456789", "email": "Jane@example.com",
 "isPremiumUser": "true", "age": "45"}
}

header = {
  'typ': "JWT",
  'alg': 'HS256'
}

encoded_token = jwt.encode((payload), CONNECT_SECRET, algorithm="HS256",
 headers=header)
});
```

   In the payload, you must create a string key `attributes` (as-is, all lowercase), with an object as its value. That object must have string-to-string key-value pairs. If anything other than a string is passed in any one of the attributes, the chat will fail to start.

   The contact attributes must follow the limitations set by the StartChatConnect API:

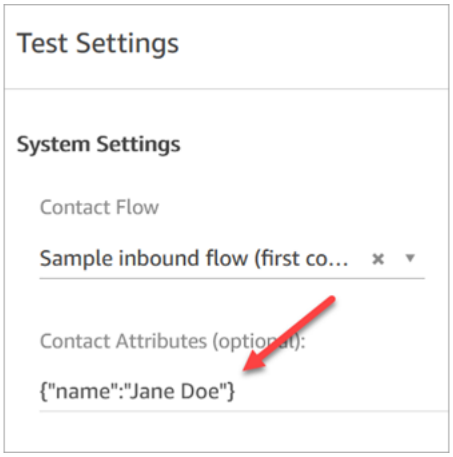
   - Keys must have a minimum length of 1
   - Values can have a minimum length of 0

Things you need to know

- The chat widget has a 6144 bytes limit for the entire encoded token. Because JavaScript uses UTF-16 encoding, 2 bytes are used per character, so the maximum size of the `encoded_token` should be around 3000 characters.
- The encoded_token should be passed in to `callback(data)`. The `authenticate` snippet does not need any additional changes. For example:

```
amazon_connect('authenticate', function(callback) {
  window.fetch('/token').then(res => {
    res.json().then(data => {
      callback(data.data);
    });
  });
});
```

- Using a JWT to pass contact attributes ensures the integrity of the data. If you safeguard the shared secret and follow appropriate security practices, you can help ensure that the data cannot be manipulated by a bad actor.
- Contact attributes are only encoded in the JWT, not encrypted, so it's possible to decode and read the attributes. Sensitive data should not be passed in the token.
- If you want to test the chat experience with the simulated chat experience (p. 148) and include contact attributes, be sure to enclose both the key and value in quotes, as shown in the following image:



Test Settings

System Settings

Contact Flow

Sample inbound flow (first co... × ▾

Contact Attributes (optional):

{"name":"Jane Doe"}

Download and customize our open source example

You can further customize the chat experience customers use to interact with agents. Use the Amazon Connect open source library on GitHub. It's a platform to help you get started quickly. Here's how it works:

- The GitHub repository links to a CloudFormation template, which starts the Amazon API Gateway endpoint that initiates a Lambda function. You can use this template as an example.
- After you create the AWS CloudFormation stack, you can call this API from your app, import the pre-built chat widget, pass the response to the widget, and start chatting.

For more information about customizing the chat experience, see:

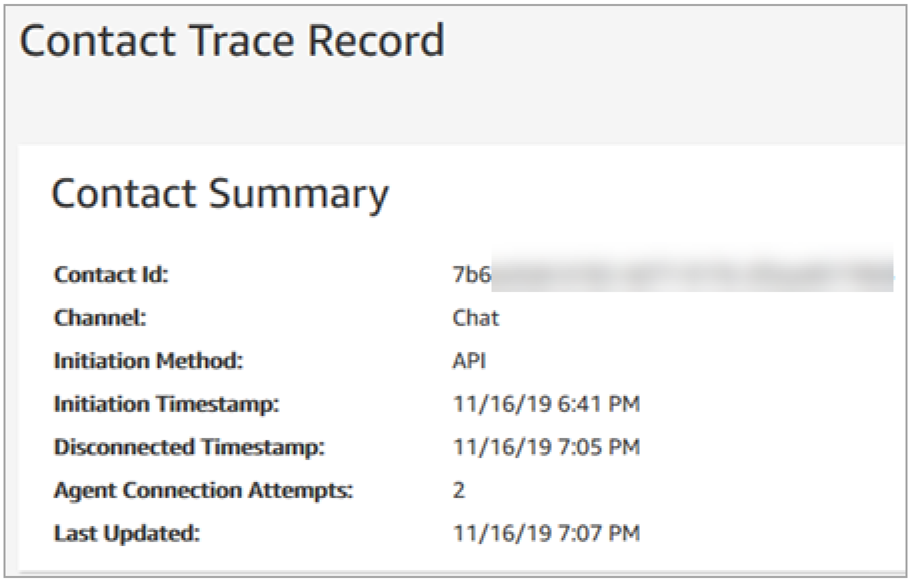
- Amazon Connect Service API Documentation, especially the StartChatConnect API.
- Amazon Connect Participant Service API.
- Amazon Connect Streams. Use to integrate your existing apps with Amazon Connect. You can embed the Contact Control Panel (CCP) components into your app.
- Amazon Connect Chat SDK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

Start chats using your own applications

You can use Amazon Connect APIs to start chats in your own applications.

The StartChatConnect API is used to start the chat.

When you explore the chat experience for the first time, you'll notice that chats aren't counted in the **Contacts Incoming** metric in your historical metrics report. This is because the initiation method for the chat in the contact record is **API**.



Contact Trace Record

Contact Summary

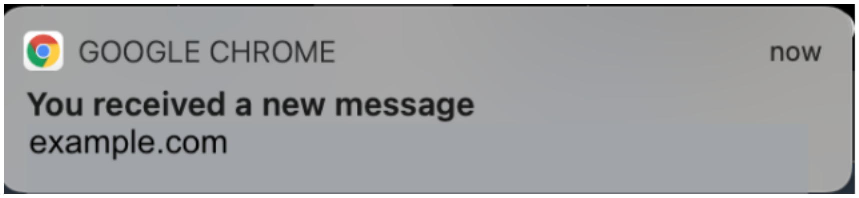
Contact Id:	7b6[redacted]
Channel:	Chat
Initiation Method:	API
Initiation Timestamp:	11/16/19 6:41 PM
Disconnected Timestamp:	11/16/19 7:05 PM
Agent Connection Attempts:	2
Last Updated:	11/16/19 7:07 PM

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

Browser notifications

The chat widget supports browser notifications for your customers through their desktop devices. Specifically, your customers will receive a notification through their web browser when they receive a new message, but are not active on the webpage that contains the chat window. When your customers click or tap this notification, they are automatically redirected to the webpage containing the chat window. Your customers can enable or disable notifications at the start of each chat conversation.

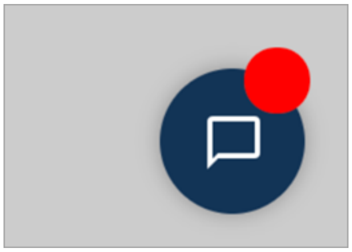
The following image shows an example of the notification banner that customers receive when they are not on the webpage that contains the chat window. The banner tells your customers that they have a new message, and it displays the name of the website.



GOOGLE CHROME now

You received a new message
example.com

Customers also receive a notification icon—a red dot—on the chat widget when it is minimized. The following image shows an image of the notification icon that customers receive when their chat window is minimized.



Both of these features are automatically included in the chat widget. You don't need to perform any steps to make them available to your customers.

Your customers receive a pop-up to allow/deny notification when they initiate a chat and have not yet allowed notifications from your website or domain. After they grant notification permissions, they start receiving browser notifications for any message or attachment sent by the agent when they are not on the webpage with the chat window. This behavior applies even if you've already implemented the chat widget.

How to test

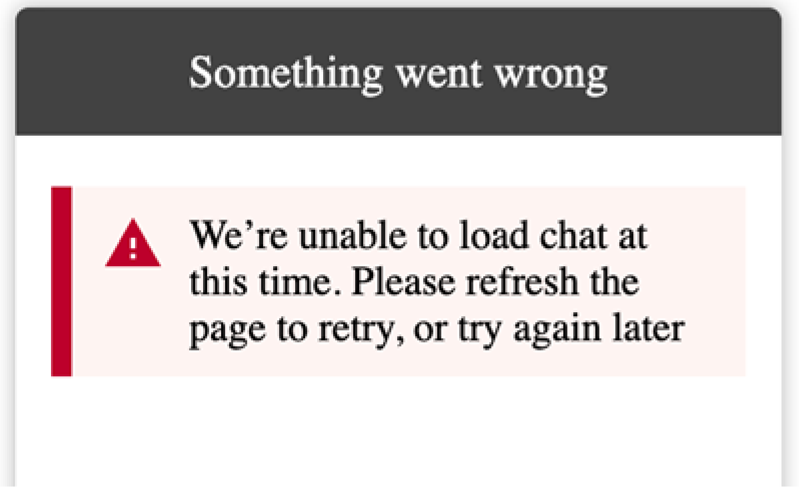
1. After you allow notifications as a test customer and the agent is connected to the chat, minimize your chat window and then open a new browser instance so you aren't on the webpage that contains the chat window.
2. Send a message from the agent window.
3. As the test customer, you'll see the notification banner.
4. Choose or tap the notification banner. You'll automatically go to the webpage that contains the chat window.
5. Because you minimized your chat window earlier, you will also see a notification icon—a red dot—on the chat widget.

If you can't see the browser notification, check the following:

- You're using a supported browser (p. 244).
- The notification permission is allowed/enabled on your browser for the webpage with chat window.
- The agent (or you from your agent chat session) has sent a new message/attachment while you're on a webpage that is different from the one that contains the chat window. For the notification icon—a red dot—on the widget to be visible, minimize your chat window.
- Notifications from the browser are not snoozed (temporarily dismissed).

Troubleshooting issues with your chat widget

If you see the following **Something went wrong** error message when loading your chat widget, open the browser tools to view the error logs.



Something went wrong

We're unable to load chat at this time. Please refresh the page to retry, or try again later

Following are common issues that cause this error.

400 Invalid request

If the logs mention a 400 invalid request, there are a few possible causes:

- Your chat widget is not being served on an allowed domain. You must specifically state the domains where you will host your widget.
- The request to the endpoint is not properly formatted. This usually occurs only if the contents of the embed snippet have been modified.

401 Unauthorized

If the logs mention a 401 unauthorized, this is a problem with the JSON Web Token (JWT) authentication. If you opt your chat widget into JWT authentication (p. 248), you must implement the callback function in the embedded snippet, as shown in the following example.

```
amazon_connect('authenticate', function(callback) {
  window.fetch('/token').then(res => {
    res.json().then(data => {
      callback(data.data);
    });
  });
});
```

If you have implemented the callback already, the following scenarios may still cause a 401:

- Invalid signature
- Expired token

404 Not found

A 404 status code indicates that your `widgetId` cannot be found. Verify that your snippet is exactly how it was copied from the Amazon Connect website, and none of the identifiers have changed.

If the identifiers have not changed and you are seeing a 404, contact AWS Support.

500 Internal server error

This can be caused by your service-linked role not having the required permissions to start chat. This happens if your Amazon Connect instance was created before October 2018 because you don't have service-linked roles set up.

Solution: Add the `connect:*` policy on the role that is associated with your Amazon Connect instance. For more information, see Use service-linked roles for Amazon Connect (p. 1120).

If your service-linked role has the correct permissions, contact AWS Support.

Enable text formatting for your customer's chat experience

With Amazon Connect message formatting, you can enable your customers and agents to quickly add structure and clarity to their chat messages.

You can provide the following types of formatting on both the chat user interface and the agent application using markdown:

- Bold
- Italic
- Bulleted list
- Numbered list
- Hyperlinks
- Attachments. To enable attachments, follow Enable attachments to share files using chat (p. 142).

How to enable message formatting

1. When you create a new chat user interface (p. 244), rich text formatting is enabled out of the box. No additional configuration is required.
2. To add text formatting capabilities to an existing chat user interface (p. 244), update the chat widget code (p. 244) with the following code that is highlighted in bold:

   ```
       (function(w, d, x, id){
           s=d.createElement('script');
           s.src='https://d3xxxx.cloudfront.net/amazon-connect-chat-interface-client.js';
           s.async=1;
           s.id=id;
           d.getElementsByTagName('head')[0].appendChild(s);
           w[x] =  w[x] || function() { (w[x].ac = w[x].ac || []).push(arguments) };
       })(window, document, 'amazon_connect', 'widget-id');
       amazon_connect('styles', { openChat: { color: 'white', backgroundColor: '#123456'},
    closeChat: { color: 'white', backgroundColor: '#123456'} });
       amazon_connect('snippetId', 'snippet-id');
       amazon_connect('supportedMessagingContentTypes', [ 'text/plain', 'text/
   markdown' ]);
   ```

   The code that is highlighted in red is set to the correct values when you get the snippet from the Amazon Connect console. The only content you choose to add or remove is the last line in bold for `supportedMessagingContentTypes`.
3. To add text formatting capabilities to your own custom chat user interface (for example, Chat Interface or your own UI solution on top of ChatJS), follow these steps:

a. Call the StartChatContact API. When calling `StartChatContact`, add the `SupportedMessagingContentTypes` parameter as shown in bold in the following example:

```
// Amazon Connect StartChatContact API
{
    "Attributes": {
        "string" : "string"
    },
    "ClientToken": "string",
    "ContactFlowId": "your contact flow ID",
    "InitialMessage": {
        "Content": "string",
        "ContentType": "string"
    },
    "InstanceId": "your instance ID",
    "ParticipantDetails": {
        "DisplayName": "string"
    }

    // optional
   "SupportedMessagingContentTypes": [ "text/plain", "text/markdown" ]
}
```

b. Import `chatjs` as an object, as shown in the following example:

```
import "amazon-connect-chatjs";

this.session = connect.ChatSession.create({
      ...
    });

this.session.sendMessage({
      message: "message-in-markdown-format",
      contentType: "text/markdown"
});
```

If you don't use ChatJs, see these topics for information about sending markdown text through Amazon Connect APIs: StartChatContact and SendMessage.

c. Send messages with markdown. See the previous code snippet for importing `chatjs` as an object for an example of how to send messages. You can use simple markdown for formatting text in chats. If you're already using chatjs today to send plaintext messages you can modify your existing logic to call SendMessage with `text/markdown` as `contentType` instead of `text/plain` when you want to send markdown messages. Be sure to update the `sendMessage` parameter to have the markdown format of your messages. For more information, see Markdown Guide Basic Syntax.

d. Implement your own logic in the UI package to render markdown messages in the input area and chat transcript. If you use React, you can use react-markdown as a reference.

Note

Text formatting capabilities appear to your agent only if the feature has been enabled for your customer in the chat user interface. If text formatting is not supported or enabled on the customer chat user interface, the agent will not have the ability to compose and send messages with text formatting.

Enable Apple Messages for Business

Your customers can engage directly with your contact center from within their Messages application on their iPhone, iPad, and Mac.

When you enable Apple Messages for Business, your customers can find answers to their questions and request help from agents to resolve issues — all while using the familiar Messages application they use every day to chat with friends and family. Any time customers use Search, Safari, Spotlight, Siri, or Maps to call your registered phone number, they will be provided with the option to chat with your contact center.

Apple Messages for Business integration with Amazon Connect enables you to use the same configuration, analytics, routing, and agent UI that you already use for Amazon Connect Chat (p. 13).

Step 1: Register with Apple

Integrate Apple Messages for Business with Amazon Connect by first registering with Apple as a brand. When you do, you'll get a unique Apple Messages for Business Account ID, and you can then link your Apple Messages for Business account to Amazon Connect.

1. Go to the Apple Messages for Business page. In the box that says **As a business, I want to connect with my customers in the Messages app**, choose **Get Started**.
2. Create an Apple ID for your business, if you don't already have one.

   An Apple ID is typically for the personal use of Apple services, such as storing personal content in iCloud and downloading apps from the App Store. If you have a personal Apple ID, we recommend that you create a separate one using your organization's email address to administer Messages for Business. A separate administrative Apple ID lets you distinguish Messages for Business communications from personal Apple communications.
3. Register a profile for a new Messages for Business account by accepting **Apple's Terms of Service**. We recommend creating a Commercial Messages for Business Account. You then provide business details, such as a logo and support hours.
4. Select Amazon Connect as your Messaging Service Provider. You can do this by selecting Amazon Connect from the drop-down or by entering the following URL:

   - **https://messagingintegrations.connect.amazonaws.com/applebusinesschat**

After you submit your application to Apple, you'll see the status of your application at the top of your **Messages for Business Account** page.

For more information about registering with Apple, see the following articles on Apple's website: Getting Started with Messages for Business and Messages for Business Policies and Best Practices.

Step 2: Gather required information

Gather the following information so you have it on hand when you open a support ticket in Step 3:

1. **Apple Messages for Business Account ID**: After you've been approved by Apple Messages for Business, you will be issued an Apple Messages for Business Account ID. For information about locating your Apple Messages for Business Account ID, see Find your Apple Messages for Business Account ID (p. 268).

   > **Note**
   > Your Apple Messages for Business Account ID is a randomized string of numbers and letters. It is not the same as your Apple ID.

2. **Apple Token**: This is a unique ID that authenticates your account. For help locating your Apple token, see Find your Apple token (p. 270).
3. **Amazon Connect instance ARN**: This is the identifier for the instance you want to link to your Apple business account. For information about locating your instance ID, see Find your Amazon Connect instance ID/ARN (p. 139).

   Note

   Make sure you have service-linked roles enabled for the integration.
   If your instance was created before **October 2018**, add the `connect:*` policy on the role that is associated with your Amazon Connect instance. For more information about service-linked roles, see Use service-linked roles for Amazon Connect (p. 1120).
4. **Amazon Connect contact flow ID**: This is the identifier for the contact flow you want to use for inbound chats. For information about locating your contact flow ID, see Find the contact flow ID (p. 270).

Step 3: Link your Apple Messages for Business ID to Amazon Connect

In this step you create an Amazon Connect support ticket to link your Apple Messages for Business ID to Amazon Connect.

1. Create a special AWS Support ticket to link your Apple Messages for Business to Amazon Connect.

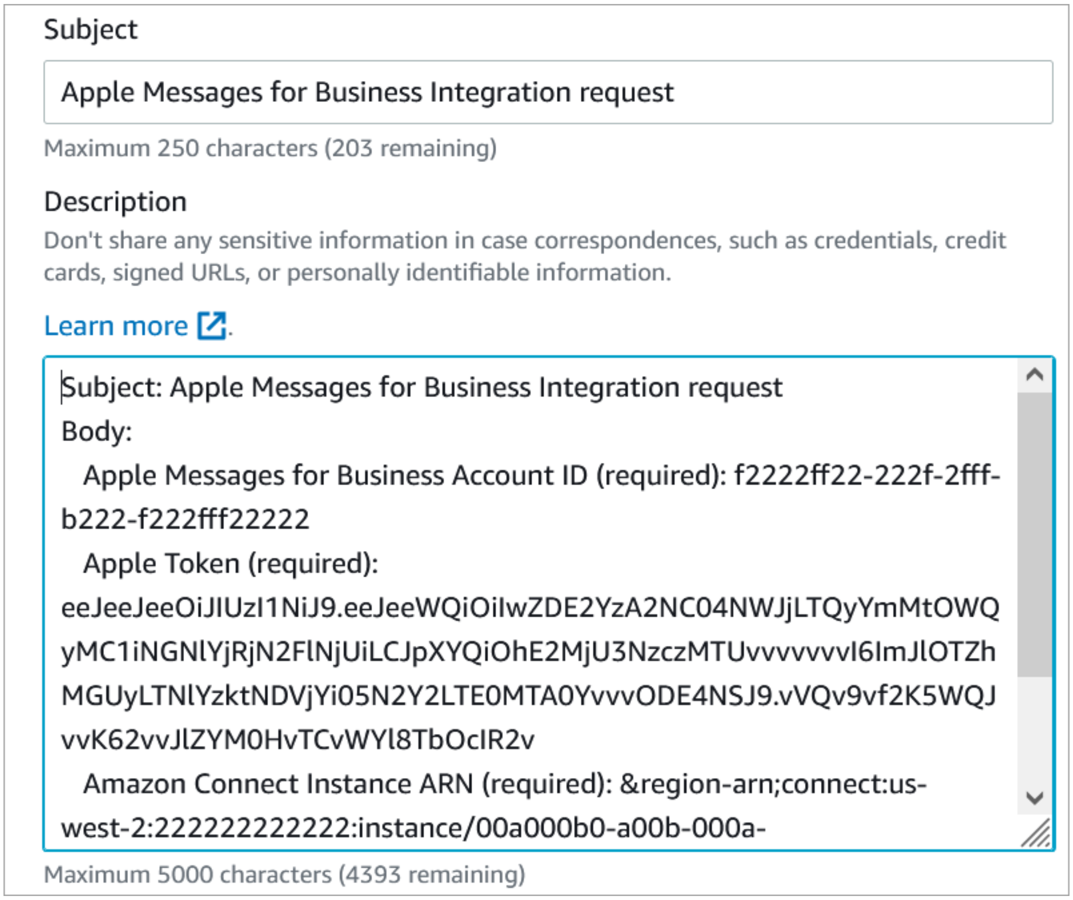
   If prompted, login using your AWS account.

   Tip

   Looking for technical support? Open an AWS Support ticket here.
2. Choose **Account and billing**.
3. Use the dropdown box to choose **Account**. For **Category** choose **Activation**, and then choose **Next step: Additional information**.
4. For **Subject** enter **Apple Messages for Business Integration request**.
5. In the **Description** box, copy and paste the following template:

```
Subject: Apple Messages for Business Integration request
   Body:

   Apple Messages for Business Account ID (required): enter your account ID
   Apple Token (required): enter your Apple token
   Amazon Connect Instance ARN (required): enter your instance ARN
   Amazon Connect Contact Flow ID (required): enter your contact flow ID
```

   The following image shows an example of a completed ticket:



Subject

Apple Messages for Business Integration request

Maximum 250 characters (203 remaining)

Description

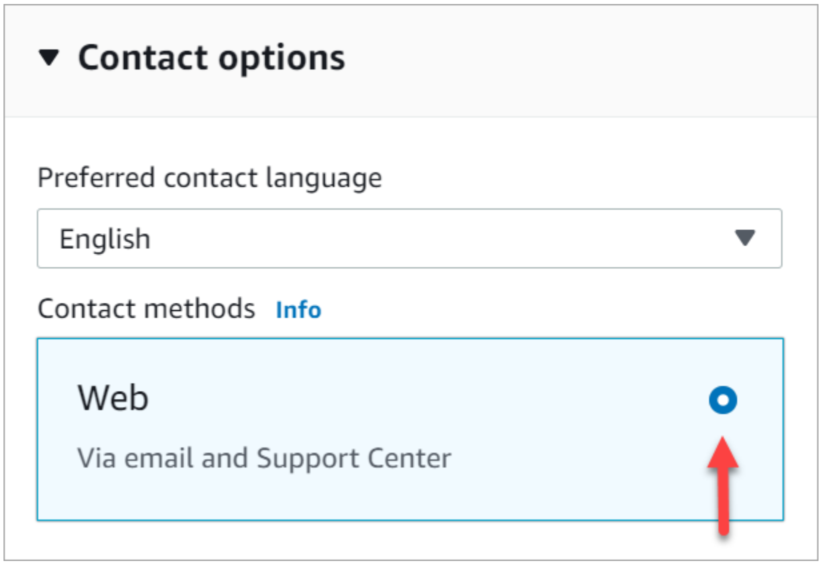
Don't share any sensitive information in case correspondences, such as credentials, credit cards, signed URLs, or personally identifiable information.

Learn more.

```
Subject: Apple Messages for Business Integration request
Body:
  Apple Messages for Business Account ID (required): f2222ff22-222f-2fff-b222-f222fff22222
  Apple Token (required):
eeJeeJeeOiJIUzI1NiJ9.eeJeeWQiOilwZDE2YzA2NC04NWJjLTQyYmMtOWQyMC1iNGNlYjRjN2FlNjUiLCJpXYQiOhE2MjU3NzczMTUvvvvvvvI6ImJlOTZhMGUyLTNlYzktNDVjYi05N2Y2LTE0MTA0YvvvODE4NSJ9.vVQv9vf2K5WQJvvK62vvJlZYM0HvTCvWYl8TbOcIR2v
  Amazon Connect Instance ARN (required): &region-arn;connect:us-west-2:222222222222:instance/00a000b0-a00b-000a-
```

Maximum 5000 characters (4393 remaining)

6. Choose **Next step**.
7. Choose **Contact us**, choose your **Preferred contact language**, and then choose **Web** as the contact method, if it's not selected by default.



▼ Contact options

Preferred contact language

English ▼

Contact methods Info

Web ●
Via email and Support Center

8. Choose **Submit**.
9. AWS Support will work directly with the Amazon Connect team on your request and follow up with any additional questions.

Next steps

After Apple Messages for Business is enabled for your Amazon Connect instance, you can add Apple Messages for Business features (p. 263) to your messages. For example:

- Deflect calls with Apple's Message Suggest.
- Embed Apple Messages for Business buttons on your website.
- Add list pickers and time pickers to your messages.
- Use rich links for URLs.
- Route Apple Messages for Business messages using contact attributes.

Send a test message for Apple Messages for Business

After onboarding to the Apple Messages for Business account, use the following steps to send a test message to make sure the integration is set up properly.

Step 1: Add internal testers to your Messages for Business account

1. Sign in to Apple Business Register.
2. Choose **Messages for Business Accounts** and select the account to add testers.
3. Scroll down the page to **Account Testing**.
4. Add the Apple IDs of your internal testers.
5. When your list is complete and you are ready to begin testing, choose **Send to new testers** to send an instructional email to your testers.

An instructional email containing a link to your Messages for Business conversation is sent to the Apple ID email address of each tester. If a tester does not receive the email, then recheck that their email address is provided in the Account Testing section. It's most likely that the email address is incorrect or it's not an Apple ID. For security reasons, Apple cannot verify Apple ID email addresses.

Step 2: Test sending and receiving messages

When your testers get the instructional email, they will need to activate the link in it. After doing this, they can send messages to your agents, who can then reply from the Contact Control Panel (CCP).

Note the following:

1. Design a test to trigger all of your Apple Messages for Business features.
2. You should observe that messages sent from an iOS device arrive to your test business. Employees testing from your support agent desktop should be able to respond to these test messages.
3. Your testers may notice your brand colors are not visible in the Messages header. Brand color is not available while your account is in test mode. The colors for your brand will display correctly after your account goes online.
4. If you send the testing link to someone whose email is not listed in the Account Testing section, they will not be able to send messages.
5. If you provide a Redirect Page URL and your testers try to enter Messages for Business from an unsupported device, they will land either on a default or redirected page. You can set your Redirect Page URL in the **Unsupported Devices** section at the bottom of your Messages for Business account page.

To begin testing

1. Check that your testers are using a device with a supported iOS: iOS 11.3 and later, or macOS 10.13.4.
2. Ask your testers to doing the following:

    a. Use their supported devices to find the email sent to them.

    b. Open the email from the supported device, and then choose the link. It takes them to a Messages for Business conversation in the Messages app.

Troubleshoot

If you encounter any issues when sending a test message, follow these steps:

1. Confirm that you've allowlisted your email address/Apple ID as a tester in your Messages for Business account.
2. Confirm the following settings on your Apple device:
    - Go to **Settings** > **Messages** and check that **iMessage** is enabled.
    - Go to **Settings** > **Messages** > **Send & Receive** and check that the AppleID is correct and messages are allowed to receive.
3. Check that you're using a supported iOS. Apple devices running iOS 11.3 and later or macOS 10.13.4 and later support Messages for Business.
4. When you selected Amazon Connect as your MSP in your Apple Account, did you select **Amazon Connect** from the dropdown? Or did you enter the following URL:
    - https://messagingintegrations.connect.amazonaws.com/applebusinesschat

    If you entered the URL, doublecheck for typos.

Add Apple Messages for Business features

Deflect calls with Apple's Message Suggest

With Message Suggest you can allow users to choose between voice and messaging when tapping on your business phone number in Safari, Maps, Siri, or Search.

To enable Message Suggest, send an email to the Apple Messages for Business Team at **registry@apple.com** with the following information and Apple can set up the channel for you:

- Provide all of your primary phone numbers, including high call volume phone numbers.
- Provide phone contact hours to set customer expectations for your after-hours message.
- Provide intent, group, and body parameters to associate with each phone number.
- Provide an estimate of how many customers your agents can support per day. This can be increased or decreased depending on operational capacity.

To learn more about enabling Message Suggest, see Apple's Message Suggest FAQs.

Embed Apple Messages for Business buttons

To embed Apple Messages for Business buttons on your website or mobile app, do the following:

1. Add Apple's Messages for Business JS (JavaScript) library to your webpage headers.

2. Add a `div` container to house the button.
3. Customize the banner, fallback support, and button color to meet your brand's needs.

The Messages for Business button must contain the following, at minimum:

- A class attribute to specify the type of container: banner, phone, or message. For more information, see Messages for Business Button Class and Data.
- A data-apple-business-id attribute with the business ID you received when you registered your company with Messages for Business.

For information about how you can enable these buttons, see Apple's documentation for Adding a Messages for Business Button to Your Website.

Start a chat from a URL

You can give your customers the ability to start a conversation with you from your website or an email message.

For example, customers may start a chat using a URL that you provide. When they click the URL, the system redirects them to Messages so they can send your business a text message.

You decide how and where to provide the URL. You can include it as a link in an email message, on your website, or use it as the action for a button in your app.

Use the URL **https://bcrw.apple.com/urn:biz:*`your-business-id`***, replacing *`your-business-id`* with the business ID you received from Apple after registering with Messages for Business.

Following are optional query string parameters you can include in the URL:

- `biz-intent-id`: Use to specify the intention, or purpose, of the chat.
- `biz-group-id`: Use to indicate the group, department, or individuals best qualified to handle the customer's specific question or problem.
- `body`: Use to prepopulate the message so the customer only presses **Send** to start the conversation.

For more information, see About Intent, Group, and Body Values on the Apple Documentation website.

Following is an example of what the URL might look like for a customer with a credit card question question for the billing department:

- https://bcrw.apple.com/urn:biz:22222222-dddd-4444-bbbb-777777777777?biz-intent-id=account_question&biz-group-id=billing_department&body=Order%20additional%20credit%20card.

Add list pickers and time pickers

A list picker prompts your customer to select an item, such as a product or the reason for their inquiry. A time picker prompts your customer to choose an available time slot, such as to schedule an appointment.

For information about how to set up list pickers and time pickers, see Add interactive messages to chat (p. 633).

Use rich links for URLs

Rich links show an inline preview of a URL that contains an image. Unlike normal URLs, customers can view the image immediately in a chat without choosing a "Tap to Load Preview" message.

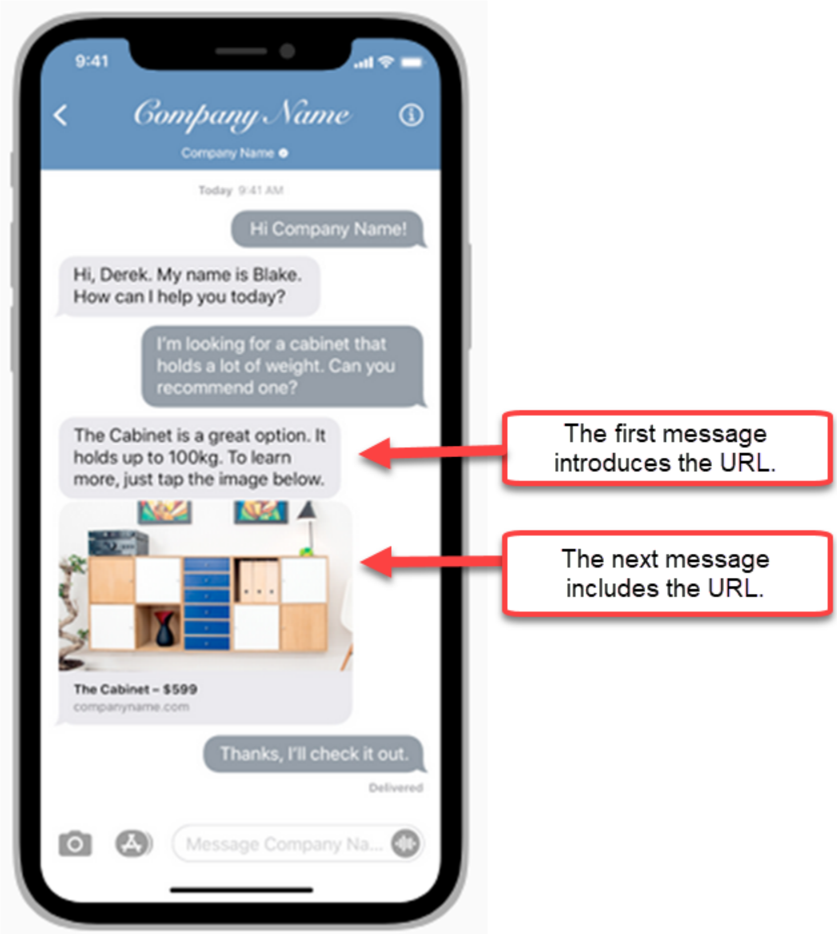
To learn more about Apple Messages for Business rich links, see Rich Links on the Apple Developer website.

Requirements for using rich links in Amazon Connect

To use rich links in Amazon Connect chat messages, your URL and images must meet the following requirements:

- Your website must use Facebook Open Graph tags. For more information, see A Guide to Sharing for Webmasters.
- The image accompanying the URL must be .jpeg, .jpg, or .png.
- The website must be HTML.

> **Note**
> When you first use the rich link feature, we recommend that you send the URL in a message separate from your chat text, as shown in the following example.



Hi Company Name!

Hi, Derek. My name is Blake. How can I help you today?

I'm looking for a cabinet that holds a lot of weight. Can you recommend one?

The Cabinet is a great option. It holds up to 100kg. To learn more, just tap the image below.

The Cabinet - $599
companyname.com

Thanks, I'll check it out.

The first message introduces the URL.

The next message includes the URL.

Use Apple Messages for Business contact attributes in contact flows

Contact attributes enable you to store temporary information about the contact so you can use it in the contact flow.

For example, if you have different lines of business using Apple Messages for Business, you can branch to different contact flows based on the **AppleBusinessChatGroup** contact attribute. Or, if you want to route

Apple Messages for Business messages differently from other chat messages, you can branch based on MessagingPlatform.

For more information about contact attributes, see Use Amazon Connect contact attributes (p. 515).

Use the following contact attributes to route Apple Messages for Business customers.

Attribute	Description	Type	JSON
MessagingPlatform	The messaging platform from where the customer request originated. Exact value: **AppleBusinessChat**	User-defined	$.Attributes.MessagingPlatform
AppleBusinessChatCustomerId	The customer's opaque ID provided by Apple. This remains constant for the AppleID and a business. You can use this to identify if the message is from a new customer or a returning customer.	User-defined	$.Attributes.AppleBusinessChatCustom
AppleBusinessChatIntent	You can define the intent or purpose of the chat. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the **Business Chat** button.	User-defined	$.Attributes.AppleBusinessChatIntent
AppleBusinessChatGroup	You define the group which designates the department or individuals best qualified to handle the customer's particular question or problem. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the **Business Chat** button.	User-defined	$.Attributes.AppleBusinessChatGroup
AppleBusinessChatLocale	Defines the language and AWS Region preferences that the user wants to see in their user interface. It consists of a language identifier (ISO 639-1) and a Region identifier	User-defined	$.Attributes.AppleBusinessChatLocale

Attribute	Description	Type	JSON
	(ISO 3166). For example, **en_US**.		

Update an Apple Messages for Business integration

You will need to update your Apple Messages for Business integration if you want to change the contact flow ID or other information.

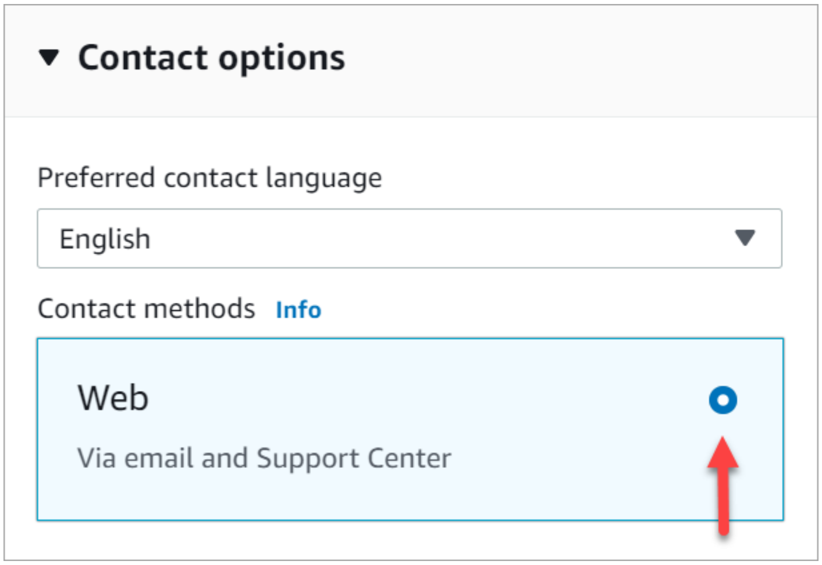
1. Open an AWS Support ticket.

   If prompted, login using your AWS account.
2. In the **Use case description** box, copy and paste the following template to indicate this is an **update** request:

```
Subject: Update Apple Messages for Business Integration request
Body:
   Apple Messages for Business Account ID (required): enter your current account ID
 change to new account ID
   Apple Token (required): enter your token
   Amazon Connect Instance ARN (required): enter your current instance ARN change
 to new instance ARN
   Amazon Connect Contact Flow ID (required): enter your current contact flow ID change
 to new contact flow ID
```

> **Note**
> If you update your Amazon Connect Instance ARN, you must also update your contact flow ID.

3. Expand **Contact options**, and then choose your **Preferred contact language**, and then choose **Web** as the contact method, if it's not selected by default.



▼ Contact options

Preferred contact language

English ▼

Contact methods Info

Web

Via email and Support Center ●

4. Choose **Submit**.
5. AWS Support will work directly with the Amazon Connect team on your request and follow up with any additional questions.

Delete an Apple Messages for Business integration

1. Open an AWS Support ticket.

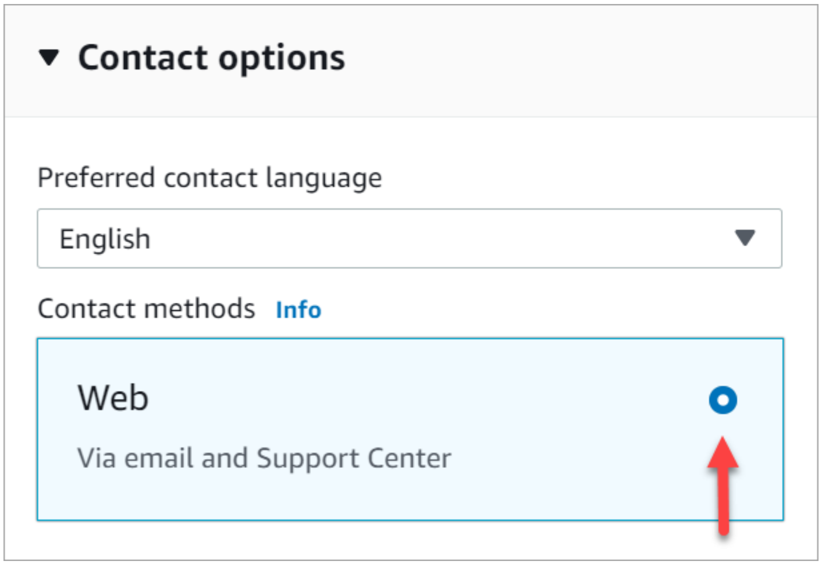
   If prompted, log in by using your AWS account.

2. In the **Use case description** box, copy and paste the following template to indicate this is an **delete** request:

```
Subject: Delete Apple Messages for Business Integration
Body:
  Apple Messages for Business Account ID (required): enter your account ID
   Amazon Connect Instance ARN (required): enter your instance ARN
   Amazon Connect Contact Flow ID (required): enter your contact flow ID
```

   The following image shows an example of a completed ticket:

3. Expand **Contact options**, and then choose your **Preferred contact language**, and then choose **Web** as the contact method, if it's not selected by default.



Contact options

Preferred contact language: English

Contact methods Info

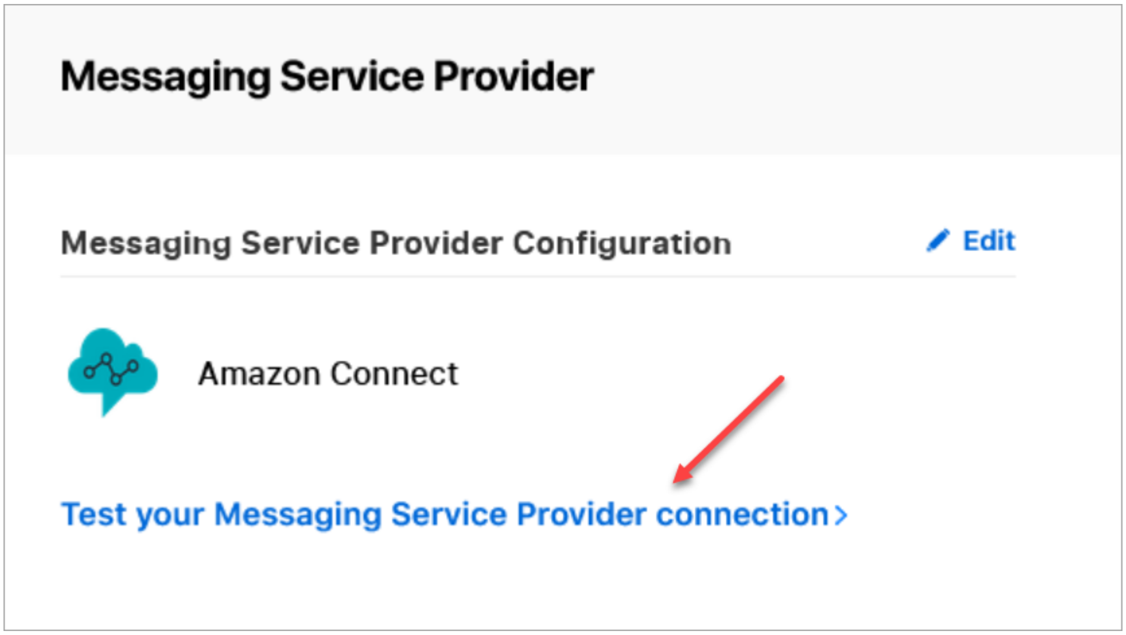
Web ● Via email and Support Center

4. Choose **Submit**.

5. AWS Support will work directly with the Amazon Connect team on your request and follow up with any additional questions.

Find your Apple Messages for Business Account ID

1. In Apple Business Register, navigate to **Message Service Provider** and click or tap **Test your Messaging Service Provider connection**.

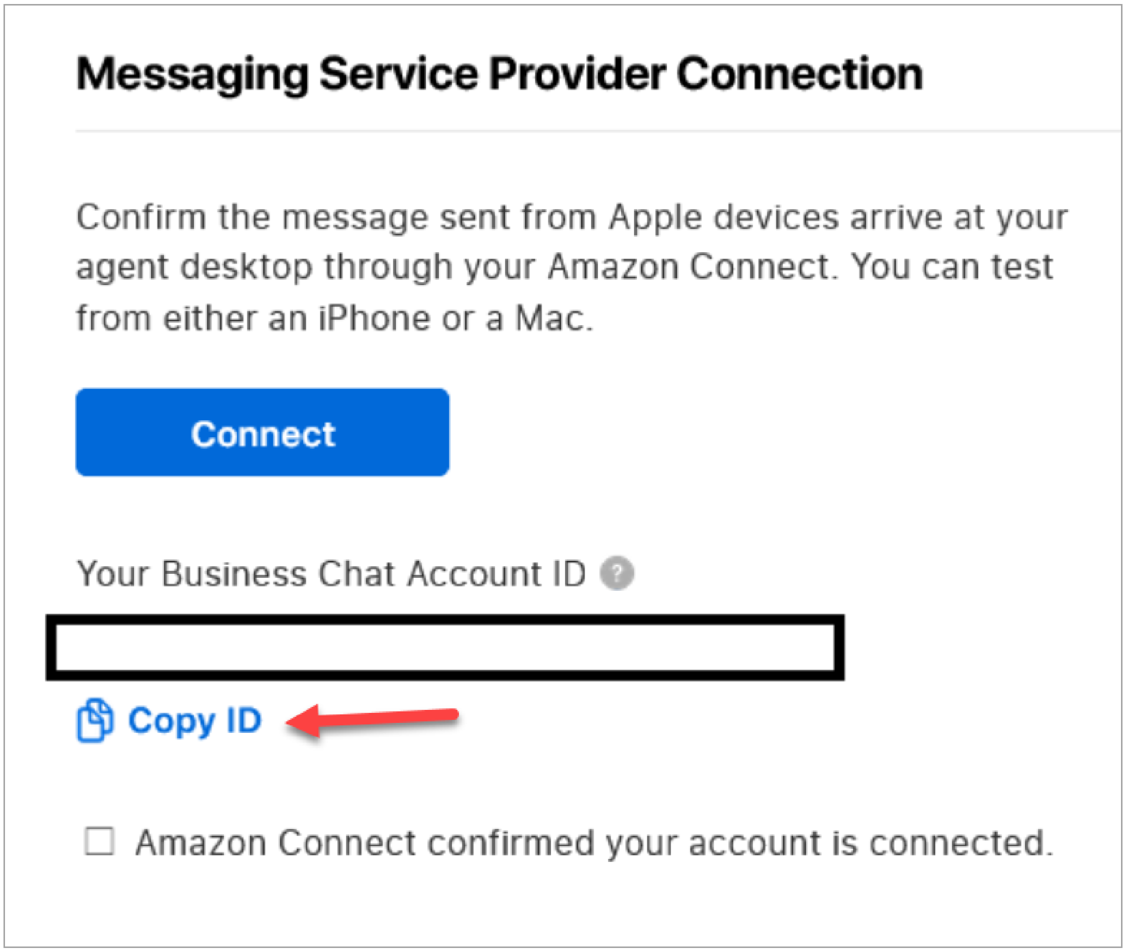


Messaging Service Provider

Messaging Service Provider Configuration

Amazon Connect

2. Click or tap **Copy ID**.



Messaging Service Provider Connection

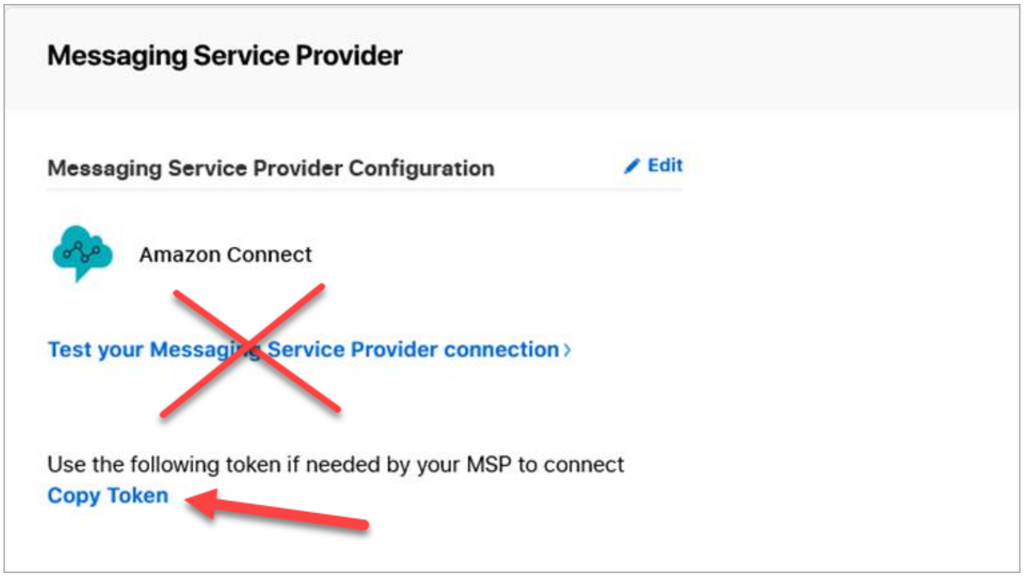
Confirm the message sent from Apple devices arrive at your agent desktop through your Amazon Connect. You can test from either an iPhone or a Mac.

Your Business Chat Account ID

□ Amazon Connect confirmed your account is connected.

Find your Apple token

- In Apple Business Register navigate to **Messaging Service Provider** and choose **Copy Token**.



Messaging Service Provider

Messaging Service Provider Configuration

Amazon Connect

Use the following token if needed by your MSP to connect

Find the contact flow ID

The contact flow ID is the contact flow you want to use for inbound Apple Messages for Business messages. Contact flows define the experiences for your customer when they begin a new chat.

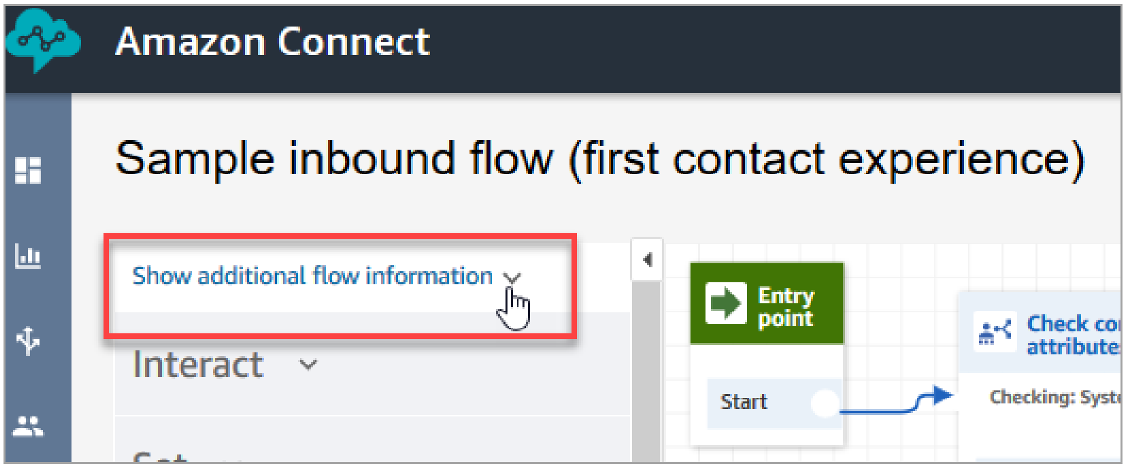
You can either reuse an existing contact flow that you're already using for voice or chat contacts, or create a new one specifically for Apple Messages for Business contacts. For instructions about creating a new inbound contact flow, see Create an inbound contact flow (p. 447).

For more information about contact flows, see Create Amazon Connect contact flows (p. 296).

To find your contact flow ID for Apple Messages for Business

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to view contact flows.
2. On the navigation menu, choose **Routing**, **Contact flows**.
3. Select the contact flow you want to use.

   Note
   Only choose flows that are type **Contact flow (inbound)**. Apple Messages for Business doesn't work with other contact flow types, such as **Customer queue**, **Customer hold**, **Customer whisper**, etc.
4. In the contact flow designer, expand **Show additional flow information**.

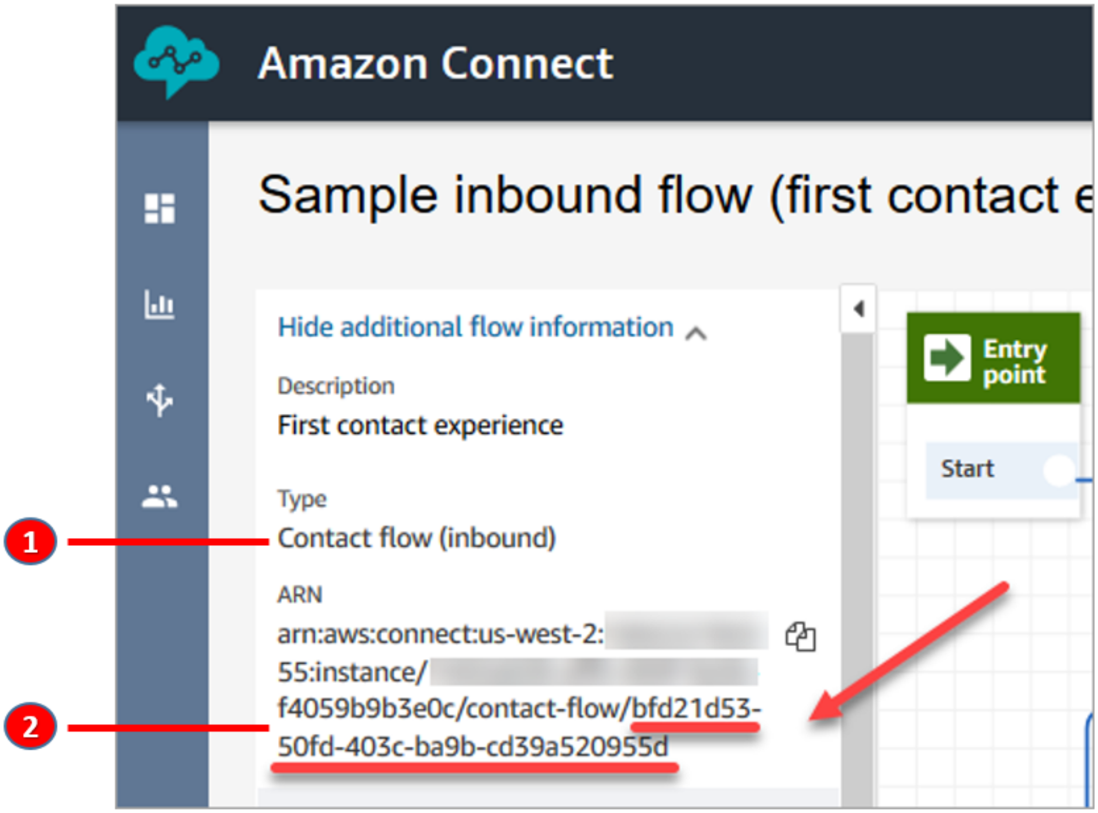


Amazon Connect

Sample inbound flow (first contact experience)

Show additional flow information

5. Under the ARN (Amazon Resource Number), copy everything after contact-flow/. For example, in the following image, you would copy the underlined part.



Amazon Connect

Sample inbound flow (first contact e

Hide additional flow information

Description
First contact experience

Type
Contact flow (inbound)

ARN
arn:aws:connect:us-west-2:[redacted]
55:instance/[redacted]
f4059b9b3e0c/contact-flow/bfd21d53-
50fd-403c-ba9b-cd39a520955d

1. Notice the **Type** = **Contact flow (Inbound)**.
2. The contact flow ID is at the end of the ARN. Only copy this end part.

Manage Apple Messages for Business chats

When you integrate Apple Messages for Business with your Amazon Connect instance, messages from Apple Messages for Business behave exactly like any other chat messages arriving to your contact center.

> **Note**
> The Amazon Connect Chat service quota limits apply to Apple Messages for Business. To learn more, see Amazon Connect service quotas (p. 1205).

Set up automatic replies

You can use Amazon Lex to set up automatic replies to chat. For a tutorial that introduces you to setting up Amazon Lex and Amazon Connect, see Add an Amazon Lex bot (p. 617).

Enable real-time chat message streaming

Amazon Connect Chat provides APIs that enable you to subscribe to a real-time stream of chat messages. Using these APIs, you can:

- Stream chat messages in real time when a new chat contact is created.
- Extend the current Amazon Connect Chat functionality to support use cases like building integrations with SMS solutions and third-party messaging applications (for example, Facebook Messenger), enabling mobile push notifications, and creating analytics dashboards to monitor and track chat message activity.

How the message streaming APIs work

The Amazon Connect message streaming APIs are triggered when certain events occur within an Amazon Connect Chat contact. For example, when a customer sends a new chat message, the event sends a payload (p. 275) to a specified endpoint containing data about the message that was just sent. Messages are published using Amazon Simple Notification Service (Amazon SNS) to a specific endpoint.

This topic describes how to set up real-time message streaming using Amazon Connect and Amazon SNS. The steps are:

1. Use the Amazon SNS console to create a new standard SNS topic and set up the messages.
2. Call the StartChatContact API to initiate the chat contact.
3. Call the StartContactStreaming API to initiate message streaming.
4. Call the CreateParticipantConnection API to create the participant's connection.

Step 1: Create a standard SNS topic

1. Go to the Amazon SNS console.
2. Create a SNS topic in your AWS account. In the **Details** section, for **Type**, choose **Standard**, enter a name for the topic, and then choose **Create topic**.

   > **Note**
   > Currently, the message streaming APIs only support standard SNS for real-time streaming of messages. They don't support Amazon SNS FIFO (first in, first out) topics.
3. After you create the topic, its Amazon Resource Name (ARN) is displayed in the **Details** section. Copy the topic ARN to the clipboard. You'll use the topic ARN in the next step, and in Step 3: Enable message streaming on the contact (p. 274).

   The topic ARN looks similar to the following example:

   ```
   arn:aws:sns:us-east-2:123456789012:MyTopic
   ```

4. Choose the **Access policy** tab, choose **Edit**, and then add a resource-based policy on the SNS topic so that Amazon Connect has permission to publish to it. Following is a sample SNS policy that you can copy and paste into the JSON editor, and then customize with your values:

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"connect.amazonaws.com"
         },
         "Action":"sns:Publish",
         "Resource":"YOUR_SNS_TOPIC_ARN",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"YOUR_AWS_ACCOUNT_ID"
            },
            "ArnEquals":{
               "aws:SourceArn":"YOUR_CONNECT_INSTANCE_ARN"
            }
         }
      }
   ]
}
```

Note

The default **Access policy** comes with conditions applied to `sourceOwner` such as:

```
"Condition": {
        "StringEquals": {
          "AWS:SourceOwner": "921772911154"
        }
      }
```

Make sure you remove it and replace with `SourceAccount`, for example:

```
"Condition":{
            "StringEquals":{
               "aws:SourceAccount":"YOUR_AWS_ACCOUNT_ID"
            },
            "ArnEquals":{
               "aws:SourceArn":"YOUR_CONNECT_INSTANCE_ARN"
            }
         }
```

This prevents a cross-service confused deputy (p. 1129) issue.

5. If you're using server-side encryption on SNS, verify you have `connect.amazonaws.com` permission enabled on the KMS key. Following is a sample policy:

```
{
        "Version": "2012-10-17",
        "Id": "key-consolepolicy-3",
        "Statement": [
            {
                "Sid": "Enable IAM User Permissions",
                "Effect": "Allow",
                "Principal": {
                    "AWS": "arn:aws:iam::your_accountId:root",
                    "Service": "connect.amazonaws.com"
                },
                "Action": "kms:*",
                "Resource": "*"
            },
            {
                "Sid": "Allow access for Key Administrators",
                "Effect": "Allow",
                "Principal": {
                    "AWS": "arn:aws:iam::your_accountId:root",
                    "Service": "connect.amazonaws.com"
                },
                "Action": [
                    "kms:Create*",
                    "kms:Describe*",
                    "kms:Enable*",
                    "kms:List*",
                    "kms:Put*",
                    "kms:Update*",
                    "kms:Revoke*",
                    "kms:Disable*",
                    "kms:Get*",
                    "kms:Delete*",
                    "kms:TagResource",
                    "kms:UntagResource",
                    "kms:ScheduleKeyDeletion",
                    "kms:CancelKeyDeletion"
                ],
                "Resource": "*"
            }
        ]
    }
```

Step 2: Initiate the chat contact

1. Call the Amazon Connect StartChatContact API to initiate the chat contact.

   For information about how to create the SDK client for calling Amazon Connect APIs, see the following topics:

   - Class AmazonConnectClientBuilder
   - Creating Service Clients

2. Keep track of `ContactId` and `ParticipantToken` from the StartChatContact response since these response attributes are used for calling other chat APIs required to enable streaming. This is described in the next steps.

Step 3: Enable message streaming on the contact

- Call StartContactStreaming to enable real-time message streaming to your SNS topic.

  - **Limits**: You can subscribe to up to two SNS topics per contact.
  - When you call StartContactStreaming, you'll need to provide the Amazon Resource Name (ARN) of the SNS topic (see Step 1: Create a standard SNS topic (p. 272)).

    A single SNS topic ARN may be used across multiple AWS accounts, but it must be in the same Region as your Amazon Connect instance. For example, if your topic ARN is in **us-east-2**, your Amazon Connect instance must be in **us-east-2**.

Step 4: Create the participant connection

- Call CreateParticipantConnection with the `ConnectParticipant` attribute passed as true.
  - You must call CreateParticipantConnection within five minutes of creating the chat.
  - Calling CreateParticipantConnection with `ConnectParticipant` set to true only works if you enabled streaming in Step 2: Initiate the chat contact (p. 274) and caller participant is `Customer`.
  - This step (creating the participant connection) is optional if you have already successfully connected to the chat contact using `WEBSOCKET`.

Next steps

You are all set for working with the message streaming APIs.

1. To verify it is working, check that messages are published to the SNS topic you created. You can do this using Amazon CloudWatch metrics. For instructions, see Monitoring Amazon SNS topics using CloudWatch.
2. Because SNS has limited retention, we recommend that you set up Amazon Simple Queue Service (Amazon SQS) Amazon Kinesis, or another service to retain messages.
3. Using StopContactStreaming is optional and not required if the chats are being disconnected (p. 362) through a contact flow, or if the customer disconnects the chat. However, `StopContactStreaming` provides the option to stop the message streaming on the SNS topic, even if the chat is active and ongoing.

Amazon SNS payload used in message streaming

After you've enabled message streaming successfully, you may need to filter the message to send it to the intended participant: agent, customer, or all.

To filter by participant, read the specific SNS headers attribute— `MessageVisibility`—to determine whether the message is intended for customer-only, agent-only, or all.

- To send to the customer only: For all code that faces the customer, clients need to filter out messages intended for the customer and build the following logic for forwarding the message to them.

```
if ( ( MessageVisibility == CUSTOMER || MessageVisibility == ALL)  && ParticipantRole !=
 CUSTOMER )
```

- To send to the agent only:

```
if ( ( MessageVisibility == AGENT || MessageVisibility == ALL)  && ParticipantRole !=
 AGENT )
```

You can also leverage the filtering capability in Amazon SNS by building custom subscription filtering policies. This offloads the message filtering logic from the SNS topic subscriber to the SNS service itself.

Message attributes in the payload

Following is a description of each message attribute in the Amazon SNS payload:

- `InitialContactId`: The initial contact ID of the chat.

- `ContactId`: The current contact ID of the chat. The `InitialContactId` and `ContactId` can differ if there has been new agent in the chat or the queue-to-queue contact flow.
- `ParticipantRole`: The participant who sent the message.
- `InstanceId`: The Amazon Connect instance ID.
- `AccountId`: The AWS account ID.
- `Type`: Possible values: `EVENT`, `MESSAGE`.
- `ContentType`: Possible values: `application/vnd.amazonaws.connect.event.typing`, `application/vnd.amazonaws.connect.event.participant.joined`, `application/vnd.amazonaws.connect.event.participant.left`, `application/vnd.amazonaws.connect.event.transfer.succeeded`, `application/vnd.amazonaws.connect.event.transfer.failed`, `application/vnd.amazonaws.connect.message.interactive`, `application/vnd.amazonaws.connect.event.chat.ended`, and more.
- `MessageVisibility`: Possible values: `AGENT`, `CUSTOMER`, `ALL`.

Example SNS payload

```
{
  "Type" : "Notification",
  "MessageId" : "ccccccccc-cccc-cccc-cccc-cccccccccccc",
  "TopicArn" : "arn:aws:sns:us-west-2:009969138378:connector-svc-test",
  "Message" :  "{\"AbsoluteTime\":\"2021-09-08T13:28:24.656Z\",\"Content\":\"help\",
\"ContentType\":\"text/plain\",\"Id\":\"333333333-be0d-4a44-889d-d2a86fc06f0c\",\"Type\":
\"MESSAGE\",\"ParticipantId\":\"bbbbbbbb-c562-4d95-b76c-dcbca8b4b5f7\",\"DisplayName\":
\"Jane\",\"ParticipantRole\":\"CUSTOMER\",\"InitialContactId\":\"33333333-abc5-46db-9ad5-
d772559ab556\",\"ContactId\":\"33333333-abc5-46db-9ad5-d772559ab556\"}",
  "Timestamp" : "2021-09-08T13:28:24.860Z",
  "SignatureVersion" : "1",
  "Signature" : "examplegggggg/1tEBYdiVDgJgBoJUniUFcArLFGfg5JCvpOr/
v6LPCHiD7A0BWy8+ZOnGTmOjBMn80U9jSzYhKbHDbQHaNYTo9sRyQA31JtHHiIseQeMfTDpcaAXqfs8hdIXq4XZaJYqDFqosfbvh56V
+tL+kk85syW/2ryjjkDYoUb+dyRGkqMy4aKA22UpfidOtdAZ/
GGtXaXSKBqazZTEUuSEzt0duLtFntQiYJanU05gtDig==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-1111111111111111111111111111111.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-west-2:000000000000:connector-svc-
test:22222222-aaaa-bbbb-cccc-333333333333",
  "MessageAttributes" : {
    "InitialContactId" : {"Type":"String","Value":"33333333-abc5-46db-9ad5-d772559ab556"},
    "MessageVisibility" : {"Type":"String","Value":"ALL"},
    "Type" : {"Type":"String","Value":"MESSAGE"},
    "AccountId" : {"Type":"String","Value":"999999999999"},
    "ContentType" : {"Type":"String","Value":"text/plain"},
    "InstanceId" : {"Type":"String","Value":"dddddddd-b64e-40c5-921b-109fd92499ae"},
    "ContactId" : {"Type":"String","Value":"33333333-abc5-46db-9ad5-d772559ab556"},
    "ParticipantRole" : {"Type":"String","Value":"CUSTOMER"}
  }
}
```

Troubleshoot issues with message streaming

Messages are not getting published to SNS

When this happens, we recommend checking the information in Step 1: Create a standard SNS topic (p. 272):

- Make sure you are using standard SNS and not Amazon SNS FIFO (first in, first out). Currently, the message streaming APIs support only standard SNS for real-time streaming of messages.

- Make sure an SNS resource-based permission is applied correctly in your account.
  - If server-side encryption is enabled, you need to give the same Amazon Connect service principal permission for encrypt and decrypt.

Contact flow doesn't start

If you're using the message streaming APIs in place of websockets, send a connection acknowledgment event; see Step 4: Create the participant connection (p. 275). This is synonymous to connecting to websocket. The contact flow begins only after that the connection acknowledgement event.

Call CreateParticipantConnection after StartContactStreaming to mark `Customer` as connected; see Step 3: Enable message streaming on the contact (p. 274). This ensures messages are sent after you have confirmed that the customer is ready to receive them.

Issue not resolved?

If after trying the previous solutions you still have issues with message streaming, contact AWS Support for help.

Amazon Connect admininstrators can choose one of the following options to contact support:

- If you have an AWS Support account, go to Support Center and submit a ticket.
- Otherwise, open the AWS Management Console and choose **Amazon Connect**, **Support**, **Create case**.

It is helpful to provide the following information:

- Your contact center instance ID/ARN. To find your instance ARN, see Find your Amazon Connect instance ID/ARN (p. 139).
- Your Region.
- A detailed description of the issue.

Upgrade to the latest CCP

The URL for the latest Contact Control Panel (CCP) ends with **ccp-v2**

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

- The URL for your CCP ends with **/ccp#** (p. 278)
- You use the Amazon Connect Streams API (p. 289). The URL associated with `initCCP()` ends with **/ccp#**

If you’re still unsure whether your using the latest CCP, go to Compare the earlier and latest CCP (p. 279) to see if your CCP looks like the latest one.

Upgrade on your own schedule, before your automatic upgrade date

To upgrade to the latest CCP before your automatic upgrade date, use the steps in the following sections:

- My CCP URL ends with /ccp# (p. 278)
- I use the Amazon Connect Streams API (p. 289)

Upgrade later, automatically

If you don't want to upgrade now, you can choose to wait until your scheduled upgrade date.

Between now and your scheduled upgrade date, we recommend the following change management steps:

- Compare how the upgraded CCP differs from the earlier one. For side-by-side visuals, see Compare the earlier and latest CCP (p. 279).
- Upgrade your CCP in a test environment. Use the latest CCP to learn how it's different, and to check your configurations.
- Communicate to your agents when the upgrade is going to take place.
- Train your agents to help them get ready.

You can see communications about your auto-upgrade date in the Personal Health Dashboard.

My CCP URL ends with /ccp#

Upgrading to the latest CCP is easy. If you want, you can try out the latest CCP and then at a later date make the switch. Here's what you do:

1. **Try it out**: Change the URL in your browser from **/ccp#** to **/ccp-v2**. The latest CCP appears automatically. If you want, change it back to /ccp# to return to the earlier CCP.
2. **Upgrade**: Change the URL in your browser from **/ccp#** to **/ccp-v2**. Bookmark the URL.
3. If you access the CCP through the Amazon Connect console by choosing the phone icon on the top right of a page, you will be re-directed according to the automatic upgrade date sent by email. Please reach out to your Amazon Solution Architect if your request is more urgent.

4. After the upgrade happens, if you use the /ccp# URL, it resolves to **/ccp-v2**.

Verify your network settings

We highly recommend setting up your network to use Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list (p. 605).

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

Update your SAML URL to ccp-v2

If you use SAML 2.0 as your identity management system, be sure to update the destination in your relay state URL to **ccp-v2**.

Change `destination=/connect/ccp` to `destination=/connect/ccp-v2`.

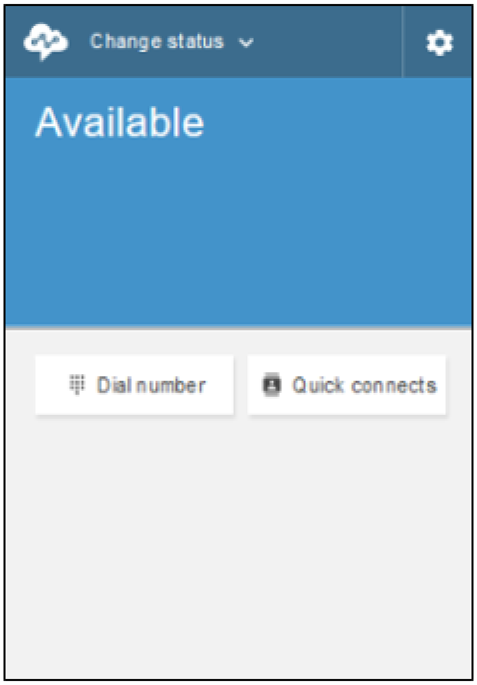
For more information, see Use a destination in your relay state URL (p. 130)

Compare the earlier and latest CCP

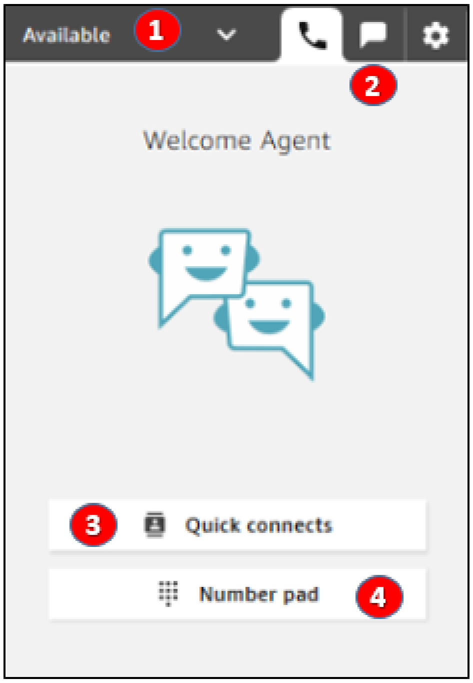
The images in this section show you how the latest CCP differs from the earlier CCP for common tasks that agents perform. The images show both CCP versions in their default state.

> **Tip**
> The chat tab appears on an agent's CCP only if their routing profile includes chat.

Set status, use chat, access quick connects and number pad



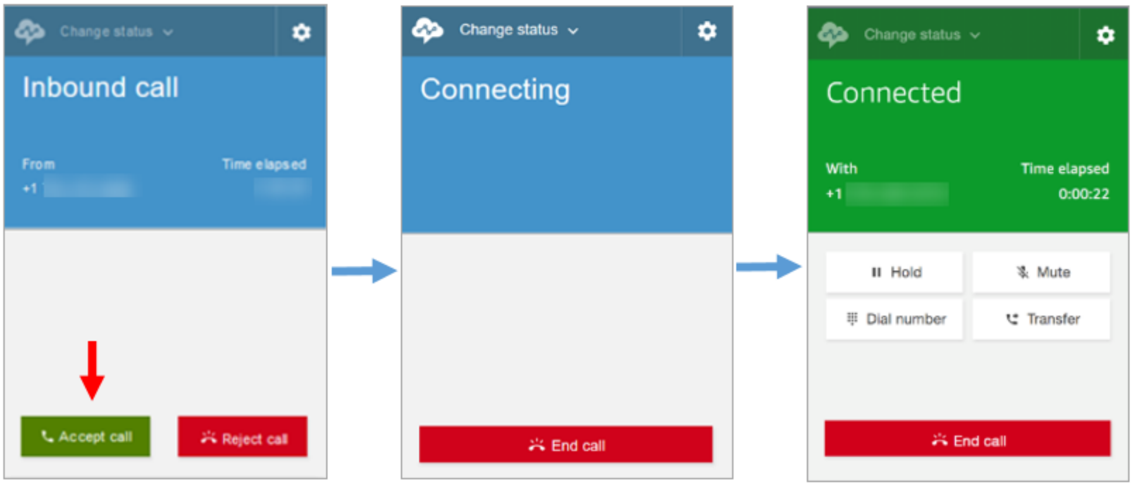
Earlier CCP



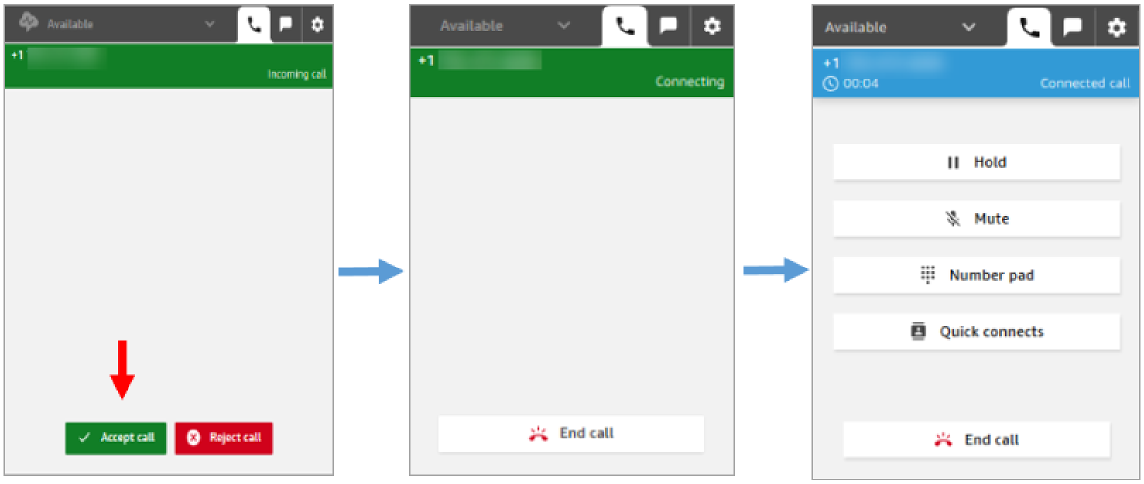
Latest CCP

1. Agents use a dropdown to set their status.
2. If you have enabled chat for the agent’s routing profile, the chat tab appears.
3. Choose the **Quick connects** button to type and call a phone number, or select a quick connect.
4. Choose the **Number pad** button to type and call a phone number. This is useful when the phone number has letters.

Receive a call

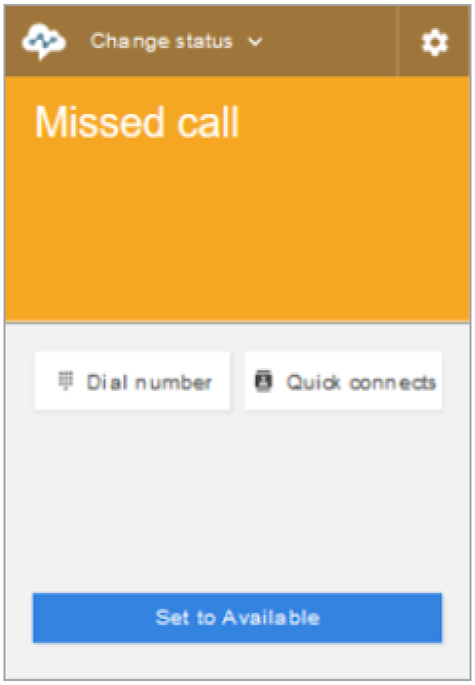


Earlier CCP

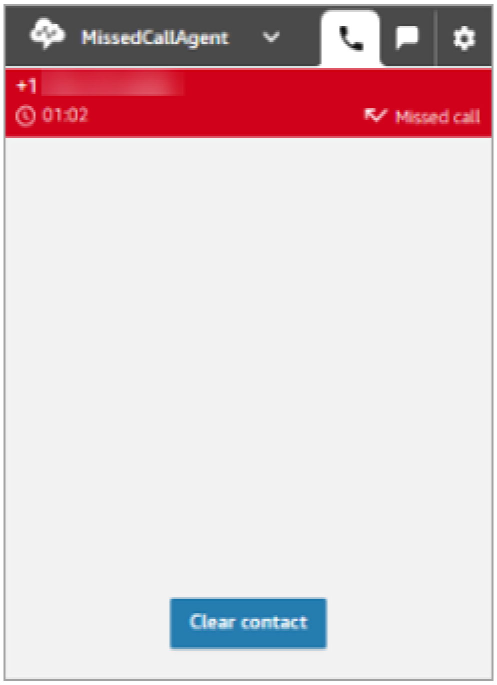


Latest CCP

Miss a call

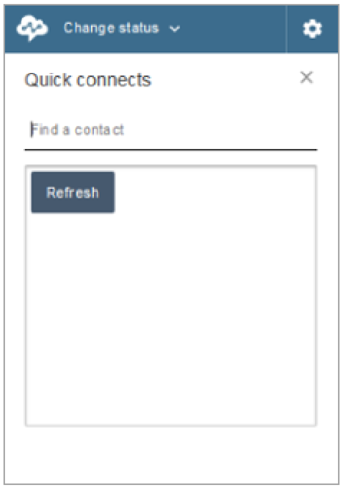


Earlier CCP

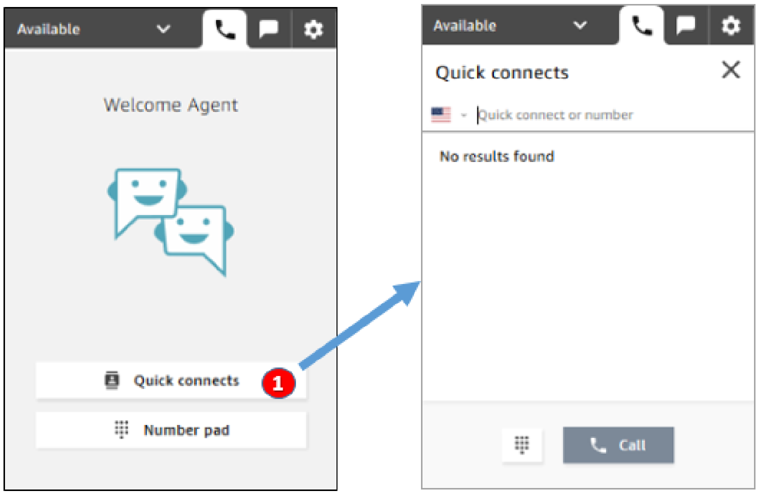


Latest CCP

Make a call: When to use Quick connects



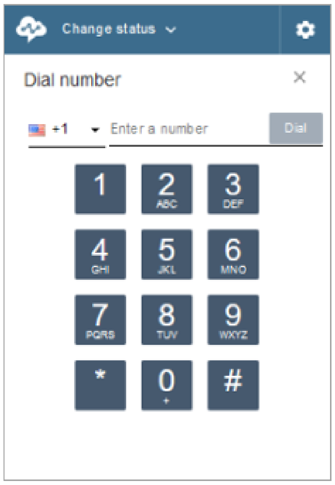
Earlier CCP

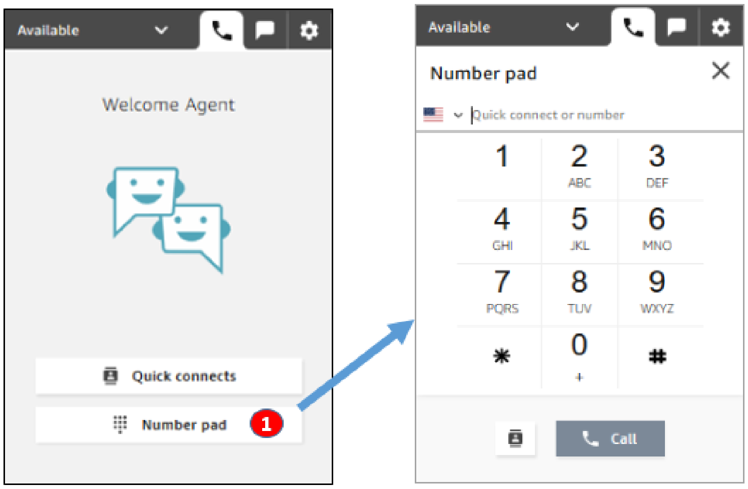


Latest CCP

- Use the **Quick connects** button to type a number or select a quick connect.

Make a call: When to use Number pad



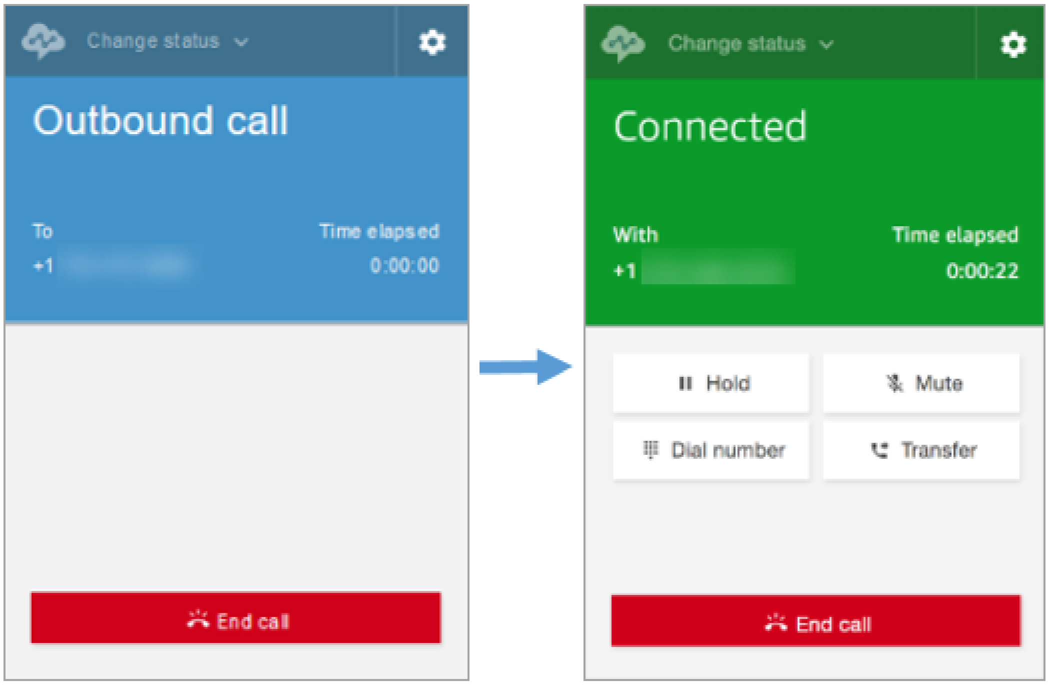


Earlier CCP

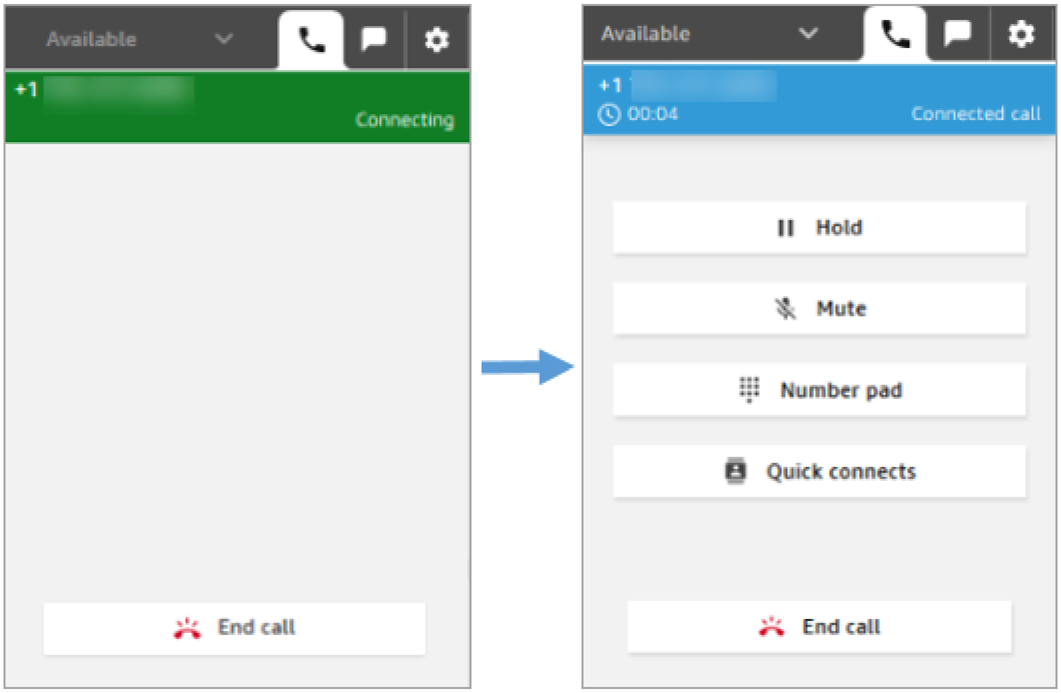
Latest CCP

- Choose the **Number pad** button to type and call a number. This is useful for corporate numbers with letters (for example, 1-800-EXAMPLE).

Make an outbound call

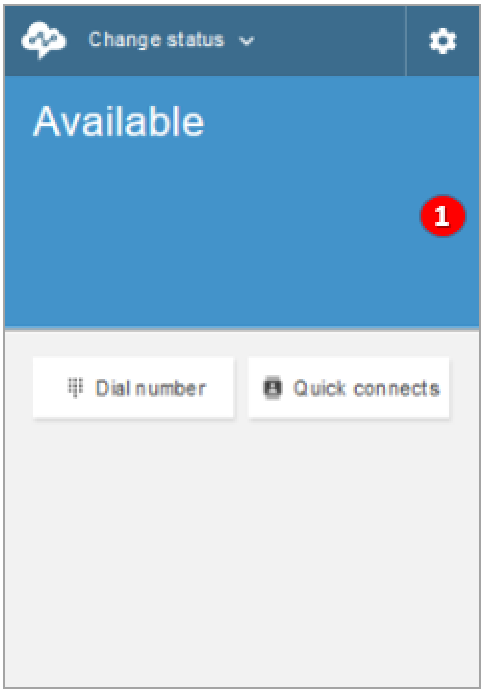


Earlier CCP

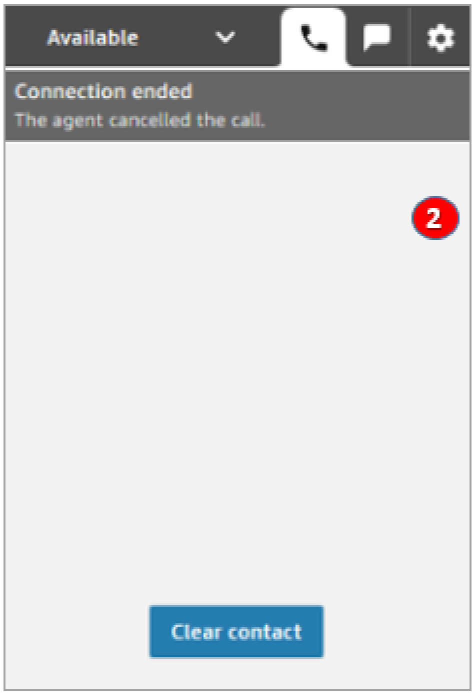


Latest CCP

Agent ends a call before being connected to the other party



Earlier CCP

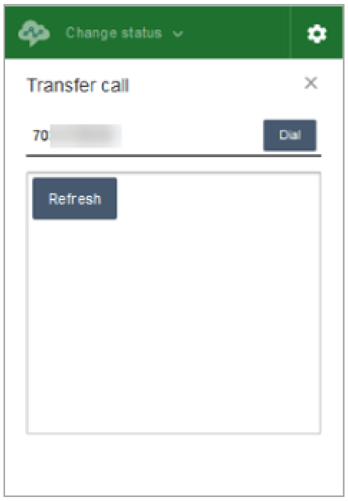


Connection ended
The agent cancelled the call.

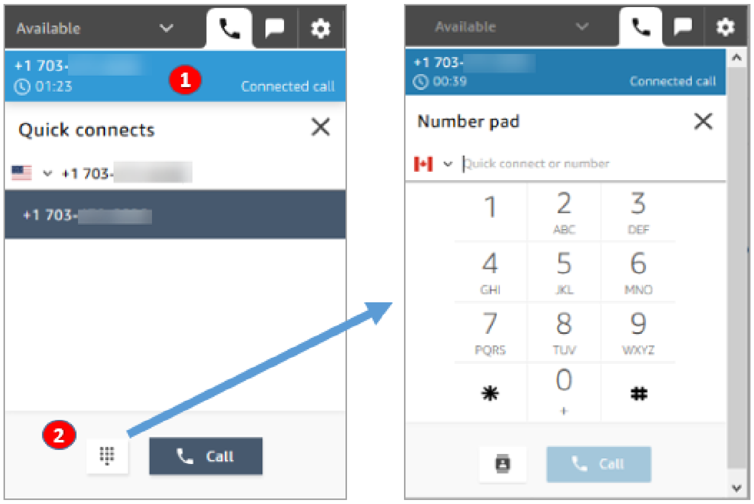
Latest CCP

1. If an agent ends a call before being connected, they are then available for a new contact to be routed to them automatically.
2. If an agent ends a call before being connected, they are prompted to choose **Clear contact**.

Make another call while connected on a call



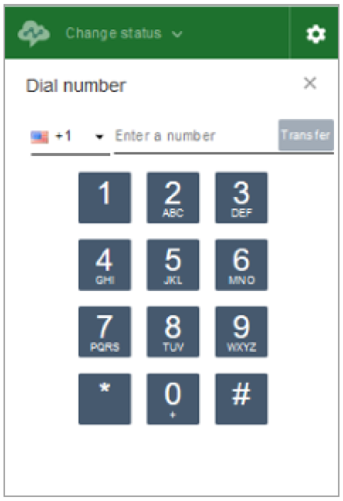
Earlier CCP



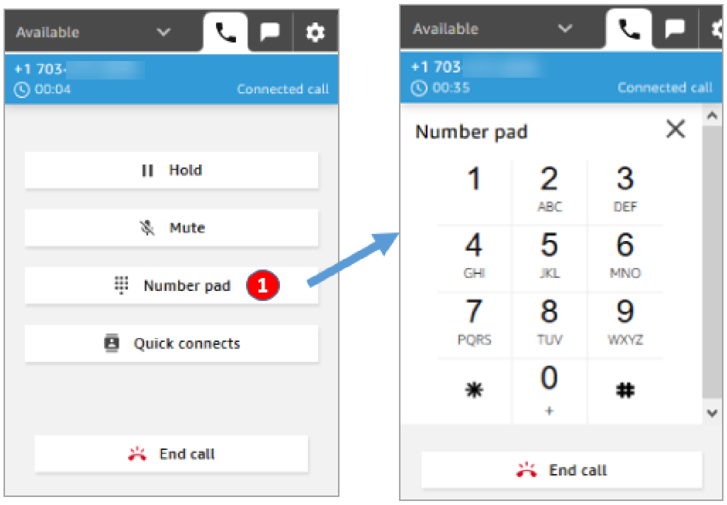
Latest CCP

1. You can see the call that you are on while typing another number or selecting a quick connect.
2. After choosing **Quick connects**, you can choose the **Number pad** button. Then on the **Number pad** page, you can enter a number.

Enter DTMF input while connected on a call



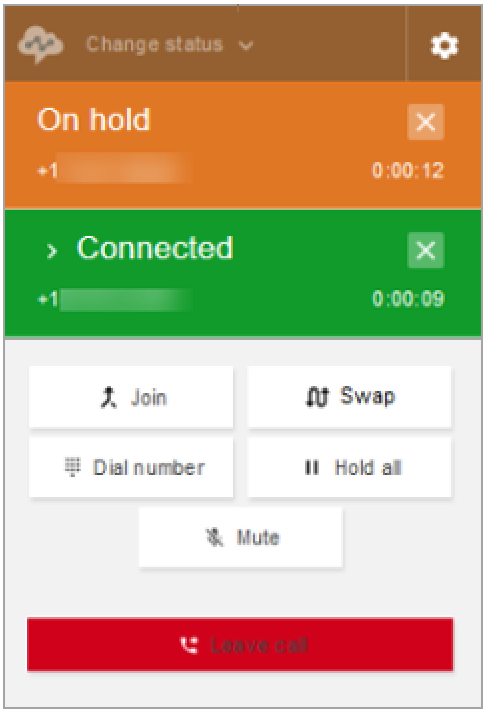
Earlier CCP



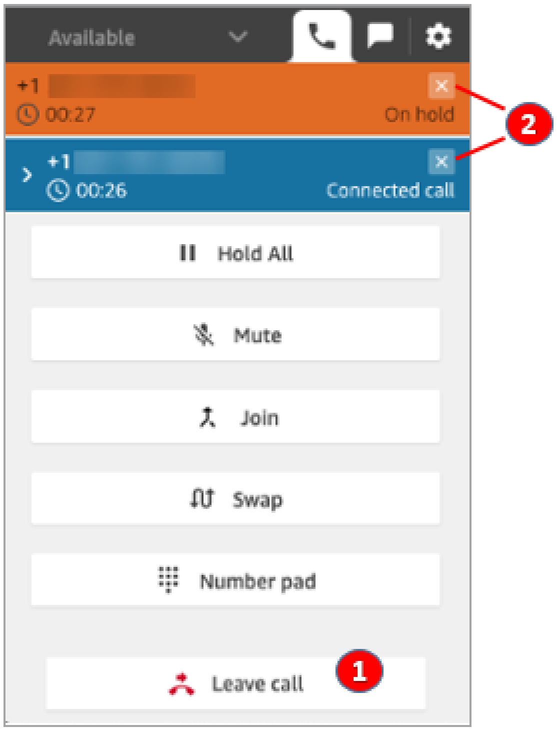
Latest CCP

- While on a call, only use **Number pad** to enter DTMF input.

Conference call scenario 1: Leaving a call when one party is on hold and the other is connected



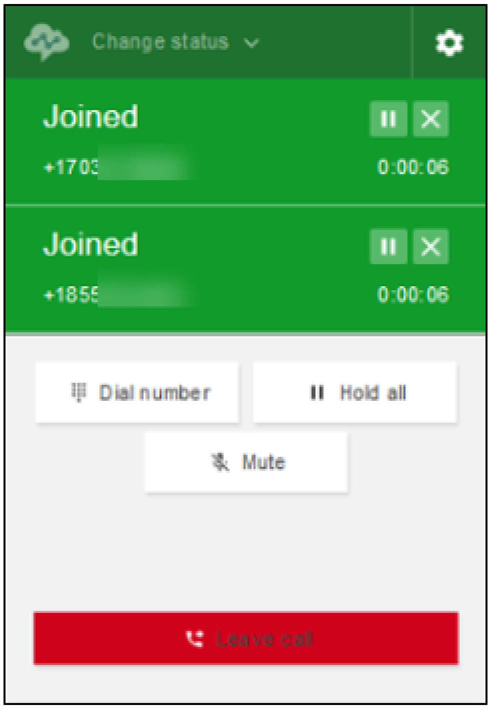
Earlier CCP



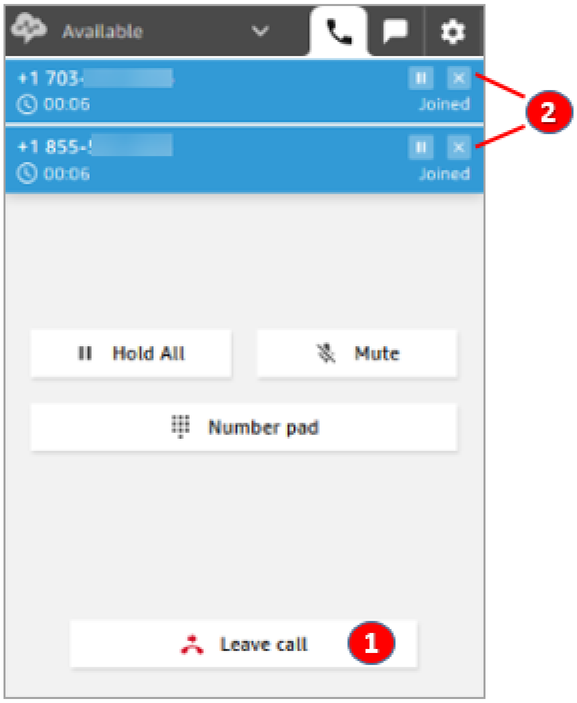
Latest CCP

1. Choose **Leave call** to leave the call. This automatically takes the first party off hold and connects them to the second party.
2. If instead you want to end the call, choose the **x** next to each party's number. This disconnects each party.

Conference call scenario 2: Leaving a call when the other parties are joined



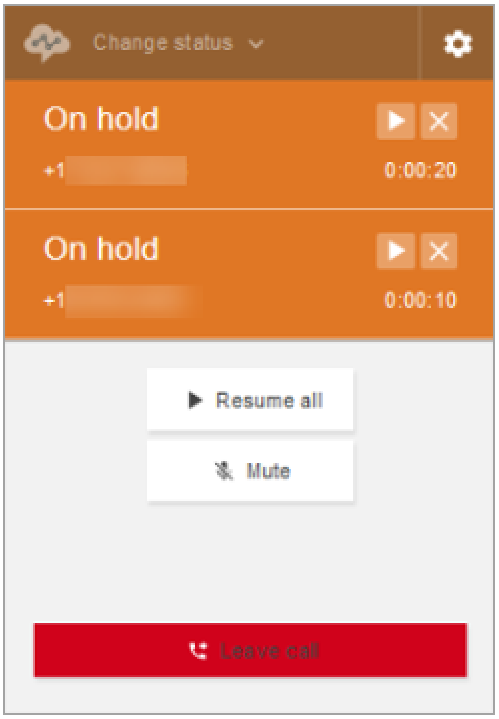
Earlier CCP



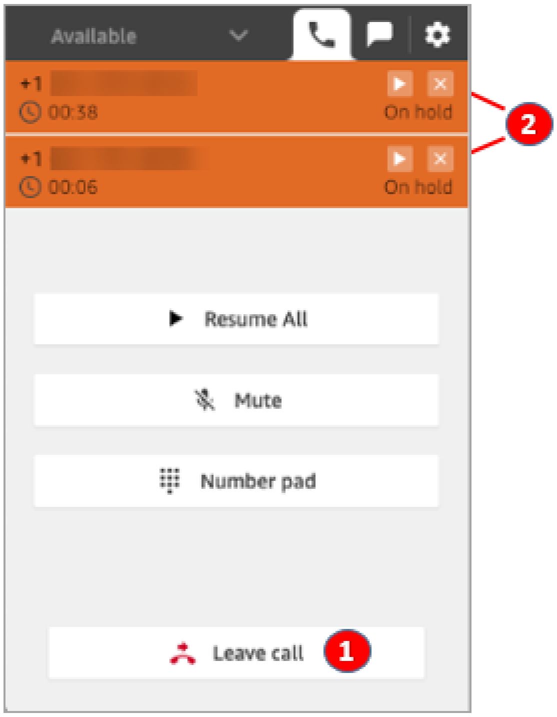
Latest CCP

1. Choose **Leave call** to leave the call. The other two parties stay joined.
2. If instead you want to end the call, choose the **x** next to each party's number. This disconnects each party.

Conference call scenario 3: Leaving a call when the other parties are on hold



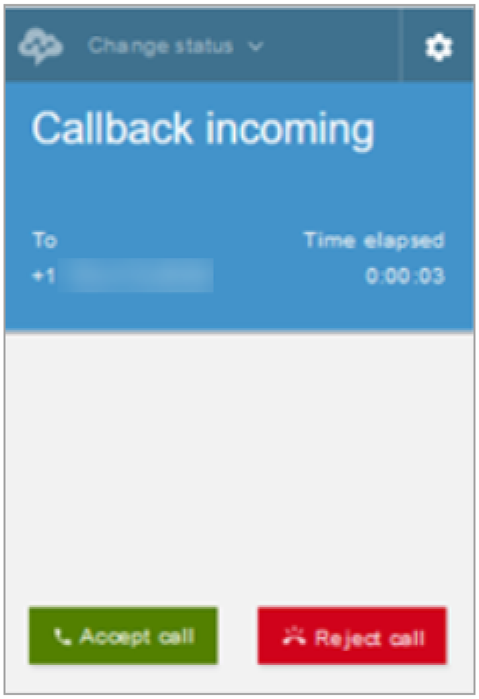
Earlier CCP



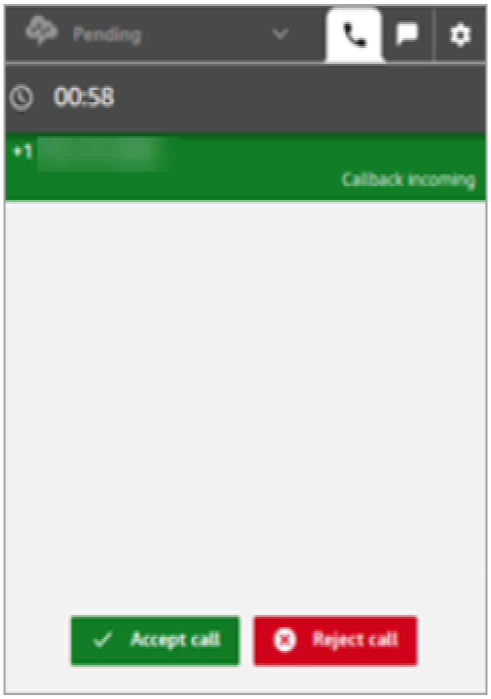
Latest CCP

1. Choose **Leave call** to leave the call. The other two parties are automatically taken off hold and connected.
2. If instead you want to end the call, choose the **x** next to each party's number. This disconnects each party.

Receive a queued callback

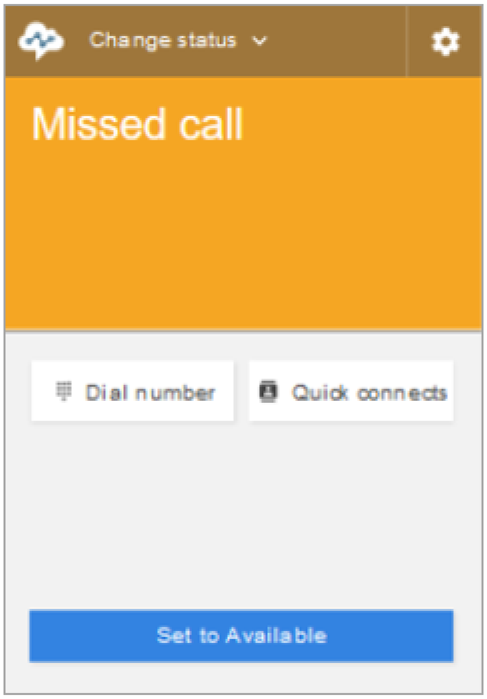


Earlier CCP

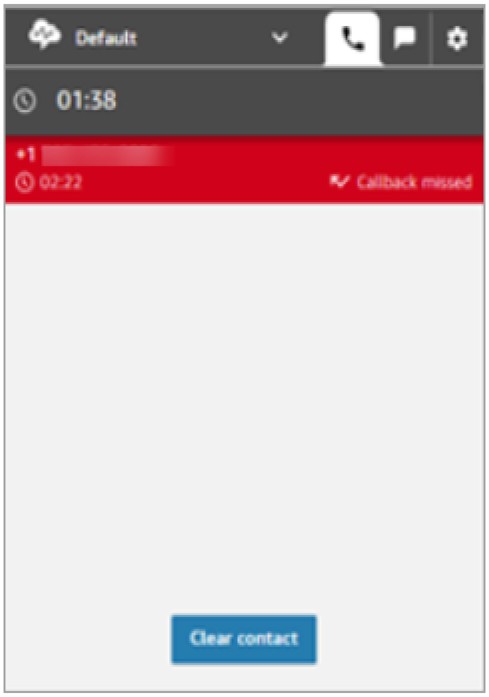


Latest CCP

Miss a queued callback

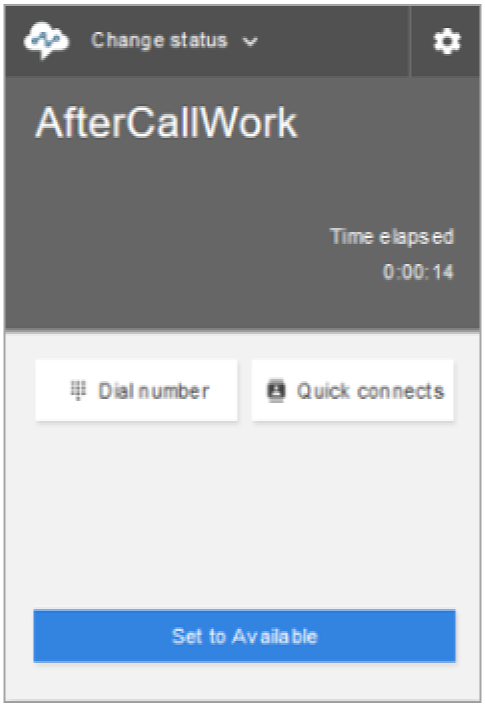


Earlier CCP

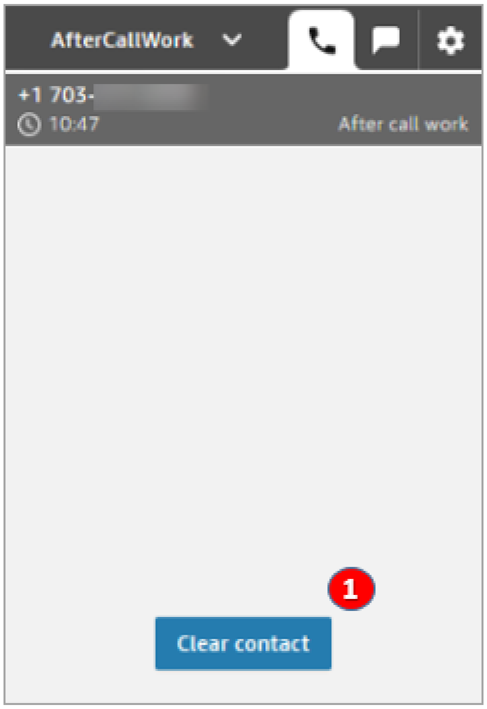


Latest CCP

Finish After contact work (ACW)



Earlier CCP



Latest CCP

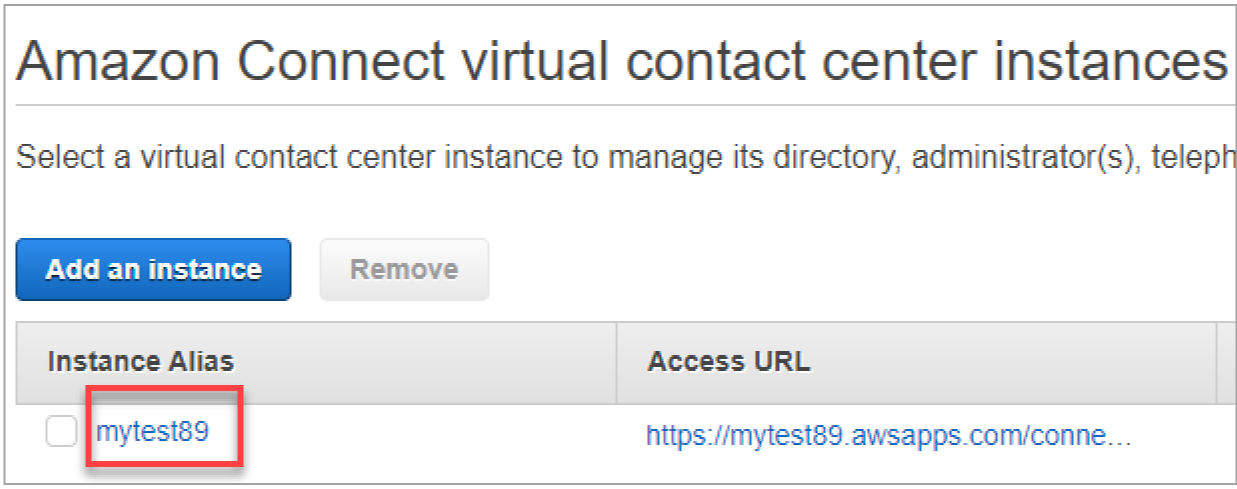
- During After contact work (ACW), agents can finish follow-up work, and then choose **Clear contact**.

I use the Amazon Connect Streams API

> **Note**
> The Amazon Connect Streams API remains the same between the earlier and latest versions of the CCP. We recommend validating custom implementations built using the Amazon Connect Streams API when upgrading versions to ensure consistency in behavior.

Use the following steps to upgrade to the latest CCP.

1. We recommend using the latest Amazon Connect Streams API.
2. Update the URL associated with `initCCP()` from **/ccp#** to **/ccp-v2**. For information about `initCCP()`, see connect.core.initCCP() in the Amazon Connect Streams API documentation on GitHub.
3. Add your domain URL to the Approved origin list:
   1. Log in to the AWS Management Console (https://console.aws.amazon.com/console) using your AWS account.
   2. Navigate to the Amazon Connect console.
   3. Check that you're in the correct Region for your Amazon Connect instance. Choose your instance.

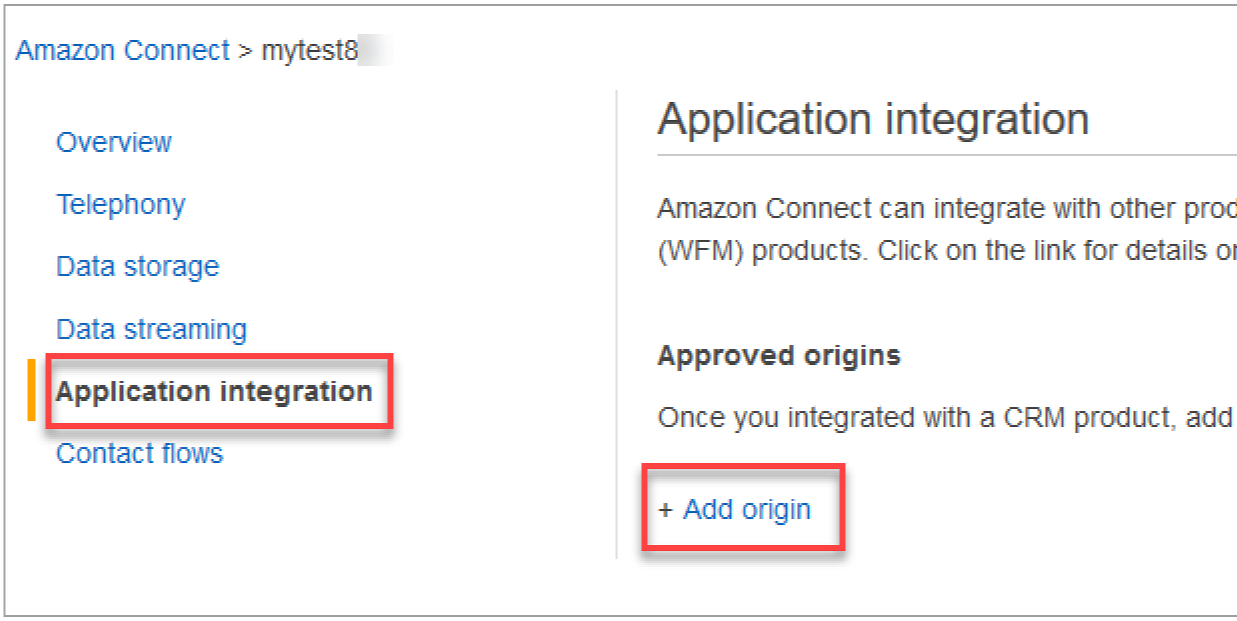


Amazon Connect virtual contact center instances

Select a virtual contact center instance to manage its directory, administrator(s), teleph

Instance Alias	Access URL
□ mytest89	https://mytest89.awsapps.com/conne...

4. Choose **Application integration**, and then choose **Add origin**.



Application integration

Amazon Connect can integrate with other prod
(WFM) products. Click on the link for details or

Approved origins

Once you integrated with a CRM product, add

5. Enter your domain URL. All domains that embed the CCP for a particular instance to be explicitly added. For more information, see this article on GitHub.

   If you use Salesforce, you need to add the Salesforce domains to your allow list to prevent any issues with the CTI Adapter CCP functionality. For detailed instructions, see the Amazon Connect CTI Adapter for Salesforce Lightning installation guide or the Amazon Connect CTI Adapter for Salesforce Classic installation guide.

Verify your network settings

We highly recommend setting up your network to use Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list (p. 605).

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

Update your SAML URL to ccp-v2

If you use SAML 2.0 as your identity management system, be sure to update the destination in your relay state URL to **ccp-v2**.

Change `destination=/connect/ccp` to `destination=/connect/ccp-v2`.

For more information, see Use a destination in your relay state URL (p. 130)

Provide access to the Contact Control Panel

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

1. Create a user name and password for agents to log into the CCP, by adding agents to your instance (p. 785).
2. At minimum, assign them the **Agent** security profile (p. 795). This grants them permissions to access the CCP, which they use to manage contacts.
3. Provide the user name, password, and the CCP website link to your agents so they can log in.

   The CCP website link is: **https://*`instance name`*.my.connect.aws/ccp-v2/**

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

   > **Tip**
   > Want your agents to manage contacts, and access customer profiles, cases, and knowledge all in one place? Use the agent application, which is a single web browser interface that hosts the CCP, Customer Profiles, Cases, and Wisdom. For more information, see Agent training guide (p. 1135).
4. Train your agents on the CCP:
   - Watch Training video: How to use the CCP (p. 1137)
   - Download a quick start cheat sheet.

Grant microphone access in Chrome or Firefox

If agents experience problems with their microphone, they may need to grant microphone access in their browser. Choose one of the following articles to get the steps appropriate for your browser:

- Use your camera and microphone in Chrome
- Firefox Page Info window

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

> **Important**
> A change introduced in Google Chrome version 64 may result in issues with receiving calls if you are using an embedded Contact Control Panel (CCP) softphone using the Amazon Connect Streams library. If you are experiencing issues with your microphone when using Chrome version 64, you can resolve the issue by building and deploying the latest version of the Amazon Connect Streams API, following the steps under *Downloading Streams*.
> You can also resolve the issue by using Firefox as your browser.

How to get help for CCP issues

Agents: Contact your manager or the technical support provided by your company.

Amazon Connect Administrators: See Troubleshooting Issues with the Contact Control Panel (CCP) (p. 1193) for detailed troubleshooting steps. Or, log in to the AWS Management Console (https://console.aws.amazon.com/console) using your AWS account. In the upper right corner of the page, choose **Support**, and open a support ticket.

Agent headset and workstation requirements for the CCP

Agent headsets and workstations in the contact center vary widely. While the Amazon Connect CCP is built to handle high levels of jitter and high latency environments, the architecture of the **workstations** that agents use, and the location and environment in which they take contacts, can impact the quality of experience.

Headset requirements

The agent's Contact Control Panel (CCP) is compatible with all types of headsets.

For the best agent and customer experience, we recommend using a USB headset.

Alternatively, you can redirect the contact to an external number, in E.164 format, using an agent's existing telephony.

> **Note**
> If the agent's audio device does not support up to 48khz and the browser asserts a sample rate of 48khz, audio issues such as an audible humming sound may be present in the agent's outgoing audio. This has been seen with Firefox but not with Chrome.
> For instructions on verifying the sample rate of the agent's headset and browser, see Humming sound in headset: Verify the headset and browser sample rates (p. 1201)

Workstation minimum requirements

Under-powered workstations can make it difficult for agents to access the tools and resources they need to service contacts. Also, keep in mind the resource requirements when scoping workstations to ensure that they can perform under load while appropriately multitasking for the use case.

Following are the minimum system requirements for the workstations using the CCP only. You'll need to scope additional memory, bandwidth, and CPU for the operating system and anything else running on the workstation to avoid resource contention.

- **Browser**—The latest three versions of Google Chrome or Mozilla Firefox
- **Network**—100 Kbps bandwidth per connected workstation
- **Memory**—2 GB RAM
- **Processor (CPU)**—2 GHz

iPhone and other mobile devices are not supported

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

How to determine whether a workstation is the source of problems

To determine whether a workstation is the source of problems, you need access to various levels of logging information. However, adding logging and monitoring to workstations that are already experiencing resource contention may further reduce available resources and invalidate test results. We recommended that your workstation meet the minimum requirements, so you leave additional resources available for logging, monitoring, malware scanning, operating system functions, and any other running processes.

Collect additional historical logging and data sources for correlation. If you see a correlation between the time of the event and the time the issue was reported, you may be able to determine the root cause with the following information:

- Round trip time (RTT) and packet loss to endpoints located within your Amazon Connect Region from your agent workstation, or an identical workstation on the same network segment. If no Region endpoints are available because of security policies, any public WAN endpoint suffices, for example, www.Amazon.com. Ideally, use your instance alias address (https://yourInstanceName.awsapps.com), and also your signaling address for endpoints.

  You can find your Region endpoints here: Amazon Connect endpoints and quotas.
- Regular monitoring of workstations that show processes running, and the current resource usage of each process.
- Workstation performance/utilization in these areas:
  - Processor (CPU)
  - Disk / drive
  - RAM / memory
  - Network throughput and performance
- Monitor all of the preceding for your VDI desktop environment, including RTT/packet monitoring between the agent workstation and the VDI environment.

Can't hear caller or caller can't hear agent?

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

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

Here's what you need to do:

- **Check that your computer recognizes your headset**—Check the settings in Device Manager to ensure that your computer recognizes the headset and allows proper headset connectivity. For example, if you're using a Windows PC:
  1. Go to **Device Manager**, then expand **Audio inputs and outputs**.
  2. If your computer recognizes your headset, you'll see it listed there.
- **Check your browser settings for your headset/microphone**
  - **Chrome**
    1. go to **Settings**, **Site Settings**, **Microphone**.
    2. Then check that the correct headset is enabled.
    3. To learn more, see Use your camera and microphone in Chrome.

- **Firefox**
  1. While in the CCP, choose the lock icon in the address bar. If needed, grant permissions to the CCP.
  2. To learn more, see Firefox Page Info window.
- **Remove your ad blocker**: If you're using an ad blocker extension, remove it and see if that fixes the problem.

Important
A change introduced in Google Chrome version 64 may result in issues with receiving calls if you are using an embedded Contact Control Panel (CCP) softphone using the Amazon Connect Streams library. If you are experiencing issues with your microphone when using Chrome version 64, you can resolve the issue by building and deploying the latest version of the Amazon Connect Streams API, following the steps under *Downloading Streams*.
You can also resolve the issue by using Firefox as your browser.

For more information about solving audio problems, see Troubleshooting Issues with the Contact Control Panel (CCP) (p. 1193).

Can't hear indicator for incoming chat?

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

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

For more information about solving audio problems, see Troubleshooting Issues with the Contact Control Panel (CCP) (p. 1193).

Embed the CCP into Salesforce

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

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

For a detailed walk-through and setup of the full CTI Adapter capabilities for Salesforce Lightning, see the Amazon Connect CTI Adapter for Salesforce Lightning installation guide.

For the CTI Adapter for Salesforce Classic, see the Amazon Connect CTI Adapter for Salesforce Classic installation guide.

We recommend that you initially install the package into your Salesforce sandbox. After the package is installed, you can configure your Salesforce Call Center configuration within Salesforce.

Embed the CCP into Zendesk

To integrate Amazon Connect and Zendesk, you need:

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

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

For more information, see How do I integrate Amazon Connect with Zendesk?

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. 297) 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

Permissions required to view, edit, create contact flows

To view, edit, create, and publish contact flows you need **Contact flows** permissions added to your security profile.

By default users who are assigned to the **Admin** and **CallCenterManager** security profiles have Contact flows permissions.

Default contact flows

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

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

> **Tip**
> If you want to change the behavior of a default contact flow, we recommend creating a new customized flow based on the default. Then call the new flow intentionally in your contact flows rather than defaulting to it. This gives you better control over how your contact flows work.

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

Contents

Change a default contact flow

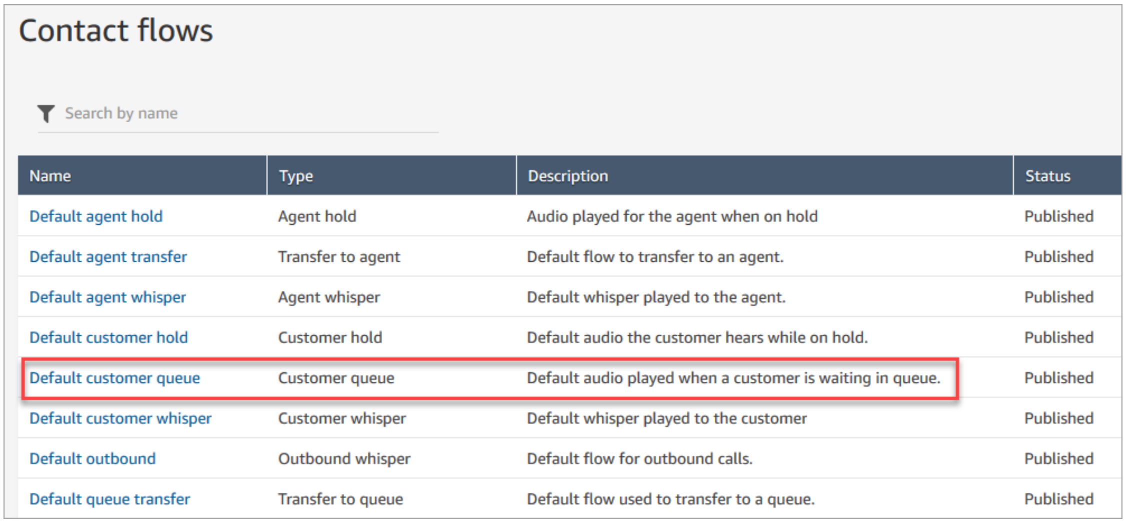
You can override the way the default flows work by editing them directly.

Generally we recommend creating new flows based on the defaults, rather than editing the default flow directly. You can make a copy of the default flow, assign a name that indicates it's a custom version, and then edit that one. This gives you more control over how your contact flows work.

Change how a default contact flow works

The following steps show how to change the default message customers hear when they are put in a queue to wait for the next available agent.

1. On the navigation menu, choose **Routing**, **Contact flows**.
2. Choose the default contact flow you want to customize. For example, choose **Default customer queue** if you want to create your own message when a customer is put in queue instead of using the one we've provided.

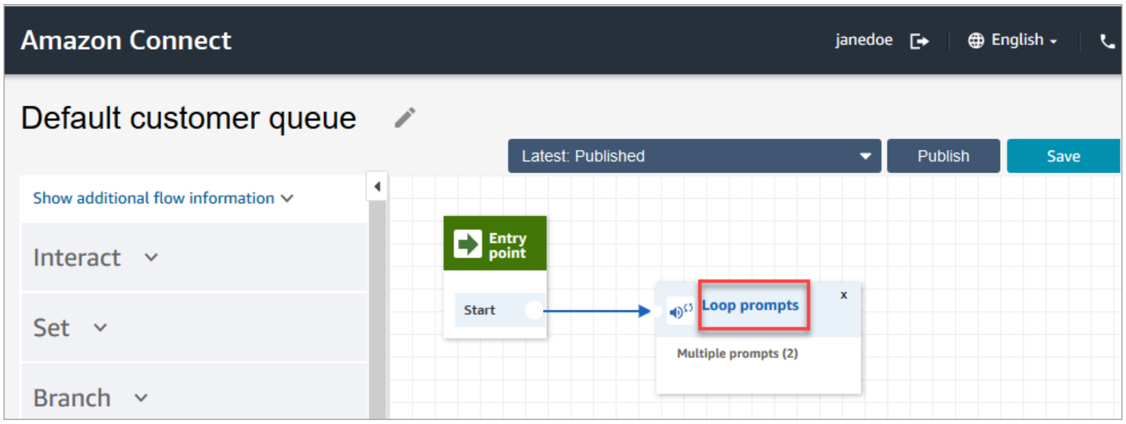


Contact flows

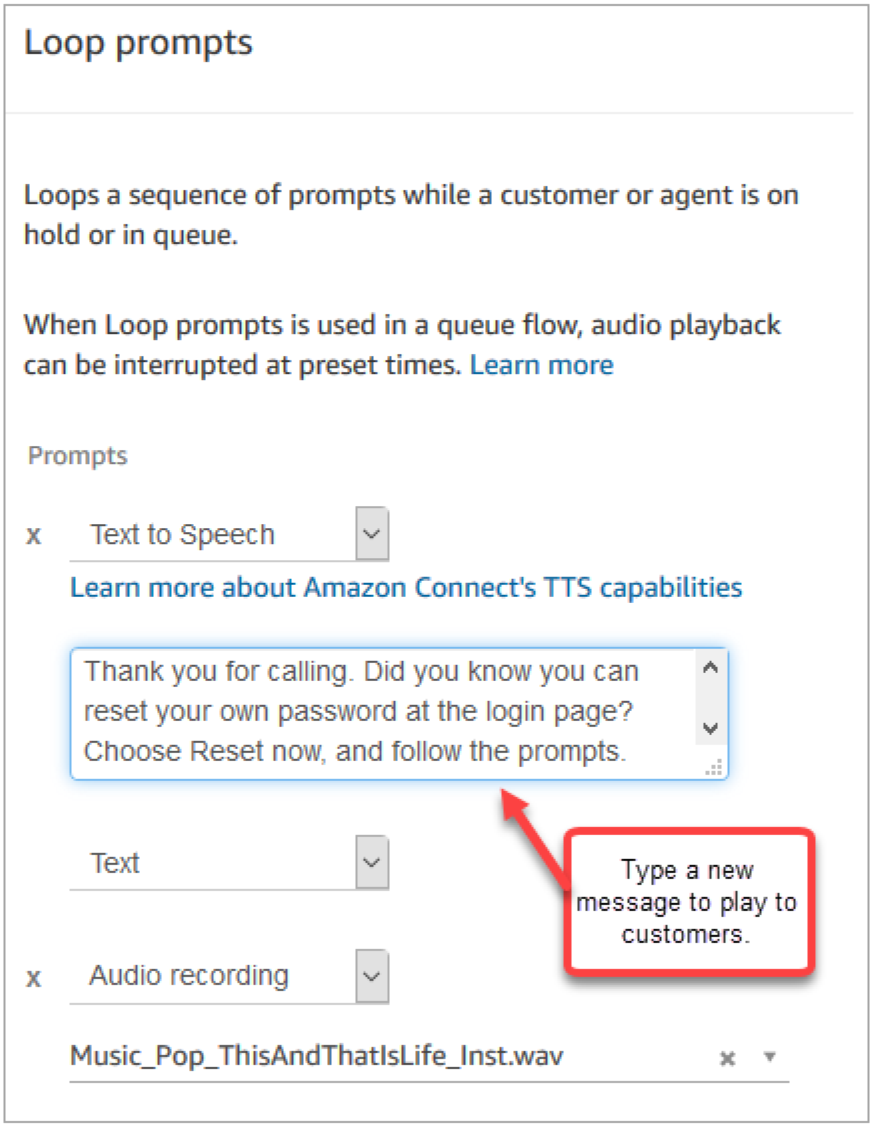
Search by name

Name	Type	Description	Status
Default agent hold	Agent hold	Audio played for the agent when on hold	Published
Default agent transfer	Transfer to agent	Default flow to transfer to an agent.	Published
Default agent whisper	Agent whisper	Default whisper played to the agent.	Published
Default customer hold	Customer hold	Default audio the customer hears while on hold.	Published
Default customer queue	Customer queue	Default audio played when a customer is waiting in queue.	Published
Default customer whisper	Customer whisper	Default whisper played to the customer	Published
Default outbound	Outbound whisper	Default flow for outbound calls.	Published
Default queue transfer	Transfer to queue	Default flow used to transfer to a queue.	Published

3. To customize the message, choose the **Loop prompts** block to open the properties page.



4. Use the dropdown box to either choose different music, or set to **Text to Speech** and then type a message to be played, as shown in the following image.



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 at preset times. Learn more

Prompts

x Text to Speech

Learn more about Amazon Connect's TTS capabilities

Thank you for calling. Did you know you can reset your own password at the login page? Choose Reset now, and follow the prompts.

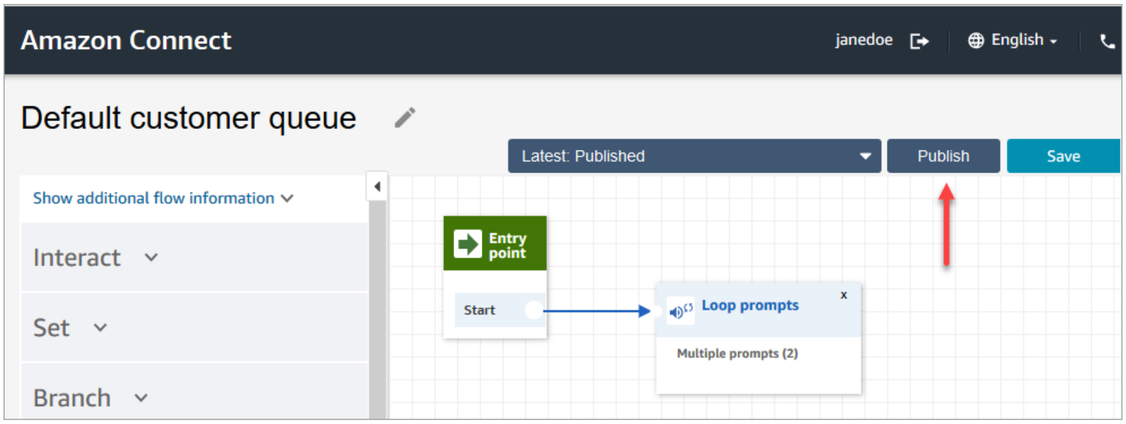
Text

x Audio recording

Music_Pop_ThisAndThatIsLife_Inst.wav

Type a new message to play to customers.

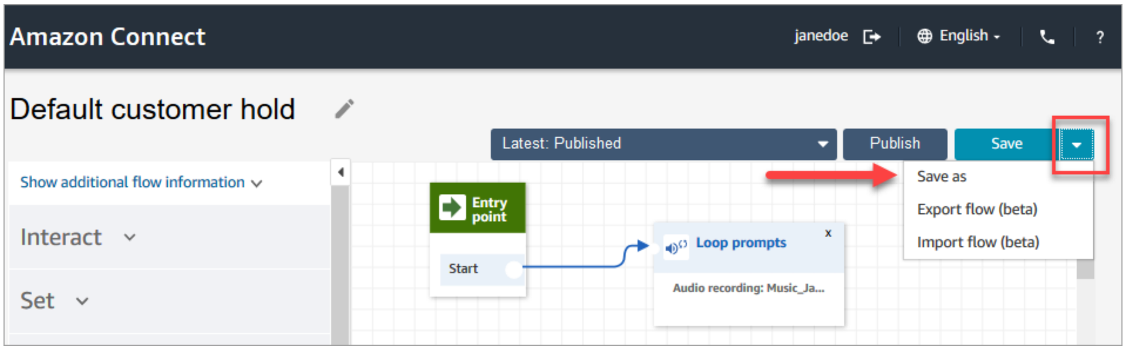
5. Choose **Save** at the bottom of the properties page.
6. Choose **Publish**. Amazon Connect starts playing the new message almost immediately (it may take a few moments for it to fully take effect).



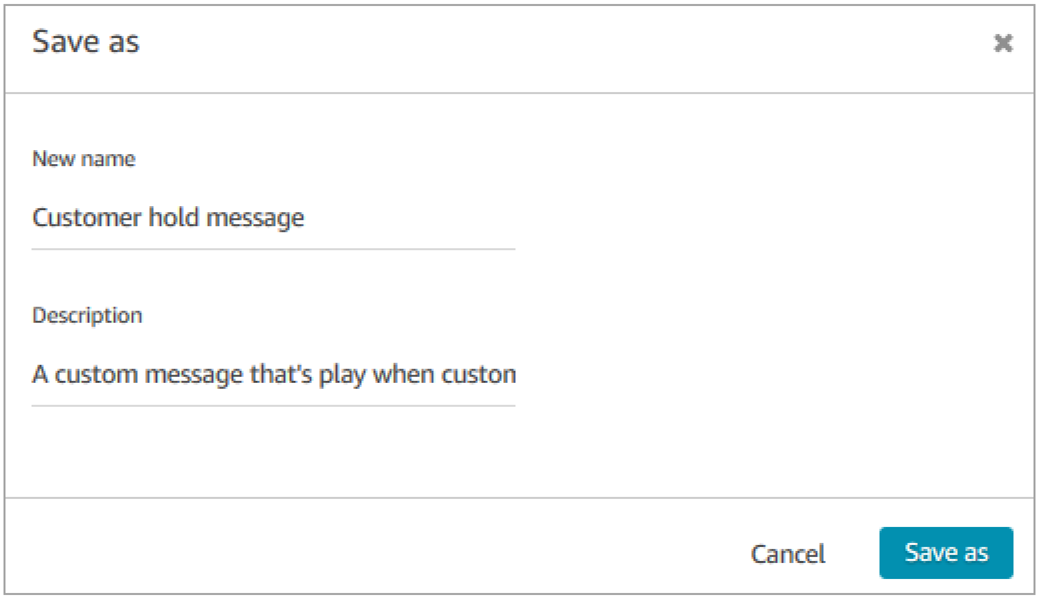
Copy a default contact flow before customizing it

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

1. On the navigation menu, choose **Routing**, **Contact flows**.
2. Choose the default contact flow you want to customize.
3. In the upper right corner of the page, choose the **Save** drop-down arrow. Choose **Save as**.



4. Assign a new name for the contact flow, for example, **Customer hold message**.



Save as

New name

Customer hold message

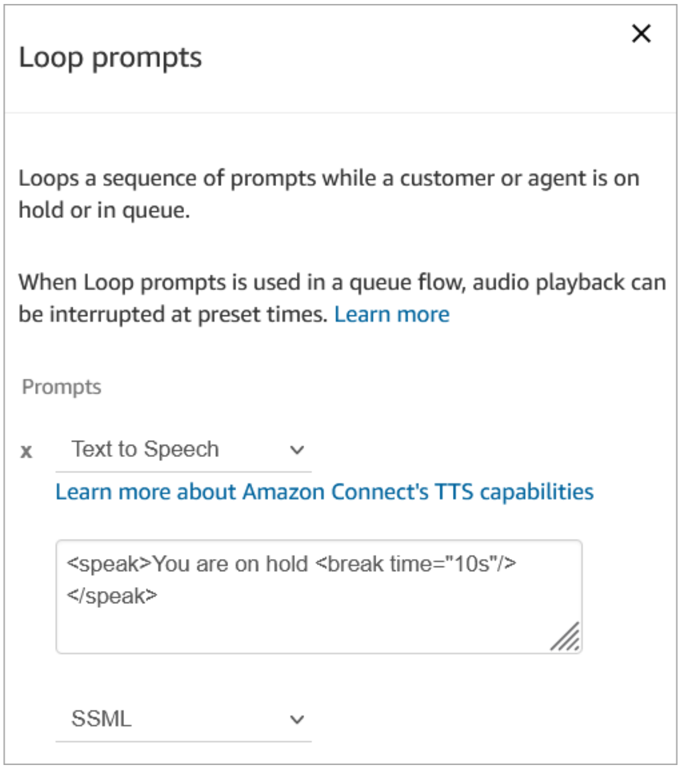
Description

A custom message that's play when custon

5. Add the new contact flow (in this case, **Customer hold message**) to the contact flows you create so it's run instead of the default.

Default agent hold: "You are on hold"

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



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 at preset times. Learn more

Prompts

x Text to Speech

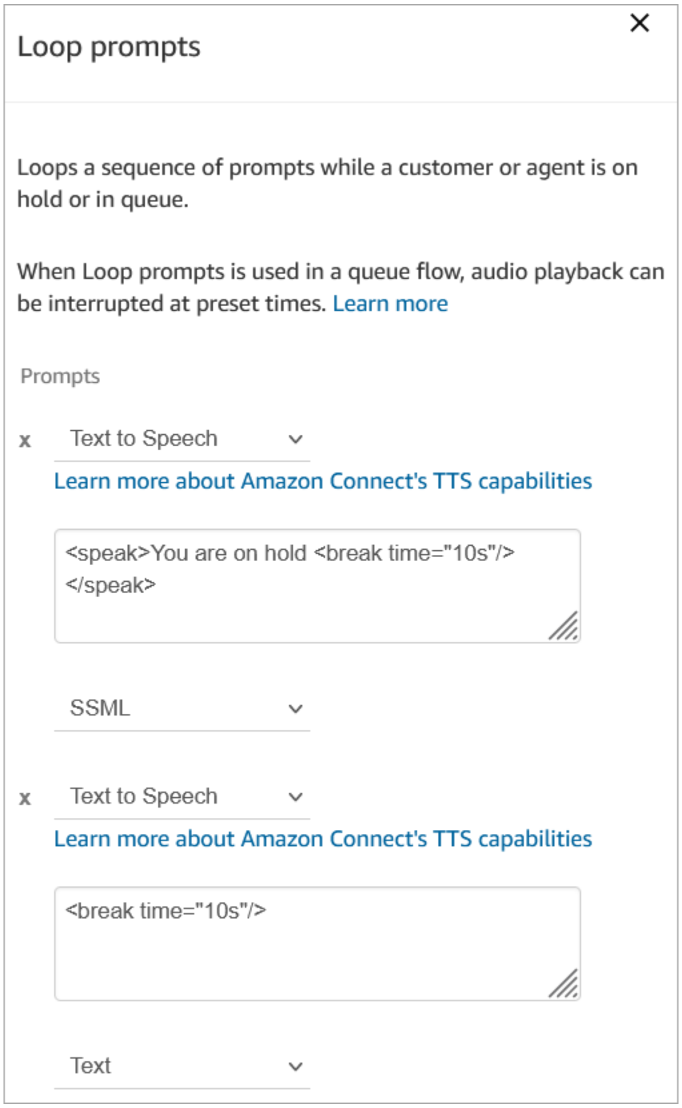
Learn more about Amazon Connect's TTS capabilities

```
<speak>You are on hold <break time="10s"/>
</speak>
```

SSML

You can set **break time** to a maximum of 10 seconds. This means the maximum amount time you can specify between **You are on hold** messages is 10 seconds. To make the time between longer, add multiple prompts to the loop. For example, if you want 20 seconds between **You are on hold** messages:

- The first prompt may say **You are on hold** with **break time="10s"**
- Add another prompt with a blank message and break time="10s".



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 at preset times. Learn more

Prompts

x Text to Speech

Learn more about Amazon Connect's TTS capabilities

```
<speak>You are on hold <break time="10s"/>
</speak>
```

SSML

x Text to Speech

Learn more about Amazon Connect's TTS capabilities

```
<break time="10s"/>
```

Text

For instructions about how to override and change a default contact flow, see Change a default contact flow (p. 297).

> **Tip**
> Wondering if a default flow has been changed? Use flow version control (p. 452) to view the original version of the flow.

Default agent transfer: "Transferring now"

This default transfer flow is what the agent experiences when transferring a contact to another agent by using Create quick connects (p. 466). A **Play prompt** plays the message “Transferring now.” Then the **Transfer to agent** block is used to transfer the contact to the agent.

> **Tip**
> The **Transfer to Agent** block is a beta feature and only works for voice interactions. To transfer a chat contact to another agent, follow these instructions: Use contact attributes to route contacts to a specific agent (p. 478).

For instructions about how to override and change a default contact flow, see Change a default contact flow (p. 297).

Tip
Wondering if a default flow has been changed? Use flow version control (p. 452) to view the original version of the flow.

Default customer queue: queue hold message and music

This default contact flow is played when a customer is placed in a queue.

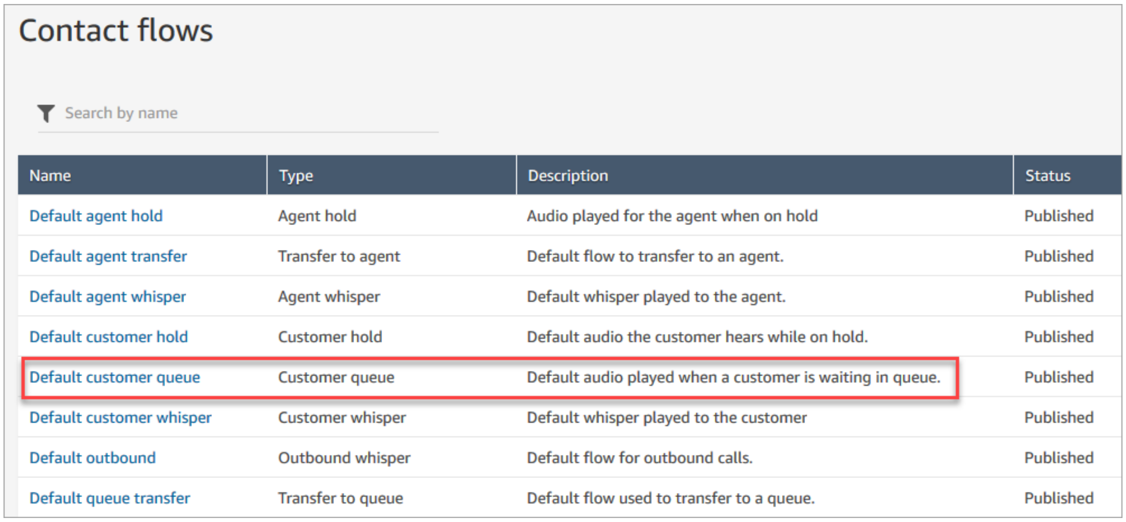
1. The loop has a one-time voice prompt:

   Thank you for calling. Your call is very important to us and will be answered in the order it was received.
2. It plays queue music in .wav format that's been uploaded to the Amazon Connect instance.
3. The customer remains in this loop until their call is answered by an agent.

Change the default message a customer hears when they are put in queue

The following steps show how to change the default message customers hear when they are put in a queue to wait for the next available agent.

1. On the navigation menu, choose **Routing**, **Contact flows**.
2. Choose **Default customer queue**.

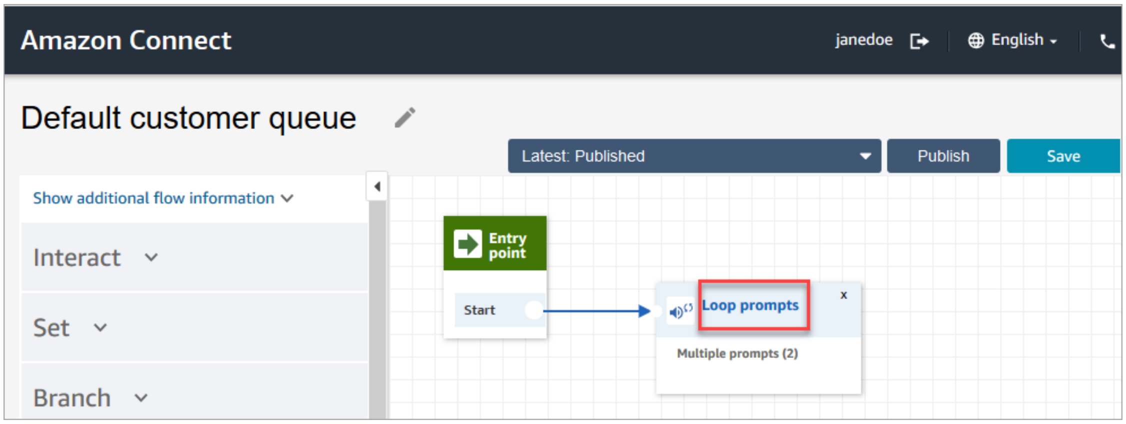


Contact flows

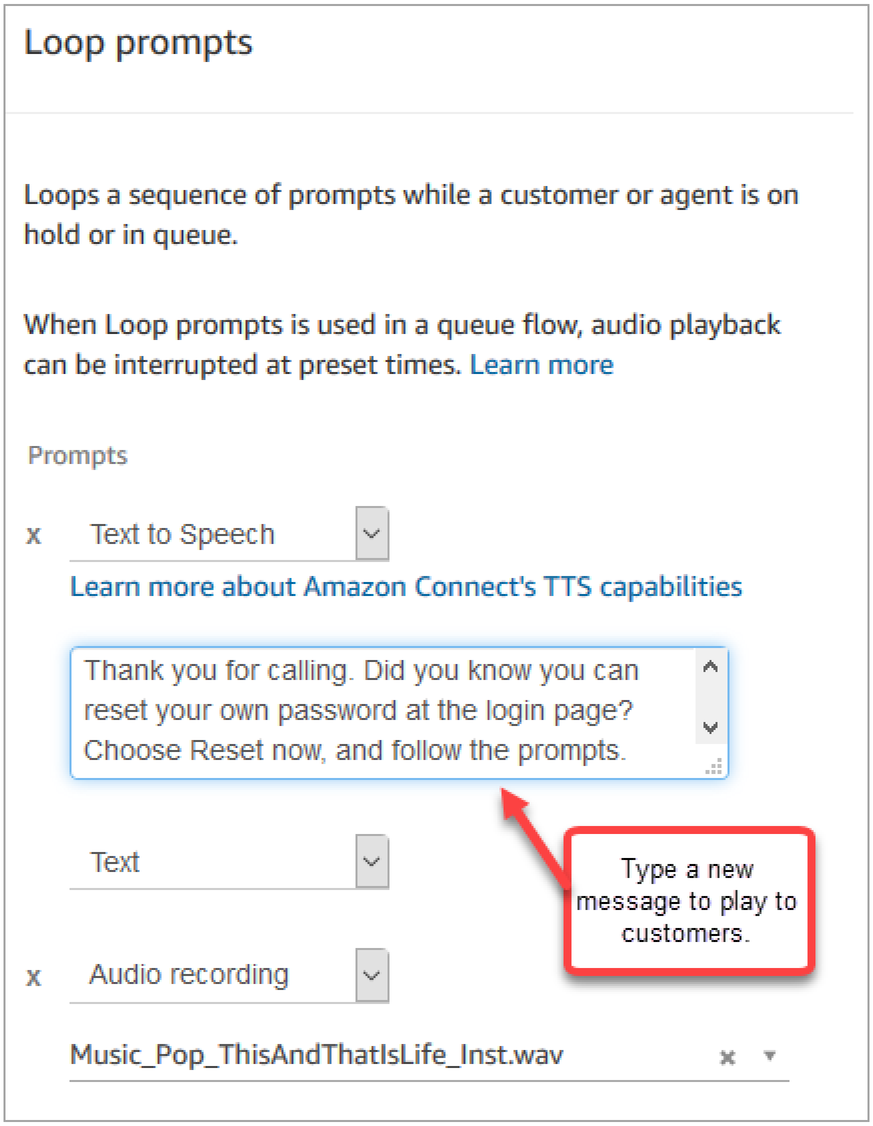
Search by name

Name	Type	Description	Status
Default agent hold	Agent hold	Audio played for the agent when on hold	Published
Default agent transfer	Transfer to agent	Default flow to transfer to an agent.	Published
Default agent whisper	Agent whisper	Default whisper played to the agent.	Published
Default customer hold	Customer hold	Default audio the customer hears while on hold.	Published
Default customer queue	Customer queue	Default audio played when a customer is waiting in queue.	Published
Default customer whisper	Customer whisper	Default whisper played to the customer	Published
Default outbound	Outbound whisper	Default flow for outbound calls.	Published
Default queue transfer	Transfer to queue	Default flow used to transfer to a queue.	Published

3. To customize the message, choose the **Loop prompts** block to open the properties page.



4. Use the dropdown box to either choose different music, or set to **Text to Speech** and then type a message to be played, as shown in the following image.



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 at preset times. Learn more

Prompts

x Text to Speech

Learn more about Amazon Connect's TTS capabilities

Thank you for calling. Did you know you can reset your own password at the login page? Choose Reset now, and follow the prompts.

Text

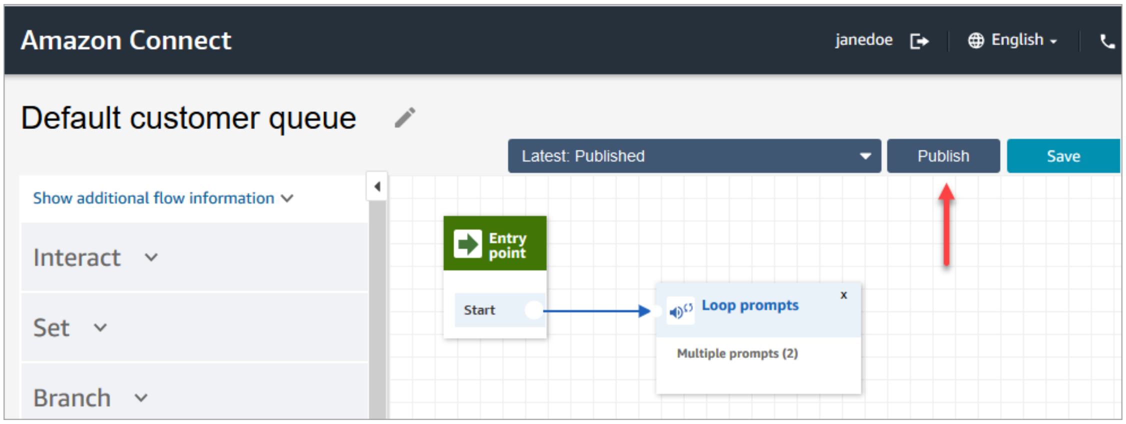
x Audio recording

Music_Pop_ThisAndThatIsLife_Inst.wav

Type a new message to play to customers.

5. Choose **Save** at the bottom of the properties page.

6. Choose **Publish**. Amazon Connect starts playing the new message almost immediately (it may take a few moments for it to fully take effect).



Default customer whisper: beep sound

This contact flow uses a Set whisper flow (p. 418) block to play a message for the customer when the customer and agent are joined. It uses a "beep" sound to notify a customer that their call has been connected to an agent.

Use the Set whisper flow (p. 418) block to override the default agent whisper in a voice conversation.

> **Important**
> For chat conversations, you need to include a Set whisper flow (p. 418) for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation (p. 305).

Default agent whisper: name of the queue

This contact flow uses a Set whisper flow (p. 418) block to play a message for the agent when the customer and agent are joined.

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

Use the Set whisper flow (p. 418) block to override the default agent whisper in a voice conversation.

> **Important**
> For chat conversations, you need to include a Set whisper flow (p. 418) for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation (p. 305).

For more information about system variables, see System attributes (p. 517).

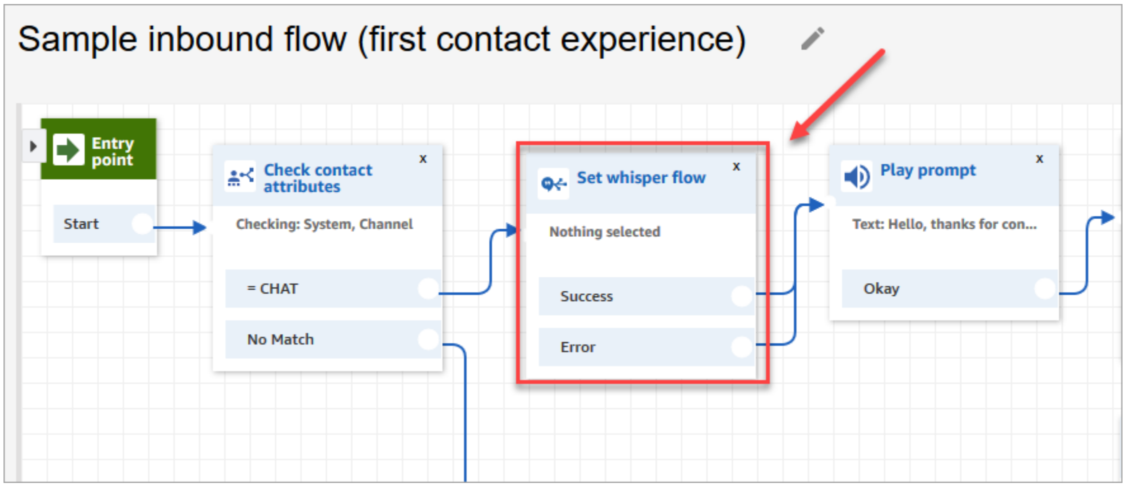
> **Tip**
> Wondering if a default flow has been changed? Use flow version control (p. 452) to view the original version of the flow.

Set the default whisper flow for a chat conversation

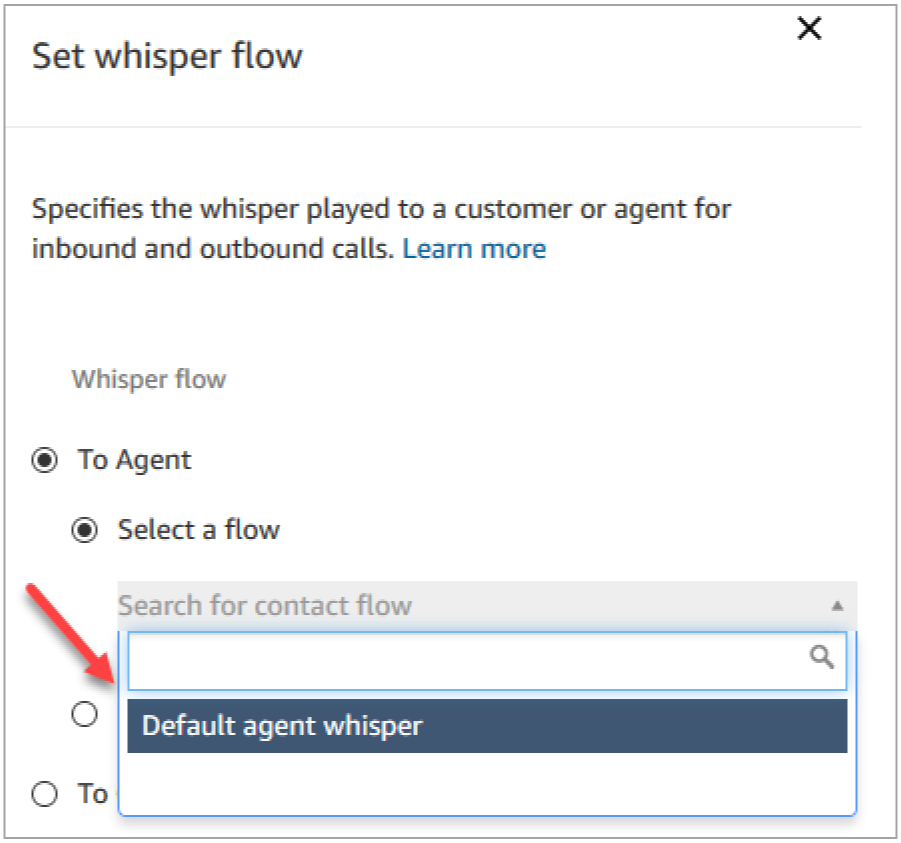
For chat conversations, you need to include a **Set whisper flow** block for default agent or customer whispers to play.

For example, to set the default whisper flow for chats that use the Sample inbound flow (p. 309):

1. Go to **Routing**, **Contact flows**, and choose the Sample inbound flow.
2. Add a **Set whisper flow** block after the chat channel has branched, as shown in the following image:



3. In the **Set whisper flow** block, open the properties page, and choose the flow you want to play as the default for chat conversations. For example, you might choose **Default whisper flow** to show agents the name of the originating queue in the chat window. This is helpful when agents are managing more than one queue.


Set whisper flow

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

Whisper flow

● To Agent

● Select a flow

Search for contact flow

Default agent whisper

○

○ To

4. Choose **Save**.

Default customer hold: hold music

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

For instructions about how to override and change a default contact flow, see Change a default contact flow (p. 297).

> **Tip**
> Wondering if a default flow has been changed? Use flow version control (p. 452) to view the original version of the flow.

Default outbound: "This call is not being recorded"

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

1. It starts with an optional **Set recording behavior** block. Then a prompt plays the following message:

   This call is not being recorded.
2. The flow ends.
3. The customer remains in the system (on the call) after the flows ends.

For instructions about how to override and change a default contact flow, see Change a default contact flow (p. 297).

> **Tip**
> Wondering if a default flow has been changed? Use flow version control (p. 452) to view the original version of the flow.

Default queue transfer: "Now transferring"

This contact flow manages what the agent experiences when they transfer a customer to another queue.

It starts with a **Check hours of operation** block to check the hours of operation for the current queue. The **In hours** option branches to the **Check staffing** block to determine whether agents are available, staffed, or online.

If it returns **True** (agents are available), the flow goes to the **Transfer to queue** block. If it returns **False** (no agents are available), the flow plays a prompt and disconnects the call.

For instructions about how to override and change a default contact flow, see Change a default contact flow (p. 297).

> **Tip**
> Wondering if a default flow has been changed? Use flow version control (p. 452) to view the original version of the flow.

Default prompts from Amazon Lex: "Sorry .. "

If you add an Amazon Lex bot to your contact center, know that it also has some default prompts that it uses for error handling. For example:

- Sorry, can you please repeat that?

- Sorry, I could not understand. Goodbye.

To change default Amazon Lex prompts

1. In Amazon Lex, go to your bot.
2. On the Editor tab, choose Error Handling.
3. Change the text as needed. Choose **Save**, then **Build** and **Publish**.

Sample contact flows

Amazon Connect includes a set of sample contact flows that show you how to perform common functions. They are designed to help you learn how to create your own contact flows that work in a similar way. For example, if you want to add a queued callback flow to your call center, take a look at the Sample queued callback (p. 314) flow.

To explore how the sample flows work

1. Claim a number if you haven't already: go to **Channels**, **Phone numbers**, **Claim a number**.
2. Choose the **DID** tab, then choose a number.
3. In **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 secure input with no agent (p. 317)

Sample inbound flow (first contact experience)

> **Note**
> This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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. 9).

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

- If the channel is chat or task, the contact is transferred to the **Set disconnect flow**.
- If the channel is voice, then based on user input the contact is either transferred to the other sample contact flows or a sample follow-up agent task is created for this contact.

Sample AB test

> **Note**
> This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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. 309).

Sample customer queue priority

> **Note**
> This sample flow is available in previous Amazon Connect instances. In new instances, you can see this functionality in Sample queue configurations (p. 311).

Type: Contact flow (inbound)

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

This sample shows how you can use the **Change routing priority/age block** to raise or lower the priority of a contact in a queue. Using this block, there are two ways you can raise or lower a customer's priority:

- Assign them a new priority value, such as 1, to raise their priority.
- Or, increase the routing age of the contact. Customers who are queued longer are routed first, when all contacts have the same queue priority value (such as 5).

Option 1: Raise the priority

- The **Get Customer Input** block prompts the customer to press 1 to move to the front of the queue. This block gets the customer's input; it doesn't actually change the customer's priority.
- If the customer presses 1, they go down the "Pressed 1" branch, which takes them to the **Change routing priority/age block**. This block changes their priority in the queue to 1, which is the highest priority.

Option 2: Change the routing age

- The **Get Customer Input** block prompts the customer to press 2 to move behind existing contacts already in queue. This block gets the customer's input; it doesn't actually change the customer's priority.
- If the customer presses 2, they go down the "Pressed 2" branch, which takes them to a different **Change routing priority/age** block. This block increases their routing age by 10 minutes. This has the effect of moving them ahead of others in the queue who have been waiting longer.

Sample disconnect flow

> **Note**
> This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

Type: Contact flow (inbound)

This sample works with voice, chat, and task contacts.

Chat contacts

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

Voice contacts

1. Sets a user-defined attribute, DisconnectFlowRun. If it = Y, disconnect.
2. Gets customer input, whether they were happy with service.
3. Terminates flow.

Task contacts

1. Checks contact attributes, whether Agent ARN = NULL.

2. Transfers to agent's queue.
3. If at capacity, disconnects.

For a list and description of all the disconnect reasons, see **DisconnectReason** in the ContactTraceRecord (p. 988).

Sample queue configurations

> **Note**
> This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

Type: Contact flow (inbound)

This contact flow shows different ways you can put a customer in queue: you can change the priority of the customer, determine the wait time in queue, and give them an option for a callback. Here's how it works:

1. The customer is put in the BasicQueue.
2. After that, the **Default customer queue** flow is invoked. This block runs a **Loop prompts** block that plays the following:

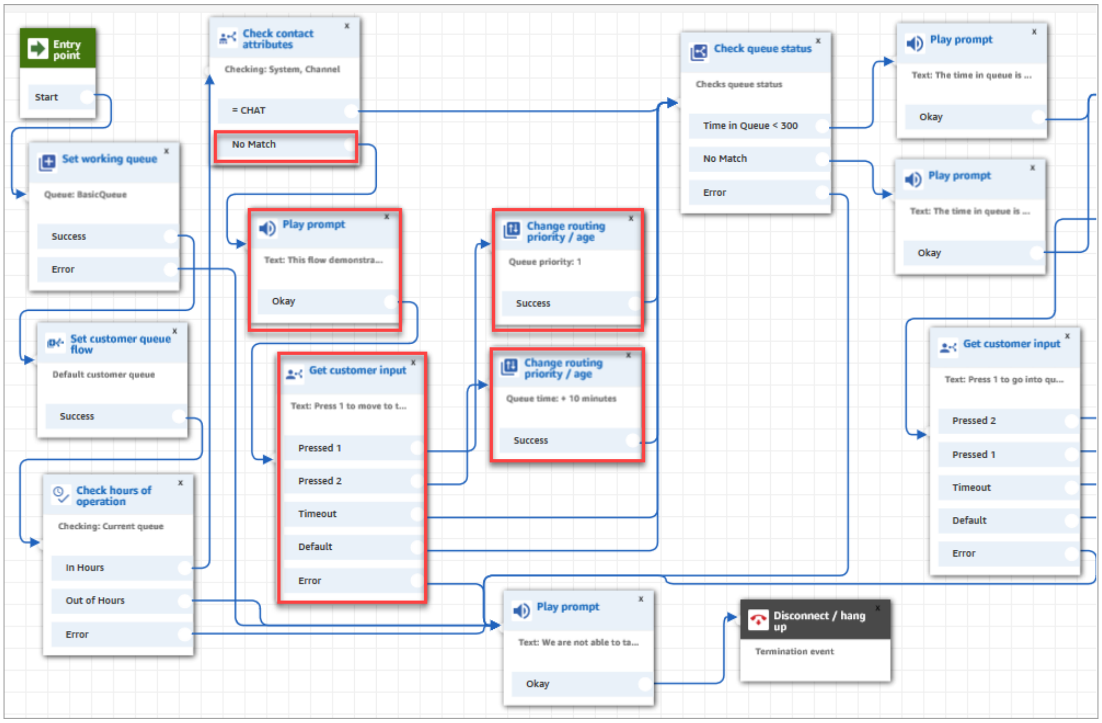
   Thank you for calling. Your call is very important to us and will be answered in the order it was received.
3. The hours of operation are checked with a **Check hours of operation** block.
4. The channel is checked with a **Check contact attributes** block:

   - If chat, we check the time in queue. If it's less than 5 minutes, the customer is placed in queue for an agent. If it's more, we check the channel again and if it's chat, put the customer in queue for an agent.
   - If voice, the customer is routed down the **No Match** branch, to a **Play prompt** block and then to a **Get customer input** block.

     In the **Get customer input** block, we give the customer the option to press 1 to move to the front of the queue or 2 to move to the end of the queue.

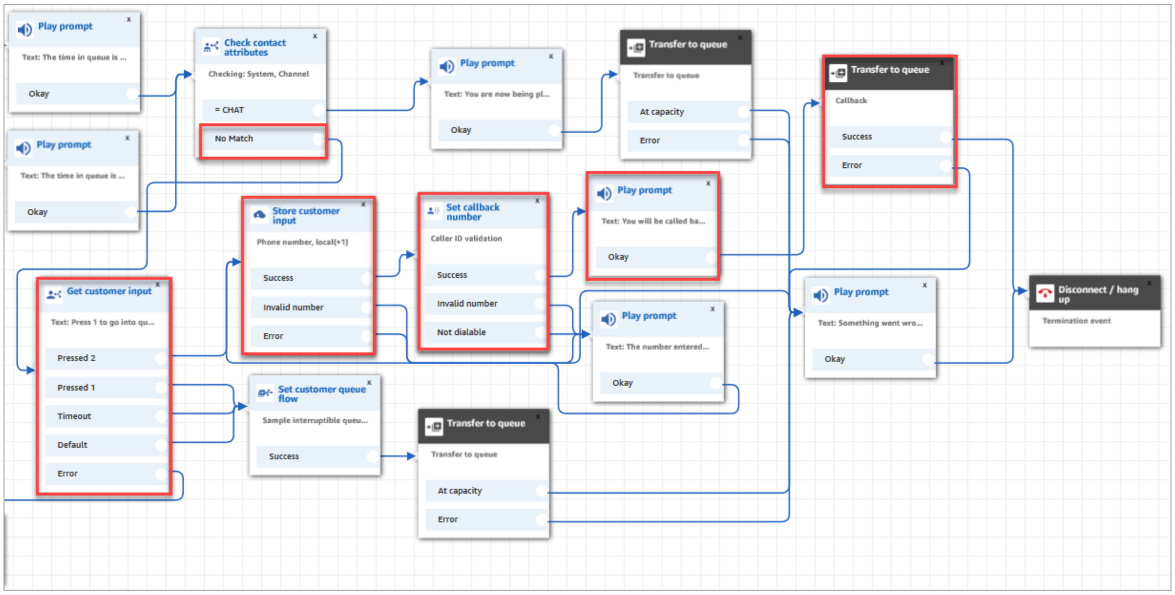
     The two **Change routing priority / age** blocks move the customer to the front or back of the queue.

     You can see this path in the following image:



5. Next we use a **Check queue status** block to check whether the time in queue is less than 300 seconds.
6. We use a **Play prompt** block to tell the customer the results.
7. We use a **Check contact attributes** block again to check the customer's channel: chat or voice/No Match.

These next steps apply to customers who were routed down the voice/**No Match** branch, as shown in the following image:

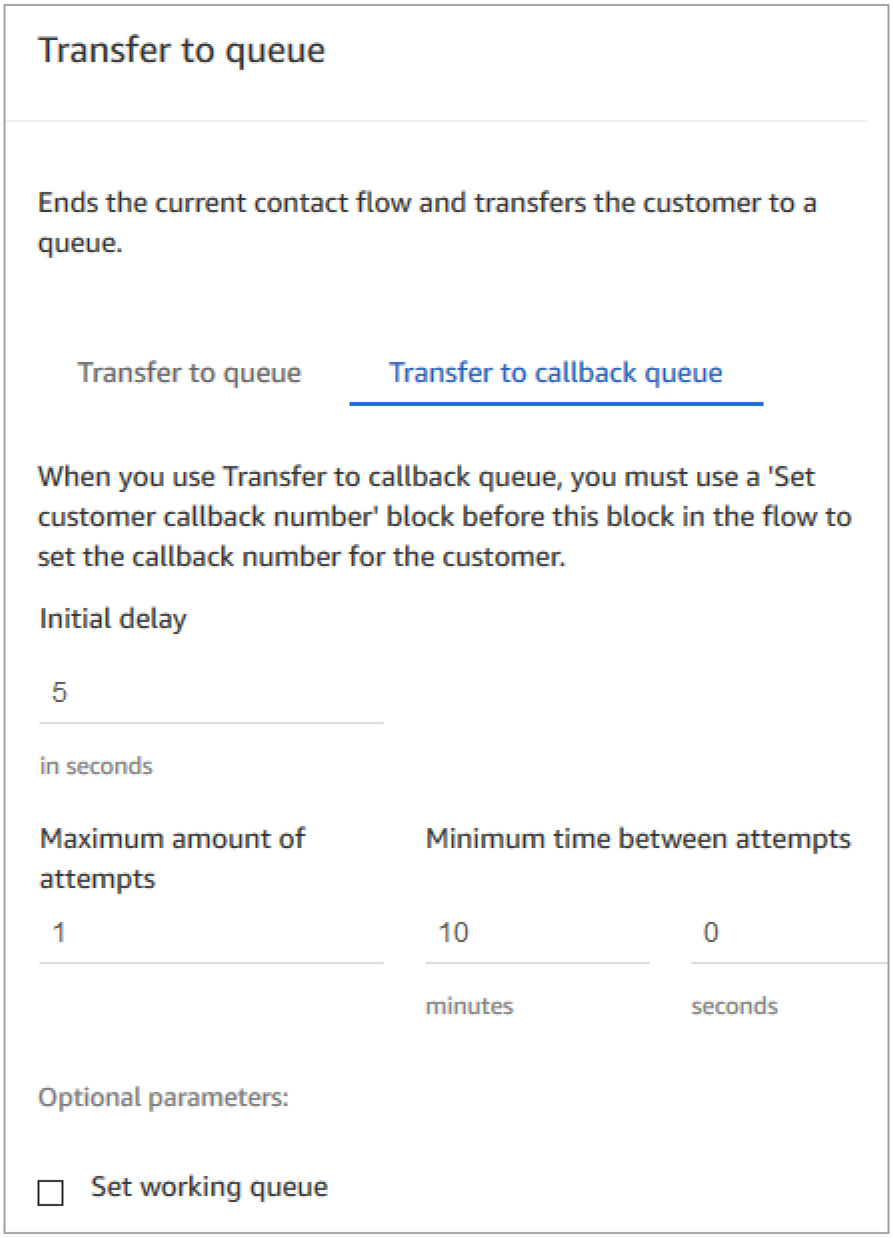


1. In the **Get customer input** block, we prompt customers to *Press 1 to go into queue or 2 to enter a callback number.*

2. If customers press 2, they are routed down the **Pressed 2** branch to the **Store customer input** block.
3. The **Store customer input** block prompts the customer for their phone number.
4. The customer's phone number is stored in the **Stored customer input attribute**, by the **Set callback number** block.
5. We use a **Transfer to queue (p. 437)** block to put the customer in a callback queue.
6. The **Transfer to queue (p. 437)** block is configured so Amazon Connect waits 5 seconds between the time the callback contact is initiated and the contact is enqueued, where it sits until it is offered to an available agent.

   If the initial callback doesn't reach the customer, Amazon Connect will attempt 1 callback. If it were configured for 2 attempted callbacks, it would wait 10 minutes between each one.

   Also, no special callback queue is specified. Rather, customers are in the BasicQueue, which was set at the beginning of the flow.



Transfer to queue

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

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

Initial delay: 5 in seconds

Maximum amount of attempts: 1

Minimum time between attempts: 10 minutes 0 seconds

Optional parameters:

□ Set working queue

For information about queued callbacks, see the following topics:

- Set up queued callback (p. 481)
- Contact block: Transfer to queue (p. 437)
- About queued callbacks in metrics (p. 1002)

Sample queue customer

Note
This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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

Note
This sample flow is available in previous Amazon Connect instances. In new instances, you can see examples of queued callback in Sample interruptible queue flow with callback (p. 315) and Sample queue configurations (p. 311).

Type: Contact flow (inbound)

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

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

For information about queued callbacks, see the following topics:

- Set up queued callback (p. 481)
- Contact block: Transfer to queue (p. 437)
- About queued callbacks in metrics (p. 1002)

Sample interruptible queue flow with callback

Note
This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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

Note
This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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, chat, task. If chat, it returns a fun fact.
4. If voice, the second **Check contact attributes** block is triggered. It checks the match conditions of **State**, which is an external attribute. It uses an external contact attribute because it's getting data by using a process that's external to Amazon Connect
5. A prompt tells you that it's returning you back to **Sample inbound flow**, and then starts the **Transfer flow** block.
6. If the transfer fails, it plays a prompt and then disconnects the contact.

For more information about using attributes, see Lambda functions and attributes (p. 542).

Sample recording behavior

Note
This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

Type: Contact flow (inbound)

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

- If the contact is a task, it is transferred to the Sample inbound flow.
- If the customer is using chat, they get a prompt that the **Set recording block** enables managers to monitor chat conversations. (To *record* chats, you only need to specify an Amazon S3 bucket where the conversation will be stored.)

  To monitor chats, the **Set recording block** is configured to record both the **Agent and Customer**.
- If the contact is using voice, a **Get customer input** block prompts them to enter the number for who they want to record. Their entry triggers the **Set recording behavior** block with the appropriate configuration.

It ends with the customer being transferred by to the Sample inbound flow (p. 309).

For more information, see the following topics:

- Set up recording behavior (p. 479)
- Monitor live conversations (p. 798)
- Review recorded conversations (p. 801)

Sample note for screenpop

> **Note**
> This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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

> **Note**
> This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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. 508) instead of this solution.

Here's how it works:

1. This flow begins with checking the customer's channel. If they are using chat, they are put in a queue.
2. If they are using voice, the agent and customer are put in a conference call.
3. A **Play prompt** tells the customer that the agent will be put on hold while customer enters their credit card information.
4. When the prompt is finished playing, the agent is put on hold using a **Hold customer or agent** block. If an error occurs, a prompt is played that agent was unable to put on hold, after which the contact flow is ended.

5. The customer's input is stored using the **Store Customer Input** block. This block encrypts the sensitive customer information using a signing key that must be uploaded in .pem format. For a detailed walkthrough that explains how to encrypt customer input, see Creating a secure IVR solution with Amazon Connect.
6. After the customer's data is collected, the agent and customer are put back on call using the **Conference All** option in another **Hold customer or agent** block.
7. The error branch runs if there's an error while capturing the customer's data.

Sample secure input with no agent

> **Note**
> This topic explains a sample contact flow that is included with Amazon Connect. For information about locating the sample flows in your instance, see Sample contact flows (p. 308).

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. 309).
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. 309).

Contact block definitions

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

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

Block	Description	
Call phone number (p. 322)	Initiates an outbound call from an outbound whisper flow.	
Amazon Connect Cases (Preview) (p. 344)	Gets, updates, and creates cases.	
Change routing priority / age (p. 325)	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.	
Check call progress (p. 327)	Engages with the output provided by an answering machine, and provides branches to route the contact	

Block	Description	
	accordingly. This block works with high-volume outbound communications only.	
Check contact attributes (p. 329)	Checks the values of contact attributes.	
Check hours of operation (p. 333)	Checks whether the contact is occurring within or outside of the hours of operation defined for the queue.	
Check queue status (p. 335)	Checks the status of the queue based on specified conditions.	
Check Voice ID (p. 339)	Branches based on the enrollment status, voice authentication status, or status of detection of fraudsters in a watchlist of the caller returned by Voice ID.	
Check staffing (p. 342)	Checks the current working queue, or queue you specify in the block, for whether agents are available, staffed, or online. Staffed availability could be on call, or after contact work status.	
Create task (p. 355)	Creates a new task, sets the tasks attributes, and initiates a contact flow to start the task. To learn more about Amazon Connect Tasks, see Tasks (p. 16).	
Customer profiles (p. 359)	Enables you to retrieve, create, and update a customer profile.	
Disconnect / hang up (p. 362)	Disconnects a contact.	
Distribute by percentage (p. 363)	Routes customers randomly based on a percentage.	
End flow / Resume (p. 365)	Ends the current flow without disconnecting the contact.	
Get customer input (p. 366)	Branches based on customer intent.	
Get queue metrics (p. 378)	Retrieves real-time metrics about queues and agents in your contact center and returns them as attributes.	
Hold customer or agent (p. 383)	Places a customer or agent on or off hold.	

Block	Description	
Invoke AWS Lambda function (p. 385)	Calls AWS Lambda, optionally returns key-value pairs.	
Invoke module (p. 387)	Calls a published module.	
Loop (p. 388)	Loops through, or repeats, the **Looping** branch for the number of loops specified.	
Loop prompts (p. 390)	Loops a sequence of prompts while a customer or agent is on hold or in queue.	
Play prompt (p. 393)	Plays an interruptible audio prompt, delivers a text-to-speech message, or delivers a chat response.	
Set callback number (p. 397)	Sets a callback number.	
Set contact attributes (p. 399)	Stores key-value pairs as contact attributes.	
Set customer queue flow (p. 402)	Specifies the flow to invoke when a customer is transferred to a queue.	
Set disconnect flow (p. 403)	Sets the flow to run after a disconnect event.	
Set hold flow (p. 405)	Links from one contact flow type to another.	
Set logging behavior (p. 407)	Enables contact flow logs so you can track events as contacts interact with contact flows.	
Set Voice ID (p. 410)	Sends audio to Amazon Connect Voice ID to verify the caller's identity and match against fraudsters in watchlist, as soon as the call is connected to a contact flow.	
Set recording and analytics behavior (p. 408)	Sets options for recording conversations.	
Set voice (p. 415)	Sets the text-to-speech (TTS) language and voice to be used in the contact flow.	
Set whisper flow (p. 418)	Overrides the default whisper by linking to a whisper flow.	
Set working queue (p. 421)	Specifies the queue to be used when **Transfer to queue** is invoked.	

Block	Description	
Start media streaming (p. 423)	Starts capturing customer audio for a contact.	
Stop media streaming (p. 425)	Stops capturing customer audio after it is started with a **Start media streaming** block.	
Store customer input (p. 426)	Stores numerical input to a contact attribute.	
Transfer to agent (beta) (p. 430)	Transfers the customer to an agent.	
Transfer to flow (p. 431)	Transfers the customer to another contact flow.	
Transfer to phone number (p. 433)	Transfers the customer to a phone number external to your instance.	
Transfer to queue (p. 437)	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.	
Wait (p. 441)	Pauses the contact flow.	
Wisdom (p. 443)	Associates a Wisdom domain to a contact to enable real-time recommendations.	

Supported channels for contact blocks

The following table lists all available contact blocks, and whether they support routing a contact through the specified channels.

Block	Voice	Chat	Task
Call phone number (p. 322)	Yes	No - Error branch	No - Error branch
Cases (p. 344)	Yes	Yes	Yes
Change routing priority / age (p. 325)	Yes	No	Yes
Check call progress (p. 327)	Yes	No - Error branch	No - Error branch
Check contact attributes (p. 329)	Yes	Yes	Yes

Block	Voice	Chat	Task
Check hours of operation (p. 333)	Yes	Yes	Yes
Check queue status (p. 335)	Yes	Yes	Yes
Check Voice ID (p. 339)	Yes	No - Error branch	No - Error branch
Check staffing (p. 342)	Yes	Yes	Yes
Create task (p. 355)	Yes	Yes	Yes
Customer profiles (p. 359)	Yes	Yes	Yes
Disconnect / hang up (p. 362)	Yes	Yes	Yes
Distribute by percentage (p. 363)	Yes	Yes	Yes
End flow / Resume (p. 365)	Yes	Yes	Yes
Get customer input (p. 366)	Yes	Yes when Amazon Lex is used Otherwise, No - Error branch	Yes
Get queue metrics (p. 378)	Yes	Yes	Yes
Hold customer or agent (p. 383)	Yes	No - Error branch	No - Error branch
Invoke AWS Lambda function (p. 385)	Yes	Yes	Yes
Invoke module (p. 387)	Yes	Yes	Yes
Loop (p. 388)	Yes	Yes	Yes
Loop prompts (p. 390)	Yes	No - Error branch	No - Error branch
Play prompt (p. 393)	Yes	Yes	No - takes the **Okay** branch, but it has no effect
Set callback number (p. 397)	Yes	No - Error branch	No - Error branch
Set contact attributes (p. 399)	Yes	Yes	Yes
Set customer queue flow (p. 402)	Yes	Yes	Yes

Block	Voice	Chat	Task
Set disconnect flow (p. 403)	Yes	Yes	Yes
Set hold flow (p. 405)	Yes	No - Error branch	No - Error branch
Set logging behavior (p. 407)	Yes	Yes	Yes
Set recording and analytics behavior (p. 408)	Yes	Yes	No - Error branch
Set Voice ID (p. 410)	Yes	No - Error branch	No - Error branch
Set voice (p. 415)	Yes	No - Success branch	No - Success branch
Set whisper flow (p. 418)	Yes	Yes	Yes
Set working queue (p. 421)	Yes	Yes	Yes
Start media streaming (p. 423)	Yes	No - Error branch	No - Error branch
Stop media streaming (p. 425)	Yes	No - Error branch	No - Error branch
Store customer input (p. 426)	Yes	No - Error branch	No - Error branch
Transfer to agent (beta) (p. 430)	Yes	No - Error branch	No - Error branch
Transfer to flow (p. 431)	Yes	Yes	Yes
Transfer to phone number (p. 433)	Yes	No - Error branch	No - Error branch
Transfer to queue (p. 437)	Yes	Yes	Yes
Wait (p. 441)	No - Error branch	Yes	Yes

Contact block: Call phone number

Description

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

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

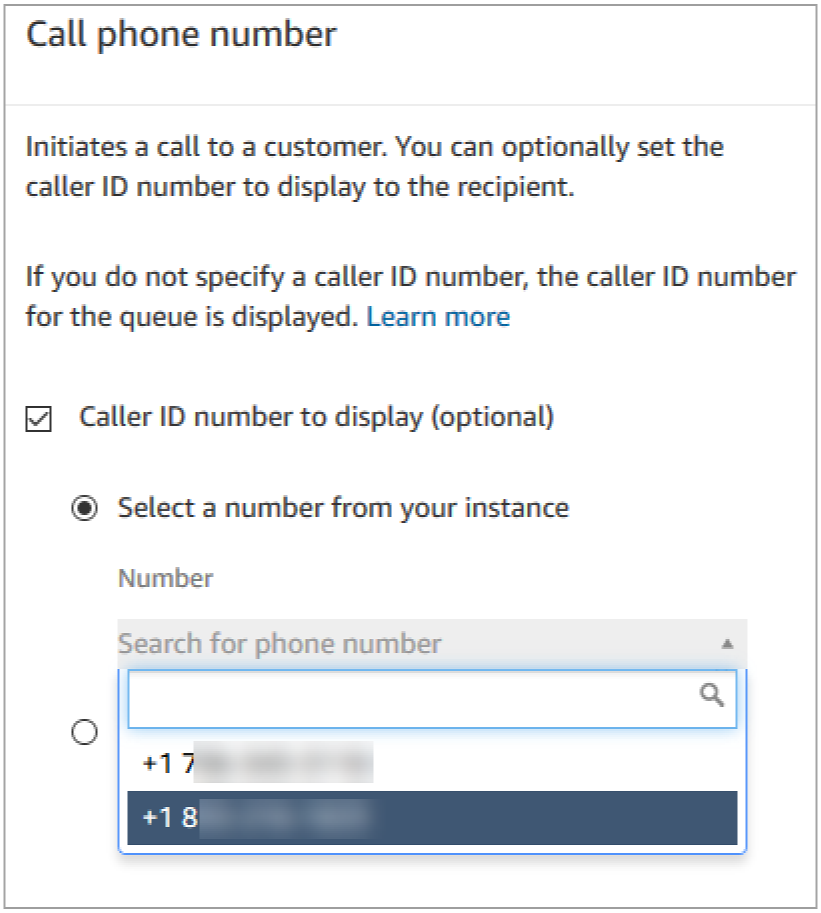
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

- Outbound Whisper flow

Properties



Call phone number

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

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

☑ Caller ID number to display (optional)

● Select a number from your instance

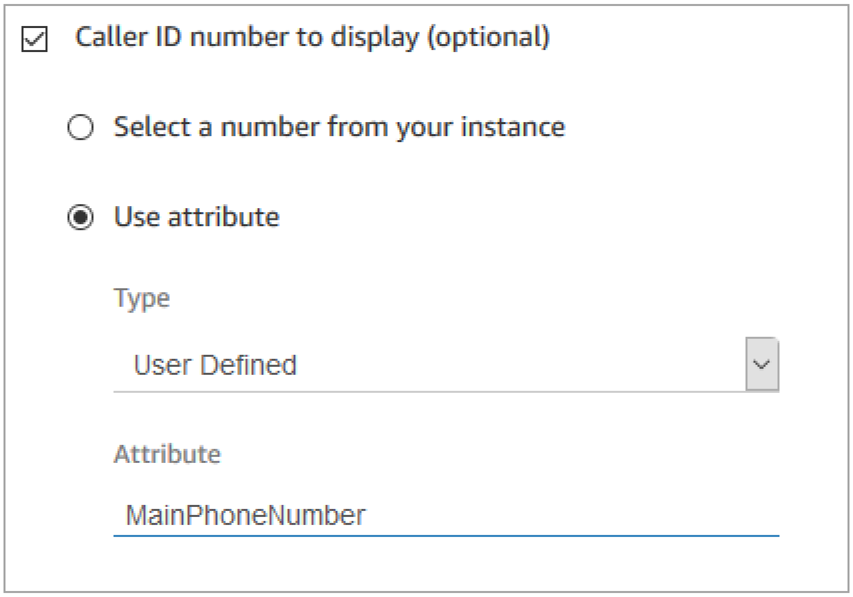
Number

Search for phone number ▲

+1 7[redacted]

+1 8[redacted]

○



☑ Caller ID number to display (optional)

○ Select a number from your instance

● Use attribute

Type

User Defined

Attribute

MainPhoneNumber

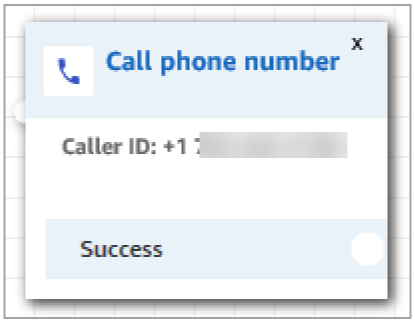
Outbound whisper flows run in Amazon Connect immediately after an agent accepts the call during direct dial and callback scenarios. When the contact flow runs:

- The caller ID number is set if one is specified in the Call phone number (p. 322) block.
- If no caller ID is specified in the Call phone number (p. 322) 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 (p. 322) block, the call is disconnected and the agent is placed in **AfterContactWork** (ACW).

Only published contact flows can be selected as the outbound whisper flow for a queue.

Configured block

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



Call phone number

Caller ID: +1 [redacted]

Success

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).

Sample flows

See these sample flows for scenarios that use this block:

- Sample customer queue priority (p. 309)

- Sample queue configurations (p. 311)

Scenarios

See these topics for more information about caller ID works:

- Set up outbound caller ID (p. 212)

Contact block: Change routing priority / age

Description

- Change a customer's position in the queue. For example, move the contact to the front of the queue, or to the back of the queue.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

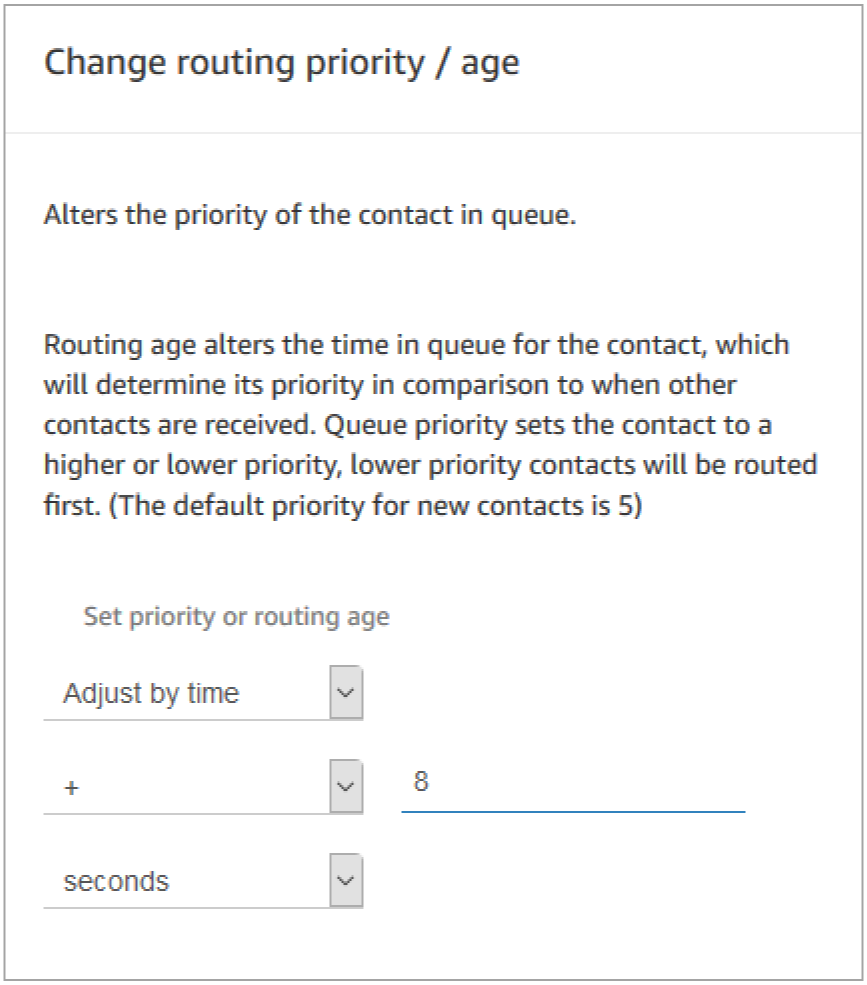
Channel	Supported?
Voice	Yes
Chat	No
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Change routing priority / age

Alters the priority of the contact in queue.

Routing age alters the time in queue for the contact, which will determine its priority in comparison to when other contacts are received. Queue priority sets the contact to a higher or lower priority, lower priority contacts will be routed first. (The default priority for new contacts is 5)

Set priority or routing age

Adjust by time

+ 8

seconds

This block gives you two options for changing a customer's position in queue:

- **Set priority**. The default priority for new contacts is 5. You can raise the priority of a contact - compared to other contacts in the queue - by assigning them a higher priority, such as 1 or 2.
- **Adjust by time**. You can add or subtract seconds or minutes from the amount of time the current contact spends in queue. Contacts are routed to agents on a first-come, first-served basis. So changing their amount of time in queue compared to others also changes their position in queue.

Here's how this block works:

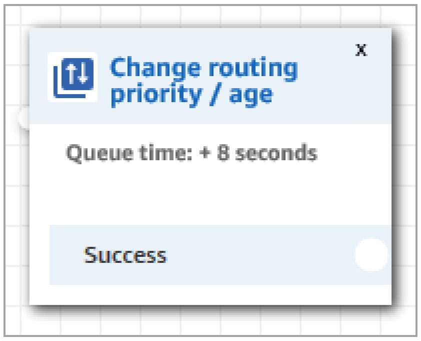
1. Amazon Connect takes the actual “time in queue” for the contact (in this case, how long this specific contact has spent in queue so far), and adds the number of seconds you specified in the **Adjust by time** property.
2. The additional seconds makes this specific contact look artificially older than it is.
3. The routing system now perceives this contact's “time in queue” as longer than it actually is, which affects its position within the ranked list.

Configuration tips

- When using this block, it takes at least 60 seconds for a change to take effect for contacts already in queue.
- If you need a change in a contact's priority to take effect immediately, set the priority before putting the contact in queue, that is, before using a Transfer to queue (p. 437) block.

Configured block

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample customer queue priority (p. 309)
- Sample queue configurations (p. 311)

Scenarios

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

- Routing profiles (p. 21)
- How routing works (p. 221)

Contact block: Check call progress

> **Important**
> This block works with high-volume outbound communications (p. 215) only. It is in public preview and not available in all Regions.

Description

- Engages with the output provided by an answering machine, and provides branches to route the contact accordingly.
- It supports the following branches:
  - **Call answered**: The call has been answered by a person.
  - **Voicemail (beep)**: Amazon Connect identifies that the call ended in a voicemail and it detects a beep.

- **Voicemail (no beep)**:
  - Amazon Connect identifies that the call ended in a voicemail but it doesn't detect a beep.
  - Amazon Connect identifies that the call ended in a voicemail, but the beep is unknown.
- **Not detected**: Could not detect whether there is voicemail. This happens when Amazon Connect is unable to make a positive determination of whether a call was answered by a live voice or an answering machine. Typical situations that land in this state include long silences or excessive background noise.
- **Error**: If any errors are encountered due to Amazon Connect not running correctly after media has been established on the call, this is the path that will be taken by the contact flow. Media is established when the call is either answered by a live voice or by an answering machine. If the call is rejected by the network or encounters a system error while placing the outbound call, the contact flow will not be run.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

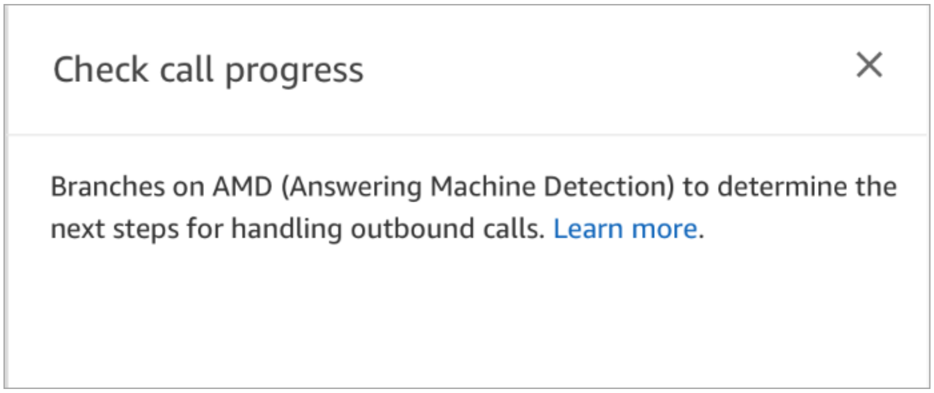
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All contact flow types

Properties

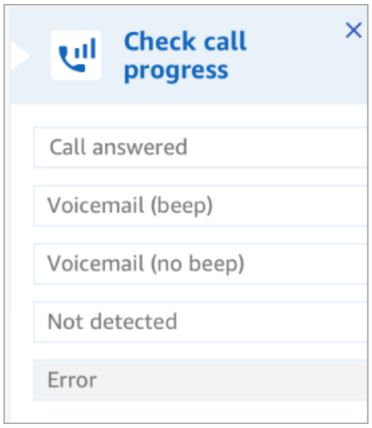


Check call progress

Branches on AMD (Answering Machine Detection) to determine the next steps for handling outbound calls. Learn more.

Configured block

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



Contact block: Check contact attributes

Description

- Branches based on a comparison to the value of a contact attribute.
- Supported comparisons include: **Equals**, **Is Greater Than**, **Is Less Than**, **Starts With**, **Contains**.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

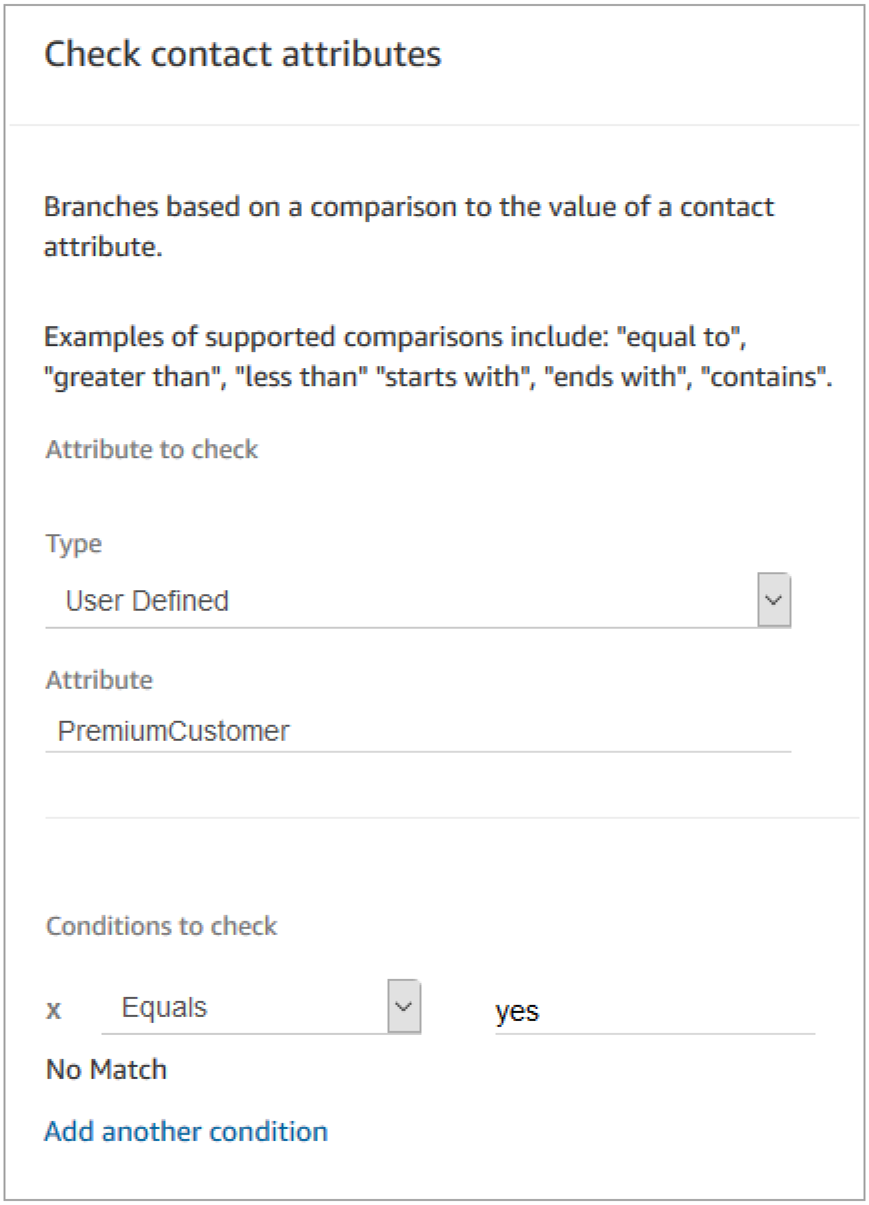
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Check contact attributes

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

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

Attribute to check

Type

User Defined

Attribute

PremiumCustomer

Conditions to check

x Equals yes

No Match

Conditions to check can be dynamic

You can check conditions like the following:

- $.Attributes.verificationCode

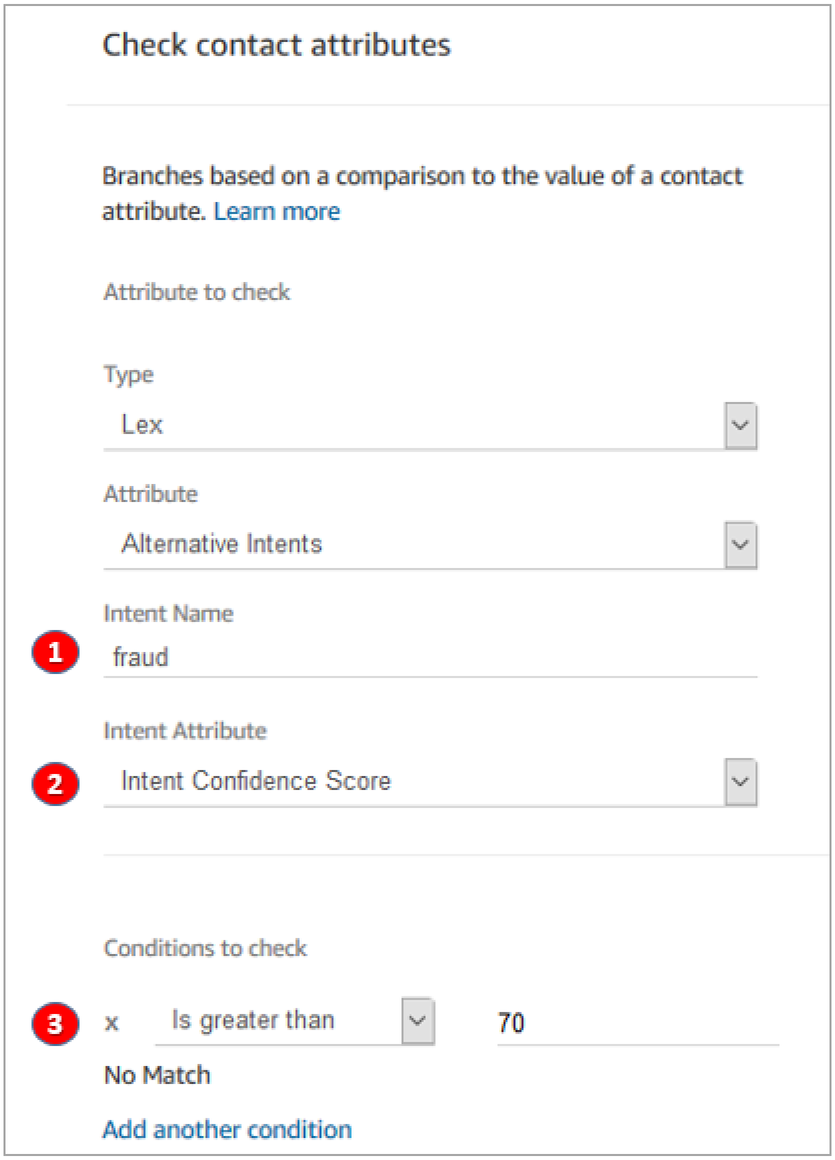
To check for a NULL value, you need to use a Lambda.

Amazon Lex attributes

You can set attributes that are **Type** = **Lex** as follows:

- **Alternative Intents**: Usually you configure contact flows to branch on the winning Lex intent. However, in some situations, you might want to branch on an alternate intent. That is, what the customer might have meant.

  For example, the following alternative intent indicates that if Amazon Lex is more than 70% confident the customer meant *fraud*, the flow should branch accordingly.

  Check contact attributes

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

  Attribute to check

  Type: Lex

  Attribute: Alternative Intents

  1 Intent Name: fraud

  2 Intent Attribute: Intent Confidence Score

  Conditions to check

  3 x Is greater than 70

  No Match

  Add another condition

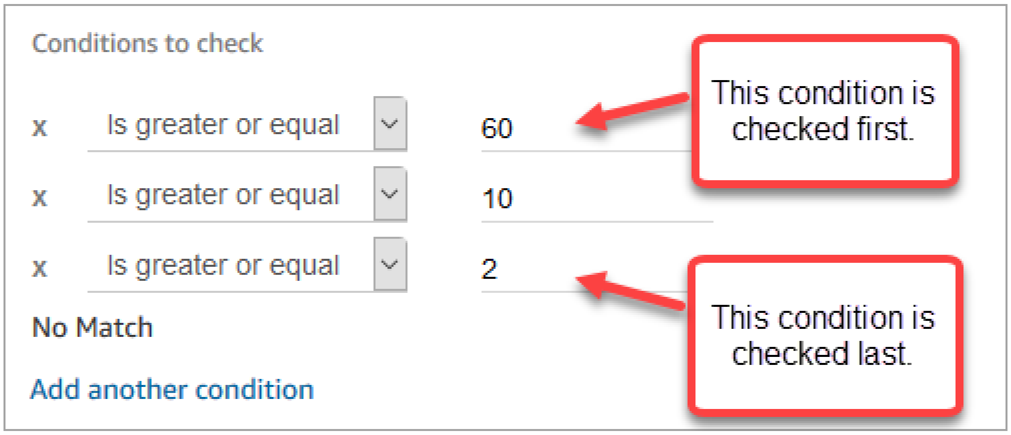
  1. **Intent name** is the name of an alternate intent in Lex. It's case sensitive and must match what's in Lex exactly.
  2. **Intent Attribute** is what Amazon Connect is going to check. In this example, it's going to check the **Intent Confidence Score**.
  3. **Conditions to check**: If Lex is 70% certain the customer meant the alternate intent instead of the winning intent, branch.
- **Intent Confidence Score**: How confident is the bot that it understands the customer's intent. For example, if the customer says "I want to update an appointment," *update* can mean *reschedule* or *cancel*. Amazon Lex provides the confidence score on a scale of 0 to 1:
  - 0 = not at all confident

  - .5 = 50% confident
  - 1 = 100% confident
- **Intent Name**: The user intent returned by Amazon Lex.
- **Sentiment Label**: What is the winning sentiment, the one with the highest score. You can branch on POSITIVE, NEGATIVE, MIXED, or NEUTRAL.
- **Sentiment Score**: Amazon Lex integrates with Amazon Comprehend to determine the sentiment expressed in an utterance:
  - Positive
  - Negative
  - Mixed: The utterance expresses both positive and negative sentiments.
  - Neutral: The utterance does not express either positive or negative sentiments.
- **Session Attributes**: Map of key-value pairs representing the session-specific context information.
- **Slots**: Map of intent slots (key/value pairs) Amazon Lex detected from the user input during the interaction.

Configuration tips

- If you have multiple conditions to compare, Amazon Connect checks them in the order they are listed.

  For example, in the following image Amazon Connect compares the **greater than 60** condition first and compares **greater than 2** last.



Conditions to check

x Is greater or equal 60

x Is greater or equal 10

x Is greater or equal 2

No Match

Add another condition

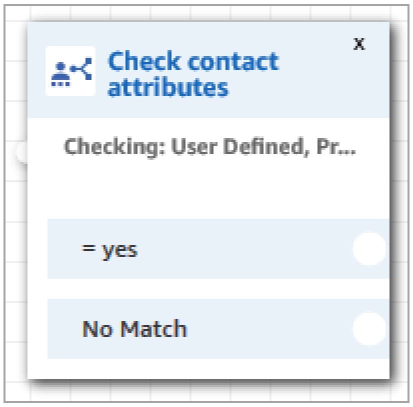
This condition is checked first.

This condition is checked last.

- This block doesn't support case-insensitive pattern matching. For example, if you're trying to match against the word **green** and the customer types **Green**, it would fail. You would have to include every permutation of upper and lower-case letters.

Configured

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 309)
- Sample interruptible queue flow with callback (p. 315)

Scenarios

See these topics for scenarios that use this block:

- How to reference contact attributes (p. 531)
- Route based on contact's channel (p. 536)
- How to reference contact attributes (p. 531)

Contact block: Check hours of operation

Description

- Checks whether the contact is occurring within or outside of the hours of operation defined for the queue.
- Branches based on specified hours of operation.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

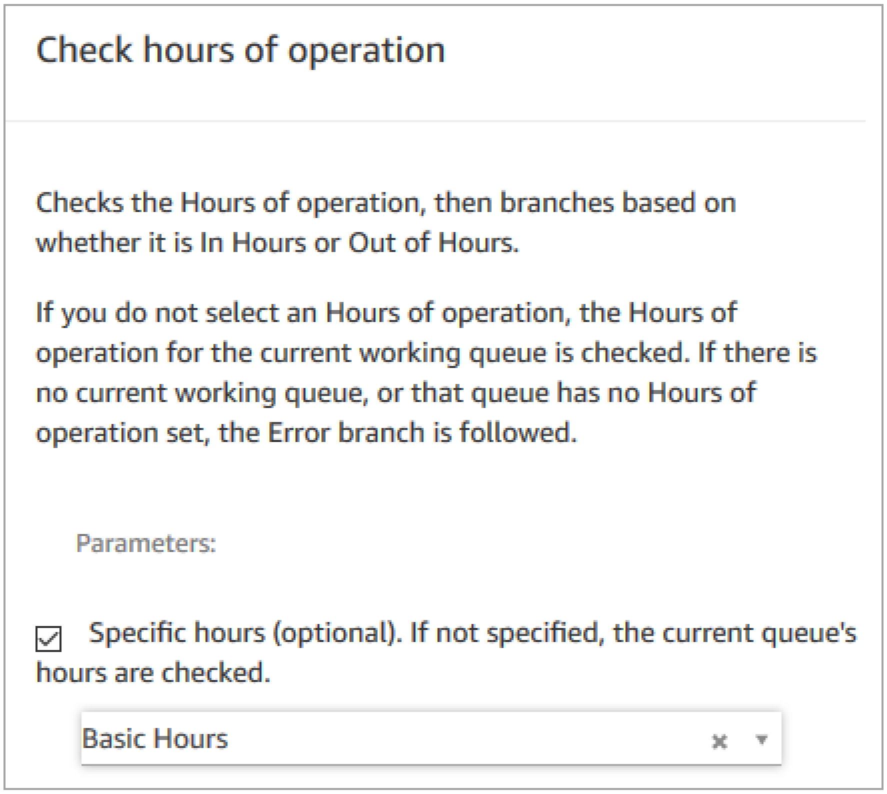
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Check hours of operation

Checks the Hours of operation, then branches based on whether it is In Hours or Out of Hours.

If you do not select an Hours of operation, the Hours of operation for the current working queue is checked. If there is no current working queue, or that queue has no Hours of operation set, the Error branch is followed.

Parameters:

☑ Specific hours (optional). If not specified, the current queue's hours are checked.

Basic Hours

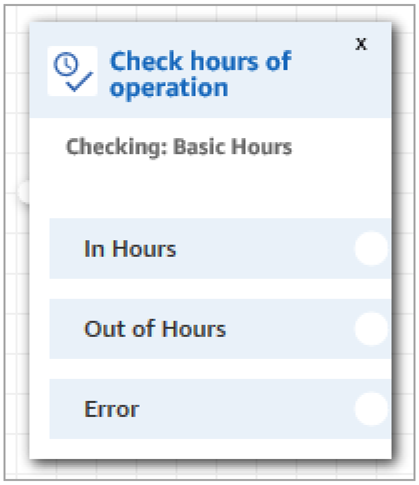
You can set up multiple hours of operation so you have one for various queues. For instructions, see Set the hours of operation and timezone for a queue (p. 225).

Configuration tips

- Agent queues (p. 22) that are automatically created for each agent in your instance do not include an hours of operation.
- If you use this block to check the hours of operation for an agent queue, the check fails and the contact is routed down the **Error** branch.

Configured block

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



Related topics

- Set the hours of operation and timezone for a queue (p. 225)

Sample flows

Sample inbound flow (first contact experience) (p. 309)

Scenarios

See these topics for scenarios that use this block:

- Manage contacts in a queue (p. 476)

Contact block: Check queue status

Description

- Checks the status of the queue based on specified conditions.
- Branches based on the comparison of **Time in Queue** or **Queue capacity**.
  - **Time in queue** is the amount of time the oldest contact spends in queue, before they are routed to an agent or removed from the queue.
  - **Queue capacity** is number of contacts waiting in a queue.
- If no match is found, the **No Match** branch is followed.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes

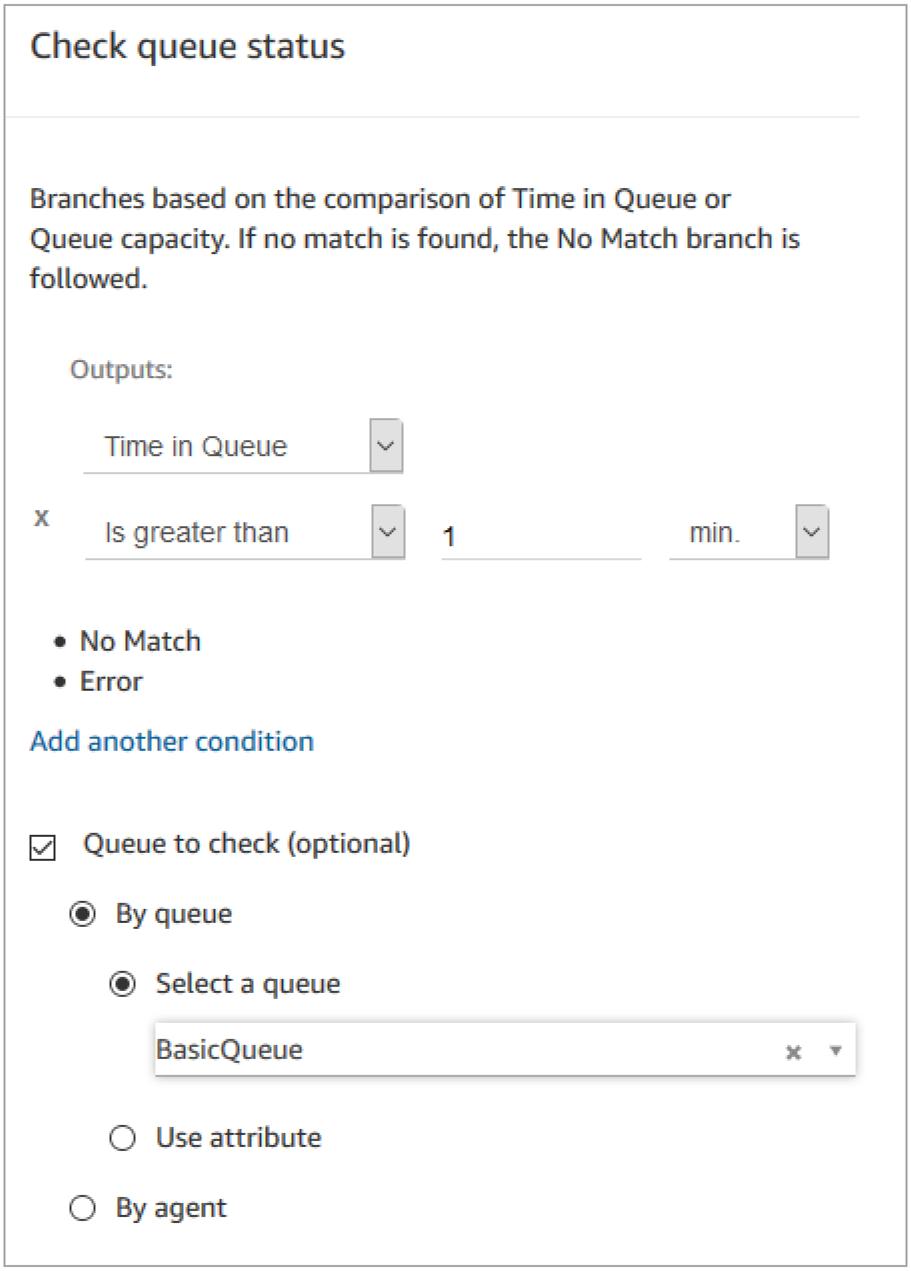
Channel	Supported?
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Check queue status

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

Outputs:

Time in Queue

x Is greater than 1 min.

- No Match
- Error

Add another condition

☑ Queue to check (optional)

● By queue

● Select a queue

BasicQueue

○ Use attribute

○ By agent

Configuration tips

The order in which you add conditions matters at the runtime. Results are evaluated against conditions in the same order in which you add them to the block. Contacts are routed down the first condition to match.

For example, in the following condition order, every value matches one of first two conditions. None of the other conditions are ever matched.

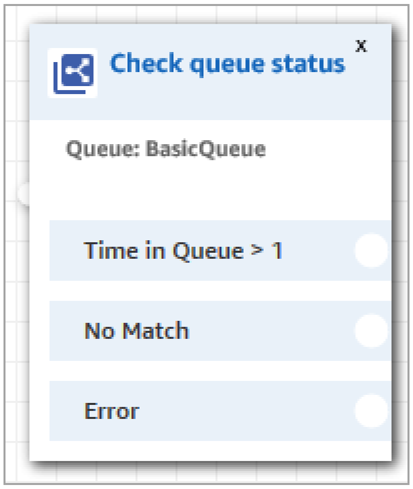
```
Time in Queue <= 90
Time in Queue >= 90
Time in Queue >= 9
Time in Queue >= 12
Time in Queue >= 15
Time in Queue >= 18
Time in Queue > 20
Time in Queue > 21
```

In this next example, all contacts with a wait time in queue of 90 or less (<=90) match first condition only. This means less than or equal to 9 (<=9), <=12, <=15, <=18, <=20, <=21 are never run. Any value greater than 90 is routed down the greater than or equal to 21 (>=21) condition branch.

```
Time in Queue <= 90
Time in Queue <= 9
Time in Queue <= 12
Time in Queue <= 15
Time in Queue <= 18
Time in Queue <= 20
Time in Queue <= 21
Time in Queue >= 21
```

Configured block

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



Queue: BasicQueue

Scenarios

See these topics for scenarios that use this block:

- Manage contacts in a queue (p. 476)

Contact block: Check Voice ID

Description

Note
The Set Voice ID (p. 410) block needs to be set in the contact flow before this one. That block sends audio to Amazon Connect Voice ID (p. 858) to verify the customer's identity, and returns a status.

The **Check Voice ID** block branches based on the results of the voice analysis and the status returned by Voice ID:

- **Enrollment status**:
  - **Enrolled**: The caller is enrolled in voice authentication.
  - **Not enrolled**: The caller has not yet been enrolled in voice authentication. When this status is returned, for example, you may want to directly route the call to an agent for enrollment.
  - **Opted out**: The caller has opted out of voice authentication.

  You are not charged for checking enrollment status.
- **Voice authentication status**:
  - **Authenticated**: The caller's identity has been verified. That is, the authentication score is greater than or equal to the threshold (default threshold of 90 or your custom threshold).
  - **Not authenticated**: The authentication score is lower than threshold that you configured.
  - **Inconclusive**: Unable to analyze a caller's speech for authentication. This is usually because Voice ID did not get the required 10 seconds to provide a result for authentication.
  - **Not enrolled**: The caller has not yet been enrolled in voice authentication. When this status is returned, for example, you may want to directly route the call to an agent for enrollment.
  - **Opted out**: The caller has opted out of voice authentication.

  You are not charged if the result is **Inconclusive**, **Not enrolled** or **Opted out**.
- **Fraud detection status**:
  - **High risk**: The risk score meets or exceeds the set threshold.
  - **Low risk**: The risk score did not meet the set threshold.
  - **Inconclusive**: Unable to analyze a caller's voice for detection of fraudsters in a watchlist.

  You are not charged if the result is **Inconclusive**.

Note
For **Enrollment status** and **Voice authentication**, the Customer ID (p. 517) system attribute needs to be set in Set contact attributes (p. 399) block because they are acting on a specific customer. You don't need to do this for **Fraud detection** because it's not acting on a specific customer but rather detecting whether the incoming caller matches a fraudster on your watchlist. This means it's possible for a customer to be successfully authenticated and still have high fraud risk.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes

Channel	Supported?
Chat	No - Error branch
Task	No - Error branch

Contact flow types

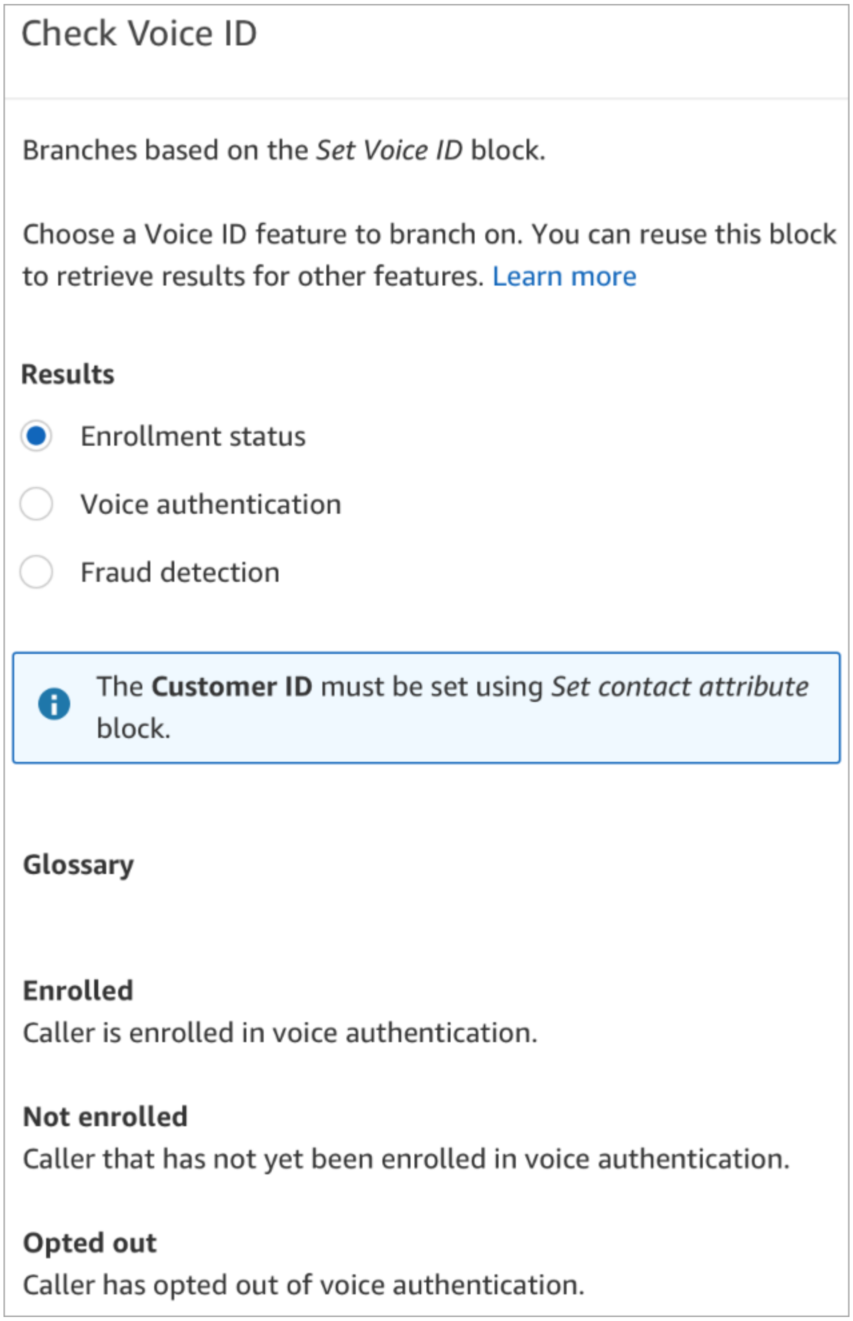
You can use this block in the following contact flow types (p. 445):

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

Properties

This block doesn't have any properties that you set. Rather, it creates branches for you to route contacts based on the result of the authentication threshold and voiceprint evaluation that Set Voice ID (p. 410) returns.

The following image shows what this block looks like when it's configured to check for Enrollment status. Different status results are returned when it's configured for **Voice authentication** or **Fraud detection**.



Check Voice ID

Branches based on the *Set Voice ID* block.

Choose a Voice ID feature to branch on. You can reuse this block to retrieve results for other features. Learn more

Results

● Enrollment status

○ Voice authentication

○ Fraud detection

The **Customer ID** must be set using *Set contact attribute* block.

Glossary

Enrolled
Caller is enrolled in voice authentication.

Not enrolled
Caller that has not yet been enrolled in voice authentication.

Opted out
Caller has opted out of voice authentication.

Configuration tips

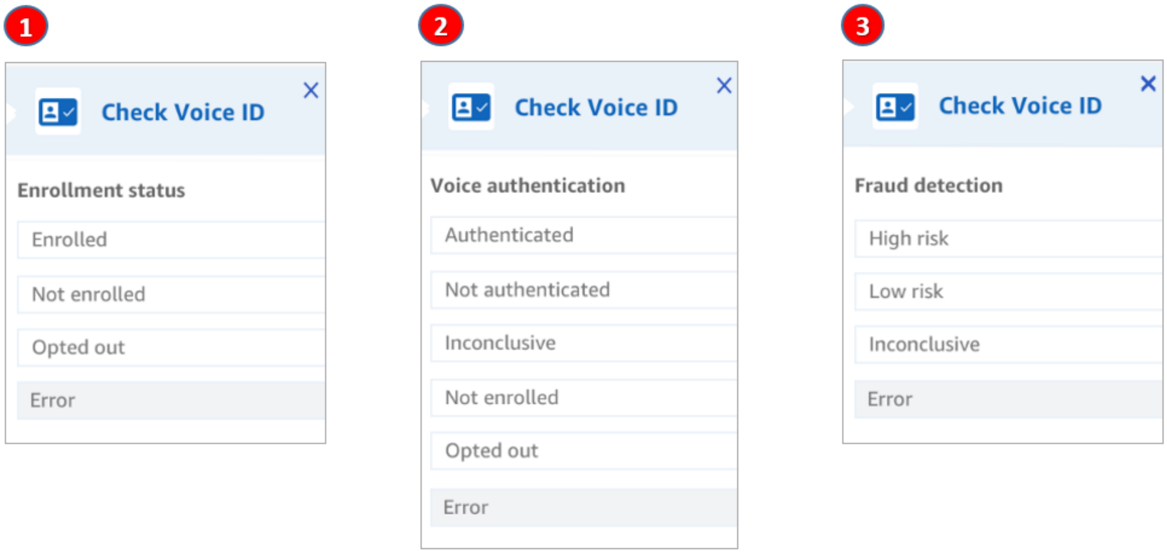
When you create a contact flow that uses this block, add these blocks in the following order:

1. Set Voice ID (p. 410) block.
2. Set contact attributes (p. 399) block: For **Enrollment status** and **Voice authentication**, the Customer ID (p. 517) system attribute needs to be set in Set contact attributes (p. 399) block because it is acting on a specific customer.
3. **Check Voice ID** block.

Configured block

The following image shows what this block looks like when it's configured to check for:

1. Enrollment status
2. Voice authentication
3. Fraud detection



More information

See the following topic for more information about this block:

- Use real-time caller authentication with Voice ID (p. 858)
- Use Voice ID (p. 1189)

Contact block: Check staffing

Description

- Checks the current working queue, or queue you specify in the block, for whether agents are available (p. 919), staffed (p. 925), or online (p. 923).
- Before transferring a call to agent and putting that call in a queue, use the **Check hours of operation** and **Check staffing** blocks. They verify that the call is within working hours and that agents are staffed to service.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes

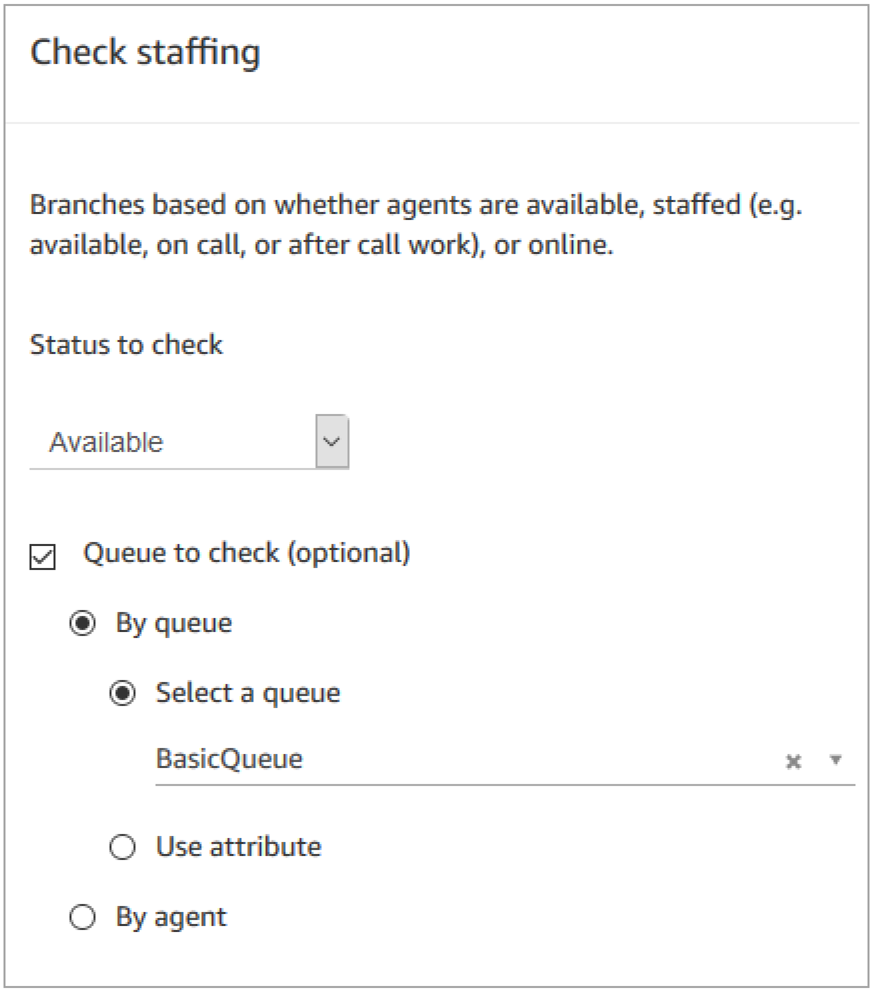
Channel	Supported?
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Check staffing

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

Status to check

Available

☑ Queue to check (optional)

● By queue

● Select a queue

BasicQueue

○ Use attribute

○ By agent

In the **Status to check** dropdown box, choose one of the following options:

- Available (p. 919) = Check whether the agent has **Available** slots to be routed a contact.

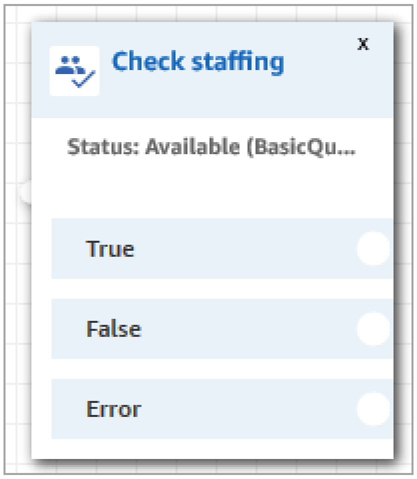
- Staffed (p. 925) = Check whether agents have **Available** slots, or are **On call**, or are in **After Contact Work**.
- Online (p. 923) = Check whether agents are **Available**, in the **Staffed** state, or in a custom state.

Configuration tips

- You must set a queue before using a **Check staffing** block in your contact flow. You can use a Set working queue (p. 421) block to set the queue.
- If a queue is not set, the contact is routed down the **Error** branch.
- When a contact is transferred from one flow to another, the queue that is set in a contact flow is passed from that flow to the next flow.

Configured block

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



Scenarios

See these topics for scenarios that use this block:

- Transfer contacts to a specific agent (p. 477)

Contact block: Cases (Preview)

Description

- Gets, updates, and creates cases.
- You can link a contact to a case, and then the contact will be recorded in the **Activity feed** of the case. When the agent accepts a contact that is linked to a case, the case automatically opens as a new tab in the agent application.
- While you can link contacts to multiple cases, there is a limit of five new case tabs automatically opening in the agent application. These will be the five most recently updated cases.
- For more information about cases, see Amazon Connect Cases (Preview) (p. 733).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

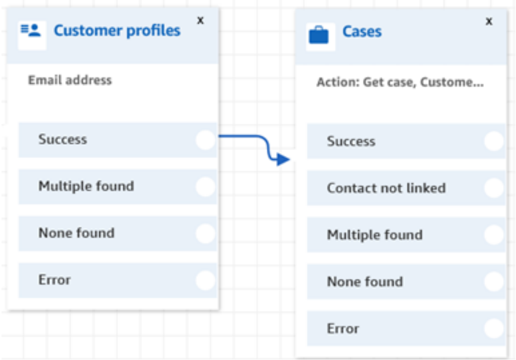
- All flows

Properties: Get case

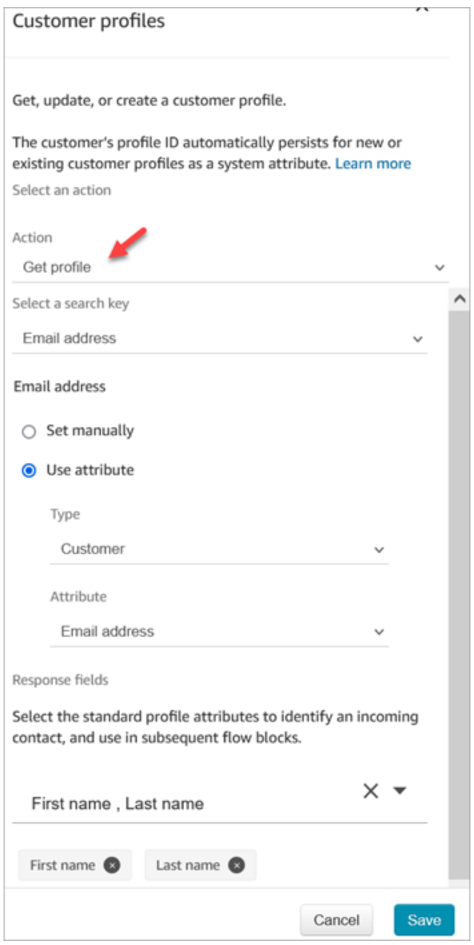
When configuring properties to get a case:

- You must provide at least one search criteria. Otherwise this block will take the **Error** branch.

  You can either use attribute in the Cases namespace or set manually. If you set manually, see to the syntax in How to persist fields throughout the flow (p. 352).
- To get cases for a given customer, add a Customer profiles (p. 359) block to the flow before creating the case.

  Configure the Customer profiles (p. 359) block to get the customer profile.



Customer profiles

Get, update, or create a customer profile.

The customer's profile ID automatically persists for new or existing customer profiles as a system attribute. Learn more

Select an action

Action: Get profile

Select a search key: Email address

Email address

○ Set manually

● Use attribute

Type: Customer

Attribute: Email address

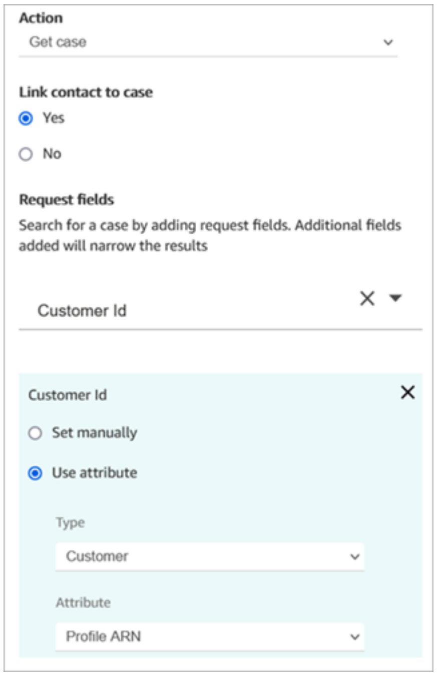
Response fields

Select the standard profile attributes to identify an incoming contact, and use in subsequent flow blocks.

First name , Last name

First name ⊗ Last name ⊗

In the **Cases** block, on the **Properties** page configure the **Customer ID** section as shown in the following image:



Action
Get case

Link contact to case
● Yes
○ No

Request fields
Search for a case by adding request fields. Additional fields added will narrow the results

Customer Id

Customer Id
○ Set manually
● Use attribute

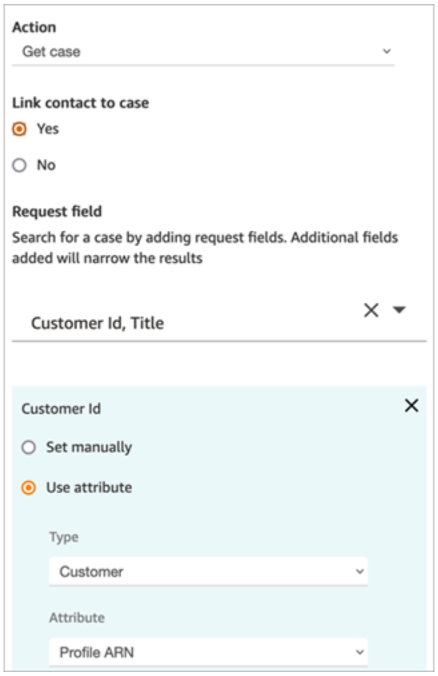
Type
Customer

Attribute
Profile ARN

- You can specify to get only the last updated case for any search criteria. This can be achieved by selecting **Get last updated case**.
- You can persist case fields in the case namespace to make use of them in blocks that are in your flow after the **Cases** block that is configured to **Get case**. This can be achieved by making use of the **Response fields** section and selecting fields that you want to use in the other blocks.

  You can either use attribute in the Cases namespace or set manually. If you set manually, see to the syntax in How to persist fields throughout the flow (p. 352).
- The **Get case** properties show the options for the single-select field type.
- The **Get case** properties use the Contains function for text field type.
- The **Get case** properties use the EqualTo function for fields of type: number, boolean.
- The **Get case** properties use greater than or equal to for any date field search.
- Contacts can be routed down the following branches:
  - **Success**: The case was found.
  - **Contact not linked**: If you specify to link the contact to case, then this error branch will appear. It might be that the contact was not linked after the case is retrieved (partial success/partial failure). If this happens, then the flow will follow this branch.
  - **Multiple found**: Multiple cases are found with the search criteria.
  - **None found**: No cases are found with the search criteria.
  - **Error**: An error was encountered while trying to find the case. This may be due to a system error or how **Get case** is configured.

The following images show an example of a **Get case** configuration. The first image shows how to configure the block to search for a case by Customer ID and Title. The Customer Id is being pulled in from the Profile ARN of the customer:



Action
Get case

Link contact to case
● Yes
○ No

Request field
Search for a case by adding request fields. Additional fields added will narrow the results

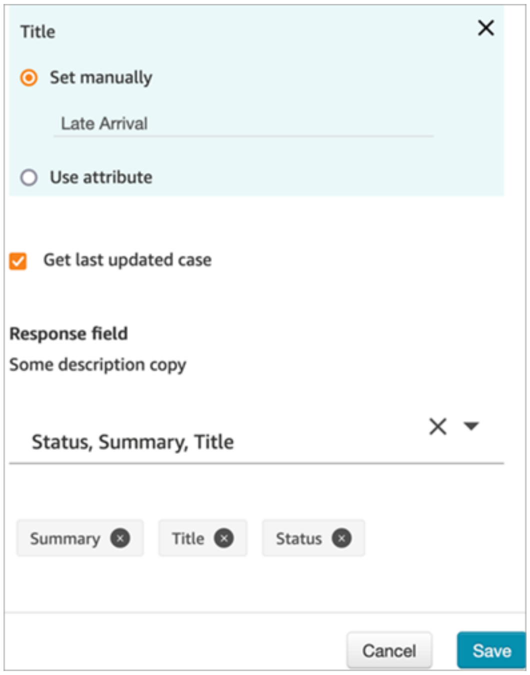
Customer Id, Title

Customer Id
○ Set manually
● Use attribute

Type
Customer

Attribute
Profile ARN

This next image shows the block configured to search by **Late Arrival**. Three fields will be shown to the agent: **Status**, **Summary**, **Title**.



Title
● Set manually
Late Arrival
○ Use attribute

☑ Get last updated case

Response field
Some description copy

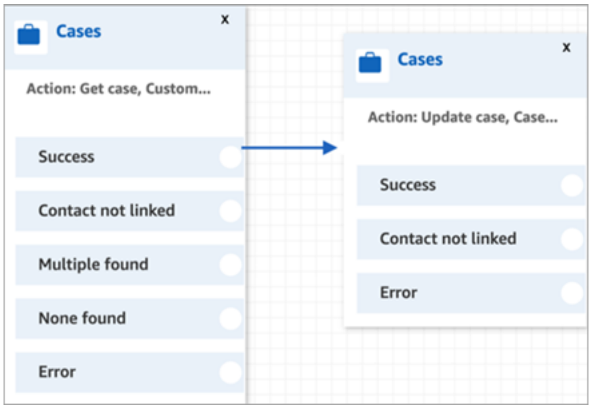
Status, Summary, Title

Summary ⓧ Title ⓧ Status ⓧ

Properties: Update case

When configuring properties to update a case:

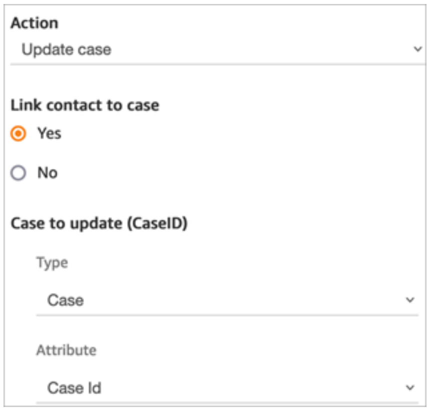
- Add a **Get case** block before an **Update case**. Use it to find the case you want to update.



- You must provide an update to at least one **Request** field. Otherwise, this block takes the **Error** branch.

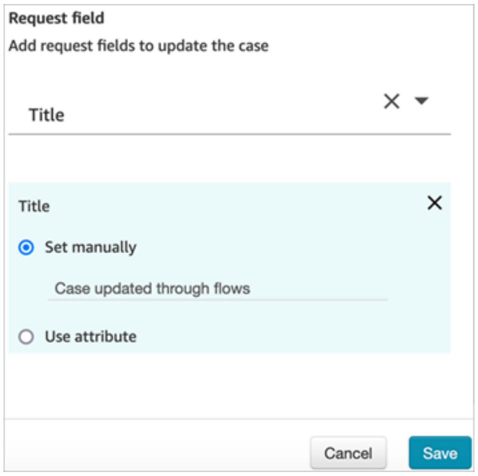
  You can either use an attribute in the Cases namespace, or set the **Request** field manually. If you set manually, see the syntax in How to persist fields throughout the flow (p. 352).
- Contacts can be routed down the following branches:
  - **Success**: The case was updated, and the contact was linked to the case.
  - **Contact not linked**: If you specify to link the contact to case, then this error branch will appear. It might be that the case was updated, but the contact was not linked to the case (partial success/ partial failure). If this happens, then the flow will follow this branch.
  - **Error**: The case was not updated. The contact was not linked to the case, as the case was not updated.

The following images show an example of an **Update case** configuration. The first image shows that as part of the update the contact is going to be linked to the case. To identify which case to update, the **Case Id** is specified.


Action
Update case

Link contact to case
● Yes
○ No

Case to update (CaseID)
Type
Case
Attribute
Case Id



Request field

Add request fields to update the case

Title

Title

● Set manually

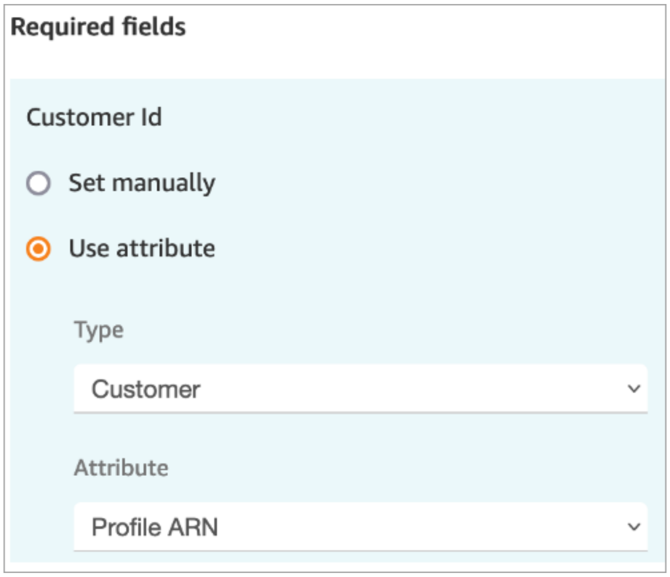
Case updated through flows

○ Use attribute

Properties: Create case

When configuring properties to create a case:

- You must provide a case template. For more information, see Create case templates (Preview) (p. 740).
- Fields that are required appear in the **Required** fields section. You must assign values to them to create a case.
- You must specify the customer to create a case.
  - We recommend adding a Customer profiles (p. 359) block to the flow before the **Cases** block. Use the Customer profiles (p. 359) block to get a customer profile with some prefetched data, or create a new customer profile and then use that to create a case.
  - To provide a value for **Customer Id** in the **Cases** block, configure the fields as shown in the following image:



Required fields

Customer Id

○ Set manually

● Use attribute

Type

Customer

Attribute

Profile ARN

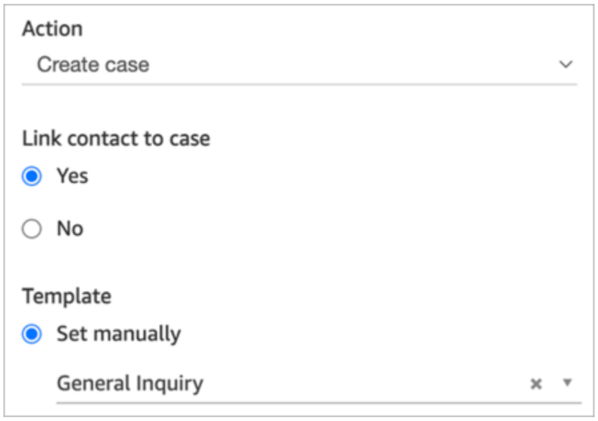
If you are setting the value manually, you must provide the full customer profile ARN in this format:

```
arn:aws:profile:your AWS Region:your AWS account ID:domains/profiles domain
name/profiles/profile ID
```

- You can specify values for fields other than the required ones in the Request fields section.

  You can either use attribute in the Cases namespace or set manually. If you set manually, see to the syntax in How to persist fields throughout the flow (p. 352).
- You can specify that a contact should be linked to case. If you link the contact to the case, then the contact and a link to contact details appear on the case that the agent sees in the agent application.
- After creating a case, the case ID that is created will be persisted in the case namespace. It can be used in other blocks by accessing the case namespace case ID attribute value.
- Contacts can be routed down the following branches:
  - **Success**: The case was created, and the contact was linked to the case.
  - **Contact not linked**: If you specify to link the contact to case, then this error branch will appear. This is because it is possible that the case was created, but the contact was not linked to the case (partial success/partial failure). If this happens, then the flow will follow this branch.
  - **Error**: The case was not created. The contact was not linked to the case, as the case was not created.

The following images show an example of a **Create case** configuration. The first image shows the new case will be created using the General inquiry template:

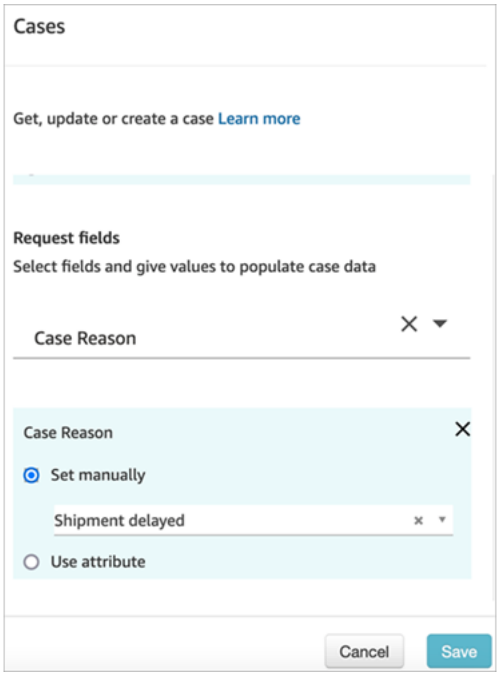


Action
Create case

Link contact to case
● Yes
○ No

Template
● Set manually
General Inquiry

The next image shows the reason for the case will be set to **Shipment delayed**.



Cases

Get, update or create a case Learn more

Request fields

Select fields and give values to populate case data

Case Reason

Case Reason

● Set manually

Shipment delayed

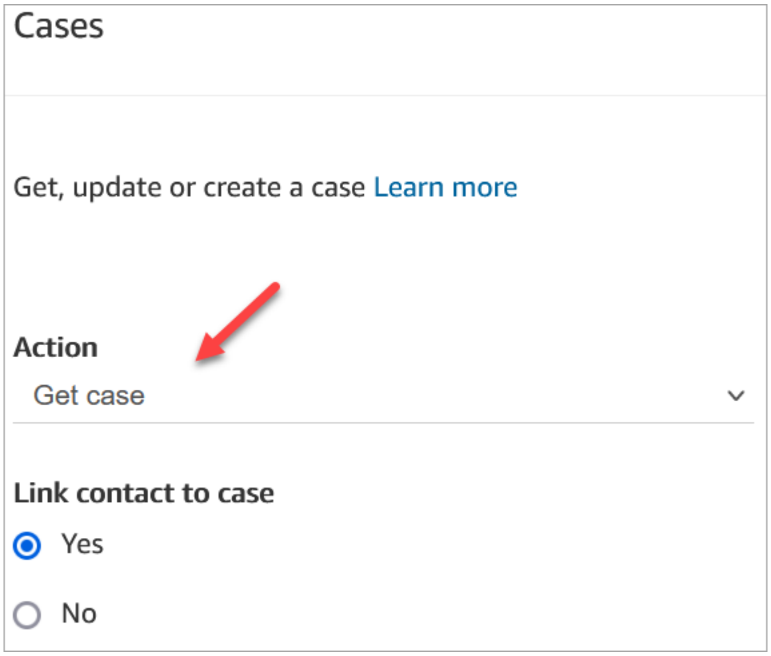
○ Use attribute

How to persist fields throughout the flow

Let's say you want customers to be able to call into your contact center and get the status of their case without ever talking to an agent. You want the IVR to read the status to the customer. You can get the status from a system field, or you might have a custom status field, for example, named *Detailed status*.

Here's how to configure your flow to get and read the status to the customer:

1. Add a **Cases** block to your flow. Configure it to **Get case** to find the case.



Cases

Get, update or create a case Learn more

Action

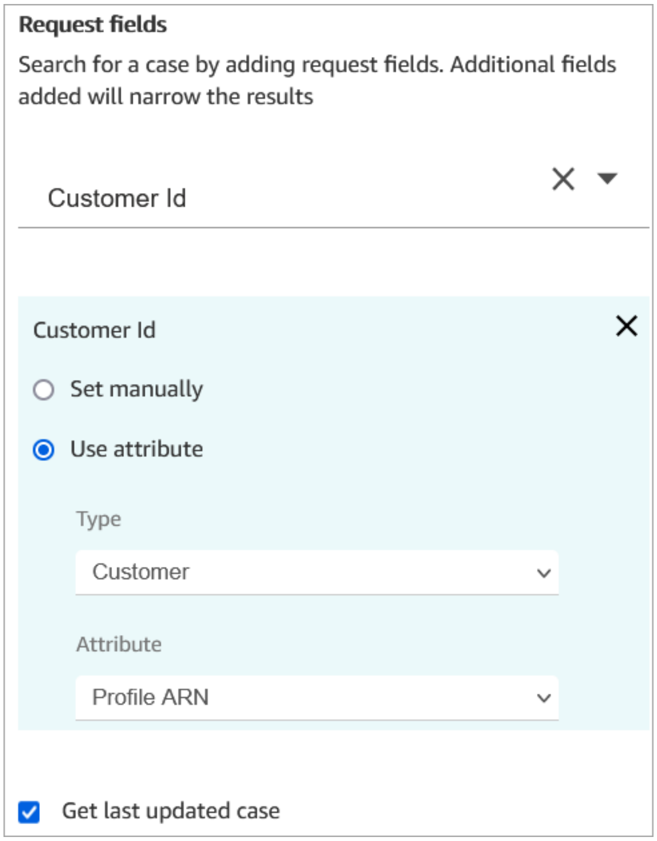
Get case

Link contact to case

● Yes

○ No

2. In the **Request fields** section, search for the case by the customer **Profile ARN**:



Request fields

Search for a case by adding request fields. Additional fields added will narrow the results

Customer Id

Customer Id

○ Set manually

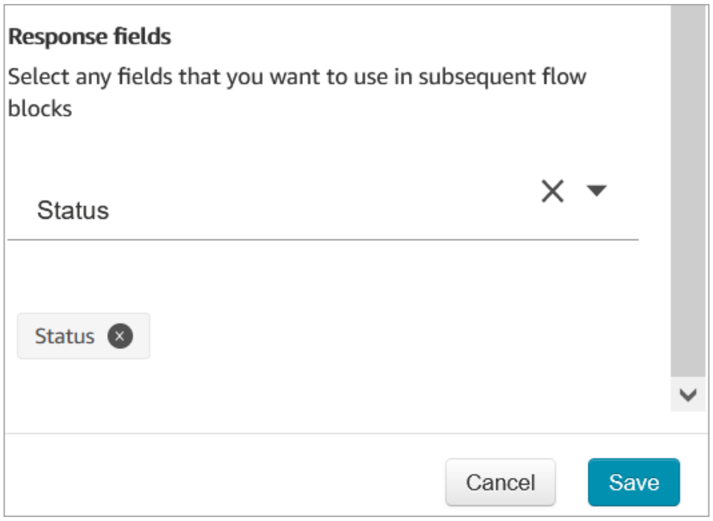
● Use attribute

Type: Customer

Attribute: Profile ARN

☑ Get last updated case

3. In the **Response fields** section, add the field that you want passed throughout the flow. For our example, choose **Status**.



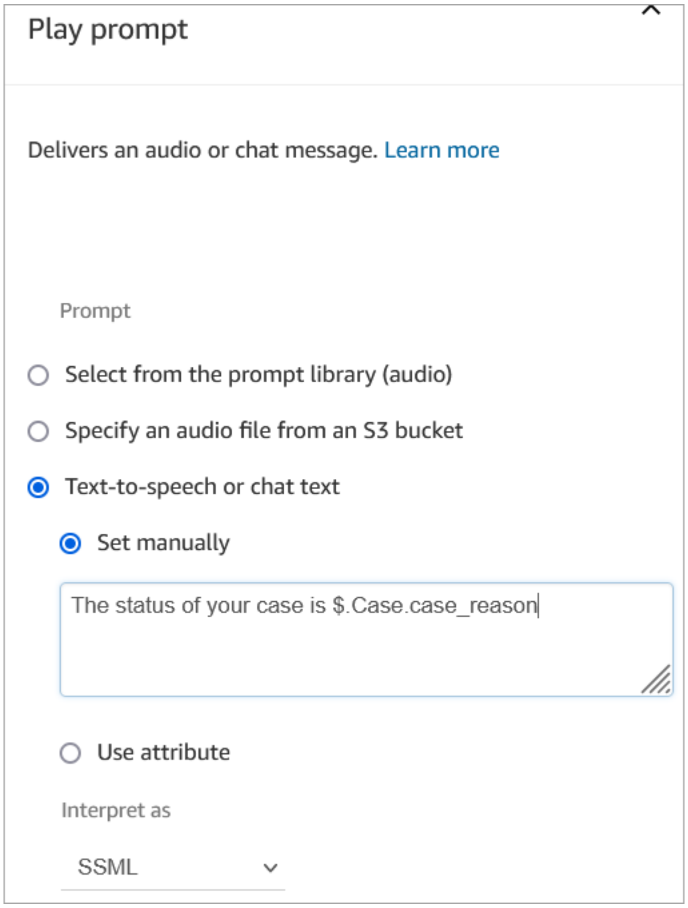
Response fields

Select any fields that you want to use in subsequent flow blocks

Status

Status

4. Add a Play prompt (p. 393) block to your flow.
5. Configure Play prompt (p. 393) to set the attribute manually:



Play prompt

Delivers an audio or chat message. Learn more

Prompt

○ Select from the prompt library (audio)

○ Specify an audio file from an S3 bucket

● Text-to-speech or chat text

● Set manually

The status of your case is $.Case.case_reason

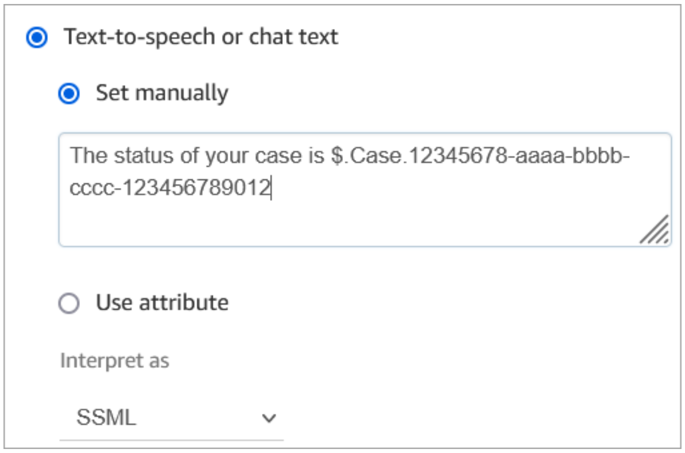
○ Use attribute

Interpret as

SSML

Use the following syntax for reading the status of the case to the customer:

- For system fields, you can read the syntax and understand which field it refers to. For example: `$.Case.status` refers to the case status. For a list of system field IDs, see the *Field ID* column in the System case fields (p. 737) topic.
- For custom fields, the syntax uses a UUID to represent the field. For example, in the following image, the UUID for the custom field named *Detailed status* is `12345678-aaaa-bbbb-cccc-123456789012`.



● Text-to-speech or chat text

● Set manually

The status of your case is $.Case.12345678-aaaa-bbbb-cccc-123456789012

○ Use attribute

Interpret as

SSML

Find the UUID of a custom field

To find the UUID of a custom field:

1. In Amazon Connect, in the navigation menu choose **Agent applications**, **Custom fields**, and then choose the custom field that you want.
2. While on the details page for the custom field, look at the URL of the page. The UUID is the last portion of the URL. For example, in the following URL:

   ```
   https://instance alias.my.connect.aws/cases/configuration/fields/
   update/12345678-aaaa-bbbb-cccc-123456789012
   ```

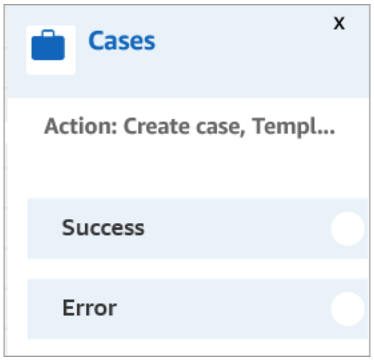
   The UUID is `12345678-aaaa-bbbb-cccc-123456789012`.

Configuration tips

- Be sure to check the Cases service quotas (p. 1208), and request increases. The quotas apply when this block creates cases.

Configured block

When this block is configured to create a cases, it looks similar to the following:



Contact block: Create task

Description

Creates a new task, sets the tasks attributes, and initiates a contact flow to start the task immediately or schedule it for a future date and time. For more information about Amazon Connect Tasks, see Tasks (p. 16).

> **Note**
> If your Amazon Connect instance was created on or before October 2018, the contact is routed down the error branch. For the contact to be routed down the success path, create an IAM policy with the following permission and attach it to the Amazon Connect service role. You can find the Amazon Connect service role on the **Account overview** page for your Amazon Connect instance.

```
{
     "Effect": "Allow",
     "Action": "connect:StartTaskContact",
     "Resource": "*"
```

```
}
```

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

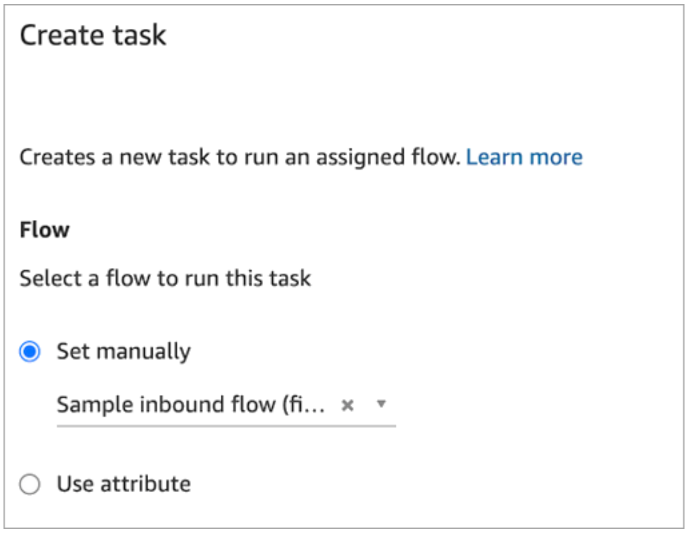
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Create task

Creates a new task to run an assigned flow. Learn more

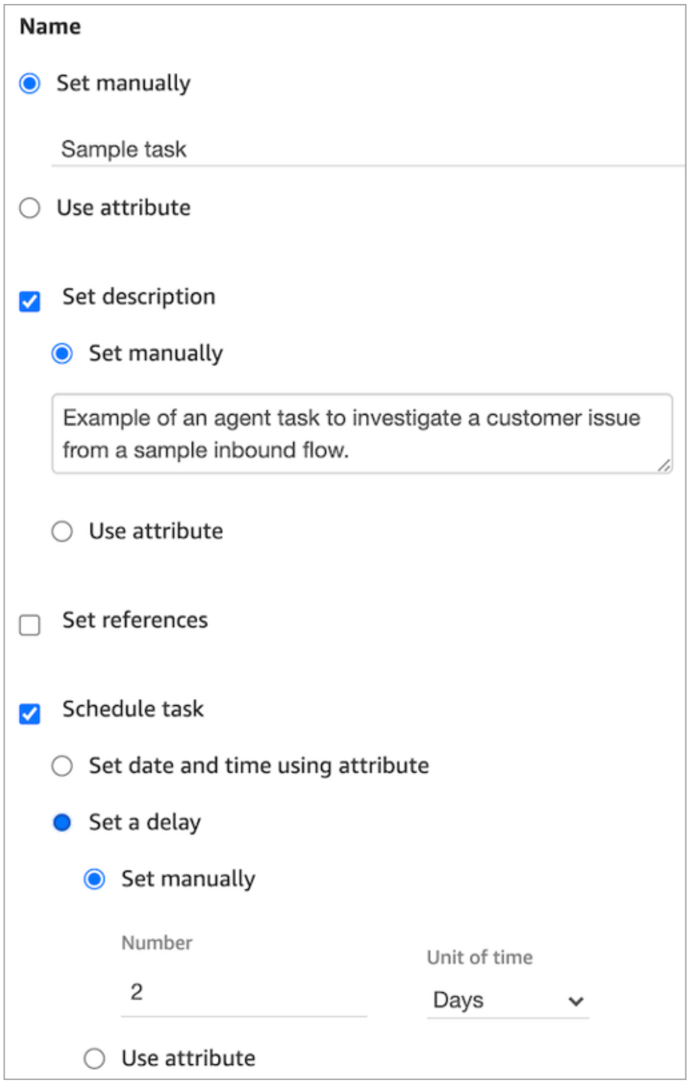
Flow

Select a flow to run this task

● Set manually

Sample inbound flow (fi… × ▾

○ Use attribute



Name

◉ Set manually

Sample task

○ Use attribute

☑ Set description

◉ Set manually

Example of an agent task to investigate a customer issue from a sample inbound flow.

○ Use attribute

☐ Set references

☑ Schedule task

○ Set date and time using attribute

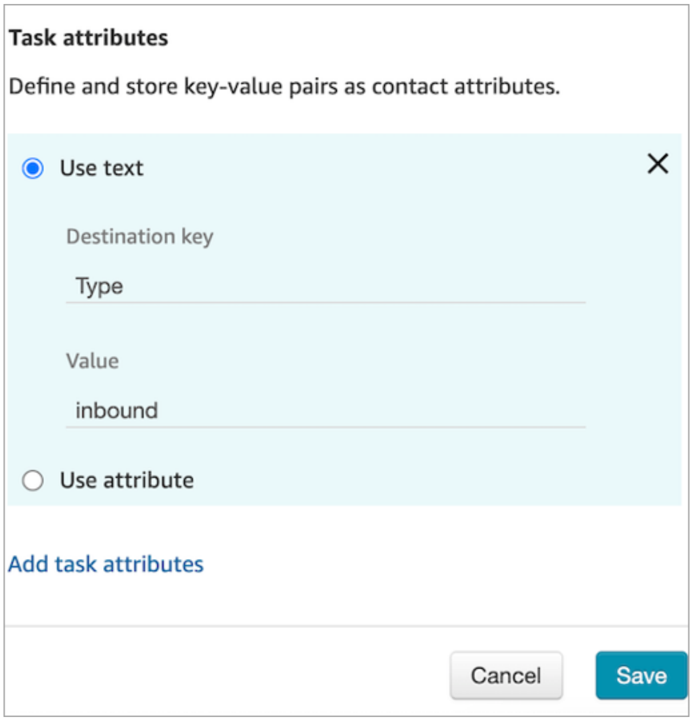
● Set a delay

◉ Set manually

Number: 2

Unit of time: Days

○ Use attribute



Task attributes

Define and store key-value pairs as contact attributes.

● Use text

Destination key: Type

Value: inbound

○ Use attribute

Configuration tips

- The **Create task** block branches based on whether the task was successfully created:
  - **Success** if task was created. It responds with the contact ID of the newly created task.
  - **Error** if task wasn't created.
- The newly created task runs the flow that you specified in the **Flow** section of the block. You can reference the contact ID of the newly created task in subsequent blocks.

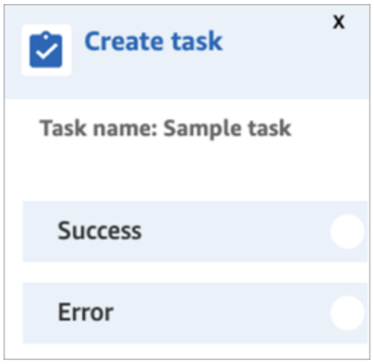
  For example, you might want to reference the task contact ID in the **Play prompt** block. You can specify the task contact ID dynamically by using the following attribute:
  - **Type: System**
  - **Attribute: Task Contact id**
- To create a scheduled task, we recommend that in the **Schedule task** section, you use **Set a delay**. Provide a value that is persistently valid and doesn't become outdated.

  You can **Set a delay** manually or use attributes.

  If there are cases where **Set date and time using attribute** is needed, you specify an actual date and time in Epoch seconds. When the date and time have passed, contacts are always routed down the **Error** branch. To avoid the **Error** branch, be sure to keep the Epoch seconds updated to a valid date and time in the future.
- Be sure to check the service quotas (p. 1205) for tasks and API throttling, and request increases, if needed. The quotas apply when this block creates tasks.

Configured block

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 309)

Contact block: Customer profiles

Description

- Enables you to retrieve, create, and update a customer profile.
- You can configure the block to retrieve profiles by phone number or email.
- When a customer profile is retrieved, the **Response fields** are stored in the contact attributes for that customer.
- You can also reference the **Response fields** by using the following JSONPath: `$.Customer.` For example, `$.Customer.City`.
- The following examples show how you might use this block:
  - Use a Play prompt (p. 393) block after retrieving a profile to provide a personalized call or chat experience by referencing the supported profile fields.
  - Use a Check contact attributes (p. 329) block after retrieving a profile to route a contact based on the value of the profile field.

Supported channels

The following table lists how this block routes a contact that is using the specified channel.

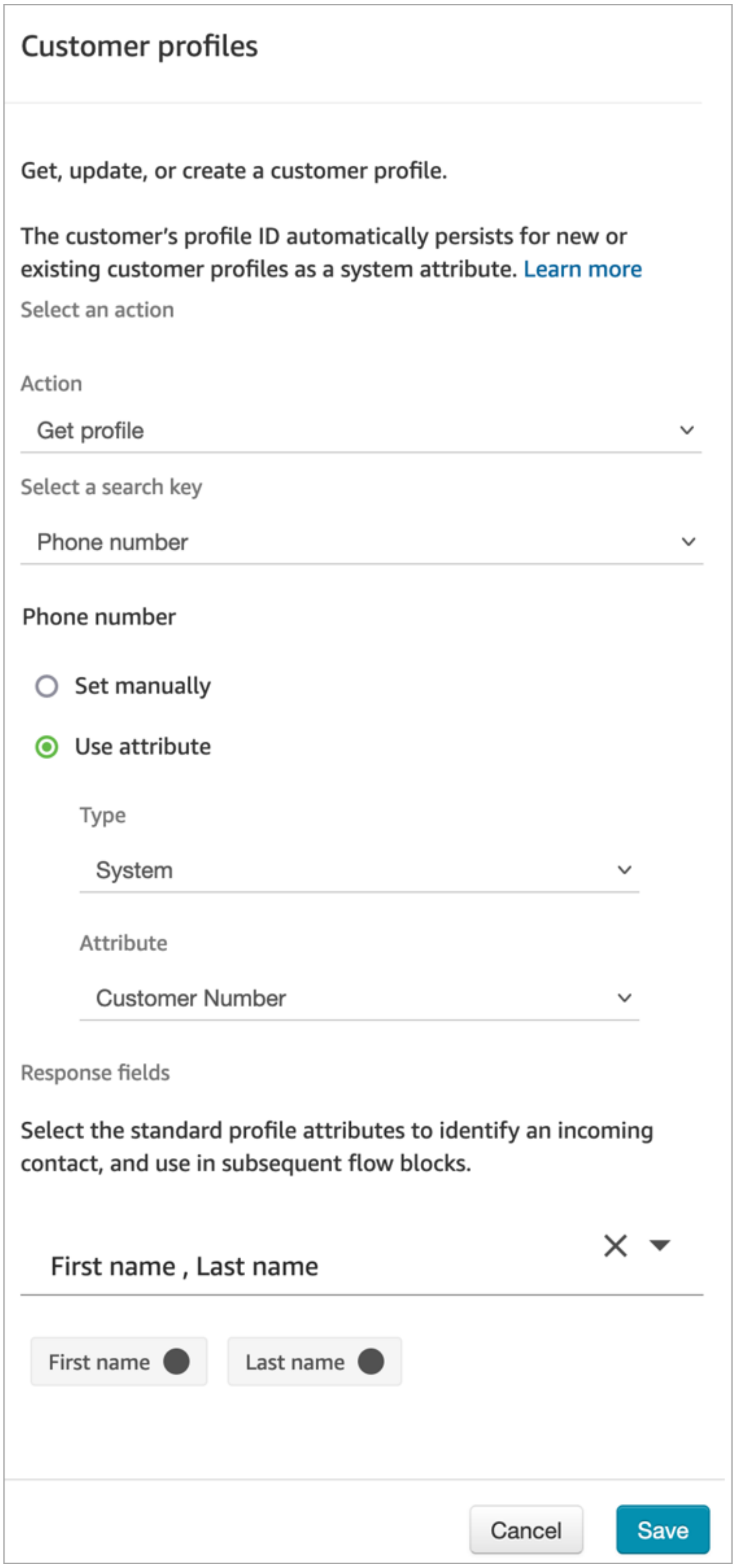
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flow types

Properties



Customer profiles

Get, update, or create a customer profile.

The customer's profile ID automatically persists for new or existing customer profiles as a system attribute. Learn more

Select an action

Action: Get profile

Select a search key: Phone number

Phone number

○ Set manually

● Use attribute

Type: System

Attribute: Customer Number

Response fields

Select the standard profile attributes to identify an incoming contact, and use in subsequent flow blocks.

First name , Last name

Under **Action**, choose from the following options:

- **Get profile**
- **Create a profile**
- **Update a profile**

Use the options under **Response fields** to identify objects that agents can search on when they use the agent application.

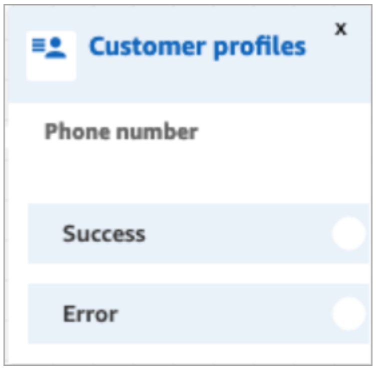
The **Action** and **Response fields** correspond to the request and response fields of the Profile API.

Configuration tips

- Before using this block, make sure Customer Profiles is enabled for your Amazon Connect instance. For instructions, see Use Customer Profiles (p. 640).
- A contact is routed down the **Error** branch in the following situations:
  - Customer Profiles is not enabled for your Amazon Connect instance.
  - Request data values are not valid. The request values cannot be over 255 characters.
  - The Customer Profiles API request has been throttled.
  - Customer Profiles is having availability issues.

Configured block

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



Contact block: Disconnect / hang up

Description

- Disconnects the contact.

Supported channels

The following table lists how this block routes a contact that is using the specified channel.

Channel	Supported?
Voice	Yes

Channel	Supported?
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Contact block: Distribute by percentage

Description

- This block is useful for doing A/B testing. It routes customers randomly based on a percentage.
- Contacts are distributed randomly, so exact percentage splits may or may not occur.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

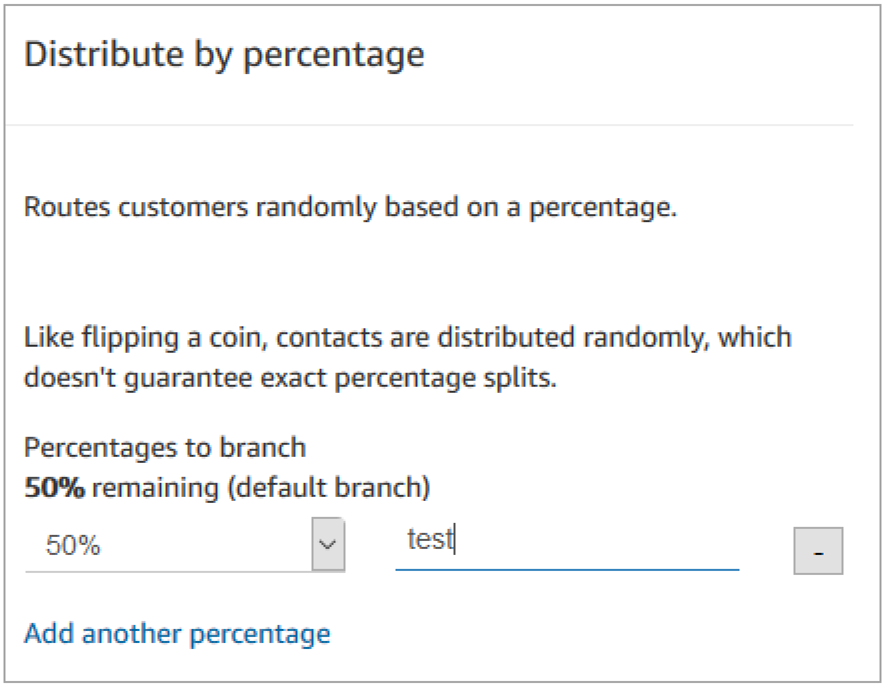
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Distribute by percentage

Routes customers randomly based on a percentage.

Like flipping a coin, contacts are distributed randomly, which doesn't guarantee exact percentage splits.

Percentages to branch
50% remaining (default branch)

50% test

How it works

This block creates static allocation rules based on how you configure it. Internal logic generates a random number between 1-100. This number identifies which branch to take. It doesn't use current or historical volume as part of it's logic.

For example, say a block is configure like this:

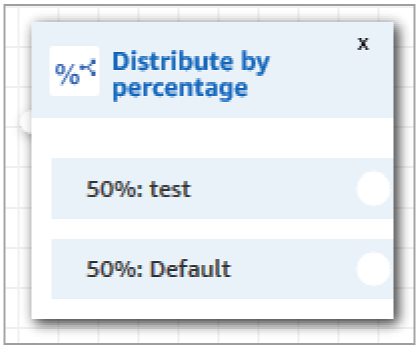
- 20% = A
- 40% = B
- 40% remaining = Default

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

- If number is between 0-20, the contact is routed down the A branch.
- Between 21-60 it's routed down the B branch.
- Greater than 60 it's routed down the Default branch.

Configured block

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample AB test (p. 309)

Contact block: End flow / Resume

Description

- Ends the current flow without disconnecting the contact.
- This block is often used for the **Success** branch of the **Transfer to queue** block. The flow doesn't end until the call is picked up by an agent.
- You also might use this block when a **Loop prompts** block is interrupted. You can return the customer to the **Loop prompts** block.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

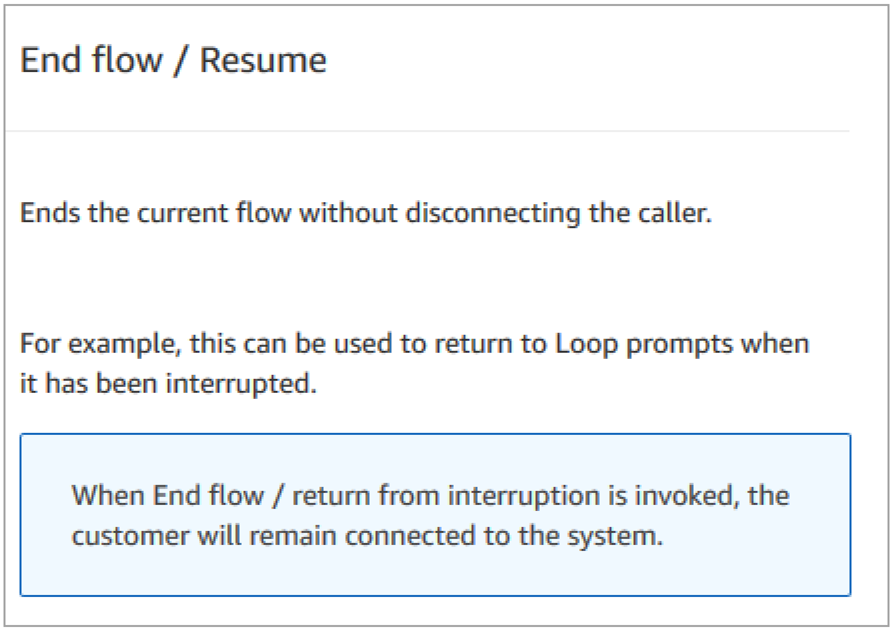
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



End flow / Resume

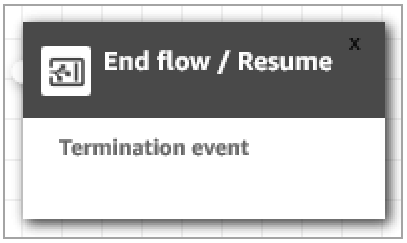
Ends the current flow without disconnecting the caller.

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

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

Configured block

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



Contact block: Get customer input

Description

- It plays a prompt to get a response from the customer. For example, "For Sales, press one. For Support, press two."
- When customers enter DTMF input (touch-tone keypad or telephone input), the prompt is interruptible.
- When an Amazon Lex bot plays a voice prompt, customers can interrupt it with their voice. To set this up, use the `barge-in-enabled` session attribute.
- It then branches based on the customer's input.
- This block works for chat only when Amazon Lex is used.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

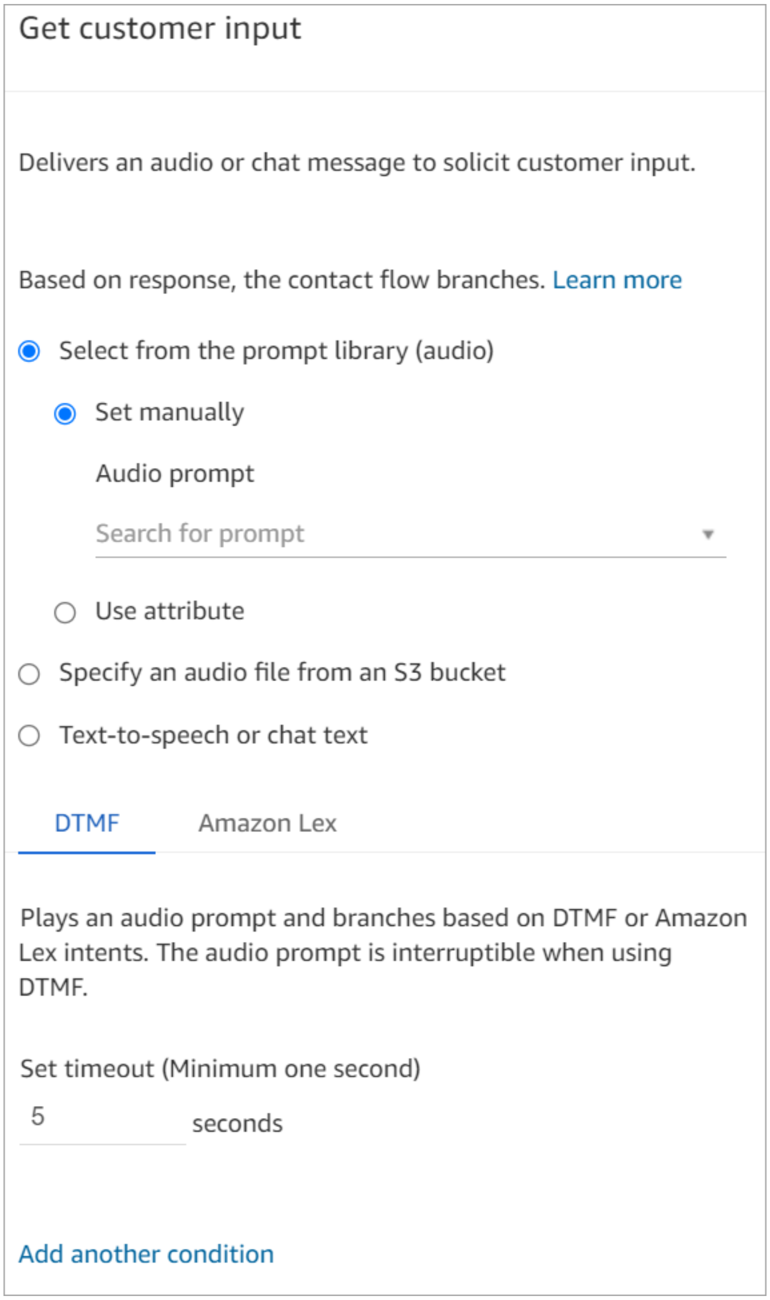
Channel	Supported?
Voice	Yes
Chat	Yes when Amazon Lex is used Otherwise, No - Error branch
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Get customer input

Delivers an audio or chat message to solicit customer input.

Based on response, the contact flow branches. Learn more

● Select from the prompt library (audio)

● Set manually

Audio prompt

Search for prompt ▾

○ Use attribute

○ Specify an audio file from an S3 bucket

○ Text-to-speech or chat text

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

Set timeout (Minimum one second)

5 seconds

> **Note**
> The **Get Customer Input** block does not currently support using a voice prompt from an S3 bucket with Amazon Lex V2.
> For information about choosing a prompt from the Amazon Connect library or an S3 bucket, see the Play prompt (p. 393) block.

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

DTMF tab properties

- **Audio prompt**: Select from a list of default audio prompts, or upload your own audio prompt.

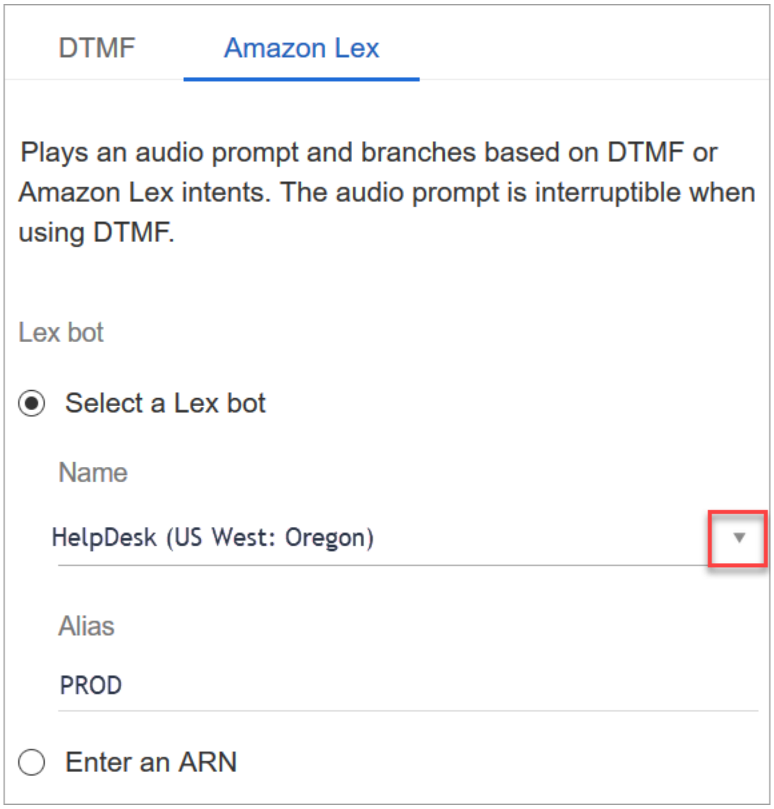
- **Set timeout**: Specify how long to wait while the user decides how they want to respond to the prompt. The maximum timeout you can set is 179 seconds.

Amazon Lex tab properties

Amazon Lex

> **Note**
> Your language attribute in Amazon Connect must match the language model used to build your Amazon Lex V2 bot. Set the language attribute using the Set voice (p. 415) block or the Set contact attributes (p. 399) block.

- **Lex bot properties**: After you create your Lex bot, enter the name and alias of the bot here. Only built bots appear in the drop-down list.



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

Lex bot

● Select a Lex bot

Name

HelpDesk (US West: Oregon) ▾

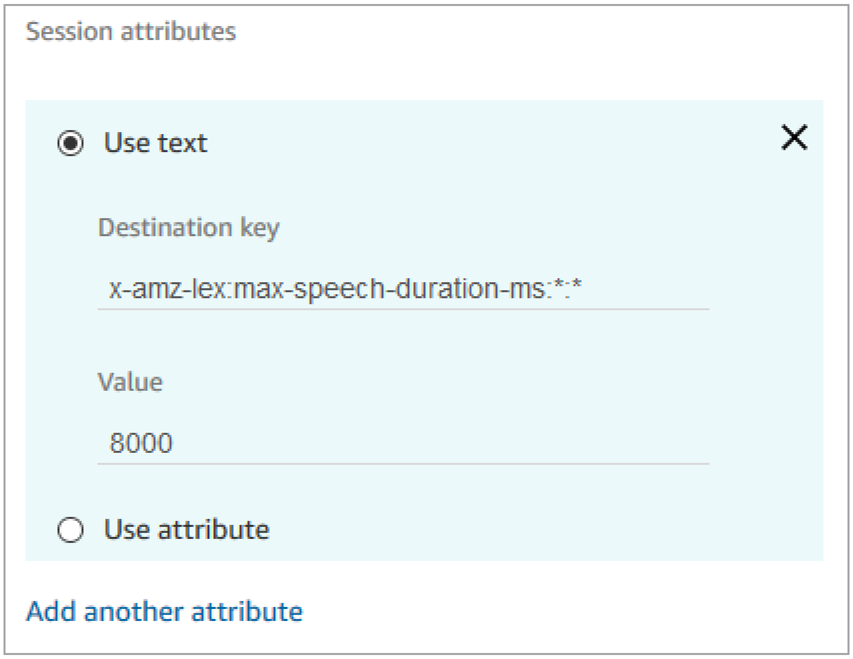
Alias

PROD

○ Enter an ARN

> **Important**
> In a production environment, always use a different alias than **TestBotAlias** for Amazon Lex and **$LATEST** for Amazon Lex classic. **TestBotAlias** and **$LATEST** support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime Service Quotas or Runtime Service Quotas (Amazon Lex Classic).

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



Session attributes

● Use text

Destination key

x-amz-lex:max-speech-duration-ms:*:*

Value

8000

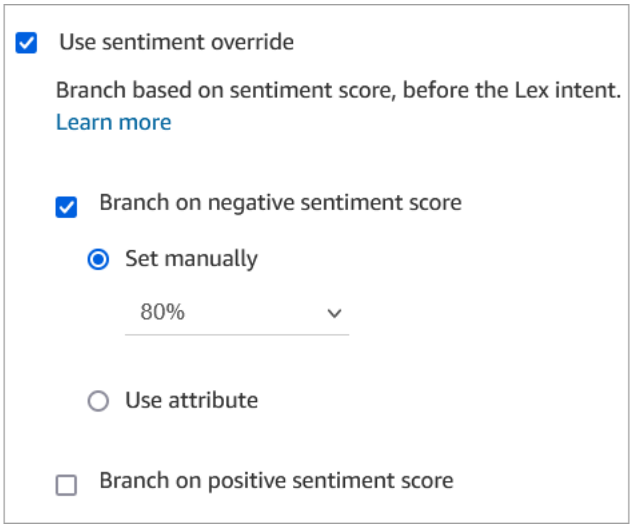
○ Use attribute

Add another attribute

- **Use sentiment override**: Branch based on sentiment score, before the Amazon Lex intent.

  The sentiment score is based on the last utterance of the customer. It is not based on the entire conversation.

  For example, a customer calls and they have an angry tone because their preferred appointment time isn't available. You can branch the flow based on their negative sentiment score, for example, if their negative sentiment is more than 80%. Or, a customer calls and has a positive sentiment of more than 80%, you can branch to upsell them on services.



☑ Use sentiment override

Branch based on sentiment score, before the Lex intent.
Learn more

☑ Branch on negative sentiment score

● Set manually

80%

○ Use attribute

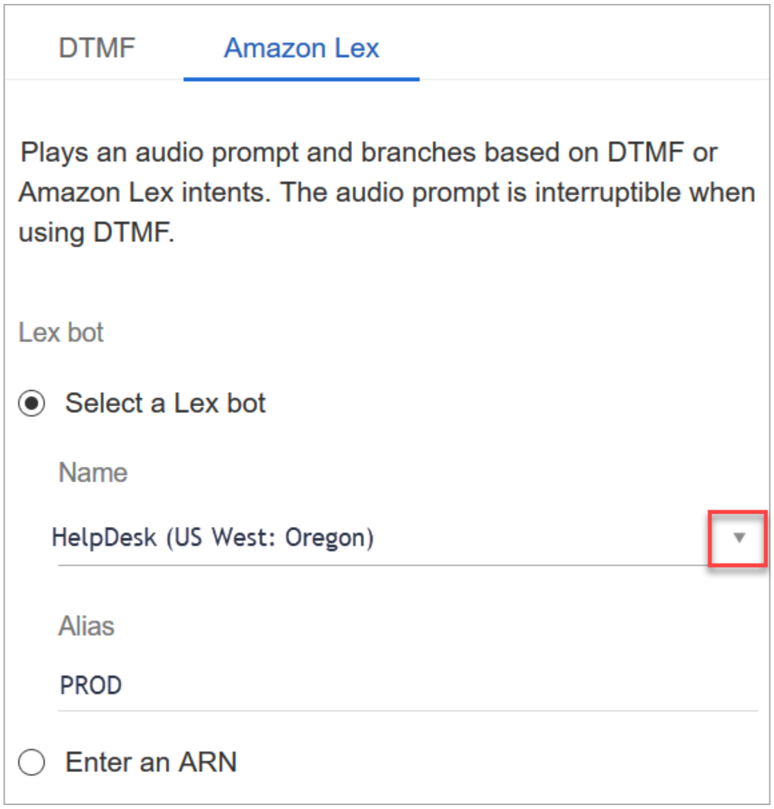
□ Branch on positive sentiment score

If you add both negative and positive sentiment scores, the negative score is always evaluated first.

For information about how to use sentiment score, alternative intents, and sentiment label with contact attributes, see Check contact attributes (p. 329).

Amazon Lex (Classic)

- **Lex bot properties**: After you create your Lex bot, enter the name and alias of the bot here. Only published bots appear in the drop-down list.



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

Lex bot

● Select a Lex bot

Name

HelpDesk (US West: Oregon)

Alias

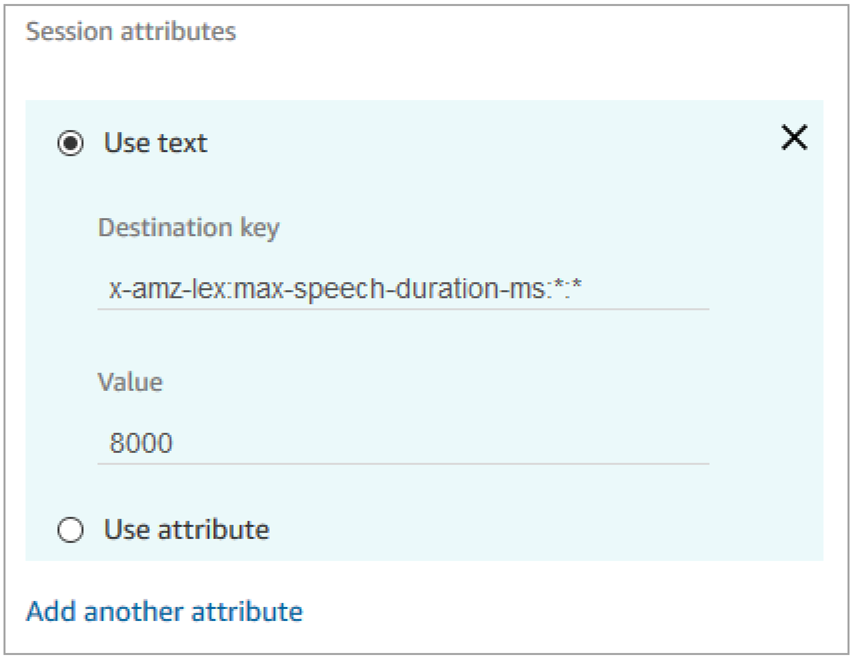
PROD

○ Enter an ARN

Important

In a production environment, always use a different alias than **TestBotAlias** for Amazon Lex and **$LATEST** for Amazon Lex classic. **TestBotAlias** and **$LATEST** support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime Service Quotas or Runtime Service Quotas (Amazon Lex Classic).

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



Session attributes

● Use text

Destination key

x-amz-lex:max-speech-duration-ms:*:*

Value

8000

○ Use attribute

Add another attribute

Configurable time-outs for voice input

To configure time-out values for voice contacts, use the following session attributes in the **Get customer input** block that calls your Lex bot. These attributes allow you to specify how long to wait for the customer to finish speaking before Amazon Lex collects speech input from callers, such as answering a yes/no question, or providing a date or credit card number.

Amazon Lex

- **Max Speech Duration**

  ```
  x-amz-lex:audio:max-length-ms:[intentName]:[slotToElicit]
  ```

  How long the customer speaks before the input is truncated and returned to Amazon Connect. You can increase the time when a lot of input is expected or you want to give customers more time to provide information.

  Default = 13000 milliseconds (13 seconds). The maximum allowed value is 15000 milliseconds.

  > **Important**
  > If you set **Max Speech Duration** to more than 15000 milliseconds, the contact is routed down the **Error** branch.

- **Start Silence Threshold**

  ```
  x-amz-lex:audio:start-timeout-ms:[intentName]:[slotToElicit]
  ```

  How long to wait before assuming that the customer isn't going to speak. You can increase the allotted time in situations where you'd like to allow the customer more time to find or recall information before speaking. For example, you might want to give customers more time to get out their credit card so they can enter the number.

  Default = 4000 milliseconds (4 seconds).

- **End Silence Threshold**

`x-amz-lex:audio:end-timeout-ms:[intentName]:[slotToElicit]`

How long to wait after the customer stops speaking before assuming the utterance has concluded. You can increase the allotted time in situations where periods of silence are expected while providing input.

Default = 600 milliseconds (0.6 seconds)

Amazon Lex (Classic)

- **Max Speech Duration**

  `x-amz-lex:max-speech-duration-ms:[intentName]:[slotToElicit]`

  How long the customer speaks before the input is truncated and returned to Amazon Connect. You can increase the time when a lot of input is expected or you want to give customers more time to provide information.

  Default = 13000 milliseconds (13 seconds). The maximum allowed value is 15000 milliseconds.

  > **Important**
  > If you set **Max Speech Duration** to more than 15000 milliseconds, the contact is routed down the **Error** branch.

- **Start Silence Threshold**

  `x-amz-lex:start-silence-threshold-ms:[intentName]:[slotToElicit]`

  How long to wait before assuming that the customer isn't going to speak. You can increase the allotted time in situations where you'd like to allow the customer more time to find or recall information before speaking. For example, you might want to give customers more time to get out their credit card so they can enter the number.

  Default = 4000 milliseconds (4 seconds).

- **End Silence Threshold**

  `x-amz-lex:end-silence-threshold-ms:[intentName]:[slotToElicit]`

  How long to wait after the customer stops speaking before assuming the utterance has concluded. You can increase the allotted time in situations where periods of silence are expected while providing input.

  Default = 600 milliseconds (0.6 seconds)

Barge-in configuration and usage for Amazon Lex

You can allow customers to interrupt the Amazon Lex bot mid-sentence using their voice, without waiting for it to finishing speaking. Customers familiar with choosing from a menu of options, for example, can now do so without having to listen to the entire prompt.

Amazon Lex

- **Barge-in**

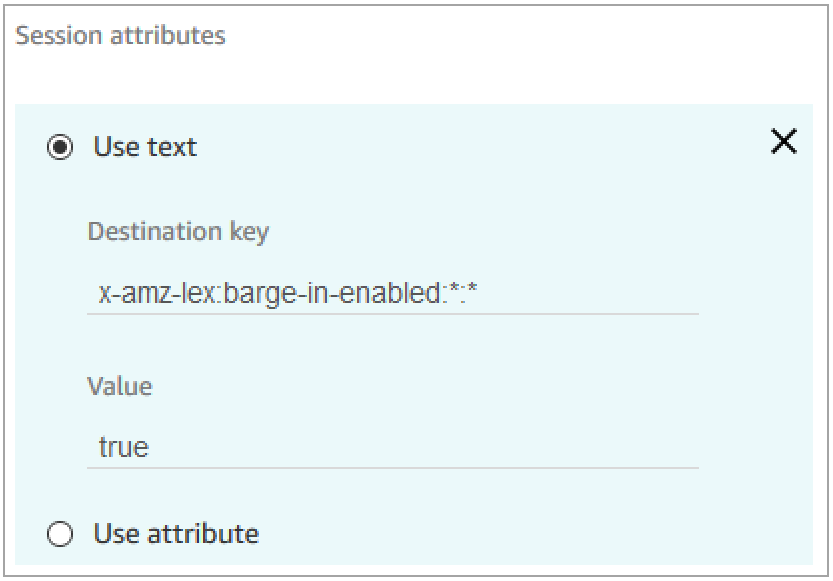
  Barge-in is enabled globally by default. You can disable it in the Amazon Lex console. For more information, see Enabling your bot to be interrupted by your user.

Amazon Lex (Classic)

- **Barge-in**

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

  Barge-in is disabled globally by default. You must set the session attribute in the **Get customer input** block that calls your Lex bot to enable it at the global, bot, or slot levels. This attribute only controls Amazon Lex barge-in; it doesn't control DTMF barge-in. For more information, see How to use Lex session attributes (p. 539).



Session attributes

● Use text

Destination key

x-amz-lex:barge-in-enabled:*:*

Value

true

○ Use attribute

Configurable fields for DTMF input

Use the following session attributes to specify how your Lex bot responds to DTMF input.

- **End character**

  ```
  x-amz-lex:dtmf:end-character:[IntentName]:[SlotName]
  ```

  The DTMF end character that ends the utterance.

  Default = #
- **Deletion character**

  ```
  x-amz-lex:dtmf:deletion-character:[IntentName]:[SlotName]
  ```

  The DTMF character that clears the accumulated DTMF digits and ends the utterance.

  Default = *
- **End timeout**

  ```
  x-amz-lex:dtmf:end-timeout-ms:[IntentName]:[SlotName]
  ```

  The idle time (in milliseconds) between DTMF digits to consider the utterance as concluded.

  Default = 5000 milliseconds (5 seconds)
- **Max number of allow DTMF digits per utterance**

`x-amz-lex:dtmf:max-length:[IntentName]:[SlotName]`

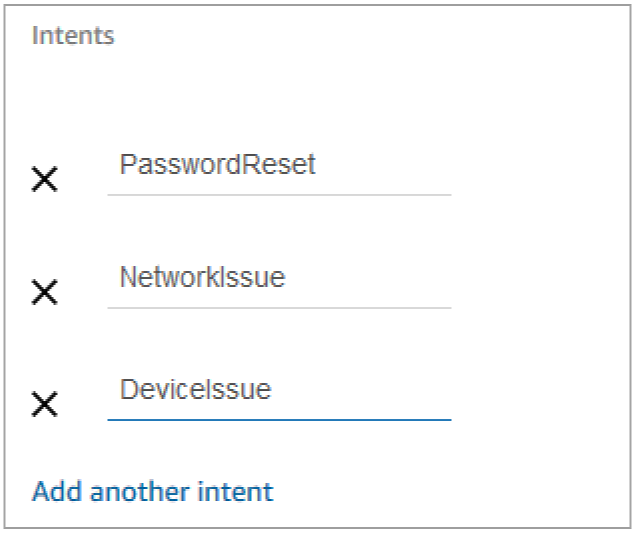
The maximum number of DTMF digits allowed in a given utterance. This cannot be increased.

Default = 1024 characters

For more information, see How to use Lex session attributes (p. 539).

Intents

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



Intents

PasswordReset

NetworkIssue

DeviceIssue

Configuration tips

- When you use text, either for text-to-speech or chat, you can use a maximum of 3,000 billed characters (6,000 total characters).
- Amazon Lex bots support both spoken utterances and keypad input when used in a contact flow.
- For both voice and DTMF, there can be only one set of session attributes per conversation. Following is the order of precedence:
  1. Lambda provided session attributes: Overrides to session attributes during customer Lambda invocation.
  2. Amazon Connect console provided session attributes: Defined in the **Get customer input** block.
  3. Service defaults: These are used only if no attributes are defined.
- You can prompt contacts to end their input with a pound key # and to cancel it using the star key *. When you use a Lex bot, if you don't prompt customers to end their input with #, they will end up waiting five seconds for Lex to stop waiting for additional key presses.
- To control time-out functionality, you can use Lex session attributes in this block, or in set them in your Lex Lambda function. If you choose to set the attributes in a Lex Lambda function, the default values are used until the Lex bot is invoked. For more information, see Using Lambda Functions in the *Amazon Lex Developer Guide*.
- When you specify one of the session attributes described in this article, you can use wildcards. They let you set multiple slots for an intent or bots.

  Following are some examples of how you can use wildcards:
  - To set all slots for a specific intent, such as PasswordReset, to 2000 milliseconds:

Name = `x-amz-lex:max-speech-duration-ms:PasswordReset:*`

Value = 2000

- To set all slots for all bots to 4000 milliseconds:

  Name = `x-amz-lex:max-speech-duration-ms:*:*`

  Value = 4000

Wildcards apply across bots but not across blocks in a contact flow.

For example, you have a Get_Account_Number bot. In the contact flow, you have two **Get customer input** blocks. The first block sets the session attribute with a wildcard. The second one doesn't set the attribute. In this scenario, the change in behavior for the bot applies only to the first **Get customer input** block, where the session attribute is set.

- Because you can specify that session attributes apply to the intent and slot level, you can specify that the attribute is set only when you're collecting a certain type of input. For example, you can specify a longer **Start Silence Threshold** when you're collecting an account number than when you're collecting a date.
- If DTMF input is provided to a Lex bot using Amazon Connect, the customer input is made available as a Lex request attribute. The attribute name is `x-amz-lex:dtmf-transcript` and the value can be a maximum of 1024 characters.

  Following are different DTMF input scenarios:

Customer input	DTMF transcript
[DEL]	[DEL]
[END]	[END]
123[DEL]	[DEL]
123[END]	123

Where:

- [DEL] = Deletion character (Default is *****)
- [END] = End character (Default is **#**)

Problems with DTMF input?

Let's say you have the following scenario with two contacts flows, each one capturing DTMF input from customers:

1. One contact flow uses the **Get customer input** block to request DTMF input from customers.
2. After the DTMF input is entered, it uses the **Transfer to flow** block to move the contact to the next contact flow.
3. In the next contact flow, there's a **Store customer input** block to get more DTMF input from the customer.

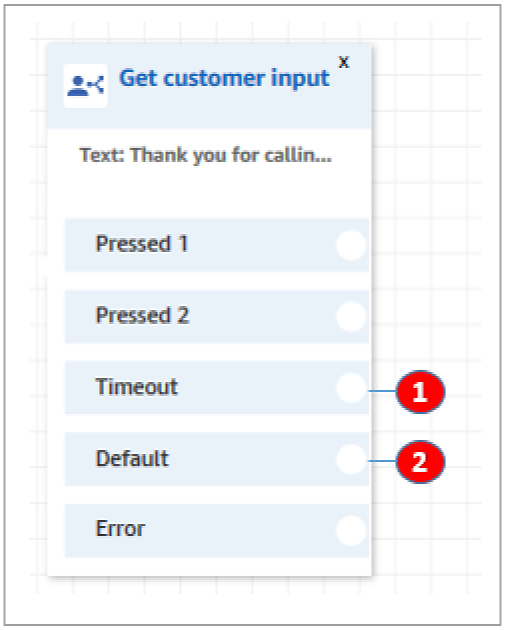
There's setup time between the first and second contact flows. This means if the customer enters DTMF input very quickly for the second flow, some of the DTMF digits might be dropped.

For example, the customer needs to press 5, then wait for a prompt from the second flow, then type 123. In this case, 123 is captured without problem. However, if they don't wait for the prompt and enter 5123 very quickly, the **Store customer input** block may capture only 23 or 3.

To guarantee the **Store customer input** block in second contact flow captures all of the digits, the customer needs to wait for the prompt to be played, and then enter their type DTMF input.

Configured block

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



1. **Timeout**: What to do when the time in the **Set timeout** property has elapsed. This branch appears only if you're using DTMF properties since that's where the **Set timeout** property is available. It doesn't appear if you're using Amazon Lex properties.
2. **Default**: What to do if a customer enters a value other than 1 or 2.

Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 309)
- Sample interruptible queue flow with callback (p. 315)
- Sample queue configurations (p. 311)
- Sample recording behavior (p. 315)

Scenarios

See these topics for scenarios that use this block:

- Add an Amazon Lex bot (p. 617)
- How to use the same bot for voice and chat (p. 540)
- Add text-to-speech to prompts (p. 456)

Contact block: Get queue metrics

Description

- Retrieves the following real-time metrics from a queue so you can make routing decisions. If there is no current activity in your contact center, nothing is returned for these metrics.
  - Queue name (p. 924)
  - Queue ARN.
  - Contacts in queue (p. 922)
  - Oldest contact in queue (p. 923)
  - Agents online (p. 923)
  - Agents available (p. 919)
  - Agents staffed (p. 925)
  - Agents after contact work (p. 917)
  - Agents busy (p. 923): Although this option maps to the **On contact** real-time metric, note that **On contact** includes ACW but **Agents busy** does not.
  - Agents missed (p. 918) (Agent non-response)
  - Agents non-productive (p. 923)
- You can choose to return metrics by channel, for example, voice or chat. You can also filter by queue or agent. These options enable you to know how many chat and voice contacts are in a queue and if you have agents available to handle those contacts.
- You can route contacts based on queue status, such as number of contacts in queue or agents available. Queue metrics are aggregated across all channels and are returned as attributes. The current queue is used by default.
- After a **Get queue metrics** block, use a Check contact attributes (p. 329) to check metric values and define routing logic based on them, such as number of contacts in a queue, number of available agents, and oldest contact in a queue.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

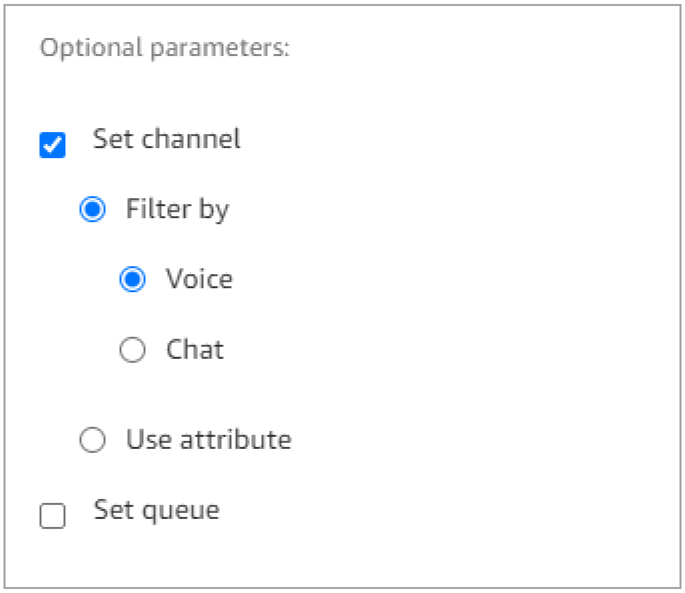
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Optional parameters:

☑ Set channel

● Filter by

● Voice

○ Chat

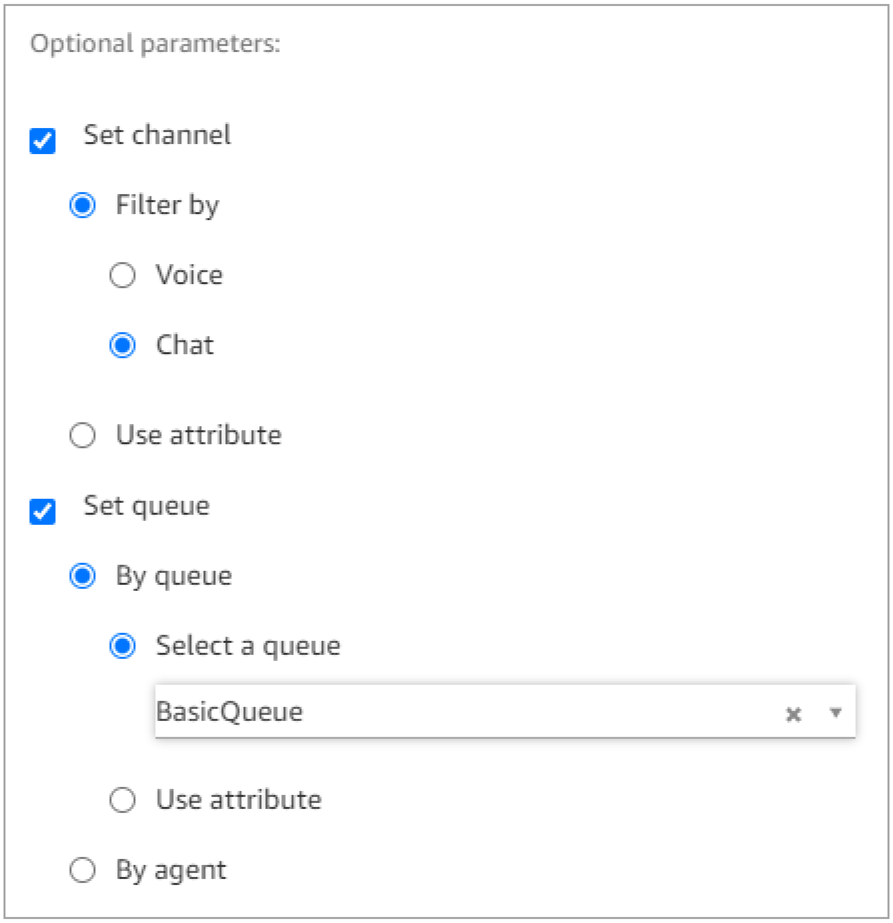
○ Use attribute

□ Set queue

You can retrieve metrics by channel, and/or by queue or agent.

- If you don't specify a channel, it returns metrics for all channels.
- If you don't specify a queue, it returns metrics for the current queue.
- Dynamic attributes can only return metrics for one channel.

For example, if you choose the following settings, **Get queue metrics** would return metrics for only the BasicQueue, filtered to include only chat contacts.



Optional parameters:

- ☑ Set channel
  - ● Filter by
    - ○ Voice
    - ● Chat
  - ○ Use attribute
- ☑ Set queue
  - ● By queue
    - ● Select a queue
      - BasicQueue
    - ○ Use attribute
  - ○ By agent

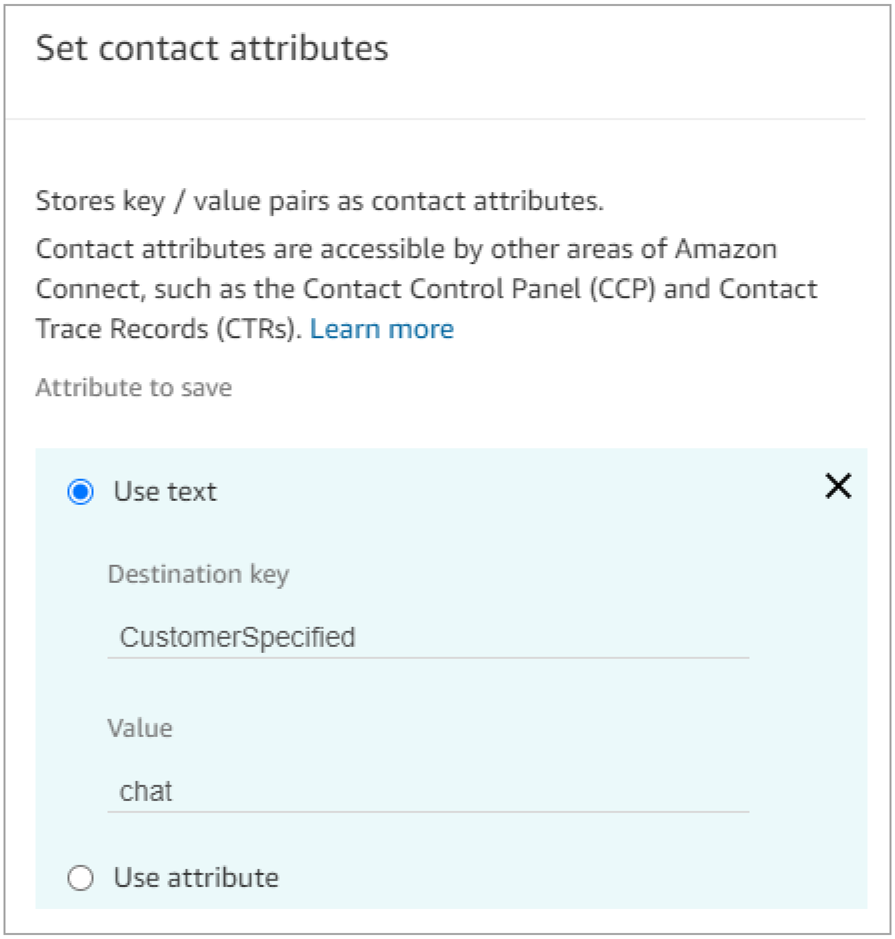
Configuration tips

Specifying a channel in the Set contact attributes block

Dynamic attributes can only return metrics for one channel.

Before you use dynamic attributes in the **Get queue metrics** block, you need to set the attributes in the Set contact attributes (p. 399) block, and specify which channel.

When you set a channel dynamically using text, as shown in the following image, for the attribute value enter **Voice** or **Chat**. This value is not case-sensitive.



Set contact attributes

Stores key / value pairs as contact attributes.

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

Attribute to save

● Use text

Destination key: CustomerSpecified

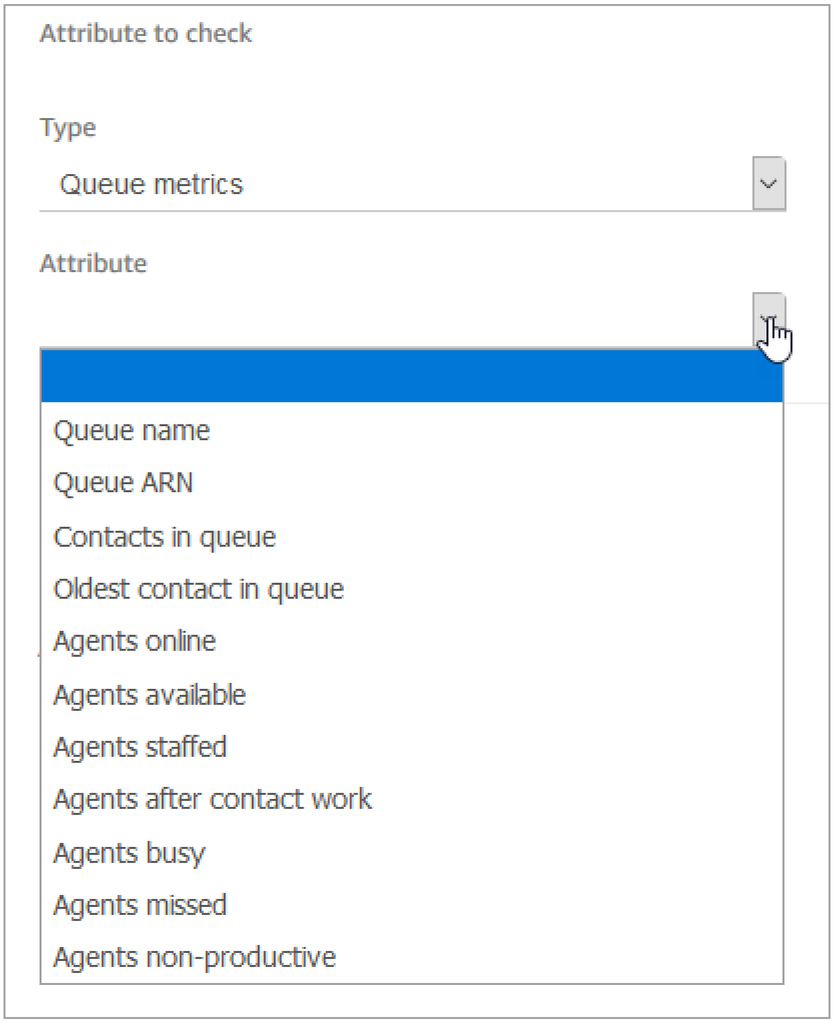
Value: chat

○ Use attribute

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

After a **Get queue metrics** block, add a Check contact attributes (p. 329) block to branch based on the returned metrics. Use the following steps:

1. After **Get queue metrics**, add a **Check contact attributes** block.
2. In the **Check contact attributes** block, set **Attribute to check** to **Queue metrics**.
3. In the **Attributes** dropdown box, you'll see that the following queue metrics are returned by the **Get queue metrics** block. Choose the metric that you want to use for the routing decision.



Attribute to check

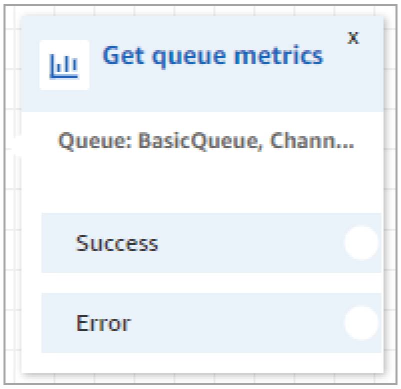
Type

Queue metrics

Attribute

Configured block

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



Scenarios

See these topics for scenarios that use this block:

- How to reference contact attributes (p. 531)

Contact block: Hold customer or agent

Description

- Places a customer or agent on or off hold. This is useful when, for example, you want to put the agent on hold while the customer enters their credit card information.
- If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

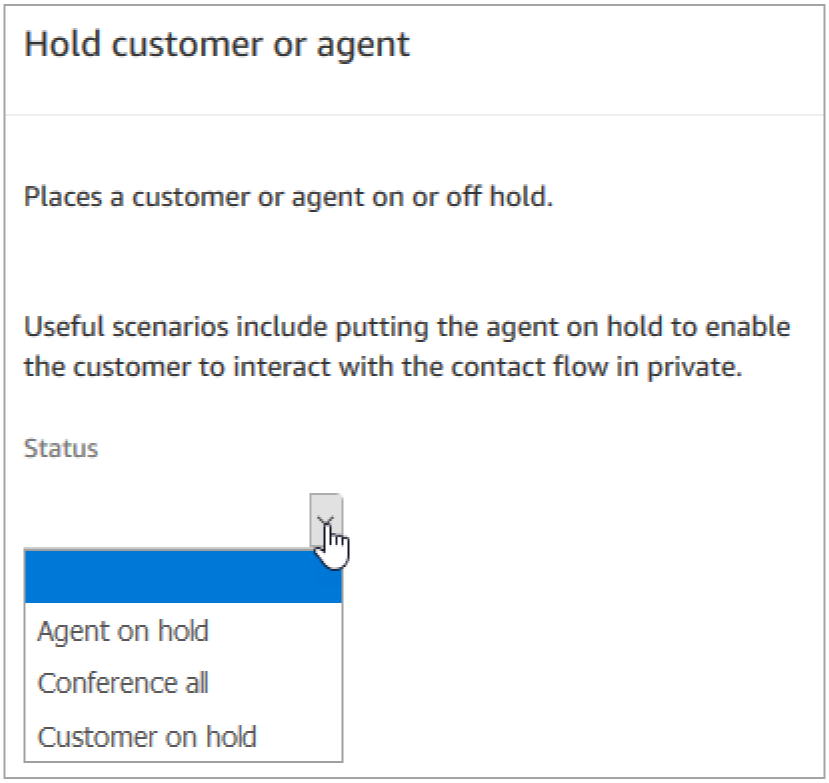
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Hold customer or agent

Places a customer or agent on or off hold.

Useful scenarios include putting the agent on hold to enable the customer to interact with the contact flow in private.

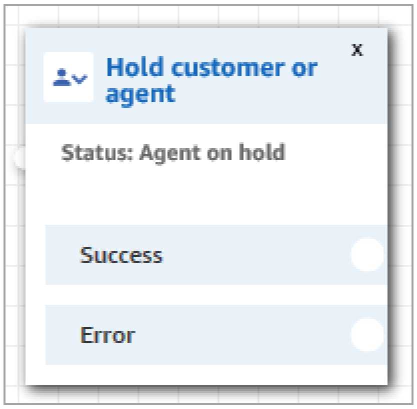
Status

The following settings are available:

- **Agent on hold** = customer is on the call
- **Conference all** = agent and customer are on the call
- **Customer on hold** = agent is on the call

Configured block

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



Hold customer or agent

Status: Agent on hold

Samples flows

Sample secure input with agent (p. 316)

Contact block: Invoke AWS Lambda function

Description

- Calls AWS Lambda, and optionally returns key-value pairs.
- The returned key-value pairs can be used to set contact attributes.
- For an example, see Tutorial: Create a Lambda function and invoke in a flow (p. 497).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

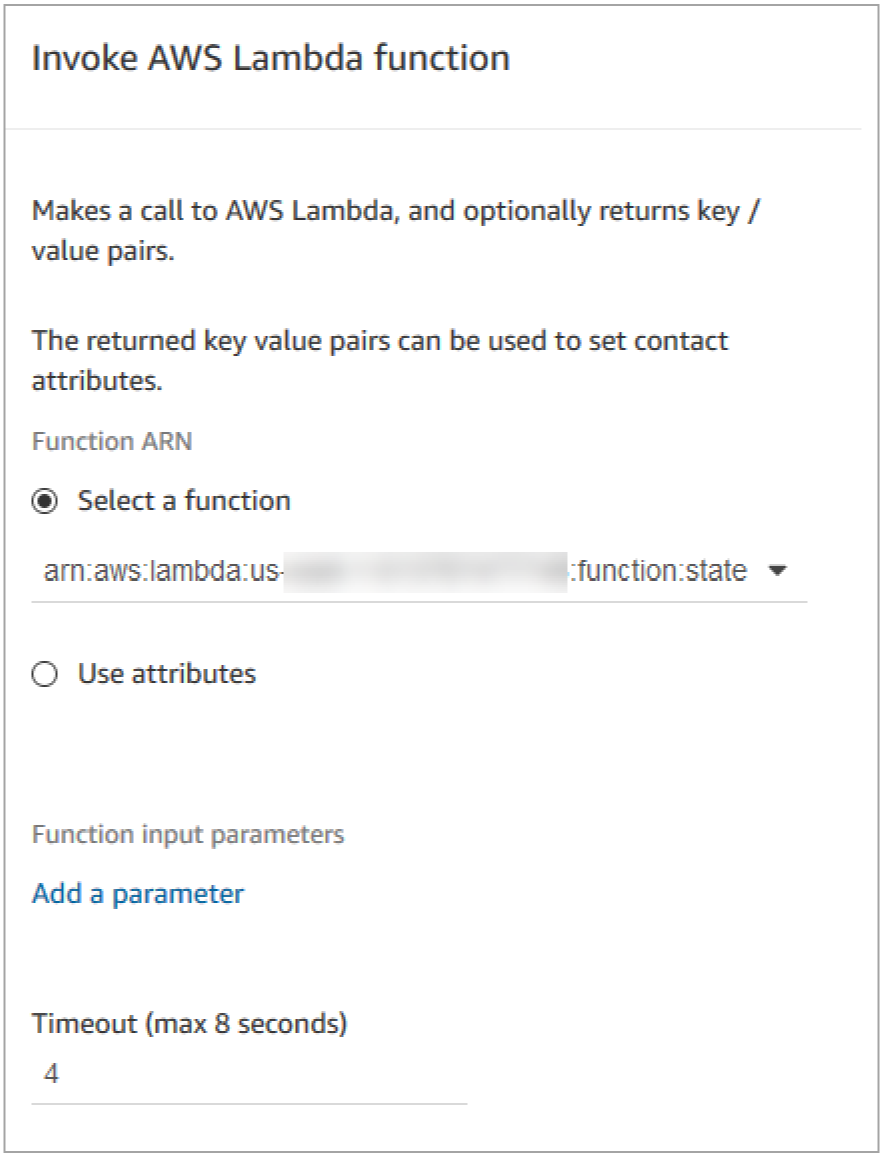
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Invoke AWS Lambda function

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

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

Function ARN

● Select a function

arn:aws:lambda:us-[redacted]:function:state ▾

○ Use attributes

Function input parameters

Add a parameter

Timeout (max 8 seconds)

4

Note the following properties:

- **Timeout**: Enter how long to wait for Lambda to time out.

  If your Lambda invocation gets throttled, the request is retried. It is also retried if a general service failure (500 error) happens.

  When a synchronous invocation returns an error, Amazon Connect retries up to three times, for a maximum of 8 seconds. At that point, the contact is routed down the **Error** branch.

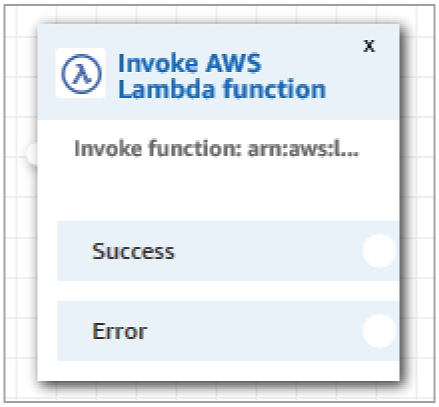
Configuration tips

- To use an AWS Lambda function in a contact flow, first add the function to your instance. For more information, see Add a Lambda function to your Amazon Connect instance (p. 489),

- After you add the function to your instance, you can select the function from the **Select a function** drop-down list in the block to use it in the contact flow.

Configured block

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



Sample flows

Sample Lambda integration (p. 315)

Scenarios

See these topics for scenarios that use this block:

- Invoke AWS Lambda functions (p. 488)

Contact block: Invoke module

Description

Calls a published module, which enables you create reusable sections of a contact flow.

For more information, see Contact flow modules for reusable functions (p. 454).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

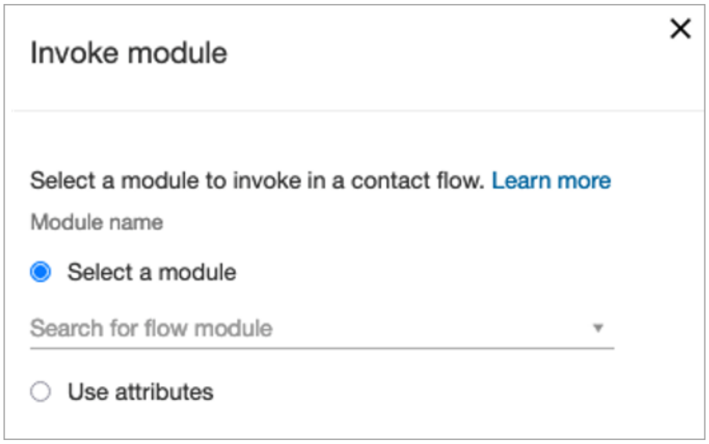
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- Inbound contact flow

Properties



Invoke module

Select a module to invoke in a contact flow. Learn more

Module name

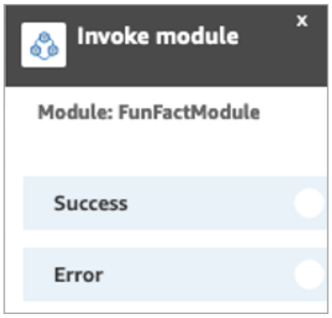
● Select a module

Search for flow module

○ Use attributes

Configured block

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



Invoke module

Module: FunFactModule

Success

Error

Contact block: Loop

Description

- Counts the number of times customers are looped through the **Looping** branch.
- After the loops are completed, the **Complete** branch is followed.
- This block is often used with a **Get customer input** block. For example, if the customer doesn't succeed in entering their account number, you can loop to give them another opportunity to enter it.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes
Chat	Yes

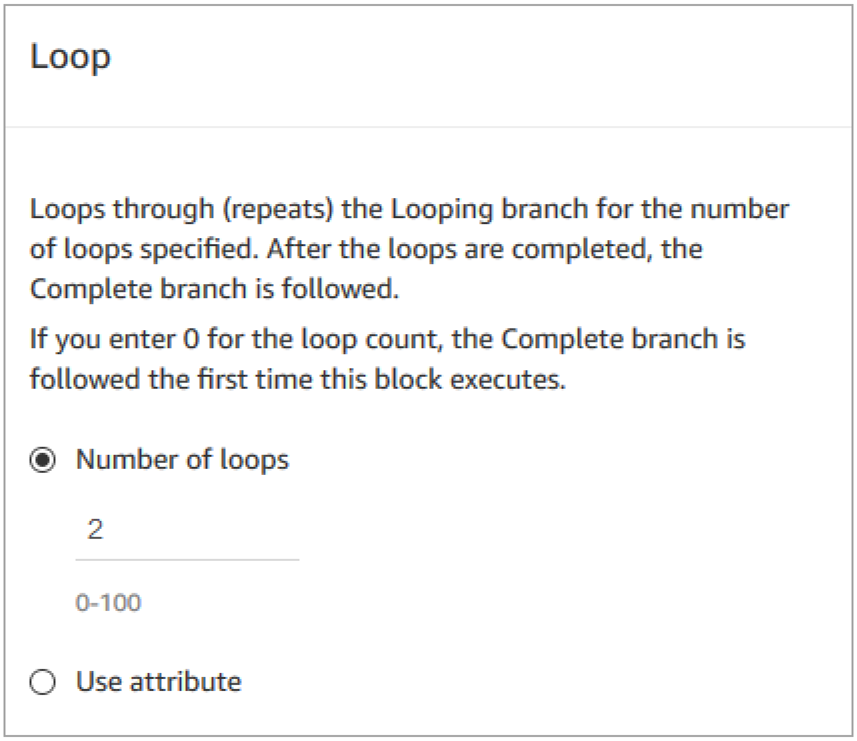
Channel	Supported?
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Loop

Loops through (repeats) the Looping branch for the number of loops specified. After the loops are completed, the Complete branch is followed.

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

● Number of loops

2

0-100

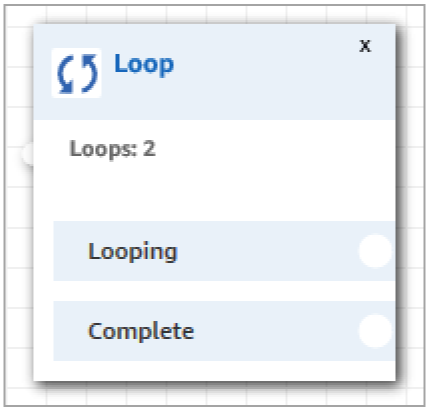
○ Use attribute

Configuration tips

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

Configured block

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



Contact block: Loop prompts

Description

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

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

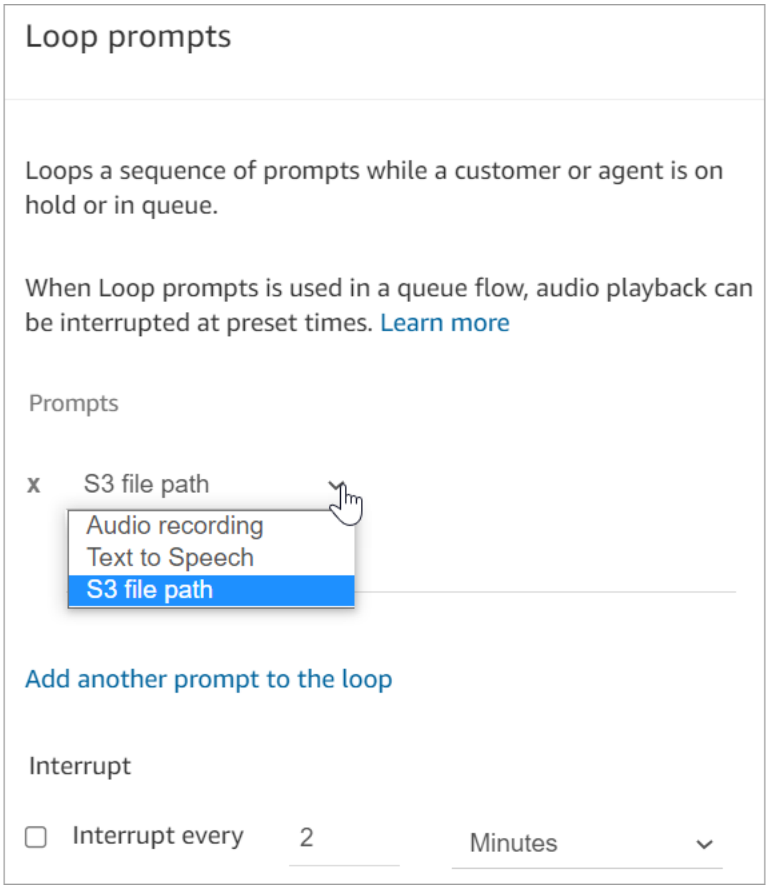
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Loop prompts

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

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

Prompts

x S3 file path

Add another prompt to the loop

Interrupt

□ Interrupt every 2 Minutes

How the Interrupt option works

Let's say you have multiple prompts and you set **Interrupt** to 60 seconds. Following is what will happen:

- The block plays prompts in the order that they are listed for the entirety of the prompt length.
- If the combined play time for the prompts is 75 seconds, after 60 seconds the prompt is interrupted and reset to the 0 second point again.
- It's possible your customers would never hear potentionally important information that is supposed to play after 60 seconds.

This scenario is especially possible when using the default audio prompts that Amazon Connect provides since these audio prompts can be as long as 4 minutes.

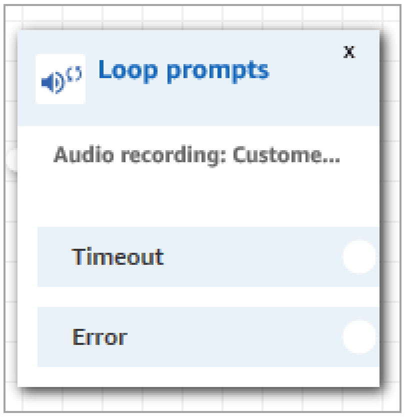
Configuration tips

- The following blocks are not allowed before the **Loop prompts** block:
  - Get customer input (p. 366)
  - Loop (p. 388)
  - Play prompt (p. 393)
  - Start media streaming (p. 423)
  - Stop media streaming (p. 425)
  - Store customer input (p. 426)

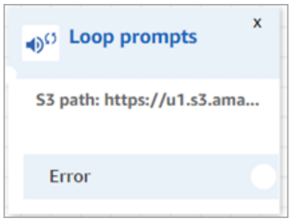
  - Transfer to phone number (p. 433)
  - Transfer to queue (p. 437), including **Transfer to callback queue**
- For information about choosing a prompt from the Amazon Connect library or an S3 bucket, see the Play prompt (p. 393) block.
- When **Loop prompts** is used in a Queue flow, audio playback can be interrupted with a flow at preset times.
- Always use an interruption period that's greater than 20 seconds. This is the amount of time an available agent has to accept the contact. If the interruption period is less than 20 seconds, you might get contacts going down the **Error** branch. This is because Amazon Connect doesn't support dequeuing the customer when they are being routed to an active agent and are in the 20 second window to join.
- The internal counter for the loop is persisted for the call, not the contact flow. If you reuse the contact flow during a call, the loop counter isn't reset.
- If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.
- Some existing contact flows have a version of the **Loop prompts** block that doesn't have an **Error** branch. In this case, a chat contact stops execution of the customer queue flow. The chat is routed when the next agent becomes available.

Configured block

When this block is configured to play a prompt from the Amazon Connect library, it looks similar to the following image:



When this block is configured to play a prompt from Amazon S3, it looks similar to the following image:



Sample flows

See these sample flows for scenarios that use this block:

- Sample interruptible queue flow with callback (p. 315)

Scenarios

See these topics for scenarios that use this block:

- Manage contacts in a queue (p. 476)

Contact block: Play prompt

Description

- This block can play an interruptible audio prompt, play a text-to-speech message, or send a chat response.
- Amazon Connect includes a set of pre-recorded prompts for you to use.
- To use your own voice prompts, you have the following options:
  - **Use the Amazon Connect library**: You can record and upload your audio prompts in using the Amazon Connect admin console. For instructions, see Create prompts (p. 456).
  - **Use Amazon S3**: You can store as many voice prompts as needed in Amazon S3 and access them in real time by using contact attributes in the **Play prompt** block.

    For example, based on a customer's preferred language, you can dynamically play a voice prompt with a local accent that greets them and thanks them for being a loyal member. You can even concatenate multiple attributes, such as line of business or language preference to create personalized interactions; for example, reservations + Spanish language.

Requirements

- Amazon Connect supports .wav files to use for your prompt. You must use .wav files that are 8KHz, and mono channel audio with U-Law encoding. Otherwise, the prompt won't play correctly. You can use publicly available third-party tools to convert your .wav files to U-Law encoding. After converting the files, upload them to Amazon Connect.
- Amazon Connect supports prompts that are less than 50MB and less than five minutes long.
- When storing prompts in an S3 bucket: for Regions that are disabled by default (also called opt-in Regions) such as Africa (Cape Town), your bucket must be in the same Region.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes
Chat	Yes
Task	No - takes the **Okay** branch but it has no effect

Contact flow types

You can use this block in the following contact flow types (p. 445):

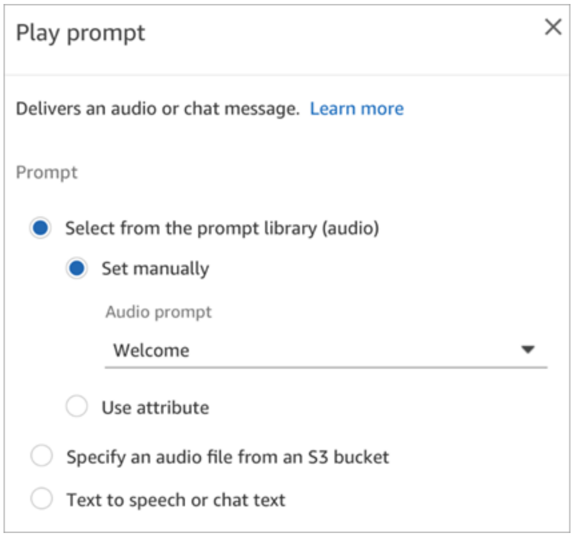
- Inbound contact flow
- Customer Queue flow
- Customer Whisper flow. You can play prompts from the Amazon Connect library but not prompts stored in Amazon S3.
- Agent Whisper flow: You can play prompts from the Amazon Connect library but not prompts stored in Amazon S3.
- Transfer to Agent flow
- Transfer to Queue flow

Properties

The properties provide you different ways to choose the prompt to be played.

Prompts stored in library

Select from the prompt library (audio): Choose from one of the pre-recorded prompts included with Amazon Connect, or use the Amazon Connect admin console to record and upload (p. 456) your own prompt. There's no way to upload prompts in bulk.



Play prompt ✕

Delivers an audio or chat message. Learn more

Prompt

● Select from the prompt library (audio)

● Set manually

Audio prompt: Welcome

○ Use attribute

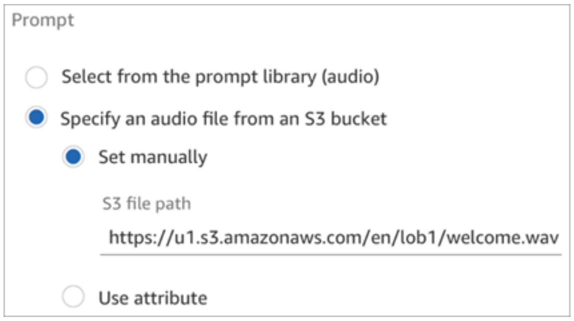
○ Specify an audio file from an S3 bucket

○ Text to speech or chat text

Prompts stored in Amazon S3

Specify an audio file from an S3 bucket: Store as many prompts as you need in an S3 bucket and then refer to them by specifying the bucket path. For best performance, we recommend creating the S3 bucket in the same Region as your Amazon Connect instance.

The following image shows an example of how to set the file path manually.



Prompt

○ Select from the prompt library (audio)

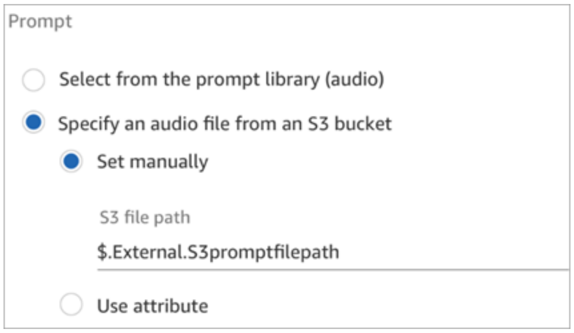
● Specify an audio file from an S3 bucket

● Set manually

S3 file path: https://u1.s3.amazonaws.com/en/lob1/welcome.wav

○ Use attribute

The following image shows how to specify the S3 bucket path using attributes:



Prompt

○ Select from the prompt library (audio)

● Specify an audio file from an S3 bucket

● Set manually

S3 file path

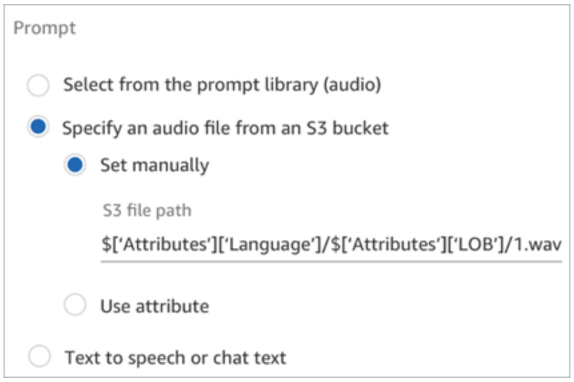
$.External.S3promptfilepath

○ Use attribute

You can provide the S3 path with concatenation, as shown in the following example. This enables you to personalize the prompt, for example, by line of business and language.

Note that only the last part of path is shown in the image but you would enter the full path, for example:

```
https://example.s3.amazon.aws.com/$['Attributes']['Language']/$['Attributes']
['LOB']/1.wav
```



Prompt

○ Select from the prompt library (audio)

● Specify an audio file from an S3 bucket

● Set manually

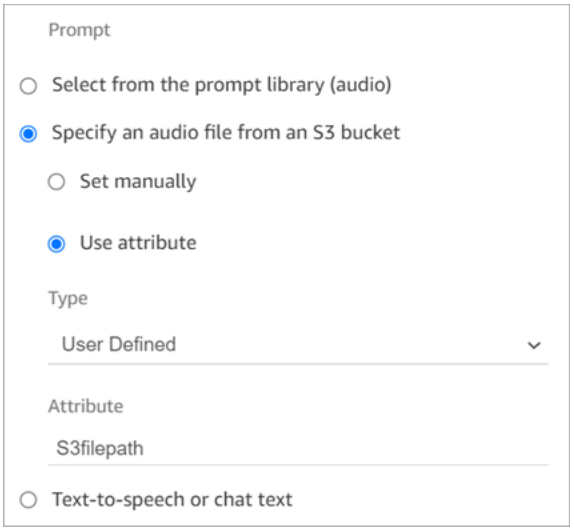
S3 file path

$['Attributes']['Language']/$['Attributes']['LOB']/1.wav

○ Use attribute

○ Text to speech or chat text

The following example shows how you can specify the S3 path dynamically using a user-defined attribute.



Prompt

○ Select from the prompt library (audio)

● Specify an audio file from an S3 bucket

○ Set manually

● Use attribute

Type

User Defined

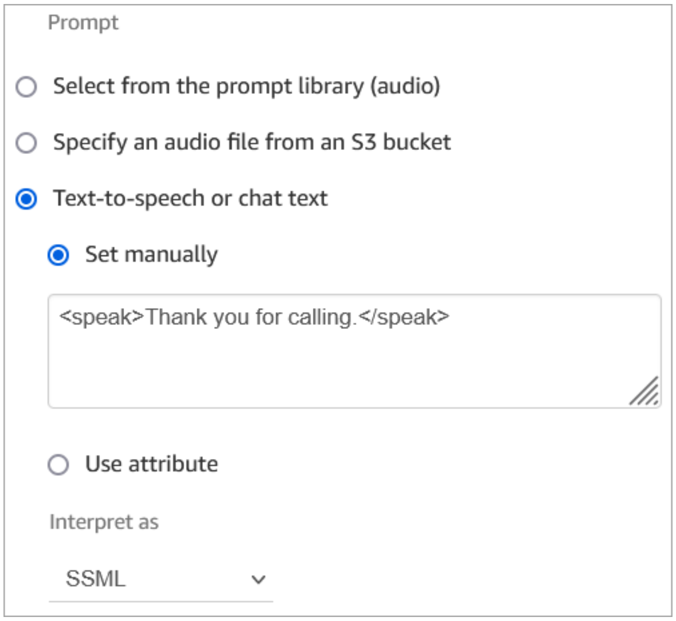
Attribute

S3filepath

○ Text-to-speech or chat text

Text-to-speech or chat text

You can enter plain text, or SSML, as shown in the following image:


Prompt

○ Select from the prompt library (audio)

○ Specify an audio file from an S3 bucket

● Text-to-speech or chat text

● Set manually

```
<speak>Thank you for calling.</speak>
```

○ Use attribute

Interpret as

SSML

SSML-enhanced input text gives you more control over how Amazon Connect generates speech from the text you provide. You can customize and control aspects of speech such as pronunciation, volume, and speed.

For a list of SSML tags you can use with Amazon Connect, see SSML tags supported by Amazon Connect (p. 464).

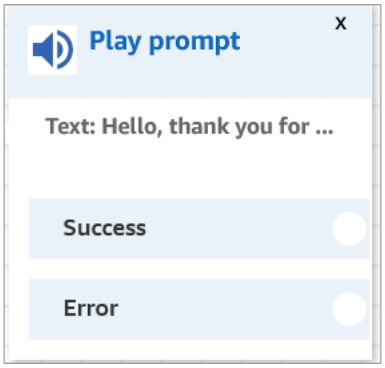
For more information, see Add text-to-speech to prompts (p. 456).

Configuration tips

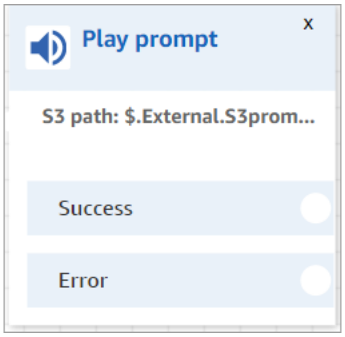
- For step-by-step instructions about how to set up a dynamic prompt using contact attributes, see Dynamically select which prompts to play (p. 459).
- When playing prompts from an S3 bucket, for best performance we recommend creating the bucket in the same Region as your Amazon Connect instance.
- When you use text, either for text-to-speech or chat, you can use a maximum of 3,000 billed characters, which is 6,000 characters total. You can also specify text in a flow using a contact attribute.
- Some existing contact flows have a version of the **Play prompt** block that doesn't have an **Error** branch. In this case, the **Okay** branch will always be taken at runtime. If you update the configuration of a **Play prompt** block that doesn't have an **Error** branch, an **Error** branch will be added to the block automatically in the editor.
- A contact is routed down the **Error** branch in the following situations:
  - Amazon Connect is unable to download the prompt from S3. This may be due to an incorrect file path, or the S3 bucket policy is not set up correctly and Amazon Connect does not have access. For instructions about how to apply the policy, and a template you can use, see Set up prompts to play from an S3 bucket (p. 461).
  - Incorrect audio file format. Only .wav files are supported.
  - The audio file is larger than 50MB or longer than five minutes.
  - The SSML is incorrect.
  - The text-to-speech length exceeds 6000 characters.
  - The the Amazon Resource Name (ARN) for the prompt is incorrect.

Configured block

The following image shows what this block looks like when it's configured for text-to-speech:



The following image shows what this block looks like when it's configured for an S3 bucket:



Sample flows

All of the sample flows use the **Play prompt** block. Take a look at the Sample inbound flow (first contact experience) (p. 309) to see a **Play prompt** for chat and one for audio.

Contact block: Set callback number

Description

- Specify the attribute to set the callback number.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

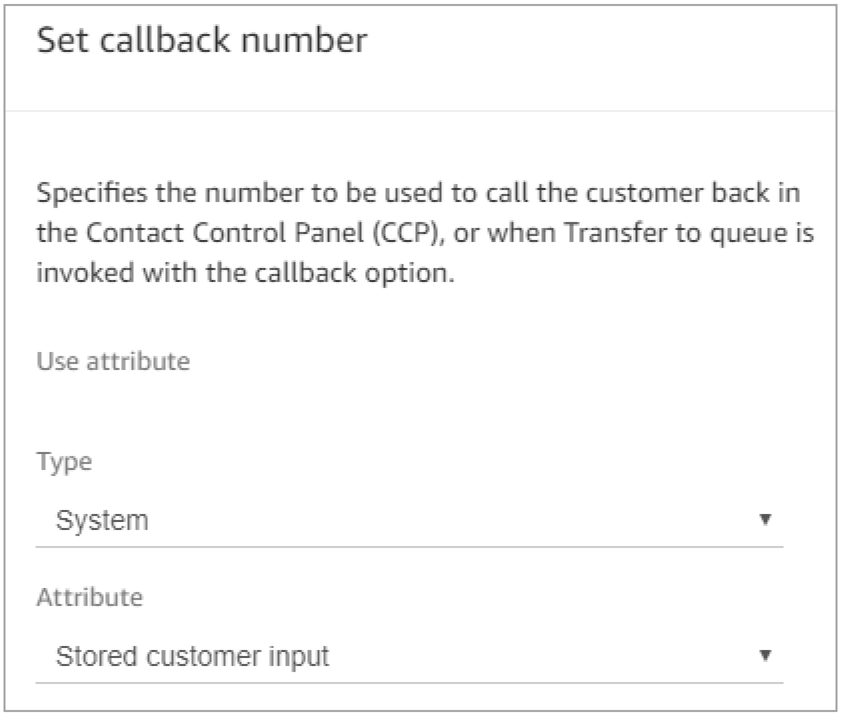
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Set callback number

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

Use attribute

Type: System

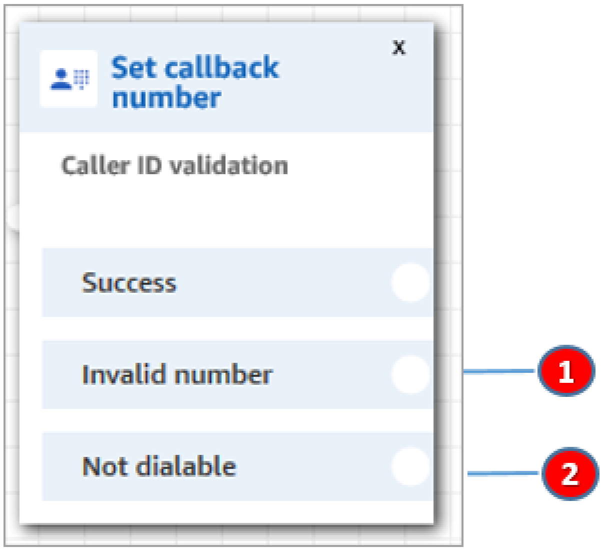
Attribute: Stored customer input

Configuration tips

- The Store customer input (p. 426) block often comes before this block. It stores the customer's callback number.

Configured block

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



1. The customer entered phone number that is not valid.
2. Amazon Connect is unable to dial that number. For example, if your instance is not allowed to make calls to +447 prefix phone numbers, and the customer requested callback to a +447 prefix number. Even though number is valid, Amazon Connect cannot call it.

Sample flows

See these sample flows for scenarios that use this block:

- Sample queue configurations (p. 311)
- Sample queued callback (p. 314): this sample only applies to previous instances of Amazon Connect.

Scenarios

See these topics for scenarios that use this block:

- Set up queued callback (p. 481)
- About queued callbacks in metrics (p. 1002)

Contact block: Set contact attributes

Description

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

  For more information about how to use contact attributes, see Use Amazon Connect contact attributes (p. 515).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

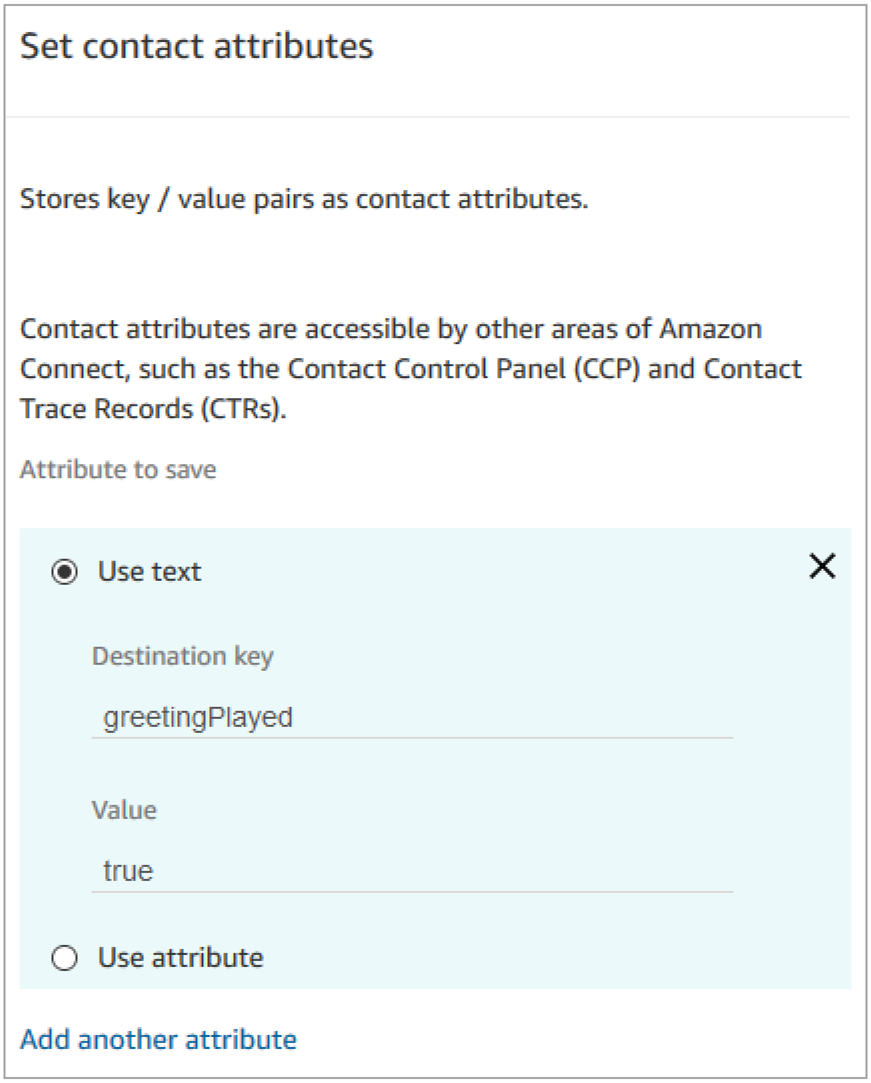
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Set contact attributes

Stores key / value pairs as contact attributes.

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

Attribute to save

● Use text

Destination key

greetingPlayed

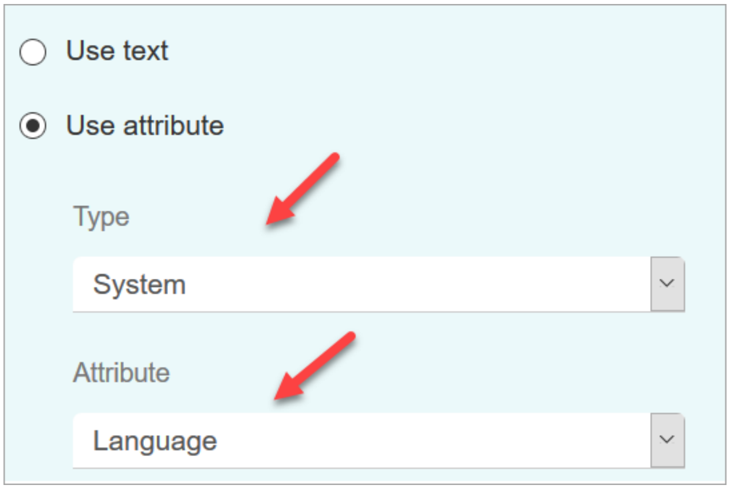
Value

true

○ Use attribute

Configuration tips

- When using a user-defined destination key, you can name it anything you want but don't include the **$** and **.** (period) characters. They are not allowed because they are both used in defining the attribute paths in JSONPath.
- You can use the **Set contact attribute** block to set the language attribute required for an Amazon Lex V2 bot. (Your language attribute in Amazon Connect must match the language model used to build your Amazon Lex V2 bot.)

  ○ Use text

  ● Use attribute

  Type

  System

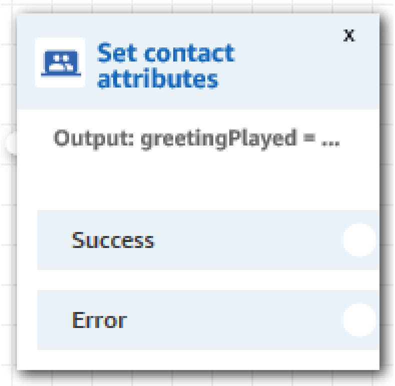
  Attribute

  Language

  Or, you can use the Set voice (p. 415) block to set the language required for an Amazon Lex V2 bot.

Configured block

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



Set contact attributes

Output: greetingPlayed = ...

Success

Error

Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 309)

Scenarios

See these topics for scenarios that use this block:

- How to reference contact attributes (p. 531)

Contact block: Set customer queue flow

Description

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

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

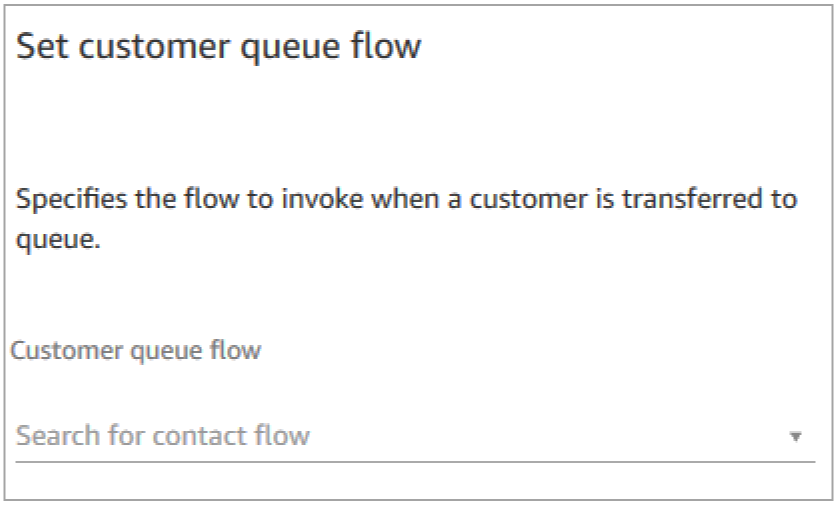
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Set customer queue flow

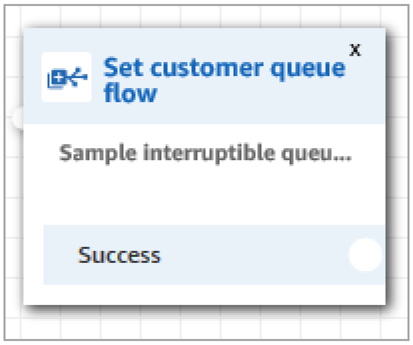
Specifies the flow to invoke when a customer is transferred to queue.

Customer queue flow

For information about using attributes, see Use Amazon Connect contact attributes (p. 515).

Configured block

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample queued callback (p. 314)

Contact block: Set disconnect flow

Description

- Specifies which contact flow to run after a disconnect event during a contact.

  A disconnect event is when:
  - A call, chat, or task is disconnected by an agent.
  - A task is disconnected as a result of a flow action.
  - A task expires. The task is automatically disconnected if it is not completed in 7 days.

  When the disconnect event occurs, the corresponding contact flow runs.
- Here are examples of when you might use this block:
  - Run post-call surveys. For example, the agent asks the customer to remain on the line for a post-call survey. The agent hangs up and a disconnect flow is run. In the disconnect flow, the customer is asked a set of questions using the Get customer input (p. 366) block. Their answers are uploaded using an Invoke AWS Lambda function (p. 385) block to an external customer feedback database. The customer is thanked and disconnected.

    For more information about creating post-call surveys, see this blog post by an AWS Solution Architect: Create post call surveys in Amazon Connect.
  - In a chat scenario, if a customer stops responding to the chat, use this block to decide whether to run the disconnect flow and call a Wait (p. 441) block, or end the conversation.
  - In task scenarios where a task may not be completed in 7 days, use this block to run a disconnect flow to determine whether the task should be requeued, or completed/disconnected (p. 362) by a flow action.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes

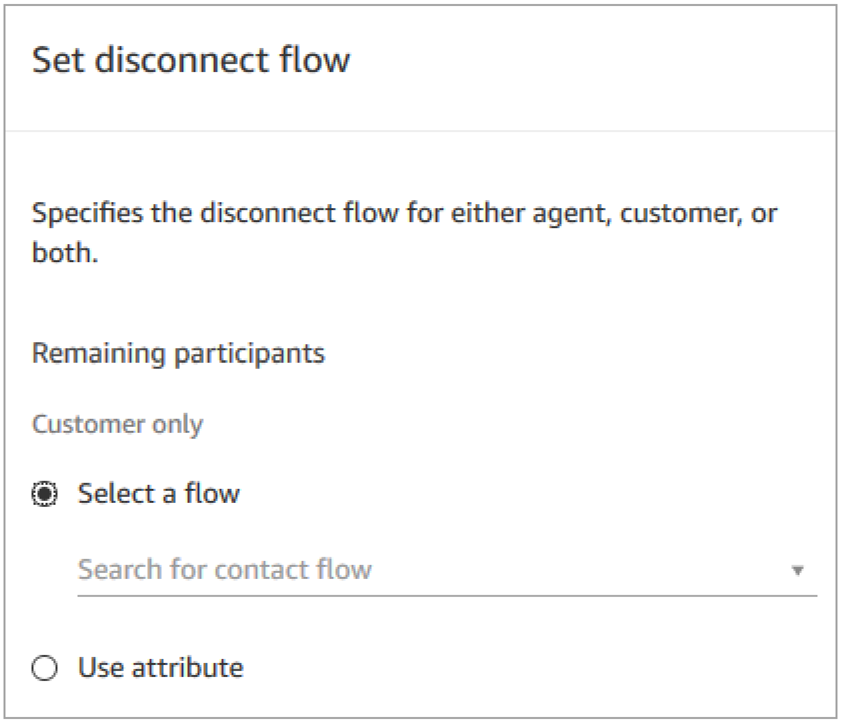
Channel	Supported?
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Set disconnect flow

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

Remaining participants

Customer only

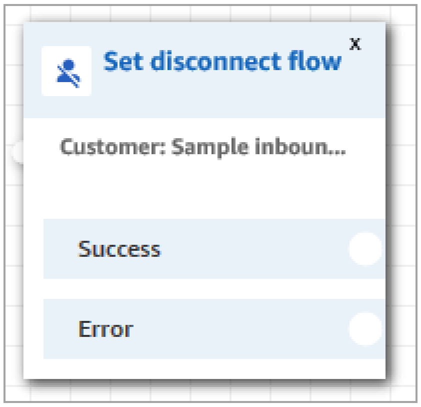
● Select a flow

Search for contact flow ▾

○ Use attribute

Configured block

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 309)

Scenarios

See these topics for scenarios that use this block:

- Example chat scenario (p. 13)
- Create post call surveys in Amazon Connect

Contact block: Set hold flow

Description

- Links from one contact flow type to another.
- Specifies the flow to invoke when a customer or agent is put on hold.

  If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

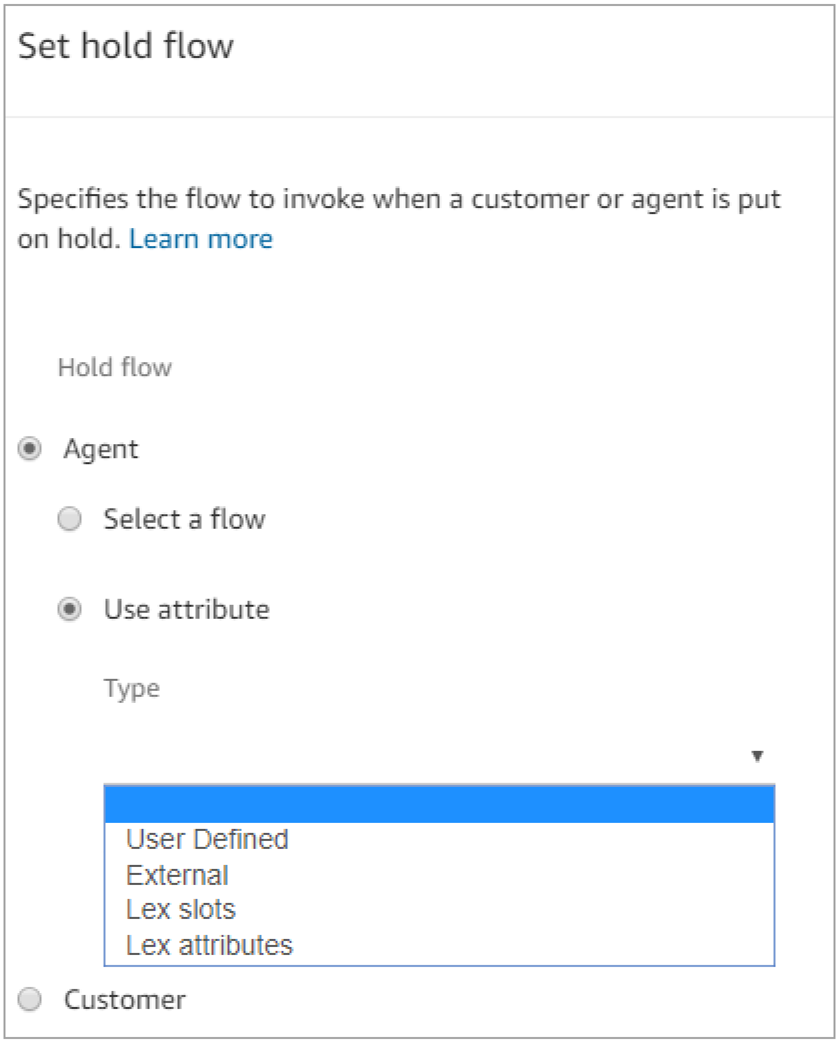
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Set hold flow

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

Hold flow

● Agent

○ Select a flow

● Use attribute

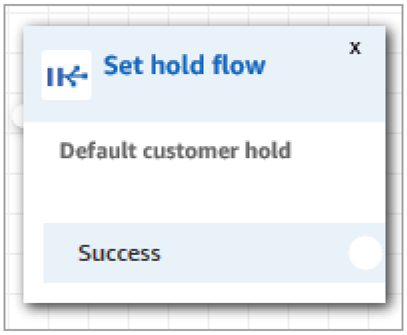
Type

○ Customer

For information about using attributes, see Use Amazon Connect contact attributes (p. 515).

Configured block

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



Contact block: Set logging behavior

Description

- Enables contact flow logs so you can track events as contacts interact with contact flows.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

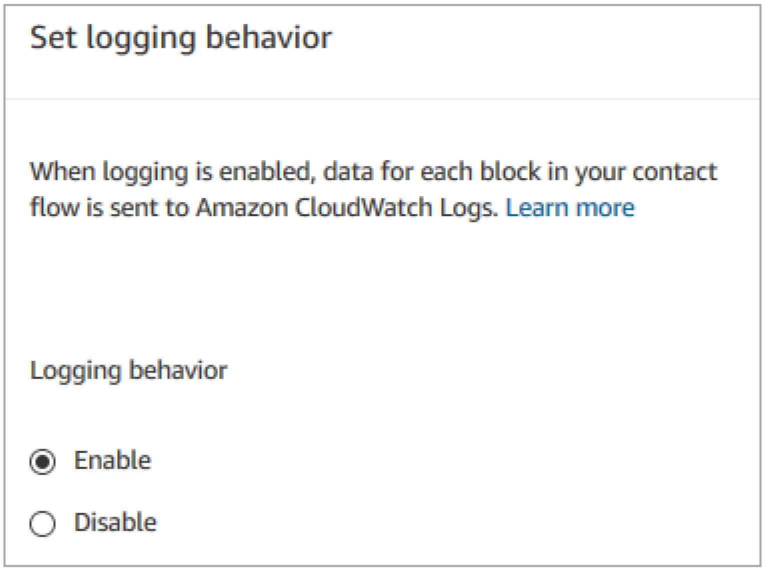
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Set logging behavior

When logging is enabled, data for each block in your contact flow is sent to Amazon CloudWatch Logs. Learn more

Logging behavior

● Enable

○ Disable

Scenarios

See these topics for more information about contact flow logs:

- Track events as customers interact with contact flows (p. 509)

Contact block: Set recording and analytics behavior

Description

- Sets options for recording and/or monitoring (listen-in) voice and chat conversations.
- It enables features in Contact Lens for Amazon Connect. For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 811).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

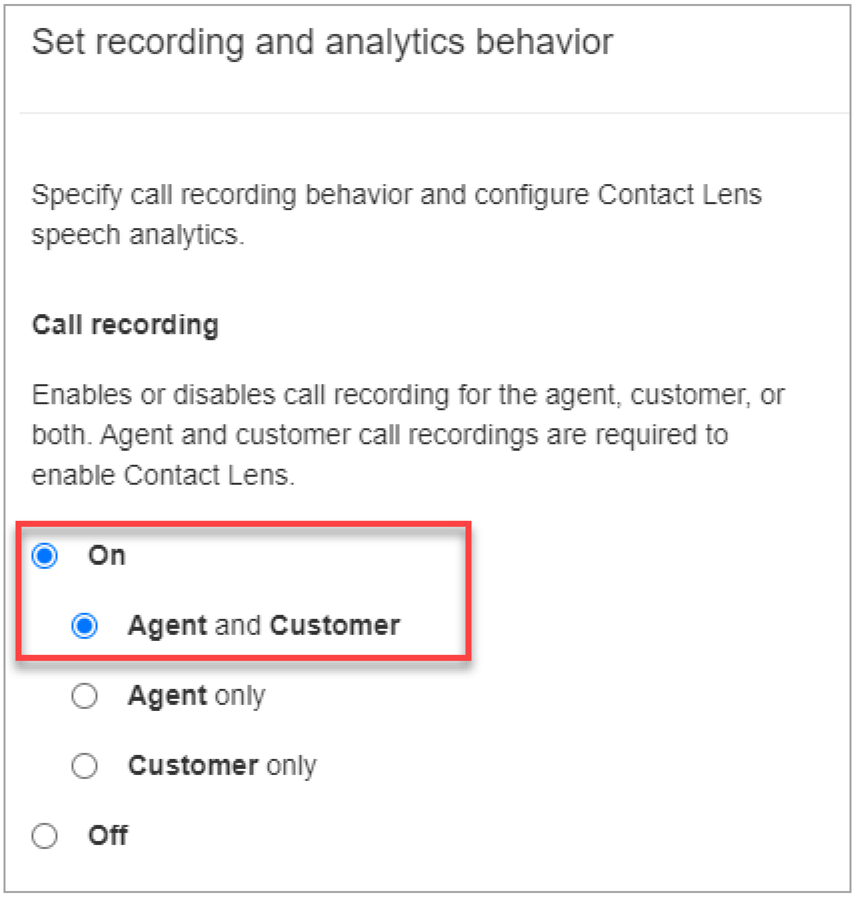
Channel	**Supported?**
Voice	Yes
Chat	Yes
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Set recording and analytics behavior

Specify call recording behavior and configure Contact Lens speech analytics.

Call recording

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

● **On**

  ● **Agent** and **Customer**

  ○ **Agent** only

  ○ **Customer** only

○ **Off**

When configuring this block to set up recording behavior (p. 479), choose as follows:

- To record voice conversations, choose what you want to record: **Agent and Customer**, **Agent only**, or **Customer only**.
- To record chat conversations, you need to choose **Agent and Customer**.
- To enable monitoring of voice and/or chat conversations, you need to choose **Agent and Customer**.

For information about using this block to enable Contact Lens, see Enable Contact Lens for Amazon Connect (p. 812).

Configuration tips

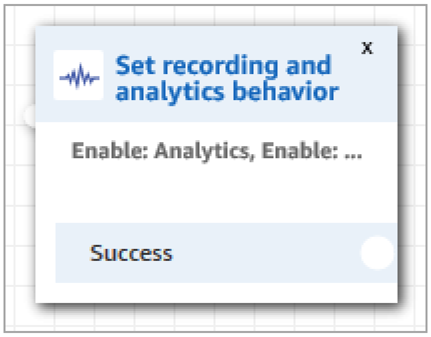
- Let's say you have a flow that links to a flow that links to another flow. Each flow might have it's own **Set recording behavior** block. The last **Set recording behavior** block overrides the settings of the previous two **Set recording behavior** blocks.

For example, you might have a contact flow with **Set recording behavior to record Agent and Customer**. But if the next **Set recording behavior** block is set to **Agent only**, that block overrides the behavior of the previous block.

- If an agent puts a customer on hold, the agent is still recorded, but the customer is not.
- If you want to transfer a contact to another agent or queue, and you want to continue using Contact Lens to collect data, you need to add to the flow another **Set recording behavior** block with **Enable analytics** turn on. This is because a transfer generates a second contact ID and contact record. Contact Lens needs to run on that contact record as well.

Configured block

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



Set recording and analytics behavior

Enable: Analytics, Enable: ...

Sample flows

See these sample flows for scenarios that use this block:

- Sample inbound flow (first contact experience) (p. 309)

Scenarios

See these topics for scenarios that use this block:

- Set up recording behavior (p. 479)
- Monitor live conversations (p. 798)
- Review recorded conversations (p. 801)
- Analyze conversations using Contact Lens for Amazon Connect (p. 811)

Contact block: Set Voice ID

Description

- Enables audio streaming and sets thresholds for voice authentication and detection of fraudsters in a watchlist. For more information about this feature, see Use real-time caller authentication with Voice ID (p. 858).

- Sends audio to Amazon Connect Voice ID to verify the caller's identity and match against fraudsters in watchlist, as soon as the call is connected to a contact flow.
- Use a Play prompt (p. 393) block before **Set Voice ID** to stream audio properly. You can edit it to include a simple message such as "Welcome."
- Use a Set contact attributes (p. 399) block after **Set Voice ID** to set the customer ID for the caller.
- Use a Check Voice ID (p. 339) block after **Set Voice ID** to branch based on the results of the enrollment check, authentication, or fraud detection.
- For information about how to use **Set Voice ID** in a contact flow, along with Check Voice ID (p. 339) and Set contact attributes (p. 399), see Step 2: Configure Voice ID in your contact flow (p. 865) in Enable Voice ID (p. 862).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

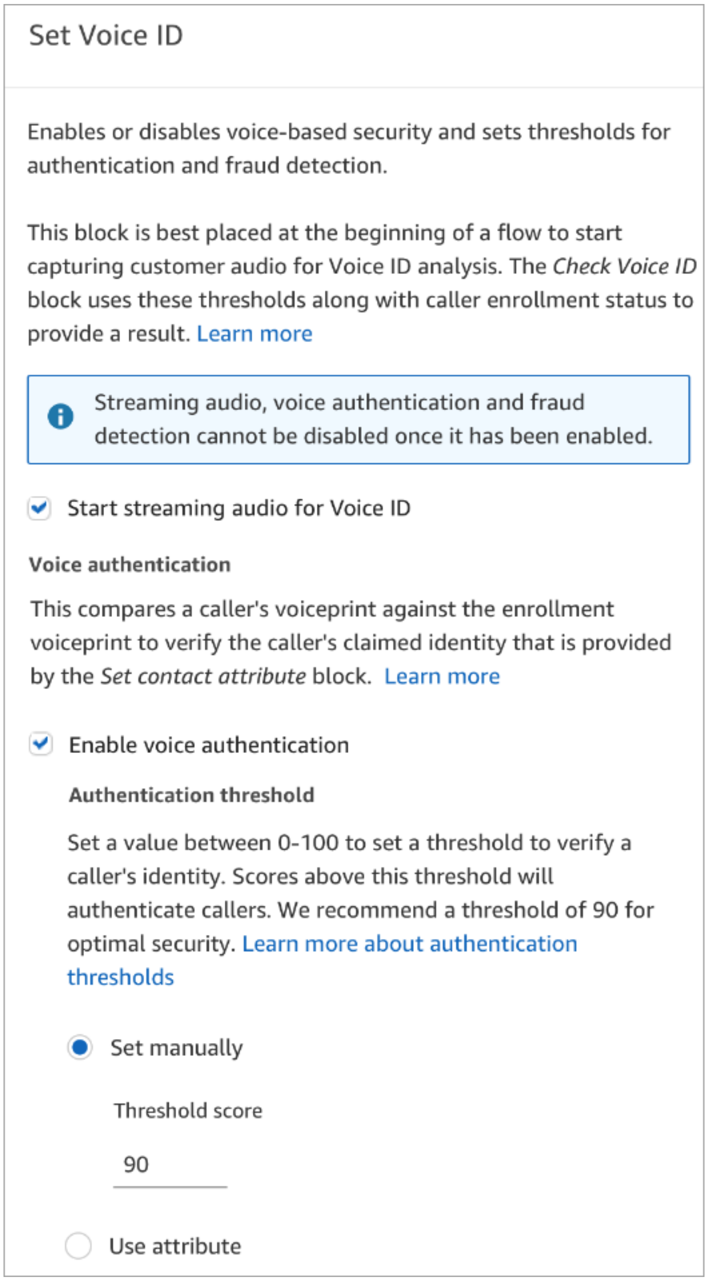
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Set Voice ID

Enables or disables voice-based security and sets thresholds for authentication and fraud detection.

This block is best placed at the beginning of a flow to start capturing customer audio for Voice ID analysis. The *Check Voice ID* block uses these thresholds along with caller enrollment status to provide a result. Learn more

Streaming audio, voice authentication and fraud detection cannot be disabled once it has been enabled.

☑ Start streaming audio for Voice ID

Voice authentication

This compares a caller's voiceprint against the enrollment voiceprint to verify the caller's claimed identity that is provided by the *Set contact attribute* block. Learn more

☑ Enable voice authentication

Authentication threshold

Set a value between 0-100 to set a threshold to verify a caller's identity. Scores above this threshold will authenticate callers. We recommend a threshold of 90 for optimal security. Learn more about authentication thresholds

● Set manually

Threshold score

90

○ Use attribute

Start streaming audio for Voice ID

When this option is selected, Amazon Connect begins streaming audio from the customer's channel to Voice ID.

You can add this block several places in a contact flow, but after **Start streaming audio** is selected, it cannot be disabled, even if later in the flow there are other **Set Voice ID** blocks that do not have it enabled.

Voice authentication

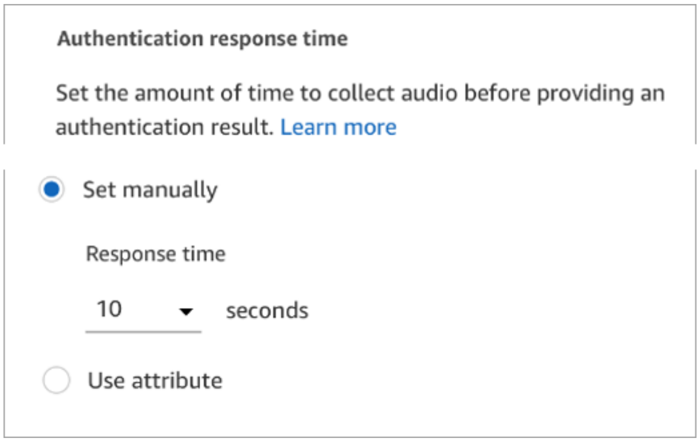
Authentication threshold: When Voice ID compares the voiceprint of the caller to the enrolled voiceprint of the claimed identity, it generates an authentication score between 0-100. This score indicates the confidence of a match. You can configure a threshold for the score which indicates whether the caller is authenticated. The default threshold of 90 provides high security for most cases.

- If the authentication score is below the configured threshold, Voice ID treats the call as not authenticated.
- If the authentication score is above the configured threshold, Voice ID treats the call as authenticated.

For example, if the person is sick and calling from a mobile device in their car, the authentication score is going to be slightly lower than when the person is well and calling from a quiet room. If an imposter is calling, the authentication score is much lower.

Authentication response time

You can set the authentication response time between 5 and 10 seconds, which determines how quickly you want Voice ID authentication analysis to complete. Lowering it makes the response time faster at the tradeoff of lower accuracy. When you're using self-service IVR options where callers do not talk a lot, you may want to reduce this time. You can then increase the time if the call needs to be transferred to an agent.



Authentication response time

Set the amount of time to collect audio before providing an authentication result. Learn more

● Set manually

Response time

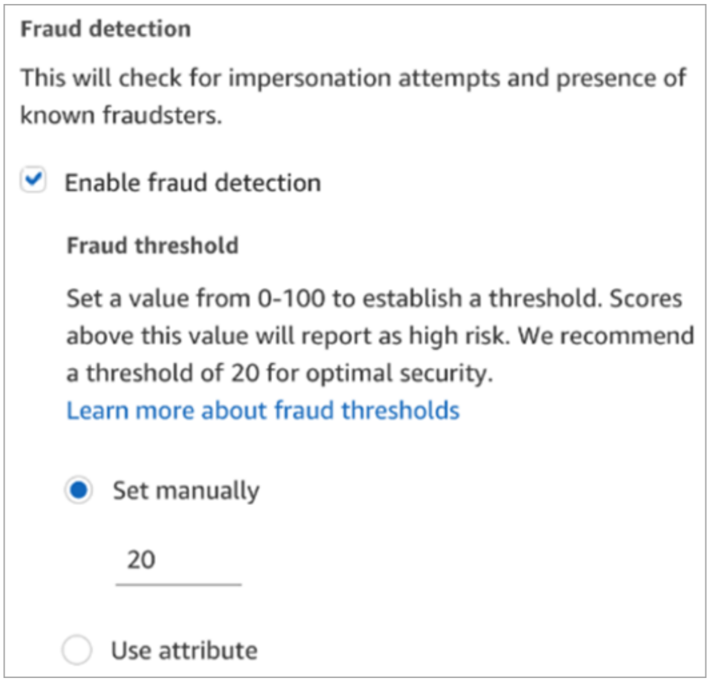
10 ▾ seconds

○ Use attribute

Use attributes to set the authentication threshold dynamically. For example, you may want to raise the threshold based on the membership level of the customer, or the type of transaction or information they are calling about.

Fraud detection

The threshold you set for fraud detection is used to measure risk. Scores higher than the threshold are reported as higher risk. Scores lower than the threshold are reported as lower risk. Raising the threshold lowers false positive rates (makes result more certain), but raises false negative rates



Fraud detection

This will check for impersonation attempts and presence of known fraudsters.

☑ Enable fraud detection

Fraud threshold

Set a value from 0-100 to establish a threshold. Scores above this value will report as high risk. We recommend a threshold of 20 for optimal security.
Learn more about fraud thresholds

● Set manually

20

○ Use attribute

Use attributes to set the fraud threshold dynamically. For example, you may want to lower the threshold for high wealth customers, or the type of transaction or information they are calling about.

Configuration tips

- For the **Authentication threshold**, we recommend that you start with the default of 90 and adjust until you find a good balance for your business.

  Every time you increase the value of the **Authentication threshold** beyond the default of 90, there's a tradeoff:

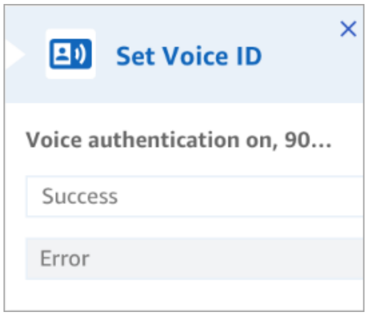
  - The higher the threshold, the greater the false reject rate (FRR), that is, the likelihood that an agent will need to verify the customer's identity.

    For example, if you set it too high, such as greater than 95, agents will need to verify every customer's identity.
  - The lower the threshold, the greater the false acceptance rate (FAR), that is, the likelihood that Voice ID will incorrectly accept an access attempt by an unauthorized caller.
- When Voice ID verifies that the voice belongs to the enrolled customer, it returns a status of **Authenticated**. Add a Check Voice ID (p. 339) block to you flow branch based on the returned status.
- For the **Fraud threshold**, we recommend that you start with the default of 20 and adjust until you find a good balance for your business.

  If the caller's score is above the threshold, it indicates there's a higher risk for fraud in that call.

Configured block

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



More information

See the following topic for more information about this block:

- Use real-time caller authentication with Voice ID (p. 858)
- Contact block: Check Voice ID (p. 339)
- Use Voice ID (p. 1189)

Contact block: Set voice

Description

- Sets the text-to-speech (TTS) language and voice to use for the contact flow.
- The default voice is configured to Joanna (Conversational speaking style).
- You can choose **Override speaking style** to make it and other voices Amazon Polly Neural Text-to-Speech (NTTS). Neural voices make automated conversations sound more lifelike by improving the pitch, inflection, intonation, and tempo.

  For a list of supported neural voices, see Neural Voices in the *Amazon Polly Developer Guide*.
- After this block is run, any TTS invocation resolves to the neural or standard voice selected.
- If this block is triggered during a chat conversation, the contact goes down the **Success** branch. It has no effect on the chat experience.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

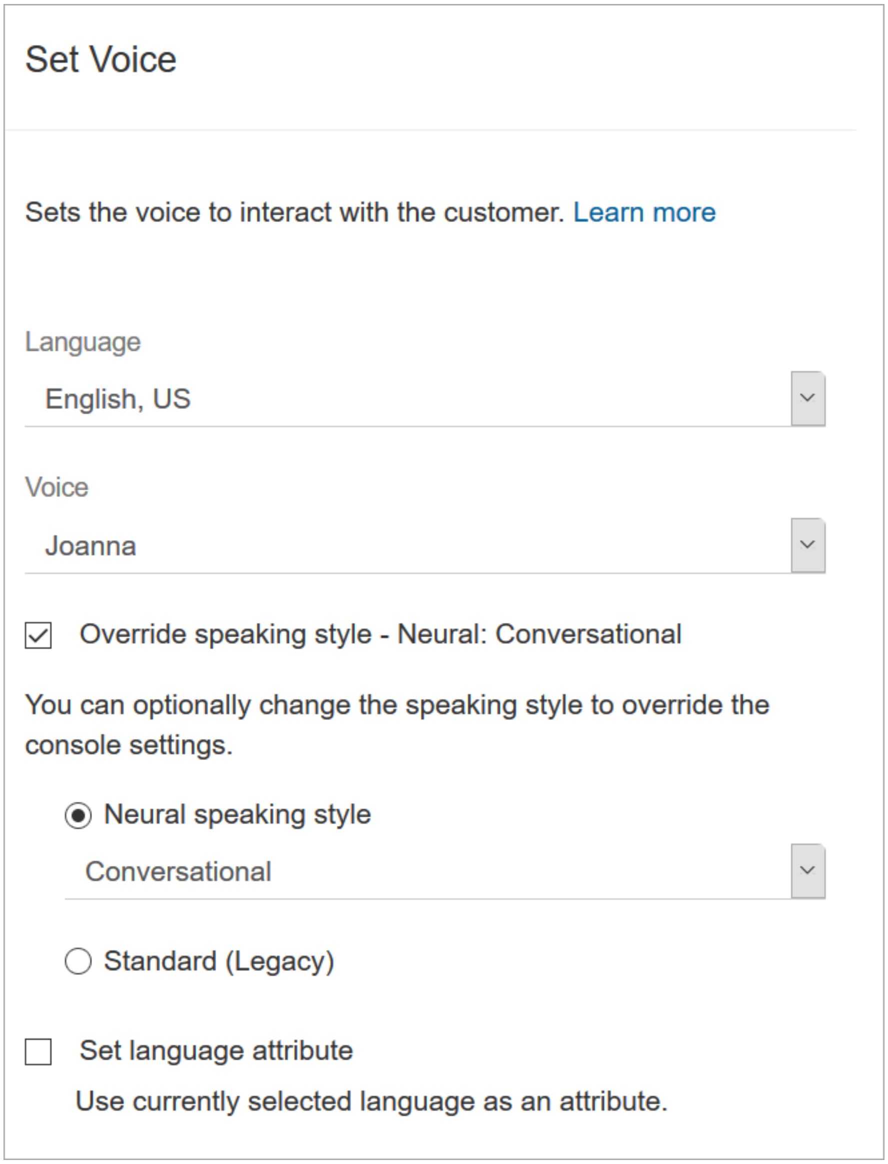
Channel	Supported?
Voice	Yes
Chat	No - Success branch
Task	No - Success branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

- All flows

Properties



Set Voice

Sets the voice to interact with the customer. Learn more

Language

English, US

Voice

Joanna

☑ Override speaking style - Neural: Conversational

You can optionally change the speaking style to override the console settings.

● Neural speaking style

Conversational

○ Standard (Legacy)

□ Set language attribute

Use currently selected language as an attribute.

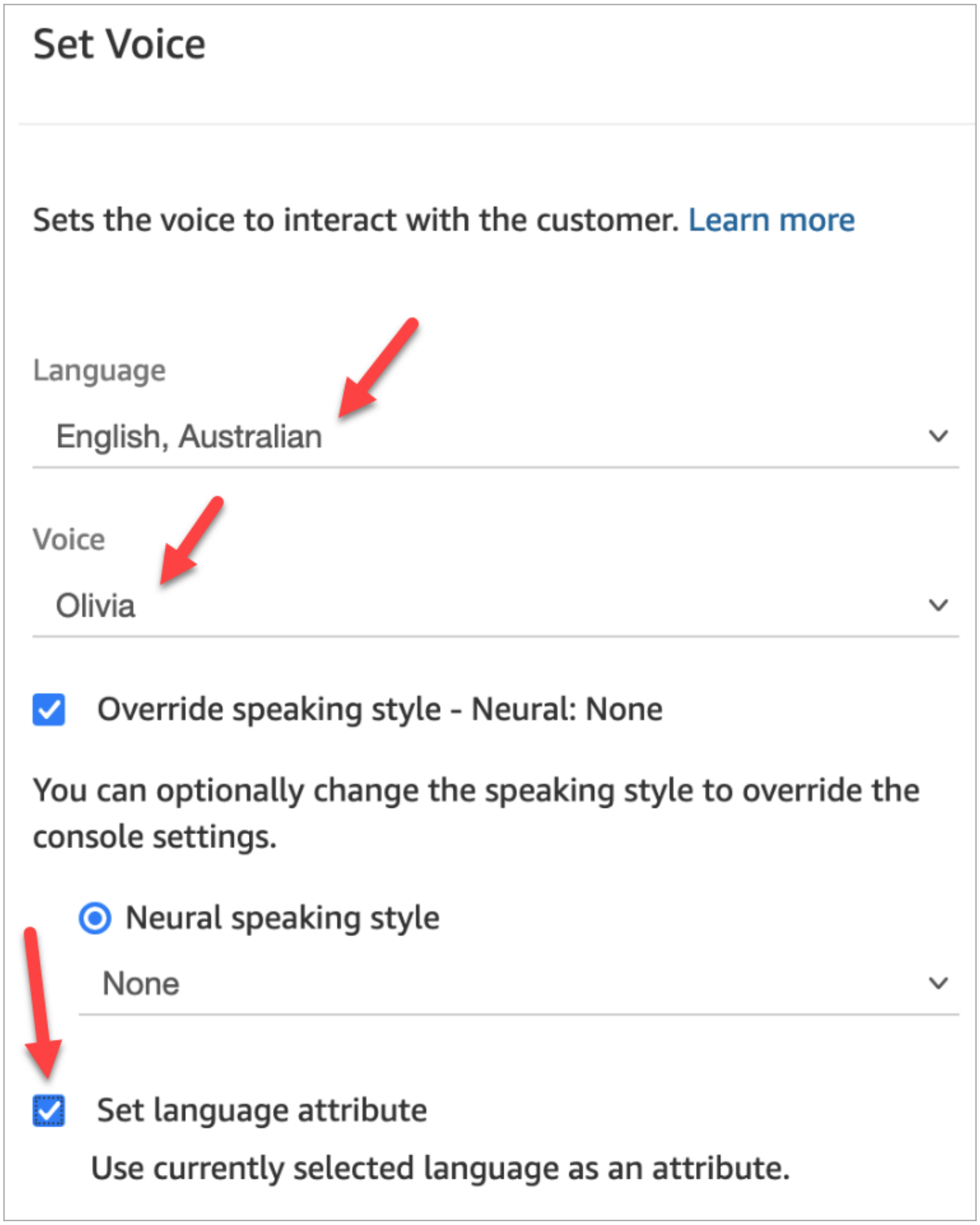
Tip
For voices that support only neural speaking styles but not standard, the **Override speaking style** is automatically selected. You do not have the option to unselect it.

Use an Amazon Lex V2 bot with Amazon Connect

If you're using an Amazon Lex V2 bot, your language attribute in Amazon Connect must match the language model used to build your Lex bot. This is different than Amazon Lex (Classic).

- If you build an Amazon Lex V2 bot with a different language model—for example, en_AU, fr_FR, es_ES, and more—under **Voice**, choose a voice that corresponds to that language, and then must choose **Set language attribute**, as shown in the following image.

- If you're not using an en-US voice with an Amazon Lex V2 bot and don't choose **Set language attribute**, the Get customer input (p. 366) block results in an error.
- For bots with multiple languages (for example, en_AU and en_GB) choose **Set language attribute** for one of the languages.



Set Voice

Sets the voice to interact with the customer. Learn more

Language

English, Australian

Voice

Olivia

☑ Override speaking style - Neural: None

You can optionally change the speaking style to override the console settings.

● Neural speaking style

None

☑ Set language attribute

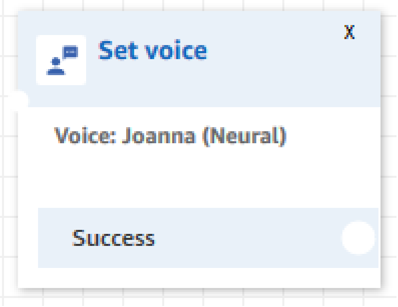
Use currently selected language as an attribute.

Configuration tips

- For the **Joanna** and **Matthew** neural voices, in American English (en-US), you can also specify a Conversational speaking style or a Newscaster speaking style.

Configured block

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



Set voice

Voice: Joanna (Neural)

Scenarios

See these topics for scenarios that use this block:

- Add text-to-speech to prompts (p. 456)

Contact block: Set whisper flow

Description

A *whisper flow* is what a customer or agent experiences when they are joined in a voice or chat conversation. For example:

- An agent and customer are joined in a **chat**. An agent whisper might display text to the agent telling them the name of the customer, for example, which queue the customer was in, or let the agent know they're talking to club member.
- An agent and customer are joined in a **call**. A customer whisper might tell the customer that the call is being recorded for training purposes, for example, or thank them for being a club member.
- An agent and customer are joined in a **chat**. Using a contact attribute, an agent whisper flow records which agent is being connected to the conversation. This attribute is then used in a disconnect flow to route the contact back to the same agent if the customer has a follow-up question after the agent disconnects.

A whisper flow has the following characteristics:

- It's a one-sided interaction: either the customer hears or sees it, or the agent does.
- It can be used to create personalized and automated interactions.
- It runs when a customer and agent are being connected.

For voice conversations, the **Set whisper flow** block overrides the default agent whisper flow (p. 305) or customer whisper flow (p. 305) by linking to a whisper flow you create.

> **Important**
> For chat conversations, you need to include a **Set whisper flow** block for default agent or customer whispers to play. For instructions, see Set the default whisper flow for a chat conversation (p. 305).

How the Set whisper flow block works

- For inbound conversations (voice or chat), the **Set whisper flow** block specifies the whisper to be played to customer or the agent when they are joined.
- For outbound voice calls, it specifies the whisper to be played to customer.
- A whisper is one direction, which means only the agent or customer hears or sees it, depending on the type of whisper you selected. For example, if a customer whisper says "This call is being recorded," the agent does not hear it.
- A whisper flow is triggered after the agent accepts the contact (either auto-accept or manual accept). The agent whisper flow runs first, before the customer is taken out of queue. After this is completed, the customer is taken out of queue and the customer whisper flow runs. Both flows run to completion before the agent and customer can talk or chat with each other.
- If an agent disconnects while the agent whisper is running, the customer remains in queue in order to be re-routed to another agent.
- If a customer disconnects while the customer whisper is running, the contact ends.
- If an agent whisper flow or customer whisper flow includes a block that chat does not support, such as Start (p. 423)/Stop (p. 425) media streaming or Set voice (p. 415), chat skips these blocks and triggers an error branch. However, it doesn't prevent the contact flow from progressing.
- Whisper flows don't appear in transcripts.
- Whispers can be a maximum of 2 minutes long. After that point, the contact or agent is disconnected.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

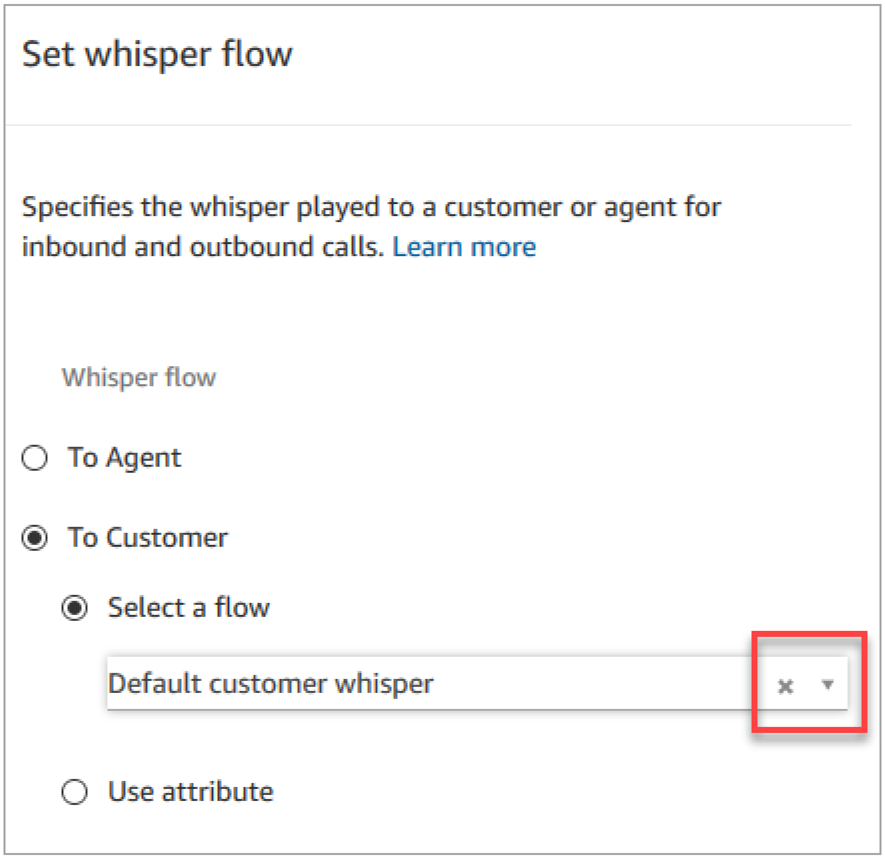
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Set whisper flow

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

Whisper flow

○ To Agent

● To Customer

● Select a flow

Default customer whisper

○ Use attribute

If you choose to **Select a flow**, you can only select from flows that are type **Agent Whisper** or **Customer Whisper**.

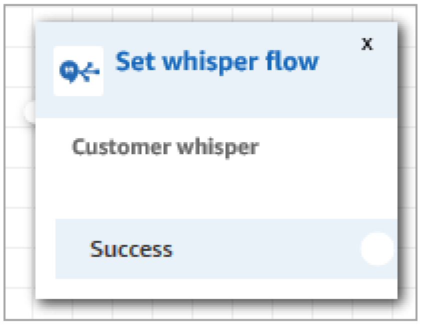
For information about using attributes, see Use Amazon Connect contact attributes (p. 515).

Configuration tips

- In a single block, you can set either a customer whisper or an agent whisper, but not both. Instead, use multiple **Set whisper flow** blocks in your contact flow.
- If you use a Play prompt (p. 393) block instead of a **Set whisper** block in an agent whisper flow or customer whisper flow, in a voice conversation the prompt is audible to both the agent and the customer. In a chat, however, only the agent or customer sees the **Play prompt** text.
- Make sure your whispers are able to complete within two minutes. Otherwise, calls will be disconnected before being established.
- If agents appear to be stuck in the "Connecting..." state before being forcefully disconnected from calls, make sure that your configured whisper flows meet the two minute maximum.

Configured block

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



Contact block: Set working queue

Description

- This block specifies the queue to be used when **Transfer to queue** is invoked.
- A queue must be specified before invoking **Transfer to queue** except when used in a customer queue flow. It's also the default queue for checking attributes, such as staffing, queue status, and hours of operation.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

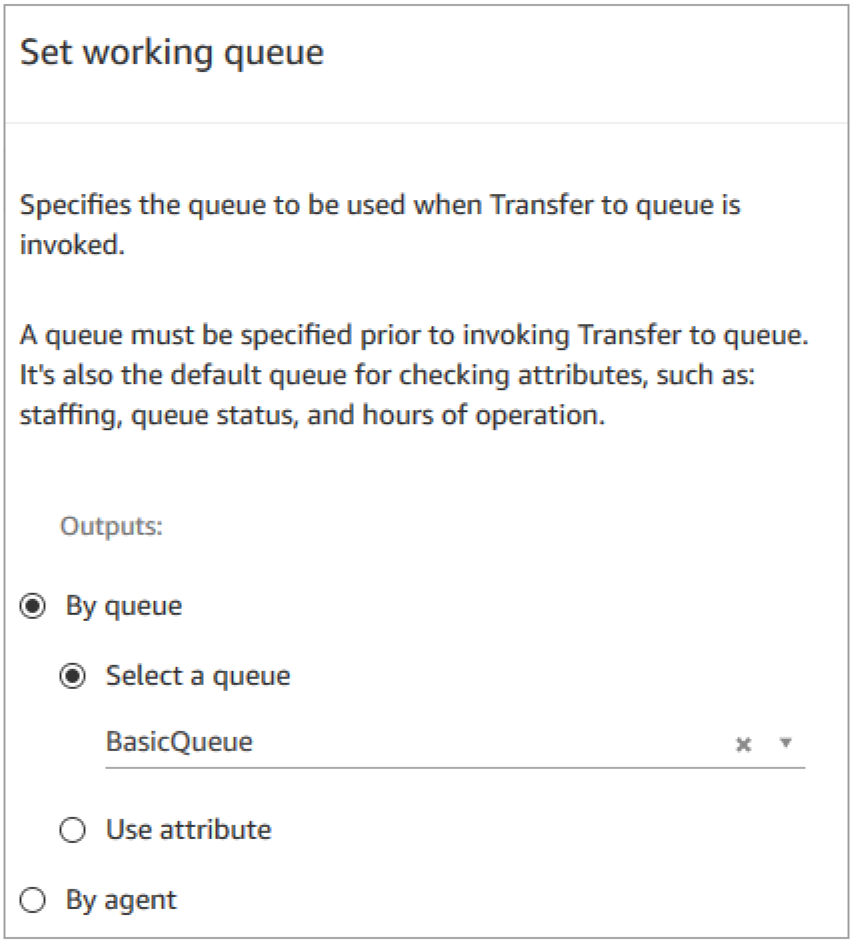
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Set working queue

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

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

Outputs:

● By queue

● Select a queue

BasicQueue

○ Use attribute

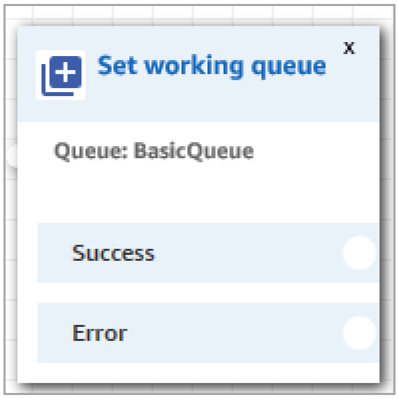
○ By agent

Note the following properties:

- **By queue > Use attribute**. To set the queue dynamically, you must specify the Amazon Resource Name (ARN) for the queue rather than the queue name. To find the ARN for a queue, open the queue in the queue editor. The ARN is included as the last part of the URL displayed in the browser address bar after /queue. For example, `.../queue/aaaaaaaa-bbbb-cccc-dddd-111111111111`.

Configured block

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



Set working queue

Queue: BasicQueue

Sample flows

See these sample flows for scenarios that use this block:

- Sample queue customer (p. 314)
- Sample queue configurations (p. 311)

Scenarios

See these topics for scenarios that use this block:

- Set up agent-to-agent transfers (p. 472)
- Transfer contacts to a specific agent (p. 477)

Contact block: Start media streaming

Description

Captures what the customer hears and says during a contact. You can then perform analysis on the audio streams to:

- Determine customer sentiment.
- Use the audio for training purposes.
- Identify and flag abusive callers.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

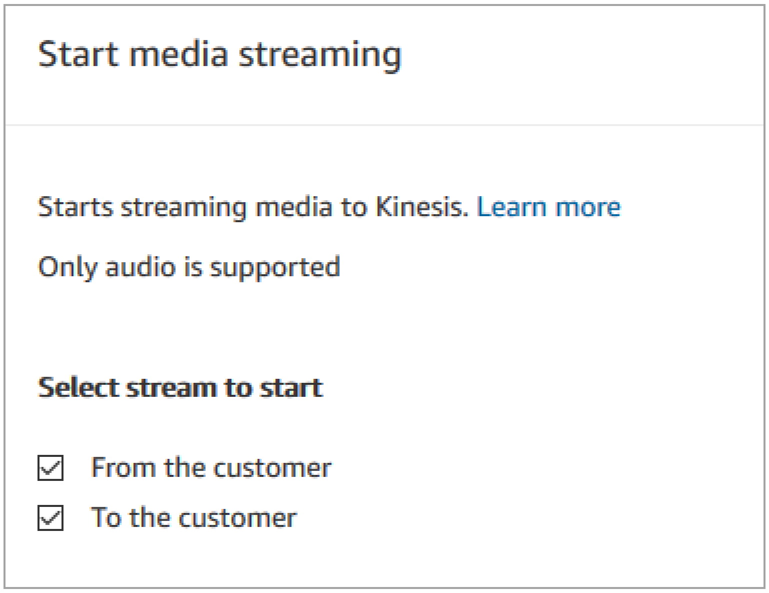
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Start media streaming

Starts streaming media to Kinesis. Learn more

Only audio is supported

Select stream to start

☑ From the customer

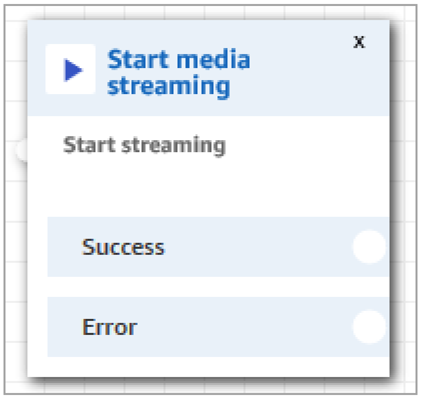
☑ To the customer

Configuration tips

- You must enable live media streaming in your instance to successfully capture customer audio. For instructions, see Capture customer audio: live media streaming (p. 775).
- When selecting the stream to start, only choose one option. Selecting both options results in an inaudible media stream.
- Customer audio is captured until a **Stop media streaming** block is invoked, even if the contact is passed to another contact flow.
- You must use a **Stop media streaming** block to stop media streaming.
- If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.

Configured block

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



Start media streaming

Start streaming

Sample flows

Example contact flow for testing live media streaming (p. 782)

Contact block: Stop media streaming

Description

- Stops capturing customer audio after it is started with a **Start media streaming** block.
- You must use a **Stop media streaming** block to stop media streaming.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties

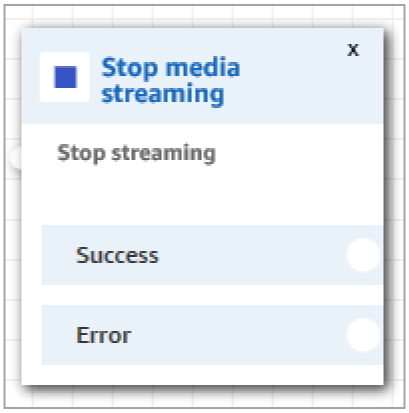
This block doesn't have any properties.

Configuration tips

- You must enable live media streaming in your instance to successfully capture customer audio. For instructions, see Capture customer audio: live media streaming (p. 775).
- Customer audio is captured until a **Stop media streaming** block is invoked, even if the contact is passed to another contact flow.
- If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.

Configured block

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



Sample flows

Example contact flow for testing live media streaming (p. 782)

Contact block: Store customer input

Description

This block is similar to **Get customer input**, but this one stores the input as a contact attribute (in the Stored customer input (p. 517) system attribute) and allows you to encrypt it. This way, you can encrypt sensitive input such as credit card numbers. This block:

- Plays an interruptible prompt to get a response from the customer. For example, "Please enter your credit card number" or "Please enter the phone number we should use to call you back."
- Plays an interruptible audio prompt or play text-to-speech for a customer to respond to.
- Stores numerical input as in the Stored customer input (p. 517) system attribute.
- Allows you to specify a custom terminating keypress.
- If during a call the customer doesn't enter any input, the contact is routed down the **Success branch** branch with a value of Timeout. Add a **Check contact attributes** block to check for timeouts.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

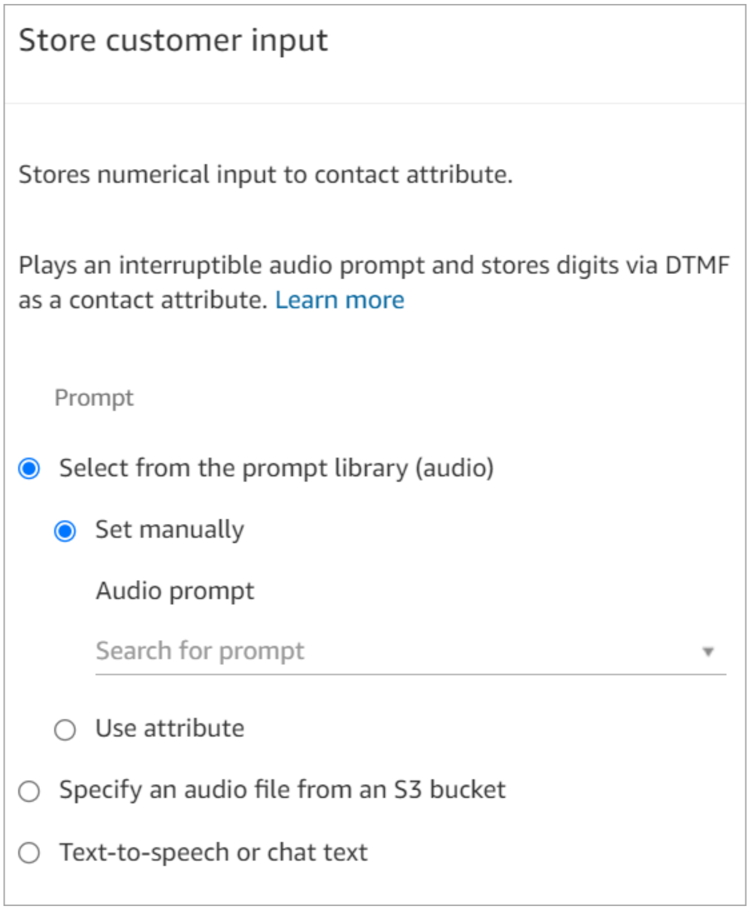
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Store customer input

Stores numerical input to contact attribute.

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

Prompt

● Select from the prompt library (audio)

● Set manually

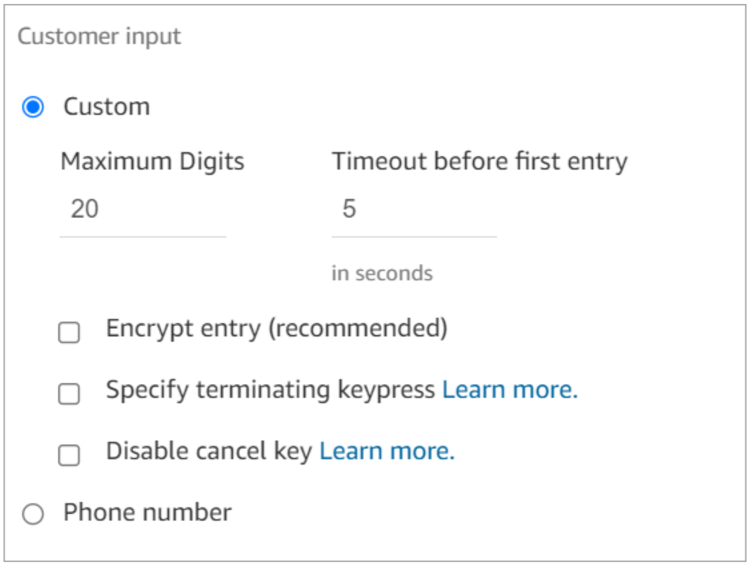
Audio prompt

Search for prompt ▾

○ Use attribute

○ Specify an audio file from an S3 bucket

○ Text-to-speech or chat text



Customer input

● Custom

Maximum Digits: 20

Timeout before first entry: 5 in seconds

□ Encrypt entry (recommended)

□ Specify terminating keypress Learn more.

□ Disable cancel key Learn more.

○ Phone number

Note the following properties:

- For information about choosing a prompt from the Amazon Connect library or an S3 bucket, see the Play prompt (p. 393) block.
- **Maximum Digits**: Define the maximum number of digits that a customer can enter.
- **Timeout before first entry**: Specify how long to wait for a customer to start entering their reply by voice. For example, you might enter 20 seconds, to give the customer time to get their credit card.

  After the contact starts entering digits, Amazon Connect waits 5 seconds for each digit, by default. You cannot change this default setting.
- **Encrypt entry**: Encrypt the customer's entry, such as their credit card information. For step-by-step instructions to get the keys that you use to input this information, see Creating a secure IVR solution with Amazon Connect.
- **Specify terminating keypress**: Define a custom terminating keypress that is used when your contacts complete their DTMF inputs. The terminating keypress can be up to five digits long, with #, * and 0-9 characters, instead of just #.

  > **Note**
  > To use a star (*) as part of the terminating keypress, you must also choose **Disable cancel key**.
- **Disable cancel key**: By default, when a customer enters * as input, it deletes all of the DTMF input that came before it. However, if you choose **Disable cancel key**, Amazon Connect treats the * as any other key.

  If you send the DMTF input to an Invoke AWS Lambda function (p. 385) block, the **Disable cancel key** property affects the input, as follows:
  - When **Disable cancel key** is selected, all the characters entered—including any *—are sent to the **Invoke Lambda function** block.
  - When **Disable cancel key** is not selected, only the * is sent to the **Invoke Lambda function** block.

  For example, let's say you chose **Disable cancel key**, and a customer entered *1#2#3*4###*, where *##* is the terminating keypress. The **Invoke Lambda function** block then receives the entire *1#2#3*4#* as input. You could program the Lambda function to ignore the character before the * character. So, the customer input would be interpreted as *1#2#4#*.
- **Phone number**: This option is useful for queued callback scenarios.

- **Local format**: If all of your customers all calling from the same country that your instance is in, choose that country from the dropdown list. Amazon Connect then auto-populates the country code for customers so that they don't have to enter it.
- **International format**: If you have customers calling from different countries, choose **International format**. Amazon Connect then requires customers to enter their country code.

Problems with DTMF input?

Let's say you have the following scenario with two contacts flows, each one capturing DTMF input from customers:

1. One contact flow uses the **Get customer input** block to request DTMF input from customers.
2. After the DTMF input is entered, it uses the **Transfer to flow** block to move the contact to the next contact flow.
3. In the next contact flow, there's a **Store customer input** block to get more DTMF input from the customer.

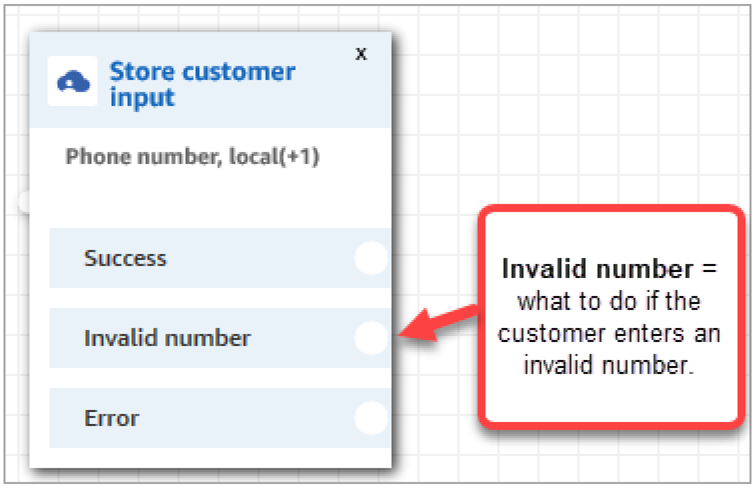
There's setup time between the first and second contact flows. This means if the customer enters DTMF input very quickly for the second flow, some of the DTMF digits might be dropped.

For example, the customer needs to press 5, then wait for a prompt from the second flow, then type 123. In this case, 123 is captured without problem. However, if they don't wait for the prompt and enter 5123 very quickly, the **Store customer input** block may capture only 23 or 3.

To guarantee the **Store customer input** block in second contact flow captures all of the digits, the customer needs to wait for the prompt to be played, and then enter their type DTMF input.

Configured block

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample secure input with agent (p. 316)
- Sample secure input with no agent (p. 317)

- Sample queue configurations (p. 311)
- Sample queued callback (p. 314)

Scenarios

Creating a secure IVR solution with Amazon Connect

Contact block: Transfer to agent (beta)

Description

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

  Note
  If the agent is already with someone else, the contact is disconnected.
  If the agent is in After Contact Work, they are automatically removed from ACW at the time of transfer.
- The **Transfer to Agent** block is a beta feature and works only for voice interactions.
- We recommend using the Set working queue (p. 421) block for agent-to-agent transfers instead of using this block. The **Set working queue** block supports omnichannel transfers such as voice and chat. For instructions, see Set up agent-to-agent transfers (p. 472).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

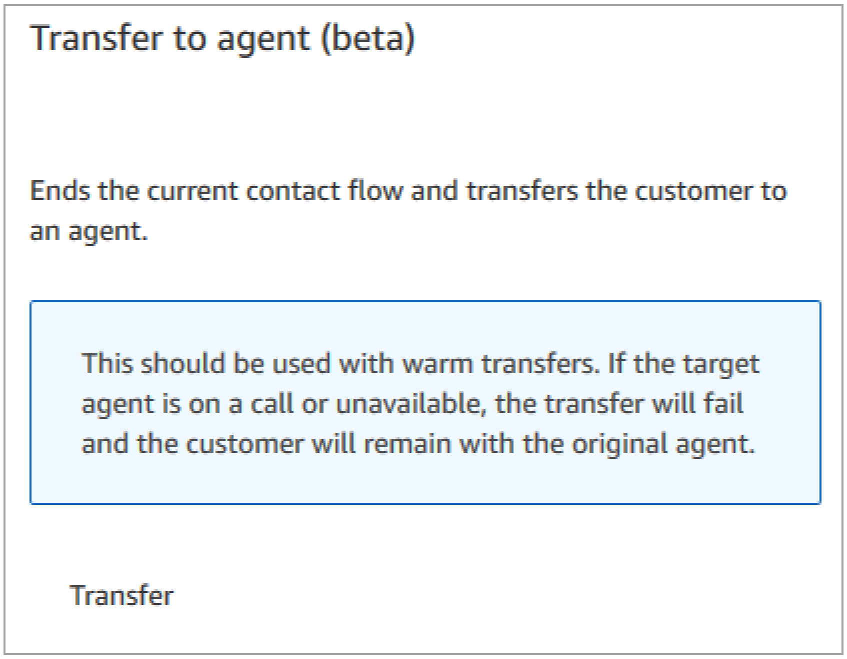
To transfer chats and tasks to agents, use the Set working queue (p. 421) block. Because Set working queue (p. 421) works for all channels, we recommend using it for voice calls too, instead of using **Transfer to agents (beta)**. For instructions, see Set up agent-to-agent transfers (p. 472).

Contact flow types

You can use this block in the following contact flow types (p. 445):

- Transfer to Agent flow
- Transfer to Queue flow

Properties



Transfer to agent (beta)

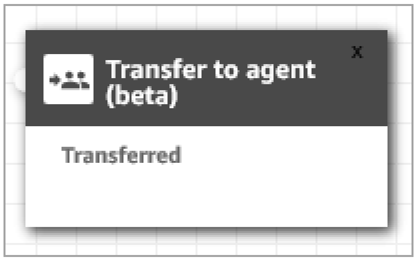
Ends the current contact flow and transfers the customer to an agent.

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

Transfer

Configured block

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



Scenarios

See these topics for scenarios that use this block:

- Set up contact transfers (p. 465)

Contact block: Transfer to flow

Description

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

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

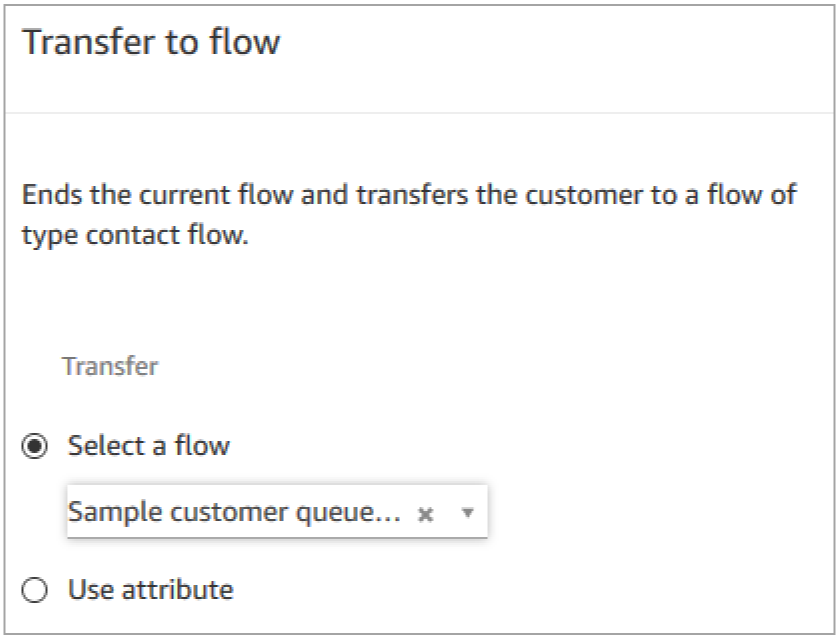
Channel	Supported?
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Transfer to flow

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

Transfer

● Select a flow

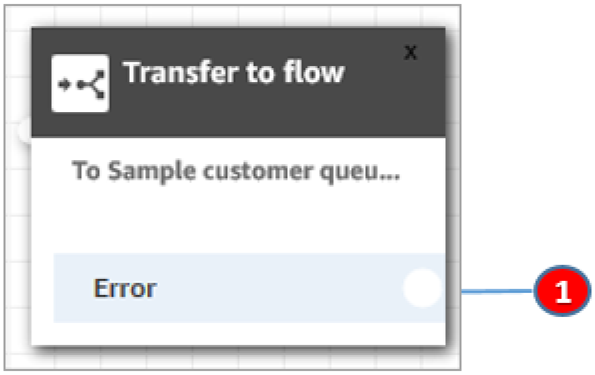
Sample customer queue...

○ Use attribute

Only published flows appear in the dropdown list.

Configured block

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



1. The contact is routed down the **Error** branch if the flow you have specified to transfer to isn't a valid flow, or it's not a valid flow type (Inbound, Transfer to Agent, or Transfer to Queue).

Sample flows

See these sample flows for scenarios that use this block:

- Sample AB test (p. 309)

Scenarios

See these topics for scenarios that use this block:

- Set up contact transfers (p. 465)

Contact block: Transfer to phone number

Description

- Transfers the customer to a phone number external to your instance.
- Amazon Connect continues to track calls after transferring to an external number. For example, it logs when a caller disconnects. This information is captured in the contact record.
- If this block is triggered during a chat conversation, the contact is routed down the **Error** branch.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

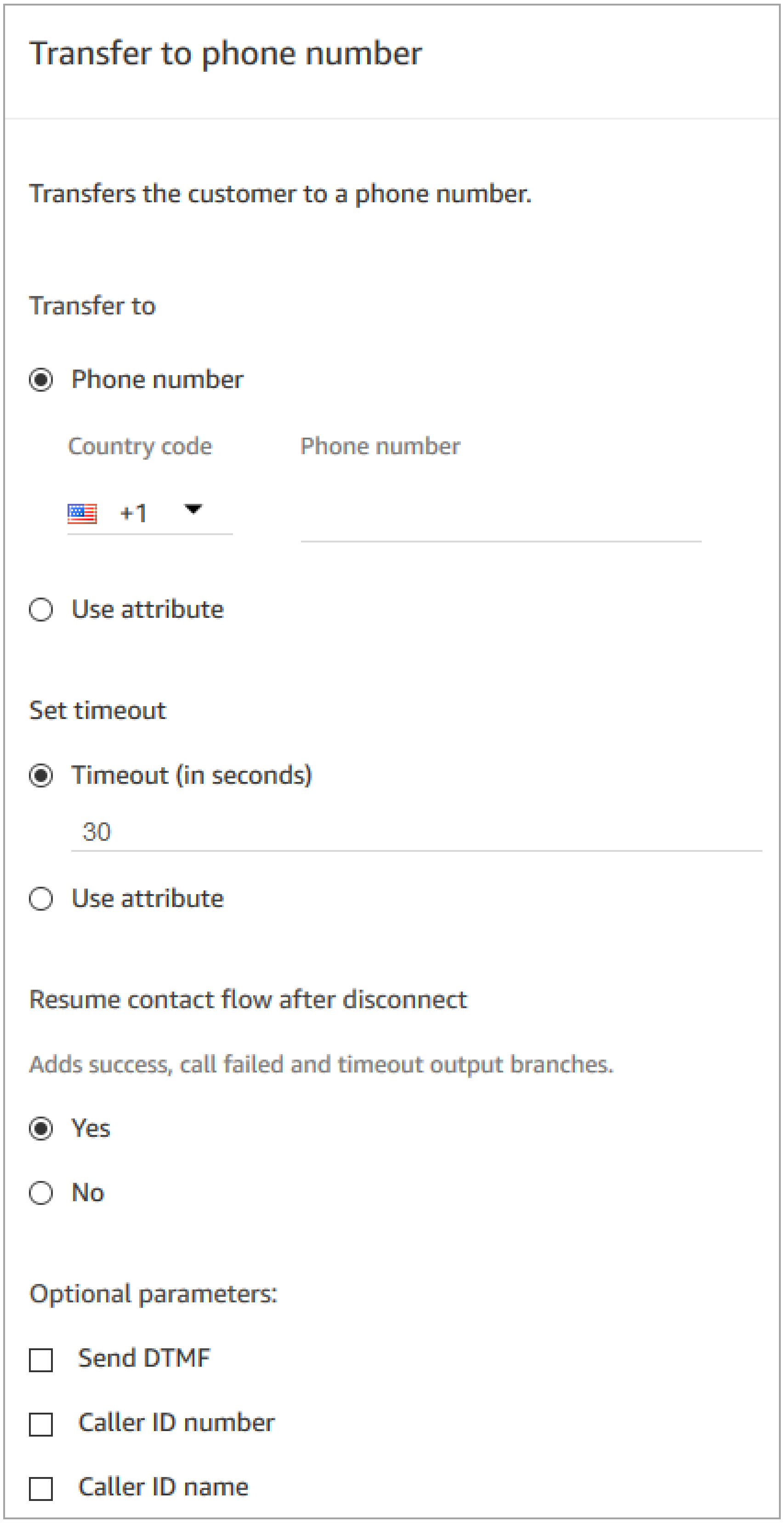
Channel	Supported?
Voice	Yes
Chat	No - Error branch
Task	No - Error branch

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Transfer to phone number

Transfers the customer to a phone number.

Transfer to

● Phone number

Country code: +1

Phone number:

○ Use attribute

Set timeout

● Timeout (in seconds)

30

○ Use attribute

Resume contact flow after disconnect

Adds success, call failed and timeout output branches.

● Yes

○ No

Optional parameters:

□ Send DTMF

□ Caller ID number

□ Caller ID name

Note the following properties:

- **Resume contact flow after disconnect**: This works only if the external party disconnects, and the customer doesn't disconnect. (If the customer disconnects, the whole call disconnects.)
- **Send DTMF**: This property is useful to bypass some of the DTMF of the external party. For example, if you know you'll need to press 1, 1, 362 to reach the external party, you can enter that here.
- **Caller ID number**: You can choose a number from your instance to appear as the caller ID. This is useful in cases where you want to use a number that's different from the one the contact flow is actually using to make the call.

  Important
  If you are using Amazon Connect outside of the United States, we recommend choosing **Caller ID number** and then selecting an Amazon Connect number. Otherwise, local regulations may cause telephony providers to block or redirect non-Amazon Connect phone numbers. This will result in service-related events, such as rejected calls, poor audio quality, delay, latency, and displaying the incorrect caller ID.
  In Australia: The caller ID must be an Amazon Connect provided DID (Direct Inward Dialing) phone number. If a toll free number or a number not provided by Amazon Connect is used in the caller ID, local telephony suppliers may reject outbound calls due to local anti-fraud requirements.
- **Caller ID name**: You can set a caller ID name, but there's no guarantee it will appear correctly to the customer. For more information, see Why your caller ID might not appear correctly to customers (p. 214).

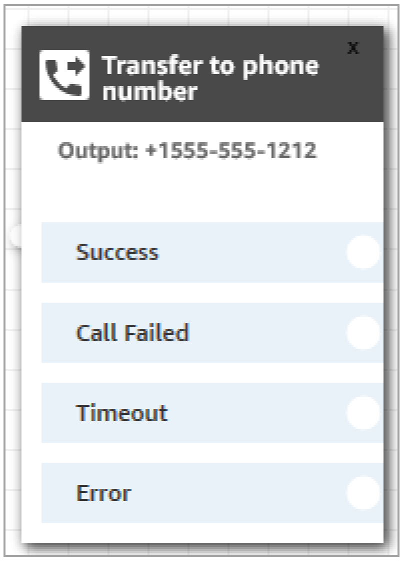
Note
When Transfer to phone number (p. 433) block is used without specifying a custom caller ID, the caller ID of the caller is passed as the caller ID. For example, if you transfer to an external number and no custom caller ID is used to specify that the call is coming from your organization, then the contact's caller ID is displayed to the external party.

Configuration tips

- Submit a service quota increase request requesting that your business be allowed to make outbound calls to the country you specified. If your business is not on the allow list for making the call, it will fail. For more information, see Countries you can call (p. 1214).
- If the country you want to select is not listed, you can submit a request to add countries you want to transfer calls to using the Amazon Connect service quotas increase form.
- You can choose to end the contact flow when the call is transferred, or choose to **Resume contact flow after disconnect**, which returns the caller to your instance and resumes the contact flow after the transferred call ends.

Configured block

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



Output: +1555-555-1212

Scenarios

See these topics for scenarios that use this block:

- Set up contact transfers (p. 465)
- Set up outbound caller ID (p. 212)

Contact block: Transfer to queue

Description

- In most types of contact flows, this block ends the current contact flow and places the customer in a queue.
- When used in a Customer Queue flow, however, this block transfers a contact already in a queue to another queue.
- When used in a callback scenario, Amazon Connect calls the agent first. After the agent accepts the call in the CCP, Amazon Connect calls the customer.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

Channel	**Supported?**
Voice	Yes
Chat	Yes
Task	Yes

Contact flow types

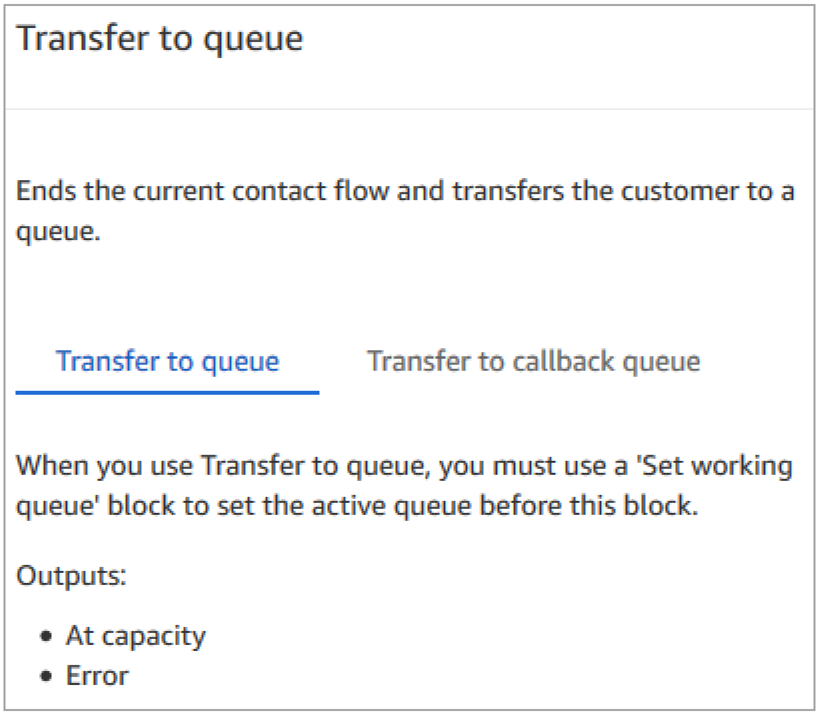
You can use this block in the following contact flow types (p. 445):

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

Properties

This block has two tabs on its properties page.

Tab 1: Transfer to queue



Transfer to queue

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

When you use Transfer to queue, you must use a 'Set working queue' block to set the active queue before this block.

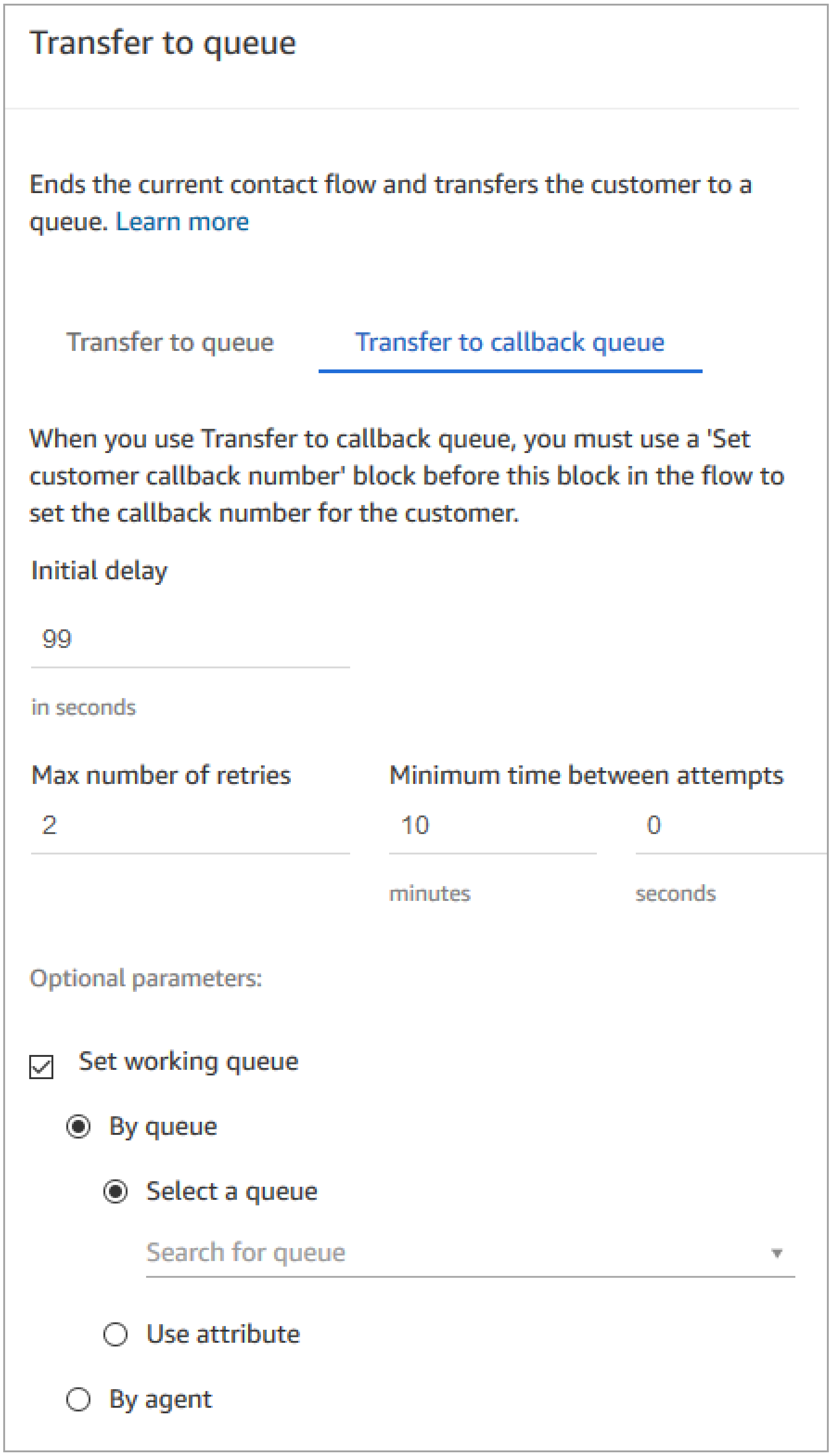
Outputs:

- At capacity
- Error

When the **Transfer to queue** block runs, it checks the queue capacity to determine whether the queue is at capacity (full). This check for queue capacity compares the current number of contacts in the queue to the Maximum contacts in queue (p. 224) limit, if one is set for the queue.

If no limit is set, the queue is limited to the number of concurrent contacts set in the service quota for the instance.

Tab 2: Transfer to callback queue



Transfer to queue

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

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

Initial delay: 99 in seconds

Max number of retries: 2

Minimum time between attempts: 10 minutes 0 seconds

Optional parameters:

☑ Set working queue

● By queue

● Select a queue

Search for queue ▾

○ Use attribute

○ By agent

The following properties are available under the **Transfer to callback queue** tab:

- **Initial delay**: Specify how much time has to pass between a callback contact being initiated in the contact flow, and the customer is put in queue for the next available agent.
- **Maximum number of retries**: If this were set to 1, then Amazon Connect would try to callback the customer at most two times: the initial callback, and 1 retry.

  Tip
  We strongly recommend that you double-check the number entered in **Maximum number of retries**. If you accidentally enter a high number, such as 20, it's going to result in unnecessary work for the agent and too many calls for the customer.
- **Minimum time between attempts**: If the customer doesn't answer the phone, this is how long to wait until trying again.
- **Set working queue**: You can transfer a callback queue to a different queue. This is useful if you set up a special queue just for callbacks. You can then view that queue to see how many customers are waiting for callbacks.

  Tip
  If you want to specify the **Set working queue** property, you need to add a **Set customer callback number** block before this block.

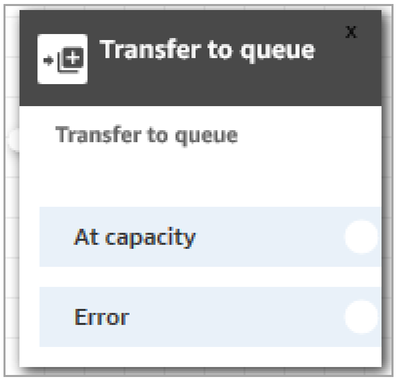
  If you don't set a working queue, Amazon Connect uses the queue that was set previously in the flow.

Configuration tips

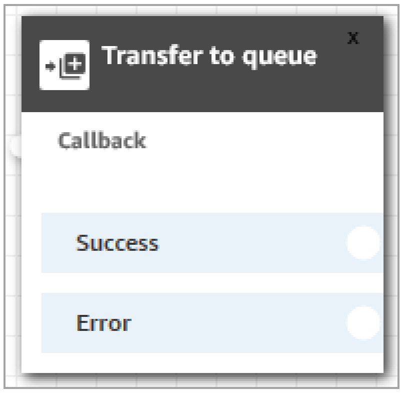
- When you use this block in a Customer Queue flow, you must add a **Loop prompts** block before this one.
- To use this block in most contact flows, you must add a **Set working queue** block first. The one exception to this rule is when this block is used in a Customer Queue flow.
- When you use text, either for text-to-speech or chat, you can use a maximum of 3,000 billed characters (6,000 total characters).
- Amazon Lex bots support both spoken utterances and keypad input when used in a contact flow.
- You can prompt contacts to end their input with a pound key # and to cancel it using the star key *.

Configured block

When this block is configured to **transfer to queue**, it looks similar to the following image. If a contact is routed down the **At capacity** branch, it remains in the current working queue.



When this block is configured to **transfer to callback queue**, it looks similar to the following image. If a contact is routed down the **Success** branch, it's transferred to the specified queue.



Scenarios

See these topics for scenarios that use this block:

- Manage contacts in a queue (p. 476)
- Set up queued callback (p. 481)
- About queued callbacks in metrics (p. 1002)

Sample flows

See these sample flows for scenarios that use this block:

- Sample queue configurations (p. 311)
- Sample customer queue priority (p. 309)
- Sample queued callback (p. 314)

Contact block: Wait

Description

This block pauses the contact flow for the specified wait time.

For example, if a contact stops responding to a chat, the block pauses the contact flow for the specified wait time, then branches accordingly, such as to disconnect.

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

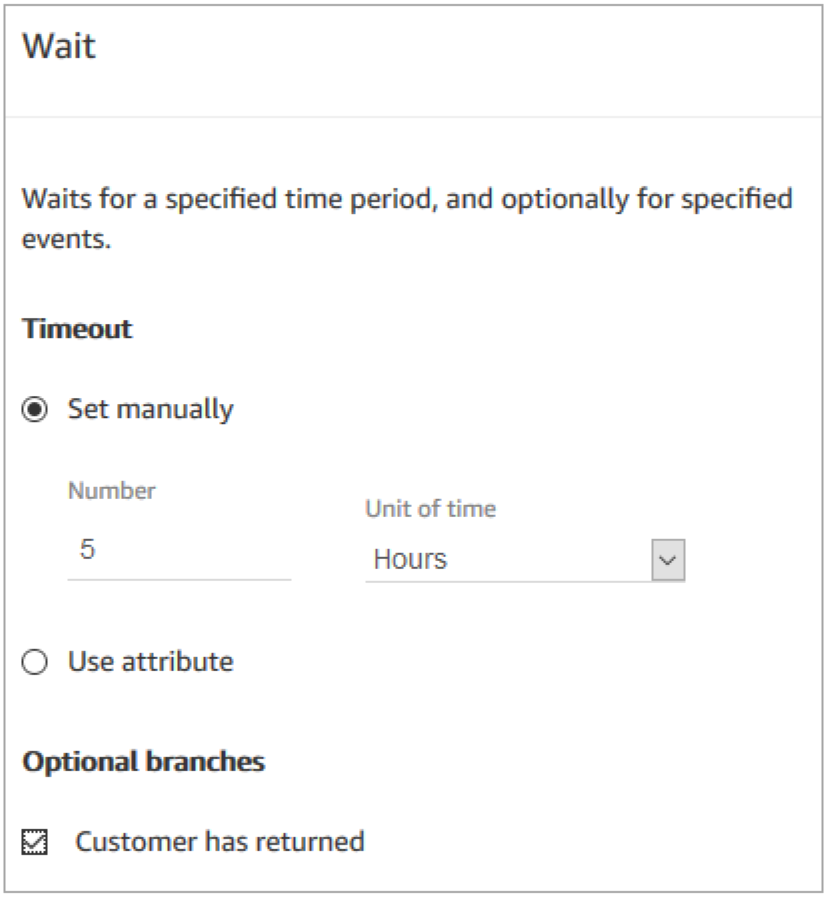
Channel	Supported?
Voice	No - Error branch
Chat	Yes
Task	Yes

Contact flow types

You can use this block in the following contact flow types (p. 445):

- Inbound contact flow
- Customer Queue flow

Properties



Wait

Waits for a specified time period, and optionally for specified events.

Timeout

● Set manually

Number: 5

Unit of time: Hours

○ Use attribute

Optional branches

☑ Customer has returned

It has two properties:

- **Timeout**: Run this branch if the customer hasn't sent a message after a specified amount of time. Maximum is 7 days.
- **Customer return**: Run this branch when the customer returns and sends a message. With this branch you can route the customer to the previous (same) agent, previous (same) queue, or override and set a new working queue or agent.

Configuration tips

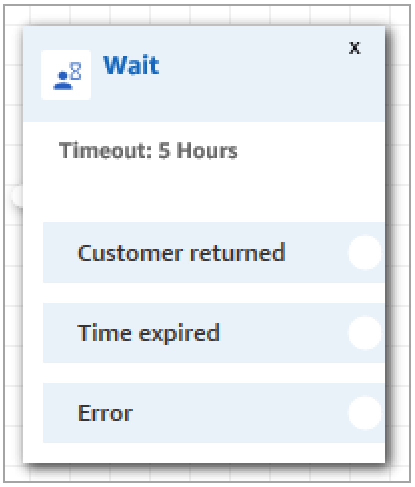
You can add multiple **Wait** blocks to your contact flows. For example:

- If the customer comes back in 5 minutes, connect them to the same agent. This is because that agent has all of the context.
- If the customer doesn't come back after 5 minutes, send a text saying "We missed you."

- If the customer comes back in 12 hours, connect to a contact flow that puts them in a priority queue. However, it doesn't route them to the same agent.

Configured block

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



Sample flows

See these sample flows for scenarios that use this block:

- Sample disconnect flow (p. 310)

Scenarios

See these topics for scenarios that use this block:

- Example chat scenario (p. 13)

Contact block: Wisdom

Description

- Associates a Wisdom domain to a contact to enable real-time recommendations.
- For more information about enabling Wisdom, see Deliver information to agents using Amazon Connect Wisdom (p. 881).

Supported channels

The following table lists how this block routes a contact who is using the specified channel.

> **Note**
> Nothing happens if a chat or task is sent to this block, however, **you will be charged**. To prevent this, add a Check contact attributes (p. 329) block before this one and route chats and tasks accordingly. For instructions, see Route based on contact's channel (p. 536).

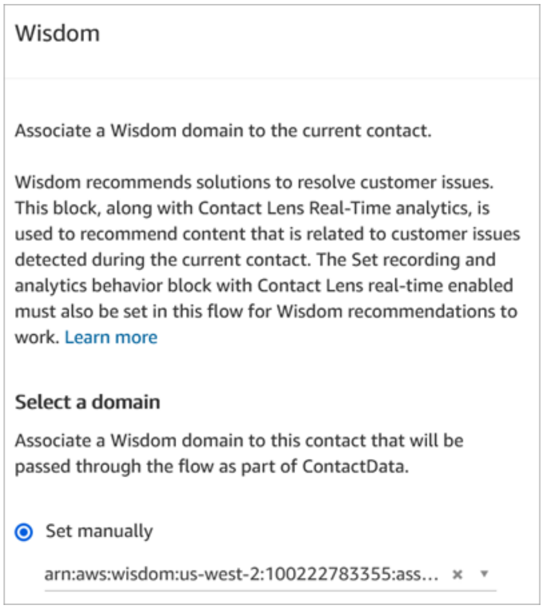
Channel	Supported?
Voice	Yes
Chat	No
Task	No

Contact flow types

You can use this block in the following contact flow types (p. 445):

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

Properties



Wisdom

Associate a Wisdom domain to the current contact.

Wisdom recommends solutions to resolve customer issues. This block, along with Contact Lens Real-Time analytics, is used to recommend content that is related to customer issues detected during the current contact. The Set recording and analytics behavior block with Contact Lens real-time enabled must also be set in this flow for Wisdom recommendations to work. Learn more

Select a domain

Associate a Wisdom domain to this contact that will be passed through the flow as part of ContactData.

● Set manually

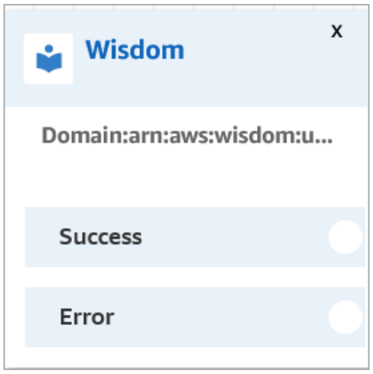
arn:aws:wisdom:us-west-2:100222783355:ass... × ▾

Configuration tips

- Amazon Connect Wisdom, along with Contact Lens Real-Time analytics, is used to recommend content that is related to customer issues detected during the current contact. The Set recording and analytics behavior (p. 408) block with Contact Lens real-time enabled must also be set in this flow for Wisdom recommendations to work. It doesn't matter where in the flow you add Set recording and analytics behavior (p. 408).

Configured block

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



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. 317).

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. After you start creating contact flows, we strongly recommend against renaming them.

Choose a contact flow type

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

Important

- When you create a contact flow, you need to choose the right type for your scenario. Otherwise, the blocks you need may not be available.
- You can't import flows of different types. This means if you start with one type and need to switch to another to get the right blocks, you have to start over.

The following contact flow types are available.

Type	When to use
Inbound contact flow	This is the generic contact flow type that's created when you choose the **Create contact flow** button, and don't select a type using the drop-down arrow. It creates an inbound contact flow. This contact flow works with voice, chat, and tasks.
Customer queue flow	Use to manage what the customer experiences while in queue, before being joined to an agent.

Type	When to use
	Customer queue flows are interruptible and can include actions such as an audio clip apologizing for a delay and offering an option to receive a callback, leveraging the **Transfer to queue** block. This contact flow works with voice, chat, and tasks.
Customer hold flow	Use to manage what the customer experiences while the customer is on hold. With this flow, one or more audio prompts can be played to a customer using the **Loop prompts** block while waiting on hold. This contact flow works with voice.
Customer whisper flow	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. This contact flow works with voice and chat.
Outbound whisper flow	Use to manage what the customer experiences as part of an outbound call before being connected with an agent. In this flow, the customer whisper is played to completion, then the two are joined. For example, this flow can be used to enable call recordings for outbound calls with the **Set recording behavior** block. This contact flow works with voice and chat.
Agent hold flow	Use to manage what the agent experiences when on hold with a customer. With this flow, one or more audio prompts can be played to an agent using the **Loop prompts** block while the customer is on hold. This contact flow works with voice.
Agent whisper flow	Use to manage what the agent experiences as part of an inbound call immediately before being joined with a customer. The agent and customer whispers are played to completion, then the two are joined. This contact flow works with voice, chat, and tasks.

Type	When to use
Transfer to agent flow	Use to manage what the agent experiences when transferring to another agent. This type of flow is associated with transfer to agent quick connects, and often plays messaging, then completes the transfer using the **Transfer to agent** block. This contact flow works with voice, chat, and tasks. **Important** Do not place any sensitive information in this flow. When a cold transfer occurs, the transferring agent disconnects before transfer is completed, and this flow is run on the caller. This means information in the flow is played to the caller, not the agent.
Transfer to queue flow	Use to manage what the agent experiences when transferring to another queue. This type of flow is associated with transfer to queue quick connects, and often plays messaging, then completes the transfer using the **Transfer to queue** block. This contact flow works with voice, chat, and tasks.

Create an inbound contact flow

Use these steps to create an inbound contact flow.

1. In the navigation pane, choose **Routing**, **Contact flows**.
2. Choose **Create contact flow**. This opens the contact flow designer and creates an inbound contact flow (Type = Contact flow).
3. Type a name and a description for your contact flow.
4. Search for a contact block using the **Search** bar, or expand the relevant group to locate the block. For descriptions of the contact blocks, see Contact block definitions (p. 317).
5. Drag and drop contract blocks onto the canvas. You can add blocks in any order or sequence, as connections between elements aren't required to be strictly linear.

   Tip
   You can move blocks around the canvas so the layout aligns to your preferences. To select multiple blocks at the same time, press the **Ctrl** key on your laptop (or the **Cmd** key on a Mac), choose the blocks you want, and then use your mouse to drag them as a group within the contact flow. You can also use the **Ctrl/Cmd** key to start at one point on the canvas and drag your pointer across the canvas to select all blocks included in the frame.
6. Double-click the title of the block. In the configuration pane, configure settings for that block and then choose **Save** to close the pane.
7. Back on the canvas, click on the first (the originating) block.
8. Choose the circle for the action to perform, such as Success.
9. Drag the arrow to the connector of the group that performs the next action. For groups that support multiple branches, drag the connector to the appropriate action.

10. Repeat the steps to create a contact flow that meets your requirements.
11. Choose **Save** to save a draft of the flow. Choose **Publish** to activate the flow immediately.

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

Delete contact flows

To delete contact flows use the DeleteContactFlow API.

Currently, there's no way to delete contact flows using the Amazon Connect admin console.

Generate logs

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

For more information about using contact flow logs, see Track events as customers interact with contact flows (p. 509).

Contact initiation methods and the types of contact flows run

Every contact in your Amazon Connect contact center is initiated by one of the following methods:

- Inbound
- Outbound
- Transfer
- Callback
- API
- Queue_Transfer
- Disconnect

You can create contact flows appropriate for a given initiation method when you know which types of contact flows (p. 445) the initiation method uses.

For each initiation method, this topic explains which types of contact flows are run.

Inbound

The customer initiated a voice (phone) contact with your contact center.

- When the contact successfully connects with the phone number of your contact center, an Inbound contact flow (p. 445) is presented to caller.
- During the transition in the **Inbound contact flow**, if the customer is put in a queue, a Customer queue flow (p. 445) is played to customer.
- After the agent becomes available to handle the caller and accept the contact, a Agent whisper flow (p. 445) is played to the agent.
- After a Agent whisper flow (p. 445) completes, a Customer whisper flow (p. 445) is played to customer.

- After the both whisper flows are played successfully to the agent and the customer respectively, the caller gets connected to agent for interaction.

To summarize, for a simple inbound call, the following contact flow types are played before caller is connected to agent:

1. **Inbound contact flow**
2. **Customer queue flow**
3. **Agent whisper flow**
4. **Customer whisper flow**

Outbound

An agent initiated voice (phone) contact to an external number, by using their CCP to make the call.

- As soon as the destination party picks the call, they are presented with an Outbound whisper flow (p. 445).
- After an **Outbound whisper flow** successfully completes, the agent and the contact are connected for interaction.

To summarize, an **Outbound contact flow** type is the only one involved in an outbound call initiated from Amazon Connect.

Transfer

The contact was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new contact record being created.

Before the agent transfers the contact to another agent or queue, all the flows involved in an INBOUND contact are run.

- Agent to Agent transfer using Agent Quick Connect
  - After the agent transfers the inbound contact to another agent:
    - A Agent transfer flow (p. 445) is played to the source agent.
    - After the destination agent accepts the call, a Agent whisper flow (p. 445) is played to destination agent, and then a Customer whisper flow (p. 445) is played to source agent.
    - After all three flows are successfully run, the interaction begins between the source and destination agents.
    - During this whole process, the inbound caller is on hold and a Customer hold flow (p. 445) is played to the inbound caller during hold time.

    After the source agent is connected with destination agent, the source agent can do one of the following actions:
    - Choose **Join**. This joins all parties on the call: source agent, destination agent, and the customer are joined in a conference call.
    - Choose **Hold all**. This puts the destination agent and the customer on hold.
    - Put destination agent on hold, so only the source agent can talk to the customer.
    - Choose **End call**. The source agent leaves the call but the destination agent and the customer are directly connected and continue talking.

  To summarize for an agent to agent transfer call, the following contact flow types are run:

  1. **Agent transfer flow**

2. **Agent whisper flow** (played to the destination agent)
3. **Customer whisper flow** (played to the source agent) during whole this process
4. **Customer hold flow** played to the original caller

- Agent to Queue transfer using Queue Quick Connect
  - After the agent transfers the inbound call to another queue:
    - A Queue transfer flow (p. 445) is played to source agent.
    - After the agent from the transferred queue accepts the call, an Agent whisper flow (p. 445) is played to destination agent, and then a Customer whisper flow (p. 445) is played to source agent.
    - After these flows run, the source and destination agent interaction begins.
    - During this whole process, the inbound caller is on hold. A Customer hold flow (p. 445) is played to the inbound caller during the hold time.

    After the source agent is connected with destination agent, the source agent can do one of the following:

    - Choose **Join**. This joins all parties on the call: source agent, destination agent, and the customer are joined in a conference call.
    - Choose **Hold all**. This puts destination agent and the customer on hold.
    - Put destination agent on hold, so only the source agent can talk to the customer.
    - Choose **End call**. The source agent leaves the call but the destination agent and the customer are directly connected and continue talking.

  To summarize for agent to queue transfer call, the following contact flows are played:

  1. **Queue transfer flow**
  2. **Agent whisper flow** (played to the destination agent)
  3. **Customer whisper flow** (played to the source agent) during whole this process
  4. **Customer hold flow** played to the original caller

Callback

The customer is contacted as part of a callback flow.

- As soon as agent accepts the callback contact, an Agent whisper flow (p. 445) is played to the agent.
- After the customer accepts the callback call, an Outbound whisper flow (p. 445) is played to customer.
- After these two flows are played, the agent and customer are connected and can interact.

To summarize, for callback contacts, the follwoing contact flow types are played:

- **Agent whisper flow**
- **Outbound whisper flow**

API

The contact was initiated with Amazon Connect by API. This could be:

1. An outbound contact you created and queued to an agent using the StartOutboundVoiceContact API.
2. A live chat that was initiated by the customer with your contact center where you called the StartChatConnect API.
3. A task that was initiated by calling the StartTaskConnect API.

Following is an example of an API initiated contact method:

- After the outbound contact is successfully initiated using the StartOutboundVoiceContact API, an Inbound contact flow (p. 445) provided in the API request is played to the customer.
- Depending on the configuration of the Inbound contact flow (p. 445), additional contact flows are played. For example, an Inbound contact flow (p. 445) transfers a customer to an agent for conversation. In this case, a Customer queue flow (p. 445) is played to customer while they waiting in queue for an agent.
- When the available agent accepts the call, an Agent whisper flow (p. 445) is played to agent.
- A Customer whisper flow (p. 445) is played to customer.
- After both whisper flows are playedd successfully to the agent and customer respectively, the caller is connected to agent for interaction.

To summarize API initiation methods, the following contact flows are played before the customer is connected to agent:

- **Inbound contact flow**
- **Customer queue flow**
- **Agent whisper flow**
- **Customer whisper flow**

Queue_Transfer

While the customer was in one queue (listening to a Customer queue flow (p. 445)), they were transferred into another queue using a contact flow block.

- The customer who is waiting in the queue for an agent is presented only with a Customer queue flow (p. 445). No additional flows are involved.

Disconnect

When a Set disconnect flow (p. 403) block runs, it specifies which contact flow to run after a disconnect event during a contact.

- You can specify only an Inbound contact flow (p. 445) in this block. Since it occurs after the disconnect event, no additional flow is presented to customer.

Override the default contact flows

For all of the initiation methods discussed in this topic, if you don't specify contact flows for **Agent whisper flow**, **Customer whisper flow**, **Customer queue flow**, or **Outbound whisper flow**, then the default contact flow of that type runs instead. For a list of default contact flows, see Default contact flows (p. 297).

To override the defaults and use your own contact flows, use the following blocks:

- Set customer queue flow (p. 402)
- Set hold flow (p. 405)
- Set whisper flow (p. 418)

For more information, see Default contact flows (p. 297).

Copy and paste contact flows

You can select, cut, copy, and paste a complete flow or multiple blocks within or across flows. The following information is copied:

- All configured settings in the selected contact blocks.
- The layout arrangements.
- The connections.

Windows: CTRL+C to copy, CTRL+V to paste, and CTRL+X to cut

1. To select multiple blocks at the same time, press the **Ctrl** key, and choose the blocks you want.
2. Press **Ctrl+C** to copy the blocks.
3. Press **CTRL+V** to paste the blocks.

Mac: Cmd+C to copy, Cmd+V to paste, and Cmd+X to cut

1. To select multiple blocks at the same time, press the **Cmd** key, and choose the blocks you want.
2. Press **Cmd+C** to copy the blocks.
3. Press **Cmd+V** to paste the blocks.

Tip
Amazon Connect uses the clipboard for this feature. Paste won't work if you edit the JSON in your clipboard and introduce a typo or other error, or if you have multiple items saved to your clipboard.

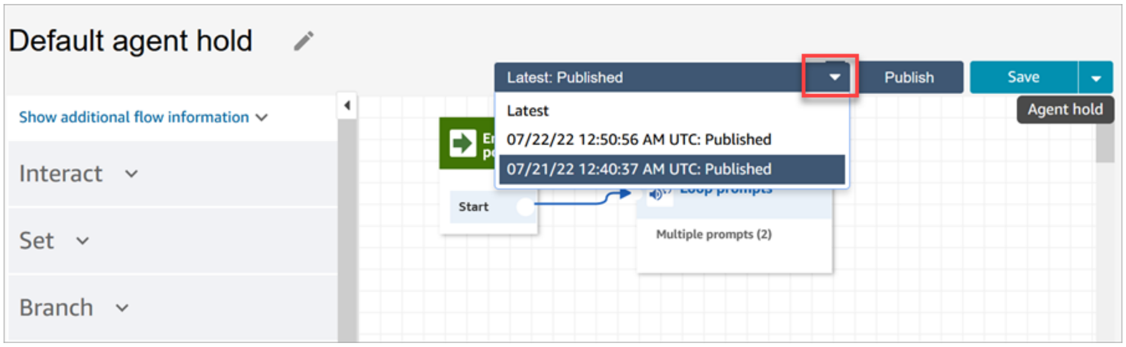
Flow version control: Roll back a contact flow

View a previous version of a flow

This procedure is especially useful if you want to research how a flow has been changed over time.

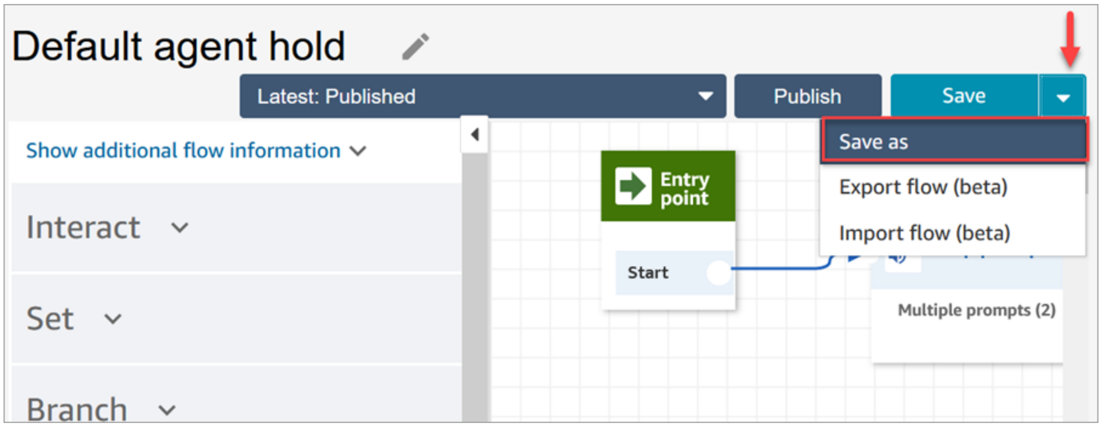
1. In the contact flow designer, open the flow you want to view.
2. Choose the **Latest: Published** dropdown to view a list of previously published versions of the flow.

   For default flows that are provided with your Amazon Connect instance, the oldest flow in the list is the original version. The date matches when your Amazon Connect instance was created. For example, in the following image, the original default flow is dated 07/21/22.



3. Choose the version of the flow to open and view it. You can view all the blocks and how they are configured.
4. Next, you can do one of the following:

   - To return to the most recently published version, choose it from the **Latest: Published** dropdown list.
   - Make changes to the previous version and choose **Save as** from the dropdown to save it with a new name. Or choose **Save** from the dropdown to assign the same name.



   - Or, choose **Publish** to return the previous version to production.

Roll back a 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.

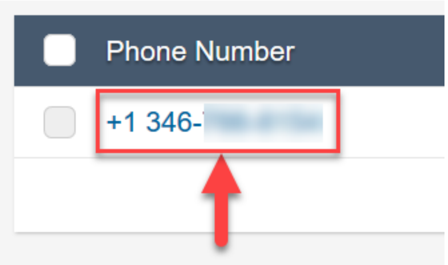
   Note
   To see a consolidated view of all changes across all flows, click the **View historical changes** link at the bottom of the Contact flows page. You can filter to a specific flow by date or user name.
3. Choose **Publish** to push that version into production.

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 at https://*instance name*.my.connect.aws/.
2. Choose **Channels**, **Phone numbers**.
3. You can search for a specific number, filter your search by queue, or select a number from the list provided (if applicable).
4. Click on the number to edit it.



□ Phone Number

□ +1 346-[redacted]

5. Expand **Contact flow / IVR**, and select the contact flow to associate with the phone number. Only published contact flows are listed.
6. Choose **Save**. When a contact calls the number, they are connected to that contact flow.

Contact flow modules for reusable functions

Contact flow modules are reusable sections of a contact flow. You can create them to extract repeatable logic across your flows, and create common functions. For example:

1. You can create a module that sends SMS text messages to customers.
2. You can invoke the module in contact flows that handle situations where customers want to reset their passwords, check their bank balances, or receive a one-time password.

Following are the benefits of using modules:

- Simplify managing common functionality across flows. For example, an SMS module could validate the format of phone number, confirm SMS opt-in preferences, and integrate with an SMS service, such as Amazon Pinpoint.
- Makes it more efficient to maintain flows. For example, you can quickly propagate changes across all flows that invoke a contact flow module.
- Helps separate flow designer responsibilities. For example, you can have both technical module designers and non-technical flow designers.

Where you can use modules

You can use modules in any contact flow that is type (p. 445) **Inbound contact flow**.

The following types of flows do not support modules: **Customer queue**, **Customer hold**, **Customer whisper**, **Outbound whisper**, **Agent hold**, **Agent whisper**, **Transfer to agent**, **Transfer to queue**.

Limitations

- Modules do not allow overriding flow local data of the invoking flow. This means you can't use the following with modules:
  - External attributes
  - Amazon Lex attributes
  - Customer Profiles attributes
  - Wisdom attributes
  - Queue metrics
  - Stored customer input
- Modules do not allow invoking another module.

Security profile permissions for modules

Before you can add modules to Inbound contact flows, you must have permissions in your security profile. By default, the **Admin** and **CallCenterManager** security profiles have these permissions.

Create a module

For information about the number of modules that you can create for each Amazon Connect instance, see Amazon Connect service quotas (p. 1205).

1. Log in to the Amazon Connect console with an account assigned to a security profile that has permissions to create modules.
2. In the navigation pane, choose **Routing**, **Contact flows**.
3. Choose **Modules**, **Create flow module**.
4. Add the blocks that you want to your module. When finished, choose **Publish**. This makes the module available to use in other contact flows.

Add a module to a contact flow

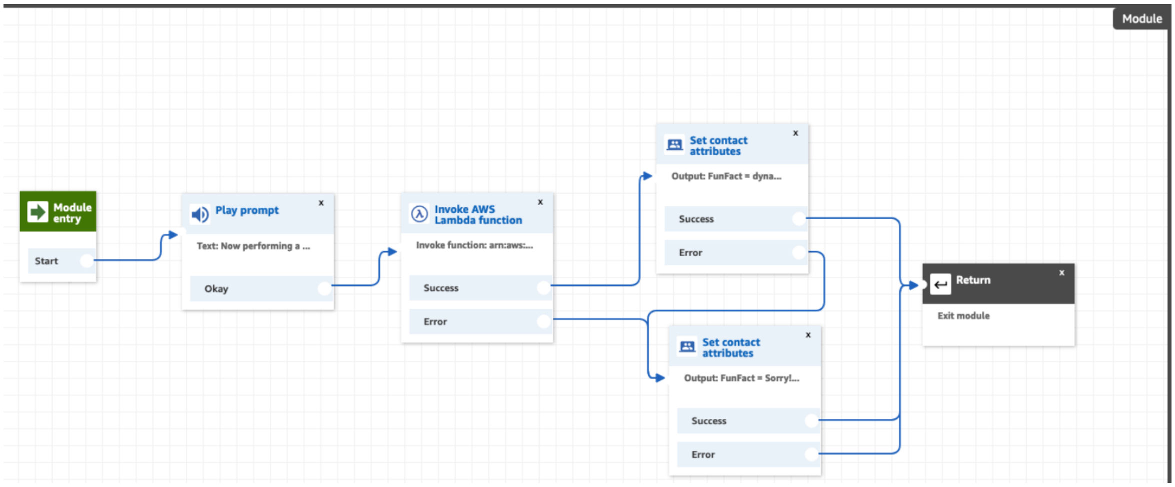
1. Log in to the Amazon Connect console with an account assigned to a security profile that has permissions to create contact flows. You don't need permissions to create modules.
2. In the navigation pane, choose **Routing**, **Contact flows**.
3. Choose **Create contact flow** or select an existing contact flow that is an **Inbound** type.
4. To add a module, go to the **Integrate** section, and choose **Invoke flow module**.
5. When you're finished creating your flow, choose **Publish**.

Example module

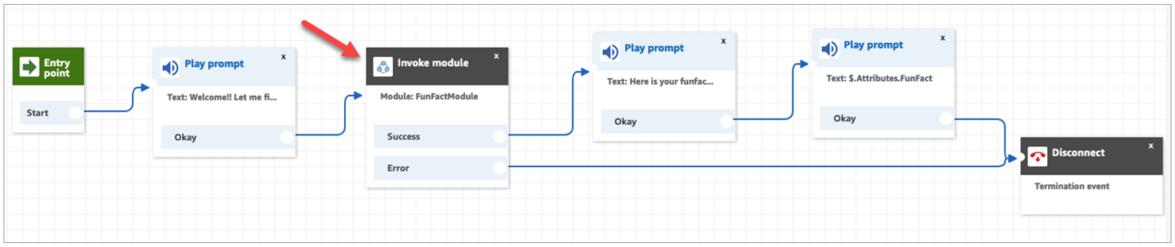
This module shows how to get a random fun fact by invoking a Lambda function. The module uses a contact attribute (`$.Attributes.FunFact`) to retrieve the fun fact. Flows that invoke this module can play a FunFact to customers, depending on their incoming contact type.

The inbound flows in your instance can invoke this common module and get the fun fact.

Following is an image of the FunFact module:



Following is an image of the FunFactSampleFlow that invokes the module:



Create prompts

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

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

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**.

Supported file types

You can upload a pre-recorded .wav file to use for your prompt, or record one in the web application.

We recommend using 8 KHz .wav files that are less than 50 MB and less than 5 minutes long. If you use higher rated audio libraries, such as 16 KHz or 16 bit files, Amazon Connect has to down sample them into 8 KHz samples because of PSTN limitations. This may result in low quality audio. For more information, see the following Wikipedia article: G.711.

Maximum length for prompts

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

Bulk upload of prompts not supported in UI, API, or CLI

Currently, bulk uploading of prompts is not supported through the Amazon Connect console or programmatically using the API or CLI.

Add text-to-speech to prompts

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

- Get customer input (p. 366)
- Loop prompts (p. 390)
- Play prompt (p. 393)
- Store customer input (p. 426)

Amazon Polly converts text-to-speech

To convert text-to-speech, Amazon Connect uses Amazon Polly, a service that converts text into lifelike speech using SSML.

Amazon Polly default voices are **free**. You are charged only for using custom voices that are associated with your account.

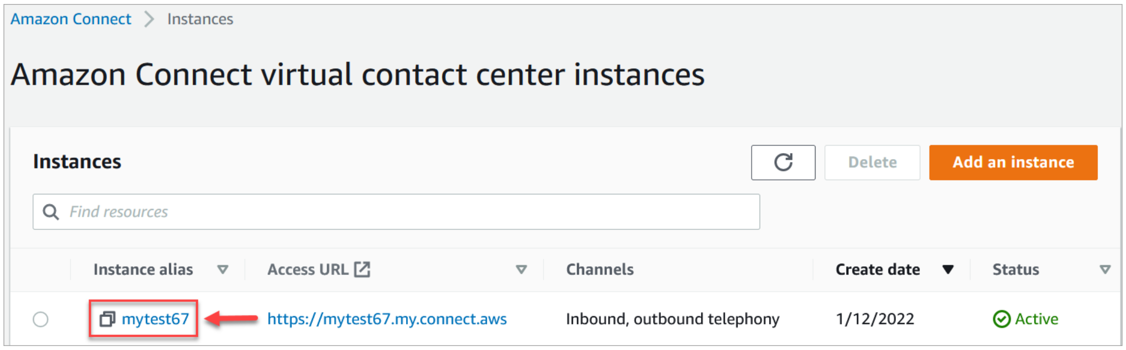
Amazon Polly best sounding voice

Amazon Polly periodically releases improved voices and speaking styles. You can choose to automatically resolve your text-to-speech to the most lifelike and natural sounding variant of a voice. For example, if your contact flows use Joanna, Amazon Connect automatically resolves to Joanna’s conversational speaking style.

> **Note**
> If no Neural version is available, Amazon Connect defaults to the standard voice.

To automatically use the best sounding voice

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. If prompted to login, enter your AWS account credentials.
3. Choose the name of the instance from the **Instance alias** column.



Amazon Connect > Instances

Amazon Connect virtual contact center instances

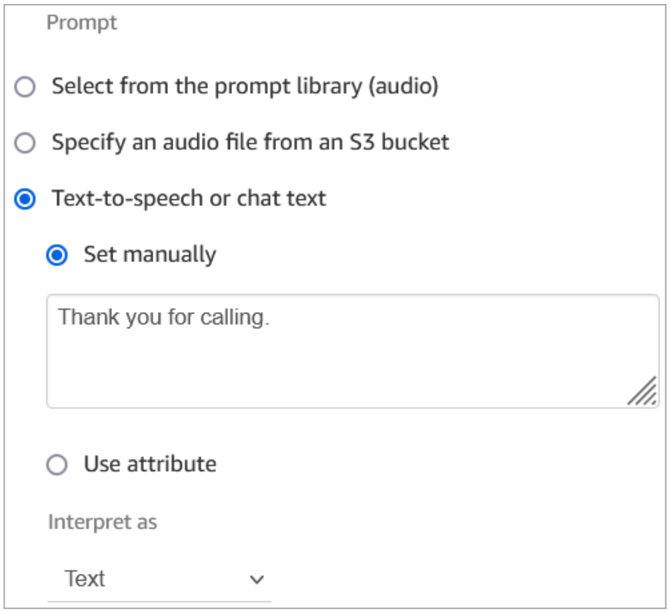
Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

4. In the navigation pane, choose **Contact flows**.
5. In the Amazon Polly section, choose **Use the best available voice**.

How to add text-to-speech

1. In a contact flow, add the block that will play the prompt. For example, add a Play prompt (p. 393) block.
2. In the **Properties**, choose **Text-to-speech**.
3. Enter plain text, as shown in the following image.



Prompt

○ Select from the prompt library (audio)

○ Specify an audio file from an S3 bucket

● Text-to-speech or chat text

● Set manually

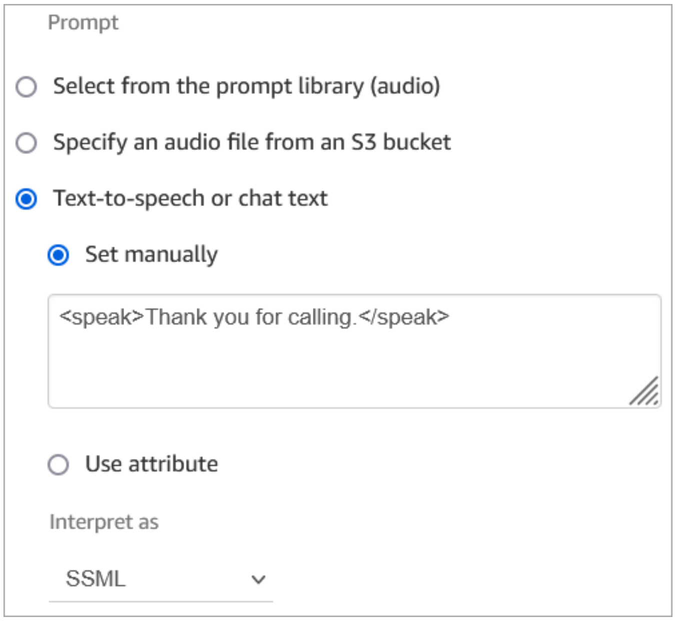
Thank you for calling.

○ Use attribute

Interpret as

Text

Or enter SSML:



Prompt

○ Select from the prompt library (audio)

○ Specify an audio file from an S3 bucket

● Text-to-speech or chat text

● Set manually

<speak>Thank you for calling.</speak>

○ Use attribute

Interpret as

SSML

SSML-enhanced input text gives you more control over how Amazon Connect generates speech from the text you provide. You can customize and control aspects of speech such as pronunciation, volume, and speed.

For a list of SSML tags you can use with Amazon Connect, see SSML tags supported by Amazon Connect (p. 464).

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

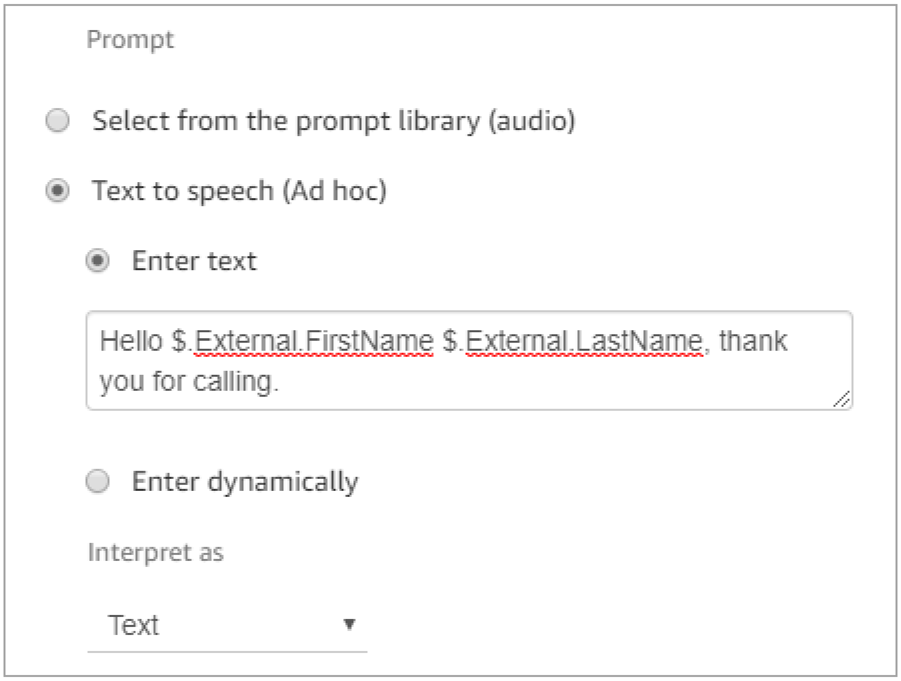
Create dynamic text strings in Play prompt block

Use a Play prompt (p. 393) 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.



Prompt

○ Select from the prompt library (audio)

● Text to speech (Ad hoc)

● Enter text

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

○ Enter dynamically

Interpret as

Text ▼

If you are referencing a user-defined attribute that was previously set as a contact attribute in the contact flow using the API, you can reference the attribute using the $.Attributes.nameOfAttribute syntax.

For example, if the contact in question has attributes "FirstName" and "LastName" set previously, reference them as follows:

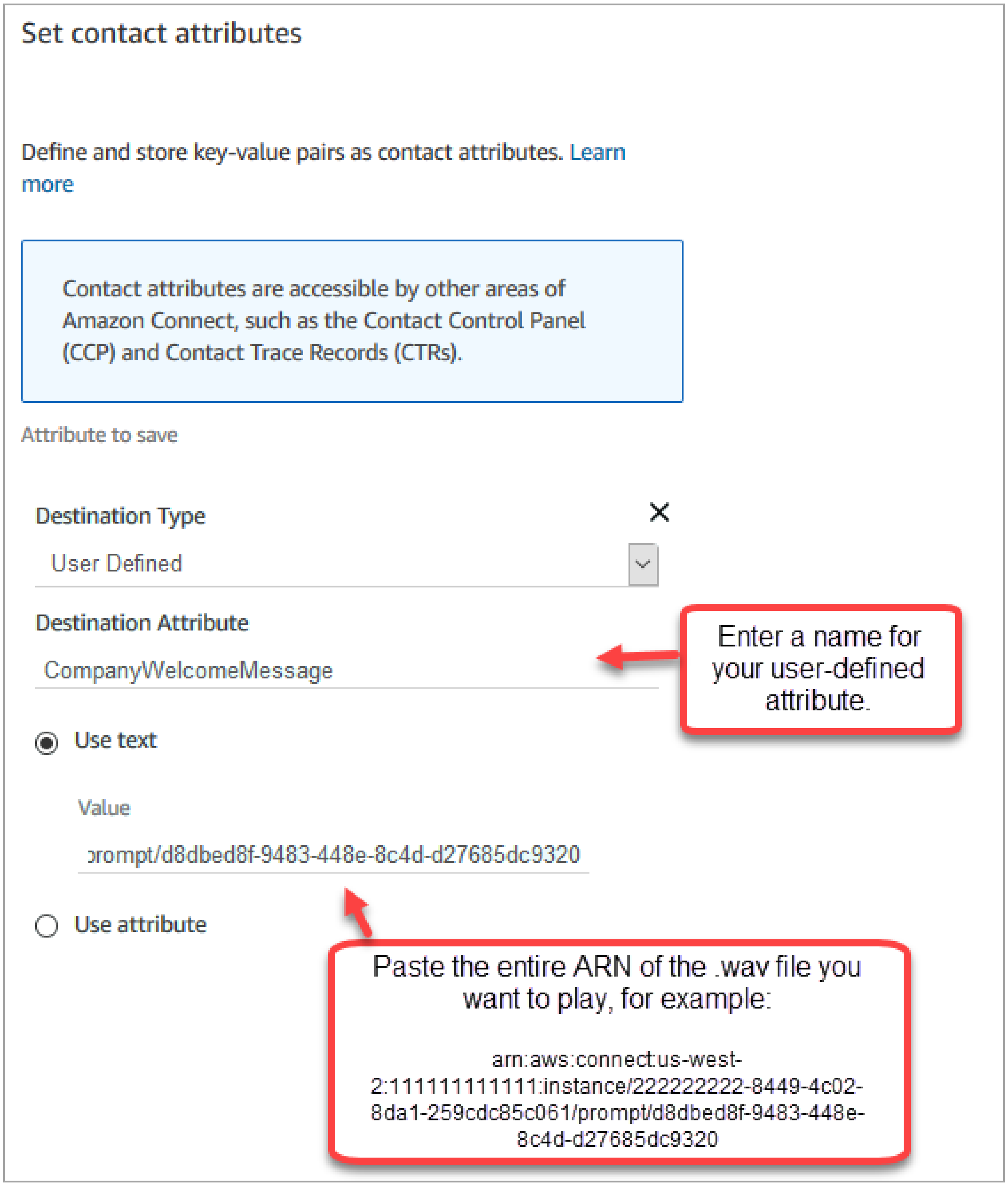
- Hello $.Attributes.FirstName $.Attributes.LastName, thank you for calling.

Dynamically select which prompts to play

You can dynamically select which prompt to play by using an attribute.

1. Add Set contact attributes (p. 399) blocks to your flow. Configure each one to play the appropriate audio prompt. For example, the first one might play the .wav file when your contact center is open. The second one might play the .wav file for when it's closed.

The following image shows how you might configure a Set contact attributes (p. 399) block. In this example, the user-defined attribute is named **CompanyWelcomeMessage**. You can name your attribute anything you want.



Set contact attributes

Define and store key-value pairs as contact attributes. Learn more

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

Attribute to save

Destination Type: User Defined

Destination Attribute: CompanyWelcomeMessage

● Use text

Value: prompt/d8dbed8f-9483-448e-8c4d-d27685dc9320

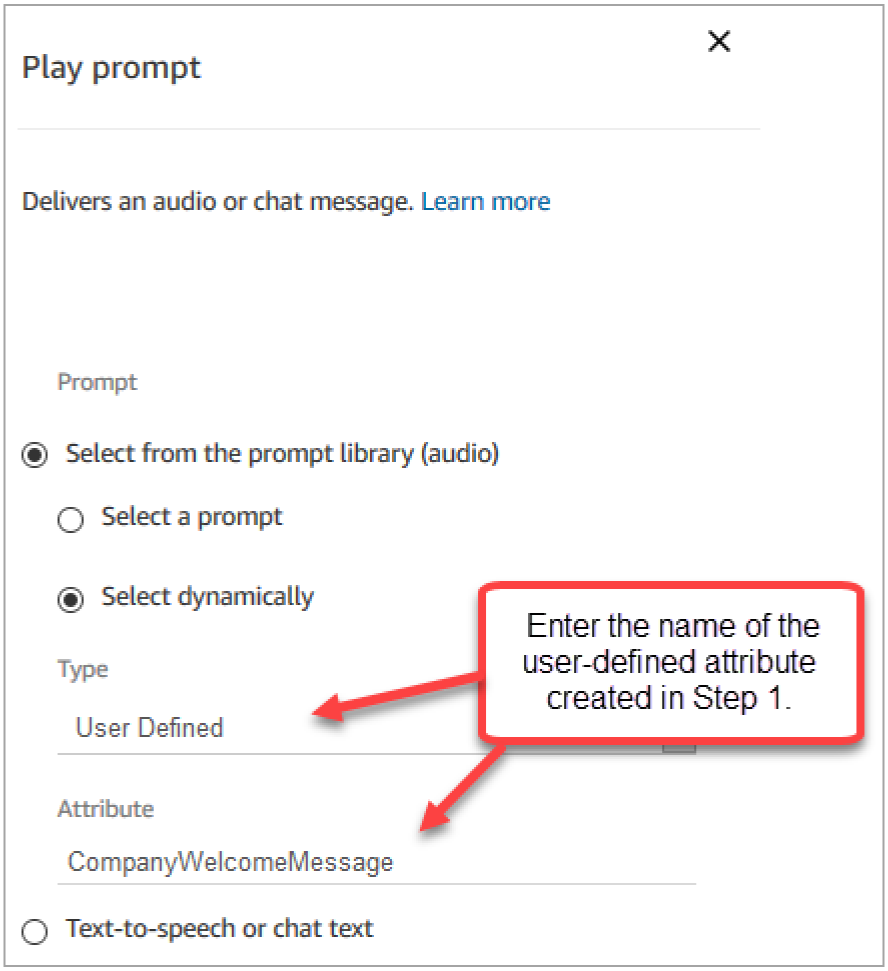
○ Use attribute

Enter a name for your user-defined attribute.

Paste the entire ARN of the .wav file you want to play, for example:

arn:aws:connect:us-west-2:111111111111:instance/222222222-8449-4c02-8da1-259cdc85c061/prompt/d8dbed8f-9483-448e-8c4d-d27685dc9320

2. In the Play prompt (p. 393) block, choose **User Defined**, and then enter the name of the attribute that you created in step 1.



Play prompt

Delivers an audio or chat message. Learn more

Prompt

● Select from the prompt library (audio)

○ Select a prompt

● Select dynamically

Type

User Defined

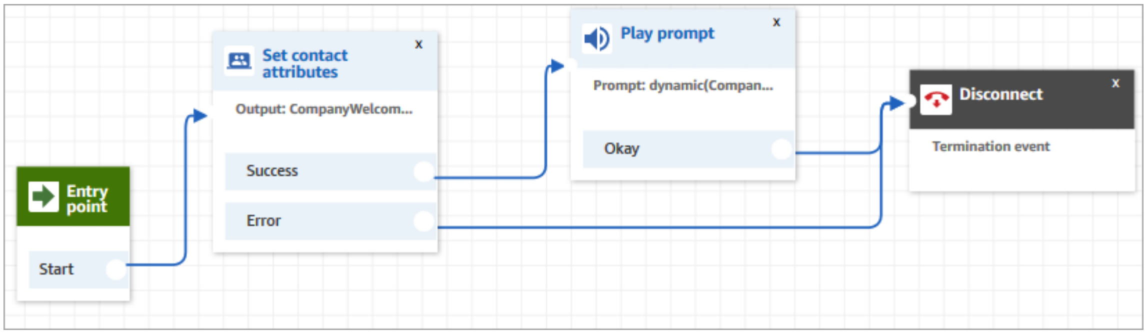
Attribute

CompanyWelcomeMessage

○ Text-to-speech or chat text

Enter the name of the user-defined attribute created in Step 1.

3. Connect the Set contact attributes (p. 399) blocks to the **Play prompt** block. The following example shows how it might look if you added one of each block to test how this works.



Set up prompts to play from an S3 bucket

When you configure prompts on the Get customer input (p. 366), Loop prompts (p. 390), Play prompt (p. 393), or Store customer input (p. 426) blocks, you can choose an S3 bucket as the source location. You can store as many voice prompts as needed in an S3 bucket and access them in real time by using contact attributes. For examples, see the Play prompt (p. 393) block.

To allow Amazon Connect to play prompts from an S3 bucket, when you set up your S3 bucket, you must update the bucket policy to grant `connect.amazonaws.com` (the Amazon Connect service principal) permission to call `s3:ListBucket` and `s3:GetObject`.

To update the S3 bucket policy:

1. Go to the Amazon S3 admin console.
2. Choose the bucket that has your prompts.
3. Choose the **Permissions** tab.
4. In the **Bucket policy** box, choose **Edit**, and paste the following policy as your template. Replace the bucket name, Region, AWS account ID, and instance ID (p. 139) with your own information, and then choose **Save changes**.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "statement1",
            "Effect": "Allow",
            "Principal": {
                "Service": "connect.amazonaws.com"
            },
            "Action": [
                "s3:ListBucket",
                "s3:GetObject"
            ],
            "Resource": [
                "arn:aws:s3:::customer-prompt-example-bucket",
                "arn:aws:s3:::customer-prompt-example-bucket/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "account-id",
                    "aws:SourceArn": "arn:aws:connect:region:account-
id:instance/instance-id"
                }
            }
        }
    ]
}
```

5. Encryption: Amazon Connect cannot download and play prompts from an S3 bucket if an AWS managed key is enabled on that S3 bucket. However, you can use a customer managed key to allow the Amazon Connect service principal ("connect.amazonaws.com") that enables your Amazon Connect instance to access the S3 bucket. See the following code snippet:

```
{
            "Sid": "Enable Amazon Connect",
            "Effect": "Allow",
            "Principal": {
                "Service": "connect.amazonaws.com"
            },
            "Action": "kms:decrypt",
            "Resource": [
             "arn:aws:kms:region:account-ID:key/key-ID"
            ]
}
```

   For information on how to find the key ID, see Finding the key ID and key ARN in the *AWS Key Management Service Developer Guide*.

After you set up your S3 bucket with the required bucket policy, configure Get customer input (p. 366), Loop prompts (p. 390), Play prompt (p. 393), or Store customer input (p. 426) to play a prompt from the bucket.

> **Tip**
> For more information about S3 buckets, including examples and limitations, see the Play prompt (p. 393) block.

Choose the voice for audio prompts

You select the text-to-speech voice and language in the Set voice (p. 415) block.

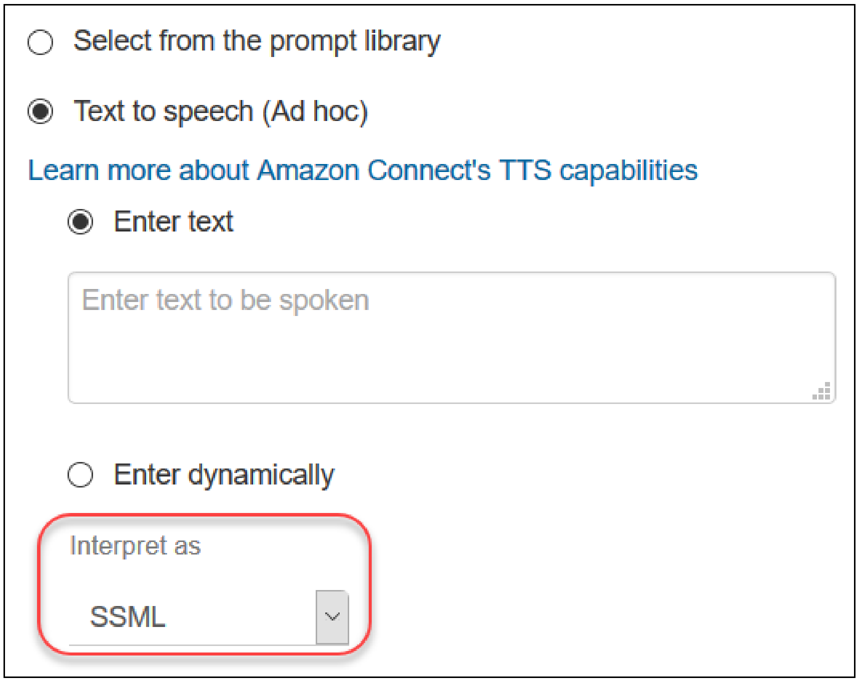
You can also use SSML in Amazon Lex bots to modify the voice used by a chat bot when interacting with your customers. For more information about using SSML in Amazon Lex bots, see Managing Messages and Managing Conversation Context in the Amazon Lex Developer Guide.

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

Use SSML tags to personalize text-to-speech

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

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



○ Select from the prompt library

● Text to speech (Ad hoc)

Learn more about Amazon Connect's TTS capabilities

● Enter text

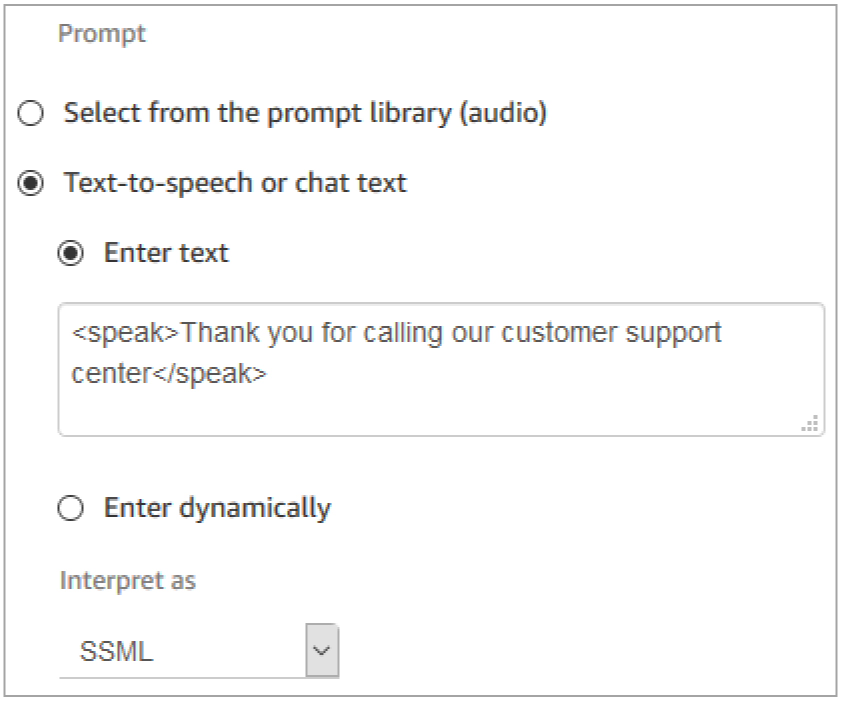
Enter text to be spoken

○ Enter dynamically

Interpret as: SSML

SSML tags aren't interpreted in chats

If you create text-to-speech text and apply SSML tags, they won't be interpreted in a chat conversation. For example, in the following image both the text **and tags** will be printed in the chat conversation.



Prompt

○ Select from the prompt library (audio)

● Text-to-speech or chat text

● Enter text

<speak>Thank you for calling our customer support center</speak>

○ Enter dynamically

Interpret as

SSML

SSML tags supported by Amazon Connect

Amazon Connect supports the following SSML tags.

> **Tip**
> If you use an unsupported tag in your input text, it's automatically ignored when it's processed.

Tag	Use to...
speak	All SSML-enhanced text must be enclosed within a pair of speak tags.
break	Add a pause to your text. The maximum duration for a pause is 10 seconds.
lang	Specify another language for specific words.
mark	Put a custom tag within the text.
p	Add a pause between paragraphs in your text.
phoneme	Make a phonetic pronunciation for specific text.
prosody	Control the volume, rate, or pitch of your selected voice.
s	Add a pause between lines or sentences in your text.
say-as	Combine with the interpret-as attribute to tell Amazon Polly how to say certain characters, words, and numbers.

Tag	Use to...
sub	Combine with the alias attribute to substitute a different word (or pronunciation) for selected text such as an acronym or abbreviation.
w	Customize the pronunciation of words by specifying the word's part of speech or alternate meaning.
amazon:effect name="whispered"	Indicate that the input text should be spoken in a whispered voice rather than as normal speech.

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

To learn more about the SSML tags, see Supported SSML Tags in the Amazon Polly Developer Guide.

Neural and Conversational Speaking Styles

For the **Joanna** and **Matthew** neural voices, in American English (en-US), you can also specify a Conversational speaking style or a Newscaster speaking style.

Set up contact transfers

Amazon Connect enables you to set up different kinds of transfers:

- Agent-to-agent transfers (p. 472): For example, if you want agents to be able to transfer calls or tasks to other agents.
- Transfers to a specific agent (p. 477): For example, if you want to route contacts to the last agent the customer interacted with, or route contacts to agents who have specific responsibilities.
- Transfers to queues (p. 466): For example, if you want to transfer the contact to a sales, support, or escalation queue. To do this, create a queue quick connect (p. 471). This works with voice, chat, and task contacts.
- Transfers to external numbers (p. 466): For example, if you want to transfer the contact to an external number, such as an on-call pager. To do this, create an external quick connect.

Overview of steps

To set up call transfers and quick connects

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

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

Create quick connects

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

Types of quick connects

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

External quick connect

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

Agent quick connect

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

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

Queue quick connect

Contacts are transferred to a queue as part of a contact flow.

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

Step 1: Create quick connects

Following are the instructions to add quick connects manually using the Amazon Connect console. To add quick connects programmatically, use the CreateQuickConnect API.

To create a quick connect

1. On the navigation menu, choose **Routing**, **Quick connects**, **Add new**.
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.
3. To add more quick connects, choose **Add new**.
4. Choose **Save**.

Step 2: Enable agents to see quick connects

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

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

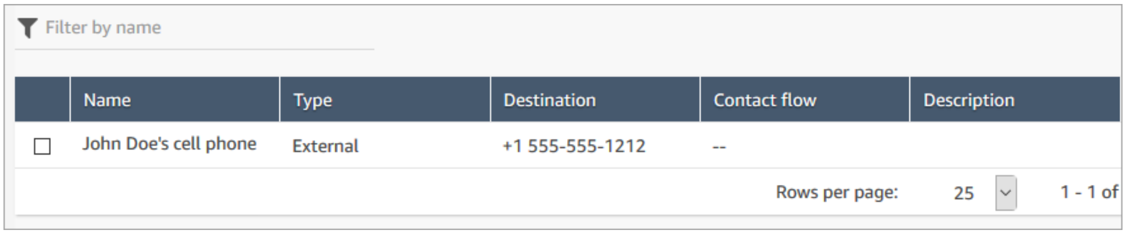
> **Tip**
> Agents see all of the quick connects for the queues associated with their routing profile.

Example: Create an external quick connect to a mobile phone

In this example, you create an external quick connect to a person's mobile phone. This might be for a supervisor, for example, so agents can call them if needed.

Create a quick connect for a person's mobile phone number

1. On the navigation menu, choose **Routing**, **Quick connects**, **Add new**.
2. Enter a name for the quick connect, for example, **John Doe's cell phone**.
3. For **Type**, select **External**.
4. For **Destination**, enter the mobile phone number, starting with the country code. In the US, the country code is 1, as shown in the following image.

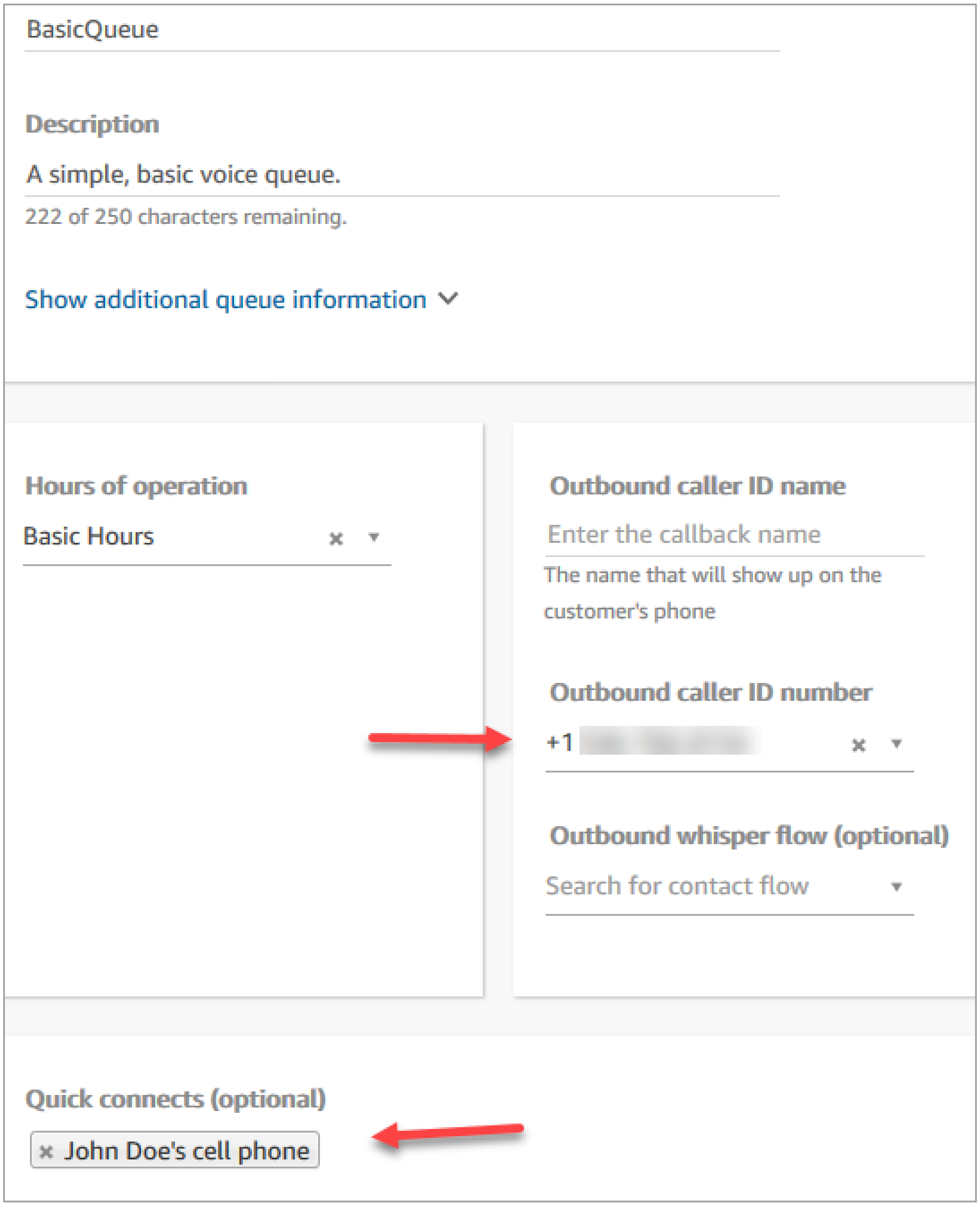


	Name	Type	Destination	Contact flow	Description
□	John Doe's cell phone	External	+1 555-555-1212	--	

5. Choose **Save**.

Add the quick connect to a queue. Agents working this queue will see the quick connect in their CCP.

1. Go to **Routing**, **Queues**, and choose the queue you want to edit.
2. On the **Edit queue** page, in **Outbound caller ID number**, choose a number claimed for your contact center. This is required to make outbound calls.
3. At the bottom of the page, in the **Quick connect** box, search for the quick connect you created, for example, **John Doe's cell phone**.
4. Select the quick connect and then choose **Save**.



BasicQueue

Description

A simple, basic voice queue.

222 of 250 characters remaining.

Hours of operation

Basic Hours

Outbound caller ID name

Enter the callback name

The name that will show up on the customer's phone

Outbound caller ID number

+1 [redacted]

Outbound whisper flow (optional)

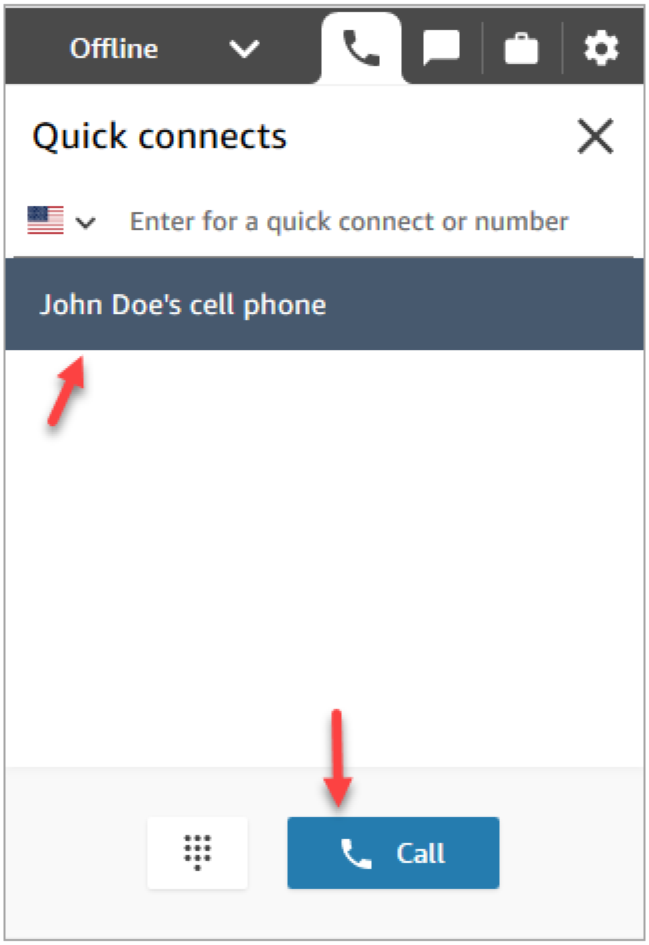
Search for contact flow

Quick connects (optional)

John Doe's cell phone

Test the quick connect

1. Open the Contact Control Panel.
2. Choose **Quick connects**.
3. Select the quick connect you created, and then choose **Call**.

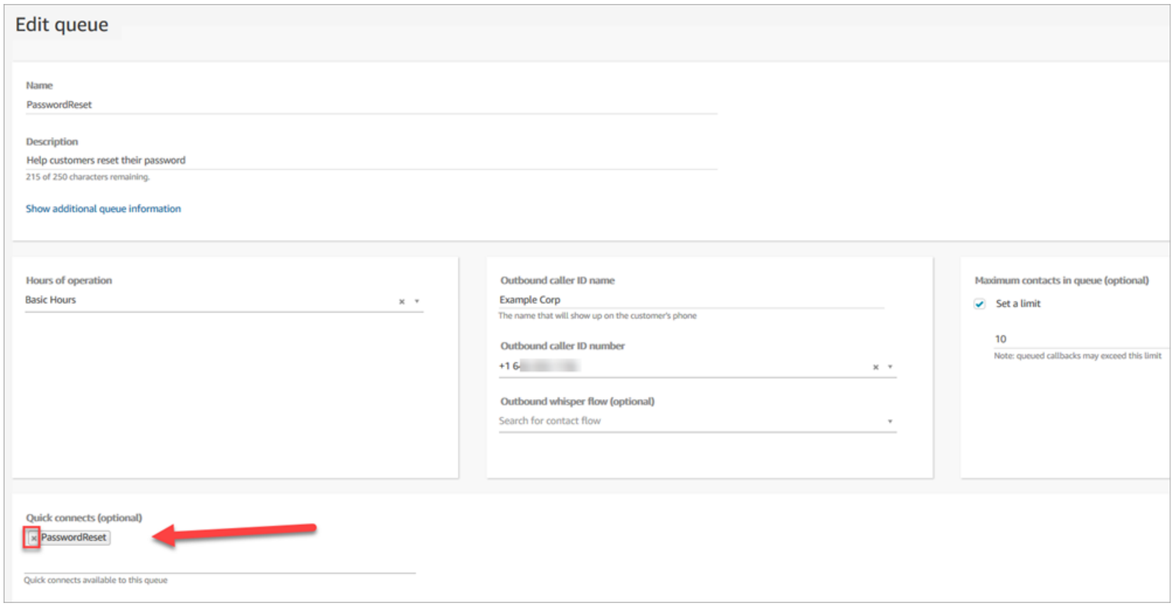


Delete quick connects

Use the DeleteQuickConnect API to delete quick connects.

At this time you can't delete quick connects using the Amazon Connect admin console. However, you can reuse them by changing the type, destination, and contact flow on the **Quick connects** page.

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



Edit queue

Name
PasswordReset

Description
Help customers reset their password
215 of 250 characters remaining.

Show additional queue information

Hours of operation
Basic Hours

Outbound caller ID name
Example Corp
The name that will show up on the customer's phone

Outbound caller ID number
+1 6[redacted]

Outbound whisper flow (optional)
Search for contact flow

Maximum contacts in queue (optional)
☑ Set a limit
10
Note: queued callbacks may exceed this limit

Quick connects (optional)
☒ PasswordReset
Quick connects available to this queue

How quick connects work

This article explains how each type of quick connect works: agent, queue, and external quick connects. It explains which contact flows are used, and what appears on the agent's Contact Control Panel (CCP).

> **Tip**
> For all three types of quick connects, when the quick connect is invoked, the contact that the agent is working on hears the Default customer hold (p. 307) flow unless you specify a different customer hold flow.

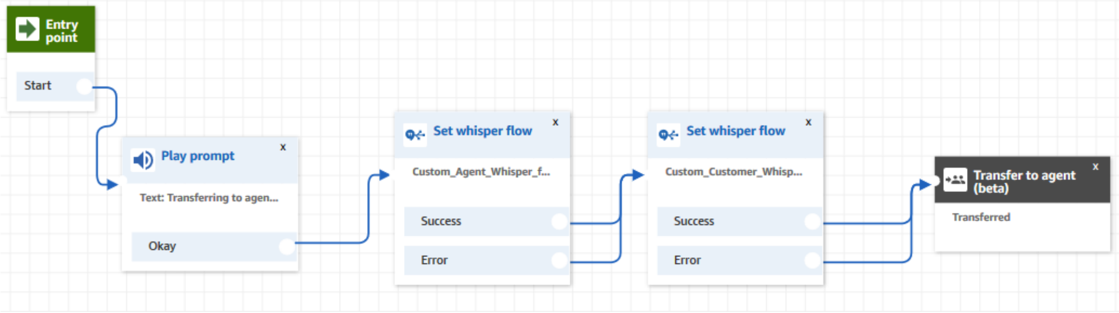
Agent quick connects

Let's say an agent named John is talking to a customer. During the conversation he needs to transfer the call to an agent named Maria. This is an agent quick connect.

Here's what John and Maria do, and what contact blocks are triggered:

1. John chooses the **Quick Connect** button on his CCP. (On the earlier CCP, the button is named **Transfer**). He selects **Maria** from the list of quick connects.

   When John does this, his CCP banner changes to **Connected**. However, the call isn't actually connected to Maria yet.
2. In our example scenario, Amazon Connect triggers an agent transfer flow that looks like the following image:



The call is not yet connected to Maria.

3. John hears the first **Play prompt**, "Transferring to agent."
4. Maria receives a notification in her CCP to either accept or reject the call.
5. Maria accepts the incoming call. The banner in her CCP changes to **Connecting**.
6. The first Set whisper flow (p. 418) block is triggered. This block sets the custom agent whisper flow. It plays the Custom_Agent_Whisper to Maria, for example, "This is an internal call transferred from another agent."

   Note
   If you don't create and then select a custom agent whisper flow, Amazon Connect plays the default agent whisper flow (p. 305), which says the queue name.
7. The next Set whisper flow (p. 418) block is triggered. It plays the Custom_Customer_Whisper to John, for example, "Your call is now connecting to an agent."

   Note
   If you don't create and then select a custom customer whisper flow, Amazon Connect plays the default customer whisper flow (p. 305), which plays a beep.
8. Maria's CCP banner shows she's **Connected**. John and Maria are connected and can start talking.
9. Now John can do one of the following on his CCP:

   - Choose **Join**. This joins all parties on the call. John, Maria, and the customer have a conference call.
   - Choose **Hold all**. This puts Maria and the customer on hold.
   - Put Maria on hold, so he only talks to the customer.
   - Choose **End call**. He leaves the call but Maria and the customer are directly connected and continue talking.

Queue quick connects

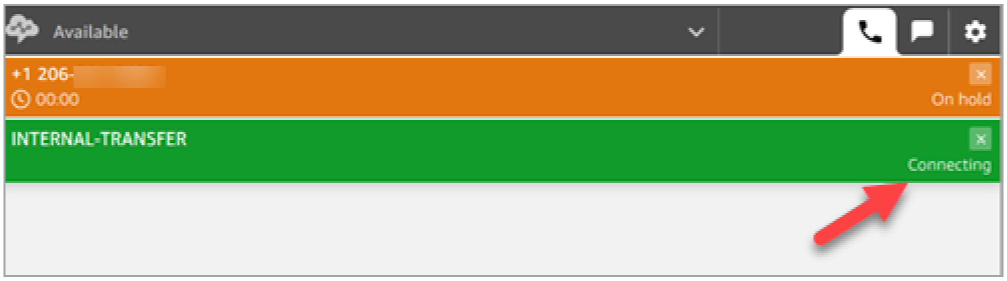
Let's say John is talking to a customer. The customer needs help resetting his password, so John needs to transfer him to the PasswordReset queue. This is a queue quick connect.

Another agent, Maria, is assigned to handle contacts in the PasswordReset queue. Her status in the CCP is **Available**.

Here's what John and Maria do, and what contact blocks are triggered:

1. John chooses the **Quick Connect** button on his CCP. (On the earlier CCP, the button is named **Transfer**). He chooses to transfer the contact to the PasswordReset queue. As soon as John chooses the PasswordReset quick connect, his CCP banner shows **Connecting**.

   Important
   Even though the status of the transferred call (internal-transfer) shows on John's CCP banner as **Connecting**, the contact is not yet transferred to the PasswordReset queue.



2. Amazon Connect invokes the queue transfer flow that's associated with the PasswordReset quick connect. In this flow, the Transfer to queue (p. 437) block transfers the contact to the PasswordReset queue since it's specified in the block. The contact is now in the PasswordReset queue.
3. Maria is notified in her CCP to accept or reject the incoming call.
4. Maria accepts the incoming call and her CCP banner changes to **Connecting**.
5. The Agent whisper flow (p. 445) is played to Maria. It says "Connecting you to PasswordReset queue."
6. The Customer whisper flow (p. 445) is played to John. It says "Connecting you to PasswordReset queue."
7. Maria's CCP banner changes to **Connected**. John and Maria are connected and can start talking.
8. Now John can do one of the following from his CCP:

   - Choose **Join**. This joins all parties on the call. John, Maria, and the customer have a conference call.
   - Choose **Hold all**. This puts Maria and the customer on hold.
   - Put Maria on hold, so he only talks to the customer.
   - Choose **End call**. He leaves the call but Maria and the customer are directly connected and continue talking.

External quick connects

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

Because no contact flow is involved in external quick connects, you can't set the outbound caller ID. Instead, the caller ID that you specified when you created the queue (p. 222) is used.

Set up agent-to-agent transfers

We recommend using these instructions to set up agent-to-agent voice, chat, and task transfers. You use a Set working queue (p. 421) block to transfer the contact to the agent's queue. The **Set working queue** block supports an omnichannel experience, whereas the Transfer to agent (beta) (p. 430) block does not.

Step 1: Create the quick connect

Following are the instructions to add quick connects manually using the Amazon Connect console. To add quick connects programmatically, use the CreateQuickConnect API.

Create a quick connect

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

   Important
   A description is required when you create a quick connect. If you don't add one, you'll get an error when you try to save the quick connect.
3. To add more quick connects, choose **Add new**.
4. Choose **Save**.
5. Go to the next procedure to enable your agents to see the quick connects in the Contact Control Panel (CCP).

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

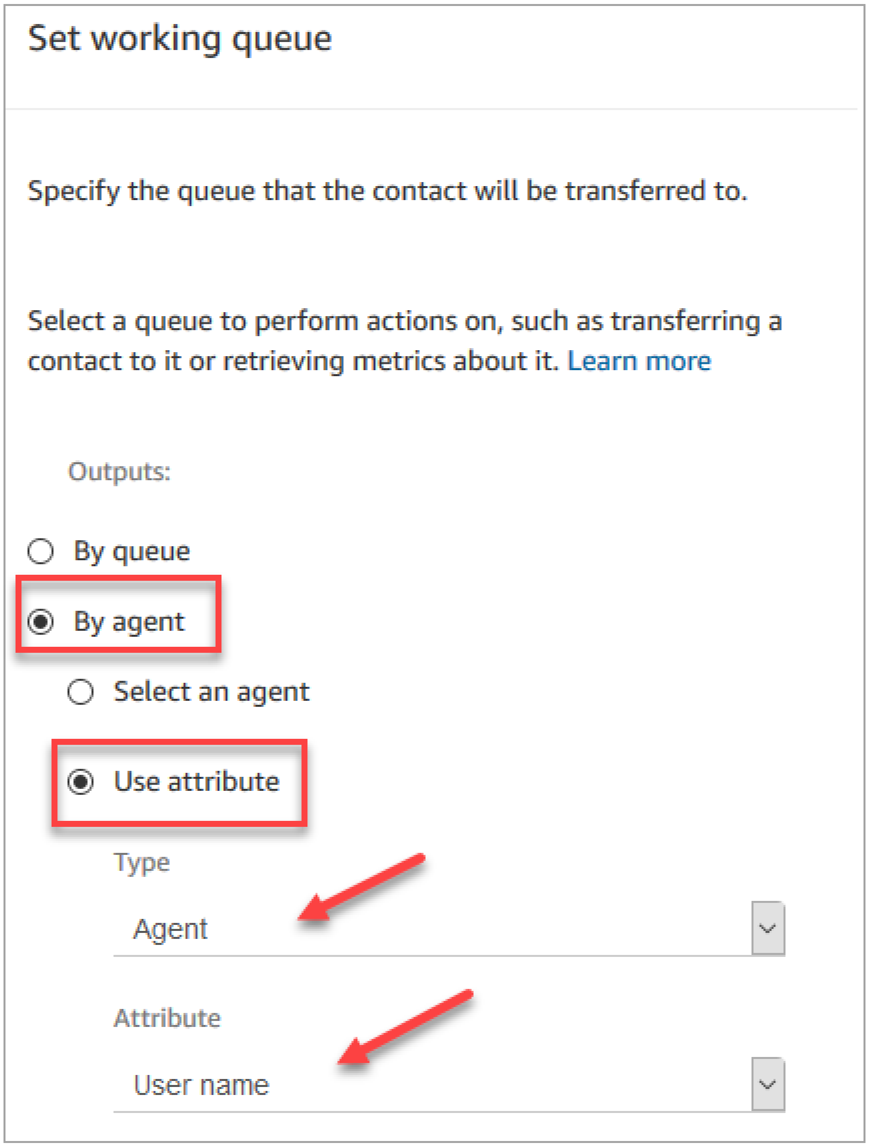
1. After you create the quick connect, go to **Routing**, **Queues** and then choose the appropriate queue for the contact to be routed to.
2. On the **Edit queue** page, in the **Quick connect** box, search for the quick connect you created.
3. Select the quick connect and then choose **Save**.

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

Step 2: Set up the "Transfer to agent" contact flow

In this step, you create a contact flow that's type **Transfer to agent** and use a Set working queue (p. 421) block to transfer the contact to the agent.

1. In the navigation pane, choose **Routing**, **Contact flows**.
2. Use the drop-down to choose **Create transfer to agent flow**.
3. Type a name and a description for your contact flow.
4. In the left navigation menu, expand **Set**, and then drag the **Set working queue** block to the canvas.
5. Configure the **Set working queue** block as shown in the following image:



Set working queue

Specify the queue that the contact will be transferred to.

Select a queue to perform actions on, such as transferring a contact to it or retrieving metrics about it. Learn more

Outputs:

○ By queue

● By agent

○ Select an agent

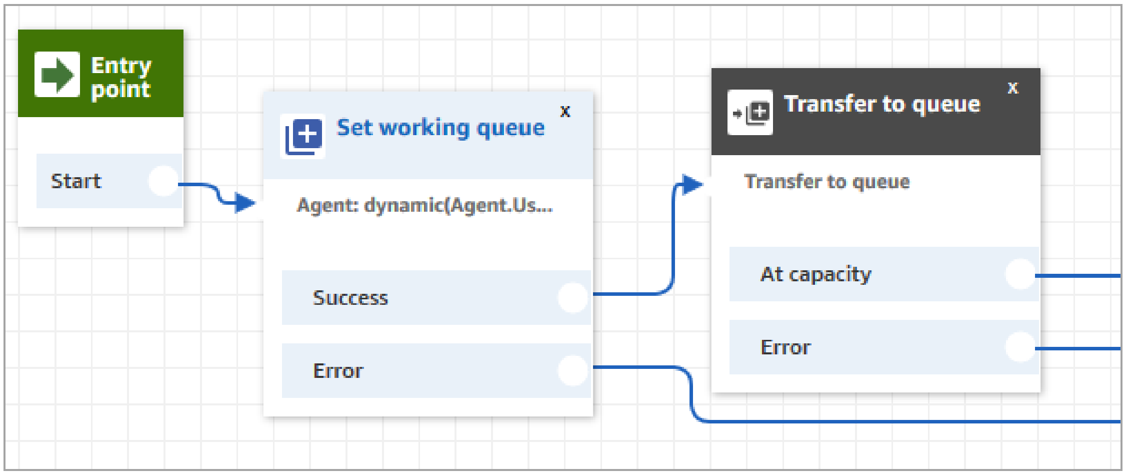
● Use attribute

Type: Agent

Attribute: User name

1. Choose **By agent**.
2. Choose **Use attribute**.
3. For **Type**, use the dropdown box to select **Agent**.
4. For **Attribute**, use the dropdown box to select **User name**.

6. Add a Transfer to queue (p. 437) block. You don't need to configure this block.



7. Save and publish this contact flow.
8. To show your agents how to transfer chats to another agent, see Transfer chats to another queue (p. 1153).

   To show your agents how to transfer tasks to another agent, see Transfer a task (p. 1179).

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

To set up a 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 contacts in a queue

For inbound contacts, you can define advanced routing decisions to minimize queue wait times, or route contacts to specific queues, using blocks in your contact flow. For example:

- Use a **Check queue status** block to check staffing or agent availability for a queue before sending a contact to that queue.
- Or, use a **Get queue metrics** block to retrieve queue metrics.
- Then use a **Check contact attributes** block to check specific queue metric attributes, and define conditions to determine which queue to route the contact to based on attribute values. For more information about using queue metrics, see Route based on number of contacts in a queue (p. 533).

After determining which queue to transfer the contact to, use a **Transfer to queue** block in a contact flow to transfer the contact to that queue. When the **Transfer to queue** block runs, it checks the queue capacity to determine whether or not the queue is at capacity (full). This check for queue capacity compares the current number of contacts in the queue to the Maximum contacts in queue (p. 224) limit, if one is set for the queue. If no limit is set, the queue is limited to the number of concurrent contacts set in the service quota (p. 1205) for the instance.

After the contact is placed in a queue, the contact remains there until an agent takes the contact, or until the contact is handled based on the routing decisions in your customer queue flow.

To change the queue associated with the call after it is already placed in a queue, use a **Loop prompts** block with a **Transfer to queue** block in a customer queue flow. In the block choose which queue to transfer the call to, or use an attribute to set the queue.

To manage contacts in a queue using a Transfer to queue block

1. In Amazon Connect, on the navigation menu choose **Routing**, **Contact flows**.

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

    Alternatively, choose **Use attribute**, then reference an attribute to specify the queue. If you use an attribute to set the queue, the value must be the queue ARN.
13. Choose **Save**.
14. Connect the **Loop prompt** block to the **Transfer to queue** block.
15. Add additional blocks to complete the contact flow that you require, such as the blocks to check queue status or metrics, then choose **Save**.

    The contact flow is not active until you publish it.

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

Transfer contacts to a specific agent

Agent queues enable you to route contacts directly to a specific agent. Following are a couple of scenarios where you might want to do this:

- Route contacts to the last agent the customer interacted with. This provides a consistent customer experience.
- Route contacts to agents who have specific responsibilities. For example, you might route all billing questions to Jane.

> **Note**
> A queue is created for all users in your Amazon Connect instance, but only users who are assigned permissions to use the Contact Control Panel (CCP) can use it to receive contacts. The Agent and Admin security profiles are the only default security profiles that include permissions to use the CCP. If you route a contact to someone who doesn't have these permissions, the contact can never be handled.

To route a contact directly to a specific agent

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

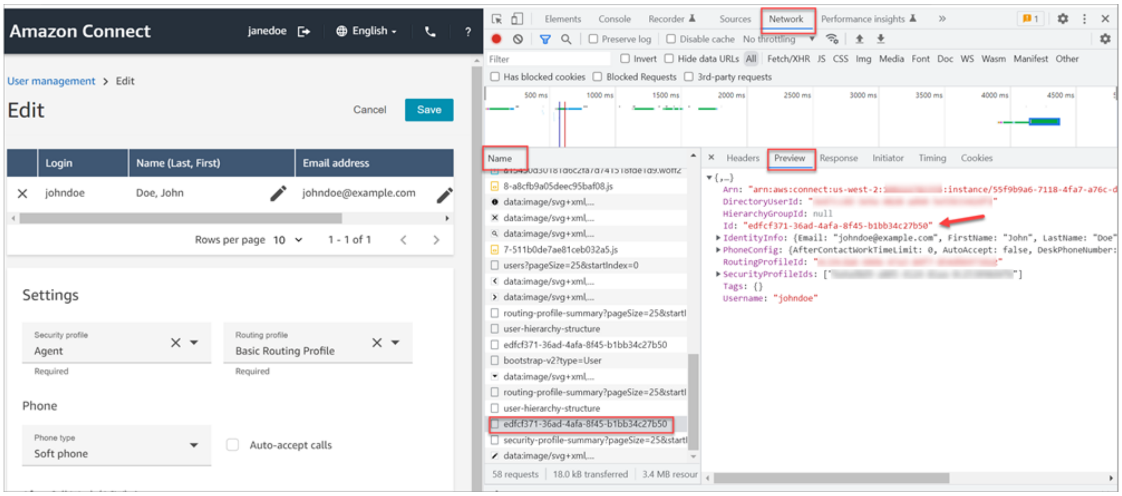
You can also choose to use an attribute to select the queue created for the agent user account. To do so, after you choose **By agent**, choose **Use attribute**.

Use contact attributes to route contacts to a specific agent

When you use contact attributes in a contact flow to route calls to an agent, the attribute value must be either the agent's user name, or the agent's user ID.

To determine the user ID for an agent so that you can use the value as an attribute, use one of these options:

- Use the **Network** tab of the browser debugger to retrieve the agent ID. For example:
  1. In a Chrome browser, press F12 and go to the **Network** tab.
  2. In Amazon Connect, in the navigation menu, choose **Users**, **User management**, and then select an agent. Monitor the content of the **Network** tab. In the **Name** list, choose the GUID.
  3. Choose the **Preview** tab. The agent ID is displayed next to the `Id` field. The following image shows an example.



	Login	Name (Last, First)	Email address
×	johndoe	Doe, John	johndoe@example.com

Rows per page 10 | 1 - 1 of 1

Security profile: Agent (Required)

Routing profile: Basic Routing Profile (Required)

Phone type: Soft phone

☐ Auto-accept calls

```
Name
8-a8cfb9a05deec95baf08.js
data:image/svg+xml,...
data:image/svg+xml,...
data:image/svg+xml,...
7-511b0de7ae81ceb032a5.js
users?pageSize=25&startIndex=0
data:image/svg+xml,...
data:image/svg+xml,...
routing-profile-summary?pageSize=25&startI
user-hierarchy-structure
edfcf371-36ad-4afa-8f45-b1bb34c27b50
bootstrap-v2?type=User
data:image/svg+xml,...
routing-profile-summary?pageSize=25&startI
user-hierarchy-structure
edfcf371-36ad-4afa-8f45-b1bb34c27b50
security-profile-summary?pageSize=25&startI
data:image/svg+xml,...
58 requests | 18.0 kB transferred | 3.4 MB resour
```

```
▼{,…}
   Arn: "arn:aws:connect:us-west-2:[redacted]:instance/55f9b9a6-7118-4fa7-a76c-d
   DirectoryUserId: "[redacted]"
   HierarchyGroupId: null
   Id: "edfcf371-36ad-4afa-8f45-b1bb34c27b50"
 ▶ IdentityInfo: {Email: "johndoe@example.com", FirstName: "John", LastName: "Doe"
 ▶ PhoneConfig: {AfterContactWorkTimeLimit: 0, AutoAccept: false, DeskPhoneNumber:
   RoutingProfileId: "[redacted]"
 ▶ SecurityProfileIds: ["[redacted]"]
   Tags: {}
   Username: "johndoe"
```

- Use the ListUsers operation to retrieve the users from your instance. The agent's user ID is returned with the results from the operation as the value of the `Id` in the UserSummary object.
- Find the user ID for an agent by using Amazon Connect agent event streams (p. 965). The agent events, which are included in the agent event data stream, include the agent ARN. The user ID is included in the agent ARN after **`agent/`**.

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

```
{
    "AWSAccountId": "123456789012",
    "AgentARN": "arn:aws:connect:us-
west-2:123456789012:instance/12345678-1234-1234-1234-123456789012/
agent/87654321-4321-4321-4321-123456789012",
    "CurrentAgentSnapshot": {
        "AgentStatus": {
            "ARN": "arn:aws:connect:us-
west-2:123456789012:instance/12345678-1234-1234-1234-123456789012/agent-
state/76543210-7654-6543-8765-765432109876",
            "Name": "Available",
            "StartTimestamp": "2019-01-02T19:16:11.011Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "IAM",
            "LastName": "IAM",
            "RoutingProfile": {
                "ARN": "arn:aws:connect:us-
west-2:123456789012:instance/12345678-1234-1234-1234-123456789012/routing-profile/aaaaaaaa-
bbbb-cccc-dddd-111111111111",
                "DefaultOutboundQueue": {
                    "ARN": "arn:aws:connect:us-
west-2:123456789012:instance/12345678-1234-1234-1234-123456789012/queue/aaaaaaaa-bbbb-cccc-
dddd-222222222222",
                    "Name": "BasicQueue"
                },
                "InboundQueues": [{
                    "ARN": "arn:aws:connect:us-
west-2:123456789012:instance/12345678-1234-1234-1234-123456789012/queue/aaaaaaaa-bbbb-cccc-
dddd-222222222222",
                    "Name": "BasicQueue"
                }],
                "Name": "Basic Routing Profile"
            },
            "Username": "agentUserName"
        },
        "Contacts": []
},
```

Set up recording behavior

Managers can monitor live conversations, and review and download recordings of past agent conversations. To set this up, you need to add the Set recording and analytics behavior (p. 408) block to your contact flows, assign managers the appropriate permissions, and show them how to monitor live conversations and access past recordings in Amazon Connect.

When is a conversation recorded?

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

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

If the agent mutes their own microphone, for example, to consult with a coworker sitting next to them, their side-bar conversation is not recorded. The customer is still recorded since their microphone hasn't been muted.

Where are recordings and transcripts stored?

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

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

Recordings are stored in the Amazon S3 bucket that are created for your instance (p. 137). Any user or application with the appropriate permissions can access the recordings in the Amazon S3 bucket.

Encryption is enabled by default for all call recordings using Amazon S3 server-side encryption with KMS. The encryption is at the object level. The reports and recording objects are encrypted; there's no encryption at the bucket level.

You shouldn't disable encryption.

> **Important**
>
> - For voice conversations to be stored in an Amazon S3 bucket, you need to enable recording in the contact flow block using the Set recording and analytics behavior (p. 408) block.
> - For chat conversations, if there's an S3 bucket for storing chat transcripts, then all chats are recorded and stored there. If no bucket exists, then no chats are recorded. However, if you want to monitor chat conversations, you still need to add the Set recording and analytics behavior (p. 408) block to the flow.

> **Tip**
>
> We recommend using the contact ID to search for recordings.
> Even though many call recordings for specific contact IDs may be named with the contact ID prefix itself (for example, 123456-aaaa-bbbb-3223-2323234.wav), there is no guarantee that the contact IDs and name of the contact recording file *always* match. By using **Contact ID** for your search on the Contact search (p. 810) page, you can find the correct recording by referring the audio file on the contact record.

When are recordings available?

When call recording is enabled, the recording is placed in your S3 bucket shortly after the contact is disconnected. Then you can review the recording (p. 801).

> **Important**
>
> You can also access the recording from the customer's contact record (p. 997). The recording is available in the contact record, however, only after the contact has left the After Contact Work (ACW) state (p. 999).

How to set up recording behavior

To view a sample contact flow with the **Set recording behavior** block configured, see Sample recording behavior (p. 315).

To set up recording behavior in your contact flows

1. Log in to your Amazon Connect instance using an account that has permissions to edit contact flows.
2. Choose **Routing**, **Contact flows**, and then open the contact flow that handles customer contacts you want to monitor.

3. Before the contact is connected to an agent, add a Set recording and analytics behavior (p. 408) block to the contact flow.
4. To configure the Set recording and analytics behavior (p. 408) block, choose from the following:
   - To record voice conversations, choose what you want to record: **Agent and Customer**, **Agent only**, or **Customer only**.
   - To record chat conversations, you need to choose **Agent and Customer**.
   - To enable monitoring of voice and/or chat conversations, you need to choose **Agent and Customer**.
5. Choose **Save** and then **Publish** to publish the updated contact flow.

To set up recording behavior for outbound calls

1. Create a contact flow, using the outbound whisper flow type.
2. Add a Set recording and analytics behavior (p. 408) block to that contact flow.
3. Set up a queue that will be used for making outbound calls. In the **Outbound whisper flow** box, choose the contact flow that has Set recording and analytics behavior (p. 408) in it.

How to set up users to monitor conversations or review recordings

To learn what permissions managers need, and how they can monitor live conversations and review recordings of past conversations, see:

- Monitor live conversations (p. 798)
- Review recorded conversations (p. 801)

Set up queued callback

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

Here's how queued callback works:

1. When a customer leaves their number it's put in a queue and then routed to the next available agent.
2. After an agent accepts the callback in the CCP, Amazon Connect calls the customer.

   If no agents are available to work on callbacks, the callbacks can stay in queue for at least 7 days and up to 14 days after they are created before Amazon Connect automatically removes them.

   Tip
   To manually remove a callback from the queue, use the StopContact API.
3. If there is no answer when the Amazon Connect calls the customer, it retries based on the number of times you've specified.
4. If the call goes to **voicemail**, it's considered connected.
5. If the customer calls again while in the callback queue, it's treated as a new call and will be handled as usual. To avoid duplicate callback requests in a callback queue, see this blog: Preventing duplicate callback requests in Amazon Connect.

How queued callbacks affect queue limits

- Queued callbacks count towards the queue size limit, but they are routed to the error branch. For example, if you have a queue that handles callbacks and incoming calls, and that queue reaches the size limit:
  - The next callback is routed to the error branch.
  - The next incoming call gets a reorder tone (also known as a fast busy tone), which indicates no transmission path to the called number is available.
- Consider setting up your queued callbacks to be lower priority than your queue for incoming calls. This way, your agents only work on queued callbacks when the incoming call volume is low.

Steps to set up queued callback

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

- Set up a queue (p. 222) specifically for callbacks. In your real-time metrics reports, you can look at that queue and see how many customers are waiting for callbacks.
- Set up caller ID (p. 212). When setting your callback queue, specify the caller ID name and phone number that appears to customers when you call back.
- Add the callback queue to a routing profile (p. 227). Set this up so that contacts waiting for a call are routed to agents.
- Create a contact flow for queued callbacks (p. 482). You offer the option for a callback to the customer.
- Associate a phone number with the inbound contact flow (p. 453).
- (Optional) Create an outbound whisper flow. When a queued call is placed, the customer hears this message after they pick up and before they connect to the agent. For example, "Hello, this is your scheduled callback..."
- (Optional) Create an agent whisper flow. This is what the agent hears right after they accept the contact, before they are joined to the customer. For example, "You're about to be connected to Customer John, who requested a refund for..."

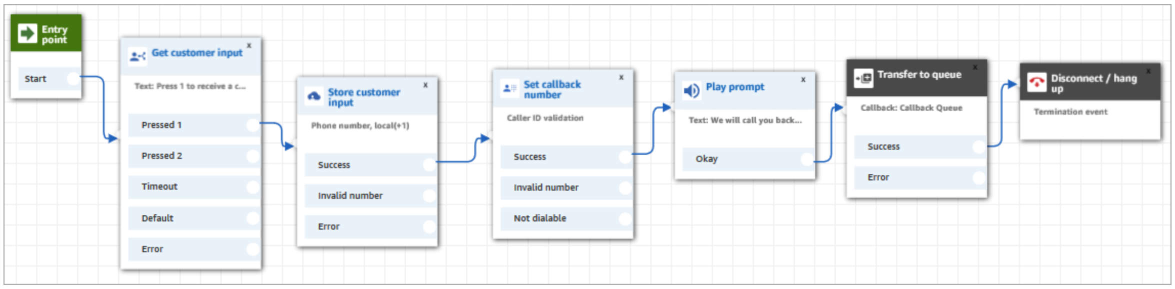
Create a contact flow for queued callbacks

To see what a flow looks like with queued callback, in new Amazon Connect instances see Sample queue configurations (p. 311). In previous instances, see Sample queued callback (p. 314).

The following procedure shows how to:

- Request a callback number from a customer.
- Store the callback number in an attribute.
- Reference the attribute in a **Set callback number** block to set the number to dial the customer.
- Transfer the customer to the callback queue.

At the basic level, here's what this queued callback flow looks like, without any of the alternative branches or error handling configured.

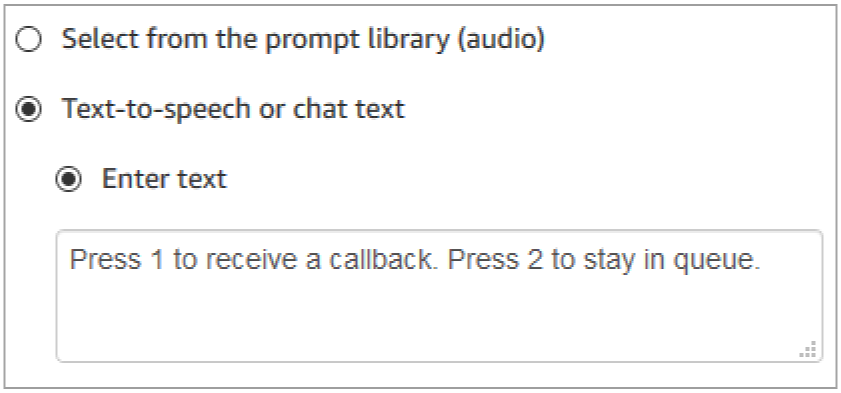


Following are the steps to create this flow.

To create a contact flow for queued callbacks

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

   Tip
   You can create this flow using different contact flow types: Customer queue flow, Transfer to agent, Transfer to queue.
3. Add a Get customer input (p. 366) block.
4. Configure the block to prompt the customer for a callback:

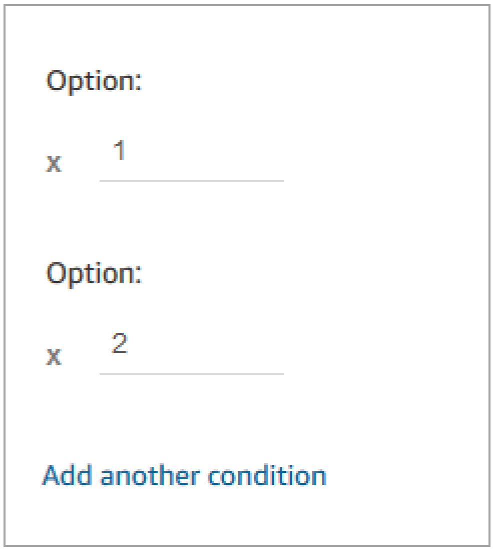
   

   ○ Select from the prompt library (audio)

   ● Text-to-speech or chat text

   ● Enter text

   Press 1 to receive a callback. Press 2 to stay in queue.
5. At the bottom of the block, choose **Add another condition**, and add options 1 and 2.

   Option:

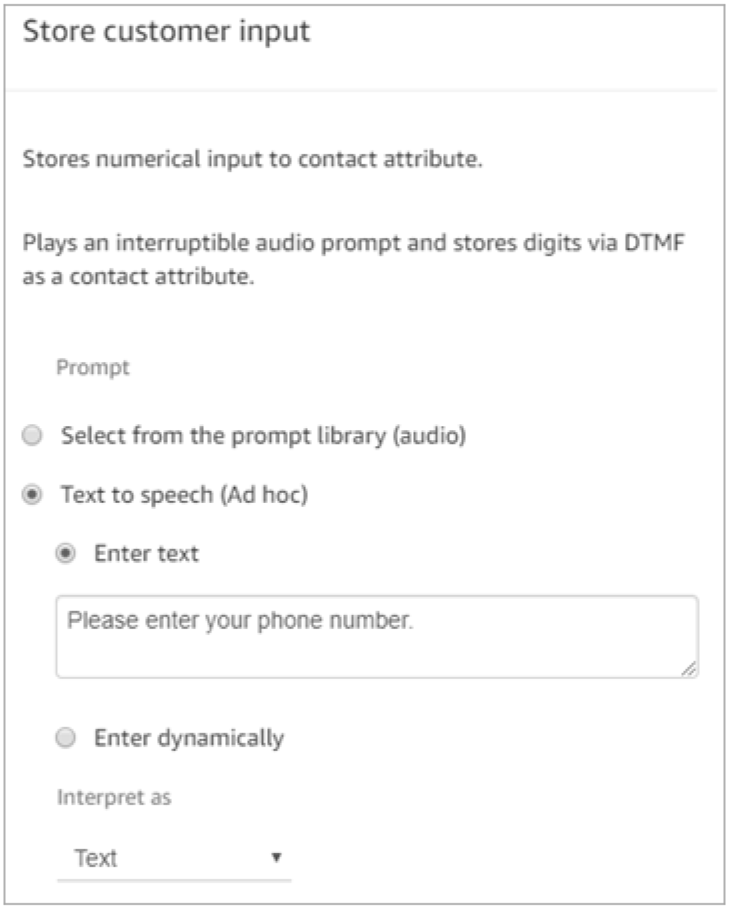
   x 1

   Option:

   x 2

   Add another condition
6. Add a Store customer input (p. 426) block.

7. Configure the block to prompt customers for their callback number, such as “Please enter your phone number.”



Store customer input

Stores numerical input to contact attribute.

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

Prompt

○ Select from the prompt library (audio)

● Text to speech (Ad hoc)

● Enter text

Please enter your phone number.

○ Enter dynamically

Interpret as

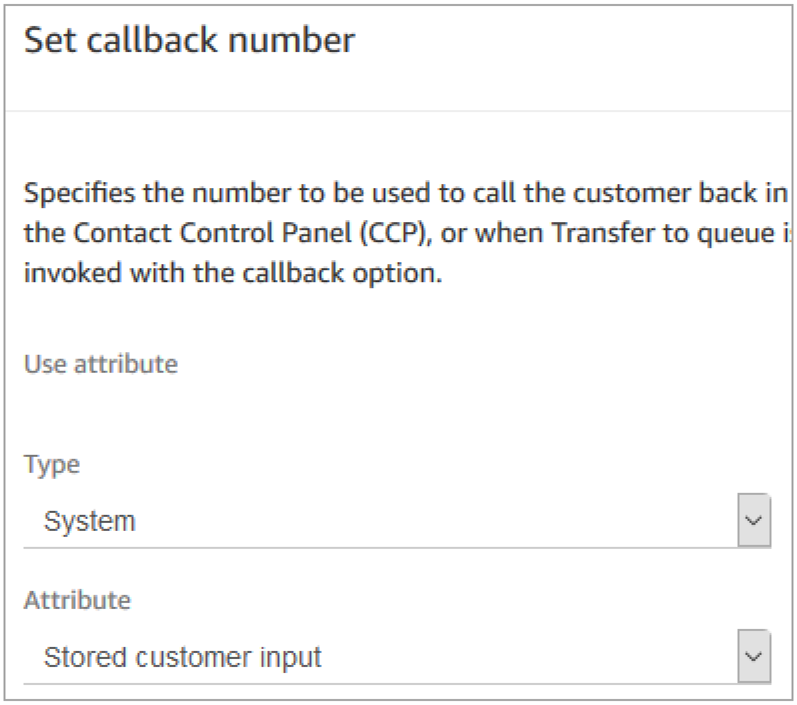
Text ▾

8. In the **Customer input** section, select **Phone number**, and then choose one of the following:

   - **Local format**: Your customers are calling from phone numbers that are in the same country as the AWS Region where you created your Amazon Connect instance.
   - **International format/Enforce E.164**: Your customers are calling from phone numbers in countries or regions other than the one where you created your instance.

9. Add a Set callback number (p. 397) block to your contact flow.

10. Configure the block to set **Type** to **System**. For **Attribute**, choose **Store customer input**. This attribute stores the customer's phone number.



Set callback number

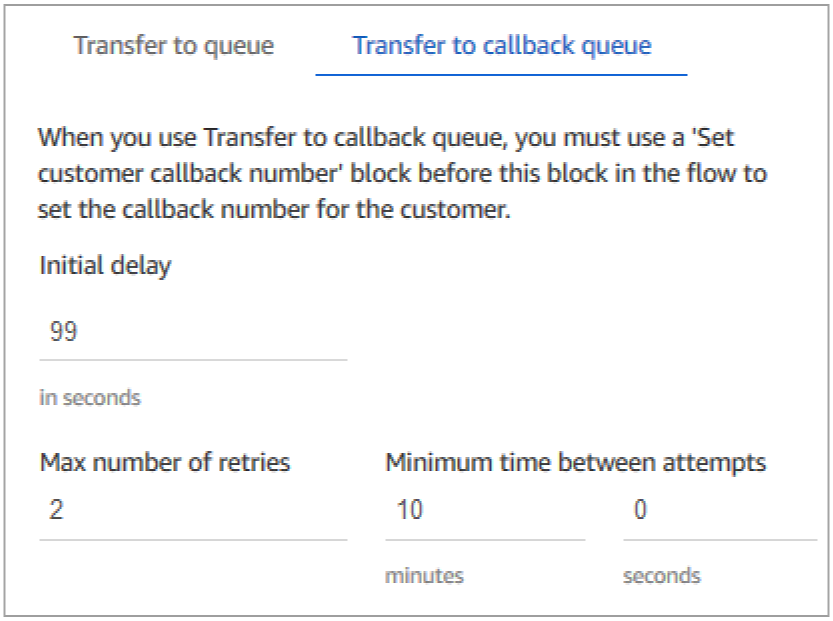
Specifies the number to be used to call the customer back in the Contact Control Panel (CCP), or when Transfer to queue i invoked with the callback option.

Use attribute

Type: System

Attribute: Stored customer input

11. Add a Transfer to queue (p. 437) block.
12. In the **Transfer to queue** block, configure the **Transfer to callback queue** tab as shown in the following image:



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

Initial delay: 99 in seconds

Max number of retries: 2

Minimum time between attempts: 10 minutes 0 seconds

The following properties are available:

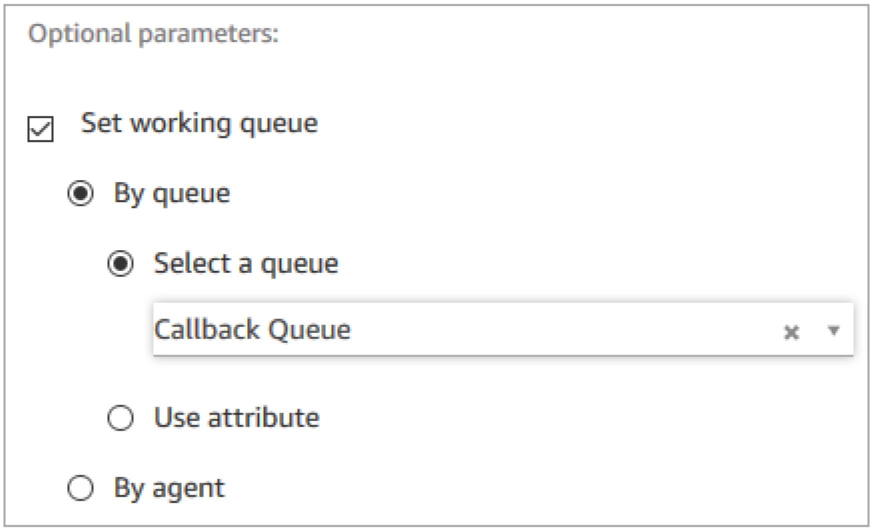
- **Initial delay**: Specify how much time has to pass between a callback contact being initiated in the contact flow, and the customer is put in queue for the next available agent. In the previous example, the time is 99 seconds.
- **Maximum number of retries**: If this is set to 2, then Amazon Connect tries to call back the customer a maximum of three times: the initial callback, and two retries.

A retry only happens if it rings but there's no answer. If the callback goes to voicemail, it's considered connected and Amazon Connect does not retry again.

> **Tip**
> We strongly recommend that you double-check the number entered in **Maximum number of retries**. If you accidentally enter a high number, such as 20, it's going to result in unnecessary work for the agent and too many calls for the customer.

- **Minimum time between attempts**: If the customer doesn't answer the phone, this is how long to wait until trying again. In the previous example, we wait 10 minutes between attempts.

13. In the Optional parameters section, choose **Set working queue** if you want to transfer the contact to a queue that you set up specifically for callbacks.



Optional parameters:

☑ Set working queue

● By queue

● Select a queue

Callback Queue

○ Use attribute

○ By agent

Creating a queue just for callbacks lets you view in your real-time metrics reports how many customers are waiting for callbacks.

If you don't set a working queue, Amazon Connect uses the queue that was set previously in the flow.

14. To save and test this flow, configure the other branches and add error handling. To see an example of how this is done, see Sample queue configurations (p. 311). For previous instances, see Sample queued callback (p. 314).
15. For information about how callbacks appear in real-time metrics reports and contact records, see About queued callbacks in metrics (p. 1002).

Learn more about queued callbacks

See the following topics to learn more about queued callbacks:

- About queued callbacks in metrics (p. 1002)
- How Initial delay affects Scheduled and In queue metrics (p. 1004)
- What counts as a "Failed Callback Attempt" (p. 1005)
- Example: Metrics for a queued callback (p. 1006)

Import/export contact flows

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

To migrate tens or hundreds of contact flows, use the APIs described in Migrate contact flows to a different instance (p. 543).

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

Export limitations

You can export contact flows that meet the following requirements:

- The flow has fewer than 100 blocks.
- The total size of the flow is less than 1MB.

We recommend dividing large flows in to smaller ones to meet these requirements.

Contact flows are exported to JSON files

A contact flow is exported to a JSON file. It has the following characteristics:

- The JSON includes a section for each block in the flow.
- The name used for a specific block, parameter, or other element of the contact flow may be different than the label used for it in the user interface (UI).

By default, contact flow export files are created without a file name extension, and saved to the default location set for your browser. We suggest saving your exported contact flows to folder that contains only exported contact flows.

How to import/export contact flows

To export a contact flow

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

To import a contact flow

1. Log in to your Amazon Connect instance. The account must be assigned a security profile that includes edit permissions for contact flows.
2. On the navigation menu, 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**.

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.

Invoke AWS Lambda functions

Amazon Connect can interact with your own systems and take different paths in contact flows dynamically. To achieve this, invoke AWS Lambda functions in a contact flow, fetch the results, and call your own services or interact with other AWS data stores or services. For more information, see the AWS Lambda Developer Guide.

To invoke a Lambda function from a contact flow, complete the following tasks.

Tasks

- Tutorial: Create a Lambda function and invoke in a flow (p. 497)

Create a Lambda function

Create a Lambda function, using any runtime, and configure it. For more information, see Get started with Lambda in the *AWS Lambda Developer Guide*.

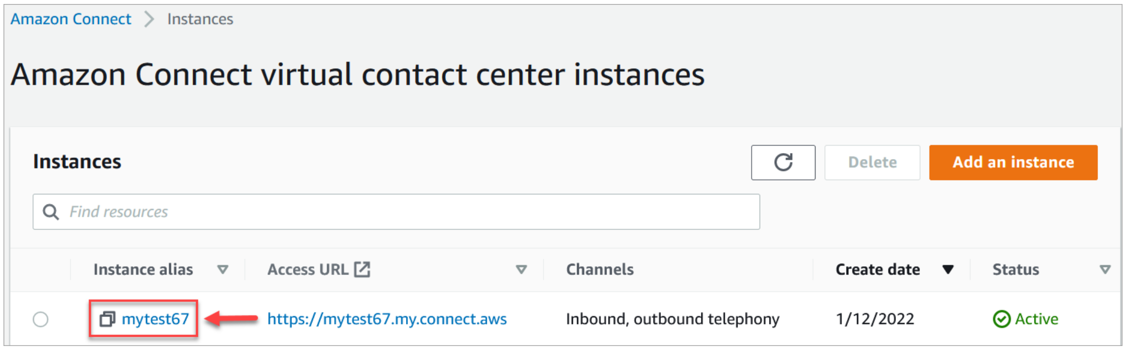
If you create the Lambda function in the same Region as your contact center, you can use the Amazon Connect console to add the Lambda function to your instance as described in the next task, Add a Lambda function to your Amazon Connect instance (p. 489). This automatically adds resource permissions that allow Amazon Connect to invoke the Lambda function. Otherwise, if the Lambda function is in a different Region, you can add it to your contact flow using the contact flow designer and add the resource permissions using the add-permission command, with a principal of `connect.amazonaws.com` and the ARN of your Amazon Connect instance. For more information, see Using Resource-Based Policies for AWS Lambda in the *AWS Lambda Developer Guide*.

Add a Lambda function to your Amazon Connect instance

Before you can use an Lambda function in a contact flow, you need to add it to your Amazon Connect instance.

Add a Lambda function to your instance

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose your instance name in the **Instance Alias** column. This instance name appears in the URL you use to access Amazon Connect.



Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Contact flows**.
4. In the **AWS Lambda** section, use the **Function** drop-down box to select the function to add to your instance.

   Tip
   The drop-down lists only those functions in the same Region as your instance. If no functions are listed, choose **Create a new Lambda function**, which opens the AWS Lambda console.
   To use a Lambda in a different Region or account, in the Invoke AWS Lambda function (p. 385), under **Select a function**, you can enter the ARN of a Lambda. Then set up the corresponding resource-based policy on that Lambda to allow the contact flow to call it.
   To call `lambda:AddPermission`, you need to:

   - Set the principal to **connect.amazonaws.com**

- Set the source account to be the account your instance is in.
- Set the source ARN to the ARN of your instance.

For more information, see Granting function access to other accounts.

5. Choose **Add Lambda Function**. Confirm that the ARN of the function is added under **Lambda Functions**.

Now you can refer to that Lambda function in your contact flows.

Invoke a Lambda function from a flow

1. Open or create a contact flow.
2. Add an Invoke AWS Lambda function (p. 385) block (in the **Integrate** group) to the grid. Connect the branches to and from the block.
3. Choose the title of the Invoke AWS Lambda function (p. 385) block to open its properties page.
4. Under **Select a function**, choose from the list of functions you've added to your instance.
5. (Optional) Under **Function input parameters**, choose **Add a parameter**. You can specify key-value pairs that are sent to the Lambda function when it is invoked. You can also specify a **Timeout** value for the function.
6. In **Timeout (max 8 seconds)**, specify how long to wait for Lambda to time out. After this time, the contact routes down the Error branch.

For every Lambda function invocation from a contact flow, you pass a default set of information related to ongoing contact, as well as any additional attributes defined in the **Function input parameters** section for the **Invoke AWS Lambda function** block added.

The following is an example JSON request to a Lambda function:

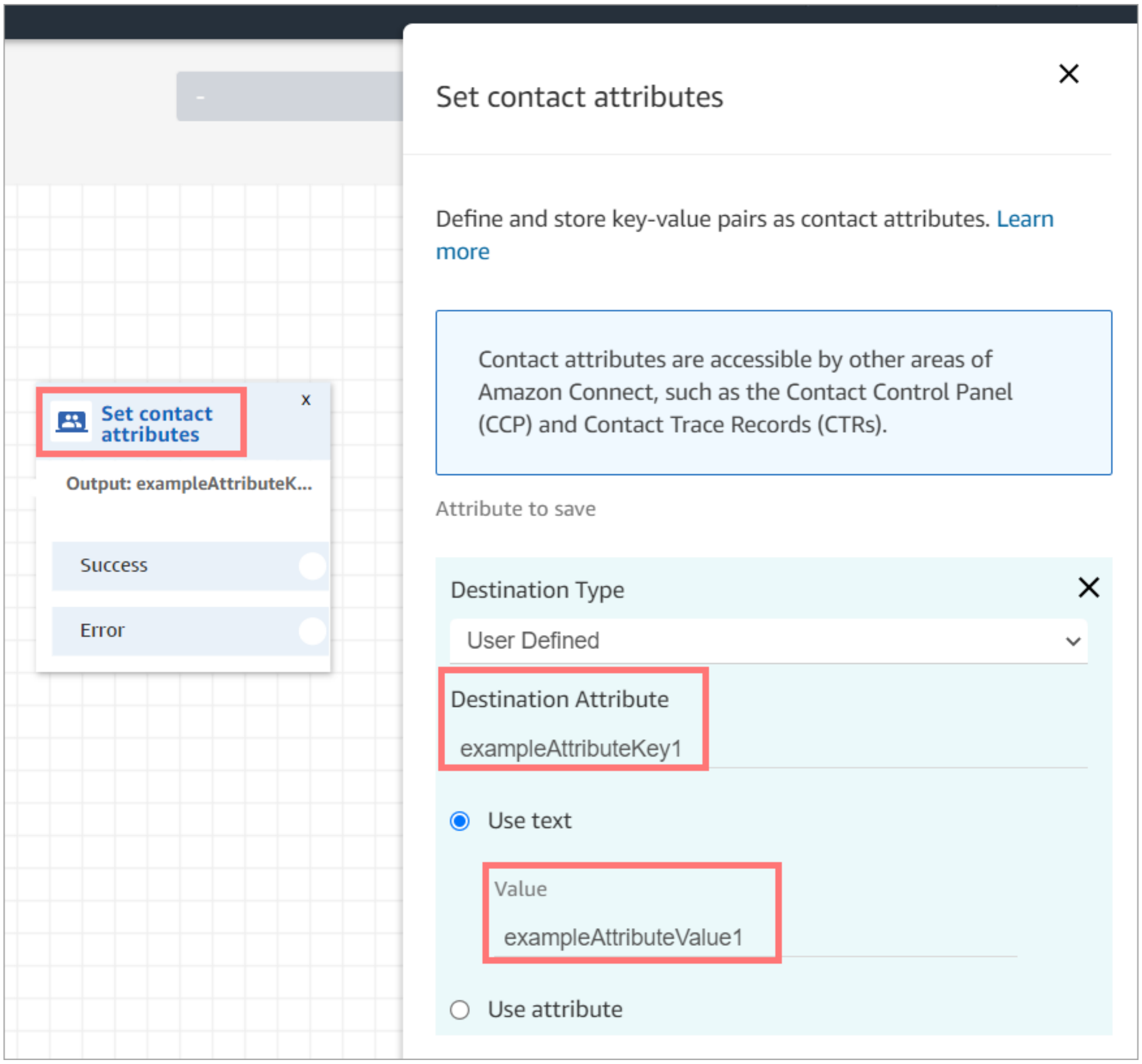
```
{
    "Details": {
        "ContactData": {
            "Attributes": {
           "exampleAttributeKey1": "exampleAttributeValue1"
          },
            "Channel": "VOICE",
            "ContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
            "CustomerEndpoint": {
                "Address": "+1234567890",
                "Type": "TELEPHONE_NUMBER"
            },
            "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
            "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
            "InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/
c8c0e68d-2200-4265-82c0-XXXXXXXXXX",
            "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
            "Queue": {
               "ARN": "arn:aws:connect:eu-west-2:111111111111:instance/cccccccc-bbbb-dddd-
eeee-ffffffffffff/queue/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
               "Name": "PasswordReset"
             },
            "SystemEndpoint": {
                "Address": "+1234567890",
                "Type": "TELEPHONE_NUMBER"
            }
        },
        "Parameters": {"exampleParameterKey1": "exampleParameterValue1",
           "exampleParameterKey2": "exampleParameterValue2"
        }
    },
    "Name": "ContactFlowEvent"
}
```

The request is divided into two parts:

- Contact data—This is always passed by Amazon Connect for every contact. Some parameters are optional.

  This section may include attributes that have been previously associated with a contact, such as when using a **Set contact attributes** block in a contact flow. This map may be empty if there aren't any saved attributes.

  The following image shows where these attributes would appear in the properties page of a **Set contact attributes**.



Set contact attributes

Define and store key-value pairs as contact attributes. Learn more

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

Attribute to save

Destination Type: User Defined

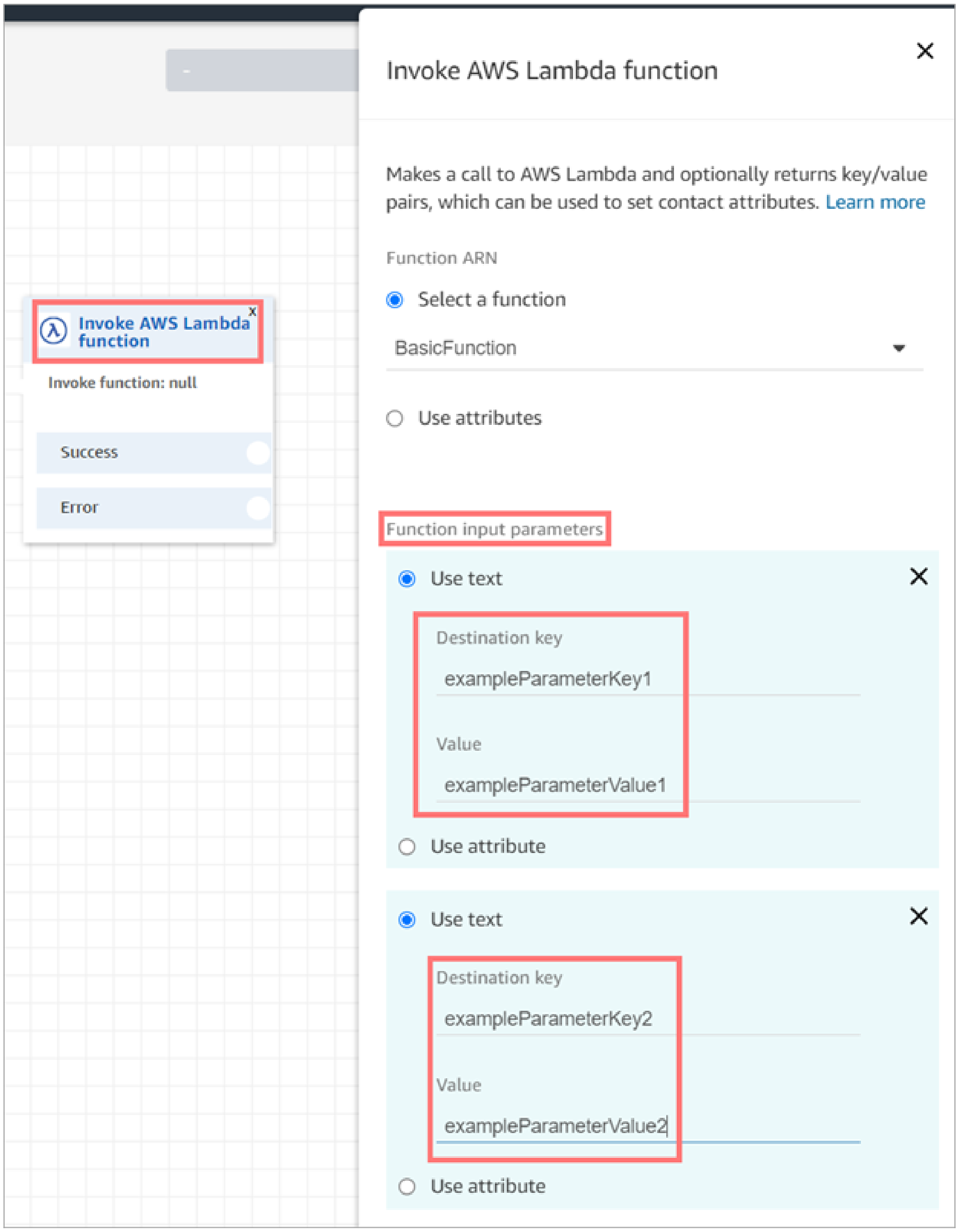
Destination Attribute: exampleAttributeKey1

● Use text

Value: exampleAttributeValue1

○ Use attribute

- Parameters—These are parameters specific to this call that were defined when you created the Lambda function. The following image shows where these parameters would appear in the properties page of the **Invoke AWS Lambda function** block.



Invoke AWS Lambda function

Makes a call to AWS Lambda and optionally returns key/value pairs, which can be used to set contact attributes. Learn more

Function ARN

● Select a function

BasicFunction

○ Use attributes

Function input parameters

● Use text

Destination key: exampleParameterKey1

Value: exampleParameterValue1

○ Use attribute

● Use text

Destination key: exampleParameterKey2

Value: exampleParameterValue2

○ Use attribute

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

Customers hear silence while a Lambda function executes. We recommend adding a **Play prompt** block between functions to keep customers engaged and aware of the long interaction.

Configure your Lambda function to parse the event

To successfully pass attributes and parameters between your Lambda function and Amazon Connect, configure your function to correctly parse the JSON request sent from the **Invoke AWS Lambda function** block or **Set contact attributes**, and define any business logic that should be applied. How the JSON is parsed depends on the runtime you use for your function.

For example, the following code shows how to access `exampleParameterKey1` from **Invoke AWS Lambda function** block and `exampleAttributeKey1` from **Set contact attributes** block using Node.JS:

```
exports.handler = function(event, context, callback) {
// Example: access value from parameter (Invoke AWS Lambda function)
let parameter1 = event['Details']['Parameters']['exampleParameterKey1'];

// Example: access value from attribute (Set contact attributes block)
let attribute1 = event['Details']['ContactData']['Attributes']['exampleAttributeKey1'];

// Example: access customer's phone number from default data
let phone = event['Details']['ContactData']['CustomerEndpoint']['Address'];

// Apply your business logic with the values
// ...
}
```

Verify the function response

The Lambda function response 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:

```
exports.handler = function(event, context, callback) {
// Extract data from the event object
let phone = event['Details']['ContactData']['CustomerEndpoint']['Address'];

// Get information from your APIs

let customerAccountId = getAccountIdByPhone(phone);
let customerBalance = getBalanceByAccountId(customerAccountId);

    let resultMap = {
        AccountId: customerAccountId,
        Balance: '$' + customerBalance,
}

callback(null, resultMap);
}
```

This example shows an example response using Python:

```
def lambda_handler(event, context):
// Extract data from the event object
  phone = event['Details']['ContactData']['CustomerEndpoint']['Address']

// Get information from your APIs
  customerAccountId = getAccountIdByPhone(phone)
  customerBalance = getBalanceByAccountId(customerAccountId)

   resultMap = {
    "AccountId": customerAccountId,
    "Balance": '$%s' % customerBalance
    }
```

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:

```
{
"AccountId": "a12345689",
"Balance": "$1000"
}
```

You may return any result as long as they are simple key-value pairs.

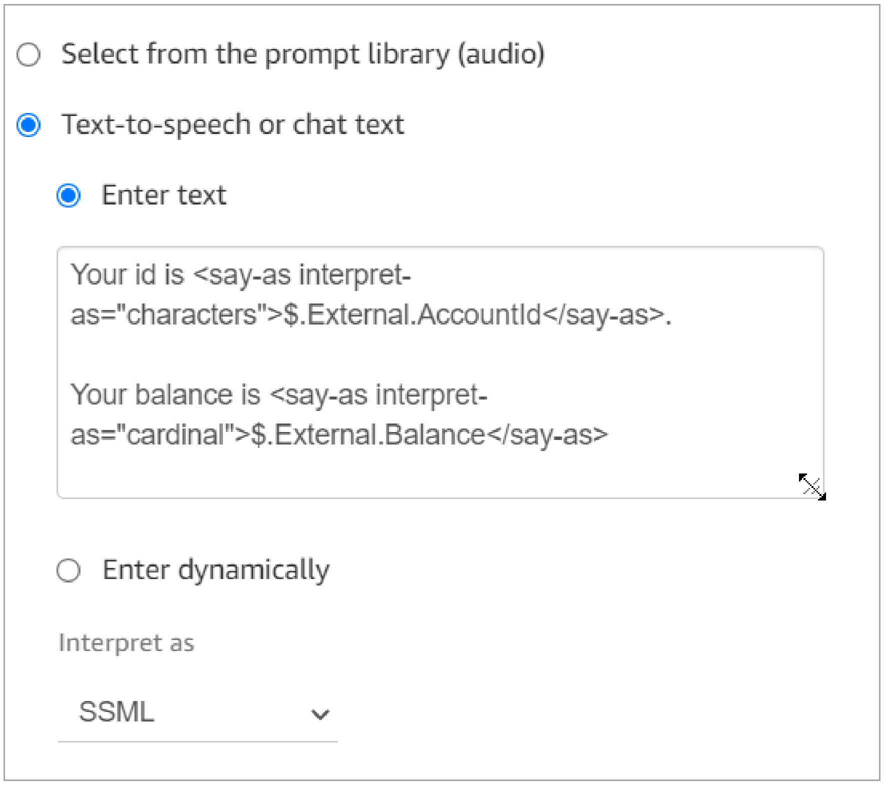
Consume the Lambda function response

There are two ways to use the function response in your 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.

1. Access variables directly

If you access the variables directly, you can use them in contact flow blocks, but they are not included in contact records. 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
```



○ Select from the prompt library (audio)

● Text-to-speech or chat text

● Enter text

Your id is <say-as interpret-as="characters">$.External.AccountId</say-as>.

Your balance is <say-as interpret-as="cardinal">$.External.Balance</say-as>

○ Enter dynamically

Interpret as

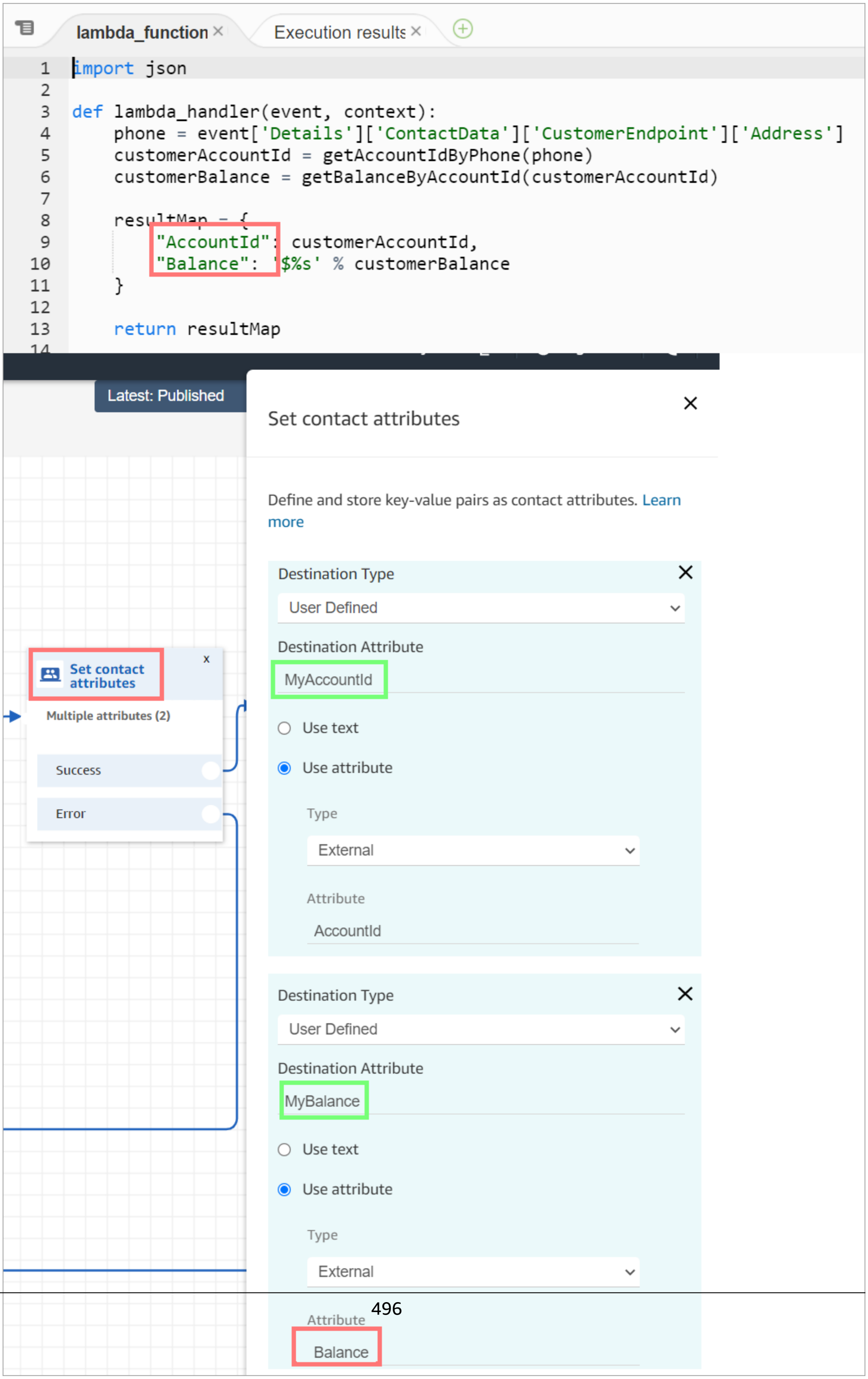
SSML

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

2. Store variables as contact attributes

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

To store the values returned as contact attributes and then reference them, use a **Set contact attributes** block in your contact flow after the **Invoke AWS Lambda function** block. Choose **Use attribute**, **External** for the **Type**. Following the example we're using, set **Destination Attribute** to `MyAccountId`, and set the **attribute** to `AccountId`, and do the same for `MyBalance` and **Balance**.



```
import json

def lambda_handler(event, context):
    phone = event['Details']['ContactData']['CustomerEndpoint']['Address']
    customerAccountId = getAccountIdByPhone(phone)
    customerBalance = getBalanceByAccountId(customerAccountId)

    resultMap = {
        "AccountId": customerAccountId,
        "Balance": '$%s' % customerBalance
    }

    return resultMap
```

Set contact attributes

Define and store key-value pairs as contact attributes. Learn more

Destination Type: User Defined

Destination Attribute: MyAccountId

○ Use text

● Use attribute

Type: External

Attribute: AccountId

Destination Type: User Defined

Destination Attribute: MyBalance

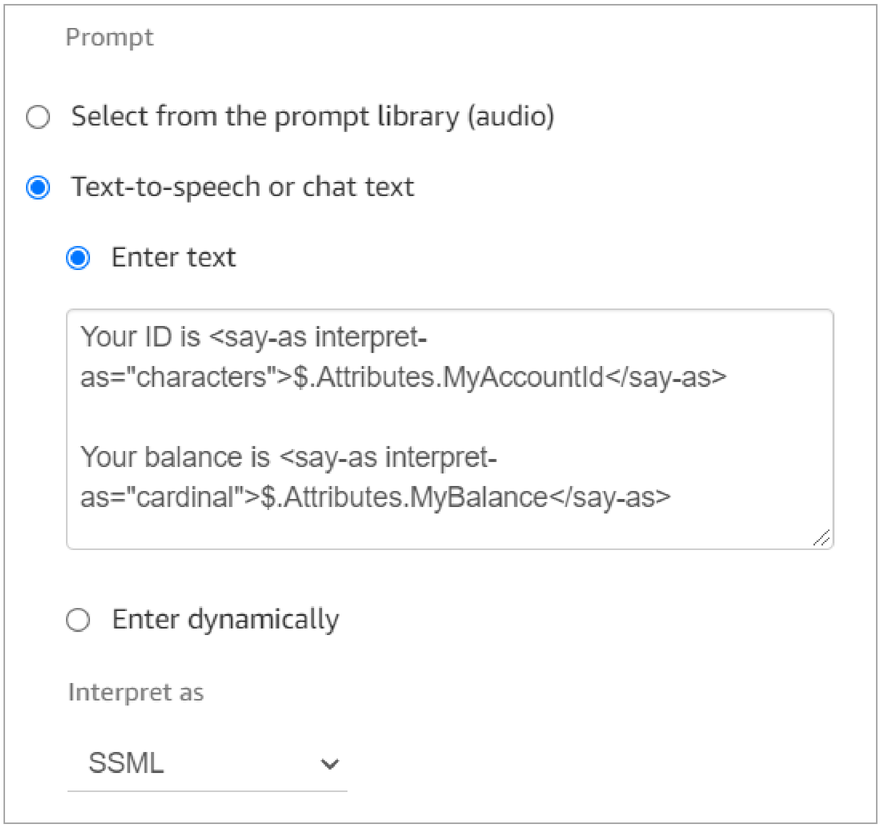
○ Use text

● Use attribute

Type: External

Attribute: Balance

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**.



Prompt

○ Select from the prompt library (audio)

● Text-to-speech or chat text

● Enter text

Your ID is <say-as interpret-as="characters">$.Attributes.MyAccountId</say-as>

Your balance is <say-as interpret-as="cardinal">$.Attributes.MyBalance</say-as>

○ Enter dynamically

Interpret as

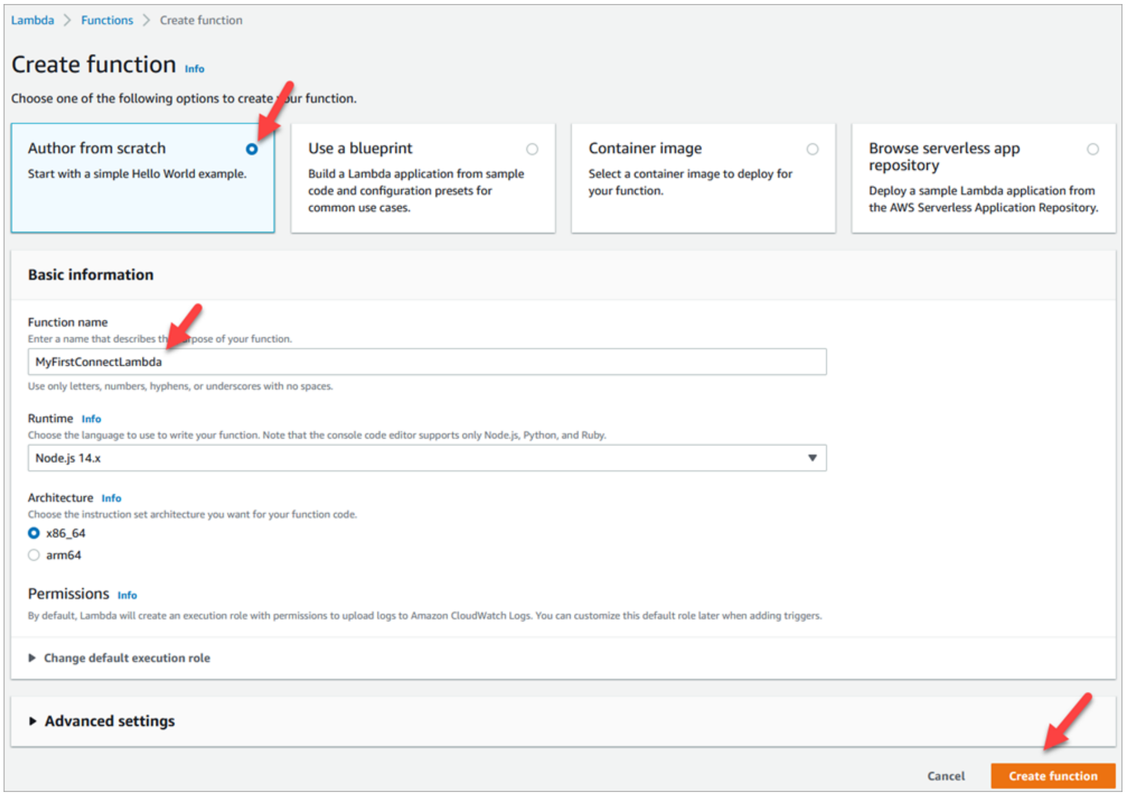
SSML

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

Tutorial: Create a Lambda function and invoke in a flow

Step 1: Create the Lambda example

1. Sign in to the AWS Management Console and open the AWS Lambda console at https://console.aws.amazon.com/lambda/.
2. In AWS Lambda, choose **Create function**.
3. Choose **Author from scratch**, if it's not selected already. Under **Basic information**, for **Function name**, enter **MyFirstConnectLambda**. For all other options, accept the defaults.



Create function Info

Choose one of the following options to create your function.

- ● Author from scratch — Start with a simple Hello World example.
- ○ Use a blueprint — Build a Lambda application from sample code and configuration presets for common use cases.
- ○ Container image — Select a container image to deploy for your function.
- ○ Browse serverless app repository — Deploy a sample Lambda application from the AWS Serverless Application Repository.

Basic information

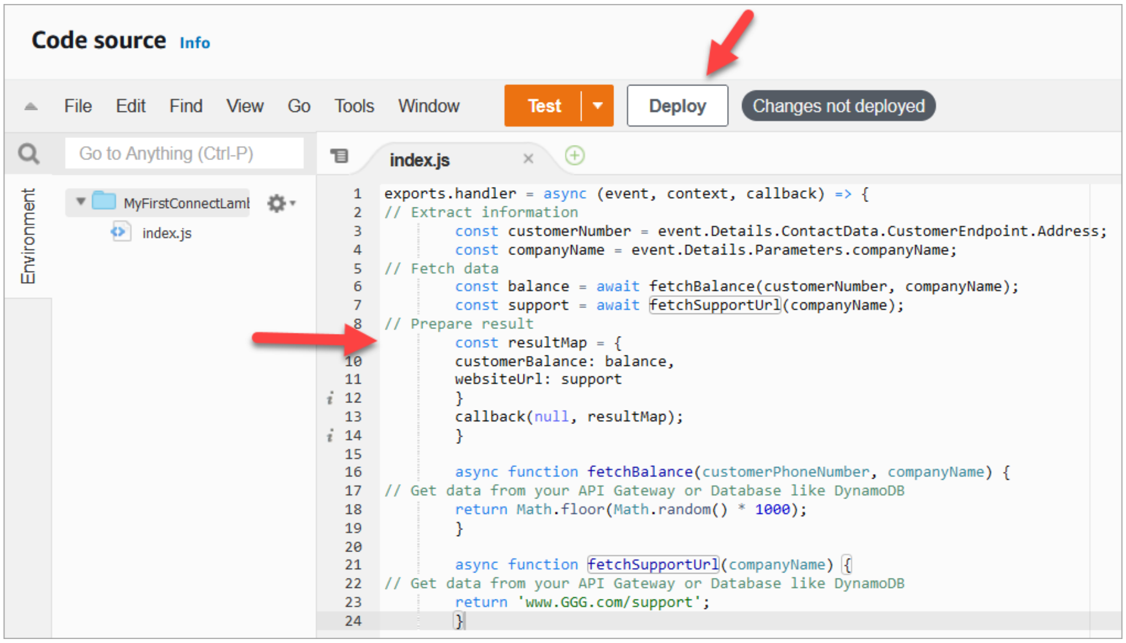
Function name
Enter a name that describes the purpose of your function.
MyFirstConnectLambda
Use only letters, numbers, hyphens, or underscores with no spaces.

Runtime Info
Choose the language to use to write your function. Note that the console code editor supports only Node.js, Python, and Ruby.
Node.js 14.x

Architecture Info
Choose the instruction set architecture you want for your function code.
● x86_64
○ arm64

Permissions Info
By default, Lambda will create an execution role with permissions to upload logs to Amazon CloudWatch Logs. You can customize this default role later when adding triggers.

4. Choose **Create function**.
5. In the **Code source** box, in the **index.js** tab, delete the template code from the code editor.
6. Copy and paste the following code into the code editor as shown in the following image:



```
exports.handler = async (event, context, callback) => {
// Extract information
        const customerNumber = event.Details.ContactData.CustomerEndpoint.Address;
        const companyName = event.Details.Parameters.companyName;
// Fetch data
        const balance = await fetchBalance(customerNumber, companyName);
        const support = await fetchSupportUrl(companyName);
// Prepare result
        const resultMap = {
        customerBalance: balance,
        websiteUrl: support
        }
        callback(null, resultMap);
        }

        async function fetchBalance(customerPhoneNumber, companyName) {
// Get data from your API Gateway or Database like DynamoDB
        return Math.floor(Math.random() * 1000);
        }

        async function fetchSupportUrl(companyName) {
// Get data from your API Gateway or Database like DynamoDB
        return 'www.GGG.com/support';
        }
```

```
exports.handler = async (event, context, callback) => {
// Extract information
        const customerNumber = event.Details.ContactData.CustomerEndpoint.Address;
        const companyName = event.Details.Parameters.companyName;
// Fetch data
        const balance = await fetchBalance(customerNumber, companyName);
        const support = await fetchSupportUrl(companyName);
// Prepare result
        const resultMap = {
        customerBalance: balance,
        websiteUrl: support
        }
        callback(null, resultMap);
        }

        async function fetchBalance(customerPhoneNumber, companyName) {
// Get data from your API Gateway or Database like DynamoDB
        return Math.floor(Math.random() * 1000);
        }

        async function fetchSupportUrl(companyName) {
// Get data from your API Gateway or Database like DynamoDB
        return 'www.GGG.com/support';
        }
```

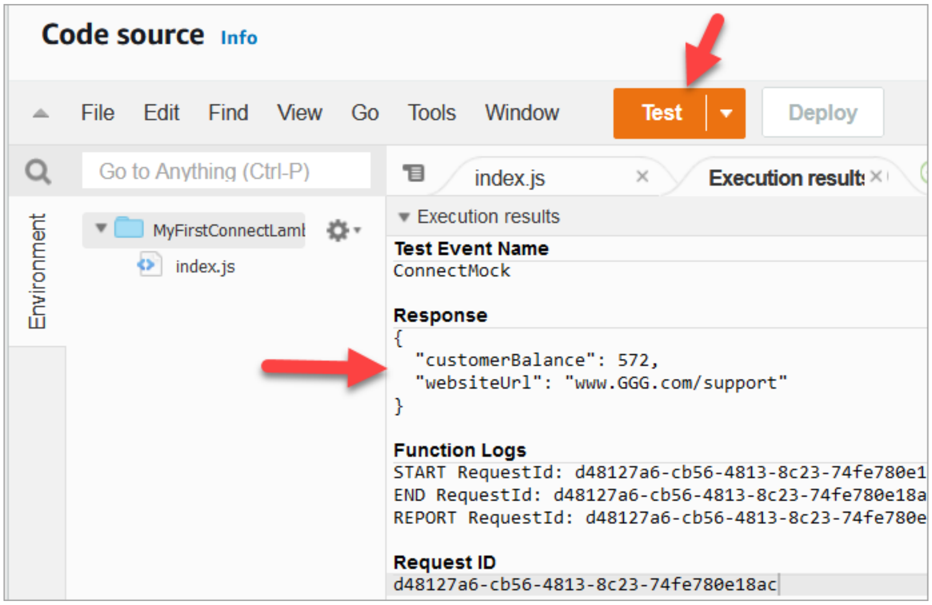
This code is going to generate a random result for the customerBalance.

7. Choose **Deploy**.
8. After you choose **Deploy**, choose **Test** to launch the test editor.
9. In the **Configure test event** dialog box, select **Create new event**. For **Event name**, enter **ConnectMock** as the test name.
10. In the **Event JSON** box, delete the sample code and enter the following code instead.

```
{
"Details": {
"ContactData": {
    "Attributes": {},
    "Channel": "VOICE",
    "ContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
    "CustomerEndpoint": {
    "Address": "+1234567890",
    "Type": "TELEPHONE_NUMBER"
    },
"InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
"InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
"InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/c8c0e68d-2200-4265-82c0-
XXXXXXXXXX",
"PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
"Queue": {
    "ARN": "arn:aws:connect:eu-west-2:111111111111:instance/cccccccc-bbbb-dddd-eeee-
ffffffffffff/queue/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee",
    "Name": "PasswordReset"
  },
"SystemEndpoint": {
    "Address": "+1234567890",
    "Type": "TELEPHONE_NUMBER"
    }
},
"Parameters": {
    "companyName": "GGG"
    }
},
"Name": "ContactFlowEvent"
}
```

11. Choose **Save**.

12. Choose **Test**. You should see the following something similar to the following image:



Test Event Name
```
ConnectMock
```

Response
```
{
  "customerBalance": 572,
  "websiteUrl": "www.GGG.com/support"
}
```

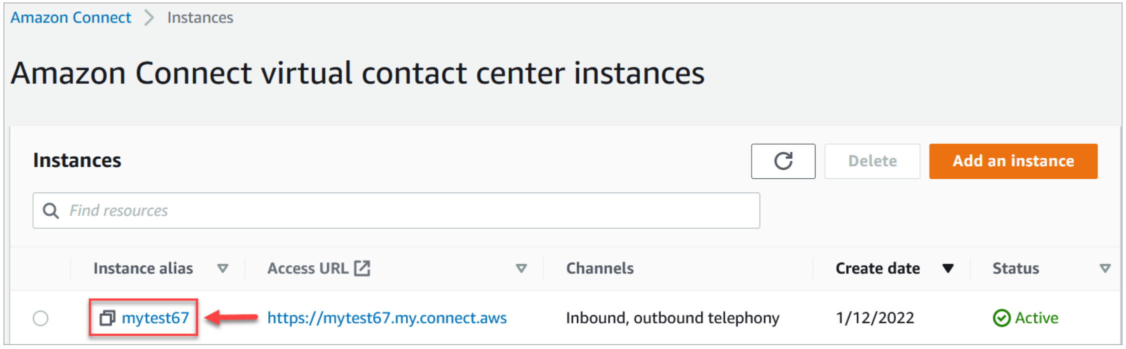
Function Logs
```
START RequestId: d48127a6-cb56-4813-8c23-74fe780e1
END RequestId: d48127a6-cb56-4813-8c23-74fe780e18a
REPORT RequestId: d48127a6-cb56-4813-8c23-74fe780e
```

Request ID
```
d48127a6-cb56-4813-8c23-74fe780e18ac
```

Your balance will be different. The code generates a random number.

Step 2: Add your Lambda to Amazon Connect

1. Go to the Amazon Connect console, at https://console.aws.amazon.com/connect/.
2. Choose your Amazon Connect instance alias.

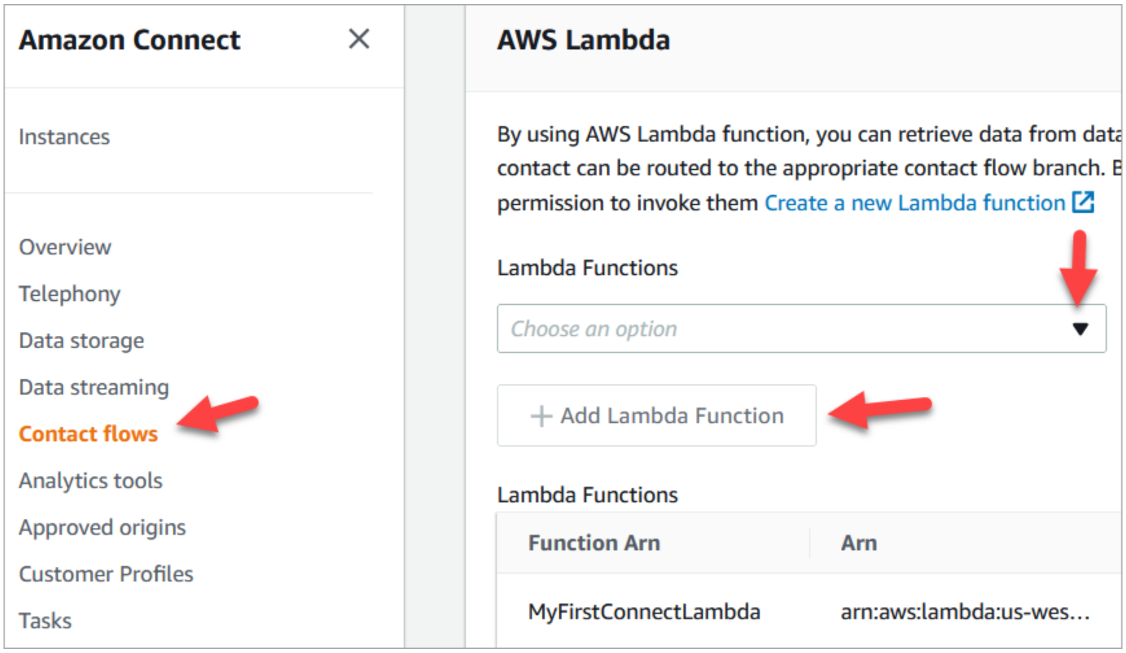


Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. On the navigation menu, choose **Contact flows**.
4. In the AWS Lambda section, use the **Lambda Functions** dropdown box to select **MyFirstConnectLambda**.



Amazon Connect ✕

Instances

Overview

Telephony

Data storage

Data streaming

Contact flows

Analytics tools

Approved origins

Customer Profiles

Tasks

AWS Lambda

By using AWS Lambda function, you can retrieve data from data
contact can be routed to the appropriate contact flow branch. E
permission to invoke them Create a new Lambda function

Lambda Functions

Choose an option ▼

+ Add Lambda Function

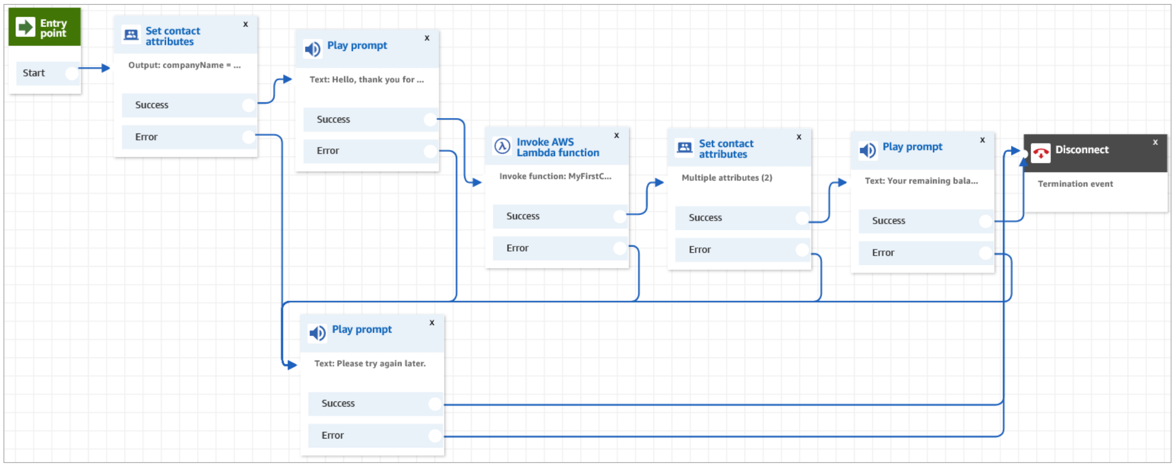
Lambda Functions

Function Arn	Arn
MyFirstConnectLambda	arn:aws:lambda:us-wes...

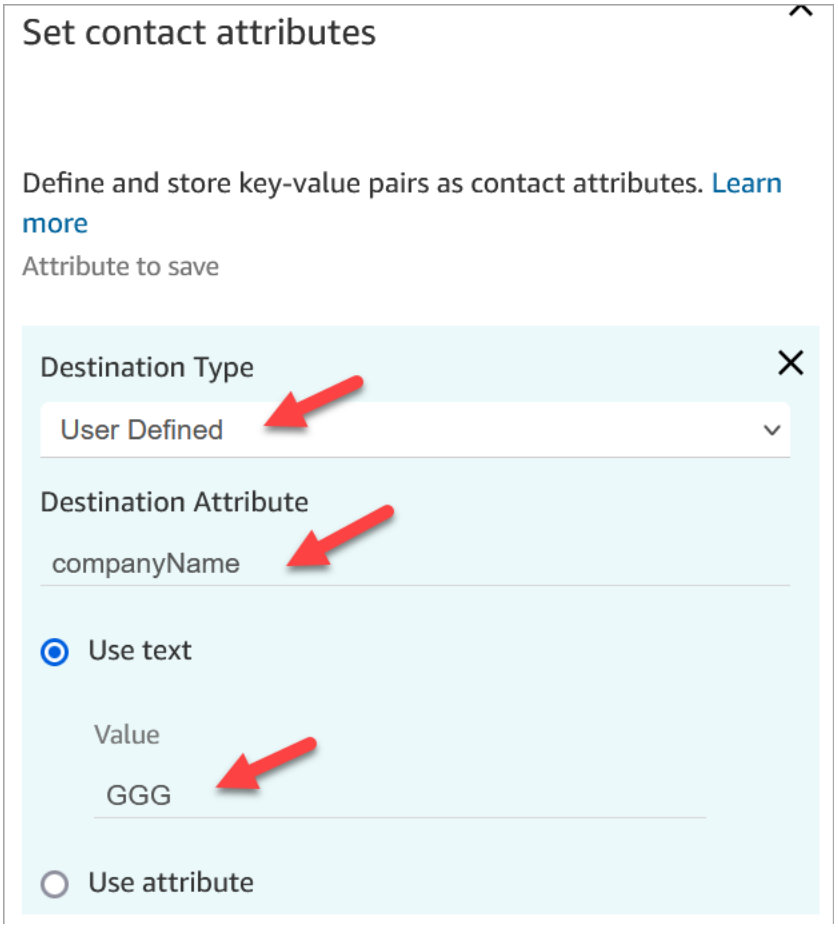
5. Choose **Add Lambda Function**.

Step 3: Create the contact flow

The following image is an example of the contact flow you are going to build using the steps in this procedure.



1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. On the navigation menu, go to **Routing**, **Contact flows**, **Create a contact flow**.
3. Drag a Set contact attributes (p. 399) block onto the grid, and configure its properties page shown in the following image:



Set contact attributes

Define and store key-value pairs as contact attributes. Learn more

Attribute to save

Destination Type

User Defined

Destination Attribute

companyName

● Use text

Value

GGG

○ Use attribute

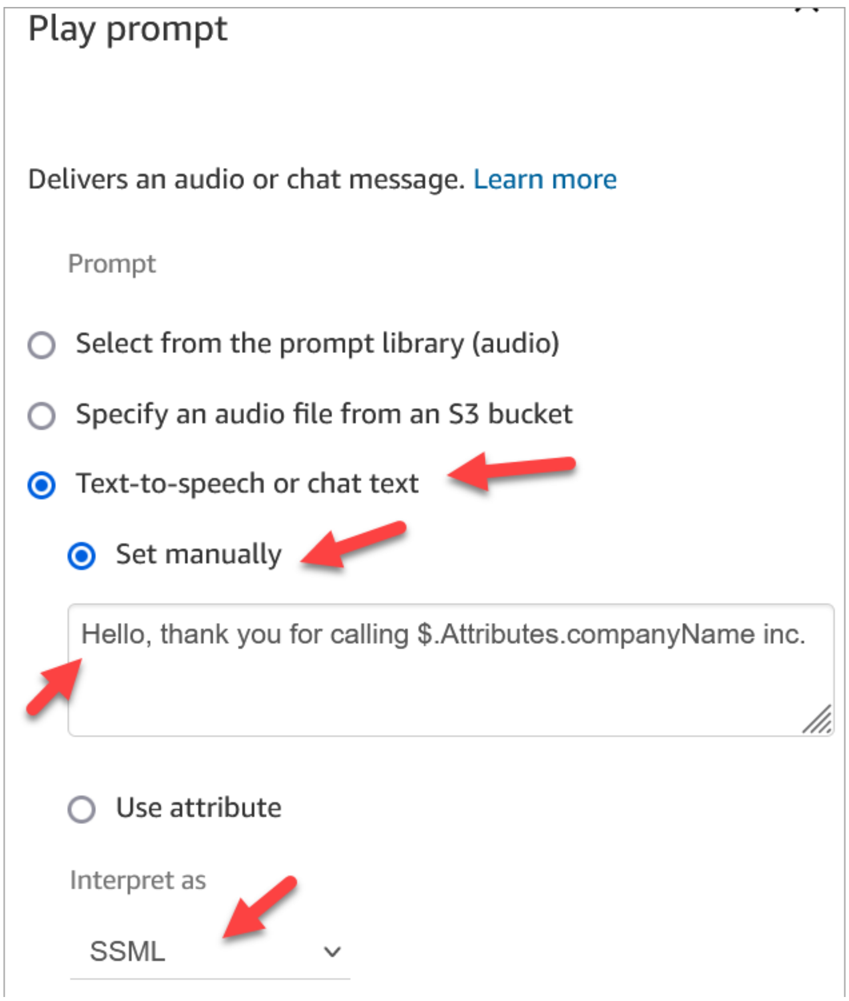
a. **Destination Type** = **User defined**.

b. **Destination Attribute** = **companyName**.

c. Choose **Use text**. **Value** = **GGG**.

d. Choose **Save**.

4. Drag a Play prompt (p. 393) block onto the grid, and configure its properties page as shown in the following image:



Play prompt

Delivers an audio or chat message. Learn more

Prompt

○ Select from the prompt library (audio)

○ Specify an audio file from an S3 bucket

● Text-to-speech or chat text

● Set manually

Hello, thank you for calling $.Attributes.companyName inc.

○ Use attribute

Interpret as

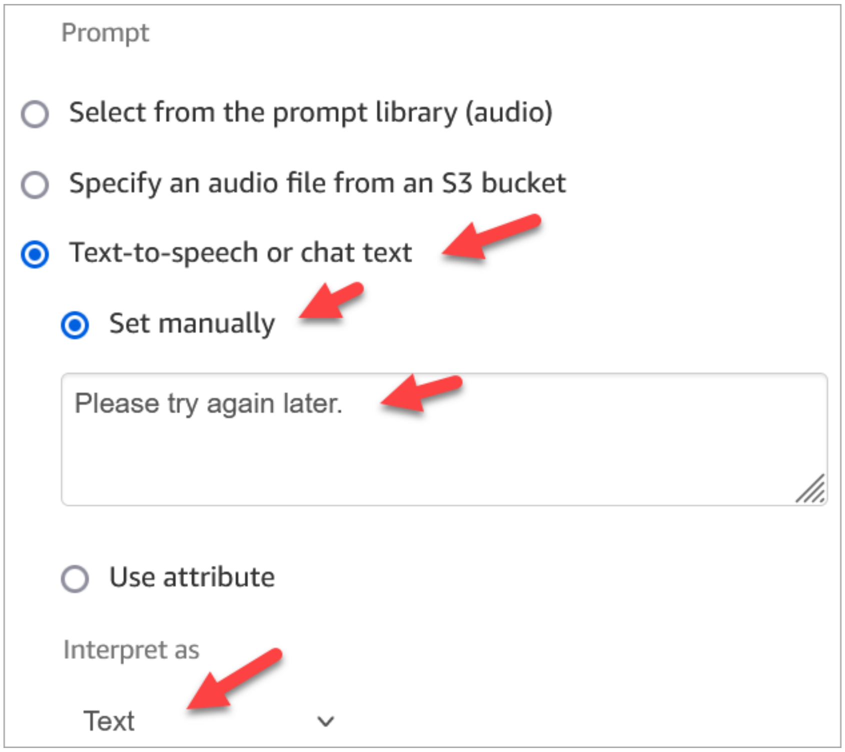
SSML

a. Choose **Text-to-speech or chat text**, **Set manually**, and set **Interpret as** to **SSML**. Enter the following text in the box for the text to be spoken:

```
Hello, thank you for calling $.Attributes.companyName inc.
```

b. Choose **Save**.

5. Drag another Play prompt (p. 393) block onto the grid, and configure its properties page as shown in the following image:



Prompt

○ Select from the prompt library (audio)

○ Specify an audio file from an S3 bucket

● Text-to-speech or chat text

● Set manually

Please try again later.

○ Use attribute

Interpret as

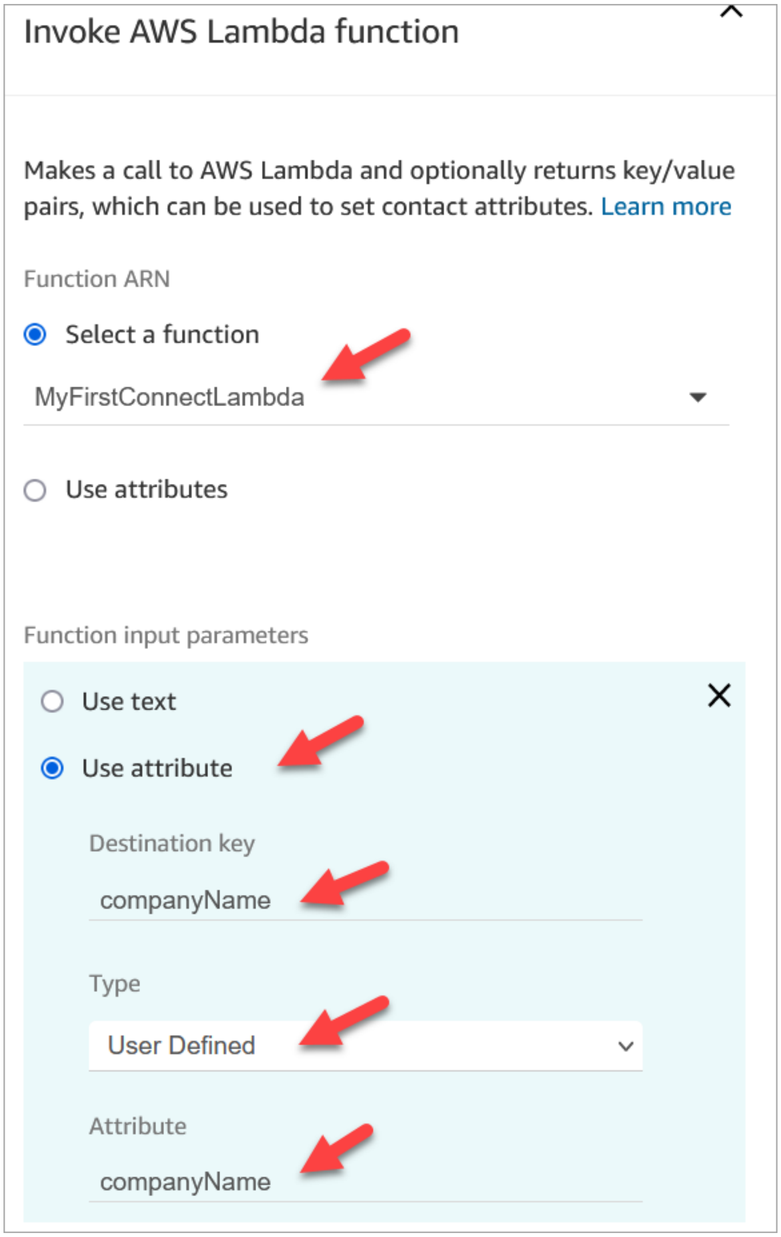
Text

a. Choose **Text-to-speech or chat text**, **Set manually**, and set **Interpret as** to **Text**. Enter the following text in the box for the text to be spoken:

```
Please try again later.
```

b. Choose **Save**.

6. Drag a Invoke AWS Lambda function (p. 385) block onto the grid, and configure its properties page as shown in the following image:



Invoke AWS Lambda function

Makes a call to AWS Lambda and optionally returns key/value pairs, which can be used to set contact attributes. Learn more

Function ARN

● Select a function

MyFirstConnectLambda

○ Use attributes

Function input parameters

○ Use text

● Use attribute

Destination key: companyName

Type: User Defined

Attribute: companyName

a. For **Select a function**, choose **MyFirstConnectLambda** from the dropdown.

b. Choose **Add a parameter**. In **Function input parameters**, choose **Use attribute**.

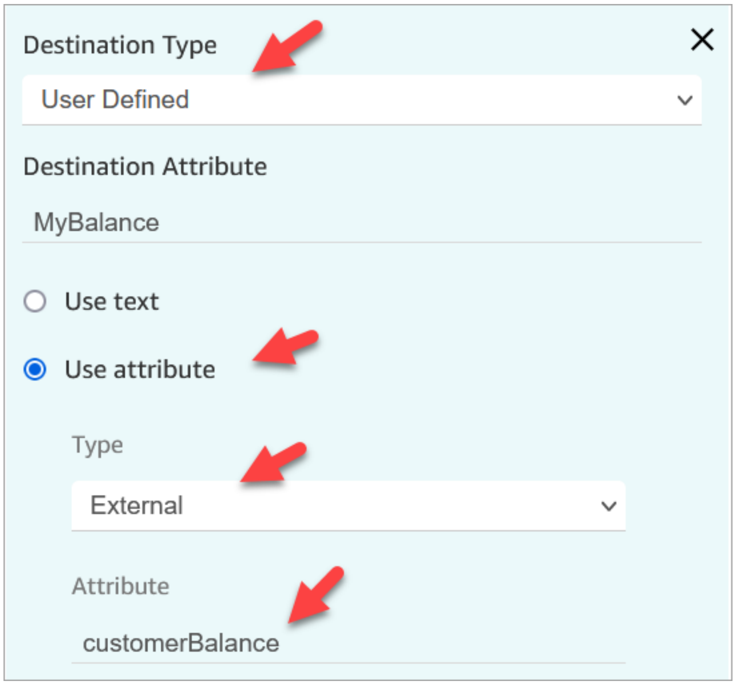
c. For **Destination key**, enter **companyName**. (This is sent to Lambda.)

d. For **Type**, select **User Defined**.

e. For **Attribute**, enter **companyName**.

f. Choose **Save**.

7. Drag a Set contact attributes (p. 399) block onto the grid, and configure its properties page as shown in the following images:



Destination Type

User Defined

Destination Attribute

MyBalance

○ Use text

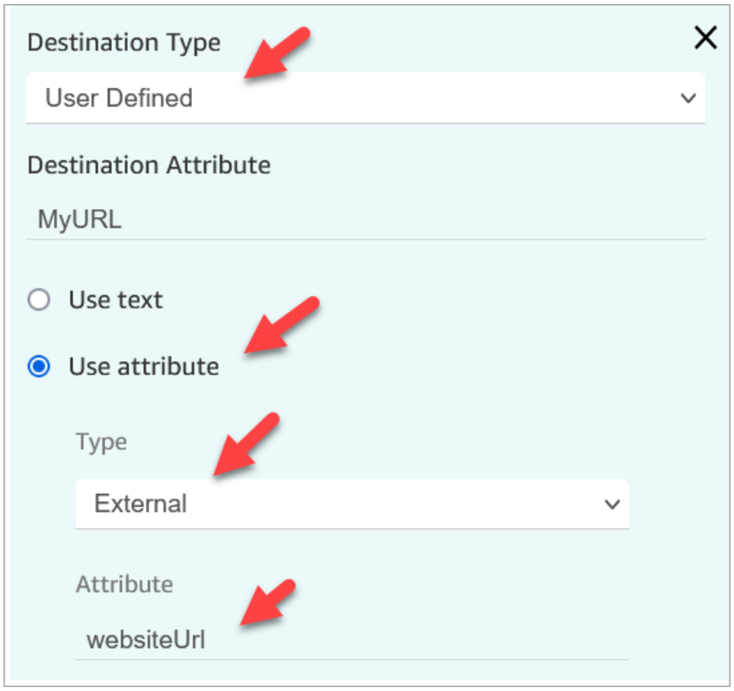
● Use attribute

Type

External

Attribute

customerBalance



Destination Type

User Defined

Destination Attribute

MyURL

○ Use text

● Use attribute

Type

External

Attribute

websiteUrl

a. **Destination Type** = **User Defined**. **Destination Attribute** = **MyBalance**.

b. Choose **Use attribute**.

c. **Type** = **External**.

d. **Attribute** = **customerBalance**. This is the result from Lambda.

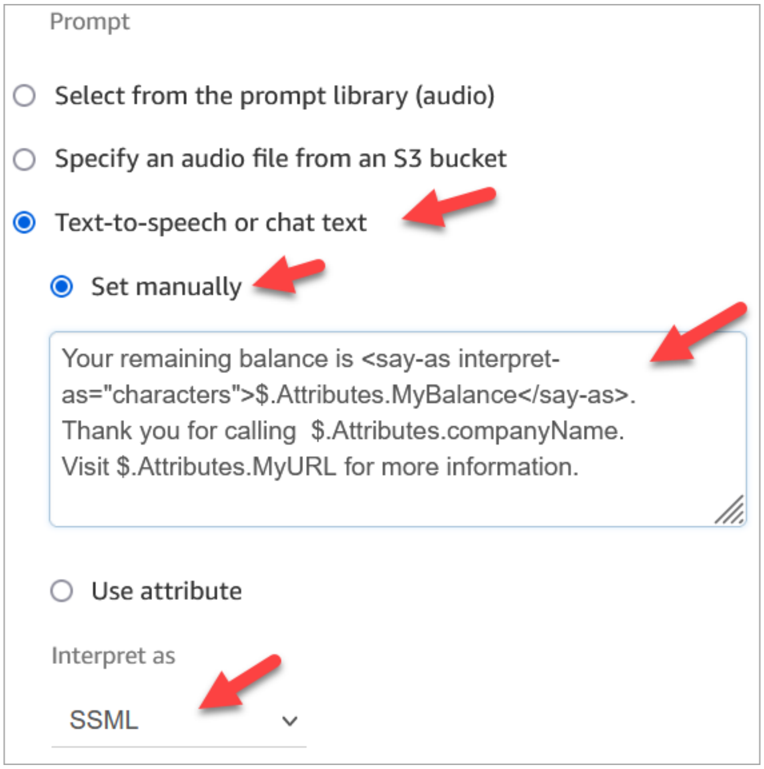
e. Choose **Add another attribute**.

f. **Destination Attribute** = **MyURL**.

g. Select **Use attribute**. **Type** =**External**.

   h. **Attribute** = **websiteUrl**. This is the result from Lambda.
   i. Choose **Save**.

8. Drag a Play prompt (p. 393) block onto the grid, and configure its properties page as shown in the following image:



Prompt

○ Select from the prompt library (audio)

○ Specify an audio file from an S3 bucket

● Text-to-speech or chat text

● Set manually

Your remaining balance is <say-as interpret-as="characters">$.Attributes.MyBalance</say-as>. Thank you for calling $.Attributes.companyName. Visit $.Attributes.MyURL for more information.

○ Use attribute

Interpret as

SSML

   a. Choose **Text-to-speech or chat text**, and set **Interpret as** to **SSML**. Enter the following text in the box:

```
Your remaining balance is <say-as interpret-as="characters">
$.Attributes.MyBalance</say-as>.

Thank you for calling $.Attributes.companyName.

Visit $.Attributes.MyURL for more information.
```

   b. Choose **Save**.

9. Drag a Disconnect / hang up (p. 362) block onto the grid.
10. Connect the all blocks so your flow looks like the image shown at the top of this procedure.
11. Enter **MyFirstConnectFlow** as the name, and then choose **Publish**.
12. On the navigation menu, go to **Channels**, **Phone numbers**.
13. Select your phone number.
14. Select **MyFirstConnectFlow** and choose **Save**.

Now try it out. Call the number. You should hear a greeting message, your balance, and the website to visit.

Encrypt customer input

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

When configuring Amazon Connect, you first provide the public key. This is the key used when encrypting data. Later, you provide the X.509 certificate, which includes a signature that proves you possess the private key.

In a contact flow that collects data, you provide an X.509 certificate to encrypt data that's captured using the **Stored customer input** system attribute. You must upload the key in `.pem` format to use this feature. The encryption key is used to verify the signature of the certificate used within the contact flow.

> **Note**
> You can have up to two encryption keys active at one time to facilitate rotation.

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

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

- Configure Amazon Connect to collect a credit card number.
- Encrypt the credit card digits.
- Send it to our backend AWS Lambda for decryption, using the customer supplied decryption key.

It provides two commands using OpenSSL:

- One to generate an RSA key pair and a self-signed X.509 certificate
- Another to extract the public key from the RSA key pair

How to decrypt data encrypted by Amazon Connect

The following code sample shows how to decrypt data using the AWS Encryption SDK.

```
package com.amazonaws;

import com.amazonaws.encryptionsdk.AwsCrypto;
import com.amazonaws.encryptionsdk.CryptoResult;
import com.amazonaws.encryptionsdk.jce.JceMasterKey;
import org.bouncycastle.jce.provider.BouncyCastleProvider;

import java.io.IOException;
import java.nio.charset.Charset;
import java.nio.file.Files;
import java.nio.file.Paths;
import java.security.GeneralSecurityException;
import java.security.KeyFactory;
import java.security.Security;
import java.security.interfaces.RSAPrivateKey;
import java.security.spec.PKCS8EncodedKeySpec;
import java.util.Base64;

public class AmazonConnectDecryptionSample {

    // The Provider 'AmazonConnect' is used during encryption, this must be used during
 decryption for key
```

```
    // to be found
    private static final String PROVIDER = "AmazonConnect";

    // The wrapping algorithm used during encryption
    private static final String WRAPPING_ALGORITHM = "RSA/ECB/
OAEPWithSHA-512AndMGF1Padding";

    /**
     * This sample show how to decrypt data encrypted by Amazon Connect.
     * To use, provide the following command line arguments: [path-to-private-key] [key-id]
 [cyphertext]
     * Where:
     *  path-to-private-key is a file containing the PEM encoded private key to use for
 decryption
     *  key-id is the key-id specified during encryption in your contact flow
     *  cyphertext is the result of the encryption operation from Amazon Connect
     */
    public static void main(String[] args) throws IOException, GeneralSecurityException {
        String privateKeyFile = args[0]; // path to PEM encoded private key to use for
 decryption
        String keyId = args[1]; // this is the id used for key in your contact flow
        String cypherText = args[2]; // the result from contact flow

        Security.addProvider(new BouncyCastleProvider());

        // read the private key from file
        String privateKeyPem = new String(Files.readAllBytes(Paths.get(privateKeyFile)),
 Charset.forName("UTF-8"));
        RSAPrivateKey privateKey =  getPrivateKey(privateKeyPem);

        AwsCrypto awsCrypto = new AwsCrypto();
        JceMasterKey decMasterKey =
                JceMasterKey.getInstance(null,privateKey, PROVIDER, keyId,
 WRAPPING_ALGORITHM);
        CryptoResult<String, JceMasterKey> result = awsCrypto.decryptString(decMasterKey,
 cypherText);

        System.out.println("Decrypted: " + result.getResult());
    }

    public static RSAPrivateKey getPrivateKey(String privateKeyPem) throws IOException,
 GeneralSecurityException {
        String privateKeyBase64 = privateKeyPem
                .replace("-----BEGIN RSA PRIVATE KEY-----\n", "")
                .replace("-----END RSA PRIVATE KEY-----", "")
                .replaceAll("\n", "");
        byte[] decoded = Base64.getDecoder().decode(privateKeyBase64);
        KeyFactory kf = KeyFactory.getInstance("RSA");
        PKCS8EncodedKeySpec keySpec = new PKCS8EncodedKeySpec(decoded);
        RSAPrivateKey privKey = (RSAPrivateKey) kf.generatePrivate(keySpec);
        return privKey;
    }
}
```

Track events as customers interact with contact flows

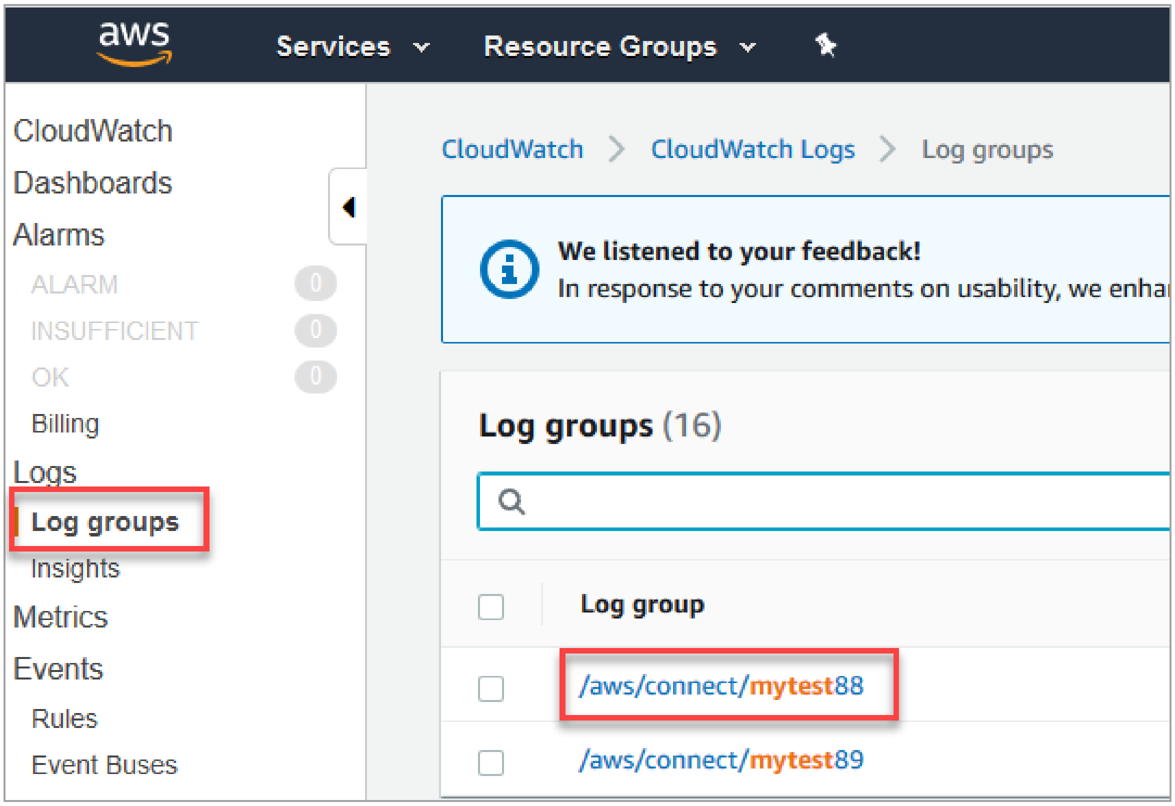
Amazon Connect contact flow logs provide you with real-time details about events in your contact flows as customers interact with them. You can also use contact flow logs to help debug your contact flows as you are creating them. If needed, you can always roll back (p. 453)to a previous version of a contact flow.

Contents

Contact flow logs stored in an Amazon CloudWatch log group

Contact flow logs are stored in an Amazon CloudWatch log group, in the same region as your Amazon Connect instance. This log group is created automatically when Enable contact flow logging (p. 511) is turned on for your instance.

For example, the following image shows the CloudWatch log groups for two test instances.



We listened to your feedback!
In response to your comments on usability, we enha

/aws/connect/mytest88
/aws/connect/mytest89

A log entry added as each block in your contact flow is triggered. You can configure CloudWatch to send alerts when unexpected events occur during active contact flows.

What happens if my log group is deleted? You need to manually re-create the CloudWatch log group. Otherwise, Amazon Connect won't publish more logs.

Pricing for contact flow logging

You are not charged for generating contact flow logs, but you are charged for using CloudWatch for generating and storing the logs. Free tier customers are charged only for usage that exceeds service quotas. For details about Amazon CloudWatch pricing, see Amazon CloudWatch Pricing.

Enable contact flow logs

> **Tip**
> Amazon Connect delivers contact flow logs at least once. They may be delivered again for multiple reasons. For example, a service retry due to an unavoidable failure.

Step 1: Enable logging for your instance

By default when you create a new Amazon Connect instance, an Amazon CloudWatch log group is created automatically to store the logs for your instance.

Use the following procedure to check that logging is enabled for your instance.

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

Step 2: Add the Set logging behavior block

Logs are generated only for contact flows that include a Set logging behavior (p. 407) block with logging set to enabled.

You control which flows, or parts of flows, logs are generated for by including multiple **Set logging behavior** blocks and configuring them as needed.

When you use a **Set logging behavior** block to enable or disable logging for a flow, logging is also enabled or disabled for any subsequent flow that a contact is transferred to, even if the flow does not include a **Set logging behavior** block. To avoid logging that persists between flows, enable or disable a **Set logging behavior** block as needed for that specific flow.

To enable or disable contact flow logs for a contact flow

1. Add a Set logging behavior (p. 407) block and connect it to another block in the flow.
2. Open the properties for the block. Choose **Enable** or **Disable**.
3. Choose **Save**.
4. If you add a **Set logging behavior** block to a contact flow that is already published, you must publish it again to start generating logs for it.

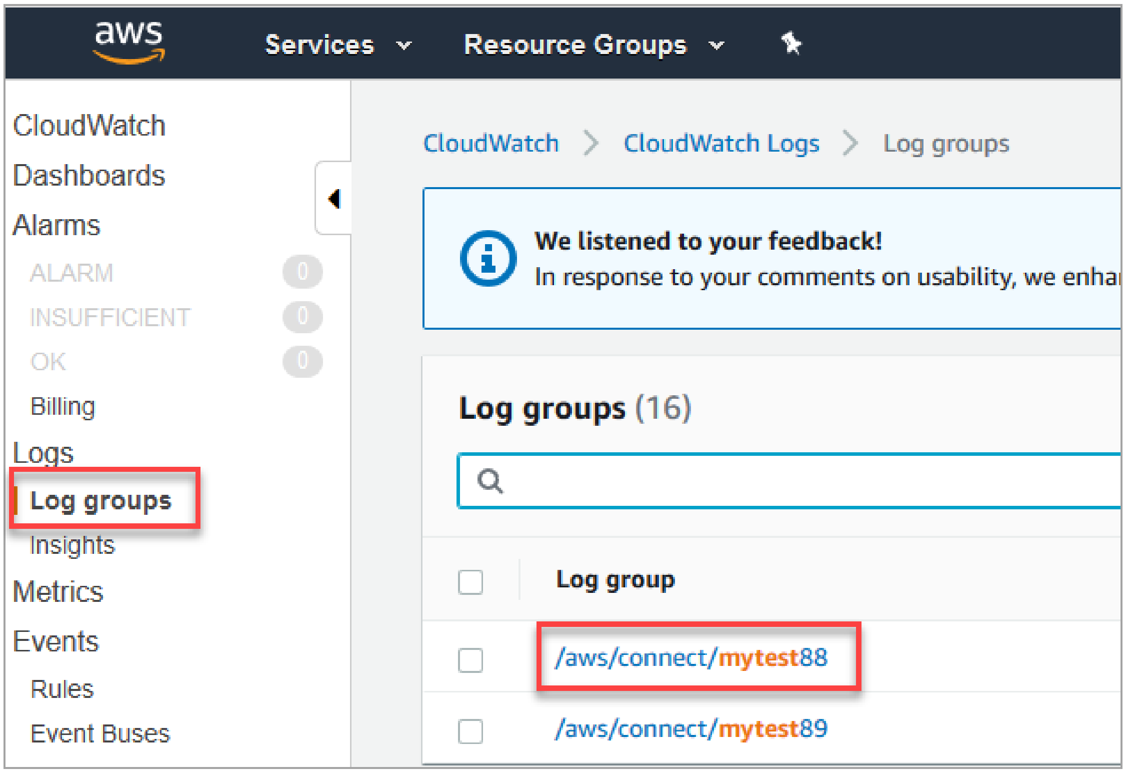
Search contact flow logs

Before you can search contact flow logs, you must first enable contact flow logging (p. 511).

Logs will be created for conversations that occur after logging is enabled.

To search contact flow logs

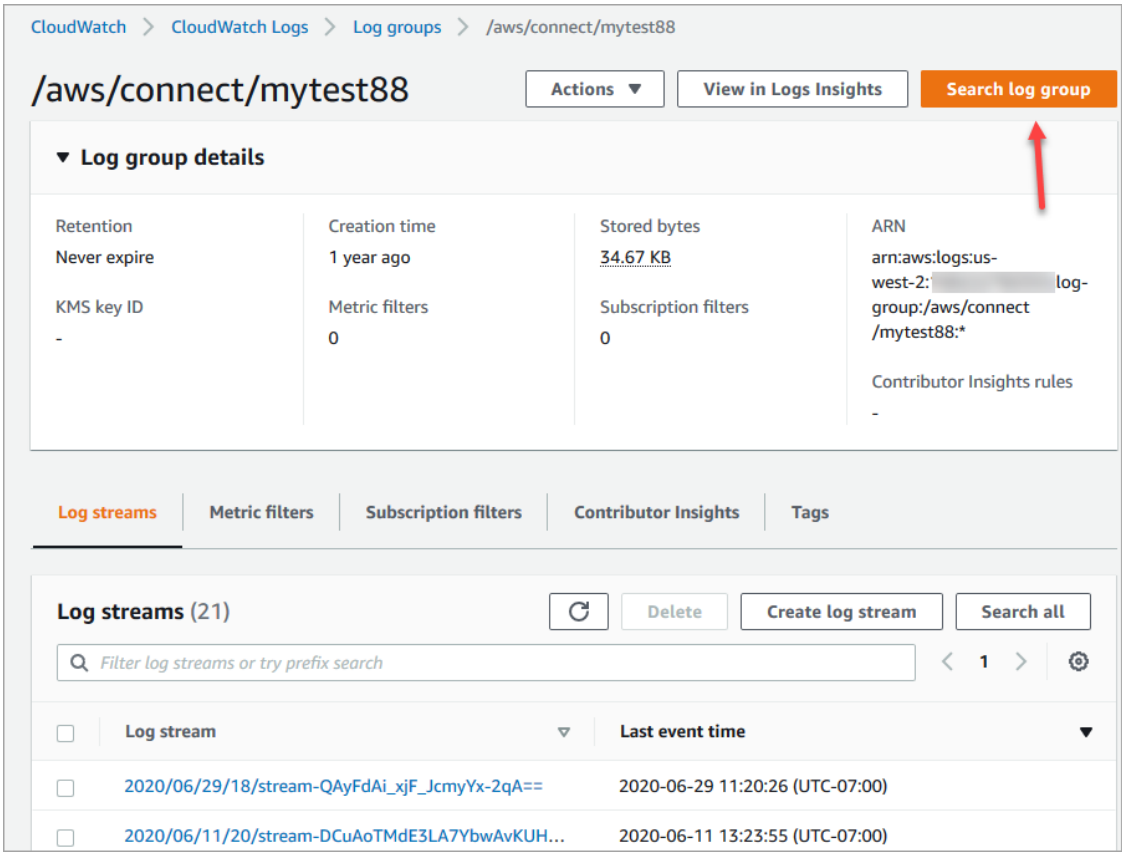
1. Open Amazon CloudWatch console, go to **Logs**, **Log groups**. The following image shows a sample log group named **mytest88**.



2. Choose the log group for your instance.

   A list of log streams will be displayed.

3. To search all the log streams in the instance, choose **Search log group**, as shown in the following image.

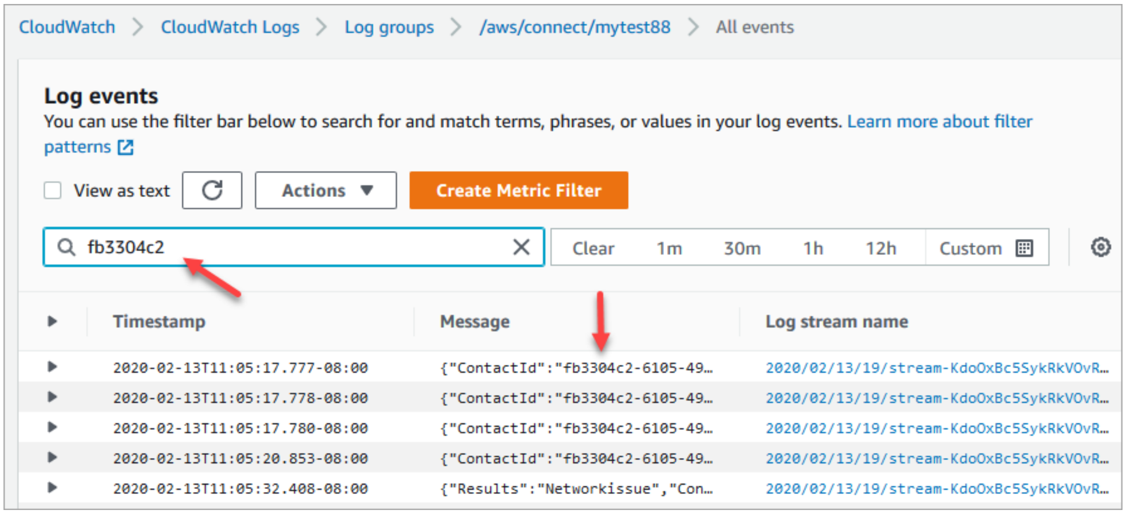


Retention	Creation time	Stored bytes	ARN
Never expire	1 year ago	34.67 KB	arn:aws:logs:us-west-2:[redacted]log-group:/aws/connect/mytest88:*
KMS key ID	Metric filters	Subscription filters	Contributor Insights rules
-	0	0	-

Log streams (21)

□	Log stream	Last event time
□	2020/06/29/18/stream-QAyFdAi_xjF_JcmyYx-2qA==	2020-06-29 11:20:26 (UTC-07:00)
□	2020/06/11/20/stream-DCuAoTMdE3LA7YbwAvKUH...	2020-06-11 13:23:55 (UTC-07:00)

4. In the search box, enter the string you want to search for, for example, all or a portion of the contact ID.
5. After a couple of moments (longer depending on how big your log is), Amazon CloudWatch returns results. The following image shows a sample contact ID **fb3304c2**, and the result.


CloudWatch > CloudWatch Logs > Log groups > /aws/connect/mytest88 > All events
□ View as text
Actions ▼
Create Metric Filter
Clear
1m
30m
1h
12h
Custom

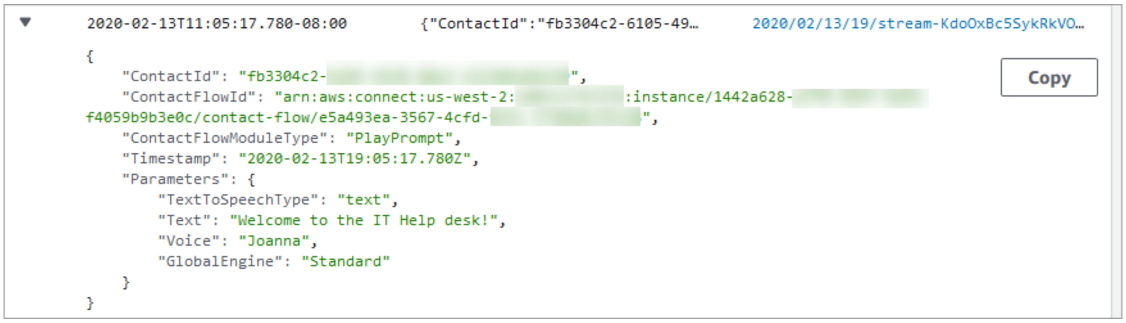
Log events

You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns

fb3304c2

	Timestamp	Message	Log stream name
▶	2020-02-13T11:05:17.777-08:00	{"ContactId":"fb3304c2-6105-49…	2020/02/13/19/stream-KdoOxBc5SykRkVOvR…
▶	2020-02-13T11:05:17.778-08:00	{"ContactId":"fb3304c2-6105-49…	2020/02/13/19/stream-KdoOxBc5SykRkVOvR…
▶	2020-02-13T11:05:17.780-08:00	{"ContactId":"fb3304c2-6105-49…	2020/02/13/19/stream-KdoOxBc5SykRkVOvR…
▶	2020-02-13T11:05:20.853-08:00	{"ContactId":"fb3304c2-6105-49…	2020/02/13/19/stream-KdoOxBc5SykRkVOvR…
▶	2020-02-13T11:05:32.408-08:00	{"Results":"Networkissue","Con…	2020/02/13/19/stream-KdoOxBc5SykRkVOvR…

6. You can open each event to see what happened. The following image shows the event for when a **Play prompt** block runs in a contact flow.



```
▼    2020-02-13T11:05:17.780-08:00      {"ContactId":"fb3304c2-6105-49…      2020/02/13/19/stream-KdoOxBc5SykRkVO…
     {
         "ContactId": "fb3304c2-[redacted]",
         "ContactFlowId": "arn:aws:connect:us-west-2:[redacted]:instance/1442a628-[redacted]
     f4059b9b3e0c/contact-flow/e5a493ea-3567-4cfd-[redacted]",
         "ContactFlowModuleType": "PlayPrompt",
         "Timestamp": "2020-02-13T19:05:17.780Z",
         "Parameters": {
             "TextToSpeechType": "text",
             "Text": "Welcome to the IT Help desk!",
             "Voice": "Joanna",
             "GlobalEngine": "Standard"
         }
     }
```

What data is gathered in contact flow logs

Log entries for contact flows include details about the block associated with the log entry, the contact ID, and the action taken after the steps in the block were completed. Any contact interaction that occurs outside of the contact flow is not logged, such as time spent in a queue or interactions with an agent.

You can set the properties of the block to disable logging during the parts of your contact flow that interact with or capture sensitive data or customers' personal information.

If you use Amazon Lex or AWS Lambda in your contact flows, the logs show the entry and exit of the contact flow going to them, and include any information about the interaction that is sent or received during entry or exit.

Because the logs also include the contact flow ID, and the contact flow ID stays the same when you change a contact flow, you can use the logs to compare the interactions with different versions of the contact flow.

The following example log entry shows a **Set working queue** block of an inbound flow.

```
{
    "ContactId": "11111111-2222-3333-4444-555555555555",
    "ContactFlowId": "arn:aws:connect:us-west-2:0123456789012:instance/
nnnnnnnnnnn-3333-4444-5555-111111111111/contact-flow/123456789000-aaaa-bbbbbbbbb-
cccccccccccc",
    "ContactFlowModuleType": "SetQueue",
    "Timestamp": "2021-04-13T00:14:31.581Z",
    "Parameters": {
        "Queue": "arn:aws:connect:us-west-2:0123456789012:instance/
nnnnnnnnnnn-3333-4444-5555-111111111111/queue/aaaaaaaa-bbbb-cccc-dddd-eeeeeeeeeeee"
    }
}
```

Track customers between contact flows

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

When a customer is transferred to a different contact flow, the ID for the contact associated with their interaction is included with the log for the new flow. You can query the logs for the contact ID to trace the customer interaction through each contact flow.

In larger, high-volume contact centers, there can be multiple streams for contact flow logs. If a contact is transferred to a different contact flow, the log may be in a different stream. To make sure that you are finding all of the log data for a specific contact, you should search for the contact ID in the entire CloudWatch log group instead of in a specific log stream.

Create alerts for contact flow log events

You can configure CloudWatch to define a filter pattern that looks for specific events in your contact flow logs and then creates an alert when an entry for that event is added to the log.

For example, you can set an alert for when a contact flow block goes down an error path as a customer interacts with the flow. Log entries are typically available in CloudWatch within a short time, giving you near real-time notification of events in contact flows.

Use Amazon Connect contact attributes

One way to make your customers feel cared for is to create personalized experiences for them in your contact center. For example, you can deliver one welcome message for customers who are using a phone and another for customers using chat. To do this, you need a way to store information about the contact and then make a decision based on the value.

Contents

What is a contact attribute?

In Amazon Connect, each interaction with a customer is a **contact**. The interaction can be a phone call (voice), a chat, or an automated interaction using an Amazon Lex bot.

Each contact can have some data that is specific to a particular interaction. This data can be accessed as a contact attribute. For example:

- The name of the customer
- The name of the agent
- The channel used for the contact, such as phone or chat
- And more

A contact attribute represents this data as a key-value pair. You might think of it as a field name together with the data entered into that field.

For example, here are a couple of key-value pairs for the customer name:

Key	Value
firstname	Jane
lastname	Doe

The advantage of contact attributes is that they enable you to store temporary information about the contact so you can use it in the contact flow.

For example, in your welcome messages, you can say their name or thank them for being a member. To do this, you need a way of retrieving data about that specific customer and using it in a contact flow.

Common use cases

Here are some common use cases for where contact attributes are used:

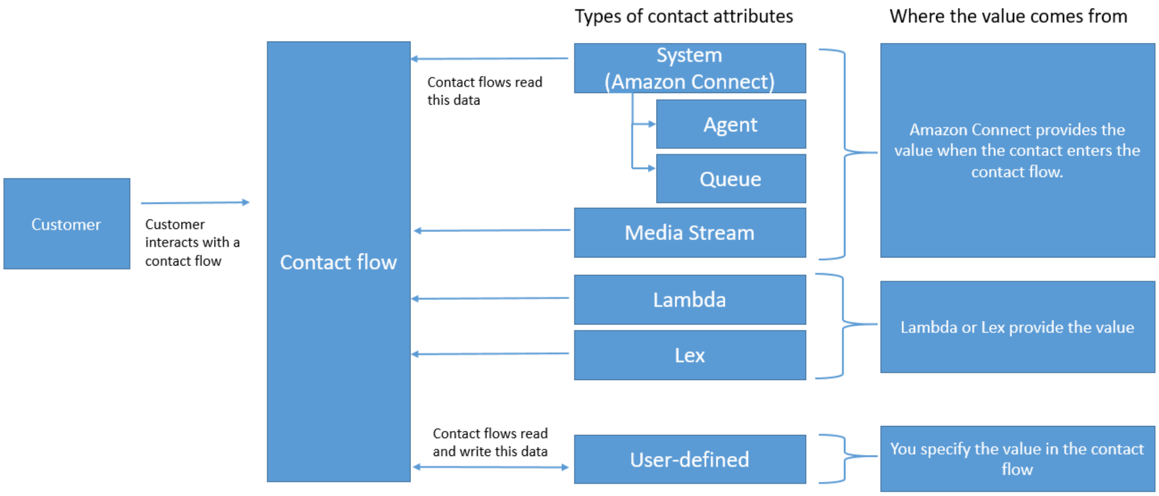
- Use the customer phone number to schedule a queued callback.
- Identify which agent is interacting with a customer so that a post call survey can be associated with a contact.
- Identify the number of contacts in a queue to decide if the contact should be routed to a different queue.
- Get the corresponding media streaming ARN to store in a database.
- Use the customer phone number to identify the status of a customer (for example, are they a member), or the status of their order (shipped, delayed, etc.) to route them to the appropriate queue.
- Based on a customer interaction with a bot, identify the slot (for example, the type of flowers to order) to be used in a flow.

Types of contact attributes

To make it faster for you to find and choose the attributes you want to use, attributes are grouped into **types**. For each contact block, we only surface those types of attributes that work with it.

Another way to think about types of contact attributes is to categorize them based on where the value comes from. The values for contact attributes have three sources:

- Amazon Connect provides the value, such as the agent's name, during the contact interaction. This is known as providing the value at runtime.
- An external process, such as Amazon Lex or AWS Lambda, provides the value.
- User-defined (p. 529). In the contact flow, you can specify the value for an attribute.


Types of contact attributes
Where the value comes from
System (Amazon Connect)
Contact flows read this data
Agent
Queue
Amazon Connect provides the value when the contact enters the contact flow.
Customer
Customer interacts with a contact flow
Contact flow
Media Stream
Lambda
Lex
Lambda or Lex provide the value
Contact flows read and write this data
User-defined
You specify the value in the contact flow

Contact attributes in the contact record

In contact records, contact attributes are shared across all contacts with the same InitialContactId.

For example, while carrying out transfers, a contact attribute updated in the transfer flow updates the attribute's value in the contact attributes of both contact records (that is, the Inbound and Transfer contact attributes).

"$" is a special character

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

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

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

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

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

List of available contact attributes and their JSONPath reference

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

The JSONPath reference for each attribute is provided so you can create dynamic text strings (p. 459).

System attributes

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

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 (p. 529) to store the data input by a customer.

Attribute	Description	Type	JSONPath Reference
Customer number	The customer's phone number. When used in an outbound whisper flow, this is the number that the agents dialed to reach the customer. When used in inbound flows, this is the number from which the customer placed the call. This attribute is included in contact records. When used	System	$.CustomerEndpoint.Address

Attribute	Description	Type	JSONPath Reference
	in a Lambda function, it's included in the input object under CustomerEndpoint.		
Customer ID	The customer's identification number.	System	$.CustomerId
Dialed number	The number the customer dialed to call your contact center. This attribute is included in contact records. When used in a Lambda function, it's included in the input object under SystemEndpoint.	System	$.SystemEndpoint.Address

Attribute	Description	Type	JSONPath Reference
Customer callback number	The number that Amazon Connect uses to call back the customer. This number can be the one used for a queued callback, or when an agent is dialing from the CCP. Transfer to callback queue functionality, or for an agent dialing from the CCP. The default value is the number that the customer used to call your contact center. However, it can be overwritten with the **Set callback number** block. This attribute is not included in contact records, and it's not accessible in Lambda input. However, you can copy the attribute to a user-defined attribute with the Set contact attribute block, which is included in contact records. You can also pass this attribute as a Lambda input parameter in an Invoke AWS Lambda function block, which is not included in contact records.	System	not applicable

Attribute	Description	Type	JSONPath Reference
Stored customer input	An attribute created from the most recent invocation of a **Store customer input** block. The attribute values created from the most recent Store customer input block invocation. This attribute is not included in contact records, and is not accessible in Lambda input. You can copy the attribute to a user-defined attribute with the Set contact attribute block, which is included in contact records. You can also pass this attribute as a Lambda input parameter in an Invoke AWS Lambda function block,	System	not applicable
Queue name	The name of the queue.	System	$.Queue.Name
Queue ARN	The ARN for the queue.	System	$.Queue.ARN
Queue outbound number	The Outbound caller ID number for the selected queue. This attribute is only available in outbound whisper contact flows.	System	
Text to speech voice	The name of the Amazon Polly voice to use for text-to-speech in a contact flow.	System	$.TextToSpeechVoiceId
Contact id	The unique identifier of the contact.	System	$.ContactId
Initial Contact id	The unique identifier for the contact associated with the first interaction between the customer and your contact center. Use the initial contact ID to track contacts between contact flows.	System	$.InitialContactId

Attribute	Description	Type	JSONPath Reference
Task Contact id	The unique identifier for the task contact. Use the task contact ID to track tasks between contact flows.	System	$.Task.ContactId
Previous Contact id	The unique identifier for the contact before it was transferred. Use the previous contact ID to trace contacts between contact flows.	System	$.PreviousContactId
Channel	The method used to contact your contact center: VOICE, CHAT, TASK.	System	$.Channel
Instance ARN	The ARN for your Amazon Connect instance.	System	$.InstanceARN
Initiation method	How the contact was initiated. Valid values include: INBOUND, OUTBOUND, TRANSFER, CALLBACK, QUEUE_TRANSFER, DISCONNECT, and API. Initiation method doesn't work in Agent whisper flows or Customer whisper flows.	System	$.InitiationMethod
Name	The name of the task.	System	$.Name
Description	A description of the task.	System	$.Description
References	Links to other documents that are related to a contact.	System	$.References.*ReferenceKey*.Value and $.References.*ReferenceKey*.Type where *ReferenceKey* is the user-defined Reference name.
Language	The language of content. Use the standard java.util.Locale. For example, en-US for United States English, jp-JP for Japanese, etc.	System	$.LanguageCode

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

Agent attributes

The following table lists the agent attributes available in Amazon Connect.

Attribute	Description	Type	JSONPath Reference
Agent User name	The user name an agent uses to log in to Amazon Connect.	System	$.Agent.UserName
Agent First name	The agent’s first name as entered in their Amazon Connect user account.	System	$.Agent.FirstName
Agent Last name	The agent’s last name as entered in their Amazon Connect user account.	System	$.Agent.LastName
Agent ARN	The ARN of the agent.	System	$.Agent.ARN

> **Note**
> When you use an agent contact attribute in a **Transfer to agent** flow, the agent attributes reflect the target agent, not the one who initiated the transfer.

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

- Agent whisper
- Customer whisper
- Agent hold
- Customer whisper

- Outbound whisper
- Transfer to agent. In this case, the agent attributes reflect the target agent, not the one who initiated the transfer.

Agent attributes are not available in the following contact flow types:

- Customer queue
- Transfer to queue
- Inbound contact flow

Queue attributes

These system attributes are returned when you use a **Get queue metrics** block in your contact flow.

If there is no current activity in your contact center, null values are returned for these attributes.

Attribute	Description	Type	JSONPath Reference
Queue name	The name of the queue for which metrics were retrieved.	System	$.Metrics.Queue.Name
Queue ARN	The ARN of the queue for which metrics were retrieved.	System	$.Metrics.Queue.ARN
Contacts in queue	The number of contacts currently in the queue.	System	$.Metrics.Queue.Size
Oldest contact in queue	For the contact that has been in the queue the longest, the length of time that the contact has been in the queue, in seconds.	System	$.Metrics.Queue.OldestContactAge
Agents online	The number of agents currently online, which means logged in and in any state other than offline.	System	$.Metrics.Agents.Online.Count
Agents available	The number of agents whose state is set to Available.	System	$.Metrics.Agents.Available.Count
Agents staffed	The number of agents currently staffed, which is agents logged in and in Available, ACW, or Busy states.	System	$.Metrics.Agents.Staffed.Count
Agents in After contact work	The number of agents currently in the ACW state.	System	$.Metrics.Agents.AfterContactWork.Co

Attribute	Description	Type	JSONPath Reference
Agents busy	The number of agents currently active on a contact.	System	$.Metrics.Agents.Busy.Count
Agents missed count	The number of agents in the Missed state, which is the state an agent enters after a missed contact.	System	$.Metrics.Agents.Missed.Count
Agents in non-productive state	The number of agents in a non-productive (NPT) state.	System	$.Metrics.Agents.NonProductive.Count

Telephony call metadata attributes (call attributes)

Telephony metadata provides additional information related to call origination from telephony carriers.

Attribute	Description	Type	JSONPath Reference
P-Asserted-Identity	The source of the end user.	System	$.Media.Sip.Headers.P-Asserted-Identity
P-Charge-Info	The party responsible for the charges associated with the call.	System	$.Media.Sip.Headers.P-Charge-Info
From	The identity of the end user associated with the request.	System	$.Media.Sip.Headers.From
To	Information about the called party or the recipient of the request.	System	$.Media.Sip.Headers.To
ISUP-OLI	Originating Line Indicator (OLI). Shows the type of line placing call (for example, PSTN, 800 service call, wireless/cellular PCS, payphone).	System	$.Media.Sip.Headers.ISUP-OLI
JIP	Jurisdiction Indication Parameter (JIP). Indicates geographic location of caller/switch. Example value: 212555	System	$.Media.Sip.Headers.JIP
Hop-Counter	Hop Counter. Example value: 0	System	$.Media.Sip.Headers.Hop-Counter

Attribute	Description	Type	JSONPath Reference
Originating-Switch	Originating Switch. Example value: 710	System	$.Media.Sip.Headers.Originating-Switch
Originating-Trunk	Originating Trunk. Example value: 0235	System	$.Media.Sip.Headers.Originating-Trunk
Call-Forwarding-Indicator	Call Forwarding Indicators (for example, Diversion header). Indicates domestic or international origin of call. Example value: sip: +15555555555@public-vip.us2.telphony-provider.com;reason=unconditional	System	$.Media.Sip.Headers.Call-Forwarding-Indicator
Calling-Party-Address	Calling Party Address (number). NPAC dip shows true line type and native geographic switch. Example value: 15555555555;noa=4	System	$.Media.Sip.Headers.Calling-Party-Address
Called-Party-Address	Called Party Address (number). Example value: 15555555555;noa=4	System	$.Media.Sip.Headers.Called-Party-Address

Note
The availability of telephony metadata is not consistent across all telephony providers and may not be available in all cases. This may result in empty values.

Media streams attributes

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

Attribute	Description	Type	JSONPath Reference
Customer audio stream ARN	The ARN of the Kinesis Video stream used for Live media streaming that includes the customer data to reference.	Media streams	$.MediaStreams.Customer.Audio.Strea
Customer audio start timestamp in the	When the customer audio stream started.	Media streams	$.MediaStreams.Customer.Audio.StartT

Attribute	Description	Type	JSONPath Reference
Kinesis video stream used for Live media streaming.			
Customer audio stop timestamp	When the customer audio stream stopped the Kinesis video stream used for Live media streaming.	Media streams	$.MediaStreams.Customer.Audio.StopT
Customer audio start fragment number	The number that identifies the Kinesis Video Streams fragment, in the stream used for Live media streaming, in which the customer audio stream started.	Media streams	$.MediaStreams.Customer.Audio.Start

Amazon Lex contact attributes

The following table lists the attributes that are returned from Amazon Lex bots.

Attribute	Description	Type	JSONPath Reference
Alternate Intents	List of alternate intents available from Amazon Lex. Each intent has a corresponding confidence score and slots to fill.	Lex	$.Lex.AlternateIntents.x.IntentName $.Lex.AlternateIntents.x.IntentConfide $.Lex.AlternateIntents.x.Slots $.Lex.AlternateIntents.y.IntentName $.Lex.AlternateIntents.y.IntentConfide $.Lex.AlternateIntents.y.Slots $.Lex.AlternateIntents.z.IntentName $.Lex.AlternateIntents.z.IntentConfide $.Lex.AlternateIntents.z.Slots
Intent Confidence Score		Lex	$.Lex.
Intent name	The user intent returned by Amazon Lex.	Lex	$.Lex.IntentName
Sentiment Label	The inferred sentiment that Amazon Comprehend has the highest confidence in.	Lex	$.Lex.SentimentResponse.Label

Attribute	Description	Type	JSONPath Reference
Sentiment scores	The likelihood that the sentiment was correctly inferred.	Lex	$.Lex.SentimentResponse.Scores.Posit $.Lex.SentimentResponse.Scores.Nega $.Lex.SentimentResponse.Scores.Mixec $.Lex.SentimentResponse.Scores.Neutr
Session attributes	Map of key-value pairs representing the session-specific context information.	Lex	$.Lex.SessionAttributes.attributeKey
Slots	Map of intent slots (key/value pairs) Amazon Lex detected from the user input during the interaction.	Lex	$.Lex.Slots.slotName
Dialog state	The last dialog state returned from an Amazon Lex bot. The value is 'Fulfilled' if an intent was returned to the contact flow.	N/A (no type appears in the UI)	$.Lex.DialogState

Case contact attributes (Preview)

The following table lists the attributes that are used with Amazon Connect Cases.

Attribute	Description	Type	JSONPath Reference	Where the data comes from
Case ID	Unique Identifier of the case in UUID format (for example, 689b0bea-aa29-4340-896d-4ca3ce9b6226)	text	$.Case.case_id	Amazon Connect
Case Reason	The reason for opening the case	$.Case.case_reason	single-select	Agent
Customer	The API is a customer profile ID. On the **Cases: Fields** page, the customer's name is displayed.	$.Case.customer_id	text	Amazon Connect
Date/Time Closed	The date and time the case was last closed. It does not guarantee that a case is closed. If a	$.Case.last_closed_datetime	date-time	Amazon Connect

Attribute	Description	Type	JSONPath Reference	Where the data comes from
	case is reopened, this field contains the date/time stamp of the last time the status was changed to closed.			
Date/Time Opened	The date and time the case was opened.	$.Case.created_datetime	date-time	Amazon Connect
Date/Time Updated	The date and time the case was last updated.	$.Case.last_updated_datetime	date-time	Amazon Connect
Reference number	A friendly number for the case in 8-digit numeric format. Reference numbers (unlike the Case ID) are not guaranteed to be unique. We recommend that you identify the customer and then collect the reference number to correctly find the right case.	$.Case.reference_number	text	Agent
Status	Current status of the case	$.Case.status	text	Agent
Summary	Summary of the case	$.Case.summary	text	Agent
Title	Title of the case	$.Case.title	text	Agent

Lambda contact attributes

Lambda attributes are returned as key-value pairs from the most recent invocation of an **Invoke AWS Lambda function** block. External attributes are overwritten with each invocation of the Lambda function.

To reference external attributes in JSONPath, use:

- `$.External.attributeName`

where `AttributeName` is the attribute name, or the key of the key-value pair returned from the function.

For example, if the function returns a contact ID, reference the attribute with `$.External.ContactId`. When referencing a contact ID returned from Amazon Connect, the JSONPath is `$.ContactId`.

> **Note**
> Note the inclusion of `.External` in the JSONPath reference when the attribute is external to Amazon Connect. Make sure to match the case for attribute names returned from external sources.

For more information about using attributes in Lambda functions, see Invoke AWS Lambda functions (p. 488).

These attributes are not included in contact records, not passed to the next Lambda invocation, and not passed to the CCP for screenpop information. However, they can be passed as Lambda function inputs on an **Invoke AWS Lambda function** block, or copied to user-defined attributes via the **Set contact attributes** block. When used in **Set contact attributes** blocks, the attributes that are copied are included in contact records, and can be used in the CCP.

User-defined attributes

For all other attributes Amazon Connect defines the key and value. For user-defined attributes, however, you provide a name for the key and the value.

Use user-defined attributes in situations where you want to store values in a contact flow, and then refer to those values later. For example, if you integrate Amazon Connect and a CRM or other system, you might want to get input from the customer such as their member number. Then you can use that member number retrieve information about the member from the CRM, and/or use the member number throughout the contact flow, etc.

Attribute	Description	Type	JSONPath Reference
Any name you choose	A user-defined attribute has two parts: • Destination key: this is any name you choose for the key. However, the **$** and **.** (period) characters are not allowed because they are both used in defining the attribute paths in JSONPath. • Value: this is can be any value you choose. You can enter several paragraphs worth of text if you want! (For the **Max size of the contact record attributes section**, see Feature specifications (p. 1210).)	User-defined	$.Attributes.*name_of_your_destinatior*

To create user-defined attributes, use the Set contact attributes (p. 399) block.

Apple Messages for Business attributes

Use the following contact attributes to route Apple Business Chat customers. For example, if you have different lines of business using Apple Business Chat, you can branch to different contact flows based on the AppleBusinessChatGroup contact attribute. Or, if you want to route Apple Business Chat messages differently from other chat messages, you can branch based on MessagingPlatform.

Attribute	Description	Type	JSON
MessagingPlatform	The messaging platform from where the customer request originated. Exact value: **AppleBusinessChat**	User-defined	$.Attributes.MessagingPlatform
AppleBusinessChatCustomerId	The customer's opaque ID provided by Apple. This remains constant for the AppleID and a business. You can use this to identify if the message is from a new customer or a returning customer.	User-defined	$.Attributes.AppleBusinessChatCustom
AppleBusinessChatIntent	You can define the intent or purpose of the chat. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the **Business Chat** button.	User-defined	$.Attributes.AppleBusinessChatIntent
AppleBusinessChatGroup	You define the group which designates the department or individuals best qualified to handle the customer's particular question or problem. This parameter is included in a URL that initiates a chat session in Messages when a customer chooses the **Business Chat** button.	User-defined	$.Attributes.AppleBusinessChatGroup
AppleBusinessChatLocale	Defines the language and AWS Region preferences that the user wants to see in their user interface. It consists of a language identifier (ISO 639-1)	User-defined	$.Attributes.AppleBusinessChatLocale

Attribute	Description	Type	JSON
	and a Region identifier (ISO 3166). For example, **en_US**.		

Customer Profiles attributes

Use the following contact attributes to autopopulate customer profiles in the agent app using the value of your choosing.

Attribute	Description	Type	JSONPath Reference
profileSearchKey	A user-defined attribute that has two parts: • Destination key: this is any name you choose for the key. However, the **$** and **.** (period) characters are not allowed because they are both used in defining the attribute paths in JSONPath. • Value: this is can be any value you choose. You can enter several paragraphs worth of text if you want! (For the **Max size of the contact record attributes section**, see Feature specifications (p. 1210).)	User-defined	$.Attributes.*name_of_your_destinatior*

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 that contain spaces in their name, such as user defined attributes, place brackets and single quotations around the attribute name. For example: `$.Attributes.['user attribute name']`.
- To reference attributes in the same namespace, such as a system attribute, you use the attribute name, or the name you specified as the **Destination key**.
- To reference values in a different namespace, such as referencing an external attribute, you specify the JSONPath syntax to the attribute.
- To use contact attributes to access other resources, set a user-defined attribute in your contact flow and use the Amazon Resource Name (ARN) of the resource you want to access as the value for the attribute.

Lambda examples

- To reference a customer name from a Lambda function lookup, use $.External.AttributeKey, replacing AttributeKey with the key (or name) of the attribute returned from the Lambda function.
- To use an Amazon Connect prompt in a Lambda function, set a user-defined attribute to the ARN for the prompt, and then access that attribute from the Lambda function.

Amazon Lex examples

- To reference an attribute from an Amazon Lex bot, you use the format $.Lex. and then include the part of the Amazon Lex bot to reference, such as $.Lex.IntentName.
- To reference the customer input to an Amazon Lex bot slot, use $.Lex.Slots.*slotName*, replacing *slotName* with the name of the slot in the bot.

Set contact attribute example

Use a Set contact attributes (p. 399) 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 (p. 399) 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.

Display contact information to the agent in the CCP

You can use contact attributes to capture information about the contact and then present it to the agent through the Contact Control Panel (CCP). For example, you might want to do this to customize the agent experience when using the CCP integrated with a customer relationship management (CRM) application.

Also use them when integrating Amazon Connect with a custom application using the Amazon Connect Streams API or Amazon Connect API. You can use all user-defined attributes, in addition to the customer number and the dialed number, in the CCP using the Amazon Connect Streams JavaScript library. For more information, see Amazon Connect Streams API or Amazon Connect API.

When you use the Amazon Connect Streams API, you can access user-defined attributes by invoking contact.getAttributes(). You can access endpoints 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.

Route based on number of contacts in a queue

Amazon Connect includes queue 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. For example, here are some common usage scenarios:

- Check the number of contacts or available agents in a queue, and how long the oldest contact has been in a queue, then route accordingly.
- To route to the queue with the fewest contacts in it:
  1. Get metrics for multiple queues.
  2. Use a **Set contact attributes** block to store the metric attributes for each queue.
  3. compare queue metric attributes using a **Check contact attributes** block, and route the contact to the queue with the fewest calls in it, or to a callback if all queues are busy.

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

1. In Amazon Connect, choose **Routing**, **Contact flows**.
2. Open an existing 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**.

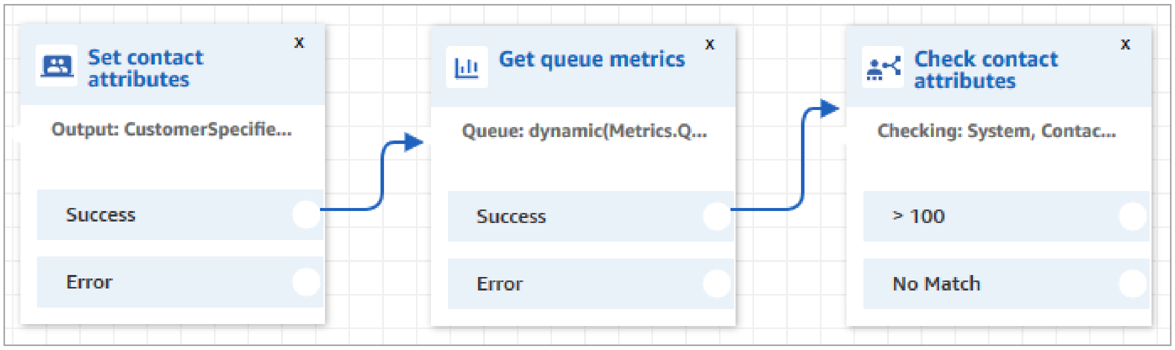
    By default, the **Check contact attributes** block includes a single condition, **No match**. The **No match** branch is followed when there are no matches for any of the conditions you define in the block.
11. Under **Conditions to check**, select **Is less than** as the operator for the condition in 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.

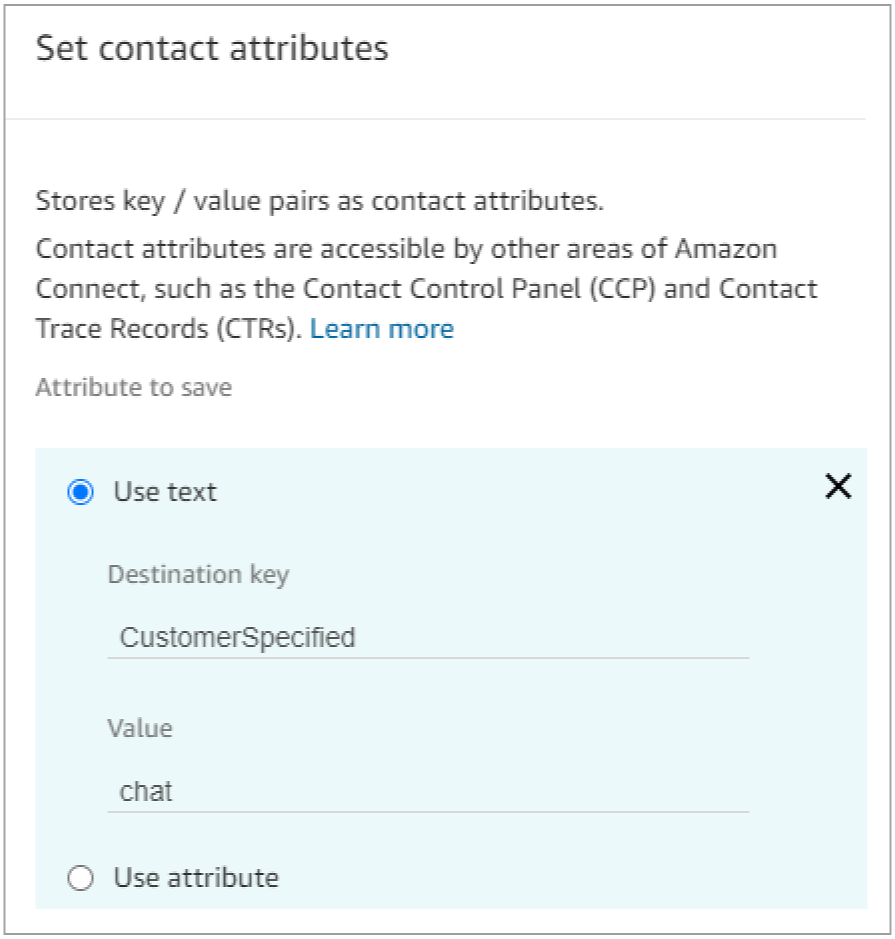
You can now add additional blocks to the contact flow to route the contact as desired. For example, connect the < 5 branch to a **Transfer to queue** block to transfer calls to the queue when there are fewer than five calls currently in the queue. Connect the > 5 branch to a Set customer callback number 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.

Route contacts based on queue metrics

Many contact centers route customers based on the number of contacts waiting in a queue. This topic explains how to configure a contact flow that looks similar to the following image.



1. Add a Set contact attributes (p. 399) block to your contact flow.
2. In the Set contact attributes (p. 399), specify the channel. If you set a channel dynamically using text, for the attribute value enter **Voice** or **Chat**, as shown in the following image. This value is not case-sensitive.



Set contact attributes

Stores key / value pairs as contact attributes.

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

Attribute to save

● Use text

Destination key: CustomerSpecified

Value: chat

○ Use attribute

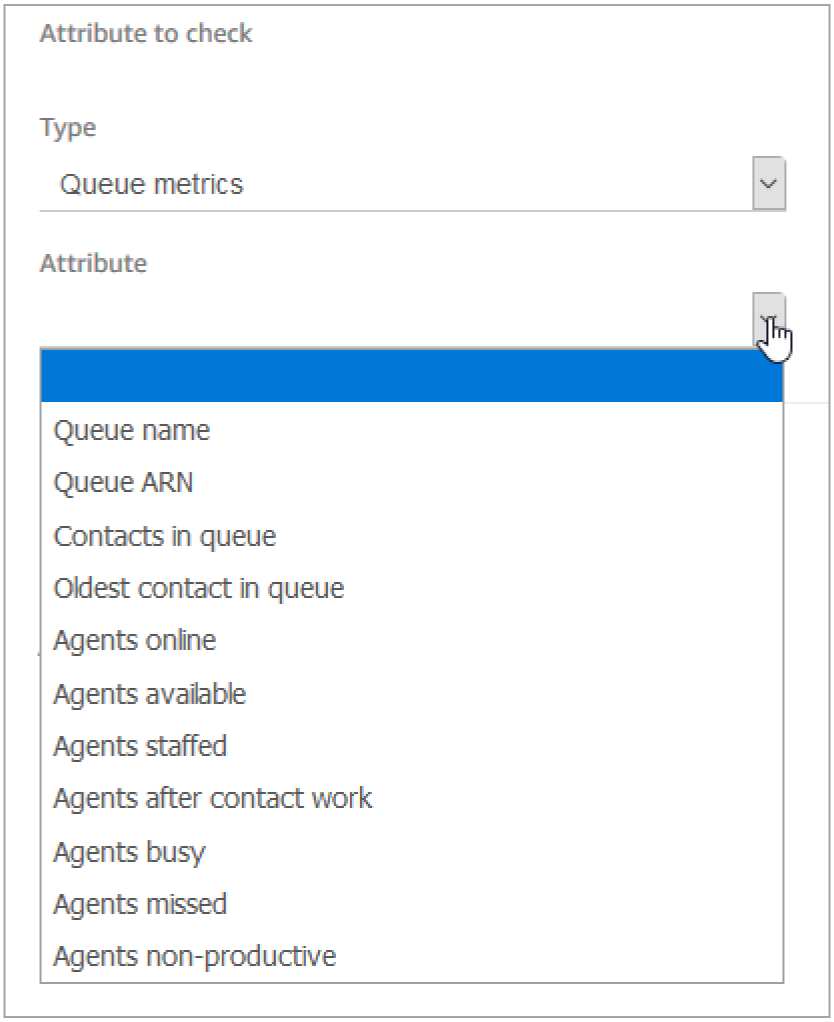
3. Add a Get queue metrics (p. 378) block to your contact flow.

In the Get queue metrics block, dynamic attributes can only return metrics for one channel

Add a Check contact attributes block after the Get queue metrics block

After a **Get queue metrics** block, add a Check contact attributes (p. 329) block to branch based on the returned metrics. Use the following steps:

1. After **Get queue metrics**, add a **Check contact attributes** block.
2. In the **Check contact attributes** block, set **Attribute to check** to **Queue metrics**.
3. In the **Attributes** dropdown box, you'll see that the following queue metrics are returned by the **Get queue metrics** block. Choose the metric that you want to use for the routing decision.



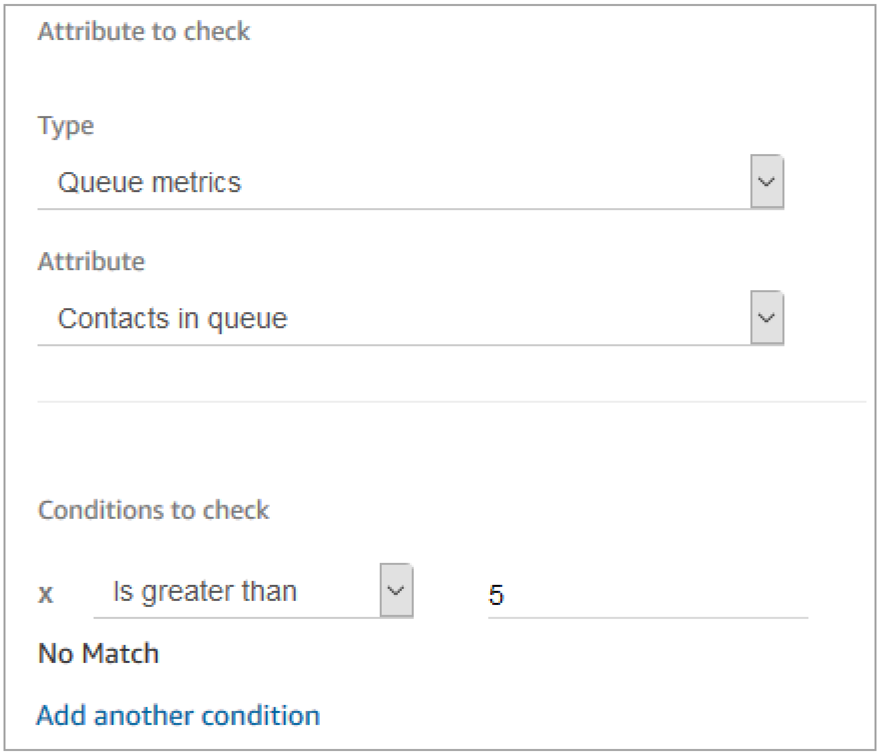
Attribute to check

Type

Queue metrics

Attribute

4. Choose **Add a condition** to enter the comparison for your routing decision.



Attribute to check

Type: Queue metrics

Attribute: Contacts in queue

Conditions to check

x Is greater than 5

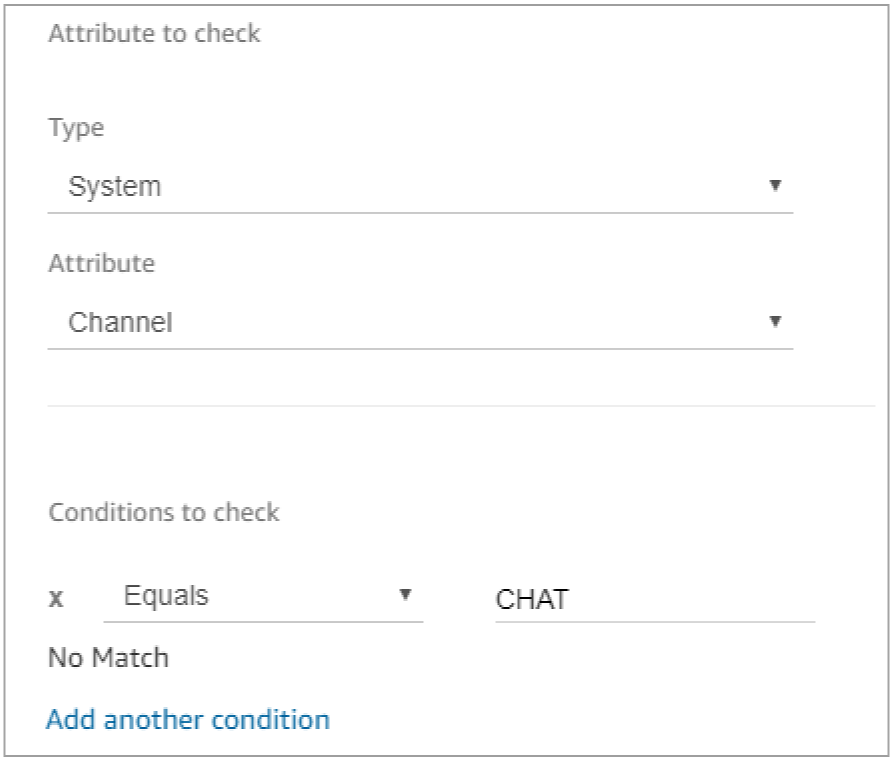
No Match

Add another condition

Route based on contact's channel

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

1. Add a **Check contact attributes** block to the beginning of your contact flow.
2. Configure the block as shown in the following image:



Attribute to check

Type

System

Attribute

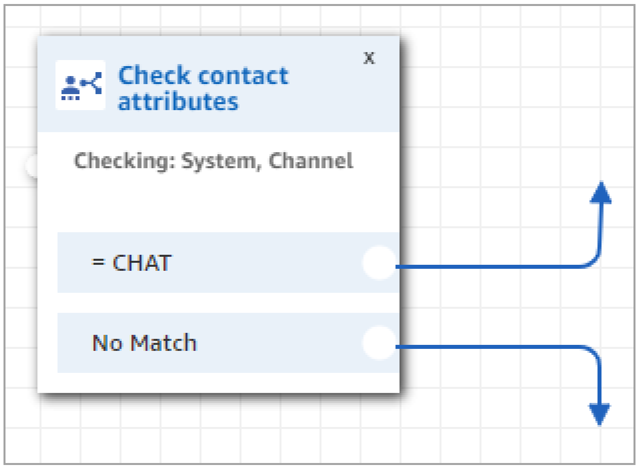
Channel

Conditions to check

x Equals CHAT

No Match

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.

Use Amazon Lex and attributes

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

For a list of Amazon Lex attributes you can use, see Amazon Lex contact attributes (p. 526).

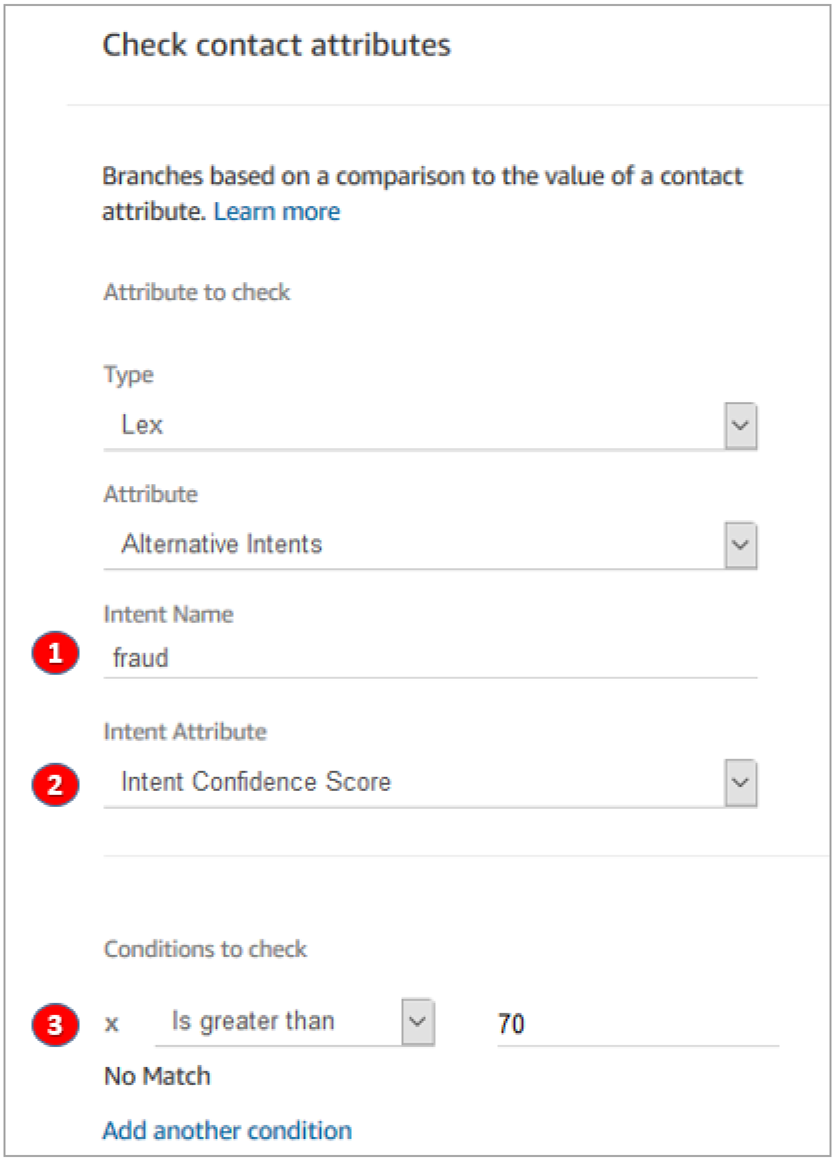
Using an Amazon Lex bot to get customer input

1. Open an existing or create a new contact flow.
2. Under **Interact**, drag a **Get customer input** block to the designer.
3. Choose the title of the block to display the block settings, then select **Text to speech (Ad hoc)**.
4. Choose **Enter text**, then enter text in the **Enter text to be spoken** field that is used as a message or greeting to your customers. For example, "Thank you for calling" followed by a request to enter information to fulfill the intents you defined in your Amazon Lex bot.
5. Choose the **Amazon Lex** tab, then from the drop-down menu, choose the Amazon Lex bot to use to get customer input.
6. By default, the **Alias** field is populated with $LATEST. To use a different alias of the bot, enter the alias value to use.

   Important
   In a production environment, always use a different alias than **TestBotAlias** for Amazon Lex and **$LATEST** for Amazon Lex classic. **TestBotAlias** and **$LATEST** support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime Service Quotas or Runtime Service Quotas (Amazon Lex Classic).
7. Optionally, to pass an attribute to Amazon Lex to use as a session attribute, choose **Add an attribute**. Specify the value to pass using either text or an attribute.
8. To create a branch from the block based on the customer intent, choose **Add an intent**, then enter the name of the intent exactly the same as the intent name in your bot.
9. Choose **Save**.

How to use Lex alternate intent attributes

Usually you configure contact flows to branch on the winning Lex intent. However, in some situations, you might want to branch on an alternate intent. That is, what the customer might have meant.



Check contact attributes

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

Attribute to check

Type: Lex

Attribute: Alternative Intents

Intent Name: fraud

Intent Attribute: Intent Confidence Score

Conditions to check

x Is greater than 70

No Match

Add another condition

1. **Intent name** is the name of an alternate intent in Lex. It's case sensitive and must match what's in Lex exactly.
2. **Intent Attribute** is what Amazon Connect is going to check. In this example, it's going to check the **Intent Confidence Score**.
3. **Conditions to check**: If Lex is 70% certain the customer meant the alternate intent instead of the winning intent, branch.

How to use Lex session attributes

When a customer starts a conversation with your bot, Amazon Lex creates a *session*. With *session attributes*, also known as *Lex attributes*, you can pass information between the bot and Amazon Connect during the session. For a list of Amazon Lex attributes you can use, see Amazon Lex contact attributes (p. 526).

Life cycle of session attributes

There's one set of session attributes per conversation. In cases where a Lambda is invoked to do some processing, following is the order of precedence:

- Service defaults: these attributes are only used if no attributes are defined.
- Session attributes provided by Amazon Connect: these attributes are defined in the Get customer input (p. 366) block.
- Session attributes provided by Lambda override everything prior: When a Lambda function is invoked and it does some processing, it overrides any session attributes set in the Get customer input (p. 366) block.

Let's say a customer utters that they want **a car**. That's the first session attribute to go through processing. When asked what kind of car, they say **luxury car**, this second utterance overrides any Lambda processing that took place on the first utterance.

For an example of how to create a Lambda function that processes session attributes, see Step 1: Create a Lambda Function in the *Amazon Lex Developer Guide*.

For the structure of the event data that Amazon Lex provides to a Lambda function, see Lambda Function Input Event and Response Format in the *Amazon Lex Developer Guide*.

Contact blocks that support Lex session attributes

You can use Lex session attributes in the following blocks when a Lex bot is called:

- Get customer input
- Set contact attributes
- Set hold flow
- Set working queue
- Set customer queue flow
- Set disconnect flow
- Set logging behavior
- Set callback number
- Set whisper flow
- Change routing priority/age
- Check contact attributes
- Loop
- Wait
- Invoke AWS Lambda function
- Transfer to phone number
- Transfer to flow

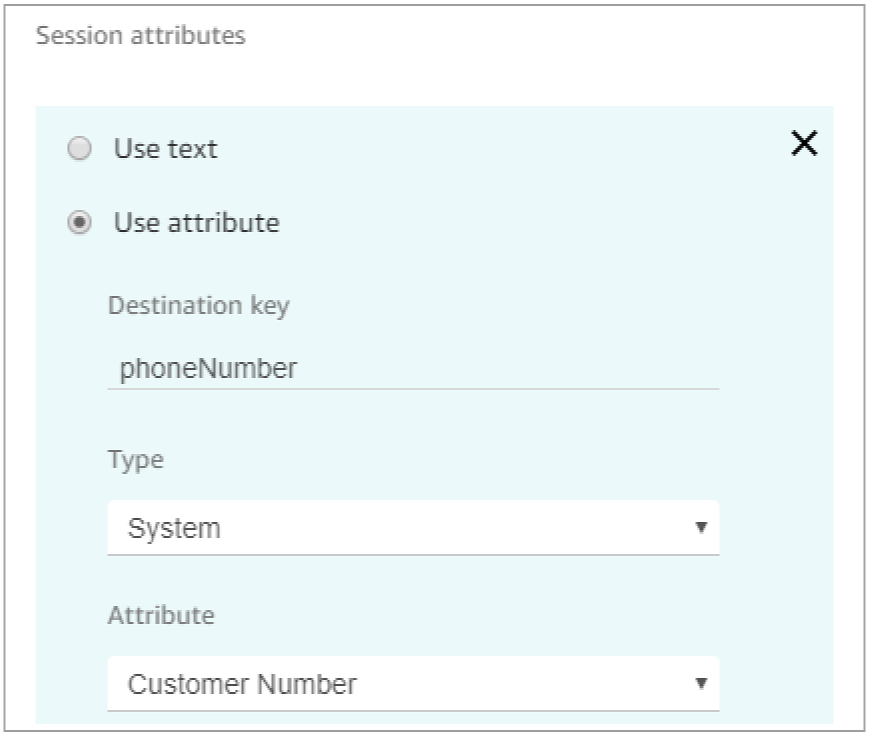
More information

For more information about using Amazon Lex session attributes, see Managing Conversation Context in the *Amazon Lex Developer Guide*.

How to use the same bot for voice and chat

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

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



Session attributes

○ Use text

● Use attribute

Destination key

phoneNumber

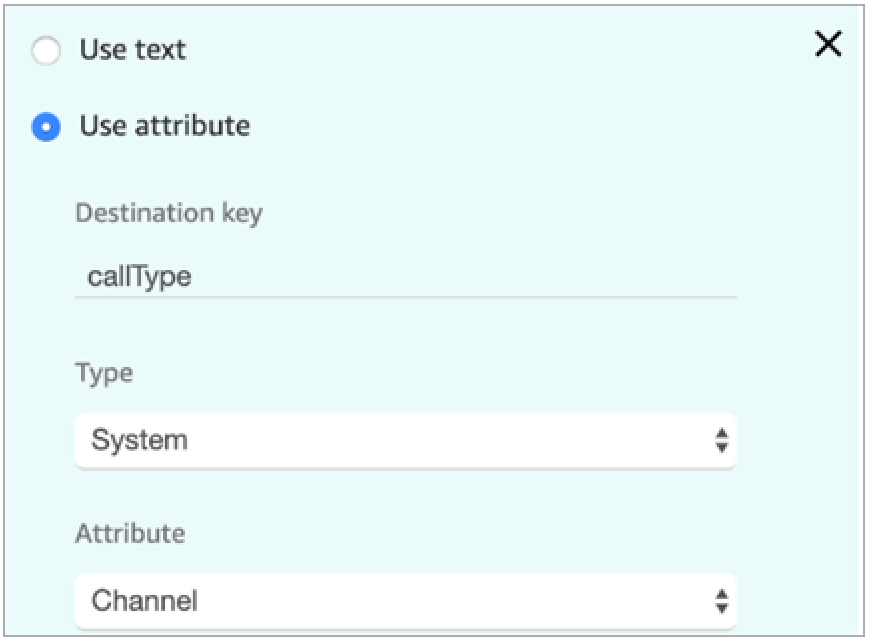
Type

System

Attribute

Customer Number

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



○ Use text

● Use attribute

Destination key

callType

Type

System

Attribute

Channel

5. Choose **Save**.
6. In your Lambda function, you can access this value in the SessionAttributes field in the incoming event.

Lambda functions and attributes

Retrieve data from a system your organization uses internally, such as an ordering system or other database with a Lambda function, and store the values as attributes that can then be referenced in a 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 **Type**, choose **External**.
9. For **Attribute**, enter the name of the attribute returned from the Lambda function. The name of the attribute returned from the function will vary depending on your internal system and the function you use.

After this block executes during a 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.

Migrate contact flows to a different instance

Amazon Connect lets you efficiently migrate contact flows to another instance. For example, you might want to expand into new Regions, or move contact flows from your development environment to your production environment.

To migrate a few contact flows, use the import/export feature (p. 487) in the contact flow designer.

To migrate hundreds of contact flows, you need developer skills. You use the following procedure:

1. Source instance
   - ListContactFlow: Retrieve the Amazon Resource Number (ARN) for the contact flows that you want to migrate.
   - DescribeContactFlow: Get information about each contact flow that you want to migrate.
2. Destination instance
   - CreateContactFlow: Create the contact flows.
   - UpdateContactFlowContent: Update the contact flow content.

You must also build an ARN-to-ARN mapping for queues, contact flows, and prompts between the source and target Amazon Connect instances, and replace every ARN in the source contact flow with the corresponding ARN from the target instance. Otherwise UpdateContactFlowContent fails with `InvalidContactFlow` error.

You can update the information in the contact flows that you migrate. For more information, see Amazon Connect Flow Language (p. 543).

Amazon Connect Flow language

This section describes the Amazon Connect Flow language and how to use it. The Flow language is a JSON-based representation of a series of flow actions, and the criteria for moving between them.

We've provided you with the Flow language so you can:

- Efficiently update contact flows that you're migrating from one instance to another.
- Write contact flows rather than drag blocks onto the contact flow designer.

Contents

Amazon Connect Flow language concepts

The following terms are used in the Flow language.

Contact

Flows can be run in context of a contact. In this case, they are referred to as *contact flows*.

Participant

Contact flows can additionally be run in a participant context. This allows participant actions—such as playing prompts or getting customer input—to be run. Certain types of contact flows, such as "No participants remaining" disconnect flows and Workitem contact flows, don't have a participant associated.

Action types

Flow actions have the following implicit types associated with them. A type determines when an action is attempted.

- Contact actions in the Amazon Connect Flow language (p. 548). These actions are attempted only when the flow is run in context of a contact. They generally result in contact data being manipulated in some way.
- Flow control actions in the Amazon Connect Flow language (p. 556). These actions are used only to determine the path through a flow. They have no side effects. Certain data may not be available. For example, contact data isn't available if the action is determining its path based on contact data. These actions generally work in every circumstance.
- Interactions in the Amazon Connect Flow language (p. 564). These actions have side effects, but don't require a contact or a participant. Interactions include actions such as invoking an AWS Lambda function. They generally work in every circumstance.
- Participant actions in the Amazon Connect Flow language (p. 569). These actions are attempted only when the flow is run in context of a participant. They generally result in an action that the participant experiences, such as playing a prompt or disconnecting.

Example contact flow in Amazon Connect Flow language

The following example shows a simple contact flow that plays a prompt using static text and disconnects.

To learn how to get block identifiers, we recommend creating a new contact flow in Amazon Connect console, and then calling the DescribeContactFlow API for it.

```
{
    "Version": "2019-10-30",  //A string representing the version of the Flow. Currently
 the only supported version is 2019-10-30.

    "StartAction": "12345678-1234-1234-1234-123456789012", //A string representing the
 first Action to run when the flow starts running.
                                                          //In this case, it's the
 identifier of the Play prompt block.
                                                         //The value of this field must
 match the Identifier of an Action in the Actions list.
    "Metadata": { //An object that may be filled in with data as desired.
        "EntryPointPosition": {
            "x": 88,
            "y": 100
        },
        "ActionMetadata": {
            "12345678-1234-1234-1234-123456789012": {    //The identifier of the Play
 prompt block.
                "Position": {
                    "x": 270,
                    "y": 98
                }
            },
            "abcdef-abcd-abcd-abcd-abcdefghijkl": {  //The identifier of the Disconnect/
hang up block.
                "Position": {
                    "x": 545,
                    "y": 92
                }
            }

        }
    },
    "Actions": [  //A list of individual Action objects. These Actions are the definition
 of the Flow's behavior and are detailed below.
                  //A single Flow may have no more than 250 Actions defined.
        {
            "Identifier": "12345678-1234-1234-1234-123456789012", //The identifier of the
 Play prompt block.
            "Type": "MessageParticipant",  //This is the flow action.
            "Transitions": {
                "NextAction": "abcdef-abcd-abcd-abcd-abcdefghijkl", //The identifier of the
 Disconnect/hang up block.
                "Errors": [],
                "Conditions": []
            },
            "Parameters": {
                "Text": "Thanks for calling the sample flow!"
            }
        },
        {
            "Identifier": "abcdef-abcd-abcd-abcd-abcdefghijkl",  //The identifier of the
 Disconnect/hang up block.
            "Type": "DisconnectParticipant",  //This is the flow action.
            "Transitions": {},
            "Parameters": {}
        }
    ]
}
```

Actions in the Amazon Connect Flow Language

An Action is a single step of a flow's run. This topic describes the fields that must be defined.

Identifier

A string that must be unique among all Actions within the same Flow. This Identifier can be up to 50 characters long, and can include any characters (including unicode and spaces). They can be opaque or user-friendly.

Type

A string that identifies the type of action being performed for a particular step of the Flow. This type must be one of a list of allowable Types, which are covered later.

Parameters

An object that defines the customizable behavior of a particular Action block. Each Action has its own format of this Parameters object, which is detailed in the individual Actions definition.

The Parameters object defines customizable behavior for the Action. For example, it defines which Attributes to set or which AWS Lambda function to run. The format differs for each Action type. To find the specific format of a specific Action's Parameter object, see the individual Action's definition below.

Transitions

An object that defines the behavior for choosing the next Action after the current Action completes. Certain Actions terminate, meaning that they finish running the flow when they're run. This is because Transitions must be defined as an empty object.

The Transitions object defines how to proceed to the next Action during flow runtime. This object must have the following fields specified:

NextAction

NextAction is a string that contains the Identifier of the Action that should be run after this Action, if no error or condition is preferentially chosen.

Errors

Errors is a list of error objects. Each error object contains a type or category of error (ErrorType), and the Identifier of the Action that should be run subsequently when that error occurs (NextAction).

Each individual Action supports specific Errors, detailed in the Action's definition later, and the following commonly supported errors:

- NoMatchingError. This is invoked when an error occurs and no other Error matches.
- NoMatchingCondition. This is invoked if no defined condition resolves to true.

Conditions

Conditions are an ordered list that defines a series of checks to evaluate against the Action's result. This result changes per Action and can also change based on Parameters - examples of these are "the number of contacts in queue" for the CheckMetricData Action if the MetricType parameter refers to the NumberOfContactsInQueue, and "the value of the attribute" for the Compare Action. Conditions are evaluated in order, and the first Condition that evaluates to true will result in it being chosen as the Transition to occur, making that Condition's Target the next Action run. The Conditions object is explained in more detail below.

A Condition is a definition of how to evaluate an Action's result, and may evaluate to true or false. The Conditions object on the flow contains an ordered list of objects. Each object contains a NextAction (the Identifier of the Action to be invoked if the Condition evaluates to be true) and the Condition to evaluate:

- NextAction: A string that contains the Identifier of the Action that should be run after this Action if this Condition is the first condition to evaluate to true.
- Condition: An object that defines the evaluation logic.

The Condition object

The Condition object must contain the following fields:

- **Operator**: A string that indicates which comparison operator that is applied to the Operands. The list of allowed Operators and a description of their logic is defined in the following table.
- **Operands**: A list of operands to which the Operator is applied. Depending on the Operator, these Operands may be strings or they may be Condition objects. The specific Operator defines which type of Operand is expected, along with the number of Operands expected (some Operators will require

only one Operand, some will support a list of up to ten Operands). Conditions may be nested no more than five Conditions deep, and a single Condition may not contain more than 50 sub-Conditions, regardless of how deeply nested they are.

List of Operators

Operator	Description	Operand type	Operand count
Equals	Returns **true** if the string specified exactly equals the result.	String	One
TextStartsWith	Returns **true** if the result, interpreted as text, begins with the specified string.	String	One
TextEndsWith	Returns **true** if the result, interpreted as text, ends with the specified string.	String	One
TextContains	Returns **true** if the result, interpreted as text, contains the specified string at least once.	String	One
NumberGreaterThan	Returns **true** if the result, interpreted as a numeric value, is larger than the specified string. If either the result or the specified string are not numeric, returns **false**.	String	One
NumberGreaterOrEqualTo	Returns **true** if the result, interpreted as a numeric value, is larger than or equal to the specified string. If either the result or the specified string are not numeric, returns **false**.	String	One
NumberLessThan	Returns **true** if the result, interpreted as a numeric value, is smaller than the specified string. If either the result or the specified string are not numeric, returns **false**.	String	One
NumberLessOrEqualTo	Returns **true** if the result, interpreted as	String	One

Operator	Description	Operand type	Operand count
	a numeric value, is smaller than or equal to the specified string. If either the result or the specified string are not numeric, returns **false**.		

Example Condition

Following is an example of a condition that returns true if the result starts with "ABC":

```
{
    "Operator": "TextStartsWith",
    "Operands": [
        "ABC"
    ]
}
```

Parameter restrictions for actions in the Amazon Connect Flow language

There are several restrictions on parameters. Here's what they mean:

- Must be defined statically. This means that JSONPath cannot be used at all in this value.
- Must be defined statically or as a single valid JSONPath identifier.

  If JSONPath is used, it must be the entirety of the value; you can't specify an input of "My name is $.Name". Further, the JSONPath must be valid - $.Attributes.stuff is okay, $.BadValue is not okay because there's no "BadValue" path on the object used by flows.
- May be defined statically or dynamically. Anything goes. A value of "My name is $.Name" is fine here, as well as a fully static value.

Contact actions in the Amazon Connect Flow language

Contact actions are attempted only for flows that run in context of a contact. They generally result in contact data being manipulated in some way.

Contents

CompleteOutboundCall

When a flow is run before an outbound call is made as part of an outbound contact, this action calls the outbound destination. If this action is not used, the first participant action implicitly completes the outbound call.

Parameter object

```
{
    "CallerId": { Optional, an override of the caller ID to present when calling
        "Number": The caller ID number to present when calling. Can either be fully static
 or a single valid JSONPath identifier
    }
}
```

Results and conditions

None.

Errors

None.

Restrictions

This action can be used only when the contact is in the process of making an outbound call, but has not yet called the outbound number.

Corresponding block in the UI

Call phone number (p. 322)

DequeueContactAndTransferToQueue

This action is a combination of a "Dequeue" action and a "TransferContactToQueue" action. This means that a contact in a queue is removed from the queue, a new contact segment is created with the existing contact as its previous contact, and the new contact is placed into the specified queue (referred to as "Queue-to-queue transfer"). If this contact has not been queued, is actively being joined to an agent, or has been routed to an agent, this action fails.

Parameter object

```
{
    "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not be
 specified. Must be either fully statically defined or a single, valid JSONPath identifier.
    "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId
 is specified, this may not be specified. Must be either fully statically defined or a
 single, valid JSONPath identifier.
}
```

Results and conditions

None.

Errors

- QueueAtCapacity - if the destination queue is at capacity and the contact cannot be queued within it.
- NoMatchingError - if no other Error matches.

Restrictions

This action is only supported in the customer queue flow. It is not supported in any other type of flow.

Corresponding block in the UI

Maps to Transfer to flow (p. 431) but only when used in a Customer queue flow.

TransferContactToAgent

Ends the current contact flow and transfers the customer to an agent. If the agent is already with someone else, the contact is disconnected. Transfer contact to agent works only for voice interactions.

Parameter object

No parameters are expected.

Results and conditions

None.

Errors

None.

Restrictions

This action is supported in only transfer to agent and transfer to queue flows.

Corresponding block in the UI

Transfer to agent (beta) (p. 430)

TransferContactToQueue

This action places a contact that is not already in a queue into the contact's TargetQueue. If the contact has already been put into a queue (meaning that it is currently being routed to an agent, being joined to an agent, or is connected to an agent), the action fails.

Parameter object

No parameters are expected.

Results and conditions

None.

Errors

- QueueAtCapacity - if the destination queue is at capacity and the contact cannot be queued within it.
- NoMatchingError - if no other Error matches.

Restrictions

This action is supported in contact flows and transfer flows. It is not supported in whisper flows, customer queue flows, or hold flows.

Corresponding block in the UI

Transfer to queue (p. 437)

UpdateContactAttributes

Behaving the same as the public API, this sets a collection of contact attributes. With this type of operation, either all attributes are set or none are set.

Parameter object

```
{
    "Attributes": { an Object that holds the attributes to be set.
        "Key": "Value" Both the key and value may be defined statically or dynamically.
    }
}
```

Results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

None. This can be used in any type of flow and any channel.

Corresponding block in the UI

Set contact attributes (p. 399)

UpdateContactCallbackNumber

Updates the contact callback number, which is the number used by the CreateCallbackContact action. This value defaults to the customer participant caller ID if this action is never used.

Parameter object

```
{
    "CallbackNumber": The callback number to set. Must be a single, valid JSONPath
 reference, and cannot be set statically.
}
```

Results and conditions

None.

Errors

- InvalidCallbackNumber - The callback number specified was not a valid (e.164) phone number.

- CallbackNumberNotDialable - The callback number specified is not dialable by the instance.

Restrictions

This is supported only in contact flows, transfer flows, and customer queue flows. This is not supported in whispers or hold flows.

Corresponding block in the UI

Set callback number (p. 397)

UpdateContactEventHooks

Sets one or more contact event hooks, which are flows associated with contact events, such as customer whisper or agent hold. For more information, see the section called “Contact events data model” (p. 980).

Parameter object

```
{
    "EventHooks": { an Object that holds the event hooks to be set. Only one entry may be
 present in this map.
        "Key": "Value" - the event hook to be set where the key is the event type and the
 value is the contact flow ID or ARN to run when that event occurs. Keys must be defined
 statically.
    }
}
```

Results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This is supported in all types of flows.

Corresponding blocks in the UI

- Set customer queue flow (p. 402)
- Set hold flow (p. 405)
- Set whisper flow (p. 418)

UpdateContactMediaStreamingBehavior

Enables or disables contact media streaming for a set of participants.

Parameter object

```
{
    "MediaStreamingState": One of "Enabled" or "Disabled". Must be specified statically.
    "Participants": [  A list of participants to include in the stream if enabling the
 stream, or disable if disabling the stream
```

```
        {
            "ParticipantType": The type of participant to stream. Currently, only
 "Customer" is supported. Must be defined statically.
            "MediaDirections": [ ] A list of the directions of media to include in the
 stream - "From" and "To".  Must be defined statically.
        }
    ],
    "MediaStreamType": The type of media to enable or disable from the stream. Currently,
 only "Audio" is supported. Must be defined statically.
}
```

Results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This is supported in contact flows, customer queue flows, transfer flows, and whisper flows. It is not supported in hold flows.

This is supported only by the voice channel.

Corresponding block in the UI

Start media streaming (p. 423) and Stop media streaming (p. 425)

UpdateContactRecordingBehavior

Sets contact recording behavior, including analysis behavior and which participants of the contact to record.

Parameter object

```
{
    "RecordingBehavior": { an object that holds the recording behavior
        "RecordedParticipants": [ ] a list of participants to record, chosen from "Agent"
 and "Customer". An empty list disables recording. Must be set statically.
    }
    "AnalyticsBehavior": { an object that holds the analytics behavior. Can only be set if
 the RecordedParticipants contains both Agent and Customer
        "Enabled": either "True" or "False". Must be set statically.
        "AnalyticsLanguage": Must be one of languages supported by Contact Lens post-call
 analysis. Must be set statically. Use the format xx-XX, for example, en-US for US English.
        "AnalyticsRedactionBehavior": either Enabled or Disabled. Defaults to Disabled if
 not set. Determines whether to redact sensitive data, such as personal information, in the
 Contact Lens output file and audio recording.
        "AnalyticsRedactionResults": either "RedactedAndOriginal" or "RedactedOnly". Can be
 set dynamically. Determines whether the customer gets both the redacted and the original
 transcripts and audio files, or just the redacted transcripts and audio files.
    }
}
```

For a list of languages supported by Contact Lens post-call analysis, see Contact Lens for Amazon Connect (p. 7). For the 4-character language code to use, see Supported languages in the *Amazon Transcribe Developer Guide*.

Results and conditions

None.

Errors

None.

Restrictions

This is supported only in contact flows, transfer flows, outbound whispers, and customer queue flows. This is not supported in agent/customer whispers or hold flows.

Analytics is only supported by the voice channel.

Corresponding block in the UI

Set recording and analytics behavior (p. 408)

UpdateContactRoutingBehavior

Updates the contact's routing details. This can move the contact forward or backward in queue, or specify a queue priority.

Parameter object

```
{
   "QueuePriority": An integer that represents the queue priority to be applied to
 the contact (lower priorities are routed preferentially). Cannot be specified if the
 QueueTimeAdjustmentSeconds or RoutingProficiencies is specified. Must be statically
 defined, must be larger than zero, and a valid integer value
   "QueueTimeAdjustmentSeconds": An integer that represents the queue time adjust
 to be applied to the contact, in seconds (longer / larger queue time are routed
 preferentially).pecified if the QueuePriority or RoutingProficiencies is specified. Must
 be statically defined and a valid integer value
}
```

Results and conditions

None.

Errors

None.

Restrictions

This is supported only in contact flows. It is not supported in transfer flows, whisper flows, customer queue flows, or hold flows.

Corresponding block in the UI

Change routing priority / age (p. 325)

UpdateContactTargetQueue

Sets the contact's TargetQueue. This is the queue is used by all other instructions that check a queue implicitly, and for TransferContactToQueue.

Parameter object

```
{
  "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not
 be specified. This must be either defined fully statically or as a single valid JSONPath
 identifier.
  "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId
 is specified, this may not be specified. This must be either defined fully statically or
 as a single valid JSONPath identifier.
}
```

Results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported only in contact flows and transfer flows. It is not supported in whisper flows, hold flows, or customer queue flows.

Corresponding block in the UI

Set customer queue flow (p. 402)

UpdateContactTextToSpeechVoice

Updates the Amazon Polly voice used by text-to-speech for voice contacts (message with text-to-speech, or Amazon Lex bots). This defaults to Joanna if this action is never run.

Parameter object

```
{
    "TextToSpeechVoice": A string holding the name of an Amazon Polly voice. Must be
 defined statically. If this is an invalid text to speech voice, text to speech is no
 longer function for this contact.
    "TextToSpeechEngine": The engine associated with the Amazon Polly voice, if it is a
 neural voice. Must be defined statically.
}
```

Results and conditions

None.

Errors

None.

Restrictions

None. This action is supported in all flow types, and across all channels.

Corresponding block in the UI

Set voice (p. 415)

UpdatePreviousContactParticipantState

This action is primarily used to forceably prevent previous participants on the contact from observing the contact. Common use cases are disconnecting the agent that initiates a transfer when they transfer a contact to a secure destination, or putting the agent on hold when transferring to a quick connect that securely gathers customer input such as credit card numbers.

Parameter object

```
{
    "PreviousContactParticipantState": One of ["AgentOnHold", "CustomerOnHold", "OffHold"],
 which are only supported for voice contacts.
}
```

Execution results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported only in contact flows and transfer flows.

Corresponding block in the UI

Hold customer or agent (p. 383)

Flow control actions in the Amazon Connect Flow language

These actions don't have any side effects and are only used to determine the path through a flow. Certain data may not be available (such as contact data, if the action is determining its path based on contact data). These actions generally work in every circumstance.

A flow control action is an action that:

- Does not need a contact or a participant to succeed.
- Controls the behavior of the flow, by either enabling or disabling flow behavior (such as logging) or by choosing a branch when the flow runs.

Contents

CheckHoursOfOperation

Returns whether the specified hours of operation object (or the hours of operation object associated with the current queue if no hours of operation is referenced) is in hours or out of hours as its result, allowing comparisons against it.

Parameter object

```
{
  "HoursOfOperationId": [Optional] An hours of operation ID or hours of operation ARN.
 *Must be either fully static or fully dynamic*. If not specified, the TargetQueue's hours
 of operation for the contact are used
}
```

Results and conditions

True or **False** based on whether the hours of operation object specified is in hours or out of hours. There must be a Condition provided for Equals **True** and a Condition for Equals **False**, and no other conditions.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is available in inbound flows, transfer flows, and customer queue flows. It is not available to hold flows or to whisper flows.

Corresponding block in the UI

Check hours of operation (p. 333)

CheckMetricData

A shortcut single action to avoid using GetMetricData and Compare for a set of simple metrics. This action loads the specified metric data for the specified queue, and allows comparisons to the loaded value. For example, it loads number of contacts in queue, age of oldest contact in queue, number of agents staffed on the queue, number of agents available on the queue, or number of agents online on the queue.

Parameter object

```
{
  "MetricType": One of [NumberOfAgentsAvailable, NumberOfAgentsStaffed,
 NumberOfAgentsOnline, OldestContactInQueueAgeSeconds, NumberOfContactsInQueue]. **Dynamic
 values are not supported**,
  "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not be
 specified. *Dynamic values are supported*,
  "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId
 is specified, this may not be specified. *Dynamic values are supported*. If neither this
 nor QueueId are specified, the contact TargetQueue is used
}
```

Execution results and conditions

A number, representing the value of the metric that was requested. This can be used for conditions. If the MetricType is NumberOfAgents* then the only supported condition is "NumberGreaterThan 0", otherwise Equals and any Number* Operands are allowed.

Errors

- NoMatchingError - if no other Error matches.
- NoMatchingCondition - if no other Condition matches (only supported if the MetricType is OldestContactInQueueAgeSeconds or NumberOfContactsInQueue).

Restrictions

This action is only usable in contact flows, queue and agent transfers, and customer queue flows. It is not available in any type of whisper or hold flows.

Corresponding block in the UI

None.

CheckOutboundCallStatus

Engages with the output provided by an answering machine, and provides branches to route the contact accordingly.

Parameter object

```
{

}
```

Execution results and conditions

- "CallAnswered" if the call has been answered by a person.
- "VoicemailBeep" if Amazon Connect identifies that the call ended in a voice mail and it detects a beep.
- "VoicemailNoBeep" if Amazon Connect identifies that call ended in a voicemail, but it doesn't detect a beep, or the beep is unknown.
- "NotDetected" if Amazon Connect could not detect whether there is a voicemail. This happens when Amazon Connect is unable to make a positive determination of whether a call was answered by a live voice or an answering machine. Typical situations that result in this state include long silences or excessive background noise.

Conditions are supported, but only the "Equals" operator is supported. "CallAnswered", "VoicemailBeep" , "VoicemailNoBeep" and "NotDetected" are the only supported operands.

Errors

- NoMatchingError if no condition matches.

Restrictions

This action works with high-volume outbound communications (p. 215) only. It is in public preview and not available in all Regions.

Corresponding block in the UI

Check call progress (p. 327)

CheckVoiceId

Checks the enrollment status, voice authentication or fraud detection results of the voice analysis returned by Voice ID.

Parameter object

```
{
 "CheckVoiceIdOption": "enrollmentStatus"
}
```

```
{
 "CheckVoiceIdOption": "voiceAuthentication"
}
```

```
{
 "CheckVoiceIdOption": "fraudDetection"
}
```

Execution results and conditions

The checkVoiceId action returns results of the voice analysis and the status returned by Voice ID. The following is returned when CheckVoiceIdOption input is set as:

- **enrollmentStatus**:
  - **Enrolled**: The caller is enrolled in voice authentication.
  - **Not enrolled**: The caller has not yet been enrolled in voice authentication. When this status is returned, for example, you may want to directly route the call to an agent for enrollment.
  - **Opted out**: The caller has opted out of voice authentication.

  You are not charged for checking enrollment status.
- **voiceAuthentication**:
  - **Authenticated**: The caller's identity has been verified. That is, the authentication score is greater than or equal to the threshold (default threshold of 90 or your custom threshold).
  - **Not authenticated**: The authentication score is lower than threshold that you configured.
  - **Inconclusive**: Unable to analyze a caller's speech for authentication. This is usually because Voice ID did not get the required 10 seconds to provide a result for authentication.
  - **Not enrolled**: The caller has not yet been enrolled in voice authentication. When this status is returned, for example, you may want to directly route the call to an agent for enrollment.
  - **Opted out**: The caller has opted out of voice authentication.

  You are not charged if the result is **Inconclusive**, **Not enrolled** or **Opted out**.
- **fraudDetection**:
  - **High risk**: The risk score meets or exceeds the set threshold.
  - **Low risk**: The risk score did not meet the set threshold.
  - **Inconclusive**: Unable to analyze a caller's voice for detection of fraudsters in a watchlist.

Errors

- NoMatchingError if no condition matches.

Restrictions

Only supported for voice channel. If used with the chat or task channels, the action takes the **Error** branch.

Corresponding block in the UI

Check Voice ID (p. 339)

Compare

Allows comparisons against the specified value.

Parameter object

```
{
  "ComparisonValue": Any **single** JSONPath identifier that is valid for the contact flow
 data object
}
```

Execution results and conditions

The value specified for comparison. This can be used for conditions.

Errors

- NoMatchingCondition - if no other Condition matches.

Restrictions

This action is available in every type of flow.

Corresponding block in the UI

Check contact attributes (p. 329)

DistributeByPercentage

Returns a random number between 1 and 100 (inclusive) as its result, allowing comparisons against it.

Parameter object

```
{

}
```

Results and conditions

A number between 1 and 100, inclusive, chosen randomly. Comparisons are supported, but they must be a chain of NumericLessThan comparisons, with each subsequent comparison checking the previous value, plus the percentage that is desired to go down this next action, and no Comparison comparing a value larger than 100.

Errors

- NoMatchingCondition if no Condition matches. This is the default option in the contact flow editor.

Restrictions

This action is available in inbound flows, transfer flows, and customer queue flows. It is not available to hold flows or to whisper flows.

Corresponding block in the UI

Distribute by percentage (p. 363)

EndFlowExecution

Finishes flow, but does not explicitly disconnect the participant. The participant may be disconnected by contact logic after this. For example, if a contact flow ends before the contact is put into queue, ending the flow results in the contact being ended.

Parameter object

```
{

}
```

Results and conditions

None. No conditions are supported.

Errors

None. This is always a terminal action.

Restrictions

This action is available only in whisper flows and customer queue flows. It is not available in contact flows, hold flows, or transfer flows.

Corresponding block in the UI

End flow / Resume (p. 365)

GetMetricData

Loads real time queue metrics for the queue specified by queue ID, agent ID (for agent queues), or the target queue, and makes them available on the flow run data. May be extended in the future to allow getting historical metric data in addition to current metric data, and to getting agent metrics in addition to queue metrics.

Parameter object

```
{
  "QueueId": [Optional] A queue ID or queue ARN. If AgentId is specified, this may not be
 specified. *Dynamic values are supported*,
  "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId
 is specified, this may not be specified. *Dynamic values are supported*
  "QueueChannel": [Optional] Either "Voice" or "Chat". Can be set dynamically. Determines
 the channel for which metrics are returned. If not specified, metrics are returned for all
 channels.
}
```

Execution results and conditions

None. No conditions are supported.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is available in every type of flow.

Corresponding block in the UI

Get queue metrics (p. 378)

Loop

When the same action (the same Action Identifier) is run multiple times, this block returns a result of "NotDone" a number of times equal to the specified loop count, then "Done" once, then reset.

Parameter object

```
{
    "LoopCount": Number of times to loop, must be between 0 and 100 (inclusive). Must
 either be fully static or fully dynamic.
}
```

Execution results and conditions

"ContinueLooping" if the loop should continue. "DoneLooping" if the loop should finish. Conditions are supported, there must be a Condition provided for Equals ContinueLooping and for Equals DoneLooping, and no other Conditions can be specified.

Errors

None.

Restrictions

This is supported in every type of flow.

Corresponding block in the UI

Loop (p. 388)

StartVoiceIdStream

Sends audio to Amazon Connect Voice ID to verify the caller's identity and match against fraudsters in watchlist, as soon as the call is connected to a flow.

Parameter object

```
{

}
```

Execution results and conditions

None. No conditions are supported.

Errors

- NoMatchingError if no condition matches.

Restrictions

Only supported for the voice channel. If used with the chat or task channels, the action takes the **Error** branch.

Corresponding block in the UI

Set Voice ID (p. 410)

TransferToFlow

Execution jumps to a different flow, and continues running at that flow's beginning.

Parameter object

```
{
    "ContactFlowId": A contact flow ID or contact flow ARN. *Must be either fully static or
 a single valid JSONPath identifier*
}
```

Execution results and conditions

None.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is available in inbound flows and transfer flows. It is not available to hold flows, customer queue flows, or whisper flows.

Corresponding block in the UI

Transfer to flow (p. 431)

UpdateFlowLoggingBehavior

Enables or disables flow logging. If this is a contact flow, this same behavior remains unless it is overridden for the rest of the contact segment. It is also automatically inherited by new segments in the chain.

Parameter object

```
{
  "FlowLoggingBehavior": One of [Enabled,Disabled]. *Dynamic values are not supported*
}
```

Results and conditions

None. No conditions are supported.

Errors

None.

Restrictions

This action is available in every type of flow.

Corresponding block in the UI

Set logging behavior (p. 407)

Wait

Pauses the flow for a specified duration, or until a specified event happens, whichever happens first.

Parameter object

```
{
    "TimeoutSeconds": The amount of time to wait before the action finishes with the
 "WaitCompleted" result. This can be either statically defined, or a single valid JSONPath
 identifier. If defined statically, this must be a positive integer value no greater than
 604800 (seven days),
    "Events": An optional list of all events that can trigger an interrupt. The only
 supported event currently is "CustomerReturned". This must be defined statically.
}
```

Execution results and conditions

If an event interrupts the wait, the run result is the event that interrupted. If no event interrupts the Wait and the time elapses, the run result is WaitCompleted. Conditions are supported, but only the "Equals" operator is supported. "WaitCompleted" is always required operand, and every specified event is also required to be present as a condition operand.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This is supported in every type of flow, but is supported only by the chat channel.

Corresponding block in the UI

Wait (p. 441)

Interactions in the Amazon Connect Flow language

Interactions actions have side effects, but they don't require a contact or a participant. They include actions such as invoking an AWS Lambda function. They generally work in every circumstance.

Contents

CreateCallbackContact

Creates a new callback contact. If no customer number is specified, and this is run in context of a contact, the contact's CustomerCallbackNumber is used as the customer number.

Parameter object

```
{
    "QueueId": [Optional] A queue ID or queue ARN. The callback contact is routed with this
 queue, or if this is not specified, the contact's current TargetQueue. Must be specified
 fully statically or with a single valid JSONPath identifier.
    "AgentId": [Optional] An agent ID or agent ARN, representing an agent queue. If QueueId
 is specified, this may not be specified. This must be either defined fully statically or
 as a single valid JSONPath identifier.
    "InitialCallDelaySeconds": The amount of time, in seconds, to wait at a minimum before
 routing the callback contact. This gives the customer enough time to end their existing
 contact before being called back. Must be larger than 0, no greater than 259,200 (three
 days), and an integer. Must be defined statically.
    "MaximumConnectionAttempts": The number of attempts at a maximum to connect this
 contact to a customer, if the callback is not answered. Must be larger than zero, and an
 integer. Must be defined statically.
    "RetryDelaySeconds": The minimum amount of time to wait, in seconds, between an
 unanswered callback attempt is made and the next attempt to reach the customer. Must
 be larger than 0, no greater than 259,200 (three days), and an integer. Must be defined
 statically.
}
```

Results and conditions

None. No conditions are supported.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported in contact flows, transfer flows, and customer queue flows. It is not supported in whisper flows or hold flows.

Corresponding block in the UI

Set callback number (p. 397)

CreateCustomerProfile

Create a customer profile.Customer Profiles must be enabled for your Amazon Connect instance.

See CreateProfile in the *Amazon Connect Customer Profiles API Reference*.

Parameter object

```
{
    "ProfileRequestData": {
    All of these fields are optional.
       "FirstName",
       "LastName",
       "PhoneNumber",
       "EmailAddress",
       "AccountNumber",
       "Address1",
       "Address2",
       "Address3",
       "Address4",
       "City",
       "Country",
       "County",
       "PostalCode",
       "Province",
       "State"
    },
   "ProfileResponseData": {
       All of these fields are optional.
       Newly created profile ID is persisted under the Customer -> ProfileID attribute +
 $.Customer.ProfileId
       "FirstName",
       "LastName",
       "PhoneNumber",
       "EmailAddress",
       "AccountNumber",
       "Address1",
       "Address2",
       "Address3",
       "Address4",
       "City",
       "Country",
       "County",
       "PostalCode",
       "Province",
       "State"
   }
}
```

Results and conditions

None. Conditions are not supported. If an error does not occur, the response's attributes are available dynamically under the `$.Customer` path based on the attributes included in `ProfileResponseData`.

Errors

- NoMatchingError - if no other Error matches.

Corresponding block in the UI

Customer profiles (p. 359)

GetCustomerProfile

Retrieve a customer profile based on email or phone number. Customer Profiles must be enabled for your Amazon Connect instance.

See SearchProfiles in the *Amazon Connect Customer Profiles API Reference*.

Parameter object

A search key (phone number or email) must be present.

```
{
    "ProfileRequestData": {
       "PhoneNumber": Phone number to search for profiles with.
       "EmailAddress": Email address to search for profiles with.
    },
   "ProfileResponseData": {
       All of these fields are optional.
       Profile ID, if a single profile is found, is always persisted under the Customer ->
 ProfileID attribute + $.Customer.ProfileId
       "FirstName",
       "LastName",
       "PhoneNumber",
       "EmailAddress",
       "AccountNumber",
       "Address1",
       "Address2",
       "Address3",
       "Address4",
       "City",
       "Country",
       "County",
       "PostalCode",
       "Province",
       "State"
   }
}
```

Results and conditions

None. Conditions are not supported. If an error does not occur, the response's attributes are available dynamically under the `$.Customer` path based on the attributes included in `ProfileResponseData`.

Errors

- MultipleFoundError - if multiple profiles were found for the associated profile search key.
- NoneFoundError - if no profiles were found for the associated profile search key.
- NoMatchingError - if no other Error matches.

Corresponding block in the UI

Customer profiles (p. 359)

UpdateCustomerProfile

Update a customer profile that was previously created or retrieved in the flow. Customer Profiles must be enabled for your Amazon Connect instance.

See UpdateProfile in the *Amazon Connect Customer Profiles API Reference*.

Parameter object

```
{
    "ProfileRequestData": {
    All of these fields are optional.
       "FirstName",
       "LastName",
       "PhoneNumber",
       "EmailAddress",
       "AccountNumber",
       "Address1",
       "Address2",
       "Address3",
       "Address4",
       "City",
       "Country",
       "County",
       "PostalCode",
       "Province",
       "State"
    },
   "ProfileResponseData": {
       All of these fields are optional.
       "FirstName",
       "LastName",
       "PhoneNumber",
       "EmailAddress",
       "AccountNumber",
       "Address1",
       "Address2",
       "Address3",
       "Address4",
       "City",
       "Country",
       "County",
       "PostalCode",
       "Province",
       "State"
   }
}
```

Results and conditions

None. Conditions are not supported. If an error does not occur, the response's attributes are available dynamically under the `$.Customer` path based on the attributes included in `ProfileResponseData`.

Errors

- NoMatchingError - if no other Error matches.

Corresponding block in the UI

Customer profiles (p. 359)

InvokeLambdaFunction

Invokes an AWS Lambda function with a collection of optional parameters. This AWS Lambda function is also given a copy of the flow run data if there is an associated contact with the flow.

Parameter object

```
{
    "LambdaFunctionARN": The ARN of the AWS Lambda function to be invoked. May be defined
 statically or dynamically.
    "InvocationTimeLimitSeconds": The number of seconds to wait for a response from the AWS
 Lambda function. Must be greater than 0, no larger than 8, and an integer. Must be set
 statically.
```

```
    "LambdaInvocationAttributes" { A map of additional data to send to the AWS Lambda
 function when invoking it. Keys and values may be set statically or dynamically.
    }
}
```

Results and conditions

None. Conditions are not supported. If an error does not occur, the response's attributes are available dynamically under the $.External path.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

None. This action is supported by all channels and in all types of flows.

Corresponding block in the UI

Invoke AWS Lambda function (p. 385)

Participant actions in the Amazon Connect Flow language

Participant actions are attempted only when the flow is run in context of a participant. They generally result in an action that the participant experiences, such as playing a prompt or disconnecting.

Contents

ConnectParticipantWithLexBot

Connects the participant with the specified Amazon Lex bot. When the interaction is over, the Intent and Slots of the bot are available to the flow during its run.

Parameter object

Provide either LexBot or LexV2Bot object depending on the Amazon Lex version in the following format.

Amazon Lex

```
{
    "PromptId": [Optional] A prompt ID or prompt ARN to play to the participant along
 with gathering input. May not be specified if Text or SSML is also specified. Must be
 specified either statically or as a single valid JSONPath identifier.
    "Text":  An optional string that defines text to send to the participant along with
 gathering input. May not be specified if PromptId or SSML is also specified. May be
 specified statically or dynamically.
    "SSML": An optional string that defines SSML to send to the participant along with
 gathering input. May not be specified if Text or PromptId is also specified May be
 specified statically or dynamically.
```

```
    "Media": { An optional object that defines an external media source
        "Uri": Location of the message
        "SourceType": The source from which the message will be fetched. The only
 supported type is S3
        "MediaType": The type of the message to be played. The only supported type is
 Audio
    }
    "LexV2Bot": { The details of the LexV2 bot to invoke
        "AliasArn": The alias ARN of the LexV2 bot to invoke. May be specified
 statically or dynamically.
    },
    "LexSessionAttributes: { A map of session attributes to pass to the Amazon LexV2
 bot when it is invoked. The keys and values may be static or dynamic.
    }
}
```

Amazon Lex (Classic)

```
{
    "PromptId": [Optional] A prompt ID or prompt ARN to play to the participant along
 with gathering input. May not be specified if Text or SSML is also specified. Must be
 specified either statically or as a single valid JSONPath identifier.
    "Text":  An optional string that defines text to send to the participant along with
 gathering input. May not be specified if PromptId or SSML is also specified. May be
 specified statically or dynamically.
    "SSML": An optional string that defines SSML to send to the participant along with
 gathering input. May not be specified if Text or PromptId is also specified May be
 specified statically or dynamically.
    "Media": { An optional object that defines an external media source
        "Uri": Location of the message
        "SourceType": The source from which the message will be fetched. The only
 supported type is S3
        "MediaType": The type of the message to be played. The only supported type is
 Audio
    }
    "LexBot": { The details of the Lex bot to invoke
        "Name": The name of the Lex bot. May be specified statically or dynamically.
        "Region": The region in which this Lex bot exists. May be specified statically
 or dynamically.
        "Alias": The specific alias of the Lex bot to invoke. May be specified
 statically or dynamically.
    },
    "LexSessionAttributes: { A map of session attributes to pass to the Amazon Lex bot
 when it is invoked. The keys and values may be static or dynamic.
    }
}
```

Results and conditions

If the Amazon Lex interaction succeeds, the result is the Intent of the bot. Conditions are supported, but only the Equals operator is supported within these conditions.

Errors

- NoMatchingCondition - If no specified condition evaluated to True.
- NoMatchingError - If an error occurred and no other error matched.

Restrictions

This action is supported by all channels.

This action is available only in contact flows, transfer flows, and customer queue flows. It is not available in whisper flows or hold flows.

Corresponding block in the UI

Get customer input (p. 366)

DisconnectParticipant

Disconnects the participant from the contact and stops this flow from running.

Parameter object

No parameters are expected.

Results and conditions

None. Conditions are not supported.

Errors

None.

Restrictions

None. This action can be used everywhere. If there is no participant on the contact, this functions as an EndFlowExecution action, and halts the flow from running.

Corresponding block in the UI

Disconnect / hang up (p. 362)

GetParticipantInput

Gathers customer input (a DTMF collection for voice contacts, or an entered string for other channels). There are many optional behaviors after gathering this: encryption, validation, storing to a "LastParticipantInput" section on the flow run data, specifying a custom DTMF terminator for voice contacts and so on. Details are in the parameter object section.

Parameter object

```
{
    "PromptId": [Optional] A prompt ID or prompt ARN to play to the participant along with
 gathering input. May not be specified if Text or SSML is also specified. Must be either
 statically defined or a single valid JSONPath identifier.
    "Text":  An optional string that defines text to send to the participant along with
 gathering input. May not be specified if PromptId or SSML is also specified. May be
 defined statically or dynamically.
    "SSML": An optional string that defines SSML to send to the participant along with
 gathering input. May not be specified if Text or PromptId is also specified. May be
 defined statically or dynamically.
    "Media": { An optional object that defines an external media source
        "Uri": Location of the message
        "SourceType": The source from which the message will be fetched. The only supported
 type is S3
        "MediaType": The type of the message to be played. The only supported type is Audio
    }
    "InputTimeoutSeconds": The number of seconds to wait for input to be collected before
 proceeding with a timeout error. For the Voice channel this is the timeout until the
 *first* DTMF digit is entered. Must be defined statically, and must be a valid integer
 larger than zero.
    "StoreInput": "True" or "False". Must be statically defined.
    "InputValidation": { An object that defines how to validate customer inputs, required
 if and only if StoreInput is True
        "PhoneNumberValidation": { Optional, one of the ways to validate inputs, make sure
 that it's a valid phone number. May not be specified if CustomValidation is specified.
             "NumberFormat": "Local" or "E164". If "Local" is specified, it is validated to
 be a local number (without the + and the country code), "E164" enforces that the customer
 input is a fully defined e.164 phone number. Must be defined statically.
             "CountryCode": If the number format is "Local", this must be defined. This is
 the two letter country code to be associated with the input number when validating. Must
 be defined statically.
        }
        "CustomValidation": { Optional, the other way to validate inputs. May not be
 specified if PhoneNumberValidation is specified.
            "MaximumLength": A number representing the maximum length of the input. Must be
 defined statically.
        }
    },
    "InputEncryption": { An optional object that defines how to encrypt the customer input.
 May only be specified if "CustomValidation" is provided.
        "EncryptionKeyId": The identifier of a key that has been uploaded in the AWS
 console for the purposes of customer input encryption. May be specified statically or
 dynamically.
        "Key": The PEM definition of the public key to use to encrypt this data. This key
 must be signed with the encryption key identified by the EncryptionKeyId. May be specified
 statically or dynamically.
    },
    "DTMFConfiguration": { An optional object to override default DTMF behavior for voice
 calls
        "InputTerminationSequence": Up to five digits to serve as the terminating sequence
 when gathering DTMF
        "DisableCancelKey": "True" or "False". If "True", the "*" key doesn't cancel
 gathering DTMF digits.
    }
}
```

Results and conditions

If the "StoreInput" option is "True", there is no run result and conditions are not supported. If the "StoreInput" option is not defined or is "False", the run result is the participant input, and conditions are supported but only the Equals operator may be used on conditions. The values being compared must be static and be a single character - 0-9 numeric, *, or #.

Errors

- NoMatchingCondition - None of the specified conditions evaluated to true. Must be defined only if StoreInput is False.
- NoMatchingError - if no other Error matches. Must always be defined.
- InvalidPhoneNumber - the stored input was not a valid phone number according to the specified PhoneNumberValidation. Must be defined only if StoreInput is true, and PhoneNumberValidation is specified.

Restrictions

This action is only supported on the voice channel.

This action can be used in contact flows, transfer flows, and customer queue flows but not in whisper flows or hold flows.

Corresponding block in the UI

Get customer input (p. 366)

MessageParticipant

Sends a message to the participant. This is an audio prompt or text-to-speech for voice contacts, or a text message for other channels.

Parameter object

```
{
    "PromptId": [Optional] A prompt ID or prompt ARN to play to the participant along with
 gathering input. May not be specified if Text or SSML is also specified. Must be specified
 either statically or as a single valid JSONPath identifier.
    "Text":  An optional string that defines text to send to the participant along with
 gathering input. May not be specified if PromptId or SSML is also specified. May be
 specified statically or dynamically.
    "SSML": An optional string that defines SSML to send to the participant along with
 gathering input. May not be specified if Text or PromptId is also specified May be
 specified statically or dynamically.
    "Media": { An optional object that defines an external media source
        "Uri": Location of the message
        "SourceType": The source from which the message will be fetched. The only supported
 type is S3
        "MediaType": The type of the message to be played. The only supported type is Audio
    }
}
```

Results and conditions

None. No conditions are supported.

Errors

NoMatchingError - If an error occurred and no other error matched.

Restrictions

This action is supported in contact flows, transfer flows, whisper flows, and customer queue flows. It is not supported in hold flows.

"PromptId" and "SSML" are only supported for the voice channel. All other channels support only the "Text" option.

Corresponding block in the UI

Play prompt (p. 393)

MessageParticipantIteratively

Loops a sequence of prompts while a customer or agent is on hold or in queue. This block can be configured with an interruption timeout when in a Queue flow that interrupts the message loop to run other flow logic. The message loop can include entries for both Text and Prompts.

Parameter object

```
{
   "Messages" : [ A List of messages to be played in a loop. These are defined with either
 TTS or a Prompt
       {
         "Text" : An optional string that defines text to send to the participant
       },
       {
         "PromptId" : A prompt ID or prompt ARN to play to the participant
       },
       {
         "SSML" : An optional string that defines the ssml
       },
       {
         "Media": { An optional object that defines an external media source
           "Uri": Location of the message
           "SourceType": The source from which the message will be fetched. The only
 supported type is S3
           "MediaType": The type of the message to be played. The only supported type is
 Audio
         }
       }

   ],
   "InterruptFrequencySeconds" : [Optional] Time to elapse before the action completes with
 "MessagesInterrupted" run result
}
```

Results and conditions

When the timeout elapses, the action completes with the result as "MessagesInterrupted". Conditions are supported, but only the "Equals" operator is supported. The only supported operand is MessagesInterrupted.

Errors

- NoMatchingError - if no other Error matches.

Restrictions

This action is supported in Customer Queue, Customer Hold, and Agent Hold flows.

"PromptId" is supported only for the Voice channel, all other channels support only the "Text" option.

If this action is used on the chat channel, it immediately takes the error branch. If no error branch is available, the flow stop running and the contact is routed to next available agent.

Corresponding block in the UI

Loop prompts (p. 390)

TransferParticipantToThirdParty

Transfers the participant to a specified phone number. Optionally continues flow running if the third party disconnects while the participant is still connected.

Parameter object

```
{
    "ThirdPartyPhoneNumber": A phone number, in e.164 format, of the external number to
 which to transfer the contact. May be defined statically or dynamically.
    "ThirdPartyConnectionTimeoutSeconds": An integer, between 0 and 600 (inclusive)
 representing the number of seconds to wait for the third party to answer before canceling
 the third party call. Only used if ContinueFlowExecution is not False. Must be defined
 fully statically or as a single valid JSONPath identifier.
    "ContinueFlowExecution": "True" or "False". If not defined or True, the flow continues
 running after the third party call finishes, if False the flow does not continue, as long
 as the phone call to the third party succeeds. Must be defined statically.
    "ThirdPartyDTMFDigits": An optional series of DTMF digits to send to the third party
 when the call succeeds. Must be defined fully statically or as a single valid JSONPath
 identifier. Must be 50 or fewer characters chosen from numeric digits, comma, asterisk,
 and pound sign
    "CallerId": { Optional, an override of the caller ID to present when dialing the third
 party
        "Number": The caller ID number to present when dialing the third party. Must be
 defined fully statically or as a single valid JSONPath identifier.
        "Name": The caller ID name to present when dialing the third party. May be defined
 statically or dynamically.
    }
}
```

Results and conditions

None. Conditions are not supported.

Errors

- ConnectionTimeLimitExceeded - the call has taken longer than the specified time limit to be answered by the third party, and has been canceled. Supported only when ContinueFlowExecution is True.
- CallFailed - The call was unable to connect successfully. Only supported when ContinueFlowExecution is True.
- NoMatchingError - if no other Error matches.

Restrictions

This action is only allowed by the Voice channel.

This action is allowed in contact flows, transfer flows, and customer queue flows.

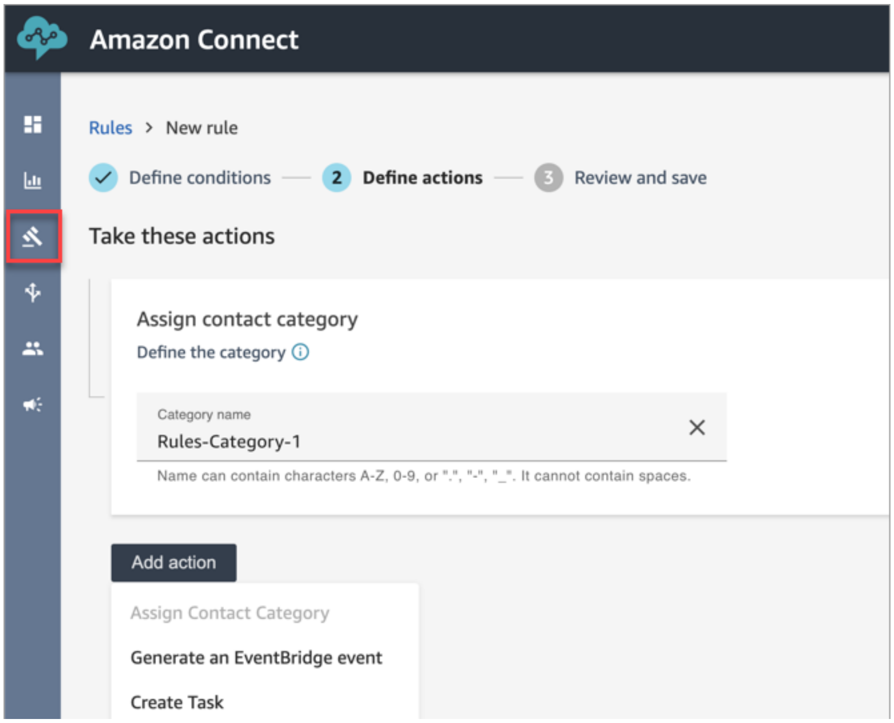
Corresponding block in the UI

Transfer to phone number (p. 433)

Create rules

A rule is an action that Amazon Connect automatically performs, based on conditions you specify. Contact center managers, supervisors and QA analysts can quickly create rules from the Amazon Connect console. No coding is required.

The following image shows the Rules user interface, and the actions available when you create a rule.



By creating rules, you can:

- Automatically categorize contacts.
- Send notifications about customer escalations.
- Display tips in the agent application.
- Assign supervisor tasks based on customer conversations.

Rules allow you to automate common and repeatable actions required for quality assurance, workforce management, and customer engagement. These actions are automated based on pre-defined trigger conditions that you define, such as keywords used on a contact, sentiment trend of a contact, frequent interruptions by agent on a contact, agents being silent for long-periods on a contact, filtering specific contact attributes or queues, and more.

Common usage scenarios

- For Contact Lens, you can create rules to automatically categorize contacts based on keywords and phrases uttered by the agent or the customer. You can also use rules with real-time contact lens to alert supervisors in real-time when a critical customer experience issue occurs and the agent requires live assistance.

- For coaching and escalation scenarios, you can create rules to automatically categorize contacts that are not meeting your compliance requirements and assign tasks for the agents to go through a certain training program on your organization's compliance policy.

Third-party integrations

Rules also provide third-party integrations with Contact Relationship Management (CRM) and IT service management (ITSM) vendors, such as Salesforce and Zendesk.

For example, you can create rules for whenever a new case or ticket is created in the Salesforce CRM or Zendesk ticket management system. You can set up the rule to automatically assign tasks to agents or supervisors based on the new case or ticket created, and to alert them to take necessary action. If you want to use email notification, you can automatically generate an EventBridge event that runs a custom email notification application to alert agents or supervisors. This enables contact center managers to integrate their existing CRM and ITSM solutions with Amazon Connect through rules, and to monitor the creation of new cases or tickets through tasks.

More information

- Alert supervisors in real-time based on keywords and phrases (p. 584)
- Automatically categorize contacts based on uttered keywords and phrases (p. 580)
- Create a task when a contact is categorized in real-time or post-call (p. 593)
- Create a Contact Lens rule that generates an EventBridge event (p. 589)
- Create rules that generate tasks for third-party integrations (p. 602)

Create rules with Contact Lens

Contact Lens rules allow you to automatically categorize contacts, receive alerts, or generate tasks based on uttered keywords, sentiment scores, customer attributes, and other criteria.

> **Tip**
> For a list of rules feature specifications (for example, how many rules you can create), see Amazon Connect Rules feature specifications (p. 1213).

Step 1: Define rule conditions

1. On the navigation menu, choose **Rules**.
2. Select **Create a rule**, **Contact Lens**.
3. Assign a name to the rule.
4. Under **When**, use the dropdown list to choose **post-call analysis** or **real-time analysis**.
5. Choose **Add condition**.

   You can combine criteria from a large set of conditions to build very specific Contact Lens rules. Following are the available conditions:

   - **Words or phrases**: Choose from Exact match, Pattern match, or Semantic match (p. 597) to trigger an alert or task when keywords are uttered.
   - **Agent**: Build rules that run on a subset of agents. For example, create a rule to ensure newly hired agents comply with company standards.

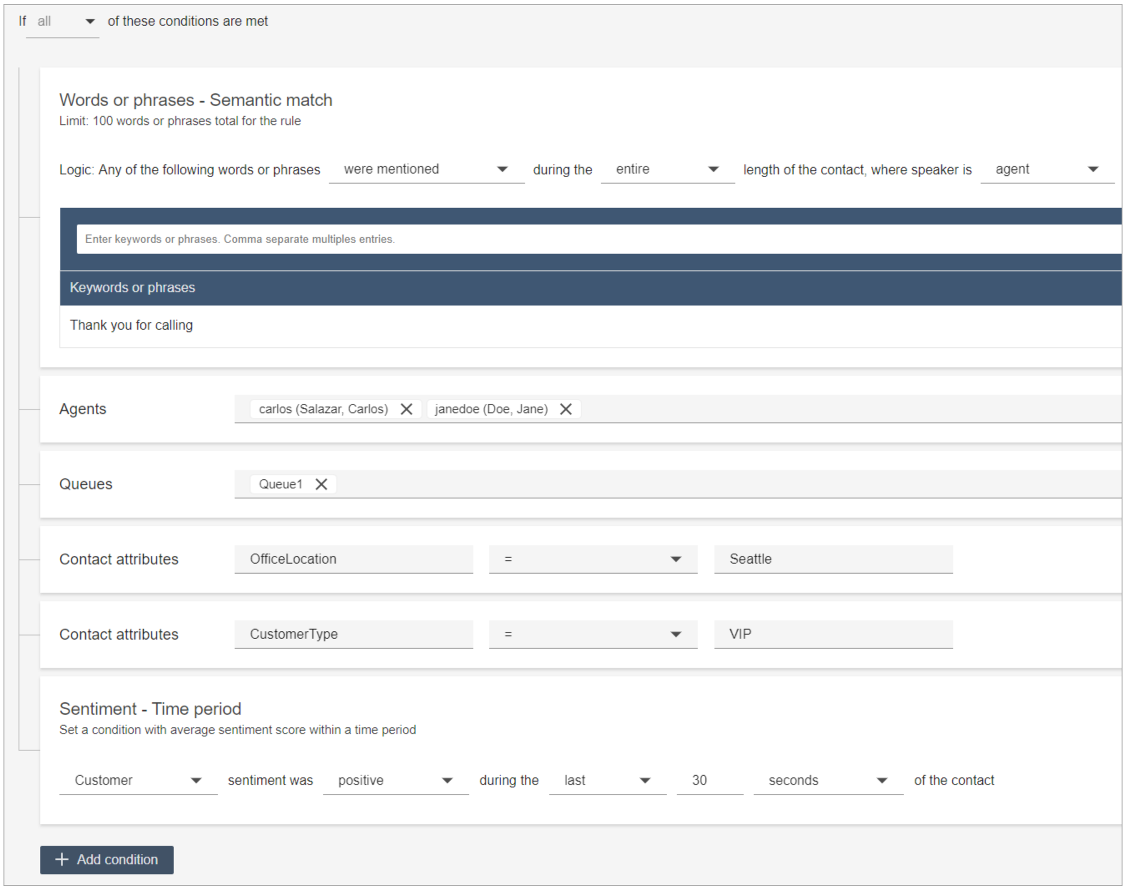
To see agent names so you can add them to rules, you need **Users - View** permissions in your security profile.

- **Queues**: Build rules that run on a subset of queues. Often organizations use queues to indicate a line of business, topic, or domain. For example, you could build rules specifically for your sales queues, tracking the impact of a recent marketing campaign or alternatively rules for your customer support queues, tracking overall sentiment.

  To see the queue names so you can add them to rules, you need **Queues - View** permissions in your security profile.
- **Contact attributes**: Build rules that run on the values of custom contact attributes (p. 515). For example, you can build rules specifically for a particular line of business or for specific customers, such as based on their membership level, their current country of residence, or if they have an outstanding order.

  You can add up to five contact attributes to a rule.
- **Sentiment - Time period**: Build rules that run on the sentiment analysis results (positive, negative, or neutral) over a trailing window of time. For example, you can build a rule for when customer sentiment has remained negative for a set period of time.
- **Sentiment - Entire contact**: Build rules that run on the value of sentiment scores over an entire contact. For example, you can build a rule when customer sentiment has remained low for the entire contact, you can create a task for a customer experience analyst to review the call transcript and follow-up.
- **Interruptions**: Build rules that detect when the agent has interrupted the customer for more than X times.
- **Non-talk time**: Build rules that run when periods of no talk time are detected. For example, when a customer and agent have not spoken for over 30 seconds which may indicate unnecessary customer wait time or highlight a customer services process that would benefit from optimisation.

Following is a sample rule with multiple conditions.



If all of these conditions are met

Words or phrases - Semantic match
Limit: 100 words or phrases total for the rule

Logic: Any of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Enter keywords or phrases. Comma separate multiples entries.

Keywords or phrases
Thank you for calling

Agents: carlos (Salazar, Carlos), janedoe (Doe, Jane)

Queues: Queue1

Contact attributes: OfficeLocation = Seattle

Contact attributes: CustomerType = VIP

Sentiment - Time period
Set a condition with average sentiment score within a time period

Customer sentiment was positive during the last 30 seconds of the contact

6. Choose **Next**.

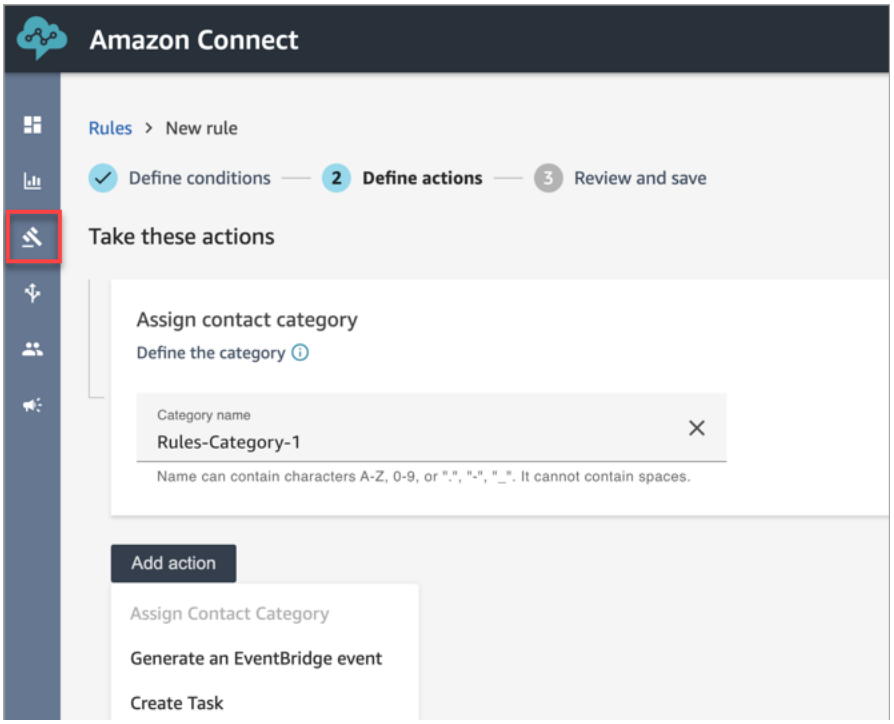
Step 2: Define rule actions

1. Under **Assign contact category**, enter a category name.

   Note
   In this step, you are naming a required rule action: **Assign Contact Category**. The action is to categorize all contacts based on the category name you create. The category name is reflected in the Contact Lens output.

2. Choose **Add action**. Since you already named **Assign Contact Category**, it's not available. You can choose the following:

   - Generate an EventBridge event (p. 589)
   - Create task (p. 593)



Take these actions

Assign contact category

Define the category

Category name: Rules-Category-1

Name can contain characters A-Z, 0-9, or ".", "-", "_". It cannot contain spaces.

3. Choose **Next**.
4. Review and make any edits, then choose **Save**.
5. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

   You cannot apply rules to past, stored conversations.

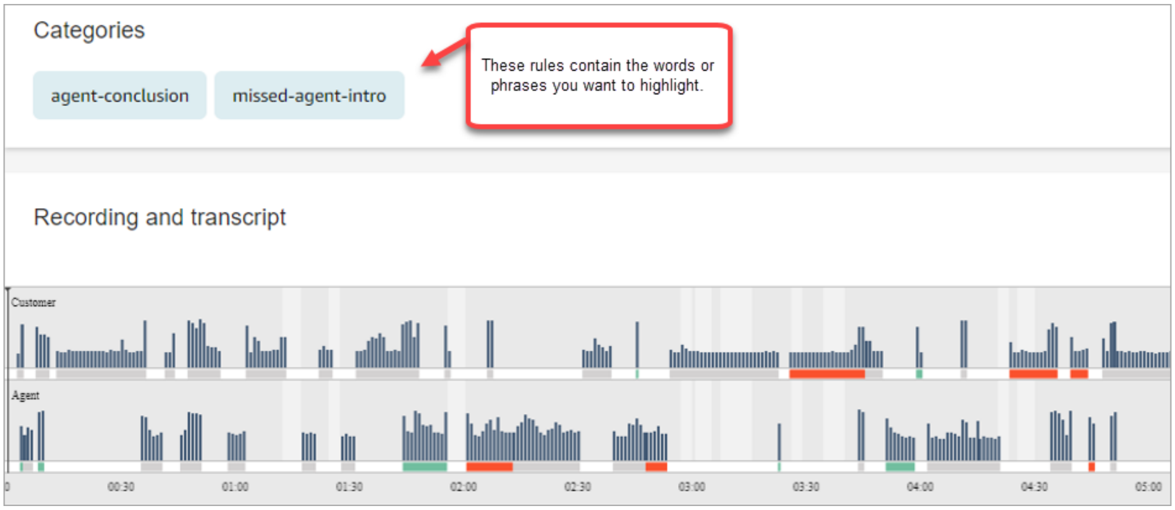
Automatically categorize contacts based on uttered keywords and phrases

You can set up Contact Lens to track issues that you know exist in your contact center ("known knowns"), and monitor any changes over time.

You can label your contacts with predefined criteria you set up, that is, keywords and phrases you want to detect. Through categorization, each contact is analyzed for these criteria, and labeled.

This is useful to do when, for example, you want to ensure that agents are speaking certain words or phrases for compliance reasons. Or, for example, you want to investigate when customers use certain words and have a negative sentiment.

To set up this feature, add rules that contain the words or phrases that you want to highlight.



Add rules to categorize contacts

Step 1: Define conditions

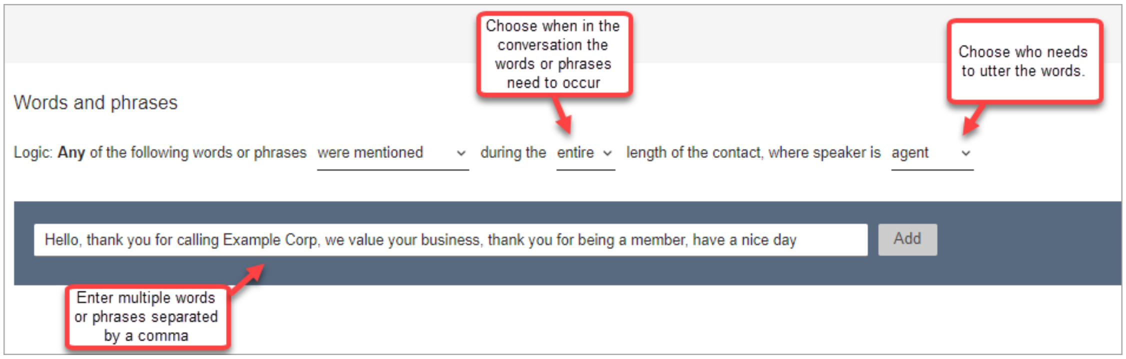
1. Log in to Amazon Connect with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for **Rules** permissions.
2. On the navigation menu, choose **Rules**.
3. Select **Create a rule**, **Contact Lens**.
4. Assign a name to the rule.
5. Under **When**, use the dropdown list to choose **post-call analysis** or **real-time analysis**.
6. Choose **Add condition**, and then choose the type of match:

   - **Exact Match**: Finds only the exact words or phrases.
   - **Semantic Match**: Finds words that may be synonyms. For example, if you enter "upset" it can match "not happy," or "hardly acceptable" can match with "unacceptable," and "unsubscribe" can match with "cancel subscription."

     Similarly, it can semantically match phrases. For example, "thank you so much for helping me out," "thanks a lot and this is so helpful," and "I am so happy that you are able to help me."

     This removes the need to define an exhaustive list of keywords while creating categories, and provides you the ability to cast a wider net for searching similar phrases that are important to you.

     For best semantic matching results, provide keywords or phrases with similar meaning within a semantic matching card. Currently, you can provide a maximum of four keywords and phrases per semantic matching card.
   - **Pattern Match**: Finds matches that may be less than 100 percent exact. You can also specify the distance between words. For example, if you are looking for contacts where the word "credit" was mentioned but you do not want to see any mention of the words "credit card," you can define a pattern matching category to look for the word "credit" that is not within a one-word distance of "card."
7. Enter the words or phrases, separated by a comma, that you want to highlight.



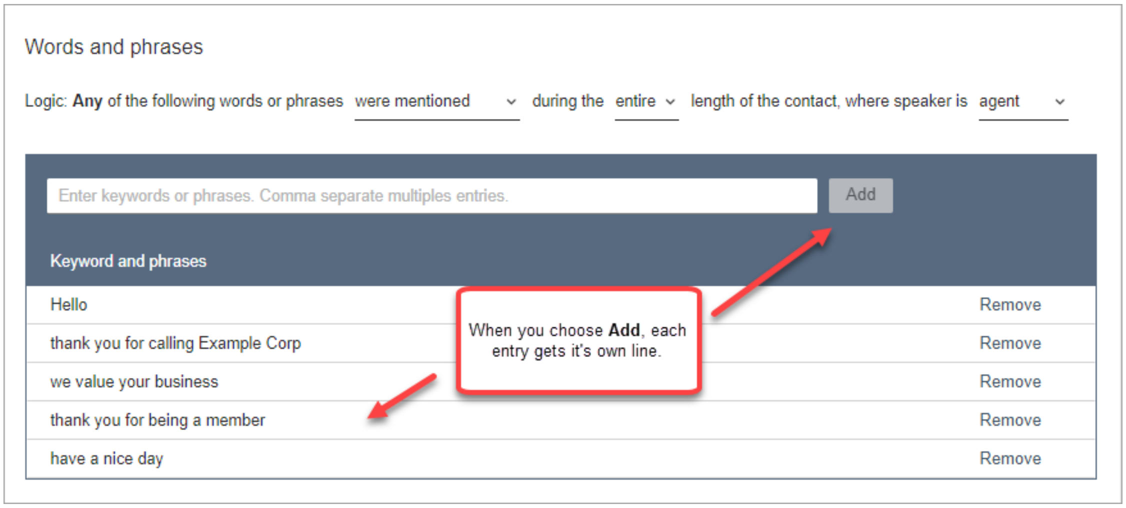
Words and phrases

Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Hello, thank you for calling Example Corp, we value your business, thank you for being a member, have a nice day

Add
Choose when in the conversation the words or phrases need to occur
Choose who needs to utter the words.
Enter multiple words or phrases separated by a comma

8. Choose **Add**. Each word or phrase separated by a comma gets its own line in the card.



Words and phrases

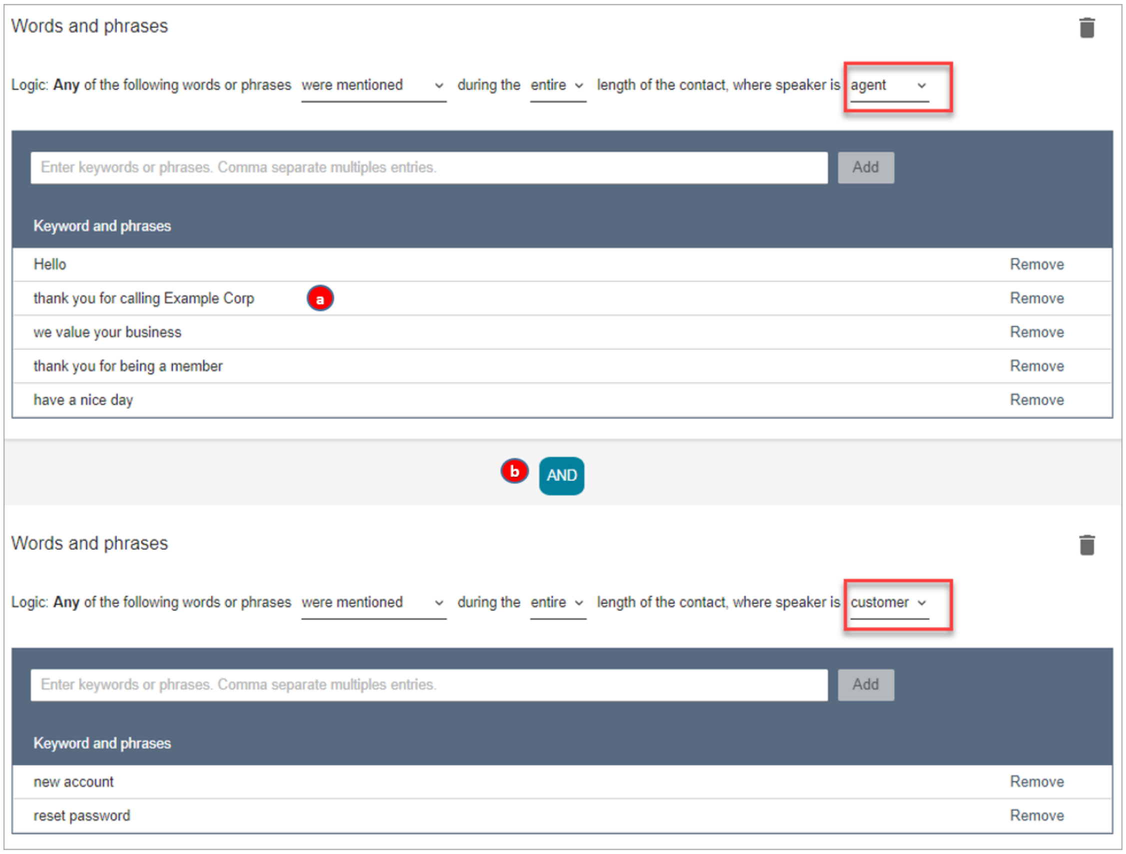
Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Enter keywords or phrases. Comma separate multiples entries.

Keyword and phrases	
Hello	Remove
thank you for calling Example Corp	Remove
we value your business	Remove
thank you for being a member	Remove
have a nice day	Remove

The logic that Contact Lens uses to read these words or phrases is: (Hello) OR (thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business), etc.

9. To add more words or phrases, choose **Add group of words or phrases**. In the following image, the first group of words or phrases are what the agent might utter, and the second group is what the customer might utter.



Words and phrases

Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Keyword and phrases	
Hello	Remove
thank you for calling Example Corp	Remove
we value your business	Remove
thank you for being a member	Remove
have a nice day	Remove

AND

Words and phrases

Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is customer

Keyword and phrases	
new account	Remove
reset password	Remove

Enter keywords or phrases. Comma separate multiples entries.
Add
a
b
Enter keywords or phrases. Comma separate multiples entries.
Add

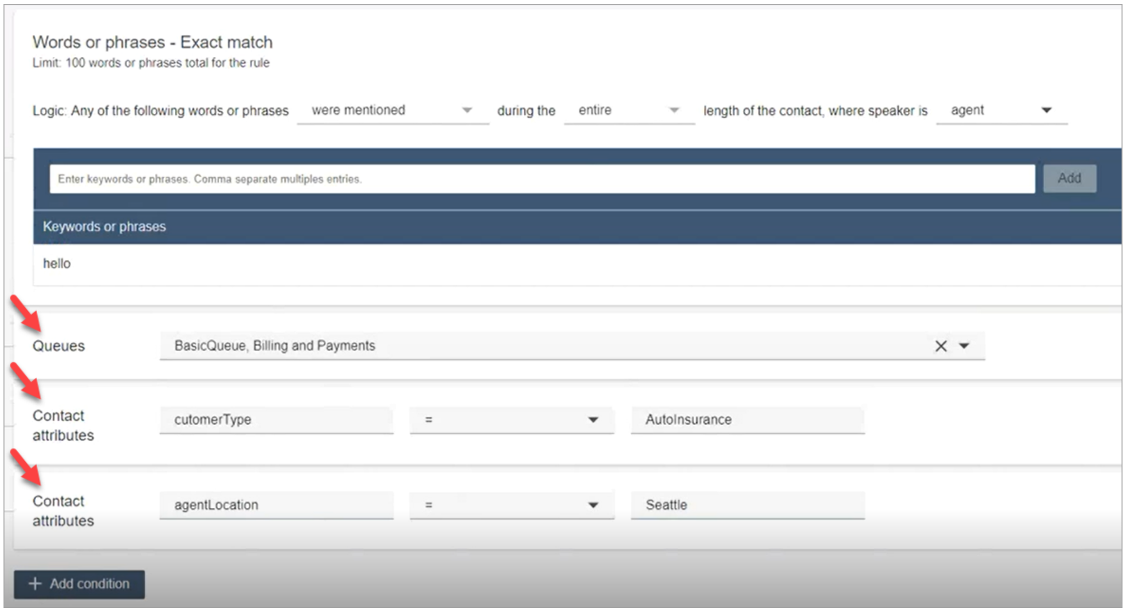
1. In this first card, Content Lens reads each line as an OR. For example: (Hello) OR (thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business).
2. The two cards are connected with an AND. This means, one of the rows in the first card needs to be uttered AND then one of the phrases in the second card needs to be uttered.

The logic that Contact Lens uses to read the two cards of words or phrases is (card 1) AND (card 2).

10. Choose **Add condition** to apply the rules to:

    - Specific queues
    - When contact attributes have certain values
    - When sentiment scores have certain values

    For example, the following image shows a rule that applies when an agent is working the BasicQueue or Billing and Payments queues, the customer is for autoinsurance, and the agent is located in Seattle.



Words or phrases - Exact match
Limit: 100 words or phrases total for the rule

Logic: Any of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Enter keywords or phrases. Comma separate multiples entries.

Keywords or phrases

hello

Queues: BasicQueue, Billing and Payments

Contact attributes: cutomerType = AutoInsurance

Contact attributes: agentLocation = Seattle

Step 2: Define actions

In addition to categorizing a contact, you can define what actions Amazon Connect should take:

1. Generate an EventBridge event (p. 589)
2. Create task (p. 593)

Step 3: Review and save

1. When done, choose **Save**.
2. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

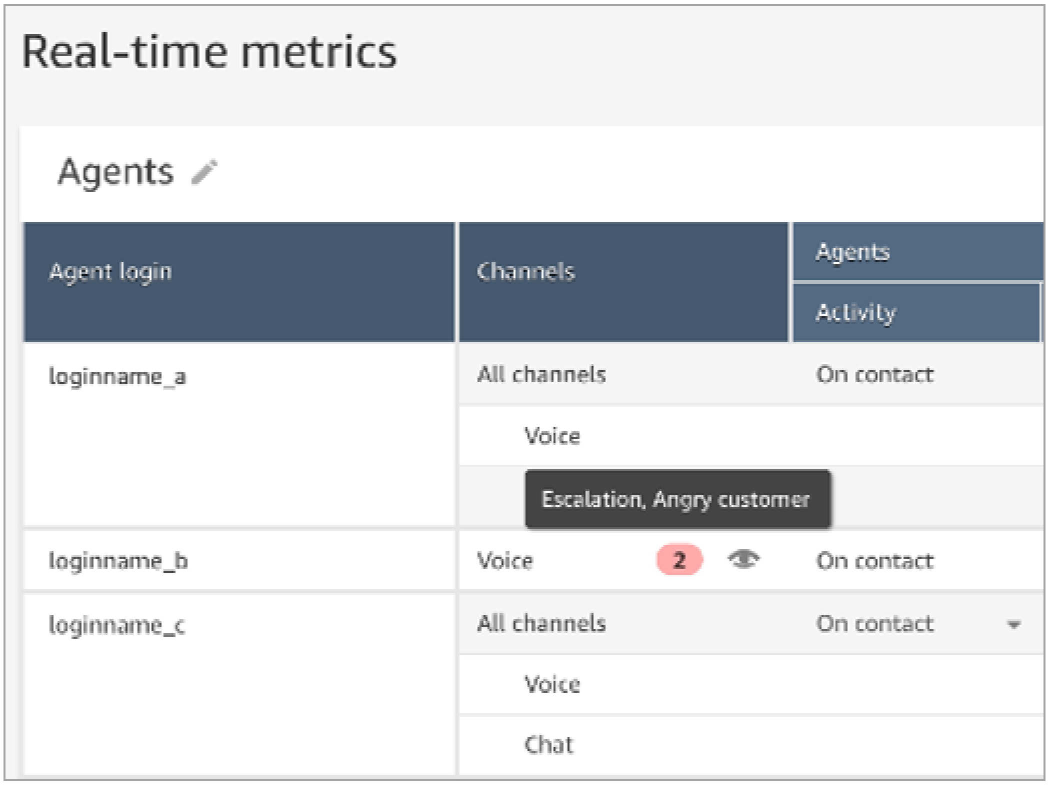
   You cannot apply rules to past, stored conversations.

Alert supervisors in real-time based on keywords and phrases

After you enable real-time analytics (p. 812) in your contact flow, you can add rules that automatically alert supervisors when a customer experience issue occurs.

For example, Contact Lens can automatically send an alert when certain keywords or phrases are uttered during the conversation, or when it detects other criteria. The supervisor sees the alert on the real-time metrics dashboard. From there, supervisors can listen in to the live call, and provide guidance to the agent over chat to help them resolve the issue faster.

The following image shows an example of what a supervisor would see on the real-time metrics report when they get an alert. In this case, Contact Lens has detected an angry customer situation.

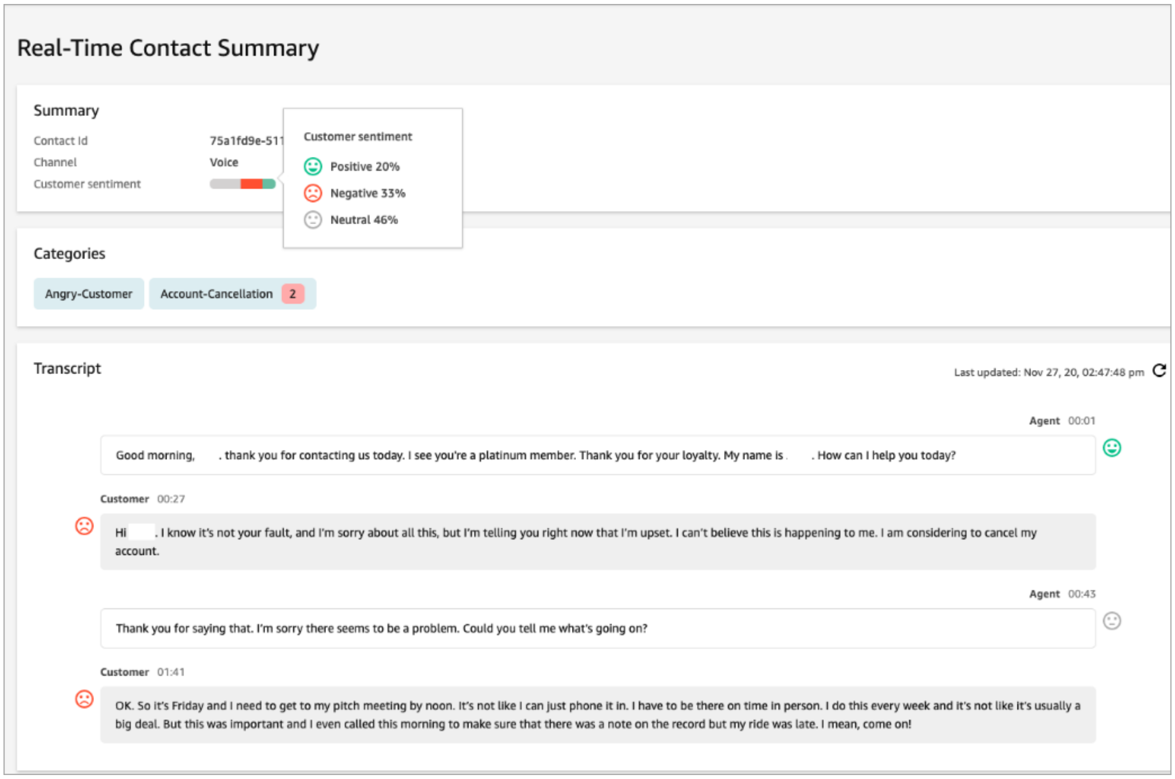


Real-time metrics

Agents

Agent login	Channels	Agents
		Activity
loginname_a	All channels	On contact
	Voice	
	Escalation, Angry customer	
loginname_b	Voice 2 👁	On contact
loginname_c	All channels	On contact ▾
	Voice	
	Chat	

When the supervisor listens in to a live call, Contact Lens provides them with a real-time transcript and customer sentiment trend that helps them understand the situation and assess the appropriate action. The transcript also eliminates the need for customers to repeat themselves if the call is transferred to another agent. Following is a sample real-time transcript.



Real-Time Contact Summary

Summary

Contact Id 75a1fd9e-511
Channel Voice
Customer sentiment

Customer sentiment
- 🙂 Positive 20%
- ☹ Negative 33%
- 😐 Neutral 46%

Categories

Angry-Customer | Account-Cancellation 2

Transcript

Last updated: Nov 27, 20, 02:47:48 pm

Agent 00:01 🙂
Good morning, . thank you for contacting us today. I see you're a platinum member. Thank you for your loyalty. My name is . How can I help you today?

Customer 00:27 ☹
Hi . I know it's not your fault, and I'm sorry about all this, but I'm telling you right now that I'm upset. I can't believe this is happening to me. I am considering to cancel my account.

Agent 00:43 😐
Thank you for saying that. I'm sorry there seems to be a problem. Could you tell me what's going on?

Customer 01:41 ☹
OK. So it's Friday and I need to get to my pitch meeting by noon. It's not like I can just phone it in. I have to be there on time in person. I do this every week and it's not like it's usually a big deal. But this was important and I even called this morning to make sure that there was a note on the record but my ride was late. I mean, come on!

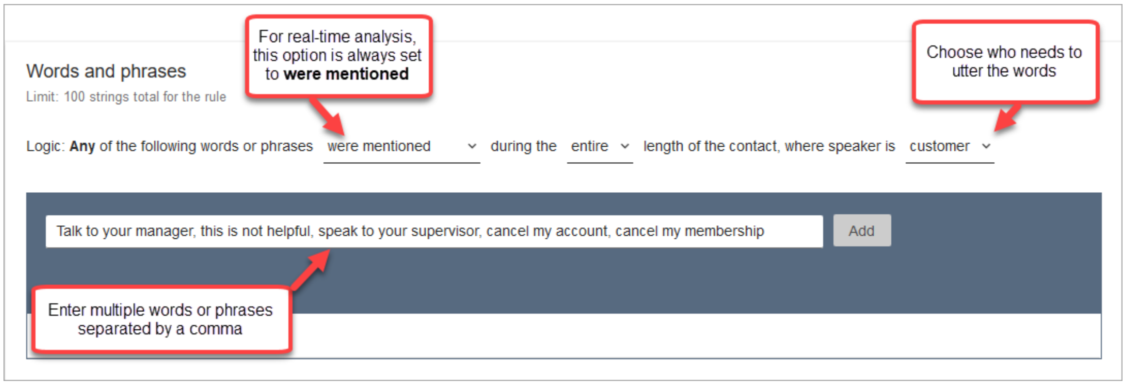
Add rules for real-time alerts

1. Log in to Amazon Connect with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for **Rules** permissions.
2. On the navigation menu, choose **Rules**.
3. Select **Create a rule**, **Contact Lens**.
4. Assign a name to the rule.
5. Under **When**, use the dropdown list to choose **real-time analysis**.
6. Choose **Add condition**, and then choose the type of match:

   - **Exact Match**: Finds only the exact words or phrases.
   - **Pattern Match**: Finds matches that may be less than 100 percent exact. You can also specify the distance between words. For example, you might look for contacts where the word "credit" was mentioned, but you do not want to see any mention of the words "credit card." You can define a pattern matching category to look for the word "credit" that is not within a one-word distance of the word "card."

   Tip

   Semantic Match isn't available for real-time analysis.
7. Enter the words or phrases, separated by a comma, that you want to highlight. Real-time rules only support any keywords or phrases that **were mentioned**.



Words and phrases

Limit: 100 strings total for the rule

Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is customer

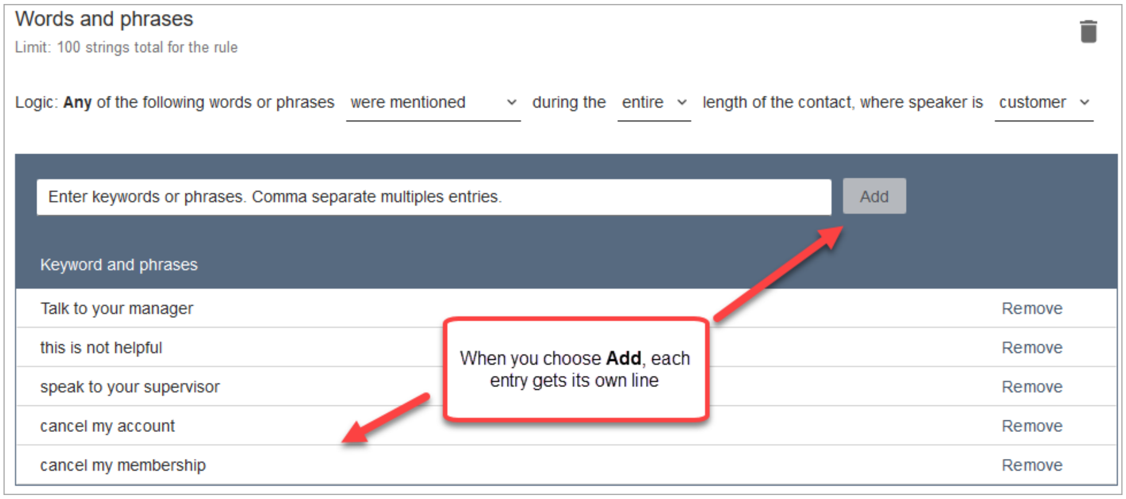
Talk to your manager, this is not helpful, speak to your supervisor, cancel my account, cancel my membership

For real-time analysis, this option is always set to **were mentioned**

Choose who needs to utter the words

Enter multiple words or phrases separated by a comma

8. Choose **Add**. Each word or phrase separated by a comma gets its own line.



Words and phrases

Limit: 100 strings total for the rule

Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is customer

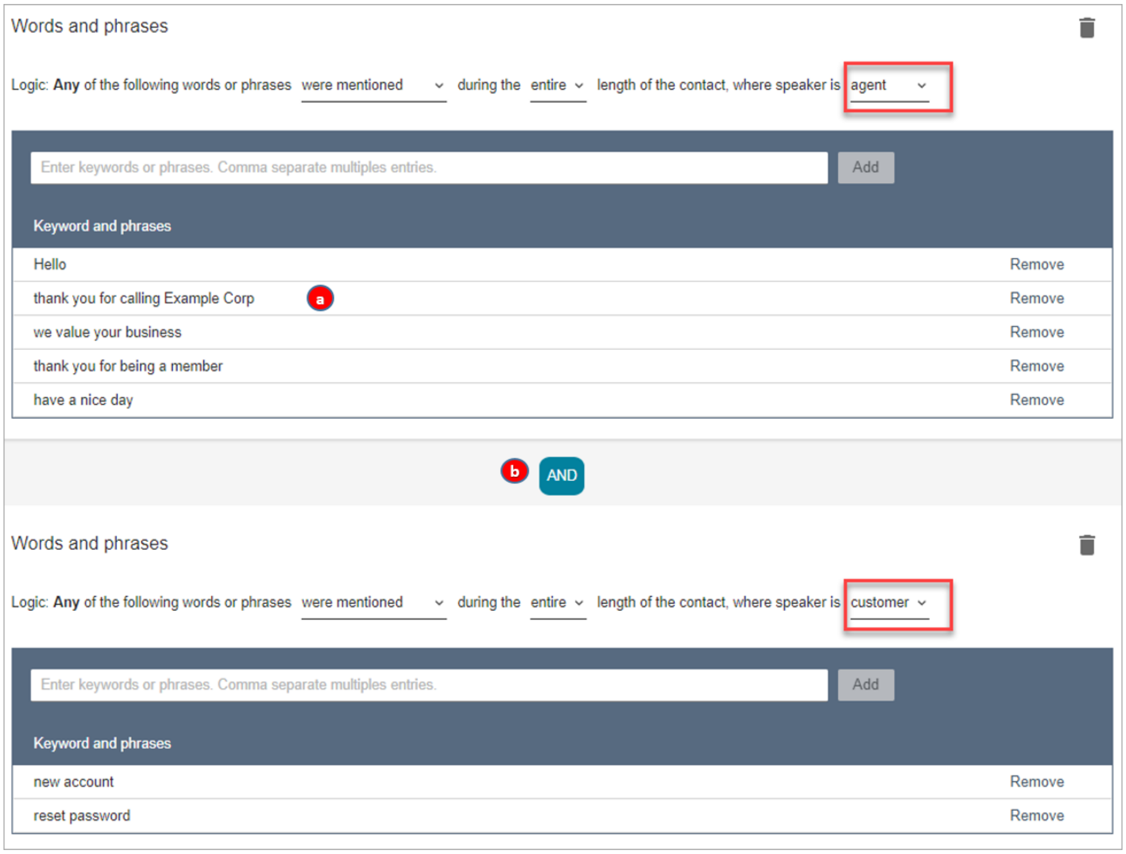
Enter keywords or phrases. Comma separate multiples entries.

Keyword and phrases	
Talk to your manager	Remove
this is not helpful	Remove
speak to your supervisor	Remove
cancel my account	Remove
cancel my membership	Remove

When you choose **Add**, each entry gets its own line

The logic that Contact Lens uses to read these words or phrases is: (Talk OR to OR your OR manager) OR (this OR is OR not OR helpful) OR (speak OR to OR your OR supervisor), etc.

9. To add more words or phrases, choose **Add group of words or phrases**. In the following image, the first group of words or phrases are what the agent might utter. The second group is what the customer might utter.



Words and phrases

Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Enter keywords or phrases. Comma separate multiples entries.

Keyword and phrases	
Hello	Remove
thank you for calling Example Corp	Remove
we value your business	Remove
thank you for being a member	Remove
have a nice day	Remove

Words and phrases

Logic: **Any** of the following words or phrases were mentioned during the entire length of the contact, where speaker is customer

Enter keywords or phrases. Comma separate multiples entries.

Keyword and phrases	
new account	Remove
reset password	Remove

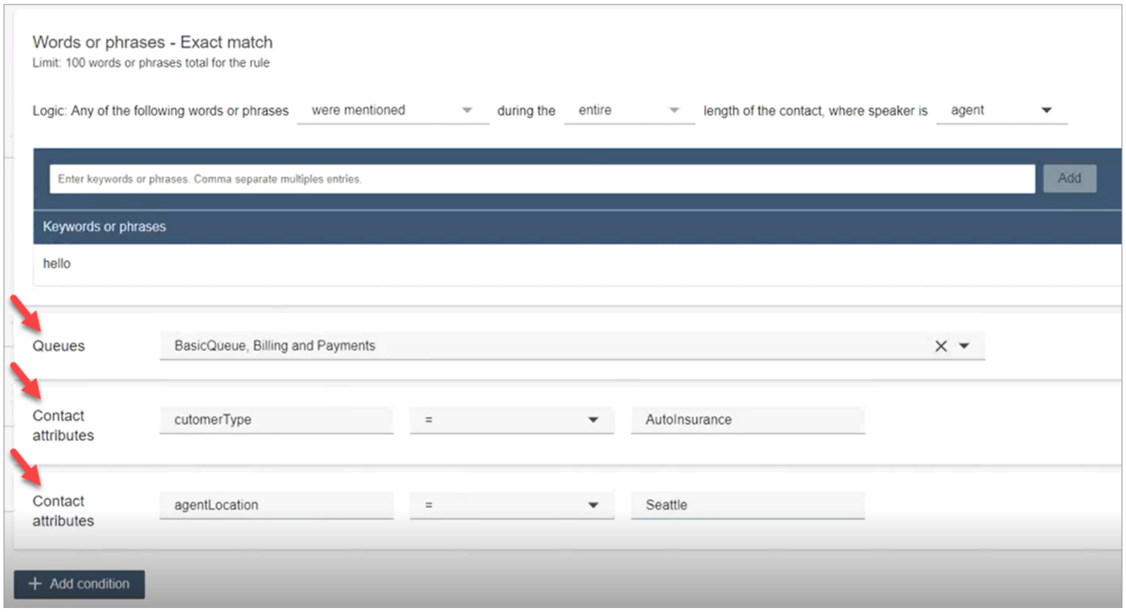
1. In this first card, Content Lens reads each line as an OR. For example: (Hello) OR (thank OR you OR for OR calling OR Example OR Corp) OR (we OR value OR your OR business).
2. The two cards are connected with an AND. This means, one of the rows in the first card needs to be uttered AND then one of the phrases in the second card needs to be uttered.

The logic that Contact Lens uses to read the two cards of words or phrases is (card 1) AND (card 2).

10. Choose **Add condition** to apply the rules to:

- Specific queues
- When contact attributes have certain values
- When sentiment scores have certain values

For example, the following image shows a rule that applies when an agent is working the BasicQueue or Billing and Payments queues, the customer is for autoinsurance, and the agent is located in Seattle.



Words or phrases - Exact match

Limit: 100 words or phrases total for the rule

Logic: Any of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Enter keywords or phrases. Comma separate multiples entries.

Keywords or phrases

hello

Queues: BasicQueue, Billing and Payments

Contact attributes: cutomerType = AutoInsurance

Contact attributes: agentLocation = Seattle

11. When done, choose **Save**.

12. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

    You cannot apply rules to past, stored conversations.

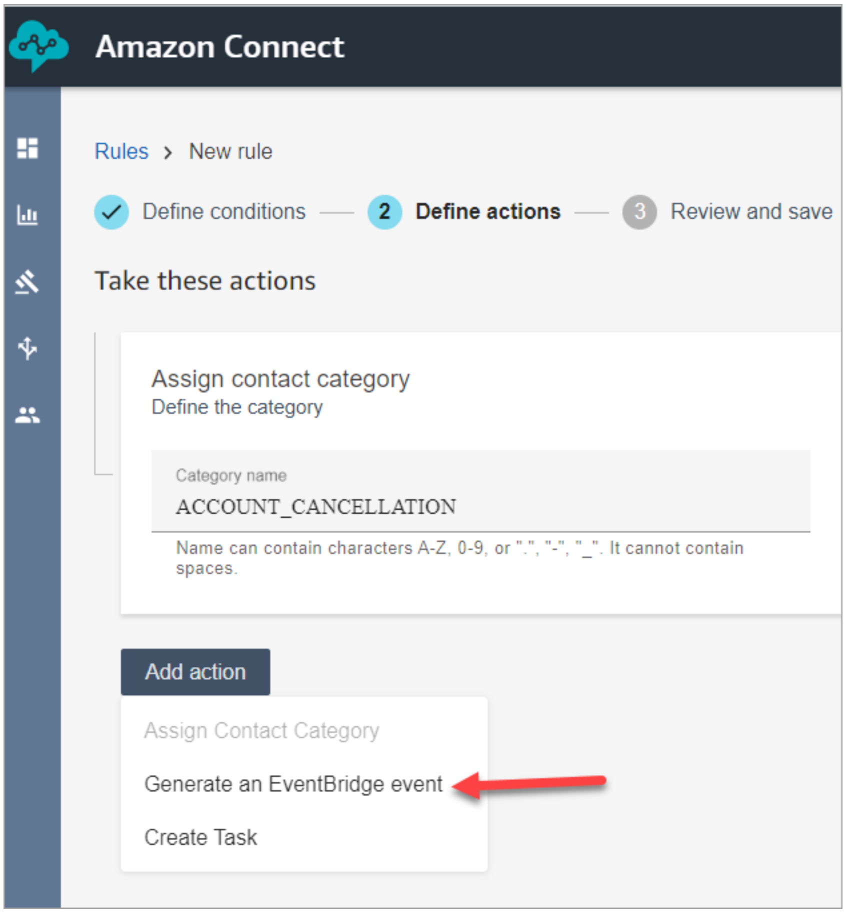
Create a Contact Lens rule that generates an EventBridge event

In real-time or post-call, you can get events and use them to trigger subsequent notifications or alerts, or aggregate reports outside of Amazon Connect. There's a lot you can do with this data. For example:

- Get real-time alerts in a QuickSight dashboard.
- Create aggregated reported outside of Amazon Connect.
- Join data with your CRM.
- Connect your notification solution to EventBridge and make sure that by end of day, all of a certain type of events go to a certain inbox. The payload tells you the contact, agent, and queue.

To create a rule that generates an EventBridge event

1. When you create your rule, choose **Generate EventBridge event** for the action.

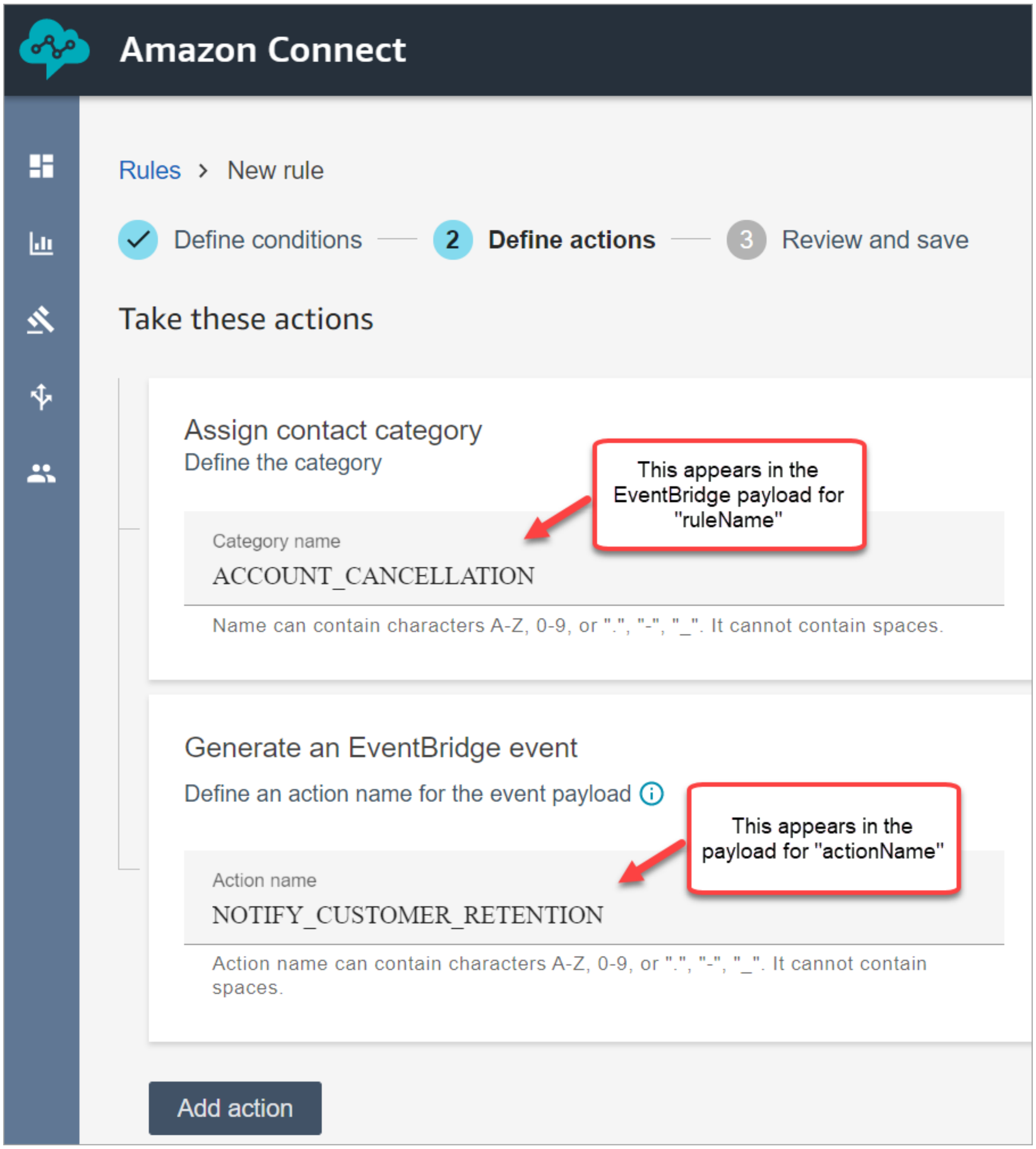


Category name
ACCOUNT_CANCELLATION

Name can contain characters A-Z, 0-9, or ".", "-", "_". It cannot contain spaces.

2. For **Action name**, enter the name for the event payload.

   Note
   The value you assign for **Action name** is visible in the EventBridge payload. When you aggregate events, the action name provides an additional dimension that you can use to process them. For example, you have 200 category names, but only 50 have a specific action name, such as NOTIFY_CUSTOMER_RETENTION.



Take these actions

Assign contact category

Define the category

Category name: ACCOUNT_CANCELLATION

Name can contain characters A-Z, 0-9, or ".", "-", "_". It cannot contain spaces.

This appears in the EventBridge payload for "ruleName"

Generate an EventBridge event

Define an action name for the event payload

Action name: NOTIFY_CUSTOMER_RETENTION

Action name can contain characters A-Z, 0-9, or ".", "-", "_". It cannot contain spaces.

This appears in the payload for "actionName"

3. Choose **Next**. Review and then **Save**.
4. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

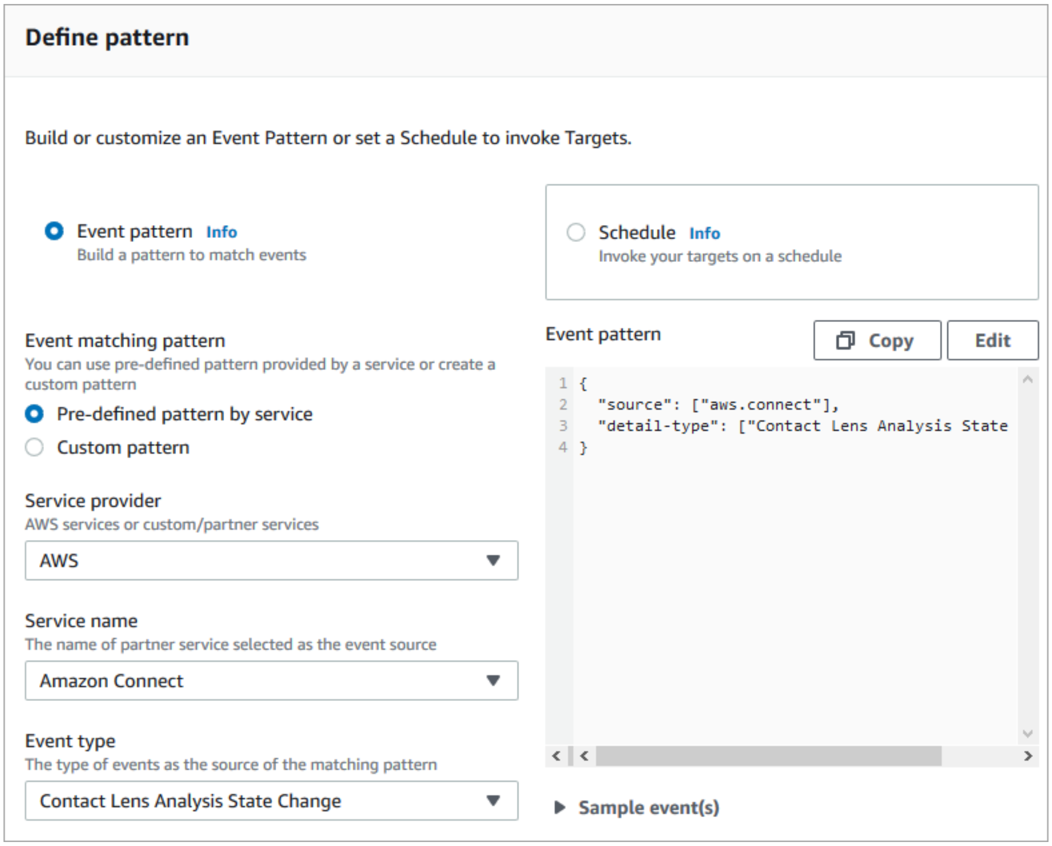
   You cannot apply rules to past, stored conversations.
5. To leverage the EventBridge data, subscribe to the EventBridge event type. See the next procedure.

Subscribe to EventBridge event types

To subscribe to EventBridge event types, create a custom EventBridge rule that matches the following:

- "source" = "aws.connect"

- "detail-type" = "Contact Lens Analysis State Change" (or **Contact Lens Post Call Rules Matched** or **Contact Lens Realtime Rules Matched**)



Define pattern

Build or customize an Event Pattern or set a Schedule to invoke Targets.

● Event pattern Info
Build a pattern to match events

○ Schedule Info
Invoke your targets on a schedule

Event matching pattern
You can use pre-defined pattern provided by a service or create a custom pattern

● Pre-defined pattern by service
○ Custom pattern

Service provider
AWS services or custom/partner services
AWS ▼

Service name
The name of partner service selected as the event source
Amazon Connect ▼

Event type
The type of events as the source of the matching pattern
Contact Lens Analysis State Change ▼

Event pattern

```
{
  "source": ["aws.connect"],
  "detail-type": ["Contact Lens Analysis State
}
```

Example EventBridge payloads

Following is an example of what the EventBridge payload looks like when **Contact Lens Post Call Rules Matched**.

```
{
 "version": "0", // set by EventBridge
 "id": "aaaaaaaa-bbbb-cccc-dddd-bf3703467718", // set by EventBridge
 "source": "aws.connect",
 "detail-type": "Contact Lens Post Call Rules Matched",
 "account": "your AWS account ID",
 "time": "2020-04-27T18:43:48Z",
 "region": "us-east-1", // set by EventBridge
 "resources": ["arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN"],
 "detail": {
    "version": "1.0",
    "ruleName": "ACCOUNT_CANCELLATION", // Rule name
    "actionName": "NOTIFY_CUSTOMER_RETENTION",
    "instanceArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN",
    "contactArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/
contact/contact-ARN",
    "agentArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/
agent/agent-ARN",
    "queueArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/
queue/queue-ARN",
    }
}
```

Following is an example of what the payload looks like when **Contact Lens Realtime Rules Matched**.

```
{
 "version": "0", // set by EventBridge
 "id": "aaaaaaaa-bbbb-cccc-dddd-bf3703467718", // set by EventBridge
 "source": "aws.connect",
 "detail-type": "Contact Lens Realtime Rules Matched",
 "account": "your AWS account ID",
 "time": "2020-04-27T18:43:48Z",
 "region": "us-east-1", // set by EventBridge
 "resources": ["arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN"],
 "detail": {
     "version": "1.0",
     "ruleName": "ACCOUNT_CANCELLATION", // Rule name
     "actionName": "NOTIFY_CUSTOMER_RETENTION",
      "instanceArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN",
     "contactArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/
contact/contact-ARN",
     "agentArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/
agent/agent-ARN",
     "queueArn": "arn:aws:connect:us-east-1:your AWS account ID:instance/instance-ARN/
queue/queue-ARN",
      }
}
```

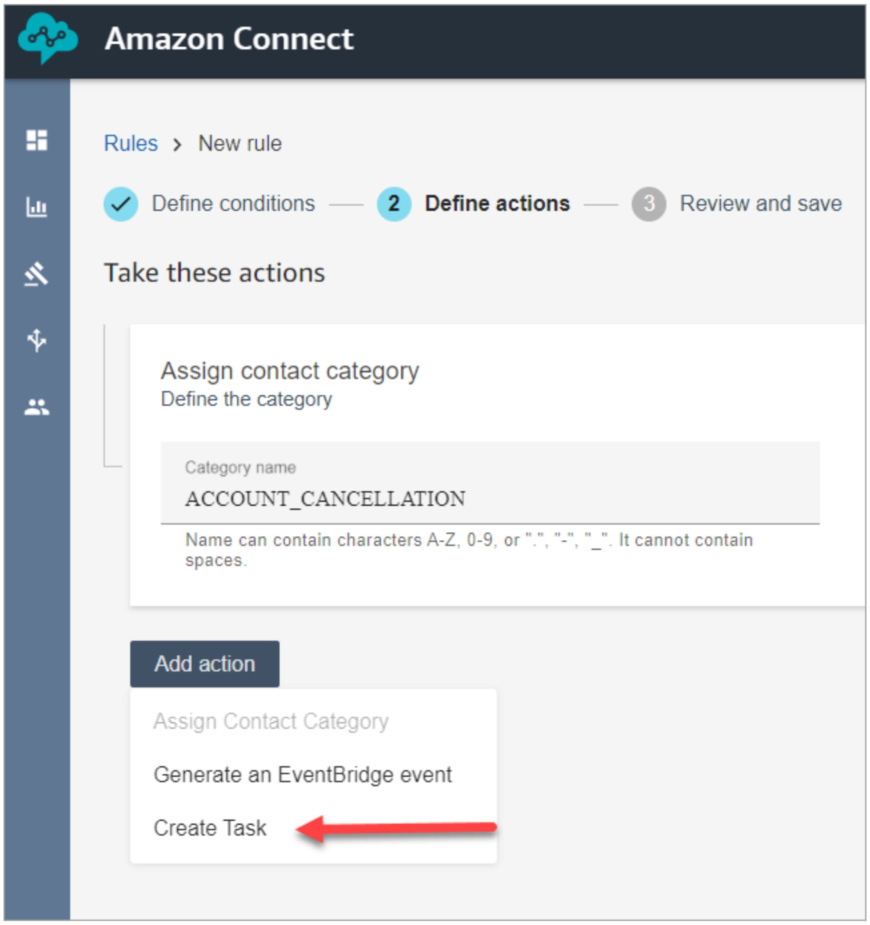
Create a task when a contact is categorized in real-time or post-call

An especially powerful use of Content Lens rules is to build rules that generate tasks. This helps you identify issues in your contact center for you to follow up, and creates traceable actions with owners. Following are some examples:

- Create a task to review a contact when the customer is fraudulent. For example, you can create a follow-up task when a customer utters words or phrases that makes them appear potentially fraudulent.
- Follow up when the customer mentions specific topics that you want to later on upsell or provide additional support by reaching out.
- Follow up when there is a serious quality issue. In addition to contacts being categorized and getting alerts, you can route a task so you have owners. You also have contact records for these tasks, so you can search for and trace them.

To create a rule that creates a task

1. When you create your rule, choose **Create Task** for the action.



Take these actions

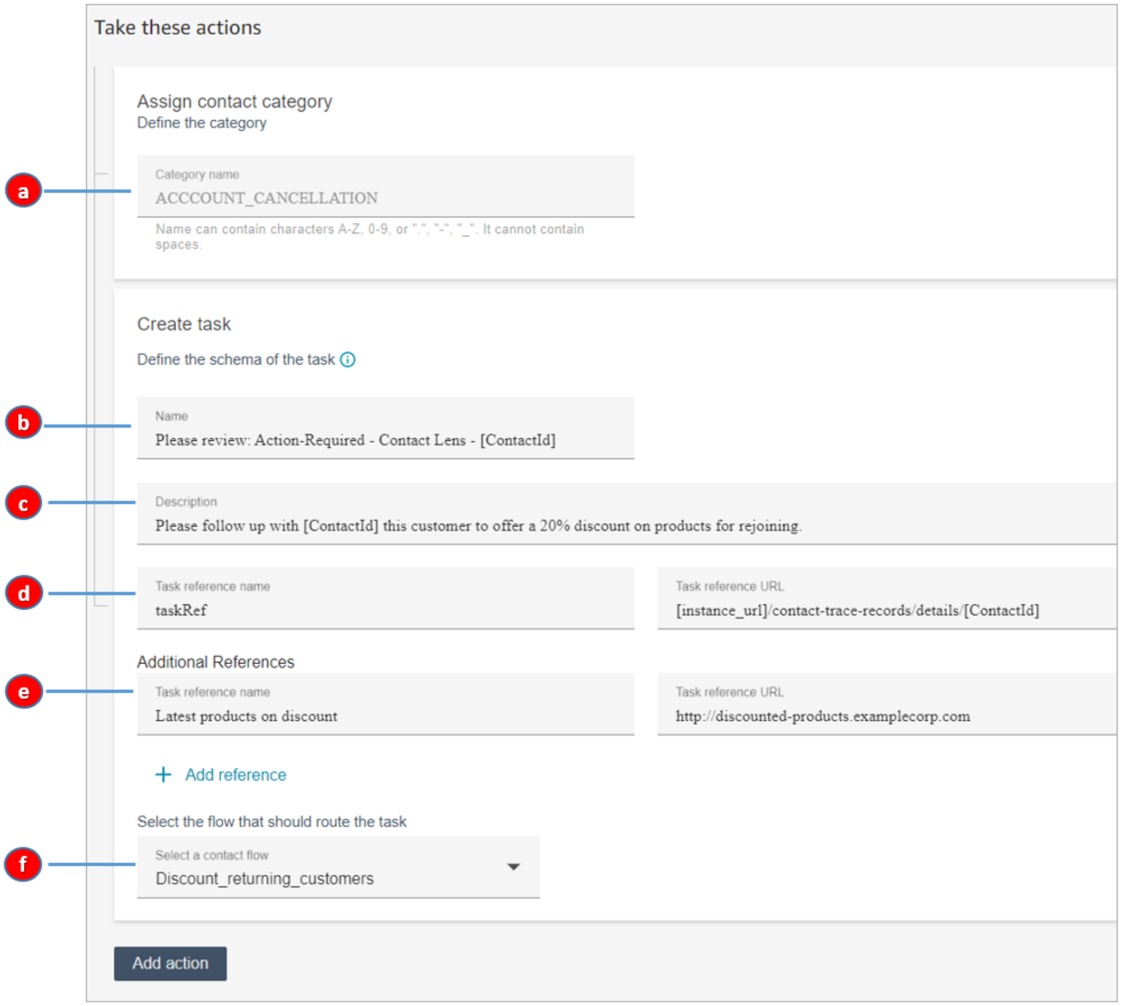
Assign contact category

Define the category

Category name: ACCOUNT_CANCELLATION

Name can contain characters A-Z, 0-9, or ".", "-", "_". It cannot contain spaces.

2. Complete the task fields as follows:



Category name: ACCCOUNT_CANCELLATION

Name can contain characters A-Z, 0-9, or ".", "-", "_". It cannot contain spaces.

Name: Please review: Action-Required - Contact Lens - [ContactId]

Description: Please follow up with [ContactId] this customer to offer a 20% discount on products for rejoining.

Task reference name: taskRef

Task reference URL: [instance_url]/contact-trace-records/details/[ContactId]

Task reference name: Latest products on discount

Task reference URL: http://discounted-products.examplecorp.com

Select a contact flow: Discount_returning_customers

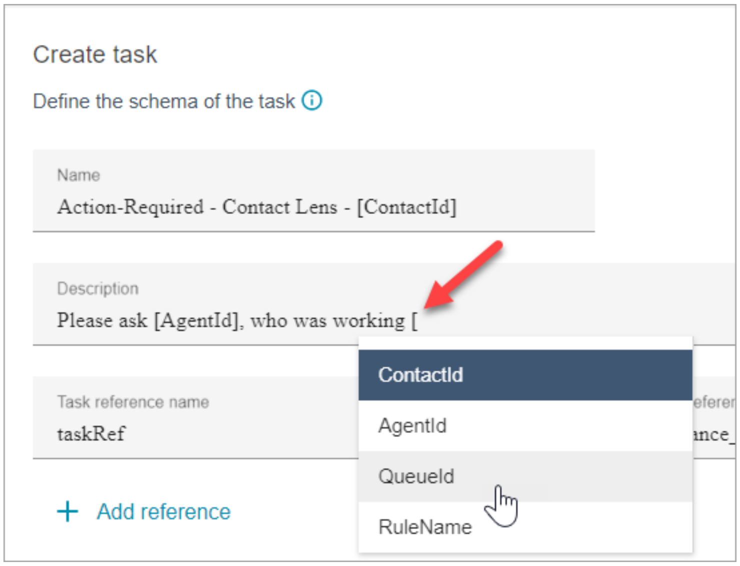
a. **Category name**: The category name appears in the contact record. Max length: 200 characters.

b. **Name**: The name appears in the agent's Contact Control Panel (CCP). Max length: 512 characters.

c. **Description**: The description appears in the agent's Contact Control Panel (CCP). Max length: 4096 characters.

Tip

In **Name** and **Description**, use [ ] to choose from a menu of dynamic values. For more information, see Create a task when a contact is categorized in real-time or post-call (p. 593).



Create task

Define the schema of the task

Name
Action-Required - Contact Lens - [ContactId]

Description
Please ask [AgentId], who was working [

Task reference name
taskRef

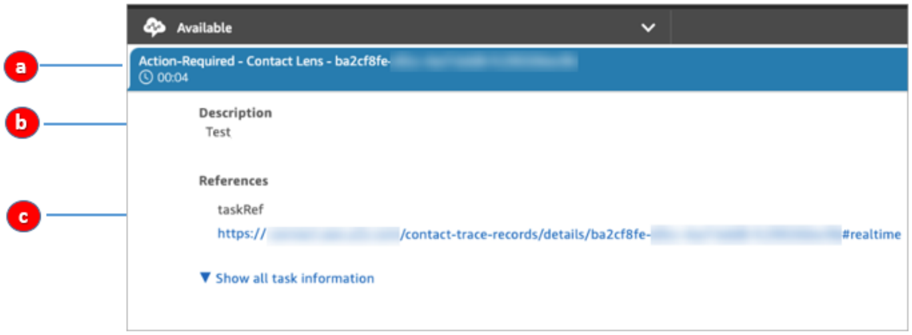
d. **Task reference name**: This is a default reference that automatically appears in the agent's CCP.

  - For real-time rules, the task reference links to the Real-time details page.
  - For post-call rules, the task reference links to the **Contact record details** page.

e. **Additional Reference name**: Max length: 4096 characters. You can add up to 25 references.

f. **Select a contact flow**: Choose the contact flow that is designed to route the task to the appropriate owner of the task. The contact flow must be saved and published for it to appear in your list of options in the dropdown.

3. The following image shows an example of how this information appears in the agent's CCP:



Action-Required - Contact Lens - ba2cf8fe-[redacted]
00:04

Description
Test

References
taskRef
https://[redacted]/contact-trace-records/details/ba2cf8fe-[redacted]#realtime

In this example, the agent sees the following values for **Name**, **Description**, and **Task reference name**:

a. **Name** = Action-Required-Contact Lens - ba2cf8fe....

b. **Description** = Test

c. **Task reference name** = taskRef and the URL to the Real-time details page

4. Choose **Next**. Review and then choose **Save** the task.

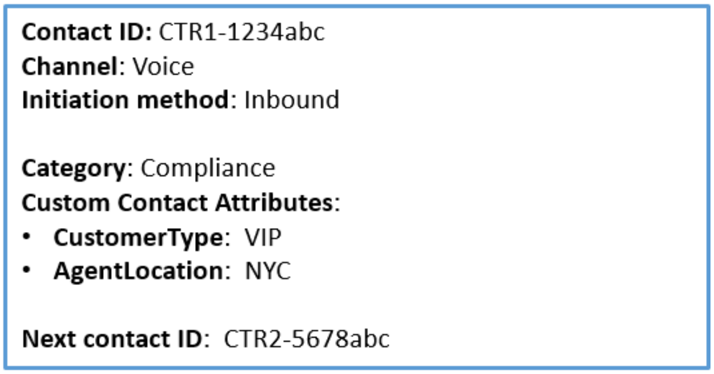
5. After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

   You cannot apply rules to past, stored conversations.

Voice and task contact records are linked

When a rule creates a task, a contact record is automatically generated for the task. It's linked to the contact record of the voice call that met the criteria for the rule to create the task.

For example, a call comes into your contact center and generates CTR1:

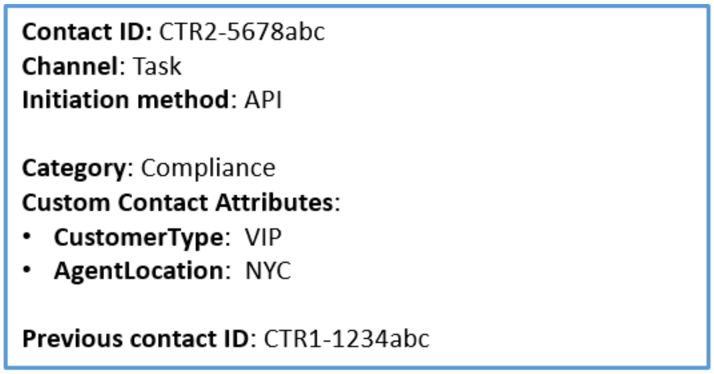


Contact ID: CTR1-1234abc
Channel: Voice
Initiation method: Inbound

Category: Compliance
Custom Contact Attributes:
- **CustomerType**: VIP
- **AgentLocation**: NYC

Next contact ID: CTR2-5678abc

The Rules engine generates a task. In the contact record for the task, the voice contact record appears as the **Previous contact ID**. In addition, the task contact record inherits contact attributes from the voice contact record, as illustrated in the following image:



Contact ID: CTR2-5678abc
Channel: Task
Initiation method: API

Category: Compliance
Custom Contact Attributes:
- **CustomerType**: VIP
- **AgentLocation**: NYC

Previous contact ID: CTR1-1234abc

About dynamic values for ContactId, AgentId, QueueId, RuleName

The dynamic values in brackets [ ] are called contact attributes (p. 515). Contact attributes enable you to store temporary information about the contact so you can use it in a contact flow.

When you add contact attributes in brackets [ ] — such as ContactId, AgentId, QueueId, or RuleName — the value is passed from one contact record to another. You can use contact attributes in your contact flow to branch and route the contact accordingly.

For more information, see Use Amazon Connect contact attributes (p. 515).

How to use exact match, pattern match, and semantic match in a rule

How to use exact match

Exact Match really is an exact word match, singular or plural.

How to use pattern match

If you want to match related words, append an asterisk (*) to the criteria. For example, if you want to match on all variations of "neighbor" (neighbors, neighborhood) you would type **neighbo***.

With **Pattern Match** you can specify the following:

- **List of values**: This is useful when you want to build expressions with interchangeable values. For example, the expression might be:

  I'm calling about a power outage in ["Beijing" or "London" or "New York" or "Paris" or "Tokyo"]

  Then in your list of values you would add the cities: Beijing, London, New York, Paris, Tokyo.

  The advantage of using values is that you can create one expression, instead of multiple. This reduces the number of cards that you need to create.
- **Number**: This option is used most frequently in compliance scripts, or if your looking for a context when you know somewhere in between there's a number. This way you can put all of your criteria into one expression instead of two. For example, an agent compliance script might say:

  I have been in this industry for [num] years and would like to discuss this topic with you.

  Or a customer might say:

  I have been a member for [num] years.
- **Proximity definition**: Finds matches that may be less than 100 percent exact. You can also specify the distance between words. For example, if you are looking for contacts where the word "credit" was mentioned but you do not want to see any mention of the words "credit card," you can define a pattern matching category to look for the word "credit" that is not within a one-word distance of "card."

  For example, a proximity definition might be:

  credit [is not within 0 to 1 word apart] card**

  > **Tip**
  > For a list of languages supported by pattern match, see Pattern match languages (p. 7).

How to use semantic match

Semantic matching is supported only for post-call analysis.

- An “intent” is an example of utterance. It can be a phrase or a sentence.
- You can enter up to four intents in one card (group).
- We recommend using semantically similar intents within one card to get the best results. For example, there's category for "politeness." It includes two intents: "greetings" and "goodbye". We recommend separating these intents into two cards:
  - Card 1: "How are you today" and "How’s everything going". They are semantically similar greetings.
  - Card 2: "Thanks for contacting us" and "Thank you for being our customer." They are semantically similar goodbyes.

  Separating the intents into two cards provides more accuracy than putting them all into one card.

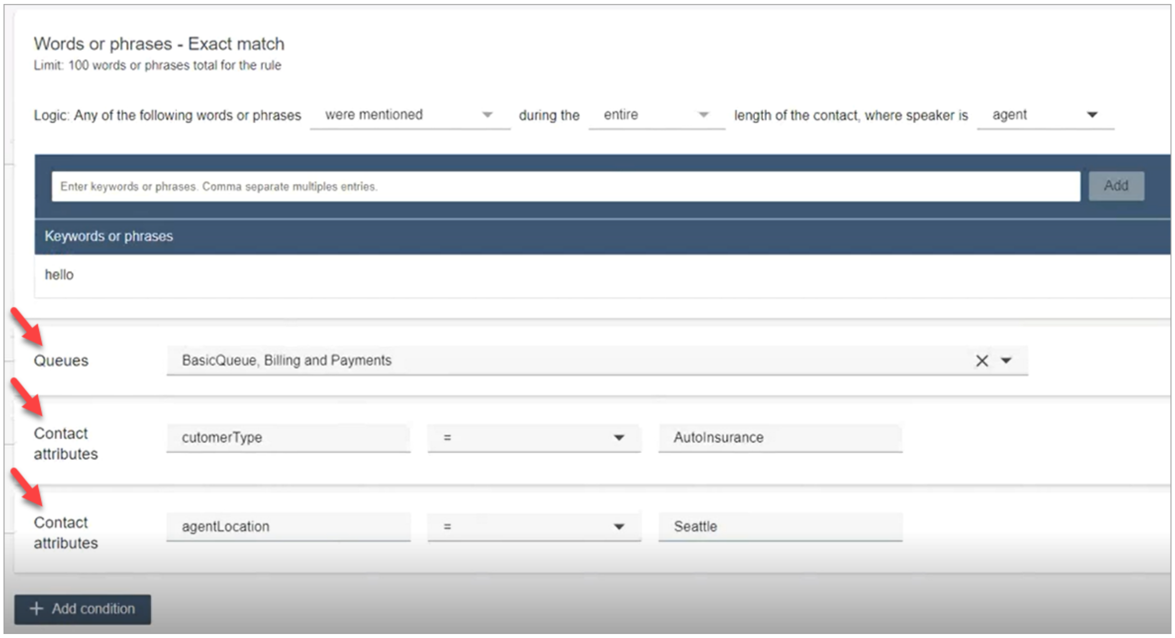
Enter a script in a rule

There are times when you may need you agents to follow an exact script. For example, a compliance script that all agents need to follow.

To enter a script in a rule, enter phrases. For example, if you want to highlight when agents say *Thank you for being a member. We appreciate your business*, enter two phrases:

- Thank you for being a member.
- We appreciate your business.

To apply the rule to certain lines of businesses, add a condition for which queues it applies to, or contact attributes. For example, the following image shows a rule that applies when an agent is working the BasicQueue or Billing and Payments queues, the customer is for autoinsurance, and the agent is located in Seattle.



Words or phrases - Exact match

Limit: 100 words or phrases total for the rule

Logic: Any of the following words or phrases were mentioned during the entire length of the contact, where speaker is agent

Enter keywords or phrases. Comma separate multiples entries.

Keywords or phrases

hello

Queues: BasicQueue, Billing and Payments

Contact attributes: cutomerType = AutoInsurance

Contact attributes: agentLocation = Seattle

Security profile permissions for Contact Lens rules

To view, edit, or add rules for automatic categorization, you must be assigned to a security profile that has **Analytics: Rules** permissions.

To see agent names so you can add them to rules, you need **Users and permissions: Users - View** permissions in your security profile.

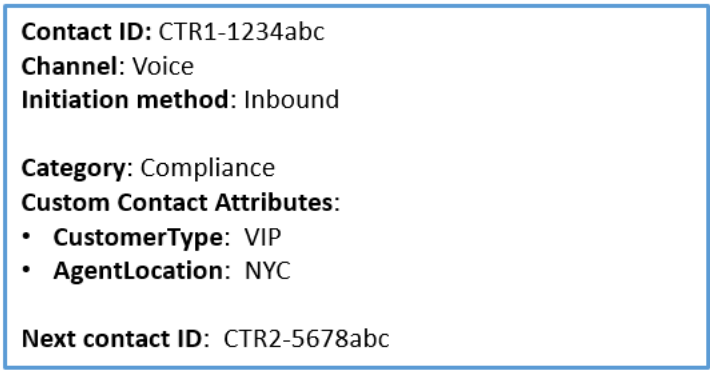
To see the queue names so you can add them to rules, you need **Routing: Queues - View** permissions in your security profile.

For more information, see Security profile permissions for Contact Lens (p. 818).

About contact attributes in a rule

You can have up to 5 contact attributes in a rule.

You can design contact flows to use the contact attributes you specify in a rule, and then route the task accordingly. For example, a call arrives in your contact center. When Contact Lens analyzes the call, it gets a hit on the **Compliance** rule. The contact record that's created for the call includes information similar to the following image:

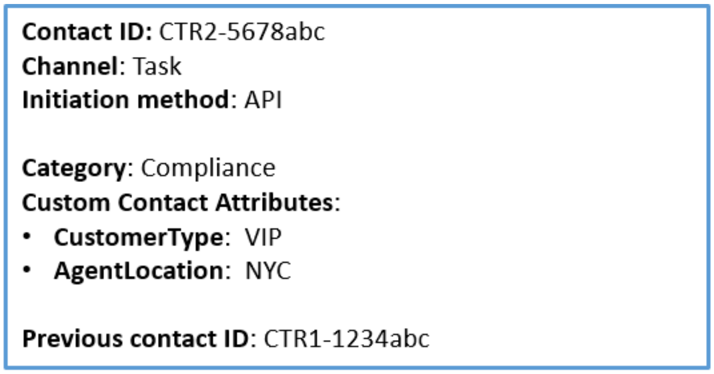


Contact ID: CTR1-1234abc
Channel: Voice
Initiation method: Inbound

Category: Compliance
Custom Contact Attributes:
- **CustomerType**: VIP
- **AgentLocation**: NYC

Next contact ID: CTR2-5678abc

The Rules engine generates a task. The contact record for the task inherits contact attributes from the voice contact record, as illustrated in the following image:



Contact ID: CTR2-5678abc
Channel: Task
Initiation method: API

Category: Compliance
Custom Contact Attributes:
- **CustomerType**: VIP
- **AgentLocation**: NYC

Previous contact ID: CTR1-1234abc

The voice contact record appears as the **Previous contact ID**.

The contact flow that you specify in the rule should be designed to use the contact attributes and route the task to the appropriate owner. For example, you may want to route tasks where **CustomerType = VIP** to a specific agent.

For more information, see Use Amazon Connect contact attributes (p. 515).

Rules are applied to new contacts

After you add rules, they are applied to new contacts that occur after the rule was added. Rules are applied when Contact Lens analyzes conversations.

You cannot apply rules to past, stored conversations.

Error notifications: When Contact Lens can't analyze a contact

It's possible that Contact Lens can't analyze a contact file, even though analysis is enabled on the contact flow. When this happens, Contact Lens sends error notifications using Amazon EventBridge events.

Events are emitted on a best effort basis.

Subscribe to EventBridge notifications

To subscribe to these notifications, create a custom EventBridge rule that matches the following:

- "source" = "aws.connect"
- "detail-type" = "Contact Lens Analysis State Change"

You can also add to the pattern to be notified when a specific event code occurs. For more information, see Event Patterns in the *Amazon EventBridge User Guide*.

The format of a notification looks like the following sample:

```
{
    "version": "0", // set by CloudWatch Events
    "id": "55555555-1111-1111-1111-111111111111", // set by CloudWatch Events
    "source": "aws.connect",
    "detail-type": "Contact Lens Analysis State Change",
    "account": "111122223333",
    "time": "2020-04-27T18:43:48Z",
    "region": "us-east-1", // set by CloudWatch Events
    "resources": [
        "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-
h9j0-7c822889931e",
        "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-
h9j0-7c822889931e/contact/efgh4567-pqrs-5678-t9c0-111111111111"
    ],
    "detail": {
        "instance": "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-
h9j0-7c822889931e",
        "contact": "arn:aws:connect:us-east-1:111122223333:instance/abcd1234-defg-5678-
h9j0-7c822889931e/contact/efgh4567-pqrs-5678-t9c0-111111111111",
        "channel": "VOICE",
        "state": "FAILED",
        "reasonCode": "RECORDING_FILE_CANNOT_BE_READ"
    }
}
```

Event codes

The following table lists the event codes that may result when Contact Lens can't analyze a contact.

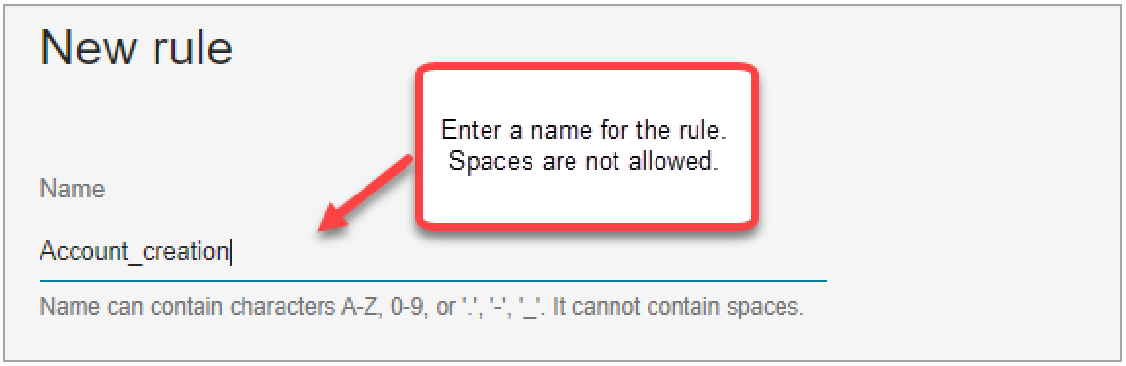
Event reason code	Description
INVALID_ANALYSIS_CONFIGURATION	Contact Lens received invalid values when the contact flow was initiated, such as an unsupported or invalid language code, or an unsupported value for redaction behavior.
RECORDING_FILE_CANNOT_BE_READ	Contact Lens can't get the recording file. This might be because file isn't present in the S3 bucket, or there are problems with permissions.
RECORDING_FILE_TOO_SMALL	The recording audio file is too small for analysis (less than 105 ms).
RECORDING_FILE_TOO_LARGE	The recording file exceeds the duration limit for analysis (more than 14,400 seconds, or 4 hours).

Event reason code	Description
RECORDING_FILE_INVALID	The audio file is invalid.
RECORDING_FILE_CANNOT_BE_READ	An error occurred when Contact Lens tried to read the audio file.
RECORDING_FILE_EMPTY	The audio file is empty.
RECORDING_SAMPLE_RATE_NOT_SUPPORTED	The sample rate of the audio file is not supported. Contact Lens currently supports audio files with an 8kHz sample rate. That is the sample rate for Amazon Connect recordings.

Create rules that generate tasks for third-party integrations

After you set up an external application to generate tasks automatically, you need to build rules that tell Amazon Connect when to create tasks, and how to route them.

1. Log in to Amazon Connect with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for **Rules** permissions.
2. In Amazon Connect, on the navigation menu, choose **Rules**.
3. On the **Rules** page, use the **Create a rule** dropdown list to choose **External application**.
4. At the **Trigger and conditions** page, assign a name to the rule.



New rule

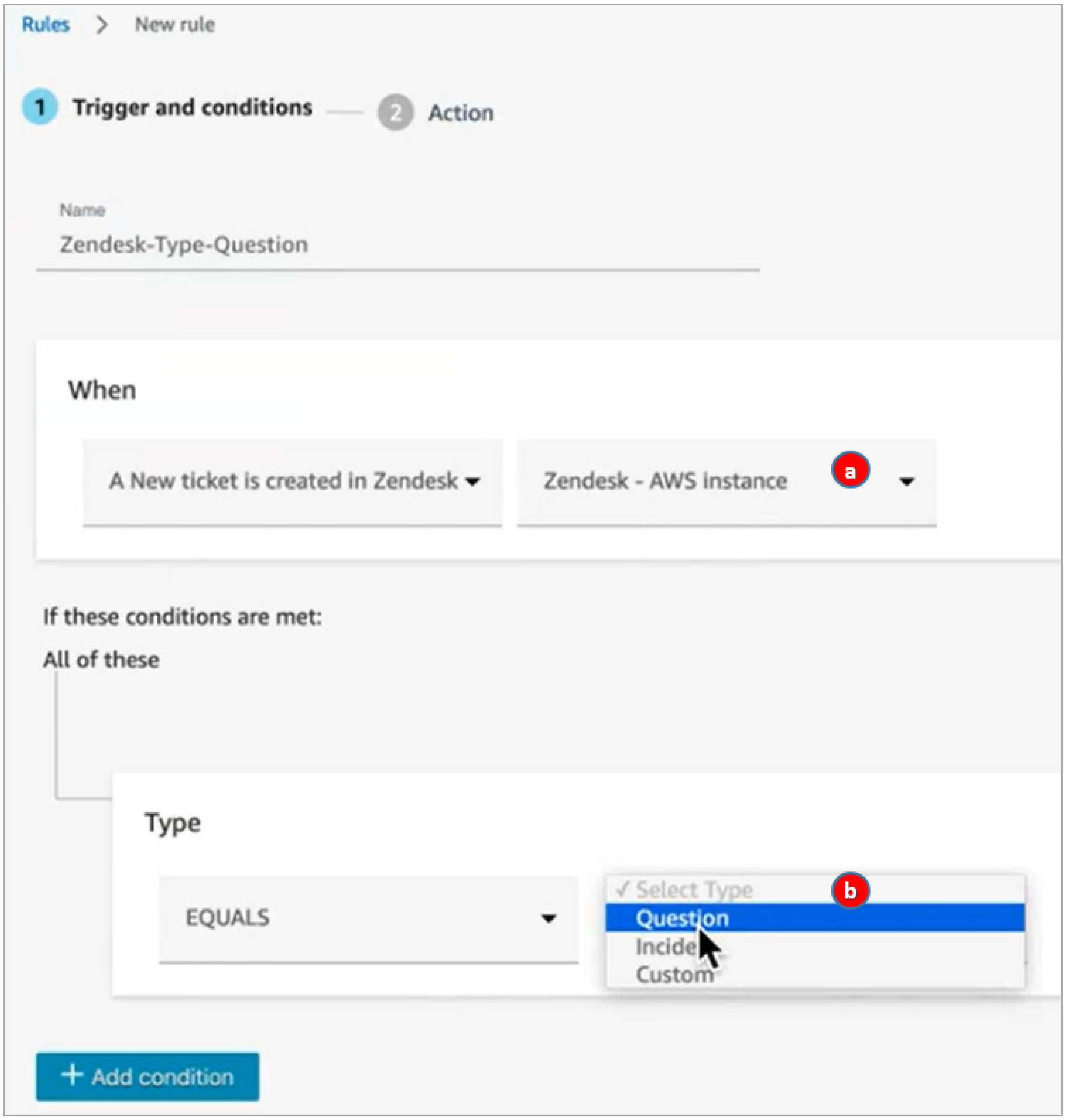
Name

Account_creation

Name can contain characters A-Z, 0-9, or '.', '-', '_'. It cannot contain spaces.

Enter a name for the rule. Spaces are not allowed.

5. Choose the event that will generate a task, and the instance of the external application where the event must occur.



Name: Zendesk-Type-Question

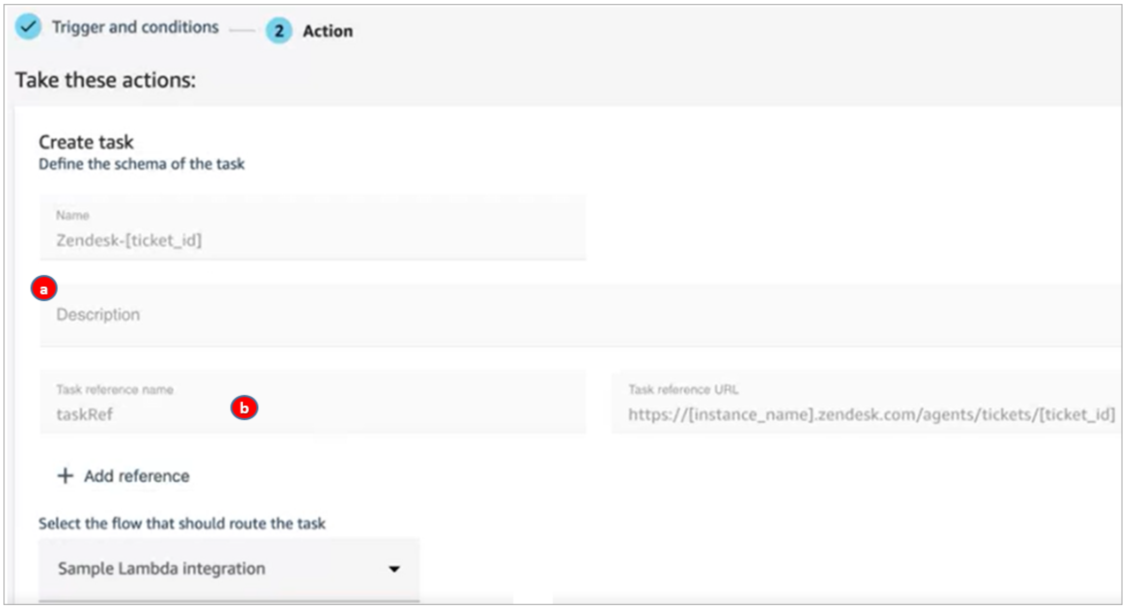
When: A New ticket is created in Zendesk; Zendesk - AWS instance

If these conditions are met:
All of these

Type: EQUALS

   1. Select the instance for the external application.
   2. Choose the conditions that must be met to generate the task.

6. Choose **Next**.
7. On the **Action** page, specify the task to be generated when the rule is met.



Take these actions:

Create task
Define the schema of the task

Name: Zendesk-[ticket_id]

Description

Task reference name: taskRef

Task reference URL: https://[instance_name].zendesk.com/agents/tickets/[ticket_id]

Select the flow that should route the task: Sample Lambda integration

1. The description of the task appears to the agent in their Contact Control Panel (CCP).
2. The task reference name appears to the agent as a link to the specified URL.

8. Choose **Save**.

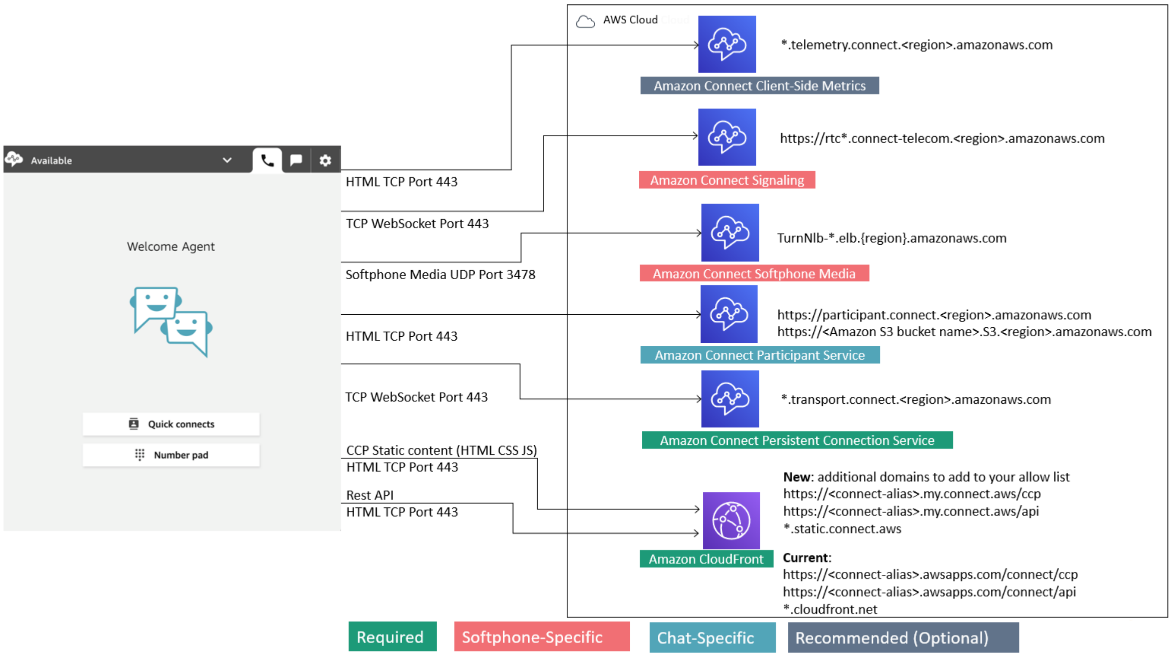
Test the rule

1. Go the external application and create the event that initiates the action. For example, in Zendesk, create a ticket that's type **Question**.
2. Go to **Analytics**, **Contact search**.
3. Under **Channel**, choose **Task**, and then choose **Search**.
4. Verify the task was created.

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.


Available
Welcome Agent
Quick connects
Number pad
HTML TCP Port 443
TCP WebSocket Port 443
Softphone Media UDP Port 3478
HTML TCP Port 443
TCP WebSocket Port 443
CCP Static content (HTML CSS JS)
HTML TCP Port 443
Rest API
HTML TCP Port 443
AWS Cloud
*.telemetry.connect.<region>.amazonaws.com
Amazon Connect Client-Side Metrics
https://rtc*.connect-telecom.<region>.amazonaws.com
Amazon Connect Signaling
TurnNlb-*.elb.{region}.amazonaws.com
Amazon Connect Softphone Media
https://participant.connect.<region>.amazonaws.com
https://<Amazon S3 bucket name>.S3.<region>.amazonaws.com
Amazon Connect Participant Service
*.transport.connect.<region>.amazonaws.com
Amazon Connect Persistent Connection Service
New: additional domains to add to your allow list
https://<connect-alias>.my.connect.aws/ccp
https://<connect-alias>.my.connect.aws/api
*.static.connect.aws
Amazon CloudFront
Current:
https://<connect-alias>.awsapps.com/connect/ccp
https://<connect-alias>.awsapps.com/connect/api
*.cloudfront.net
Required
Softphone-Specific
Chat-Specific
Recommended (Optional)

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

Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list

This first option lets you significantly reduce your blast radius.

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

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.

Domain/URL allow list	AWS Region	Ports	Direction	Traffic
rtc*.connect-telecom.{*region*}.amazonaws.com This is used by ccp# (v1). Please see the note following this table.	Replace {region} with the Region where your Amazon Connect instance is located	443 (TCP)	OUTBOUND	SEND/RECEIVE
***.my.connect.aws** {*myInstanceName*}.my.connect.aws/ccp-v2 {*myInstanceName*}.my.connect.aws/api *.static.connect.aws *.cloudfront.net **.awsapps.com:** {*myInstanceName*}.awsapps.com/connect/ccp-v2 {*myInstanceName*}.awsapps.com/connect/api *.cloudfront.net	Replace {*myInstanceName*} with the alias of your Amazon Connect instance	443 (TCP)	OUTBOUND	SEND/RECEIVE
*.telemetry.connect.{*region*}.amazonaws.com	Replace {*region*} with the location of your Amazon Connect instance	443 (TCP)	OUTBOUND	SEND/RECEIVE
participant.connect.{*region*}.amazonaws.com	Replace {*region*} with the location of your Amazon Connect instance	443 (TCP)	OUTBOUND	SEND/RECEIVE
*.transport.connect.{*region*}.amazonaws.com This is used by ccp-v2.	Replace {*region*} with the location of your Amazon Connect instance	443 (TCP)	OUTBOUND	SEND/RECEIVE
{*Amazon S3 bucket name*}.s3.{*region*}.amazonaws.com	Replace *Amazon S3 bucket name* with the name of the location where you store	443 (TCP)	OUTBOUND	SEND/RECEIVE

Domain/URL allow list	AWS Region	Ports	Direction	Traffic
	attachments. Replace {*region*} with the location of your Amazon Connect instance			
TurnNlb-*.elb.{*region*}.amazonaws.com To instead add specific endpoints to your allow list based on Region, see NLB endpoints (p. 608).	Replace {*region*} with the location of your Amazon Connect instance	3478 (UDP)	OUTBOUND	SEND/RECEIVE
GLOBALACCELERATOR	GLOBAL and Region where your Amazon Connect instance is located (add GLOBAL AND any region-specific entry to your allow list)	443 (HTTPS) and 80 (HTTP)	OUTBOUND	SEND/RECEIVE

Note

If you're using SAML Sign-In to your Amazon Connect instance, add the Global Accelerator domain to your allow list: ***.awsglobalaccelerator.com**.

Tip

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

The following table lists the CloudFront domains used for static assets if you want to add domains to your allow list instead of IP ranges:

Region	CloudFront Domain
us-east-1	https://dd401jc05x2yk.cloudfront.net/ https://d1f0uslncy85vb.cloudfront.net/
us-west-2	https://d38fzyjx9jg8fj.cloudfront.net/ https://d366s8lxuwna4d.cloudfront.net/
ap-northeast-1	https://d3h58onr8hrozw.cloudfront.net/ https://d13ljas036gz6c.cloudfront.net/
ap-southeast-1	https://d2g7up6vqvaq2o.cloudfront.net/ https://d12o1dl1h4w0xc.cloudfront.net/

Region	CloudFront Domain
ap-southeast-2	https://d2190hliw27bb8.cloudfront.net/ https://d3mgrlqzmisce5.cloudfront.net/
eu-central-1	https://d1n9s7btyr4f0n.cloudfront.net/ https://d3tqoc05lsydd3.cloudfront.net/
eu-west-2	https://dl32tyuy2mmv6.cloudfront.net/ https://d2p8ibh10q5exz.cloudfront.net/

ca-central isn't included in the table because we host static contents behind the domain `*.my.connect.aws` so no addition to the allow list is needed.

If your business does not use SAML, and you have firewall restrictions, you can add the following entries per Region:

Region	CloudFront Domain
us-east-1	https://d32i4gd7pg4909.cloudfront.net/
us-west-2	https://d18af777lco7lp.cloudfront.net/
eu-west-2	https://d16q6638mh01s7.cloudfront.net/
ap-northeast-1	https://d2c2t8mxjhq5z1.cloudfront.net/
ap-southeast-1	https://d3qzmd7y07pz0i.cloudfront.net/
ap-southeast-2	https://dwcpoxuuza83q.cloudfront.net/
eu-central-1	https://d1whcm49570jjw.cloudfront.net/
ca-central-1	https://d2wfbsypmqjmog.cloudfront.net/
us-gov-east-1:	https://s3-us-gov-east-1.amazonaws.com/warp-drive-console-static-content-prod-osu/
us-gov-west-1:	https://s3-us-gov-west-1.amazonaws.com/warp-drive-console-static-content-prod-pdt/

NLB endpoints

The following table lists the specific endpoints for the Region the Amazon Connect instance is in. If you don't want to use the TurnNlb-*.elb.{*region*}.amazonaws.com wildcard, you can add these endpoints to your allow list instead.

Region	Turn Domain/URL
us-west-2	TurnNlb-8d79b4466d82ad0e.elb.us-west-2.amazonaws.com TurnNlb-dbc4ebb71307fda2.elb.us-west-2.amazonaws.com

Region	Turn Domain/URL
us-east-1	TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com TurnNlb-31a7fe8a79c27929.elb.us-east-1.amazonaws.com TurnNlb-7a9b8e750cec315a.elb.us-east-1.amazonaws.com
af-south-1	TurnNlb-29b8f2824c2958b8.elb.af-south-1.amazonaws.com
ap-northeast-1	TurnNlb-3c6ddabcbeb821d8.elb.ap-northeast-1.amazonaws.com
ap-northeast-2	TurnNlb-a2d59ac3f246f09a.elb.ap-northeast-2.amazonaws.com
ap-southeast-1	TurnNlb-261982506d86d300.elb.ap-southeast-1.amazonaws.com
ap-southeast-2	TurnNlb-93f2de0c97c4316b.elb.ap-southeast-2.amazonaws.com
ca-central-1	TurnNlb-b019de6142240b9f.elb.ca-central-1.amazonaws.com
eu-central-1	TurnNlb-ea5316ebe2759cbc.elb.eu-central-1.amazonaws.com
eu-west-2	TurnNlb-1dc64a459ead57ea.elb.eu-west-2.amazonaws.com
us-gov-west-1	TurnNlb-d7c623c23f628042.elb.us-gov-west-1.amazonaws.com

Option 2 (not recommended): Allow IP address ranges

The second option relies on using an allow list, also known as whitelisting, the IP addresses used by Amazon Connect. You create this allow list using the IP addresses in the AWS ip-ranges.json file.

For more information about this file, see About Amazon Connect IP address ranges (p. 610).

IP-Ranges entry	AWS Region	Ports/Protocols	Direction	Traffic
AMAZON_CONNECT	GLOBAL and Region where your Amazon Connect instance is located (add GLOBAL AND any region-specific entry to your allow list)	3478 (UDP)	OUTBOUND	SEND/RECEIVE

IP-Ranges entry	AWS Region	Ports/Protocols	Direction	Traffic
EC2	GLOBAL and Region where your Amazon Connect instance is located (GLOBAL only if a region-specific entry doesn't exist)	443 (TCP)	OUTBOUND	SEND/RECEIVE
CLOUDFRONT	Global*	443 (TCP)	OUTBOUND	SEND/RECEIVE
GLOBALACCELERATOR	GLOBAL and Region where your Amazon Connect instance is located (add GLOBAL AND any region-specific entry to your allow list)	443 (HTTPS) and 80 (HTTP)	OUTBOUND	SEND/RECEIVE

Note
If you're using SAML Sign-In to your Amazon Connect instance, be sure to add the Global Accelerator domain to your allow list: ***.awsglobalaccelerator.com**.

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

About Amazon Connect IP address ranges

In the AWS ip-ranges.json file, the whole /19 IP address range is owned by Amazon Connect. All traffic to and from the /19 range comes to and from Amazon Connect.

The /19 IP address range isn't shared with other services. It's for the exclusive use to Amazon Connect globally.

In the AWS ip-ranges.json file, you can see the same range listed twice. For example:

```
{ "ip_prefix": "15.193.0.0/19",
"region": "GLOBAL",
"service": "AMAZON"
},
{
"ip_prefix": "15.193.0.0/19",
"region": "GLOBAL",
"service": "AMAZON_CONNECT"
},
```

AWS always publishes any IP range twice: one for the specific service, and one for “AMAZON” service. There could even be a third listing for a more specific use case within a service.

When there are new IP address ranges supported for Amazon Connect, they are added to the publicly available ip-ranges.json file. They are kept for a minimum of 30 days before they are used by the service.

After 30 days, softphone traffic through the new IP address ranges increases over the subsequent two weeks. After two weeks, traffic is routed through the new ranges equivalent to all available ranges.

For more information about this file and IP address ranges in AWS, see AWS IP Address Ranges.

Stateless firewalls

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

IP-Range entry	Port	Direction	Traffic
AMAZON_CONNECT	49152-65535 (UDP)	INBOUND	SEND/RECEIVE

Allow DNS resolution for softphones

If you already added Amazon Connect IP ranges to your allow list, and you don't have any restriction on DNS name resolution, then you don't need to add **TurnNlb-*.elb.{*region*}.amazonaws.com** to your allow list.

- To check whether there are restrictions on DNS name resolution, while on your network, use the `nslookup` command. For example:

  ```
  nslookup TurnNlb-d76454ac48d20c1e.elb.us-east-1.amazonaws.com
  ```

If you can't resolve the DNS, you must add the TurnNLB endpoints listed above (p. 608) or **TurnNlb-*.elb.{*region*}.amazonaws.com** to your allow list.

If you don't allow this domain, your agents will get the following error in their Contact Control Panel (CCP) when they try to answer a call:

- Failed to establish softphone connection. Try again or contact your administrator with the following: Browser unable to establish media channel with turn:TurnNlb-xxxxxxxxxxxxx.elb.{*region*}.amazonaws.com:3478?transport=udp

Port and protocol considerations

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

- You need to allow traffic for all addresses and ranges for the Region in which you created your Amazon Connect instance.
- If you are using a proxy or firewall between the CCP and Amazon Connect, increase the SSL certificate cache timeout to cover the duration of an entire shift for your agents, Do this to avoid connectivity issues with certificate renewals during their scheduled working time. For example, if your agents are scheduled to work 8 hour shifts that include breaks, increase the interval to 8 hours plus time for breaks and lunch.
- When opening ports, Amazon EC2 and Amazon Connect require only the ports for endpoints in the same Region as your instance. CloudFront, however, serves static content from an edge location that has the lowest latency in relation to where your agents are located. IP range 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 agents. If you need to set up an instance in a specific Region to comply with company policies or other regulations, choose the configuration that results in the fewest network hops between your agents' computers and your Amazon Connect instance.
- **Location of your callers**—Because calls are anchored to your Amazon Connect Region endpoint, they are subject to PSTN latency. Ideally your callers and transfer endpoints are geographically located as closely as possible to the AWS Region where your Amazon Connect instance is hosted for lowest latency.

  For optimal performance, and to limit the latency for your customers when they call in to your contact center, create your Amazon Connect instance in the Region that is geographically closest to where your customers call from. You might consider creating multiple Amazon Connect instances, and providing contact information to customers for the number that is closest to where they call from.
- **External transfers**—from Amazon Connect remain anchored to your Amazon Connect Region endpoint for the duration of the call. Per-minute usage continues to accrue until the call is disconnected by the recipient of the transferred call. The call is not recorded after the agent drops or the transfer completes. The contact record data and associated call recording of a transferred call are generated after the call is terminated. Whenever possible, don't transfer calls that could be transferred back into Amazon Connect, known as circular transfers, to avoid compounding PSTN latency.

Agents using Amazon Connect remotely

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

Rerouting audio

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

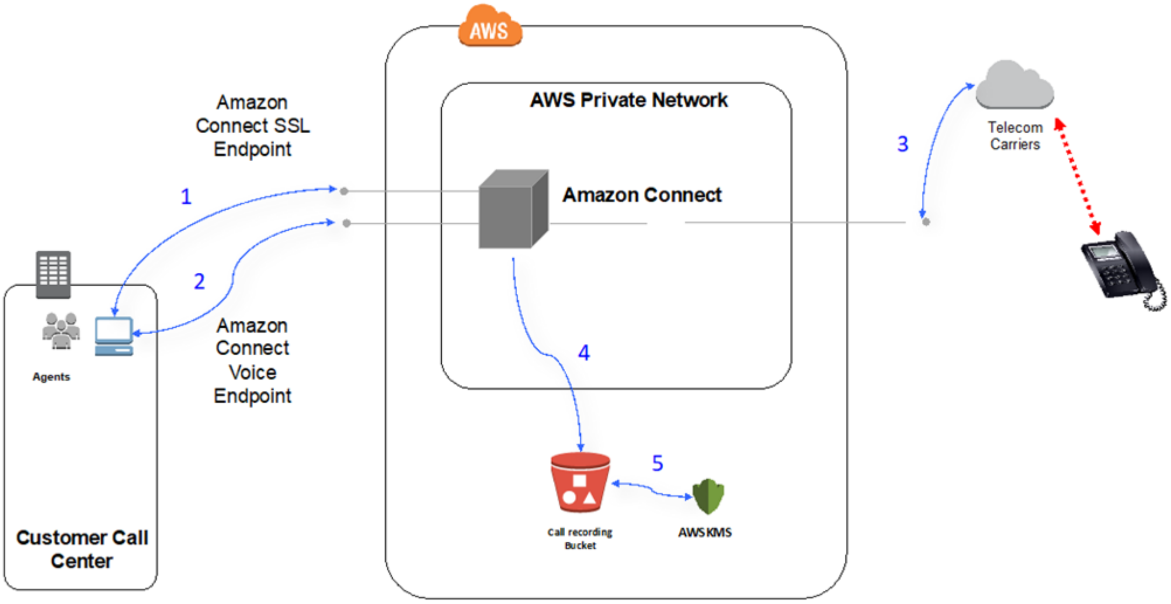
Using AWS Direct Connect

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

Detailed network paths for Amazon Connect

Voice calls

The following diagram shows how voice calls flow through Amazon Connect

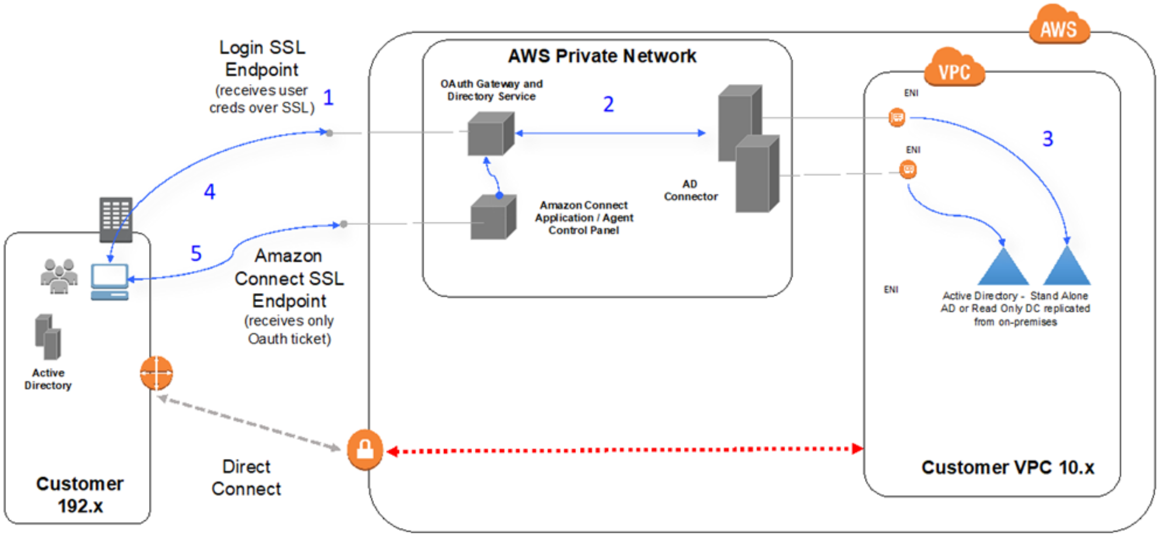


1. Users access the Amazon Connect application using a web browser. All communications are encrypted in transit using TLS.
2. Users establish voice connectivity to Amazon Connect from their browser using WebRTC. Signaling communication is encrypted in transit using TLS. Audio is encrypted in transit using SRTP.
3. Voice connectivity to traditional phones (PSTN) is established between Amazon Connect and AWS's telecommunications carrier partners using private network connectivity. In cases where shared network connectivity is used, signaling communication is encrypted in transit using TLS and audio is encrypted in transit using SRTP.
4. Call recordings are stored in your Amazon S3 bucket that Amazon Connect has been given permissions to access. This data is encrypted between Amazon Connect and Amazon S3 using TLS.

5. Amazon S3 server-side encryption is used to encrypt call recordings at rest using a customer-owned KMS key.

Authentication

The following diagram shows using the AD Connector with AWS Directory Service to connect to an existing customer Active Directory installation. The flow is similar to using AWS Managed Microsoft AD.


Login SSL Endpoint (receives user creds over SSL)
1
AWS
AWS Private Network
OAuth Gateway and Directory Service
2
AD Connector
Amazon Connect Application / Agent Control Panel
VPC
ENI
ENI
3
ENI
Active Directory - Stand Alone AD or Read Only DC replicated from on-premises
4
5
Amazon Connect SSL Endpoint (receives only Oauth ticket)
Active Directory
Customer 192.x
Direct Connect
Customer VPC 10.x

1. The user's web browser initiates authentication to an OAuth gateway over TLS via the public internet with user credentials (Amazon Connect login page).
2. OAuth gateway sends the authentication request over TLS to AD Connector.
3. AD Connector does LDAP authentication to Active Directory.
4. The user's web browser receives OAuth ticket back from gateway based on authentication request.
5. The client loads the Contact Control Panel (CCP). The request is over TLS and uses OAuth ticket to identify user/directory.

Using Amazon Connect in a VDI environment

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

- **Location of your agents**—Ideally, there are as few hops as possible with the lowest round trip time between the location from which your agents use the CCP and the VDI host location.
- **Host location of your VDI solution**—Ideally, your VDI host location is on the same network segment as your agents, with as few hops as possible from both internal resources as well as an edge router. You also want the lowest round-trip time possible to both WebRTC and Amazon EC2 range endpoints.
- **Network**—Each hop that traffic goes through between endpoints increases the possibility of failure and adds opportunity to introduce latency. VDI environments are particularly susceptible to call quality

issues if the underlying route is not optimized or the pipe isn't either fast or wide enough. While AWS Direct Connect can improve call quality from the edge router to AWS, it will not address internal routing issues. You may need to upgrade or optimize your private LAN/WAN, or redirect to an external device to circumvent call audio issues. In most scenarios, if this is required, the CCP is not the only application that is having issues.

- **Dedicated resources**—at the Network and desktop level are recommended to prevent an impact to available agent resources from activities, such as backups and large file transfers. One way to prevent resource contention is by restricting the desktop access to Amazon Connect users who will be using their environment similarly, instead of sharing resources with other business units who may use those resources differently.
- **Using a soft phone with remote connections**—in VDI environments can cause impact to audio quality.

> **Tip**
> If your agents connect to a remote endpoint and operates in that environment, we recommend either rerouting audio to an external E.164 endpoint or connecting the media through the local device and then signaling through the remote connection.

You can build a custom CCP with the Amazon Connect Streams API by creating a CCP with no media for call signaling. This way, the media is handled on the local desktop using standard CCP, and the signaling and call controls are handled on the remote connection with the CCP with no media. For more information about the streams API, see the GitHub repository at https://github.com/aws/amazon-connect-streams.

CCP connectivity

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

Outbound calls

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

Inbound calls

- When an inbound call is received, the call is anchored to an Amazon Connect endpoint. Any external transfers or conferences also use this anchor until the call is disconnected.
- When an agent is available, the call is pushed through 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, contact records and associated recordings are generated and made available for the call.

Missed calls

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

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 **Approved origins**.
4. Choose **Add origin**.
5. Type the URL and choose **Add**.

Add an Amazon Lex bot

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

With Amazon Lex, you can build conversational interactions (bots) that feel natural to your customers. Amazon Connect with Amazon Lex bots can also capture customer input as digits that customers enter on their numeric keypad when used in an Amazon Connect 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.

> **Tip**
> You can also use Amazon Lex to power interactive messages for Amazon Connect chat. Interactive messages are rich messages that present a prompt and pre-configured display options that a customer can select from. These messages are powered by Amazon Lex and configured through Amazon Lex using a Lambda. For more information, see Add interactive messages to chat (p. 633).

Create an Amazon Lex bot

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

Amazon Lex

1. Open the Amazon Lex console.
2. Choose **Create bot**.
3. On the **Configure bot settings** page, choose **Create - Create a blank bot** and provide the following information:
   - **Bot name** — For this walkthrough, name the bot **AccountBalance**.
   - **IAM permissions** — Select a role if you have one created. Otherwise, choose **Create a role with basic Amazon Lex permissions**.
   - **COPPA** — Choose whether the bot is subject to the Child Online Privacy Protection Act.
   - **Session timeout** — Choose how long the bot should wait to get input from a caller before ending the session.
4. Choose **Next**.
5. Provide language and voice specific information:
   - **Language** — Select language and locale from the list of Languages and locales supported by Amazon Lex.
   - **Voice interaction** — Select the voice for your bot to use when speaking to callers. The default voice for Amazon Connect is Joanna.
6. Choose **Done**. The AccountBalance bot is created, and the **Intent** page is displayed.

Amazon Lex (Classic)

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

Configure the Amazon Lex bot

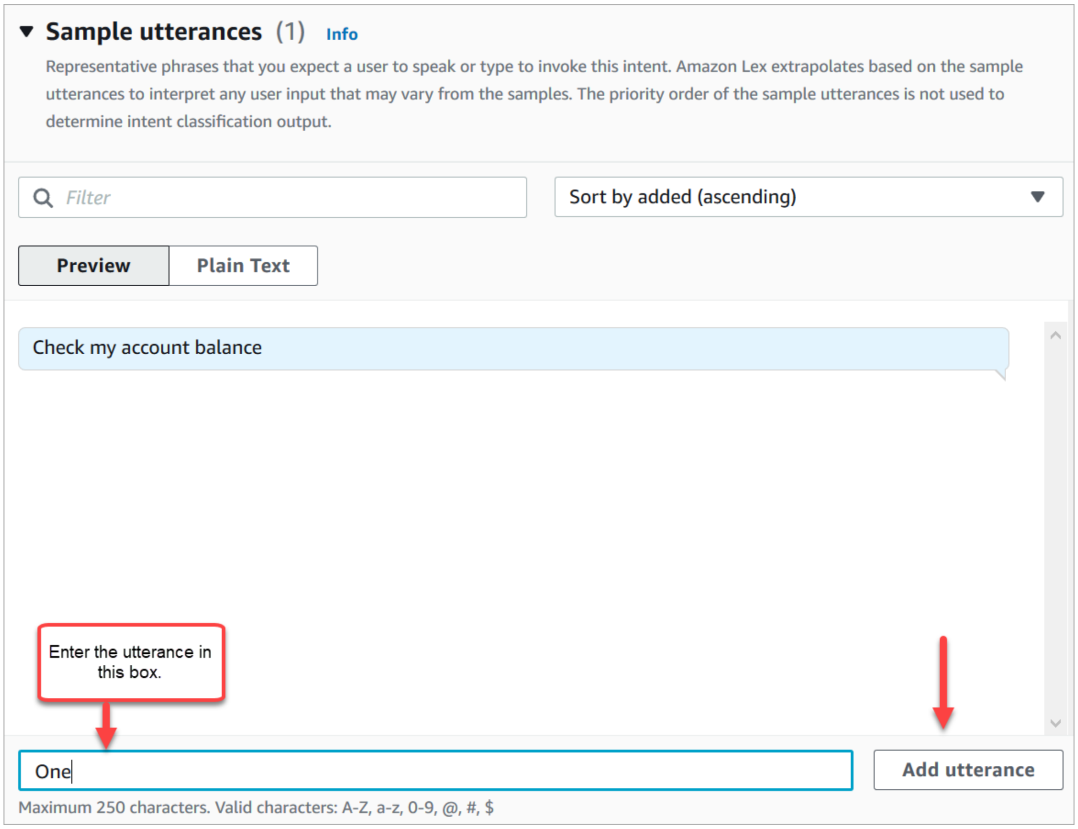
In this step you'll determine how the bot responds to customers by providing intents, sample utterances, slots for input, and error handling.

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

Create AccountLookup intent

Amazon Lex

1. After you created the bot, you are on the **Intents** page the Amazon Lex console. If you're not there, you can get there by choosing **Bots**, **AccountBalance**, **Bot versions**, **Draft version**, **Intents**. Choose **Add intent**, **Add empty intent**.
2. In the **Intent name** box, enter **AccountLookup**.
3. Scroll down the page to **Sample utterances**. In this step you enter utterances that allow the customer to elicit the AccountLookup intent. Enter the following utterances, and choose **Add utterance** after each one.
   - **Check my account balance**
   - **One**: This assigns the utterance of “one” or key press of “1” to the **AccountLookup** intent.



▼ Sample utterances (1) Info
Representative phrases that you expect a user to speak or type to invoke this intent. Amazon Lex extrapolates based on the sample utterances to interpret any user input that may vary from the samples. The priority order of the sample utterances is not used to determine intent classification output.
Filter
Sort by added (ascending)
Preview
Plain Text
Check my account balance
Enter the utterance in this box.
One
Add utterance
Maximum 250 characters. Valid characters: A-Z, a-z, 0-9, @, #, $

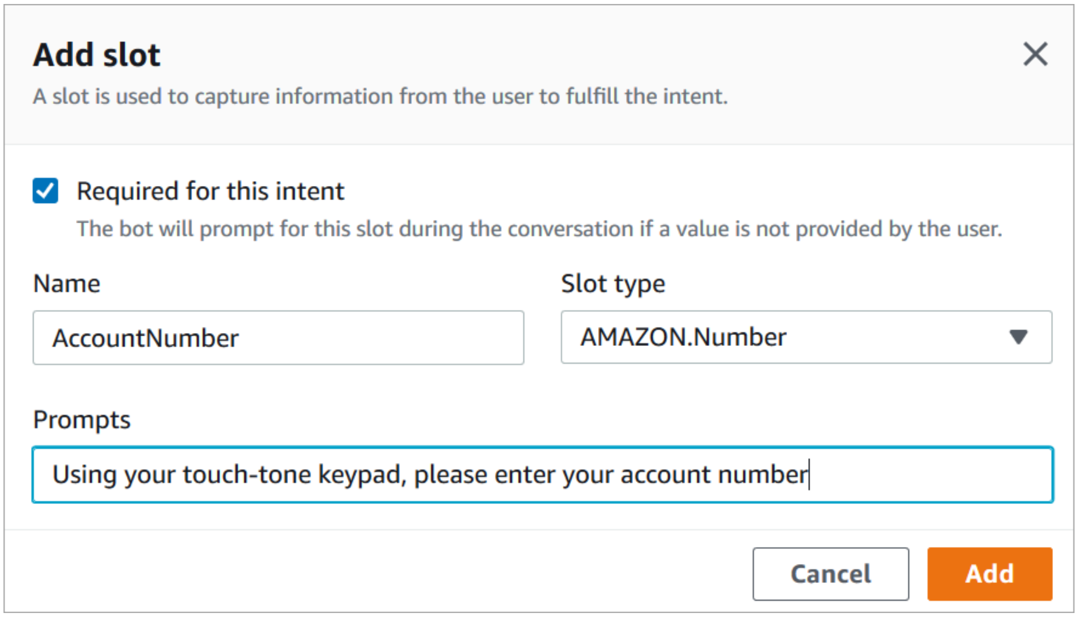
4. Scroll to the **Slots** section, and choose **Add slot**. Complete the box as follows:

   a. **Required for this intent** = selected.

   b. **Name** = **AccountNumber**.

   c. **Slot type** = **AMAZON.Number**.

   d. **Prompts** = the text to be spoken when the call is answered. For example, ask callers to enter their account number using their keypad: **Using your touch-tone keypad, please enter your account number**. Choose **Add**.



Add slot

A slot is used to capture information from the user to fulfill the intent.

☑ Required for this intent

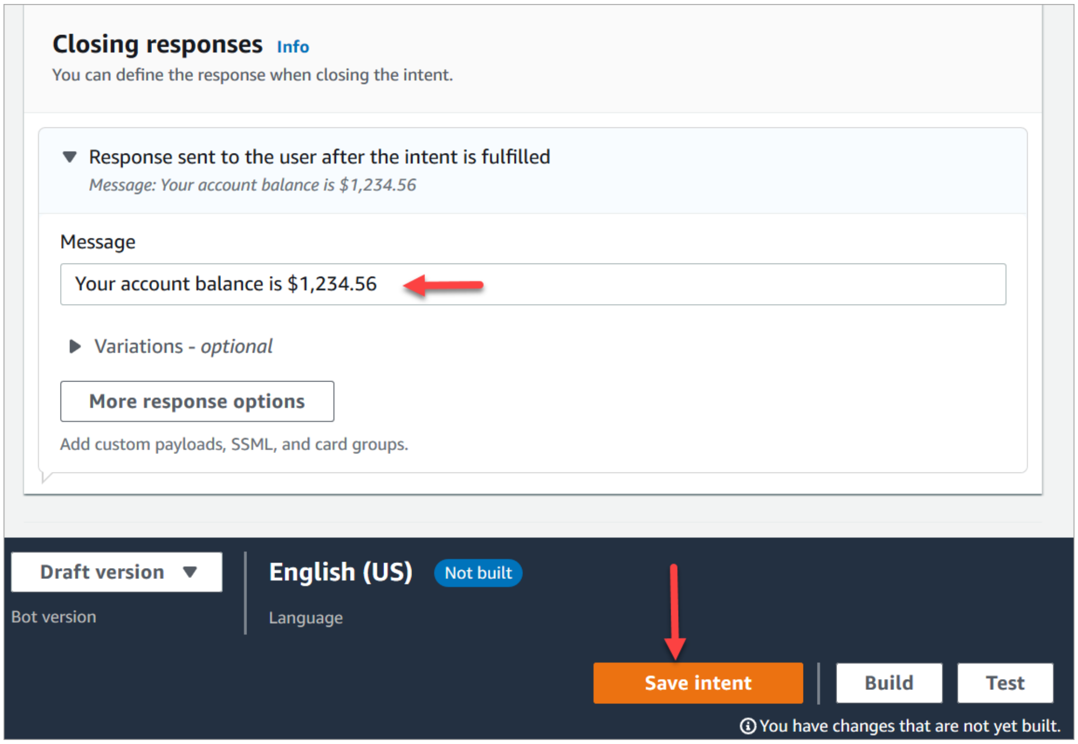
The bot will prompt for this slot during the conversation if a value is not provided by the user.

Name: AccountNumber

Slot type: AMAZON.Number

Prompts: Using your touch-tone keypad, please enter your account number

5. Scroll to the **Closing responses** section. Add a message for the bot to say to customers. For example, **Your account balance is $1,234.56**. (For this walkthrough, we aren't going to actually get the data, which is what you would do in reality.)



Closing responses Info

You can define the response when closing the intent.

▼ Response sent to the user after the intent is fulfilled

Message: Your account balance is $1,234.56

Message: Your account balance is $1,234.56

▶ Variations - *optional*

Add custom payloads, SSML, and card groups.

ⓘ You have changes that are not yet built.

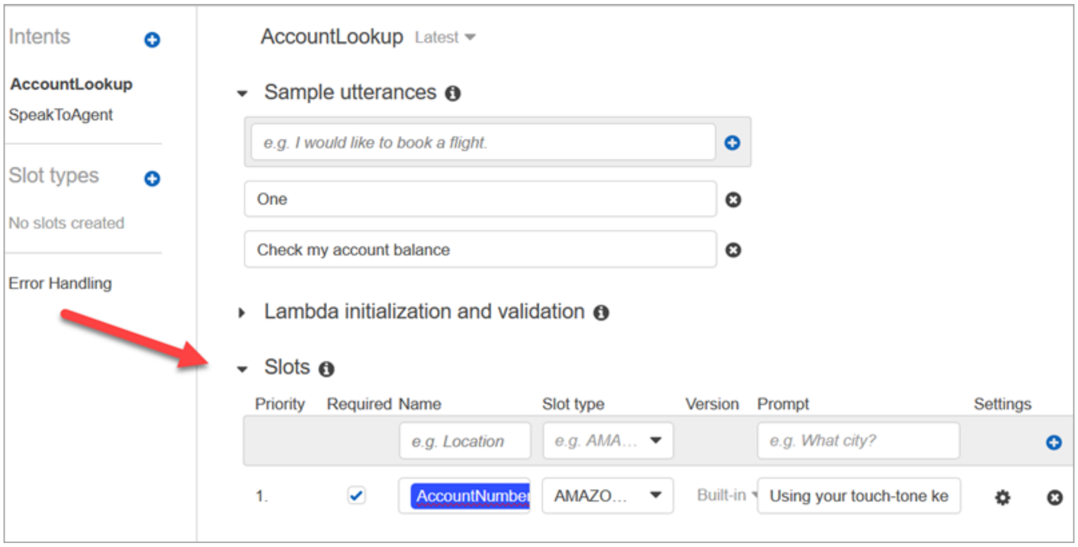
6. Choose **Save intent**.

Amazon Lex (Classic)

1. In the Amazon Lex console choose the **+** icon next to **Intents**, and choose **Create new intent**.

2. Name the intent **AccountLookup**.
3. Add a sample utterance, such as *Check my account balance*, and choose the **+** icon.
4. Add a second utterance, such as *One* and choose the **+** icon. This assigns the utterance of “one” or key press of “1” to the **AccountLookup** intent.

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



One

Check my account balance

1. ☑ AccountNumber AMAZO... Built-in Using your touch-tone ke

6. For **Slot type**, use the drop-down to choose **AMAZON.NUMBER**.
7. For **Prompt**, add the text to be spoken when the call is answered. For example, ask callers to enter their account number using their keypad: *Using your touch-tone keypad, please enter your account number*.
8. Choose the + icon.
9. Make sure that the **Required** check box is selected.
10. In the **Response** section, add a message for the bot to say to customers. For example, **Your account balance is $1,234.56**.
11. Choose **Save Intent**.

Create SpeakToAgent intent

Amazon Lex

1. Navigate to the **Intents** page: choose **Back to intents list**.
2. Choose **Add intent**, **Add empty intent**.
3. In the **Intent name** box, enter **SpeakToAgent**, and then choose **Add**.
4. Scroll down to **Sample utterances** section. Enter the following utterances, which allow the customer to elicit the SpeakToAgent intent:

   - **Speak to an agent**
   - **Two**

5. Scroll down to the **Closing responses** section. Add a message for the bot to say to customers. For example, **Okay, an agent will be with you shortly**.
6. Choose **Save intent**.

Amazon Lex (Classic)

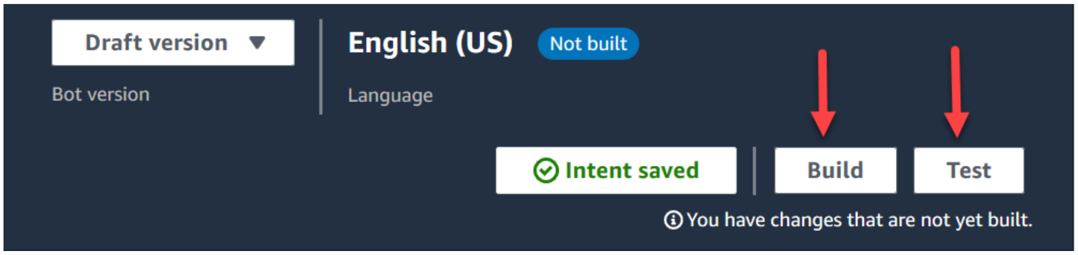
1. In the Amazon Lex console choose the **+** icon next to **Intents**, and choose **Create new intent**.
2. Name the intent **SpeakToAgent**.
3. Select **SpeakToAgent**.
4. Add a sample utterance, such as *Speak to an agent*, and choose **+**.
5. Add a second utterance, such as *Two*, and choose **+**.
6. Add a message that lets callers know that their call is being connected to an agent. For example, “Okay, an agent will be with you shortly.”
7. Choose **Save Intent**.

Build and test the Amazon Lex bot

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

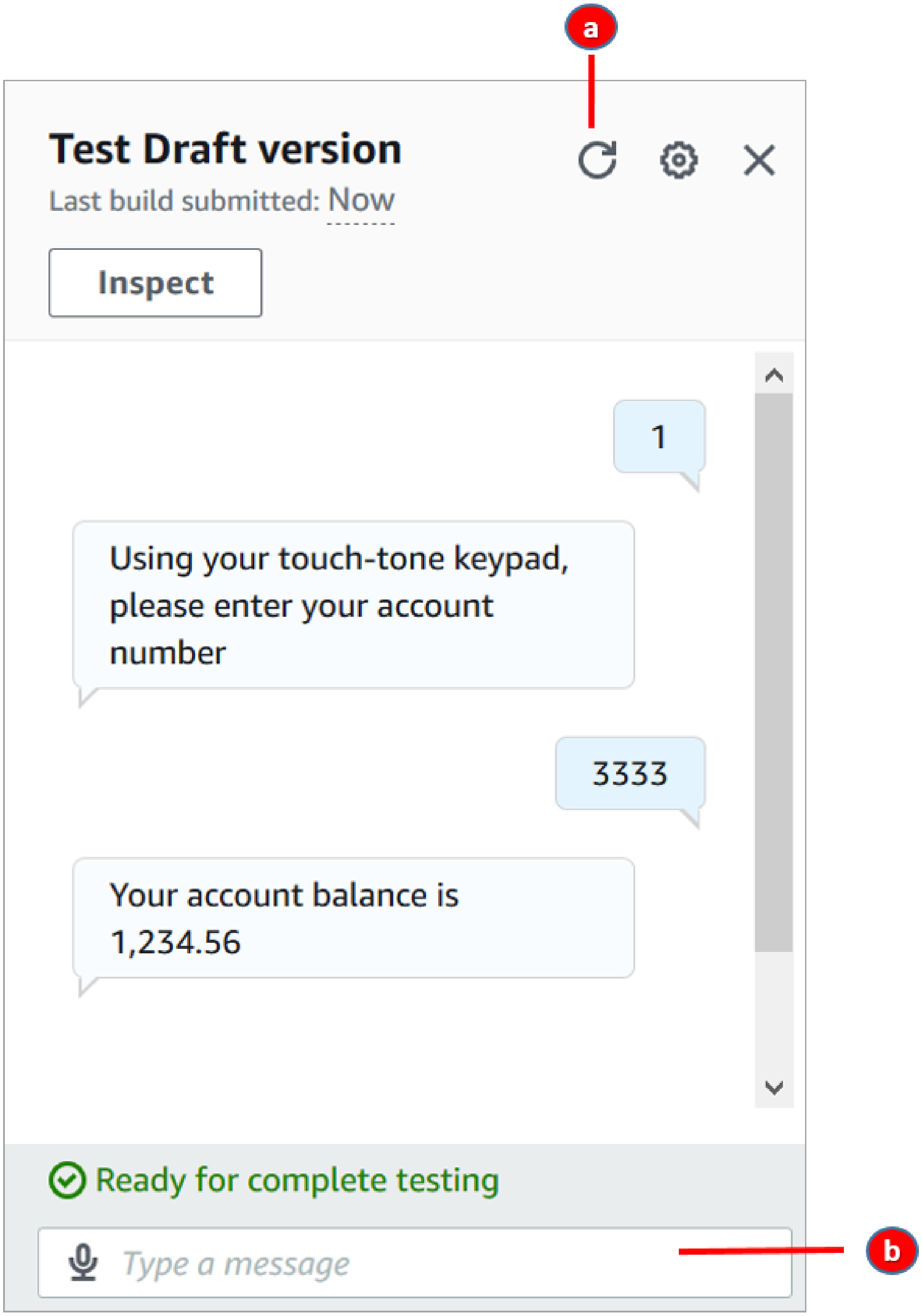
Amazon Lex

1. At the bottom of the page, choose **Build**. It may take a minute or two.



You have changes that are not yet built.

2. When it's finished building, choose **Test**.
3. Let's test the **AccountLookup** intent: In the **Test Draft version** pane, in the **Type a message** box, type **1** and press Enter. Then type a fictitous account number and press Enter.



1

Using your touch-tone keypad, please enter your account number

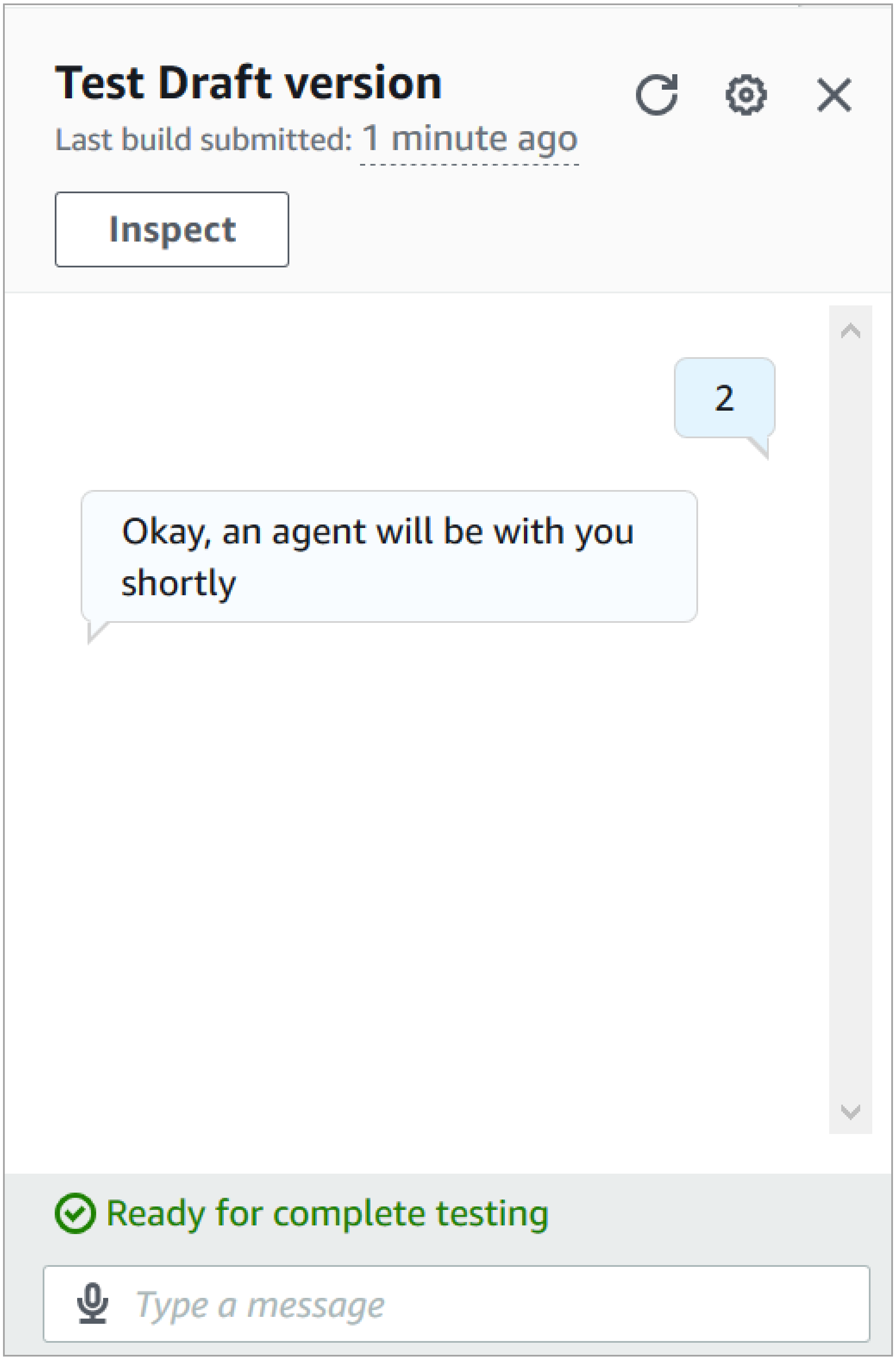
3333

Your account balance is 1,234.56

a. Clear the test box.

b. Type the intents you want to test.

4. To confirm that the **SpeakToAgent** intent is working, clear the test box, and then type **2** and press Enter.



Test Draft version
Last build submitted: 1 minute ago
Inspect

2

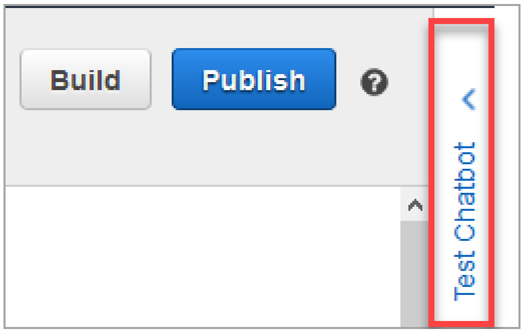
Okay, an agent will be with you shortly

Ready for complete testing
Type a message

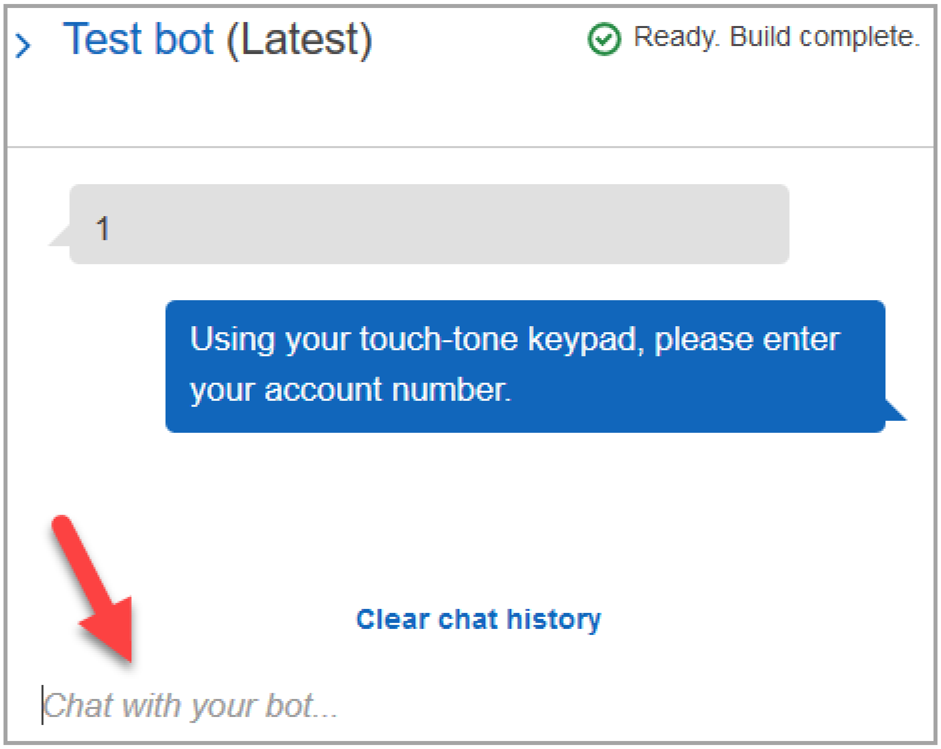
5. Close the **Test Draft version** pane.

Amazon Lex (Classic)

1. Choose **Build**. It may take a minute or two.
2. When it's finished building, choose **Test Chatbot**.



3. Let's test the **AccountLookup** intent: In the **Test Chatbot** pane, in the **Chat with your bot** box, type **1**. Then type a fictitious account number.



4. Choose **Clear chat history**.
5. To confirm that the **SpeakToAgent** intent is working, type **2**.

Create a bot version (Optional)

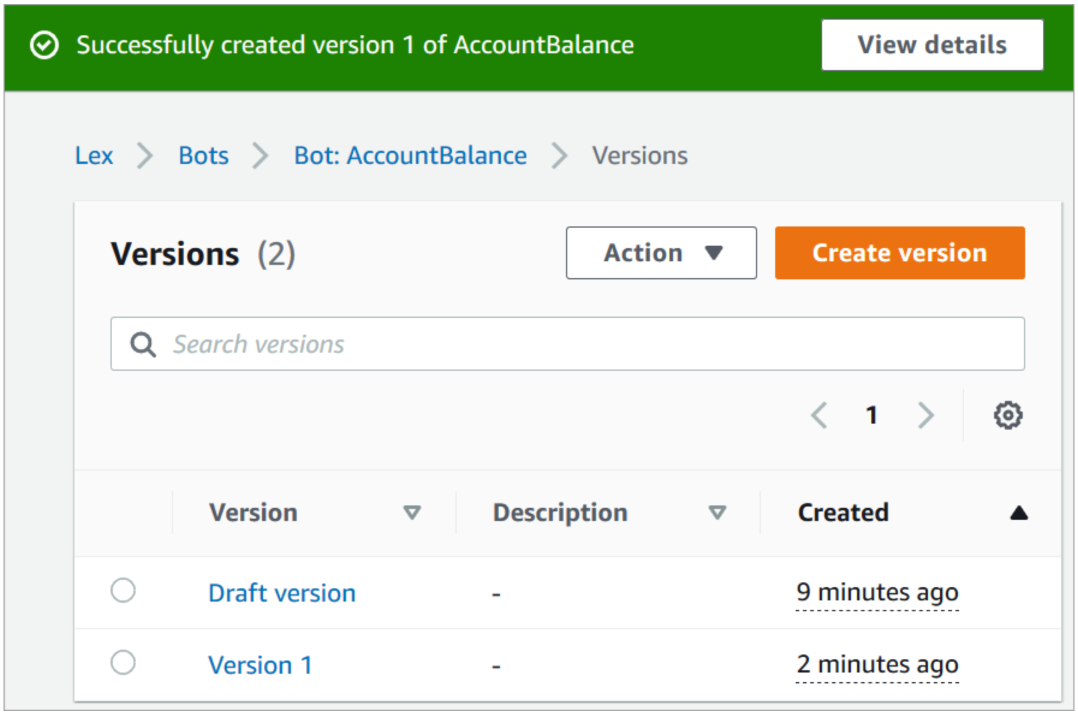
In this step you create a new bot version to use in an alias. It's how you create an alias that can be used in a production environment. Test aliases are subject to lower throttling limits. Although this is a test walkthrough, creating a version is a best practice.

Amazon Lex

1. If you're on the **Intents** page, choose **Back to intents list**.

2. On the left menu, choose **Bot versions**.
3. Choose **Create version**.
4. Review the details of the **AccountBalance** bot, and then choose **Create**.

   This creates a version of your bot (Version 1). to associate a version directly with an alias. You can switch versions on an non-test alias without having to track which version is getting published.

   Successfully created version 1 of AccountBalance

	Version	Description	Created
○	Draft version	-	9 minutes ago
○	Version 1	-	2 minutes ago

Create an alias for the bot

Amazon Lex

1. In the left menu, choose **Aliases**.
2. On the **Aliases** page, choose **Create alias**.
3. In the **Alias name** box, enter a name, such as **Test**. Later in this walkthrough you'll use this alias to specify this version of the bot in your contact flow.

   Important
   In a production environment, always use a different alias than **TestBotAlias** for Amazon Lex and **$LATEST** for Amazon Lex classic. **TestBotAlias** and **$LATEST** support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime Service Quotas.
4. For **Associated version**, choose the version you just created, such as **Version 1**.
5. Choose **Create**.

Amazon Lex (Classic)

1. Choose **Publish**.

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

   Important

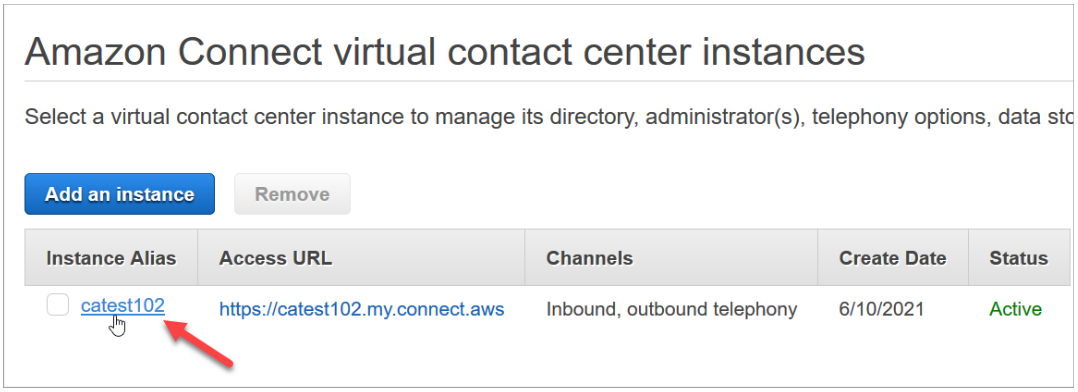
   In a production environment, always use a different alias than **TestBotAlias** for Amazon Lex and **$LATEST** for Amazon Lex classic. **TestBotAlias** and **$LATEST** support a limited number of concurrent calls to an Amazon Lex bot. For more information, see Runtime Service Quotas.

3. Choose **Publish**.

Add the Amazon Lex bot to your Amazon Connect instance

Amazon Lex

1. Open the Amazon Connect console.
2. Select the Amazon Connect instance that you want to integrate with your Amazon Lex bot.

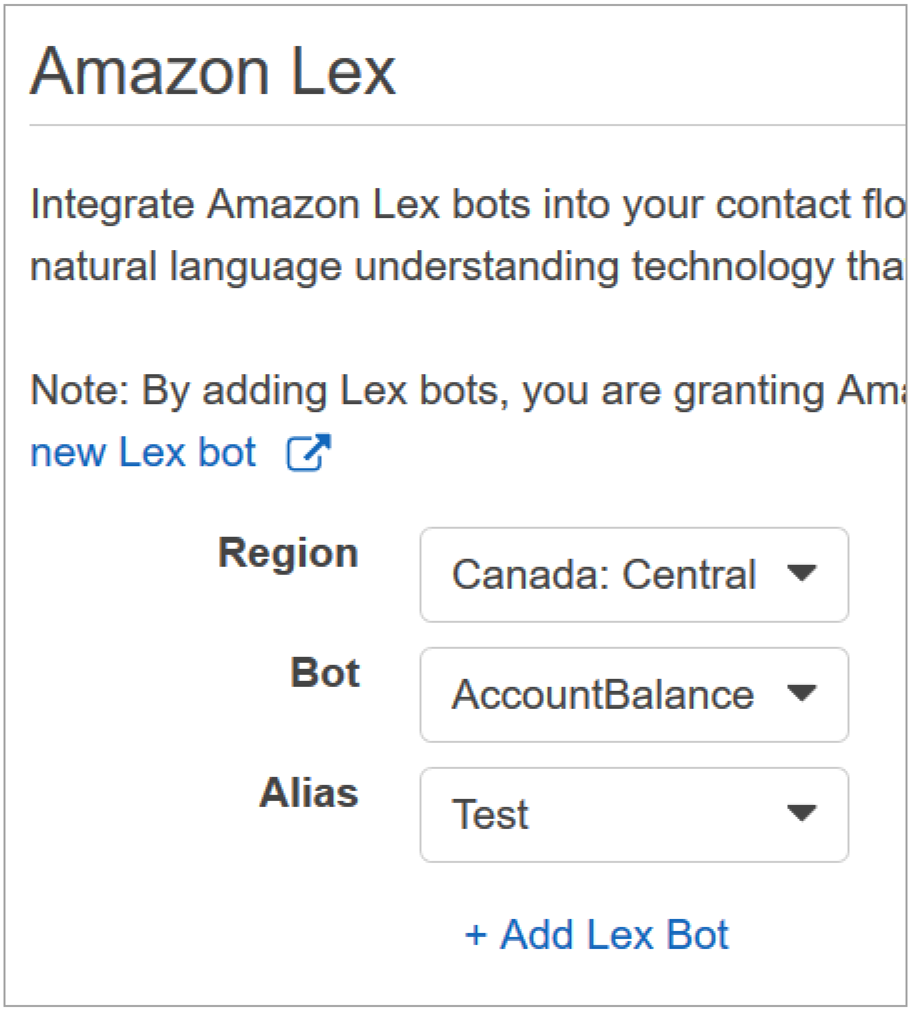


Amazon Connect virtual contact center instances

Select a virtual contact center instance to manage its directory, administrator(s), telephony options, data stc

Instance Alias	Access URL	Channels	Create Date	Status
□ catest102	https://catest102.my.connect.aws	Inbound, outbound telephony	6/10/2021	Active

3. On the navigation menu, choose **Contact flows**.
4. Under **Amazon Lex**, use the dropdown to select the Region of your Amazon Lex bot, and then select your Amazon Lex bot, **AccountBalance**.
5. Select the Amazon Lex bot alias name from the dropdown (**Test**), and then choose **+ Add Lex Bot**.



Amazon Lex

Integrate Amazon Lex bots into your contact flo
natural language understanding technology tha

Note: By adding Lex bots, you are granting Am
new Lex bot

Region: Canada: Central

Bot: AccountBalance

Alias: Test

Note
Amazon Connect uses Amazon Lex resource-based policies to make calls to your Amazon Lex bot. When you associate an Amazon Lex bot with your Amazon Connect instance, the resource-based policy on the bot is updated to give Amazon Connect permission to invoke the bot. For more information on Amazon Lex resource-based policies, see How Amazon Lex works with IAM.

Amazon Lex (Classic)

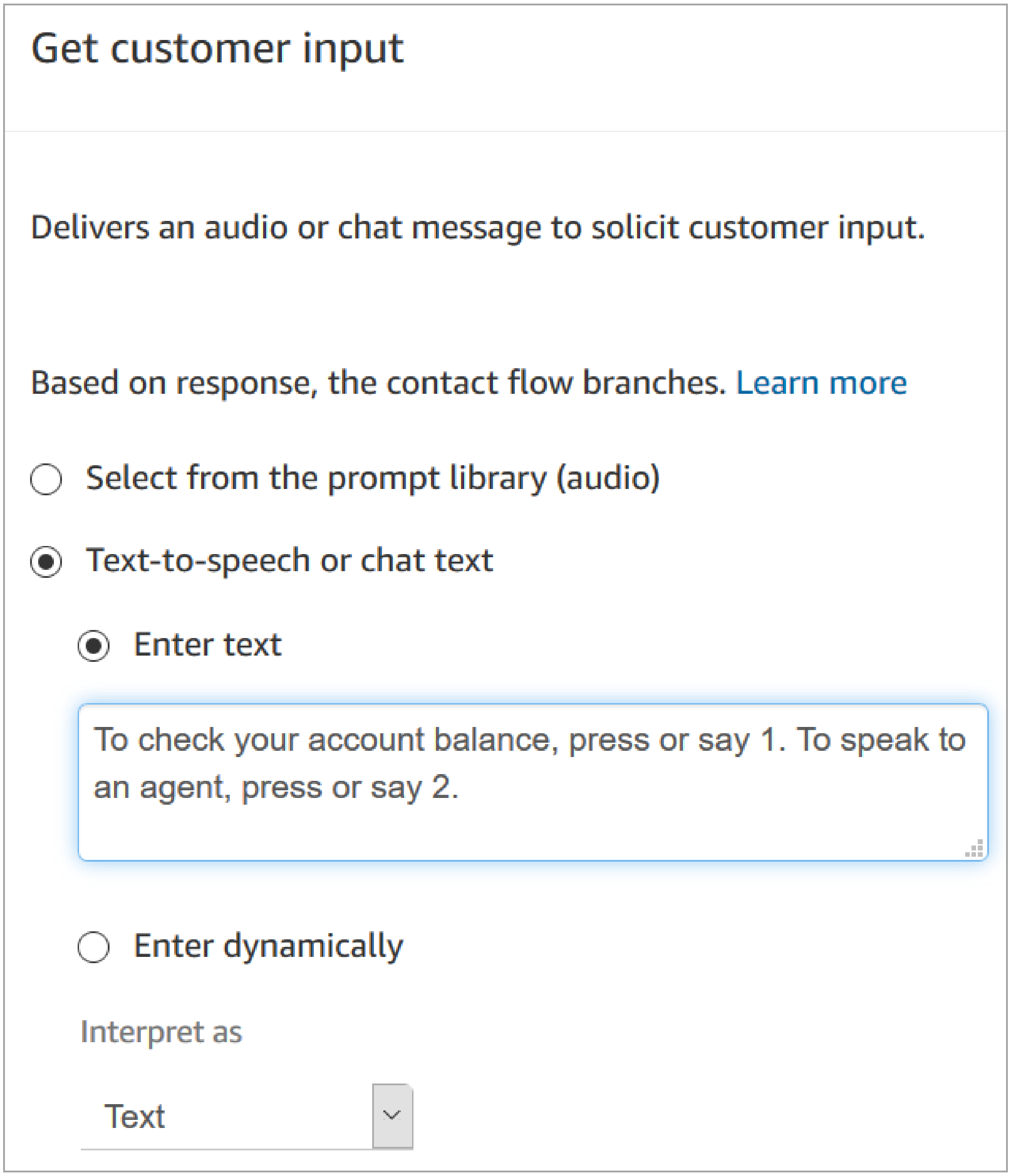
1. Open the Amazon Connect console.
2. Select the Amazon Connect instance that you want to integrate with your Amazon Lex bot.
3. On the navigation menu, choose **Contact flows**.
4. Under **Amazon Lex**, select the Region of your Amazon Lex classic bot from the dropdown, and then select your Amazon Lex classic bot. It’s name will have the suffix “(Classic)”. Then choose **Add Lex Bot**.

Create a contact flow and add your Amazon Lex bot

Important
If you're using an Amazon Lex V2 bot, your language attribute in Amazon Connect must match the language model used to build your Lex bot. This is different than Amazon Lex (Classic). Use a Set voice (p. 416) block to indicate the Amazon Connect language model, or use a Set contact attributes (p. 399) block.

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. On the navigation menu, choose **Routing, Contact flows, Create contact flow**, and type a name for the flow.
3. Under **Interact**, drag a Get customer input (p. 366) 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 or chat text, Enter text**.
5. Type a message that provides callers with information about what they can do. For example, use a message that matches the intents used in the bot, such as “To check your account balance, press or say 1. To speak to an agent, press or say 2.”



Get customer input

Delivers an audio or chat message to solicit customer input.

Based on response, the contact flow branches. Learn more

○ Select from the prompt library (audio)

● Text-to-speech or chat text

● Enter text

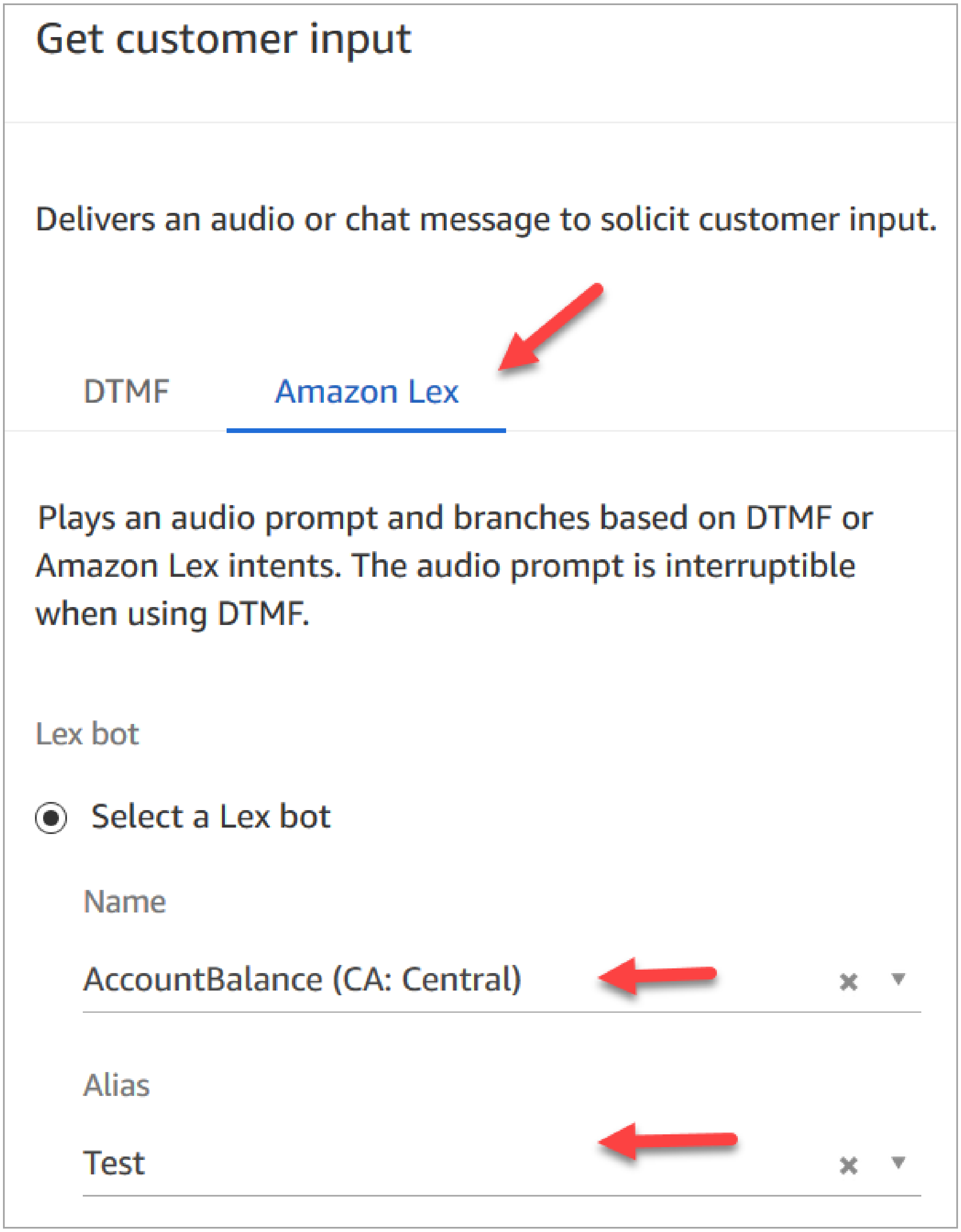
To check your account balance, press or say 1. To speak to an agent, press or say 2.

○ Enter dynamically

Interpret as

Text

6. Select the **Amazon Lex** tab.



Get customer input

Delivers an audio or chat message to solicit customer input.

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

Lex bot

● Select a Lex bot

Name

AccountBalance (CA: Central)

Alias

Test

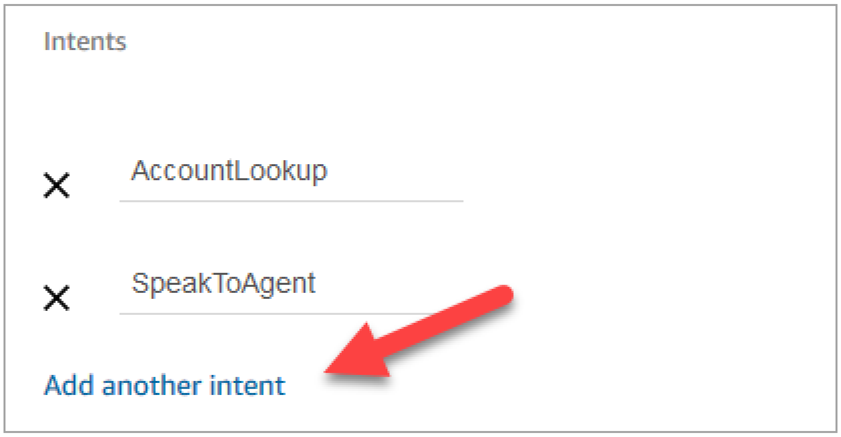
7. In the **Name** dropdown, select the **AccountBalance** bot you created earlier.

   a. If you selected an Amazon Lex bot, under **Alias** use the dropdown menu to select the bot alias, **Test**. from

   b. Amazon Lex Classic bots have the suffix "(Classic)" appended to their names. If you have selected a Classic bot, enter the alias you want to use in the **Alias** field.

   c. For Amazon Lex bots, you also have the option of manually setting a bot alias ARN. Choose **Set manually**, then either type the ARN of the bot alias you want to use or set the ARN using a dynamic attribute.

8. Under **Intents**, choose **Add an intent**.
9. Type **AccountLookup** and choose **Add another intent**.



Intents

10. Type **SpeakToAgent** and choose **Save**.

Finish the contact flow

In this step you finish adding parts to the contact flow that run after the caller interacts with the bot:

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

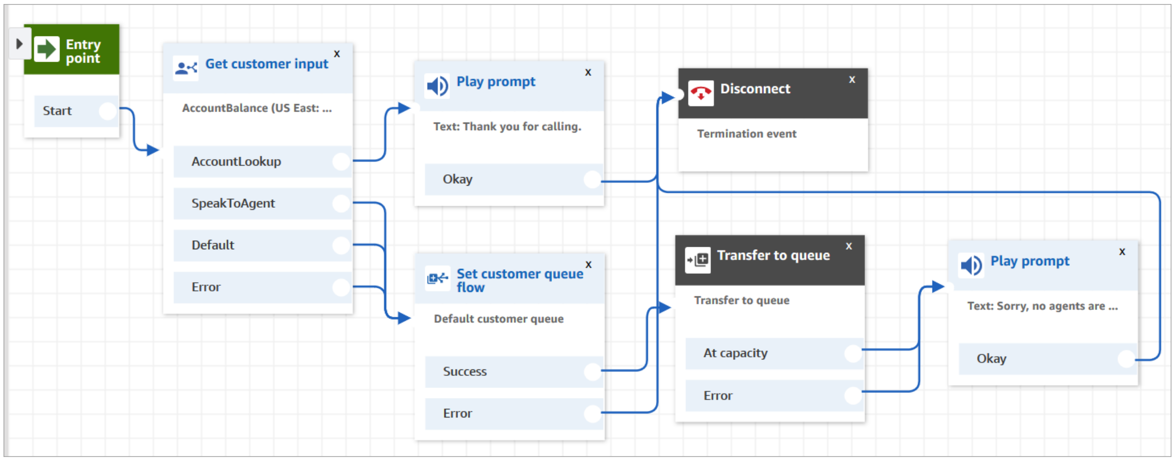
Here are the steps to create the contact flow:

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

To complete the **SpeakToAgent** intent:

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

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



Tip
If your business uses multiple locales in a single bot, add a Set contact attributes (p. 399) block to the beginning of your flow. Configure this block to use the $.LanguageCode (p. 517) system attribute.

Assign the contact flow to a phone number

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

1. Open the Amazon Connect console.
2. Choose **Routing, Phone numbers**.
3. On the **Manage Phone numbers** page, select the phone number to assign to the 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.

Add interactive messages to chat

Interactive messages are rich messages that present a prompt and pre-configured display options that a customer can select from. These messages are powered by Amazon Lex and configured through Amazon Lex using a Lambda.

Tip
For step-by-step instructions on how to add interactive messages through Amazon Lex and Lambda, see this blog: Set up interactive messages for your Amazon Connect chatbot.

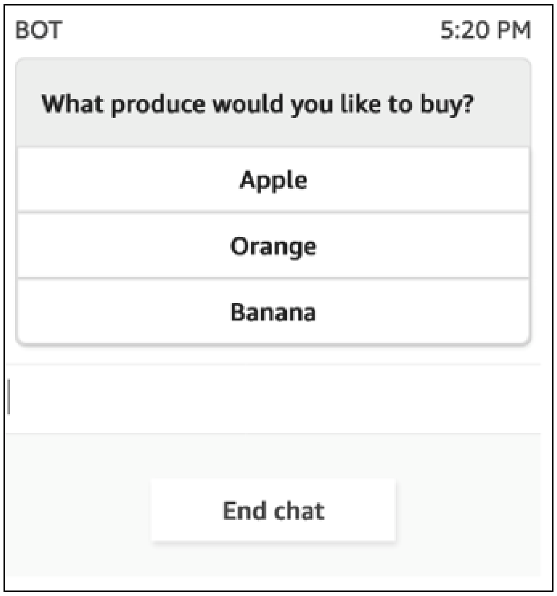
Amazon Connect provides two message display templates: a list picker and a time picker. These templates define how the information is going to render, and what information is surfaced in the chat interface. When interactive messages are sent through chat, contact flows validate that the message format follows one of these templates.

This topic provides details about these interactive message templates.

List picker template

Following are examples of how the list picker template renders information in a chat.

List picker



BOT 5:20 PM

What produce would you like to buy?

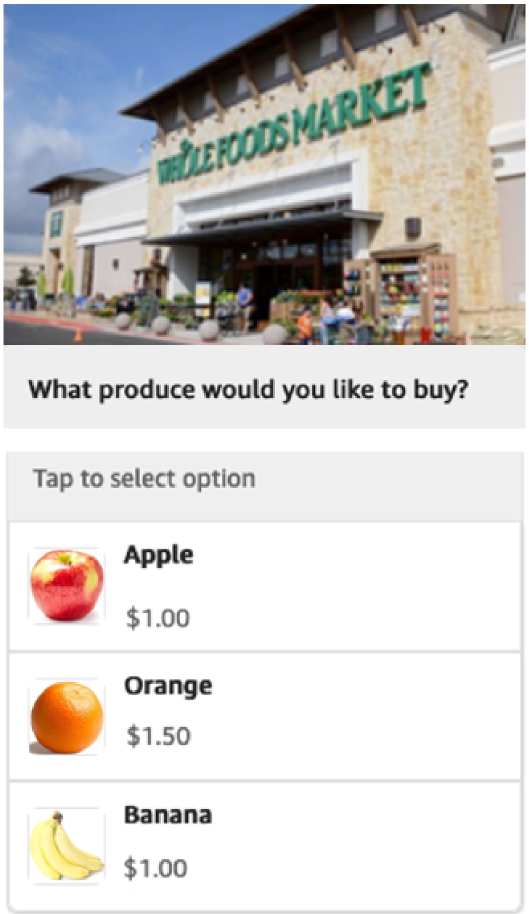
Apple

Orange

Banana

End chat

List picker with images



What produce would you like to buy?

Tap to select option

Apple $1.00

Orange $1.50

Banana $1.00

The following code is the list picker template that you can use in your Lambda. Note the following:

- **Bold text** is a mandatory parameter.
- In some cases, if the parent element exists in the request and it isn't mandatory/bold, but the fields in it are, then the fields are mandatory. For example, see `data.replyMessage` structure in the following template. If the structure exists, title is mandatory. Otherwise complete `replyMessage` is optional.

> **Important**
> Images should be uploaded in Amazon S3 and publicly accessible.

```
{
   "templateType":"ListPicker",                          (mandatory)
   "version":"1.0",                                      (mandatory)
   "data":{                                              (mandatory)
      "replyMessage":{
         "title":"Thanks for selecting!",                (mandatory)
         "subtitle":"Produce selected",
         "imageType":"URL",
         "imageData":"https://interactive-msg.s3-us-west-2.amazonaws.com/fruit_34.3kb.jpg",

         "imageDescription":"Select a produce to buy"
      },
      "content":{                                        (mandatory)
         *"title":"What produce would you like to buy?", (mandatory)
         "subtitle":"Tap to select option",
         "imageType":"URL",
         "imageData":"https://interactive-msg.s3-us-west-2.amazonaws.com/fruit_34.3kb.jpg",

         "imageDescription":"Select a produce to buy",
         "elements":[                                   (mandatory, 1-6 items)
            {
               "title":"Apple",                          (mandatory)
               "subtitle":"$1.00"
               "imageType":"URL",
               "imageData":"https://interactive-message-testing.s3-us-west-2.amazonaws.com/
apple_4.2kb.jpg"
            },
            {
               "title":"Orange",                         (mandatory)
               "subtitle":"$1.50"
               "imageType":"URL",
               "imageData":"https://interactive-message-testing.s3-us-west-2.amazonaws.com/
orange_17.7kb.jpg",
            },
             {
               "title":"Banana",                         (mandatory)
               "subtitle":"$10.00"
               "imageType":"URL",
               "imageData":"https://interactive-message-testing.s3-us-west-2.amazonaws.com/
banana_7.9kb.jpg",
               "imageDescription":"Banana"
            }
         ]
      }
   }
}
```

List picker limits

The following table lists the limits for each of the list picker elements, should you choose to build your own Lambda from scratch. The mandatory parameters are in bold.

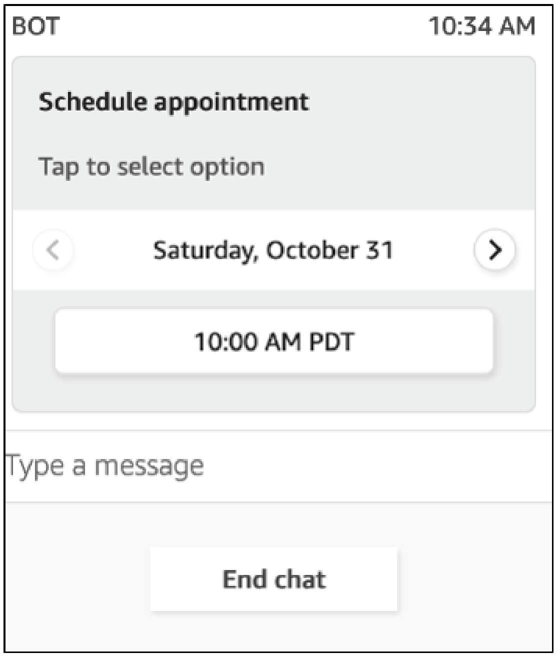
Parent field	Field	Required	Minimum characters	Maximum characters	Other requirement
	templateType	Yes			Valid template type
	data	Yes			
	version	Yes			Must be "1.0"
data	**content**	Yes			
	replyMessage	No			

Parent field	Field	Required	Minimum characters	Maximum characters	Other requirement
content	title	Yes	1	100	Should be a description for promptless templates
	elements	Yes	1 item	6 items	This is an array of elements. Maximum 6 elements in the array.
	subtitle	No	0	200	
	imageType	No	0	50	Must be "URL"
	imageData	No	0	200	Must be a valid public Amazon S3 URL
	imageDescription	No	0	50	
elements	**title**	Yes	1	100	
	subtitle	No	0	200	
	imageType	No	0	50	Must be "URL"
	imageData	No	0	200	Must be a valid public Amazon S3 URL
	imageDescription	No	0	50	Cannot exist without an image
replyMessage	**title**	Yes	1	100	
	subtitle	No	0	200	
	imageType	No	0	50	Must be "URL"
	imageData	No	0	200	Must be a valid public Amazon S3 URL
	imageDescription	No	0	50	Cannot exist without an image

Time picker template

Following are two examples of how the time picker template renders information in a chat.

Time picker with 1 timeslot



BOT 10:34 AM

Schedule appointment

Tap to select option

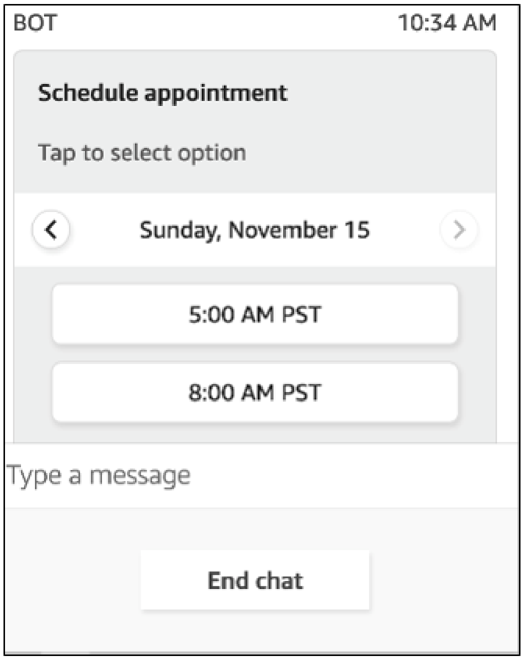
Saturday, October 31

10:00 AM PDT

Type a message

End chat

Time picker with 2 time slots



BOT 10:34 AM

Schedule appointment

Tap to select option

Sunday, November 15

5:00 AM PST

8:00 AM PST

Type a message

End chat

The following code is the time picker template that you can use in your Lambda. Note the following:

- **Bold text** is a mandatory parameter.
- In some cases, if the parent element exists in the request and it isn't mandatory/bold, but the fields in it are, then the fields are mandatory. For example, see `data.replyMessage` structure in the following template. If the structure exists, title is mandatory. Otherwise complete `replyMessage` is optional.

```
{
   "templateType":"TimePicker",                                    (mandatory)
   "version":"1.0",                                                (mandatory)
   "data":{                                                        (mandatory)
      "replyMessage":{
         "title":"Thanks for selecting",                           (mandatory)
         "subtitle":"Appointment selected",
      },
      "content":{                                                  (mandatory)
         "title":"Schedule appointment",                           (mandatory)
         "subtitle":"Tap to select option",
         "timeZoneOffset":-450
         "location":{
            "latitude":47.616299,                                  (mandatory)
            "longitude":-122.4311,                                 (mandatory)
            "title":"Oscar"                                        (mandatory)
            "radius":1,
         },
         "timeslots":[                                             (mandatory, 1-20 items)
               {
                  "date" : "2020-10-31T17:00+00:00"                (mandatory)
                  "duration": 60,                                  (mandatory)
               },
               {
                  "date" : "2020-11-15T13:00+00:00"              (mandatory)
                  "duration": 60,                                (mandatory)
               },
               {
                  "date" : "2020-11-15T16:00+00:00"            (mandatory)
                  "duration": 60,                              (mandatory)
               }
            ],
         }
      }
   }
}
```

Time picker limits

The following table lists the limits for each of the time picker elements. Use this information if you choose to build your own Lambda from scratch. The mandatory parameters are in bold.

Parent field	Field	Required	Minimum characters	Maximum characters	Other requirement
	templateType	Yes			Valid template type
	data	Yes			
	version	Yes			Must be "1.0"
data	replyMessage	No			
	content	Yes			
replyMessage	**title**	Yes	1	100	
	subtitle	No	0	200	
	title	Yes	1	100	Should be description for promptless templates
	subtitle	No	0	200	
content	**title**	Yes	1	100	Should be description for promptless templates
	subtitle	No	0	200	
	timezone offset	No	-720	840	This is an optional field when not set. Our sample client defaults to the user's timezone. If set, this displays per the timezone

Parent field	Field	Required	Minimum characters	Maximum characters	Other requirement
					entered. The field should be an integer representing the number of minutes from GMT, specifying the timezone of the event's location.
	location	No			
	timeslots	Yes	1	20	This is an array of timeslots. Maximum of 20 elements in the array.
location	**longitude**	Yes	-180	180	Must be double
	latitude	Yes	-90	90	Must be double
	title	Yes	1	100	
	radius	No	0	200	
timeslots	**date**	Yes			Should be in ISO-8601 time format: YYYY-MM-DDTHH.MM +00.00 For example: "2020-08-14T21:21+00.00"
	duration	Yes	1	3600	

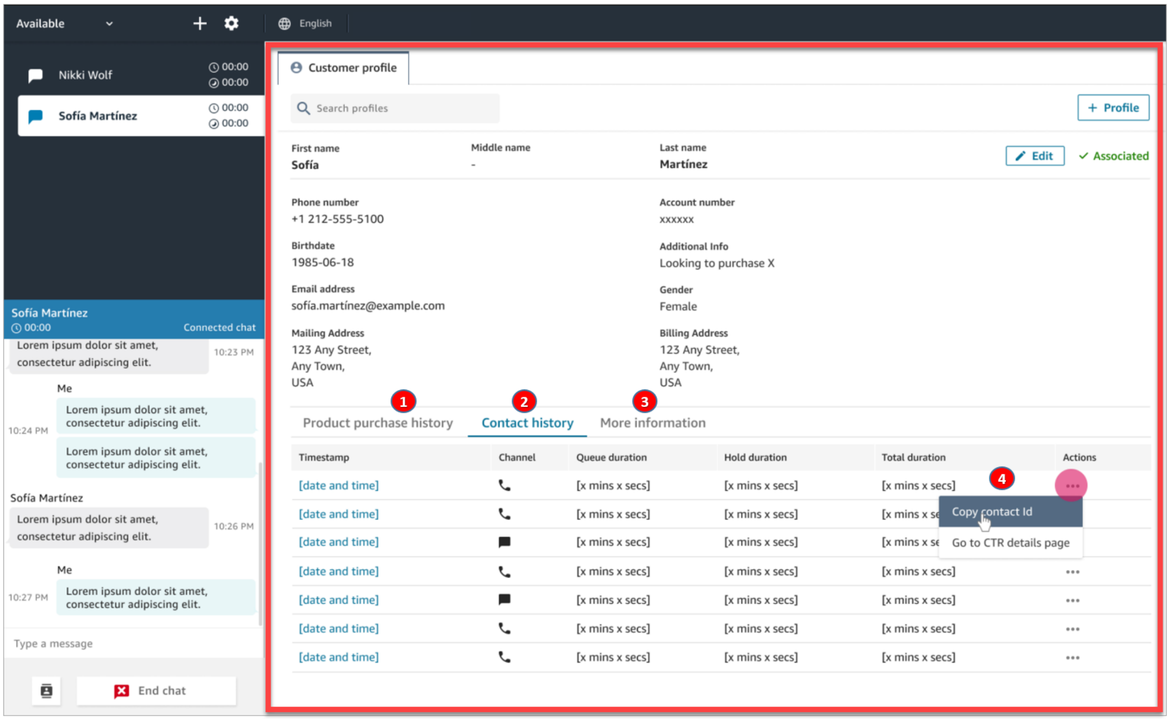
Use Customer Profiles

To help agents deliver more efficient and personalized customer service, Amazon Connect enables you to combine information from external applications, such as Salesforce, with contact history from Amazon Connect. This creates a customer profile that has all the information agents need during customer interactions in a single place.

With a single view of customer information and contact history, agents can quickly confirm the customer's identity and determine the reason for the call or chat.

Currently, Amazon Connect Customer Profiles can be used in compliance with GDPR and is pending additional certifications held by Amazon Connect.

The following image shows an agent's Contact Control Panel (CCP); for the purposes of this documentation, Amazon Connect Customer Profiles highlighted in the red box. The agent's application is optimized for multi-tasking: working on calls, and multiple chats and tasks, with customer profile information in the same browser window.



Sofía Martínez
00:00 Connected chat

Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:23 PM

Me
10:24 PM Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Sofía Martínez
Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:26 PM

Me
10:27 PM Lorem ipsum dolor sit amet, consectetur adipiscing elit.

First name
Sofía

Middle name
-

Last name
Martínez

Phone number
+1 212-555-5100

Account number
xxxxxx

Birthdate
1985-06-18

Additional Info
Looking to purchase X

Email address
sofía.martínez@example.com

Gender
Female

Mailing Address
123 Any Street,
Any Town,
USA

Billing Address
123 Any Street,
Any Town,
USA

Timestamp	Channel	Queue duration	Hold duration	Total duration	Actions
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x se	Copy contact Id
[date and time]	💬	[x mins x secs]	[x mins x secs]	[x mins x se	Go to CTR details page
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	💬	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••

1. **Product purchase history**: All the assets purchased by a customer can be populated here. The data is ingested from an external app such as Salesforce or Zendesk that you've integrated (p. 661) with Customer Profiles.
2. **Contact history**: Date, times, and duration when this customer contacted your contact center in the past.
3. **More information**: Information that an agent can use to verify the contact, such as cell phone number and shipping address.
4. **Actions**: Agents can copy the contact ID, or choose to go directly to the contact's **Contact record details** page.

What is a customer profile?

A customer profile stores contact history combined with information about customers, such as account number, additional information, birth date, email, multiple addresses, name, and party type.

After you enable Amazon Connect Customer Profiles, a unique customer profile is created for every contact. This allows you to create a customer profile that has all the information agents need during customer interactions in a single place at no charge.

To access customer profiles in your flows, use the Customer profiles (p. 359) block. Agents access customer profiles (p. 657) in their agent application.

You can use the paid features of Customer Profiles to enrich your customer profiles by ingesting data from external applications (p. 661). See pricing for details.

You can also add custom fields and objects to the customer profiles by using the Amazon Connect Customer Profiles APIs.

How is customer profile data stored?

Amazon Connect stores contact history in unique customer profiles. It parses data ingested from external applications and stores it as customer profile attributes.

Amazon Connect does not replace or update the data in the external application. If a data source is removed, the data from the external application is no longer available in the customer profile.

For information about how customer profile data are secured, see Data protection in Amazon Connect (p. 1063).

For more information about how to access the data that is stored in a customer profile, see Access Customer Profiles in the agent application or Use the Customer Profiles API.

Enable Customer Profiles for your instance

Amazon Connect provides pre-built integrations so you can quickly combine customer information from multiple external applications, with contact history from Amazon Connect. This allows you to create a customer profile that has all the information agents need during customer interactions in a single place.

Before you begin

Following is an overview of key concepts and the information that you'll be prompted for during the setup process.

About the customer profiles domain

When you enable Amazon Connect Customer Profiles, you create a customer profiles domain: a container for all data, such as customer profiles, object types, profile keys, and encryption keys. Following are guidelines for creating Customer Profile domains:

- Each Amazon Connect instance can only be associated with one domain.
- You can create multiple domains, but they don't share external application integrations or customer data between each other.

- All the external application integrations you create are at a domain level. All of the Amazon Connect instances associated with a domain inherit the domain's integrations.
- You can change the association of your Amazon Connect instance from your current domain to a new domain at any time, by choosing a different domain. This isn't recommended, however, because the customer profiles from the earlier domain won't be moved to the new domain.

How do you want to name your customer profiles domain?

When you enable customer profiles, you are prompted to provide a friendly domain name that's meaningful to you such as your organization name, for example, *CustomerProfiles-ExampleCorp*. You can change the friendly name using the API at any time.

Do you want to use a dead-letter queue?

A dead-letter queue is used for reporting errors associated with processing data from external applications.

Amazon AppFlow handles connecting to the external application and moving data from it to Amazon Connect Customer Profiles. Amazon Connect then processes the file.

- If an error occurs during the connection or while transporting the data to Amazon Connect, Amazon AppFlow surfaces the error but it doesn't write the error to the dead-letter queue.

  For example, a processing error could be that the external data didn’t match the specified schema or that the format of the external data format isn't correct (currently only JSON is supported).
- If Amazon Connect encounters an error while processing the file, it writes the error to your dead-letter queue. You can look at the queue later and try to reprocess the error.

When you enable Customer Profiles, you have the option of specifying an Amazon SQS queue as your dead-letter queue. If you select this option, add the following resource policy to Amazon SQS so Customer Profiles has permissions to send messages to that queue:

```
{
      "Sid": "Customer Profiles SQS policy",
      "Effect": "Allow",
      "Principal": {
        "Service": "profile.amazonaws.com"
      },
      "Action": "SQS:SendMessage",
      "Resource": "arn:aws:sqs:region:accountID:YourQueueName"
}
```

To prevent a confused deputy security issue, see Amazon Connect Customer Profiles cross-service confused deputy prevention (p. 1130) for an example policy to apply.

Step-by-step instructions are provided in Enable Customer Profiles (p. 643). For general information, see Basic examples of Amazon SQS policies.

Create a KMS key to be used by Customer Profiles to encrypt data (required)

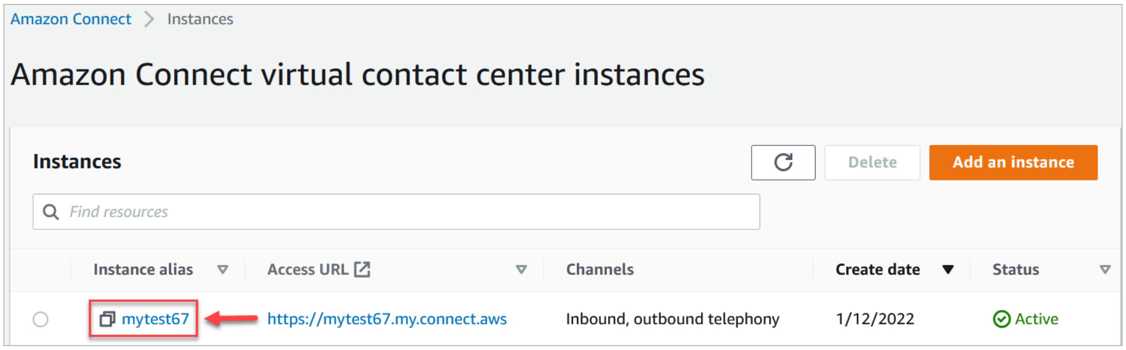
When you enable Customer Profiles, you are prompted to create or provide a AWS Key Management Service KMS key. Step-by-step instructions for creating a KMS key are provided in Enable Customer Profiles (p. 643).

All data at rest for Customer Profiles is encrypted under the KMS key you choose. Your customer managed key is created, owned, and managed by you. You have full control over the KMS key (AWS KMS charges apply).

If you choose to set up a KMS key where someone else is the administrator, it must have a policy that allows `kms:GenerateDataKey`, `kms:CreateGrant`, and `kms:Decrypt` permissions to the Customer Profiles service principal. For information about how to change a key policy, see Changing a key policy in the AWS Key Management Service Developer Guide. In addition, to prevent cross-service impersonation, see Cross-service confused deputy prevention (p. 1129) for sample policies that you should apply.

Enable Customer Profiles

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



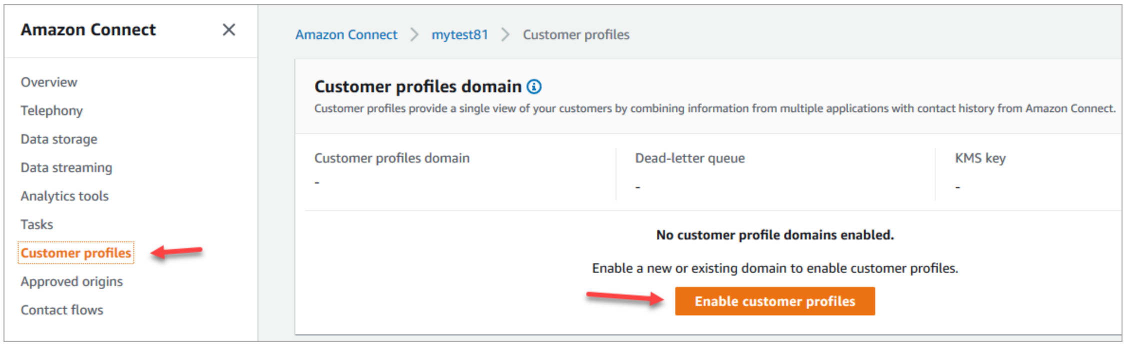
Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Customer profiles**.

   The **Customer profiles domain** page lists the applications that are available for integration.



Customer profiles domain

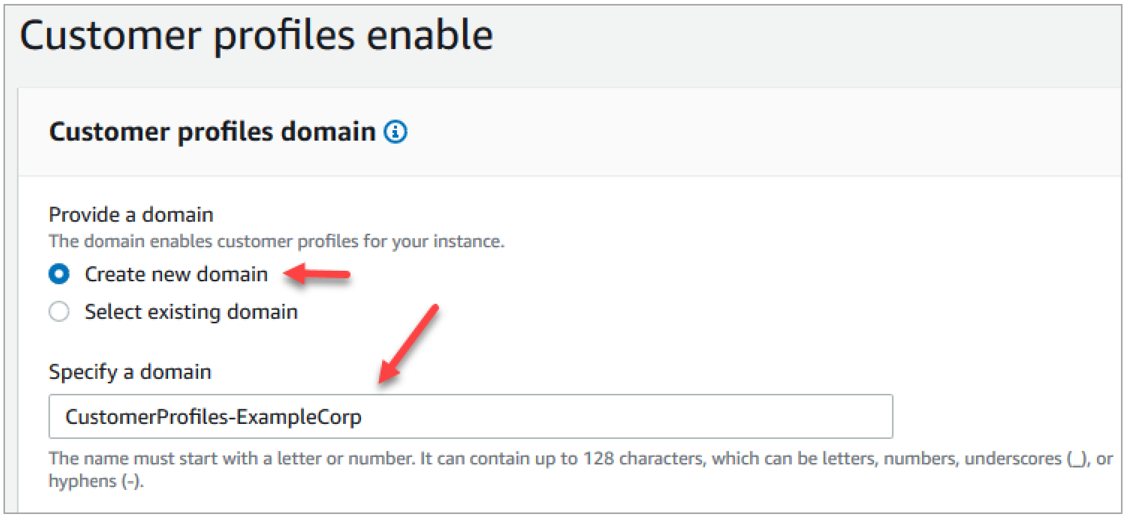
Customer profiles provide a single view of your customers by combining information from multiple applications with contact history from Amazon Connect.

Customer profiles domain	Dead-letter queue	KMS key
-	-	-

No customer profile domains enabled.

Enable a new or existing domain to enable customer profiles.

4. Choose **Enable customer profiles** to get started.
5. At the **Customer profiles enable** page, choose **Create new domain**. Under **Specify a domain**, enter a friendly name that's meaningful to you, such as your organization name, for example, *CustomerProfiles-ExampleCorp*.



Customer profiles enable

Customer profiles domain

Provide a domain
The domain enables customer profiles for your instance.

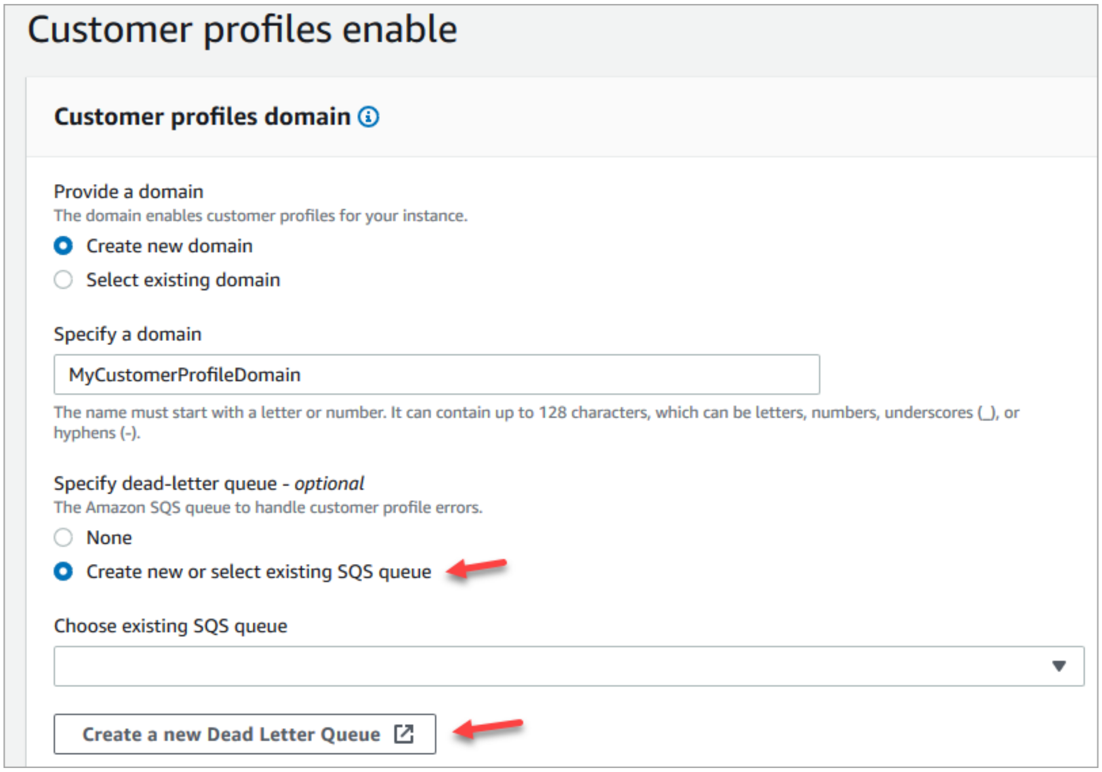
● Create new domain
○ Select existing domain

Specify a domain
CustomerProfiles-ExampleCorp
The name must start with a letter or number. It can contain up to 128 characters, which can be letters, numbers, underscores (_), or hyphens (-).

6. Under **Specify dead-letter queue**, choose whether to send failed events to a dead-letter queue. This is helpful if you want to get visibility into data that failed to be ingested. It also gives you the option to retry these failed data ingestions in the future.

   Following are the steps to create a dead-letter queue:

   - On the **Customer profiles enable** page, choose **Create new or select existing SQS queue** and then choose **Create a new Dead Letter Queue**.



Customer profiles enable

Customer profiles domain

Provide a domain
The domain enables customer profiles for your instance.

● Create new domain
○ Select existing domain

Specify a domain
MyCustomerProfileDomain
The name must start with a letter or number. It can contain up to 128 characters, which can be letters, numbers, underscores (_), or hyphens (-).

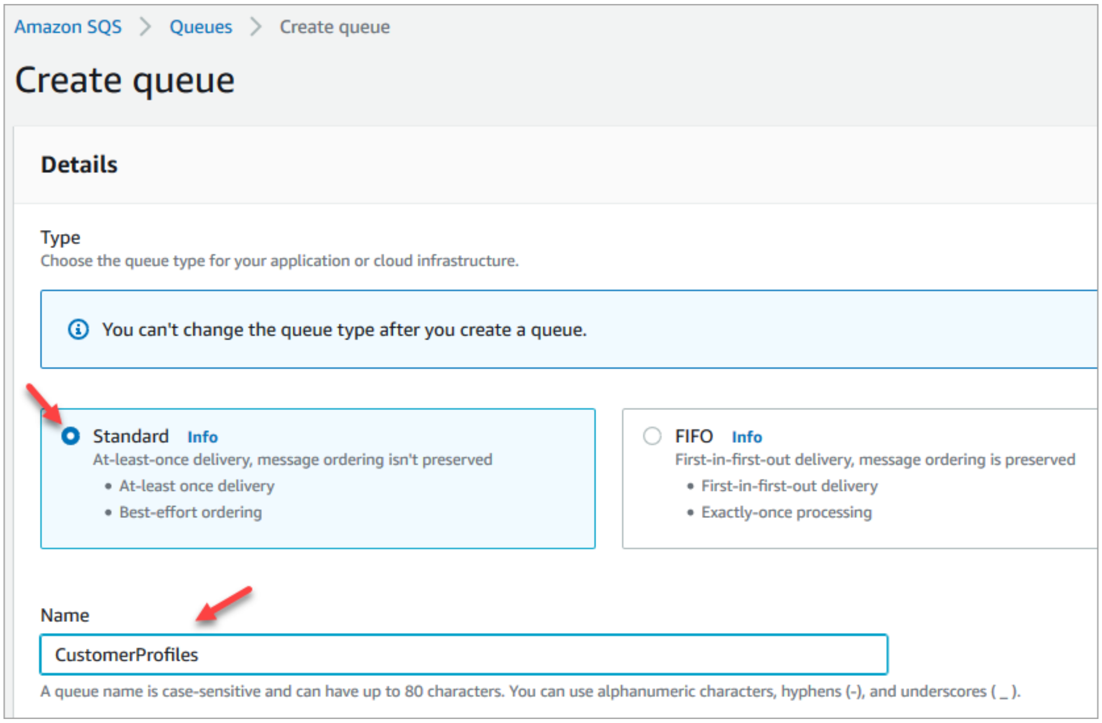
Specify dead-letter queue - *optional*
The Amazon SQS queue to handle customer profile errors.

○ None
● Create new or select existing SQS queue

Choose existing SQS queue

Create a new Dead Letter Queue

   - A new tab in your browser opens for the Amazon SQS console. Choose **Create queue**.
   - On the **Create queue** page, choose **Standard**, then assign a name to your queue.



Amazon SQS > Queues > Create queue

Create queue

Details

Type
Choose the queue type for your application or cloud infrastructure.

You can't change the queue type after you create a queue.

● Standard Info
At-least-once delivery, message ordering isn't preserved
- At-least once delivery
- Best-effort ordering

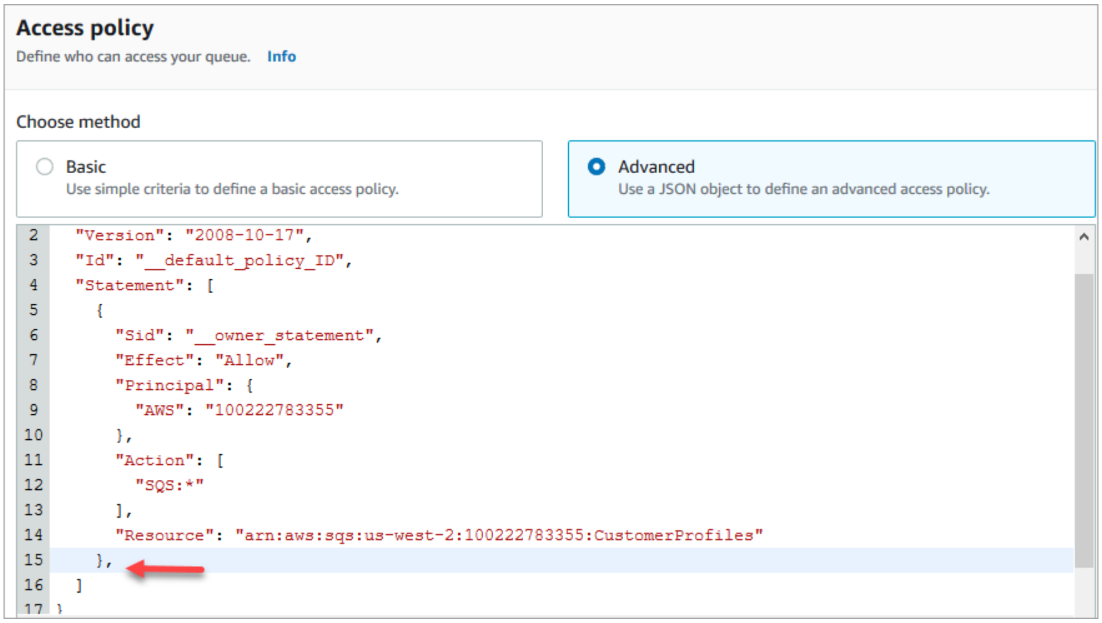
○ FIFO Info
First-in-first-out delivery, message ordering is preserved
- First-in-first-out delivery
- Exactly-once processing

Name
CustomerProfiles
A queue name is case-sensitive and can have up to 80 characters. You can use alphanumeric characters, hyphens (-), and underscores (_).

- In the **Access policy** section, choose **Advanced**.

  The Version name, policy ID, and Statement appear. If needed, update this section to give access to only the appropriate roles.

- At the end of the Statement section (line 15 in the following image) add a comma after }, and press `Enter`.



Access policy
Define who can access your queue. Info

Choose method

○ Basic
Use simple criteria to define a basic access policy.

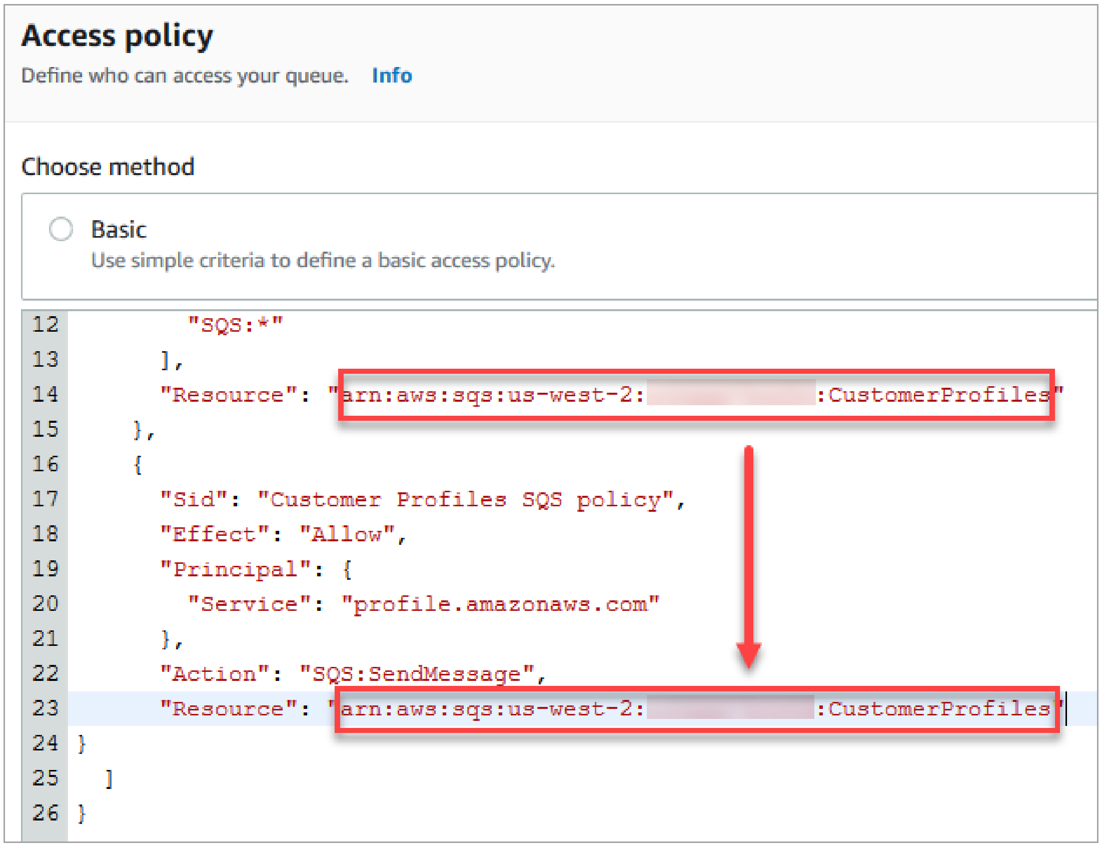
● Advanced
Use a JSON object to define an advanced access policy.

```
2    "Version": "2008-10-17",
3    "Id": "__default_policy_ID",
4    "Statement": [
5      {
6        "Sid": "__owner_statement",
7        "Effect": "Allow",
8        "Principal": {
9          "AWS": "100222783355"
10       },
11       "Action": [
12         "SQS:*"
13       ],
14       "Resource": "arn:aws:sqs:us-west-2:100222783355:CustomerProfiles"
15     },
16   ]
17 }
```

- Then copy and paste the following code:

```
{
       "Sid": "Customer Profiles SQS policy",
       "Effect": "Allow",
       "Principal": {
         "Service": "profile.amazonaws.com"
       },
       "Action": "SQS:SendMessage",
       "Resource": "arn:aws:sqs:region:accountID:YourQueueName"
}
```

- To replace *region*, *accountID*, and *YourQueueName* with your information, copy and paste the `Resource` information from line 14.



Access policy

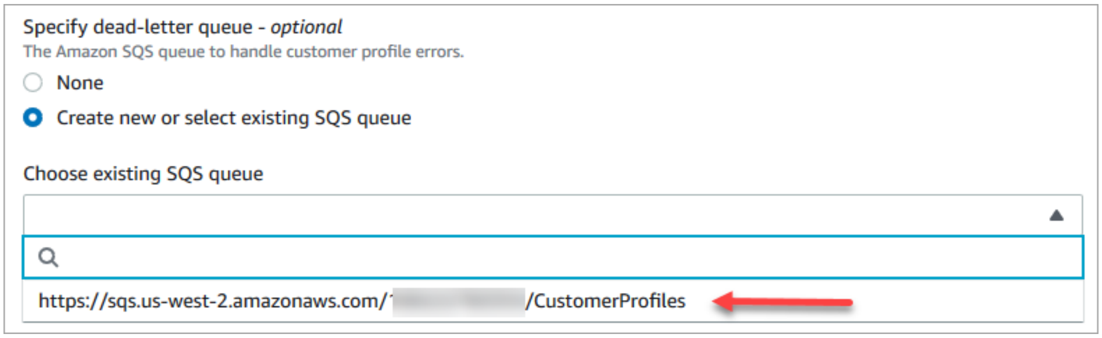
Define who can access your queue. **Info**

Choose method

○ Basic
Use simple criteria to define a basic access policy.

```
12            "SQS:*"
13          ],
14          "Resource": "arn:aws:sqs:us-west-2:[redacted]:CustomerProfiles"
15        },
16        {
17          "Sid": "Customer Profiles SQS policy",
18          "Effect": "Allow",
19          "Principal": {
20            "Service": "profile.amazonaws.com"
21          },
22          "Action": "SQS:SendMessage",
23          "Resource": "arn:aws:sqs:us-west-2:[redacted]:CustomerProfiles"
24    }
25      ]
26    }
```

- Choose **Create queue**.
- Return to the tab in your browser for the Amazon Connect console, **Customer profiles enable** page. Click or tap in the **Choose existing SQS queue** box to select the queue you just created from the dropdown list.



Specify dead-letter queue - *optional*
The Amazon SQS queue to handle customer profile errors.

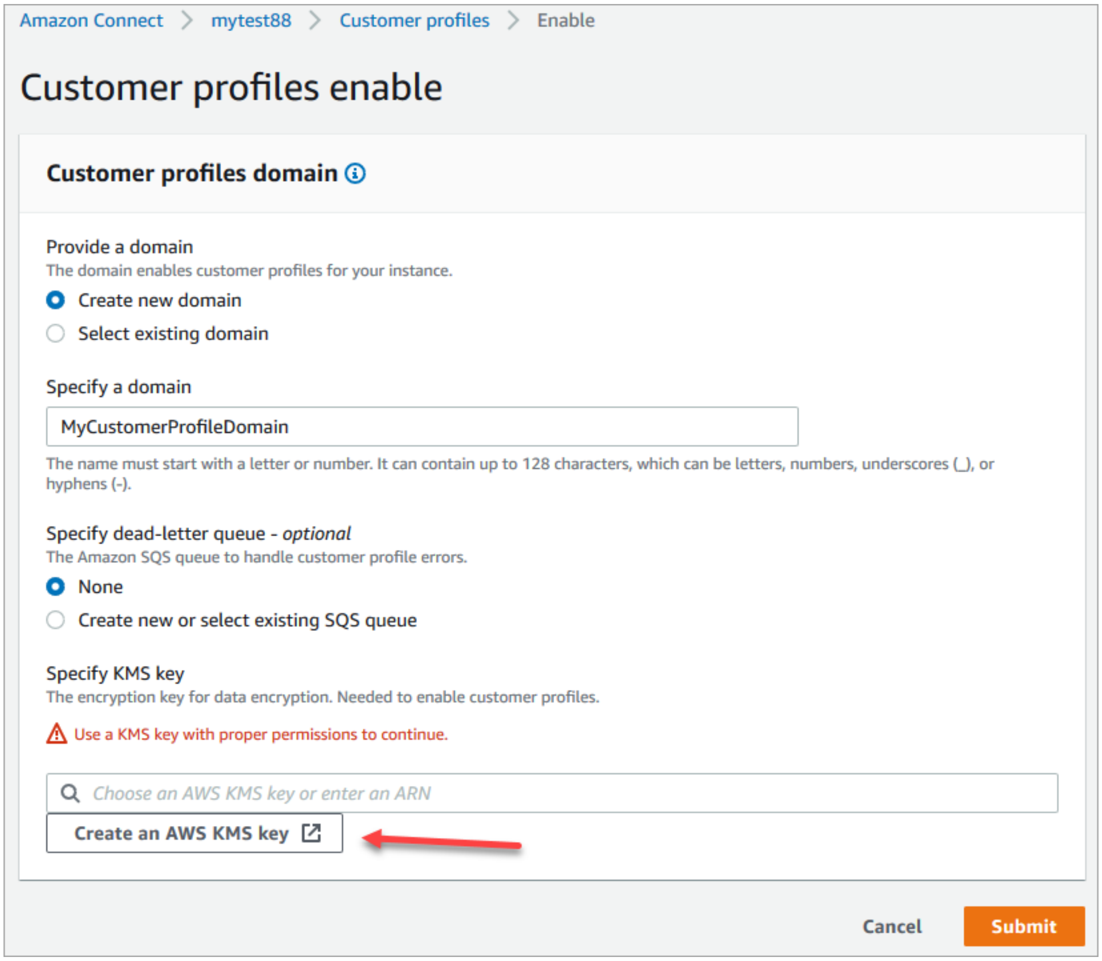
○ None
● Create new or select existing SQS queue

Choose existing SQS queue

https://sqs.us-west-2.amazonaws.com/[redacted]/CustomerProfiles

7. Under **Specify KMS key**, create or enter your own AWS KMS key for encryption. Following are the steps to create your AWS KMS key:

- On the **Customer profiles enable** page, choose **Create an AWS KMS key**.



Amazon Connect > mytest88 > Customer profiles > Enable

Customer profiles enable

Customer profiles domain

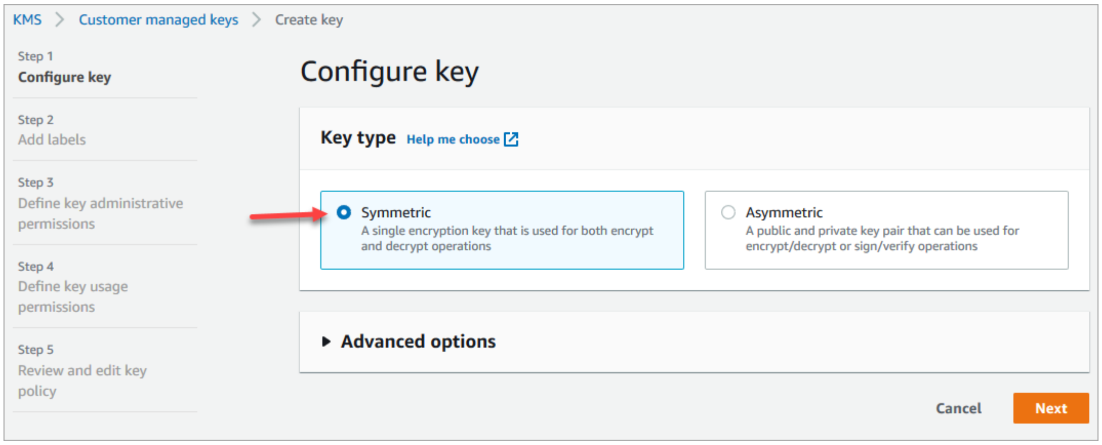
Provide a domain
The domain enables customer profiles for your instance.
● Create new domain
○ Select existing domain

Specify a domain
MyCustomerProfileDomain
The name must start with a letter or number. It can contain up to 128 characters, which can be letters, numbers, underscores (_), or hyphens (-).

Specify dead-letter queue - *optional*
The Amazon SQS queue to handle customer profile errors.
● None
○ Create new or select existing SQS queue

Specify KMS key
The encryption key for data encryption. Needed to enable customer profiles.
⚠ Use a KMS key with proper permissions to continue.

- A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review and edit key policy

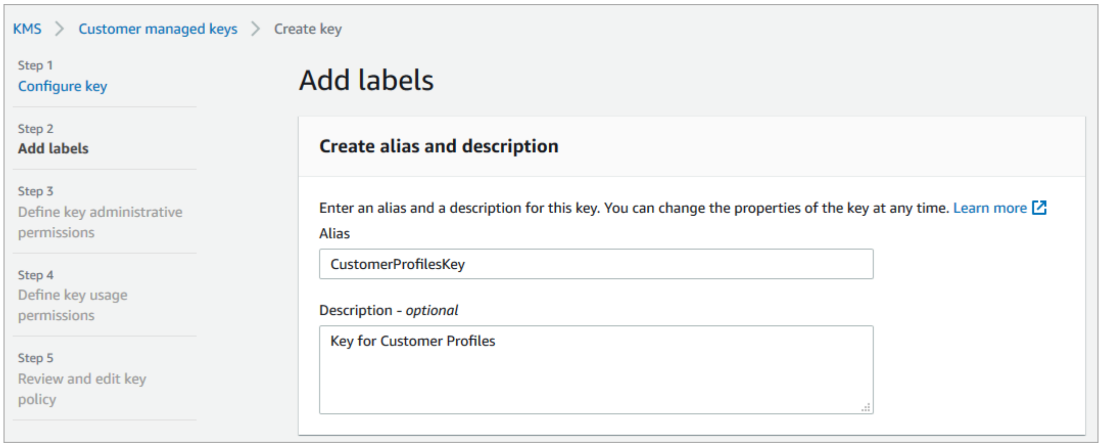
Configure key

Key type Help me choose

● Symmetric
A single encryption key that is used for both encrypt and decrypt operations

○ Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

- On the **Add labels** page, add a name and description for the key, and then choose **Next**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review and edit key policy

Add labels

Create alias and description

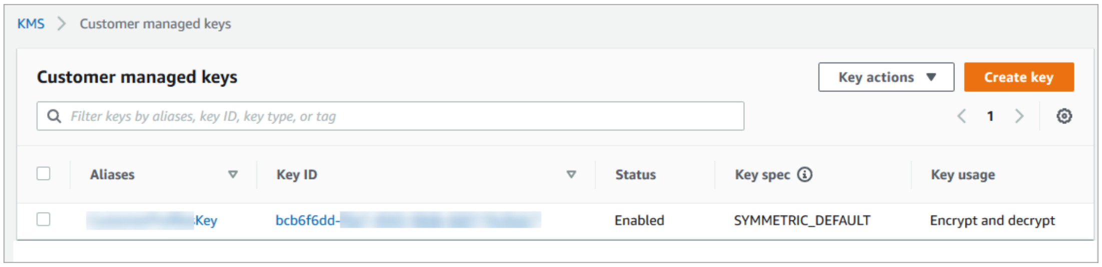
Enter an alias and a description for this key. You can change the properties of the key at any time. Learn more

Alias: CustomerProfilesKey

Description - *optional*: Key for Customer Profiles

- On the **Define key administrative permissions** page, choose **Next**.
- On the **Define key usage permissions** page, choose **Next**.
- On the **Review and edit key policy** page, choose **Finish**.

  In the following example, the name of the key starts with **bcb6fdd**:

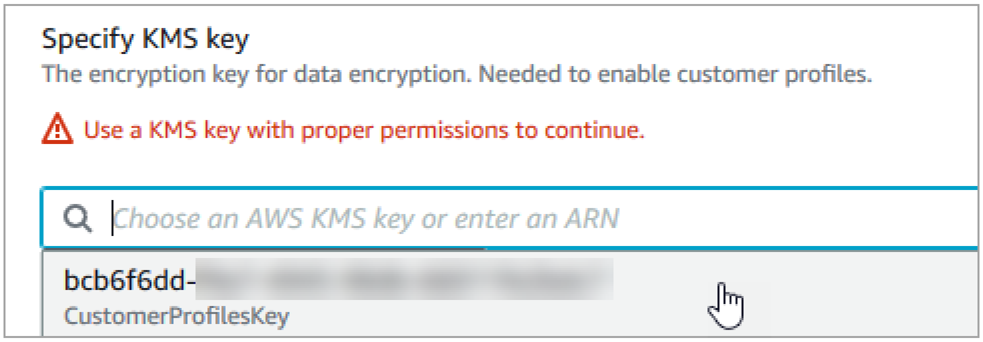


KMS > Customer managed keys

Customer managed keys

□	Aliases	Key ID	Status	Key spec	Key usage
□	[redacted]Key	bcb6f6dd-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

- Return to the tab in your browser for the Amazon Connect console, **Customer profiles enable** page. Click or tap in the **Specify KMS key box** for the key you created to appear in a dropdown list. Choose the key you created.



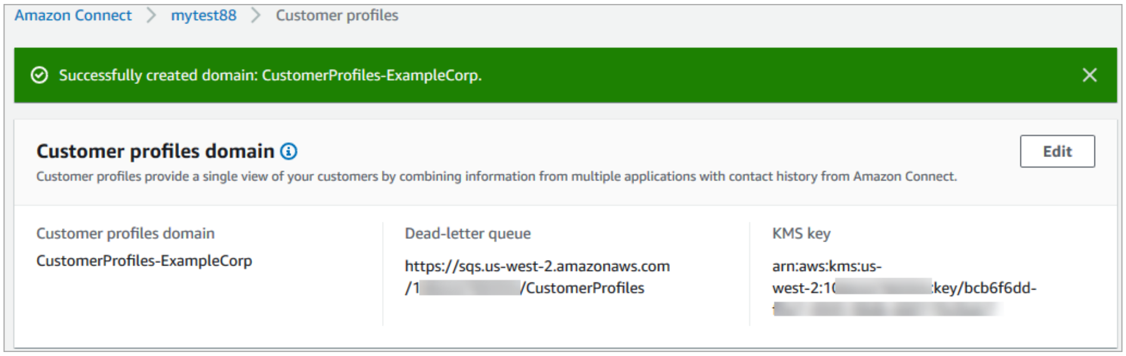
Specify KMS key

The encryption key for data encryption. Needed to enable customer profiles.

Use a KMS key with proper permissions to continue.

bcb6f6dd-[redacted]
CustomerProfilesKey

8. Choose **Submit**. The completed page looks similar to the following image.



Successfully created domain: CustomerProfiles-ExampleCorp.

Customer profiles domain

Customer profiles provide a single view of your customers by combining information from multiple applications with contact history from Amazon Connect.

Customer profiles domain	Dead-letter queue	KMS key
CustomerProfiles-ExampleCorp	https://sqs.us-west-2.amazonaws.com/1[redacted]/CustomerProfiles	arn:aws:kms:us-west-2:1[redacted]:key/bcb6f6dd-[redacted]

You're done! Amazon Connect Customer Profiles is enabled. Now with every new contact that comes in, Amazon Connect creates a customer profile record. It then tracks the contact history for that phone number (voice) or email address (chat).

Your agents can create new customer profiles (p. 1185) and view contact records for your customers.

Next steps

1. Make Customer Profiles available through the agent application (p. 657).
2. Assign agents permissions to access Customer Profiles in the agent application (p. 661).
3. Integrate with external applications that profile customer profile data (optional) (p. 661).
4. Enable Identity Resolution to identify two or more similar profiles, and consolidate them (p. 649).

Use Identity Resolution to consolidate similar profiles

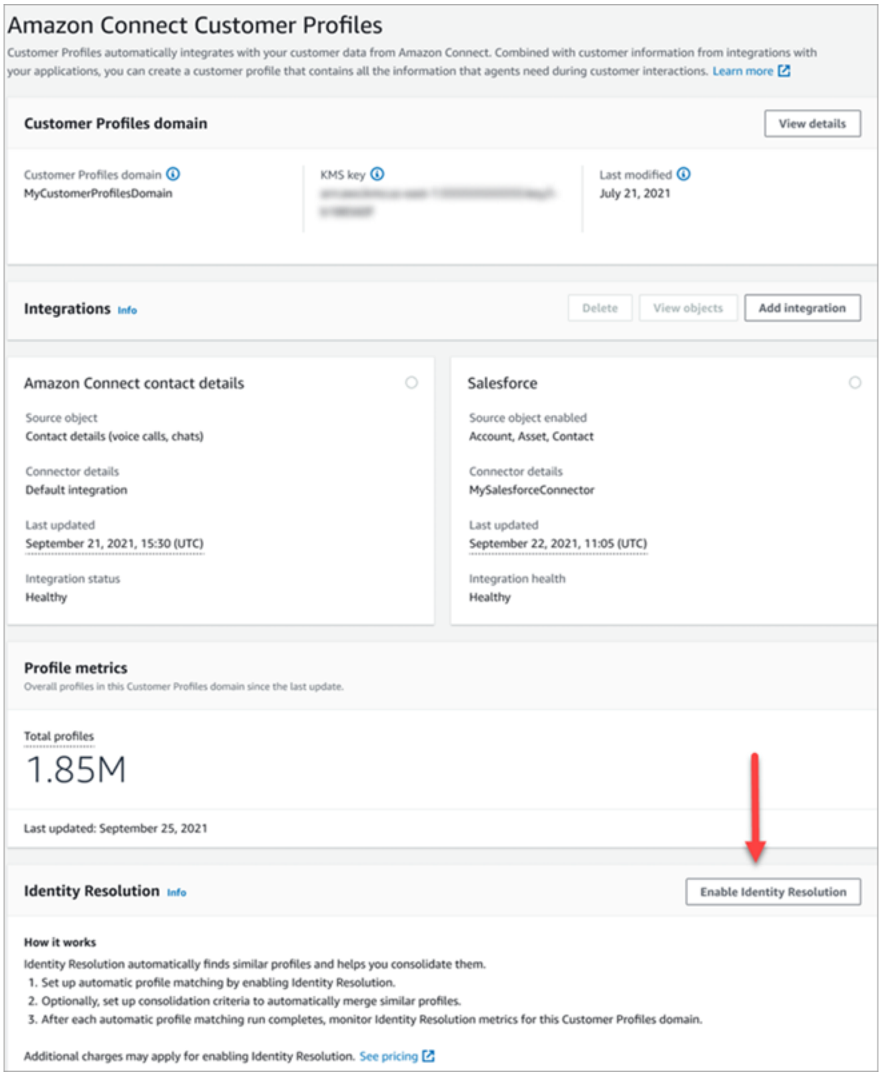
A *similar profile* is when two or more profiles are determined to be for the same contact. There can be multiple profiles when customer records are captured across multiple channels and applications for the same customer, and do not share a common unique identifier.

Identity Resolution automatically finds similar profiles and helps you consolidate them. It runs an Identity Resolution Job on a weekly basis, which performs the following steps:

1. Automatic profile matching (p. 650)
2. Automatic merging of similar profiles (p. 651) based on your consolidation criteria

Each time an Identity Resolution Job runs, it displays metrics on the **Customer Profiles** page. The metrics show the number of profiles it reviewed, the number of match groups found, and the number of profiles consolidated.

Additional charges may apply for enabling Identity Resolution. For more information, see Amazon Connect pricing.



Amazon Connect Customer Profiles

Customer Profiles automatically integrates with your customer data from Amazon Connect. Combined with customer information from integrations with your applications, you can create a customer profile that contains all the information that agents need during customer interactions. Learn more

Customer Profiles domain

Customer Profiles domain: MyCustomerProfilesDomain

KMS key: [redacted]

Last modified: July 21, 2021

Integrations Info

Amazon Connect contact details

Source object: Contact details (voice calls, chats)

Connector details: Default integration

Last updated: September 21, 2021, 15:30 (UTC)

Integration status: Healthy

Salesforce

Source object enabled: Account, Asset, Contact

Connector details: MySalesforceConnector

Last updated: September 22, 2021, 11:05 (UTC)

Integration health: Healthy

Profile metrics

Overall profiles in this Customer Profiles domain since the last update.

Total profiles: 1.85M

Last updated: September 25, 2021

Identity Resolution Info

How it works

Identity Resolution automatically finds similar profiles and helps you consolidate them.

1. Set up automatic profile matching by enabling Identity Resolution.
2. Optionally, set up consolidation criteria to automatically merge similar profiles.
3. After each automatic profile matching run completes, monitor Identity Resolution metrics for this Customer Profiles domain.

Additional charges may apply for enabling Identity Resolution. See pricing

How Identity Resolution works

This topic describes how Identity Resolution performs automatic profile matching, and if set up, how it automatically merges similar profiles.

Automatic profile matching

To identify similar profiles, Identity Resolution uses machine learning to review the following Personal Identifiable Information (PII) attributes in each profile:

- Name: All names are reviewed for similarity, including first name, middle name, and last name.
- Email: All email addresses are reviewed for similarity, including personal email and business email. They are not case sensitive.
- Phone number: All phone numbers and formats are reviewed for similarity, including home phone, mobile phone, and business phone.
- Address: All address types and format are reviewed for similarity, including business address, mailing address, shipping address, and billing address.
- Date of birth: All birth dates and formats are reviewed for similarity.

It uses this information to create match groups of similar profiles.

Match groups

A match group consists of all similar profiles which represents a customer. Each match group contains the following information:

- A match ID, which uniquely identifies the group of two or more similar profiles that represent a contact
- The number of profile IDs in the match group
- A confidence score associated with the match group

Confidence scores

After the auto-matching process runs, you can query the S3 bucket or use the GetMatches API to filter results based on confidence scores. For example, you can filter out high confidence matches for a further review.

A confidence score is a number between 0 and 1 that represents the confidence level of assigning profiles to a match group. A score of 1 likely indicates an exact match.

Automatic merging of similar profiles

After the profiles are matched, the Identity Resolution Job can optionally merge similar profiles based on your criteria. If you delete or update criteria, the updated criteria is applied to similar profiles in the next run.

> **Important**
> You cannot undo the consolidation process. We strongly recommend using the GetAutoMergingPreview API to do a dry run of the automatic merging process before running the Identity Resolution Job.

How the auto-merging process works

- **All selected attributes in a consolidation criteria are connected with `AND` criteria with exact value comparison before merging**.
  - For example, when multiple attributes are specified in the criteria, such as `email address` and `phone number`, then all similar profiles in a match group that have the exact same value of `email address` and `phone number` are merged.
  - If one or more of the similar profiles in a match group have a different value or missing value for one or more of the attributes in a criteria, the similar profiles are merged.

    For example, one match group may be five similar profiles out of which three profiles are consolidated, because these three profiles meet the criteria. The other two profiles are not merged, because they do not meet the criteria.
- **Multiple criteria are evaluated in the order of priority starting with Criteria 1**.
  - The sequence in which consolidation criteria are applied. It starts with Criteria 1 as the highest priority to Criteria 10 as the lowest priority.
  - After the Identity Resolution Job applies one criteria, it applies the next criteria to the consolidated profiles and the remaining similar profiles in a match group.
  - You can have a maximum of 10 consolidation criteria.
- **Each criteria runs independently and operates as an `OR` with other criteria**.
  - When you have multiple criteria, each criteria is applied individually and in the sequence of priority order before the Identity Resolution Job moves on to the next criteria.

  - All criteria is applied in the sequence in which you listed them. It doesn't matter whether the criteria fails or succeeds to consolidate similar profiles in a match group.
- **By default, profile conflicts are managed by recency**.
  - When two or more similar profiles in a match group meet a consolidation criteria, the resulting consolidated profile is created by comparing each value of the profile attributes constituent similar profiles.
  - Each attribute may have an exact match in value. In this case, any value may be selected for that attribute.
  - If there is a conflict between values of two or more constituent similar profiles, the most recently updated attribute is chosen.

    For example, if Jane Doe has three different values in the `Address` attribute of the constituent similar profiles, Identity Resolution picks the most recent addressed to create the unified profile.
  - By default, the **Last updated timestamp** is used to determine the record that was most recently updated.
- **Profile conflicts are managed by source object type and recency**.
  - You can also change default behavior of conflict resolution to choose a similar constituent profile from a specific source as the source of truth to inform conflict resolution.
  - If you want to specify a data source to use for profile conflicts, you can choose one of your object types as a data source if you select **Source with last updated timestamp**.
  - The most recently updated record from the specified object type is used for resolving profile conflicts.
- **Last updated timestamp identifies which record was most recently updated**.
  - The timestamp attribute associated with the source record's object type is used to identify which record was most recently updated.
  - If the timestamp attribute is not available for the object type, the timestamp on which the record was ingested into your Customer Profiles domain is used.
  - If you have custom object types, you need to add timestamps. See Missing timestamp for profile conflicts (p. 655) for more information.
- **Consolidation is a one-way process and cannot be undone**.
  - Choose your criteria carefully before starting the consolidation process. For more information, see Tips for creating strong criteria (p. 654).
  - Use the GetAutoMergingPreview API to test the auto-merging settings of your Identity Resolution without merging your data.

For an example that shows how criteria is applied, see Example: How sample criteria are applied (p. 655).

Enable Identity Resolution for your Customer Profiles domain

When you enable Identity Resolution you specify the following information:

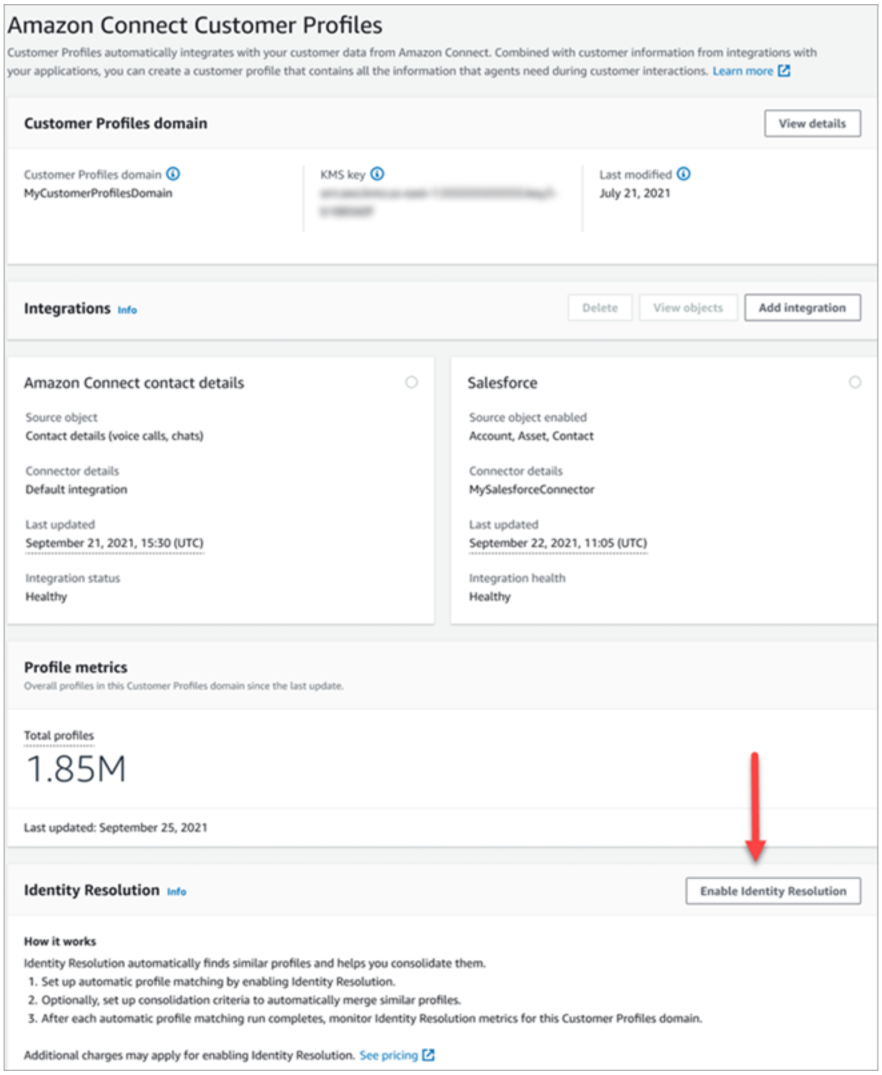
- When the Identity Resolution Job should run on a weekly basis. By default, it runs Saturdays at 12AM UTC.
- The Amazon S3 bucket where the Identity Resolution Job should write the results of the automatic profile matching process. If you don't have an S3 bucket, you'll have the option to create one during the enablement process.

  You can query the Amazon S3 bucket or use the GetMatches API to filter results based on confidence scores (p. 651).

> **Note**
>
> After you enable Identity Resolution you'll see the option to create consolidation criteria (p. 654) for the optional auto-merging process.

To enable Identity Resolution

1. You must have a Customer Profiles domain enabled for your instance. For instructions, see Enable Customer Profiles for your instance (p. 641).
2. In the navigation pane, choose **Customer profiles**.
3. In the **Identity Resolution** section, choose **Enable Identity Resolution**.

   Amazon Connect Customer Profiles

   Customer Profiles automatically integrates with your customer data from Amazon Connect. Combined with customer information from integrations with your applications, you can create a customer profile that contains all the information that agents need during customer interactions. Learn more

   Customer Profiles domain

   Customer Profiles domain: MyCustomerProfilesDomain

   KMS key: [redacted]

   Last modified: July 21, 2021

   Integrations

   Amazon Connect contact details

   Source object: Contact details (voice calls, chats)

   Connector details: Default integration

   Last updated: September 21, 2021, 15:30 (UTC)

   Integration status: Healthy

   Salesforce

   Source object enabled: Account, Asset, Contact

   Connector details: MySalesforceConnector

   Last updated: September 22, 2021, 11:05 (UTC)

   Integration health: Healthy

   Profile metrics

   Overall profiles in this Customer Profiles domain since the last update.

   Total profiles: 1.85M

   Last updated: September 25, 2021

   Identity Resolution

   How it works

   Identity Resolution automatically finds similar profiles and helps you consolidate them.
   1. Set up automatic profile matching by enabling Identity Resolution.
   2. Optionally, set up consolidation criteria to automatically merge similar profiles.
   3. After each automatic profile matching run completes, monitor Identity Resolution metrics for this Customer Profiles domain.

   Additional charges may apply for enabling Identity Resolution. See pricing

4. On the **Enable Identity Resolution** page, specify the date and time when you want the Identity Resolution Job to run.
5. If you want to review the matched profile IDs from an Amazon S3 bucket, select **Write profile ID matches to Amazon S3**. Otherwise, you can use the GetMatches API to review matching profiles.

   - Specify the Amazon S3 bucket where the Identity Resolution Job should write the profile matches.

We recommend applying a policy to prevent a confused deputy security issue. For more information and a sample policy, see Amazon Connect Customer Profiles cross-service confused deputy prevention (p. 1130).

6. When done, choose **Enable Identity Resolution**.
7. After you enable Identity Resolution the Identity Resolution Job runs for the first time within 24 hours.

   Note

   Before running an Identity Resolution Job for the first time on a new Customer Profiles domain, we recommend checking your profile metrics to make sure that profiles have been created. Otherwise, there won't be any matching results.
8. You may want to set up consolidation criteria for auto-merging matching profiles. If so, see Set up consolidation criteria for Identity Resolution (p. 654).

Set up consolidation criteria for Identity Resolution

Note

You must enable Identity Resolution (p. 654) in order to access the option to create consolidation criteria using the Amazon Connect admin console.

When similar profiles are detected by an Identity Resolution Job, the process can automatically merge them into a unified profile based on consolidation criteria that you specify.

The attributes that you select are compared across all similar profiles in a match group for exact match. For example, if you specify `email` as an attribute in the criteria, then all similar profiles in a match group that have exact same value of `email address` are merged into a unified profile.

Tip

If you want to set up your own merging logic, use the MergeProfiles API.

Limits

You can select any attribute from the standard profile (p. 696) to compare similar profiles. For example, you might choose phone number, email address, and name, as well as custom attributes.

You can specify up to:

- 10 consolidation criteria
- 20 attributes per criteria

Tips for creating strong criteria

To improve the targeting of unique profiles and to avoid consolidating profiles that are not duplicates, we recommend the following steps:

- Select attributes that can uniquely identify a customer and are not likely to be the same across customers, such as an account number or a form of government ID.
- Avoid single attribute criteria. Select multiple attributes to create a combination of attributes to improve targeting. For example:
  - **Phone number** with **First name**, **Middle name**, **Last name** is stronger criteria

  than

  - **Phone number** alone, or
  - The combination of **First name, Middle, name, Last name** alone

- Select all attributes within a specific attribute group, when applicable. For example, if you want to use name, select all the related name attributes: **First name, Middle name, Last name**. If you want to use business address, select all the related business address attributes.
- Include one of the following attributes likely to uniquely identify a customer in combination with other attributes in the criteria:
  - Account number
  - Phone number
  - Email

How to set up automerging criteria

Before setting up your consolidation criteria for automatic merging, or automerging, we recommend reviewing How the auto-merging process works (p. 651).

1. After you enable Identity Resolution, on the **Identity Resolution** page you'll have the option of setting up auto-merging criteria. Choose **Create consolidation criteria**.
2. If you receive a **Missing timestamp** dialog box, we recommend adding new timestamp attributes to your custom object types before continuing. See Missing timestamp for profile conflicts (p. 655).
3. In the **Profile conflicts** section, choose how profile conflicts should be resolved when two or more records have conflicts.
4. In the **Consolidation criteria** section, create one or more criteria. We recommend including at least two or more attributes per criteria.

Missing timestamp for profile conflicts

The **Missing timestamp** message is displayed if you have custom object type mappings.

Use the PutProfileObjectType API to add the following new attributes to your custom object type:

- `sourceLastUpdatedTimestamp`
- `sourceLastUpdatedTimestampFormat`

If the timestamp attribute is not specified, you can continue to create consolidation criteria, however, a default timestamp of when the records were ingested into Customer Profiles is used. We recommend adding the new attributes before creating your consolidation criteria.

If you have already defined a custom object type and want to update your custom object type, we run a scheduled backfill every week to update your existing profiles with the `sourceLastUpdatedTimestamp`. To opt in to the scheduled backfill:

1. Update your custom profile object type by using the PutProfileObjectType API.
2. After you update your custom profile object type, open an AWS Support ticket and we'll schedule the backfill for you. The scheduled backfill runs until end of February 2022.

Alternatively, you can delete and then re-create the ingestion/connector you have for your domain that uses the custom object type. All of your data will be re-ingested using your updated object type and `sourceLastUpdatedTimestamp` will be parsed from it.

Example: How sample criteria are applied

In this example there are three criteria:

- **Resolve profile conflicts** is set to **Use last updated timestamp**. This means when two fields have conflicting values, Identity Resolution is going to use the last updated timestamp to determine which value to use.
- Criteria 1:
  - First name, Last name
  - Email
- Criteria 2:
  - Phone number

These criteria are applied to the following profiles:

- Profile A
  - John Doe [last updated **05:00**a]
  - doefamily@anyemail.com [last updated **05:00**a]
  - 555-555-5555 [last updated **07:00**a]
- Profile B
  - John Doe [last updated **04:00**a]
  - doefamily@anyemail.com [last updated **06:00**a]
  - 555-555-555**6** [last updated *04:00*a]
- Profile C
  - **Jane** Doe [last updated **06:00**a]
  - doefamily@anyemail.com [last updated **07:00**a]
  - 555-555-5555 [last updated **06:00**a]

Following are the results when Criteria 1 is applied:

- Profile A and B are merged = Profile AB

This results in ProfileAB, which looks like the following:

- John Doe [last updated **05:00**a]
- doefamily@anyemail.com [last updated **07:00**a]
- 555-555-555**5** [last updated **06:00**a]

Because there's a conflict between the phone numbers, Identity Resolution uses the last timestamp to choose the 555-555-555 number.

Next, Criteria 2 is applied. Following are the results:

- Profile AB and C are merged = Profile ABC

This results in ProfileABC, which looks like the following:

- **Jane** Doe [last updated **06:00**a]
- doefamily@anyemail.com [last updated **07:00**a]
- 555-555-555**5** [last updated **07:00**a]

Identity Resolution uses the First name, Last name, and Email from Profile C because they have the most recent timestamps.

Identity Resolution metrics

Each time an Identity Resolution Job completes, metrics about the process are displayed on the Customer Profiles dashboard. You can review historic metrics for past runs by choosing the **Run history** tab on the **Identity Resolution** page.

The following metrics are generated each time the Identity Resolution Job runs:

- **Profiles reviewed**: The number of profiles that the Identity Resolution Job reviewed for matches.
- **Match groups found**: The number of match groups that were found.
- **Profiles consolidated**: The number of profiles that were consolidated based on the specified consolidation criteria.

Disable Identity Resolution

You can disable Identity Resolution when you no longer want it to automatically find similar profiles. If you have consolidation criteria, all your criteria will be deleted and your profiles will no longer be automatically consolidated. Profiles that have already been consolidated will remain consolidated.

Access Customer Profiles in the agent application

After you enable Amazon Connect Customer Profiles, you need to take steps to make the functionality available through the agent application. This topic explains your options.

> **Tip**
>
> Make sure your agents have **Customer profiles** permissions in their security profile so they can access Customer Profiles. For more information, see Security profile permissions for Customer Profiles (p. 661).

Option 1: Use Customer Profiles with the CCP out-of-the-box

Customer Profiles is already embedded alongside the Contact Control Panel (CCP). Your agents will access the CCP and Customer Profiles in the same browser window using a link that looks like this:

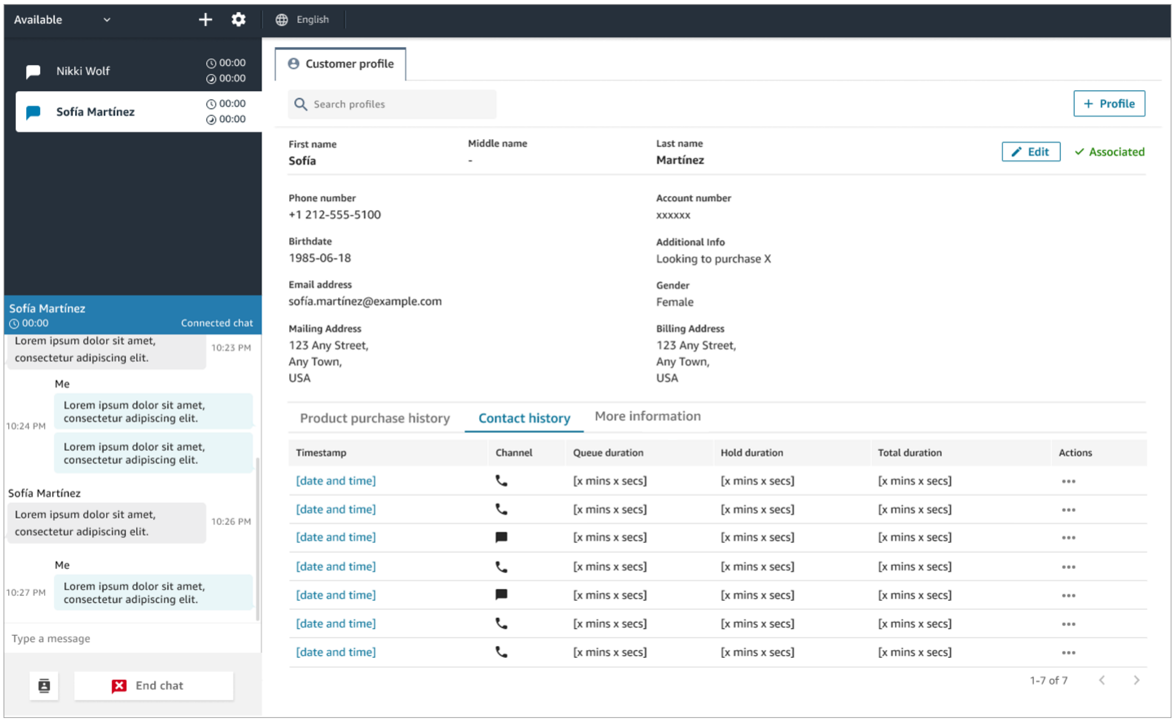
- **https://*`instance name`*.my.connect.aws/agent-app-v2/**

If you access your instance using the **awsapps.com** domain, use the following URL:

- **https://*`instance name`*.awsapps.com/connect/agent-app-v2/**

For help finding your instance name, see Find your Amazon Connect instance name (p. 139).

Following is an example of what the CCP and Customer Profiles look like in the same browser window.



Sofía Martínez
00:00 Connected chat

Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:23 PM

Me
10:24 PM
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Sofía Martínez
Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:26 PM

Me
10:27 PM
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

First name: Sofía
Middle name: -
Last name: Martínez

Phone number: +1 212-555-5100
Account number: xxxxxx
Birthdate: 1985-06-18
Additional Info: Looking to purchase X
Email address: sofía.martínez@example.com
Gender: Female
Mailing Address: 123 Any Street, Any Town, USA
Billing Address: 123 Any Street, Any Town, USA

Product purchase history | Contact history | More information

Timestamp	Channel	Queue duration	Hold duration	Total duration	Actions
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	💬	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	💬	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••
[date and time]	☎	[x mins x secs]	[x mins x secs]	[x mins x secs]	•••

1-7 of 7

Option 2: Embed Customer Profiles into a custom agent application

When you embed your Contact Control Panel (CCP), you have the option of showing or hiding the pre-built CCP user interface. For example, you may want to develop a custom agent application that has a user interface you design, with customized buttons to accept and reject calls. Or, you may want to embed the pre-built CCP that's included with Amazon Connect into another custom app.

Regardless of whether you display the pre-built CCP user interface, or hide it and build your own, you use the Amazon Connect Streams library to embed the CCP and Customer Profiles into the agent's application. This way, Amazon Connect Streams is initialized, and the agent can connect and authenticate to Amazon Connect, and Customer Profiles.

For information about embedding Customer Profiles, see Initialization for CCP, Customer Profiles, and Wisdom.

To build your own widget while using raw data from Customer Profiles, see the Github documentation about how to use the CustomerProfilesJS open source library.

> **Tip**
> When you customize the agent's application, you determine the URL agents will use to access their agent application, and it might very different from the one provided by Amazon Connect. For example, your URL could be https://example-corp.com/agent-support-app.

Use contact attributes to autopopulate customer profiles

By default, Amazon Connect Customer Profiles uses the following values to search for and autopopulate a customer profile in its user interface:

- For voice contacts: Phone number
- For chat contacts: Customer name

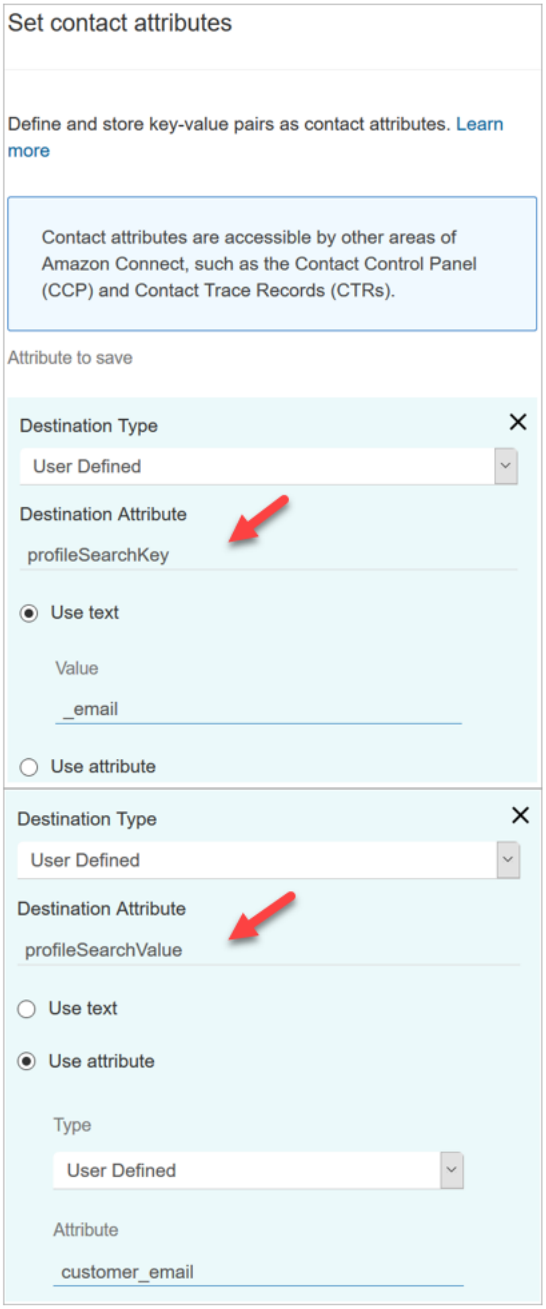
To customize this behavior, use the following contact attributes:

Attribute	Description	Type	JSONPath Reference
profileSearchKey	The name of the attribute you want to use to search for a profile.	User-defined	Not applicable
profileSearchValue	The value of the key you want to search for, such as customer name or account number.	User-defined	Not applicable

For example, to search by email for chat contacts, you can set the `profileSearchKey` attribute to the `_email` search key, and provide the email value as the `profileSearchValue`.

If you have defined custom keys in your profile objects, you can search by those search keys as well. To make sure your custom keys are searchable, see Key definition details (p. 688).

The following image shows how you might use these attributes in the Set contact attributes (p. 399) block.



Set contact attributes

Define and store key-value pairs as contact attributes. Learn more

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

Attribute to save

Destination Type: User Defined

Destination Attribute: profileSearchKey

● Use text

Value: _email

○ Use attribute

Destination Type: User Defined

Destination Attribute: profileSearchValue

○ Use text

● Use attribute

Type: User Defined

Attribute: customer_email

Automatically associate a customer profile with a contact

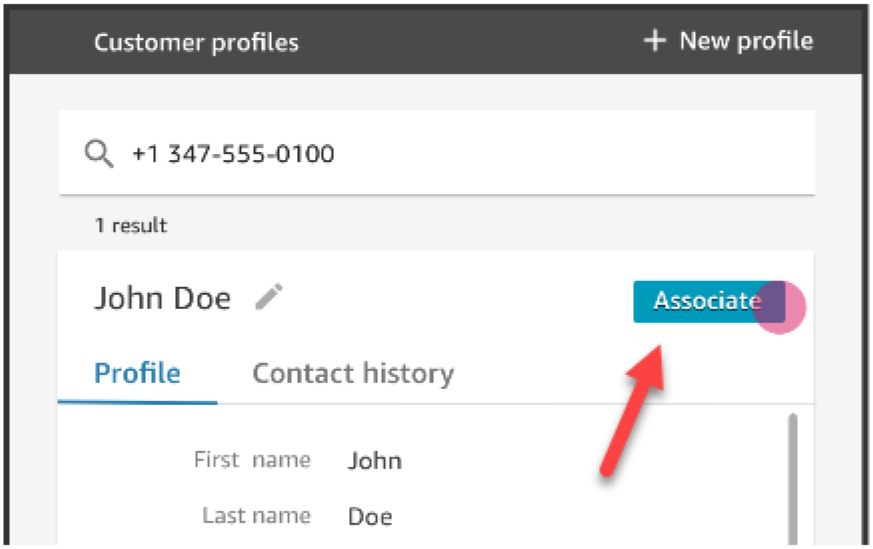
By default, agents need to manually associate a customer profile with a contact based after they've verified the customer's identity. To change this behavior to automatically associate contacts with a profile based on the phone number, see Change behavior of inferred profiles to automatically associate the contact record with one profile found (p. 692).

If multiple profiles match a contact's phone number, the multiple matched profiles are shown to the agent. The agent needs to choose which profile to associate with the contact.

Security profile permissions for Customer Profiles

Assign the following **Customer profiles** permissions as needed to the agent's security profile:

- **View**: Enables agents to see the Customer profiles application. They can:
  - View profiles that are autopopulated in the agent app.
  - Search for profiles.
  - View details stored in customer profiles (for example, Name, Address).
  - Associate contact records to profiles, as shown in the following image.



- **Edit**: Enables agents to edit details in the customer profile (for example, change address). They inherit **View** permissions by default.
- **Create**: Enables agents to create and save a new profile. They inherit **View** permissions by default, but don't inherit **Edit** permissions.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

By default, the **Admin** security profile already has permissions to perform all Customer profiles activities.

Integrate external applications with Customer Profiles

Amazon Connect provides a set of pre-built integrations powered by Amazon AppFlow and Amazon EventBridge. After you enable Amazon Connect Customer Profiles, you can use these integrations to combine information from external applications such as Salesforce or Zendesk, with contact history from Amazon Connect. This creates a customer profile that has all the information agents need during customer interactions in a single place.

You can also use Customer Profiles in Amazon AppFlow. Amazon AppFlow supports `CustomerProfiles` as a destination. You can use Amazon AppFlow APIs to send data into Customer Profiles using `CustomerProfiles` as the destination name.

Before you begin, make sure you are using a customer managed key. For more information about configuring KMS keys, see Create a KMS key to be used by Customer Profiles to encrypt data (required) (p. 642).

Contents

Set up integration for Salesforce, ServiceNow, Marketo, or Zendesk

These integrations use Amazon AppFlow to provide periodic updates to Amazon Connect Customer Profiles.

Before you begin

Bulk ingestion of data

When you set up your integration, you are prompted to enter a date how far back you want to go to ingest data. If you choose a date that is more than two months ago, Customer Profiles automatically enables bulk ingestion by creating multiple flows. It does this so you don't have to calculate how many flows you need to ingest data.

When automatic bulk ingestion is enabled, Customer Profiles does the following:

- Sets the batch size to two months.
- Retries on transient failures up to three times before failing.

You can use the CreateIntegrationWorkflowRequest API to call your own batch size.

Why am I asked to select or create an IAM role?

For Salesforce, Marketo, and ServiceNow, Customer Profiles helps improve the historical ingestion of these sources by using your IAM role to create several workflows to ingest your data quickly and efficiently.

For these sources, if you select more than 60 days back in the **Date for importing records** date picker, you will be prompted to create a new IAM role or select an existing one. This role allows Customer Profiles to manage your integration. It provides Customer Profiles with the necessary permissions to update and create a workflow to ingest your data. After the workflow is complete, Customer Profiles creates a standard, continuous integration that ingests your new data as it is updated in your source.

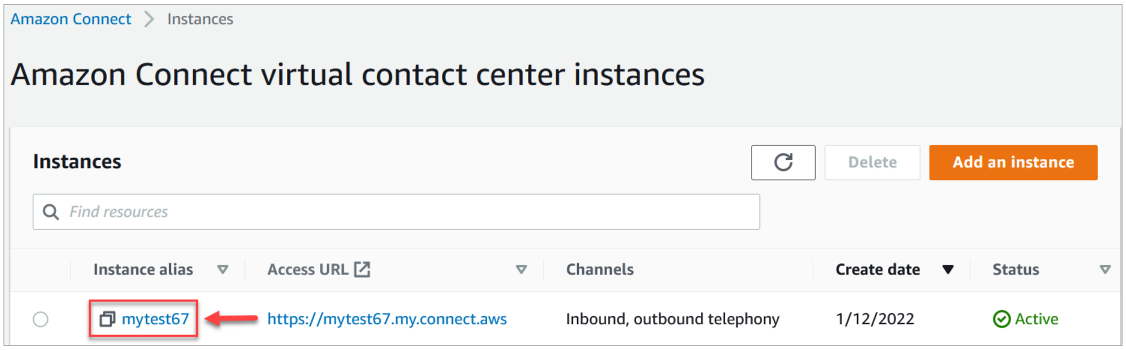
The role created in the console is only useable by the domain it was created on. This is because Amazon Connect limits the access of the role to only the KMS key used by the domain.

For more information, see Grant least privilege access to your Customer Profiles execution role (p. 666).

Integration setup steps

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

2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



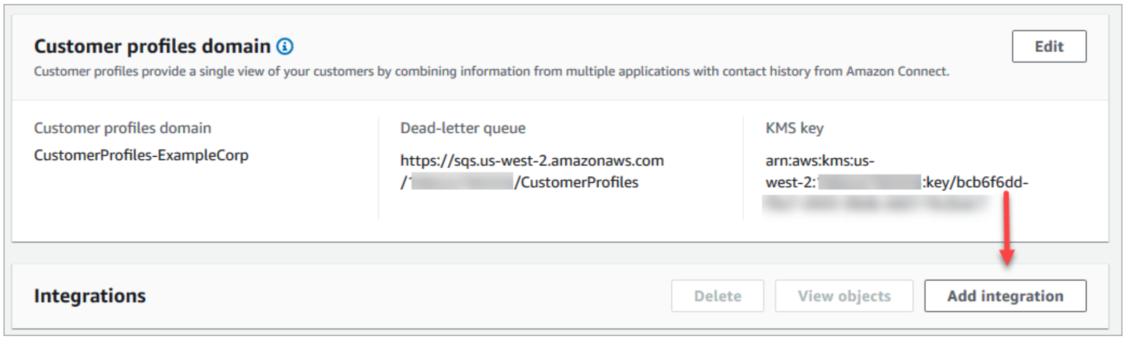
Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Customer profiles**.

4. On the **Customer profiles configuration** page, choose **Add integration**.



Customer profiles domain

Customer profiles provide a single view of your customers by combining information from multiple applications with contact history from Amazon Connect.

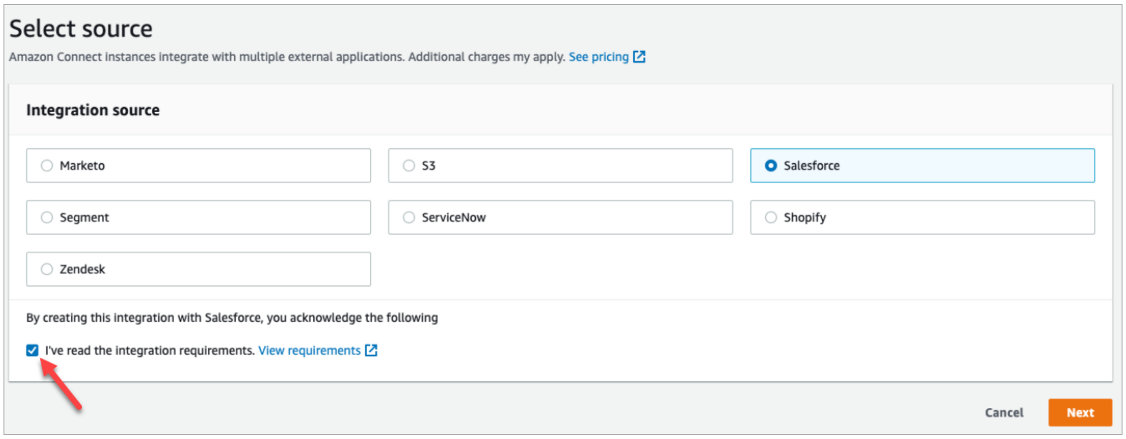
Customer profiles domain: CustomerProfiles-ExampleCorp

Dead-letter queue: https://sqs.us-west-2.amazonaws.com/[redacted]/CustomerProfiles

KMS key: arn:aws:kms:us-west-2:[redacted]:key/bcb6f6dd-[redacted]

Integrations

5. On the **Select source** page, choose which external application you want to get customer profiles data from: Salesforce, Zendesk, ServiceNow, or Marketo. Select **I've read the integration requirements** to indicate you understand the connection requirements for your application.



Select source

Amazon Connect instances integrate with multiple external applications. Additional charges my apply. See pricing

Integration source

○ Marketo ○ S3 ● Salesforce

○ Segment ○ ServiceNow ○ Shopify

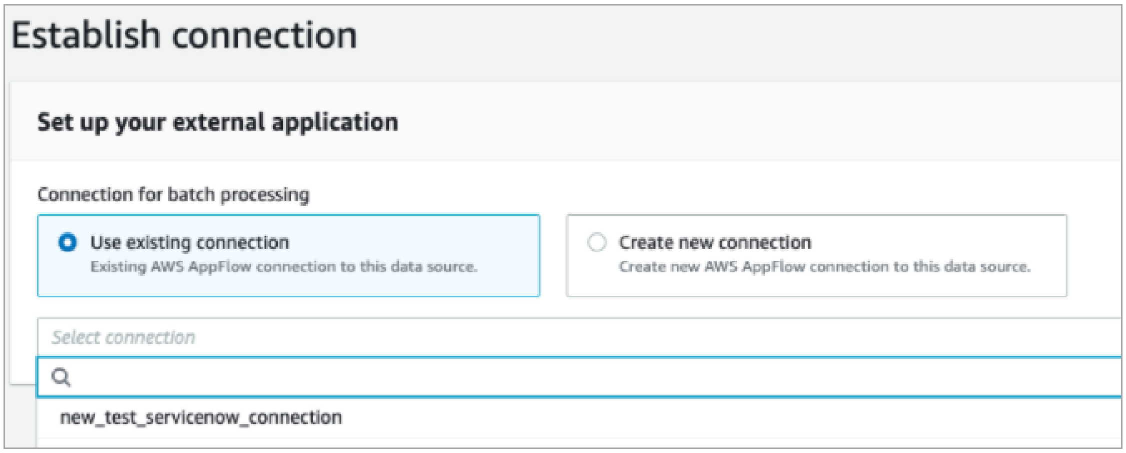
○ Zendesk

By creating this integration with Salesforce, you acknowledge the following

☑ I've read the integration requirements. View requirements

6. On the **Establish connection** page, choose one of the following:

- **Use existing connection**: This allows you to reuse existing Amazon AppFlow resources you may have created in your AWS account..
- **Create new connection**: Enter the information required by the external application.



Establish connection

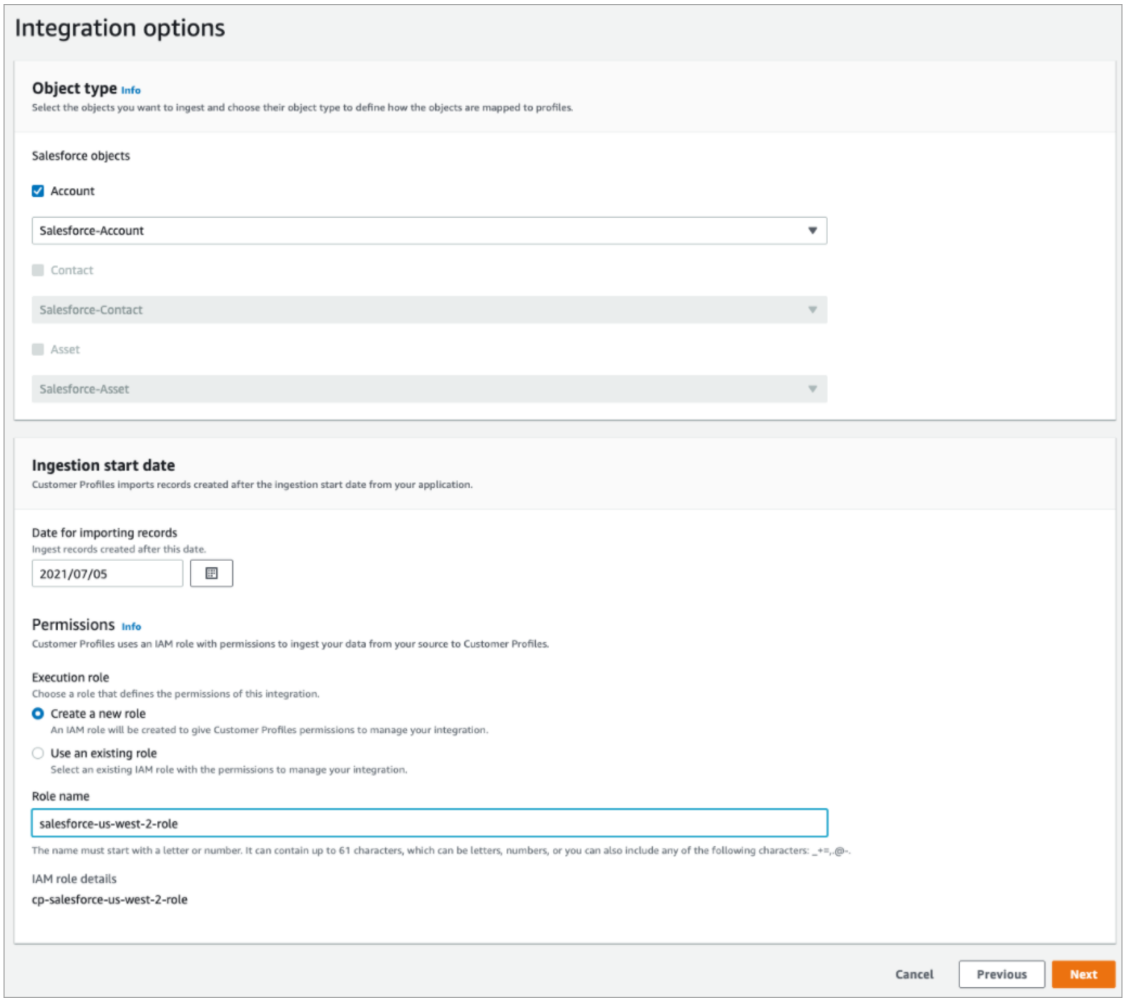
Set up your external application

Connection for batch processing

● Use existing connection
Existing AWS AppFlow connection to this data source.
○ Create new connection
Create new AWS AppFlow connection to this data source.
Select connection
new_test_servicenow_connection

7. On the **Integration options** page, choose which source objects you want to ingest and select their object type.

   Object types store your ingested data. They also define how objects from your integrations are mapped to profiles when they are ingested. Customer Profiles provides default object type templates you can use that define how attributes in your source objects are mapped to the standard objects in Customer Profiles. You can also use the object mappings that you've created from the PutProfileObjectType.



Integration options

Object type

Select the objects you want to ingest and choose their object type to define how the objects are mapped to profiles.

Salesforce objects

☑ Account

Salesforce-Account

□ Contact

Salesforce-Contact

□ Asset

Salesforce-Asset

Ingestion start date

Customer Profiles imports records created after the ingestion start date from your application.

Date for importing records

Ingest records created after this date.

2021/07/05

Permissions

Customer Profiles uses an IAM role with permissions to ingest your data from your source to Customer Profiles.

Execution role

Choose a role that defines the permissions of this integration.

● Create a new role

An IAM role will be created to give Customer Profiles permissions to manage your integration.

○ Use an existing role

Select an existing IAM role with the permissions to manage your integration.

Role name

salesforce-us-west-2-role

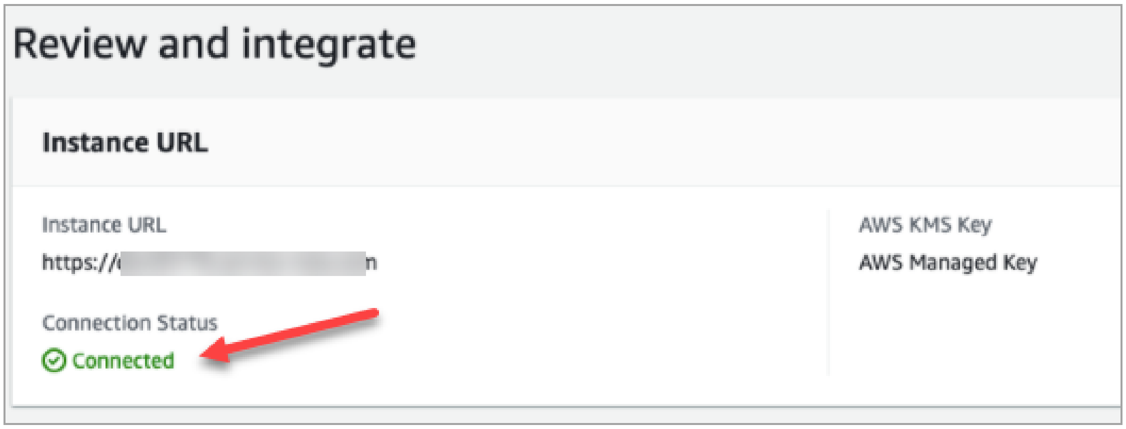
The name must start with a letter or number. It can contain up to 61 characters, which can be letters, numbers, or you can also include any of the following characters: _+=,.@-.

IAM role details

cp-salesforce-us-west-2-role

8. For the **Ingestion start date**, Customer Profiles starts ingesting records created after this date. By default, the date for importing records is set at 30 days prior.

9. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Create integration**.



Review and integrate

Instance URL

Instance URL

https://[redacted]n

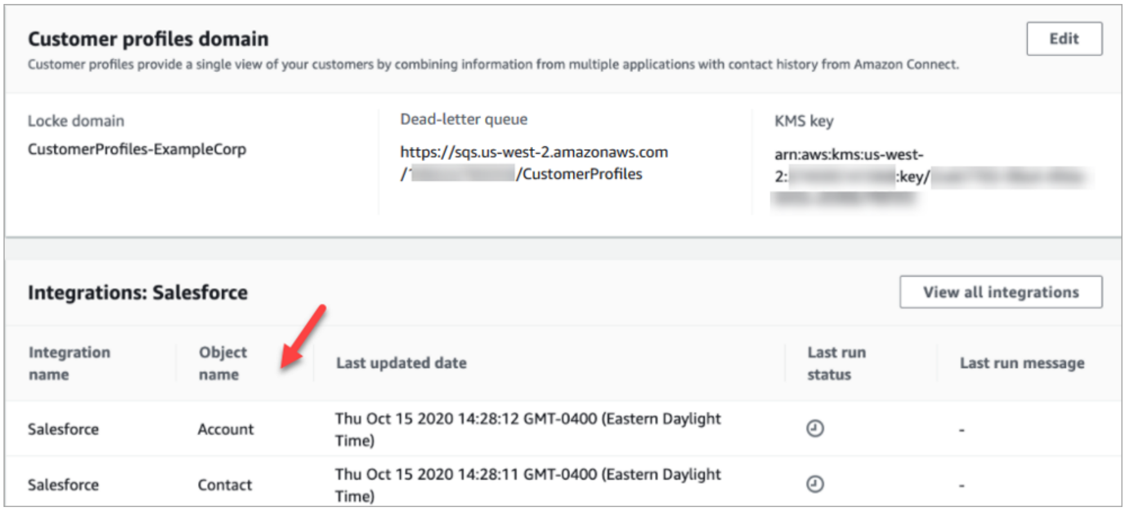
Connection Status

Connected

AWS KMS Key

AWS Managed Key

10. After the integration is set up, back on the **Customer profiles configuration** page, choose **View objects** to see what data is being batched and sent. Currently, this process ingests records that were created or modified in the last 30 days.



Customer profiles domain

Customer profiles provide a single view of your customers by combining information from multiple applications with contact history from Amazon Connect.

Locke domain
CustomerProfiles-ExampleCorp

Dead-letter queue
https://sqs.us-west-2.amazonaws.com
/[redacted]/CustomerProfiles

KMS key
arn:aws:kms:us-west-
2:[redacted]:key/[redacted]

Integrations: Salesforce

Integration name	Object name	Last updated date	Last run status	Last run message
Salesforce	Account	Thu Oct 15 2020 14:28:12 GMT-0400 (Eastern Daylight Time)	◷	-
Salesforce	Contact	Thu Oct 15 2020 14:28:11 GMT-0400 (Eastern Daylight Time)	◷	-

Grant least privilege access to your Customer Profiles execution role

If you want to create your own IAM role, we recommend using the permissions shown in the following code to limit the role to the least permissions needed. Use the snippet below to create your role manually. Use your own KMS key and specify your Region where needed.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:RequestTag/awsOwningService": "customer-profiles-integration-
workflow"
                }
            },
            "Action": [
                "appflow:CreateFlow",
                "appflow:TagResource",
                "profile:TagResource",
                "profile:PutIntegration"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "CreateFlowResources"
        },
        {
            "Action": [
                "appflow:UseConnectorProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "UseConnectorResources"
        },
        {
            "Condition": {
                "ForAnyValue:StringEquals": {
                    "aws:ResourceTag/awsOwningService": "customer-profiles-integration-
workflow"
                }
            },
            "Action": [
                "appflow:DescribeFlow",
                "appflow:DescribeFlowExecutionRecords",
                "appflow:DeleteFlow",
                "appflow:StartFlow",
                "appflow:StopFlow",
                "appflow:UpdateFlow",
                "profile:DeleteIntegration"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AccessFlowResources"
        },
    {
      "Action": [
        "kms:CreateGrant",
        "kms:ListGrants"
      ],
      "Resource": "{{YourKMSKeyConsumedByTheDomain}}",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": [
            "appflow.{{region}}.amazonaws.com"
          ]
        }
      },
      "Effect": "Allow",
      "Sid": "KMSAppflow"
    },
    {
      "Action": [
        "kms:CreateGrant"
      ],
      "Resource": "{{YourKMSKeyConsumedByTheDomain}}",
      "Condition": {
        "StringEquals": {
          "kms:ViaService": [
            "profile.{{region}}.amazonaws.com"
          ]
        },
        "ForAllValues:StringEquals": {
          "kms:GrantOperations": [
            "Decrypt"
          ]
        }
      },
      "Effect": "Allow",
      "Sid": "KMSCustomerProfiles"
    }
  ]
}
```

Monitor your Customer Profiles integrations

After your connection is established, if it stops working, delete the integration and then re-establish it.

What to do if objects aren't being sent

If an object fails to be sent, choose **Flow details** to learn more about what's gone wrong.

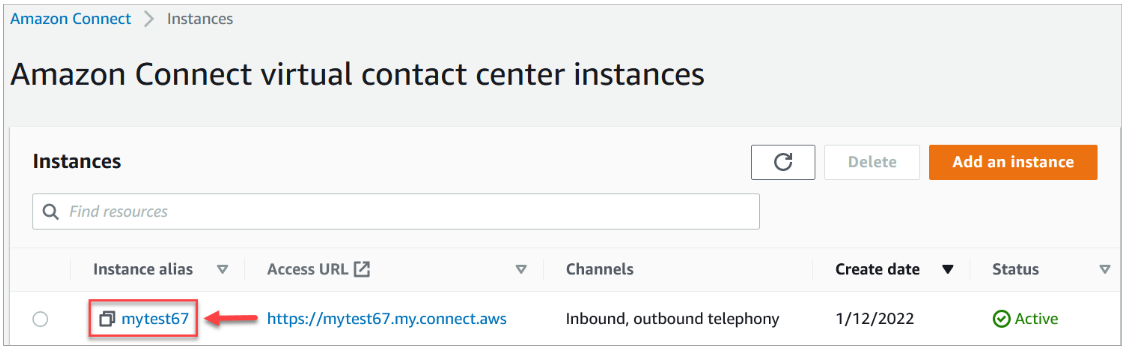
You may need to delete the configuration and re-connect to the external application.

Set up integration for Segment

To provide periodic updates to Amazon Connect Customer Profiles, you can integrate with Segment using Amazon AppFlow. You first set up the connection in Amazon Connect and Segment, and then verify the Segment integration.

Set up the connection in Amazon Connect and Segment

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



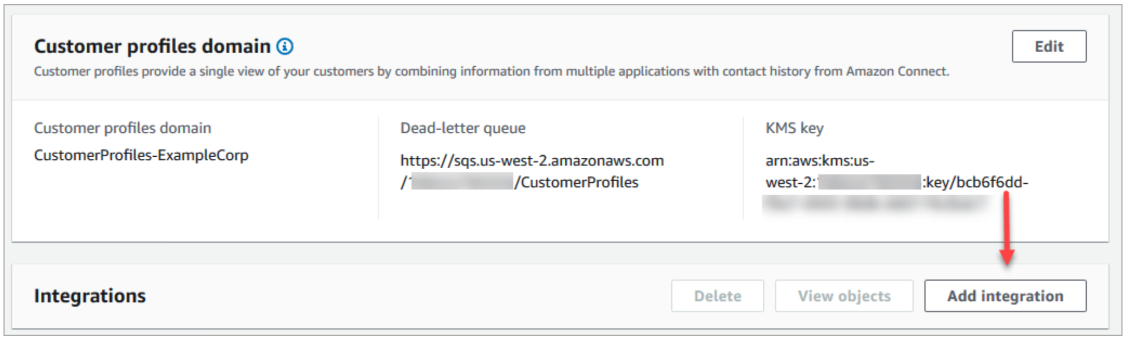
Amazon Connect > Instances

Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Customer profiles**.
4. On the **Customer profiles configuration** page, choose **Add integration**.



Customer profiles domain

Customer profiles provide a single view of your customers by combining information from multiple applications with contact history from Amazon Connect.

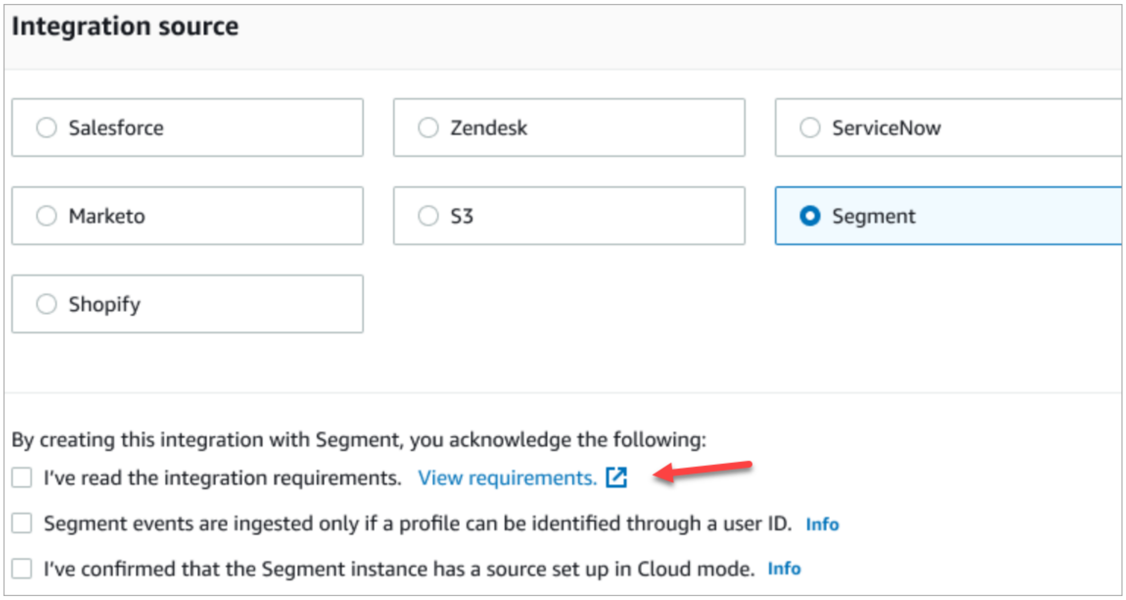
Customer profiles domain
CustomerProfiles-ExampleCorp

Dead-letter queue
https://sqs.us-west-2.amazonaws.com/[redacted]/CustomerProfiles

KMS key
arn:aws:kms:us-west-2:[redacted]:key/bcb6f6dd-[redacted]

Integrations

5. On the **Select source** page, choose **Segment**. Review the application requirements that are listed on the **Select application** page.



Integration source

○ Salesforce
○ Zendesk
○ ServiceNow
○ Marketo
○ S3
● Segment
○ Shopify

By creating this integration with Segment, you acknowledge the following:

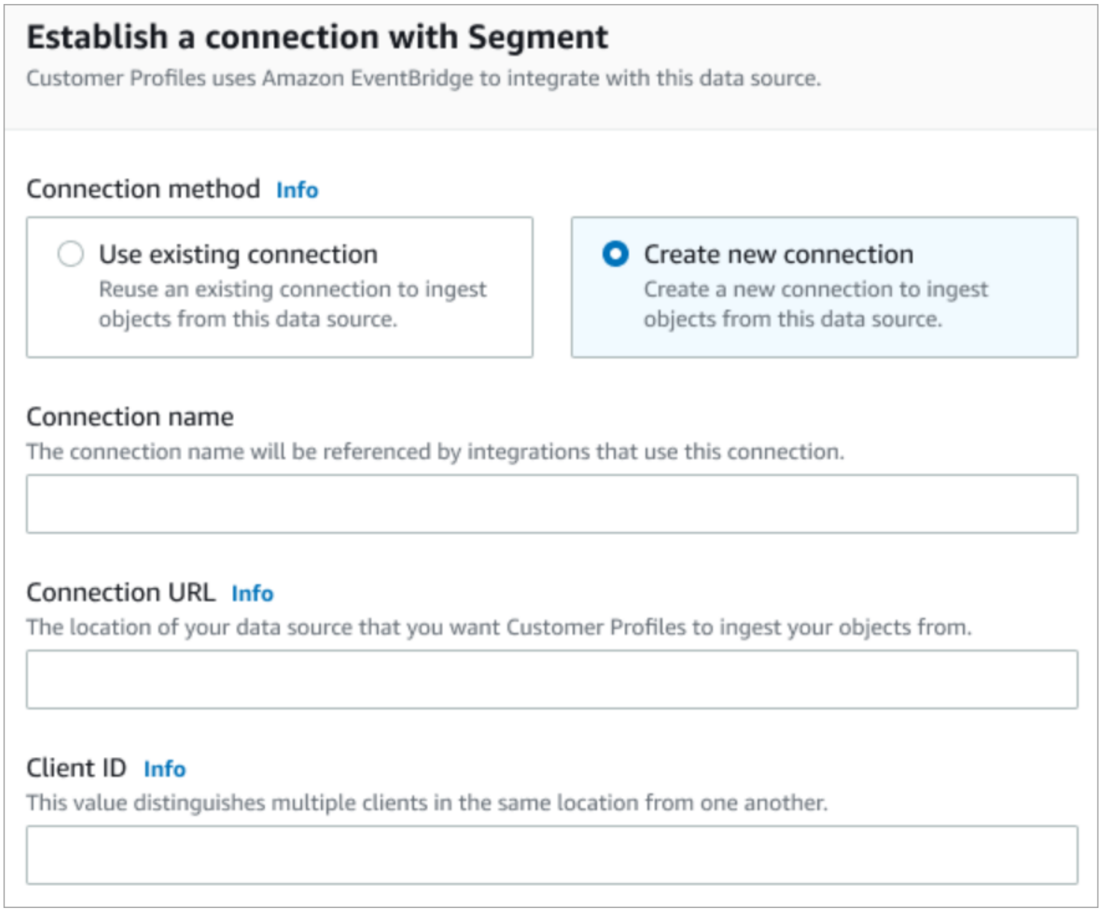
□ I've read the integration requirements. View requirements.

□ Segment events are ingested only if a profile can be identified through a user ID. Info

□ I've confirmed that the Segment instance has a source set up in Cloud mode. Info

6. On the **Establish connection** page, choose one of the following:

   - **Use existing connection**: This allows you to reuse existing Amazon EventBridge resources that you may have created in your AWS account.
   - **Create new connection**: Enter the information required by the external application.



Establish a connection with Segment

Customer Profiles uses Amazon EventBridge to integrate with this data source.

Connection method Info

○ Use existing connection
Reuse an existing connection to ingest objects from this data source.

● Create new connection
Create a new connection to ingest objects from this data source.

Connection name
The connection name will be referenced by integrations that use this connection.

Connection URL Info
The location of your data source that you want Customer Profiles to ingest your objects from.

Client ID Info
This value distinguishes multiple clients in the same location from one another.

- **Connection name**: Provide a name for your connection. The connection name is referenced by integrations that use this connection.
- **Connection URL**: Enter your application connection URL. This URL is used for deep-linking into the objects created in your external application. The connection URL is the Segment workspace URL available on the application website.

  To find your workspace URL:

  1. Log in to your segment.com account.
  2. Go to **Settings**, **General settings**.
  3. Copy the URL from your browser.
- **Client ID**: Enter your application client ID. This is a string that uniquely distinguishes the client in your external application. This client ID is the Source Name available on the application website. You use the ID that you specify here to identify the client that you want Customer Profiles to ingest your objects from.

  To find your source ID:

  1. Log in to your segment.com account.
  2. Go to **Sources**, and choose a source.
  3. Go to **Settings**, **API Keys**.
  4. Copy your **Source ID**.

7. Customer Profiles uses Amazon EventBridge for integrations with Segment. Log in to your application to continue setting up the Amazon EventBridge event source.
8. On the **Source set up** page, copy your AWS account ID to your clipboard, and then choose **Log in to Segment** to configure Amazon EventBridge.
9. Use the following instructions to set up Segment:

   a. Log in to Segment.

   b. In your application, select a source to set up the destination to Customer Profiles.

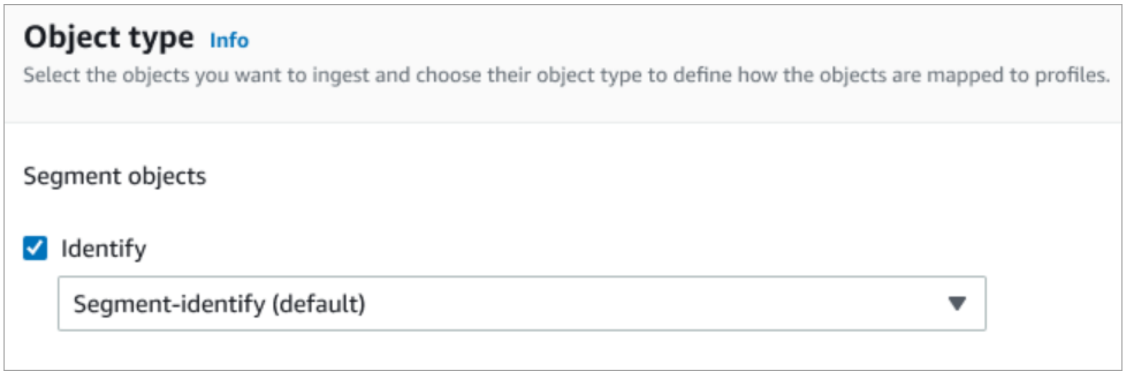
   c. Paste in your AWS account ID and select your AWS Region.

   d. Toggle **ON**, to activate your partner event source.

   e. Go to **Event Tester**, and send a test event to complete activating your partner event source.

   f. After you set up the event source destination, return to Customer Profiles. You will see an alert that indicates Amazon Connect has successfully connected with Segment.
10. On the **Integration options** page, choose which source objects you want to ingest and select their object type.

    Object types store your ingested data. They also define how objects from your integrations are mapped to profiles when they are ingested. Customer Profiles provides default object type templates you can use that define how attributes in your source objects are mapped to the standard objects in Customer Profiles. You can also use the object mappings that you've created from the PutProfileObjectType.



Object type Info

Select the objects you want to ingest and choose their object type to define how the objects are mapped to profiles.

Segment objects

☑ Identify

Segment-identify (default) ▼

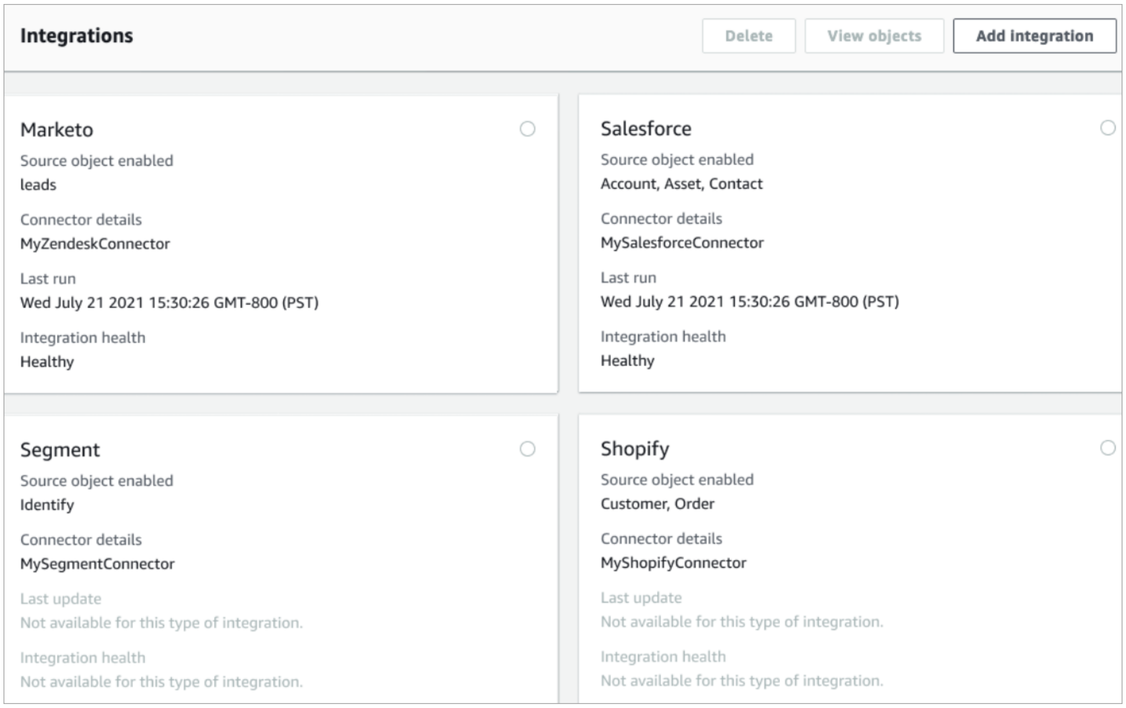
11. For the **Ingestion start date**, Customer Profiles starts ingesting records created after the integration is added.

    Note

    If you need historical records, you can use Amazon S3 as an integration source to import them (p. 730).

12. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Add integration**.

13. After the integration is set up, back on the **Customer profiles configuration** page, the **Integrations** page displays which integrations are currently set up. The **Last run** and **Integration health** are not currently available for this type of integration.



Marketo ○
Source object enabled
leads
Connector details
MyZendeskConnector
Last run
Wed July 21 2021 15:30:26 GMT-800 (PST)
Integration health
Healthy

Salesforce ○
Source object enabled
Account, Asset, Contact
Connector details
MySalesforceConnector
Last run
Wed July 21 2021 15:30:26 GMT-800 (PST)
Integration health
Healthy

Segment ○
Source object enabled
Identify
Connector details
MySegmentConnector
Last update
Not available for this type of integration.
Integration health
Not available for this type of integration.

Shopify ○
Source object enabled
Customer, Order
Connector details
MyShopifyConnector
Last update
Not available for this type of integration.
Integration health
Not available for this type of integration.

To see what data is being sent, choose the integration and+ then choose **View objects** .

Verify your Segment integration

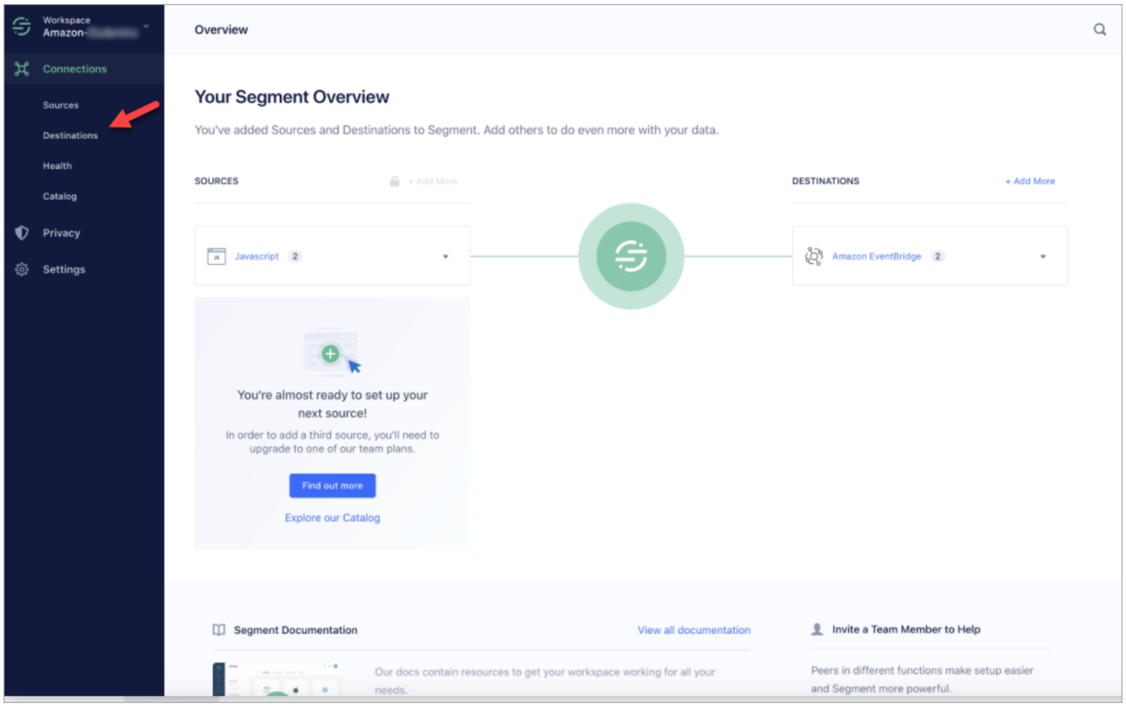
To perform this step you need the following prerequisites:

- Access to your Segment workspace.

- Access to the Amazon Connect Contact Control Panel (p. 291).

To verify your Segment integration

1. Go to your Segment workspace dashboard and choose **Destinations**.



Your Segment Overview

You've added Sources and Destinations to Segment. Add others to do even more with your data.

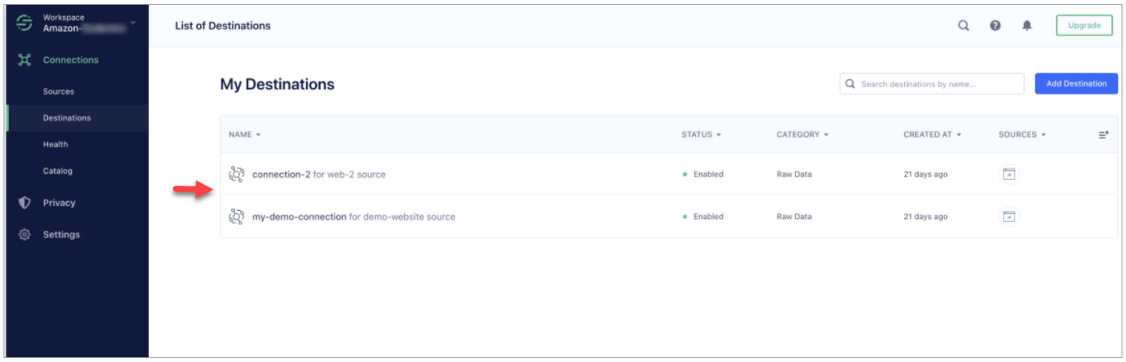
You're almost ready to set up your next source!

In order to add a third source, you'll need to upgrade to one of our team plans.

Our docs contain resources to get your workspace working for all your needs.

Peers in different functions make setup easier and Segment more powerful.

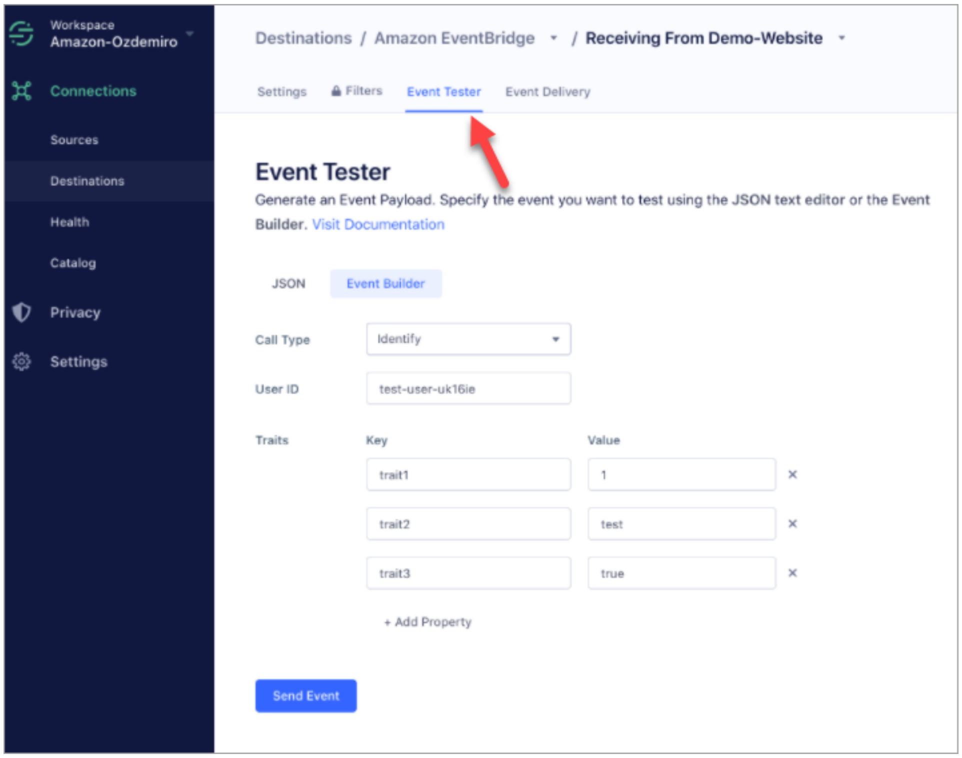
2. You will see a list of destinations where that Segment sends data. Choose the EventBridge destination for Customer Profiles.



My Destinations

NAME	STATUS	CATEGORY	CREATED AT	SOURCES
connection-2 for web-2 source	● Enabled	Raw Data	21 days ago	
my-demo-connection for demo-website source	● Enabled	Raw Data	21 days ago	

3. Choose the **Event Tester** tab. From this page you will send a test event to Customer Profiles. The event is ingested and turned into a customer profile that you can view in the Amazon Connect agent application.



Event Tester

Generate an Event Payload. Specify the event you want to test using the JSON text editor or the Event Builder. Visit Documentation

Call Type: Identify

User ID: test-user-uk16ie

Traits	Key	Value
	trait1	1
	trait2	test
	trait3	true

4. Select **Identify** as the event type, and select **Event Builder** as your input method.
5. You can specify a **User ID** and some traits. Agents can search for these traits in the agent application.
6. Choose **Send Event**.
7. The event delivery should be almost instantaneous but allow it a minute for it to be delivered and create a customer profile.
8. Open the Amazon Connect agent application. Search for the user ID you entered in the **Event Builder**. You should be able to see the customer profile with the user ID and the traits you entered.
9. If you cannot see the customer profile, then there is a problem with your integration. To troubleshoot:

   1. Go to the Amazon EventBridge console.
   2. Check whether the EventSource is Active and the matching EventBus exists and is running.

   If these are working, contact AWS Support for assistance investigating the issue.

Monitor your Customer Profiles integrations

After your connection is established, if it stops working, delete the integration and then re-establish it.

What to do if objects aren't being sent

If an object fails to be sent, choose **Flow details** to learn more about what's gone wrong.

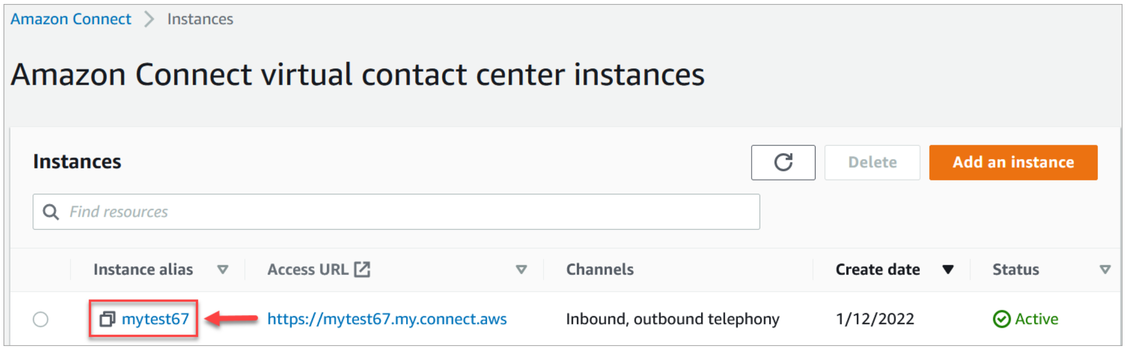
You may need to delete the configuration and re-connect to the external application.

Set up integration for Shopify

To provide periodic updates to Amazon Connect Customer Profiles, you can integrate with Shopify using Amazon AppIntegrations. You first set up the connection in Amazon Connect and Shopify, and then verify the Shopify integration.

Set up the connection in Amazon Connect and Shopify

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.

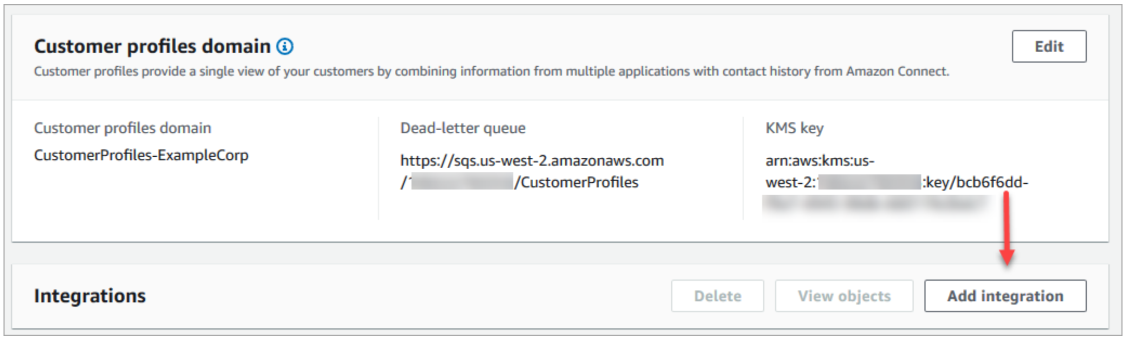


Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Customer profiles**.
4. On the **Customer profiles configuration** page, choose **Add integration**.



Customer profiles domain

Customer profiles provide a single view of your customers by combining information from multiple applications with contact history from Amazon Connect.

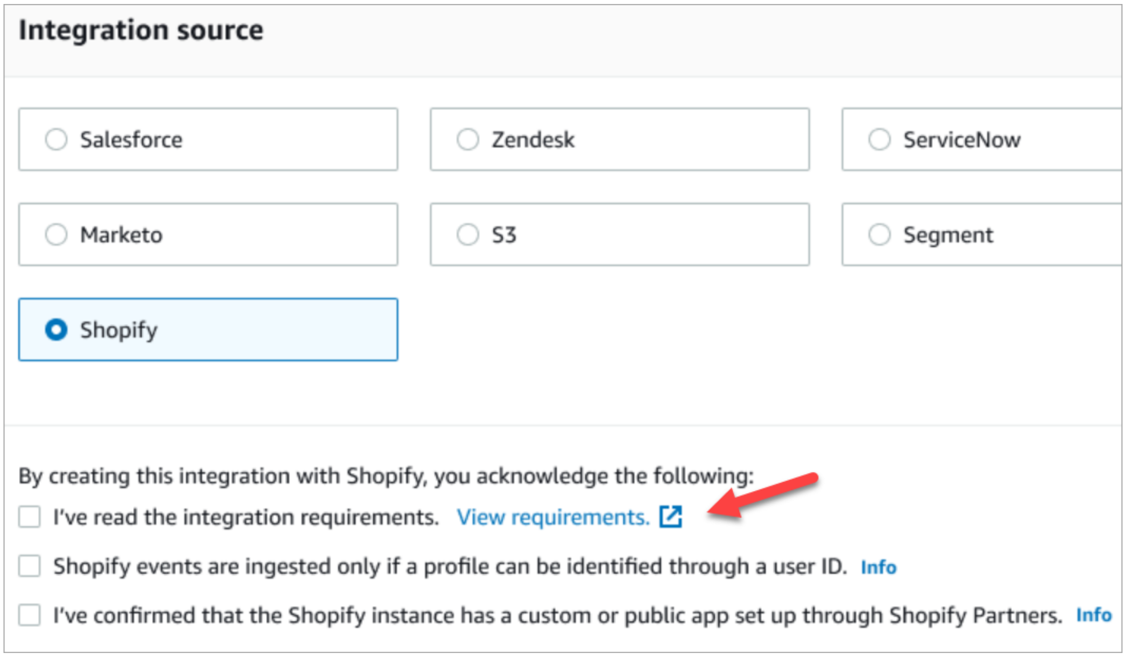
Customer profiles domain
CustomerProfiles-ExampleCorp

Dead-letter queue
https://sqs.us-west-2.amazonaws.com/[redacted]/CustomerProfiles

KMS key
arn:aws:kms:us-west-2:[redacted]:key/bcb6f6dd-[redacted]

Integrations

5. On the **Select source** page, choose **Shopify**. Review the application requirements that are listed on the **Select application** page.



Integration source

○ Salesforce
○ Zendesk
○ ServiceNow
○ Marketo
○ S3
○ Segment
● Shopify

By creating this integration with Shopify, you acknowledge the following:

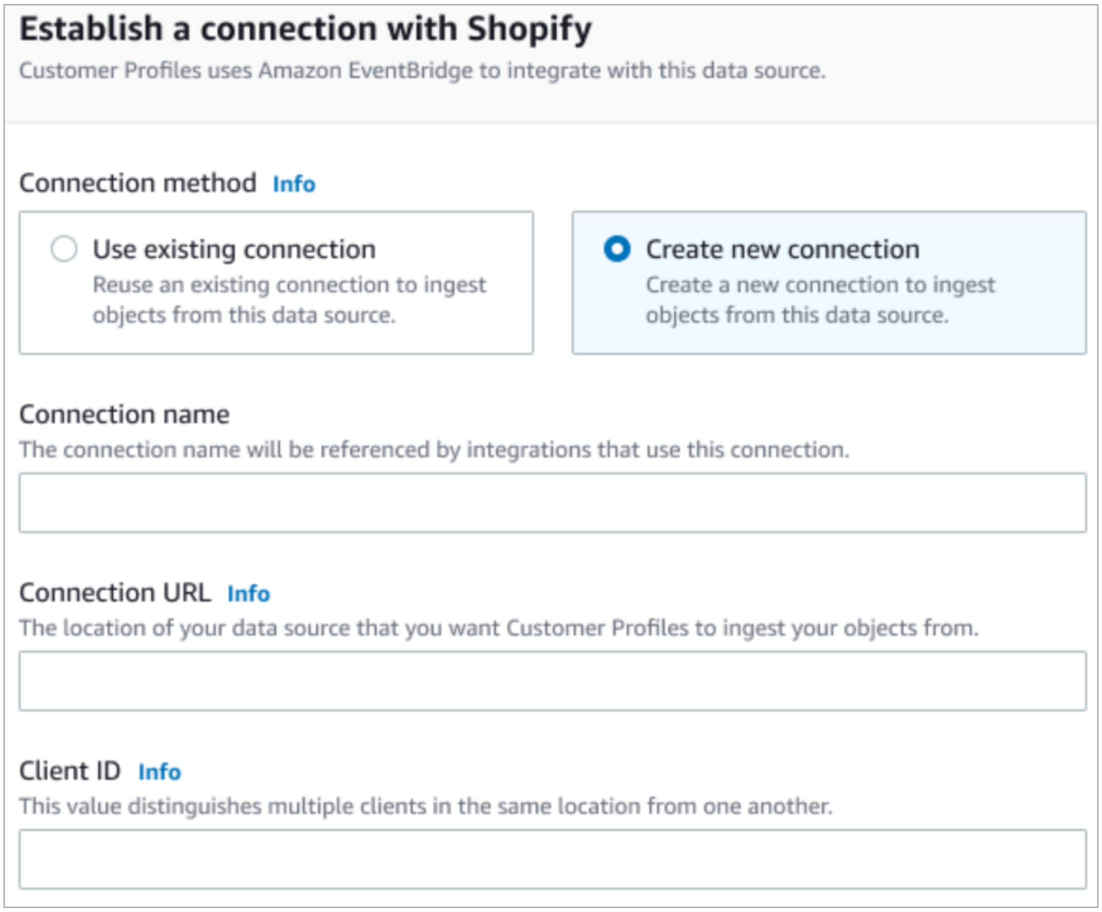
□ I've read the integration requirements. View requirements.

□ Shopify events are ingested only if a profile can be identified through a user ID. Info

□ I've confirmed that the Shopify instance has a custom or public app set up through Shopify Partners. Info

6. On the **Establish connection** page, choose one of the following:

   - **Use existing connection**: This allows you to reuse existing Amazon EventBridge resources that you may have created in your AWS account.
   - **Create new connection**: Enter the information required by the external application.



Establish a connection with Shopify

Customer Profiles uses Amazon EventBridge to integrate with this data source.

Connection method Info

○ Use existing connection
Reuse an existing connection to ingest objects from this data source.

● Create new connection
Create a new connection to ingest objects from this data source.

Connection name
The connection name will be referenced by integrations that use this connection.

Connection URL Info
The location of your data source that you want Customer Profiles to ingest your objects from.

Client ID Info
This value distinguishes multiple clients in the same location from one another.

- **Connection name**: Provide a name for your connection. The connection name is referenced by integrations that use this connection.
- **Connection URL**: Enter your application connection URL. This URL is used for deep-linking into the objects created in your external application. The connection URL is the Shopify Partner app URL available on the application website.

  To find your Shopify Partner app URL:

  - Log in to your partners.shopify.com account.
  - Go to your app.
  - Copy the URL from your browser.
- **Client ID**: Enter your application client ID. This is a string that uniquely distinguishes the client in your external application. This client ID is the Source Name available on the application website. You use the ID that you specify here to identify the client that you want Customer Profiles to ingest your objects from. Your client ID may be available after following the Source setup steps.

  To find your source name:

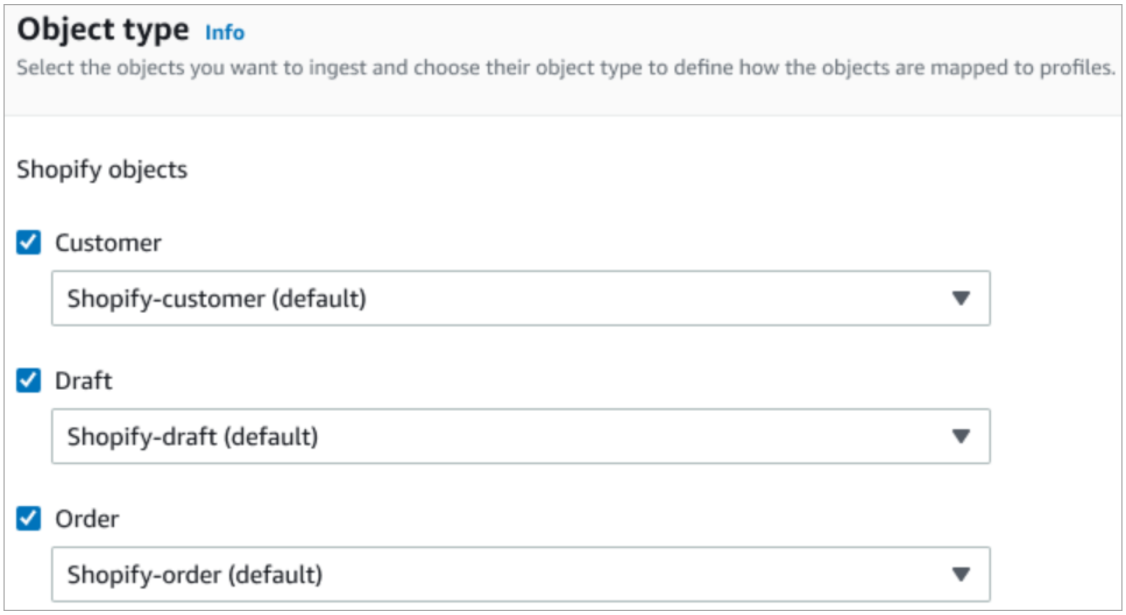
  - Log in to your partners.shopify.com account.
  - Go to your app.
  - Copy the source name from your Amazon EventBridge event source.

7. On the **Source set up** page, copy your AWS account ID to your clipboard, and then choose **Log in to Shopify**.
8. Use the following instructions to set up Shopify:

   a. Log in to partners.shopify.com.
   b. Under Amazon EventBridge, choose **Create source**.
   c. Paste in your AWS account ID and select your AWS Region.
   d. After you set up the event source destination, return to Customer Profiles. You will see an alert that indicates Amazon Connect has successfully connected with Shopify.

9. On the **Integration options** page, choose which source objects you want to ingest and select their object type.

   Object types store your ingested data. They also define how objects from your integrations are mapped to profiles when they are ingested. Customer Profiles provides default object type templates you can use that define how attributes in your source objects are mapped to the standard objects in Customer Profiles. You can also use the object mappings that you've created from the PutProfileObjectType.



Object type Info

Select the objects you want to ingest and choose their object type to define how the objects are mapped to profiles.

Shopify objects

☑ Customer

Shopify-customer (default)

☑ Draft

Shopify-draft (default)

☑ Order

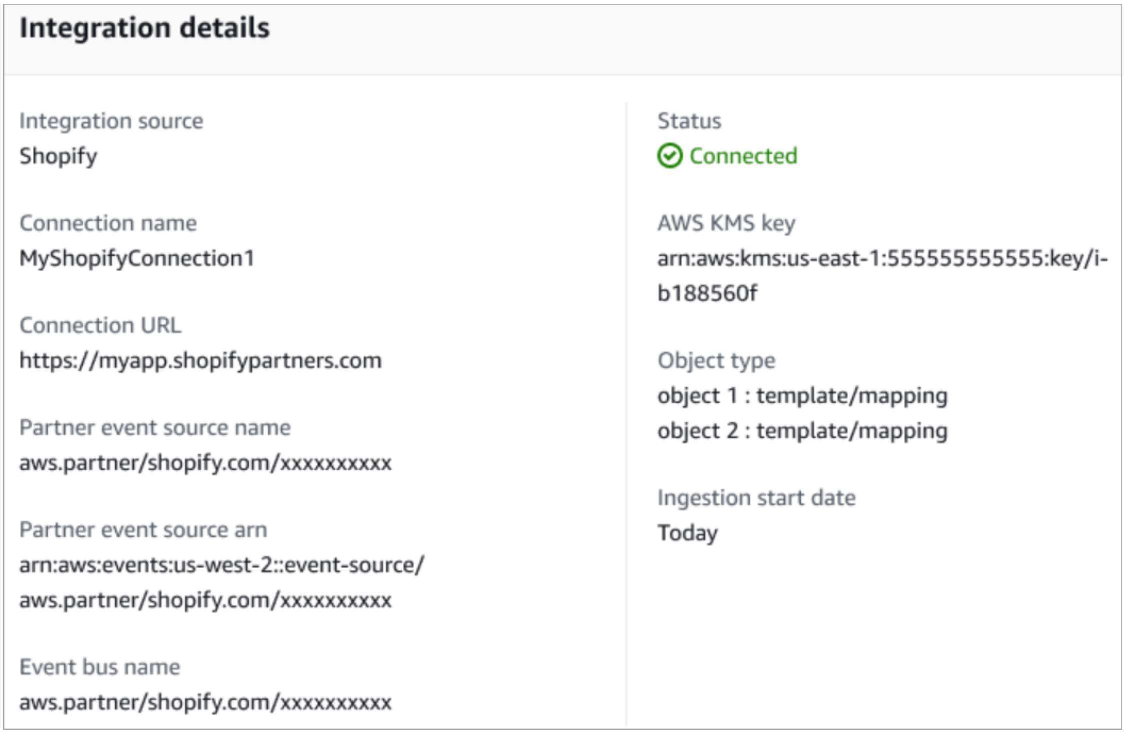
Shopify-order (default)

10. For the **Ingestion start date**, Customer Profiles starts ingesting records created after the integration is added.

    Note
    If you need historical records, you can use Amazon S3 as an integration source to import them (p. 730).

11. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Add integration**.

    Note
    After adding this integration, you need to set up webhook subscriptions (p. 679) to allow events to start flowing into this integration.



Integration details

Integration source
Shopify

Connection name
MyShopifyConnection1

Connection URL
https://myapp.shopifypartners.com

Partner event source name
aws.partner/shopify.com/xxxxxxxxxx

Partner event source arn
arn:aws:events:us-west-2::event-source/aws.partner/shopify.com/xxxxxxxxxx

Event bus name
aws.partner/shopify.com/xxxxxxxxxx

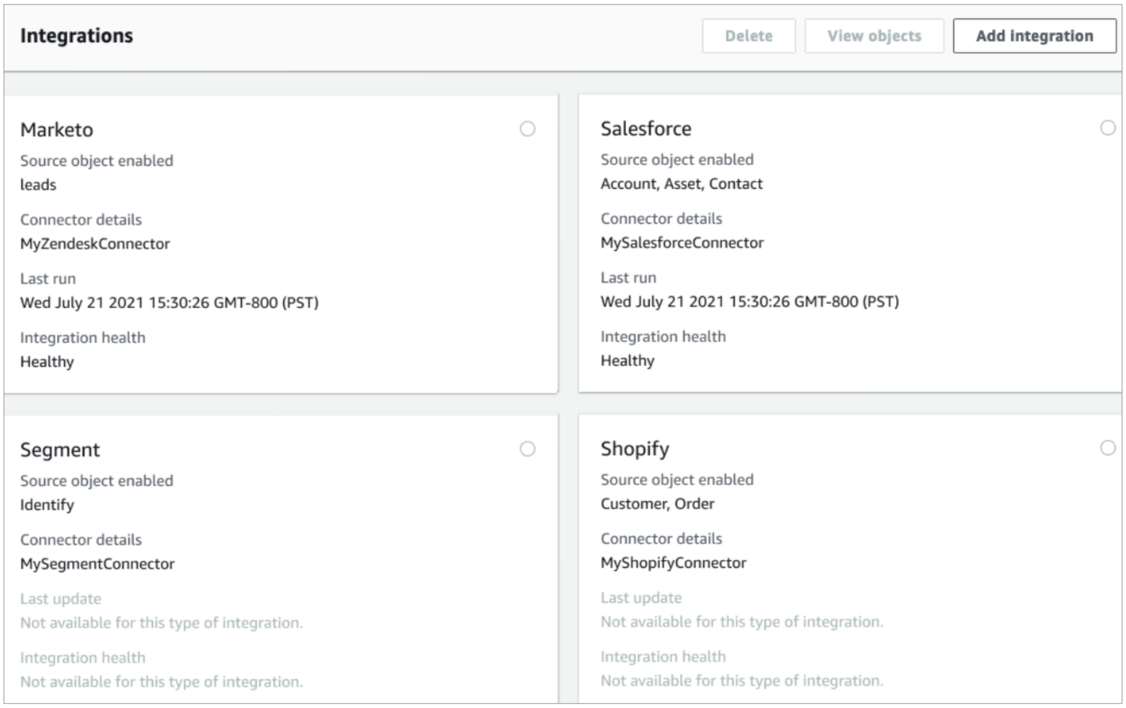
Status
Connected

AWS KMS key
arn:aws:kms:us-east-1:555555555555:key/i-b188560f

Object type
object 1 : template/mapping
object 2 : template/mapping

Ingestion start date
Today

12. After the integration is set up, back on the **Customer profiles configuration** page, the **Integrations** page displays which integrations are currently set up. The **Last run** and **Integration health** are not currently available for this type of integration.



Marketo
Source object enabled
leads
Connector details
MyZendeskConnector
Last run
Wed July 21 2021 15:30:26 GMT-800 (PST)
Integration health
Healthy

Salesforce
Source object enabled
Account, Asset, Contact
Connector details
MySalesforceConnector
Last run
Wed July 21 2021 15:30:26 GMT-800 (PST)
Integration health
Healthy

Segment
Source object enabled
Identify
Connector details
MySegmentConnector
Last update
Not available for this type of integration.
Integration health
Not available for this type of integration.

Shopify
Source object enabled
Customer, Order
Connector details
MyShopifyConnector
Last update
Not available for this type of integration.
Integration health
Not available for this type of integration.

To see what data is being sent, choose the integration and then choose **View objects**.

13. Go to the next step to use the API to set up **webhook subscriptions** so events can start flowing into this integration.

Set up webhook subscriptions

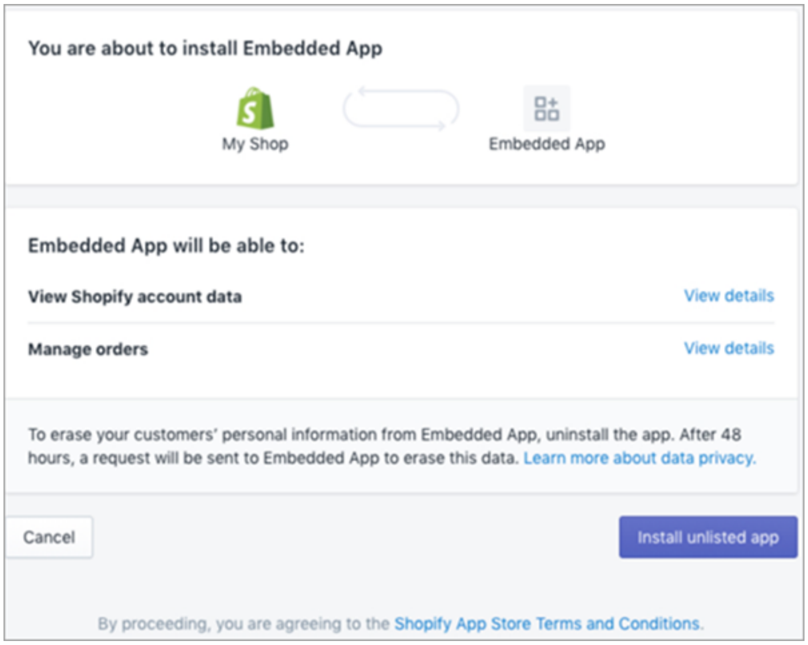
1. Use the following URL to make sure your app has the required permissions:

```
https://{shop}.myshopify.com/admin/oauth/authorize?
client_id={api_key}&scope={scopes}&redirect_uri={redirect_uri}&state={nonce}
```

   Where:

   - `shop` is the name of your Shopify store.
   - `api_key` is the API Key of your Shopify app. You can find this on the Shopify **App** details page.
   - `scopes` should have the value `read_customers,read_orders,read_draft_orders`.
   - `redirect_uri` is the redirect URI you specified for your app when you created it. For our purposes it can be any valid URL.
   - `nonce` can be any unique value to identify a given authorization request from others. We recommend using a timestamp.

   After you have constructed the URL, paste it into your browser. An installation/authorization page similar to the following image is displayed, asking the store owner to give permissions for the defined scope.



You are about to install Embedded App

Embedded App will be able to:

View Shopify account data

Manage orders

To erase your customers' personal information from Embedded App, uninstall the app. After 48 hours, a request will be sent to Embedded App to erase this data. Learn more about data privacy.

By proceeding, you are agreeing to the Shopify App Store Terms and Conditions.

2. Choose **Install unlisted app** to install and authorize the app on behalf of your store.

   You will be taken to the redirect URI that you entered with an authorization code appended to redirect URI as a query parameter. For example:

```
https://example.org/some/redirect/uri?
code={authorization_code}&hmac=da9d83c171400a41f8db91a950508985&host={base64_encoded_hostname}&time
```

3. Copy the `authorization_code` from this URI. You're going to use it to get a permanent access token in the next steps.

4. Go to whatever tool you use to make API calls. For example, CURL or POSTMAN.
5. To get a permanent access token, make a POST request to the Shopify `Admin` API to this endpoint:

   ```
   https://{shop}.myshopify.com/admin/oauth/access_token
   ```

   with the following request body:

   ```
   {
       "code": "authorization_code_received_from_redirect_uri",
       "client_id": "your_app_api_key",
       "client_secret": "your_app_api_secret"
   }
   ```

   This request returns the following response:

   ```
   {
       "access_token": "permanent_access_token",
       "scope": "read_customers,read_orders,read_draft_orders"
   }
   ```
6. Note the `access_token`. This is a permanent token that has the provided scope from a previous step. Now you are ready to create webhook subscriptions.
7. For the following API calls, make sure you set the HTTP header key `X-Shopify-Access-Token` to the `access_token` you received from the earlier call's response.
8. To setup webhook subscriptions, make the following POST request for each of the `topic` values listed in the next step:

   Endpoint: `https://{shop}.myshopify.com/admin/api/2021-04/webhooks.json`

   Request Body:

   ```
   {
       "webhook": {
           "topic": "replace_this_with_one_of_the_topics_in_the_list_below",
           "address":
    "this_is_the_event_source_arn_generated_when_you_created_the_event_integration",
           "format": "json"
       }
   }
   ```
9. For each subscription replace the value for `topic` with the following values:

   - `customers/create`
   - `customers/enable`
   - `customers/update`
   - `draft_orders/create`
   - `draft_orders/update`
   - `orders/cancelled`
   - `orders/create`
   - `orders/fulfilled`
   - `orders/paid`
   - `orders/partially_fulfilled`
   - `orders/updated`

You're now all set to receive events from your Shopify store. Next, verify your Shopify integration.

Verify your Shopify integration

1. Sign in as Admin to your Shopify Store.
2. In the left navigation menu, choose **Customers**.
3. Select **Add Customer**.
4. Enter your customer details. Be sure to enter a phone number and email. These don't have to belong to a real customer. You will delete this customer entry after verifying the integration.
5. Save the customer object.
6. The event delivery should be almost instantaneous but allow a minute for it to be delivered and to create a customer profile.
7. Open the Amazon Connect agent experience and look up the user by the email or phone number you entered into the Shopify Store. You should be able to see the customer profile with the same email or phone number.
8. If you cannot see the customer profile, then there is a problem with your integration. To troubleshoot:

    1. Go to the Amazon EventBridge console.
    2. Check whether the EventSource is Active and the matching EventBus exists and is running.

    If these are working, contact AWS Support for assistance investigating the issue.

Monitor your Customer Profiles integrations

After your connection is established, if it stops working, delete the integration and then re-establish it.

What to do if objects aren't being sent

If an object fails to be sent, choose **Flow details** to learn more about what's gone wrong.

You may need to delete the configuration and re-connect to the external application.

Delete/stop Customer Profiles integrations

If at any time you want to stop the ingestion of customer profile data, choose the application and then choose **Delete**.

- To delete customer profiles data for a specific integration, use the `DeleteObjectType` API.
- To delete the integrations, customer profiles, and all the customer profile data, use the `DeleteDomain` API.

To re-enable the ingestion of customer profile data, go through the setup steps again.

Object type mapping

Contents

Concepts and terminology for customer object type mappings

The following terminology and concepts are central to your understanding of custom object type mappings.

Standard profile object

A *standard profile object* is a predefined object that all profiles contain.

A standard profile object contains standard fields, such as phone numbers, email addresses, name and other standard data. This data can be retrieved in a standard format regardless of the source (for example, Salesforce, ServiceNow, or Marketo).

Profile object

A *profile object* is a single unit of information known about a profile. For example, the information about a phone call, a ticket, a case, or even a click-stream record from a web site.

A single profile object can be up to 250 KB and can be any structured JSON document.

- Every profile object has a type. For example, the profile object can be an Amazon Connect contact record, ServiceNow Users, or Marketo Leads.
- The type refers to the object type mapping.
- The object type mapping defines how that specific object should be ingested into Customer Profiles.

Profile

A *profile* contains all the information known about a specific customer or contact. It includes a single standard profile object and any number of additional profile objects.

Object type mapping

The *object type mapping* tells Customer Profiles how to ingest a specific type of data. It provides Customer Profiles with the following information:

- How data should be populated from the object and ingested into the standard profile object.
- What fields should be indexed in the object and how those fields should then be used to assign objects of this type to a specific profile.

Mapping template

A *mapping template* is a predefined object type mapping included with the Customer Profiles service.

Customer Profiles includes mapping templates for Amazon Connect contact records, Salesforce Accounts, ServiceNow Users, and Marketo Leads. For a complete list of available mapping templates, use the ListProfileObjectTypeTemplates API.

With mapping templates you can quickly ingest data from well known sources without having to specify any additional information.

Create an object type mapping

An object type mapping tells Customer Profiles how to ingest a specific type of data from a source application—such as Salesforce, Zendesk, or S3—into a unified standard profile object. You can then display data in that object (for example, customer address and email) to your agents using the agent application.

The object type mapping provides Customer Profiles with the following information:

- How data should be populated from the object and ingested into the standard profile object.
- What fields should be indexed in the object and how those fields should then be used to assign objects of this type to a specific profile.

There are two ways you can create an object type mapping:

- Use the Amazon Connect console. The user interface makes data mapping features readily accessible. For example, you can add custom attributes, and define search and unique identifiers for contact models. No coding required!
- Use the Customer Profiles API. For more information, see the Amazon Connect Customer Profiles API Reference.

This topic explains how to create a mapping using the Amazon Connect console.

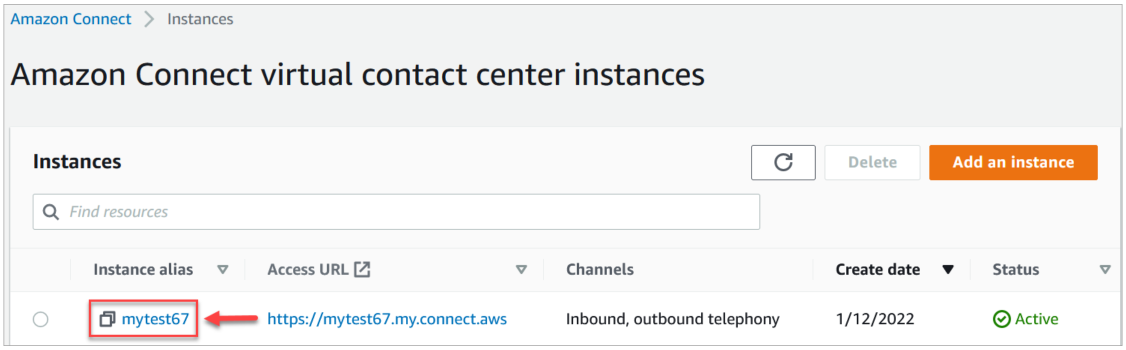
Create a data mapping using the Amazon Connect console

Amazon Connect provides a no-code experience for mapping customer data from homegrown and third-party applications with Amazon S3, Salesforce, ServiceNow, Zendesk, and Marketo.

To create a data mapping, you define an object type mapping that describes what the custom profile object looks like. This mapping defines how fields from your data can be used to either populate fields in the standard profile or how they can be used to assign the data to a specific profile.

Step 1: Set up data mapping

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



Amazon Connect > Instances

Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Customer profiles**, **Data mappings**.
4. Choose **Create data mapping** to get started.

5. At the **Set up data mapping** page, in the **Description** section, add a name that will help you identify the source or purpose of this mapping. This is the meta-data of the object type.
6. In the **Data source** section:

   a. Choose where the data is coming from, such as Salesforce or Zendesk. Based on your selection, Amazon Connect automatically selects the available destinations based on the predefined template.

   b. Choose the source object. This is used for you to build your unified profile.

   c. In the **Mapping destination** section, choose the data that you want to use to build your unified customer profile. This information can be surfaced to your contact flows and agents to personalize the interactions with contacts.

      For more information about supported mapping destinations, see About mapping destinations (p. 686).

   d. In the **Additional options** section, you can choose when to opt out of creating new profiles, and how long to retain them. These options help you manage costs.

      > **Note**
      > By default the domain retention period is 366 days. To change the retention period set on your domain, use the UpdateDomain API.

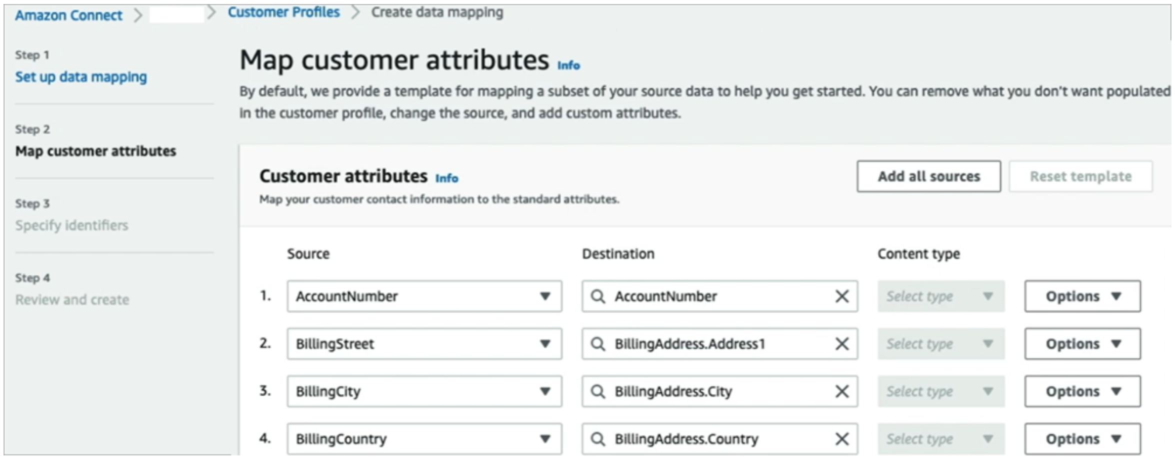
7. If you chose a source other than S3, in the **Establish a connection with** *`application`* section, choose an existing Amazon AppFlow or Amazon EventBridge connection to connect your data, or create a new connection. You can create a new connection by entering details about your account for this data source.

   After the connection is established, you will choose the objects that you want to ingest from your data source.
8. Choose **Next**.

Step 2: Map attributes

On the **Map *type* attributes** page, you'll see the field mappings table filled with the predefined template, based on the mapping destination. For example, it's filled with customer, product, case, or order attributes. You can change the predefined template by choosing an attribute (such as AccountNumber) and then selecting a different destination, or enter one of your own custom attributes.

The following image shows an example of the page filled with customer attributes from the template.



Amazon Connect > > Customer Profiles > Create data mapping

Step 1
Set up data mapping

Step 2
Map customer attributes

Step 3
Specify identifiers

Step 4
Review and create

Map customer attributes Info

By default, we provide a template for mapping a subset of your source data to help you get started. You can remove what you don't want populated in the customer profile, change the source, and add custom attributes.

Customer attributes Info

Map your customer contact information to the standard attributes.

	Source	Destination	Content type	
1.	AccountNumber	AccountNumber	Select type	Options
2.	BillingStreet	BillingAddress.Address1	Select type	Options
3.	BillingCity	BillingAddress.City	Select type	Options
4.	BillingCountry	BillingAddress.Country	Select type	Options

You can remove what you don’t want populated in the customer profile, change the source, and add custom attributes.

This mapping uses your data source to populate customer contact information, such as a phone number in the customer profile. It uses attributes from the standard profile template.

> **Tip**
> If you choose to add custom attributes, the destination will always have the prefix `Attributes.` added to it. This enables Amazon Connect to recognize that it is a custom attribute.

Step 3: Specify identifiers

On the **Specify identifiers** page, complete the following sections. Depending on what data your mapping, it's possible not all of these will appear on your page.

- **Unique identifier**: You must have a unique identifier for your data in order to avoid an error when it is ingested. This identifier is also known as the unique key. Customer Profiles uses it to distinquish this data from other data source objects, and to index for search and update data.

  There can be only one unique identifier.
- **Customer identifier**: You must have at least one customer identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the profile key.

  Customer Profiles uses it to determine if the data case be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

  You can have mutliple customer identifiers.
- **Product identifier**: You must have at least one product identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the asset key.

  Customer Profiles uses it to distinquish this data from other customer product purchase data. It is also used to determine if the data can be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

  You can have multiple product identifiers.
- **Case identifier**: You must have at least one case identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the case key.

  Customer Profiles uses it to distinquish this data from other customer case data. It is also used to determine if the data can be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

  You can have multiple case identifiers.
- **Order identifier**: You must have at least one order identifier for your data in order to avoid an error when it is ingested. The identifier is also known as the order key.

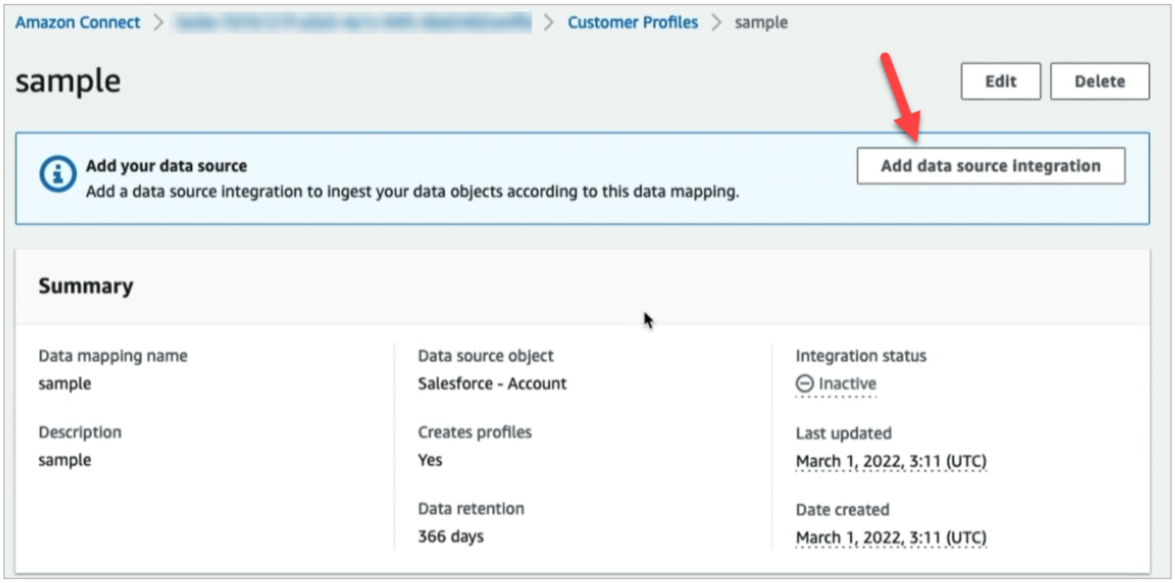
  Customer Profiles uses it to distinquish this data from other customer order data. It is also used to determine if the data can be associated to an existing profile or used to create a new profile by searching other profiles for this identifier.

  You can have multiple order identifiers.
- **Additional search attributes - optional**: You can choose attributes in your data source object that you want to index to be searchable. By default, all your identifiers are indexed.
- **Data object timestamp**: The data object timestamp is used to resolve profile conflicts when Identity Resolution is enabled for consolidating similar profiles. When two or more similar profiles have conflicting records, the records from the profile with the most recently updated timestamp will be used.

  You can choose an attribute in your object to reference for when your object was last updated.

Step 4: Review and create

After the data mapping is created, you can choose **Add data source integration** to use this object type.



Amazon Connect > [redacted] > Customer Profiles > sample

sample

Add your data source

Add a data source integration to ingest your data objects according to this data mapping.

Summary

Data mapping name
sample

Description
sample

Data source object
Salesforce - Account

Creates profiles
Yes

Data retention
366 days

Integration status
Inactive

Last updated
March 1, 2022, 3:11 (UTC)

Date created
March 1, 2022, 3:11 (UTC)

About mapping destinations

A mapping destination is your mapping from a source to a standard definition that is already defined in Amazon Connect.

The following table lists the supported mapping destinations.

Source object	Destination: Customer, Product, Order, Case
S3	Any
Salesforce-Account	Customer
Salesforce-Contact	Customer
Zendesk-users	Customer
Marketo-leads	Customer
Servicenow-sys_user	Customer
Segment-Identify	Customer
Segment-Customer	Customer
Shopify-Customer	Customer
Shopify-DraftOrder	Order
Salesforce-Asset	Product
Zendesk-tickets	Case
Servicenow-task	Case
Servicenow-incident	Case

Object type mapping requirements

The following information needs to be in your object type mapping so Customer Profiles can process the incoming data:

- A definition of all the fields in the ingested object that should be mapped to the standard profile, or used for assigning the data to a profile. This tells Customer Profiles which fields in the ingested **source** object should be mapped to given fields in the standard profile object.
- Which fields in the source object from your custom data should be indexed and how.

  When the source data is ingested by Customer Profiles, the indexed fields determine:
  - Which profile a specific object belongs to.
  - Which objects are related to each other and should be placed in the same profile. For example, an account number or a contact ID in a contact record.
  - What values can be used to find a profile. For example, the contact's name can be indexed. This would allow agents to find all profiles that belong to customers with a specific name.

Key requirements

You must define at least one key. Customer Profiles uses this key to map your custom profile object to a profile.

The custom profile object mapping also needs at least one key that uniquely identifies the object so that it can be updated by specifying the same value of this field (these requirements can be satisfied with a single key).

Each key can be made up of one or more fields.

Field requirements

A field definition specifies how to read a value for that field name from a source object. The field definition also specifies what kind of data is stored in the field.

Object type names can be any alpha numerical string or the '-' and '_' character, they also cannot start with a '_' character, which is used for reserved standard object types.

Object type mapping definition details

The object type mapping definition has two parts: the field definition and the key definition.

> **Tip**
> To learn how to create an object type mapper, see this blog post: Unify and organize customer information with Amazon Connect Customer Profiles with the pre-built Amazon S3 connector. Or, check out this video on YouTube: How to Integrate Customer Profile Data into your Contact Center Experiences.

Field definition details

The field definition defines the source, destination (target), and type of field. For example:

```
"Fields": {
        "{fieldName}": {
            "Source": "{source}",
            "Target": "{target}",
            "ContentType": "{contentType}"
        }, ...
```

```
    }, ...
```

- `Source`: This can be a JSON accessor for the field or a Handlebar macro for generating the value of the field.

  The source object being parsed is named `_source` so all fields in the source fields need to be prefaced by this string. Only the `_source` object is supported.

  Use the Handlebar macro solution for generating constants and combining multiple source object fields into a single field. This is useful for indexing.
- `Target`: Specifies where in a standard object type the data of this field should be mapped.

  Populating the standard profile allows you to use data ingested from any data source with applications built on top of Customer Profiles without any specific knowledge of the format of the data being ingested.

  This field is optional. You might want to define fields solely for the purpose of including them in a key.

  The format of this field is always a JSON accessor. The only supported target object is `_profile`.
- `ContentType`: The following values are supported STRING, NUMBER, PHONE_NUMBER, EMAIL_ADDRESS, NAME. If no `ContentType` is specified STRING is assumed.

  `ContentType` is used to determine how to index the value so agents can search for it. For example, if `ContentType` is set to PHONE_NUMBER, a phone number is processed so agents can search for it in any format: the string "+15551234567" matches "(555)-123-4567".

Key definition details

A key contains one or more fields that together define a key that can be used to search for objects (or the profiles they belong to) using the SearchProfiles API. The key can also be defined to uniquely identify a profile or uniquely identify the object itself.

```
"Keys": {
        "{keyName}": [{
            "StandardIdentifiers": [...],
            "FieldNames": [ "{fieldname}", ...]
        }], ...
    }, ...
```

Key names are global to a domain. If you have two keys, with the same name in two different object type mappings:

- Those keys should occupy the same namespace
- They can be used to potentially link profiles together between different objects. If they match between the objects, Customer Profiles places the two objects in the same profile.

To phrase this in another way: keys should have the same key name in a domain if, and only if, the same value means that they are related. For example, a phone number specified in one type of object would be related to the same phone number specified in another type of object. An internal identifier specified for an imported object from Salesforce might not be related to another object imported from Marketo, even if they have exactly the same value.

Keys definitions are used in two ways:

- Inside of Customer Profiles during ingestion, they are used to figure out what profile the object should be assigned to.

- They allow you to use the SearchProfiles API to search for the key value and find the profile.

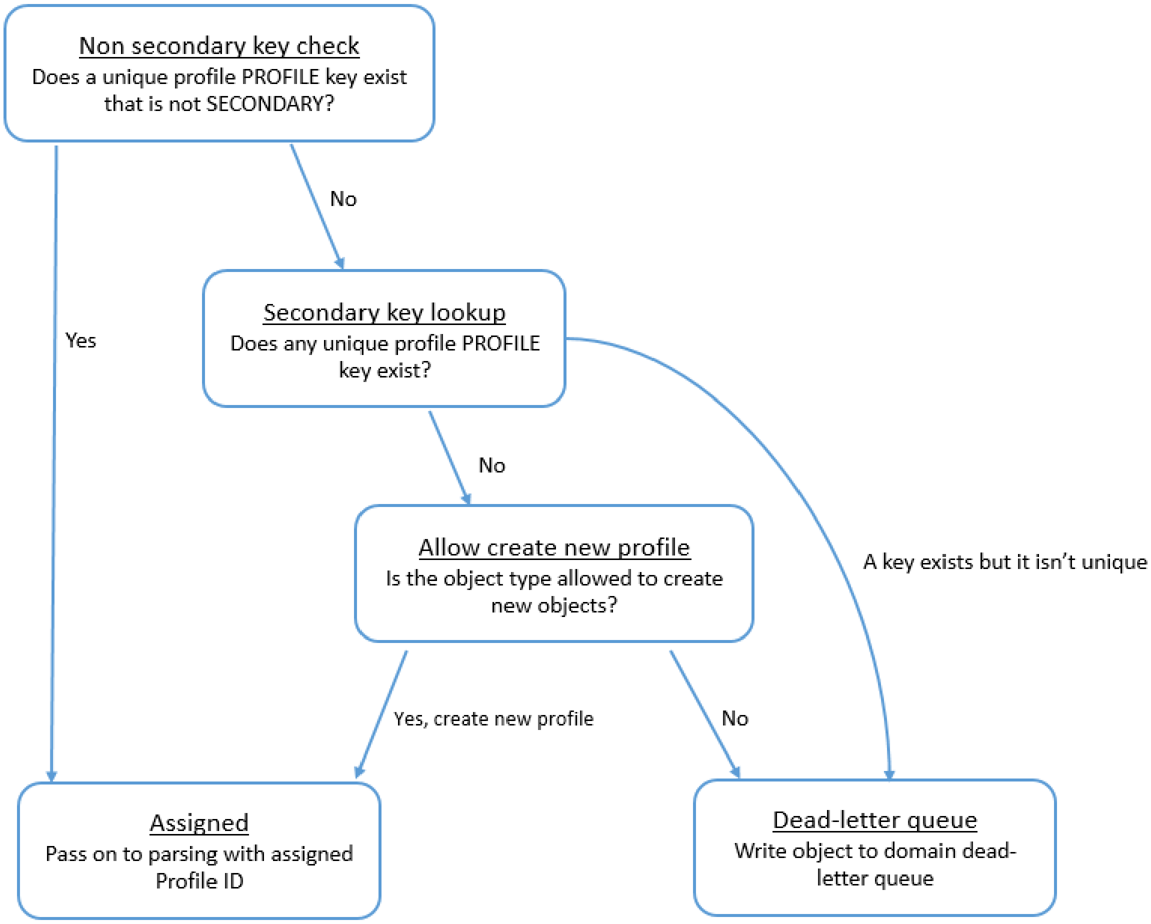
Standard identifiers

Standard identifiers allow you to set attributes on the key. Decide which identifiers to use based on how you want the data to be ingested in the profiles. For example, you mark phone number with the identifier PROFILE. This means phone number is to be treated as unique identifier. If Customer Profiles gets two contacts with the same phone number, the contacts are going to be merged into a single profile.

Identifier name	Description
UNIQUE	This identifier must be specified by exactly one index for each object type. This key is used to uniquely identify objects of the object type for either fetching them or if needed update a submitted object at a later date. All the fields that make up the UNIQUE keys are required to be specified when submitting a new object or it is rejected.
PROFILE	This identifier means that this key uniquely identifies a profile. When this identifier is specified, it means that during ingestion Custom Profiles looks for any profile that has this key associated with it. • If a profile is found, then the object is assigned to that profile. • If more than one profile is found when searching for this key, the match is rejected. (Only keys that uniquely identify a profile should be used as unique keys except for special circumstances.)
LOOKUP_ONLY	This identifier indicates the key is not stored after ingesting the object. The key is only to be used for determining the profile during ingestion. The key value is not not associated with the profile during ingestion, which means it can't be used to allow searching for it or matching later ingested objects to the same key.
NEW_ONLY	If the profile does not already exist before the object is ingested, the key is associated with the profile. Otherwise the key is only used for matching objects to profiles.
SECONDARY	During the matching of an object to a profile, Customer Profiles first looks up all PROFILE keys that do not have the SECONDARY identifier. These are considered first. SECONDARY keys are only considered if no matching profile is found using these keys.

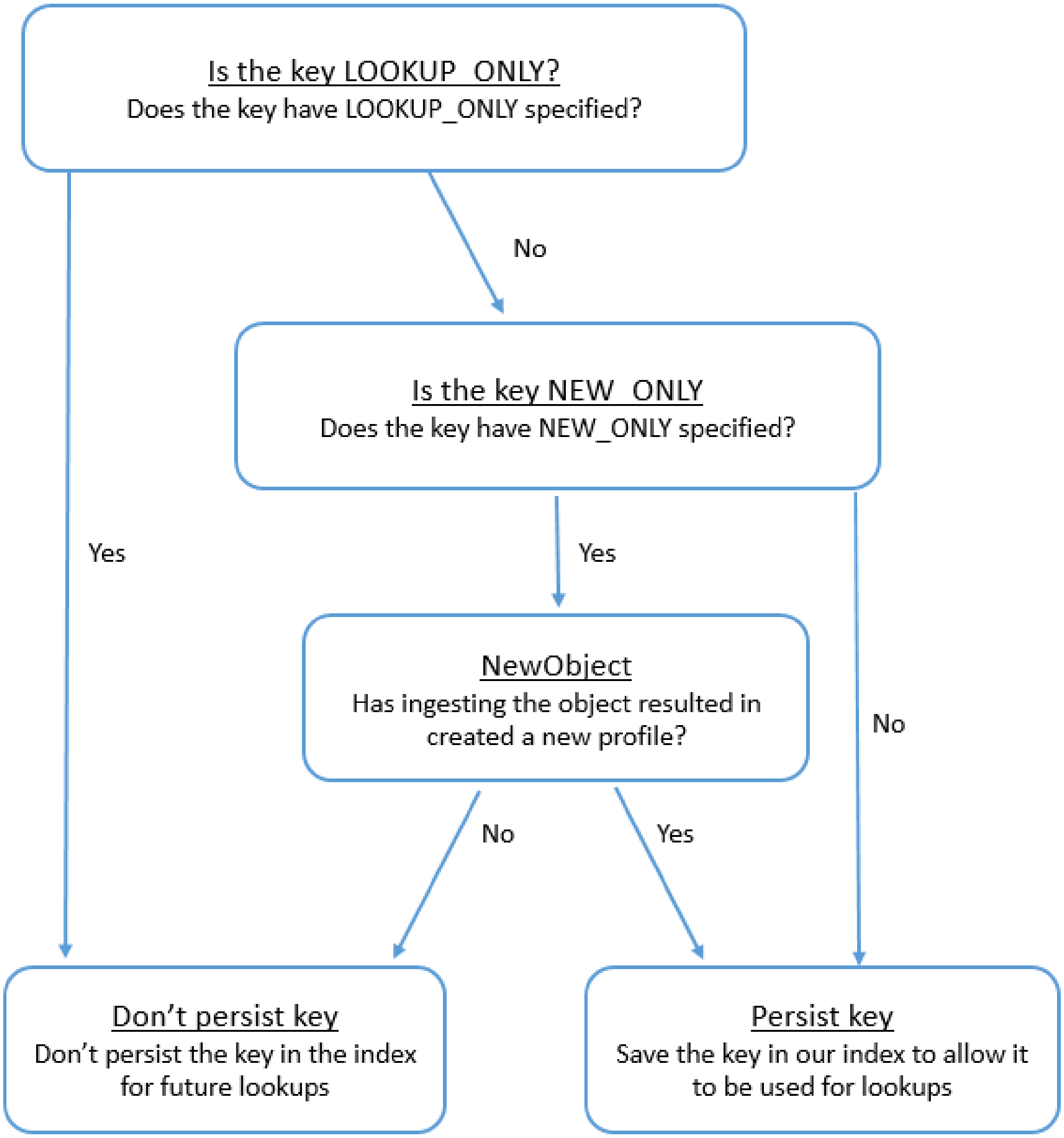
How profile assignment works using key definitions

When Customer Profiles ingests the custom object mappings, it processes the key definitions. The following diagram shows how it processes standard identifiers in key definitions to determine which profile to assign the object to.


Non secondary key check
Does a unique profile PROFILE key exist that is not SECONDARY?
No
Yes
Secondary key lookup
Does any unique profile PROFILE key exist?
No
Allow create new profile
Is the object type allowed to create new objects?
A key exists but it isn't unique
Yes, create new profile
No
Assigned
Pass on to parsing with assigned Profile ID
Dead-letter queue
Write object to domain dead-letter queue

How keys are added to the index for future look ups

The following diagram shows how Customer Profiles processes the standard identifiers to determine whether to persist the key.


Is the key LOOKUP_ONLY?
Does the key have LOOKUP_ONLY specified?
No
Is the key NEW_ONLY
Does the key have NEW_ONLY specified?
Yes
Yes
NewObject
Has ingesting the object resulted in created a new profile?
No
No
Yes
Don’t persist key
Don’t persist the key in the index for future lookups
Persist key
Save the key in our index to allow it to be used for lookups

Additional properties of object types

A property type defines which key should be used to encrypt any data of the object type.

There is an option that defines if new profiles can be created by the ingestion of this object. Normally when an object is ingested that cannot be matched to an existing profile, a new profile is created as long as this option is true. If it is not true then the ingested object is created and written to the domain dead-letter queue.

It also contains how long data of this object type should be retained in Customer Profiles.

> **Note**
> Retention on individual objects is set at the time of ingestion of data. Changing the retention for a specific object type only applies to new data being ingested. It does not apply to existing data already ingested.

Inferred profiles

When a profile is created by the ingestion of an object that has no fields, the standard profile object of this new profile is empty. This empty standard profile object is an **inferred profile**.

When creating an inferred profile, the following two fields are populated in the standard object from the profile object, if available.

- If there is any field defined with the content type of `EMAIL_ADDRESS` in the ingested object then this value will be populated into the `EmailAddress` field of the standard profile.
- If there is any field with the content type of `PHONE_NUMBER` in the ingested object then this value will be populated into the `PhoneNumber` field of the standard profile.

Values for these fields are populated into the standard profile even if the fields do not have a target defined in the field definition.

Change behavior of inferred profiles to automatically associate the contact record with one profile found

You can change the behavior of inferred profiles so contact records are automatically associated to one profile found.

Run the following command on the CLI:

```
aws customer-profiles put-profile-object-type --domain-name {domain} --object-type-name CTR --description "No inferred contact record profiles" --template-id CTR-NoInferred
```

In order to re-enable inferred profile behavior, run the following command on the CLI:

```
aws customer-profiles put-profile-object-type --domain-name {domain} --object-type-name CTR --description "No inferred contact record profiles" --template-id CTR
```

Examples of object type mappings

An object type mapping that generates a profile

The following example shows data that populates the standard profile.

Following is the incoming object:

```
{
  "account": 1234,
  "email": "john@examplecorp.com",
  "address": {
     "address1": "Street",
     "zip": "Zip",
     "city": "City"
  },
  "firstName": "John",
  "lastName": "Doe"
}
```

The following code shows that incoming object mapping into a standard profile object and indexing `PersonalEmailAddress`, `fullName`, and `accountId`, which is a unique key.

```
{
    "Fields": {
        "accountId": {
            "Source": "_source.account",
            "Target": "_profile.AccountNumber",
            "ContentType": "NUMBER"
        },
        "shippingAddress.address1": {
            "Source": "_source.address.address1",
            "Target": "_profile.ShippingAddress.Address1"
        },
        "shippingAddress.postalCode": {
            "Source": "_source.address.zip",
            "Target": "_profile.ShippingAddress.PostalCode"
        },
        "shippingAddress.city": {
            "Source": "_source.address.city",
            "Target": "_profile.ShippingAddress.City"
        },
        "personalEmailAddress": {
            "Source": "_source.email",
            "Target": "_profile.PersonalEmailAddress",
            "ContentType": "EMAIL_ADDRESS"
        },
        "fullName": {
            "Source": "{{_source.firstName}} {{_source.lastName}}"
        },
        "firstName": {
            "Source": "_source.firstName",
            "Target": "_profile.FirstName"
        },
        "lastName": {
            "Source": "_source.lastName",
            "Target": "_profile.LastName"
        }
    },
    "Keys": {
        "_email": [
            {
                "FieldNames": ["personalEmailAddress"]
            }
        ],
        "_fullName": [
            {
                "FieldNames": ["fullName"]
            }
        ],
        "_account": [
            {
                "StandardIdentifiers": ["PROFILE","UNIQUE"],
                "FieldNames": ["accountId"]
            }
        ]
    }
}
```

Note that `email` and `fullname` are indexed, but they aren't used to search for the profile. The account is the unique key. It is required to specify the object. Any time an object with the same account ID is ingested it overwrites the previous object with the same account ID.

Several fields are populated in the standard profile object (see the fields that have `Target` defined).

An object type mapping that doesn't populate the standard profile

This example shows a more complicated use case. It ingests data related to a profile but it doesn't necessarily populate the standard profile object.

Following is the incoming object:

```
{
  "email": "john@examplecorp.com",
  "timestamp": "2010-01-01T12:34:56Z",
  "subject": "Whatever this is about",
  "body": "Body of ticket"
}
```

Following is one way of mapping this data:

```
{
    "Fields": {
        "email": {
            "Source": "_source.email",
            "ContentType": "EMAIL_ADDRESS"
        },
        "timestamp": {
            "Source": "_source.timestamp",
            "Target": "_profile.ShippingAddress.Address1"
        }
    },
    "Keys": {
        "_email": [
            {
                "StandardIdentifiers": ["PROFILE","LOOKUP_ONLY"],
                "FieldNames": ["email"]
            }
        ],
        "ticketEmail": [
            {
                "StandardIdentifiers": ["PROFILE","SECONDARY","NEW_ONLY"],
                "FieldNames": ["email"]
            }
        ],
        "uniqueTicket": [
            {
                "StandardIdentifiers": ["UNIQUE"],
                "FieldNames": ["email","timestamp"]
            }
        ]
    }
}
```

This example ingests the data and, at first lookup, it ingests the email address.

- If the email address matches a single profile, it is used to attach the data to that specific profile. The unique identifier for the ticket is comprised of the email and the timestamp since no other unique identifier exists.

- If no profile exists with the specified email, a new profile is created with the single field of `EmailAddress` filled in. The ingested object is attached to this new **inferred profile**. The two searchable keys that can find the profile are `_email` and `uniqueTicket`.
- If more than one profile exists with the specified email address, a new profile is created with the single field of `EmailAddress` filled in and the object is attached to this new profile. This profile is created with the `ticketEmail` key defined, in addition to `_email` and `uniqueTicket`. Any subsequent tickets from that email are assigned to this new **inferred profile**. The reason for this is that the `_email` key is referring to three profiles and is thus discarded, however the `ticketEmail` key only refers to a single profile (the new inferred one) and is still valid.
- In cases where a new **inferred profile** is created, the `EmailAddress` field is populated from the first object that created it.

Implicit profile object types

You can use any object type that matches the name of a template ID (as returned by the ListProfileObjectTypeTemplates API) without explicitly defining it. The object type will exactly match the definition of the template definition of this object type. If an explicit object type is defined, it replaces the implicit one.

Implicit object types are included in the ListProfileObjectTypes API or returned by GetProfileObjectType operations, but they can still be deleted if you want to remove all data ingested from that object type.

Object type mapping for the standard profile

The topics in this section provide the standard profile definition, and the object type mapping from external applications to the standard profile.

Contents

Amazon AppFlow access requirements

Following are the Amazon AppFlow access requirements to create and delete Zendesk, Marketo, Salesforce, and ServiceNow integrations:

- appflow:CreateFlow
- appflow:DeleteFlow

Amazon AppIntegrations access requirements

Following are the Amazon AppIntegrations access requirements to create and delete Segment and Shopify integrations:

- app-integrations:GetEventIntegration
- app-integrations:ListEventIntegrationAssociations
- app-integrations:CreateEventIntegrationAssociation
- app-integrations:DeleteEventIntegrationAssociation

Amazon EventBridge access requirements

Following are the Amazon EventBridge access requirements to create and delete Segment and Shopify integrations:

- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:DeleteRule
- events:RemoveTargets

Standard profile definition

The following table lists all the fields in the Customer Profiles standard profile. object.

Standard profile field	Data type	Description
ProfileId	String	The unique identifier of a customer profile.
AccountNumber	String	A unique account number that you have given to the customer.
AdditionalInformation	String	Any additional information relevant to the customer's profile.
PartyType	String	The type of profile used to describe the customer. Valid values: INDIVIDUAL | BUSINESS | OTHER
BusinessName	String	The name of the customer's business.
FirstName	String	The customer's first name.
MiddleName	String	The customer's middle name.
LastName	String	The customer's last name.
BirthDate	String	The customer's birth date.

Standard profile field	Data type	Description
Gender	String	The gender with which the customer identifies.
PhoneNumber	String	The customer's phone number, which has not been specified as a mobile, home, or business number.
MobilePhoneNumber	String	The customer's mobile phone number.
HomePhoneNumber	String	The customer's home phone number.
BusinessPhoneNumber	String	The customer's business phone number.
EmailAddress	String	The customer’s email address, which has not been specified as a personal or business address.
BusinessEmailAddress	String	The customer’s business email address.
Address	Address	A generic address associated with the customer that is not mailing, shipping, or billing.
ShippingAddress	Address	The customer's shipping address.
MailingAddress	Address	The customer's mailing address.
BillingAddress	Address	The customer's billing address.
Attributes	String-to-string map	Key-value pair of attributes of a customer profile.

Address data type

Standard profile field	Data type	Description
Address1	String	The first line of a customer address.
Address2	String	The second line of a customer address.
Address3	String	The third line of a customer address.
Address4	String	The fourth line of a customer address.
City	String	The city in which the customer lives.

Standard profile field	Data type	Description
Country	String	The country in which the customer lives.
County	String	The county in which the customer lives.
PostalCode	String	The postal code of the customer address.
Province	String	The province in which the customer lives.
State	String	The state in which the customer lives.

Mapping Salesforce objects to the standard profile

This topic lists which fields in Salesforce objects map to fields inthe standard profile object in Customer Profiles.

Salesforce-Account object

Following is a list of all the fields in a Salesforce-Account object. The fields in your Salesforce-Account object may vary depending on the configuration of your Salesforce instance.

- Id
- IsDeleted
- MasterRecordId
- Name
- Type
- ParentId
- BillingStreet
- BillingCity
- BillingState
- BillingPostalCode
- BillingCountry
- BillingLatitude
- BillingLongitude
- BillingGeocodeAccuracy
- BillingAddress.City
- BillingAddress.Country
- BillingAddress.geocodeAccuracy
- BillingAddress.latitude
- BillingAddress.longitude
- BillingAddress.postalCode
- BillingAddress.state
- BillingAddress.street

- ShippingStreet
- ShippingCity
- ShippingState
- ShippingPostalCode
- ShippingCountry
- ShippingLatitude
- ShippingLongitude
- ShippingGeocodeAccuracy
- ShippingAddress.city
- ShippingAddress.country
- ShippingAddress.latitude
- ShippingAddress.longitude
- ShippingAddress.postalCode
- ShippingAddress.state
- ShippingAddress.street
- Phone
- Fax
- AccountNumber
- Website
- PhotoUrl
- Sic
- Industry
- AnnualRevenue
- NumberOfEmployees
- Ownership
- TickerSymbol
- Description
- Rating
- Site
- OwnerId
- CreatedDate
- CreatedById
- LastModifiedDate
- LastModifiedId
- SystemModstamp
- LastActivityDate
- LastViewedDate
- LastReferencedDate
- Jigsaw
- JigsawCompanyId
- CleanStatus
- AccountSource

- DunsNumber
- Tradestyle
- NaicsCode
- NaicsDesc
- YearStarted
- SicDesc
- DandbCompanyId
- IsBuyer

Mapping a Salesforce-Account object to a standard profile

A subset of the fields in the Salesforce-Account object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Salesforce-Account object to the standard profile. (The table includes the mapping for a Salesforce instance that has been configured to include Person fields.)

Salesforce-Account source field	Standard profile target field
Id	Attributes.sfdcAccountId
Name	BusinessName
Phone	PhoneNumber
BillingStreet	BillingAddress.Address1
BillingCity	BillingAddress.City
BillingState	BillingAddress.State
BillingCountry	BillingAddress.Country
BillingPostalCode	BillingAddress.PostalCode
ShippingStreet	ShippingAddress.Address1
ShippingCity	ShippingAddress.City
ShippingState	ShippingAddress.State
ShippingCountry	ShippingAddress.Country
ShippingPostalCode	ShippingAddress.PostalCode
IsPersonAccount	PartyType
PersonMobilePhone	MobilePhoneNumber
PersonHomePhone	HomePhoneNumber
PersonEmail	PersonalEmailAddress
PersonMailingAddress.Street	MailingAddress.Address1
PersonMailingAddress.City	MailingAddress.City

Salesforce-Account source field	Standard profile target field
PersonMailingAddress.State	MailingAddress.State
PersonMailingAddress.Country	MailingAddress.Country
PersonMailingAddress.PostalCode	MailingAddress.PostalCode
PersonBirthDate	BirthDate
PersonOtherStreet	Address.Address1
PersonOtherCity	Address.City
PersonOtherState	Address.State
PersonOtherCountry	Address.Country
PersonOtherPostalCode	Address.PostalCode
FirstName	FirstName
LastName	LastName
MiddleName	MiddleName
AccountNumber	AccountNumber

The Salesforce-Account customer data from the Salesforce object is associated with an Amazon Connect customer profile using the indexes in the following table.

Standard Index Name	Salesforce-Account source field
_salesforceAccountId	Id

For example, you can use `_salesforceAccountId` as a key name with the SearchProfiles API to find a profile. You can find the Salesforce-Account objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Salesforce-Account`.

Salesforce-Contact object

Following is a list of all the fields in a Salesforce-Contact object.

- Id
- IsDeleted
- MasterRecordId
- Accountd
- LastName
- FirstName
- Salutation
- Name
- OtherStreet
- OtherCity
- OtherState

- OtherPostalCode
- OtherCountry
- OtherLatitude
- OtherLongitude
- OtherGeocodeAccuracy
- OtherAddress.city
- OtherAddress.country
- OtherAddress.geocodeAccuracy
- OtherAddress.latitude
- OtherAddress.postalCode
- OtherAddress.state
- OtherAddress.street
- MailingStreet
- MailingCity
- MailingState
- MailingPostalCode
- MailingCountry
- MailingLatitude
- MailingLongitude
- MailingGeocodeAccuracy
- MailingAddress.city
- MailingAddress.country
- MailingAddress.geocodeAccuracy
- MailingAddress.latitude
- MailingAddress.longitude
- MailingAddress.postalCode
- MailingAddress.state
- MailingAddress.street
- Phone
- Fax
- MobilePhone
- HomePhone
- OtherPhone
- AssistantPhone
- ReportsToId
- Email
- Title
- Department
- AssistantName
- LeadSource
- Birthdate
- Description
- OwnerId

- CreatedDate
- CreatedById
- LastModifiedDate
- LastModifiedById
- SystemModstamp
- LastActivityDate
- LastCURequestDate
- LastCUUpdateDate
- LastViewedDate
- LastReferencedDate
- EmailBouncedReason
- EmailBouncedDate
- IsEmailBounced
- PhotoUrl
- Jigsaw
- JigawContactId
- CleanStatus
- IndividualId

Mapping a Salesforce-Contact object to a standard profile

A subset of the fields in the Salesforce-Contact object map to the standard profile object in Customer Profiles. The following table lists which fields can be mapped from the Salesforce-Contact object to the standard profile object.

Salesforce-Contact source field	Standard profile target field
Id	Attributes.sfdcContactId
AccountId	Attributes.sfdcAccountId
LastName	LastName
FirstName	FirstName
MiddleName	MiddleName
OtherStreet	Address.Address1
OtherCity	Address.City
OtherState	Address.State
OtherCountry	Address.Country
OtherPostalCode	Address.PostalCode
MailingStreet	MailingAddress.Address1
MailingCity	MailingAddress.City
MailingState	MailingAddress.State

Salesforce-Contact source field	Standard profile target field
MailingCountry	MailingAddress.Country
MailingPostalCode	MailingAddress.PostalCode
Phone	PhoneNumber
HomePhone	HomePhoneNumber
MobilePhone	MobilePhoneNumber
Email	EmailAddress
Birthdate	BirthDate

The Salesforce-Contact customer data from a Salesforce object is associated with an Amazon Connect customer profile using the indexes in the following table.

Standard Index Name	Salesforce-Contact source field
_salesforceContactId	Id
_salesforceAccountId	AccountId

For example, you can use `_salesforceAccountId` and `_salesforceContactId` as a key name with the SearchProfiles API to find a profile. You can find the Salesforce-Contact objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Salesforce-Contact`.

Mapping Zendesk objects to the standard profile

This topic lists which fields in Zendesk objects map to fields in the standard profile in Customer Profiles.

Zendesk-users object

Following is a list of all the fields in a Zendesk-users object.

- id
- url
- external_id
- email
- active
- chat_only
- customer_role_id
- role_type
- details
- last_login_at
- locale
- locale_id
- moderator

- notes
- only_private_comments
- default_group_id
- phone
- shared_phone_number
- photo
- restricted_agent
- role
- shared
- tags
- signature
- suspended
- ticket_restriction
- time_zone
- two_factor_auth_enabled
- user_fields
- verified
- report_csv
- created_at
- updated_at

Mapping Zendesk users to a standard profile

A subset of the fields in the Zendesk-users object map to the standard profile in Customer Profiles. The following table lists which fields can be mapped from the Zendesk-users object to the standard profile.

Zendesk-users source field	Standard profile target field
id	Attributes.ZendeskUserId
external_id	Attributes.ZendeskExternalId
email	EmailAddress
phone	PhoneNumber

The Zendesk-users customer data from the Zendesk object is associated with a Amazon Connect customer profile using the following indexes.

Standard Index Name	Zendesk-user source field
_zendeskUserId	Id
_zendeskExternalId	external_id

For example, you can use `_zendeskUserId` and `_zendeskExternalId` as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Zendesk-users objects associated with a specific customer profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Zendesk-users`.

Mapping Marketo objects to the standard profile

This topic lists which fields in Marketo objects map to fields in the standard profile object in Customer Profiles.

Marketo-leads object

Following is a list of all the fields in a Marketo-leads object

- id
- firstName
- lastName
- middleName
- email
- phone
- mobilePhone
- billingStreet
- billingCity
- billingState
- billingCountry
- billingPostalCode
- address
- city
- state
- country
- postalcode
- gender
- dateOfBirth

Mapping Marketo-leads to a standard profile

A subset of fields in the Marketo-leads object map to the standard profile.

Marketo-leads source field	Standard profile target field
id	Attributes.MarketoLeadId
sfdcAccountId	Attributes.sfdcAccountId
sfdcContactId	Attributes.sfdcContactId
firstName	FirstName
lastName	LastName
middleName	MiddleName
email	EmailAddress

Marketo-leads source field	Standard profile target field
phone	PhoneNumber
mobilePhone	MobilePhoneNumber
mobilePhone	MobilePhoneNumber
billingStreet	BillingAddress.Address1
billingCity	BillingAddress.City
billingState	BillingAddress.State
billingCountry	BillingAddress.Country
billingPostalCode	BillingAddress.PostalCode
address	Address.Address1
city	Address.City
state	Address.State
country	Address.Country
postalcode	Address.PostalCode
gender	Gender
dataOfBirth	BirthDate

The Marketo-leads customer data from Marketo is associated with an Amazon Connect customer profile using the indexes in the following table.

Standard Index Name	Marketo-leads source field
_marketoLeadId	id
_salesforceAccountId	sfdcAccountId
_salesforceContactId	sfdcContactId

For example, you can use `_marketoLeadId`, `_salesforceAccountId`, and `_salesforceContactId` as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Marketo-leads objects associated with a specific customer profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Marketo-leads`.

Mapping ServiceNow objects to the standard profile object

This topic lists which fields in ServiceNow objects map to fields in the standard profile object in Amazon Connect Customer Profiles.

Servicenow-sys_user object

Following is a list of all the fields in a Servicenow-sys_user object

- sys_id
- active
- building
- calendar_integration
- city
- company
- cost_center
- country
- date_format
- default_perspective
- department
- edu_status
- email
- employee_number
- enable_multifactor_authn
- failed_attempts
- first_name
- gender
- home_phone
- internal_integration_user
- introduction
- last_login
- last_login_device
- last_login_time
- last_name
- last_password
- ldap_server
- location
- locked_out
- manager
- middle_name
- mobile_phone
- name
- notification
- password_needs_reset
- phone
- photo
- preferred_language
- roles
- schedule
- source
- state
- street

- sys_class_name
- sys_created_by
- sys_created_on
- sys_domain.link
- sys_domain.value
- sys_domain_path
- sys_id
- sys_mod_count
- sys_updated_by
- sys_udpated_on
- time_format
- time_zone
- title
- user_name
- user_password
- web_service_access_only
- zip

Mapping Servicenow-sys_users to a standard profile object

A subset of the fields in the Servicenow-sys_users object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Servicenow-sys_users object to the standard profile.

Servicenow-sys_users source field	Customer profiles target field
sys_id	Attributes.ServiceNowSystemId
first_name	FirstName
last_name	LastName
middle_name	MiddleName
gender	Gender
email	EmailAddress
phone	PhoneNumber
home_phone	HomePhoneNumber
mobile_phone	MobilePhoneNumber
street	Address.Address1
city	Address.City
state	Address.State
country	Address.Country

Servicenow-sys_users source field	Customer profiles target field
zip	Address.PostalCode

The Servicenow-sys_user customer data from Servicenow object is associated with an Amazon Connect customer profile using the indexes in the following table.

Standard Index Name	Servicenow-sys_user source field
_serviceNowSystemId	sys_id

For example, you can use `_serviceNowSystemId` and `_serviceNowIncidentId` as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Servicenow-sys_user objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Servicenow-sys_user`.

Mapping Segment objects to the standard profile object

This topic lists which fields in Segment objects map to fields in the standard profile object in Amazon Connect Customer Profiles.

Segment-Identify object

Following is a list of all the fields in a Segment-Identify object.

- userId
- common fields - see Spec: Common Fields in the Segment documentation
- Segment reserved traits - see Traits in the Segment documentation
- traits.address.street
- traits.address.city
- traits.address.state
- traits.address.postalCode
- traits.address.country
- traits.age
- traits.avatar
- traits.birthday
- traits.company.name
- traits.company.id
- traits.company.industry
- traits.company.employee_count
- traits.company.plan
- traits.createdAt
- traits.description
- traits.email
- traits.firstName

- traits.gender
- traits.id
- traits.lastName
- traits.name
- traits.phone
- traits.title
- traits.username
- traits.website

Mapping a Segment-Identify to a standard profile object

A subset of the fields in the Segment-Identify object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Segment-Identify object to the standard profile.

Segment-Identify source field	Standard profile target field
userId	Attributes.SegmentUserId
traits.company.name	BusinessName
traits.firstName	FirstName
traits.lastName	LastName
traits.birthday	BirthDate
traits.gender	Gender
traits.phone	PhoneNumber
traits.email	EmailAddress
traits.address.street	Address.Address1
traits.address.city	Address.City
traits.address.state	Address.State
traits.address.country	Address.Country
traits.address.postalCode	Address.PostalCode

Example

The following example shows how to map a source field to a target field.

```
"segmentUserId": {
    "Source": "_source.detail.event.detail.userId",
    "Target": "_profile.Attributes.SegmentUserId"
}
```

The Segment-Identify customer data from the Segment object is associated with an Amazon Connect customer profile using the following index.

Standard Index Name	Segment-Identify source field
_segmentUserId	userId

For example, you can use `_segmentUserId` as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Segment-Identify objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Segment-Identify`.

Mapping Shopify objects to the standard profile object

This topic lists which fields in Shopify objects map to fields in the standard profile object in Amazon Connect Customer Profiles.

Shopify-Customer object

Following is a list of all the fields in a Shopify-Customer object.

- accepts_marketing
- accepts_marketing_updated_at
- addresses
- currency
- created_at
- default_address.address1
- default_address.address2
- default_address.city
- default_address.company
- default_address.country
- default_address.country_code
- default_address.country_name
- default_address.customer_id
- default_address.default
- default_address.first_name
- default_address.id
- default_address.last_name
- default_address.name
- default_address.phone
- default_address.province
- default_address.province_code
- default_address.zip
- email
- first_name
- id
- last_name
- last_order_id

- last_order_name
- metafield.key
- metafield.value
- metafield.namespace
- metafield.value_type
- marketing_opt_in_level
- multipass_identifier
- note
- orders_count
- phone
- sms_marketing_consent.state
- sms_marketing_consent.opt_in_level
- sms_marketing_consent.consent_updated_at
- sms_marketing_consent.consent_collected_from
- state
- tags
- tax_exempt
- tax_exemptions
- total_spent
- updated_at
- verified_email

Mapping a Shopify-Customer object to a standard profile

A subset of the fields in the Shopify-Customer object map to the standard profile object in Customer Profiles.

The following table lists which fields can be mapped from the Shopify-Customer object to the standard profile.

Shopify-Customer source field	Standard profile target field
id	Attributes.ShopifyCustomerId
email	EmailAddress
first_name	FirstName
last_name	LastName
note	AdditionalInformation
phone	PhoneNumber
default_address.address1	Address.Address1
default_address.address2	Address.Address2
default_address.city	Address.City
default_address.province	Address.Province
default_address.country	Address.Country

default_address.zip	Address.PostalCode

Example

The following example shows how to map a source field to a target field.

```
"shopifyCustomerId": {
    "Source": "_source.detail.event.detail.payload.id",
    "Target": "_profile.Attributes.ShopifyCustomerId"
}
```

The Shopify-Customer customer data from the Shopify object is associated with an Amazon Connect customer profile using the following index.

Standard Index Name	Shopify-Customer source field
_shopifyCustomerId	id

For example, you can use `_shopifyCustomerId` as a key name with the SearchProfiles API to find an Amazon Connect customer profile. You can find the Shopify-Customer objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Shopify-Customer`.

Object type mapping for the standard order

The topics in this section provide the standard order definition, and the object type mapping from external applications to the standard order.

Contents

Amazon AppIntegrations access requirements

Following are the Amazon AppIntegrations access requirements to create and delete Shopify integrations:

- app-integrations:GetEventIntegration
- app-integrations:ListEventIntegrationAssociations
- app-integrations:CreateEventIntegrationAssociation
- app-integrations:DeleteEventIntegrationAssociation

Amazon EventBridge access requirements

Following are the Amazon EventBridge access requirements to create and delete Shopify integrations:

- events:ListTargetsByRule
- events:PutRule
- events:PutTargets
- events:DeleteRule
- events:RemoveTargets

Standard order definition

The following table lists all the fields in the Customer Profiles standard order object.

Standard order field	Data type	Description
OrderId	String	The unique identifier of a standard order.
CustomerEmail	String	The customer's email address.
CustomerPhone	String	The customer's phone number.
CreatedDate	String	The order's date created.
UpdatedDate	String	The order's date updated.
ProcessedDate	String	The order's date processed.
ClosedDate	String	The order's date closed.
CancelledDate	String	The order's date cancelled.
CancelReason	String	The order's cancel reason.
Name	String	The order's name.
AdditionalInformation	String	Any additional information relevant to the order.
Gateway	String	The order's payment gateway.
Status	String	The order's status.
StatusCode	String	The order's status code.Valid values: DRAFT | ACTIVATED
StatusUrl	String	The order's status URL.
CreditCardNumber	String	The customer's credit card last four digits.
CreditCardCompany	String	The customer's credit card company.
FulfillmentStatus	String	The order's fulfillment status.
TotalPrice	String	The order's total price.
TotalTax	String	The order's total tax.
TotalDiscounts	String	The order's total discounts.
TotalItemsPrice	String	The order's total items price.

TotalShippingPrice	String	The order's total shipping price.
TotalTipReceived	String	The order's total tip received.
Currency	String	The order's currency.
TotalWeight	String	The order's total weight.
BillingAddress	OrderAddress	The customer's billing address.
ShippingAddress	OrderAddress	The customer's shipping address.
OrderItems	OrderItem list	The order's items.
Attributes	String-to-string map	Key-value pair of attributes of a standard order.

OrderAddress data type

Standard order field	Data type	Description
Name	String	The name associated with an order address.
Address1	String	The first line of an order address.
Address2	String	The second line of an order address.
Address3	String	The third line of an order address.
Address4	String	The fourth line of an order address.
City	String	The city of an order address.
County	String	The county of an order address.
State	String	The state of an order address.
Province	String	The province of an order address.
Country	String	The country of an order address.
PostalCode	String	The postal code of an order address.

OrderItem data type

Standard order field	Data type	Description
Title	String	The title of an order item.
Price	String	The price of an order item.
Quantity	String	The quantity of an order item.

Mapping Shopify objects to the standard order

This topic lists which fields in Shopify objects map to fields in the standard order object in Customer Profiles.

Shopify-DraftOrder object

For a list of all the fields in a Shopify-DraftOrder object see The DraftOrder object in the Shopify documentation.

Mapping a Shopify-DraftOrder object to a standard order

A subset of the fields in the Shopify-DraftOrder object map to the standard order object in Customer Profiles.

The following table lists which fields can be mapped from the Shopify-DraftOrder object to the standard order.

The `StatusCode` is `ACTIVATED` if `order_status_url` exists in the source. Otherwise, the `StatusCode` is `DRAFT`.

Shopify-DraftOrder source field	Standard order target field
id	Attributes.ShopifyOrderId
customer.id	Attributes.ShopifyCustomerId
note	AdditionalInformation
email	CustomerEmail
currency	Currency
created_at	CreatedDate
updated_at	UpdatedDate
name	Name
status	Status
order_status_url	StatusCode
billing_address.address1	BillingAddress.Address1
billing_address.address2	BillingAddress.Address2
billing_address.city	BillingAddress.City
billing_address.zip	BillingAddress.PostalCode
billing_address.province	BillingAddress.Province
billing_address.country	BillingAddress.Country
billing_address.name	BillingAddress.Name
shipping_address.address1	ShippingAddress.Address1
shipping_address.address2	ShippingAddress.Address2

shipping_address.city	ShippingAddress.City
shipping_address.zip	ShippingAddress.PostalCode
shipping_address.province	ShippingAddress.Province
shipping_address.country	ShippingAddress.Country
shipping_address.name	ShippingAddress.Name
invoice_url	StatusUrl
total_price	TotalPrice
total_tax	TotalTax
line_items[].title	OrderItems[].Title
line_items[].price	OrderItems[].Price
line_items[].quantity	OrderItems[].Quantity

Example

The following example shows how to map a source field to a target field.

```
"shopifyOrderId": {
    "Source": "_source.detail.event.detail.payload.id",
    "Target": "_order.Attributes.ShopifyOrderId"
}
```

The Shopify-DraftOrder customer data from the Shopify object is associated with an Amazon Connect standard order using the following index.

Standard Index Name	Shopify-DraftOrder source field
_shopifyOrderId	id

For example, you can use `_shopifyOrderId` as an `ObjectFilter.KeyName` with the the ListProfileObjects API to find a standard order. You can find the Shopify-DraftOrder objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Shopify-DraftOrder`.

Shopify-Order object

For a list of all the fields in a Shopify-Order object see The Order object in the Shopify documentation.

Mapping a Shopify-Order object to a standard order

A subset of the fields in the Shopify-Order object map to the standard order object in Customer Profiles.

The following table lists which fields can be mapped from the Shopify-Order object to the standard order.

The `StatusCode` is `ACTIVATED` if `order_status_url` exists in the source. Otherwise, the `StatusCode` is `DRAFT`.

Shopify-Order source field	Standard order target field
id	Attributes.ShopifyOrderId
customer.id	Attributes.ShopifyCustomerId
cancelled_at	CancelledDate
cancel_reason	CancelReason
closed_at	ClosedDate
created_at	CreatedDate
currency	Currency
email	CustomerEmail
financial_status	Status
order_status_url	StatusCode
fulfillment_status	FulfillmentStatus
gateway	Gateway
name	Name
note	AdditionalInformation
order_status_url	StatusUrl
phone	CustomerPhone
processed_at	ProcessedDate
total_discounts	TotalDiscounts
total_line_items_price	TotalItemsPrice
total_price	TotalPrice
total_shipping_price_set.shop_money.amount	TotalShippingPrice
total_tax	TotalTax
total_tip_received	TotalTipReceived
total_weight	TotalWeight
updated_at	UpdatedDate
billing_address.address1	BillingAddress.Address1
billing_address.address2	BillingAddress.Address2
billing_address.city	BillingAddress.City
billing_address.zip	BillingAddress.PostalCode
billing_address.province	BillingAddress.Province
billing_address.country	BillingAddress.Country
billing_address.name	BillingAddress.Name

payment_details.credit_card_number	CreditCardNumber
payment_details.credit_card_company	CreditCardCompany
shipping_address.address1	ShippingAddress.Address1
shipping_address.address2	ShippingAddress.Address2
shipping_address.city	ShippingAddress.City
shipping_address.zip	ShippingAddress.PostalCode
shipping_address.province	ShippingAddress.Province
shipping_address.country	ShippingAddress.Country
shipping_address.name	ShippingAddress.Name
line_items[].title	OrderItems[].Title
line_items[].price	OrderItems[].Price
line_items[].quantity	OrderItems[].Quantity

Example

The following example shows how to map a source field to a target field.

```
"shopifyOrderId": {
    "Source": "_source.detail.event.detail.payload.id",
    "Target": "_order.Attributes.ShopifyOrderId"
}
```

The Shopify-Order customer data from the Shopify object is associated with an Amazon Connect standard order using the following index.

Standard Index Name	Shopify-Order source field
_shopifyOrderId	id

For example, you can use `_shopifyOrderId` as an `ObjectFilter.KeyName` with the the ListProfileObjects API to find a standard order. You can find the Shopify-Order objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Shopify-Order`.

Object type mapping for the standard asset

The topics in this section provide the standard asset definition, and the object type mapping from external applications to the standard asset.

Contents

Amazon AppFlow access requirements

Following are the Amazon AppFlow access requirements to create and delete Salesforce integrations:

- appflow:CreateFlow
- appflow:DeleteFlow

Standard asset definition

The following table lists all the fields in the Customer Profiles standard asset object.

Standard asset field	Data type	Description
AssetId	String	The unique identifier of a standard asset.
AssetName	String	The asset's name.
SerialNumber	String	The asset's serial number.
ModelNumber	String	The asset's model number.
ModelName	String	The asset's model name.
ProductSKU	String	The asset's stock keeping unit.
PurchaseDate	String	The asset's purchase date.
UsageEndDate	String	The asset's usage end date.
Status	String	The asset's status.
Price	String	The asset's price.
Quantity	String	The asset's quantity.
Description	String	The asset's description.
Additional information	String	Any additional information relevant to the asset.
DataSource	String	The asset's data source.
Attributes	String-to-string map	Key-value pair of attributes of a standard asset.

Mapping Salesforce objects to the standard asset

This topic lists which fields in Salesforce objects map to fields in the standard asset object in Customer Profiles.

Salesforce-Asset object

Following is a list of all the fields in a Salesforce-Asset object.

- Id

- ContactId
- AccountId
- ParentId
- RootAssetId
- Product2Id
- ProductCode
- IsCompetitorProduct
- CreatedDate
- CreatedById
- LastModifiedDate
- LastModifiedById
- SystemModstamp
- IsDeleted
- Name
- SerialNumber
- InstallDate
- PurchaseDate
- UsageEndDate
- LifecycleStartDate
- LifecycleEndDate
- Status
- Price
- Quantity
- Description
- OwnerId
- AssetProvidedById
- AssetServiceById
- IsInternal
- AssetLevel
- StockKeepingUnit
- HasLifecycleManagement
- CurrentMrr
- CurrentLifecycleEndDate
- CurrentQuantity
- CurrentAmount
- LastViewedDate
- LastReferencedDate

Mapping a Salesforce-Asset object to a standard asset

A subset of the fields in the Salesforce-Asset object map to the standard asset object in Customer Profiles.

The following table lists which fields can be mapped from the Salesforce-Asset object to the standard asset.

Saleforce-Asset source field	Standard asset target field
Id	Attributes.sfdcAssetId
ContactId	Attributes.sfdcContactId
AccountId	Attributes.sfdcAccountId
SerialNumber	SerialNumber
StockKeepingUnit	ProductSKU
UsageEndDate	UsageEndDate
Status	Status
Price	Price
Quantity	Quantity
Description	Description

The Salesforce-Asset customer data from the Salesforce object is associated with an Amazon Connect standard asset using the indexes in the following table.

Standard Index Name	Salesforce-Asset source field
_salesforceAssetId	Id
_salesforceContactId	ContactId
_salesforceAccountId	AccountId

For example, you can use `_salesforceAssetId` and `_salesforceAccountId` as an `ObjectFilter.KeyName` with the ListProfileObjects API to find a standard asset. You can find the Salesforce-Asset objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Salesforce-Asset`.

Object type mapping for the standard case

The topics in this section provide the standard case definition, and the object type mapping from external applications to the standard case.

Contents

Amazon AppFlow access requirements

Following are the Amazon AppFlow access requirements to create and delete Zendesk and ServiceNow integrations:

- appflow:CreateFlow
- appflow:DeleteFlow

Standard case definition

The following table lists all the fields in the Customer Profiles standard case object.

Standard case field	Data type	Description
CaseId	String	The unique identifier of a standard case.
Title	String	The case's title
Summary	String	The case's summary.
Status	String	The case's status.
Reason	String	The case's reason.
CreatedBy	String	The case's creator.
CreatedDate	String	The case's date created.
UpdatedDate	String	The case's date updated.
ClosedDate	String	The case's date closed.
AdditionalInformation	String	Any additional information relevant to the case.
DataSource	String	The case's data source.
Attributes	String-to-string map	Key-value pair of attributes of a standard case.

Mapping Zendesk objects to the standard case

This topic lists which fields in Zendesk objects map to fields in the standard case in Customer Profiles.

Zendesk-tickets object

Following is a list of all the fields in a Zendesk-tickets object.

- id
- url
- type
- subject
- raw_subject
- description
- priority
- status
- recipient

- requester_id
- submitter_id
- assignee_id
- organization_id
- group_id
- collaborator_ids
- email_cc_ids
- follower_ids
- forum_topic_id
- problem_id
- has_incidents
- due_at
- tags
- via.channel
- custom_fields
- satisfaction_rating
- sharing_agreement_ids
- followup_ids
- ticket_form_id
- brand_id
- allow_channelback
- allow_attachments
- is_public
- created_at
- updated_at

Mapping Zendesk-tickets object to a standard case

A subset of the fields in the Zendesk-tickets object map to the standard case in Customer Profiles. The following table lists which fields can be mapped from the Zendesk-tickets object to the standard case.

Zendesk-tickets source field	Standard case target field
requester_id	Attributes.ZendeskUserId
id	Attributes.ZendeskTicketId
subject	Title
description	Summary
status	Status
requester_id	CreatedBy
created_at	CreatedDate
updated_at	UpdatedDate
Price	Price

Zendesk-tickets source field	Standard case target field
Quantity	Quantity
Description	Description

The Zendesk-tickets customer data from the Zendesk object is associated with a Amazon Connect standard case using the following indexes.

Standard Index Name	Zendesk-tickets source field
_zendeskUserId	requester_id
_zendeskTicketId	id

For example, you can use `_zendeskUserId` and `_zendeskTicketId` as an `ObjectFilter.KeyName` with the ListProfileObjects API to find a standard case. You can find the Zendesk-tickets objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Zendesk-tickets`.

Mapping ServiceNow objects to the standard case

This topic lists which fields in ServiceNow objects map to fields in the standard case in Amazon Connect Customer Profiles.

Servicenow-task object

Following is list of all the fields in a Servicenow-task object.

- sys_id
- active
- activity_due
- additional_assignee_list
- approval
- approval_history
- approval_set
- assigned_to
- assignment_group
- business_duration
- business_service
- calendar_duration
- closed_at
- closed_by
- cmdb_ci.display_value
- cmdb_ci.link
- comments
- comments_and_work_notes
- company
- contact_type

- contract
- correlation_display
- active
- correlation_id
- delivery_plan
- delivery_task
- description
- due_date
- escalation
- expected_start
- follow_up
- group_list
- impact
- knowledge
- location
- made_sla
- number
- opened_at
- opened_by.display_value
- order
- parent
- priority
- reassignment_count
- service_offering
- short_description
- sla_due
- state
- sys_class_name
- sys_created_by
- sys_created_on
- active
- sys_domain.global
- sys_domain.link
- sys_domain_path
- sys_mod_count
- sys_updated_by
- sys_updated_on
- time_worked
- upon_approval
- upon_reject
- urgency
- user_input
- watch_list
- work_end
- work_notes

- work_notes_list
- work_start

Mapping Servicenow-task to a standard case

A subset of the fields in the Servicenow-task object map to the standard case in Customer Profiles.

The following table lists which fields can be mapped from the Servicenow-task object to the standard case.

Servicenow-task source field	Standard case target field
sys_id	Attributes.ServiceNowTaskId
opened_by.link	Attributes.ServiceNowUserId
short_description	Title
description	Summary
status	Status
sys_created_by	CreatedBy
sys_created_on	CreatedDate
sys_updated_on	UpdatedDate

The Servicenow-task customer data from Servicenow is associated with an Amazon Connect standard case using the indexes in the following table.

Standard Index Name	Servicenow-task source field
_serviceNowTaskId	sys_id
_serviceNowSystemId	open_by.link

For example, you can use `_serviceNowTaskId` and `_serviceNowSystemId` as an `ObjectFilter.KeyName` with the ListProfileObjects API to find a standard case. You can find the Servicenow-task objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Servicenow-task`.

Servicenow-incident object

Following is a list of all the fields in a Servicenow-incident object.

- sys_id
- business_stc
- calendar_stc
- caller_id.link
- caller_id.value
- category
- caused_by

- child_incidents
- close_code
- hold_reason
- incident_state
- notify
- parent_incident
- problem_id
- reopened_by
- reopened_time
- reopen_count
- resolved_at
- resolved_by.link
- resolved_by.value
- rfc
- severity
- subcategory

Mapping Servicenow-incident to a standard case

A subset of the fields in the Servicenow-incident object map to the standard case in Customer Profiles.

The following table lists which fields can be mapped from the Servicenow-incident object to the standard case.

Servicenow-Incident source field	Standard case target field
sys_id	Attributes_ServiceNowIncidentId
caller_id.link	Attributes_ServiceNowSystemUserId
incident_status	Status
caller_id.link	CreatedBy
resolved_at	ClosedDate
category	Reason

The Servicenow-incident customer data from the Servicenow object is associated with an Amazon Connect standard case using the indexes in the following table.

Standard Index Name	Servicenow source field
_serviceNowIncidentId	sys_id
_serviceNowSystemId	caller_id.link

For example, you can use `_serviceNowIncidentId` and `_serviceNowSystemId` as a ObjectFilter.KeyName with the ListProfileObjects API to find a standard case. You can find the Servicenow-incident objects associated with a specific profile by using the ListProfileObjects API with the `ProfileId` and `ObjectTypeName` set to `Servicenow-incident`.

Create and ingest customer data into Customer Profiles by using Amazon S3

You can define data from any source using Amazon S3 and seamlessly enrich a customer profile without the need for custom or pre-built integrations. For example, say you want to provide agents with relevant purchase history information. You can import purchase transaction data from an internal application into a spreadsheet file on S3 and then link it to a customer profile.

To set this up, you need to define an object type mapping (p. 681) that describes what the custom profile object looks like. This mapping defines how fields from your data can be used to either populate fields in the standard profile or how it can be used to assign the data to a specific profile.

After you create the object type mapping, you can use the PutProfileObject API to upload the custom profile data from your CRM into the custom profile object.

Use the Customer Profiles API

For information about how to programmatically manage domains and profiles, see the Amazon Connect Customer Profiles API Reference.

We recommend using the CustomerProfileJS open source library when integrating Customer Profiles into your own agent application. For more information, see the CustomerProfilesJS repo on Github.

For more information about how to integrate your existing apps with Amazon Connect use Amazon Connect Streams. You can embed the Contact Control Panel (CCP) components into your app.

Example: Programmatically integrate S3 with Customer Profiles

Using the Customer Profiles PutIntegration API, you can programmatically create integrations for S3, Salesforce, Marketo, and more.

In this topic we show how to create an S3 integration with a sync interval of 15 minutes, the minimum value currently supported.

Step 1: Create a JSON file

Create a JSON file with the following contents:

```
{
    "DomainName": "YOUR-DOMAIN",
    "ObjectTypeName": "YOUR-OBJECT-NAME",
    "FlowDefinition": {
        "FlowName": "YOUR-FLOW-NAME",
        "KmsArn": "THE KEY ARN IS THE SAME AS YOUR DOMAIN'S KEY",
        "Description": "Created by Customer Profiles",
        "TriggerConfig": {
            "TriggerType": "Scheduled",
            "TriggerProperties": {
                "Scheduled": {
                    "ScheduleExpression": "rate(15minutes)",
                    "DataPullMode": "Incremental",
                    "ScheduleStartTime": 1634244800.435,
                    "FirstExecutionFrom": 1594166400
                }
            }
        },
        "SourceFlowConfig": {
            "ConnectorType":"S3",
            "SourceConnectorProperties": {
                "S3": {
                    "BucketName": "YOUR-BUCKET",
                    "BucketPrefix": "YOUR-PREFIX"
                }
            }
        },
        "Tasks": [
            {"TaskType":"Filter","SourceFields":["colA","colB"],"ConnectorOperator":
{"S3":"PROJECTION"}},
            {"ConnectorOperator":{"S3":"NO_OP"},"DestinationField":"colA","TaskProperties":
{},"SourceFields":["colA"],"TaskType":"Map"},
            {"ConnectorOperator":{"S3":"NO_OP"},"DestinationField":"colB","TaskProperties":
{},"SourceFields":["colB"],"TaskType":"Map"}
        ]
    }
}
```

To customize the JSON with your own values, follow these guidelines:

- `FlowName`: Can be STRING [a-zA-Z0-9][\w!@#.-]+
- `ScheduleStartTime`: Set to the current `DateTime` + 5 minutes in epoch time.
- `FirstExecutionFrom`: Go to S3, look at the file date, and use a date that is before the oldest date.
- `Tasks`: Define `TaskType`. In the `Sourcefields` field you have to supply ALL the columns you have in your CSV in that array. Then, for each of the items in that array, you need to specify the `ConnectorOperator`. This example is for a CSV document with two columns: `colA` and `colB`.

Step 2: Call the PutIntegration API

After you have created and customized the JSON file with your values, call the PutIntegration API, as shown in the following example:

```
aws customer-profiles put-integration --cli-input-json file:///put_integration_s3_cli.json
 --region us-west-2
```

The response from `PutIntegration` returns a flow URI. For example:

```
{
    "DomainName": "testDomain",
    "Uri": "arn:aws:appflow:us-west-2:9999999999999:flow/
Customer_Profiles_testDomain_S3_Salesforce-Account_1634244122247",
    "ObjectTypeName": "your objec type",
    "CreatedAt": "2021-10-14T13:51:57.748000-07:00",
    "LastUpdatedAt": "2021-10-14T13:51:57.748000-07:00",
    "Tags": {}
}
```

Step 3: Call the Amazon AppFlow StartFlow API

Use the flow URI to call the Amazon AppFlow StartFlow API. For example:

```
aws appflow start-flow —flow-name uri --region us-west-2
```

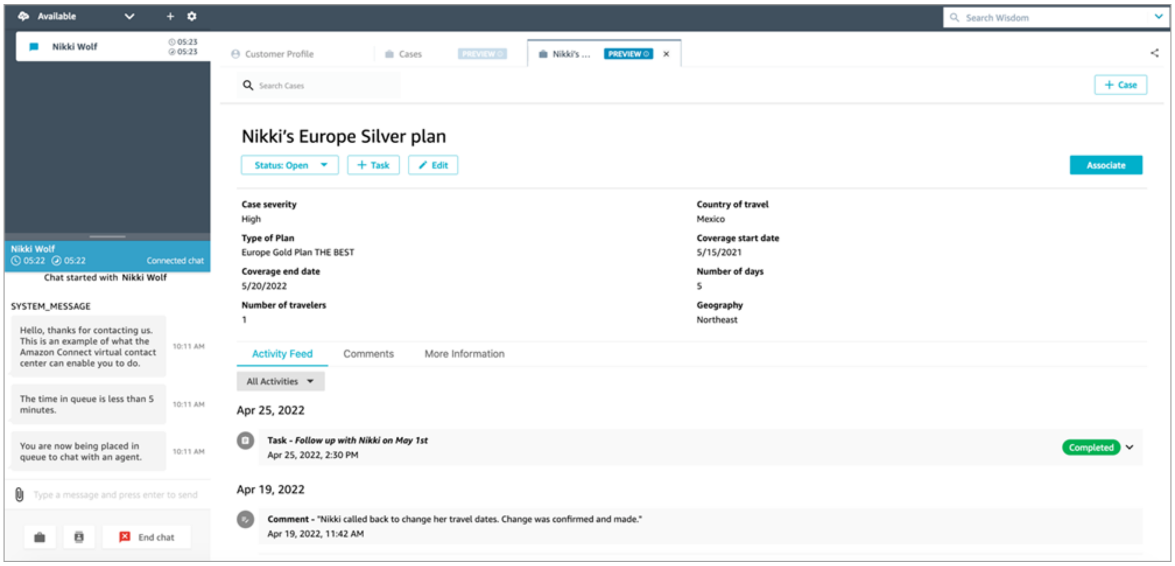
Amazon Connect Cases (Preview)

Amazon Connect Cases enables your customer service organization to track, collaborate, and resolve customer cases.

A *case* represents a customer's issue. It is created to record the customer's issue, the steps and interactions taken to resolve the customer's issue, and the outcome.

Without doing any integration work, you can enable Cases for your contact center. You can set up cases to be created when contacts come in, and collect information from the customer to display on the case. Alternatively, agents can manually create cases. When an agent accepts a contact, they have context about an issue and can immediately start solving it. You can create tasks to track and route follow up steps to resolve the case.

The following image shows an example case as it appears in the agent application.



Nikki Wolf
05:22 05:22 Connected chat
Chat started with Nikki Wolf

SYSTEM_MESSAGE

Hello, thanks for contacting us. This is an example of what the Amazon Connect virtual contact center can enable you to do. 10:11 AM

The time in queue is less than 5 minutes. 10:11 AM

You are now being placed in queue to chat with an agent. 10:11 AM

Nikki's Europe Silver plan

Case severity
High

Type of Plan
Europe Gold Plan THE BEST

Coverage end date
5/20/2022

Number of travelers
1

Country of travel
Mexico

Coverage start date
5/15/2021

Number of days
5

Geography
Northeast

Apr 25, 2022

Task - *Follow up with Nikki on May 1st*
Apr 25, 2022, 2:30 PM

Apr 19, 2022

Comment - "Nikki called back to change her travel dates. Change was confirmed and made."
Apr 19, 2022, 11:42 AM

Getting started with Cases

We recommend reviewing these topics to help you get started:

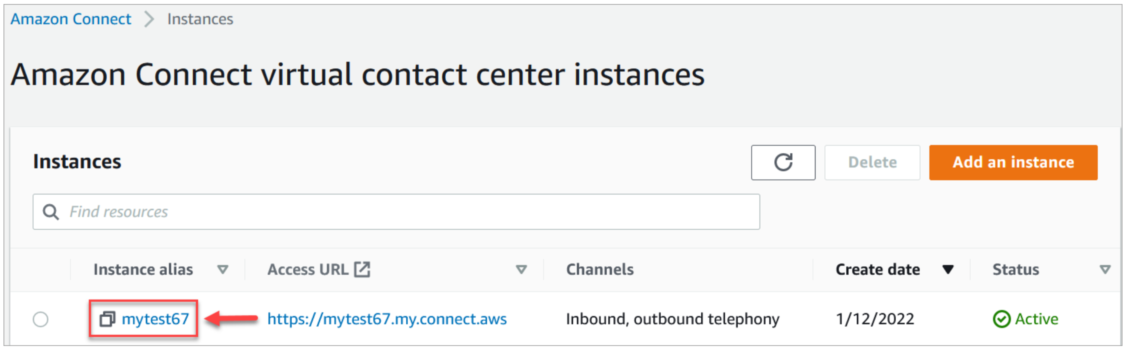
- Enable Cases (p. 733)
- Assign permissions (p. 734)
- Create case fields (p. 736) and case templates (p. 740)
- How agents use Cases (p. 743)
- Cases block (p. 344)
- Case event streams (p. 750)
- Cases quotas (p. 1208)

Enable Cases (Preview)

This topic explains how to enable Amazon Connect Cases using the Amazon Connect console. To use the API, see Amazon Connect Cases API Reference.

Tip
A case is always associated with a customer profile. You must have Customer Profiles enabled. Check your instance settings in the Amazon Connect console, and if a Customer Profiles domain does not yet exist, see Enable Customer Profiles for your instance (p. 641).

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.


Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Cases**. This option is currently available in the US East (N. Virginia) and US West (Oregon) Regions.
4. Choose **Enable cases** to get started.
5. On the **Cases** page, choose **Add domain**.
6. On the **Add domain** page, enter a unique, friendly name that's meaningful to you, such as your organization name.
7. Choose **Add domain**. The domain is created.

   If the domain is not created, choose **Try again**. If that doesn't work, contact AWS Support.

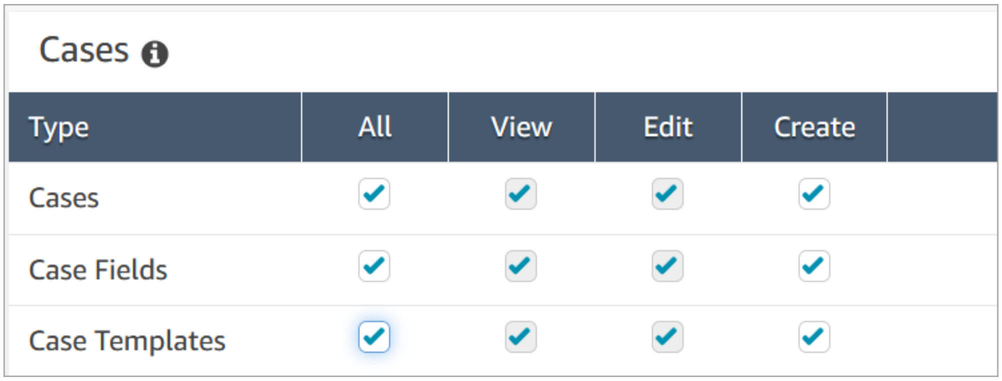
Next steps

After your cases domain is created, do the following:

1. Assign security profile permissions (p. 734) to agents and call center managers.
2. Create case fields (p. 736). Fields are the building blocks of your case templates.
3. Create case templates (p. 740). Case templates are forms that agents complete and reference in the agent application. Templates ensure the right information is collected and referenced for different types of customer issues.
4. Optionally, add the Cases (p. 344) block to your flows. This block enables you to get, update, or create cases automatically.
5. Optionally, set up case event streams (p. 750) to get near real-time updates when cases are created or modified.

Security profile permissions for Cases (Preview)

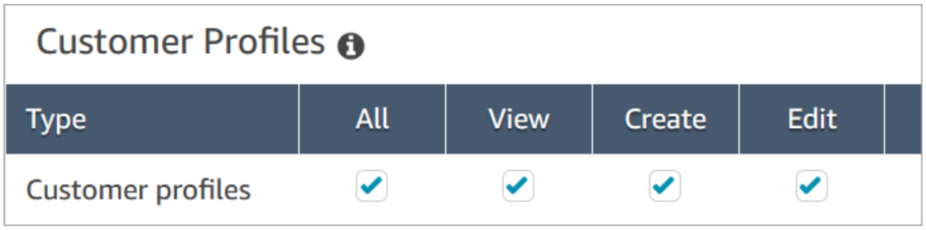
The following image shows the security permissions used to manage access to Amazon Connect Cases (p. 733) functionality:



Cases

Type	All	View	Edit	Create
Cases	☑	☑	☑	☑
Case Fields	☑	☑	☑	☑
Case Templates	☑	☑	☑	☑

Also, to use Amazon Connect Cases, your users also need permissions to Customer Profiles permissions.



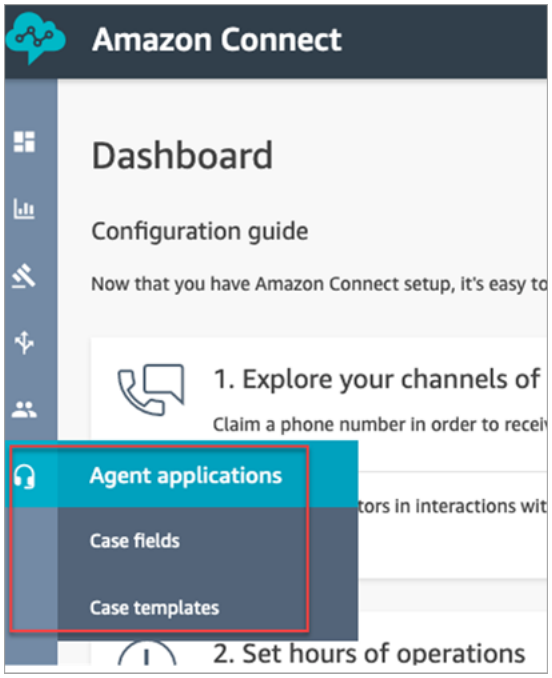
Customer Profiles

Type	All	View	Create	Edit
Customer profiles	☑	☑	☑	☑

Assign the following permissions to manage who can create, view, and edit cases, case fields, and case templates:

- **Cases**: Manage who can access cases by using the agent application.
  - **View case**: Allows the user to view and search cases in the agent application. This includes viewing case data (for example, status, title, summary), contact history (for example, calls, chats, tasks with information such as start time, end time, duration, etc.), and comments.
  - **Edit case**: Allows the user to edit cases, which includes editing case data (for example, update case status), add comments, and associate contacts to cases.
  - **Create case**: Allows the user to create new cases, and associate contacts to cases.
- **Case Fields**: Manage who can configure case fields by using the Amazon Connect console.
  - **View Case Fields**: Allows users to view the case fields page and all of the existing case fields (could be system or custom).
  - **Edit Case Fields**: Allows users to edit any of the case fields (for example, change title, description, single-select options).
  - **Create Case Fields**: Allows users to create new case fields.
- **Case Templates**: Manage who can configure case templates by using the Amazon Connect console.
  - **View Case Fields**: Allows users to view the case fields page and all of the existing case fields (could be system or custom).
  - **Edit Case Fields**: Allows users to edit any of the case fields (for example, change title, description, single-select options).
  - **Create Case Fields**: Allows users to create new case fields.

When users have permissions to **View Case Fields** and **View Case Templates**, they will see the **Case fields** and **Case templates** options in their left navigation menu, as shown in the following image:


Amazon Connect
Dashboard
Configuration guide
Now that you have Amazon Connect setup, it's easy to
1. Explore your channels of
Claim a phone number in order to recei
Agent applications
tors in interactions wit
Case fields
Case templates
2. Set hours of operations

Create case fields (Preview)

Case fields are the building blocks for *case templates*. You create all of the possible fields of information (for example, VIN number, policy number, make/model of car) that you want agents to collect for a given customer issue.

After you create case fields, you can create case templates.

There are two types of case fields:

- System case fields (p. 737): Amazon Connect provides system fields. You cannot change the name or description.
- Custom case fields (p. 738): You can create custom case fields that are specific for your business. You must name the case field, and optionally provide a description. Note that the description appears only in the Amazon Connect console. It doesn't appear to agents.

How to create case fields

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to create fields. For a list of required permissions, see Security profile permissions for Cases (Preview) (p. 734).
2. Verify the quota for case fields and request an increase if needed. For more information, see Amazon Connect Cases service quotas (Preview) (p. 1208).
3. In the left navigation bar, choose **Agent applications**, **Case fields**.
4. The first time you create new fields, you'll notice several system fields (p. 737) are already present. You cannot change the name of these fields, but in some cases you can edit them.

   For example, **Case Id** is a system field. When a case is created, Amazon Connect adds a case ID automatically, and you cannot change it. **Case reason** is also a system field but you can edit it and enter reasons that are specific to your contact center.

5. Choose **+ New field**.
6. Select the type of field you want to create. For example, you might choose **Text** if you want agents to be able to enter free form notes.
7. Assign a name to the field. It will appear to agents in the agent application.
8. Optionally, provide a description. It will only appear to admins on the Amazon Connect console. It does not appear to agents in the agent application.
9. Choose **Save**.
10. When you're done adding fields, you're ready to create a template (p. 740).

System case fields

Amazon Connect provides system fields. You cannot change the name or description of a system field.

The following table lists the system case fields:

Field name	**Field ID (how you call the field in the API)**	**Field type**	**Description**	**Where the data comes from**
Case ID	case_id	text	Unique Identifier of the case in UUID format (for example, 689b0bea-aa29-4340-896d-4ca3ce9b6226)	Amazon Connect
Case Reason	case_reason	single-select	The reason for opening the case	Agent
Customer	customer_id	text	The API is a customer profile ID. On the **Cases: Fields** page, the customer's name is displayed.	Amazon Connect
Date/Time Closed	last_closed_datetime	date-time	The date and time the case was last closed. It does not guarantee that a case is closed. If a case is reopened, this field contains the date/time stamp of the last time the status was changed to closed.	Amazon Connect
Date/Time Opened	created_datetime	date-time	The date and time the case was opened.	Amazon Connect

Field name	Field ID (how you call the field in the API)	Field type	Description	Where the data comes from
Date/Time Updated	last_updated_datetime	date-time	The date and time the case was last updated.	Amazon Connect
Reference number	reference_number	text	A friendly number for the case in 8-digit numeric format. Reference numbers (unlike the Case ID) are not guaranteed to be unique. We recommend that you identify the customer and then collect the reference number to correctly find the right case.	Agent
Status	status	single-select	Current status of the case	Agent
Summary	summary	text	Summary of the case	Agent
Title	title	text	Title of the case	Agent

Custom case fields

You can create custom case fields that are specific for your business. You must name the case field, and optionally provide a description. Note that the description appears only in the Amazon Connect console. It doesn't appear to agents.

You can create fields that are type: number, text, single-select, or true/false.

Single-select fields

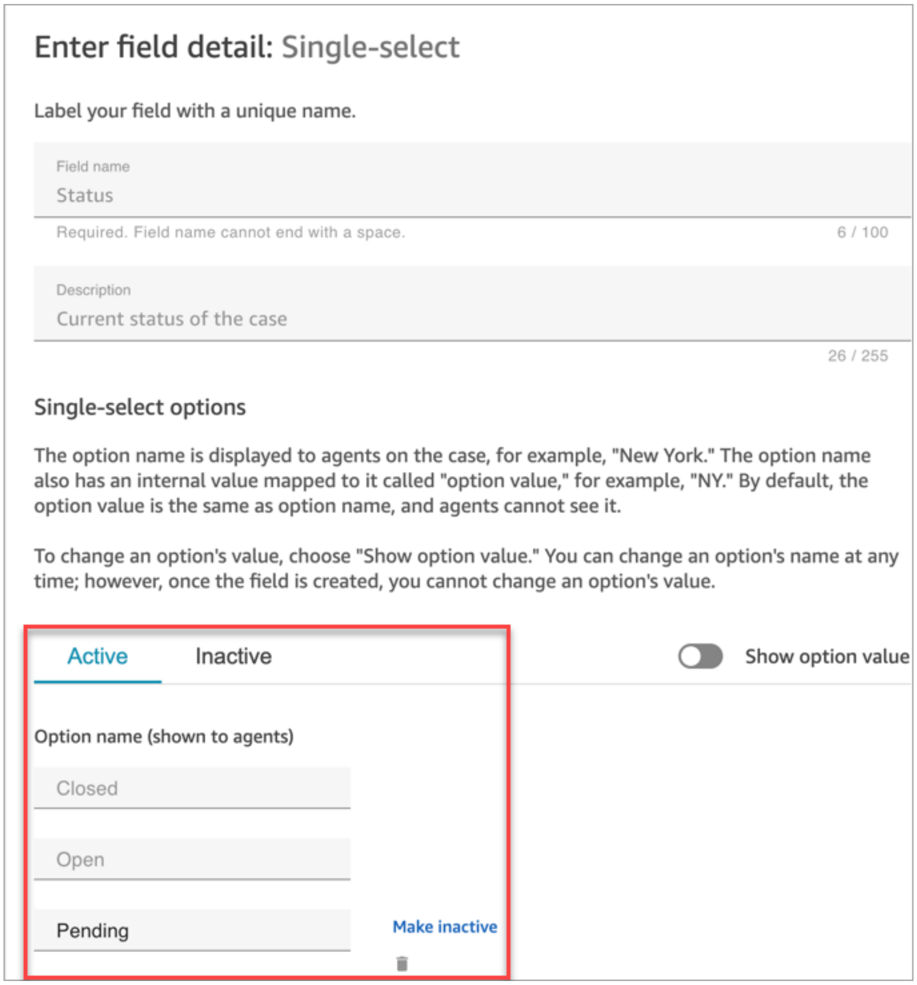
For single-select case fields, whether system or custom, you can add value options that the field can take. For example, you can add options to the single-select system field Case reason such as **General inquiry**, **Billing issue**, or **Product defect**, that reflect the types of issues in your contact center.

About the Status field

You can add options to the single-select **Status** field, such as **Investigating** or **Escalated to manager**. The field comes with two options, **Open** and **Closed**, which cannot be changed.

Active/inactive field options

Single-select case fields can be active or inactive.



Enter field detail: Single-select

Label your field with a unique name.

Field name
Status

Required. Field name cannot end with a space. 6 / 100

Description
Current status of the case

26 / 255

Single-select options

The option name is displayed to agents on the case, for example, "New York." The option name also has an internal value mapped to it called "option value," for example, "NY." By default, the option value is the same as option name, and agents cannot see it.

To change an option's value, choose "Show option value." You can change an option's name at any time; however, once the field is created, you cannot change an option's value.

Closed

Open

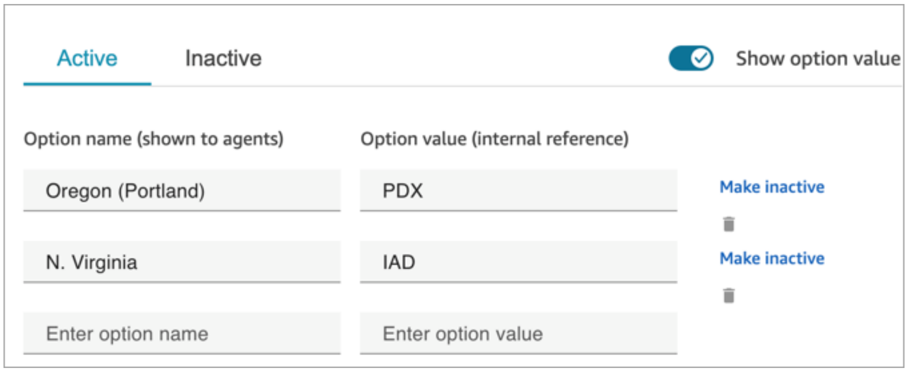
Pending

- **Active**: If a field option is active, it means that the field can be given that option. For example, based on the following image, the Status field can be set to **Closed**, **Open**, or **Pending**, as these are the only active options.
- **Inactive**: If you make the **Pending** option inactive, then the field can no longer be given that option. Any existing cases remain unchanged and can still have the status as **Pending**.

Single-select options have two parts:

1. Option name (shown to agents): The label that is displayed to agents in the agent application.
2. Option value (internal reference): The data that's collected. For example, for AWS Region, you may want to display **US West (Oregon)** but collect the data as **PDX**.

   Field options appear to the agent in alphabetical order.



Option name (shown to agents)	Option value (internal reference)	
Oregon (Portland)	PDX	Make inactive
N. Virginia	IAD	Make inactive
Enter option name	Enter option value	

Create case templates (Preview)

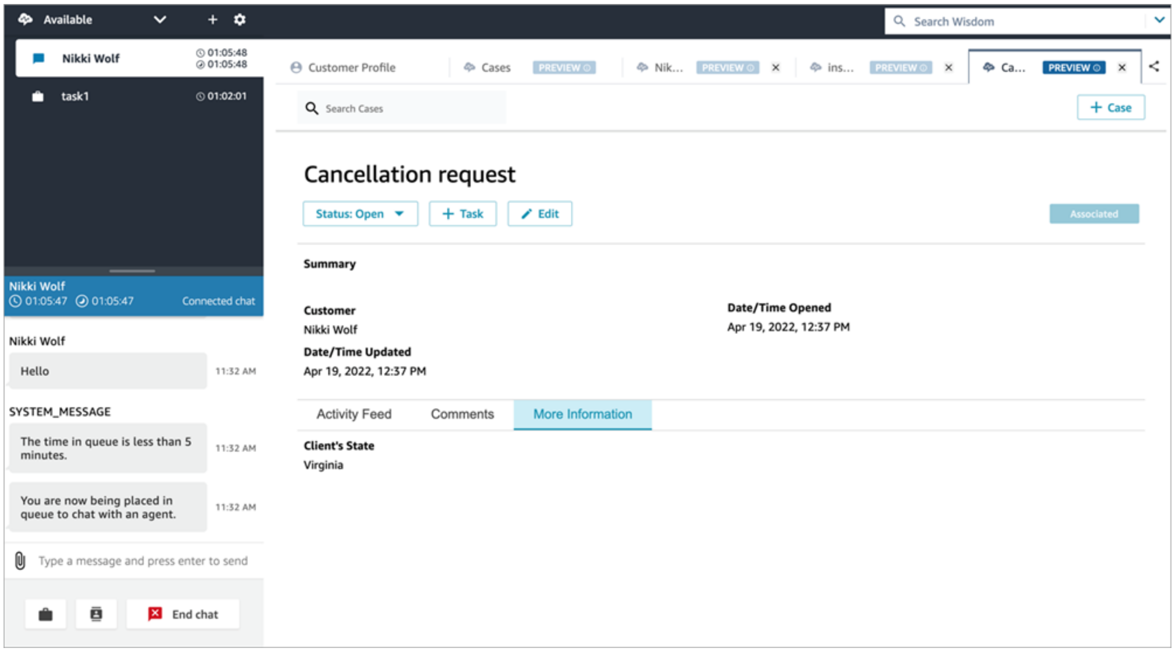
Case templates are forms that ensure agents collect and reference the right information for different types of customer issues. For example, you can create a case template for vehicle damage issues, and require agents complete certain fields when they talk to a customer filing an insurance claim.

When you create a case template, you choose the name that appears to agents, the fields on the form, and the order of the fields.

> **Important**
> Cases are always created based on a template.

How case templates look in the agent application

In the agent application, the agent sees the case fields in a Z-formation: case fields are displayed in two columns from left to right, top to bottom.



Nikki Wolf
01:05:47 01:05:47 Connected chat

Nikki Wolf
Hello 11:32 AM

SYSTEM_MESSAGE
The time in queue is less than 5 minutes. 11:32 AM
You are now being placed in queue to chat with an agent. 11:32 AM

Cancellation request

Summary

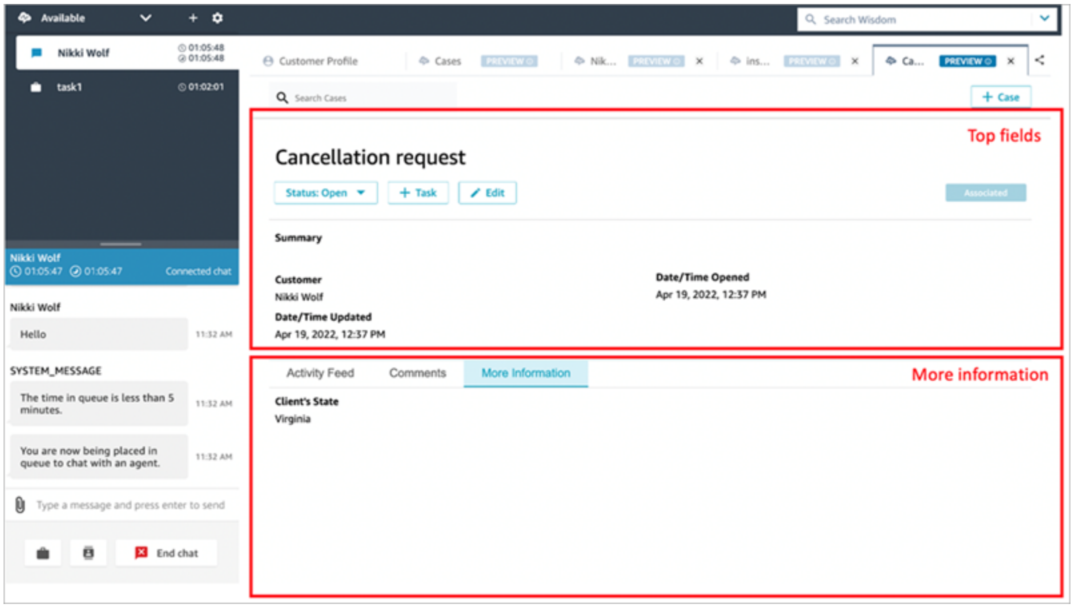
Customer
Nikki Wolf

Date/Time Opened
Apr 19, 2022, 12:37 PM

Date/Time Updated
Apr 19, 2022, 12:37 PM

Client's State
Virginia

When you're building a case template, think of the information in the agent application as being is divided into two sections where case fields are displayed to the agent:



Nikki Wolf
01:05:47 01:05:47 Connected chat

Nikki Wolf

Hello 11:32 AM

SYSTEM_MESSAGE

The time in queue is less than 5 minutes. 11:32 AM

You are now being placed in queue to chat with an agent. 11:32 AM

Cancellation request

Summary

Customer
Nikki Wolf

Date/Time Opened
Apr 19, 2022, 12:37 PM

Date/Time Updated
Apr 19, 2022, 12:37 PM

Client's State
Virginia

- Top fields: This section is always visible on the case, even when agent is viewing sub-sections of the case (for example, **Activity Feed** or **Comments**).
- More information: This is a tabbed subsection of the case. It is visible when agent is viewing another subsection, such as **Activity Feed** or **Comments**.

When you create and edit a template, you can do the following in each section:

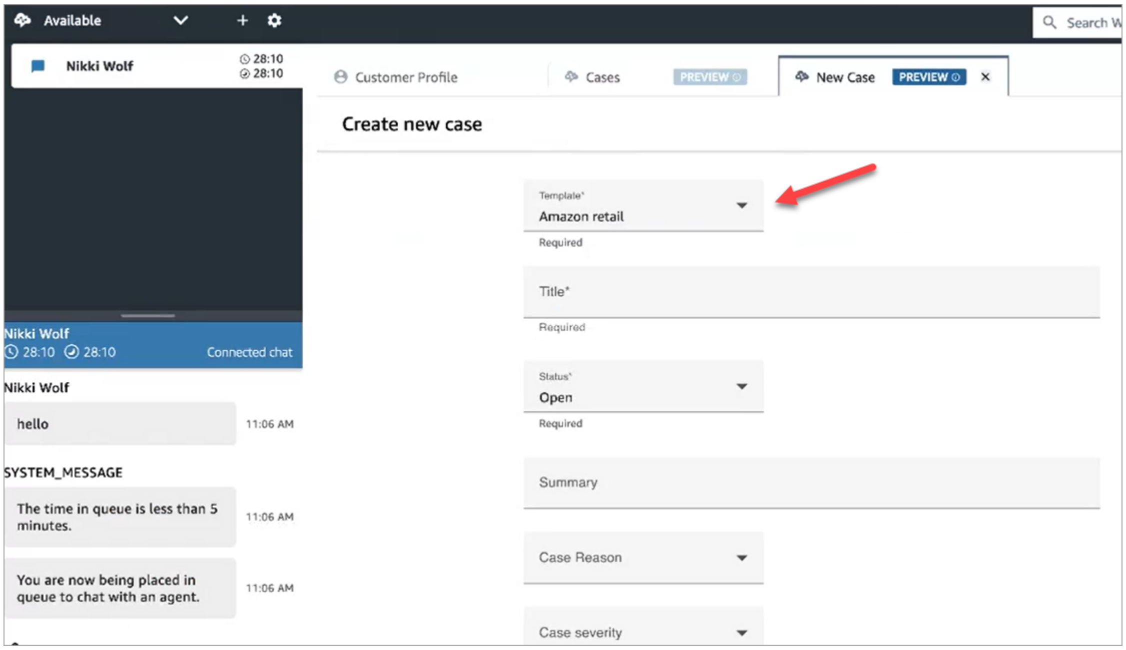
- Change the order of the fields.
- Indicate if fields are required.

Some system fields, such as **Title** and **Status**, appear on all cases and are required. Other system fields, such as **Customer**, **Summary**, and **Reference number**, appear by default on the case details page. You can remove or rearrange these fields.

Each case that is created is connected to a customer profile from your Amazon Connect instance. On new case templates, the customer name appears by default on the case details page. You can remove or rearrange this field from your templates from the Amazon Connect console.

How to create a template

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to create templates. For a list of required permissions, see Security profile permissions for Cases (Preview) (p. 734).
2. Verify the quota for case templates and request an increase if needed. For more information, see Amazon Connect Cases service quotas (Preview) (p. 1208).
3. Verify the case fields (p. 736) you want to add to your case template have already been created.
4. In the left navigation bar, choose **Agent applications**, **Case templates**.
5. Choose **+ New Template**.
6. Assign a name to the template. It will appear to agents in the agent application. The following image shows an example of how templates appear, by default in alphabetical order:



Nikki Wolf 28:10 28:10

Create new case

Template* Amazon retail Required

Title* Required

Status* Open Required

Summary

Case Reason

Case severity

Nikki Wolf

hello 11:06 AM

The time in queue is less than 5 minutes. 11:06 AM

You are now being placed in queue to chat with an agent. 11:06 AM

7. In the **Top fields** section, you'll see some system fields already there. Choose **Add fields**, and use the dropdown to choose the field. Fields that are gray-out are already a part of the template. If you want agents to complete the field in order to save the form, choose **Required**.
8. In the **More information** section, choose the fields you want to appear.
9. When you're done, choose **Publish**. The template is immediately made available to agents in the agent application.

Case layouts (Preview)

This topic is intended for developers who are using the Amazon Connect Cases APIs.

There is an underlying resource called a *case layout* that is linked to the case template. Technically, it is the case layout that holds the display elements for a case, such as:

- Which fields to display.
- The section, either Top panel or More information.
- The order within a section to display these fields

Whereas it's the case template that mandates a particular schema, such as required case fields.

The case layout is linked to a case template.

> **Note**
> You can create a case template and not link it to a case layout. Any case created with a case template that is not linked to a case layout will display system fields in a default order.

Access Cases in the agent application (Preview)

After you enable Amazon Connect Cases, you need to take steps to make the functionality available through the agent application. This topic explains your options.

> **Tip**
> Make sure your agents have **Cases** permissions in their security profile so they can access Cases. For more information, see Security profile permissions for Cases (Preview) (p. 734).

Option 1: Use Customer Profiles with the CCP out-of-the-box

Cases is already embedded alongside the Contact Control Panel (CCP). Your agents will access the CCP and Cases in the same browser window using a link that looks like this:

- **https://*instance name*.my.connect.aws/agent-app-v2/**

If you access your instance using the **awsapps.com** domain, use the following URL:

- **https://*instance name*.awsapps.com/connect/agent-app-v2/**

For help finding your instance name, see Find your Amazon Connect instance name (p. 139).

Option 2: Embed Cases into a custom agent application

When you embed your Contact Control Panel (CCP), you have the option of showing or hiding the pre-built CCP user interface. For example, you may want to develop a custom agent application that has a user interface you design, with customized buttons to accept and reject calls. Or, you may want to embed the pre-built CCP that's included with Amazon Connect into another custom app.

Regardless of whether you display the pre-built CCP user interface, or hide it and build your own, you use the Amazon Connect Streams library to embed the CCP and Cases into the agent's application. This way, Amazon Connect Streams is initialized, and the agent can connect and authenticate to Amazon Connect, and Cases.

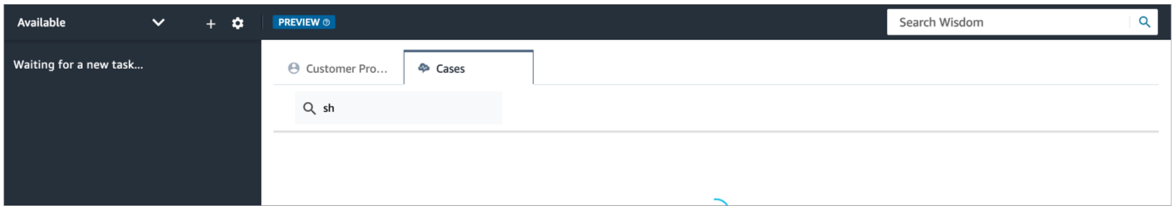
For information about embedding Cases, see Initialization for CCP, Customer Profiles, and Wisdom.

> **Tip**
> When you customize the agent's application, you determine what URL agents will use to access their agent application. This might be very different from the one provided by Amazon Connect. For example, your URL could be https://example-corp.com/agent-support-app.

How agents use Cases (Preview)

A case represents a customer's issue. A case is created to record the customer's issue, the steps and interactions taken to resolve the customer's issue, and the outcome.

If you have permission to view cases then you will see the **Cases** tab in the Amazon Connect agent application. The following image shows an example **Cases** tab.

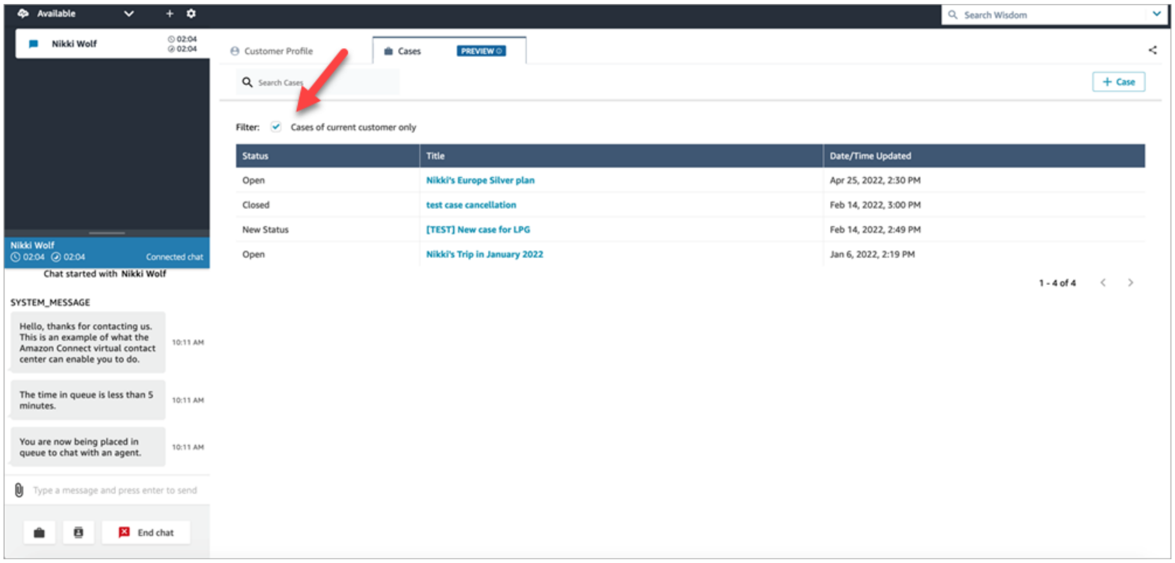


Contents

Search and view cases (Preview)

You can search cases using a keyword match. Amazon Connect searches data across all system and custom fields. The results are sorted from most-recently to least-recently updated case.

If you are on a contact, and the contact has been associated to a customer profile, then search automatically filters to cases of current customer.



Filter: ☑ Cases of current customer only

Status	Title	Date/Time Updated
Open	Nikki's Europe Silver plan	Apr 25, 2022, 2:30 PM
Closed	test case cancellation	Feb 14, 2022, 3:00 PM
New Status	[TEST] New case for LPG	Feb 14, 2022, 2:49 PM
Open	Nikki's Trip in January 2022	Jan 6, 2022, 2:19 PM

Chat started with Nikki Wolf

SYSTEM_MESSAGE

Hello, thanks for contacting us. This is an example of what the Amazon Connect virtual contact center can enable you to do. 10:11 AM

The time in queue is less than 5 minutes. 10:11 AM

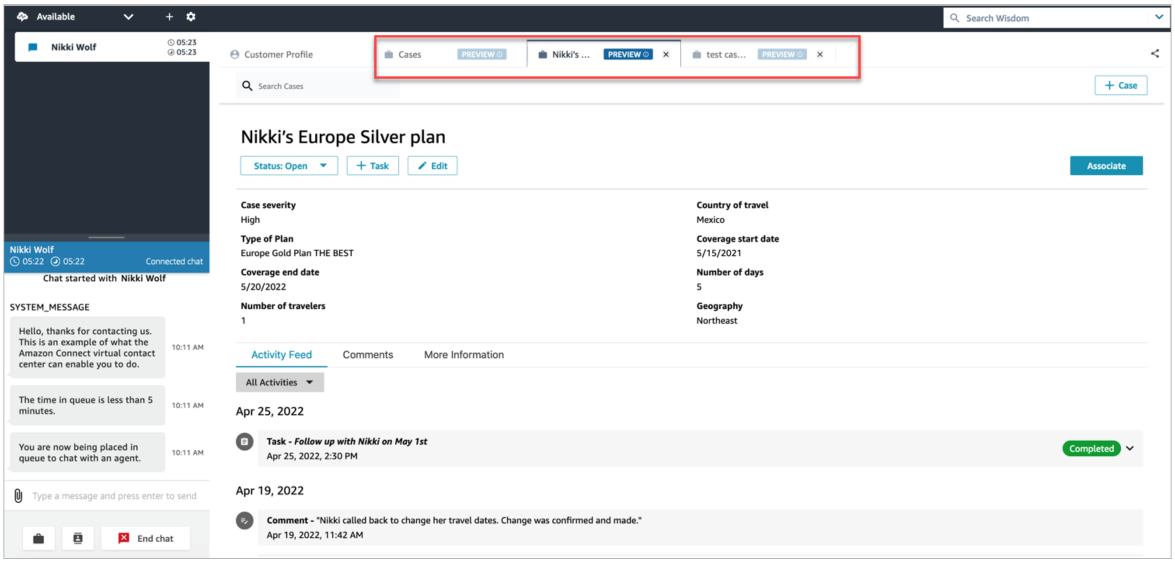
You are now being placed in queue to chat with an agent. 10:11 AM

Regardless of whether you are on a contact, you have the option to do a general search. If you are on a contact and want to search beyond the current customer, clear the selection for **Cases of current customer only**.

View a case

When you select any of the cases in the search results to view the case, a new tab opens. This enables you to have multiple cases open at the same time.

If you add a Cases (p. 344) block to a flow, and configure it with **Link contact to case** enabled, then cases will open automatically when the agent accepts the contact.



Nikki Wolf 05:23 05:23

Nikki Wolf 05:22 05:22 Connected chat

Chat started with Nikki Wolf

SYSTEM_MESSAGE

Hello, thanks for contacting us. This is an example of what the Amazon Connect virtual contact center can enable you to do. 10:11 AM

The time in queue is less than 5 minutes. 10:11 AM

You are now being placed in queue to chat with an agent. 10:11 AM

Type a message and press enter to send

Nikki's Europe Silver plan

Case severity High	**Country of travel** Mexico
Type of Plan Europe Gold Plan THE BEST	**Coverage start date** 5/15/2021
Coverage end date 5/20/2022	**Number of days** 5
Number of travelers 1	**Geography** Northeast

Apr 25, 2022

Task - *Follow up with Nikki on May 1st* Completed
Apr 25, 2022, 2:30 PM

Apr 19, 2022

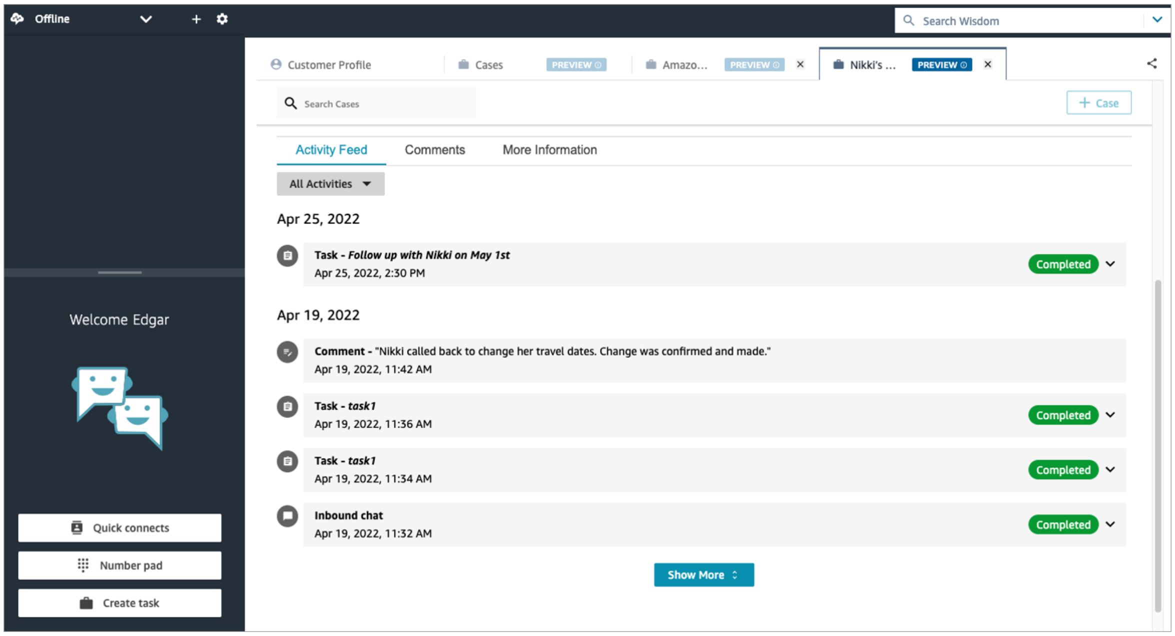
Comment - "Nikki called back to change her travel dates. Change was confirmed and made."
Apr 19, 2022, 11:42 AM

Activity feed

The activity feed shows calls, chats, tasks, and comments from the most recent to least recent Started data.

Contacts will have an indicator of Ongoing or Completed. If the contact was completed, there will a Completed/Terminated date/time and a link to **Contact details** that takes user directly to the **Contact details** page.

Only users that have access to this page will be able to see contact details for a given contact. Even within this page, there are more granular permissions so different users may see different information. Information might include: basic contact details/contact attachments, transcripts and recordings with Contact Lens categories, sentiment, and summaries, recordings, etc.



Apr 25, 2022

Task - *Follow up with Nikki on May 1st* Completed
Apr 25, 2022, 2:30 PM

Apr 19, 2022

Comment - "Nikki called back to change her travel dates. Change was confirmed and made."
Apr 19, 2022, 11:42 AM

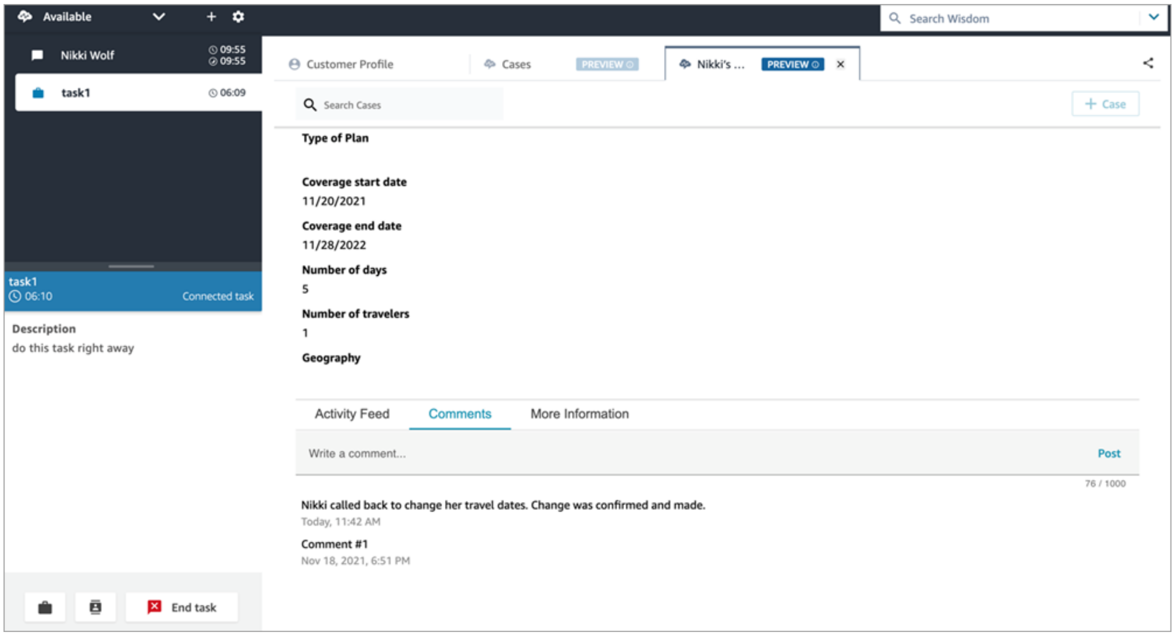
Task - *task1* Completed
Apr 19, 2022, 11:36 AM

Task - *task1* Completed
Apr 19, 2022, 11:34 AM

Inbound chat Completed
Apr 19, 2022, 11:32 AM

Comments

Agents have the ability to view and add comments.



Description
do this task right away

Type of Plan

Coverage start date
11/20/2021

Coverage end date
11/28/2022

Number of days
5

Number of travelers
1

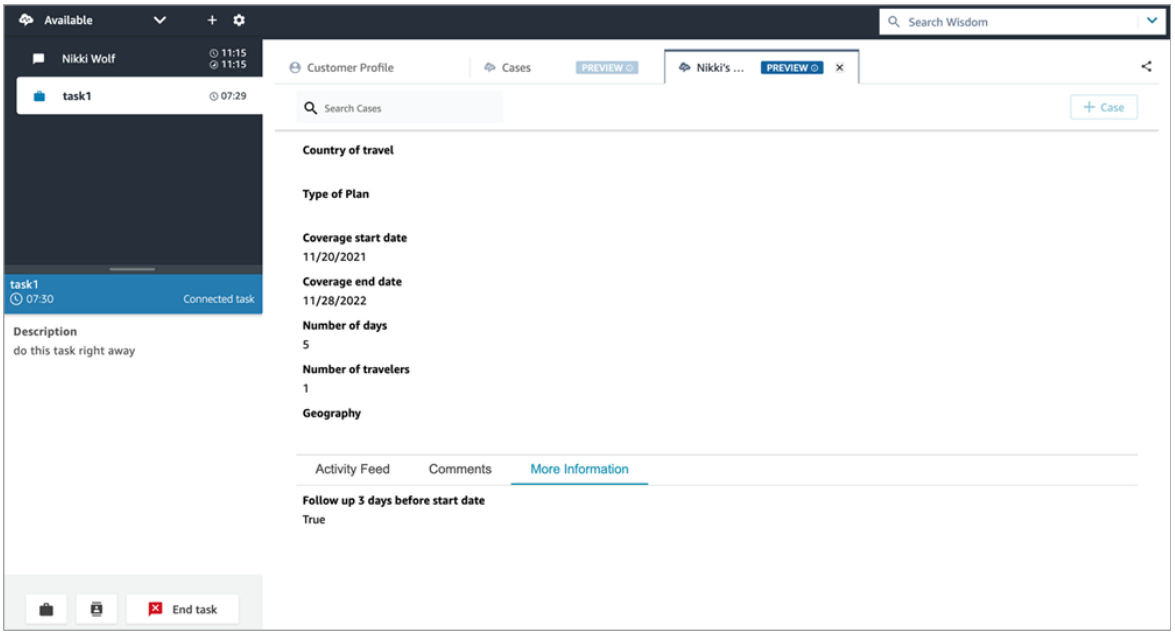
Geography

Nikki called back to change her travel dates. Change was confirmed and made.
Today, 11:42 AM

Comment #1
Nov 18, 2021, 6:51 PM

More information

There may be additional information for agents to view and populate on the **More information** tab, depending on the case template is designed.



Description
do this task right away

Country of travel

Type of Plan

Coverage start date
11/20/2021

Coverage end date
11/28/2022

Number of days
5

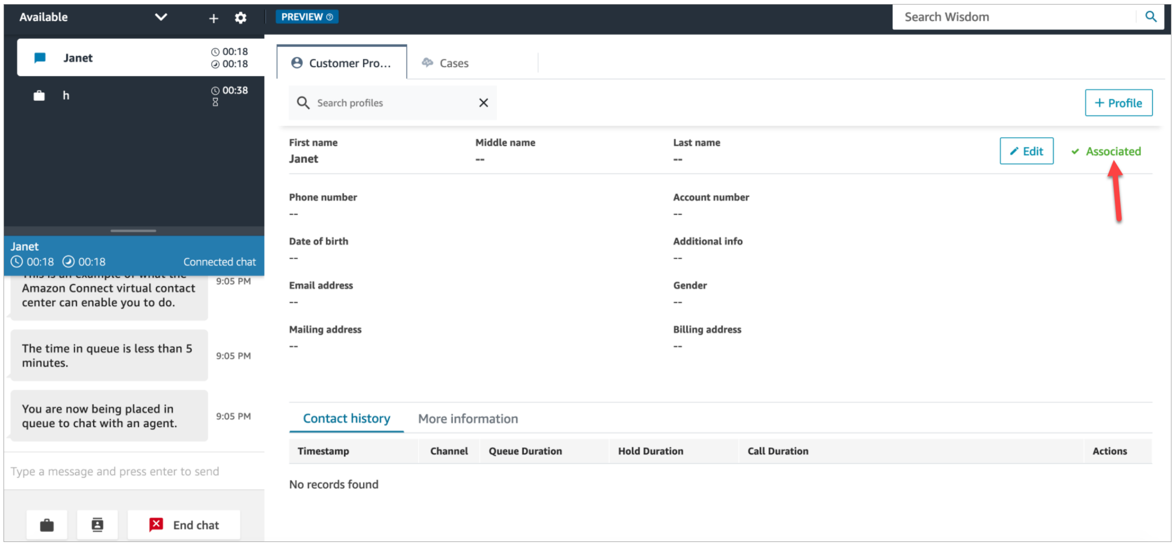
Number of travelers
1

Geography

Follow up 3 days before start date
True

Create a case (Preview)

To create a case, you must be on a contact (call, chat, or task) and have associated the contact with a customer profile, as shown in the following image.



Janet 00:18 00:18

h 00:38

Janet 00:18 00:18 Connected chat

This is an example of what the Amazon Connect virtual contact center can enable you to do. 9:05 PM

The time in queue is less than 5 minutes. 9:05 PM

You are now being placed in queue to chat with an agent. 9:05 PM

Type a message and press enter to send

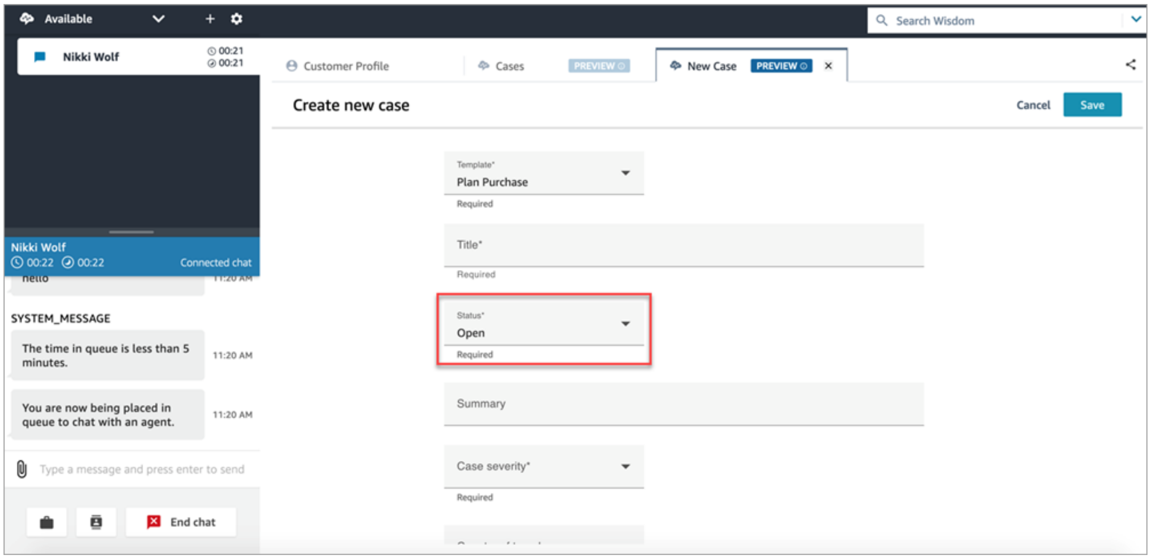
First name: Janet
Middle name: --
Last name: --
Phone number: --
Account number: --
Date of birth: --
Additional info: --
Email address: --
Gender: --
Mailing address: --
Billing address: --

Timestamp	Channel	Queue Duration	Hold Duration	Call Duration	Actions

No records found

For a case to be created:

- The **Status** must be **Open**.



Nikki Wolf 00:21 00:21

Nikki Wolf 00:22 00:22 Connected chat

hello 11:20 AM

SYSTEM_MESSAGE

The time in queue is less than 5 minutes. 11:20 AM

You are now being placed in queue to chat with an agent. 11:20 AM

Type a message and press enter to send

Create new case

Template*: Plan Purchase (Required)

Title* (Required)

Status*: Open (Required)

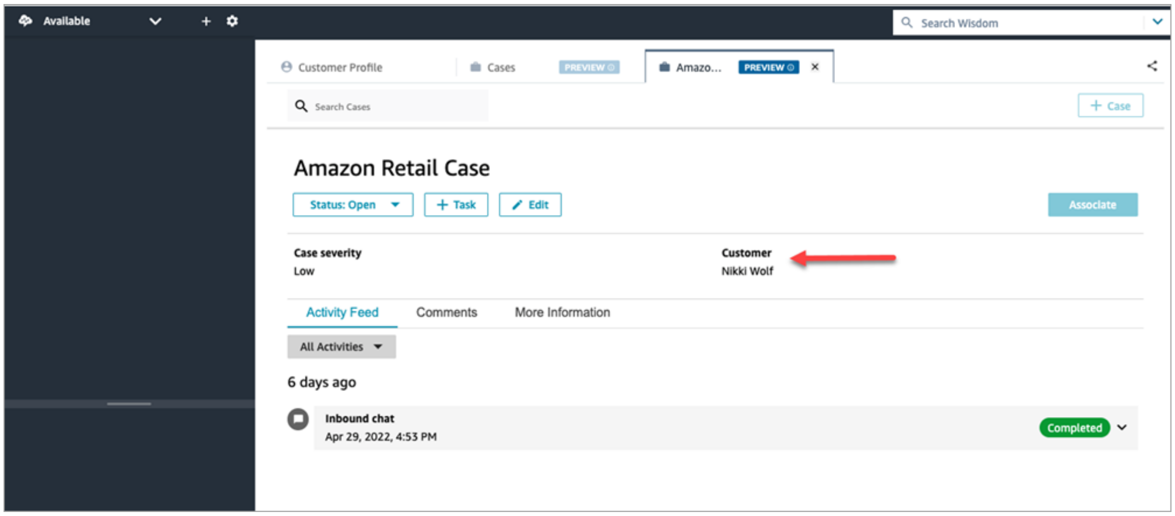
Summary

Case severity* (Required)

- All required fields must be filled in.

Customer name

Each case that is created is connected to a customer profile from your Amazon Connect instance. On new case templates, the "customer" name appears by default on the case details page. You can rearrange this field on your case template, or even remove it entirely.



Amazon Retail Case

Case severity
Low

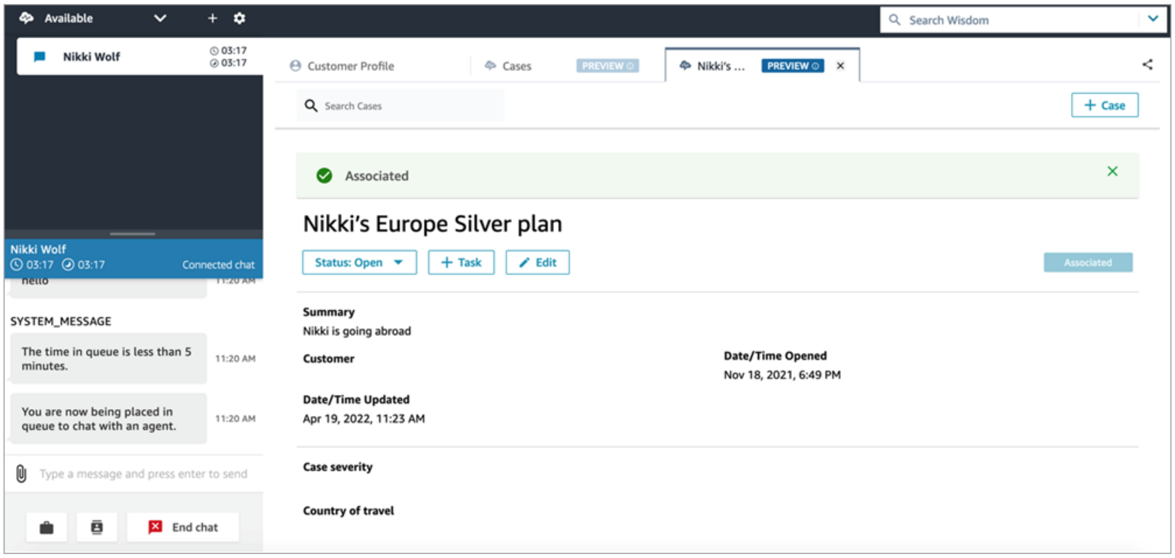
Customer
Nikki Wolf

6 days ago

Inbound chat
Apr 29, 2022, 4:53 PM

Associate a contact with a case (Preview)

The agent can associate the contact to an existing case, such that the contact will appear on the activity feed of the case with indicator **Ongoing**.



hello 11:20 AM

SYSTEM_MESSAGE

The time in queue is less than 5 minutes. 11:20 AM

You are now being placed in queue to chat with an agent. 11:20 AM

Nikki's Europe Silver plan

Summary
Nikki is going abroad

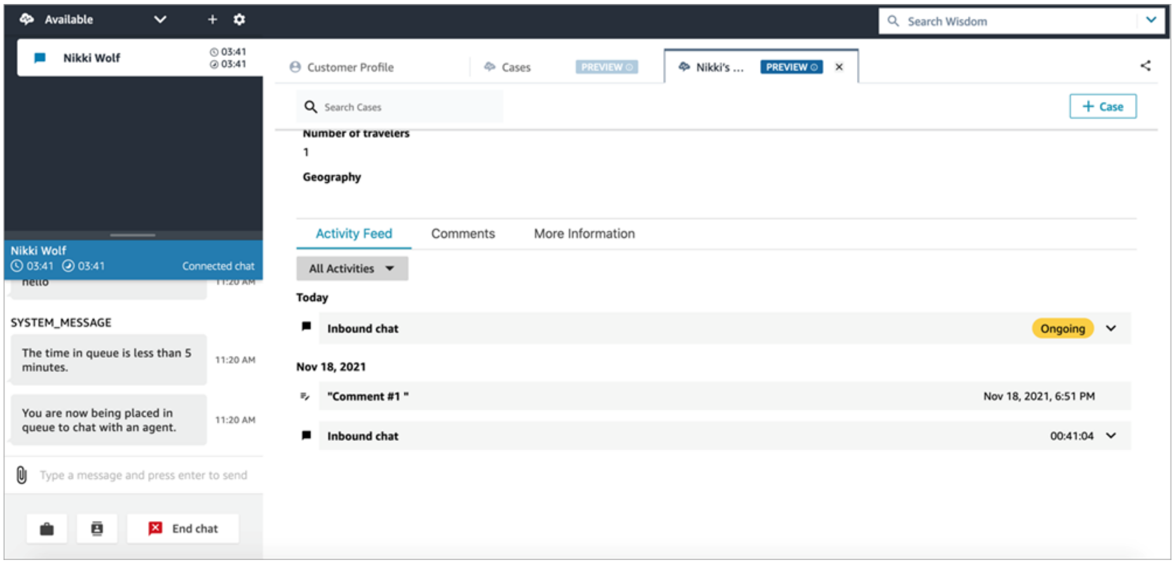
Customer

Date/Time Opened
Nov 18, 2021, 6:49 PM

Date/Time Updated
Apr 19, 2022, 11:23 AM

Case severity

Country of travel



Number of travelers
1
Geography

The time in queue is less than 5 minutes.

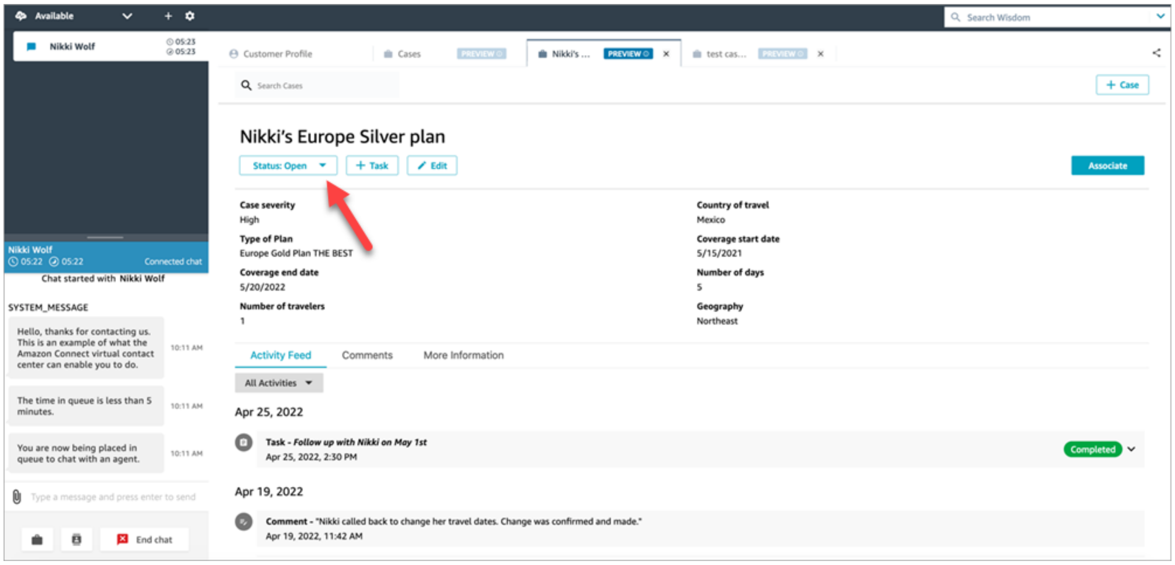
You are now being placed in queue to chat with an agent.

"Comment #1 "

Edit a case (Preview)

To edit a case, the agent chooses **Edit** and **Save** to save any changes.

You can edit a case only when it is not in a **Closed** status. If the case is **Closed**, you must update the status, then choose **Edit** to make your changes.



Nikki's Europe Silver plan

Case severity
High

Type of Plan
Europe Gold Plan THE BEST

Coverage end date
5/20/2022

Number of travelers
1

Country of travel
Mexico

Coverage start date
5/15/2021

Number of days
5

Geography
Northeast

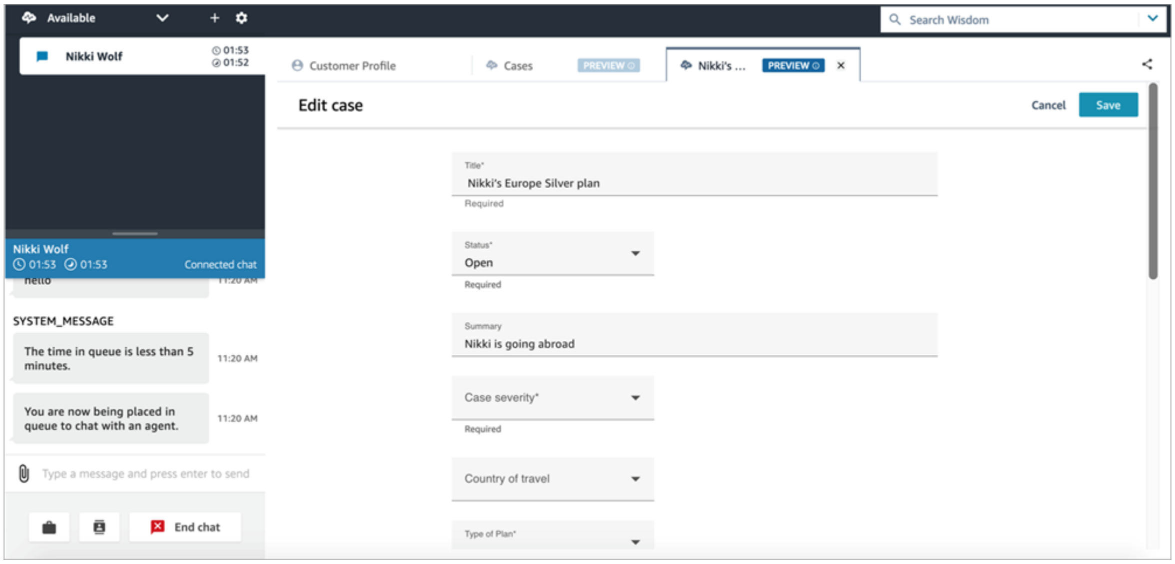
Hello, thanks for contacting us. This is an example of what the Amazon Connect virtual contact center can enable you to do.

The time in queue is less than 5 minutes.

You are now being placed in queue to chat with an agent.

Task - *Follow up with Nikki on May 1st*
Apr 25, 2022, 2:30 PM

Comment - "Nikki called back to change her travel dates. Change was confirmed and made."
Apr 19, 2022, 11:42 AM



The time in queue is less than 5 minutes.

You are now being placed in queue to chat with an agent.

Title*: Nikki's Europe Silver plan (Required)

Status*: Open (Required)

Summary: Nikki is going abroad

Case severity* (Required)

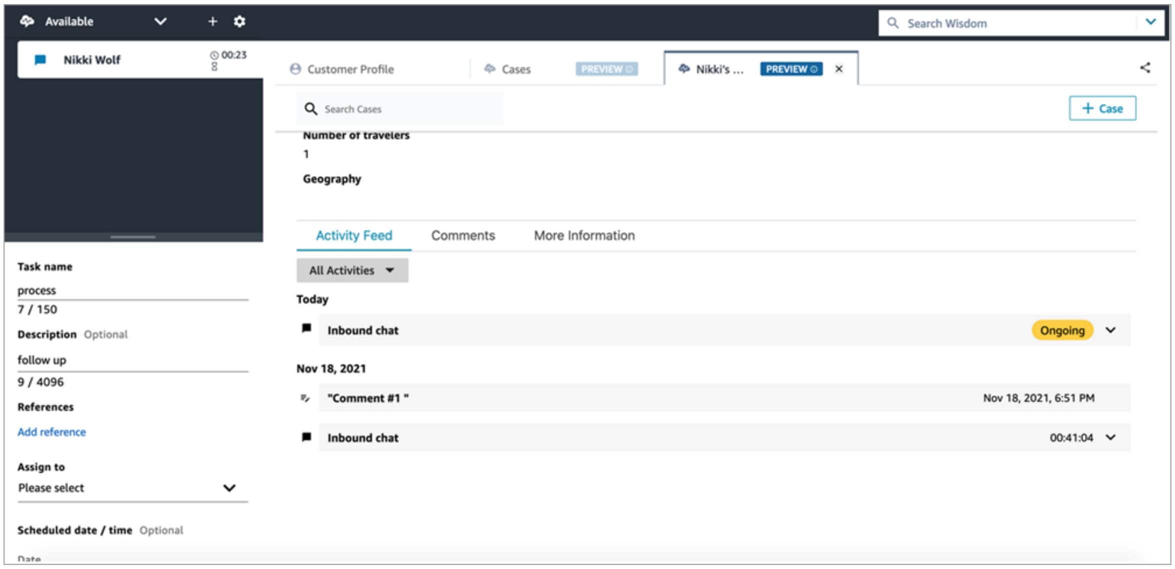
Country of travel

Type of Plan*

Create a task from a case (Preview)

In the agent application, agents can add a task from a case. In the Contact Control Panel (CCP), they will see the task creation form.

When an agent creates a task from a case, the task is automatically associated with the case and it appears on the activity feed.



Task name: process (7 / 150)

Description Optional: follow up (9 / 4096)

References

Assign to: Please select

Scheduled date / time Optional

Date

Number of travelers: 1

Geography

Today
Inbound chat — Ongoing

Nov 18, 2021
"Comment #1 " — Nov 18, 2021, 6:51 PM
Inbound chat — 00:41:04

Case event streams (Preview)

Amazon Connect Cases event streams provide you with near real-time updates when cases are created or modified within your Amazon Connect Cases domain. The events published to the stream include these resource events:

- Case created

- Cases modified
- Related items (Comments, Calls, Chats, Tasks) are added to a case

You can use the case event streams to integrate streams into your data lake solutions, create dashboards that display case performance metrics, implement business rules or automated actions based on case events, and configure alerting tools to trigger custom notifications of specific case activity.

Contents

Set up case event streams (Preview)

This topic explains how to set up and use case event streams as part of the Amazon Connect Cases Preview. Since this is a preview release, some of the onboarding steps require you to call Amazon Connect Cases APIs.

Step 1: Create an Amazon Connect instance and enable Customer Profiles

1. Ensure you have an working Amazon Connect instance in the US East (N. Virginia) or US West (Oregon) AWS Region. Cases Preview is available only in US East (N. Virginia) and US West (Oregon).

   For information about creating an instance, see Create an Amazon Connect instance (p. 135).
2. Enable Amazon Connect Customer Profiles. For instructions, see Enable Customer Profiles for your instance (p. 641).

   Amazon Connect Cases requires Customer Profiles because each case must be associated with a customer profile from the Customer Profiles service.

Step 2: Configure your AWS CLI to call Cases APIs

In this step, you will make few API calls to setup and work with case event streams successfully.

1. If you need to install or update AWS CLI, see Configuration basics in the *AWS Command Line Interface User Guide*.
2. Run the following command to configure your AWS CLI Region, output format, and credentials:

```
aws configure

AWS Access Key ID [None]: access key for iam user with connect:*, cases:*, profile:*
 permissions
AWS Secret Access Key [None]: secret key for iam user with connect:*, cases:*,
 profile:* permissions
Default region name [None]: the AWS Region of your Amazon Connect instance
Default output format [None]: json
```

3. By default, AWS CLI is included with AWS services that are in General Availability. Since Amazon Connect Cases is in Preview, you need to configure the AWS CLI so that the Amazon Connect Cases APIs are available. Do the following steps:

   a. Download `AmazonConnectCases_CLI_Model.json` to your computer.

b. Run the following command:

```
aws configure add-model --service-name cases --service-model file://path
to the AmazonConnectCases_CLI_Model.json file
```

c. Run the following command to see if the Case APIs are available to the AWS CLI:

```
aws cases help
```

Step 3: Add a Cases domain to your Amazon Connect instance

For instructions, see Enable Cases (Preview) (p. 733).

If you want to add a case domain using the API, see the CreateDomain API in the *Amazon Connect Cases API Reference*.

Step 4: Create a case template

Create a case template (p. 740). In *Step 6: Test case event streams*, you'll use the template.

If you want to create a case template using the API, see the CreateTemplate API in the *Amazon Connect Cases API Reference*.

Step 5: Enable case event streams and setup to receive events into an SQS queue

Run the following command to enable case event streams for your Cases domain. After this command runs, when cases are created or updated, an event is published to the default-bus of the EventBridge service in your account (it must be in the same AWS Region as your Cases domain).

```
aws cases put-case-event-configuration --domain-id cases-domain-id --event-
bridge '{"enabled": true}'
```

By default, the events published by Amazon Connect Cases only contain metadata about the case, such as `templateId`, `caseId`, `caseArn`, `approximateChangeTime`, and more. You can run the following command to get more information about the case (at the time the event was generated) to be included in the event.

```
# You can include any other field defined in your cases domain in the fields section.
# If you want to know what fields are defined in your cases domain, you can call list-
fields API.
aws cases put-case-event-configuration --domain-id cases-domain-ID --event-bridge '{
            "enabled": true,
            "includedData": {
              "caseData": {
                "fields": [
                  {
                    "id": "status"
                  },
                  {
                    "id": "title"
                  },
                  {
                    "id": "customer_id"
                  }
                ]
              },
              "relatedItemData": {
                "includeContent": true
            }
          }
        }'
```

Next, create an Amazon SQS queue and set that as a target for the Amazon Connect Cases events on your EventBridge bus so that all the case events are delivered to the SQS queue for later processing.

```
# Create an SQS queue
aws sqs create-queue --queue-name case-events-queue

# Create an rule on the EventBridge defualt bus that represents the case events
aws events put-rule --name case-events-to-sqs-queue --event-pattern '{"source":
 ["aws.cases"]}' --state ENABLED

# Ask event bridge to publish case events to the SQS queue.
aws events put-targets --rule case-events-to-sqs-queue --target '[
            {
              "Id": "target-1",
              "Arn": "arn:aws:sqs:The AWS Region of your Amazon Connect instance:your AWS
 account ID:case-events-queue"
            }]'
```

Step 6: Test case event streams

Use the Amazon Connect agent application to:

1. Accept a chat contact.
2. Create a customer profile and associate that to the chat contact.
3. Create a case.

> **Note**
> The **Create case** button on the **Cases** tab is inactive until you accept a contact and associate that contact with a customer profile.

For this preview, navigate to the Amazon SQS console and check that a case event (type: `CASE.CREATED`) for the newly created case is available in your SQS Queue. Similarly, you can modify the case created above and get a corresponding case event (type: `CASE.UPDATED`) in your SQS queue. You can associate the contact to the case, and leave a comment on the case to get case events for those actions, too.

Step 7: Use cases for the case event streams

Case event streams publish events every time a case is created, case is updated, contact is associated to the case, and comment is added on a case. You can use these events for:

- Metrics, analytics and dashboards
- Build Apps that notify users (for example, send emails)
- Automated actions that are triggered based on certain type of case updates

For example, you can use the SQS target on EventBridge (as shown on step 6) to temporarily store the case events in the SQS queue, and use Lambda functions to process events in the SQS to build custom applications such as sending emails to the customer when their case is updated, automatically resolving any tasks linked to the case, and more. Similarly, you can use the Kinesis Data Firehose target on the EventBridge to store the case events into an S3 bucket and then use the AWS Glue for ETL, Athena for ad-hoc analytics, and Amazon QuickSight for dashboards.

Case event payload and schema (Preview)

When you request to include case data in the event payload, the data reflects the version of the case after that particular edit.

Amazon Connect Cases default limits guarantee that the payload will be less than 256KB (the maximum size of an Eventbus event). Since you can customize the case object model (for example, you can define custom fields on case objects to capture business specific information), case event schema reflect the customizations made to the case object as shown in the following examples (for example, see how customer-specific UUIDs are being use as JSON properties).

Example case event payload for the case resource

```
// Given the limits on the "includedData" configuration
// this payload is guaranteed to less than 256KB at launch.
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Amazon Connect Cases Event",
    "source": "aws.cases",
    "account": "your AWS account ID",
    "time": "2022-03-16T23:43:26Z",
    "region": "The AWS Region of your Amazon Connect instance",
    "resources": [
        "arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case
 domain ID",
        "arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case
 domain ID/case/case ID"
    ],
    "detail": {
        "version": "0",
        "eventType": "CASE.UPDATED", //(or "CASE.CREATED" or "CASE.DELETED")
        "approximateChangeTime": "2022-03-16T23:16:57.893Z",  // Can be used for ordering
        "changedFieldIds": ["status", "last_updated_datetime"],

        "case": {
            "caseId": "case ID",
            "templateId": "template ID",
            "createdDateTime": "2022-03-16T23:16:57.893Z",

            // This section contains only non-null field values for the
            // fields that customers have configured in the "includedData".

            // Field values included in this section reflects the case
            // after this particular change is applied.
            "fields": {
                "status": {
                    "value": {
                        "stringValue": "open"
                    }
                },
                "case_reason": {
                    "value": {
                        "stringValue": "Shipment lost"
                    }
                },
                "custom-field-uuid-1": {
                    "value": {
                        "stringValue": "Customer didn't receive the product"
                    }
                }
            }
        }
    }
}
```

Example case event payload for the related-item resource

```
// Given the limits on the "includedData" configuration
// this payload is guaranteed to less than 256KB
{
    "version": "0",
    "id": "event ID",
    "detail-type": "Amazon Connect Cases Event",
    "source": "aws.cases",
    "account": "your AWS account ID",
    "time": "2022-03-16T23:43:26Z",
    "region": "The AWS Region of your Amazon Connect instance",
    "resources": [
        "arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case
 domain ID",
        "arn:aws:cases:your Amazon Connect AWS Region:your AWS account ID:domain/case
 domain ID/case/case ID/related-item/related-item ID"
    ],

    "detail": {
        "version": "0",
        "eventType": "RELATED_ITEM.CREATED", //(or "RELATED_ITEM.UPDATED" or
 "CASE.RELATED_ITEM.DELETED")
        "approximateChangeTime": "2022-03-16T23:16:57.893Z", // Can be used for ordering
        "changedAttributes": ["comment.commentText"],

        "relatedItem": {
            "relatedItemType": "Comment", // (OR Contact)
            "relatedItemId": "related-item ID",
            "caseId": "case id that this related item is a sub-resource of",
            "createdDateTime": "2022-03-16T23:16:57.893Z",

            // This section includes any attributes that customers have configured
            // in the "includedData" configuration.
            "comment": {
                "body": "Gave a $5 refund to customer to make them happy",
            },

            // if the related item was of type contact.
            // "contact": {
            //      "contactArn": ".......",
            // }
        }
    }
}
```

Preview AWS CLI and AWS SDKs

> **Note**
> Amazon Connect Cases is in preview release and is subject to change. We recommend that you use the service only with test data, and not in production environments.
> While Amazon Connect Cases is in preview, you must download the preview AWS SDK and AWS CLI to use the API operations for this service. These API operations aren't available in the public AWS SDK or AWS CLI.

Because Amazon Connect Cases is in preview, you must download the AWS CLI and SDK resources from the following links to use the feature in your scripts and applications.

To install AWS SDK for Python (Boto3)

1. From a command prompt, run `python3 -V` to determine if Python 3.6 or later is installed. If you don't have it installed, follow the instructions to install Python 3.
2. Download the AwsSdkPythonCli-Cases.zip file.
3. Unzip the `AwsSdkPythonCli-Cases.zip` file to get the AwsSdkPythonCli-Cases folder.
4. Navigate to the AwsSdkPythonCli-Cases directory where you see the `boto3-1.24.4-py3-none-any.whl` file.
5. To install AWS SDK for Python (Boto3), run the following command.

   ```
   python3 -m pip install boto3-1.24.4-py3-none-any.whl
   ```

For more information about how to use AWS SDK for Python (Boto), see the AWS SDK for Python (Boto) Documentation.

Configure the AWS CLI

To enable Amazon Connect Cases commands in the AWS CLI, complete these steps.

From a command prompt, run `aws --version` to determine if the AWS CLI is installed. If you don't have it installed, follow the instructions to install the AWS CLI.

To enable the Amazon Connect Cases API in the AWS CLI

1. Download the cases-preview.zip file.
2. Navigate to the directory where you downloaded the `cases-preview.zip` file.
3. Unzip the file to get the `AmazonConnectCases_CLI_Model.json` file.
4. From a command prompt, run the following command:

   ```
   aws configure add-model --service-name cases --service-model file://
   AmazonConnectCases_CLI_Model.json
   ```
5. From a command prompt, run the following command to make sure Amazon Connect Cases AWS CLI commands are available:

   ```
   aws cases help
   ```

Set up pre-built integrations

Use pre-built integrations to generate tasks based on events in external applications, or create customer profiles based on data in external applications. These integrations are built on top of Amazon AppFlow and Amazon EventBridge to enable easy access to your data that's stored outside of Amazon Connect.

For more information about Amazon AppFlow and Amazon EventBridge, see the documentation: Amazon AppFlow User Guide and Amazon EventBridge User Guide.

In addition, check out the Amazon AppIntegrations Service API Reference, which enables you to access and configure AppIntegrations associations programmatically with Amazon Connect instances.

Contents

Set up applications for task creation

You can set up applications for task creation in just a few steps, no coding required. Amazon Connect uses Amazon EventBridge to pull data from your external application.

> **Tip**
> If your organization is using custom IAM policies to manage access to the Amazon Connect console, make sure users have the appropriate permissions to set up applications for task creation. For a list of required permissions, see Tasks page (p. 1090).
> If your instance was created before October 2018, for information about how to configure your service-linked roles (SLR), see For instances created before October 2018 (p. 1121).

Contents

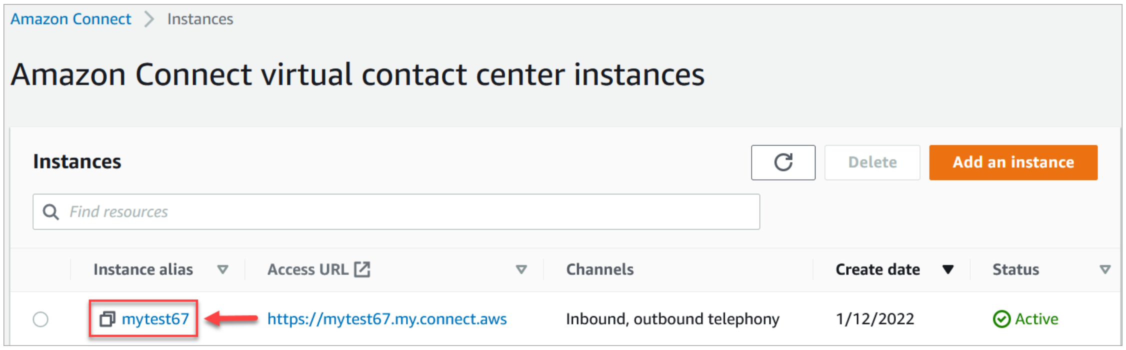
Set up application integration for Salesforce

If you integrate with Salesforce for event creation, Amazon Connect also uses Amazon AppFlow to put the data into EventBridge. This is because of how Salesforce sends events through the Amazon AppFlow APIs. To learn more about how Amazon Connect uses EventBridge and Amazon AppFlow resources to power Salesforce integrations, see this blog post: Building Salesforce integrations with Amazon EventBridge and Amazon AppFlow.

> **Note**
> If you use custom AWS Identity and Access Management (IAM) policies, for a list of the required IAM permissions to set up Amazon Connect Tasks, see Tasks page (p. 1090).

To integrate Salesforce for task creation

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.

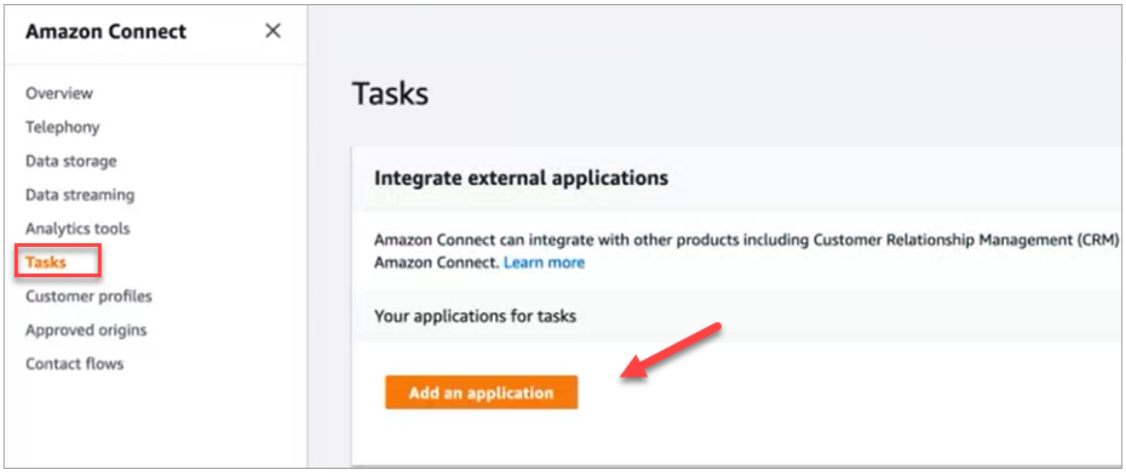


Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. Choose **Tasks**, and then choose **Add an application**.



Tasks

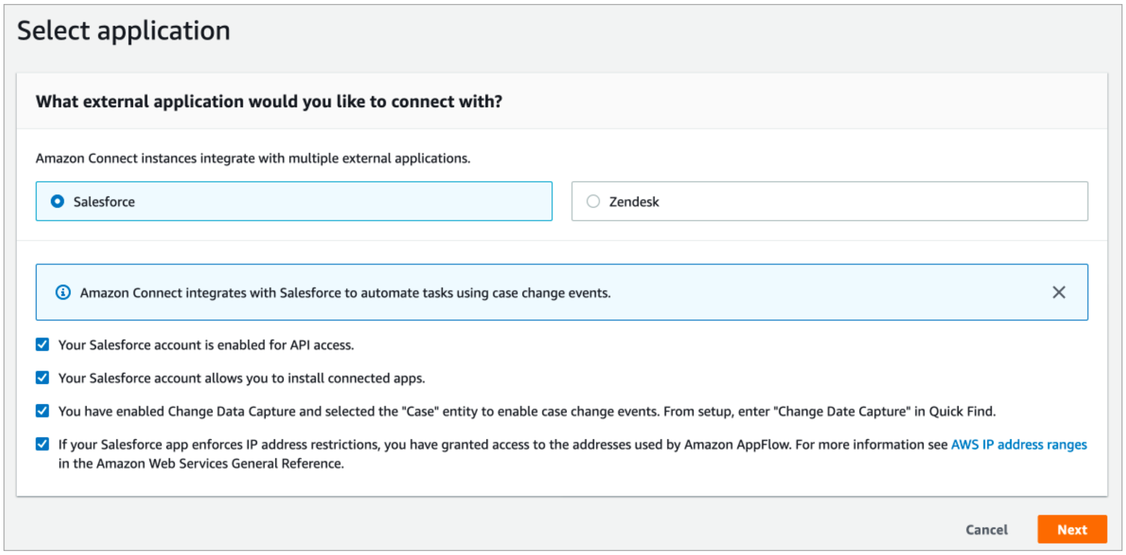
Integrate external applications

Amazon Connect can integrate with other products including Customer Relationship Management (CRM) Amazon Connect. Learn more

Your applications for tasks

4. On the **Select application** page, choose **Salesforce**.
5. Review the application requirements that are listed on the **Select application** page.

   The following image shows the requirements for Salesforce.



Select application

What external application would you like to connect with?

Amazon Connect instances integrate with multiple external applications.

● Salesforce ○ Zendesk

Amazon Connect integrates with Salesforce to automate tasks using case change events.

☑ Your Salesforce account is enabled for API access.

☑ Your Salesforce account allows you to install connected apps.

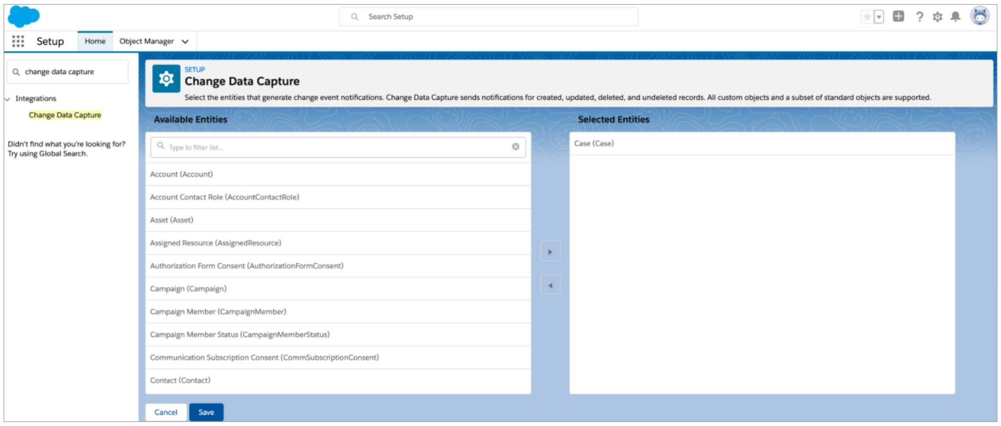
☑ You have enabled Change Data Capture and selected the "Case" entity to enable case change events. From setup, enter "Change Date Capture" in Quick Find.

☑ If your Salesforce app enforces IP address restrictions, you have granted access to the addresses used by Amazon AppFlow. For more information see AWS IP address ranges in the Amazon Web Services General Reference.

1. To verify that Salesforce is compatible with Amazon AppFlow, log in to Salesforce, for example, https://[instance_name].my.salesforce.com.

Important

Verify that you have enabled **Change Data Capture** in Salesforce. The following image shows an example **Change Data Capture** page in Salesforce where you select the Case entities:



Change Data Capture

Select the entities that generate change event notifications. Change Data Capture sends notifications for created, updated, deleted, and undeleted records. All custom objects and a subset of standard objects are supported.

Available Entities

- Account (Account)
- Account Contact Role (AccountContactRole)
- Asset (Asset)
- Assigned Resource (AssignedResource)
- Authorization Form Consent (AuthorizationFormConsent)
- Campaign (Campaign)
- Campaign Member (CampaignMember)
- Campaign Member Status (CampaignMemberStatus)
- Communication Subscription Consent (CommSubscriptionConsent)
- Contact (Contact)

Selected Entities

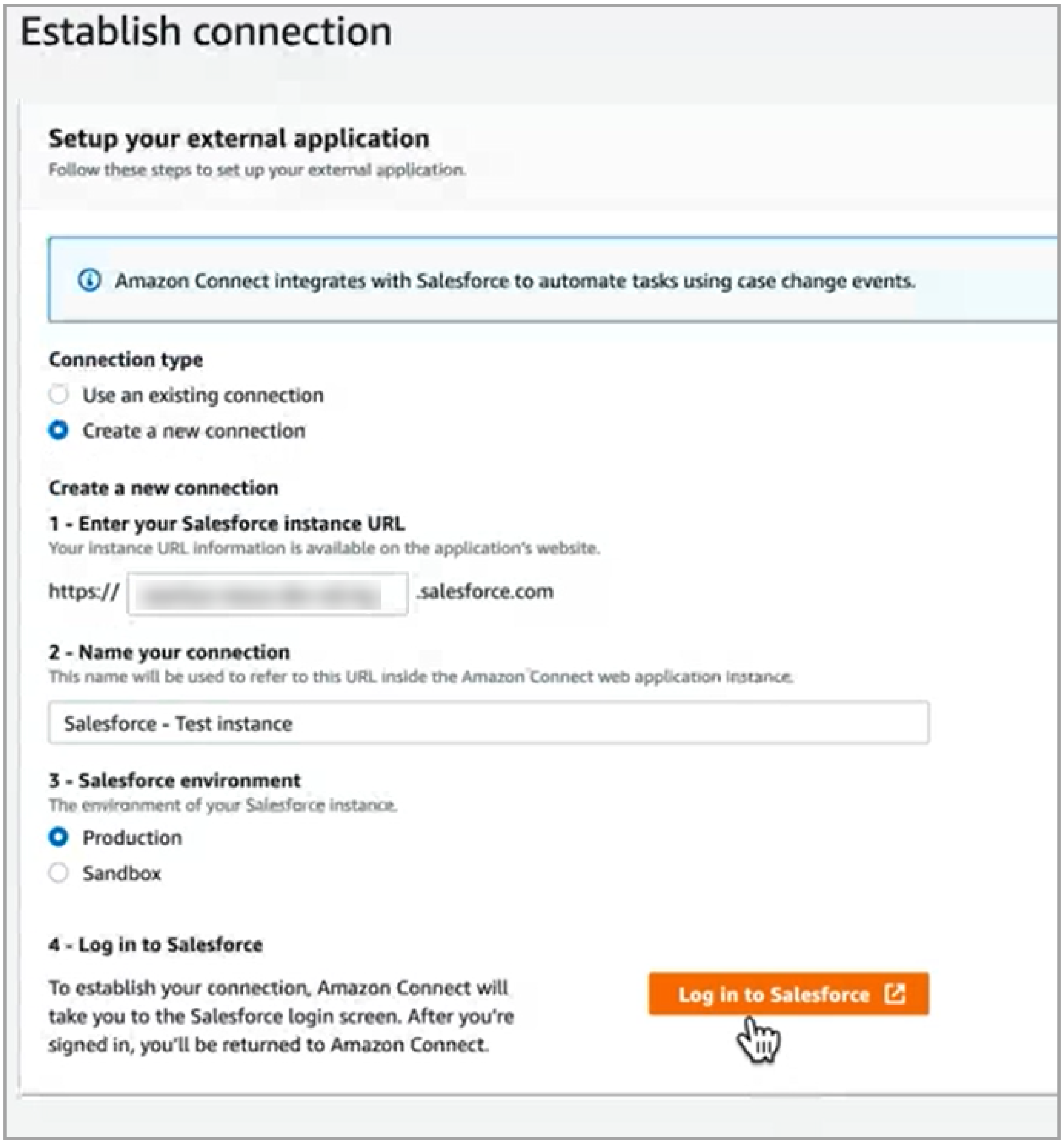
- Case (Case)

6. After you verify Salesforce requirements, on the **Select application** page, choose **Next**.

7. On the **Establish connection** page, choose one of the following:

   - **Use an existing connection**. This allows you to reuse existing EventBridgeresources that are linked to Amazon AppFlow flows that you may have created in your AWS account.
   - **Create a new connection**: Enter the information required by the external application.

     1. Enter your application instance URL. This URL is used for deep-linking into the tasks created in your external application.
     2. Provide a friendly name for your connection, for example, **Salesforce - Test instance**. Later, when you add rules (p. 602), you'll refer to this friendly name.
     3. Specify whether this is a production or sandbox environment.



Establish connection

Setup your external application

Follow these steps to set up your external application.

ⓘ Amazon Connect integrates with Salesforce to automate tasks using case change events.

Connection type

○ Use an existing connection

● Create a new connection

Create a new connection

1 - Enter your Salesforce instance URL

Your instance URL information is available on the application's website.

https:// [redacted] .salesforce.com

2 - Name your connection

This name will be used to refer to this URL inside the Amazon Connect web application instance.

Salesforce - Test instance

3 - Salesforce environment

The environment of your Salesforce instance.

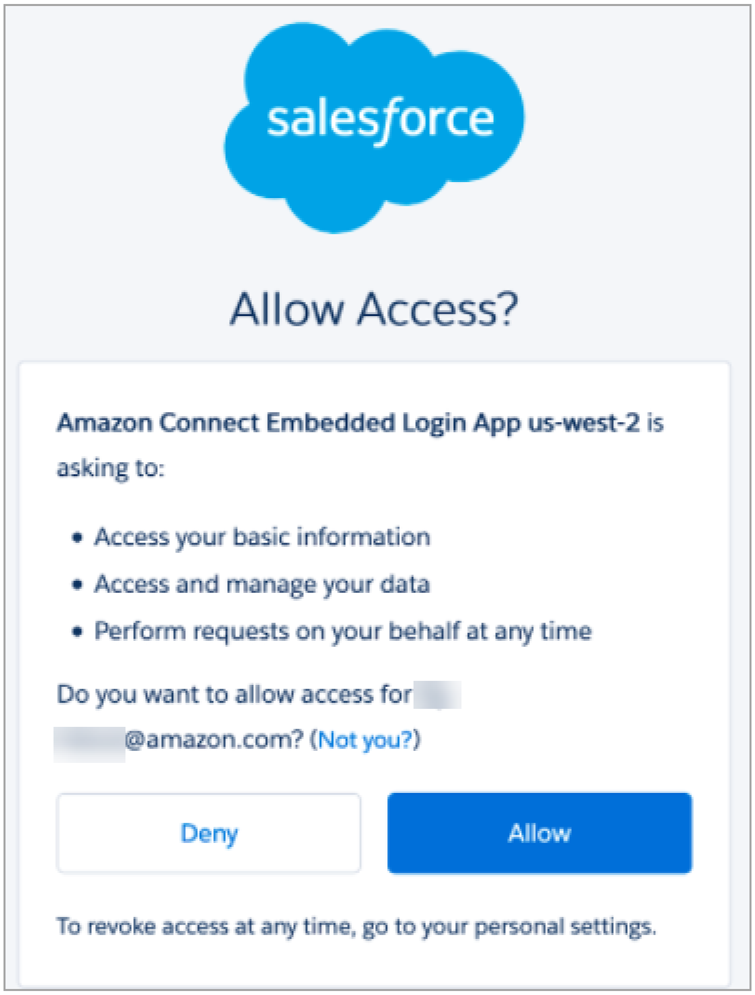
● Production

○ Sandbox

4 - Log in to Salesforce

To establish your connection, Amazon Connect will take you to the Salesforce login screen. After you're signed in, you'll be returned to Amazon Connect.

8. Choose **Log in to Salesforce**.
9. In Salesforce, choose to allow access to Amazon Connect Embedded Login App [Region].



Allow Access?

Amazon Connect Embedded Login App us-west-2 is asking to:

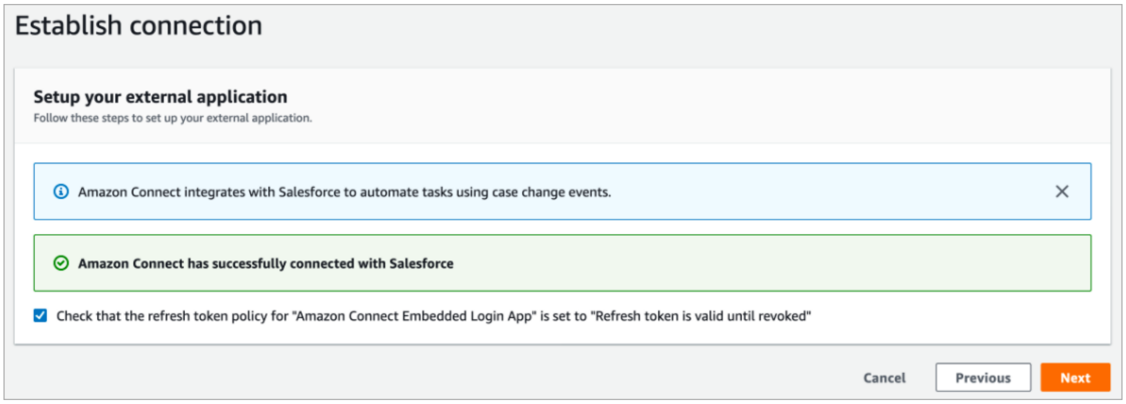
- Access your basic information
- Access and manage your data
- Perform requests on your behalf at any time

Do you want to allow access for [redacted] @amazon.com? (Not you?)

To revoke access at any time, go to your personal settings.

10. After Amazon Connect has successfully connected with the Salesforce, go to Salesforce and verify that the refresh token policy for Amazon Connect Embedded Login App is set to **Refresh token is valid until revoked**. This grants Amazon AppFlow access to pull data from your Salesforce account without re-authenticating.

11. On the **Establish connection** page, select the box shown in the following image, and choose **Next**.



Establish connection

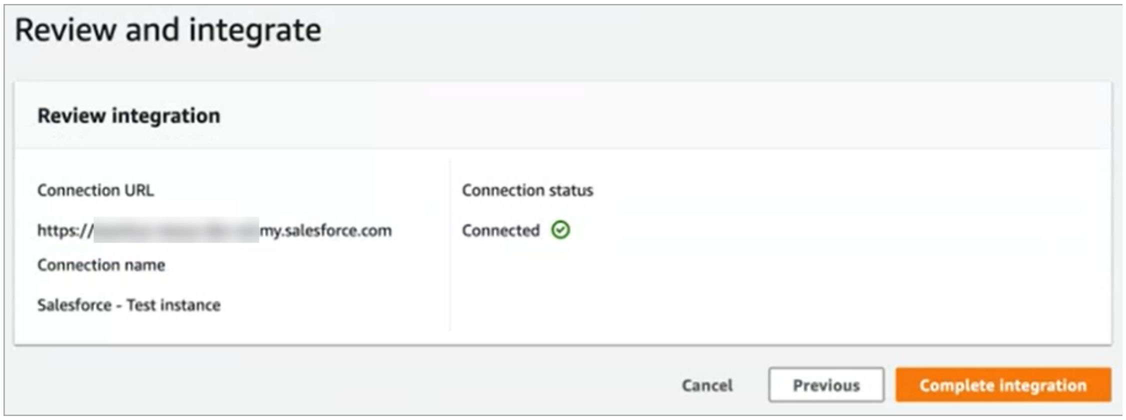
Setup your external application
Follow these steps to set up your external application.

Amazon Connect integrates with Salesforce to automate tasks using case change events.

Amazon Connect has successfully connected with Salesforce

☑ Check that the refresh token policy for "Amazon Connect Embedded Login App" is set to "Refresh token is valid until revoked"

12. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Complete integration**.



Review and integrate

Review integration

Connection URL

https://[redacted]my.salesforce.com

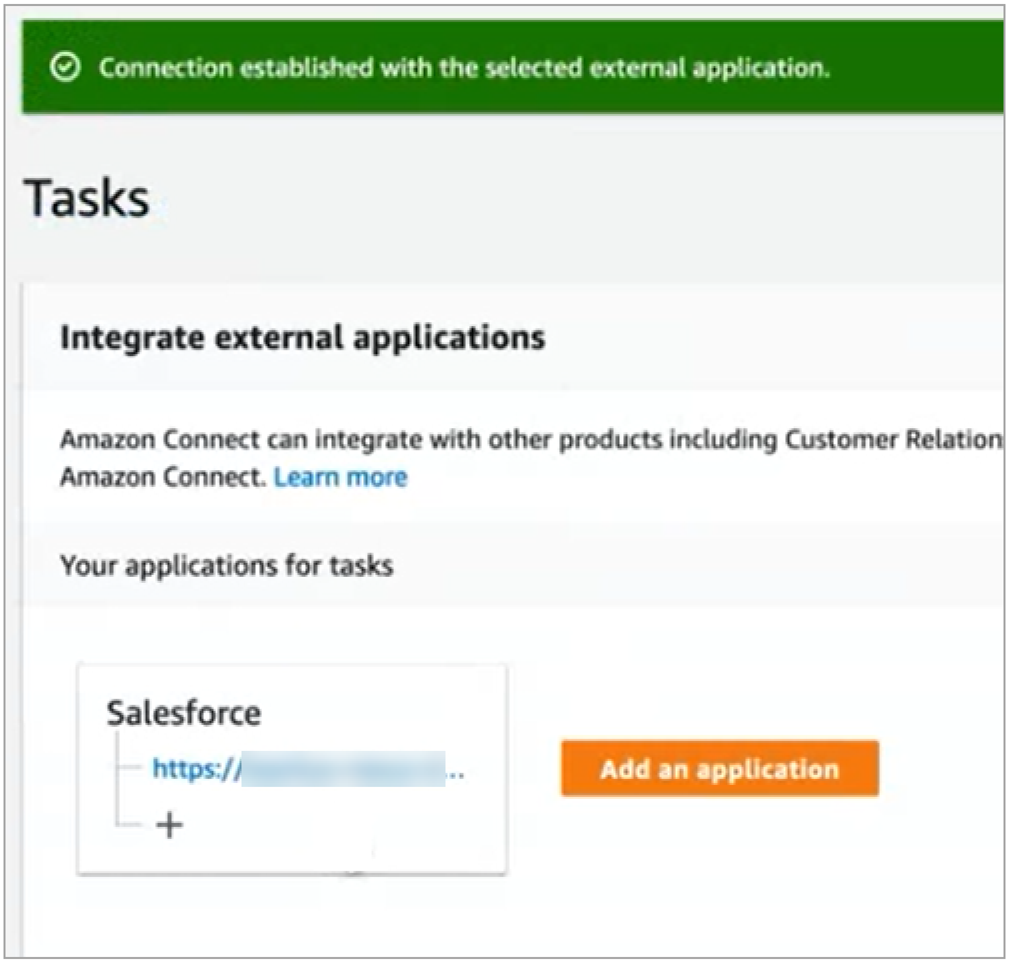
Connection name

Salesforce - Test instance

Connection status

Connected ✓

13. On the **Tasks** page, the new connection is listed.



Connection established with the selected external application.

Tasks

Integrate external applications

Amazon Connect can integrate with other products including Customer Relation
Amazon Connect. Learn more

Your applications for tasks

Salesforce

https://[redacted]..

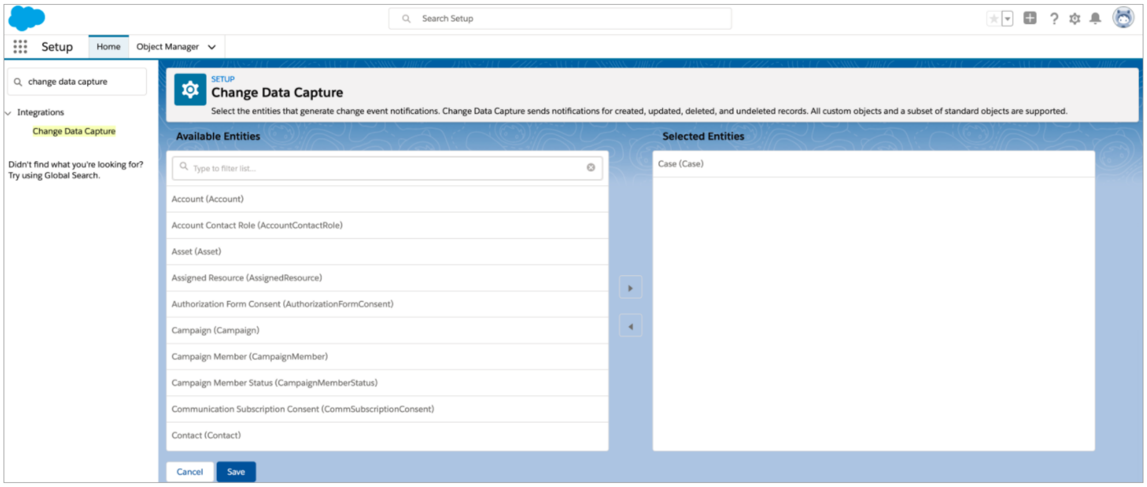
You're done! Next, add rules that tell Amazon Connect when to create a task and how to route it. For instructions, see Create rules that generate tasks for third-party integrations (p. 602).

What to do when is a connection isn't successfully established

A connection might fail to be established for Salesforce if you didn’t follow the instructions next to the check boxes to verify that it's compatible with Amazon AppFlow.

A common error is not setting up the **Case** entity in the **Change Data Capture** settings to capture these events. To fix:

1. Log in to Salesforce, go to the **Change Data Capture**, and select the Case entity.

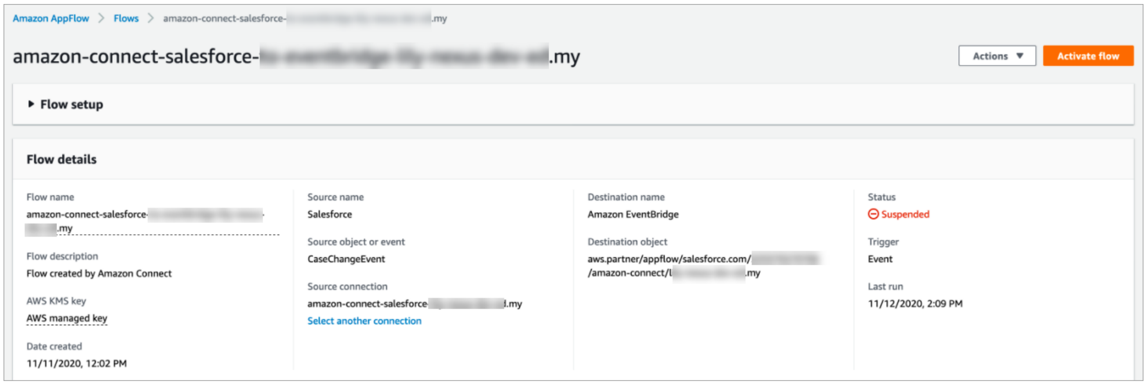


Change Data Capture

Select the entities that generate change event notifications. Change Data Capture sends notifications for created, updated, deleted, and undeleted records. All custom objects and a subset of standard objects are supported.

Available Entities	Selected Entities
Account (Account)	Case (Case)
Account Contact Role (AccountContactRole)	
Asset (Asset)	
Assigned Resource (AssignedResource)	
Authorization Form Consent (AuthorizationFormConsent)	
Campaign (Campaign)	
Campaign Member (CampaignMember)	
Campaign Member Status (CampaignMemberStatus)	
Communication Subscription Consent (CommSubscriptionConsent)	
Contact (Contact)	

2. Open the Amazon AppFlow console at https://console.aws.amazon.com/appflow) to select the flow that was just created, and then choose **Activate flow**.


Amazon AppFlow > Flows > amazon-connect-salesforce-[redacted].my
Actions ▼
Activate flow
▸ Flow setup

amazon-connect-salesforce-[redacted].my

Flow details

Flow name: amazon-connect-salesforce-[redacted].my
Flow description: Flow created by Amazon Connect
AWS KMS key: AWS managed key
Date created: 11/11/2020, 12:02 PM

Source name: Salesforce
Source object or event: CaseChangeEvent
Source connection: amazon-connect-salesforce[redacted].my
Select another connection

Destination name: Amazon EventBridge
Destination object: aws.partner/appflow/salesforce.com/[redacted]/amazon-connect/[redacted].my

Status: ⊖ Suspended
Trigger: Event
Last run: 11/12/2020, 2:09 PM

Alternatively, you might need to delete the Amazon AppFlow Salesforce connection and flow, and start again.

Set up application integration for Zendesk

Step 1: Enable the events connector for Amazon EventBridge

If you don't already have the EventBridge connector for Zendesk enabled, you need to set it up first. Otherwise, go to Step 2: Integrate Zendesk with Amazon Connect for task creation (p. 764).

1. Copy your AWS account number:

   a. In the Amazon EventBridge console, go to **Partner event sources**.

   b. Search for or scroll to **Zendesk**, and choose **Set up**.

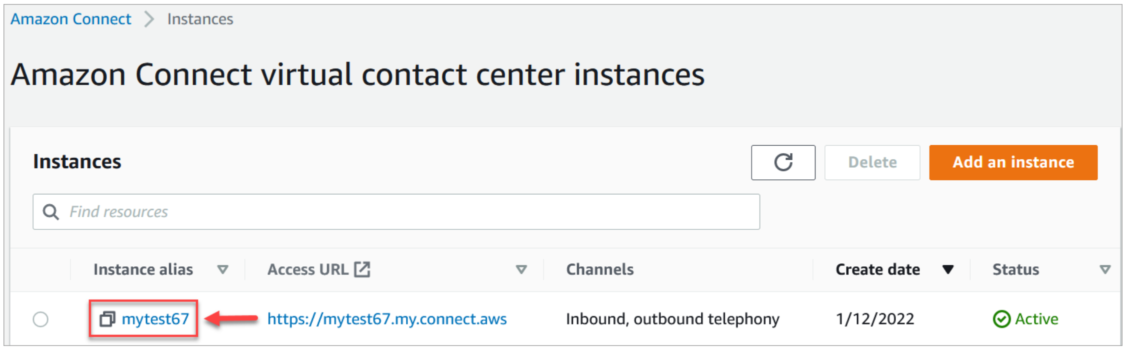
   c. Choose **Copy** to copy your AWS account information.

2. Go to Setting up the events connector for Amazon EventBridge in the Zendesk Help and follow the instructions.

Step 2: Integrate Zendesk with Amazon Connect for task creation

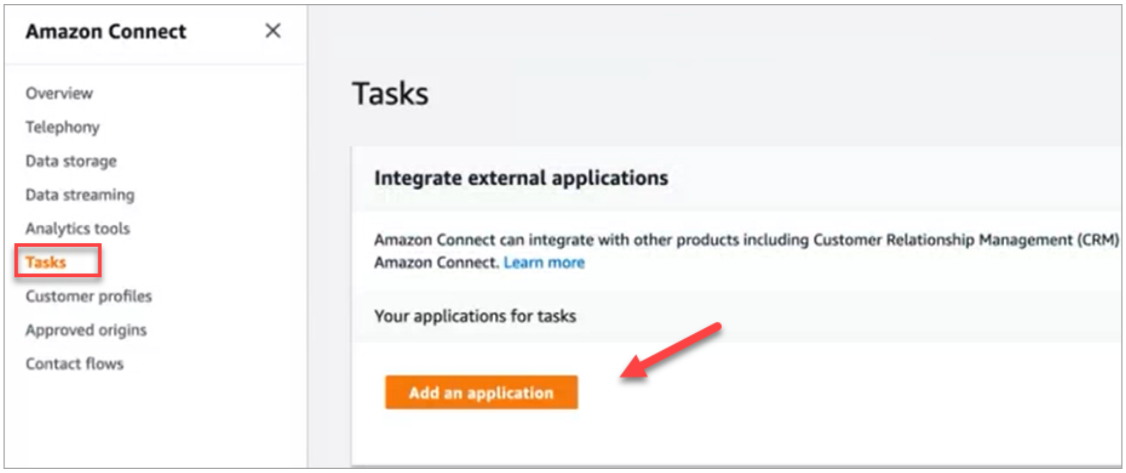
> **Note**
> If you use custom AWS Identity and Access Management (IAM) policies, for a list of the required IAM permissions to set up Amazon Connect Tasks, see Tasks page (p. 1090).

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.


Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

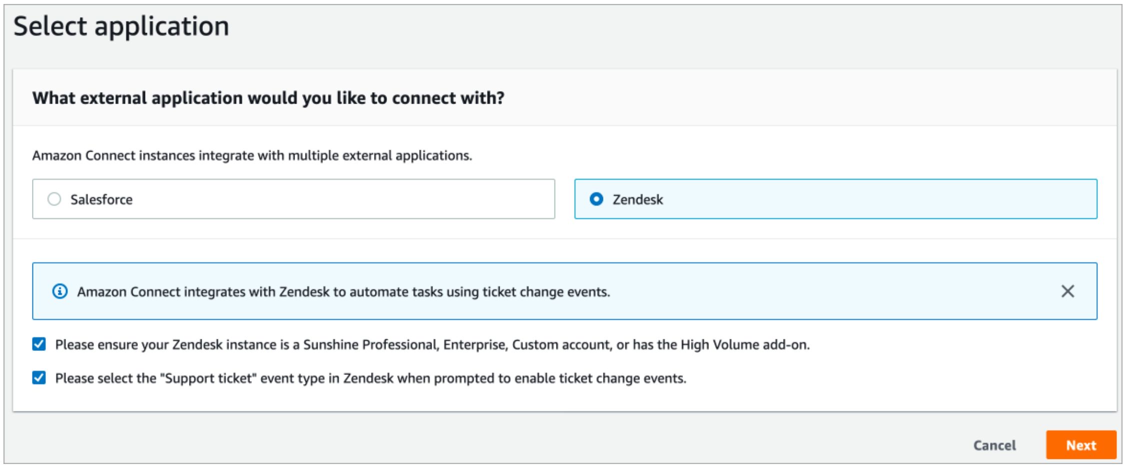
3. Choose **Tasks**, and then choose **Add an application**.



Amazon Connect can integrate with other products including Customer Relationship Management (CRM)
Amazon Connect. Learn more

4. On the **Select application** page, choose **Zendesk**.
5. After you choose to integrate with Zendesk, the application requirements are listed on the page.

   The following image shows the requirements for Zendesk. In this procedure, we walk you through the steps to select the "Support ticket" event type in Zendesk. Acknowledge the steps and choose **Next**.



Select application

What external application would you like to connect with?

Amazon Connect instances integrate with multiple external applications.

○ Salesforce ● Zendesk

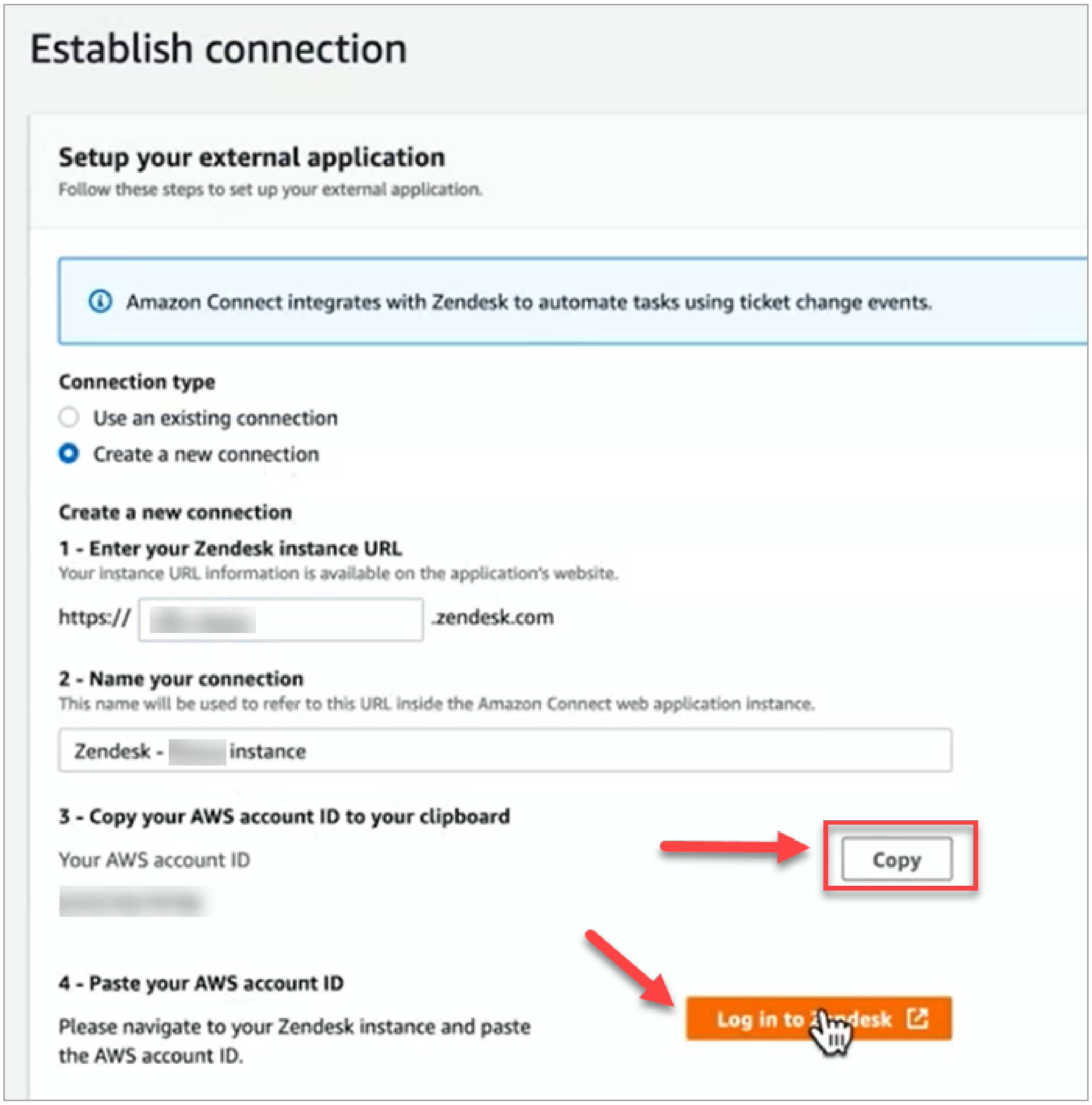
ⓘ Amazon Connect integrates with Zendesk to automate tasks using ticket change events.

☑ Please ensure your Zendesk instance is a Sunshine Professional, Enterprise, Custom account, or has the High Volume add-on.

☑ Please select the "Support ticket" event type in Zendesk when prompted to enable ticket change events.

6. On the **Establish connection** page, choose one of the following:

   - **Use an existing connection**. This allows you to reuse existing EventBridge resources you may have created in your AWS account.
   - **Create a new connection**: Enter the information required by the external application.
     1. Enter your application instance URL. This URL is used for deep-linking into the tasks created in your external application.
     2. Provide a friendly name for your connection, for example, **Zendesk - Test instance**. Later, when you add rules (p. 602), you'll refer to this friendly name.



Establish connection

Setup your external application

Follow these steps to set up your external application.

ⓘ Amazon Connect integrates with Zendesk to automate tasks using ticket change events.

Connection type

○ Use an existing connection

● Create a new connection

Create a new connection

1 - Enter your Zendesk instance URL

Your instance URL information is available on the application's website.

https:// [redacted] .zendesk.com

2 - Name your connection

This name will be used to refer to this URL inside the Amazon Connect web application instance.

Zendesk - [redacted] instance

3 - Copy your AWS account ID to your clipboard

Your AWS account ID

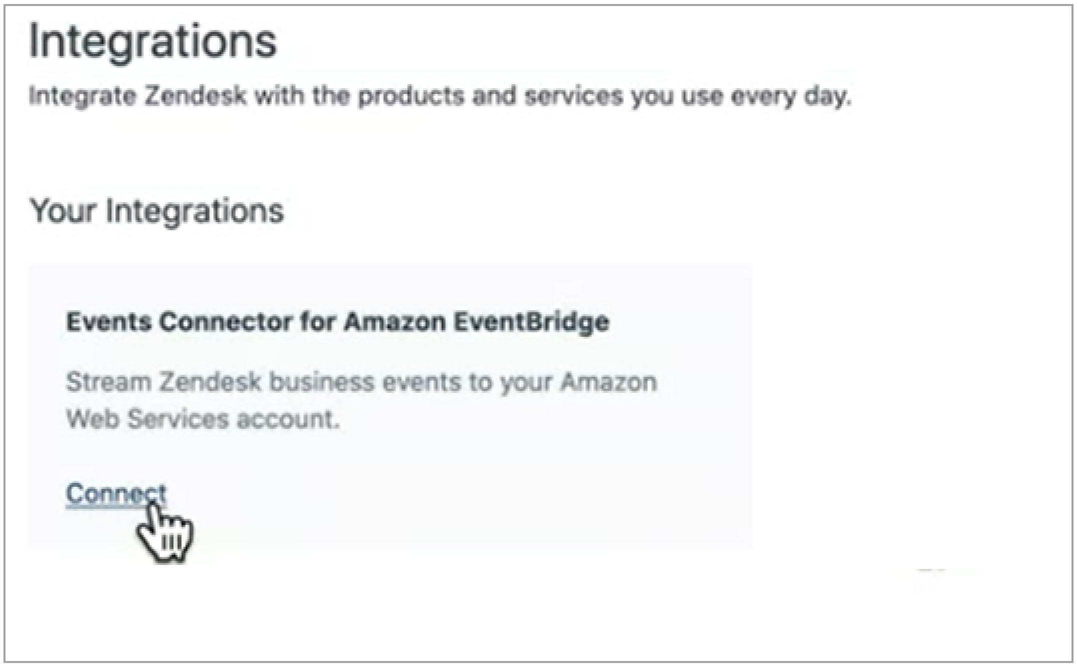
[redacted]

4 - Paste your AWS account ID

Please navigate to your Zendesk instance and paste the AWS account ID.

7. Choose **Copy** to copy your AWS account ID, and then choose **Login to Zendesk**. This takes you away from the **Establish connection** page for now, but you return to it shortly.

8. After you're logged in to Zendesk, choose **Connect** to connect the Events Connector for Amazon EventBridge.



Integrations

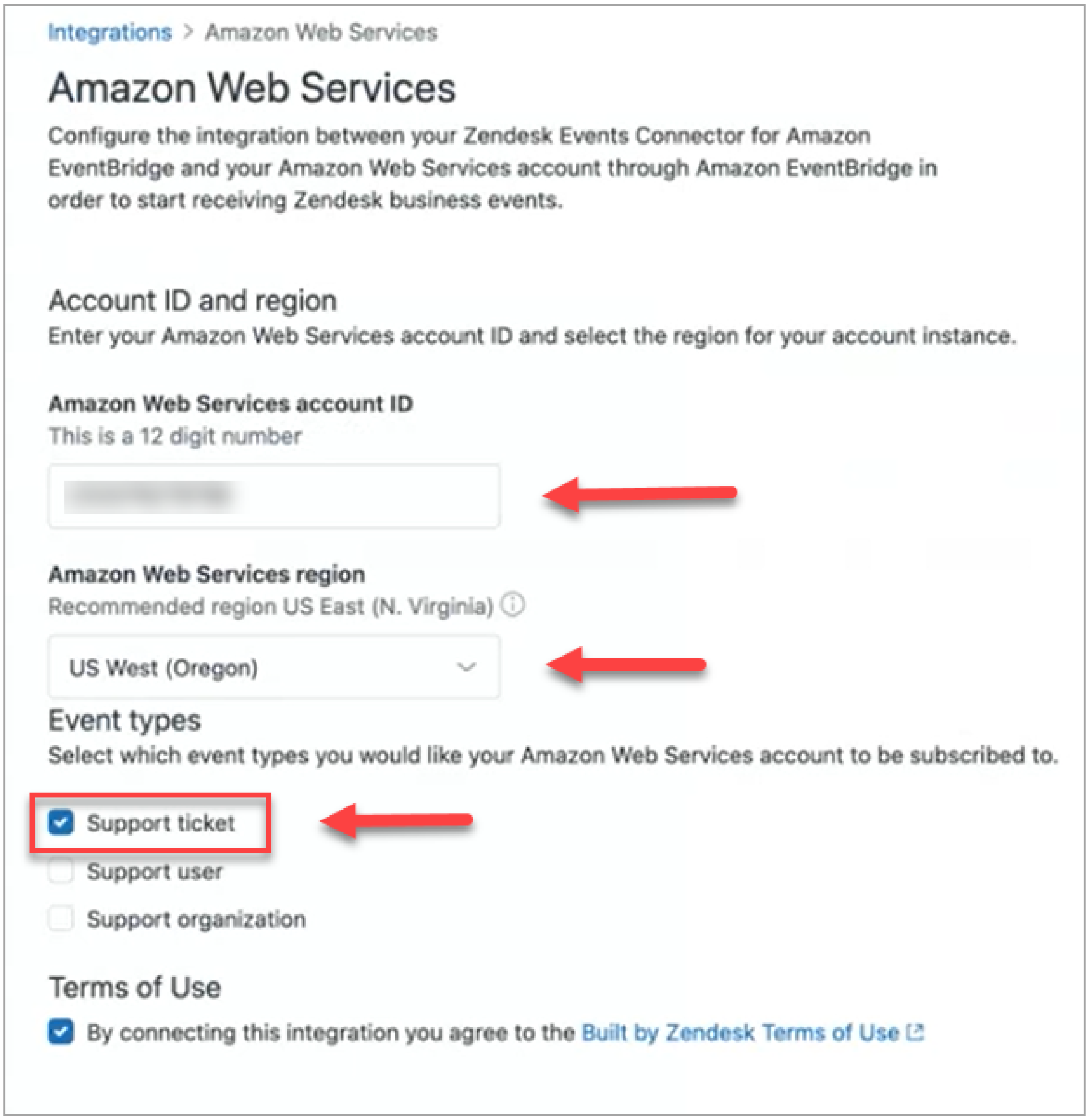
Integrate Zendesk with the products and services you use every day.

Your Integrations

Events Connector for Amazon EventBridge

Stream Zendesk business events to your Amazon Web Services account.

9. In Zendesk, on the **Amazon Web Services** page, paste in your Amazon Web Service account ID, choose your Region, choose **Support ticket**, acknowledge the terms of use, and the choose **Connect**. Zendesk creates a resource in Amazon EventBridge.



Integrations > Amazon Web Services

Amazon Web Services

Configure the integration between your Zendesk Events Connector for Amazon EventBridge and your Amazon Web Services account through Amazon EventBridge in order to start receiving Zendesk business events.

Account ID and region

Enter your Amazon Web Services account ID and select the region for your account instance.

Amazon Web Services account ID

This is a 12 digit number

[redacted]

Amazon Web Services region

Recommended region US East (N. Virginia)

US West (Oregon)

Event types

Select which event types you would like your Amazon Web Services account to be subscribed to.

☑ Support ticket

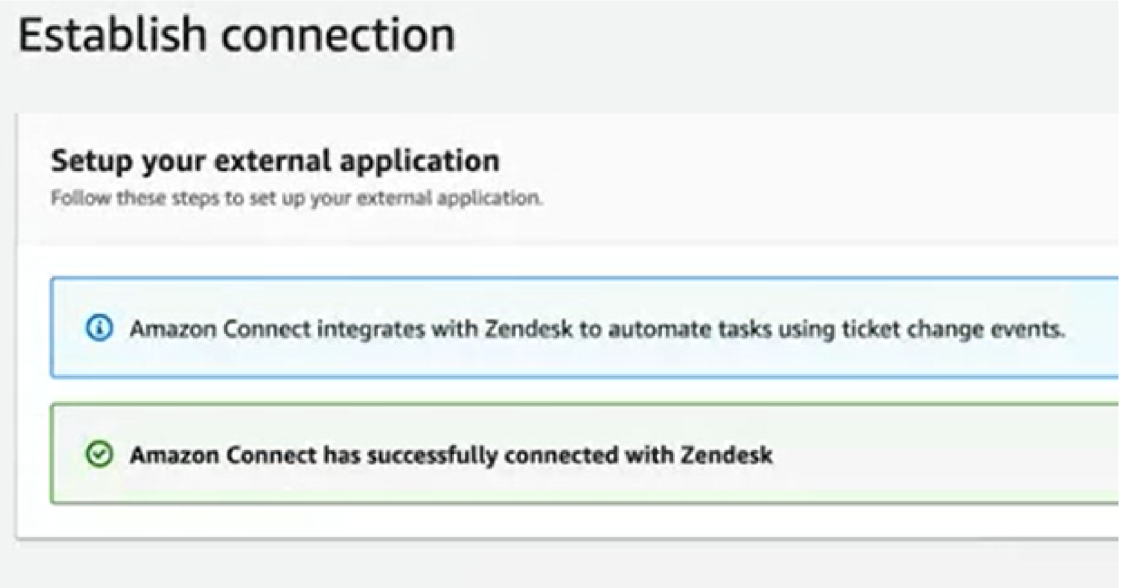
□ Support user

□ Support organization

Terms of Use

☑ By connecting this integration you agree to the Built by Zendesk Terms of Use

10. Return to the **Establish connection** page in Amazon Connect choose **Next**.
11. On the **Establish** page, you'll see the message that Amazon Connect has successfully connected with Zendesk. Choose **Next**.



Establish connection

Setup your external application

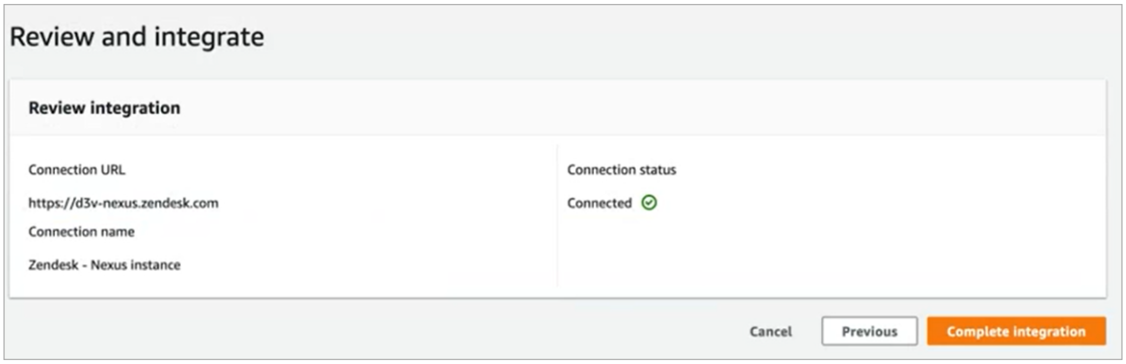
Follow these steps to set up your external application.

Amazon Connect integrates with Zendesk to automate tasks using ticket change events.

Amazon Connect has successfully connected with Zendesk

12. On the **Review and integrate** page, check that the **Connection status** says **Connected**, and then choose **Complete integration**.

    This creates a connection that associates the EventBridge resource for Zendesk to Amazon Connect.



Review and integrate

Review integration

Connection URL

https://d3v-nexus.zendesk.com

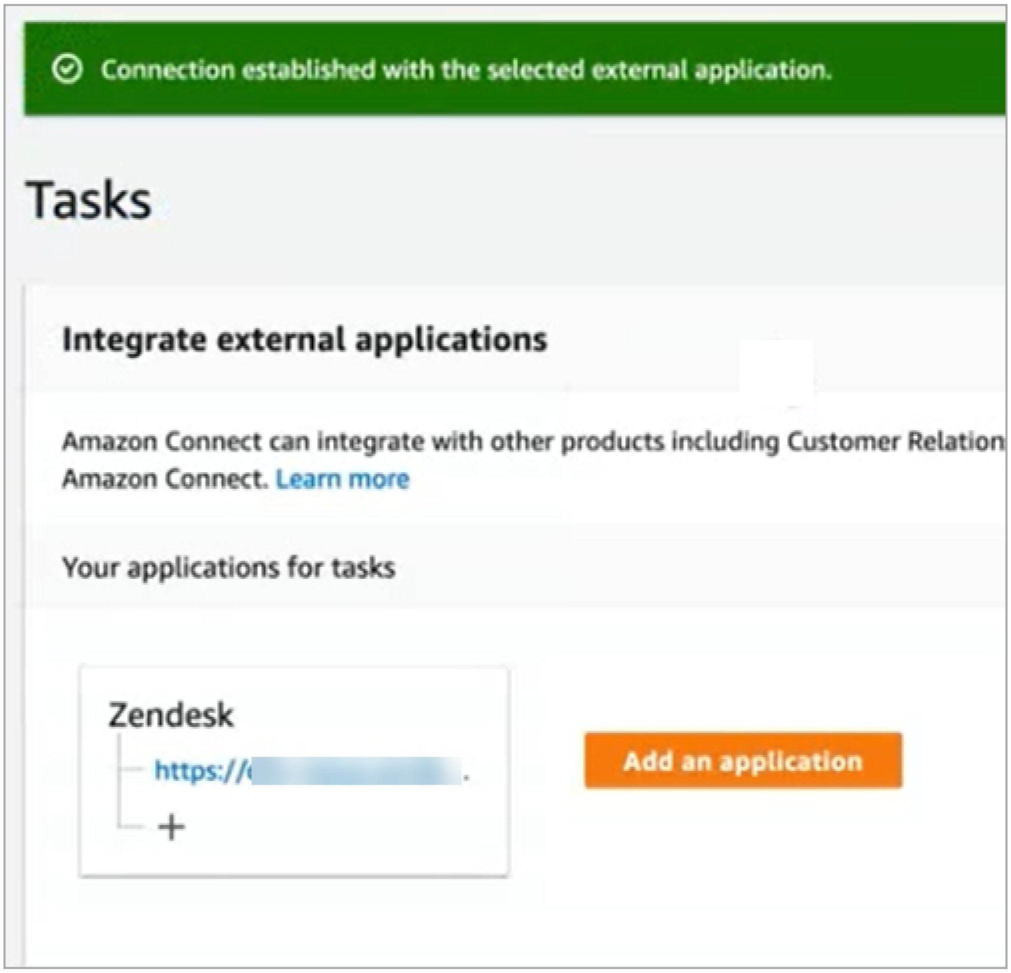
Connection name

Zendesk - Nexus instance

Connection status

Connected ✓

13. On the **Tasks** page, the new connection is listed.



Connection established with the selected external application.

Tasks

Integrate external applications

Amazon Connect can integrate with other products including Customer Relation
Amazon Connect. Learn more

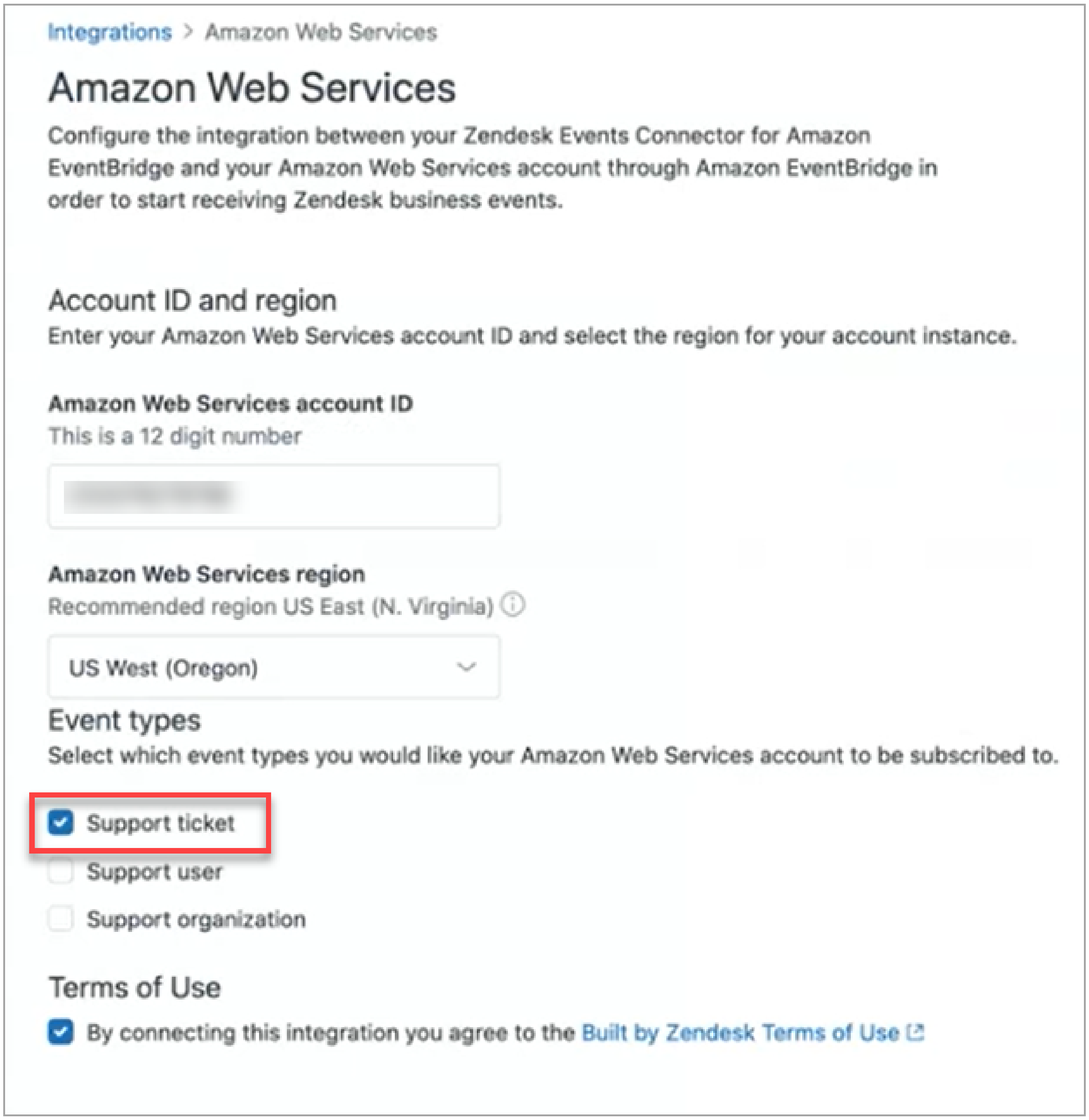
Your applications for tasks

Zendesk
https://

You're done! Next, add rules that tell Amazon Connect when to create a task and how to route it. For instructions, see Create rules that generate tasks for third-party integrations (p. 602).

What to do when is a connection isn't successfully established

A connection might fail to create a task if you do not correctly select the **Support ticket** event type when setting up the connection in Zendesk, after being prompted to do so in the flow. To fix this, log in to Zendesk, and update that setting, as shown in the following image.



Integrations > Amazon Web Services

Amazon Web Services

Configure the integration between your Zendesk Events Connector for Amazon EventBridge and your Amazon Web Services account through Amazon EventBridge in order to start receiving Zendesk business events.

Account ID and region

Enter your Amazon Web Services account ID and select the region for your account instance.

Amazon Web Services account ID

This is a 12 digit number

[redacted]

Amazon Web Services region

Recommended region US East (N. Virginia) ⓘ

US West (Oregon)

Event types

Select which event types you would like your Amazon Web Services account to be subscribed to.

☑ Support ticket

□ Support user

□ Support organization

Terms of Use

☑ By connecting this integration you agree to the Built by Zendesk Terms of Use

There is also another case where you may not have selected the correct AWS Region that the Amazon Connect instance is in, when setting up EventBridge. To fix:

1. Go to the EventBridge console at https://console.aws.amazon.com/events/.
2. Disconnect your EventBridge connection.
3. In the Amazon Connect console, restart the flow.

Monitor task creation

After your connection is established, if it stops working, in Amazon Connect disassociate the connection, and then re-establish it. If that doesn't solve the issue, do the following:

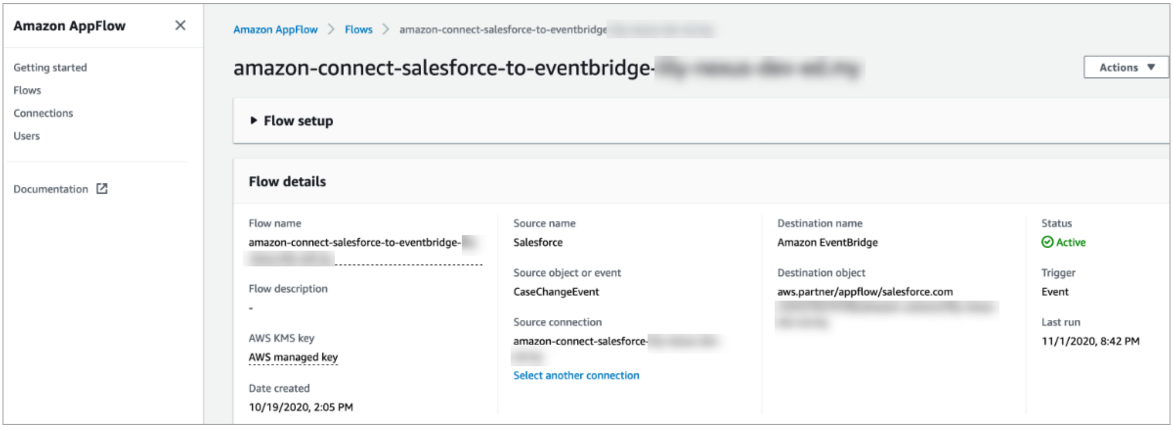
Zendesk

1. Go to the EventBridge console at https://console.aws.amazon.com/events/.
2. Check the status of the event source connection to see if it is active.

Salesforce

1. Go to the Amazon AppFlow console at https://console.aws.amazon.com/appflow).
2. Monitor the flow that was created for the account that was set up.

The following image shows what a flow looks like in the Amazon AppFlow console for Salesforce. It contains information about the status of the connection, and when it was last run.



amazon-connect-salesforce-to-eventbridge-[redacted]

Flow details

Flow name: amazon-connect-salesforce-to-eventbridge-[redacted]

Flow description: -

AWS KMS key: AWS managed key

Date created: 10/19/2020, 2:05 PM

Source name: Salesforce

Source object or event: CaseChangeEvent

Source connection: amazon-connect-salesforce-[redacted]

Select another connection

Destination name: Amazon EventBridge

Destination object: aws.partner/appflow/salesforce.com[redacted]

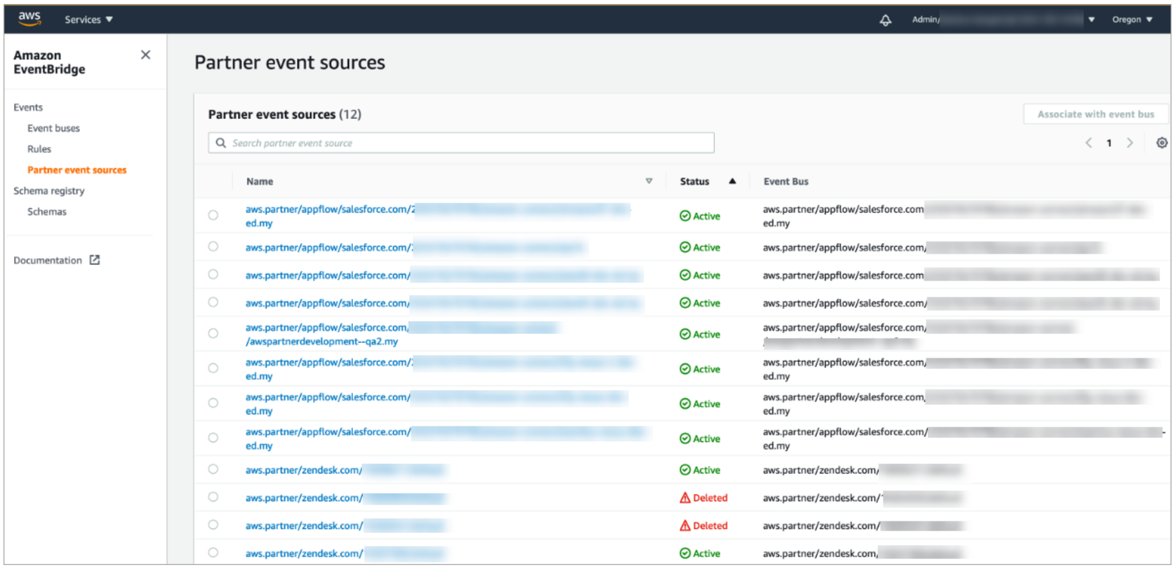
Status: ✓ Active

Trigger: Event

Last run: 11/1/2020, 8:42 PM

For both Zendesk and Salesforce, you can go to the EventBridge console at https://console.aws.amazon.com/events/ to see your connection state and see if it is active, pending, or deleted.

The following image shows an example EventBridge console.



Partner event sources

Partner event sources (12)

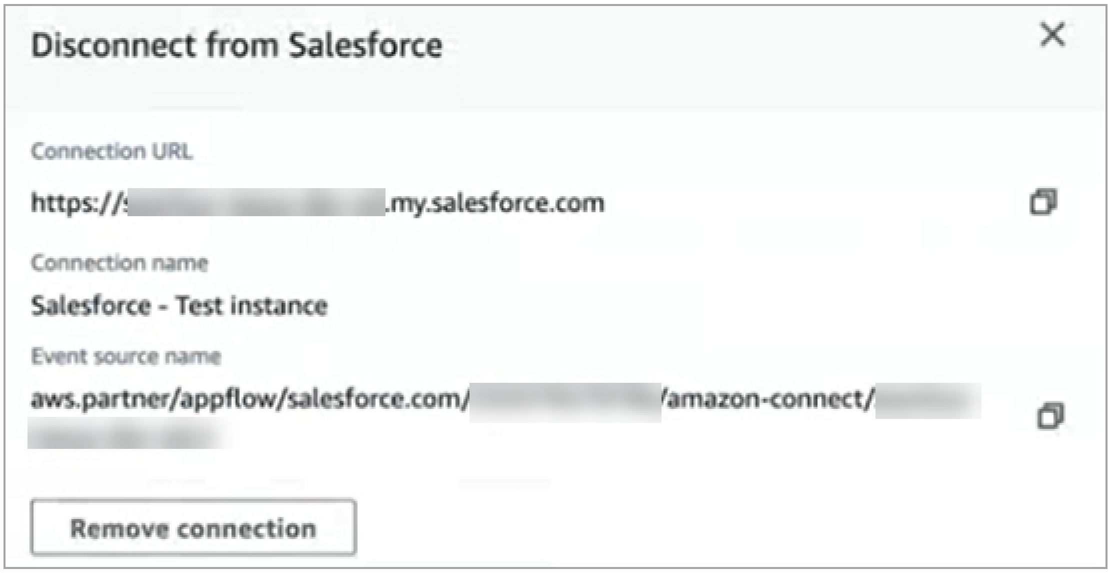
	Name	Status	Event Bus
○	aws.partner/appflow/salesforce.com/[redacted]ed.my	✓ Active	aws.partner/appflow/salesforce.com[redacted]ed.my
○	aws.partner/appflow/salesforce.com/[redacted]	✓ Active	aws.partner/appflow/salesforce.com/[redacted]
○	aws.partner/appflow/salesforce.com/[redacted]	✓ Active	aws.partner/appflow/salesforce.com[redacted]
○	aws.partner/appflow/salesforce.com/[redacted]	✓ Active	aws.partner/appflow/salesforce.com/[redacted]
○	aws.partner/appflow/salesforce.com/[redacted]/awspartnerdevelopment--qa2.my	✓ Active	aws.partner/appflow/salesforce.com/[redacted]
○	aws.partner/appflow/salesforce.com/[redacted]ed.my	✓ Active	aws.partner/appflow/salesforce.com/[redacted]ed.my
○	aws.partner/appflow/salesforce.com/[redacted]ed.my	✓ Active	aws.partner/appflow/salesforce.com/[redacted]ed.my
○	aws.partner/appflow/salesforce.com/[redacted]ed.my	✓ Active	aws.partner/appflow/salesforce.com/[redacted]ed.my
○	aws.partner/zendesk.com/[redacted]	✓ Active	aws.partner/zendesk.com/[redacted]
○	aws.partner/zendesk.com/[redacted]	⚠ Deleted	aws.partner/zendesk.com/[redacted]
○	aws.partner/zendesk.com/[redacted]	⚠ Deleted	aws.partner/zendesk.com/[redacted]
○	aws.partner/zendesk.com/[redacted]	✓ Active	aws.partner/zendesk.com/[redacted]

Disassociate an Amazon Connect connection

At any time you can disassociate a connection, and stop the automatic generation of tasks based on events from the external application.

To stop the automatic generation of tasks

1. Choose the application, and then choose **Remove connection**.



Disconnect from Salesforce

Connection URL

https://s[redacted].my.salesforce.com

Connection name

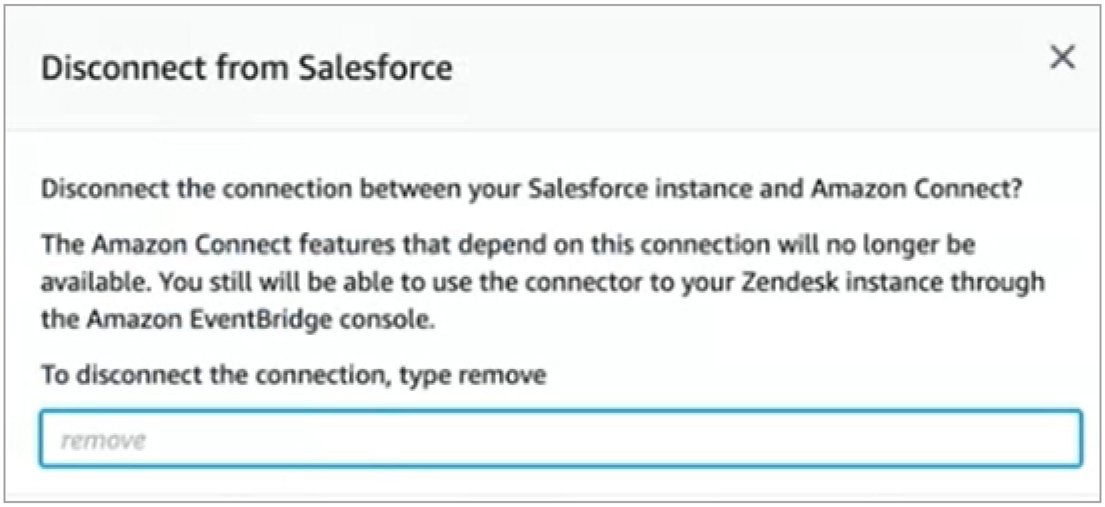
Salesforce - Test instance

Event source name

aws.partner/appflow/salesforce.com/[redacted]/amazon-connect/[redacted]
[redacted]

2. Type **Remove**, and then choose **Remove**.

   If you need to debug, you are still able to go to Amazon AppFlow (Salesforce) or EventBridge.



Disconnect from Salesforce

Disconnect the connection between your Salesforce instance and Amazon Connect?

The Amazon Connect features that depend on this connection will no longer be available. You still will be able to use the connector to your Zendesk instance through the Amazon EventBridge console.

To disconnect the connection, type remove

To remove the connection altogether from Zendesk

1. Log in to Zendesk, and navigate to **https://[subdomain].zendesk.com/admin/platform/integrations**.
2. Disconnect the EventBridge connection.

To remove the connection altogether from Salesforce

- Open the Amazon AppFlow console at https://console.aws.amazon.com/appflow, and delete the Salesforce connection and flow that were created in Amazon Connect.

  Flows are created with the name pattern of amazon-connect-salesforce-to-eventbridge-[subdomain].

  Connections are created with the name pattern of amazon-connect-salesforce-[subdomain]

To re-enable the automatic generation of tasks, repeat the setup steps.

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

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

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

Do you need to increase your service quotas?

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

Contact AWS Support to request an increase to **Number of Streams**.

To request an increase to your service quota, in the AWS Support Center, choose **Create Case** and then choose **Service Quota Increase**.

> **Tip**
> We make sure that **PutMedia** requests always stay within the 5 TPS quota. You don't need to request an increase.

How long do you need to store audio?

Customer audio is stored in Kinesis for the time defined by your retention settings in an Amazon Connect instance. For instructions for setting this value, see Enable live media streaming in your instance (p. 776).

> **Tip**
> If you want to use the audio streaming feature, you need to retain the streams that are created by Amazon Connect. Don't delete them, unless you're going to stop using the streaming feature.

Do you need to change the audio streams?

We recommend that you refrain from modifying the streams. Doing so can cause unexpected behavior.

Who requires IAM permissions to retrieve data?

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

Enable live media streaming in your instance

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

To enable live media streaming

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.
3. In the navigation pane, choose **Data storage**.
4. Under **Live media streaming**, choose **Edit**. Choose **Enable live media streaming**.
5. Enter a prefix for the Kinesis Video Streams created for your customer audio. This prefix makes it easier for you to identify the stream with the data.
6. Choose the KMS key to use to encrypt the data sent to Kinesis. The KMS key must be in the same Region as the instance.
7. Specify a number and unit for the **Data retention period**. 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. 782).

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

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

import com.amazonaws.auth.AWSSessionCredentials;
import com.amazonaws.auth.AWSSessionCredentialsProvider;
import com.amazonaws.kinesisvideo.parser.examples.LMSExample;
import com.amazonaws.regions.Regions;


import java.io.FileOutputStream;
import java.io.IOException;
```

```
public class LMSDemo {

    public static void main(String args[]) throws InterruptedException, IOException {
        LMSExample example = new LMSExample(Regions.US_WEST_2,
                                            "<<StreamName>>",
                                            "<<FragmentNumber>>",
                             new AWSSessionCredentialsProvider() {
                                                @Override
                             public AWSSessionCredentials getCredentials() {
                                 return new AWSSessionCredentials() {
                                                        @Override
                             public String getSessionToken() {
                                 return "<<AWSSessionToken>>";
                                                        }

                                                        @Override
                             public String getAWSAccessKeyId() {
                                 return "<<AWSAccessKey>>";
                                                        }

                                                        @Override
                             public String getAWSSecretKey() {
                                 return "<<AWSSecretKey>>";
                                                        }
                                                    };
                                                }

                                                @Override
                             public void refresh() {

                                                }
                                            },
                             new FileOutputStream("<<FileName>>.raw"));

                                 example.execute();
    }

}
```

LMSExample.java

```
package com.amazonaws.kinesisvideo.parser.examples;

import com.amazonaws.auth.AWSCredentialsProvider;
import com.amazonaws.kinesisvideo.parser.ebml.MkvTypeInfos;
import com.amazonaws.kinesisvideo.parser.mkv.MkvDataElement;
import com.amazonaws.kinesisvideo.parser.mkv.MkvElementVisitException;
import com.amazonaws.kinesisvideo.parser.mkv.MkvElementVisitor;
import com.amazonaws.kinesisvideo.parser.mkv.MkvEndMasterElement;
import com.amazonaws.kinesisvideo.parser.mkv.MkvStartMasterElement;
import com.amazonaws.kinesisvideo.parser.utilities.FragmentMetadataVisitor;
import com.amazonaws.kinesisvideo.parser.utilities.FrameVisitor;
import com.amazonaws.kinesisvideo.parser.utilities.LMSFrameProcessor;
import com.amazonaws.regions.Regions;
import com.amazonaws.services.kinesisvideo.model.StartSelector;
import com.amazonaws.services.kinesisvideo.model.StartSelectorType;

import java.io.Closeable;
import java.io.FileNotFoundException;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.OutputStream;
import java.io.PipedInputStream;
import java.io.PipedOutputStream;
import java.util.concurrent.ExecutorService;
import java.util.concurrent.Executors;
import java.util.concurrent.TimeUnit;

public class LMSExample extends KinesisVideoCommon {

    private final ExecutorService executorService;
    private GetMediaProcessingArguments getMediaProcessingArguments;
    private final StreamOps streamOps;
    private final OutputStream outputStreamFromCustomer;
    private final OutputStream outputStreamToCustomer;
    private final String fragmentNumber;

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

    public void execute () throws InterruptedException, IOException {
        getMediaProcessingArguments =
 GetMediaProcessingArguments.create(outputStreamFromCustomer, outputStreamToCustomer);
        try (GetMediaProcessingArguments getMediaProcessingArgumentsLocal =
 getMediaProcessingArguments) {
            //Start a GetMedia worker to read and process data from the Kinesis Video
 Stream.
            GetMediaWorker getMediaWorker = GetMediaWorker.create(getRegion(),
            getCredentialsProvider(),
            getStreamName(),
            new
 StartSelector().withStartSelectorType(StartSelectorType.FRAGMENT_NUMBER).withAfterFragmentNumber(fragm
            streamOps.amazonKinesisVideo,
            getMediaProcessingArgumentsLocal.getFrameVisitor());
            executorService.submit(getMediaWorker);

            //Wait for the workers to finish.
            executorService.shutdown();
            executorService.awaitTermination(120, TimeUnit.SECONDS);
            if (!executorService.isTerminated()) {
                System.out.println("Shutting down executor service by force");
                executorService.shutdownNow();
            } else {
                System.out.println("Executor service is shutdown");
            }
        } finally {
            outputStream.close();
        }

    }

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

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

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

       private long fragmentCount = 0;

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

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

           }
       }

       @Override
       public void visit(MkvDataElement dataElement) throws MkvElementVisitException {
       }
   }

   private static class GetMediaProcessingArguments implements Closeable {

       public FrameVisitor getFrameVisitor() {
           return frameVisitor;
       }

       private final FrameVisitor frameVisitor;

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

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

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

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

           return new GetMediaProcessingArguments(frameVisitor);
       }

       @Override
       public void close() throws IOException {

       }
```

```
    }
}
```

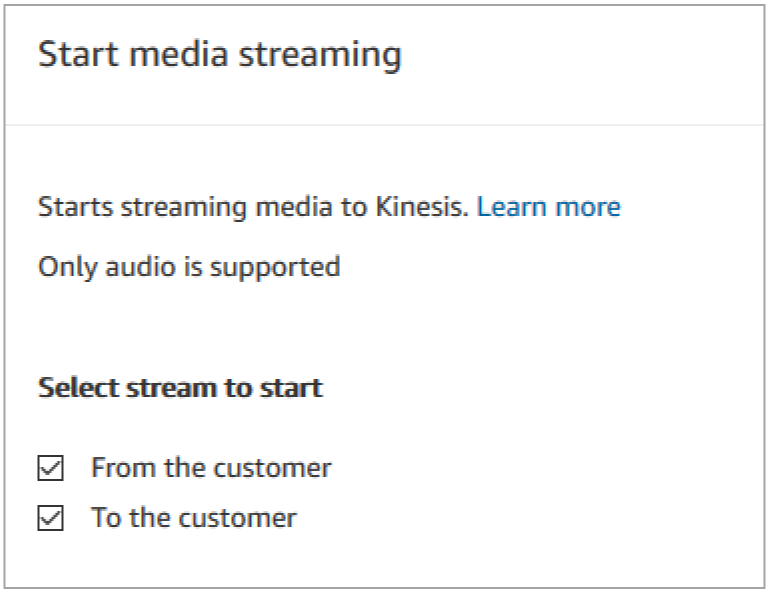
LMSFrameProcessor.java

```
package com.amazonaws.kinesisvideo.parser.utilities;

import com.amazonaws.kinesisvideo.parser.mkv.Frame;
import com.amazonaws.kinesisvideo.parser.utilities.FragmentMetadataVisitor;
import com.amazonaws.kinesisvideo.parser.utilities.MkvTrackMetadata;

import java.io.IOException;
import java.io.OutputStream;
import java.nio.ByteBuffer;

public class LMSFrameProcessor implements FrameVisitor.FrameProcessor {

    private OutputStream outputStreamFromCustomer;
    private OutputStream outputStreamToCustomer;
    private FragmentMetadataVisitor fragmentMetadataVisitor;

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

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

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

    private void saveToOutPutStream(final Frame frame) {
        ByteBuffer frameBuffer = frame.getFrameData();
        long trackNumber = frame.getTrackNumber();
        MkvTrackMetadata metadata =
 fragmentMetadataVisitor.getMkvTrackMetadata(trackNumber);
        String trackName = metadata.getTrackName();

        try {
            byte[] frameBytes = new byte[frameBuffer.remaining()];
            frameBuffer.get(frameBytes);
            if (Strings.isNullOrEmpty(trackName) ||
 "AUDIO_FROM_CUSTOMER".equals(trackName)) {
            outputStreamFromCustomer.write(frameBytes);
            } else if ("AUDIO_TO_CUSTOMER".equals(trackName)) {
            outputStreamToCustomer.write(frameBytes);
            } else {
              // Unknown track name. Not writing to output stream.
            }

        } catch (IOException e) {
            e.printStackTrace();
        }
    }

}
```

Example contact flow for testing live media streaming

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

1. Add a **Start media streaming** block at the point where you want to enable customer audio streaming.
2. Connect the **Success** branch to the rest of your flow.
3. Add a **Stop media streaming** block to where you want to stop streaming.
4. Configure both blocks to specify what you want to stream: **From the customer** and/or **To the customer**.



Start media streaming

Starts streaming media to Kinesis. Learn more

Only audio is supported

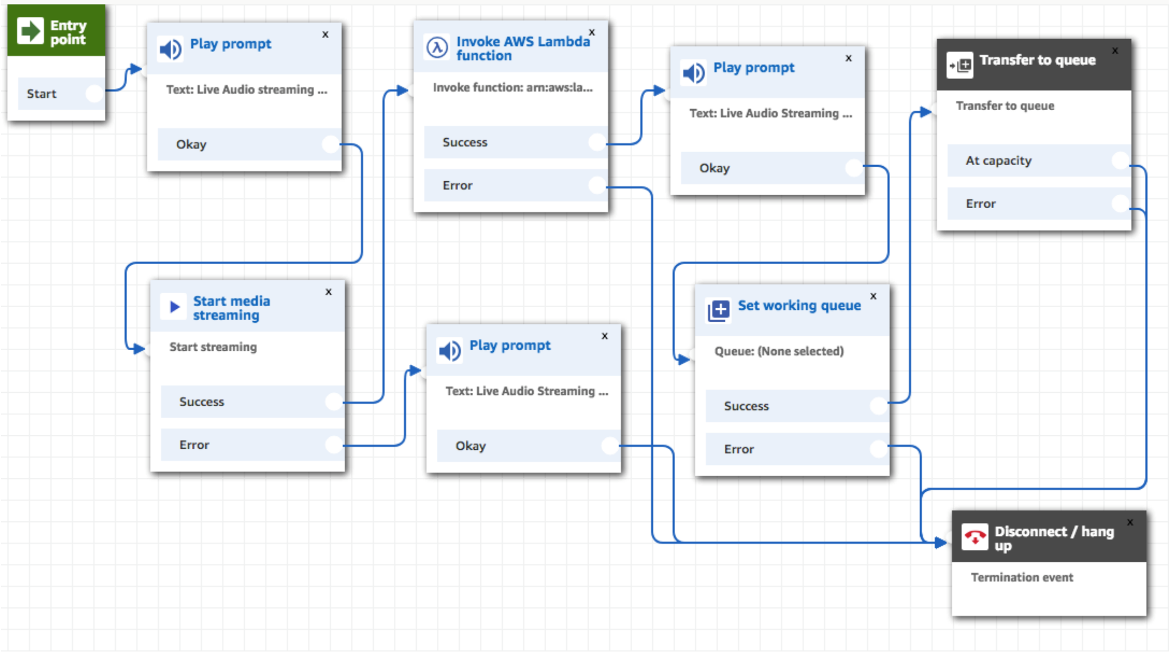
Select stream to start

☑ From the customer
☑ 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 contact record includes the attributes. You can then view the contact record to determine the media streaming data associated with a specific contact. You can also pass the attributes to an AWS Lambda function.

The following example 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. 783).

Contact attributes for live media streaming

The attributes are displayed when you select **Media streams** for the **Type** in a contact flow block that supports attributes, such as the **Start media streaming** block. They include the following:

Customer audio stream ARN

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

JSONPath format: $.MediaStreams.Customer.Audio.StreamARN

Customer audio start timestamp

The time at which the customer audio stream started.

JSONPath format: $.MediaStreams.Customer.Audio.StartTimestamp

Customer audio stop timestamp

The time at which the customer audio stream stopped.

JSONPath format: $.MediaStreams.Customer.Audio.StopTimestamp

Customer audio start fragment number

The number that identifies the Kinesis Video Streams fragment in which the customer audio stream started.

JSONPath format: $.MediaStreams.Customer.Audio.StartFragmentNumber

For more information about Amazon Kinesis Video Streams fragments, see Fragment in the *Amazon Kinesis Video Streams Developer Guide*.

Manage users in Amazon Connect

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

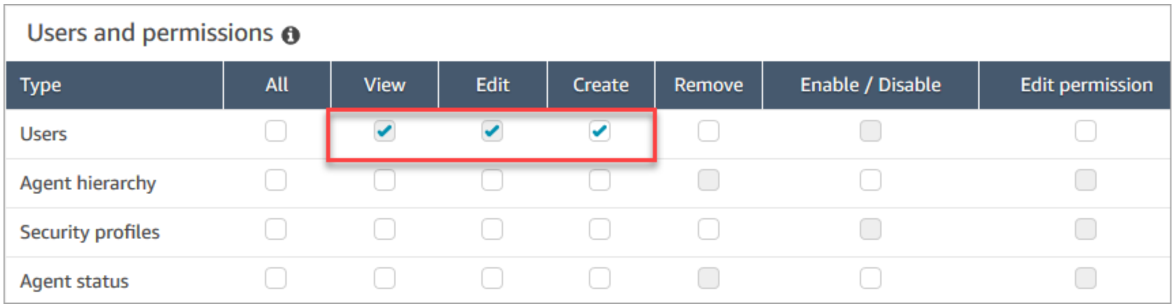
Contents

Add users to Amazon Connect

You can add users and configure them with permissions that are appropriate to their roles (for example, agents or managers). For more information, see Security profiles (p. 789). Contacts can be routed based on the skills required of the agents. For more information, see Create a routing profile (p. 227).

Required permissions for adding users

Before you can add users to Amazon Connect, you need the following permissions assigned to your security profile: **Users - Create**.



Users and permissions

Type	All	View	Edit	Create	Remove	Enable / Disable	Edit permission
Users	□	☑	☑	☑	□	□	□
Agent hierarchy	□	□	□	□	□	□	□
Security profiles	□	□	□	□	□	□	□
Agent status	□	□	□	□	□	□	□

By default, the Amazon Connect **Admin** security profile has these permissions.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

Add a user individually

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to create users.
2. Choose **Users**, **User management**.
3. Choose **Add new users**.
4. Choose **Create and set up a new user** and then choose **Next**.

5. Enter the name, email address, and password for the user.
6. Choose a routing profile and a security profile.
7. Choose **Save**. If the Save button isn't active, it means you're logged in with an Amazon Connect account that doesn't have the required security profile permissions.

   To fix this issue, log in with an account that is assigned to the Amazon Connect Admin security profile. Or, ask another Admin to help.
8. For information about adding agents, see Configure agent settings: routing profile, phone type, and auto-accept calls (p. 233).

Add users in bulk from a .csv file

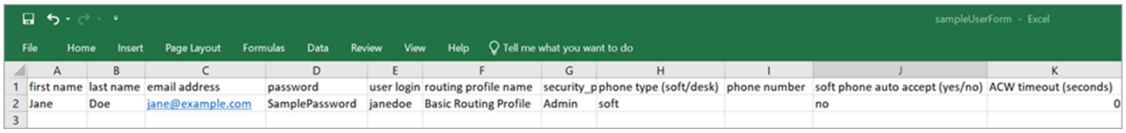
Use these steps to add several users from a .csv file such as an Excel spreadsheet.

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to create users.
2. Choose **Users**, **User management**.
3. Choose **Add new users**.
4. Choose **Upload my users from a template (.csv)** and then choose **Next**.

   The .csv template has the following columns in the first row:

   - first name
   - last name
   - email address
   - password
   - user login
   - routing profile name
   - security_profile_name_1|security_profile_name_2
   - phone type (soft/desk)
   - phone number
   - soft phone auto accept yes/no)
   - ACW timeout (seconds)

   The following image shows a sample of what the .csv template looks like in an Excel spreadsheet:

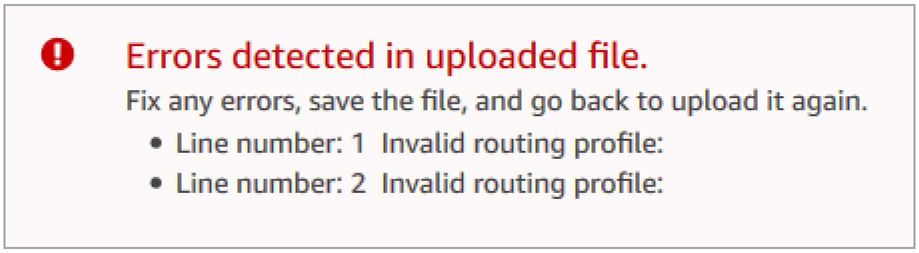


	A	B	C	D	E	F	G	H	I	J	K
1	first name	last name	email address	password	user login	routing profile name	security_p	phone type (soft/desk)	phone number	soft phone auto accept (yes/no)	ACW timeout (seconds)
2	Jane	Doe	jane@example.com	SamplePassword	janedoe	Basic Routing Profile	Admin	soft		no	0
3											

5. Choose **Download template**.
6. Add your users to the template and upload it to Amazon Connect.

If you get an error message, it usually indicates that one of the required columns is missing information, or there's a typo in one of the cells.

- We recommend checking the format of the phone number as a starting point in your investigation.
- If you get an error message that **Security profile is not found**, check whether there's a typo in one of the cells in the **security_profile_name_1** column.
- Update the .csv file and try uploading it again.



Errors detected in uploaded file.

Fix any errors, save the file, and go back to upload it again.

- Line number: 1 Invalid routing profile:
- Line number: 2 Invalid routing profile:

Delete users from your Amazon Connect instance

When a user is deleted from Amazon Connect, you won't be able to configure their agent settings any more. For example, you won't be able to assign a routing profile to them.

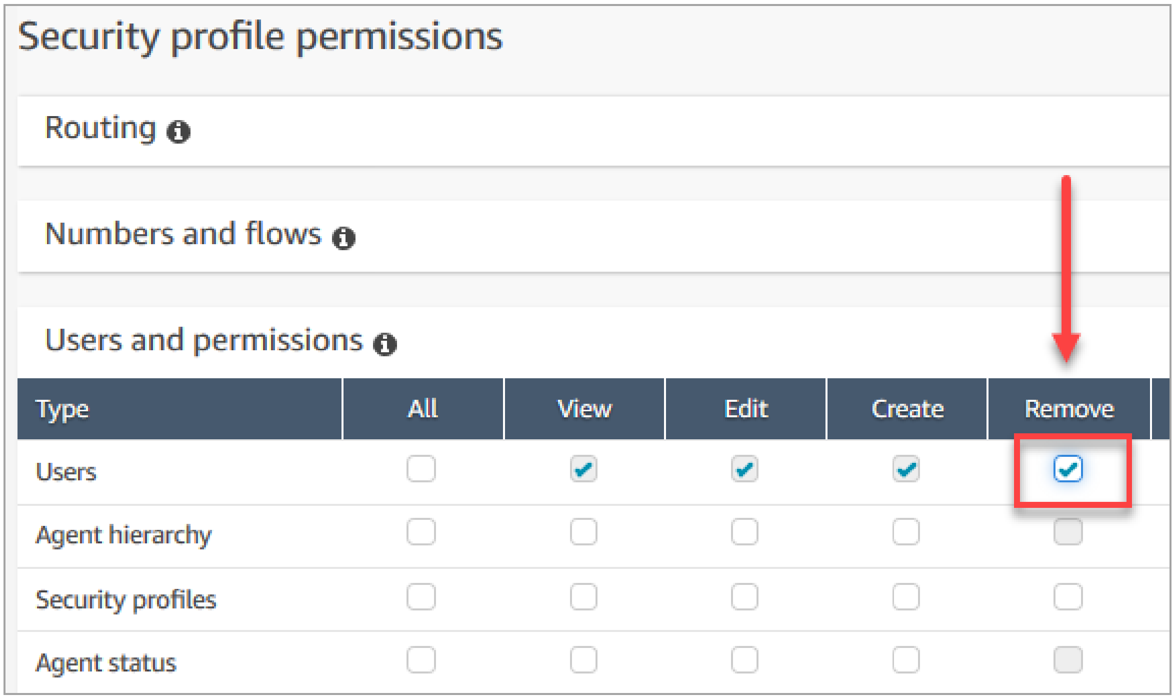
What happens to the user's metrics?

The user's data in contact records and reports is retained. The data is preserved for the consistency of the historical metrics.

In the historical metrics reports, the agent's data will be included in the **Agent performance** metrics report. However, you won't be able to see an **Agent activity audit** of the deleted agent because their name won't appear in the drop-down list.

Required permissions to delete users

Before you can update permissions in a security profile, you must be logged in with an Amazon Connect account that has the following permissions: **Users - Remove**.



Security profile permissions

Routing

Numbers and flows

Users and permissions

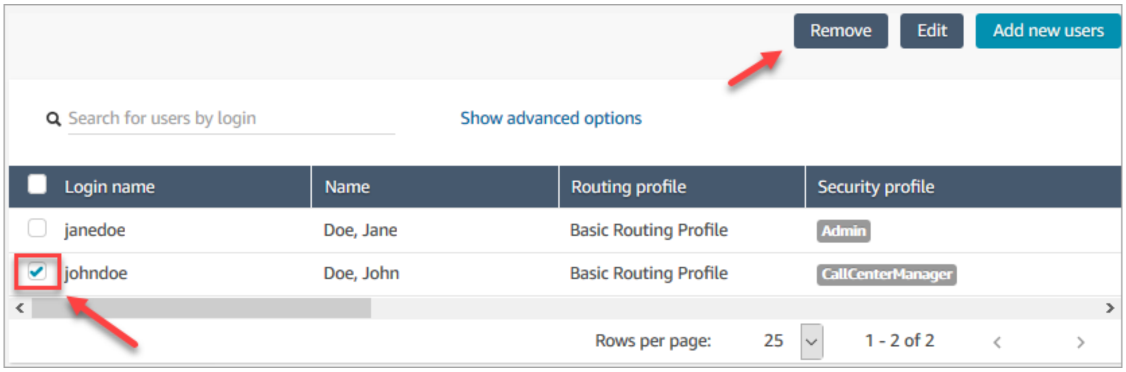
Type	All	View	Edit	Create	Remove
Users	☐	☑	☑	☑	☑
Agent hierarchy	☐	☐	☐	☐	☐
Security profiles	☐	☐	☐	☐	☐
Agent status	☐	☐	☐	☐	☐

By default, the Amazon Connect **Admin** security profile has these permissions.

How to delete users

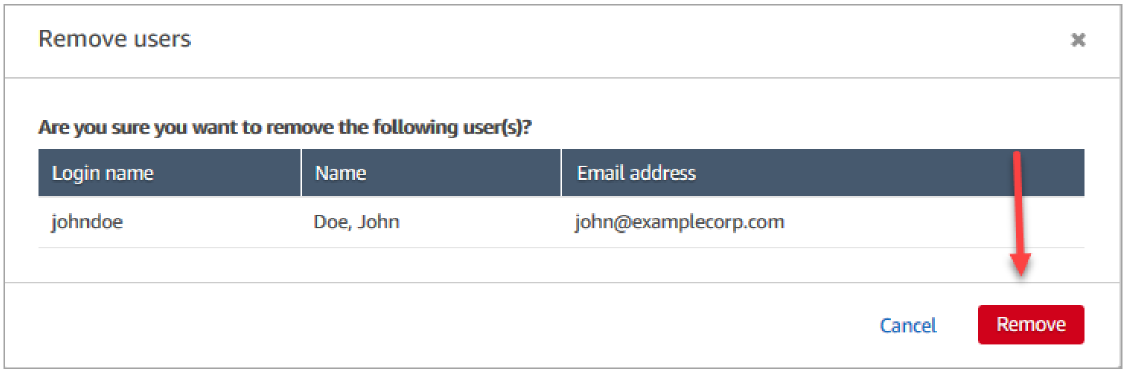
You can't undo a deletion.

1. Log in to the Amazon Connect console with an **Admin** account, or an account assigned to a security profile that has permissions to remove users.
2. Choose the user account you want to delete, and then choose **Remove**.



☐ Login name	Name	Routing profile	Security profile
☐ janedoe	Doe, Jane	Basic Routing Profile	Admin
☑ johndoe	Doe, John	Basic Routing Profile	CallCenterManager

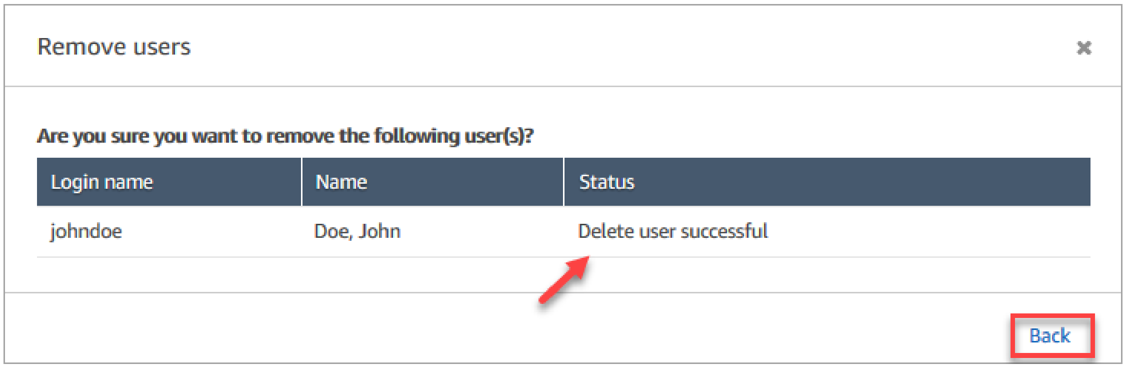
3. Confirm you want to delete that account.



Are you sure you want to remove the following user(s)?

Login name	Name	Email address
johndoe	Doe, John	john@examplecorp.com

4. Note the status of account. Choose **Back** to return to the **User management** page.



Are you sure you want to remove the following user(s)?

Login name	Name	Status
johndoe	Doe, John	Delete user successful

Reset a user's password for Amazon Connect

To reset a password for a user

1. Log in to your contact center at https://*instance name*.my.connect.aws/.

2. Choose **Users**, **User management**.
3. Select the user and choose **Edit**.
4. Choose **reset password**. Specify a new password and then choose **Submit**.

   Resetting the user's password will immediately log them out of the Contact Control Panel.
5. Communicate the new password to the user.

Reset your own lost or forgotten Amazon Connect admin password

- See Emergency admin login (p. 146).

Reset your agent or manager password

Use the following steps if you want to change your password, or if you forgot it and need a new one.

1. If you're an Amazon Connect agent or manager, at the login page, choose **Forgot Password**.
2. Type the characters you see in the image, and then choose **Recover Password**.
3. A message will be sent to your email address with a link that you can use to reset your password.

Reset your own lost or forgotten AWS password

- To reset the password you used when you first created your AWS account, see Resetting a Lost or Forgotten Root User Password in the *IAM User Guide*.

Security profiles

A security profile is a group of permissions that map to a common role in a contact center. For example, the Agent security profile contains permissions needed to access the Contact Control Panel (CCP).

Security profiles help you manage who can access the Amazon Connect dashboard and Contact Control Panel (CCP), and who can perform specific tasks.

Contents

Best practices for security profiles

- Limit who has **Users - Edit or Create** permissions

People with these permissions pose a risk to your contact center because they can do the following:

- Reset passwords, including that of the administrator.
- Grant other users permission to the Admin security profile. People assigned to the Admin security profile have full access to your contact center.

Doing these things would enable someone to lock out those who need to access Amazon Connect, and allow in others who can steal customer data and damage your business.

To reduce the risk, as a best practice we recommend limiting the number of people who have **Users - Edit or Create** permissions.

- Use AWS CloudTrail (p. 1025) to log the requests and responses of UpdateUserIdentityInfo. This enables you to track changes made to user information. Someone who has the ability to call the `UpdateUserIdentityInfo` API can change a user's email address to one owned by an attacker, and then reset the password through email.
- Understand inherited permissions (p. 790)

  Some security profiles included inherited permissions: when you assign dedicated permissions to one object, by default permissions are granted to sub-objects. For example, when you grant dedicated permission to edit users, you also grant them permission to list all security profiles for your Amazon Connect instance. This because to edit users, the person has access to drop-down list of security profiles.

  Before assigning security profiles, review the list of inherited permissions.
- Track who accesses recordings (p. 806).

  In the **Analytics** permission group, you can enable a download icon for recorded conversations. When members of this group go to **Analytics**, **Contact search**, and then search contacts, they will see an icon to download recordings.

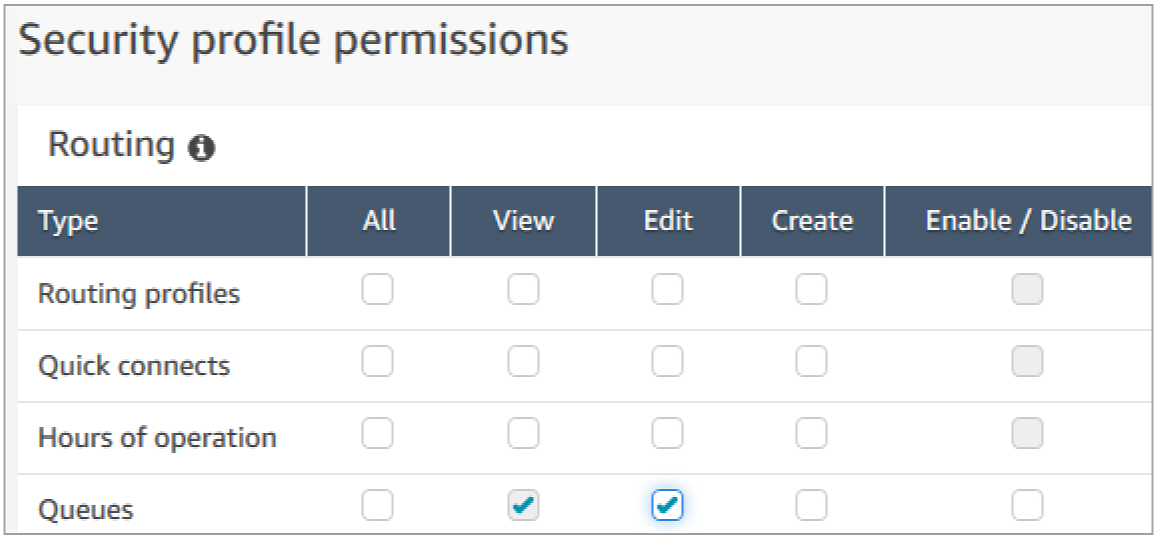
  > **Important**
  > This setting isn't a security feature. **Users who don't have this permission can still download recordings using other less-discoverable ways**.

  We recommend that you track who in your organization accesses recordings.

About inherited permissions

Some security profiles included inherited permissions: when you give a user explicit permissions to **View** or **Edit** one resource type, such as queues, they implicitly inherit permissions to **View** another resource type, such as phone numbers.

For example, assume you explicitly grant someone permission to **Edit/View** queues, as shown in the following image:

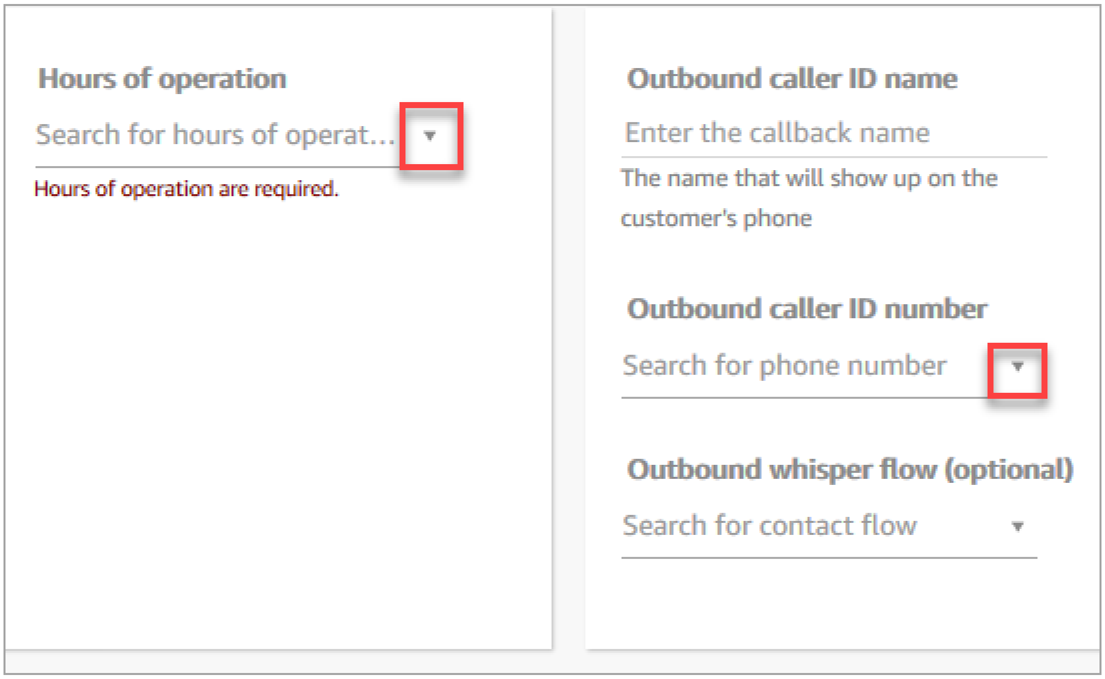


Security profile permissions

Routing

Type	All	View	Edit	Create	Enable / Disable
Routing profiles	□	□	□	□	□
Quick connects	□	□	□	□	□
Hours of operation	□	□	□	□	□
Queues	□	☑	☑	□	□

By doing this you also implicitly grant them permissions to **View** a list of all phone numbers and hours of operation in your Amazon Connect instance, **when they add them to the queue**. On the **Add new queue** page, the phone numbers and hours of operation appear in the drop-down lists, as shown in the following image:



Hours of operation

Search for hours of operat...

Hours of operation are required.

Outbound caller ID name

Enter the callback name

The name that will show up on the customer's phone

Outbound caller ID number

Search for phone number

Outbound whisper flow (optional)

Search for contact flow

However, the user doesn't have permissions to **Edit** the phone numbers and hours of operation.

In this case, they also don't inherit permissions to **View** contact flows (the outbound whisper flow) and quick connects because those resources are optional.

List of inherited permissions

The following table lists permissions that are implicitly inherited when you assign dedicated permissions.

Tip
When a user has only explicit **View** permissions and not also **Edit** permissions, the objects are retrieved but Amazon Connect doesn't surface them in drop-down lists for the user to peruse.

Dedicated permission	Inherited permissions
Users - View or Edit	When someone edits a user's information in the Amazon Connect console, they can **view** the following information in drop-down boxes when they add it to the user's account: • All security profiles in the instance • All routing profiles in the instance • All agent hierarchies in the instance
Queues - View or Edit	When someone edits queues in the Amazon Connect console, they can **view** the following information in drop-down and search boxes when they add it to the queue: • All quick connects in the instance • All phone numbers in the instance • All operating hours in the instance
Quick connects - View	• All queues in the instance • All contact flows in the instance • All users in the instance
Phone numbers - View or Edit	When someone edits phone numbers in the Amazon Connect console (not the CCP), they can **view** the following information in a drop-down box when they associate it with the phone number: • All contact flows in the instance

List of security profile permissions

The security profile permissions in Amazon Connect allow users access to perform particular tasks in Amazon Connect.

- AccessMetrics
- AgentGrouping.Create
- AgentGrouping.Edit
- AgentGrouping.EnableAndDisable
- AgentGrouping.View
- AgentStates.Create
- AgentStates.Edit
- AgentStates.EnableAndDisable
- AgentStates.View
- AgentTimeCard.View
- Audio.View

- BasicAgentAccess
- Campaigns.Create
- Campaigns.Delete
- Campaigns.Edit
- Campaigns.Manage
- Campaigns.View
- ChatTestMode
- ConfigureContactAttributes.View
- ContactAttributes.View
- ContactFlowModules.Create
- ContactFlowModules.Delete
- ContactFlowModules.Edit
- ContactFlowModules.Publish
- ContactFlowModules.View
- ContactFlows.Create
- ContactFlows.Delete
- ContactFlows.Edit
- ContactFlows.Publish
- ContactFlows.View
- ContactLensCustomVocabulary.Edit
- ContactLensCustomVocabulary.View
- ContactRecording.Access
- ContactSearch.View
- ContactSearchWithCharacteristics.Access
- ContactSearchWithCharacteristics.View
- ContactSearchWithKeywords.Access
- ContactSearchWithKeywords.View
- CustomerProfiles.Create
- CustomerProfiles.Edit
- CustomerProfiles.View
- DeleteCallRecordings
- DownloadCallRecordings
- GraphTrends.View
- HistoricalChanges.View
- HoursOfOperation.Create
- HoursOfOperation.Delete
- HoursOfOperation.Edit
- HoursOfOperation.View
- ListenCallRecordings
- ManagerListenIn
- MetricsReports.Create
- MetricsReports.Delete
- MetricsReports.Edit
- MetricsReports.Publish
- MetricsReports.Schedule
- MetricsReports.Share

- MetricsReports.View
- OutboundCallAccess
- PhoneNumbers.Claim
- PhoneNumbers.Edit
- PhoneNumbers.Release
- PhoneNumbers.View
- Prompts.Create
- Prompts.Delete
- Prompts.Edit
- Prompts.View
- Queues.Create
- Queues.Edit
- Queues.EnableAndDisable
- Queues.Purge
- Queues.View
- RealtimeContactLens.View
- RedactedData.View
- ReportsAdmin.Access
- ReportsAdmin.Delete
- ReportsAdmin.Publish
- ReportsAdmin.Schedule
- ReportsAdmin.View
- ReportSchedules.Create
- ReportSchedules.Delete
- ReportSchedules.Edit
- ReportSchedules.View
- RestrictContactAccessByHierarchy.View
- RoutingPolicies.Create
- RoutingPolicies.Edit
- RoutingPolicies.View
- Rules.Create
- Rules.Delete
- Rules.Edit
- Rules.View
- SecurityProfiles.Create
- SecurityProfiles.Delete
- SecurityProfiles.Edit
- SecurityProfiles.View
- TaskTemplates.Create
- TaskTemplates.Delete
- TaskTemplates.Edit
- TaskTemplates.View
- Transcript.View
- TransferDestinations.Create
- TransferDestinations.Delete
- TransferDestinations.Edit

- TransferDestinations.View
- UnredactedData.View
- Users.Create
- Users.Delete
- Users.Edit
- Users.EditPermission
- Users.EnableAndDisable
- Users.View
- VoiceId.Access
- VoiceIdAttributesAndSearch.View
- Wisdom.View

Default security profiles

Amazon Connect includes default security profiles for general roles. You can review the permissions granted by these profiles and use them if they align with the permissions that your users need. Otherwise, create a security profile that grants your users only the permissions they need.

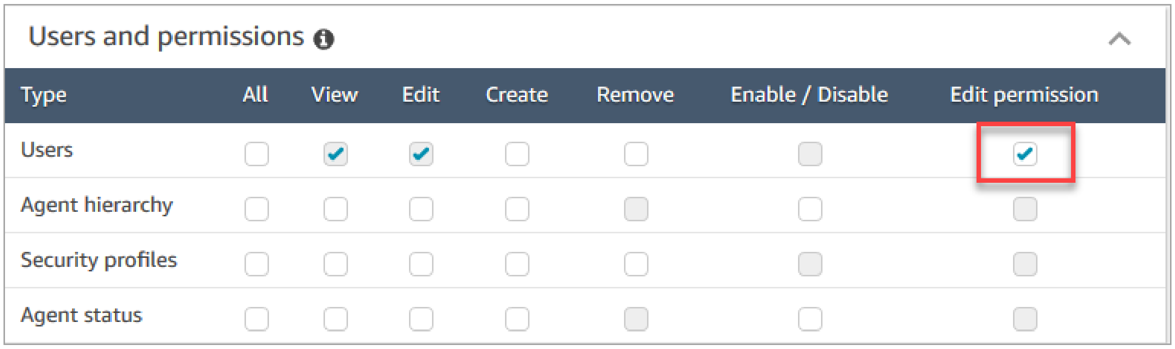
The following table lists the default security profiles:

Security profile	Description
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.

Assign a security profile to a user

Required permissions to assign security profiles

Before you can assign a security profile to a user, you must be logged in with an Amazon Connect account that has the **Users - Edit** permission. Or, if you're creating the user's account for the first time, you need **Users - Create** permission.



Users and permissions

Type	All	View	Edit	Create	Remove	Enable / Disable	Edit permission
Users	☐	☑	☑	☐	☐	☐	☑
Agent hierarchy	☐	☐	☐	☐	☐	☐	☐
Security profiles	☐	☐	☐	☐	☐	☐	☐
Agent status	☐	☐	☐	☐	☐	☐	☐

By default, the Amazon Connect **Admin** security profile has these permissions.

How to assign security profiles

1. Review Best practices for security profiles (p. 789).
2. Log in to your contact center at https://*instance name*.my.connect.aws/.
3. Choose **Users**, **User management**.
4. Select one or more users and choose **Edit**.
5. For **Security Profiles**, add or remove security profiles as needed. To add a security profile, put your cursor in the field and select the security profile from the list. To remove a security profile, click the **x** next to its name.
6. Choose **Save**.

Create a security profile

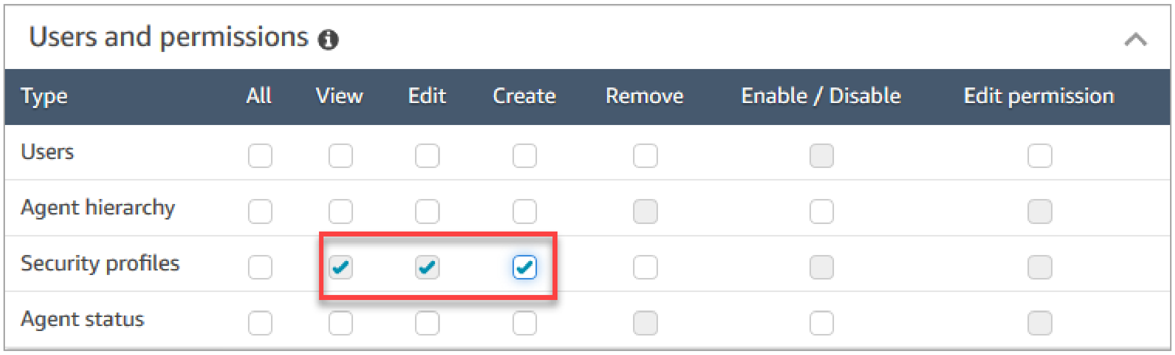
Creating a security profile enables you to grant your users only the permissions that they need.

For each permission group, there is a set of resources and supported set of actions. For example, users are part of the **Users and permissions** group, which supports the following actions: view, edit, create, remove, enable/disable, and edit permission.

Some actions depend on other actions. When you choose an action that depends on another action, the dependent action is automatically chosen and must also be granted. For example, if you add permission to edit users, we also add permission to view users.

Required permissions to create security profiles

Before you can create a new security profile, you must be logged in with an Amazon Connect account that has the following permissions: **Security profiles - Create**.



Users and permissions

Type	All	View	Edit	Create	Remove	Enable / Disable	Edit permission
Users	□	□	□	□	□	□	□
Agent hierarchy	□	□	□	□	□	□	□
Security profiles	□	☑	☑	☑	□	□	□
Agent status	□	□	□	□	□	□	□

By default, the Amazon Connect **Admin** security profile has these permissions.

How to create security profiles

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. Choose **Users**, **Security profiles**.
3. Choose **Add new security profile**.
4. Type a name and description for the security profile.
5. Choose the appropriate permissions for the security profile from each permission group. For each permission type, choose one or more actions. Selecting some actions results in other actions

being selected. For example, selecting **Edit** also selects **View** for the resource and any dependent resources.

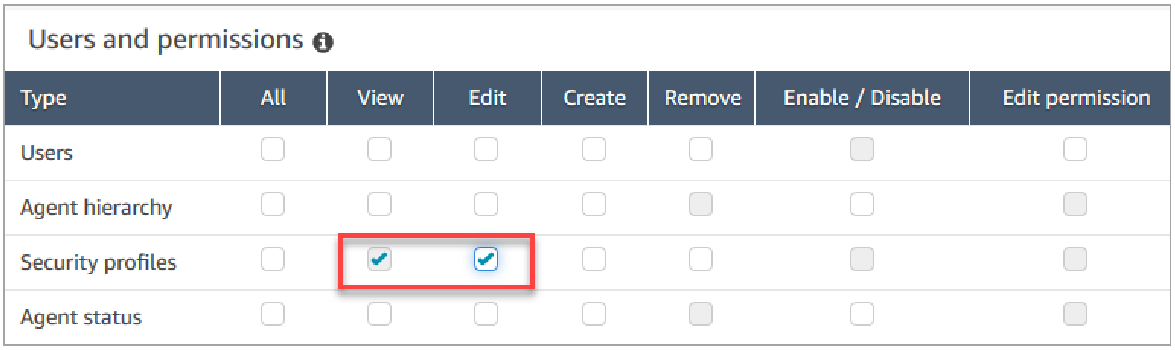
6. Choose **Save**.

Update security profiles

You can update a security profile at any time to add or remove permissions.

Required permissions to update security profiles

Before you can update permissions in a security profile, you must be logged in with an Amazon Connect account that has the following permissions: **Security profiles - Edit**.



Users and permissions

Type	All	View	Edit	Create	Remove	Enable / Disable	Edit permission
Users	□	□	□	□	□	□	□
Agent hierarchy	□	□	□	□	□	□	□
Security profiles	□	☑	☑	□	□	□	□
Agent status	□	□	□	□	□	□	□

By default, the Amazon Connect **Admin** security profile has these permissions.

How to update security profiles

1. Log in to your contact center at https://*instance name*.my.connect.aws/. You must be logged in with an Amazon Connect account that has permissions to update security profiles.
2. Choose **Users**, **Security profiles**.
3. Select the name of the profile.
4. Update the name, description, and permissions as needed.
5. Choose **Save**.

Monitor live and recorded conversations

The articles in this section explain how to monitor (listen-in) on conversations between agents and contacts.

Contents

Monitor live conversations

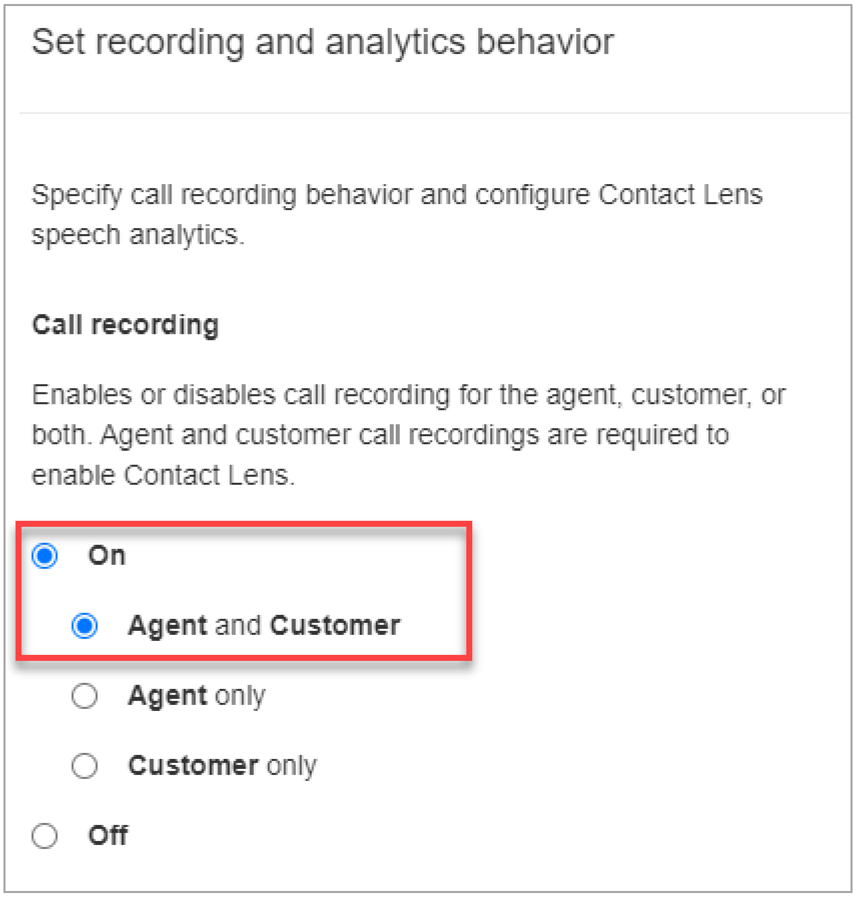
Managers and agents in training can monitor live conversations between agents and customers. To set this up, you need to add the **Set recording behavior** block to your voice/chat contact flow, assign managers and trainees the appropriate permissions, and then show them how to monitor the conversations.

Looking for how many people can monitor the same conversation at one time? See Feature specifications (p. 1210).

Set up live monitoring for voice and/or chat

1. Add the Set recording and analytics behavior (p. 408) block to your contact flow. Do this to monitor calls, chats, or both.

   To enable monitoring of voice and/or chat conversations, in the block's properties choose **Agent and Customer**.



Set recording and analytics behavior

Specify call recording behavior and configure Contact Lens speech analytics.

Call recording

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

● On

● Agent and Customer

○ Agent only

○ Customer only

○ Off

For more information, see Set up recording behavior (p. 479).

2. Choose whether to record the conversations you monitor.

   Although you need to add the **Set recording behavior** block to your contact flow, you don't need to record voice and/or chat conversations for monitoring to work. By default when you set up your instance, Amazon S3 buckets are created (p. 137) to store call recordings and chat transcripts. The existence of these buckets enables call recording and chat transcripts at the instance level.

   To not record the calls or chats you're monitoring, disable the Amazon S3 buckets. For instructions, see Update instance settings (p. 140).

Assign permissions to monitor live conversations

For managers to monitor live conversations, you assign them the **CallCenterManager** and **Agent** security profiles. To allow agent trainees to monitor live conversations, you may want to create a security profile specific for this purpose.

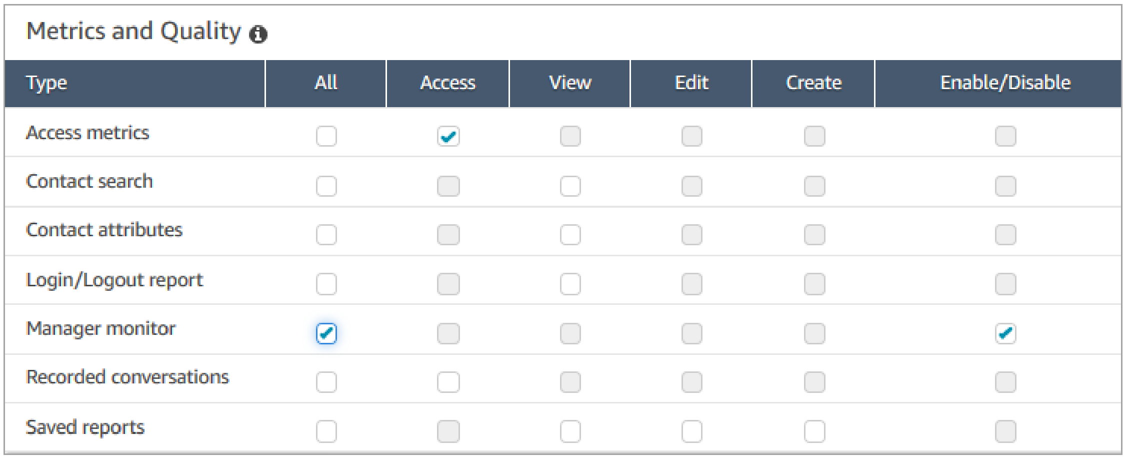
To assign a manager permissions to monitor a live conversation

1. Go to **Users**, **User management**, choose the manager, and then choose **Edit**.
2. In the Security Profiles box, assign the manager to the **CallCenterManager** security profile. This security profile also includes a setting that makes the icon to download recordings appear in the results of the **Contact search** page.

3. Assign the manager to the **Agent** security profile so they can access the Contact Control Panel (CCP), and use it to monitor the conversation.
4. Choose **Save**.

To create a new security profile for monitoring live conversations

1. Choose **Users**, **Security profiles**.
2. Choose **Add new security profile**.
3. Expand **Analytics**, then choose **Access metrics** and **Manager monitor**.

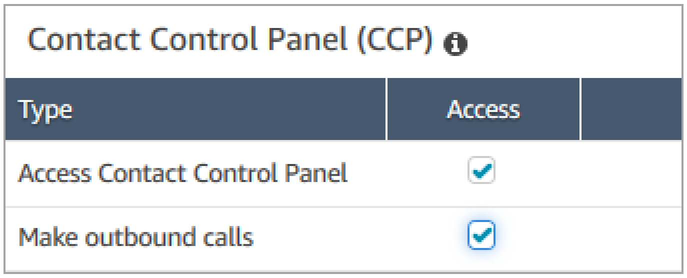


Metrics and Quality

Type	All	Access	View	Edit	Create	Enable/Disable
Access metrics	□	☑	□	□	□	□
Contact search	□	□	□	□	□	□
Contact attributes	□	□	□	□	□	□
Login/Logout report	□	□	□	□	□	□
Manager monitor	☑	□	□	□	□	☑
Recorded conversations	□	□	□	□	□	□
Saved reports	□	□	□	□	□	□

Access metrics is needed so they can access the real-time metrics report, which is where they choose which conversations to monitor.

4. Expand **Contact Control Panel**, then choose **Access Contact Control Panel** and **Make outbound calls**.



Contact Control Panel (CCP)

Type	Access	
Access Contact Control Panel	☑	
Make outbound calls	☑	

These permissions are needed so they can monitor the conversation through the Contact Control Panel.

5. Choose **Save**.

Monitor live conversations with contacts

Tip
Call barge-in is not currently supported. That is, if you're listening to a conversation, your microphone stays muted.

1. Check that the Set recording and analytics behavior (p. 408) block is in the contact flow you want to monitor. It has to be there whether you're monitoring calls or chats. In the block's Properties, choose **Agent and Customer**.

2. Log in to your Amazon Connect instance with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for the **Manager monitor** permission.
3. Open the Contact Control Panel (CCP) by choosing the phone icon in the top-right corner of your screen. You'll need the CCP open to connect to the conversation.
4. To choose the agent conversation you want to monitor, in Amazon Connect choose **Analytics**, **Real-time metrics**, **Agents**.
5. To monitor voice conversations: Next to the names of agents in a live voice conversation, you'll see an eye icon. Choose the icon to start monitoring the conversation.

   When you're monitoring a conversation, the status in your CCP changes to **Monitoring**.
6. To monitor chat conversations: For each agent you'll see the number of live chat conversations they're in. Click on the number. Then choose the conversation you want to start monitoring.

   When you're monitoring a conversation, the status in your CCP changes to **Monitoring**.
7. To stop monitoring the conversation, in the CCP choose **End call** or **End chat**.

   When the agent ends the conversation, monitoring stops automatically.

Review recorded conversations

Managers can review past conversations between agents and customers. To set this up, you need to set up recording behavior (p. 479), assign managers the appropriate permissions, and then show them how to access the recorded conversations.

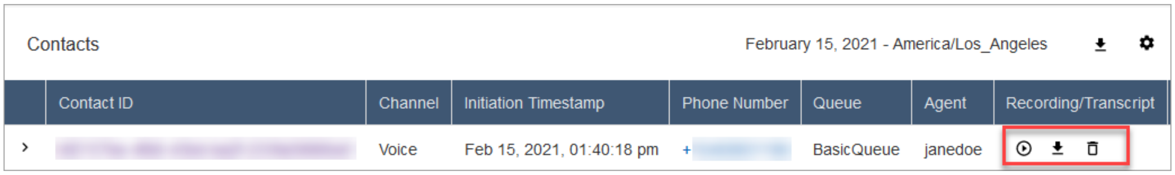
When is a conversation recorded? A conversation is recorded only when the contact is connected to an agent. The contact is not recorded before then, when they are connected to the IVR. If the call is transferred externally, the call recording stops when the agent drops from the call.

> **Tip**
> When call recording is enabled, the recording is placed in your S3 bucket shortly after the contact is disconnected. Then the recording is available for you to review it using the steps in this article.
> You can also access the recording from the customer's contact record (p. 997). The recording is available in the contact record, however, only after the contact has left the After Contact Work (ACW) state (p. 999).

How do I manage access to recordings? Use the **Recorded conversations (unredacted)** security profile permission to manage who can listen to recordings, and access the corresponding URLs that are generated in S3. For more information about this permission, see Assign permissions to review recordings of past conversations (p. 801).

Assign permissions to review recordings of past conversations

Assign the **CallCenterManager** security profile so a user can listen to call recordings or review chat transcripts. This security profile also includes a setting that makes the icon to download recordings appear in the results of the **Contact search** page.

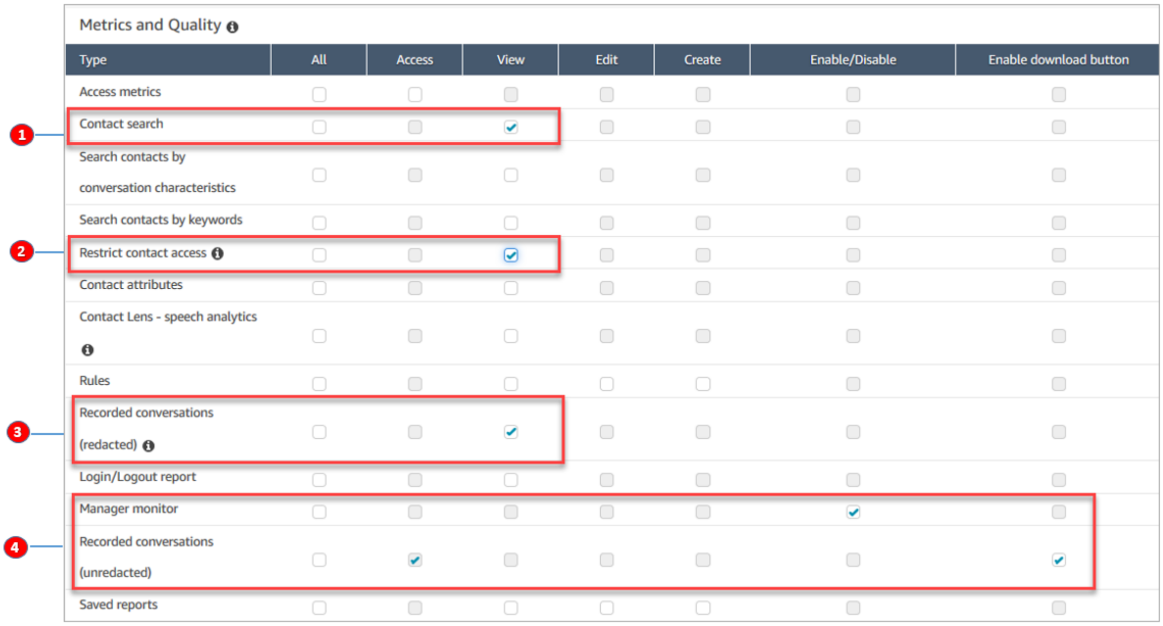


Contacts

February 15, 2021 - America/Los_Angeles ⬇ ⚙

	Contact ID	Channel	Initiation Timestamp	Phone Number	Queue	Agent	Recording/Transcript
›	[redacted]	Voice	Feb 15, 2021, 01:40:18 pm	+ [redacted]	BasicQueue	janedoe	▶ ⬇ 🗑

Or, assign the following individual permissions.



Metrics and Quality

Type	All	Access	View	Edit	Create	Enable/Disable	Enable download button
Access metrics	☐	☐	☐	☐	☐	☐	☐
Contact search	☐	☐	☑	☐	☐	☐	☐
Search contacts by conversation characteristics	☐	☐	☐	☐	☐	☐	☐
Search contacts by keywords	☐	☐	☐	☐	☐	☐	☐
Restrict contact access	☐	☐	☑	☐	☐	☐	☐
Contact attributes	☐	☐	☐	☐	☐	☐	☐
Contact Lens - speech analytics	☐	☐	☐	☐	☐	☐	☐
Rules	☐	☐	☐	☐	☐	☐	☐
Recorded conversations (redacted)	☐	☐	☑	☐	☐	☐	☐
Login/Logout report	☐	☐	☐	☐	☐	☐	☐
Manager monitor	☐	☐	☐	☐	☐	☑	☐
Recorded conversations (unredacted)	☐	☑	☐	☐	☐	☐	☑
Saved reports	☐	☐	☐	☐	☐	☐	☐

1. **Contact search**: This permission is required so users can access the **Contact search** page, which is where they can search contacts so they can listen to recordings and review transcripts.
2. **Restrict contact access**: Manage access to results on the **Contact search** page based on their agent hierarchy group.

   For example, agents who are assigned to AgentGroup-1 can only view contact trace records (CTRs) for contacts handled by agents in that hierarchy group, and any groups below them. (If they have permissions for **Recorded conversations**, they can also listen to call recordings and view transcripts.) Agents assigned to AgentGroup-2 can only access CTRs for contacts handled by their group, and any groups below them.

   Managers and others who are in higher level groups can view CTRs for contacts handled by all the groups below them, such as AgentGroup-1 and 2.

   For this permission, **All** = **View** since **View** is the only action granted.

   For more information about hierarchy groups, see Set up agent hierarchies (p. 230).

   Note

   When you change a the hierarchy group of a user, it may take a couple of minutes for their contact search results to reflect their new permissions.
3. **Recorded conversations (redacted)**: If your organization uses Contact Lens for Amazon Connect, you can assign this permission so agents access only those call recordings and transcripts in which sensitive data has been removed.

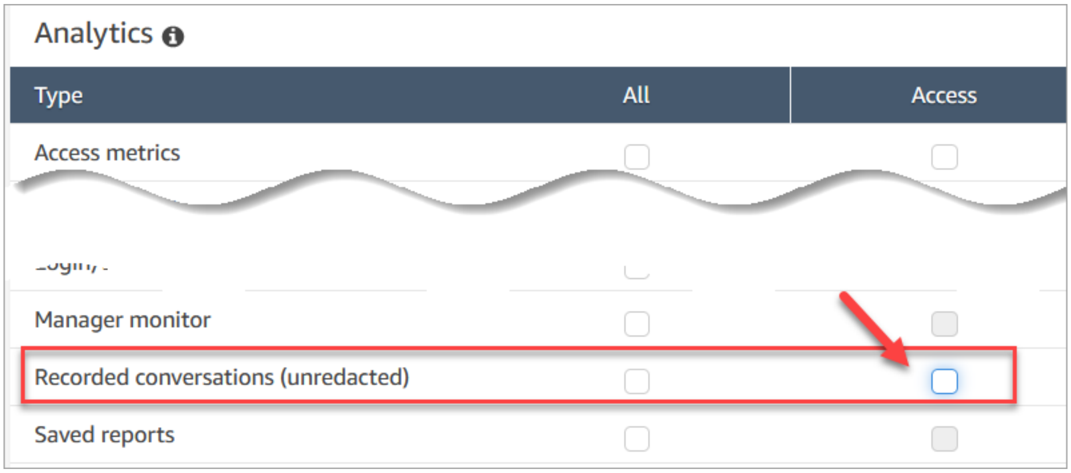
   The redaction feature is provided as part of Contact Lens for Amazon Connect. For more information, see Use sensitive data redaction (p. 837).
4. **Manager monitor**: This permission allows users to monitor live conversations and listen to recordings.

   Tip

   Be sure to assign managers to the **Agent** security profile so they can access the Contact Control Panel (CCP). This enables them can monitor the conversation through the CCP.
5. **Recorded conversations (unredacted)**: If your organization isn't using Contact Lens for Amazon Connect, use this permission to manage who can listen to recordings, access the corresponding URLs that are generated in S3, and delete recordings.

Note the following:

- To restrict access to recordings, ensure users do not have **Analytics** - **Recorded conversations (unredacted) - Access** permissions, as shown in the following image.



Analytics

Type	All	Access
Access metrics	□	□
Manager monitor	□	□
Recorded conversations (unredacted)	□	□
Saved reports	□	□

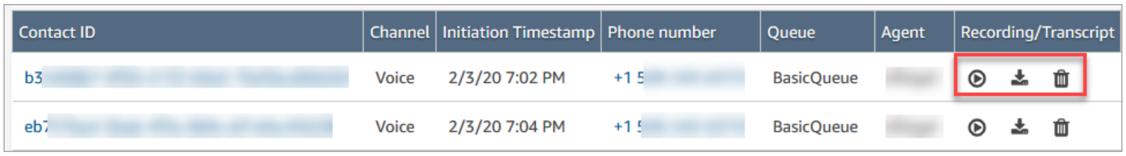
- If users do not have **Recorded conversations** permission—or they're not logged in to Amazon Connect—they cannot listen to the call recording or access the URL in S3, even if they know how the URL is formed.
- The **Enable download button** permission controls only whether the download button appears in the user interface. It does not control access to the recording.
- To enable a user to delete recordings, choose the **Delete** permission. By default, the **Enable download button** permission is granted too so the user can delete recordings through the user interface.

Review recordings/transcripts of past conversations

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

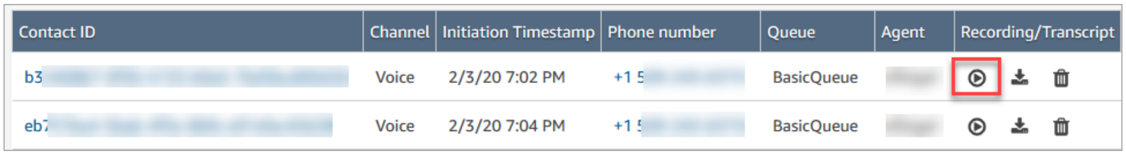
1. Log in to Amazon Connect with a user account that has permissions to access recordings (p. 801).
2. In Amazon Connect choose **Analytics**, **Contact search**.
3. Filter the list of contacts by date, agent login, phone number, or other criteria. Choose **Search**.

   Tip
   We recommend using the **Contact ID** filter to search for recordings (p. 810). This is the best way to ensure you get the right recording for the contact. Many recordings have the same name as the contact ID, but not all.
4. Conversations that were recorded have icons in the **Recording/Transcript** column. If you don't have the appropriate permissions, you won't see these icons.



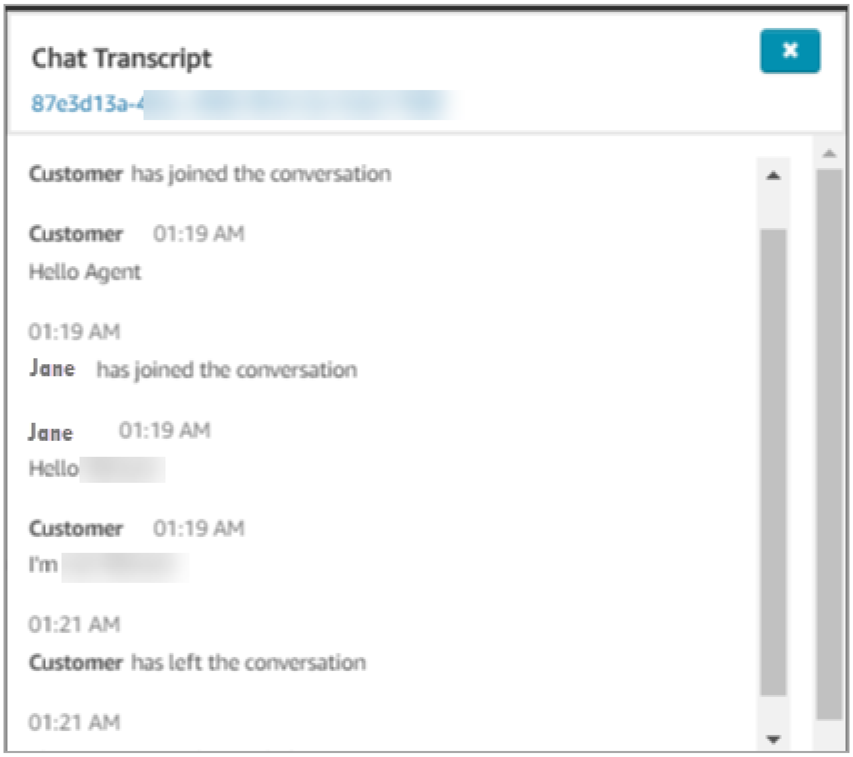
Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

5. To listen to a recording of a voice conversation, or read the transcript of a chat, choose the **Play** icon.



Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

6. The following image shows a sample chat transcript.



Chat Transcript

87e3d13a-4[redacted]

Customer has joined the conversation

Customer 01:19 AM
Hello Agent

01:19 AM
Jane has joined the conversation

Jane 01:19 AM
Hello [redacted]

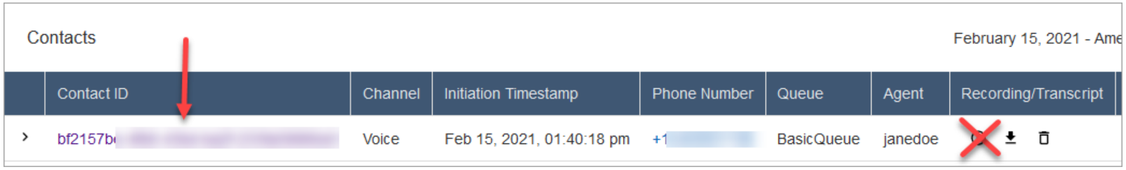
Customer 01:19 AM
I'm [redacted]

01:21 AM
Customer has left the conversation

01:21 AM

Pause, rewind, or fast-forward a recording

1. Instead of choosing the **Play** icon, choose the contact ID to open the contact record.

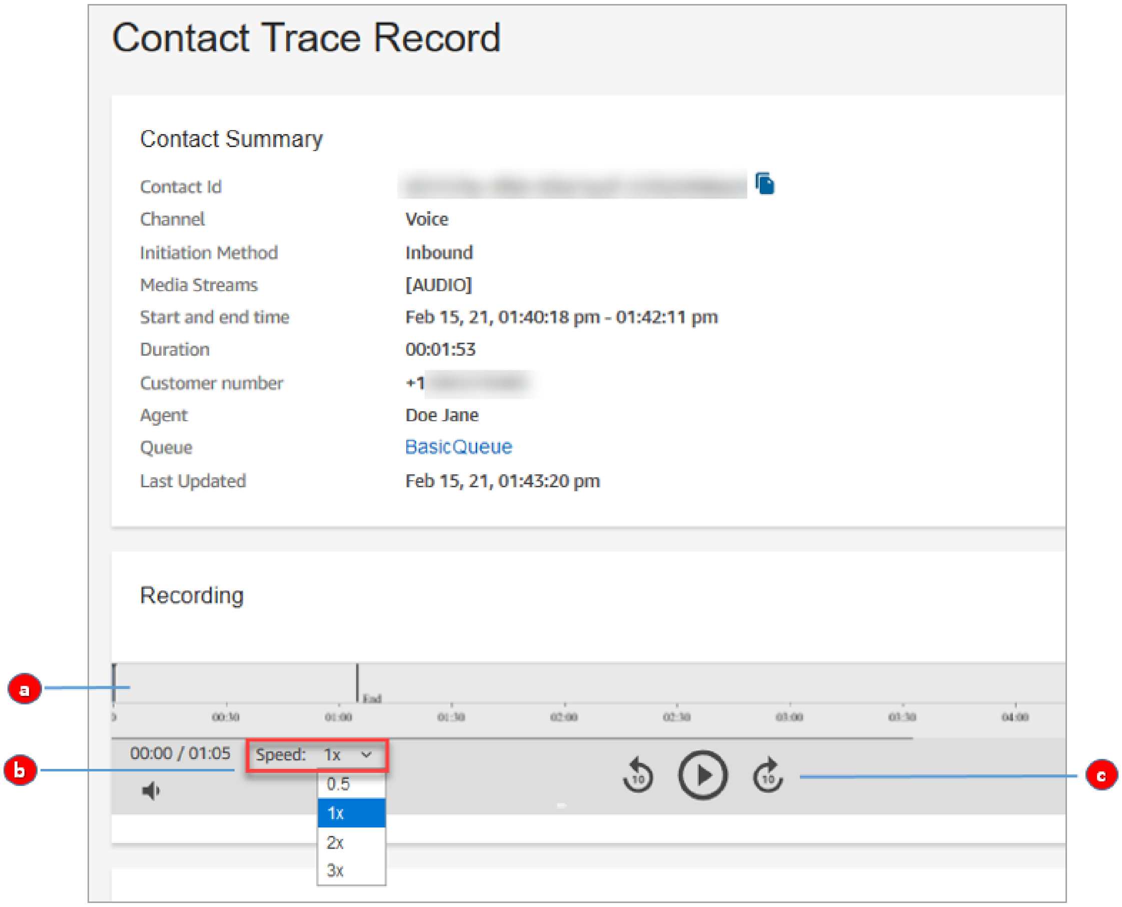


Contacts

February 15, 2021 - Ame

	Contact ID	Channel	Initiation Timestamp	Phone Number	Queue	Agent	Recording/Transcript
›	bf2157b[redacted]	Voice	Feb 15, 2021, 01:40:18 pm	+1[redacted]	BasicQueue	janedoe	

2. On the **Contact record** page, there are more controls to navigate the recording.



Contact Trace Record

Contact Summary

Contact Id	[redacted]
Channel	Voice
Initiation Method	Inbound
Media Streams	[AUDIO]
Start and end time	Feb 15, 21, 01:40:18 pm - 01:42:11 pm
Duration	00:01:53
Customer number	+1 [redacted]
Agent	Doe Jane
Queue	BasicQueue
Last Updated	Feb 15, 21, 01:43:20 pm

Recording

1. Click or tap to the time you want to investigate.
2. Adjust the playing speed.
3. Play, pause, skip backwards or forwards in 10 second increments.

Troubleshoot problems pausing, rewinding, or fast-fowarding

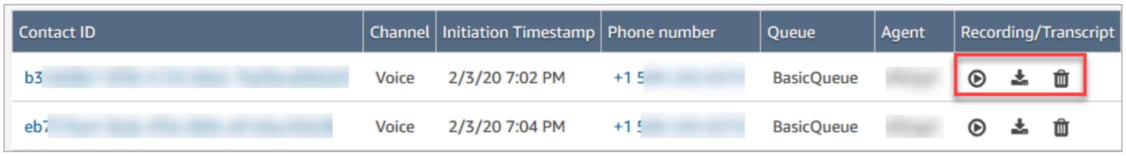
If you are unable to pause, rewind or fast-forward recordings on the **Contact search** page, one possible reason could be that your network is blocking HTTP range requests. See HTTP range requests on the MDN Web Docs site. Work with your network administrator to unblock HTTP range requests.

Download recordings/transcripts of past conversations

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

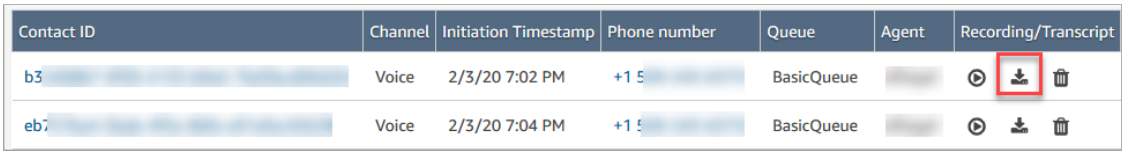
1. Log in to Amazon Connect with a user account that has permissions to access recordings (p. 801).
2. In Amazon Connect choose **Analytics**, **Contact search**.
3. Filter the list of contacts by date, agent login, phone number, or other criteria. Choose **Search**.

4. Conversations that were recorded have icons in the **Recording/Transcript** column. If you don't have the appropriate permissions, you won't see these icons.



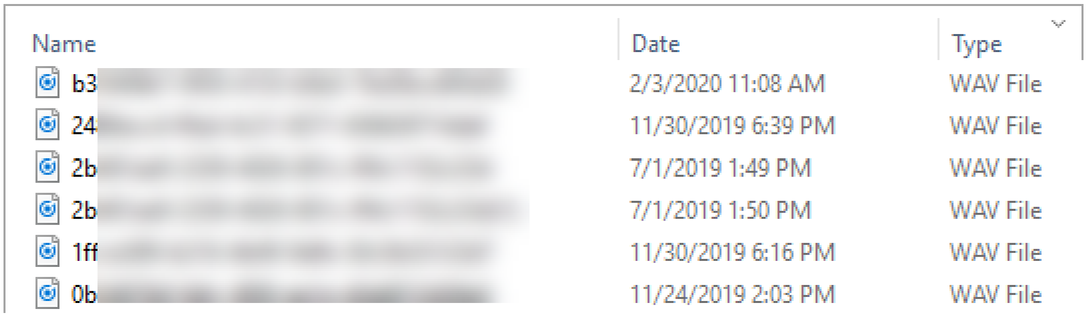
Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

5. Choose the **Download** icon.



Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

6. The recording is saved automatically to your **Downloads** folder as a .wav file.



Name	Date	Type
b3[redacted]	2/3/2020 11:08 AM	WAV File
24[redacted]	11/30/2019 6:39 PM	WAV File
2b[redacted]	7/1/2019 1:49 PM	WAV File
2b[redacted]	7/1/2019 1:50 PM	WAV File
1ff[redacted]	11/30/2019 6:16 PM	WAV File
0b[redacted]	11/24/2019 2:03 PM	WAV File

The name of the file is the contact ID.

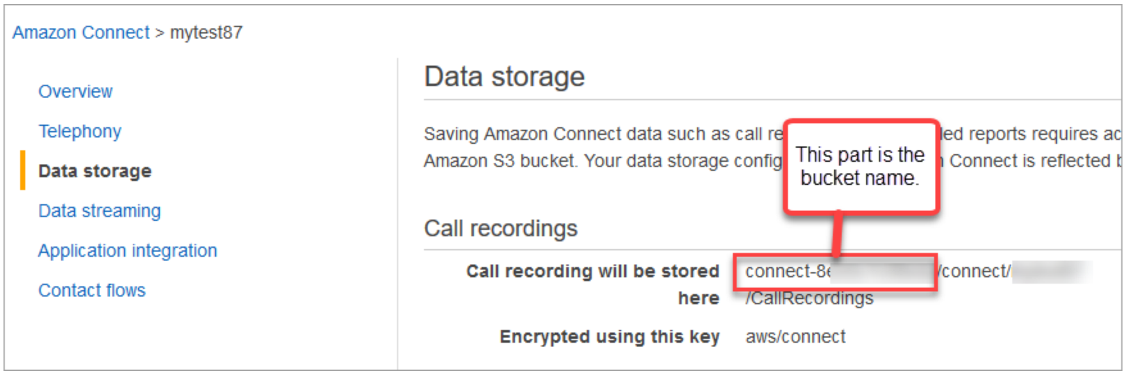
Tip
You may hear only the agent, only the customer, or both the agent and customer in the recording. This is determined by how the Set recording and analytics behavior (p. 408) block is configured (p. 480).

Track who deleted or listened to recordings

You need an AWS account to do these steps.

Set up logging

1. If you have multiple instances and buckets, look up the name of the Amazon S3 bucket for your instance. Go to the Amazon Connect console, choose the instance alias, and choose **Data storage**.



Data storage

Saving Amazon Connect data such as call re… …ed reports requires ac… Amazon S3 bucket. Your data storage config… …Connect is reflected b…

This part is the bucket name.

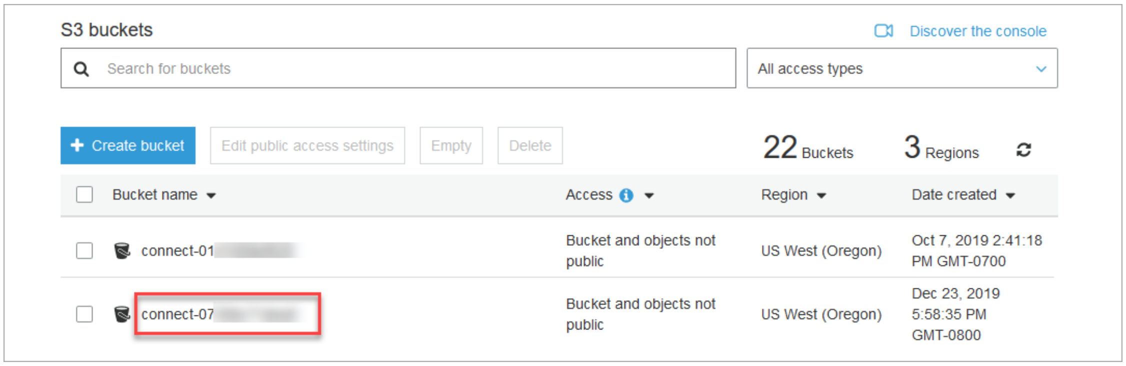
Call recordings

Call recording will be stored here connect-8e[redacted]/connect/[redacted]/CallRecordings

Encrypted using this key aws/connect

2. Go to the Amazon S3 console.

3. Choose the Amazon S3 bucket where your recordings are stored.



S3 buckets

□	Bucket name	Access	Region	Date created
□	connect-01[redacted]	Bucket and objects not public	US West (Oregon)	Oct 7, 2019 2:41:18 PM GMT-0700
□	connect-07[redacted]	Bucket and objects not public	US West (Oregon)	Dec 23, 2019 5:58:35 PM GMT-0800

4. Choose the **Properties** tab.

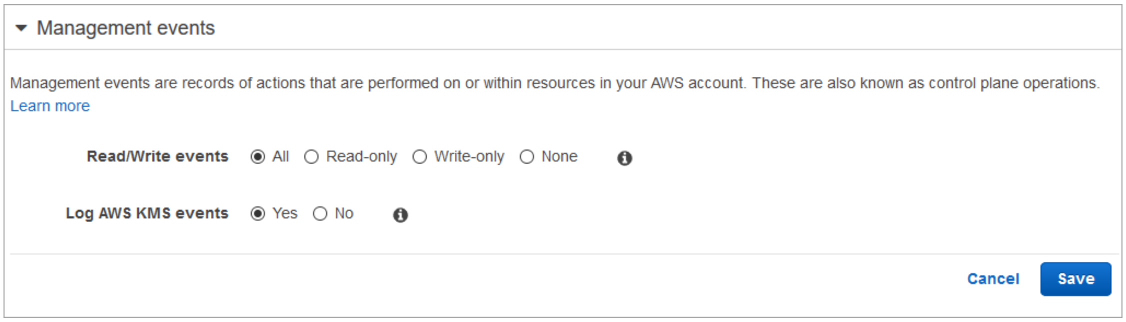
5. Choose **Object-level logging** and then choose **View CloudTrail trails**.

   It opens the AWS CloudTrail console.

6. In the navigation menu, choose **Trails** and then choose the trail name.

7. In the upper right corner, toggle **Logging** to **ON**, if it's not on already.

8. Under **Management** events, choose the edit icon. To log only who deletes recordings, you set this to **Write-only**. To also log who listens to recordings, set to **All**. Choose **Save**.



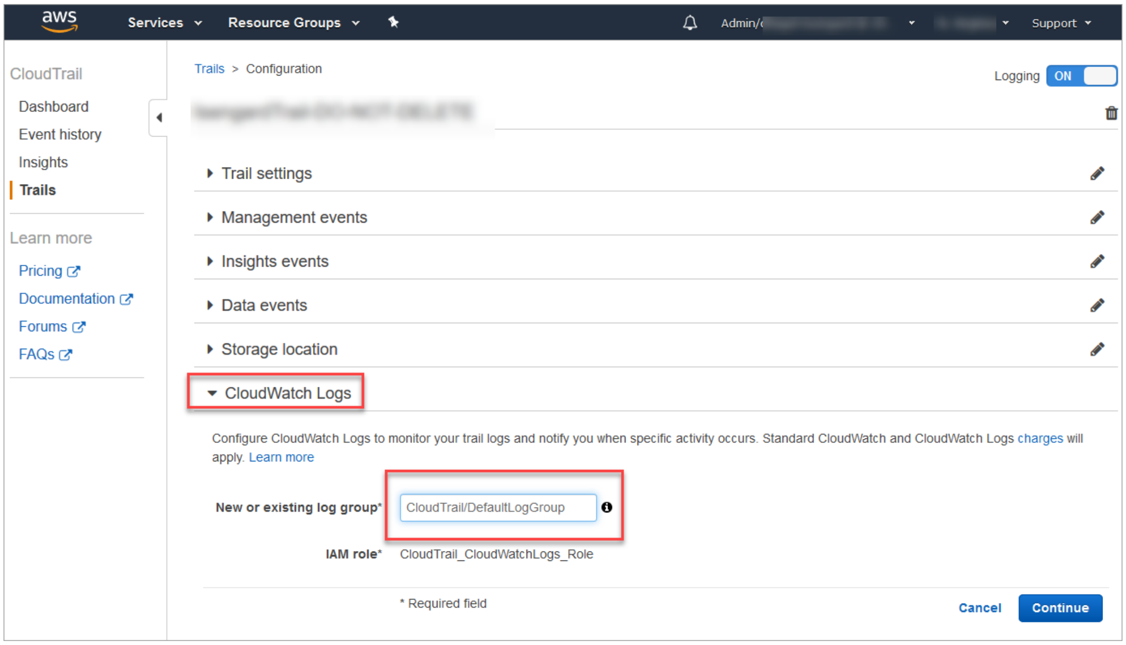
Management events

Management events are records of actions that are performed on or within resources in your AWS account. These are also known as control plane operations. Learn more

Read/Write events ● All ○ Read-only ○ Write-only ○ None

Log AWS KMS events ● Yes ○ No

9. Under **CloudWatch Logs** choose the edit icon. Either accept the default name for your log group (CloudTrail/DefaultLogGroup), or specify a new name. Choose **Continue**.



Trails > Configuration

Logging ON

[redacted]

- Trail settings
- Management events
- Insights events
- Data events
- Storage location
- CloudWatch Logs

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges will apply. Learn more

New or existing log group* CloudTrail/DefaultLogGroup

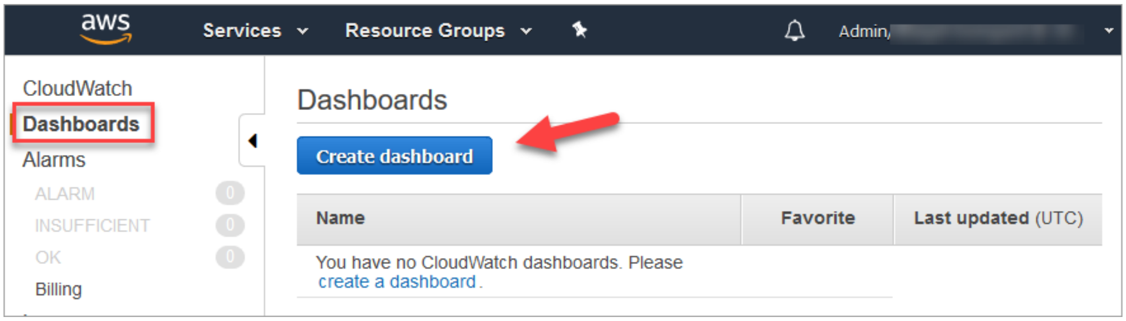
IAM role* CloudTrail_CloudWatchLogs_Role

* Required field

10. Choose **Allow**. You can now close the AWS CloudTrail console.

Find who deleted or listened to recordings

1. Go to the Amazon CloudWatch console.
2. Choose **Create dashboard**.



Name	Favorite	Last updated (UTC)
You have no CloudWatch dashboards. Please create a dashboard.		

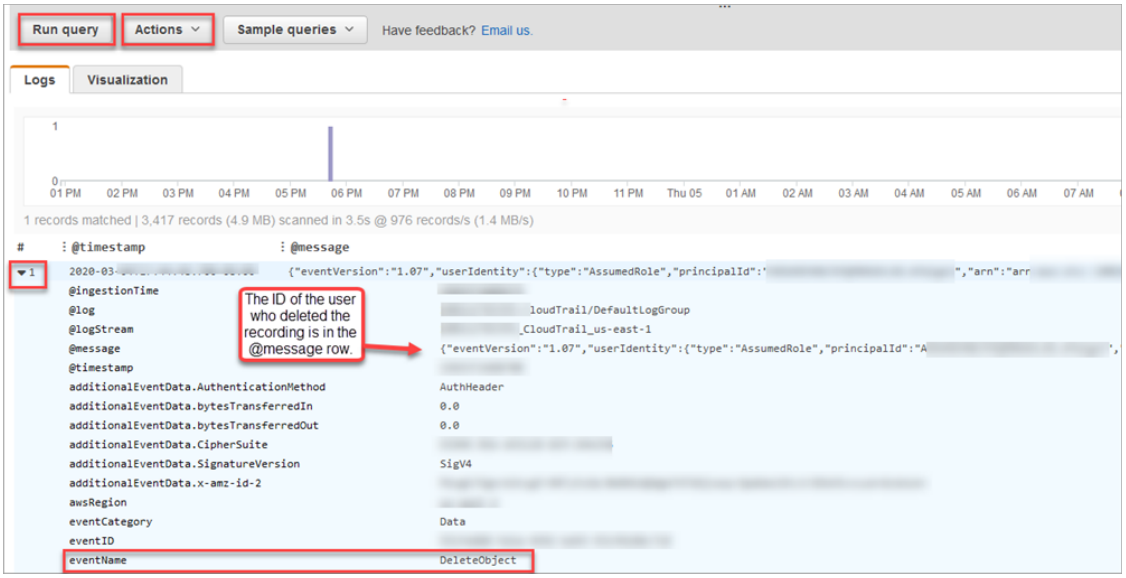
3. Enter a name, such as **CloudTrail-logging**.
4. On the **Add to this dashboard** dialog box, choose **Query results**. Choose **Configure**.
5. In the **Select log groups**, use the drop-down arrow to choose the log group for your instance, such as **CloudTrail/DefaultLogGroup**.
6. In the query box, delete the current query, and then copy and paste the one shown below instead. This query will find all API events where the recording was deleted:

```
fields @timestamp, @message
| filter eventSource ='s3.amazonaws.com'
| filter eventName = 'DeleteObject'
```

7. In the time box, choose how far back you want to search.
8. Choose **Run query**.

   It returns all of the events that are named **DeleteObject**.

9. Next to the event, choose the arrow. It expands to show you detailed information about the event, including the ID of the user who deleted the recording.



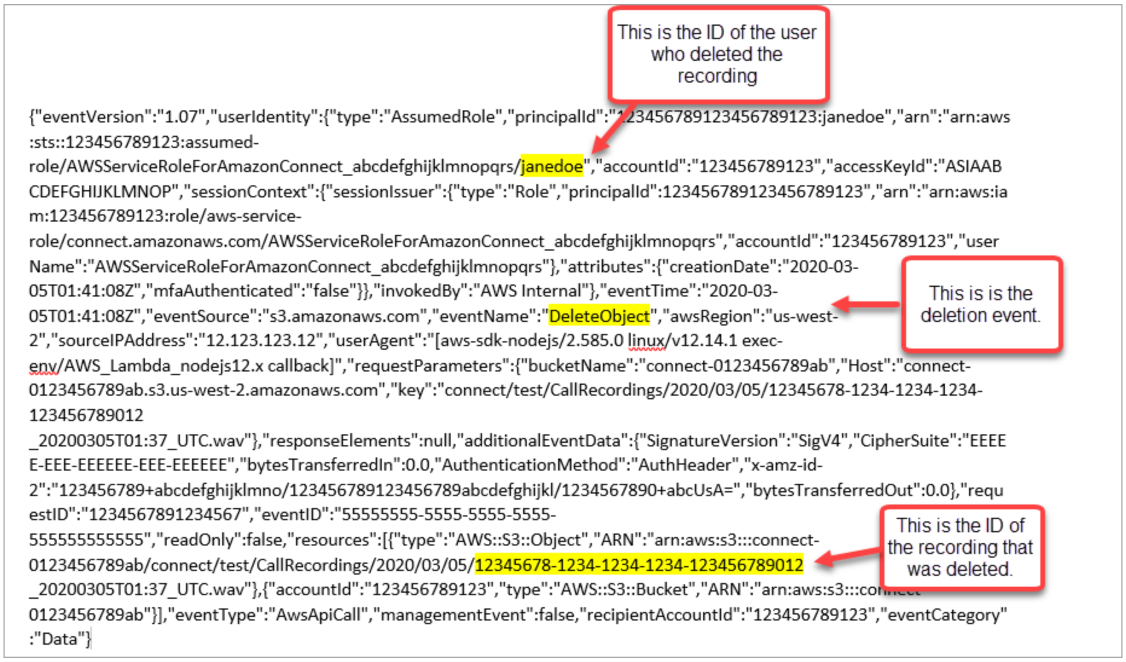
1 records matched | 3,417 records (4.9 MB) scanned in 3.5s @ 976 records/s (1.4 MB/s)

```
#   @timestamp        @message
▾1  2020-03-[redacted]  {"eventVersion":"1.07","userIdentity":{"type":"AssumedRole","principalId":'[redacted]","arn":"arr[redacted]
    @ingestionTime                         [redacted]
    @log                                   [redacted]loudTrail/DefaultLogGroup
    @logStream                             [redacted]_CloudTrail_us-east-1
    @message                               {"eventVersion":"1.07","userIdentity":{"type":"AssumedRole","principalId":"A[redacted]',
    @timestamp                             [redacted]
    additionalEventData.AuthenticationMethod  AuthHeader
    additionalEventData.bytesTransferredIn    0.0
    additionalEventData.bytesTransferredOut   0.0
    additionalEventData.CipherSuite           [redacted]
    additionalEventData.SignatureVersion      SigV4
    additionalEventData.x-amz-id-2            [redacted]
    awsRegion                                 [redacted]
    eventCategory                             Data
    eventID                                   [redacted]
    eventName                                 DeleteObject
```

The ID of the user who deleted the recording is in the @message row.

10. If a lot of records are returned, choose the **Actions** arrow, and then choose **Download query results (CSV)**. The data is exported to Excel. From there you can format the spreadsheet so it's easier for you to search and see the names of the users who deleted recordings.

   The following image shows what the @message column looks like in the CSV file.



This is the ID of the user who deleted the recording

{"eventVersion":"1.07","userIdentity":{"type":"AssumedRole","principalId":"123456789123456789123:janedoe","arn":"arn:aws
:sts::123456789123:assumed-
role/AWSServiceRoleForAmazonConnect_abcdefghijklmnopqrs/janedoe","accountId":"123456789123","accessKeyId":"ASIAAB
CDEFGHIJKLMNOP","sessionContext":{"sessionIssuer":{"type":"Role","principalId":123456789123456789123","arn":"arn:aws:ia
m:123456789123:role/aws-service-
role/connect.amazonaws.com/AWSServiceRoleForAmazonConnect_abcdefghijklmnopqrs","accountId":"123456789123","user
Name":"AWSServiceRoleForAmazonConnect_abcdefghijklmnopqrs"},"attributes":{"creationDate":"2020-03-
05T01:41:08Z","mfaAuthenticated":"false"}},"invokedBy":"AWS Internal"},"eventTime":"2020-03-
05T01:41:08Z","eventSource":"s3.amazonaws.com","eventName":"DeleteObject","awsRegion":"us-west-
2","sourceIPAddress":"12.123.123.12","userAgent":"[aws-sdk-nodejs/2.585.0 linux/v12.14.1 exec-
env/AWS_Lambda_nodejs12.x callback]","requestParameters":{"bucketName":"connect-0123456789ab","Host":"connect-
0123456789ab.s3.us-west-2.amazonaws.com","key":"connect/test/CallRecordings/2020/03/05/12345678-1234-1234-1234-
123456789012
_20200305T01:37_UTC.wav"},"responseElements":null,"additionalEventData":{"SignatureVersion":"SigV4","CipherSuite":"EEEE
E-EEE-EEEEEE-EEE-EEEEEE","bytesTransferredIn":0.0,"AuthenticationMethod":"AuthHeader","x-amz-id-
2":"123456789+abcdefghijklmno/123456789123456789abcdefghijkl/1234567890+abcUsA=","bytesTransferredOut":0.0},"requ
estID":"1234567891234567","eventID":"55555555-5555-5555-5555-
555555555555","readOnly":false,"resources":[{"type":"AWS::S3::Object","ARN":"arn:aws:s3:::connect-
0123456789ab/connect/test/CallRecordings/2020/03/05/12345678-1234-1234-1234-123456789012
_20200305T01:37_UTC.wav"},{"accountId":"123456789123","type":"AWS::S3::Bucket","ARN":"arn:aws:s3:::connect-
0123456789ab"}],"eventType":"AwsApiCall","managementEvent":false,"recipientAccountId":"123456789123","eventCategory"
:"Data"}

This is is the deletion event.

This is the ID of the recording that was deleted.

11. If you're also logging who listened to recordings, update the query to search for the eventName **GetBucketLocation**.

```
fields @timestamp, @message
| filter eventSource ='s3.amazonaws.com'
| filter eventName = 'GetBucketLocation'
```

Tips

Mirroring CloudTrail logs to CloudWatch is useful but optional. Mirroring the CloudWatch log allows you to use CloudWatch Insight to search the events easily.

If you have a large contact center, you may not want to use object logging because it generates many logs that are stored in your Amazon S3 bucket.

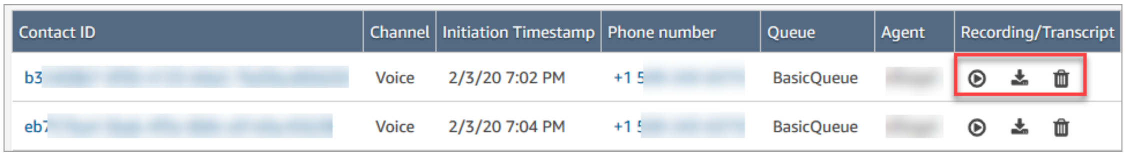
Another option is to write an AWS Lambda function to process the CloudTrail events. You can also search the logs manually.

Search for recordings by contact ID

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

> **Tip**
> We recommend using the contact ID to search for recordings.
> Even though many call recordings for specific contact IDs may be named with the contact ID prefix itself (for example, 123456-aaaa-bbbb-3223-2323234.wav), there is no guarantee that the contact IDs and name of the contact recording file always match. By using **Contact ID** for your search on the **Contact search** page, you can find the correct recording by referring the audio file on the contact's record.

1. Log in to Amazon Connect with a user account that has permissions to access recordings (p. 801).
2. In Amazon Connect choose **Analytics**, **Contact search**.
3. In the **Contact ID**, enter the contact ID, and then choose **Search**.
4. Conversations that were recorded have icons in the **Recording/Transcript** column. If you don't have the appropriate permissions, you won't see these icons.



Contact ID	Channel	Initiation Timestamp	Phone number	Queue	Agent	Recording/Transcript
b3[redacted]	Voice	2/3/20 7:02 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑
eb7[redacted]	Voice	2/3/20 7:04 PM	+1 5[redacted]	BasicQueue	[redacted]	▶ ⬇ 🗑

To learn more about searching, see Search for contacts (p. 907).

Analyze conversations using Contact Lens for Amazon Connect

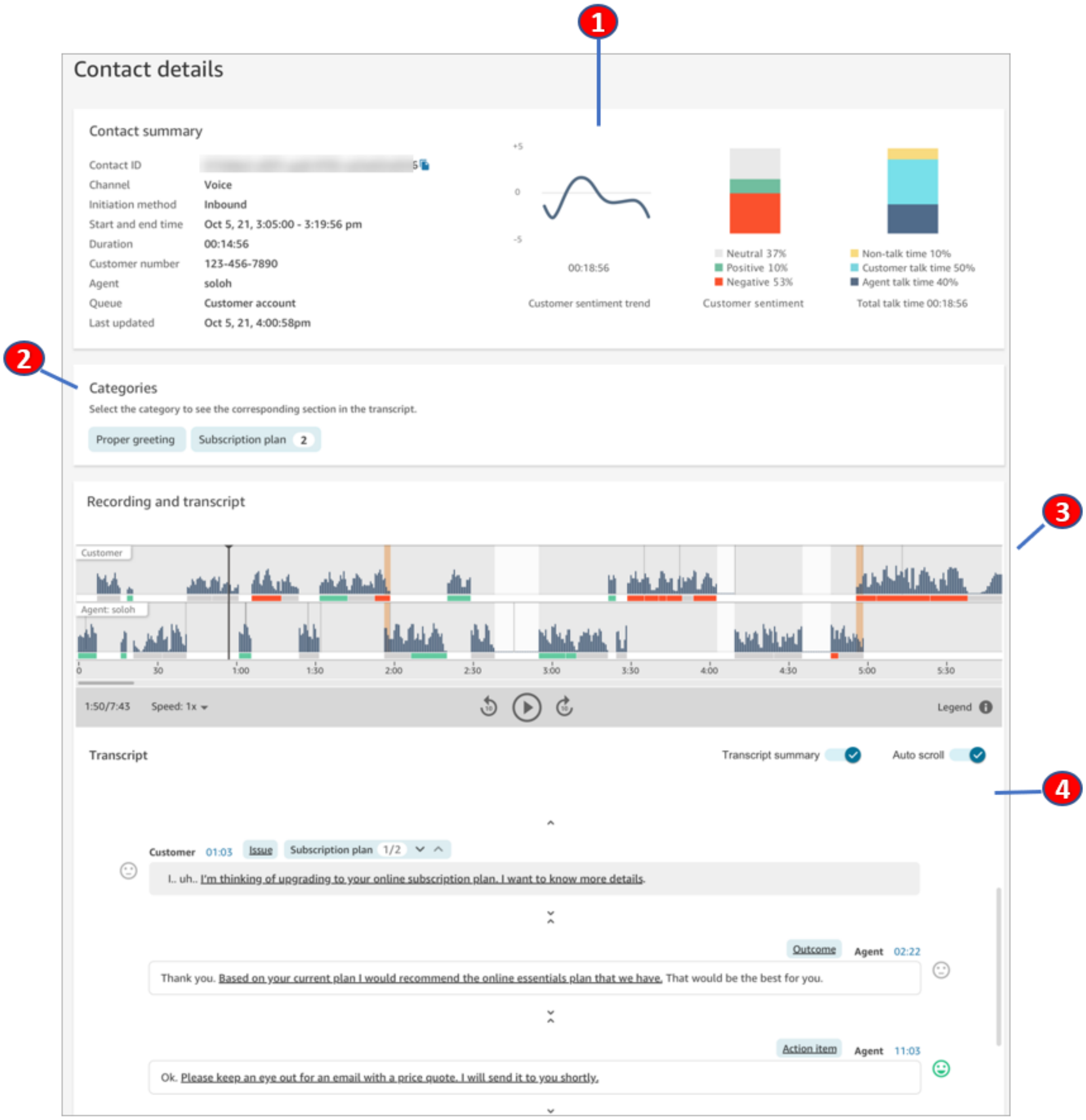
Contact Lens for Amazon Connect enables you to analyze conversations between customer and agents, by using speech transcription, natural language processing, and intelligent search capabilities. It performs sentiment analysis, detects issues, and enables you to automatically categorize contacts.

Contact Lens for Amazon Connect provides both real-time and post-call analytics of customer-agent conversations.

- **Real-time analytics**: Use to detect and resolve customer issues more proactively while the call is progress. For example, it can analyze and alert you when a customer is getting frustrated because the agent is unable to resolve a complicated problem. This allows you to provide assistance proactively.
- **Post-call analytics**: Use to understand trends of customer conversations, and agent compliance. This helps you identify opportunities to coach an agent after the call.

To protect your customer's privacy, sensitive data such as name, address, and credit card information, can be redacted from transcripts and audio recordings.

The results of the sentiment analysis appear in the customer's contact record. The following image shows a sample contact record.



Contact details

Contact summary

Contact ID	[redacted]5
Channel	Voice
Initiation method	Inbound
Start and end time	Oct 5, 21, 3:05:00 - 3:19:56 pm
Duration	00:14:56
Customer number	123-456-7890
Agent	soloh
Queue	Customer account
Last updated	Oct 5, 21, 4:00:58pm

Categories

Select the category to see the corresponding section in the transcript.

Recording and transcript

Transcript

Customer 01:03 Issue Subscription plan 1/2

I.. uh.. I'm thinking of upgrading to your online subscription plan. I want to know more details.

Outcome Agent 02:22

Thank you. Based on your current plan I would recommend the online essentials plan that we have. That would be the best for you.

Action item Agent 11:03

Ok. Please keep an eye out for an email with a price quote. I will send it to you shortly.

1. This section displays a summary of speech analytics.
2. The **Categories** section list the categories that have been set up.
3. The **Recording** section provides controls you can use to listen to an audio recording of the contact.
4. The **Transcript** section enables you to review a summary of the transcript with the issue, action, and outcome highlighted.

Enable Contact Lens for Amazon Connect

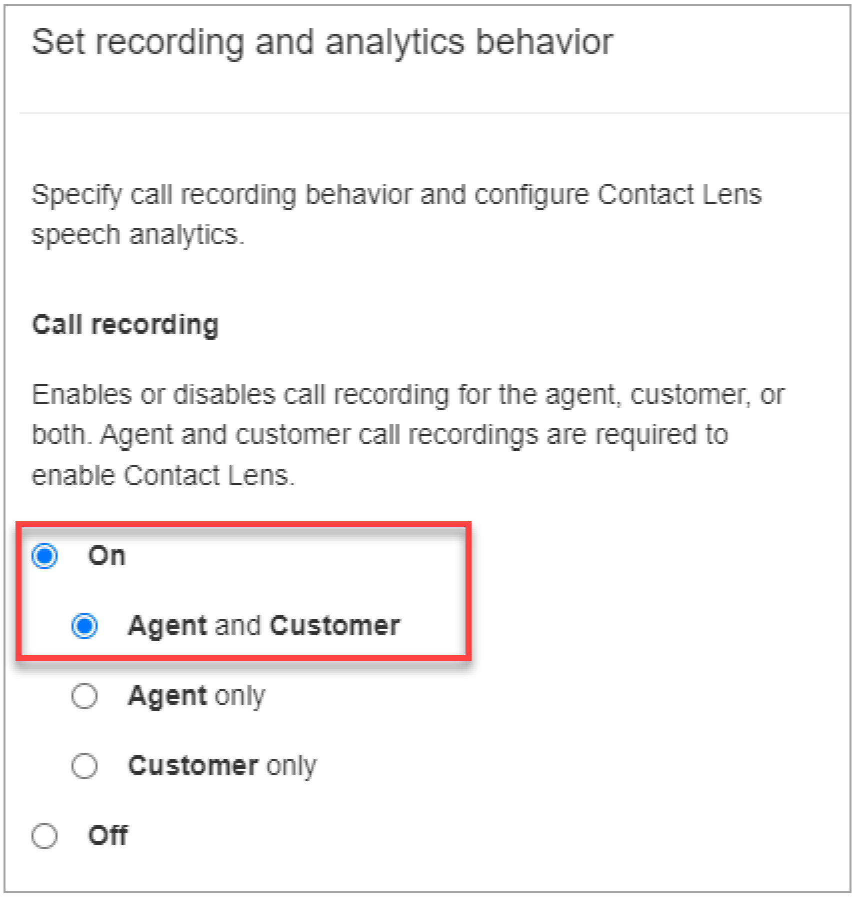
You can enable Contact Lens for Amazon Connect in just a few steps. Just add a Set recording and analytics behavior (p. 408) block to a flow, and configure it for Contact Lens.

To enable Contact Lens in a flow

1. Add the Set recording and analytics behavior (p. 408) block to a flow.

2. In the contact block, under **Call recording**, choose **On**, **Agent and Customer**.

   Both agent and customer call recordings are required to use Contact Lens



Set recording and analytics behavior

Specify call recording behavior and configure Contact Lens speech analytics.

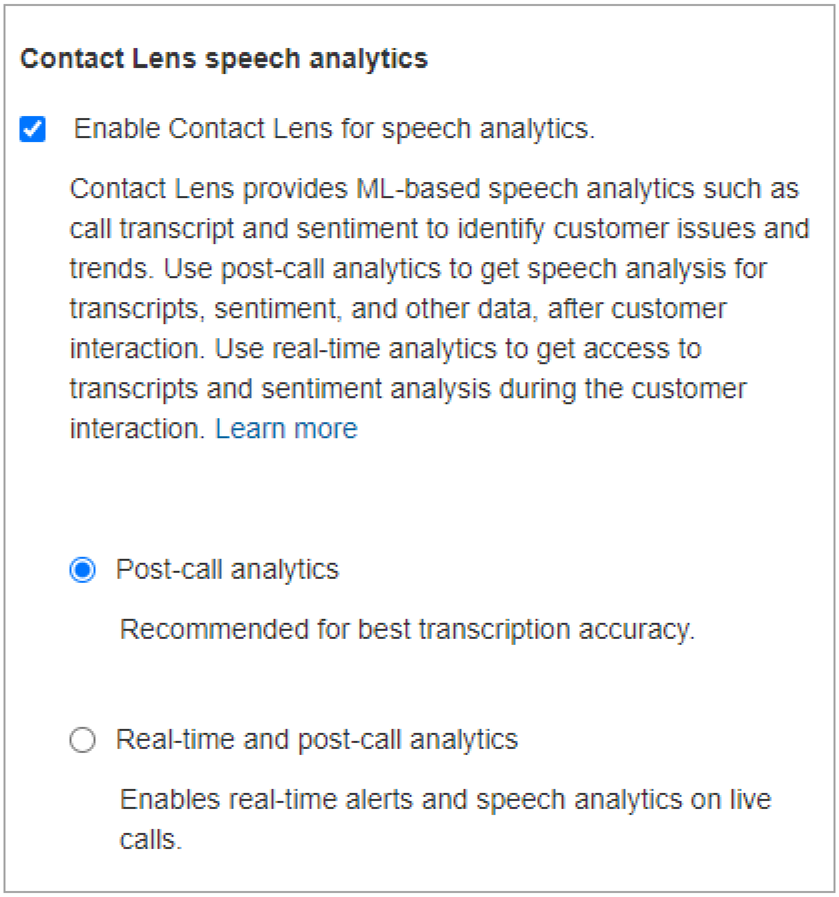
Call recording

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

- ● On
  - ● Agent and Customer
  - ○ Agent only
  - ○ Customer only
- ○ Off

3. Select **Enable Contact Lens for speech analytics**.

   If you don't see this option, Contact Lens for Amazon Connect hasn't been enabled for your instance. To enable it, see Update instance settings (p. 140).



Contact Lens speech analytics

☑ Enable Contact Lens for speech analytics.

Contact Lens provides ML-based speech analytics such as call transcript and sentiment to identify customer issues and trends. Use post-call analytics to get speech analysis for transcripts, sentiment, and other data, after customer interaction. Use real-time analytics to get access to transcripts and sentiment analysis during the customer interaction. Learn more

● Post-call analytics

Recommended for best transcription accuracy.

○ Real-time and post-call analytics

Enables real-time alerts and speech analytics on live calls.

4. Choose one of the following:

   - **Post-call analytics**: Contact Lens analyzes the call recording after the conversation and After Contact Work (ACW) is complete. This option provides the best transcription accuracy.
   - **Real-time analytics**: Contact Lens provides both real-time insights during the call, and post-call analytics after the conversation has ended and After Contact Work (ACW) is complete.

     If you choose this option, we recommend setting up alerts based on keywords and phrases that the customer may utter during the call. Contact Lens analyzes the conversation real-time to detect the specified keywords or phrases, and alerts supervisors. From there, supervisors can listen in on the live call and provide guidance to the agent to help them resolve the issue faster.

     For information about setting up alerts, see Alert supervisors in real-time based on keywords and phrases (p. 584).

     If your instance was created before October 2018, additional configuration is needed to access real-time analytics. For more information, see Service-linked role permissions for Amazon Connect (p. 1120).
5. Choose the language. For a list of available languages for various Contact Lens features, see Supported languages (p. 6).

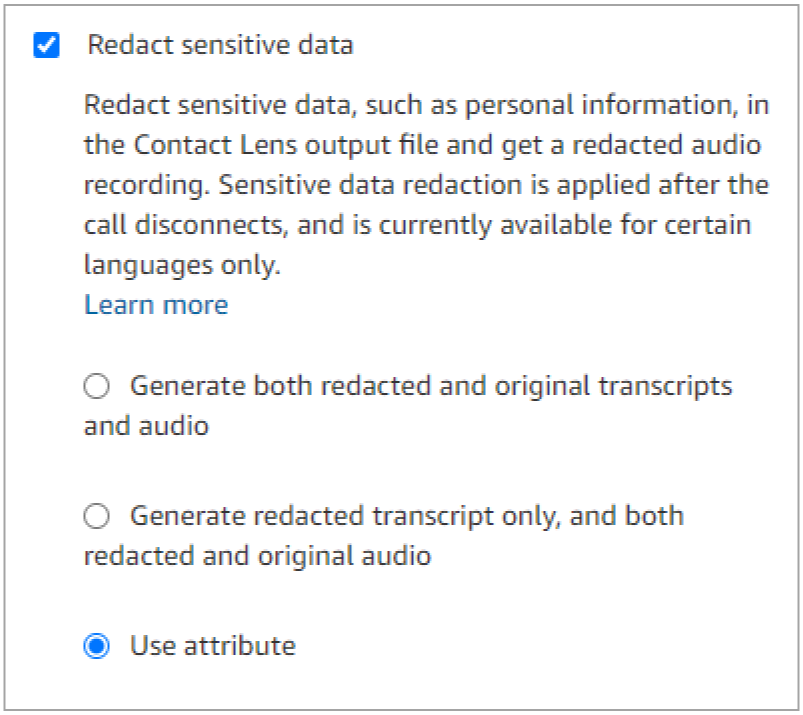
   For instructions on using an attribute, see Use contact attributes (p. 816).
6. Choose **Save**.
7. If the contact is going to be transferred to another agent or queue, repeat these steps to add another Set recording and analytics behavior (p. 408) block with **Enable Contact Lens for speech analytics** enabled.

Tip
If you want to continue using Contact Lens to collect data after transferring a contact to another agent or queue, you need to add another Set recording and analytics behavior (p. 408) block with **Enable analytics** enabled for the flow. This is because a transfer generates a second contact ID and contact record. Contact Lens needs to run on that contact record as well.

How to enable redaction of sensitive data

To enable redaction of sensitive data in a contact flow, choose **Redact sensitive data**. No other configuration is needed. Contact Lens determines what data can be redacted.

For more information about using redaction, see Use sensitive data redaction (p. 837).



☑ Redact sensitive data

Redact sensitive data, such as personal information, in the Contact Lens output file and get a redacted audio recording. Sensitive data redaction is applied after the call disconnects, and is currently available for certain languages only.
Learn more

○ Generate both redacted and original transcripts and audio

○ Generate redacted transcript only, and both redacted and original audio

● Use attribute

Review sensitive data redaction for accuracy

The redaction feature is designed to identify and remove sensitive data. However, due to the predictive nature of machine learning, it may not identify and remove all instances of sensitive data in a transcript generated by Contact Lens. We recommend you review any redacted output to ensure it meets your needs.

Important
The redaction feature does not meet the requirements for de-identification under medical privacy laws like the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), so we recommend you continue to treat it as protected health information after redaction.

For the location of redacted files and examples, see Example Contact Lens output files (p. 846).

Dynamically enable Contact Lens using contact attributes

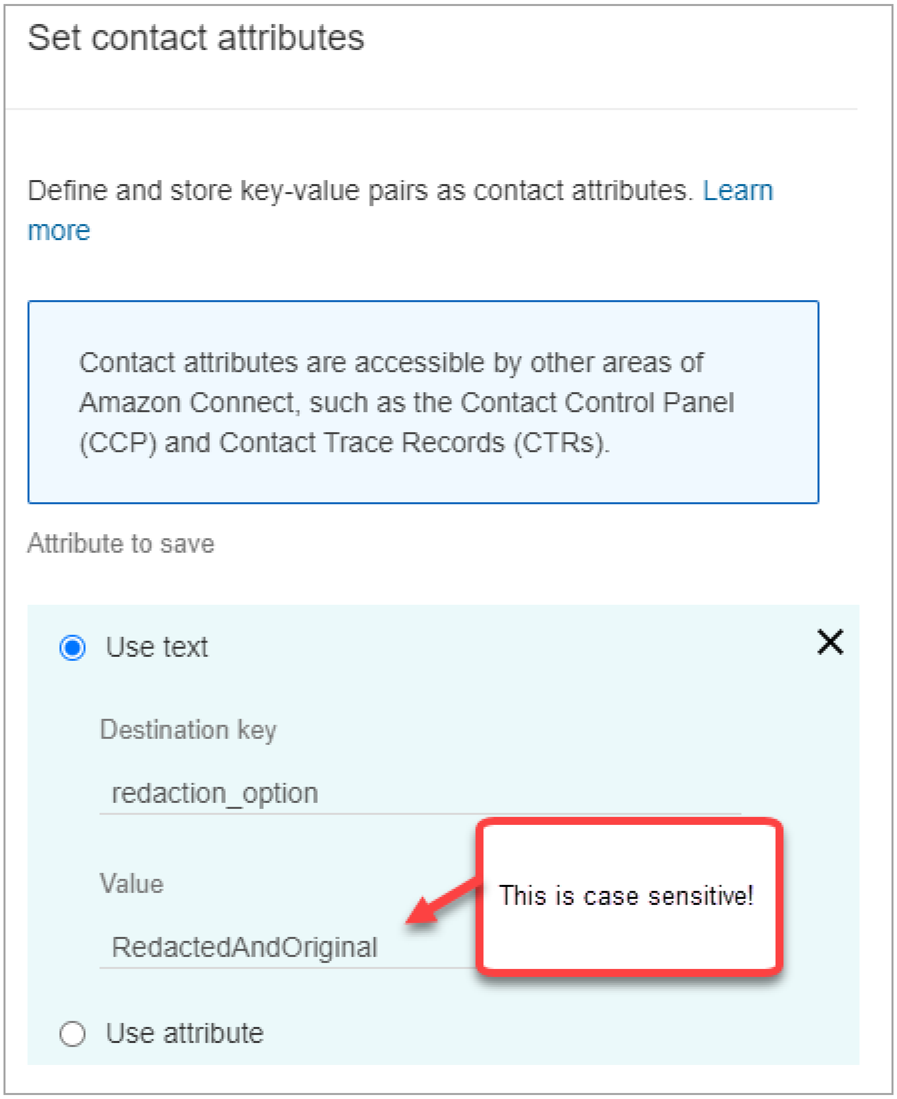
You can dynamically enable Contact Lens and the redaction of the output files based on the language of the customer. For example, for customers using en-US, you may want only a redacted file whereas for those using en-GB, you may want both the original and redacted output files.

- Redaction: choose one of the following (they are case sensitive)
  - None
  - RedactedOnly
  - RedactedAndOriginal
- Language: Choose from the list of available languages (p. 7).

You can set these attributes in the following ways:

- User defined: use a **Set contact attributes** block. For general instructions about using this block, see How to reference contact attributes (p. 531). Define the **Destination key** and **Value** for redaction and language as needed.

  The following image shows how to use contact attributes for redaction. Note that **Value** is case sensitive.



Set contact attributes

Define and store key-value pairs as contact attributes. Learn more

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

Attribute to save

● Use text

Destination key

redaction_option

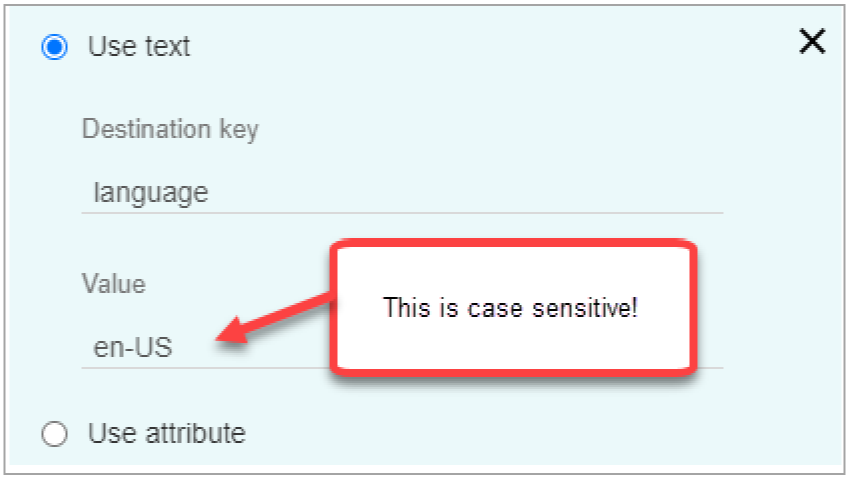
Value

RedactedAndOriginal

This is case sensitive!

○ Use attribute

The following image show how to use contact attributes for language:



● Use text

Destination key

language

Value

en-US

This is case sensitive!

○ Use attribute

- Use a Lambda function (p. 542). This is similar to how you set up user-defined contact attributes. An AWS Lambda function can return the result as a key-value pair, depending on the language of the Lambda response. The following example shows a Lambda response in JSON:

```
{
   'redaction_option': 'RedactedOnly',
   'language': 'en-US'
}
```

Availability of Contact Lens features by Region

Region	Post-call analytics	Real-time analytics	Extended language support
US East (N. Virginia)	Yes	Yes	Yes
US West (Oregon)	Yes	Yes	Yes
Canada (Central)	Yes	Yes	Yes
Europe (Frankfurt)	Yes	Yes	Yes
Europe (London)	Yes	Yes	Yes
Asia Pacific (Singapore)	Yes	-	-
Asia Pacific (Sydney)	Yes	Yes	Yes
Asia Pacific (Tokyo)	Yes	Yes	Yes

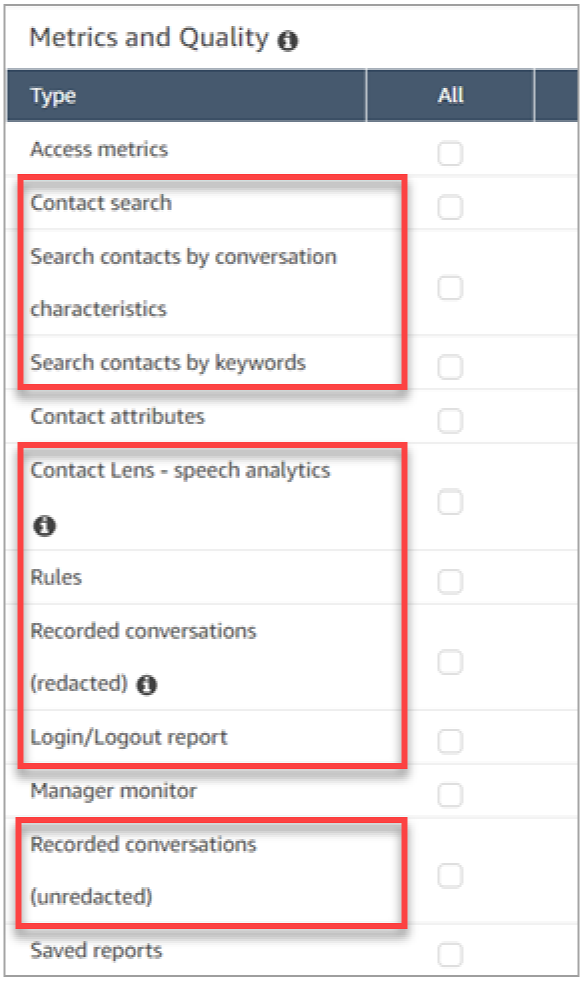
Multi-party calls and Contact Lens

We do not support multi-party calls in Contact Lens. For example, if there are more than two parties (agent and customer) on a call, the quality of the transcription and analytics, such as sentiment and categories, is degraded.

Security profile permissions for Contact Lens

To keep customer data secure, you can set up permissions to have granular control on who can access information generated by Contact Lens.

The security profile permissions shown in the following image apply to Contact Lens.



Metrics and Quality

Type	All
Access metrics	☐
Contact search	☐
Search contacts by conversation characteristics	☐
Search contacts by keywords	☐
Contact attributes	☐
Contact Lens - speech analytics	☐
Rules	☐
Recorded conversations (redacted)	☐
Login/Logout report	☐
Manager monitor	☐
Recorded conversations (unredacted)	☐
Saved reports	☐

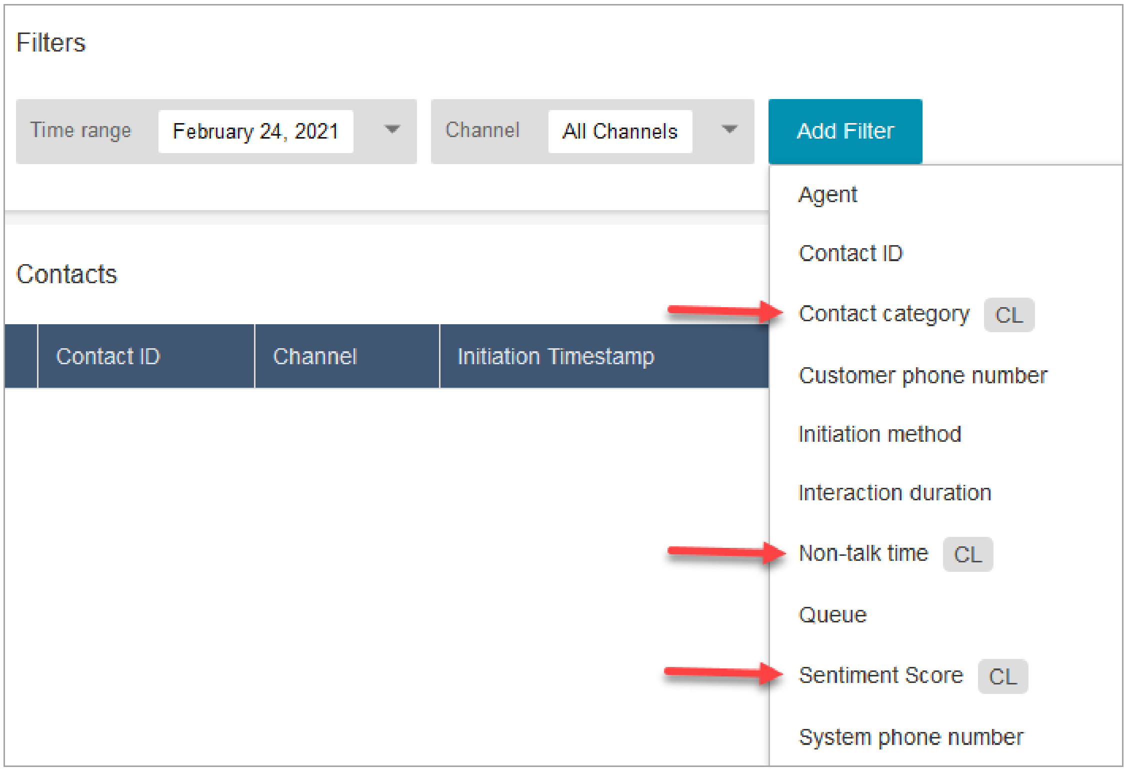
Following is a description of each of these permissions:

Contact search

This permission isn't specific to Contact Lens, but it is required so you can access the **Contact search** page, which is where you can search contacts so you can review the analyzed recording and transcript. In addition, you can do fast, full-text search on call transcripts, and search by sentiment score and non-talk time.

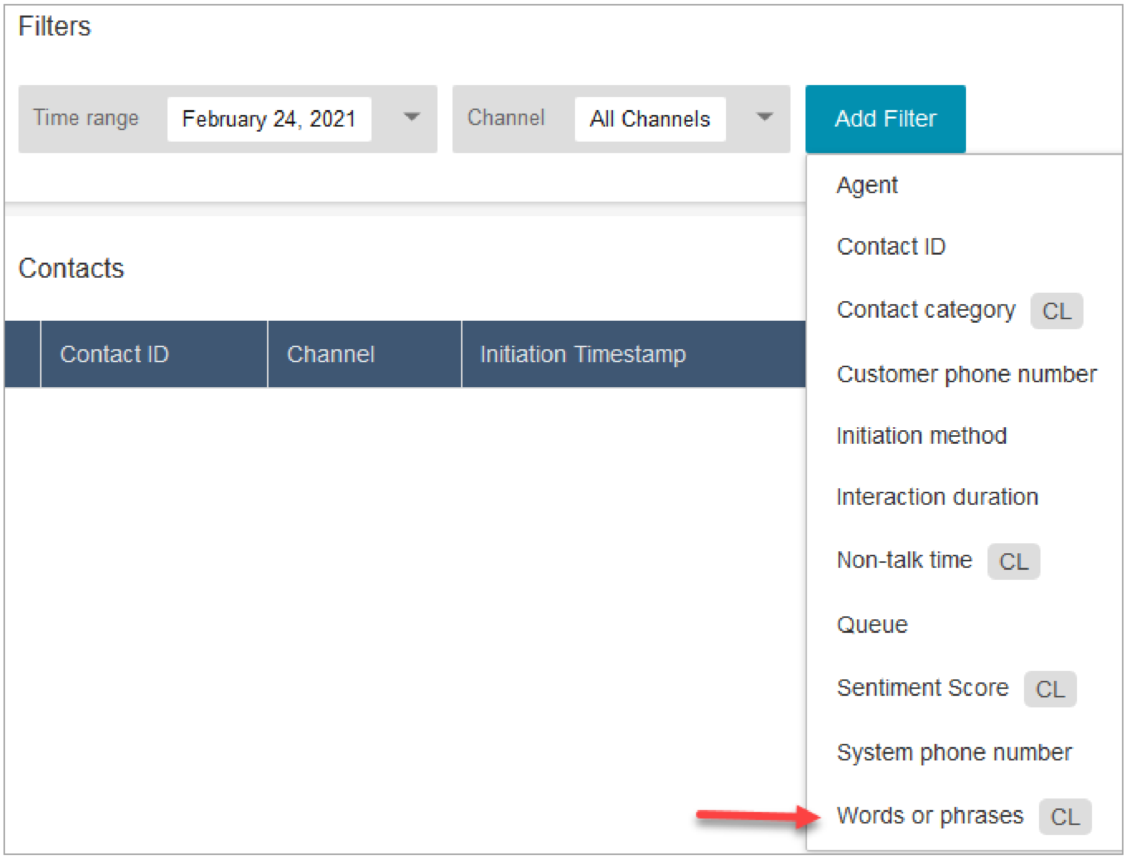
Search contacts by conversation characteristics

On the **Contact Search** page, you can access additional filters that allow you to return results by sentiment score and non-talk time. In addition, you can search conversations that fall into specific contact categories. For more information, see Search for sentiment score (p. 827), Search for non-talk time (p. 829), and Search a contact category (p. 829).



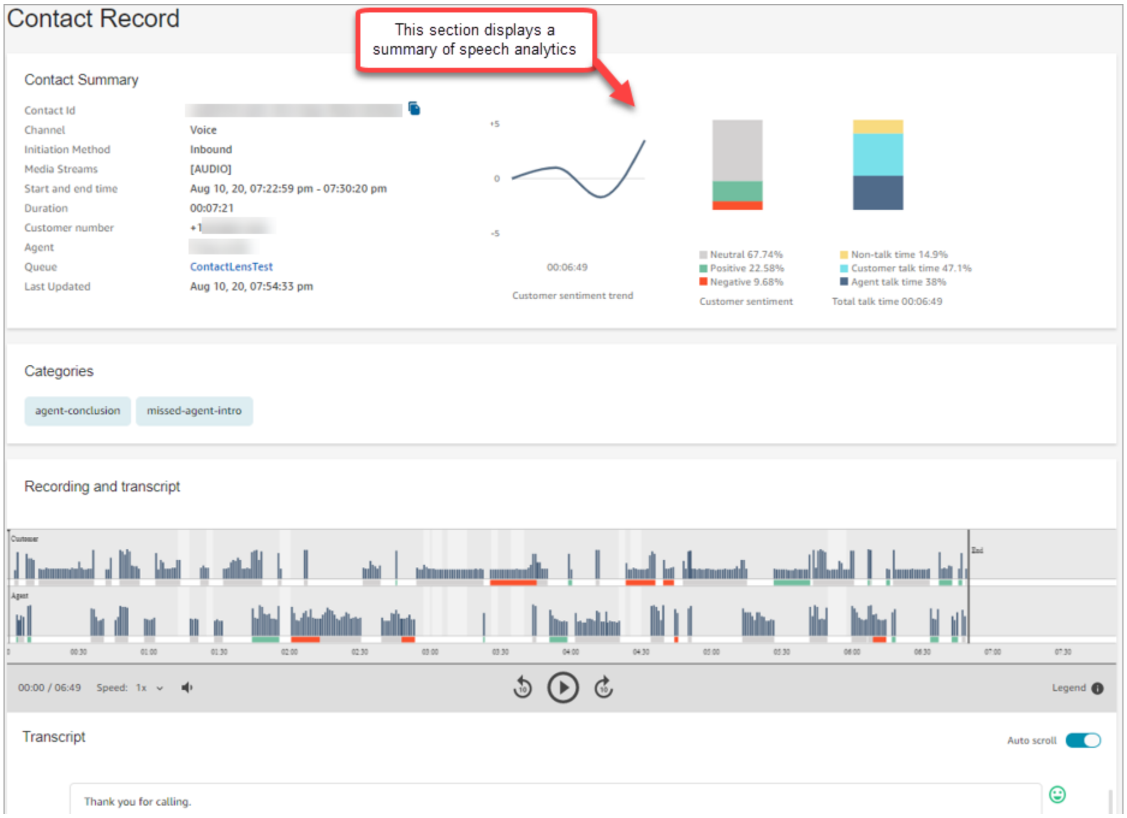
Search contacts by keywords

On the **Contact Search** page, you can access additional filters that allow you to search call transcripts by keywords or phrases, such as "*thank you for your business*." For more information, see Search for keywords (p. 826).



Contact Lens - speech analytics

On the **Contact Record** page for a contact, you can view graphs that summarize speech analytics: customer sentiment trend, sentiment, and talk time. For example, the following image shows how this information is displays on the contact record page for a contact.



Contact Record

This section displays a summary of speech analytics

Contact Summary

Contact Id	[redacted]
Channel	Voice
Initiation Method	Inbound
Media Streams	[AUDIO]
Start and end time	Aug 10, 20, 07:22:59 pm - 07:30:20 pm
Duration	00:07:21
Customer number	+1 [redacted]
Agent	[redacted]
Queue	ContactLensTest
Last Updated	Aug 10, 20, 07:54:33 pm

Categories

Recording and transcript

Transcript

Thank you for calling.

Rules

This permission allows you to view, edit, or create rules for categorizing contacts. For more information, see Automatically categorize contacts based on uttered keywords and phrases (p. 580).

Recorded conversations (redacted)

On the **Contact Record** page for a contact, this permission allows you to listen to call recording files and view call transcripts in which the sensitive data has been removed. For more information, see Example redacted file (p. 852).

Recorded conversations (unredacted)

This permission manages access to unredacted content that contains sensitive data such as name and credit card information. It manages access to the following unredacted content:

- Original, unredacted chat transcripts
- Original, unredacted transcripts analyzed by Contact Lens
- Original, unredacted audio recordings

You can access this content on the **Contact Record** page for a contact. For more information, see Example original, analyzed file (p. 847).

> **Important**
> If you have permissions to both **Recorded conversations (redacted)** and **Recorded conversations (unredacted)**, by default only redacted recordings are made available on the **Contact Record** page.
> You must remove permissions to **Recorded conversations (redacted)** to access unredacted conversations.
> You can't access redacted and unredacted content at the same time.

Contact Lens notification types

Contact Lens provides the following notification types:

- Contact Lens Post Call Rules Matched: An EventBridge event is delivered whenever a Contact Lens rule is matched and has triggered post call.

  This event contains useful information about the Contact Lens rule that is triggered including the category assigned, and details of the agent, contact and queue.
- Contact Lens Real Time Call Rules Matched: An EventBridge event is delivered whenever a Contact Lens rule is matched and has triggered in real time.

  This event contains useful information about the Contact Lens rule that is triggered including the category assigned, and details of the agent, contact and queue
- Contact Lens Analysis State Change: An EventBridge event is delivered when Contact Lens is unable to analyze a contact file. The event contains the Event Reason Code which provides the details on why it was unable to process the file.

You can use these notification types in a variety of scenarios. For example, use Contact Lens analysis State Change events to signal unexpected errors in the processing of a contact file where EventBridge event details can be subsequently stored in a CloudWatch log for additional review, trigger additional workflows, or alert relevant support teams for further investigation.

The Contact Lens post-call and real-time events enable numerous new use cases such as surfacing and visualization of additional insights, for example:

- Generate alerts on real-time customer sentiment drops across all calls
- Aggregating and reporting on reoccurring issues and topics
- Measuring the impact of the latest marketing campaign by detecting how many customers referenced it during a call a
- Customizing agent compliance standards for each Region and lines of business, and enrolling agents into additional training where required.

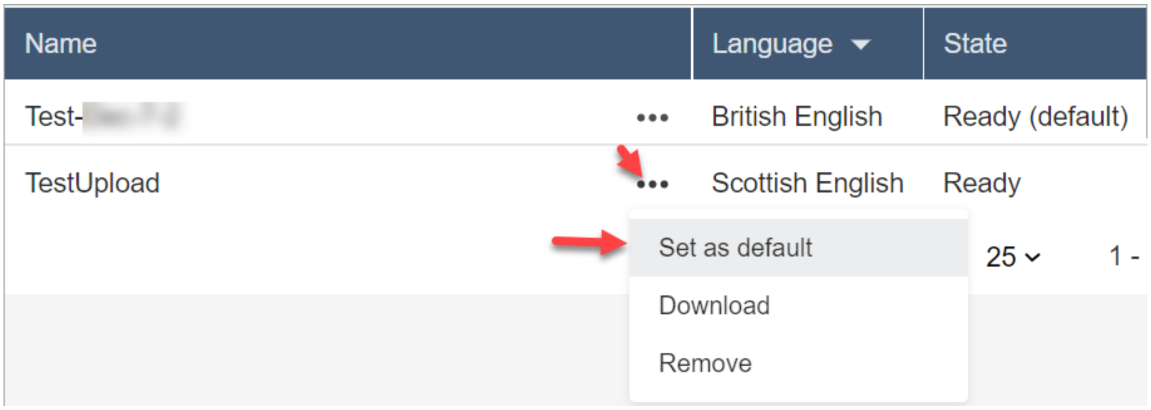
Add custom vocabularies

You can improve the accuracy of speech recognition for product names, brand names, and domain-specific terminology, by expanding and tailoring the vocabulary of the speech-to-text engine in Contact Lens.

This topic explains how to add custom vocabularies using the Amazon Connect console. You can also add them using the CreateVocabulary and AssociateDefaultVocabulary APIs.

Things to know about custom vocabularies

- You must set a vocabulary as the **default** for it to be applied to the analyses to generate transcripts.



Name	Language	State
Test-[redacted]	British English	Ready (default)
TestUpload	Scottish English	Ready

- You can have one vocabulary per language applied to the analyses. This means only one file per language can be in the **Ready (default)** state.
- You can upload more than 20 vocabulary files. However, you can activate only 20 custom vocabulary files at the same time.
- Transcription is a one-time event. A newly uploaded vocabulary isn't applied retroactively to existing transcriptions.
- Your text file must be in LF format. If you use any other format, such CRLF format, your custom vocabulary is not accepted by Amazon Transcribe.
- For limits to the size of a vocabulary file and other requirements, see Custom vocabularies in the *Amazon Transcribe Developer Guide*.

Required permissions

Before you can add custom vocabularies to Amazon Connect, you need the **Analytics**, **Contact Lens - custom vocabularies** permission assigned to your security profile.

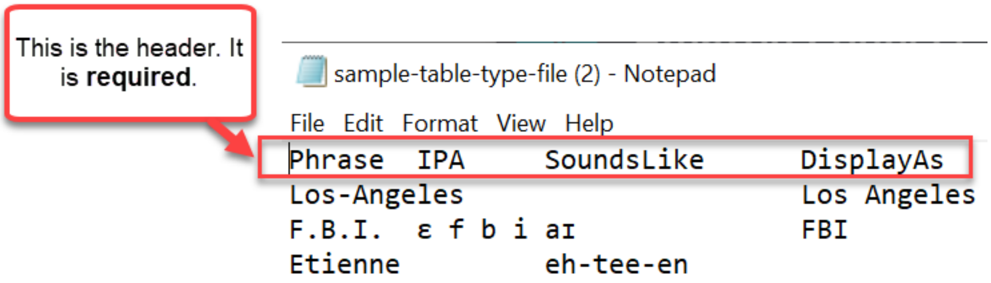
By default, in new instances of Amazon Connect the **Admin** and **CallCenterManager** security profiles have this permission.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

Add a custom vocabulary

1. Log in to Amazon Connect with a user account that has the required permissions to add custom vocabularies.
2. Navigate to **Analytics**, **Custom vocabularies**.
3. Choose **Add custom vocabulary**.
4. On the **Add custom vocabulary** page, enter a name for the vocabulary, choose a language, and then choose **Download a sample** file.

   The following image shows what the sample file looks like:

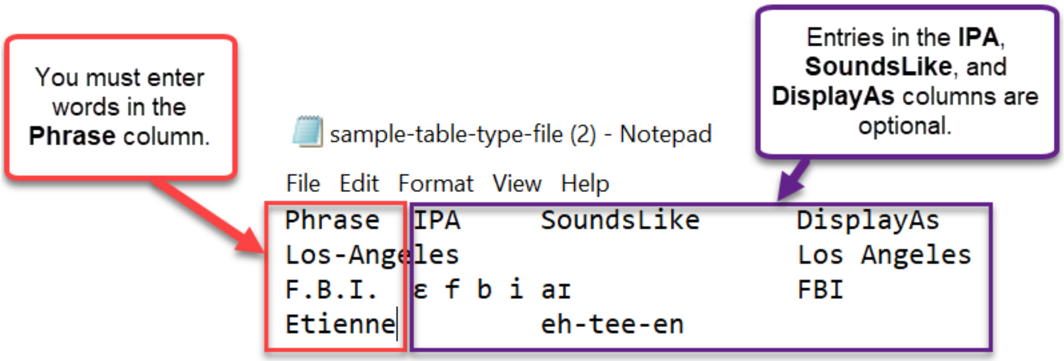


This is the header. It is **required**.

sample-table-type-file (2) - Notepad
File Edit Format View Help

```
Phrase  IPA      SoundsLike      DisplayAs
Los-Angeles                      Los Angeles
F.B.I.  ɛ f b i aɪ               FBI
Etienne          eh-tee-en
```

5. The information in the file is separated by one [TAB] per entry. For details about how to add words and acronyms to your vocabulary file, see Creating a custom vocabulary using a table in the *Amazon Transcribe Developer Guide*.



You must enter words in the **Phrase** column.

Entries in the **IPA**, **SoundsLike**, and **DisplayAs** columns are optional.

sample-table-type-file (2) - Notepad
File Edit Format View Help

```
Phrase  IPA      SoundsLike      DisplayAs
Los-Angeles                      Los Angeles
F.B.I.  ɛ f b i aɪ               FBI
Etienne          eh-tee-en
```

To enter multiple words in the **Phrase** column, separate each word with a hyphen (-); do not use spaces.

Vocabulary states

- **Ready (default)**: The vocabulary is being applied to the analyses to generate transcripts. It is applied to both real-time and post-call analyses.
- **Ready**: The vocabulary is not being applied to analyses, but it is a valid file and available. To apply it to analyses, set it to default.
- **Processing**: Amazon Connect is validating your uploaded vocabulary and trying to apply it to the analyses to generate transcripts.
- **Deleting**: You chose to **Remove** the vocabulary, and Amazon Connect is deleting it now.

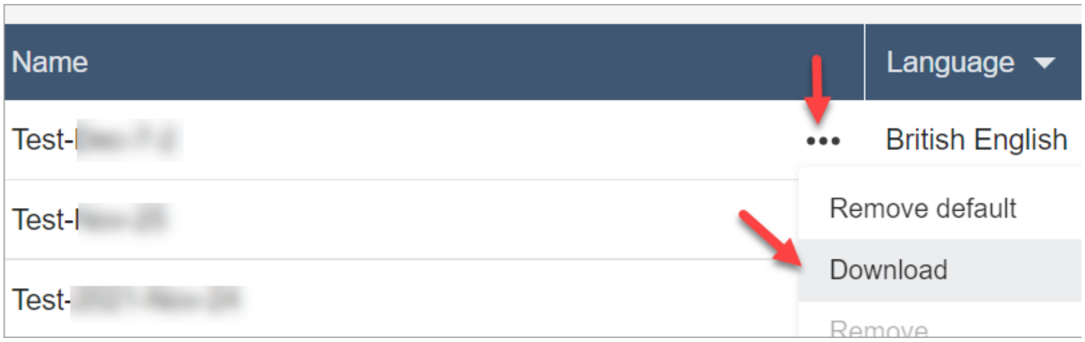
  It takes about 90 minutes for Amazon Connect to delete a vocabulary.

If you attempt to upload a vocabulary that does not validate, it results in a **Failed** state. For example, if you add multiple-word phrases to the **Phrase** column, and separate them with spaces instead of hyphens, it will fail.

Download and view a custom vocabulary

To view a custom vocabulary that has been uploaded, you download and open the file. Only files in the **Ready** state can be downloaded and viewed.

1. Navigate to **Analytics**, **Custom vocabularies**.
2. Choose **More**, **Download**.



3. Open the download to view the contents.
4. You can change the contents, and then choose **Save and upload**.

Search conversations analyzed by Contact Lens

You can search the analyzed and transcribed recordings based on:

- Speaker.
- Keywords.
- Sentiment score.
- Non-talk time.

In addition, you can search conversations that are in specific contact categories (that is, the conversation has been categorized based on uttered keywords and phrases).

These criteria are described in the following sections.

> **Important**
> After a call ends **and** the agent completes After Contact Work (ACW), Contact Lens analyzes and transcribes the recording of the customer-agent conversation. The agent must choose **Clear contact** first.

Required permissions for searching conversations

Before you can search conversations, you need the following permissions, which allow you to do the type of search you want.

- **Contact search**. This is required so you can get to the Contact Search page.
- **Search contacts by conversation characteristics**. This includes non-talk time, sentiment score, and contact category.
- **Search contacts by keywords**

For more information, see Security profile permissions for Contact Lens (p. 818).

Search for keywords

For search, Contact Lens uses the `standard` analyzer in Amazon OpenSearch Service. This analyzer is not case sensitive. For example, if you enter *thank you for your business 2 CANCELLED Flights*, the search looks for:

[thank, you, for, your, business, 2, cancelled, flights]

If you enter *"thank you for your business", two, "CANCELLED Flights"*, the search looks for:

[thank you for your business, two, cancelled flights]

To search conversations for keywords

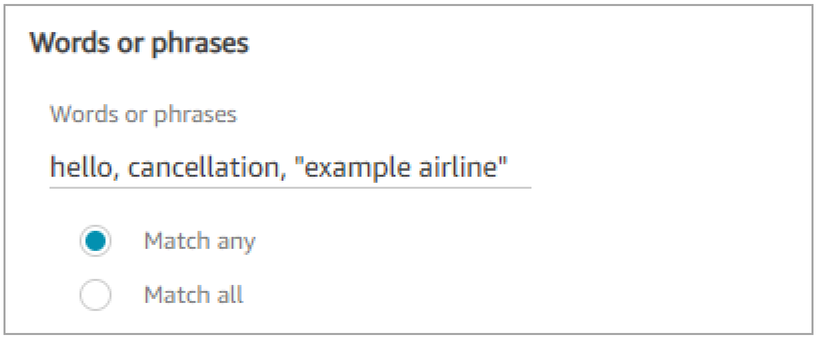
1. In Amazon Connect, log in with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for the **Search contacts by keywords** permission.
2. Choose **Analytics**, **Contact search**.
3. In the **Filter** section, specify the time period that you want to search. Include other information to narrow your search. For instructions, see Search for contacts (p. 907).

   Tip
   When searching by date, you can search up to 8 weeks at a time.
4. In the **Conversation** section, enter the words to search, separated by commas. If you enter a phrase, surround it with quotation marks.

   You can enter up to 128 characters.

   - Choose **Match any** to return contacts that have any of the words present in the transcripts.

     For example, the following query means match (hello OR cancellation OR "example airline").

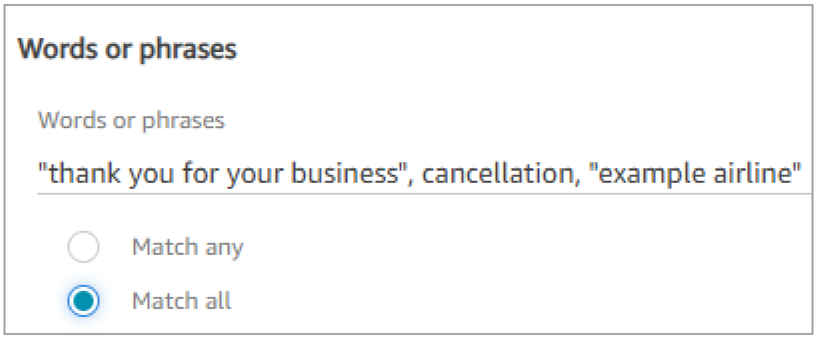
     Words or phrases

     Words or phrases: hello, cancellation, "example airline"

     ● Match any
     ○ Match all

   - Choose **Match all** to return contacts that have all of the words present in the transcripts.

     For example, the following query means match ("thank you for your business" AND cancellation AND "example airline").

     Words or phrases

     Words or phrases: "thank you for your business", cancellation, "example airline"

     ○ Match any
     ● Match all

Search for sentiment score or evaluate sentiment shift

With Contact Lens, you can search conversations for sentiment scores on a scale of -5 (most negative) to +5 (most positive). This enables you to identify patterns and factors for why calls go well or poorly.

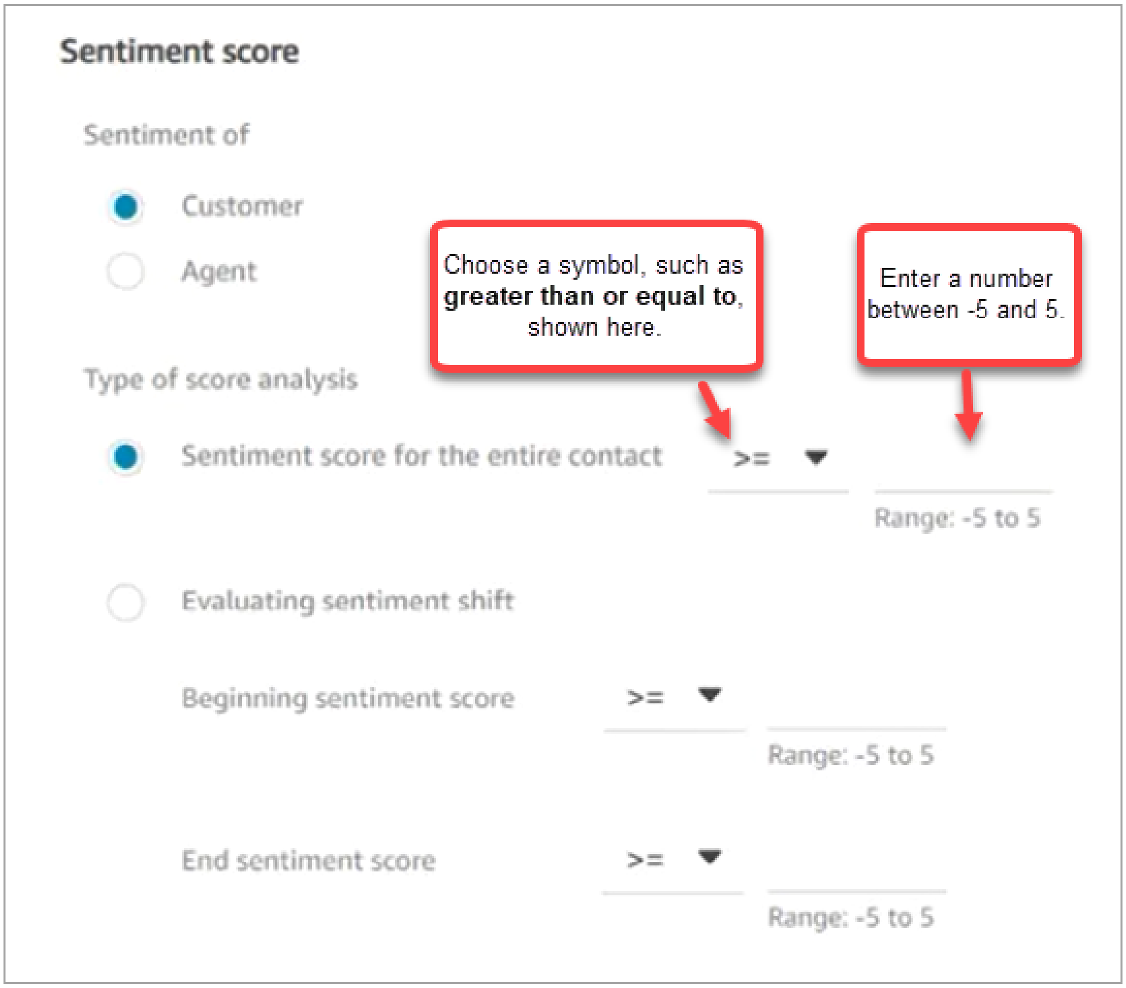
For example, suppose you want to identify and investigate all the calls where the customer sentiment ended negatively. You might search for all calls where the sentiment score is **<=** (less than or equal to) -1.

To search for sentiment scores or evaluate sentiment shift

1. In Amazon Connect, log in with a user account that is assigned the **CallCenterManager** security profile, or that is enabled for the **Search contacts by conversation characteristics** permission.
2. On the **Contact search** page, specify whether you want the sentiment score for words or phrases spoken by the customer or agent.
3. In **Type of score analysis**, specify what type of scores to return:

   - **Sentiment score for the entire contact**: This returns the average score for the customer or agent's portion of the conversation.
   - **Evaluating sentiment shift**: Identify where the customer or agent's sentiment changed during the contact.

     For example, you might search where the customer's sentiment score begins at less than or equal to -1 and ends at greater than or equal to +1.



Sentiment score

Sentiment of

● Customer

○ Agent

Type of score analysis

● Sentiment score for the entire contact >=

Range: -5 to 5

○ Evaluating sentiment shift

Beginning sentiment score >=

Range: -5 to 5

End sentiment score >=

Range: -5 to 5

Choose a symbol, such as **greater than or equal to**, shown here.

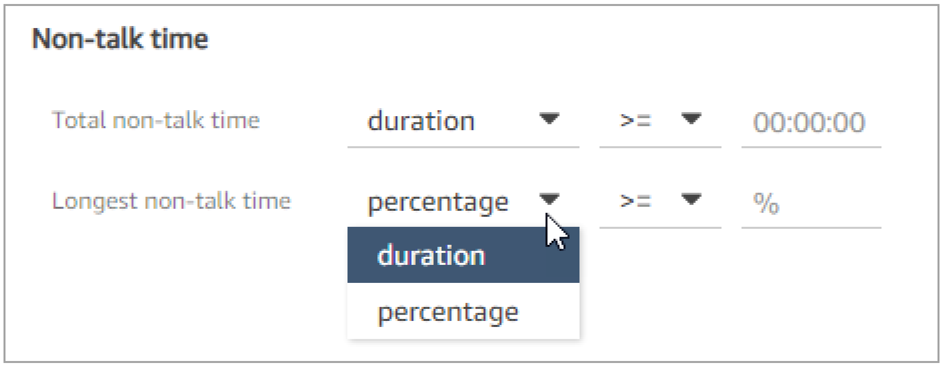
Enter a number between -5 and 5.

Search for non-talk time

To help you identify which calls to investigate, you can search for non-talk time. For example, you might want to find all calls where the non-talk time is greater than 20%, and then investigate them.

Non-talk time includes hold time and any silence where both participants aren't talking for longer than three seconds. This duration can't be customized.

Use the drop-down arrow to specify whether to search conversations for the duration or percentage of non-talk time.

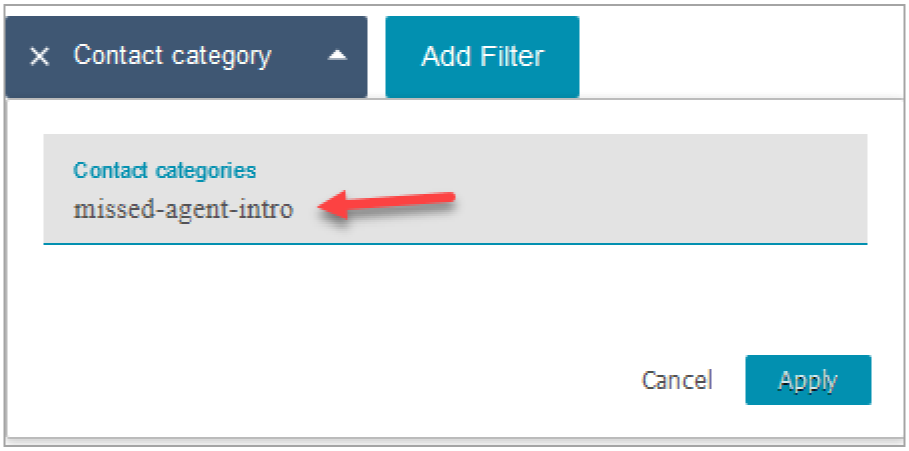

Non-talk time

Total non-talk time: duration ▼ >= ▼ 00:00:00

Longest non-talk time: percentage ▼ >= ▼ %

Search a contact category

1. On the **Contact search** page, choose **Add filter**, **Contact category**.
2. In the **Contact categories** box, type the name of the category that you want to search, and then choose **Apply**.

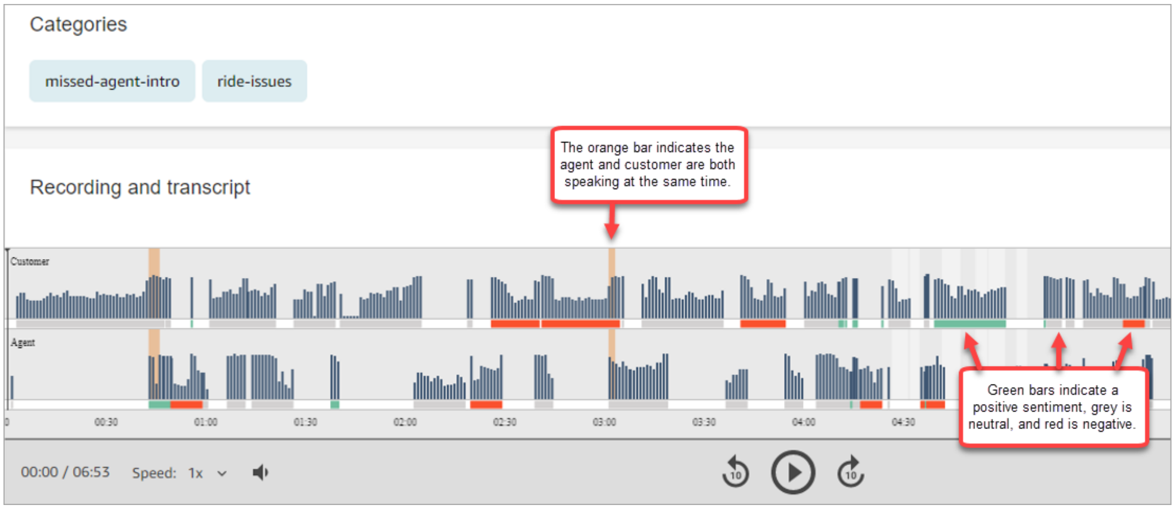


Contact categories: missed-agent-intro

Review analyzed conversations using Contact Lens

By using Contact Lens for Amazon Connect, you can review the transcript and identify what part of the call is of interest. You won't need to listen to an entire call or read an entire transcript to find out what's interesting about it. You can focus on specific parts of the audio or transcript. Both are highlighted for you wherever there are points of interest.

For example, you might scan the transcript of the call and see a red sentiment emoji for a customer turn, which indicates the customer is expressing a negative sentiment. You can choose the timestamp and jump to that portion of audio recording.


Categories
missed-agent-intro
ride-issues
Recording and transcript
The orange bar indicates the agent and customer are both speaking at the same time.
Customer
Agent
00:30
01:00
01:30
02:00
02:30
03:00
03:30
04:00
04:30
Green bars indicate a positive sentiment, grey is neutral, and red is negative.
00:00 / 06:53
Speed: 1x
10
10

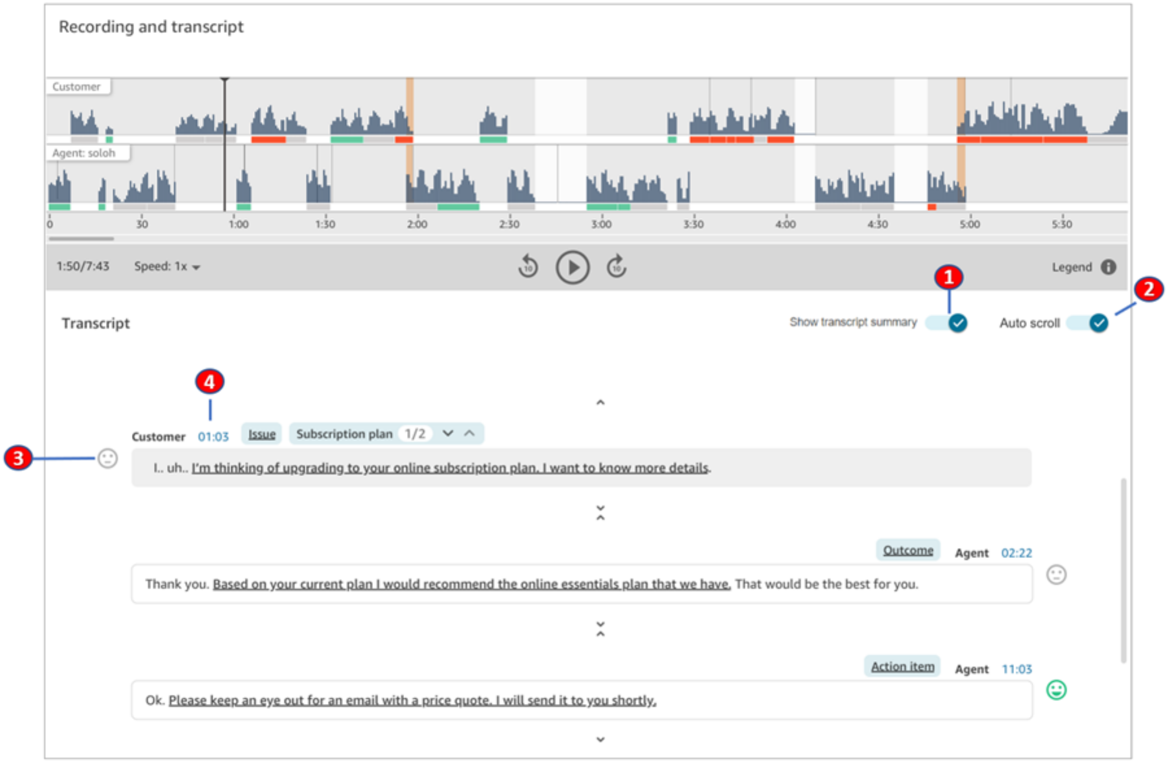
To review analyzed conversations

1. Log in to Amazon Connect with a user account that has **Contact search** and **Contact Lens - speech analytics** permissions in the security profile.
2. In Amazon Connect, choose **Analytics**, **Contact search**.
3. Use the filters on the page to narrow your search for a contact. For date, you can search up to 14 days at a time. For more information about searching for contacts, see Search for contacts (p. 907).
4. Choose the contact ID to view the contact record for the contact.
5. In the **Recording and transcript** section of the contact record, review what was spoken and when, and their sentiment.
6. If desired, choose the play prompt to listen to the recording. Or, download the recording and fast-forward to only the portion you're interested in.

Quickly navigate transcripts and audio

Supervisors are often required to review many agents calls for quality assurance purposes. The turn-by-turn transcript and sentiment data helps you quickly identify and navigate to the portion of the recording that is of interest to you.

The following image shows features that enable you to quickly navigate transcripts and audio to find areas that need your attention.



Customer 01:03 Issue Subscription plan 1/2

I.. uh.. I'm thinking of upgrading to your online subscription plan. I want to know more details.

Outcome Agent 02:22

Thank you. Based on your current plan I would recommend the online essentials plan that we have. That would be the best for you.

Action item Agent 11:03

Ok. Please keep an eye out for an email with a price quote. I will send it to you shortly.

1. Use Show transcript summary (p. 831) to review only the issue, outcome, and/or action item.
2. Use Autoscroll (p. 832) to jump around the audio or transcript. The two always stay in sync.
3. Scan for sentiment emojis (p. 832) to quickly identify a part for the transcript you want to listen to.
4. Choose the timestamp to jump to that part of the audio recording.

Show transcript summary

It can be time-consuming to review contact transcripts that are hundreds of lines long. To make this process faster and more efficient, Contact Lens provides the option for you to view a transcript summary. The summary shows only those lines where Contact Lens has identified an issue, outcome, or action item in the transcript.

- **Issue** represents the call driver. For example, "I'm thinking of upgrading to your online subscription plan."
- **Outcome** represents the likely conclusion or outcome of the contact. For example, "Based on your current plan I would recommend the online essentials plans that we have."
- **Action item** represents the action item the agent takes. For example, "Please keep an eye out for an email with a price quote. I will send it to you shortly."

Each contact has no more than one issue, one outcome, and one action item. Not all contacts will have all three.

> **Note**
>
> If Contact Lens displays the message **There is no summary information for this transcript**, it means no issue, outcome, or action item was identified.

You don't need to configure call summarization. It works out-of-the-box without any training of the machine learning model.

Turn on autoscroll to synchronize the transcript and audio

Autoscroll enables you to jump around the audio or transcript, and the two always stay in sync. For example:

- When you listen to a conversation, the transcript moves along with it, showing you sentiment emojis and any detected issue.
- You can scroll through the transcript, and choose the timestamp for the turn to listen to that specific point in the recording.

Because the audio and transcript are aligned, the transcript can help you understand what the agent and customer are saying. This is especially useful when:

- The audio is bad, maybe due to a connection issue. The transcript can help you understand what's being said.
- There's a dialect or language variant. Our models are trained on different accents so the transcript can help you understand what's being said.

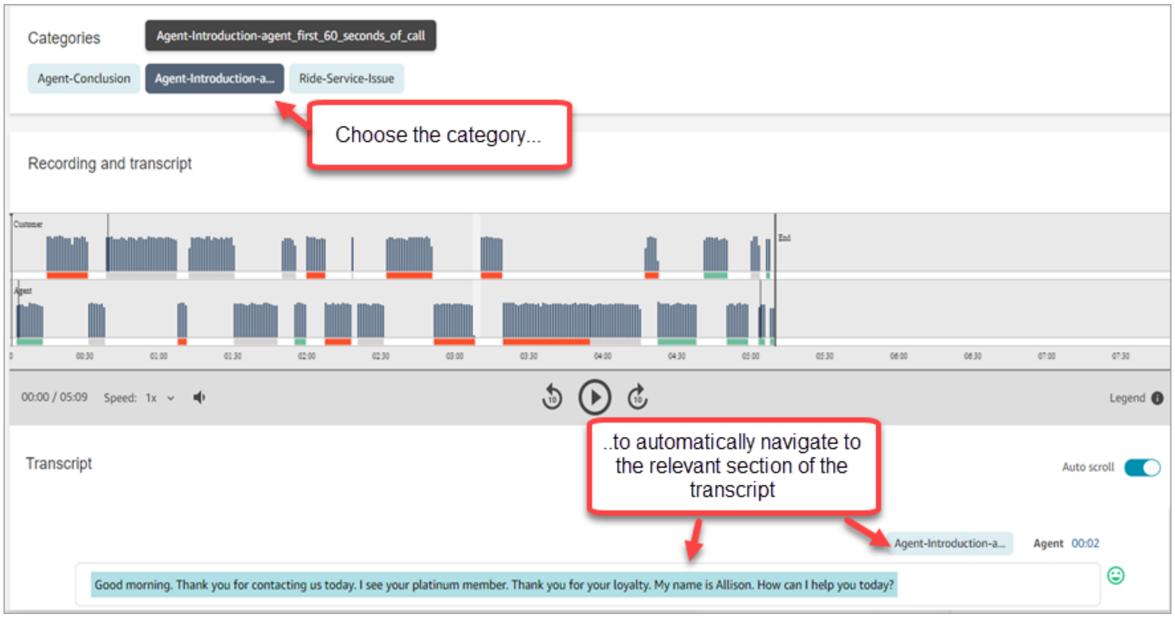
Scan for sentiment emojis

Sentiment emojis help you quickly scan a transcript so you can listen to that part of the conversation.

For example, where you see red emojis for customer turns and then a green emoji, you might choose the timestamp to jump to that specific point of the recording to hear how that agent helped the customer.

Tap or click category tags to navigate through transcript

When you tap or click on the category tags, Contact Lens auto-navigates to the corresponding point-of-interests in the transcript. There are also category markers in the recording playback visualization to indicate which part of the audio file has utterances related to the category.



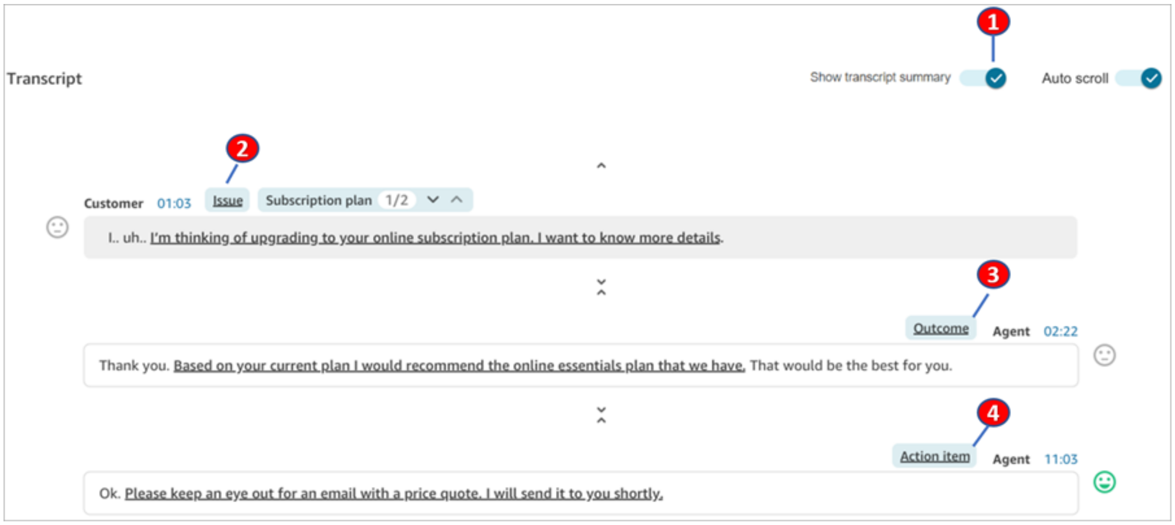
Choose the category...

..to automatically navigate to the relevant section of the transcript

Good morning. Thank you for contacting us today. I see your platinum member. Thank you for your loyalty. My name is Allison. How can I help you today?

View call summary

It can be time-consuming to review contact transcripts that are hundreds of lines long. To make this process faster and more efficient, Contact Lens provides the option for you to view a transcript summary. The summary shows only those lines where Contact Lens has identified an issue, outcome, or action item in the transcript.



I.. uh.. I'm thinking of upgrading to your online subscription plan. I want to know more details.

Thank you. Based on your current plan I would recommend the online essentials plan that we have. That would be the best for you.

Ok. Please keep an eye out for an email with a price quote. I will send it to you shortly.

1. Toggle **Show transcript summary** on and off as needed.
2. **Issue** represents the call driver. For example, "I'm thinking of upgrading to your online subscription plan."
3. **Outcome** represents the likely conclusion or outcome of the contact. For example, "Based on your current plan I would recommend the online essentials plans that we have."
4. **Action item** represents the action item the agent takes. For example, "Please keep an eye out for an email with a price quote. I will send it to you shortly."

Each contact has no more than one issue, one outcome, and one action item. Not all contacts will have all three.

> **Note**
> If Contact Lens displays the message **There is no summary information for this transcript**, it means no issue, outcome, or action item was identified.

You don't need to configure call summarization. It works out-of-the-box without any training of the machine learning model.

Investigate sentiment scores in Contact Lens

What are sentiment scores?

A sentiment score is an analysis of text, and a rating of whether it includes mostly positive, negative, or neutral language. Supervisors can use sentiment scores to search conversations and identify calls that are associated with varying degrees of customer experiences, positive or negative. It helps them identify which of their calls to investigate.

You can view a sentiment score for the entire conversation, as well as scores for each quarter of the call.

How to investigate sentiment scores

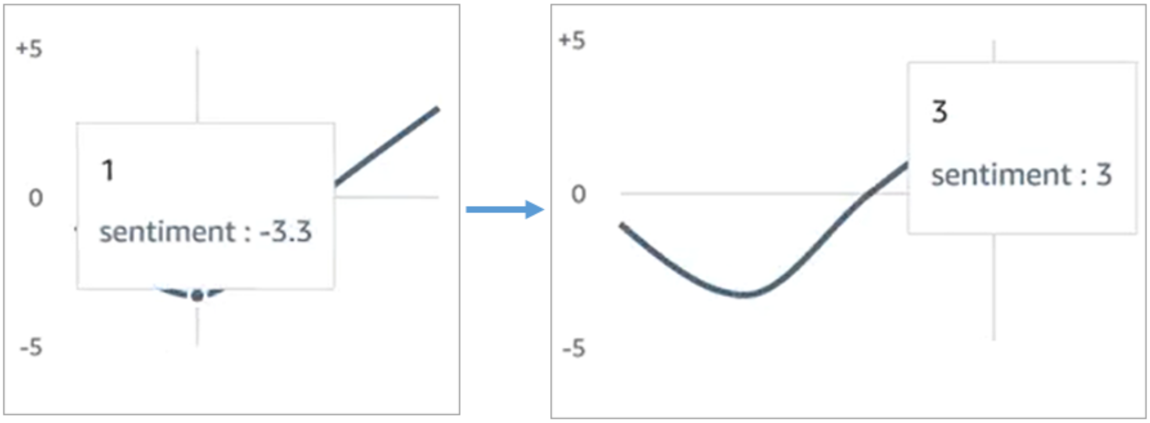
When working to improve your contact center, you may want to focus on the following:

- Calls that start with a positive sentiment score but end negative in the last quarter.

  If you want to focus on a limited set of contacts to sample for quality assurance, for example, you can look at calls where you know the customer had a positive sentiment at the start but ended with a negative sentiment. That shows you they left the conversation unhappy about something.
- Calls that start with a negative sentiment score in the first quarter but end positive.

  Analyzing these calls will help you identify what experiences you can recreate in your contact center. You can share successful techniques with other agents.

An additional way of looking at sentiment progression is to check the sentiment trendline. You can see the variation in the customer's sentiment as the call progresses. For example, the following images show a conversation with a very low sentiment score in the first quarter of the conversation, and a very positive one at the end.



How sentiment scores are determined

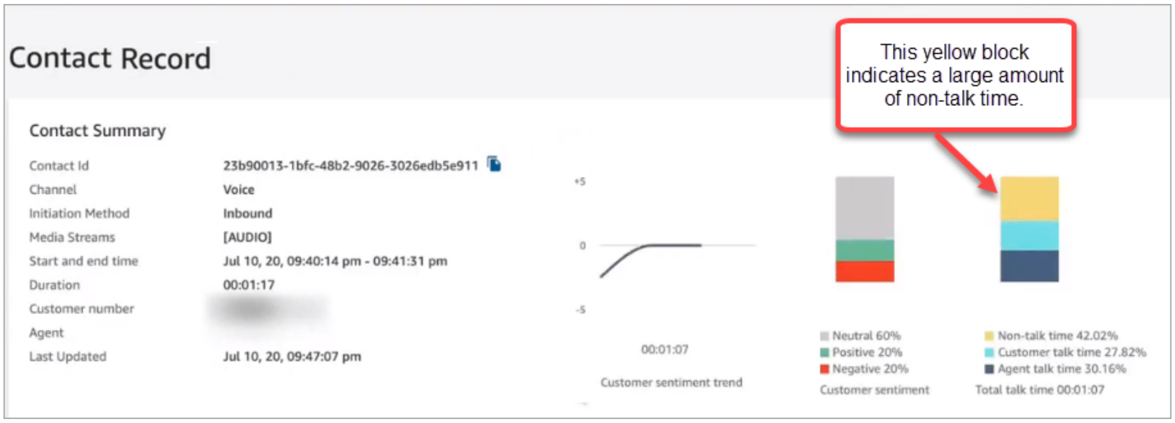
To determine the sentiment score, Contact Lens for Amazon Connect analyzes the sentiment for every speaker turn during the conversation. It uses the frequency and proximity of the resulting sentiment for each speaker turn to assign a score that ranges from -5 to +5 for each portion of the call.

The final sentiment score for the entire conversation is an average of the scores assigned during the call.

Investigate non-talk time in Contact Lens

What is non-talk time?

Contact Lens for Amazon Connect also identifies the amount of *non-talk time* in a call. Non-talk time equals hold time, plus any silence where both participants aren't talking for more than 3 seconds. This duration can't be customized.



Contact Record

Contact Summary

Contact Id	23b90013-1bfc-48b2-9026-3026edb5e911
Channel	Voice
Initiation Method	Inbound
Media Streams	[AUDIO]
Start and end time	Jul 10, 20, 09:40:14 pm - 09:41:31 pm
Duration	00:01:17
Customer number	[redacted]
Agent	
Last Updated	Jul 10, 20, 09:47:07 pm

This yellow block indicates a large amount of non-talk time.

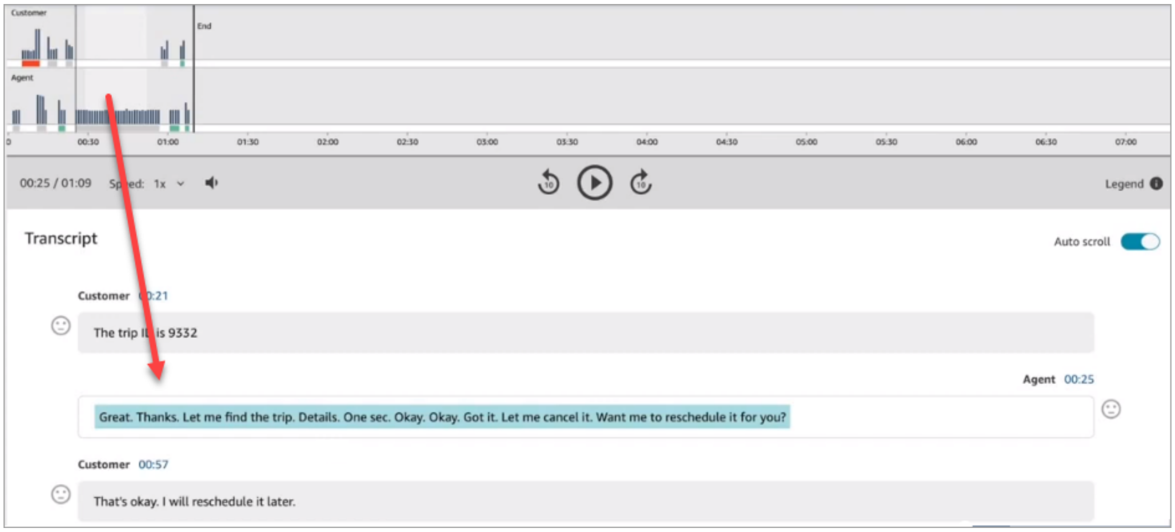
How to investigate non-talk time

Non-talk time can help you identify calls that have gone poorly. This may be because:

- The customer was asking a question that's new for your contact center.
- It's taking the agent a long time to do something but they are well-trained. This indicates there may be an issue with the tools the agent is using. For example, the tools aren't responsive enough or aren't easy to use.
- The agent didn't have a ready answer, but they are fairly new. This indicates they need more training.

You can decide whether to focus on these contacts to improve your contact center. For example, you can go to that section of the audio, and then look at the transcript to see what was going on.

In the following example, the non-talk time occurred when the agent was looking up the caller's trip ID. This could indicate there's an issue with the agent's tools. Or if the agent is new, they need more training.



Customer 00:21

The trip ID is 9332

Agent 00:25

Great. Thanks. Let me find the trip. Details. One sec. Okay. Okay. Got it. Let me cancel it. Want me to reschedule it for you?

Customer 00:57

That's okay. I will reschedule it later.

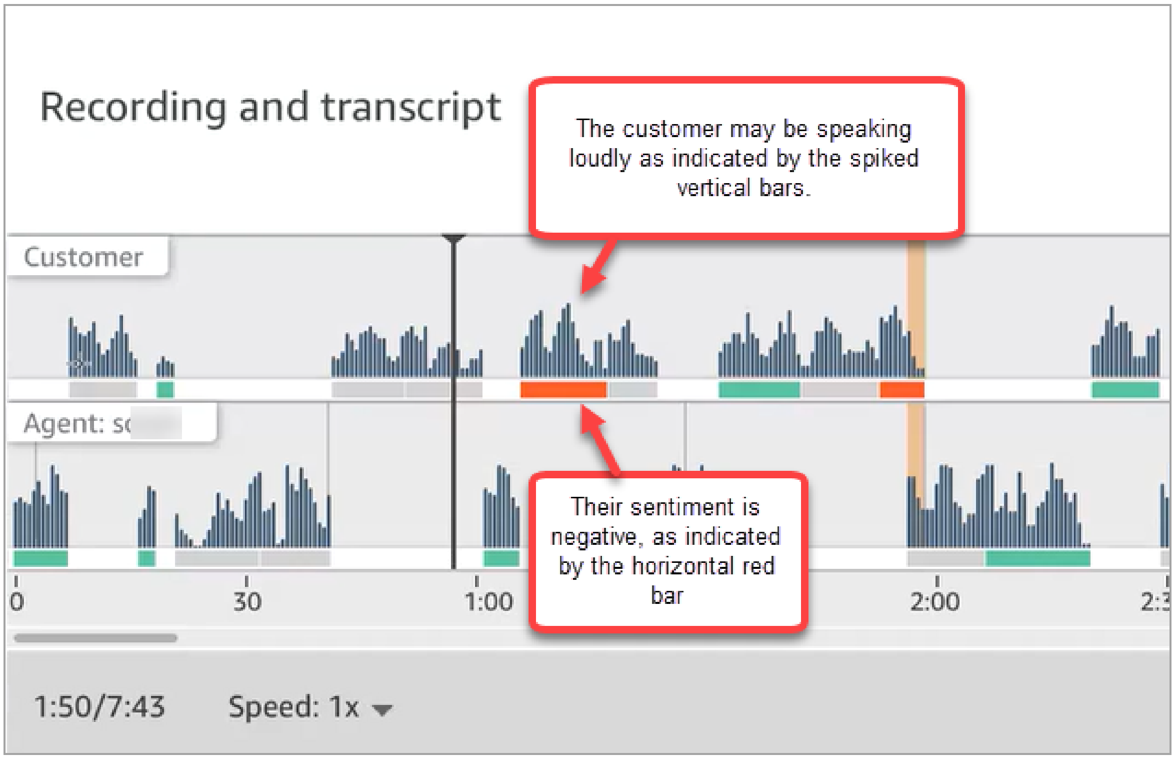
Investigate loudness scores in Contact Lens

A loudness score measures how loudly the customer or agent are speaking. Contact Lens displays an analysis of the conversation that lets you identify where the customer or agent may be talking loudly and have a negative sentiment.

How to use loudness scores

We recommend using loudness scores together with sentiments. Look for areas of the conversation where the loudness score is high and the sentiment is low. Then read that portion of the transcript or listen to that section of the call.

For example, the following image shows where the customer is talking loudly and their sentiment is negative.


Recording and transcript
The customer may be speaking loudly as indicated by the spiked vertical bars.
Customer
Agent: sc
Their sentiment is negative, as indicated by the horizontal red bar
0
30
1:00
2:00
2:3
1:50/7:43
Speed: 1x

Use sensitive data redaction

To help you protect your customer's privacy, Contact Lens lets you automatically redact sensitive data from conversation transcripts and audio files. It redacts sensitive data, such as name, address, and credit card information using Natural Language Understanding.

No configuration is needed. Contact Lens determines what data can be redacted.

To enable redaction, choose the option on the Set recording and analytics behavior (p. 408) block. For more information, see How to enable redaction of sensitive data (p. 815).

Sensitive data redaction is applied after a call disconnects.

> **Important**
> The redaction feature is designed to identify and remove sensitive data. However, due to the predictive nature of machine learning, it may not identify and remove all instances of sensitive data in a transcript generated by Contact Lens. We recommend you review any redacted output to ensure it meets your needs.
> The redaction feature does not meet the requirements for de-identification under medical privacy laws like the U.S. Health Insurance Portability and Accountability Act of 1996 (HIPAA), so we recommend you continue to treat it as protected health information after redaction.

For a list of the languages supported by Contact Lens redaction, see Languages supported by Amazon Connect (p. 6).

About redacted files

Redacted files are stored in your Amazon S3 bucket: Connect-instanceARN / Analysis.

- You cannot access redacted files through the Amazon Connect console (the Amazon Connect user interface).
- You can access redacted files through the AWS console, using the Amazon S3 user interface.

When redaction is enabled, Contact Lens generates the following files:

- A redacted file. This file is generated by default when Redaction is enabled. It's the output schema, with sensitive data redacted. For an example file, see Example redacted file (p. 852).
- An original (raw), analyzed file. This file is generated only when you choose **Get redacted and original transcripts with redacted audio** in the Set recording and analytics behavior (p. 408) block. For an example file, see Example original, analyzed file (p. 847).

  Important
  The original analyzed file is the only place where the complete conversation is stored. If you delete it, there will be no record of the sensitive data that was redacted.
- A redacted audio file (wav). Sensitive data in audio files is redacted as silence. These silent times are not flagged in the Amazon Connect console or elsewhere as non-talk time.

Use your file retention policies to determine how long to keep these files.

Use the API for real-time analytics

Use the real-time analytics API—ListRealtimeContactAnalysisSegments—to build solutions that make your contact center more efficient.

This real-time analytics API is a polling API, with a standard request/response architecture, where you don't need to integrate with any other service. However, there are rate limitations (p. 1217). If needed, you can eliminate these limitations by using the real-time streaming API (p. 838). It requires integration with Amazon Kinesis Data Streams.

Following are two use cases for the real-time analytics API.

Better call transfers

When a contact is transferred from one agent to another agent, you can transfer a transcript of the conversation to the new agent. The new agent then has context for why the customer is calling, and the customer doesn't need to repeat everything they already said. Use the ListRealtimeContactAnalysisSegments API to get the entire transcript of the conversation up to a certain point, and share it with the new agent.

Automatic call summaries

While handling a call agents may need to make notes, such as listing action items. Since you have the entire transcript available, you can build machine learning models to identify the key notes and summarize them at the end of the conversation. These notes are then available for any other agent or supervisor to reference. This helps agents focus on the conversation and the customer rather than focus on taking notes for the call summary.

Use streaming for real-time contact analysis

Real-time contact analysis segment streams enable you to access Contact Lens analytics in near real-time. Real-time streaming overcomes the scaling limitations of existing real-time analytics API (p. 838).

It also provides access to a data segment called `Utterance` that allows you to access partial transcripts. This enables you to meet ultra-low latency requirements to assist agents on live calls.

This section explains how to integrate with Amazon Kinesis Data Streams for real-time streaming.

Through real-time streaming, you can receive the following event types:

- STARTED events published at the beginning of a real-time contact analysis session.
- SEGMENTS events published during the real-time contact analysis sessions. These events contain a list of segments with analyzed information.
- COMPLETED or FAILED events published at the end of a real-time contact analysis session.

Contents

Enable real-time contact analysis segment streams

Real-time contact analysis segment streams are not enabled by default. This topic explains how to enable them.

Step 1: Create a Kinesis stream

Create the data stream on the same account and Region where your Amazon Connect instance resides. For instructions, see Step 1: Create a Data Stream in the *Amazon Kinesis Data Streams Developer Guide*.

> **Tip**
> We recommend creating a separate stream for each type of data. While it's possible to use the same stream for real-time contact analysis segment streams, agent events, and contact records, it is much easier to manage and get data from the stream when you use a separate stream for each one. For more information, see the Amazon Kinesis Data Streams Developer Guide.

Step 2: Set up server-side encryption for the Kinesis stream (optional but recommended)

There are several ways you can do this.

- Option 1: Use the Kinesis AWS managed key (`aws/kinesis`). This works with no additional setup from you.
- Option 2: Use the same customer managed key for call recordings, chat transcripts, or exported reports in your Amazon Connect instance.

  Enable encryption, and use a customer managed key for call recordings, chat transcripts, or exported reports in your Amazon Connect instance. Then choose the same KMS key for your Kinesis data stream. This key already has the permission (grant) required to be used.
- Option 3: Use a different customer managed key.

  Use an existing customer managed key or create a new one and add required permissions for Amazon Connect role to use the key. To add permissions using AWS KMS grants, see the following example:

```
aws kms create-grant \
    --key-id your key ID \
    --grantee-principal arn:aws:iam::your AWS account ID:role/aws-service-role/
connect.amazonaws.com/AWSServiceRoleForAmazonConnect_11111111111111111111 \
    --operations GenerateDataKey \
    --retiring-principal arn:aws:iam::your AWS account ID:role/adminRole
```

Where `grantee-principal` is the ARN of the service-linked role associated to your Amazon Connect instance. To find the ARN of the service-linked role, in the Amazon Connect console, go to **Overview**, **Distribution settings**, **Service-linked role**.

Step 3: Associate the Kinesis stream

Use Amazon Connect AssociateInstanceStorageConfig API to associate the resource type `REAL_TIME_CONTACT_ANALYSIS_SEGMENTS` along with the Kinesis stream where real-time contact analysis segments will be published. You'll need the instance ID and the Kinesis stream ARN.

AWS CLI

```
aws connect associate-instance-storage-config --instance-id
                        your Amazon Connect instance ID --
resource-type REAL_TIME_CONTACT_ANALYSIS_SEGMENTS --storage-config
 'StorageType=KINESIS_STREAM,KinesisStreamConfig={StreamArn=the ARN of your Kinesis
 stream}'
```

AWS SDK

```
import { Connect } from 'aws-sdk';

async function associate (): Promise <void> {
  const clientConfig: Connect.ClientConfiguration = {
    region: 'the Region of your Amazon Connect instance',
  };

  const connect = new Connect(clientConfig);

  // Build request
  const request: Connect.Types.AssociateInstanceStorageConfigRequest = {
    InstanceId: 'your Amazon Connect instance ID',
    ResourceType: 'REAL_TIME_CONTACT_ANALYSIS_SEGMENTS',
    StorageConfig: {
      StorageType: 'KINESIS_STREAM',
      KinesisStreamConfig: {
        StreamArn: 'the ARN of your Kinesis stream',
      },
    }
  };

  try {
    // Execute request
    const response: Connect.Types.AssociateInstanceStorageConfigResponse = await
 connect.associateInstanceStorageConfig(request).promise();

    // Process response
    console.log('raw response: ${JSON.stringify(response, null, 2)}');
  } catch (err) {
    console.error('Error calling associateInstanceStorageConfig. err.code: ${err.code},' +
      'err.message: ${err.message}, err.statusCode: ${err.statusCode}, err.retryable:
 ${err.retryable}');
  }
}

associate().then(r => console.log('Done'));
```

Step 4: Enable Contact Lens for your Amazon Connect instance

For instructions, see Enable Contact Lens for Amazon Connect (p. 812).

Step 5 (Optional): Review a sample segment stream

We recommend you review a sample segment stream to familiarize yourself with what it looks like. See Sample real-time contact analysis segment stream (p. 844).

Real-time contact analysis segment streams data model

Real-time contact analysis segment streams are generated in JSON. Event JSON blobs are published to the associated stream for every contact that has real-time contact analysis enabled. The following types of events can be published for a real-time contact analysis session:

- STARTED events—Each real-time contact analysis session publishes one STARTED event at the beginning of the session.
- SEGMENTS events—Each real-time contact analysis session may publish zero or more SEGMENTS events during the session. These events contain a list of segments with analyzed information. The list of segments may include "`Utterance`," "`Transcript`," or "`Categories`" segments.
- COMPLETED or FAILED events—Each real-time contact analysis session publishes one COMPLETED or FAILED event at the end of the session.

Common properties included in all events

Every event includes the following properties:

Version

The version of the event schema.

Type: String

Channel

The type of channel for this contact.

Type: String

Valid values: `VOICE`, `CHAT`, `TASK`

For more information about channels, see Channels and concurrency (p. 26).

AccountId

The identifier of the account where this contact takes place.

Type: String

ContactId

The identifier of the contact being analyzed.

Type: String

InstanceId

The identifier of the instance where this contact takes place.

Type: String

LanguageCode

The language code associated to this contact.

Type: String

Valid values: the language code for one of the supported languages for Contact Lens real-time analytics (p. 7).

EventType

The type of event published.

Type: String

Valid values: `STARTED`, `SEGMENTS`, `COMPLETED`, `FAILED`

STARTED event

`STARTED` events include only the common properties:

- Version
- Channel
- AccountId
- ContactId
- LanguageCode
- EventType: STARTED

SEGMENTS event

`SEGMENTS` events include the following properties:

- Version
- Channel
- AccountId
- ContactId
- LanguageCode
- EventType: SEGMENTS
- Segments: In addition to the common properties, `SEGMENTS` events include a list of segments with analyzed information.

  Type: Array of Segment (p. 842) objects

Segment

An analyzed segment for a real-time analysis session.

Each segment is an object with the following optional properties. Only one of these properties is present, depending on the segment type:

- Utterance
- Transcript
- Categories

Utterance

The analyzed utterance.

Required: No

- **Id**

  The identifier of the utterance.

  Type: String
- **TranscriptId**

  The identifier of the transcript associated to this utterance.

  Type: String
- **ParticipantId**

  The identifier of the participant.

  Type: String
- **ParticipantRole**

  The role of participant. For example, is it a customer, agent, or system.

  Type: String
- **PartialContent**

  The content of the utterance.

  Type: String
- **BeginOffsetMillis**

  The beginning offset in the contact for this transcript.

  Type: Integer
- **EndOffsetMillis**

  The end offset in the contact for this transcript.

  Type: Integer

Transcript

The analyzed transcript.

Type: Transcript object

Required: No

Categories

The matched category rules.

Type: Categories object

Required: No

COMPLETED event

`COMPLETED` events include only the following common properties:

- Version
- Channel
- AccountId

- ContactId
- LanguageCode
- EventType: STARTED

FAILED event

`FAILED` events include only the following common properties:

- Version
- Channel
- AccountId
- ContactId
- LanguageCode
- EventType: FAILED

Sample real-time contact analysis segment stream

This topic provides sample segment streams for STARTED, SEGMENTS, COMPLETED, and FAILED events.

Sample STARTED event

- EventType: STARTED
- Published at the beginning of the real-time contact analysis session.

```
{
    "Version": "1.0.0",
    "Channel": "VOICE",
    "AccountId": "your AWS account ID",
    "InstanceId": "your Amazon Connect instance ID",
    "ContactId": "the ID of the contact",
    "LanguageCode": "the language code of the contact",
    "EventType": "STARTED"
}
```

Sample SEGMENTS event

- EventType: SEGMENTS
- Published during a real-time contact analysis session. This event contains a list of segments with analyzed information. The list of segments may include "`Utterance`," "`Transcript`," or "`Categories`" segments.

```
{
    "Version": "1.0.0",
    "Channel": "VOICE",
    "AccountId": "your AWS account ID",
    "InstanceId": "your Amazon Connect instance ID",
    "ContactId": "the ID of the contact",
    "LanguageCode": "the language code of the contact",
    "EventType": "SEGMENTS",
    "Segments": [
        {
            "Utterance": {
                "Id": "the ID of the utterance",
                "TranscriptId": "the ID of the transcript",
                "ParticipantId": "AGENT",
                "ParticipantRole": "AGENT",
                "PartialContent": "Hello, thank you for calling Example Corp. My name is
 Adam.",
                "BeginOffsetMillis": 19010,
                "EndOffsetMillis": 22980
            }
        },
        {
            "Utterance": {
                "Id": "the ID of the utterance",
                "TranscriptId": "the ID of the transcript",
                "ParticipantId": "AGENT",
                "ParticipantRole": "AGENT",
                "PartialContent": "How can I help you?",
                "BeginOffsetMillis": 23000,
                "EndOffsetMillis": 24598
            }
        },
        {
            "Transcript": {
                "Id": "the ID of the transcript",
                "ParticipantId": "AGENT",
                "ParticipantRole": "AGENT",
                "Content": "Hello, thank you for calling Example Corp. My name is Adam. How
 can I help you?",
                "BeginOffsetMillis": 19010,
                "EndOffsetMillis": 24598,
                "Sentiment": "NEUTRAL"
            }
        },
        {
            "Transcript": {
                "Id": "the ID of the transcript",
                "ParticipantId": "CUSTOMER",
                "ParticipantRole": "CUSTOMER",
                "Content": "I'm having trouble submitting the application, number AX876293
 on the portal. I tried but couldn't connect to my POC on the portal. So, I'm calling on
 this toll free number",
                "BeginOffsetMillis": 19010,
                "EndOffsetMillis": 22690,
                "Sentiment": "NEGATIVE",
                "IssuesDetected": [
                    {
                        "CharacterOffsets": {
                            "BeginOffsetChar": 0,
                            "EndOffsetChar": 81
                        }
                    }
                ]
            }
        },
        {
            "Categories": {
                "MatchedCategories": [
                    "CreditCardRelated",
                    "CardBrokenIssue"
                ],
                "MatchedDetails": {
                    "CreditCardRelated": {
                        "PointsOfInterest": [
                            {
                                "BeginOffsetMillis": 19010,
                                "EndOffsetMillis": 22690
                            }
                        ]
                    },
                    "CardBrokenIssue": {
                        "PointsOfInterest": [
                            {
                                "BeginOffsetMillis": 25000,
                                "EndOffsetMillis": 29690
                            }
                        ]
                    }
                }
            }
        }
    ]
}
```

Sample COMPLETED event

- EventType: COMPLETED
- Published at the end of the real-time contact analysis session if the analysis completed successfully.

```
{
    "Version": "1.0.0",
    "Channel": "VOICE",
   "AccountId": "your AWS account ID",
    "InstanceId": "your Amazon Connect instance ID",
    "ContactId": "the ID of the contact",
    "LanguageCode": "the language code of the contact",
    "EventType": "COMPLETED"
}
```

Sample FAILED event

- EventType: FAILED
- Published at the end of the real-time contact analysis session if the analysis failed.

```
{
    "Version": "1.0.0",
    "Channel": "VOICE",
    "AccountId": "your AWS account ID",
    "InstanceId": "your Amazon Connect instance ID",
    "ContactId": "the ID of the contact",
    "LanguageCode": "the language code of the contact",
    "EventType": "FAILED"
}
```

Example Contact Lens output files

Example output locations

Following are examples of what Contact Lens output files look like when they are stored in the Amazon S3 bucket for your instance.

- Original analyzed transcript file (JSON)
  - /connect-instance- bucket/**Analysis/Voice**/2020/02/04/*contact's_ID*_**analysis**_2020-02-04T21:14:16Z.json
- Redacted analyzed transcript file in (JSON)
  - /connect-instance- bucket/**Analysis/Voice/Redacted**/2020/02/04/*contact's_ID*_**analysis_redacted**_2020-02-04T21:14:16Z.json
- Redacted audio file
  - /connect-instance- bucket/**Analysis/Voice/Redacted**/2020/02/04/*contact's_ID*_**call_recording_redacted**_2020-02-04T21:14:16Z.**wav**

Important
To delete a recording, you must delete the files for both the redacted and unredacted recordings.

Example original, analyzed file

This section shows an example schema for a conversation that Contact Lens has analyzed. The example shows loudness, issue detection/call drivers, and what information is going to be redacted.

Note the following about the analyzed file:

- It doesn't indicate what sensitive data was redacted. All data are referred to as PII (personally identifiable information).
- Each turn includes a `Redacted` section only if it includes PII.
- If a `Redacted` section exists, it includes the offset in milliseconds. In a .wav file, the redacted portion will be silence. If desired, you can use the offset to replace the silence with something else, such as a beep.
- If two or more PII redactions exist in a turn, the first offset applies to the first PII, the second offset applies to the second PII, and so on.

```
{
    "Version": "1.1.0",
    "AccountId": "your AWS account ID",
    "Channel": "VOICE",
    "ContentMetadata": {
        "Output": "Raw"
    },
    "JobStatus": "COMPLETED",
    "LanguageCode": "en-US",
    "Participants": [
        {
            "ParticipantId": "CUSTOMER",
            "ParticipantRole": "CUSTOMER"
        },
        {
            "ParticipantId": "AGENT",
            "ParticipantRole": "AGENT"
        }
    ],
    "Categories": {
        "MatchedCategories": [],
        "MatchedDetails": {}
    },
    "ConversationCharacteristics": {
        "TotalConversationDurationMillis": 32110,
        "Sentiment": {
            "OverallSentiment": {
                "AGENT": 0,
                "CUSTOMER": 3.1
            },
            "SentimentByPeriod": {
                "QUARTER": {
                    "AGENT": [
                        {
                            "BeginOffsetMillis": 0,
                            "EndOffsetMillis": 7427,
                            "Score": 0
                        },
                        {
                            "BeginOffsetMillis": 7427,
                            "EndOffsetMillis": 14855,
                            "Score": -5
                        },
                        {
                            "BeginOffsetMillis": 14855,
                            "EndOffsetMillis": 22282,
                            "Score": 0
                        },
                        {
                            "BeginOffsetMillis": 22282,
                            "EndOffsetMillis": 29710,
                            "Score": 5
                        }
                    ],
                    "CUSTOMER": [
                        {
                            "BeginOffsetMillis": 0,
                            "EndOffsetMillis": 8027,
                            "Score": -2.5
                        },
                        {
                            "BeginOffsetMillis": 8027,
                            "EndOffsetMillis": 16055,
                            "Score": 5
                        },
                        {
                            "BeginOffsetMillis": 16055,
                            "EndOffsetMillis": 24082,
                            "Score": 5
                        },
                        {
                            "BeginOffsetMillis": 24082,
                            "EndOffsetMillis": 32110,
                            "Score": 5
                        }
                    ]
                }
            }
        },
        "Interruptions": {
            "InterruptionsByInterrupter": {},
            "TotalCount": 0,
            "TotalTimeMillis": 0
        },
        "NonTalkTime": {
            "TotalTimeMillis": 0,
            "Instances": []
        },
        "TalkSpeed": {
            "DetailsByParticipant": {
                "AGENT": {
                    "AverageWordsPerMinute": 239
                },
                "CUSTOMER": {
                    "AverageWordsPerMinute": 163
                }
            }
        },
        "TalkTime": {
            "TotalTimeMillis": 28698,
            "DetailsByParticipant": {
                "AGENT": {
                    "TotalTimeMillis": 15079
                },
                "CUSTOMER": {
                    "TotalTimeMillis": 13619
                }
            }
        }
    },
    "CustomModels": [],
    "Transcript": [
        {
            "BeginOffsetMillis": 0,
            "Content": "Okay.",
            "EndOffsetMillis": 90,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                79.27
            ]
        },
        {
            "BeginOffsetMillis": 160,
            "Content": "Just hello. My name is Peter and help.",
            "EndOffsetMillis": 4640,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                66.56,
                40.06,
                85.27,
                82.22,
                77.66
            ],
            "Redaction": {
                "RedactedTimestamps": [
                    {
                        "BeginOffsetMillis": 3290,
                        "EndOffsetMillis": 3620
                    }
                ]
            }
        },
        {
            "BeginOffsetMillis": 4640,
            "Content": "Hello. Peter, how can I help you?",
            "EndOffsetMillis": 6610,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                70.23,
                73.05,
                71.8
            ],
            "Redaction": {
                "RedactedTimestamps": [
                    {
                        "BeginOffsetMillis": 5100,
                        "EndOffsetMillis": 5450
                    }
                ]
            }
        },
        {
            "BeginOffsetMillis": 7370,
            "Content": "I need to cancel. I want to cancel my plan subscription.",
            "EndOffsetMillis": 11190,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "NEGATIVE",
            "LoudnessScore": [
                77.18,
                79.59,
                85.23,
                81.08,
                73.99
            ],
            "IssuesDetected": [
                {
                    "CharacterOffsets": {
                        "BeginOffsetChar": 0,
                        "EndOffsetChar": 55
                    },
                    "Text": "I need to cancel. I want to cancel my plan subscription"
                }
            ]
        },
        {
            "BeginOffsetMillis": 11220,
            "Content": "That sounds very bad. I can offer a 20% discount to make you stay
with us.",
            "EndOffsetMillis": 15210,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEGATIVE",
            "LoudnessScore": [
                75.92,
                75.79,
                80.31,
                80.44,
                76.31
            ]
        },
        {
            "BeginOffsetMillis": 15840,
            "Content": "That sounds interesting. Thank you accept.",
            "EndOffsetMillis": 18120,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                73.77,
                79.17,
                77.97,
                79.29
            ]
        },
        {
            "BeginOffsetMillis": 18310,
            "Content": "Alright, I made all the changes to the account and now these
discounts applied.",
            "EndOffsetMillis": 21820,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                83.88,
                86.75,
                86.97,
                86.11
            ],
            "OutcomesDetected": [
                {
                    "CharacterOffsets": {
                        "BeginOffsetChar": 9,
                        "EndOffsetChar": 77
                    },
                    "Text": "I made all the changes to the account and now these discounts
applied"
                }
            ]
        },
        {
            "BeginOffsetMillis": 22610,
            "Content": "Awesome. Thank you so much.",
            "EndOffsetMillis": 24140,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                79.11,
                81.7,
                78.15
            ]
        },
        {
            "BeginOffsetMillis": 24120,
            "Content": "No worries. I will send you all the details later today and call
you back next week to check up on you.",
            "EndOffsetMillis": 29710,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                87.07,
                83.96,
                76.38,
                88.38,
                87.69,
                76.6
            ],
            "ActionItemsDetected": [
                {
                    "CharacterOffsets": {
                        "BeginOffsetChar": 12,
                        "EndOffsetChar": 102
                    },
                    "Text": "I will send you all the details later today and call you back
next week to check up on you"
                }
            ]
        },
        {
            "BeginOffsetMillis": 30580,
            "Content": "Thank you. Sir. Have a nice evening.",
            "EndOffsetMillis": 32110,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                81.42,
                82.29,
                73.29
            ]
        }
    ]
    }
}
```

Example redacted file

This section shows an example redacted file. It's a twin of the original analyzed file. The only difference is that sensitive data are redacted.

```
{
    "Version": "1.1.0",
    "AccountId": "your AWS account ID",
    "ContentMetadata": {
        "RedactionTypes": [
            "PII"
        ],
        "Output": "Redacted"
    },
    "Channel": "VOICE",
    "JobStatus": "COMPLETED",
    "LanguageCode": "en-US",
    "Participants": [
        {
            "ParticipantId": "CUSTOMER",
            "ParticipantRole": "CUSTOMER"
        },
        {
            "ParticipantId": "AGENT",
            "ParticipantRole": "AGENT"
        }
    ],
    "Categories": {
        "MatchedCategories": [],
        "MatchedDetails": {}
    },
    "ConversationCharacteristics": {
        "TotalConversationDurationMillis": 32110,
        "Sentiment": {
            "OverallSentiment": {
                "AGENT": 0,
                "CUSTOMER": 3.1
            },
            "SentimentByPeriod": {
                "QUARTER": {
                    "AGENT": [
                        {
                            "BeginOffsetMillis": 0,
                            "EndOffsetMillis": 7427,
                            "Score": 0
                        },
                        {
                            "BeginOffsetMillis": 7427,
                            "EndOffsetMillis": 14855,
                            "Score": -5
                        },
                        {
                            "BeginOffsetMillis": 14855,
                            "EndOffsetMillis": 22282,
                            "Score": 0
                        },
                        {
                            "BeginOffsetMillis": 22282,
                            "EndOffsetMillis": 29710,
                            "Score": 5
                        }
                    ],
                    "CUSTOMER": [
                        {
                            "BeginOffsetMillis": 0,
                            "EndOffsetMillis": 8027,
                            "Score": -2.5
                        },
                        {
                            "BeginOffsetMillis": 8027,
                            "EndOffsetMillis": 16055,
                            "Score": 5
                        },
                        {
                            "BeginOffsetMillis": 16055,
                            "EndOffsetMillis": 24082,
                            "Score": 5
                        },
                        {
                            "BeginOffsetMillis": 24082,
                            "EndOffsetMillis": 32110,
                            "Score": 5
                        }
                    ]
                }
            }
        },
        "Interruptions": {
            "InterruptionsByInterrupter": {},
            "TotalCount": 0,
            "TotalTimeMillis": 0
        },
        "NonTalkTime": {
            "TotalTimeMillis": 0,
            "Instances": []
        },
        "TalkSpeed": {
            "DetailsByParticipant": {
                "AGENT": {
                    "AverageWordsPerMinute": 239
                },
                "CUSTOMER": {
                    "AverageWordsPerMinute": 163
                }
            }
        },
        "TalkTime": {
            "TotalTimeMillis": 28698,
            "DetailsByParticipant": {
                "AGENT": {
                    "TotalTimeMillis": 15079
                },
                "CUSTOMER": {
                    "TotalTimeMillis": 13619
                }
            }
        }
```

```
    },
    "CustomModels": [],
    "Transcript": [
        {
            "BeginOffsetMillis": 0,
            "Content": "Okay.",
            "EndOffsetMillis": 90,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                79.27
            ]
        },
        {
            "BeginOffsetMillis": 160,
            "Content": "Just hello. My name is [PII] and help.",
            "EndOffsetMillis": 4640,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                66.56,
                40.06,
                85.27,
                82.22,
                77.66
            ],
            "Redaction": {
                "RedactedTimestamps": [
                    {
                        "BeginOffsetMillis": 3290,
                        "EndOffsetMillis": 3620
                    }
                ]
            }
        },
        {
            "BeginOffsetMillis": 4640,
            "Content": "Hello. [PII], how can I help you?",
            "EndOffsetMillis": 6610,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                70.23,
                73.05,
                71.8
            ],
            "Redaction": {
                "RedactedTimestamps": [
                    {
                        "BeginOffsetMillis": 5100,
                        "EndOffsetMillis": 5450
                    }
                ]
            }
        },
        {
            "BeginOffsetMillis": 7370,
            "Content": "I need to cancel. I want to cancel my plan subscription.",
            "EndOffsetMillis": 11190,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "NEGATIVE",
            "LoudnessScore": [
                77.18,
                79.59,
                85.23,
                81.08,
                73.99
            ],
            "IssuesDetected": [
                {
                    "CharacterOffsets": {
                        "BeginOffsetChar": 0,
                        "EndOffsetChar": 55
                    },
                    "Text": "I need to cancel. I want to cancel my plan subscription"
                }
            ]
        },
        {
            "BeginOffsetMillis": 11220,
            "Content": "That sounds very bad. I can offer a 20% discount to make you stay
with us.",
            "EndOffsetMillis": 15210,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEGATIVE",
            "LoudnessScore": [
                75.92,
                75.79,
                80.31,
                80.44,
                76.31
            ]
        },
        {
            "BeginOffsetMillis": 15840,
            "Content": "That sounds interesting. Thank you accept.",
            "EndOffsetMillis": 18120,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                73.77,
                79.17,
                77.97,
                79.29
            ]
        },
        {
            "BeginOffsetMillis": 18310,
            "Content": "Alright, I made all the changes to the account and now these
discounts applied.",
            "EndOffsetMillis": 21820,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "NEUTRAL",
            "LoudnessScore": [
                83.88,
                86.75,
                86.97,
                86.11
            ],
            "OutcomesDetected": [
                {
                    "CharacterOffsets": {
                        "BeginOffsetChar": 9,
                        "EndOffsetChar": 77
                    },
                    "Text": "I made all the changes to the account and now these discounts
applied"
                }
            ]
        },
        {
            "BeginOffsetMillis": 22610,
            "Content": "Awesome. Thank you so much.",
            "EndOffsetMillis": 24140,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                79.11,
                81.7,
                78.15
            ]
        },
        {
            "BeginOffsetMillis": 24120,
            "Content": "No worries. I will send you all the details later today and call
you back next week to check up on you.",
            "EndOffsetMillis": 29710,
            "Id": "the ID of the turn",
            "ParticipantId": "AGENT",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                87.07,
                83.96,
                76.38,
                88.38,
                87.69,
                76.6
            ],
            "ActionItemsDetected": [
                {
                    "CharacterOffsets": {
                        "BeginOffsetChar": 12,
                        "EndOffsetChar": 102
                    },
                    "Text": "I will send you all the details later today and call you back
next week to check up on you"
                }
            ]
        },
        {
            "BeginOffsetMillis": 30580,
            "Content": "Thank you. Sir. Have a nice evening.",
            "EndOffsetMillis": 32110,
            "Id": "the ID of the turn",
            "ParticipantId": "CUSTOMER",
            "Sentiment": "POSITIVE",
            "LoudnessScore": [
                81.42,
                82.29,
                73.29
            ]
        }
    ]
}
```

Troubleshoot issues in Contact Lens

Why don't I see color-coded bars on my Amazon Connect console?

If your Amazon Connect console doesn't include color-coded bars similar to those shown in the preceding image, check whether the conversation that you're trying to analyzed occurred before June 30, 2020.

This view of conversations works only if the Contact Lens is enabled, and then the conversation occurred after June 30, 2020. This is because the feature that displays analyzed conversations in this format was released on June 30, 2020, and it can only be applied to conversations that happen after that time.

Why don't I see or hear unredacted content?

If your organization is using the Contact Lens redaction feature, by default only redacted content appears in the Amazon Connect console.

You must have permissions to view unredacted content. For more information, see Security profile permissions for Contact Lens (p. 818).

Use real-time caller authentication with Voice ID

Amazon Connect Voice ID provides real-time caller authentication and fraud risk detection which make voice interactions in contact centers more secure and efficient. Voice ID uses machine learning to verify the identity of genuine customers by analyzing a caller's unique voice characteristics. This allows contact centers to use an additional security layer that doesn't rely on the caller answering multiple security questions, and makes it easy to enroll and verify customers without changing the natural flow of their conversation. Voice ID also offers real-time detection of fraudsters who frequently target your contact center, thereby reducing losses due to fraud.

With Amazon Connect Voice ID you can:

- Passively enroll customers for voice authentication without requiring them to repeat a particular word or phrase.
- Migrate customers into Voice ID by enrolling them in batch.
- Verify the enrolled customer's identity by analyzing their unique voice characteristics.
- Detect fraudsters from a watchlist that you have created.

How Voice ID works

Customer enrollment

1. When a customer calls for the first time, the agent confirms the identity of the caller by using existing security measures, such as asking for mother's maiden name or a one-time passcode (OTP) delivered by SMS. This ensures that only genuine customers are enrolled in Voice ID.
2. Voice ID starts listening to the customer's speech after the contact has encountered the Set Voice ID (p. 410) block, where Voice ID is enabled. Voice ID listens to the call until one of the following happens:
   - It gets enough audio to evaluate the speaker for authentication, fraud, and enroll the speaker (if requested). This is 30 seconds of customer speech, excluding silence.
   - The call ends.
3. Voice ID then creates the enrollment voiceprint. A voiceprint is a mathematical representation that implicitly captures unique aspects of an individual's voice such as speech rhythm, pitch, intonation, and loudness.

   The caller does not need to say or repeat any specific phrases to enroll in Voice ID.

Customer authentication

1. When the enrolled customer calls back in, they are verified through an interaction with an IVR, or during their interaction with an agent.

   By default Voice ID is configured to require 10 seconds of a caller's speech to authenticate, which can be done as part of a typical customer interaction in the IVR or with the agent (such as "what's your first and last name?" and "what are you calling about?"). You can adjust the amount of required speech using the Authentication response time (p. 413) property in the Set Voice ID (p. 410) block.

2. Voice ID uses the audio to generate the caller's voiceprint and compares it with the enrolled voiceprint corresponding to the claimed identity, and returns an authentication result.

For more information about the agent's experience, see Use Voice ID (p. 1189).

How much speech is needed for enrollment and authentication

- Enrollment: 30 seconds of customer net speech (speech that excludes any silence) to create a voiceprint and enroll a customer.
- Verification: By default, 10 seconds of customer net speech to verify that the voice belongs to the claimed identity. The speech can be from interacting with an IVR or an agent. You can adjust the amount of required speech using the Authentication response time (p. 413) property in the Set Voice ID (p. 410).

Batch enrollment

You can get a jump start on using biometrics by batch enrolling customers who have already consented for biometrics. Using stored audio recordings in your S3 bucket, and a JSON input file that provides the speaker identifier and a link to the audio recordings, you can invoke the Voice ID batch APIs.

For more information, see Batch enrollment using audio data from prior calls (p. 870).

Known fraudster detection

1. Create a watchlist of known fraudsters by using fraudster registration API on your stored audio recordings in your S3 bucket. For more information, see Create and edit a fraudster watchlist (p. 873).
2. When a fraudster from the watchlist calls in, Voice ID analyzes the call audio to return a risk score and outcome to indicate how closely the caller's voiceprint matches the fraudsters voiceprint that is created from audio recordings from your S3 bucket.

What data is stored?

Voice ID stores audio files of the speaker's voice, voiceprints, and speaker identifiers. This data is encrypted using a KMS key that you provide.

If you enable detection of fraudsters in a watchlist, Voice ID also stores the fraudster audio and voiceprints. For more information, see Data handled by Amazon Connect (p. 1064).

Expired speakers

For BIPA compliance, Voice ID automatically expires speakers that have not been accessed for enrollment, re-enrollment, or successful authentication for three years.

To view a speaker's last access, look at the `lastAccessedAt` attribute that is returned by the `DescribeSpeaker` and `ListSpeakers` APIs.

If you try to use the `EvaluateSesssion` API to authenticate an expired speaker, a `SPEAKER_EXPIRED` authentication decision is returned.

To use the expired speaker again, they must be re-enrolled.

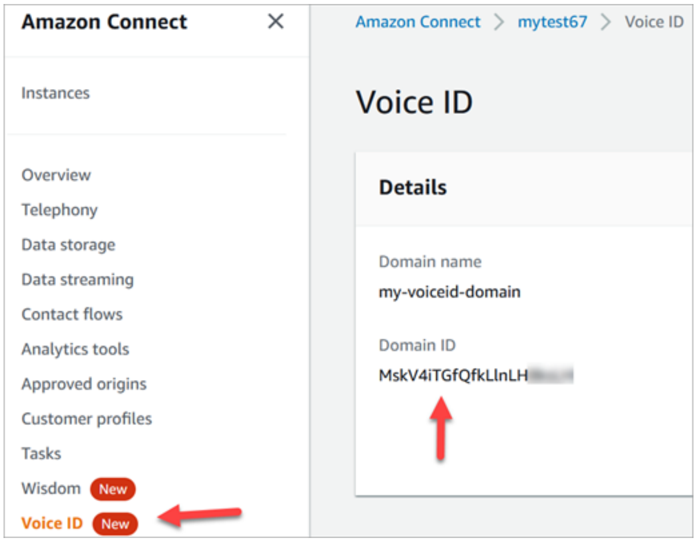
Voice ID domains

When you enable Amazon Connect Voice ID, you create a Voice ID domain: a container for all Voice ID data, such as speaker identifiers (which serves as the customer identifier), the voiceprints, the customer audio that was used for creating the enrollment voiceprints, and the enrollment statuses (enrolled, opted out, etc.) associated with the speaker identifiers. For detection of fraudsters in a watchlist, the Voice ID domain stores the fraudster identifiers, voiceprints, and audio used for creating the voiceprints.

Following are guidelines for creating Voice ID domains:

- Each Amazon Connect instance can be associated with only one Voice ID domain.
- Each Voice ID domain can be associated with multiple Amazon Connect instances. This enables you to use the same stored customer data across multiple Amazon Connect instances.
- You can create multiple domains, but they don't share customer data between each other.
- We recommend creating a new Voice ID domain to associate with a Amazon Connect instance when:
  - You are enabling Voice ID for the first time on your account in an AWS Region.
  - You want to ensure that you isolate the Voice ID domains used for your test and production environments.
- We recommend using an existing Voice ID domain when:
  - You want to use the same set of enrolled callers and fraudsters across different Amazon Connect instances (that may belong to different customer service teams)
  - You want to use the same test environment across different test Amazon Connect instances.

    Note
    Only existing Voice ID domains in the same Region in your Amazon Connect account can be shared across Amazon Connect instances in that Region.
- You can change the association of your Amazon Connect instance from your current domain to a new domain at any time, by choosing a different domain.
- To delete a Voice ID domain, use the DeleteDomain Voice ID API. `DeleteDomain` soft deletes the domain. Amazon Connect waits 30 days before completely erasing the domain data. During this period, Voice ID; is disabled for all the Amazon Connect instances it is associated with. To restore a domain during this window, submit an AWS Support ticket and provide the domain ID. You can find the domain ID on the Voice ID section of the Amazon Connect console, as shown in the following example:



Voice ID

Details

Domain name
my-voiceid-domain

Domain ID
MskV4iTGfQfkLlnLH[redacted]

Deleting a Voice ID domain deletes all stored customer data, such as audio recordings, voiceprints, and speaker identifiers, as well as any fraudster watchlists that you managed.

Enrollment status

Voice ID stores three different enrollment status for a speaker: `ENROLLED`, `OPTED_OUT` and `EXPIRED`. You can recall these speaker status using Amazon Connect Voice ID APIs and using contact flow blocks to take appropriate action.

- `ENROLLED`: When you enroll a new caller is enrolled into Voice ID, Voice ID creates a new voiceprint and set the speaker status as `ENROLLED`. Even if you re-enroll the same caller into Voice ID, the status stays as `ENROLLED`.
- `OPTED_OUT`: If a caller does not provide consent to enroll into biometrics, you can opt out the caller (in the Contact Control Panel) or using APIs. Voice ID creates a new entry for this caller and set the speaker's status `OPTED_OUT`. Voice ID does not generate any voiceprint or store any audio recording for the speaker. Future enrollment requests for this speaker is rejected unless their entry is deleted.
- `EXPIRED`: If a caller's voiceprint has not been accessed or refreshed for 3 years, Voice ID changes the status to `EXPIRED`, and you are no longer able to perform authentications for this caller. You can re-enroll the caller again or delete the caller from Voice ID.

Speaker and fraudster identifiers

Voice ID uses speaker identifiers to refer to and retrieve the voiceprints in a Voice ID domain. We recommend that you use identifiers that do not contain an Personally Identifiable Information (PII) in the identifiers.

Voice ID creates two fields to refer to a caller:

- `CustomerSpeakerId`: A identifier provided by the customer. It can be between 1-256 characters and can only contain: **a-z**, **A-Z**, **0-9**, **-** and **_**
- `GeneratedSpeakerId`: A unique 22-character alphanumeric string that Voice ID creates and returns at the time of enrollment of the caller.

Amazon Connect Voice ID speaker APIs accept either form of speaker identifiers, but only emit `GeneratedSpeakerId` in the Voice ID event streams and contact records. If you want to re-record the caller to redo the voiceprint, you can enroll the caller with the same `CustomerSpeakerId`.

Similarly, Voice ID creates unique fraudster identifiers called `GeneratedFraudsterID` for every fraudster that you add to a watchlist in the domain. Voice ID returns the fraudster identifier if a fraudster is detected in a call when performing fraud risk detection.

Enable Voice ID

There are two ways you can enable Voice ID for your instance:

- Use the Amazon Connect console. This topic provides instructions.
- Use the Amazon Connect Voice ID API. For more information, see the Amazon Connect Voice ID API Reference.

Before you begin

Before you get started, complete the following tasks.

Tasks

Grant the required permissions

You must grant the required permissions to IAM users, groups, or roles. For more information, see AmazonConnectVoiceIDFullAccess (p. 1113).

Decide how to name your Voice ID domain

When you enable Voice ID, you are prompted to provide a friendly domain name that's meaningful to you such as your organization name, for example, *Voice ID-ExampleCorp*.

Create an AWS KMS key to encrypt data stored in the domain

When you enable Voice ID, you are prompted to create or provide an AWS KMS key. It encrypts the customer data stored by Voice ID such as audio files, voiceprints, and the speaker identifiers.

Step-by-step instructions for creating these KMS keys are provided in Step 1: Create a new Voice ID domain and encryption key (p. 863).

Data at rest—specifically, freeform fields that you provide plus audio files/voiceprints—are encrypted under the KMS key you choose. Your customer managed key is created, owned, and managed by you. You have full control over the KMS key (AWS KMS charges apply).

When making calls to Voice ID for anything other than `CreateDomain` or `UpdateDomain`, the user making the call requires `kms:Decrypt` permissions for the key associated with the domain. When making calls to `CreateDomain` or `UpdateDomain`, the user also requires `kms:DescribeKey` and `kms:CreateGrant` permissions for the key. When you create (or update) a Voice ID domain, it creates a grant on the KMS key so that it can be used by Voice ID asynchronous processes (such as speaker enrollment) and by the Amazon Connect service-linked role during your contact flows. This grant includes an encryption context specifying the domain with which the key is associated. For more on grants, see Using grants in the AWS Key Management Service Developer Guide.

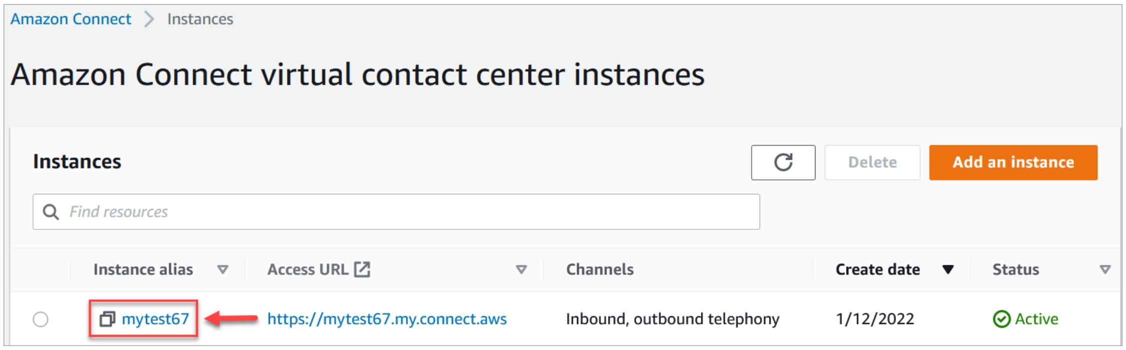
If you create a domain and associate it with one key, store some data, and then change the KMS key to a different key, an asynchronous process will be triggered to re-encrypt the old data with the new KMS key. After this process completes, all of your domain's data will be encrypted under the new KMS key, and you may safely retire the old key. For more information, see UpdateDomain.

> **Tip**
> You can create KMS keys or provide an existing KMS key programmatically. For more information, see Amazon Connect Voice ID APIs.

Step 1: Create a new Voice ID domain and encryption key

Following are instructions for how to create a new domain and encryption key.

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



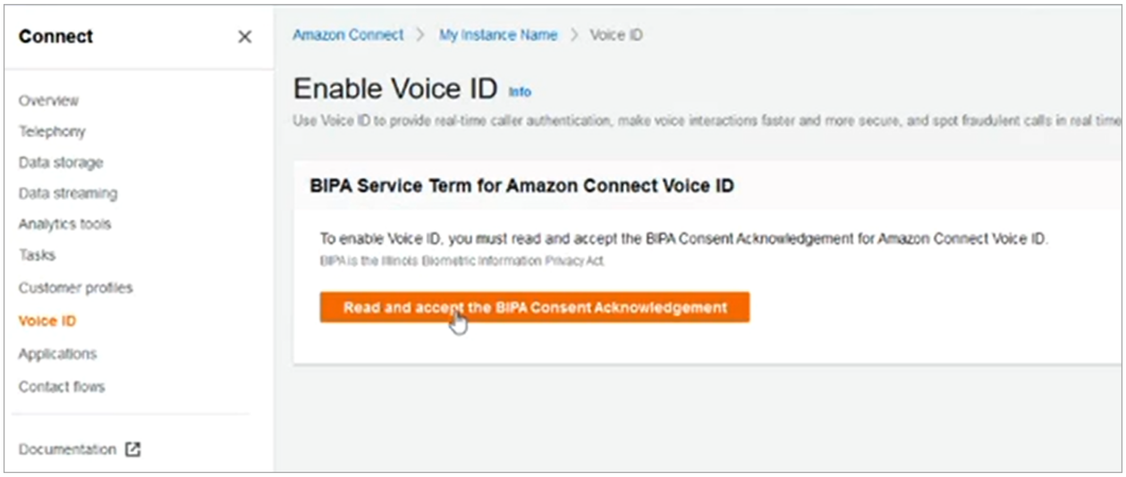
Amazon Connect > Instances

Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Voice ID**. Read the BIPA Consent Acknowledgement, and accept if you agree.



Amazon Connect > My Instance Name > Voice ID

Enable Voice ID Info

Use Voice ID to provide real-time caller authentication, make voice interactions faster and more secure, and spot fraudulent calls in real time

BIPA Service Term for Amazon Connect Voice ID

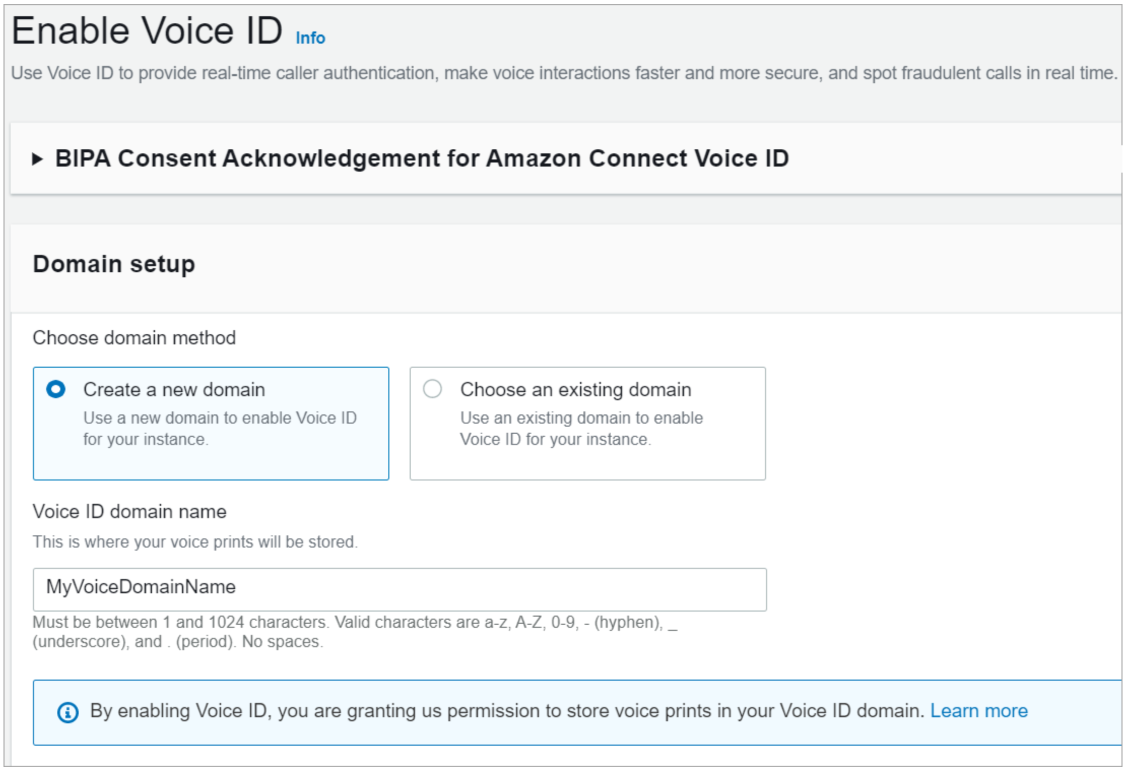
To enable Voice ID, you must read and accept the BIPA Consent Acknowledgement for Amazon Connect Voice ID.

BIPA is the Illinois Biometric Information Privacy Act

This is a requirement to enable Voice ID and is needed only once per account, across all Regions. This cannot be done using APIs.

For more information about the Biometric Privacy Act (BIPA) in general, see this Wikipedia article.

4. In the **Domain setup** section, choose **Create a new domain**.



Enable Voice ID Info

Use Voice ID to provide real-time caller authentication, make voice interactions faster and more secure, and spot fraudulent calls in real time.

▸ BIPA Consent Acknowledgement for Amazon Connect Voice ID

Domain setup

Choose domain method

● Create a new domain
Use a new domain to enable Voice ID for your instance.

○ Choose an existing domain
Use an existing domain to enable Voice ID for your instance.

Voice ID domain name
This is where your voice prints will be stored.

MyVoiceDomainName

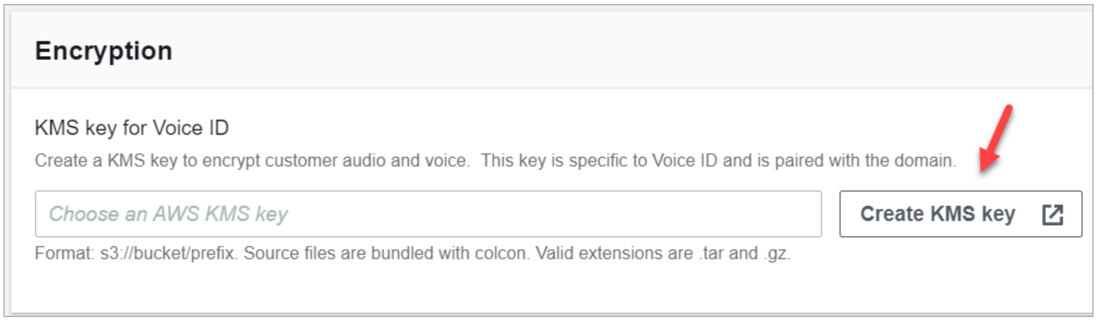
Must be between 1 and 1024 characters. Valid characters are a-z, A-Z, 0-9, - (hyphen), _ (underscore), and . (period). No spaces.

ⓘ By enabling Voice ID, you are granting us permission to store voice prints in your Voice ID domain. Learn more

5. In the **Domain name** box, enter a friendly name that's meaningful to you, such as your organization name, for example, *VoiceID-ExampleCorp*.

6. Under **Encryption**, create or enter your own AWS KMS key for encrypting your Voice ID domain. Following are the steps to create your KMS key key:

   1. Choose **Create KMS key**.



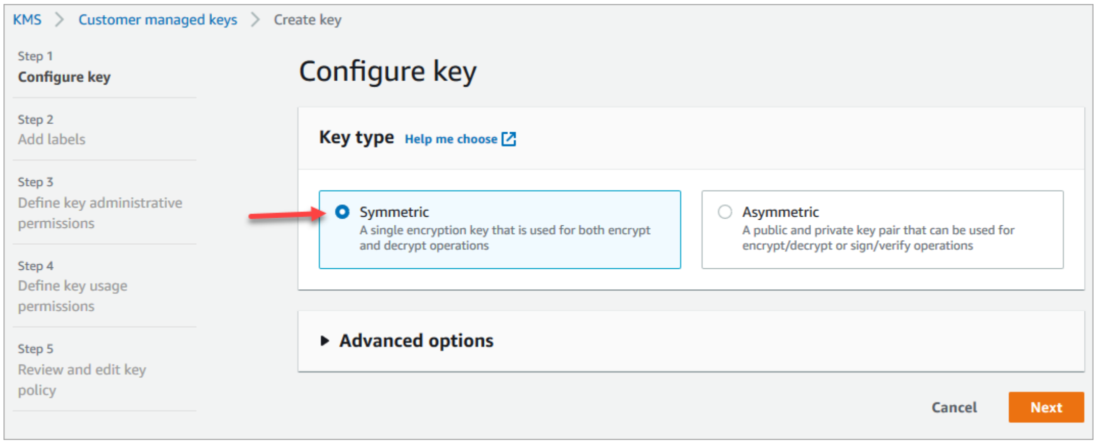
Encryption

KMS key for Voice ID
Create a KMS key to encrypt customer audio and voice. This key is specific to Voice ID and is paired with the domain.

Choose an AWS KMS key

Format: s3://bucket/prefix. Source files are bundled with colcon. Valid extensions are .tar and .gz.

   2. A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.


KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review and edit key policy
Help me choose
▸ Advanced options
Cancel
Next

Configure key

Key type

● Symmetric
A single encryption key that is used for both encrypt and decrypt operations

○ Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

   3. On the **Add labels** page, add a name and description for the KMS key, and then choose **Next**.
   4. On the **Define key administrative permissions** page, choose **Next**.
   5. On the **Define key usage permissions** page, choose **Next**.
   6. On the **Review and edit key policy** page, choose **Finish**.
   7. Return to the tab in your browser for the Amazon Connect console, **Voice ID** page. Click or tap in the **AWS KMS key** for the key you created to appear in a dropdown list. Choose the key you created.

7. Choose **Enable Voice ID**.

You've enabled Voice ID for your instance. Next, in Step 2 you configure how you want Voice ID to work in your contact flow.

Step 2: Configure Voice ID in your contact flow

In this step you add the required blocks to your contact flow and configure how you want Voice ID to work.

- Play prompt (p. 393): Add this block before the Set Voice ID (p. 410) block to stream audio properly. You can edit it to include a simple message such as "Welcome."
- Set Voice ID (p. 410): After the Play prompt (p. 393) block, add the Set Voice ID (p. 410) block. It should be at the start of a call. You use this block to start streaming audio to Amazon Connect Voice ID to verify the caller's identity, as soon as the call is connected to a contact flow. In this block you configure the authentication threshold, response time, and fraud threshold.
- Set contact attributes (p. 399): Use to pass the `CustomerId` attribute to Voice ID. The `CustomerId` may be a customer number from your CRM, for example. You can create a Lambda function to pull the unique customer ID of the caller from your CRM system. Voice ID uses this attribute as the `CustomerSpeakerId` for the caller.
- Check Voice ID (p. 339): Use to check the response from Voice ID for enrollment status, voice authentication, and fraud detection, and then branch based on one of the returned statuses.

Example Voice ID contact flow

Caller not enrolled

1. When a customer calls for the first time, their `CustomerId` is passed to Voice ID using the Set contact attributes (p. 399) block.
2. Voice ID looks for `CustomerId` in its database. Since it's not there, it sends a **Not enrolled** result message. The Check Voice ID (p. 339) block branches based on this result, and you can decide

what the next step should be. For example, you might want agents to enroll the customer in voice authentication.

3. Voice ID starts listening to the customer's speech after the contact has encountered the Set Voice ID (p. 410) block, where Voice ID is enabled. It listens until it accummulates 30 seconds of net speech or the call ends, whichever happens first.

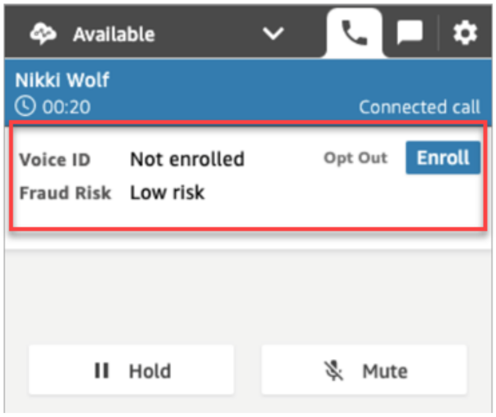
Caller enrolled

1. The next time the customer calls, Voice ID finds their `CustomerId` in the database.
2. Voice ID starts listening to the audio to create a voiceprint. The voiceprint that is created this time is used for authentication purposes so Voice ID can compare if the caller had been enrolled previously.
3. It compares the caller's current voiceprint with the stored voiceprint associated with the claimed identity. It returns a result based on the **Authentication threshold** property you configured in the Set Voice ID (p. 410) block.
4. After it evaluates the speech, it returns the message **Authenticated** if the voiceprints are similar. Or it returns one of the other statuses.
5. The contact is then routed down the appropriate branch by the Check Voice ID (p. 339) block.

Security profile permissions for Voice ID

- To enable users to search for contacts by their Voice ID status, assign the following **Analytics** permission to their security profile:
  - **Voice ID - attributes and search**: Enables users to search for and view Voice ID results on the **Contact detail** page.
- To grant agents access to Voice ID in the Contact Control Panel, assign the following permission in the **Contact Control Panel** group:
  - **Voice ID - Access**: Enables controls in the Contact Control Panel so agents can:
    - View authentication outcomes.
    - Opt-out or re-authenticate a caller.
    - Update `SpeakerID`.
    - View fraud detection results, rerun fraud analysis (fraud detection decision, fraud type and score).

The following image shows an example of these controls on the CCP:



For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

By default, the **Admin** security profile already has permissions to perform all Voice ID activities.

Search and review Voice ID results

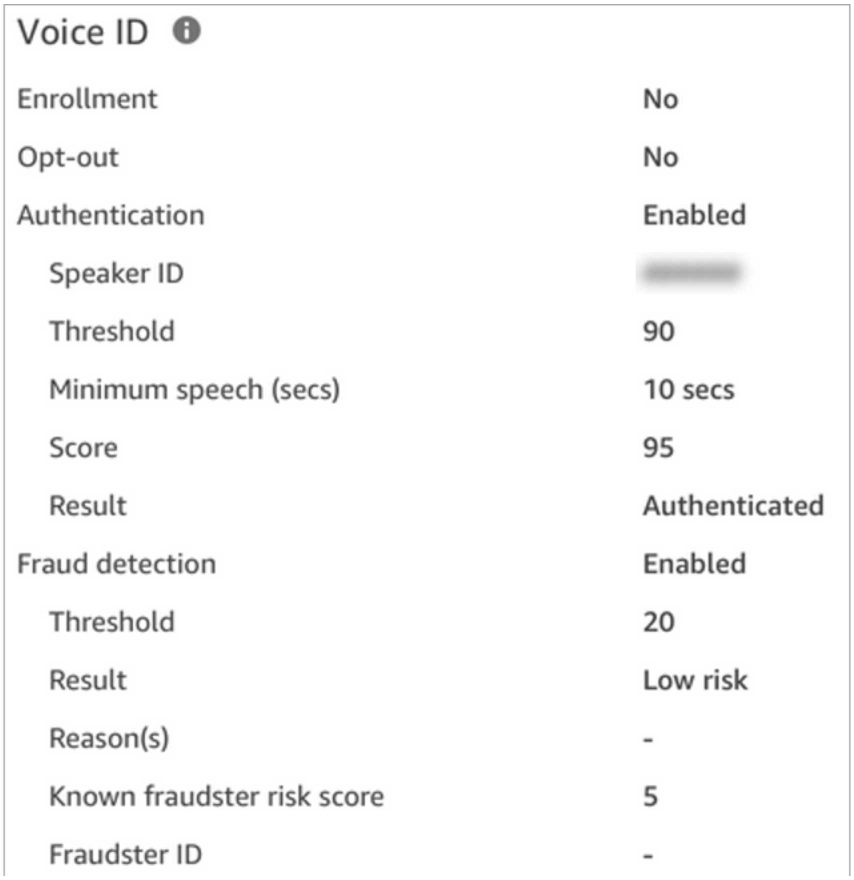
Use the Contact search (p. 907) page to search for and review the results of enrollment status, voice authentication, and detection of fraudsters in a watchlist. With the required security profile permissions (p. 911) (**Analytics** - **Voice ID - attributes and search - View**), you can search for Voice ID results using the following filters:

- **Speaker actions**: Use this filter to search for contacts where the caller was enrolled into Voice ID or chose to opt-out of Voice ID altogether.
- **Authentication result**: Use this filter to search for contacts where Voice ID authentication returned the following results:
  - Authenticated
  - Not authenticated
  - Opted out
  - Inconclusive
  - Not enrolled

  For example, if you want to search for all contacts where the authentication status was returned as **Not authenticated** or **Opted out**, select both these options and choose **Apply**.
- **Fraud detection result**: Use this filter to search for contacts where Voice ID fraud analysis returned the following results:
  - High risk for fraud
  - Low risk for fraud
  - Inconclusive
- **Fraud detection reason**: Use this filter to search for contacts where specific fraud risk mechanisms were detected:
  - Known fraudster: the caller's voice matches a fraudster from the fraudster watchlist you have created.
  - Voice spoofing: the caller is modifying their voice or is using speech synthesis to spoof the agent.

Voice ID results in a Contact Record

After you search for a contact, you can choose an ID to view their contact record. The following image shows an example of the fields in the Voice ID section of the contact record:



Voice ID

Enrollment	No
Opt-out	No
Authentication	Enabled
Speaker ID	[redacted]
Threshold	90
Minimum speech (secs)	10 secs
Score	95
Result	Authenticated
Fraud detection	Enabled
Threshold	20
Result	Low risk
Reason(s)	-
Known fraudster risk score	5
Fraudster ID	-

Use the Voice ID APIs

To manage Voice ID programmatically, see Amazon Connect Voice ID APIs.

This section explains how to perform common scenarios using the Voice ID APIs.

Contents

Voice ID domain operations

Amazon Connect Voice ID provides APIs for you manage Voice ID domains. You can find equivalents for Create, Update, Describe and List in the AWS Console.

1. CreateDomain: To create a new Voice ID domain, you can use the `CreateDomain` Voice ID API. You can only invoke this for your account after you have acknowledged the BIPA Consent in the AWS console. You must also specify the KMS key for the Voice ID domain at the time of creation.

   Creating a domain doesn't associate it with an Amazon Connect instance. You must call the Amazon Connect association APIs to do so.
2. UpdateDomain: To update the name and encryption configuration for a domain, you can use the `UpdateDomain` Voice ID API. This API clobbers existing attributes, and you must provide both these fields.

   When you change the KMS key associated with the Voice ID domain, following the `UpdateDomain` call your domain's existing data will be asynchronously re-encrypted under the new KMS key. You can check status of this process from your domain's `ServerSideEncryptionUpdateDetails` attribute via `DescribeDomain` API. While this update process is in progress, you must retain your old KMS key in an accessible state, otherwise this process may fail. After this process completes, the old KMS key may be safely retired.
3. DescribeDomain: Use this API to return the name, description and encryption configuration of an existing domain identified by its `DomainID`.
4. ListDomains: Use this API to list all your Voice ID domains owned by your account in the Region.
5. DeleteDomain: To delete a Voice ID domain, you must invoke the `DeleteDomain` Voice ID API and provide the domain ID. If this domain was associated with an Amazon Connect instance, Voice ID API calls and Voice ID contact flow blocks will return runtime error. Deleting a Voice ID domain deletes all stored customer data such as audio recordings, voiceprints and speaker identifiers, as well as fraudster lists that you managed.

Voice ID and Amazon Connect Integration Association APIs

You can use the following APIs to manage associations with Amazon Connect instances. You can perform these operations on the AWS Console as well.

1. CreateIntegrationAssociation: To enable Voice ID on an Amazon Connect instance, you will need to associate a Voice ID domain with a Amazon Connect instance using a `CreateIntegrationAssociation` request. You can only associate one Voice ID domain to an Amazon Connect instance. If the instance is already associated with a domain, the API returns the following error:

   `DuplicateResourceException` (409) - Request is trying to created a duplicate resource.
2. DeleteIntegrationAssociation: To delete an existing association between an Amazon Connect instance and a Voice ID domain, you will need to call the `DeleteIntegrationAssociation` APIs along with the Amazon Connect InstanceID and the `IntegrationAssociationID` returned by `CreateIntegrationAssociation`. This is a required step if you want to associate a different Voice ID domain to this Amazon Connect instance. We do not recommend deleting associations in a production setup as it can cause unpredictable behavior for Voice ID in your Amazon Connect instance.
3. ListIntegrationAssociations: To list all the associations between Amazon Connect instance and Voice ID domains for your account in this Region, you can invoke `ListIntegrationAssociations` API.

Voice ID speaker and fraudster management APIs

Amazon Connect Voice ID includes APIs to manage speakers enrolled into a Voice ID domain and fraudsters registered in the domain. All speaker APIs except `ListSpeakers` accept either the `CustomerSpeakerId` or `GeneratedSpeakerId`.

1. DescribeSpeaker: Use this API to describe a speaker's status in a domain (ENROLLED, OPTED_OUT, EXPIRED) (p. 861), and to map a `GeneratedSpeakerId` to a `CustomerSpeakerId`, and vice versa.
2. OptOutSpeaker: To opt out a caller from a Voice ID domain, you can use this API. This API doesn't require the speaker to be present in Voice ID. A non-existing speaker can be opted-out using this API and Voice ID persists the opted out status and rejects future enrollment requests for this speaker. Opting out also removes voiceprints and any stored audio recordings for this caller.
3. DeleteSpeaker: To completely remove all records for a caller/speaker from a Voice ID domain, you can use this API. All voiceprints and enrollment status is deleted immediately, and associated audio recordings are removed within 24 hours.
4. ListSpeakers: To list all the speakers whose entries are present in a Voice ID domain, you can use this API, which returns both the `CustomerSpeakerId` and `GeneratedSpeakerId` for a speaker. It returns a paginated output with the page size dictated in the API request.
5. DescribeFraudster: You can use this API to describe a fraudster's status in the Voice ID domain.
6. DeleteFraudster: To delete a fraudster from a Voice ID domain, you can use this API. It deletes all voiceprints and any stored audio recordings.

Batch enrollment using audio data from prior calls

You can get a jump start on using biometrics by batch enrolling customers who have already consented for biometrics. Using stored audio recordings in your S3 bucket, and a JSON input file that provides the speaker identifier and a link to the audio recordings, you can invoke the Voice ID batch APIs.

To enroll customers programmatically, pass the following data to the API:

1. The domain ID to specify the domain to associate recordings to.
2. The location for the output file.
3. An input file containing a list of speakers. See Input and output file schema for Speaker Enrollment Job (p. 871).

   For each speaker the file must include:
   - A link to a call audio recording in a .wav file with 8KHz sample rate and PCM-16 encoding.
   - The corresponding `CustomerSpeakerId` for the customer.
   - A channel for the caller in the audio recording. If the audio has multiple channels, you can select only one.
4. A KMS key to use when writing the output.
5. A role that Voice ID can assume. It must have access to the S3 bucket where the audio files are stored. This role must have access to any KMS key used to encrypt the files. It must also be able to write to the specified output location and use the KMS key requested for writing the output. Specifically, it must have the following permissions:
   - `s3:GetObject` on the input bucket.
   - `s3:PutObject` on the output bucket.
   - `kms:Decrypt` on the KMS key used for input bucket’s default encryption.
   - `kms:Decrypt` and `kms:GenerateDataKey` on the KMS key provided in the input which will be used for writing output file to the output bucket.

   You must have `iam:PassRole` permissions when making the call and providing the `dataAccessRole`. To enable confused deputy protection for the `dataAccessRole`, see Amazon Connect Voice ID cross-service confused deputy prevention (p. 1131).
6. Optionally, a fraud check skip flag in case you want to skip fraud checking on the enrollment audio.
7. Optionally, the fraud threshold in case you want to raise or lower the risk.
8. Optionally, a flag to re-enroll enrolled customers. This is useful if you want to refresh the audio recording, since the default is to ignore previously enrolled customers.

The batch enrollment returns the `CustomerSpeakerId`, `GeneratedSpeakerId`, and associated status for each entry. It stores this data in a JSON file at the output path you specify in the API.

> **Note**
> You are charged for enrolling speakers. For more information, see Amazon Connect Voice ID Pricing.

Input and output file schema for Speaker Enrollment Job

Input file schema

Following is the schema of the input manifest file for the Speaker Enrollment Job:

```
{
  "Version": "string",
  "SpeakerEnrollmentRequests": [
      {
          "RequestId": "string",
          "SpeakerId": "string",
          "AudioSpecifications": [
              {
                  "S3Uri": "string",
                  "ChannelId": number
              }
           ]
      }
   ]
}
```

> **Note**
> All the fields in the schema are **required**.

Following is a description of each attribute of the input schema.

- `Version`: The version of the input schema document. Currently, this should be `1.0`.
- `SpeakerEnrollmentRequests`: List of speaker enrollment requests to be fulfilled as part of the job.
  - `RequestId`: An identifier for this speaker enrollment request. It must be unique within the input file. It is used for mapping and identifying entries in the output file.
  - `SpeakerId`: The client-provided identifier of the speaker who needs to be enrolled. You must pass the `CustomerSpeakerId` in this field. The `GeneratedSpeakerId` is not currently supported.
  - `AudioSpecifications`: The list of audio files that Voice ID can use for enrolling this speaker. Voice ID uses these audio files together to gather required amount of speech for enrollment. Currently, the maximum number of audio files allowed for an enrollment request is **10**. Each file can be a .wav file up to 20MB, containing audio with 8KHz sample rate and PCM-16 encoding.
    - `S3URI`: The Amazon S3 location of the audio file in .wav format that needs to be used for enrolling the speaker.
    - `ChannelId`: The audio channel to be used for enrolling the speaker in a multi-channel audio file. Voice ID supports audio files with up to two channels, so this value is restricted to either **0** or **1**.

Output file schema

Following is the schema of the output file generated for the Speaker Enrollment Job:

```
{
  "Version": "string",
  "Errors": [
       {
          "RequestId": "string",
          "ErrorCode": number,
          "ErrorMessage": "string"
       }
   ],
   "SuccessfulEnrollments": [
       {
          "RequestId": "string",
          "GeneratedSpeakerId": "string",
          "CustomerSpeakerId": "string",
          "EnrollmentStatus": "DUPLICATE_SKIPPED" | "NEW_ENROLLMENT" |
 "ENROLLMENT_OVERWRITE"
       }
   ]
}
```

Following is a description of each attribute of the output schema.

- `Version`: The version of the output schema document. Currently, this should be `1.0`.
- `Errors`: The list of errors for the speaker enrollment requests that failed at some point during enrollment.
- - `RequestId`: The request identifier associated with this request. This is the same as the `RequestId` specified in the input file for this request.
  - `ErrorCode`: The HTTP error code representing the type of error. Some example error scenarios are described below.

    > **Note**
    > This is not an exhaustive list.

    - 400 (Bad Request Exception):
      - The input JSON file is malformed and cannot be parsed.
      - The provided audio files do not have enough speech for enrollment.
      - Fraud verification checks failed for the given speaker.
    - 402 (ServiceQuotaLimitExceededException):
      - Speaker limit exceeded.
    - 409 (Conflict Exception):
      - Conflicting action: You cannot request an enrollment for an opted out speaker.
    - 500 (Internal Failure):
      - Internal Server Error (Unexpected error on the Service-side).
  - `ErrorMessage`: A message describing the cause of the enrollment failure.
- `SuccessfulEnrollments`: The list of enrollment requests that succeeded.
  - `RequestId`: The request identifier associated with this request. This is the same as the `RequestId` specified in the input file for this request.
  - `CustomerSpeakerId`: The client-provided identifier for the speaker who was enrolled.
  - `GeneratedSpeakerId`: The service-generated identifier for the speaker who was enrolled.
  - `EnrollmentStatus`: The status of successful speaker enrollment
    - `DUPLICATE_SKIPPED`: The speaker is already enrolled, and the enrollment was skipped.
    - `NEW_ENROLLMENT`: The speaker was newly enrolled into the system.
    - `ENROLLMENT_OVERWRITE`: The speaker is already enrolled, but was re-enrolled/overwritten using the new audio.

Create and edit a fraudster watchlist

To create and edit a fraudster watchlist, invoke the StartFraudsterRegistrationJob API for batch enrollment of fraudsters.

To add speakers the fraudster watchlist programmatically, pass the following data to the API:

1. The domain ID to specify the domain to associate recordings to.
2. An input file containing a list of fraudsters. See Input and output file schema for Fraudster Registration Job (p. 873).
3. The location for output file.
4. A KMS key to use when writing the output.
5. A role that Voice ID can assume. It must have access to the S3 bucket where the audio files are stored. This role must have access to any KMS key used to encrypt the files. It must also be able to write to the specified output location and use the KMS key requested for writing the output. Specifically, it must have the following permissions:
   - `s3:GetObject` on the input bucket.
   - `s3:PutObject` on the output bucket.
   - `kms:Decrypt` on the KMS key used for input bucket's default encryption.
   - `kms:Decrypt` and `kms:GenerateDataKey` on the KMS key provided in the input which will be used for writing output file to the output bucket.

   You must have `iam:PassRole` permissions when making the call and providing the `dataAccessRole`. To enable confused deputy protection for the `dataAccessRole`, see Amazon Connect Voice ID cross-service confused deputy prevention (p. 1131).
6. The threshold for establishing the duplicate status of fraudsters.
7. A flag to ignore fraudster duplicates.

Voice ID updates the fraudster list with successful additions, and return a `GeneratedFraudsterID` associated with entry back to the same S3 location. If duplicates are identified, Voice ID returns a "duplicate" status for the entry and provides the closest matching `GeneratedFraudsterId`.

Voice ID is not able to perform detection of fraudsters in a watchlist before the fraudster list is created.

For quotas for the fraudster list, see Amazon Connect service quotas (p. 1205).

> **Note**
> You are charged for adding to the fraudster list. For more information, see Amazon Connect Voice ID Pricing.

Input and output file schema for Fraudster Registration Job

Input file schema

Following is the schema of the input manifest file for Fraudster Registration Jobs:

```
{
 "Version": "string",
    "FraudsterRegistrationRequests": [
       {
           "RequestId": "string",
           "AudioSpecifications": [
               {
                   "S3Uri": "string",
                   "ChannelId": number
               }
           ]
       }
    ]
}
```

> **Note**
> All the fields in the schema are **required**.

Following is a description of each attribute of the input schema.

- `Version`: The version of the schema document. Currently, this should be `1.0`.
- `FraudsterRegistrationRequests`: List of fraudster registration requests to be fulfilled as part of the job.
  - `RequestId`: An identifier for this fraudster registration request. It must be unique within the input file. It is used for mapping and identifying entries in the output file.
  - `AudioSpecifications`: The list of audio files that Voice ID can use for registering this fraudster. Voice ID uses these audio files together to gather required amount of speech for registration. Currently, the maximum number of audio files allowed for a registration request is **10**.
    - `S3URI`: The Amazon S3 location of the audio file in .wav format that needs to be used for registering the fraudster.
    - `ChannelId`: The audio channel to be used for registering the fraudster in a multi-channel audio file. Voice ID supports audio files with up to two channels, so this value is restricted to either **0** or **1**.

Output file schema

Following is the schema of the output manifest file for Fraudster Registration Jobs:

```
{
 "Version": "string",
   "Errors": [
       {
          "RequestId": "string",
          "ErrorCode": number,
          "ErrorMessage": "string"
       }
   ],
   "SuccessfulRegistrations": [
       {
          "RequestId": "string",
          "GeneratedFraudsterId": "string",
          "RegistrationStatus": "DUPLICATE_SKIPPED" | "NEW_REGISTRATION",
          "FraudsterSimilarityScore": number
       }
   ]
}
```

Following is a description of each attribute of the output schema.

- `Version`: The version of the output schema document. Currently, this should be `1.0`.
- `Errors`: The list of errors for the fraudster registration requests that failed at some point during registration.

- - RequestId: The request identifier associated with this request. This is the same as the RequestId specified in the input file for this request.
  - ErrorCode: The HTTP error code representing the type of error. Some example error scenarios are described below.

    Note
    This is not an exhaustive list.

    - 400 (Bad Request Exception):
      - The input JSON file is malformed and cannot be parsed.
      - The provided audio files do not have enough speech for registration.
    - 402 (ServiceQuotaLimitExceededException):
      - Fraudster limit exceeded.
    - 500 (Internal Failure):
      - Internal Server Error (Unexpected error on the Service-side).
  - ErrorMessage: A message describing the cause of the fraudster registration failure.
- SuccessfulRegistrations: The list of registration requests that succeeded.
  - RequestId: The request identifier associated with this request. This is the same as the RequestId specified in the input file for this request.
  - RegistrationStatus: The status of successful fraudster registration.
    - DUPLICATE_SKIPPED: The fraudster was identified as a duplicate, and the registration was skipped.
    - NEW_FRAUDSTER: The Fraudster was newly enrolled into the system.
  - GeneratedFraudsterId: The service-generated identifier for the fraudster who was registered. In case the RegistrationStatus is DUPLICATE_SKIPPED, this is the identifier of the fraudster already in the domain that is the closest match to the given fraudster.
  - FraudsterSimilarityScore: An optional field that is populated when the fraudster registration is skipped due to it being a duplicate. This represents the similarity of the given fraudster with the closest matching fraudster already existing in the domain.

Amazon Connect Streams Voice ID APIs

Use the following Amazon Connect Streams APIs to integrate Voice ID into your existing agent web applications.

- enrollSpeakerInVoiceId: Enroll a customer to Voice ID after obtaining their consent to enroll.
- evaluateSpeakerWithVoiceId: Check the customer's Voice ID authentication status, and to detect fraudsters.
- optOutVoiceIdSpeaker: Opt out a customer from Voice ID.
- getVoiceIdSpeakerStatus: Describe the enrollment status of a customer.
- getVoiceIdSpeakerId: Get the SpeakerID for a customer.
- updateVoiceIdSpeakerId: Update the SpeakerID for a customer.

You can also use the Voice ID widget in the Contact Control Panel (CCP) if you don't want to build a custom agent interface. For more information about Voice ID in the CCP, see Use Voice ID (p. 1189).

Voice ID event schema

Voice ID generates events for every transaction: enrollment, authentication, or detection of fraudsters in a watchlist. Events are sent to the EventBridge default event bus.

You can create an analytics pipeline for Voice ID authentication outcomes and detection of fraudsters in a watchlist by using EventBridge to monitor Voice ID events. Using the schema available in this topic, you can configure EventBridge rules to listen and filter for Voice ID events that are relevant, and then process them through Amazon Kinesis Data Firehose to store in a data warehouse of your choice.

For example, you may want near real-time tracking of Voice ID analysis. To do that, you can pull all the `Evaluate-Session` events, and get the `authenticationResult` and `fraudDetectionResult`.

Events are emitted on a best effort basis.

Common fields in the event

- `version` - The version of the event data.
- `id` - A unique identifier of the event generated by EventBridge
- `detail-type` - An identifier for the details of the event.
- `source` - The source of the event. This is always `aws.voiceid`.
- `account` - AWS account ID.
- `timestamp` - The date and time that the event was published in UTC.
- `region` - The AWS Region where the API call was made.
- `resources` - Resources used by the API call.
- `detail` - Details about the event:
  - `detail.sourceId` - A unique ID generated by Voice ID that you can use for de-duplication.
  - `detail.action` - Analogous to the API being invoked.
  - `detail.status` - Specifies the status of the action: success or failure.
  - `detail.errorInfo` - Is populated when the specified action errors out at Voice ID.

Following are the schemas for the events are that emitted.

Start Session Action

Emits events on stream start (after setup), stream end, and on failures.

```
{...commonfields
    "detail-type": "VoiceId Start Session Action",
    "detail": {
        "sourceId": String,
        "action": "START_SESSION",
        "status": String,
        "domainId": String,
        "session": {
            "sessionId": String,
            "sessionName": String,
            "authenticationConfiguration": {
                "acceptanceThreshold":Integer
            },
            "fraudDetectionConfiguration": {
                "riskThreshold":Integer
            },
            "streamingConfiguration": {
                "authenticationMinimumSpeechInSeconds": Integer
            },
            "enrollmentAudioProgress": {
                "audioAggregationStatus": String,
                "audioAggregationStartedAt": "Timestamp",
                "audioAggregationEndedAt": "Timestamp"
            },
            "authenticationAudioProgress": {
                "audioAggregationStartedAt": "Timestamp",
                "audioAggregationEndedAt": "Timestamp"
            },
            "fraudDetectionAudioProgress": {
                "audioAggregationStartedAt": "Timestamp",
                "audioAggregationEndedAt": "Timestamp"
            },
            "generatedSpeakerId": String
        },
        "errorInfo": {
            "errorMessage": String,
            "errorType": String,
            "errorCode": Integer
       }
    }
}
```

Update Session Action

Emits events when the internal session update succeeds or fails.

```
{...commonfields
"detail-type": "VoiceId Update Session Action",
"detail": {
    "sourceId": String,
    "action": "UPDATE_SESSION",
    "status": String,
    "domainId": String,
    "session": {
        "sessionId": String,
        "sessionName": String,
        "authenticationConfiguration": {
            "acceptanceThreshold": Integer
        },
        "fraudDetectionConfiguration": {
            "riskThreshold": Integer
        },
        "streamingConfiguration": {
            "authenticationMinimumSpeechInSeconds": Integer
        },
        "generatedSpeakerId": String
    },
    "errorInfo": {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
    }
}
}
```

Evaluate Session Action

Emits events when the session evaluation succeeds or fails.

```
{...commonfields
"detail-type": "VoiceId Evaluate Session Action",
"detail": {
    "sourceId": String,
    "action": "EVALUATE_SESSION",
    "status": String,
    "domainId": String,
    "session": {
        "sessionId": String,
        "sessionName": String,
        "generatedSpeakerId": String,
        "streamingStatus": String,
        "authenticationResult": {
            "authenticationResultId": String,
            "decision": String,
            "score": Integer,
            "audioAggregationStartedAt": "Timestamp",
            "audioAggregationEndedAt": "Timestamp",
            "configuration": {
                "acceptanceThreshold": Integer
            }
        },
        "fraudDetectionResult": {
            "fraudDetectionResultId": String,
            "decision": String,
            "reasons": [String],
            "audioAggregationStartedAt": "Timestamp",
            "audioAggregationEndedAt": "Timestamp",
            "configuration":
                {"riskThreshold": Integer},
            "riskDetails":
                {"knownFraudsterRisk":
                    {"generatedFraudsterId": String,
                    "riskScore": Integer}
                 }
         }
     },
     "errorInfo": : {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
    }
}
}
```

Speaker Action

Emits events on the success or failure to opt out a speaker, delete a speaker, or enroll a speaker.

```
{...commonfields
"detail-type": "VoiceId Speaker Action",
"detail": {
    "sourceId": String,
    "domainID": String,
    "action": String,
    "status": String,
    "generatedSpeakerId": String,
    "data": {
        "enrollmentSource": String,
        "enrollmentSourceId": String,
        "enrollmentStatus": String},
    "errorInfo": {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
     }
}
}
```

Fraudster Action

Emits events on the success or failure to delete a fraudster or registering a fraudster.

```
{...commonfields
"detail-type": "VoiceId Fraudster Action",
"detail": {
    "sourceId": String,
    "domainID": String,
    "action": String,
    "status": String,
    "generatedFraudsterId": String,
    "data": {
        "registrationSource": String,
        "registrationSourceId": String,
        "registrationStatus": String
    },
    "errorInfo": {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
    }
}
}
```

EnrollBySession

Emits this event when an enrollment request is submitted. A `Speaker` event is emitted when the actual enrollment succeeds or fails.

```
{...commonfields
"detail-type": "VoiceId Session Speaker Enrollment Action",
"detail": {
    "sourceId": String,
    "domainId": String,
    "action": "SESSION_ENROLLMENT_REQUEST",
    "status": String,
    "sessionId": String,
    "sessionName": String,
    "errorInfo": {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
    }
}
}
```

StartSpeakerEnrollmentJob

Emits this event when a batch enrollment request is submitted, succeeds, or fails. A `Speaker` event is emitted for each of the individual speakers to indicate if corresponding enrollment succeeds or fails.

```
{...commonfields
"detail-type": "VoiceID Batch Speaker Enrollment Action",
"detail": {
    "sourceId": String,
    "domainId": String,
    "action": "BATCH_ENROLLMENT_REQUEST",
    "status": String,
    "batchJobId": String,
    "data": {
        "dataAccessRoleArn": String,
        "enrollmentConfig": {
            "existingEnrollmentAction": String,
            "fraudDetectionConfig": {
            "fraudDetectionAction": String,
            "riskThreshold": Integer
            }
        },
        "inputDataConfig": {
            "s3Uri": String
         },
        "outputDataConfig": {
            "s3Uri": String,
            "kmsKeyId": String
        }
    },
    "errorInfo": {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
    }
}
}
```

StartFraudsterRegistrationJob

Emits this event when a batch registration request is submitted, succeeds, or fails. A `Fraudster` event is emitted for each of the individual fraudsters to indicate if corresponding registration succeeds or fails.

```
{...commonfields
"detail-type": "VoiceId Batch Fraudster Registration Action",
"detail": {
    "sourceId": String,
    "domainId": String,
    "action": "BATCH_REGISTRATION_REQUEST",
    "status": String,
    "batchJobId": String,
    "data": {
        "dataAccessRoleArn": String,
        "registrationConfig": {
            "duplicateRegistrationAction": String,
            "fraudsterSimilarityThreshold": Integer
        }
        "inputDataConfig": {
            "s3Uri": String
        },
        "outputDataConfig": {
            "s3Uri": String,
            "kmsKeyId": String
        }
    },
    "errorInfo": {
        "errorMessage": String,
        "errorType": String,
        "errorCode": Integer
    }
}
}
```

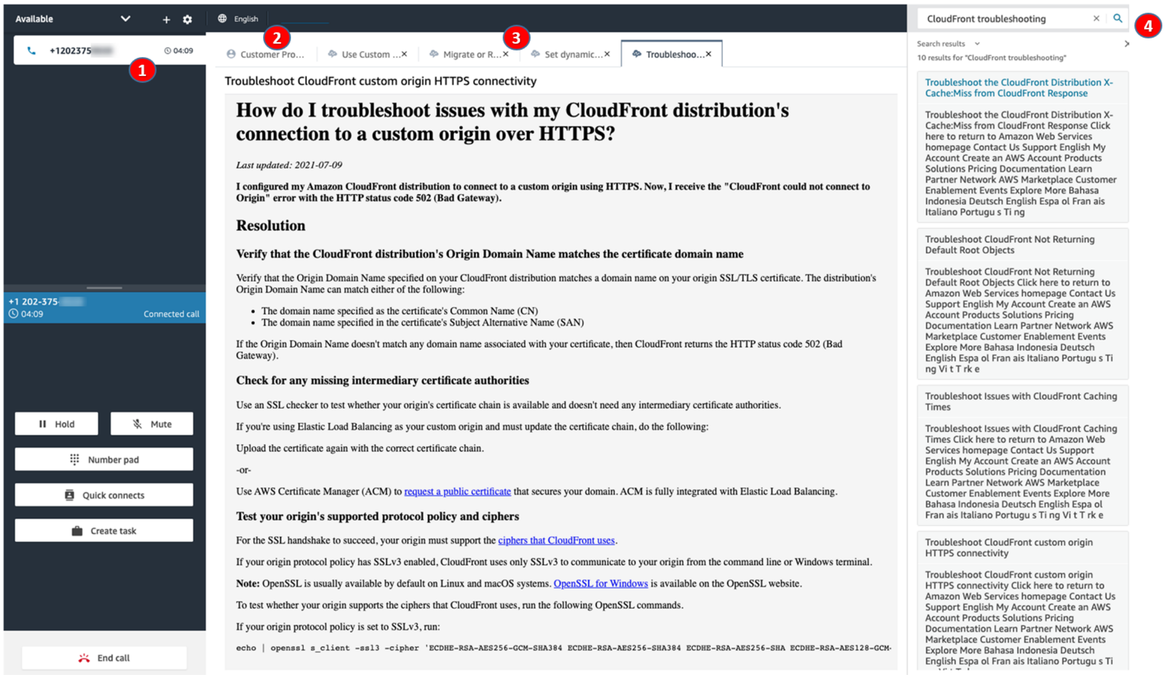
Deliver information to agents using Amazon Connect Wisdom

With Amazon Connect Wisdom, agents can search and find content across multiple repositories, such as frequently asked questions (FAQs), wikis, articles, and step-by-step instructions for handling different customer issues. They can type questions or phrases in a search box (such as, "how long after purchase can handbags be exchanged?") without having to guess which keywords will work.

If your organization uses real-time analytics from Contact Lens for Amazon Connect to automatically detect customer issues during calls, then Wisdom can proactively recommend information to help resolve the issue. For example, Contact Lens can detect phrases such as "product broke during shipping" and then display text snippets, FAQs, and instructions for exchanging damaged products.

Currently, Amazon Connect Wisdom can be used in compliance with GDPR and is pending additional certifications held by Amazon Connect.

The following image shows how an article may appear in the agent application when the agent is on a call.



Troubleshoot CloudFront custom origin HTTPS connectivity

How do I troubleshoot issues with my CloudFront distribution's connection to a custom origin over HTTPS?

Last updated: 2021-07-09

I configured my Amazon CloudFront distribution to connect to a custom origin using HTTPS. Now, I receive the "CloudFront could not connect to Origin" error with the HTTP status code 502 (Bad Gateway).

Resolution

Verify that the CloudFront distribution's Origin Domain Name matches the certificate domain name

Verify that the Origin Domain Name specified on your CloudFront distribution matches a domain name on your origin SSL/TLS certificate. The distribution's Origin Domain Name can match either of the following:

- The domain name specified as the certificate's Common Name (CN)
- The domain name specified in the certificate's Subject Alternative Name (SAN)

If the Origin Domain Name doesn't match any domain name associated with your certificate, then CloudFront returns the HTTP status code 502 (Bad Gateway).

Check for any missing intermediary certificate authorities

Use an SSL checker to test whether your origin's certificate chain is available and doesn't need any intermediary certificate authorities.

If you're using Elastic Load Balancing as your custom origin and must update the certificate chain, do the following:

Upload the certificate again with the correct certificate chain.

-or-

Use AWS Certificate Manager (ACM) to request a public certificate that secures your domain. ACM is fully integrated with Elastic Load Balancing.

Test your origin's supported protocol policy and ciphers

For the SSL handshake to succeed, your origin must support the ciphers that CloudFront uses.

If your origin protocol policy has SSLv3 enabled, CloudFront uses only SSLv3 to communicate to your origin from the command line or Windows terminal.

Note: OpenSSL is usually available by default on Linux and macOS systems. OpenSSL for Windows is available on the OpenSSL website.

To test whether your origin supports the ciphers that CloudFront uses, run the following OpenSSL commands.

If your origin protocol policy is set to SSLv3, run:

```
echo | openssl s_client -ssl3 -cipher 'ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-GCM-
```

10 results for "CloudFront troubleshooting"

Troubleshoot the CloudFront Distribution X-Cache:Miss from CloudFront Response

Troubleshoot the CloudFront Distribution X-Cache:Miss from CloudFront Response Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti ng

Troubleshoot CloudFront Not Returning Default Root Objects

Troubleshoot CloudFront Not Returning Default Root Objects Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti ng Vi t T rk e

Troubleshoot Issues with CloudFront Caching Times

Troubleshoot Issues with CloudFront Caching Times Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti ng Vi t T rk e

Troubleshoot CloudFront custom origin HTTPS connectivity

Troubleshoot CloudFront custom origin HTTPS connectivity Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti

1. The agent is on a call.
2. The Customer profile tab is available.
3. The agent can have multiple articles open at the same time.
4. The agent can search for articles.

Enable Amazon Connect Wisdom for your instance

There are two ways you can enable Wisdom for your instance:

- Use the new (p. 1230) Amazon Connect console. There are instructions on this page.
- Use the Amazon Connect Wisdom API. You can ingest content using the Amazon Connect Wisdom APIs. To learn more, see this blog post: Ingesting content to power real-time recommendations and search with Amazon Connect Wisdom.

  The APIs support the ingestion of HTML and text; plain text files must be in UTF-8. For more information, see the Amazon Connect Wisdom API Reference.

Following is an overview of the steps to enable Wisdom:

1. Create a Wisdom Assistant (domain). An Assistant is made up of one knowledge base.
2. Create an encryption key to encrypt the excerpt that is provided in the recommendations to the agent.
3. Create a knowledge base using external data:
   - Add data integrations from Salesforce and ServiceNow using prebuilt connectors in the Amazon Connect console.
   - Encrypt the content importing from these applications using a KMS key.
   - Specify the sync frequency.

Before you begin

Following is an overview of key concepts and the information that you'll be prompted for during the setup process.

About the Wisdom domain

When you enable Amazon Connect Wisdom, you create a Wisdom domain: an Assistant that is made up of one knowledge base. Following are guidelines for creating Wisdom domains:

- You can create multiple domains, but they don't share external application integrations or customer data between each other.
- Each domain can be associated with one or more Amazon Connect instances, but each Amazon Connect instance can be associated with only one domain.
- All the external application integrations you create are at a domain level. All of the Amazon Connect instances associated with a domain inherit the domain's integrations.
- You can change the association of your Amazon Connect instance from your current domain to a new domain at any time, by choosing a different domain.

How do you want to name your Wisdom domain?

When you enable Wisdom, you are prompted to provide a friendly domain name that's meaningful to you such as your organization name, for example, *Wisdom-ExampleCorp*.

Create AWS KMS keys to encrypt the domain and the connection

When you enable Wisdom, by default the domain and connection are encrypted with an AWS owned key. However, you have the option to create or provide two AWS KMS keys:

1. One for the Wisdom domain, used to encrypt the excerpt provided in the recommendations.

2. Another to encrypt the content imported from Salesforce and ServiceNow. Note that Wisdom search indices are always encrypted at rest using an AWS owned key.

Step-by-step instructions for creating these KMS keys are provided in Step 1: Add integration (p. 883).

Your customer managed key is created, owned, and managed by you. You have full control over the KMS key (AWS KMS charges apply).

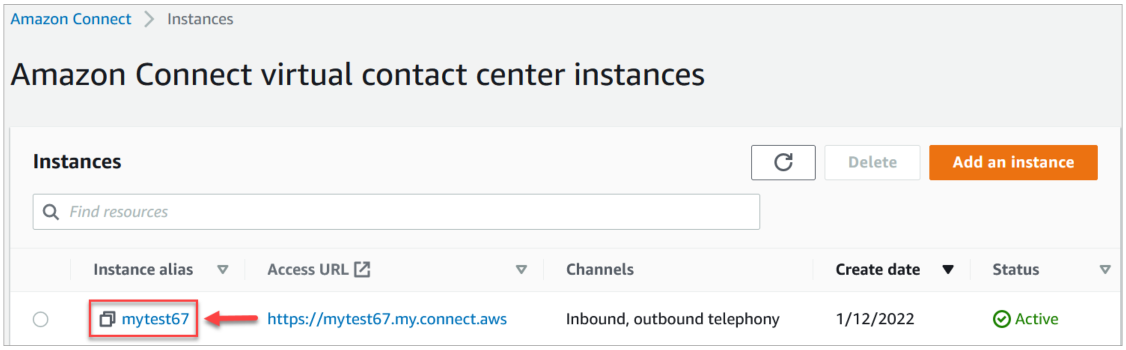
If you choose to set up a KMS key where someone else is the administrator, the key must have a policy that allows `kms:CreateGrant` and `kms:DescribeKey` permissions to the IAM identity using the key to invoke Wisdom. For information about how to change a key policy, see Changing a key policy in the AWS Key Management Service Developer Guide.

> **Tip**
> You can create KMS keys or provide an existing KMS key programmatically. For more information, see

Step 1: Add integration

Following are instructions for how to create a new domain and add an integration.

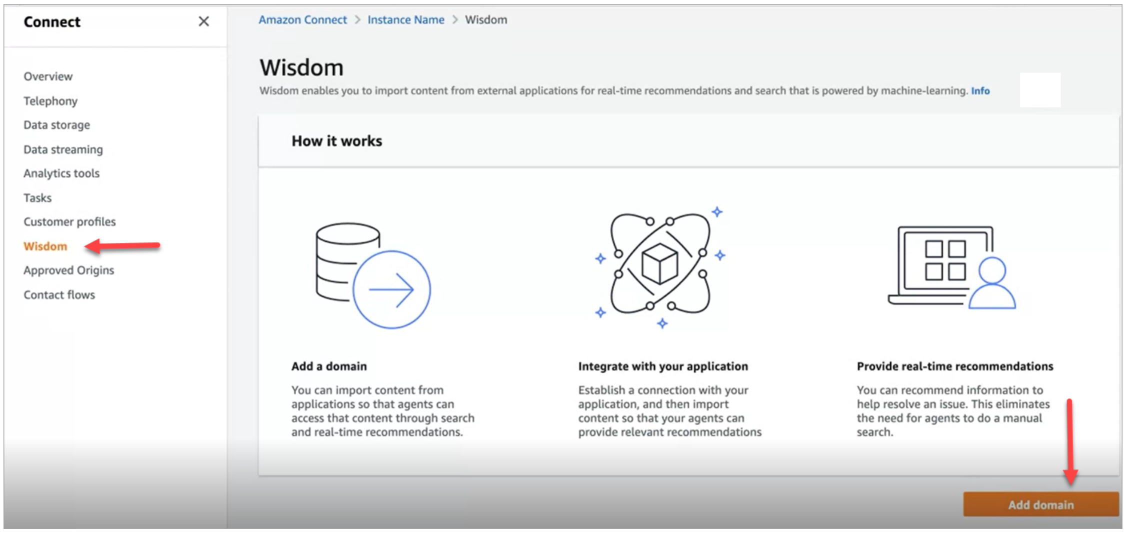
1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



Amazon Connect > Instances
Amazon Connect virtual contact center instances
Instances
Delete
Add an instance
Find resources

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Wisdom**, and then choose **Add domain**.



Wisdom enables you to import content from external applications for real-time recommendations and search that is powered by machine-learning.

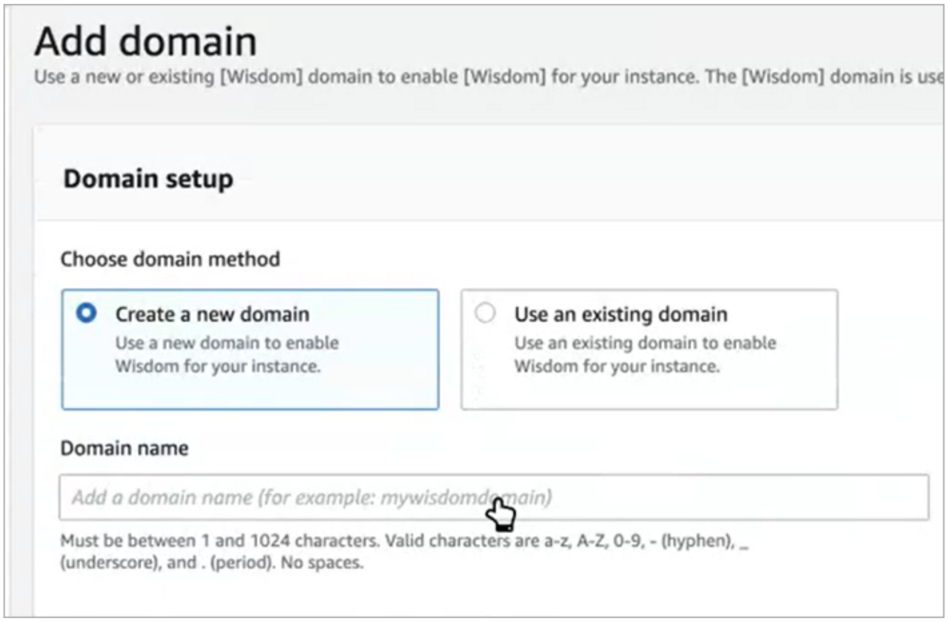
Add a domain
You can import content from applications so that agents can access that content through search and real-time recommendations.

Integrate with your application
Establish a connection with your application, and then import content so that your agents can provide relevant recommendations

Provide real-time recommendations
You can recommend information to help resolve an issue. This eliminates the need for agents to do a manual search.

4. On the **Add domain** page, choose **Create a domain**.

5. In the **Domain name** box, enter a friendly name that's meaningful to you, such as your organization name, for example, *Wisdom-ExampleCorp*.



Add domain

Use a new or existing [Wisdom] domain to enable [Wisdom] for your instance. The [Wisdom] domain is use

Domain setup

Choose domain method

● Create a new domain
Use a new domain to enable Wisdom for your instance.

○ Use an existing domain
Use an existing domain to enable Wisdom for your instance.

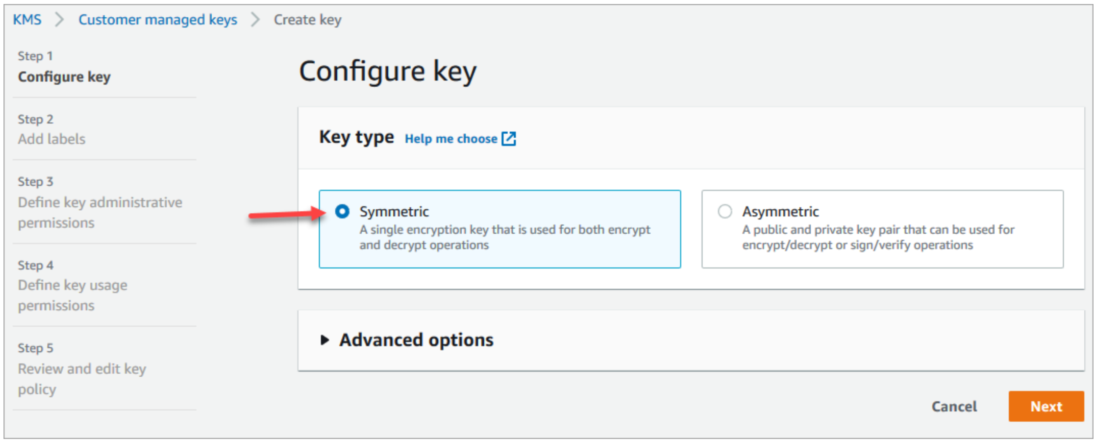
Domain name

Add a domain name (for example: mywisdomdomain)

Must be between 1 and 1024 characters. Valid characters are a-z, A-Z, 0-9, - (hyphen), _ (underscore), and . (period). No spaces.

6. Under **Encryption**, create or enter your own AWS KMS key for encrypting your Wisdom domain. Following are the steps to create your KMS key:

   1. On the **Add domain** page, choose **Create an AWS KMS key**.
   2. A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review and edit key policy

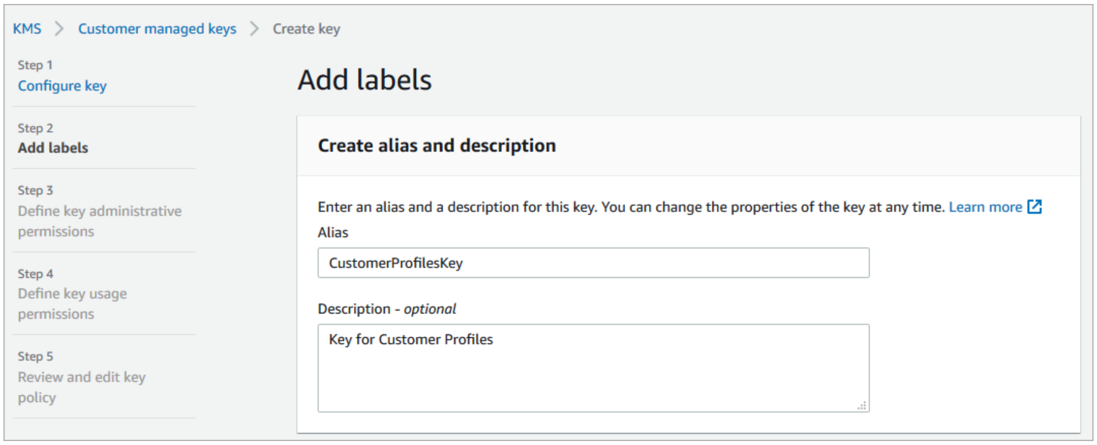
Configure key

Key type Help me choose

● Symmetric
A single encryption key that is used for both encrypt and decrypt operations

○ Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

   3. On the **Add labels** page, add a name and description for the KMS key, and then choose **Next**.


KMS > Customer managed keys > Create key
Step 1
Configure key
Step 2
Add labels
Step 3
Define key administrative permissions
Step 4
Define key usage permissions
Step 5
Review and edit key policy

Add labels

Create alias and description

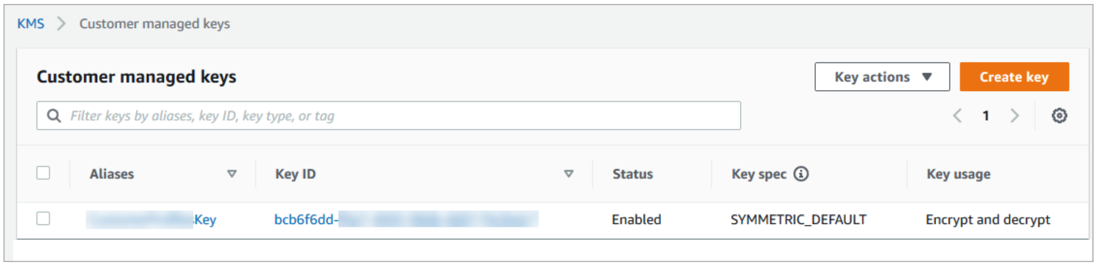
Enter an alias and a description for this key. You can change the properties of the key at any time. Learn more

Alias: CustomerProfilesKey

Description - *optional*: Key for Customer Profiles

4. On the **Define key administrative permissions** page, choose **Next**.
5. On the **Define key usage permissions** page, choose **Next**.
6. On the **Review and edit key policy** page, choose **Finish**.

   In the following example, the name of the KMS key starts with **bcb6fdd**:

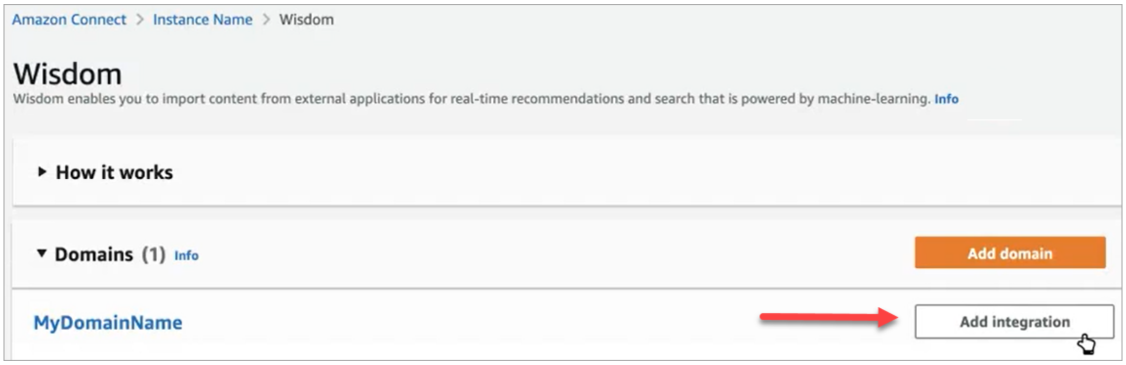

KMS > Customer managed keys
Customer managed keys
Key actions ▼
Create key
Filter keys by aliases, key ID, key type, or tag
1

□	Aliases	Key ID	Status	Key spec	Key usage
□	[redacted]Key	bcb6f6dd-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

7. Return to the tab in your browser for the Amazon Connect console, **Wisdom** page. Click or tap in the **AWS KMS key** for the key you created to appear in a dropdown list. Choose the key you created.

7. Choose **Add domain**.

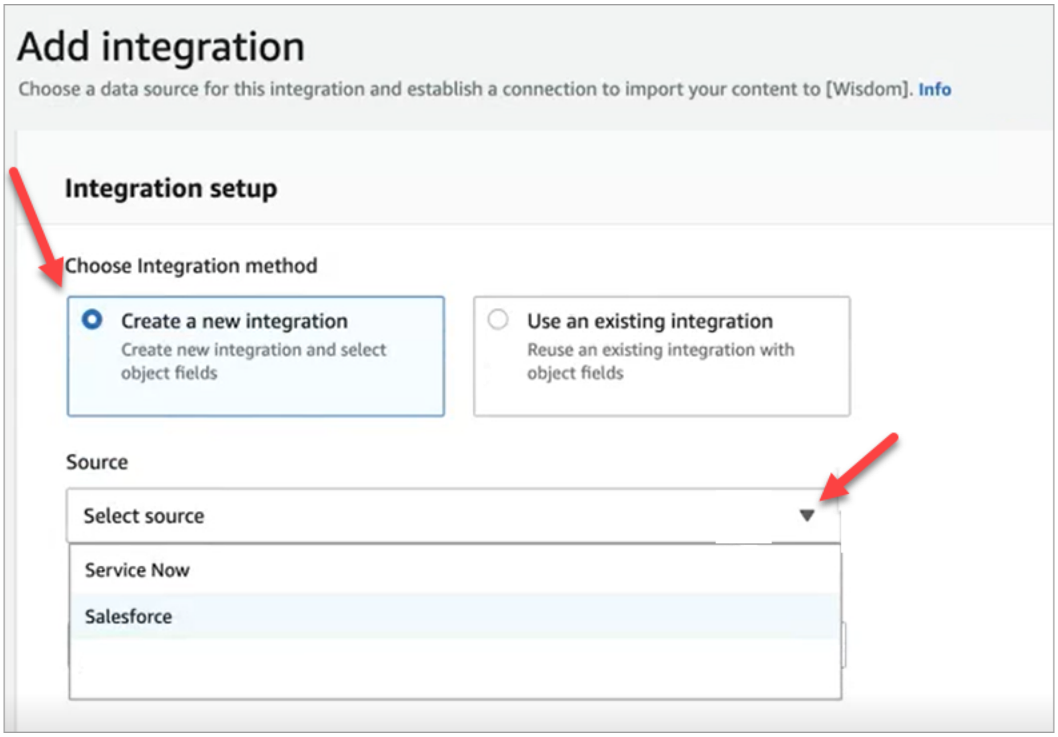
8. On the **Wisdom** page, choose **Add integration**.



Wisdom

Wisdom enables you to import content from external applications for real-time recommendations and search that is powered by machine-learning. Info

9. On the **Add integration** page, choose **Create a new integration**, and then select the source.



Add integration

Choose a data source for this integration and establish a connection to import your content to [Wisdom]. Info

Integration setup

Choose Integration method

● Create a new integration
Create new integration and select object fields

○ Use an existing integration
Reuse an existing integration with object fields

Source

Select source ▼

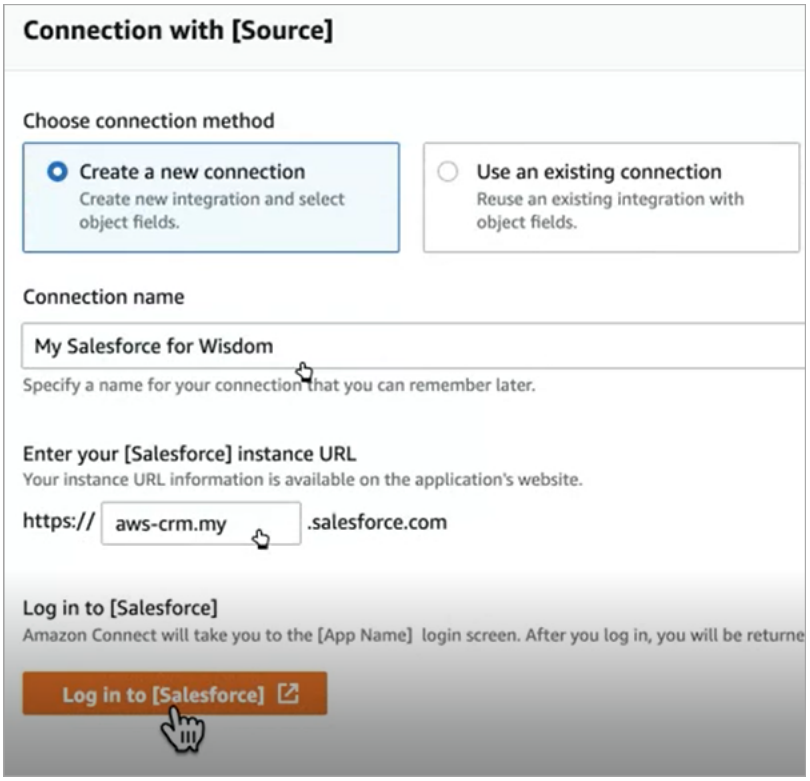
Service Now

Salesforce

10. In the **Integration name** box, assign a friendly name to the integration, one that is meaningful to you.

    Tip
    If you are going to have multiple integrations from the same source, we recommend you develop a naming convention to make them easy to distinguish.

11. Under **Connection with [Source]**, choose **Create a new connection**, and then enter a friendly name for the connection that is meaningful to you.
12. Enter the instance URL of the source you want to connect to, and then choose **Log in to [Source]**.



Connection with [Source]

Choose connection method

● Create a new connection
Create new integration and select object fields.

○ Use an existing connection
Reuse an existing integration with object fields.

Connection name

My Salesforce for Wisdom

Specify a name for your connection that you can remember later.

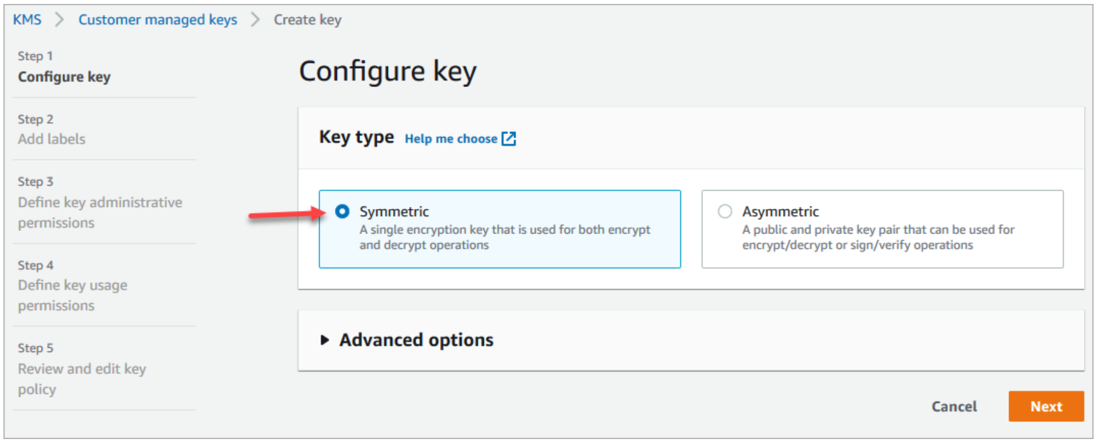
Enter your [Salesforce] instance URL
Your instance URL information is available on the application's website.

https:// aws-crm.my .salesforce.com

Log in to [Salesforce]
Amazon Connect will take you to the [App Name] login screen. After you log in, you will be returne

13. Under **Encryption**, choose **Create an AWS KMS key**. This key encrypts the connection to the external application that stores content. Following are the steps to create your KMS key:

    1. On the **Add domain** page, choose **Create an AWS KMS key**.
    2. A new tab in your browser opens for the Key Management Service (KMS) console. On the **Configure key** page, choose **Symmetric**, and then choose **Next**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review and edit key policy

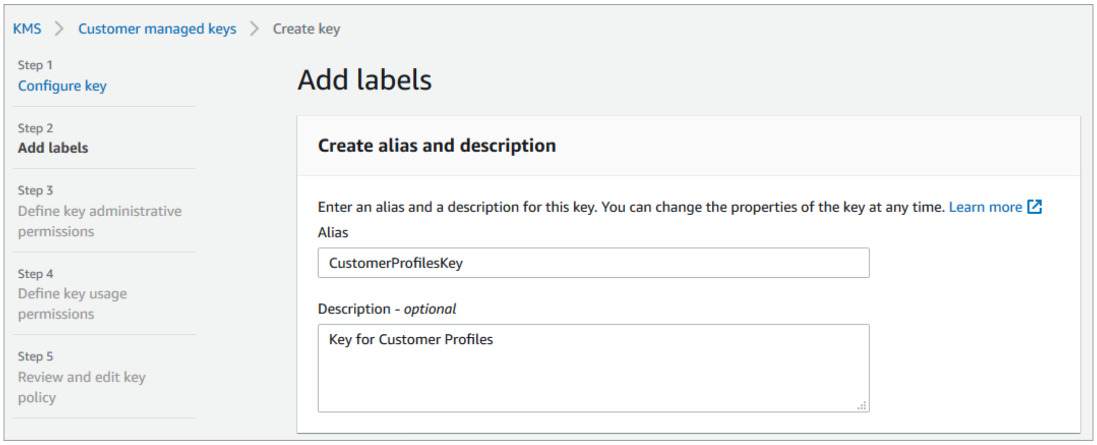
Configure key

Key type Help me choose

● Symmetric
A single encryption key that is used for both encrypt and decrypt operations

○ Asymmetric
A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

    3. On the **Add labels** page, add a name and description for the KMS key, and then choose **Next**.



KMS > Customer managed keys > Create key

Step 1
Configure key

Step 2
Add labels

Step 3
Define key administrative permissions

Step 4
Define key usage permissions

Step 5
Review and edit key policy

Add labels

Create alias and description

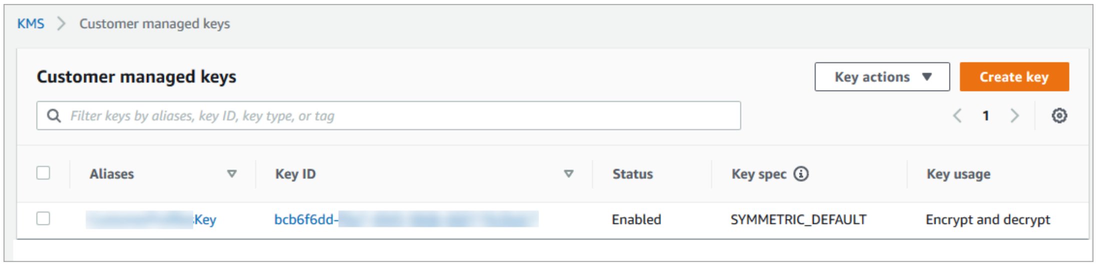
Enter an alias and a description for this key. You can change the properties of the key at any time. Learn more

Alias: CustomerProfilesKey

Description - *optional*: Key for Customer Profiles

4. On the **Define key administrative permissions** page, choose **Next**.
5. On the **Define key usage permissions** page, choose **Next**.
6. On the **Review and edit key policy** page, choose **Finish**.

   In the following example, the name of the KMS key starts with **bcb6fdd**:

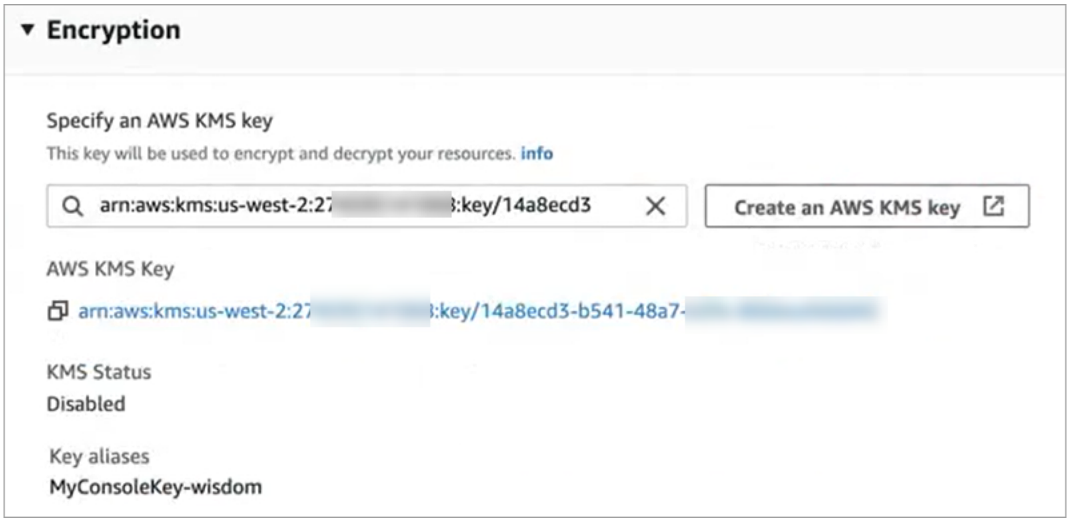
   

   KMS > Customer managed keys

   Customer managed keys

□	Aliases	Key ID	Status	Key spec	Key usage
□	[redacted]Key	bcb6f6dd-[redacted]	Enabled	SYMMETRIC_DEFAULT	Encrypt and decrypt

7. Return to the tab in your browser for the Amazon Connect console, **Wisdom** page. Click or tap in the **AWS KMS key** for the key you created to appear in a dropdown list. Choose the key you created.

   ▼ **Encryption**

   Specify an AWS KMS key

   This key will be used to encrypt and decrypt your resources. info

   arn:aws:kms:us-west-2:27[redacted]3:key/14a8ecd3

   AWS KMS Key

   arn:aws:kms:us-west-2:27[redacted]3:key/14a8ecd3-b541-48a7-[redacted]

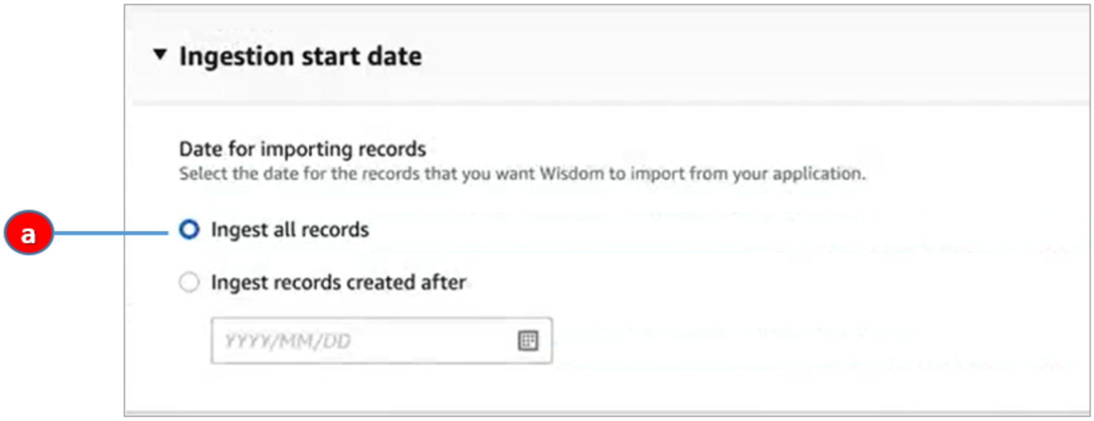
   KMS Status

   Disabled

   Key aliases

   MyConsoleKey-wisdom

14. Under **Ingestion start date**, choose when you want Wisdom to import records from your application, and how often.


▾ Ingestion start date

Date for importing records
Select the date for the records that you want Wisdom to import from your application.

● Ingest all records

○ Ingest records created after

YYYY/MM/DD

1. Defaults to the earliest date possible.

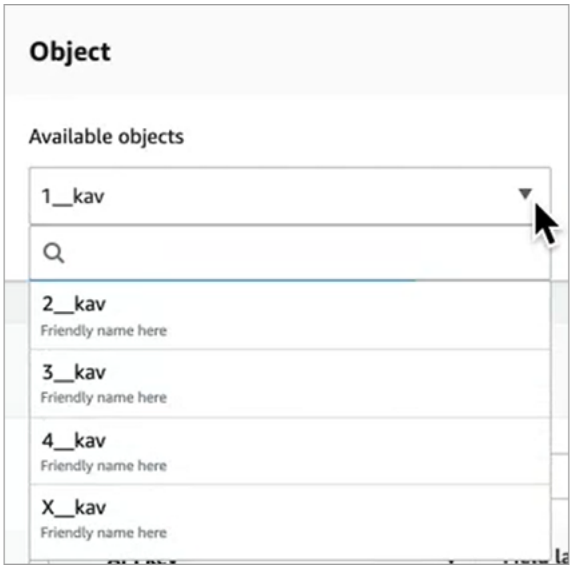
15. Under **Sync frequency**, the default is hourly. You can use the dropdown to choose **Every 3 hours** or **Daily**. On-demand syncing is not available.
16. Choose **Next**.

Note
Currently Wisdom does not process hard deletes of objects that are completed in SaaS applications. To remove content from your knowledge base that's also been removed from your SaaS application, you must archive objects in Salesforce and retire articles in ServiceNow.
For Zendesk, Wisdom does not process hard deletes or archives of articles. You need to unpublish articles in Zendesk to remove them from your knowledge base.

Step 2: Select object and fields

In this step you choose the object and fields from the source that you want to make available to your agents in Wisdom.

1. In the **Available objects** dropdown menu, choose the object you want. Only knowledge objects appear in the menu.


Object

Available objects

1__kav ▾

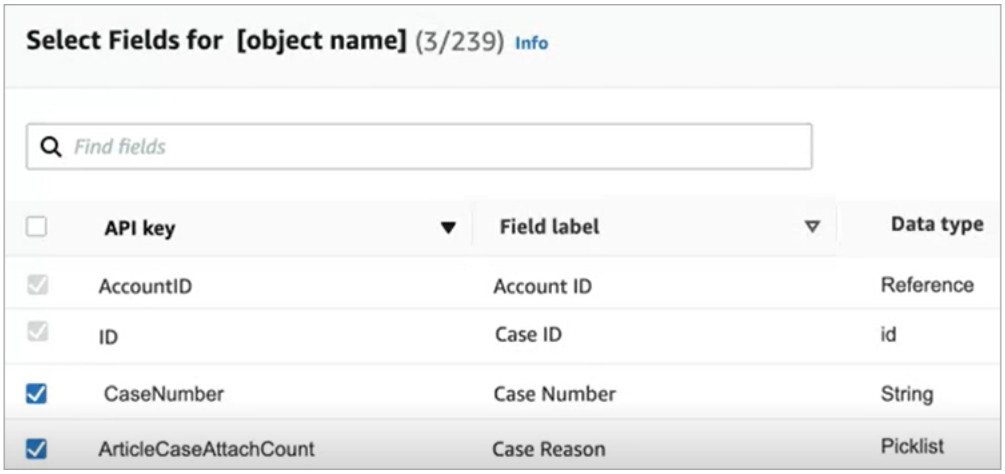
2__kav
Friendly name here

3__kav
Friendly name here

4__kav
Friendly name here

X__kav
Friendly name here

2. Under **Select Fields for [object name]**, choose the fields you want to include. You'll notice that some fields, such as **AccountID** and **ID**, are already selected by default. These fields are required.



Select Fields for [object name] (3/239) Info

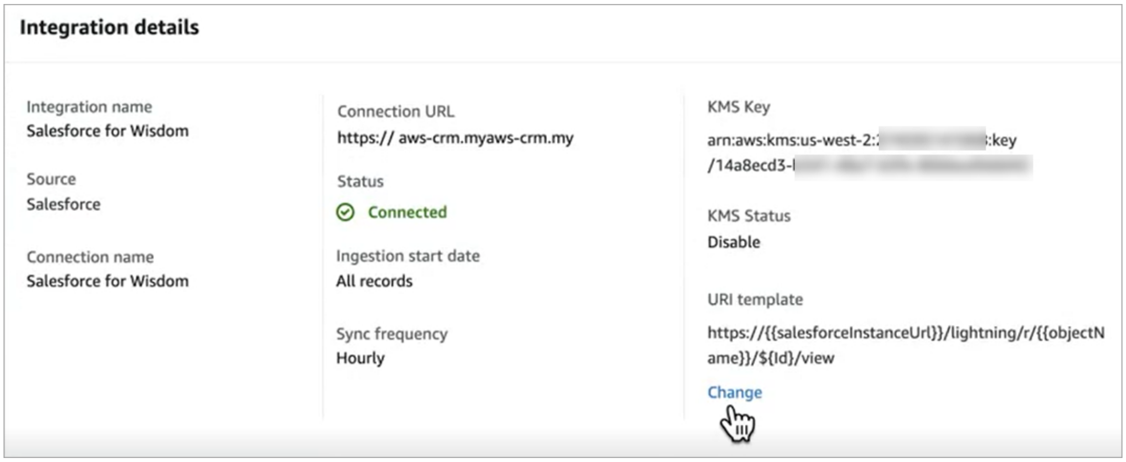
Find fields

□	API key ▼	Field label ▽	Data type
☑	AccountID	Account ID	Reference
☑	ID	Case ID	id
☑	CaseNumber	Case Number	String
☑	ArticleCaseAttachCount	Case Reason	Picklist

3. Choose **Next**.

Step 3: Review and integrate

1. Review all the integration details.



Integration details

Integration name
Salesforce for Wisdom

Source
Salesforce

Connection name
Salesforce for Wisdom

Connection URL
https:// aws-crm.myaws-crm.my

Status
✓ Connected

Ingestion start date
All records

Sync frequency
Hourly

KMS Key
arn:aws:kms:us-west-2:[redacted]:key
/14a8ecd3-[redacted]

KMS Status
Disable

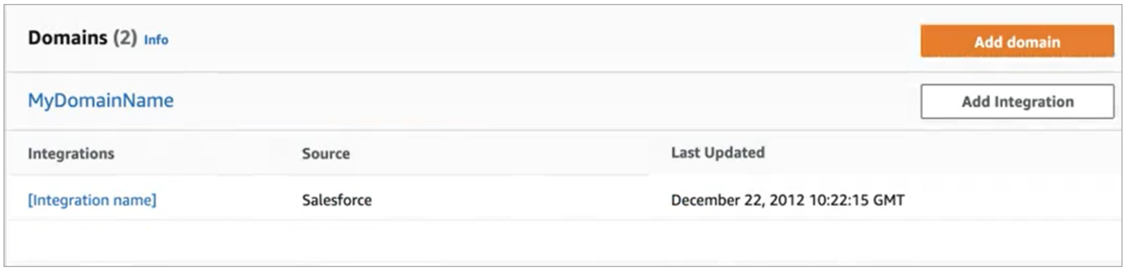
URI template
https://{{salesforceInstanceUrl}}/lightning/r/{{objectName}}/${Id}/view

Change

> **Note**
> The URI template is based on your version of Salesforce (such as Lightning), and the object you chose. You may want to change it if, for example, you're on a different version of Salesforce, or you have a connector that has a different desktop client.

2. Choose **Add integration**.

3. The integration is added to your list, as shown in the following example.



Domains (2) Info

MyDomainName

Integrations	Source	Last Updated
[Integration name]	Salesforce	December 22, 2012 10:22:15 GMT

4. After an integration is created, you can edit the URI, but no other information.

Step 4: Add a Wisdom block to your contact flow

By adding a Wisdom (p. 443) block to your contact flow, you associate a Wisdom domain to the current contact. This enables you to display information from a specific domain, based on criteria about the contact.

> **Note**
> Amazon Connect Wisdom, along with Contact Lens Real-Time analytics, is used to recommend content that is related to customer issues detected during the current contact. The Set recording and analytics behavior (p. 408) block with Contact Lens real-time enabled must also be set in this flow for Wisdom recommendations to work. It doesn't matter where in the flow you add Set recording and analytics behavior (p. 408).

When was your knowledge base last updated?

To confirm the last date and time that your knowledge base was updated (meaning a change in the content available), use the GetKnowledgeBase API to reference `lastContentModificationTime`.

Security profile permissions for Wisdom

Assign the following **Agent Applications** permission to the agent's security profile:

- **Wisdom - Access**: Enables agents to search for and view content. They can also receive automatic recommendations if Contact Lens is enabled.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

By default, the **Admin** security profile already has permissions to perform all Wisdom activities.

Access Wisdom in the agent application

If you're using the CCP that is provided with Amazon Connect, after you enable Wisdom, share the following URL with your agents so they can access it:

- **https://*instance name*.my.connect.aws/agent-app-v2/**

If you access your instance using the **awsapps.com** domain, use the following URL:

- **https://*instance name*.awsapps.com/connect/agent-app-v2/**

For help finding your instance name, see Find your Amazon Connect instance name (p. 139).

By using the new URL, your agents can view the CCP and Wisdom in the same browser window.

If CCP is embedded in your agent's application, see Initialization for CCP, Customer Profiles, and Wisdom in the *Amazon Connect Streams Documentation* for information about how to include Wisdom.

For more information about the agent's experience using Wisdom, see Search for content using Amazon Connect Wisdom (p. 1188).

Monitor metrics and run reports

In Amazon Connect, data about contacts are captured in contact records. This data can include the amount of time a contact spends in each state: customer on hold, customer in queue, agent interaction time.

The basis for most historical and real-time metrics in Amazon Connect is the data in the contact record. When you create metrics reports, the values displayed for **most** (not all) metrics in the report are calculated using the data in the contact records.

Contact records are available within your instance for 24 months from the time when the associated contact was initiated. You can also stream contact records to Amazon Kinesis to retain the data longer, and perform advanced analysis on it.

> **Tip**
> For detailed information about the activity of agents in your contact center, use Amazon Connect agent event streams (p. 965).

Contents

What's new in metrics

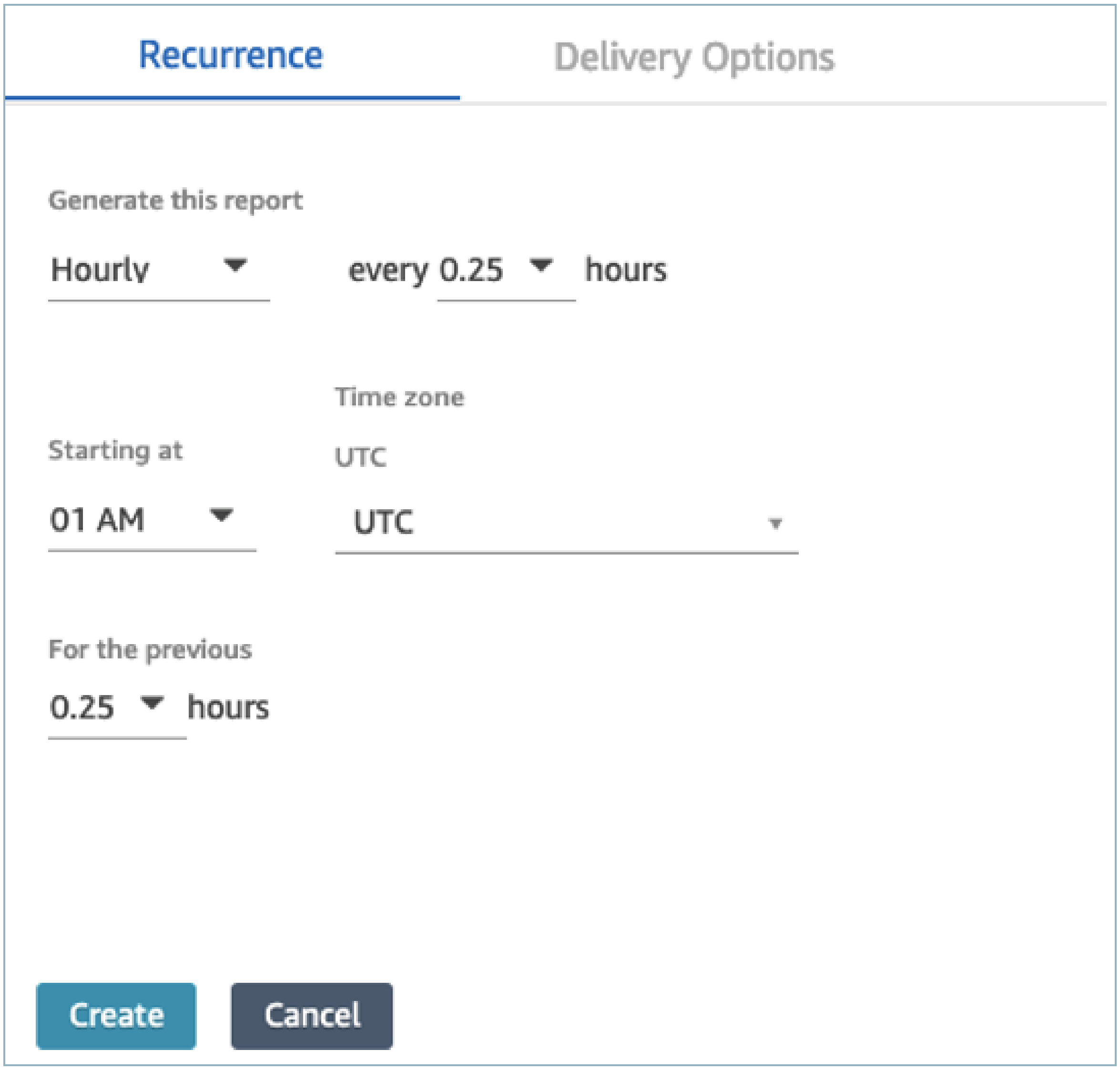
Thanks to your feedback, we've made changes to Amazon Connect metrics. This topic gives you an overview of the improvements.

June 2022

The following updates were released in June 2022.

15 minute scheduled reports

You can now schedule historical metrics to refresh every 15 minutes. To select 15-minute schedules, select generate this report **Hourly** every .25 hours (this is the top most option in the second dropdown), for the previous .25 hours. The following image shows the values that you need to select.



Generate this report
Hourly every 0.25 hours

Starting at
01 AM

Time zone
UTC
UTC

For the previous
0.25 hours

Filter Real-Time Metrics Agent Table by Agent

You can now filter the agent table on the Real-Time Metrics page by agent. This filter functions the same as the existing queues, routing profiles, and agent hierarchy filters.

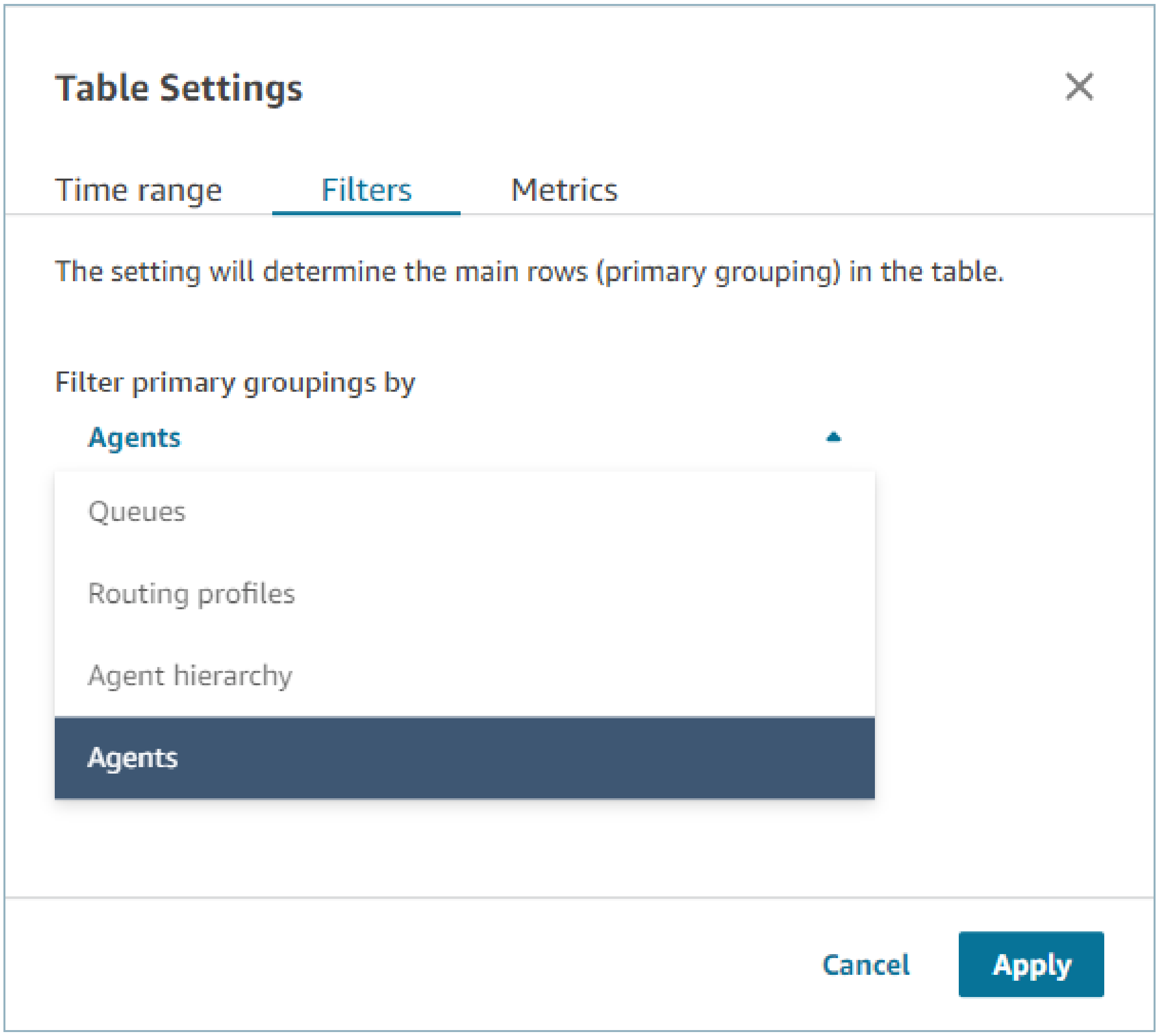


Table Settings

Time range | Filters | Metrics

The setting will determine the main rows (primary grouping) in the table.

Filter primary groupings by

Agents

- Queues
- Routing profiles
- Agent hierarchy
- Agents

New contact transferred related metrics

We are upgrading the existing Contacts transferred in (p. 948) and Contacts transferred out (p. 949) historical metrics to have consistent definitions. We are adding Contacts transferred in by agent (p. 948) and Contacts transferred out by agent (p. 949) for more granular contact transferred related metrics.

Changes to real-time metrics agent tables

We are rolling out a new service to maintain the high availability from metrics that you expect from Amazon Connect. Due to this change, the agent tables will now be sorted by availability status by default, rather than by agent login.

Additionally, the queues and routing profiles table will sort by agents online by default instead of queue or routing profile name.

Faster reload times for the Real-time metrics page

We are upgrading the performance of the **Real-time metrics** page so reload times are faster. The page will have the same functionality and user experience as the existing **Real-time metrics** page.

April 2021

The following updates were released in April 2021.

- Amazon Connect incorrectly reported that chat contacts that were created from disconnect flows were created from transfer flows.
- With these fixes, Amazon Connect correctly reflects in the contact records and agent event stream that these chat contacts were created from disconnect flows.

There is no impact to voice or task contacts.

Chat contacts created through disconnect flows no longer increment the following metrics:

- Contact flow time (p. 945)
- Contacts incoming (p. 947)
- Contacts handled incoming (p. 946)
- Contacts transferred in (p. 948)

In addition, note the following fixes for contact records and the agent event stream for chat contacts:

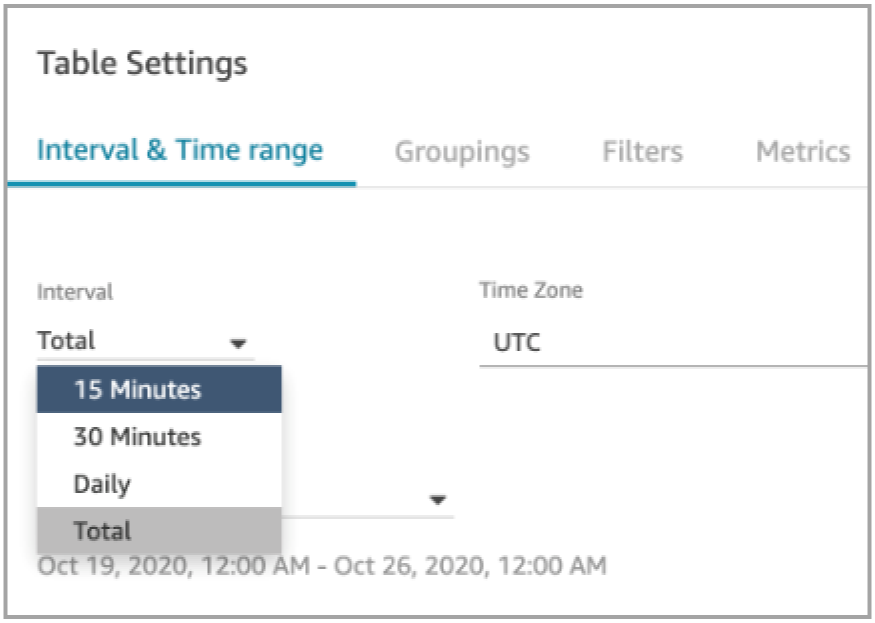
- Contact records: There was an issue in the **Attributes** section of a chat contact record where the initiation method is **API** for both disconnect and transfer contacts. With this fix, the initiation method correctly reflect **Disconnect** and **Transfer**, respectively.
- Agent event stream: Chat contacts created from disconnect flows now have **Disconnect** as the initiation method.

March 2021

The following updates were released in March 2021.

When customizing a historical metrics report, you have the option to select a 15 minutes interval, in addition to the current option of a 30 minutes interval.

The 15 minutes interval works the same as the 30 minutes interval. For example, you can query up to three days of data at a time, for the past 35 days.



February 2021

The following updates were released in February 2021.

New metric groupings and categories

With the release of custom service level metrics (p. 899), we also made the following changes:

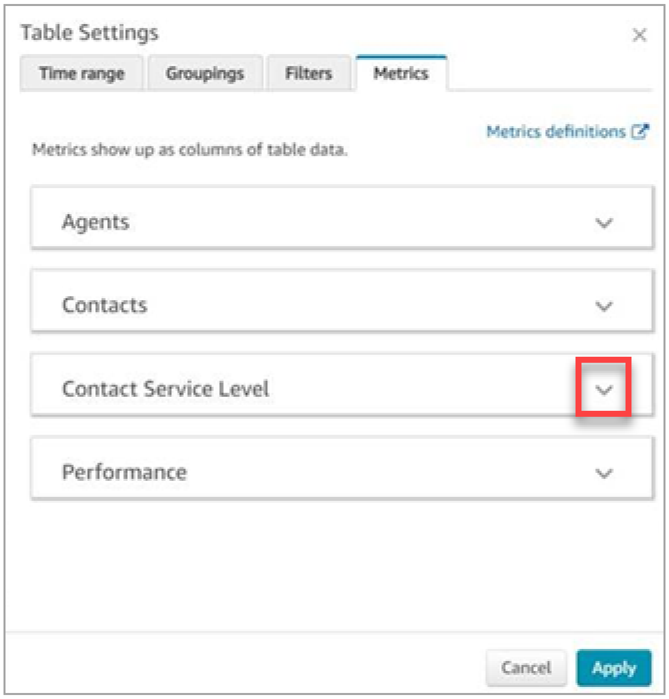
- On the **Table settings** pages, pre-set and custom service level metrics (p. 899) are in a new group called **Contact Service Levels**.
- Historical metrics on the **Table settings** page are grouped into categories.
- The order of metric columns on historical metrics reports changed to match the order of the metrics on the **Table settings** page.

Following is more information about these changes.

Real-time metrics: New Contact Service Level category

A new category of metrics appears on the **Table settings** page: **Contact Service Level**.

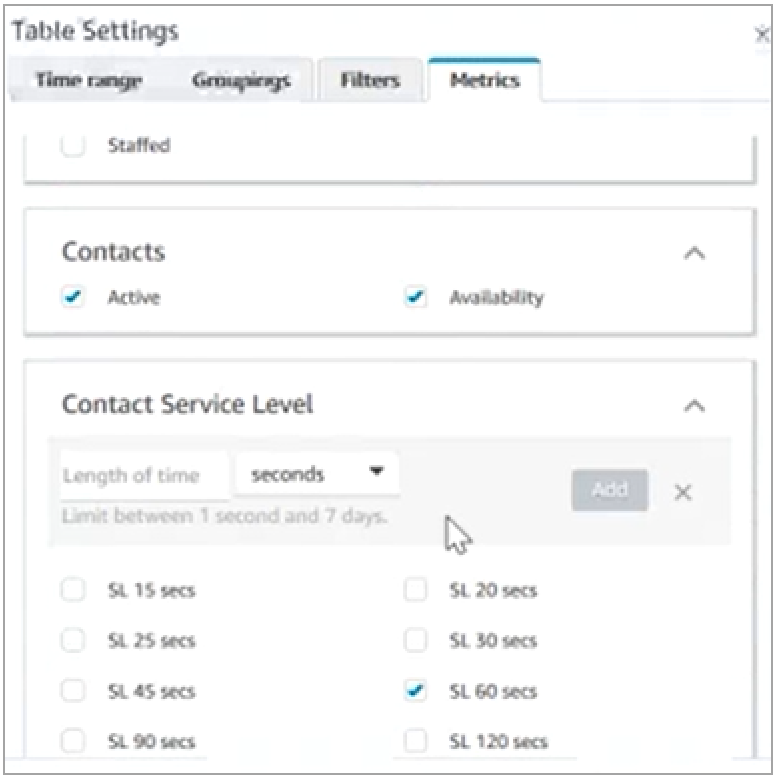
The following image shows this new category on the **Table settings** page, in an expandable group. Choose the arrow next to the group to view and select the metrics you want to add to your report.



Metrics show up as columns of table data.

Use the **Contact Service Level** category to choose pre-set service level metrics, and to create custom service level metrics.

The following image shows the user interface for creating custom service level metrics.



□ Staffed

☑ Active ☑ Availability

Limit between 1 second and 7 days.

□ SL 15 secs □ SL 20 secs

□ SL 25 secs □ SL 30 secs

□ SL 45 secs ☑ SL 60 secs

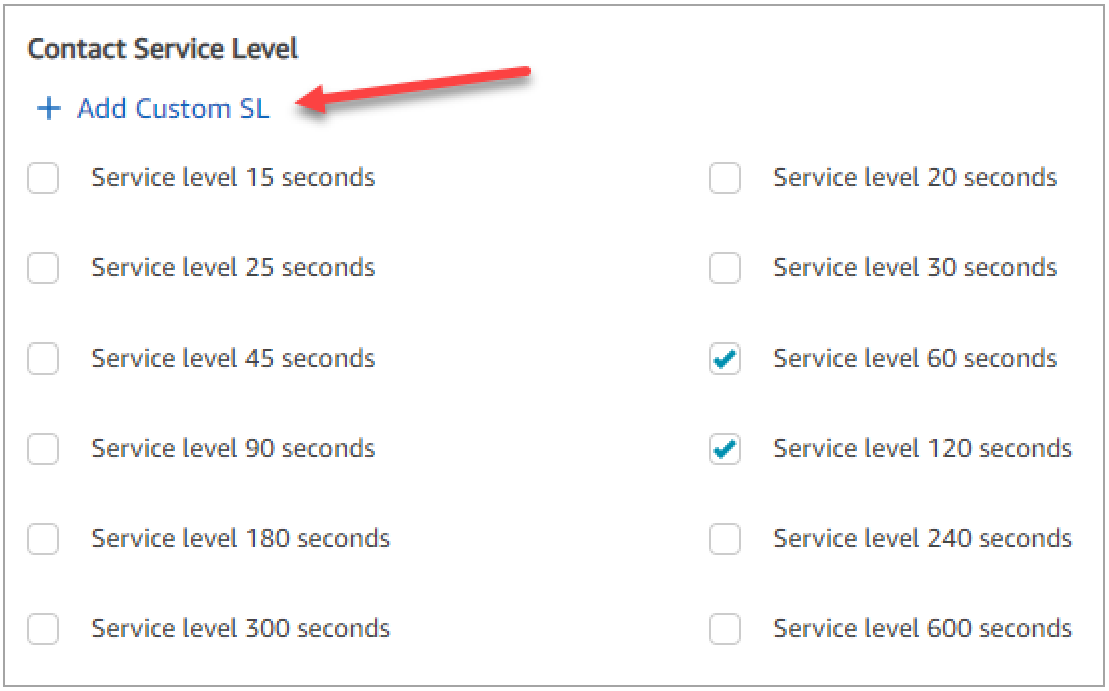
□ SL 90 secs □ SL 120 secs

Historical metrics: New categories for metrics

To make it easier to find the historical metrics you want to add to a report, metrics on the **Table settings** page are grouped into the following categories:

- Agents
- Contacts Abandoned
- Contact Service Level: This group contains preset and custom service levels.
- Contacts Answered
- Performance

Choose **Add Custom SL** to add custom service levels to your historical metrics report.



Contact Service Level

☐ Service level 15 seconds	☐ Service level 20 seconds
☐ Service level 25 seconds	☐ Service level 30 seconds
☐ Service level 45 seconds	☑ Service level 60 seconds
☐ Service level 90 seconds	☑ Service level 120 seconds
☐ Service level 180 seconds	☐ Service level 240 seconds
☐ Service level 300 seconds	☐ Service level 600 seconds

The order of the metric columns on the historical metrics reports has changed

The order of the metric columns on the historical metrics reports matches the updated grouping scheme and order of the metrics on the **Table settings** page.

This change supports the addition of custom service level metrics (p. 899). It also allows us to make future improvements for where, for example, control of how a report looks resides on the **Real-time metrics** page and the **Historical metrics** page, not the **Table settings** page.

Note how metric columns now appear on reports:

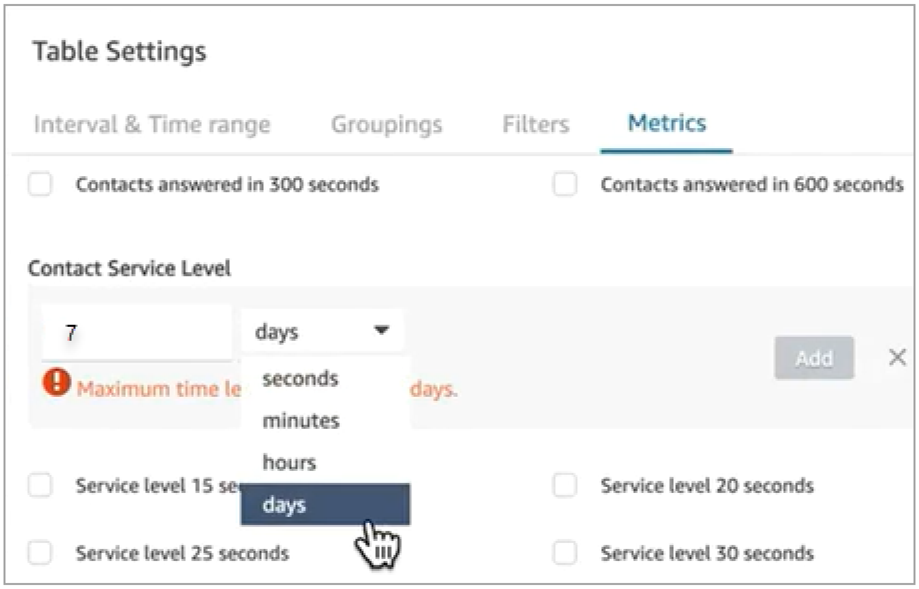
- When you open the **Real-time metrics** page, custom service levels appear at the end of the **Performance** group.
- Metrics on existing **Scheduled reports** (the processed documents that arrive in your Amazon S3 buckets) are not re-ordered automatically. However, if you update an existing report, the metrics are re-ordered to match the order on the **Table settings** page.
- **Service level metrics**:
  - Real-time metrics reports: Service level metrics are always added to the end of the **Performance** group, in ascending order.

- Historical metrics reports: When you add custom service level metrics, they are added to the end of the report in the order they were created.

Custom service level metrics

You have the ability to add custom service level metrics. You can also choose from additional durations, such as minutes, hours, or days.

The maximum duration for a custom service level is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.



Group by channel in a historical metrics report

To group by channel on historical metrics reports

1. On the navigation menu, choose **Analytics**, **Historical metrics**, and then choose a report.
2. Choose **Settings**.
3. On the **Table Settings** page, choose the **Groupings** tab. Add **Channel**, and choose **Apply**.

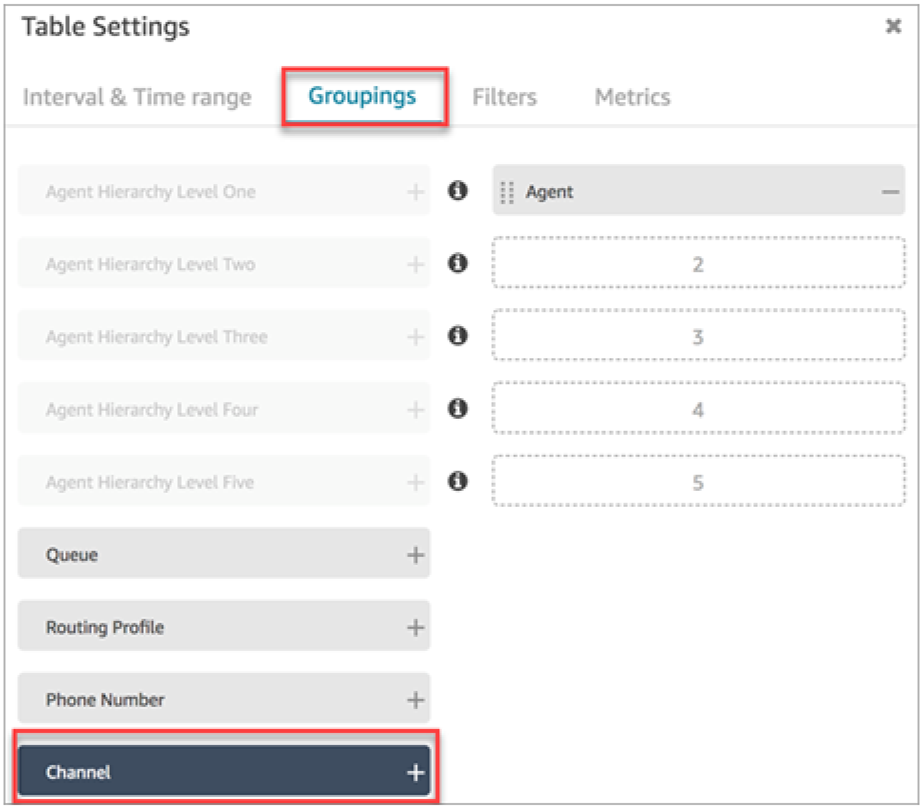
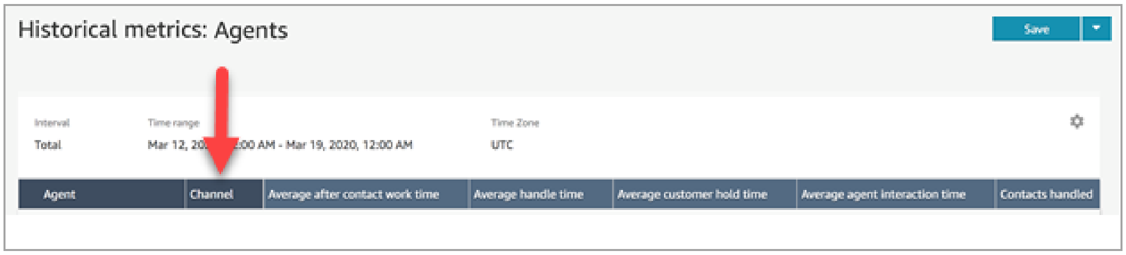


Table Settings
Interval & Time range
Groupings
Filters
Metrics
Agent Hierarchy Level One
Agent Hierarchy Level Two
Agent Hierarchy Level Three
Agent Hierarchy Level Four
Agent Hierarchy Level Five
Queue
Routing Profile
Phone Number
Channel
Agent
2
3
4
5

4. The table shows a column for **Channel**, as shown in the following image.



Interval: Total

Time range: Mar 12, 20 :00 AM - Mar 19, 2020, 12:00 AM

Time Zone: UTC

Agent	Channel	Average after contact work time	Average handle time	Average customer hold time	Average agent interaction time	Contacts handled

October 2020

New historical metrics for inbound and outbound contact time

Released the following real-time metrics:

- Avg callback connecting time (p. 920)
- Avg incoming connecting time (p. 920)
- Avg outbound connecting time (p. 921)

Released the following historical metrics:

- Agent API connecting time (p. 939)
- Agent callback connecting time (p. 940)
- Agent incoming connecting time (p. 940)

- Agent outbound connecting time (p. 941)
- Average agent API connecting time (p. 942)
- Average agent callback connecting time (p. 942)
- Average agent incoming connecting time (p. 942)
- Average agent outbound connecting time (p. 943)

One-click drill-downs for Routing profiles and Queues tables

In real-time metrics reports, for **Routing profiles** and **Queues** tables, you can open pre-filtered tables that display the associated queues, routing profiles, or agents. These one-click filters provide a way for you to drill into the performance data.

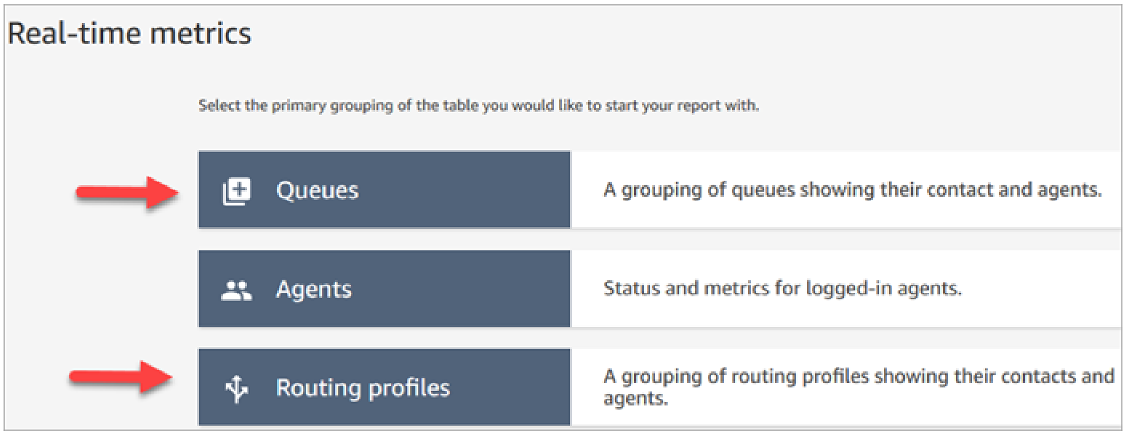
For more information, see Use one-click drill-downs for Routing profiles and Queues tables (p. 927)

June 2020: Changes for omnichannel support

Group by channel

To group queues or routing profiles by channel on real-time metrics reports

1. On the navigation menu, choose **Analytics**, **Real-time metrics**, and then select either **Queues** or **Routing profiles**.



Real-time metrics

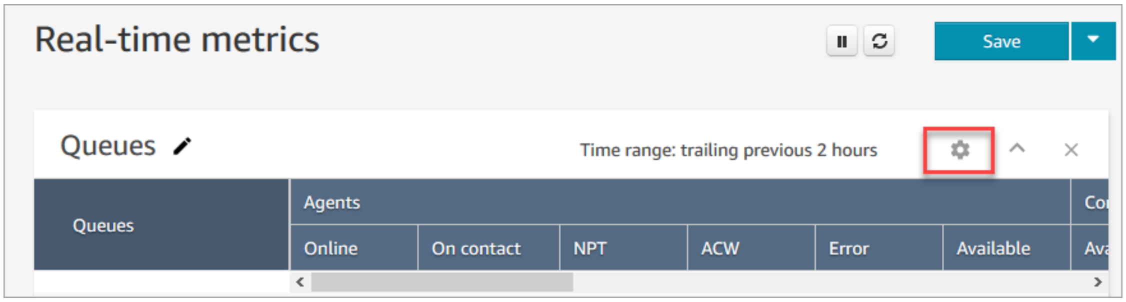
Select the primary grouping of the table you would like to start your report with.

Queues: A grouping of queues showing their contact and agents.

Agents: Status and metrics for logged-in agents.

Routing profiles: A grouping of routing profiles showing their contacts and agents.

2. Choose **Settings**.



3. On the **Table Settings** page, choose the **Groupings** tab and then select **Queues grouped by channels**. Or, if you're setting up a **Routing profiles** report, choose **Routing profiles grouped by channels**.

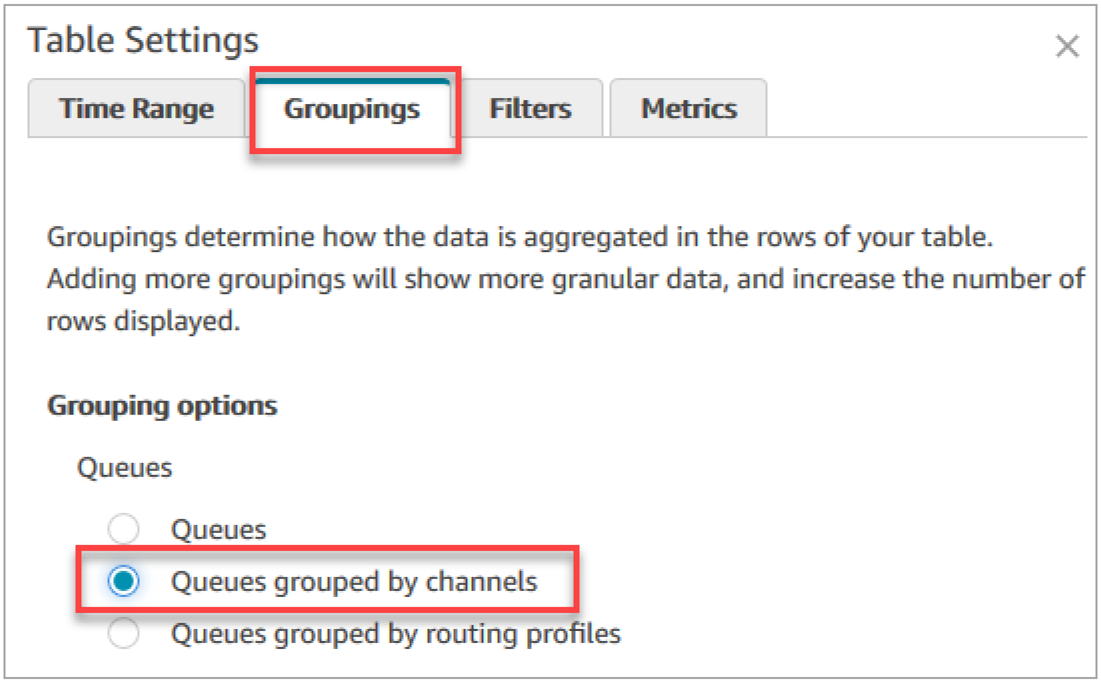


Table Settings

Groupings determine how the data is aggregated in the rows of your table. Adding more groupings will show more granular data, and increase the number of rows displayed.

Grouping options

Queues

○ Queues

● Queues grouped by channels

○ Queues grouped by routing profiles

4. Choose **Apply**.
5. The table shows a column for **Channel**.

Group by queue in historical metrics reports

In the historical metrics report, when you group or filter metrics by **Queue**, the results for the following metrics aren't accurate:

- Agent idle time (not supported in queue grouping as of June, 2020)
- Agent on contact time (not supported in queue grouping as of June, 2020)
- Occupancy (not supported in queue grouping as of June, 2020)

Because of this, on the **Table Settings** page, **Metrics** tab, these metrics are inactive, as shown in the following image:

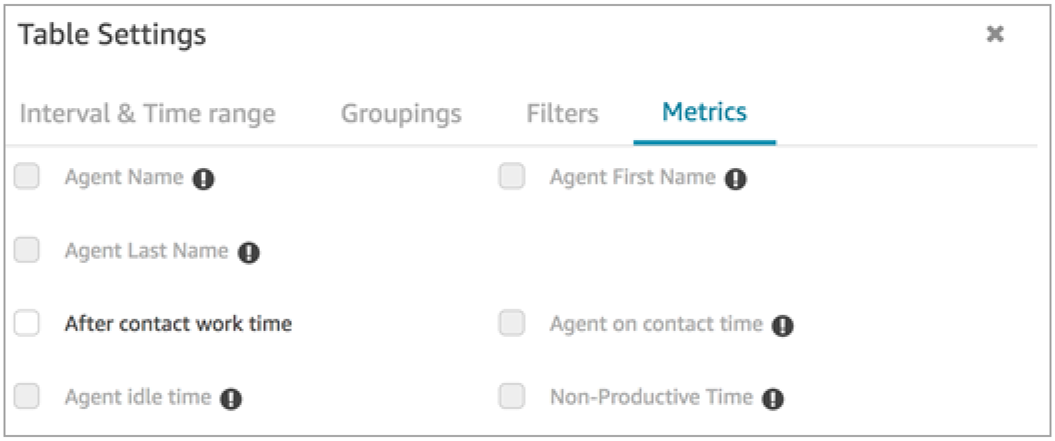


Table Settings

□ Agent Name

□ Agent First Name

□ Agent Last Name

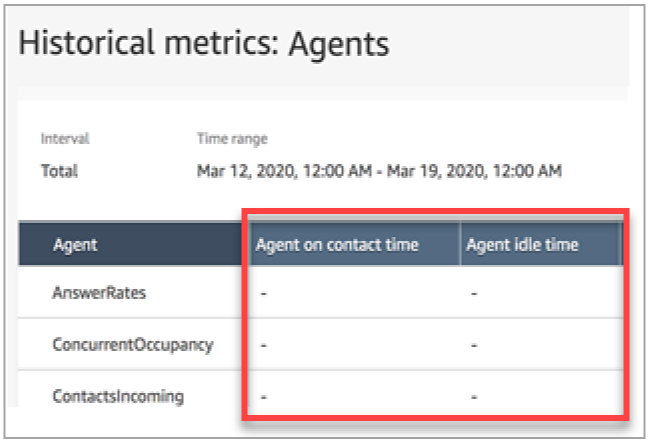
□ After contact work time

□ Agent on contact time

□ Agent idle time

□ Non-Productive Time

In addition, in the historical metrics report, Amazon Connect displays a hyphen (-) in place of results for these metrics, and the cells are inactive (gray).



Historical metrics: Agents

Interval: Total

Time range: Mar 12, 2020, 12:00 AM - Mar 19, 2020, 12:00 AM

Agent	Agent on contact time	Agent idle time
AnswerRates	-	-
ConcurrentOccupancy	-	-
ContactsIncoming	-	-

Effect of queue grouping on saved and scheduled reports

If the **Queue** grouping or filter is used on the following reports, note these effects:

- **Saved reports**. The columns for these metrics don't appear in the saved reports when *grouped* by Queue. When the saved report is *filtered* by Queue, however, it shows "-".
- **Scheduled reports**. These reports continue to run successfully, but no results are returned for these metrics.

Agent on contact time (not supported in queue grouping as of June, 2020)

On historical metrics reports when an agent handles multiple chats concurrently, **Agent on contact time** shows wall clock time: the amount of time spent chatting. However, there isn't a metric that shows the time an agent spends chatting with each contact.

In addition, no results are returned when you use the **Queue** grouping or filter with **Agent on contact time**.

Agent idle time (not supported in queue grouping as of June, 2020

The **Agent idle time** metric divides the idle time into each queue associated with the agent. When contacts are grouped or filtered by **Queue**, however, Amazon Connect doesn't provide an accurate view into the how the agent is working. Because of this, Amazon Connect doesn't show **Agent idle time** when you apply the **Queue** grouping or filter to your report.

Occupancy (not supported in queue grouping as of June, 2020)

With the addition of chat, the **Occupancy** metric is now defined as the percentage of time that an agent was active on contacts. This percentage is calculated as follows:

- (Agent on contact (wall clock time) / (Agent on contact (wall clock time) + Agent idle time))

Because **Agent idle time** is now inaccurate when contacts are grouped or filtered by **Queues**, the **Occupancy** metric is also inaccurate. As a result, when contacts are grouped or filtered by Queues, **Occupancy** doesn't appear on the report.

Occupancy no longer appears on the **Dashboard** page.

November 2019

Name changes for "Missed" and "Agent status" and "On call"

The following real-time metrics were renamed:

Old name	New name
Missed	Agent non-response
Agent status	Agent activity
On call	On contact

For each metric, existing saved reports automatically start displaying the new name; you don't need to do anything for the new name to appear in your reports.

The column order for a saved report containing one of these metrics stays the same. For example, if you previously saved a report where **Agent status** was the third metric, now when you open that saved report, **Agent activity** is the name for the third metric.

For **Missed**, only the name of the metric changed; the underlying calculation stayed the same. We've changing the name of this metric to **Agent non-response** so it better reflects its definition:

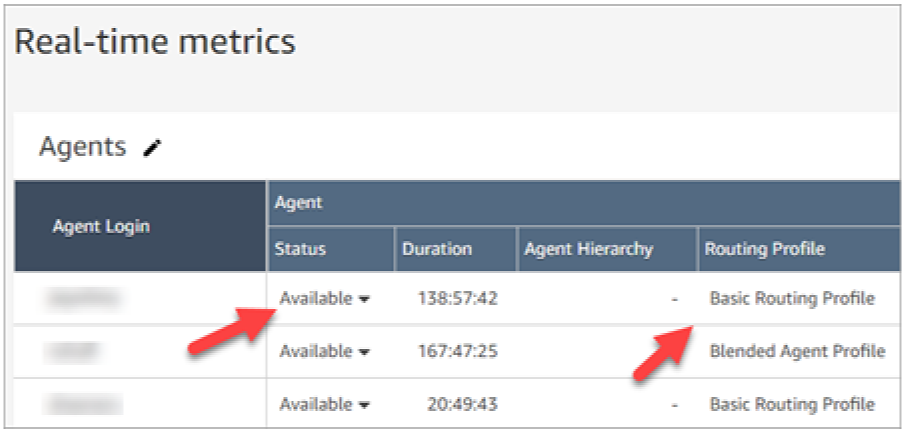
- **Agent non-response** increments whenever a contact is offered to an agent, and the agent doesn't respond to the contact for whatever reason.

  For example, the agent could have intentionally let the timer run out, or the agent could have forgotten to grant microphone access in the Contact Control Panel and never heard the ring. In these situations, Amazon Connect doesn't drop the contact. Instead, the routing engine will offer it to another available agent, while the customer continues to wait in queue. This means a single contact could result in multiple **Agent non-responses** before an agent responds and handles the contact.

For **On call**, the name change to **On Contact** applies to the Real-time metrics UI only. You can continue using `AGENTS_ON_CALL` with the `GetCurrentMetricData` API to retrieve data for this metric.

Label updates for "Agent activity" and "Contact state"

Labels are the values returned in a report. For example, in the following image **Available** and **Basic Routing Profile** are labels.



Real-time metrics

Agents

Agent Login	Agent			
	Status	Duration	Agent Hierarchy	Routing Profile
[redacted]	Available	138:57:42	-	Basic Routing Profile
[redacted]	Available	167:47:25		Blended Agent Profile
[redacted]	Available	20:49:43	-	Basic Routing Profile

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:

Scenario	Before: Agent Status Labels	After: Agent Activity Labels	Notes
Agent is logged in but offline	Not shown	Not shown	
Agent switches to **Available** in the CCP	Available	Available	
Agent has an incoming call	CallIncoming	Incoming	ContactState = Incoming contact
Agent has an incoming callback	CallbackIncoming	Incoming	ContactState = Inbound callback
Agent accepted a callback, which is now making an outbound call to the customer	Calling	On Contact	ContactState = Outbound callback
Agent makes outbound call (regardless of what status the agent chose in their CCP)	Calling	On Contact	ContactState = Outbound contact
Agent missed a phone call due to timer expired	MissedCallAgent	Missed	
Agent is interacting with customer on phone call (regardless of what status the agent chose in their CCP)	On call	On Contact	

Scenario	Before: Agent Status Labels	After: Agent Activity Labels	Notes
Agent puts customer on hold while on phone call (regardless of what status the agent chose in their CCP)	On call	On Contact	
After agent hangs up call	After call work	After contact work	
Agent is on Lunch (a custom status)	Lunch	Lunch	
Supervisor's activity state if they are monitoring some agent	Monitoring	Monitoring	
Agent's activity state if they are connected to customer while being monitored by a supervisor	On call	On Contact	

The following table shows the how the labels changed for **Contact State**.

Scenario	Label Name Before	Label Name After
Agent is logged in but offline		
Agent switches to **Available** in the CCP	-	-
Agent has an incoming call	-	Incoming contact
Agent has an incoming callback	-	Inbound callback
Agent accepted a callback, which is now making an outbound call to the customer	Initial	Outbound callback
Agent makes outbound call (regardless of what status the agent chose in their CCP)	Initial	Outbound contact
Agent missed a phone call due to timer expired	Missed call	Missed contact
Agent is interacting with customer on phone call (regardless of what status the agent chose in their CCP)	Busy	Connected
Agent puts customer on hold while on phone call (regardless of what status the agent chose in their CCP)	OnHold	On hold

Scenario	Label Name Before	Label Name After
After agent hangs up call	After call work	After contact work
Agent is on Lunch (a custom status)	-	-
Supervisor's contact state if they are monitoring an agent	Monitoring	Monitoring

Search for contacts

Important things to know

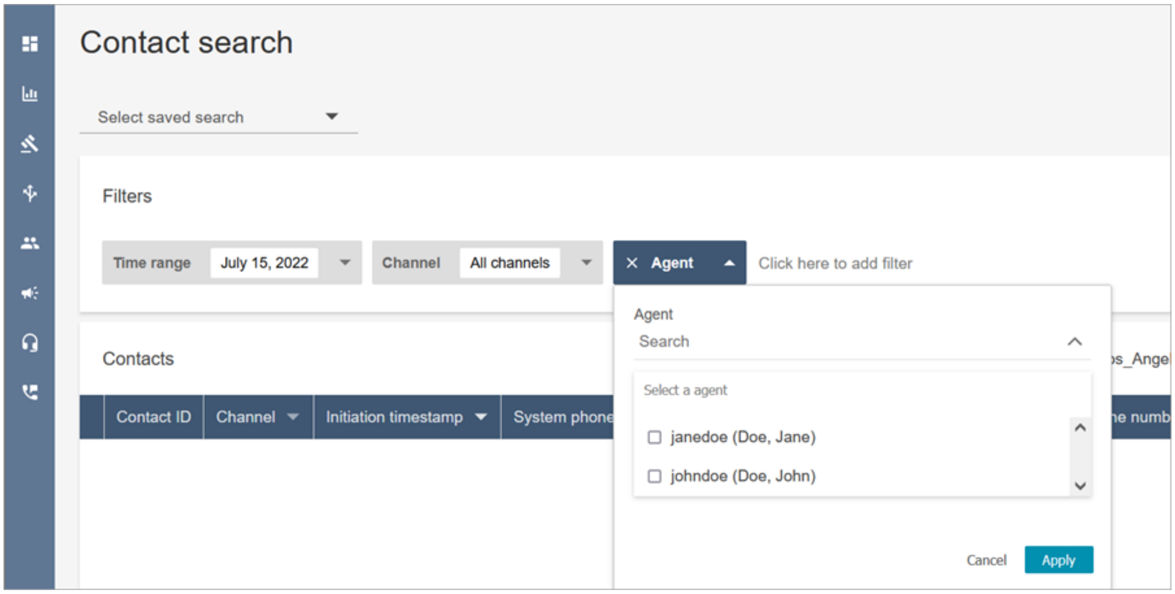
- You can search for contacts as far back as two years ago.
- Amazon Connect returns results for completed contacts. If an agent is still doing After Contact Work (ACW) on a contact, for example, that contact is not considered closed and won't be returned in the search results.
- The search results for 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.

What's new in contact search

Thanks to your feedback, we've made the following changes to contact search.

Search contacts by agent's first or last name

The following image shows the Agent filter, and the option to choose agents by name.

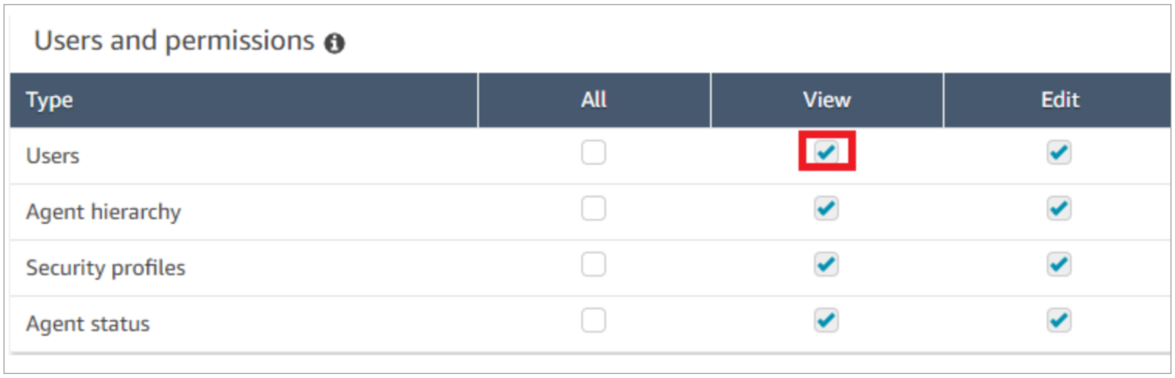


Time range: July 15, 2022

Channel: All channels

Required permissions to "Agent" search filter

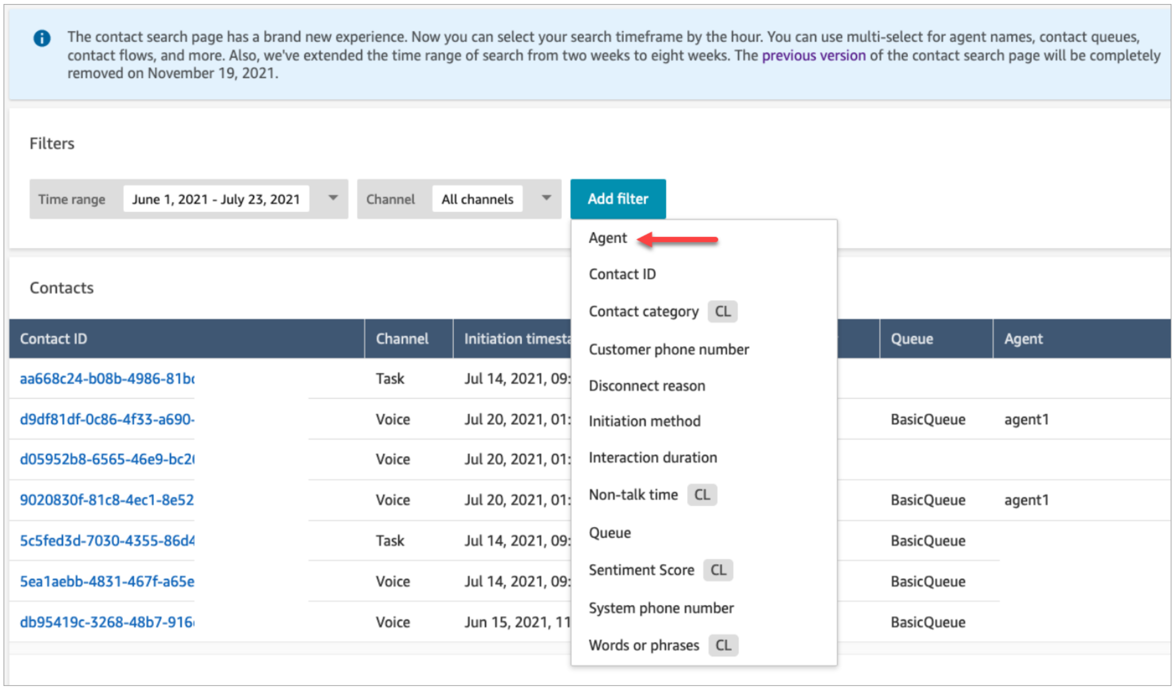
To use the **Agent** filter on the **Contact search** page, in your Amazon Connect security profile you must have **Users - View** permissions, as shown in the following image:



Users and permissions

Type	All	View	Edit
Users	□	☑	☑
Agent hierarchy	□	☑	☑
Security profiles	□	☑	☑
Agent status	□	☑	☑

When you have **Users - View** permissions, on the **Contact search** page the **Agent** filter appears, as shown in the following image:



The contact search page has a brand new experience. Now you can select your search timeframe by the hour. You can use multi-select for agent names, contact queues, contact flows, and more. Also, we've extended the time range of search from two weeks to eight weeks. The previous version of the contact search page will be completely removed on November 19, 2021.

Filters

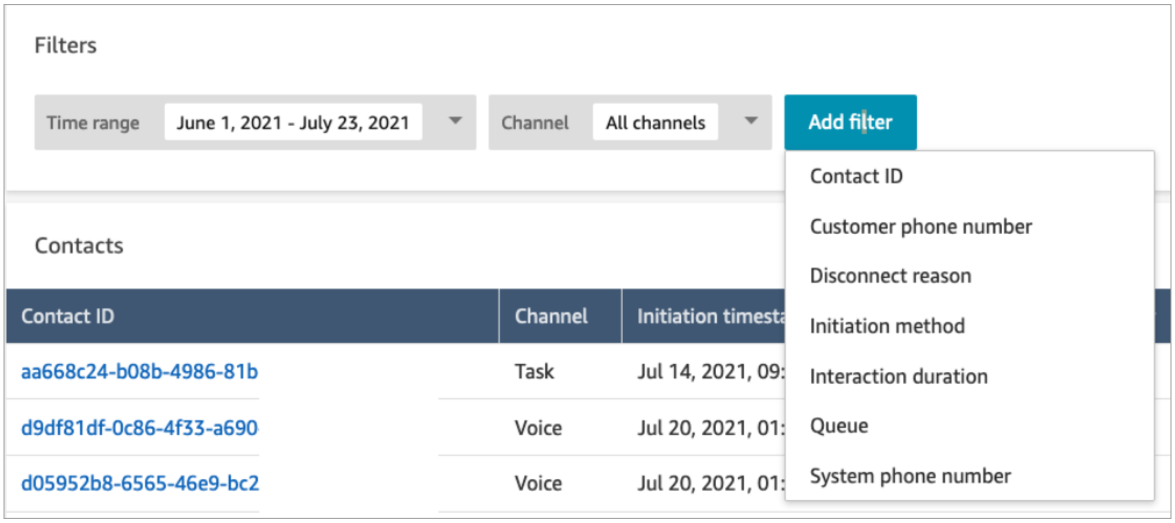
Time range: June 1, 2021 - July 23, 2021

Channel: All channels

Contacts

Contact ID	Channel	Initiation timesta	Queue	Agent
aa668c24-b08b-4986-81b	Task	Jul 14, 2021, 09:		
d9df81df-0c86-4f33-a690-	Voice	Jul 20, 2021, 01:	BasicQueue	agent1
d05952b8-6565-46e9-bc2	Voice	Jul 20, 2021, 01:		
9020830f-81c8-4ec1-8e52	Voice	Jul 20, 2021, 01:	BasicQueue	agent1
5c5fed3d-7030-4355-86d4	Task	Jul 14, 2021, 09:	BasicQueue	
5ea1aebb-4831-467f-a65e	Voice	Jul 14, 2021, 09:	BasicQueue	
db95419c-3268-48b7-916	Voice	Jun 15, 2021, 11	BasicQueue	

Without **User - View** permissions, the **Agent** filter is not visible, and searching contacts by Agent login is not supported, as shown in the following image:



Filters

Time range: June 1, 2021 - July 23, 2021

Channel: All channels

Contacts

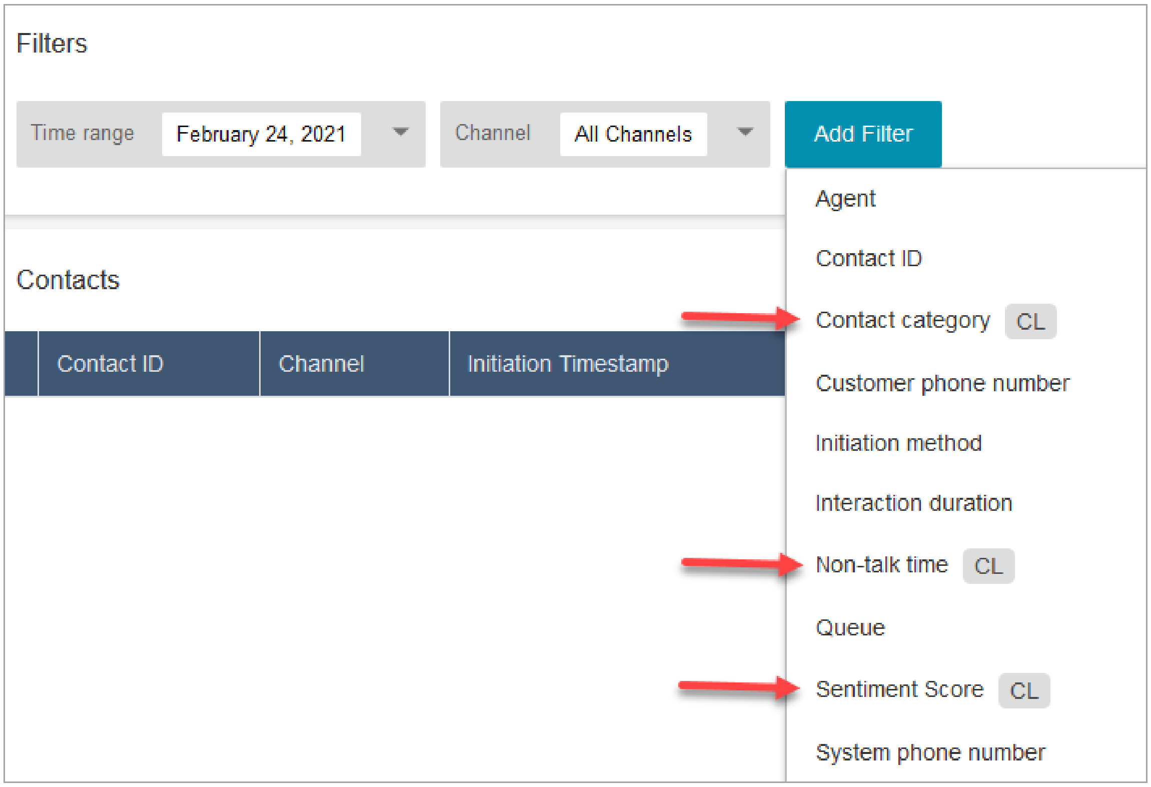
Contact ID	Channel	Initiation timesta
aa668c24-b08b-4986-81b	Task	Jul 14, 2021, 09:
d9df81df-0c86-4f33-a690	Voice	Jul 20, 2021, 01:
d05952b8-6565-46e9-bc2	Voice	Jul 20, 2021, 01:

Key search features

- Search by custom contact attributes (p. 913) (user-defined attributes).
- Search a time range up to 8 weeks.
- Multi-select for filters such as agent names, contact queues, contact flows, and more.

  This feature is available only for searches with a date range that starts November 2, 2020, or later, when the feature was released. If you search for contacts that occurred before November 2, 2020, you will be prompted to ensure only one value is selected for each filter mentioned above.
- Filters for Contact Lens for Amazon Connect (p. 811). You can search for Contact categories (p. 829) by specifying the full category name.

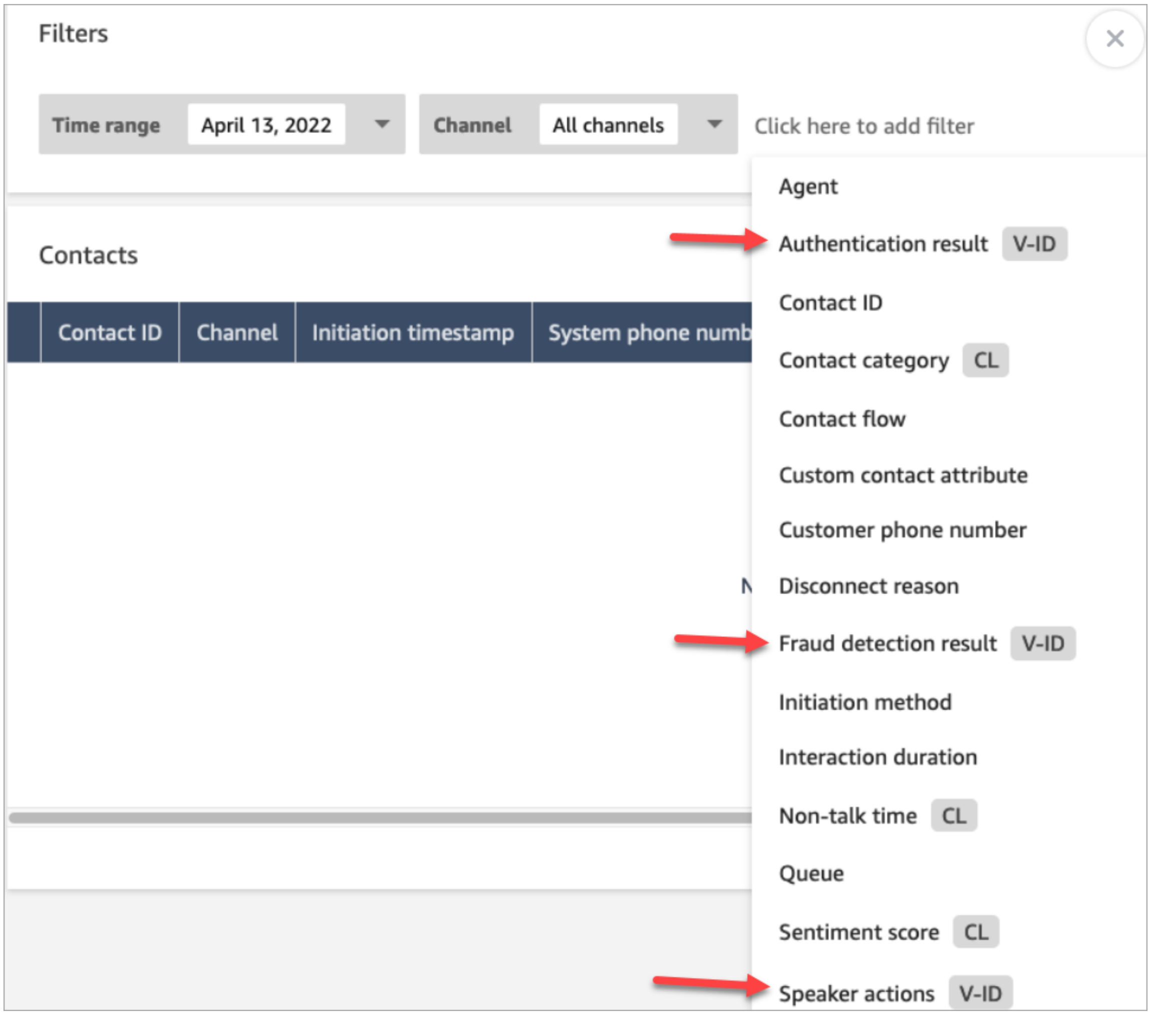
  In the **Add filter** drop-down box, the Contact Lens filters have **CL** next to them. You can apply these filters only if your organization has enabled Contact Lens.



If you want to remove the Contact Lens filters from a user's drop-down list, remove the following permissions from their security profile:

- **Search contacts by conversation**: This controls access to the sentiment scores, non-talk time, and category searches.
- **Search contacts by keywords**: This controls access to the keywords search.
- **Contact Lens - speech analytics**: On the Contact Trace Record page, this displays graphs that summarize speech analytics.

- Filters for Voice ID (p. 858). You can search for the Voice ID authentication and fraud detection status of contacts, if your organization has enabled Voice ID. To access this functionality, on your security profile, you need **Analytics**, **Voice ID - attributes and search** - **View** permission.



Filters

Time range: April 13, 2022

Channel: All channels

Manage who can search for contacts and access detailed information

Before users can search for contacts in Amazon Connect, or access detailed contact information, they need to be assigned to the **CallCenterManager** security profile, or have the following **Analytics** permissions:

- **Access metrics - Access** (Required): Grants access to metrics data.
- **Contact search - View** (Required): Grants access to the **Contact search** page, and the ability to search for contacts.
- **Restrict contact access** (Optional): Manage a user's access to results on the **Contact search** page based on their agent hierarchy group.

  For example, agents who are assigned to AgentGroup-1 can only view contact records for contacts handled by agents in that hierarchy group, and any groups below them. (If they have permissions for **Recorded conversations**, they can also listen to call recordings and view transcripts.) Agents assigned to AgentGroup-2 can only access contact records for contacts handled by their group, and any groups below them.

Managers and others who are in higher level groups can view contact records for contacts handled by all the groups below them, such as AgentGroup-1 and 2.

For this permission, **All** = **View** since **View** is the only action granted.

For more information about hierarchy groups, see Set up agent hierarchies (p. 230).

> **Note**
> When you change a user's hierarchy group, it may take a couple of minutes for their contact search results to reflect their new permissions.

- **Contact Lens - speech analytics**: On the Contact Record page for a contact, you can view graphs that summarize speech analytics: customer sentiment trend, sentiment, and non-talk time.
- **Recorded conversations (redacted)**: If your organization uses Contact Lens for Amazon Connect, you can assign this permission so agents access only those call recordings and transcripts in which sensitive data has been removed.
- **Recorded conversations (unredacted)**: If your organization isn't using Contact Lens, agents need **Recorded conversations (unredacted)** to listen to call recordings or view transcripts. If desired, you can use **Restrict contact access** to ensure they only have access to detailed information for those contacts handled by their hierarchy group.
- **Voice ID - attributes and search**: If your organization uses Voice ID, users with this permission can search for and view Voice ID results in the **Contact detail** page.
- **Users - View** permission: You must have this permission to use the **Agent** filter on the **Contact search** page.

By default, the Amazon Connect **Admin** and **CallCenterManager** security profiles have these permissions.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

How to search for a contact

1. Log in to Amazon Connect with a user account that has permissions to access contact records (p. 911).
2. In Amazon Connect choose **Analytics**, **Contact search**.
3. Use the filters on the page to narrow your search. For date, you can search up to 8 weeks at a time.

> **Tip**
> To see if a conversation was recorded, you need to be assigned to a profile that has **Manager monitor** permissions. If a conversation was recorded, by default the search result will indicate so with an icon in the **Recording** column. You won't see this icon if you don't have permission to review the recordings.

Additional fields: Add columns to your search results

Use the options under **Additional fields** to add columns in your search results. These options are not used to filter your search.

For example, if you want to include columns for **Agent Name** and **Routing profile** in your search output, choose those columns here.

Tip

The **Is transferred out** option indicates whether the contact was transferred to an external number. For the date and time (in UTC time) when the transfer was connected, see `TransferCompletedTimestamp` in the ContactTraceRecord (p. 988).

Download search results

You can download up to 3,000 search results at a time.

Search by custom contact attributes

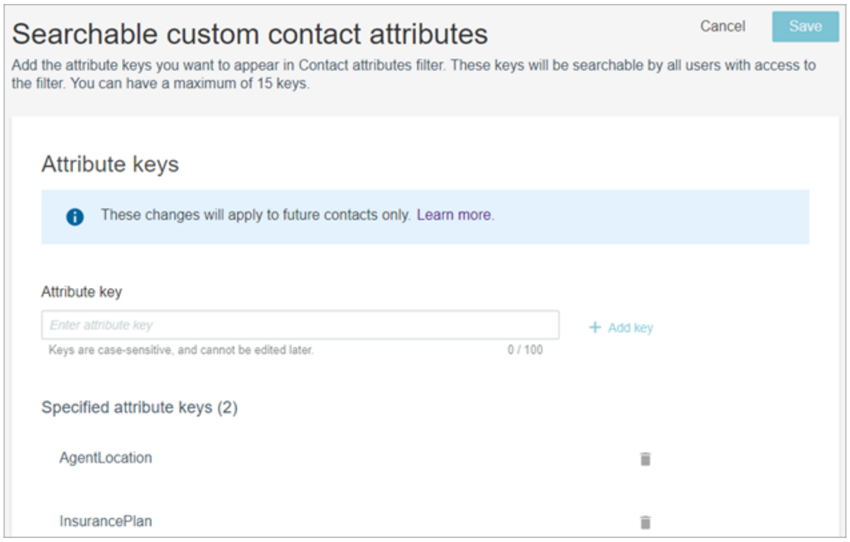
You can create search filters based on custom contact attributes (also called user-defined contact attributes (p. 529)). For example, if you add `AgentLocation` and `InsurancePlanType` to your contact records as custom attributes, you can search for contacts with specific values in these attributes, such as calls handled by agents located in Seattle, or calls made by customers who purchased homeowners insurance.

Required permissions to configure searchable contact attributes

By default, a custom attribute isn't indexed until someone with appropriate permissions, such as an admin or manager, specifies it should be searchable. You grant permissions to select users so they can configure which custom contact attributes can be added as a search filter.

Assign the following permissions to their security profile:

- **Contact search**: Controls basic access to the **Contact search** page.
- **Contact attributes**: Allows users to view contact attributes. Also controls access to the search filters based on contact attributes.
- **Configure searchable contact attributes** - **All**: People who have this permission determine what custom data will be searchable (by people who have the **Contact attributes** permission). It allows them to access the following configuration page:



Searchable custom contact attributes

Add the attribute keys you want to appear in Contact attributes filter. These keys will be searchable by all users with access to the filter. You can have a maximum of 15 keys.

Attribute keys

These changes will apply to future contacts only. Learn more.

Attribute key: Enter attribute key

Keys are case-sensitive, and cannot be edited later. 0 / 100

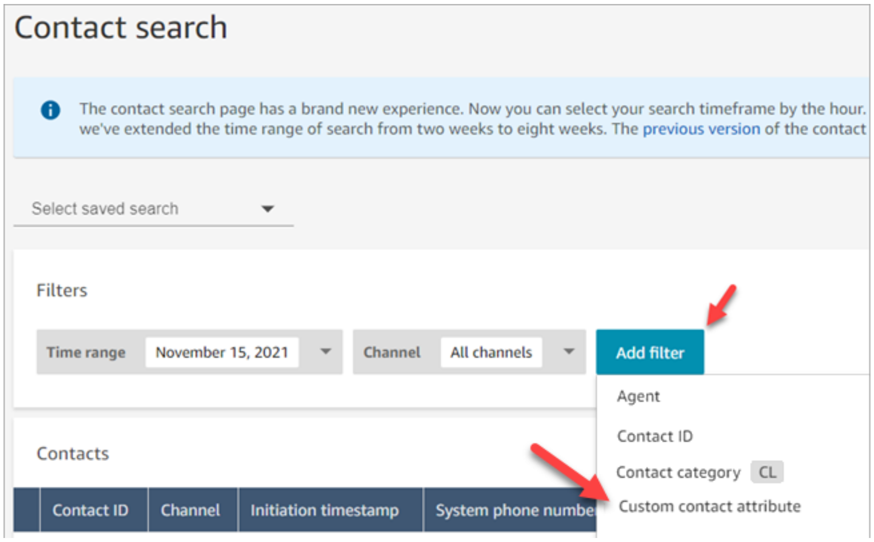
Specified attribute keys (2)

AgentLocation

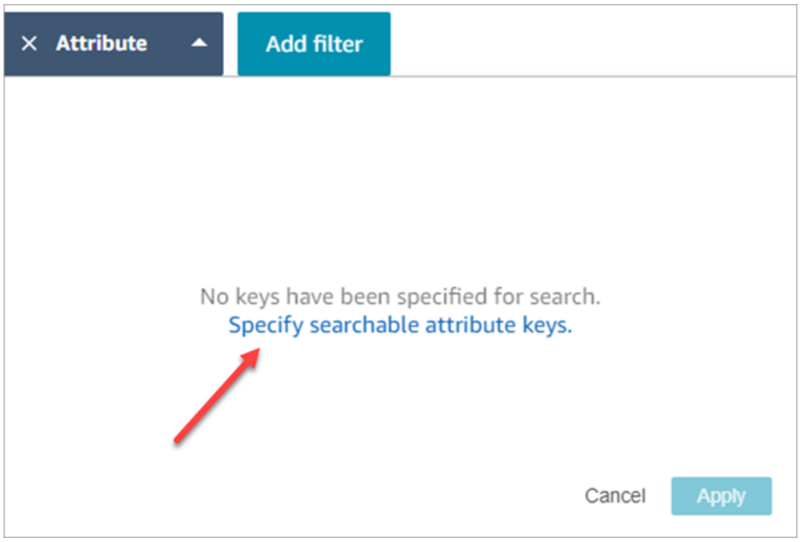
InsurancePlan

Configure searchable custom contact attributes

1. On the **Contact search** page, choose **Add filter**, **Custom contact attribute**. Only people with **Configure searchable contact attributes** permissions in their security profile see this option.



2. The first time you choose **Custom contact attribute**, the following box appears, indicating no attributes have been configured for this Amazon Connect instance. Choose **Specify searchable attribute keys**.



× Attribute
Add filter
No keys have been specified for search.
Specify searchable attribute keys.
Cancel
Apply

3. In the **Attribute key** box, type the name of your custom attribute, and then choose **Add key**.

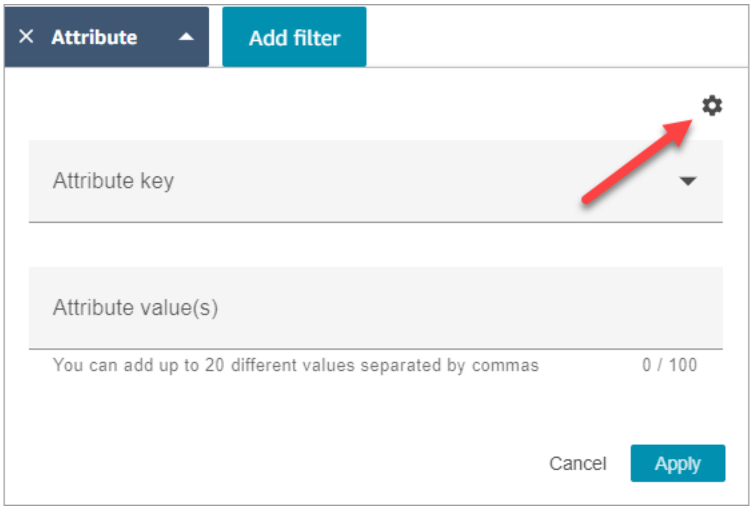
   Important
   You must type the exact key name. It is case sensitive.

4. When finished, choose **Save**.

Your users will be able to search on these keys for any future contacts.

Edit, add, or remove contact attributes

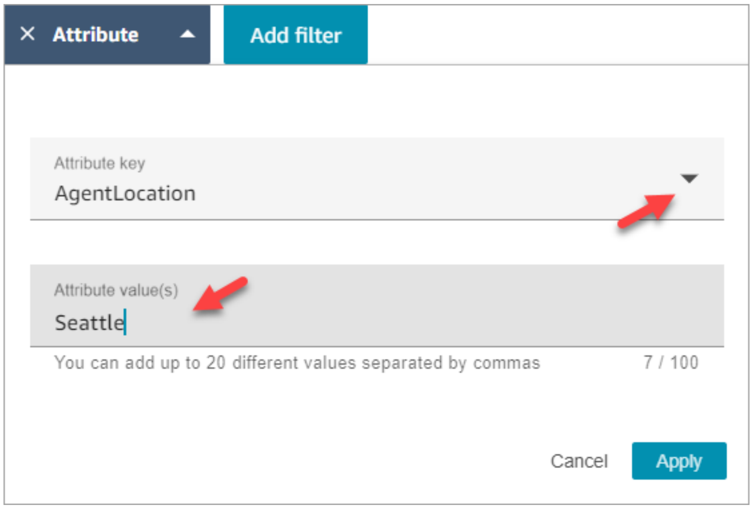
To edit, add, or remove keys, choose **Attribute**, **Settings**. If you don't see the **Settings** option, you don't have the required permissions.



Search for custom contact attributes

Users who have the **Contact attributes** permission in their security profile can find contacts by using the contact attribute filters.

1. On the **Contact search** page, choose **Add filter**, **Custom contact attribute**.
2. In the **Attribute key** box, choose the dropdown to select the key to search.
3. In the **Attribute values** box, choose value you want to find. Note that the **Settings** icon doesn't appear in the following image because this user doesn't have **Configure searchable contact attributes** permissions in their security profile.



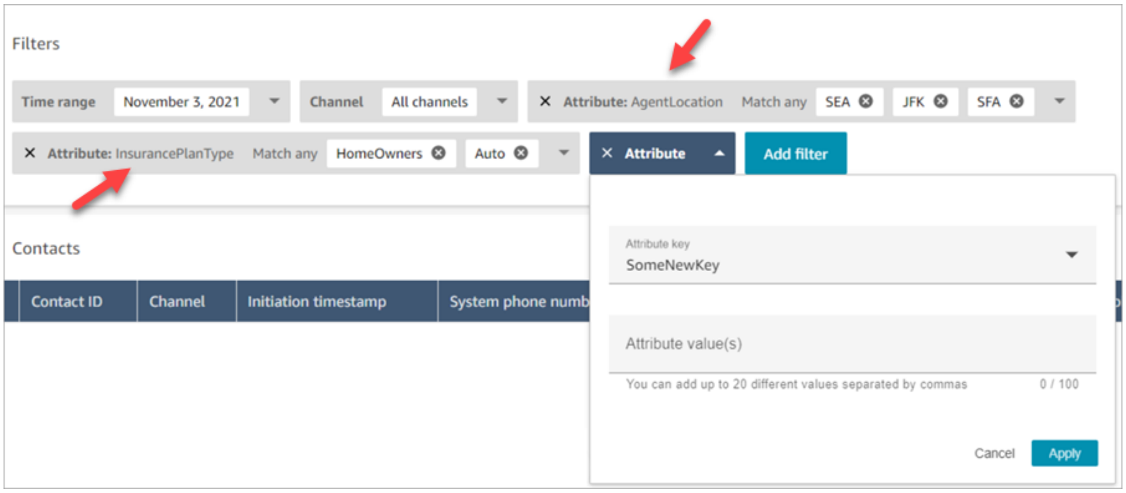
Attribute key
AgentLocation

Attribute value(s)
Seattle

You can add up to 20 different values separated by commas
7 / 100

4. To create a query with multiple custom attributes, choose **Add filter** and **Custom contact attribute** again, and add a different attribute name and specify the value to search for.

   The following image shows a query that includes two custom attributes: one for **AgentLocation** and another for **InsurancePlanType**.



Real-time metrics reports

Real-time metrics reports show real-time or near-real time metrics information about activity in your contact center. Metrics such as **Online** show the number of agents currently online in real-time, updating every 15 seconds. Metrics such as **Handled** and **Abandoned** reflect near real-time values for your contact center.

You can customize the reports, specify a time range for each report, select metrics for each report, and select filters for data to include or exclude from each report.

You can also use the Amazon Connect Service APIs to create custom reports, such as real-time reports that are filtered by teams of agents.

Contents

Real-time metrics definitions

The following metrics are available to include in real-time metrics reports in Amazon Connect. The metrics available to include in a report depend on the report type.

Tip

Developers can use the GetCurrentMetricData API to get a subset of the following real-time metrics from the specified Amazon Connect instance.

Abandoned

Count of contacts disconnected by the customer while in the queue during the specified time range. Contacts queued for callback are not counted as abandoned. When you create a customized real-time metrics report, to include this metric, choose a **Queues** report for the type. On the **Filters** tab, choose **Queues**, then on the **Metrics** tab you'll have the option to include **Abandoned**.

Active

Count of active slots. This number is incremented for each contact where the contact state is either Connected, On Hold, After contact work, or Outbound ring.

In the GetCurrentMetricData API, this metric is `SLOTS_ACTIVE`.

ACW

Count of contacts who are in an **AfterContactWork** state. (After contact work is also known as After call work.) After a conversation between an agent and customer ends, the contact is moved into the ACW state.

In the GetCurrentMetricData API, this metric is `AGENTS_AFTER_CONTACT_WORK`. The name of this metric is confusing because in the Amazon Connect console, ACW counts the number of *contacts* who are in an ACW state, not the number of agents.

To learn more about agent status and contact states, see About agent status (p. 998) and About contact states (p. 1000).

Agent Activity

If an agent is handling a single contact, this metric may have the following values: Available, Incoming, On contact, Rejected, Missed, Error, After contact work, or a custom status.

If an agent is handling concurrent contacts, Amazon Connect uses the following logic to determine the state:

- If at least one contact is in Error, Agent Activity = Error.
- Else if at least one contact is Missed contact, Agent Activity = Missed.
- Else if at least one contact is Rejected contact, Agent Activity = Rejected.
- Else if at least one contact is Connected, On Hold, or Outbound contact/Outbound callback, Agent Activity = On contact.
- Else if at least one contact is After contact work, Agent Activity = After Contact Work.
- Else if at least one contact is Incoming/Inbound Callback, Agent Activity = Incoming.
- Else if agent status is a custom status, Agent Activity is the custom status.
- Else if agent status is Available, Agent Activity = Available.

If a supervisor is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, then the supervisor's Agent Activity will display as Monitoring. The Agent Activity of the agent who is being monitored is still On Contact.

Agent First Name

The first name of the agent, as entered in their Amazon Connect user account.

Agent Hierarchy

The hierarchy the agent is assigned to, if any.

Agent hung up

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

Agent Last Name

The last name of the agent, as entered in their Amazon Connect user account.

Agent Name

The name of the agent, displayed as follows: **Agent Last Name**, **Agent First Name**.

Agent non-response

Count of contacts routed to an agent but not answered by that agent, including contacts abandoned by the customer.

If a contact is not answered by a given agent, we attempt to route it to another agent to handle; the contact is not dropped. Because a single contact can be missed multiple times (including by the same agent), it can be counted multiple times: once for each time it is routed to an agent but not answered.

This metric was previously named **Missed**.

AHT (Average Handled Time)

The average time, from start to finish, that a contact was connected with an agent (average handled time). It includes talk time, hold time, and After Contact Work (ACW) time.

AHT is calculated by averaging **the amount of time between the contact being answered by an agent** and **the completion of work on that contact by an agent**.

API contacts handled

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

Availability

For each agent, the number of available slots they have that can be routed contacts.

The number of available slots for an agent are based on their routing profile (p. 227). For example, let's say an agent's routing profile specifies they can handle either one voice contact **or** up to three chat contacts simultaneously. If they are currently handling one chat, they have two available slots left, not three.

What causes this number to go down? A slot is considered unavailable when:

- A contact in the slot is: connected to the agent, in After Contact Work, inbound ringing, outbound ringing, missed, or in an error state.
- A contact in the slot is connected to the agent and on hold.

Amazon Connect doesn't count an agent's slots when:

- The agent has set their status in the CCP to a custom status, such as Break or Training. Amazon Connect doesn't count these slots because agents can't take inbound contacts when they've set their status to a custom status.
- The agent can't take contacts from that channel per their routing profile.

In the GetCurrentMetricData API, this metric is `SLOTS_AVAILABLE`.

Available

The number of agents who can take an inbound contact. An agent can only take inbound contacts when they manually set their status to Available in the CCP (or in some cases when their supervisor changes it).

This is different from how many more inbound contacts an agent could take. If you want to know how many more contacts an agent can have routed to them, look at the Availability metric. It indicates how many slots the agent has free.

What causes this number to go down? An agent is considered **unavailable** when:

- The agent has set their status in the CCP to a custom status, such as Break or Training. Amazon Connect doesn't count these slots because agents can't take inbound contacts when they've set their status to a custom status.
- The agent has at least one contact ongoing.
- The agent has a contact in a missed or error state, which prevents the agent from taking any more contacts until they are flipped back to routable.

In the GetCurrentMetricData API, this metric is `AGENTS_AVAILABLE`.

Average API Connecting Time

The average time between when a contact is initiated using an Amazon Connect API, and the agent is connected.

Avg abandon time

Average time, in seconds, that abandoned contacts were in the queue before being abandoned.

Avg ACW

Average time, in seconds, that contacts spent in the **After contact work** state, during the specified time range.

This is not the average amount of time agents spent on contacts.

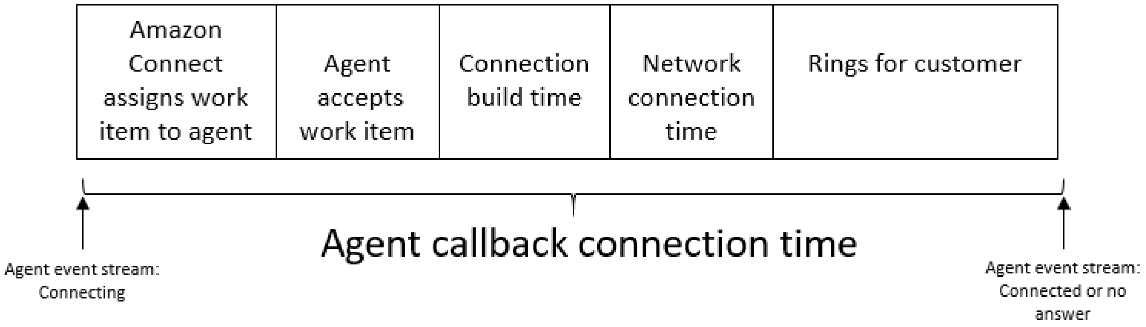
To learn more about agent status and contact states, see About agent status (p. 998) and About contact states (p. 1000).

Avg callback connecting time

Then average time between when callback contacts are initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

No equivalent to this metric is available in the GetCurrentMetricData API.

The following image shows the five parts that go into calculating **Avg callback connecting time**. It also shows what is in the agent event stream.


Amazon Connect assigns work item to agent
Agent accepts work item
Connection build time
Network connection time
Rings for customer
Agent callback connection time
Agent event stream: Connecting
Agent event stream: Connected or no answer

Avg hold time

Average time, in seconds, that a contact in the queue was on hold.

This metric doesn't apply to tasks so you'll notice a value of 0 on the report for them.

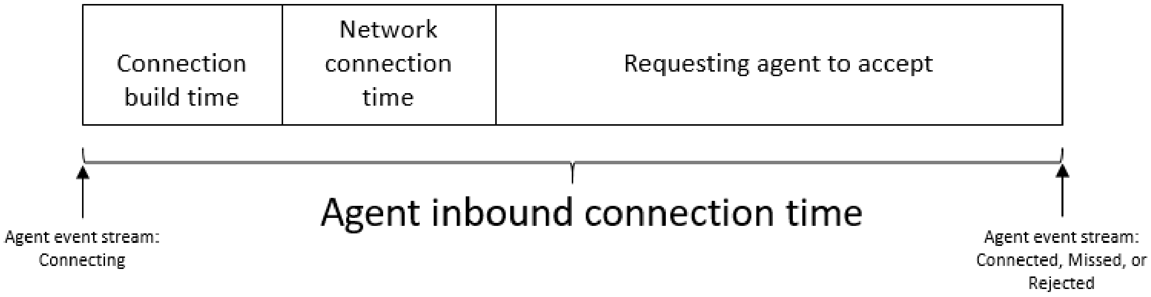
Avg incoming connecting time

The average time between when contacts are initiated Amazon Connect reserving the agent for the contact, and the agent is connected.

In the agent event stream, this time is calculated by averaging the duration between the contact state of STATE_CHANGE event changes from CONNECTING to CONNECTED/MISSED/ERROR.

No equivalent to this metric is available in the GetCurrentMetricData API.

The following image shows the three parts that go into calculating **Avg incoming connecting time**. It also shows what is in the agent event stream.


Connection build time
Network connection time
Requesting agent to accept
Agent inbound connection time
Agent event stream: Connecting
Agent event stream: Connected, Missed, or Rejected

Avg interaction time

Average time, in seconds, that contacts were connected to and interacting with agents. This does not include hold time or time spent waiting in the queue.

Avg interaction and hold time

Average time, in seconds, that contacts in the queue spent interacting with agents and on hold. This is calculated as follows:

Avg hold time + Avg interaction time

Avg queue answer time

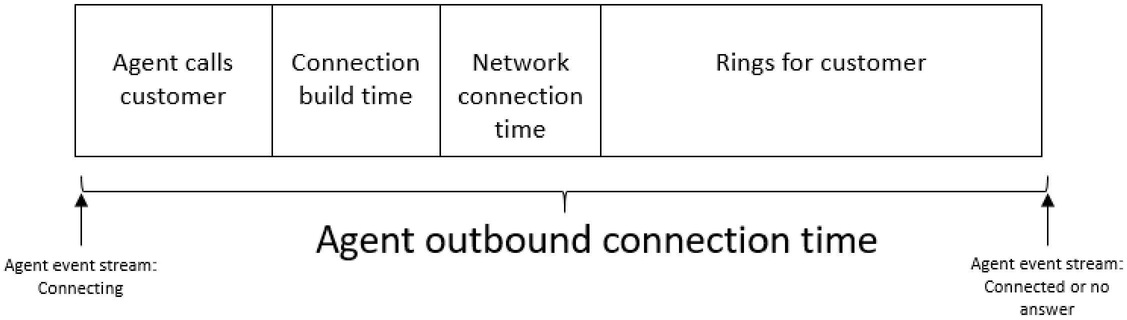
Average time, in seconds, that a contact was in the queue before being answered by an agent. This is calculated using the amount of time that the contact was in the queue, not any time that the contact spent in prior steps of the contact flow, such as listening or responding to prompts.

Avg outbound connecting time

The average time between when outbound contacts are initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

No equivalent to this metric is available in the GetCurrentMetricData API.

The following image shows the four parts that go into calculating **Avg outbound connecting time**. It also shows what is in the agent event stream.


Agent calls customer
Connection build time
Network connection time
Rings for customer
Agent outbound connection time
Agent event stream: Connecting
Agent event stream: Connected or no answer

Callback contacts handled

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

Capacity

Displays the maximum capacity that's set in the routing profile currently assigned to the agent. This column can be filtered by channel.

If an agent's routing profile is configured to handle either one voice **or** up to three chats, then their maximum capacity equals three, when not filtered by channel.

Consult

Deprecated May 2019. When used in a report, it returns a dash (-).

Count of contacts in the queue that were handled by an agent, and the agent consulted with another agent or a call center manager during the contact.

Contact State

The state of the contacts the agent is currently handling. The state can be: **Connected**, **On Hold**, **After contact work**, **Incoming**, **Calling**, or **Missed contact**.

For queued callbacks, the contact state can also **Callback incoming** or **Callback dialing**.

If a supervisor is using the Manager Monitor feature to monitor a particular agent as they interact with a customer, the superviser's contact state is Monitoring; the agent's contact state is Connected.

Duration

Amount of time that the agent has been in the current Agent Activity State.

Error

A count of agents in Error state. An agent is included in this metric if they miss a call or reject a chat/task (most common). They could also be counted if there is a connection failure.

In the GetCurrentMetricData API, this metric is `AGENTS_ERROR`.

Handled

Count of contacts in the queue that were answered by an agent.

Handled in

Count of incoming contacts handled by an agent during the specified time range that were initiated using one of the following methods: inbound call, transfer to agent, transfer to queue, or queue-to-queue transfer.

Handled out

Count of contacts handled by an agent during the specified time range that were initiated by an agent placing an outbound call using the CCP.

Hold abandons

Count of contacts that disconnected while the customer was on hold. A disconnect could be because the customer hung up while on hold, or that there was a technical issue with the contact while on hold.

In queue

Count of contacts currently in the queue.

To learn how this is different from Scheduled contacts in a callback scenario, see How Initial delay affects Scheduled and In queue metrics (p. 1004).

In the GetCurrentMetricData API, this metric is `CONTACTS_IN_QUEUE`.

Max queued

The longest time that a contact spent waiting in the queue. This includes all contacts added to the queue, even if they were not connected with an agent, such as abandoned contacts.

NPT (Non-Productive Time)

Count of agents who have set their status in the CCP to a custom status. That is, their CCP status is other than **Available** or **Offline**.

> **Tip**
> Although agents aren't routed any *new inbound* contacts while their CCP status is set to a custom status, it's possible for them to change their CCP status to a custom status while still handling a contact. For example, let's say an agent is being routed contacts very quickly. To go on break, they set their status to **Break** proactively, while still finishing up the last contact. This allows them to go on break and avoid accidentally missing a contact that's routed to them in the sliver of time between the last contact ending and setting their status to Break.
> Because agents can be **On call** or doing **ACW**, for example, while their CCP is set to a custom status, this means it's possible for agents to be counted as **On call** and **NPT** at the same time.

In the GetCurrentMetricData API, this metric is `AGENTS_NON_PRODUCTIVE`.

Occupancy

Percentage of time that an agent was active on contacts. This percentage is calculated as follows:

(Agent on contact (wall clock time) / (Agent on contact (wall clock time) + Agent idle time))

Where:

- (Agent on contact + Agent idle time) = total amount of agent time
- So (Agent on contact)/(total amount of agent time) = percentage of time agents were active on contacts.

> **Important**
> **Occupancy** doesn't account for concurrency. That is, an agent is considered 100% occupied for a given interval if they are handling at least one contact for that entire duration.

Oldest

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

In the GetCurrentMetricData API, this metric is `OLDEST_CONTACT_AGE`.

On contact

Count of agents currently on a contact. An agent is "on a contact" when they are handling at least one contact who is either connected, on hold, in After contact work, or outbound ring.

In the GetCurrentMetricData API, this metric is `AGENTS_ON_CONTACT`. This metric used to be named On call. You can still use `AGENTS_ON_CALL` to retrieve data for this metric.

Online

Count of agents who have set their status in the CCP to something other than **Offline**. For example, they may have set their status to Available, or to a custom value such as Break or Training.

The Online metric doesn't tell you how many agents can be routed contacts. For that metric, see Available (p. 919).

This metric can be confusing so let's look at an example. Say you see this in a Queues report:

- Online = 30
- On Call = 1
- NPT = 30
- ACW = 0
- Error = 0
- Available = 0

This means 30 agents have set their status in the CCP to a custom status. 1 of those 30 agents is currently on a contact.

In the GetCurrentMetricData API, this metric is `AGENTS_ONLINE`.

Queue

The name of the queue associated with the contact the agent is currently handling.

Queued

Count of contacts added to the queue during the specified time range.

Routing Profile

The routing profile for the agent.

Scheduled

Count of customers in the queue for which there is a callback scheduled.

To learn how this is different from In queue contacts in a callback scenario, see How Initial delay affects Scheduled and In queue metrics (p. 1004).

In the GetCurrentMetricData API, this metric is `CONTACTS_SCHEDULED`.

SL *X*

Percentage of contacts removed from the queue between 0 and *X* after being added to it (Service Level). A contact is removed from the queue when one of the following occurs: an agent answers the call, the customer abandons the call, or the customer requests a call back.

For X, you can can choose from pre-set times in seconds: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

Custom service levels

You can also create custom service level metrics. You can also choose from additional durations, such as minutes, hours, or days.

You can add up to 10 custom service levels per report.

The maximum duration for a custom service level is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.

Staffed

Count of agents who are online in the CCP, and not in NPT (a custom status).

Another way of thinking about this is, there are two scenarios in which **Staffed** is not incremented:

- The agent's status in the CCP is set to **Offline**.
- The agent's status in the CCP is set to a custom status.

For example, let's say an agent sets their status in the CCP to a custom status such as Break and they make an outbound call. Now the agent is **On call**, but **Staffed** is 0.

If the agent sets their status in the CCP to **Available** and makes an outbound call, the agent is **On call** and **Staffed** is 1.

This metric is available on the Queues report.

In the GetCurrentMetricData API, this metric is `AGENTS_STAFFED`.

Transferred in

Count of contacts transferred into the queue during the specified time range.

Transferred in from queue

Count of contacts transferred into the queue from another queue during a **Customer queue flow**.

Transferred in by agent

Count of contacts transferred in by an agent using the CCP.

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 by agent

Count of contacts transferred out by an agent using the CCP.

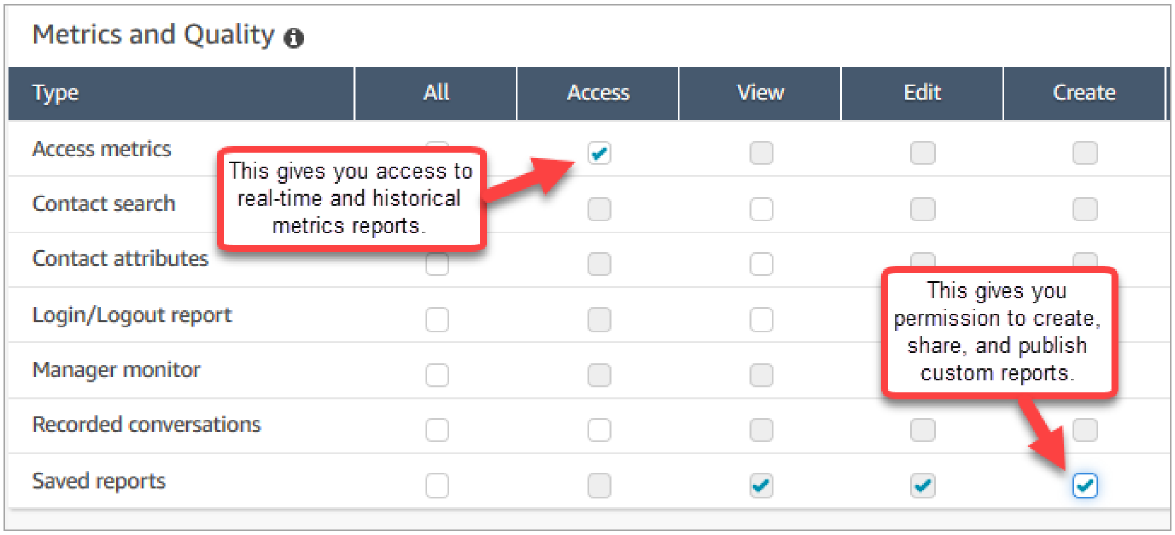
Transferred out from queue

Count of contacts transferred out of the queue to another queue during a **Customer queue flow**.

Permissions required to view real-time metrics reports

To view real-time metrics reports, you need to be assigned to a security profile that has **Access metrics** permission.

To create, share, and publish saved reports, you need the **Saved reports**, **Create** permission.



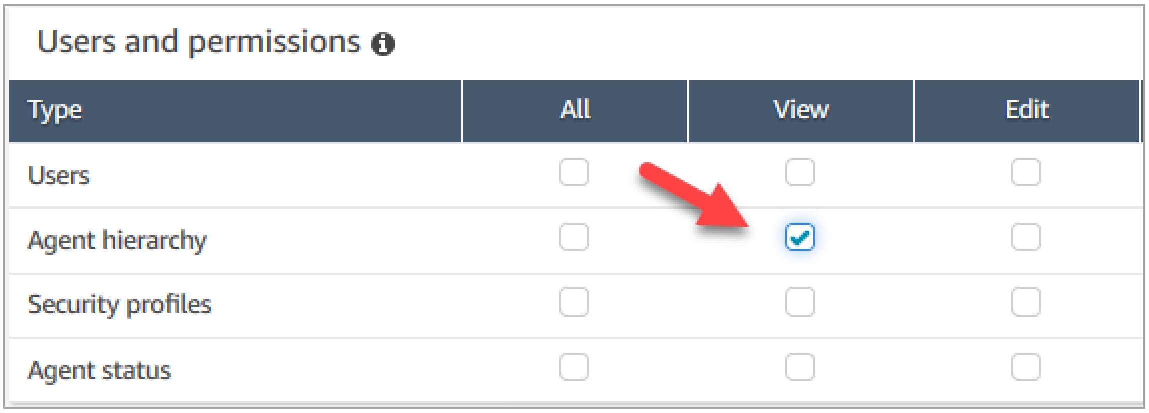
Metrics and Quality

Type	All	Access	View	Edit	Create
Access metrics	☐	☑	☐	☐	☐
Contact search		☐	☐	☐	☐
Contact attributes	☐	☐	☐	☐	☐
Login/Logout report	☐	☐	☐		
Manager monitor	☐	☐	☐		
Recorded conversations	☐	☐	☐	☐	☐
Saved reports	☐	☐	☑	☑	☑

This gives you access to real-time and historical metrics reports.

This gives you permission to create, share, and publish custom reports.

To view the agent's hierarchy information in a real-time metrics report, which can include their location and skill set data, you need the **View - Agent hierarchy** permission:



Users and permissions

Type	All	View	Edit
Users	☐	☐	☐
Agent hierarchy	☐	☑	☐
Security profiles	☐	☐	☐
Agent status	☐	☐	☐

How often real-time metrics refresh

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

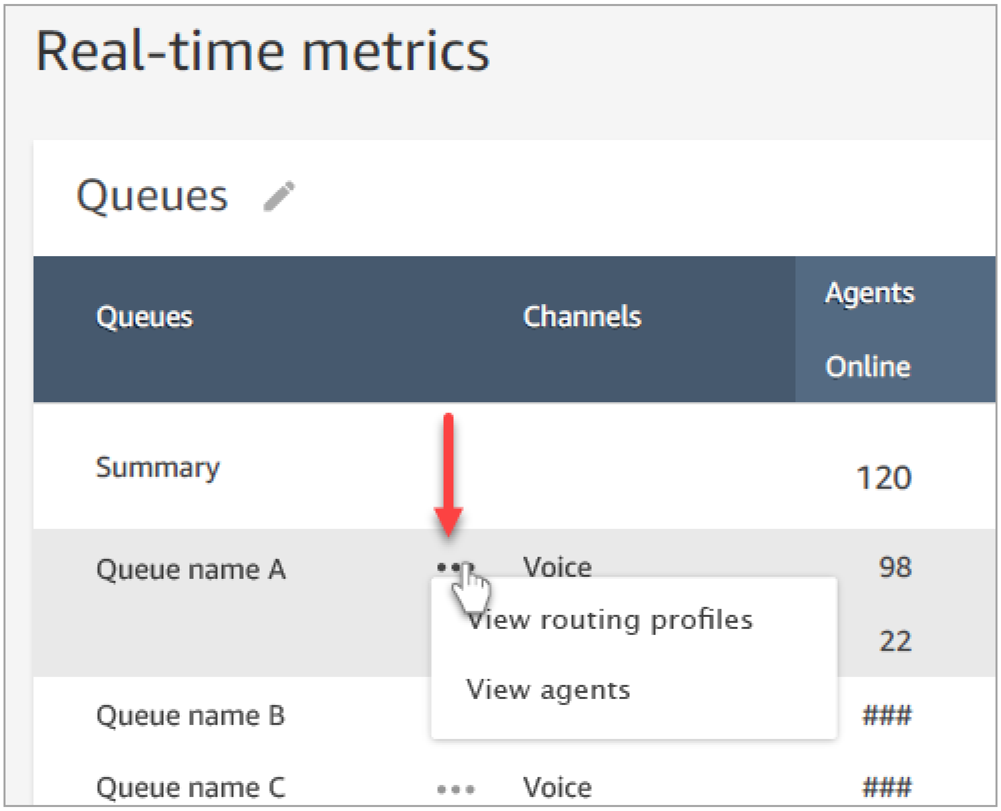
- The **Real-time metrics** page refreshes every 15 seconds, as long as the page is active. For example, if you have multiple tabs open in your browser and navigate to a different tab, the real-time metric page won't be updated until you return to it.
- Metrics such as **Active** and **Availability** refresh as activity occurs, with a small system delay for processing the activity.
- Agent near real-time metrics, such as **Missed** and **Occupancy**, refresh as activity occurs, with a small delay for processing.
- Contact near real-time metrics refresh about a minute after a contact ends.

Use one-click drill-downs for Routing profiles and Queues tables

In real-time metrics reports, for **Routing profiles** and **Queues** tables, you can open pre-filtered tables that display the associated queues, routing profiles, or agents. These one-click filters provide a way for you to drill into the performance data.

Example 1: Queues table -> Routing profiles table -> Agents table

For example, at a **Queues** table, choose the dropdown and then choose **View routing profiles**.

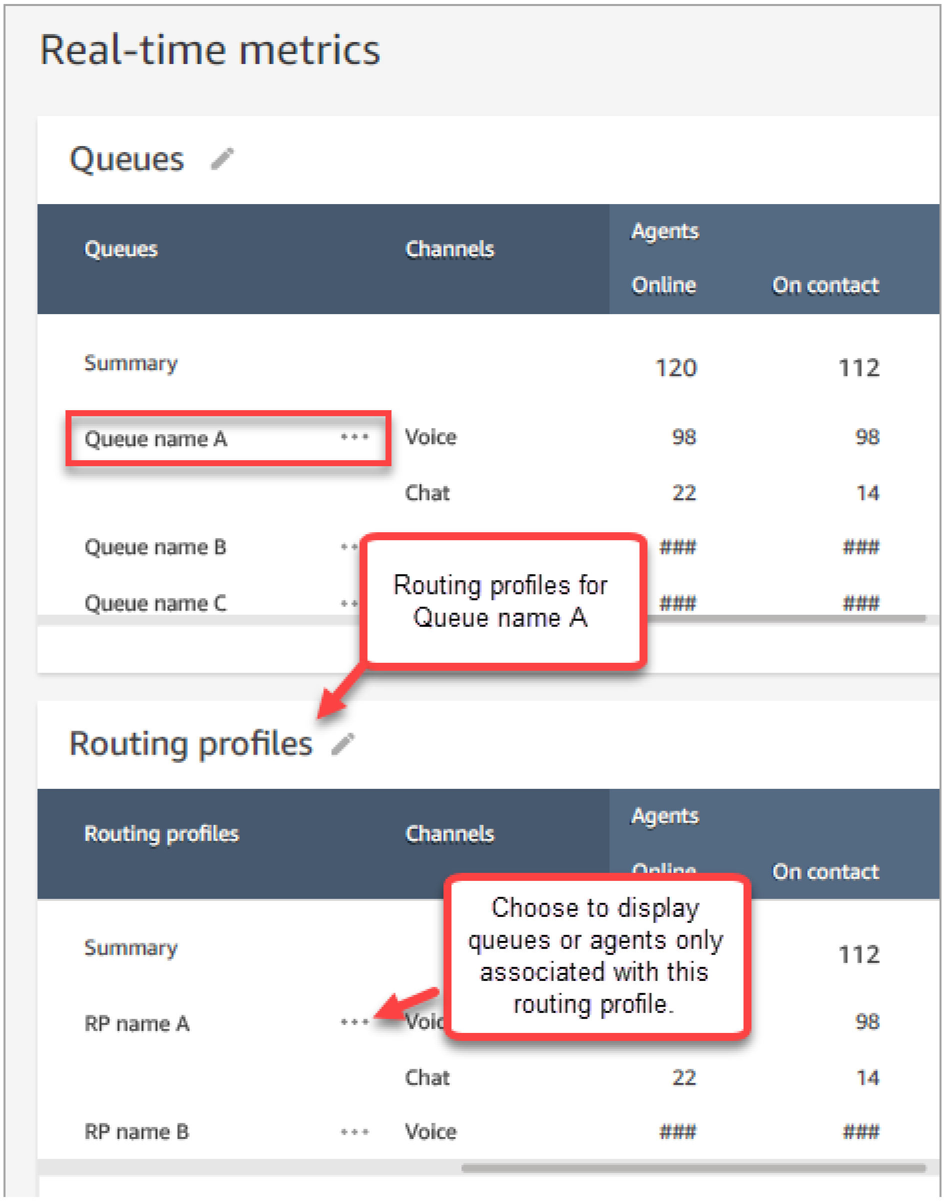


Real-time metrics

Queues

Queues	Channels	Agents Online
Summary		120
Queue name A	Voice	98
		22
Queue name B		###
Queue name C	Voice	###

Below the **Queues** table, a **Routing profiles** table appears. It is filtered to display only the routing profiles associated with the queue. On the **Routing profiles** table, you can choose quick filters to display queues or agents *only associated with that routing profile*.



Real-time metrics

Queues

Queues	Channels	Agents	
		Online	On contact
Summary		120	112
Queue name A •••	Voice	98	98
	Chat	22	14
Queue name B •••		###	###
Queue name C •••		###	###

Routing profiles for Queue name A

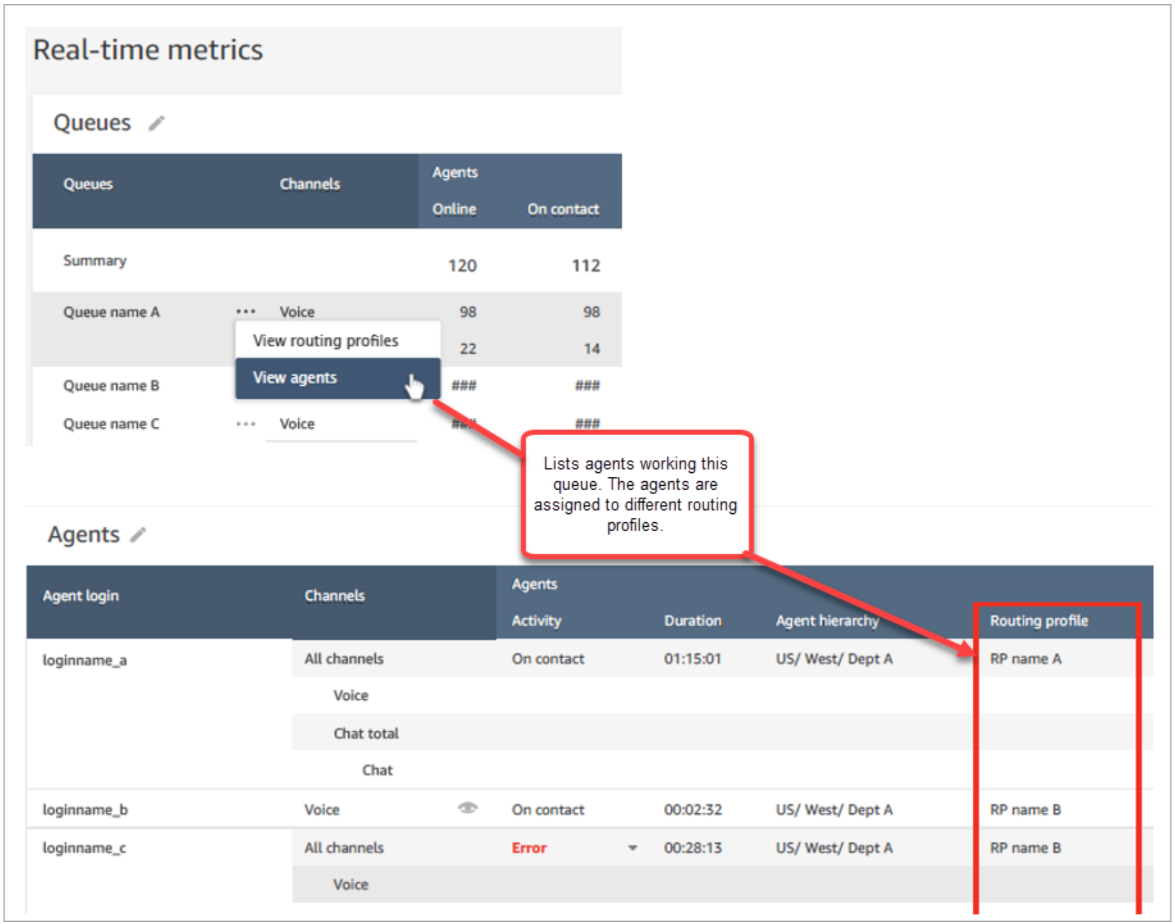
Routing profiles

Routing profiles	Channels	Agents	
		Online	On contact
Summary			112
RP name A •••	Voic		98
	Chat	22	14
RP name B •••	Voice	###	###

Choose to display queues or agents only associated with this routing profile.

Example 2: Queues table -> Agents table

At the **Queues** table, choose **View agents**. Below the **Queues** table, an **Agents** table appears. It is filtered to display all the agents working that queue. The agents may be associated with different routing profiles.



Real-time metrics

Queues

Queues	Channels	Agents	
		Online	On contact
Summary		120	112
Queue name A	Voice	98	98
		22	14
Queue name B		###	###
Queue name C	Voice	###	###

Lists agents working this queue. The agents are assigned to different routing profiles.

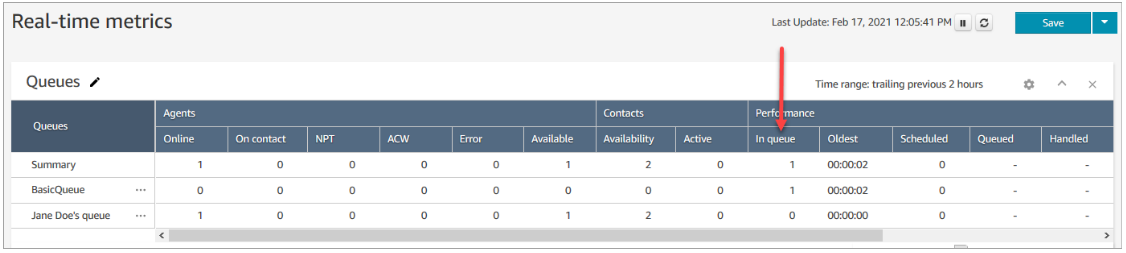
Agents

Agent login	Channels	Agents			
		Activity	Duration	Agent hierarchy	Routing profile
loginname_a	All channels	On contact	01:15:01	US/ West/ Dept A	RP name A
	Voice				
	Chat total				
	Chat				
loginname_b	Voice	On contact	00:02:32	US/ West/ Dept A	RP name B
loginname_c	All channels	Error	00:28:13	US/ West/ Dept A	RP name B
	Voice				

View how many contacts are waiting in queue

To see the number of customers waiting in queue

1. Go to **Analytics**, **Real-time metrics**, **Queues**.
2. This column counts all customers who are in waiting a queue for an agent, including the callback customers.



Real-time metrics

Last Update: Feb 17, 2021 12:05:41 PM

Queues

Time range: trailing previous 2 hours

Queues	Agents						Contacts		Performance				
	Online	On contact	NPT	ACW	Error	Available	Availability	Active	In queue	Oldest	Scheduled	Queued	Handled
Summary	1	0	0	0	0	1	2	0	1	00:00:02	0	-	-
BasicQueue	0	0	0	0	0	0	0	0	1	00:00:02	0	-	-
Jane Doe's queue	1	0	0	0	0	1	2	0	0	00:00:00	0	-	-

View how many contacts are in an agent's queue

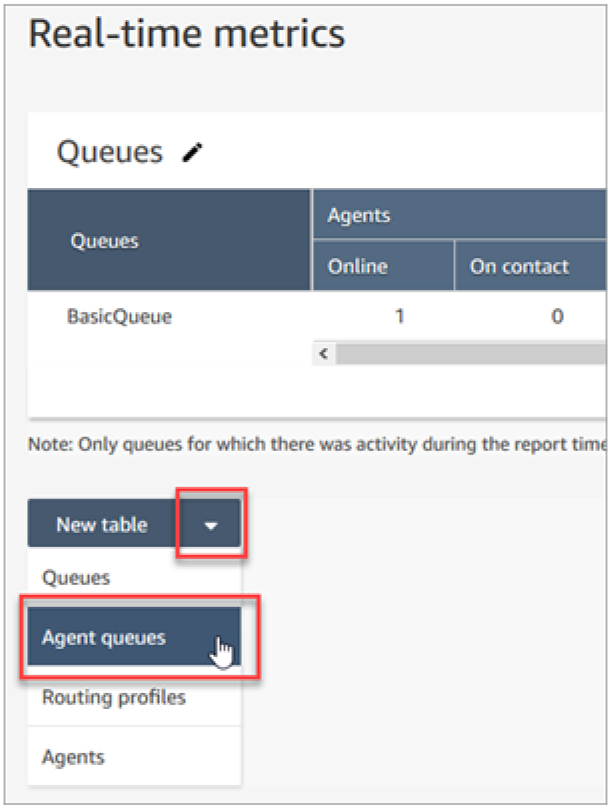
To see how many contacts are in an agent's personal queue, add an **Agent queues** table to your **Real-time metrics**, **Queues** report. Then view these two metrics:

- **In Queue**—how many contacts are in an agent's personal queue.

- **Queued**—the number of contacts added to their personal queue during the specified time range.

Use the following procedure.

1. Go to **Analytics**, **Real-time metrics**, **Queues.**
2. Choose **New table**, **Agent queues**.



Real-time metrics

Queues

Queues	Agents	
	Online	On contact
BasicQueue	1	0

Note: Only queues for which there was activity during the report time

The **In queue** column displays how many contacts are in the agent's queue.

3. Review the metrics in then **In queue** and **Queue** columns.

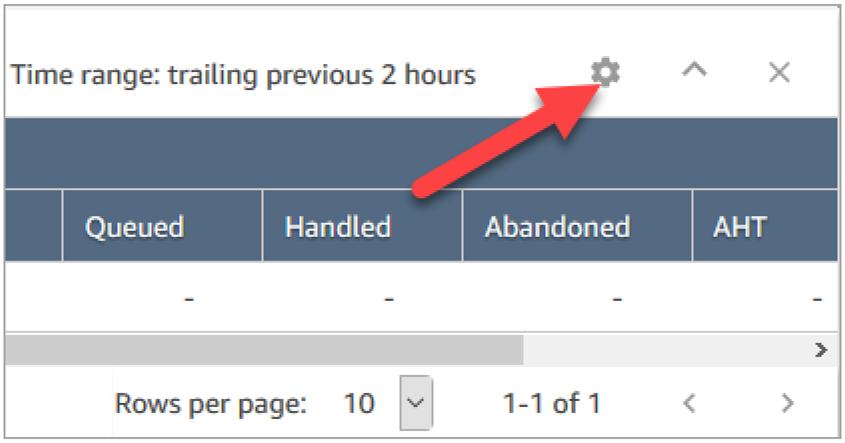
Tip

An agent is included in the **Agent queues** table only if they are online or there is at least one contact in the their queue.

Add In Queue and Queue to the Agent queue table

If **In queue** or **Queue** don't appear in your **Agent queue** table, use the following steps to add them.

1. On the **Agent queues** table, choose **Settings**.



Time range: trailing previous 2 hours

	Queued	Handled	Abandoned	AHT
	-	-	-	-

Rows per page: 10 1-1 of 1

2. Choose the **Metrics** tab.
3. Scroll to the **Performance** section and choose **In queue** and **Queue**, and then **Apply**.

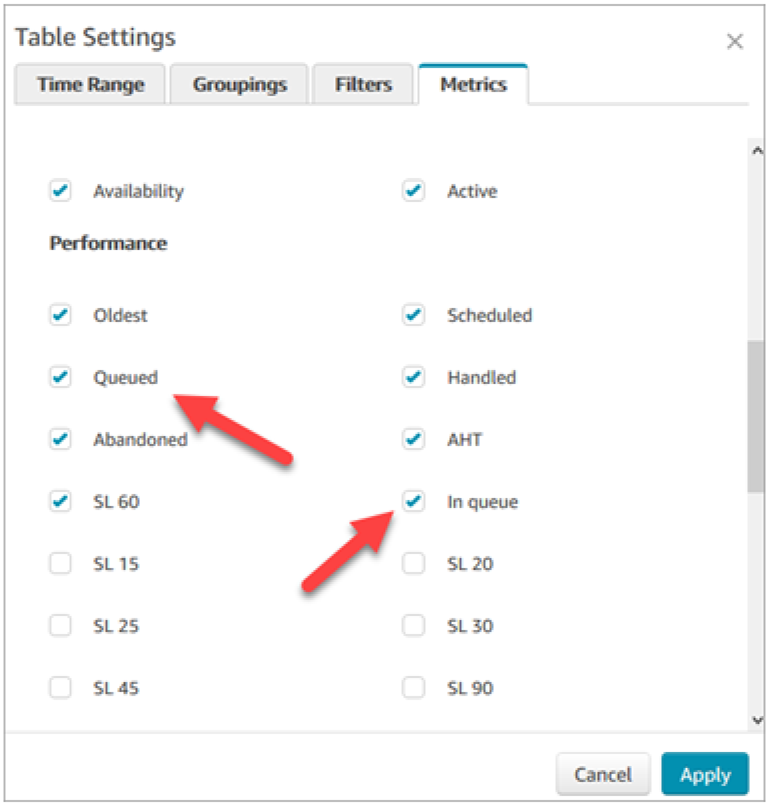


Table Settings

☑ Availability ☑ Active

Performance

☑ Oldest ☑ Scheduled
☑ Queued ☑ Handled
☑ Abandoned ☑ AHT
☑ SL 60 ☑ In queue
□ SL 15 □ SL 20
□ SL 25 □ SL 30
□ SL 45 □ SL 90

The changes appear in your table immediately.

4. Choose **Save** to add this report to your list of Saved reports.

View how many contacts are waiting for a callback

To see only the number of customers who are waiting for a call back, you need to create a queue that only takes callback contacts. To learn how to do this, see Set up routing (p. 220).

Currently there isn't a way to see the phone numbers of the contacts waiting for callbacks.

Create a real-time metrics report

You can create a real-time metrics report to view real-time or near-real time metrics data for activity in your contact center. You must have permission to access metric data. The **CallCenterManager** and **QualityAnalyst** security profiles include this permission. For more information, see Security profiles (p. 789).

To create a real-time metrics report

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. Choose **Analytics**, **Real-time metrics**.
3. Choose one of the following report types. They group and order the data in different ways and include different metrics by default.

   - **Queues**
   - **Agents**
   - **Routing profiles**
4. To add another report to the page, choose **New table** and then choose a report type. You can add multiple reports of the same report type.

   There's no limit to the number of tables you can add, but you might start experiencing performance issues if you add a lot of them.
5. To customize a report, choose the gear icon from its table.
6. On the **Time Range** tab, do the following:

   a. For **Trailing windows for time**, select the time range, in hours, for the data to include in the report.

   b. (Optional) If you select **Midnight to now**, the time range is from midnight to the current time, based on the **Time Zone** that you select. If you select a time zone other than the one you are currently in, the time range starts at midnight for the calendar day in that time zone, not your current time zone.
7. (Optional) On the **Filters** tab, specify filters to scope the data to be included in the report. The available filters depend on the report type. The following are the possible filters:

   - **Agents**—Includes data only for the agents that you select from **Include**.
   - **Agent Hierarchies**—Includes data only for the agent hierarchies that you select from **Include**.
   - **Queues**—Includes data only for the queues that you select from **Include**.
   - **Routing profiles**—Includes data only for the routing profiles that you select from **Include**.
8. On the **Metrics** tab, choose the metrics and fields to include in the report. The available metrics and fields depend on the report type and filters that you select. For more information, see Real-time metrics definitions (p. 916).
9. When you are finished customizing the report, choose **Apply**.
10. (Optional) To save your report for future reference, choose **Save**, provide a name for the report, and then choose **Save**.

    To view your saved real-time metrics reports, choose **Analytics**, **Saved reports**, and then choose the **Real-time metrics** tab.

No metrics or too few rows in a queues report?

It's possible to run a manually configured queues report and have no metrics returned, or fewer rows than expected.

This is because a queues report only includes data for a maximum of 100 queues, using one row per queue. If a queue doesn't have any activity* during the time range for the report, it's excluded from the report rather than included with null values. This means that if you create a report, and there is no activity for any of the queues included in the report, your report will not include any data.

This applies to the `GetCurrentMetricsData` API as well. This means that if a queue is not considered active, if you query for its metrics using the API you won't get any data.

> **Tip**
> *Here's how we define whether a queue is active: there's at least one contact in queue or there's at least one online agent for that queue. Otherwise, it's considered inactive.

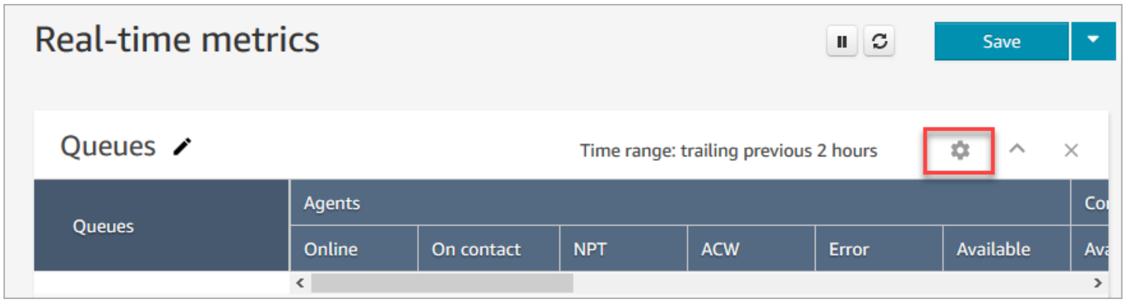
In the following situations, you could end up with no metrics or fewer rows than expected:

1. You're attempting to run a report with no filters or groupings, and have more than 100 queues in your instance. The report pulls metrics for the first 100 queues, and then displays only those that are active.
2. You're attempting to run a report with filters and groupings, but it still has more than 100 queues matching that criteria. To process this request, Amazon Connect applies all the specified filters and groupings. This pulls the first 100 queues matching that criteria. Then out of those queues, it displays only the active ones.

   For example, let's say you have 300 queues in your instance. Of these, 200 match your criteria; 100 are active and by coincidence all happen to be Queues #100-#200. When you run the report, you'd get just 1 row (Queue #100) since the other 99 queues that were returned (Queues #1-#99) were considered inactive and were not displayed.
3. You're running a report with fewer than 100 queues. While you may expect to see metrics for all filtered queues, only active queues are shown on the real-time metrics report page. Try changing the settings for the report, such as changing the time range.

List queues grouped by routing profile

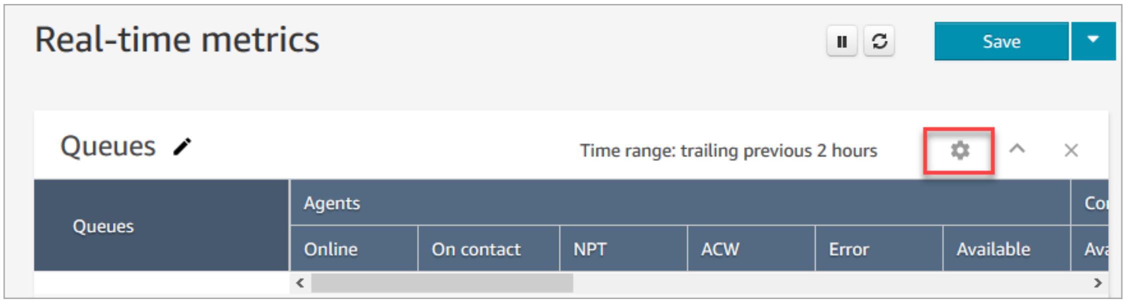
1. Go to **Analytics**, **Real-time metrics**, **Queues**.
2. Click **Settings**.



3. On the **Groupings** tab, choose **Queues grouped by routing profiles**.
4. Choose **Apply**.

List agents grouped by routing profile

1. Go to **Analytics**, **Real-time metrics**, **Queues**.
2. Choose **New table**, **Agents**.
3. Click **Settings**.



Real-time metrics

Queues

Time range: trailing previous 2 hours

Queues	Agents						Co
	Online	On contact	NPT	ACW	Error	Available	Ava

4. On the **Filters** tab, choose **Routing profiles**. In **Include**, select the routing profiles you want included in the table.

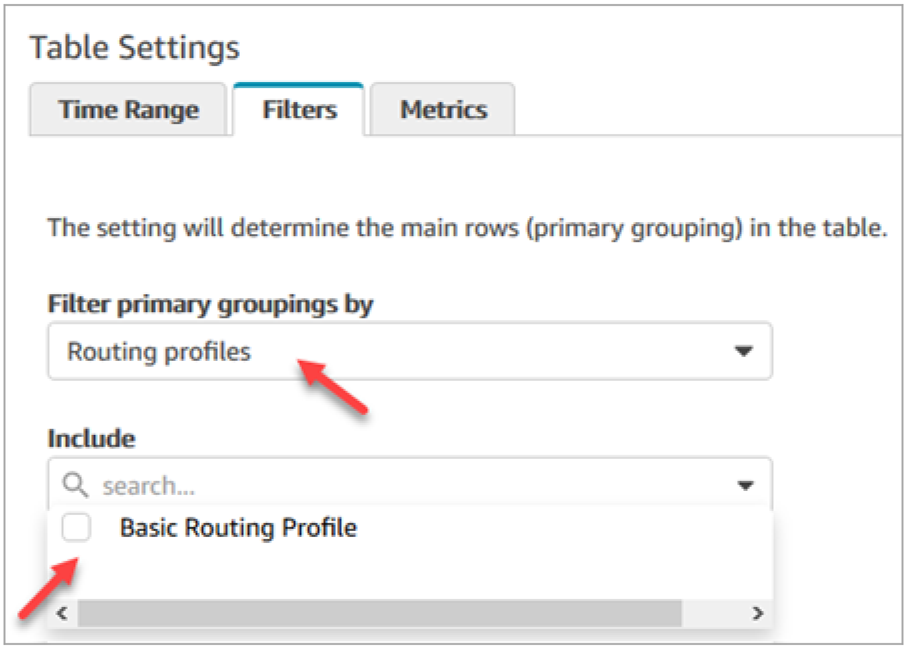


Table Settings

The setting will determine the main rows (primary grouping) in the table.

Filter primary groupings by

Routing profiles

Include

search...

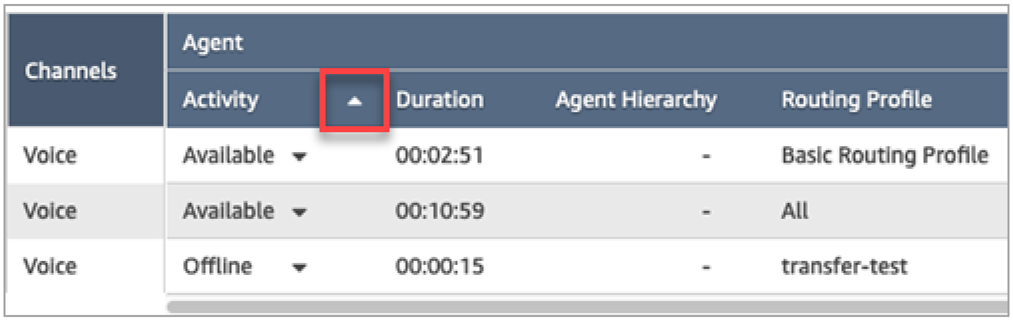
□ Basic Routing Profile

5. Choose **Apply**.

Sort agents by activity in a real-time metrics report

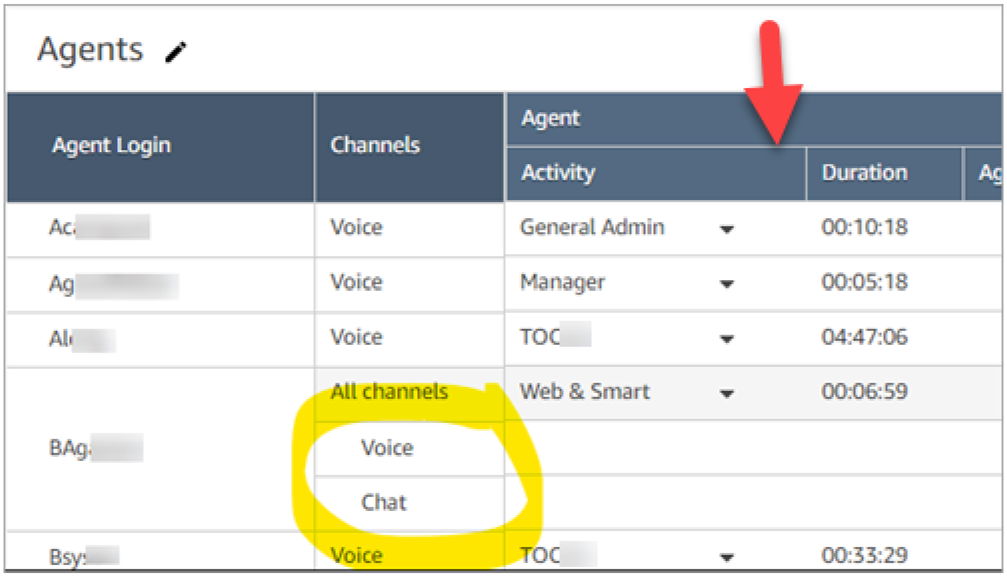
On the real-time metrics **Agents** report, you can sort agents by **Activity** when agents are enabled to use the same channel.

For example, the following image shows that you can sort agents by the **Activity** column because all the agents are enabled to use the same channel: voice.



Channels	Agent			
	Activity ▲	Duration	Agent Hierarchy	Routing Profile
Voice	Available	00:02:51	-	Basic Routing Profile
Voice	Available	00:10:59	-	All
Voice	Offline	00:00:15	-	transfer-test

However, if one or more agents are enabled to handle voice, chat, and tasks—or any two of the channels —you can't sort them by the **Activity** column because of the multiple channels. In this case, there's no option to sort by the **Activity** column, as shown in the following image:



Agents

Agent Login	Channels	Agent		Ag
		Activity	Duration	
Ac[redacted]	Voice	General Admin ▾	00:10:18	
Ag[redacted]	Voice	Manager ▾	00:05:18	
Al[redacted]	Voice	TOC[redacted] ▾	04:47:06	
BAg[redacted]	All channels	Web & Smart ▾	00:06:59	
	Voice			
	Chat			
Bsy[redacted]	Voice	TOC[redacted] ▾	00:33:29	

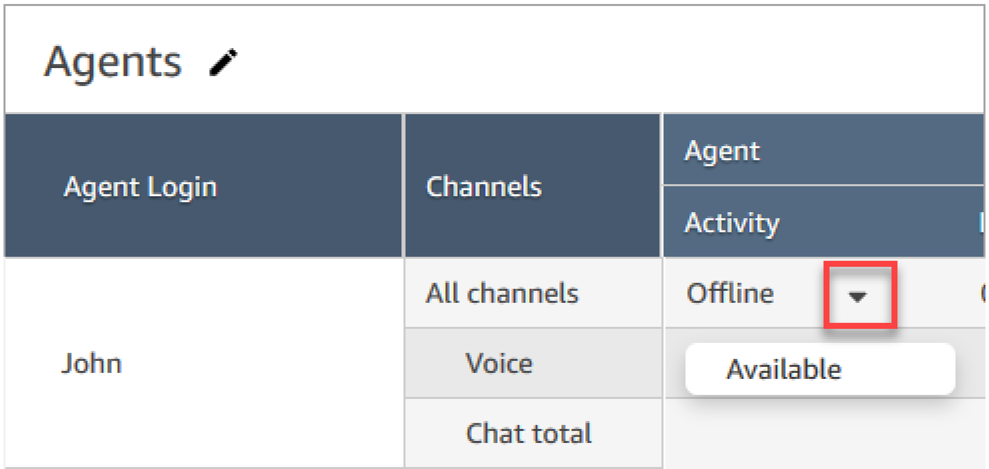
Note

The real-time metrics Agents report doesn't support secondary sorting. For example, you can't sort by **Activity**, and then sort by **Duration**.

Change the "Agent activity" status in a real-time metrics report

Agents manually set their status in the Contact Control Panel (CCP). However, on the real-time metrics report, supervisors can manually change the **Agent Activity** status of an agent. This overrides what the agent has set in the CCP.

When you choose the **Agent Activity** column, you can select a status, such as **Offline**, **Available**, or **Break**.

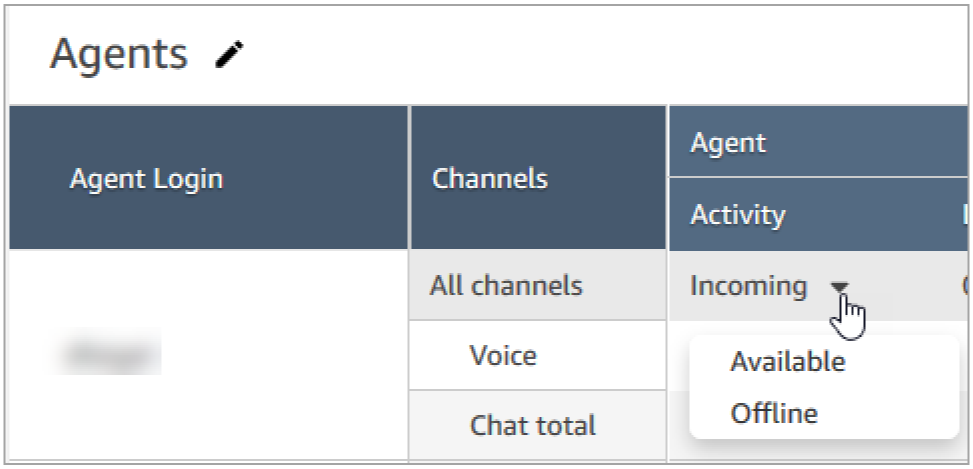


Agents

Agent Login	Channels	Agent
		Activity
John	All channels	Offline ▾
	Voice	Available
	Chat total	

This change appears in the agent event stream.

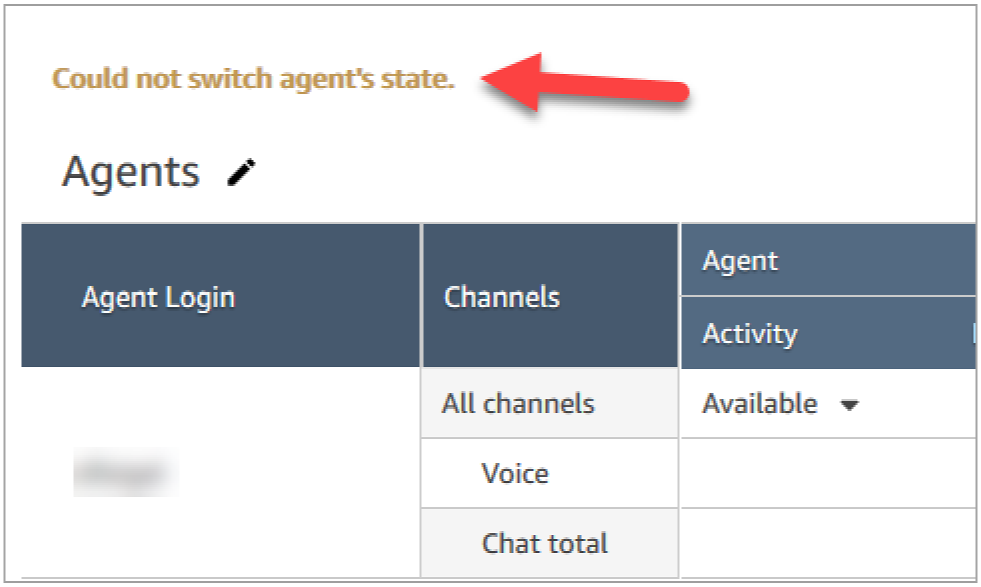
You can't select or change any of the contact states that appear in the **Agent Activity** column, such as **Incoming** or **On contact**.



Agents

Agent Login	Channels	Agent Activity
[redacted]	All channels	Incoming
	Voice	
	Chat total	

You'll get an error message, as shown in the following image.



Could not switch agent's state.

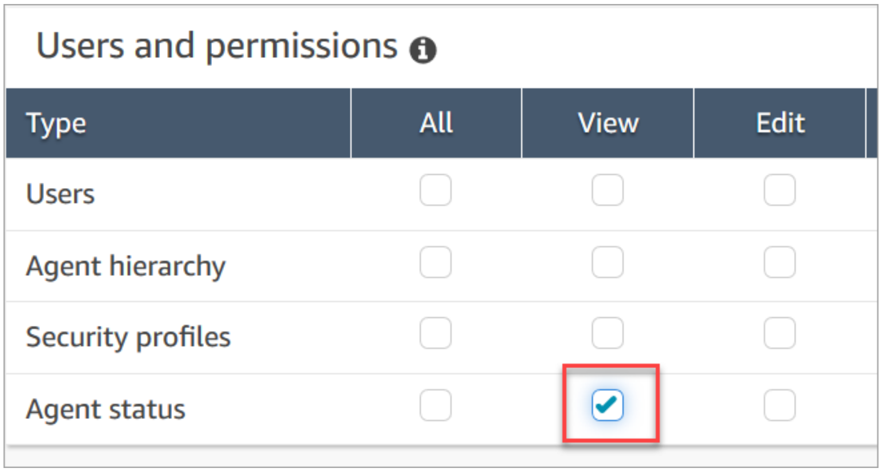
Agents

Agent Login	Channels	Agent Activity
[redacted]	All channels	Available
	Voice	
	Chat total	

Required permissions to change an agent's activity status

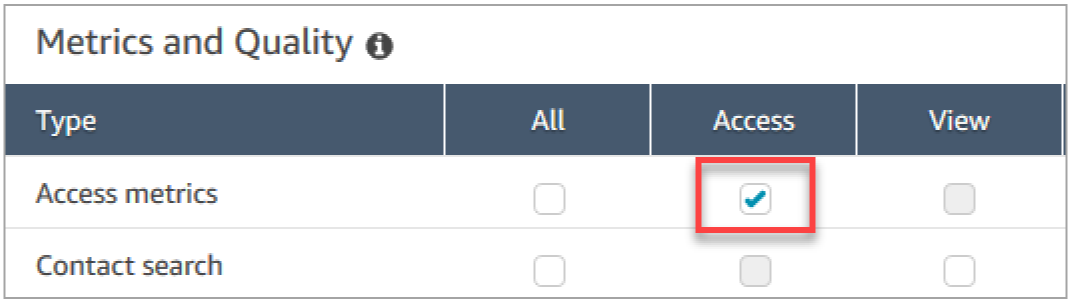
For someone such as a supervisor to be able to change an agent's activity status, they need to be assigned a security profile that has the following permissions:

- View - Agent Status
- Access metrics



Users and permissions

Type	All	View	Edit
Users	☐	☐	☐
Agent hierarchy	☐	☐	☐
Security profiles	☐	☐	☐
Agent status	☐	☑	☐



Metrics and Quality

Type	All	Access	View
Access metrics	☐	☑	☐
Contact search	☐	☐	☐

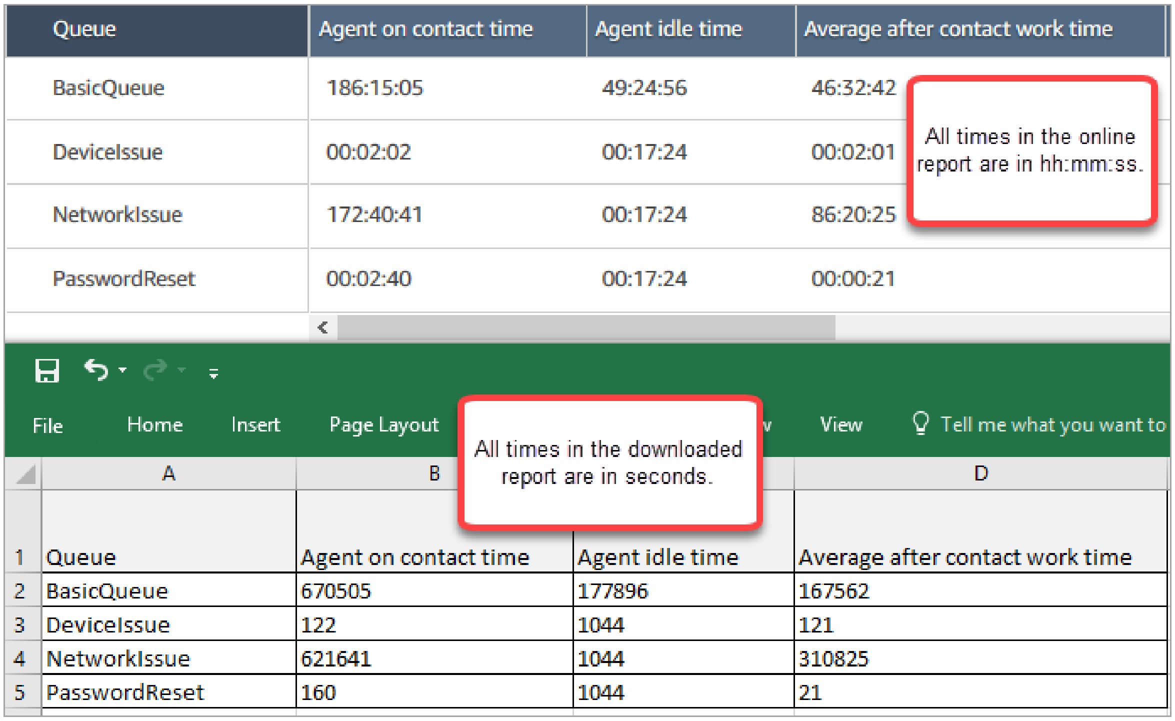
Download a real-time metrics report

You can download the data included in your report as a comma-separated value (CSV) file so that you can use it with other applications. If there is no data for one of the selected metrics, the field in the downloaded CSV file contains a dash.

All exported times are in seconds.

To download a real-time metrics report as a CSV file

1. Create the report.
2. Choose the down arrow next to **Save** in the top-right corner of the page and choose **Download CSV**.
3. When prompted, confirm whether to open or save the file.



Queue	Agent on contact time	Agent idle time	Average after contact work time
BasicQueue	186:15:05	49:24:56	46:32:42
DeviceIssue	00:02:02	00:17:24	00:02:01
NetworkIssue	172:40:41	00:17:24	86:20:25
PasswordReset	00:02:40	00:17:24	00:00:21

All times in the online report are in hh:mm:ss.

All times in the downloaded report are in seconds.

	A	B	C	D
1	Queue	Agent on contact time	Agent idle time	Average after contact work time
2	BasicQueue	670505	177896	167562
3	DeviceIssue	122	1044	121
4	NetworkIssue	621641	1044	310825
5	PasswordReset	160	1044	21

You can convert the seconds to minutes using an Excel formula. Alternatively, if you have a short report, you can copy and paste the data from Amazon Connect to Excel and it will preserve the format.

Historical metrics reports

Historical metrics reports include data about past, completed activity and performance in your contact center. Amazon Connect includes built-in historical reports that you can start using right away. You can also build your own custom reports.

When creating and analyzing your historical metrics reports, keep in mind that there are two categories of metrics:

Contact record-driven metrics

> These metrics are based on formed contact record records. For a given interval, contact records whose disconnect date falls in the interval are selected to calculate metrics. For example, if a contact starts at 05:23 and ends at 06:15, this contact contributes 52 minutes of metrics for the 06:00-06:30 interval.
>
> Example contact record-driven metrics are **Service level**, **Agent interaction time**, and **After contact work time**.

Agent activity-driven metrics

> These metrics are based on agent activities, like agent status changes, agent conversation changes. The metrics reflect on the actual time the activity happens. For example, if agent handles a contact from 05:23 to 06:15, the **Agent on contact time** has 7 minutes for the 05:00-05:30 interval, 30 minutes for the 05:30-06:00 interval, and 15 minutes for the 06:00-06:30 interval.
>
> For example, an agent activity-driven metric is **Non-Productive Time**.

You can customize the report settings to get the view of the data that is most meaningful for your organization. You can change the time frame for the report, which metrics are included in the report, and how data is grouped in the report. After you have customized a report, you can save it for future reference. You can generate a report using a recurring schedule that you define.

Contents

Historical metrics definitions

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

> **Tip**
> Developers can use the GetMetricData API to get a subset of the following historical metrics from the specified Amazon Connect instance.

After contact work time

The total time that an agent spent doing ACW for a contact.

You specify the amount of time an agent has to do ACW in their agent configuration settings (p. 233). When a conversation with a contact ends, the agent is automatically allocated to do ACW for the contact. They stop doing ACW for a contact when they indicate they are ready for another contact in the CCP.

In the GetMetricData API, this metric is AFTER_CONTACT_WORK_TIME.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Agent answer rate

Percentage of contacts routed to an agent that were answered.

- Type: String
- Min value: 0.00%
- Max value: 100.00%
- Category: Agent activity-driven metric

Agent API connecting time

The total time between when a contact is initiated using an Amazon Connect API, and the agent is connected.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Agent callback connecting time

The total time between when a callback contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Agent first name

The first name of the agent, as entered in their Amazon Connect user account. This metric is available only when grouping by agent.

- Type: String
- Length: 1-255

Agent idle time

After the agent sets their status in the CCP to **Available**, this is the amount of time they weren't handling contacts + any time their contacts were in an Error state.

Agent idle time doesn’t include the amount of time from when Amazon Connect starts routing the contact to the agent, to when agent picks up or declines the contact.

- Type: String (*hh:mm:ss*)
- Category: Agent activity-driven metric

Agent incoming connecting time

The total time between when a contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

In the agent event stream, this is the duration between the contact state of STATE_CHANGE event changes from CONNECTING to CONNECTED/MISSED/ERROR.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Agent interaction and hold time

Sum of Agent interaction time (p. 940) and Customer hold time (p. 949).

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Agent interaction time

Total time that agents spent interacting with customers on inbound and outbound contacts. This does not include Customer Hold Time (p. 949) or After Contact Work Time (p. 939).

- Type: String (*hh:mm:ss*)
- Category: contact record-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. 949) and After Contact Work Time (p. 939). This does **not** include time spent on a contact while in a custom status or **Offline** status. (Custom status = the agent's CCP status is other than **Available** or **Offline**. For example, Training would be a custom status.)

> **Tip**
> If you want to include the time spent in a custom status and **Offline** status, see Contact handle time (p. 945).

- Type: String (*hh:mm:ss*)
- Category: Agent activity-driven metric

Agent outbound connecting time

The total time between when an outbound contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

API contacts

Count of contacts that were initiated using an Amazon Connect API operation, such as `StartOutboundVoiceContact`. This includes contacts that were not handled by an agent.

- Type: Integer
- Category: contact record-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.

In the GetMetricData API, this metric is API_CONTACTS_HANDLED.

- Type: Integer
- Category: contact record-driven metric

Average after contact work time

Average amount of time that an agent spent doing After Contact Work (ACW) for contacts. This is calculated by averaging AfterContactWorkDuration (p. 986) (from the contact record) for all contacts included in the report, based on the selected filters.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Average agent API connecting time

The average time between when a contact is initiated using an Amazon Connect API, and the agent is connected.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Average agent callback connecting time

The average time between when a callback contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Average agent incoming connecting time

The average time between when contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected. This is the ring time for configurations where the agent is not set to auto-answer.

No equivalent to this metric is available in the `GetMetricData` API.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Average agent interaction and customer hold time

Average of the sum of the agent interaction and customer hold time. This is calculated by averaging the sum of the following values from the contact record: AgentInteractionDuration (p. 986) and CustomerHoldDuration (p. 986).

In the GetMetricData API, this metric is INTERACTION_AND_HOLD_TIME.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Average agent interaction time

Average time that agents interacted with customers during inbound and outbound contacts. This does not include Customer Hold Time (p. 949) or After Contact Work Time (p. 939).

In the GetMetricData API, this metric is INTERACTION_TIME.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Average agent outbound connecting time

The average time between when an outbound contact is initiated by Amazon Connect reserving the agent for the contact, and the agent is connected.

Type: String (hh:mm:ss)

Category: Agent activity-driven metric

Average customer hold time

Average time that customers spent on hold while connected to an agent. This is calculated by averaging CustomerHoldDuration (p. 986) (from the contact record).

In the GetMetricData API, this metric is HOLD_TIME.

This average only includes contacts that went on hold.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

This metric doesn't apply to tasks so you'll notice a value of 0 on the report for them.

Average handle time

The average time, from start to finish, that a contact was connected with an agent (average handled time). It includes talk time, hold time, and After Contact Work (ACW) time.

AHT is calculated by averaging the amount of time between the contact being answered by an agent and the conversation ending. It applies to both inbound and outbound calls.

In the GetMetricData API, this metric is HANDLE_TIME.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Average outbound after contact work time

Average time that agents spent doing After Contact Work (ACW) for an outbound contact.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Average outbound agent interaction time

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

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Average queue abandon time

Average time that contacts waited in the queue before being abandoned. This is calculated by averaging the difference between EnqueueTimestamp (p. 993) and DequeueTimestamp (p. 993) (from the contact record) for abandoned contacts.

A contact is considered abandoned if it was removed from a queue but not answered by an agent or queued for callback.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

In the GetMetricData API, this metric is ABANDON_TIME.

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. 993) (from the contact record).

In the GetMetricData API, this metric is QUEUE_ANSWER_TIME.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Callback contacts

Count of contacts that were initiated from a queued callback.

- Type: Integer

- Category: contact record-driven metric

Callback contacts handled

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

In the GetMetricData API, this metric is CALLBACK_CONTACTS_HANDLED.

- Type: Integer
- Category: contact record-driven metric

Contact flow time

Total time a contact spent in a contact flow.

Outbound contacts don't start in a contact flow, so outbound contacts aren't included.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Contact handle time

Total time that an agent spent on contacts, including Customer Hold Time (p. 949) and After contact work time (p. 939). This includes any time spent on contacts while in a custom status. (Custom status = the agent's CCP status is other than **Available** or **Offline**. For example, Training would be a custom status.)

> **Tip**
> If you want to exclude the amount of time spent in a custom status, see Agent on contact time (p. 941).

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Contact abandoned

Count of contacts disconnected by the customer while in the queue. Contacts queued for callback are not counted as abandoned. When you create customized historical reports, to include this metric, on the **Groupings** tab choose either **Queue** or **Phone Number**.

In the GetMetricData API, this metric is CONTACTS_ABANDONED.

- Type: Integer
- Category: contact record-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: contact record-driven metric

Contacts agent hung up first

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

In the GetMetricData API, this metric is CONTACTS_AGENT_HUNG_UP_FIRST.

- Type: Integer
- Category: contact record-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. 993). The possible values for *X* are: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600.

- Type: Integer
- Category: contact record-driven metric

Contacts consulted

Deprecated May 2019. When used in a report, it returns a dash (-).

Count of contacts handled by an agent who consulted with another agent in Amazon Connect. The agent interacts with the other agent, but the customer is not transferred to the other agent.

In the GetMetricData API, this metric is CONTACTS_CONSULTED.

- Type: Integer
- Category: contact record-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**.

In the GetMetricData API, this metric is CONTACTS_HANDLED.

- Type: Integer
- Category: contact record-driven metric

Contacts handled incoming

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

In the GetMetricData API, this metric is CONTACTS_HANDLED_INCOMING

- Type: Integer
- Category: contact record-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.

In the GetMetricData API, this metric is CONTACTS_HANDLED_OUTBOUND

- Type: Integer
- Category: contact record-driven metric

Contacts hold agent disconnect

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

- Type: Integer
- Category: contact record-driven metric

Contacts hold customer disconnect

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

In the GetMetricData API, this metric is CONTACTS_HOLD_ABANDONS.

- Type: Integer
- Category: contact record-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: contact record-driven metric

Contacts incoming

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

- Type: Integer
- Category: contact record-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**.

In the GetMetricData API, this metric is CONTACTS_MISSED

- 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: contact record-driven metric

Contacts queued

Count of contacts placed in the queue.

In the GetMetricData API, this metric is CONTACTS_QUEUED.

- Type: Integer
- Category: contact record-driven metric

Contacts transferred in

Count of contacts transferred in from queue to queue, and transferred in by an agent using the CCP.

In the GetMetricData API, this metric is CONTACTS_TRANSFERRED_IN.

- Type: Integer
- Category: contact record-driven metric

Contacts transferred in by agent

Count of contacts transferred in by an agent using the CCP.

In the GetMetricData API, this metric is CONTACTS_TRANSFERRED_IN_BY_AGENT.

- Type: Integer
- Category: contact record-driven metric

Contacts transferred in from queue

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

In the GetMetricData API, this metric is CONTACTS_TRANSFERRED_IN_FROM_Q.

- Type: Integer
- Category: contact record-driven metric

Contacts transferred out

Count of contacts transferred out from queue to queue, and transferred out by an agent using the CCP.

In the GetMetricData API, this metric is CONTACTS_TRANSFERRED_OUT.

- Type: Integer
- Category: contact record-driven metric

Contacts transferred out by agent

Count of contacts transferred out by an agent using the CCP.

In the GetMetricData API, this metric is CONTACTS_TRANSFERRED_OUT_BY_AGENT.

- Type: Integer
- Category: contact record-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: contact record-driven metric

Contacts transferred out queue

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

In the GetMetricData API, this metric is CONTACTS_TRANSFERRED_OUT_FROM_QUEUE.

- Type: Integer
- Category: contact record-driven metric

Contacts transferred out internal

Count of contacts for the queue that an agent transferred to an internal source, such as a queue or another agent. An internal source is any source that can be added as a Quick Connect.

- Type: Integer
- Category: contact record-driven metric

Customer hold time

Total time that customers spent on hold after being connected to an agent. This includes time spent on a hold when being transferred, but does not include time spent in a queue.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Error status time

For a specific agent, the total time contacts were in an error status. This metric can't be grouped or filtered by queue.

- Type: String (*hh:mm:ss*)
- Category: Agent activity-driven metric

Maximum queued time

The longest time that a contact spent waiting in the queue. This includes all contacts added to the queue, even if they were not connected with an agent, such as abandoned contacts.

In the GetMetricData API, this metric is QUEUED_TIME.

- Type: String (*hh:mm:ss*)
- Category: contact record-driven metric

Non-Productive Time

Total time that agents spent in a custom status (p. 232). That is, their CCP status is other than **Available** or **Offline**.

This metric doesn't mean that the agent was spending their time unproductively.

> **Tip**
> Agents can handle contacts while their CCP status is set to a custom status. For example, agents can be **On contact** or doing **ACW** while their CCP is set to a custom status. This means it's possible for agents to be counted as **On contact** and **NPT** at the same time.

This metric can't be grouped or filtered by queue.

- Type: String (*hh:mm:ss*)
- Category: Agent activity-driven metric

Occupancy

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

(Agent on contact (wall clock time) / (Agent on contact (wall clock time) + Agent idle time))

Where:

- (Agent on contact + Agent idle time) = total amount of agent time
- So (Agent on contact)/(total amount of agent time) = percentage of time agents were active on contacts.

> **Important**
> **Occupancy** doesn't account for concurrency. That is, an agent is considered 100% occupied for a given interval if they are handling at least one contact for that entire duration.
> In the GetMetricData API, this metric is OCCUPANCY.

- Type: String

- Min value: 0.00%
- Max value: 100.00%
- Category: Agent activity-driven metric

Online time

Total time that an agent spent with their CCP set to a status other than **Offline**. This includes any time spent in a custom status. This metric can't be grouped or filtered by queue, phone number, or channels.

- Type: String
- Category: Agent activity-driven metric

Service level *X*

Percentage of contacts removed from the queue between 0 and *X* after being added to it. A contact is removed from a queue when the following occurs: an agent answers the contact, the customer abandons the contact, or the customer requests a call back.

For *X* you can choose from pre-set times in seconds: 15, 20, 25, 30, 45, 60, 90, 120, 180, 240, 300, and 600. This percentage is calculated as follows:

(Contacts removed from queue in *X* seconds / Contacts queued) * 100

In the GetMetricData API, this metric is SERVICE_LEVEL.

- Type: String
- Min value: 0.00%
- Max value: 100.00%
- Category: contact record-driven metric

Custom service levels

You can also create custom service level metrics. Choose from additional durations, such as minutes, hours, or days.

Custom service levels are localized to the report where they are created. For example, you create a report that has a custom service level of 75. You leave the page and then create another report. The custom service level 75 won't exist in the second report. You'll need to create it again.

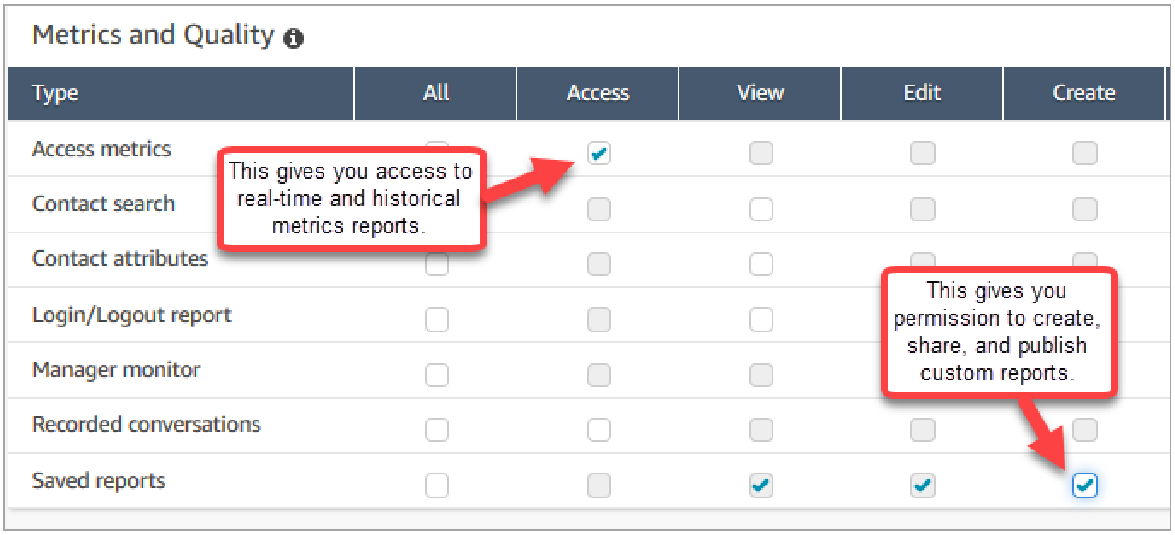
The maximum duration for a custom service level is 7 days. That's because in Amazon Connect you can't have a contact that goes longer than 7 days.

You can add up to 10 custom service levels per report.

Permissions required to view historical metrics reports

To view historical metrics reports, you need to be assigned to a security profile that has **Access metrics** permission.

To create, share, and publish saved reports, you need the **Saved reports**, **Create** permission.



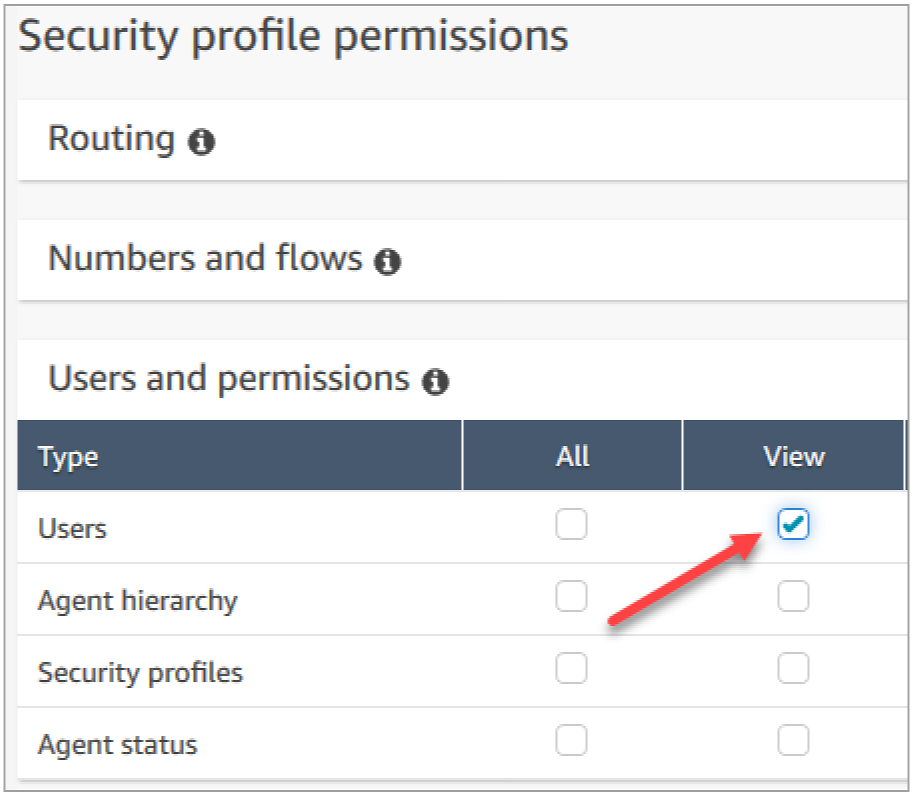
Metrics and Quality

Type	All	Access	View	Edit	Create
Access metrics	□	☑	□	□	□
Contact search		□	□	□	□
Contact attributes	□	□	□	□	□
Login/Logout report	□	□	□		
Manager monitor	□	□	□		
Recorded conversations	□	□	□	□	□
Saved reports	□	□	☑	☑	☑

This gives you access to real-time and historical metrics reports.

This gives you permission to create, share, and publish custom reports.

To view the Agent activity audit report, you need **Users**, **View** permissions:



Security profile permissions

Routing

Numbers and flows

Users and permissions

Type	All	View
Users	□	☑
Agent hierarchy	□	□
Security profiles	□	□
Agent status	□	□

Create a historical metrics report

Although Amazon Connect includes built-in historical reports, you can create your own custom reports so you look at only the data that's of interest to your organization.

Requirement

- You must have permission to access metric data. The following security profiles include this permission: **CallCenterManager** and **QualityAnalyst**. For more information, see Security profiles (p. 789).

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 at https://*instance name*.my.connect.aws/.
2. Choose **Analytics**, **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. 953).
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. 953).
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. 939).
9. When you are finished customizing your report, choose **Apply**.
10. (Optional) To save your report for future use, choose **Save**, provide a name for the report, and then choose **Save**.

Historical report limits

Historical metrics reports have the following limits:

Data only for active queues

- You can get data only for active queues. A queue is inactive if there are no contacts in the queue and no agents available.

Query data for three days at a time, for the past 35 days

- When you create a report that uses 15 minute intervals, you can return data for three days at a time, for the past 35 days. For 30 minute intervals you can return data for only three days at a time, but the data is available based on the retention period of contact records.

The availability of historical metric data is based on the retention period of contact records

- Historical metrics are based contact records. For the current retention period for contact records, see Feature specifications (p. 1210).

80k cell limit

There is currently an 80k cell limitation on historical metrics reports and scheduled reports. This applies to the total number of cells (columns * rows), accounting for grouping and filtering.

For example, let's say you create a historical metrics report with this criteria:

- Grouped by agents
- With an interval of 30 minutes
- For the last 24 hours
- Configured to include only 5 metrics
- Filtered to show only contacts handled in BasicQueue

If only 10 agents handled contacts in BasicQueue during this time, then you would expect to see (24*2)*5*10 = 2400 cells that count towards the 80k limit.

A message informs you if you reach the limit.

Schedule a historical metrics report

Before you schedule a historical metrics report, here are a few things you need to know:

Others can access the report

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

Scheduled reports are located in an Amazon S3 bucket

- Scheduled reports are saved as CSV files in the Amazon S3 bucket specified for reports for your contact center. When you set up the scheduled report, you can add a prefix to the location in Amazon S3 for the report files.
- When the report is exported to your Amazon S3 bucket, the file name includes the date and UTC time when the report was created. The **Last modified date** for the file is displayed using the time zone for the Amazon S3 bucket, and may not match the creation time for the report, which is in UTC.

There's a 15 minute delay

- For scheduled reports, there is a delay of 15 minutes after the scheduled report time before the report is generated. This is to ensure that the report includes the data for all of the activity that occurred during the time range specified for the report. Data from your contact center is not immediately processed and available to include in reports, so some data from the time range might not be captured in a report if the report is generated at the second the time range ends.
- For example, if you create a scheduled report for time frame of 8:00 AM to 5:00 PM, and there is activity in your contact center between 4:46:00 PM and 4:59:59 PM, the data about that activity may not be aggregated prior 5:00 PM when the report is scheduled to generate. Instead, the report is generated after 5:15 PM, by which time the data for the last 15 minutes of the time range is included in the report.

A scheduled Yesterday report works like a Last 24 hours report

- Usually **Yesterday** specifies the previous calendar day while **Last 24 hours** specifies the 24 hours prior to the current time. However, if you schedule to run a **Yesterday** report, it will work like a **Last 24 hours** report.

All scheduled reports use the UTC day, regardless of the timezone of the report

- For example, let's say you are in PST (Pacific Standard Time) and you schedule a **Last 24 hours** report to run at 16:00 every day. Here's the logic we use to run the report on May 15, 2020, for example:

Item	Value
Current time	2020-05-15T16:00:00.000Z
Minus 24 hours	2020-05-14T16:00:00.000Z
Get the date	2020-05-14
Get the time range	2020-05-14T00:00:00.000Z - 2020-05-15T00:00:00.000Z (this is the UTC day)

No message if a scheduled report doesn't run

- If a scheduled report fails to run, you won't get any message in the Amazon Connect UI. You just won't see the report in the Amazon S3 location.

Use your messaging system to email scheduled reports

- To email a scheduled report to a list of co-workers, you need to generate the email manually using your messaging system. Amazon Connect doesn’t provide an option to email the scheduled report automatically.

How to schedule a historical metrics report

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. Create a new report and save it, or open a saved report.
3. Choose the down arrow next to **Save** in the top-right corner of the page and choose **Schedule**.

4. On the **Recurrence** tab, specify how often this report should be run (for example, weekly on Saturdays) and the range (for example, from midnight for the previous 5 days).
5. (Optional) On the **Delivery Options** tab, specify a prefix for the location in Amazon S3 for the report files.
6. Choose **Create**.

How to delete a scheduled report

To get to the page where you can delete a scheduled report, you need to create another temporary scheduled report.

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. On the navigation menu, choose **Analytics**, **Saved reports**.
3. On the **View reports** page, choose the **Historical metrics** tab.
4. Click or tap on the saved report that has been scheduled.
5. Choose the down arrow next to **Save** in the top-right corner of the page and choose **Schedule**.
6. Choose **Create**.
7. On the **Schedule Report** page, choose **Delete** next to the scheduled reports you want to delete.

For instructions on deleting saved reports, see How to delete saved reports (p. 1009).

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 at https://*instance name*.my.connect.aws/.
2. Choose **Analytics**, **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**.

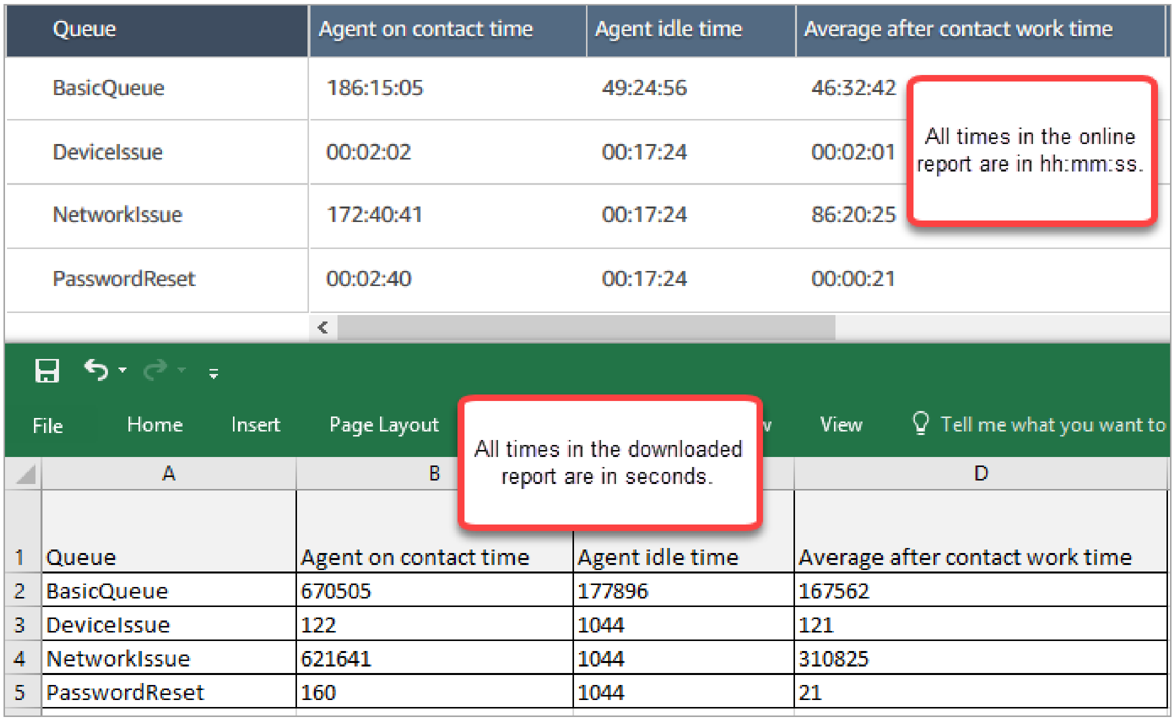
Download a historical metrics report

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 at https://*instance name*.my.connect.aws/.
2. Create a new report or open a saved report.
3. Choose the down arrow next to **Save** in the top-right corner of the page and choose **Download CSV**.
4. When prompted, confirm whether to open or save the file.

Although the times in the online report are in hh:mm:ss, all times in the downloaded report are in seconds.



Queue	Agent on contact time	Agent idle time	Average after contact work time
BasicQueue	186:15:05	49:24:56	46:32:42
DeviceIssue	00:02:02	00:17:24	00:02:01
NetworkIssue	172:40:41	00:17:24	86:20:25
PasswordReset	00:02:40	00:17:24	00:00:21

All times in the online report are in hh:mm:ss.

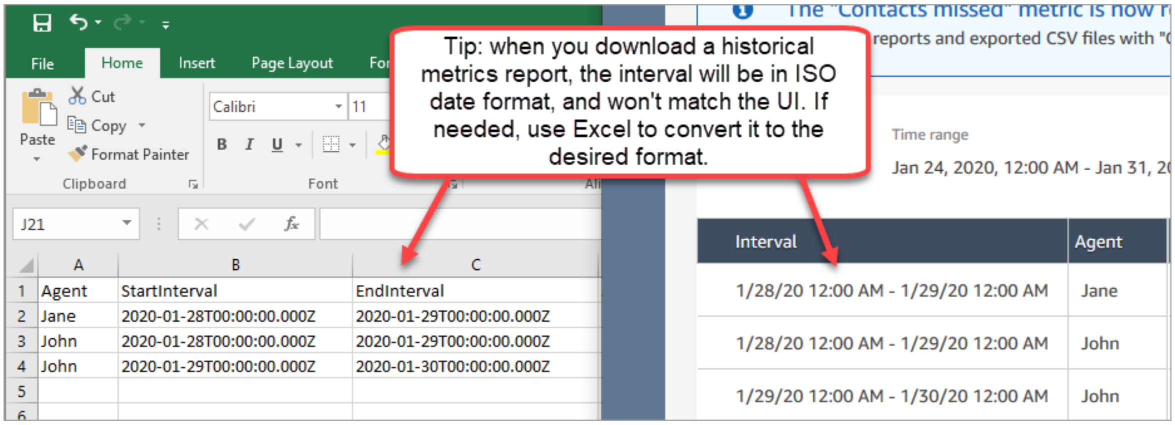
All times in the downloaded report are in seconds.

	A	B	C	D
1	Queue	Agent on contact time	Agent idle time	Average after contact work time
2	BasicQueue	670505	177896	167562
3	DeviceIssue	122	1044	121
4	NetworkIssue	621641	1044	310825
5	PasswordReset	160	1044	21

You can convert the seconds to minutes using an Excel formula. Alternatively, if you have a short report, you can copy and paste the data from Amazon Connect to Excel and it will preserve the format.

Interval downloaded in ISO date format

The interval is downloaded in ISO date format, as shown in the following image.



Tip: when you download a historical metrics report, the interval will be in ISO date format, and won't match the UI. If needed, use Excel to convert it to the desired format.

	A	B	C
1	Agent	StartInterval	EndInterval
2	Jane	2020-01-28T00:00:00.000Z	2020-01-29T00:00:00.000Z
3	John	2020-01-28T00:00:00.000Z	2020-01-29T00:00:00.000Z
4	John	2020-01-29T00:00:00.000Z	2020-01-30T00:00:00.000Z
5			
6			

The "Contacts missed" metric is now r
reports and exported CSV files with "(

Time range
Jan 24, 2020, 12:00 AM - Jan 31, 2(

Interval	Agent
1/28/20 12:00 AM - 1/29/20 12:00 AM	Jane
1/28/20 12:00 AM - 1/29/20 12:00 AM	John
1/29/20 12:00 AM - 1/30/20 12:00 AM	John

Download all historical metric results

If you need to download more than a page or two of historical metrics, we recommend using the following steps:

1. Schedule the report to run as often as needed.

   For example, you might schedule the Login/Logout report to run daily at midnight.
2. The full report is saved to your Amazon S3 bucket.

3. Go to your Amazon S3 bucket and download the report.

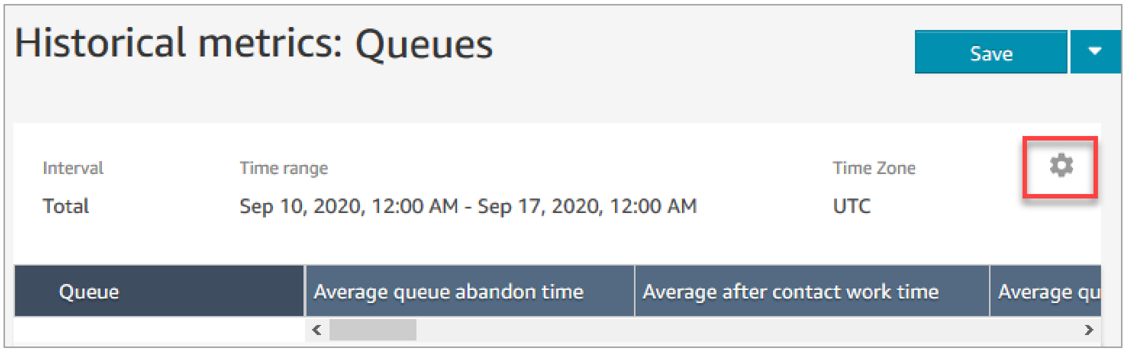
To learn how scheduled reports work, see Schedule a historical metrics report (p. 955).

Show agent queues in a Queues table

By default agent queues don't appear in a Queues table in a historical metrics report. You can choose to show them.

To show agent queues in a Queues table

1. In a historical metrics report, choose the **Settings** icon.



Historical metrics: Queues

Interval	Time range	Time Zone
Total	Sep 10, 2020, 12:00 AM - Sep 17, 2020, 12:00 AM	UTC

2. Choose **Filters**, **Show agent queues**, **Agent queues**, and then use the drop-down to choose the agent's queues you want to include in the table.

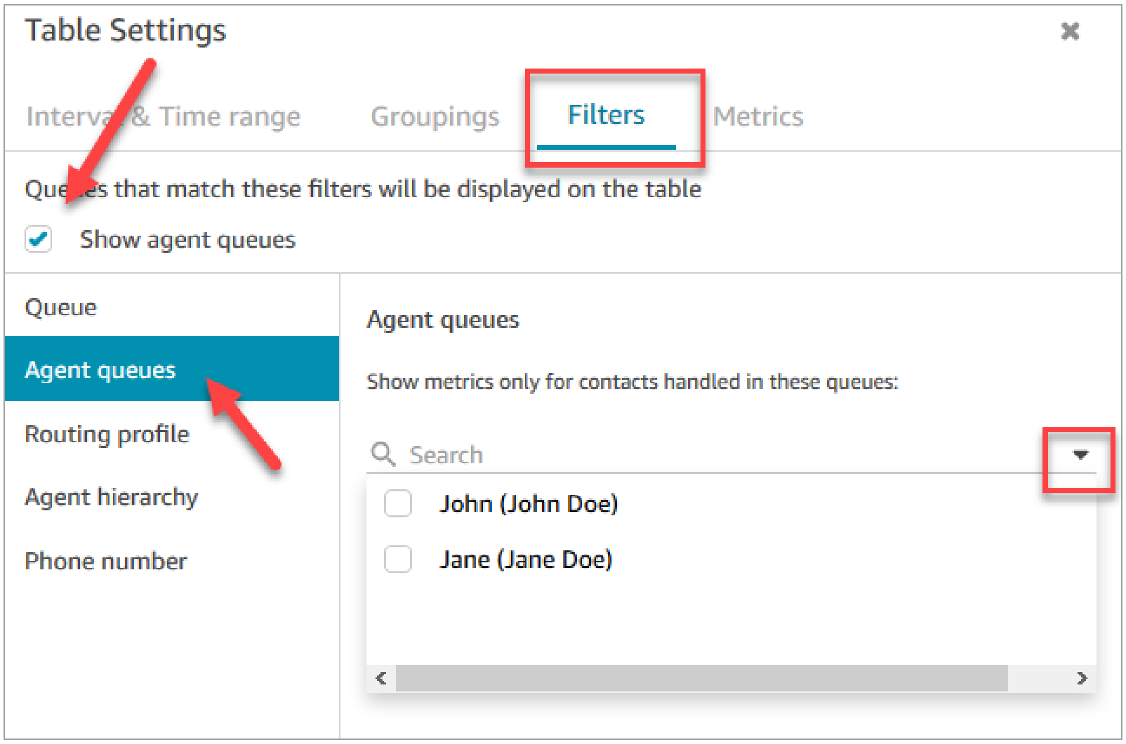


Table Settings

Queues that match these filters will be displayed on the table

☑ Show agent queues

Agent queues

Show metrics only for contacts handled in these queues:

□ John (John Doe)

□ Jane (Jane Doe)

3. Choose **Apply**. The agent queues you selected appear in the Queues table in the historical metrics report.

How many contacts in queue on a specific date

The historical metrics reports don't provide a way for you to determine how many contacts were in queue on a specific date, at a specific time.

To get this information in a historical report, you need the help of a developer. The developer uses the GetCurrentMetricData API to store the data so you can look it up later.

About the agent activity audit report

The agent activity audit is like a report version of the agent event stream (p. 965). All of the data in this report is also in the agent event stream.

For example, if there's something in the audit report you want to recreate, or if you want to recreate a different time period, you can do so using the agent event stream.

Status definitions

The following values may appear in the **Status** column on agent activity audit report.

- **Available**: The agent has set their status in the Contact Control Panel (CCP) to **Available**. Contacts can be routed to them.
- **Offline**: The agent has set their status in the Contact Control Panel (CCP) to **Offline**. Contacts can not be routed to them.
- **Custom status**: The agent has set their status in the Contact Control Panel (CCP) to a custom status. Contacts can not be routed to them.
- **Joining Customer**: The state between an inbound contact arriving in the contact flow and routing to the agent.
- **Connecting Agent**: The state between an inbound contact being routed to an agent and the agent receiving the contact.
- **Connected**: When an inbound contact has been established by the agent choosing **Accept** in their CCP.
- **Busy**: The agent is interacting with a customer.
- **Agent Disconnected**: When the agent doesn't choose **Accept** on the inbound contact in 20 seconds, or they choose **Reject**.
- **Calling Customer**: The state before an outbound call is established.
- **Telecom issue**: When an outbound call is ended before the call is established. For example, there was an error with the agent's soft phone connection.

> **Note**
> If a status appears in your report but is not listed on this page, it is a custom status created by your organization. Contact your Amazon Connect admin to learn the definition.

Login/Logout reports

The Login/Logout report displays the login and logout information for the users in your contact center (for example, agents, managers, and administrators). For each user session, the login and logout times are displayed as a row in the report. You can use the report to determine the time users were logged in to Amazon Connect. The report also displays the amount of time for each session that user was logged in to Amazon Connect.

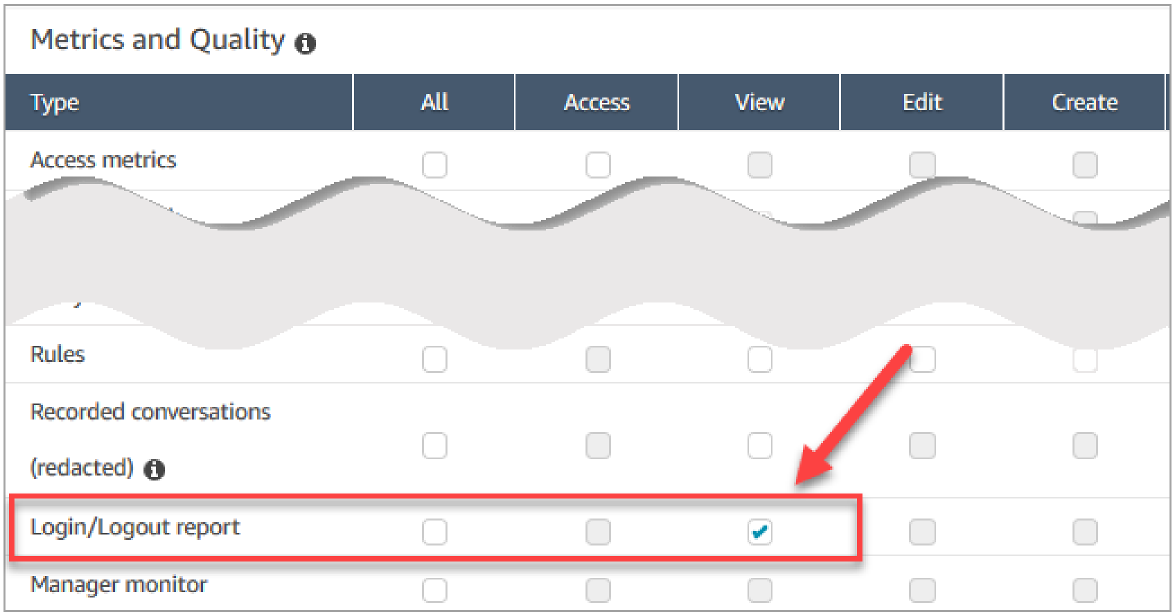
Important
By default, when an agent closes their CCP window, they are not logged out. Unless you have customized your CCP for automatic logout (p. 235), agents must choose the **Logout** button. Until they choose the **Logout** button, the Login/Logout report shows them as logged in.

Login/Logout report limit: 10,000 rows

- If you try to generate a Login/Logout report that has more than 10,000 rows, it won't complete.
- The Login/Logout report page displays only 10,000.
- If you schedule a Login/Logout report that contains more than 10,000 rows, the report will fail. In addition, no report output will be saved to your S3 bucket, and you cannot view the report.
- If you have a contact center with a lot of users, and your reports fail to complete, you can specify a shorter time range to reduce the size of the report generated, or apply filters to the report, such as routing profile and agent hierarchy. You can then use other filters to capture all of the login/logout data for your instance.

Required permissions to access the Login/Logout report

Before you can generate a Login/Logout report, you need the following permissions assigned to your security profile: **Login/Logout report - View**.



Metrics and Quality

Type	All	Access	View	Edit	Create
Access metrics	□	□	□	□	□
Rules	□	□	□	□	□
Recorded conversations (redacted)	□	□	□	□	□
Login/Logout report	□	□	☑	□	□
Manager monitor	□	□	□	□	□

By default, the Amazon Connect **Admin** security profile has these permissions.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

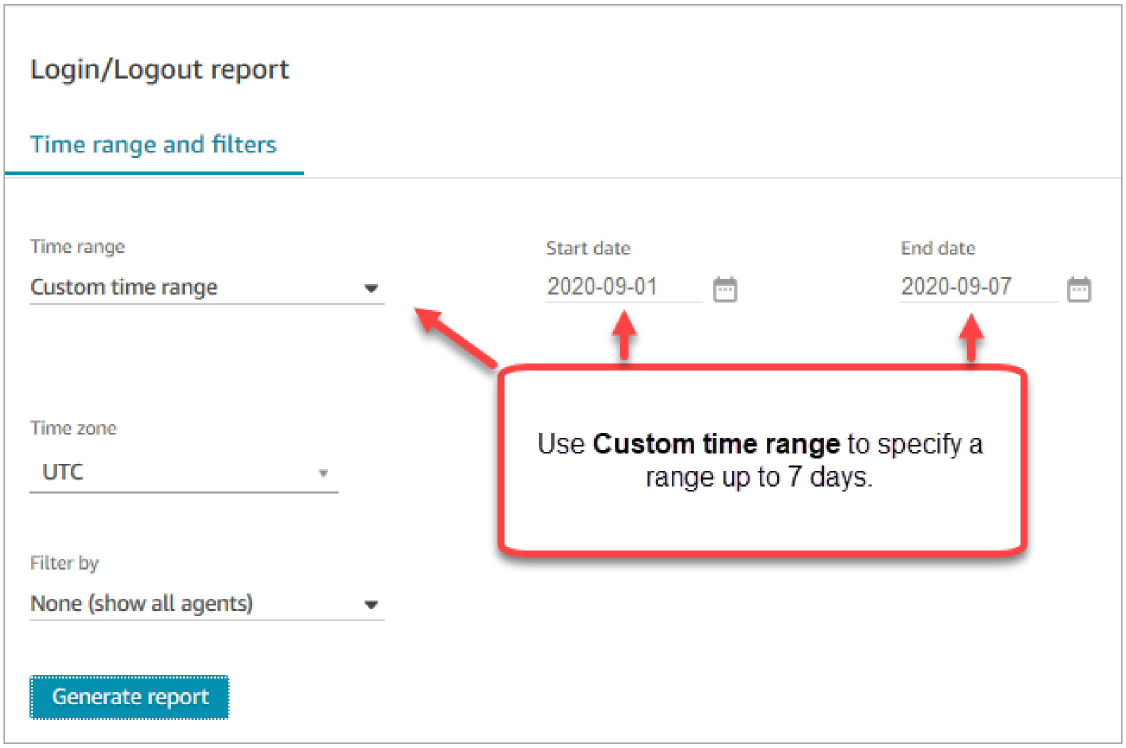
Generate a Login/Logout report

A Login/Logout report includes only login or logout actions by your users that occurred during the specified time range.

- If user logged in during the time range and did not log out, the report shows a login time but not a logout time.
- If the user logged in before the start of the time range, and then logged out during the time range, the report shows both the login and logout times even though the login occurred before the start of the time range. This is so you can view the duration of the user session associated with the most recent logout.

To generate a Login/Logout report

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. Choose **Analytics**, **Login/Logout report**.
3. On the **Login/Logout report** page, choose the **Time range** for the records to include in the report. Choose **Custom time range** to specify a range up to 7 days.



Login/Logout report

Time range and filters

Time range: Custom time range

Start date: 2020-09-01

End date: 2020-09-07

Time zone: UTC

Filter by: None (show all agents)

Use **Custom time range** to specify a range up to 7 days.

4. Choose the **Time zone** to use for your report.
5. To filter data included in the report, for **Filter by**, choose a value.
6. Choose **Generate report**, **Save**.
7. Provide a name for the report, and choose **Save**.

Edit a Saved Login/Logout Report

After you save your report, you can edit it at any time. When you open a saved report, the time frame and date range displayed show the date and time defined when you saved the report.

To edit a saved Login/Logout report

1. Log in to your contact center at https://*instance name*.my.connect.aws/.
2. Choose **Analytics**, **Saved reports**.

3. Choose **Login/Logout report** and select the report to edit.
4. Update the **Time range**, **Time zone**, and **Filter by** settings.
5. To overwrite your existing report, choose **Save**.
6. To save the changes as a new report, choose **Save**, **Save as**. Provide a name for the report and choose **Save as**.

Download a Login/Logout report as a CSV File

When you have generated a report, you can download it as a comma-separated value (CSV) file so that you can use it other applications to work with the data, such as a spreadsheet or database.

To download a report as a CSV file

1. Open the report to download.
2. On the **Login/Logout report** page, at the top right corner, choose the **Share report** menu (arrow) next to **Save**.
3. Choose **Download CSV**. The file `Login_Logout report.csv` is downloaded to your computer.

Share a Login/Logout report

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

To share a Login/Logout report

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

Schedule a Login/Logout report

To generate a report with the same settings on a regular basis, you can schedule the report to run daily or on specific days of the week. Note that *scheduled* Login/Logout reports work differently than Login/Logout reports you generate (p. 961) from the user interface for a specified time range.

Important things to know

- When you schedule a report, it is automatically published to your organization. Anyone with appropriate permissions can view the report. Users with all permissions for Login/Logout reports can also edit, schedule, or delete the report.
- For scheduled Login/Logout reports, the trailing window value is always the last 24 hours.
- A scheduled report always runs at 12AM on the day you select, in the time zone that you choose.

  For example, if you select Wednesday, the report runs at midnight Wednesday and does not include any data for Wednesday.

- Scheduled reports are saved as CSV files in your Amazon S3 bucket. The default time zone is UTC. To have your report run at 12AM in your local time, choose your time zone instead.
- To email a scheduled report to a list of co-workers, you need to generate the email manually using your messaging system. Amazon Connect doesn't provide an option to email the scheduled report automatically.

How to schedule a Login/Logout report

1. If you already have a saved report to schedule open, skip to step 4. Otherwise, in the dashboard, choose **Analytics**, **Saved reports**.
2. Choose **Login/Logout report**.
3. Hover the mouse pointer over the row containing the name of the report to schedule, and choose the **Schedule report** icon.
4. On the **Schedule report** page, under **Recurrence**, for **Generate this report**, choose whether to generate the report **Daily** or **Weekly**.
5. If you choose **Weekly**, select the day or days of the week on which to run the report.
6. Choose the **Time zone**.
7. To add a prefix to the S3 path to the saved report, choose **Delivery Options** and enter a value in the **Prefix** field.

   The prefix is added to the path between /Reports and the report name. For example: .../Reports/*my-prefix*/report-name-YYYY-MM-DD...
8. Choose **Create**.

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

To edit or delete the schedule for a report

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

Delete a Saved Login/Logout report

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

To delete a saved Login/Logout report

1. Open your Amazon Connect dashboard.
2. Choose **Analytics**, **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

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

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

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

To enable agent event streams

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

Sample agent event stream

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

Note

For how many chats and tasks an agent can take concurrently, see Amazon Connect service quotas (p. 1205).

```
{
    "AWSAccountId": "012345678901",
    "AgentARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent/agent-ARN",
    "CurrentAgentSnapshot":
      {
    "AgentStatus": {
            "ARN": "example-ARN", //The ARN for the agent's current agent status (not for
 the agent).
            "Name": "Available",  //This shows the agent status in the CCP is set to
 Available.
            "StartTimestamp": "2019-08-13T20:52:30.704Z"
        },
     "NextAgentStatus": {
            "Name": "Lunch", //They set their next status, which pauses new contacts being
 routed to them while they finish their current contacts.
            "ARN": "example-ARN2",  //The ARN of the agent status that the agent has set as
 their next status.
            "EnqueueTimestamp": "2019-08-13T20:58:00.004Z",   //When the agent set their
 next status and paused routing of incoming contacts.
        }
      } ,
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "AgentEventStreamTest",
            "LastName": "Agent",
            "RoutingProfile": {
                "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/routing-profile/routing-profile-ARN",
                "Concurrency": [
                    {
                        "AvailableSlots": 3, //This shows the agent has 3 slots available.
                                            //They aren't on any chats right now.
                        "Channel": "CHAT",
                        "MaximumSlots": 3  //The agent's routing profile allows them to
 take up to 3 chats.
                    },
                    {
                        "AvailableSlots": 1, //The agent has 1 slot available to take a
 call.
                        "Channel": "VOICE",
                        "MaximumSlots": 1  //The agent's routing profile allows them to
 take 1 call at a time.
                    }
                ],
                "DefaultOutboundQueue": {
                    "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN",
                    "Channels": [
                        "VOICE"  //This outbound queue only works for calls.
                    ],
                    "Name": "OutboundQueue"
                },
                "InboundQueues": [
                    {
                        "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/agent/agent-ARN",
                        "Channels": [
                            "VOICE",
                            "CHAT"
                        ],
                        "Name": null  //This queue has a name of "null" because it's an
 agent queue,
                                      //and agent queues don't have names.
                    },
                    {
                        "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/queue-ARN",
                        "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",
    "InstanceARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111",
    "PreviousAgentSnapshot": {
        "AgentStatus": {
            "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent-state/agent-state-ARN",
            "Name": "Offline",
            "StartTimestamp": "2019-08-13T20:52:30.704Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "AgentEventStreamTest",
            "LastName": "Agent",
            "RoutingProfile": {
                "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/routing-profile/routing-profile-ARN",
                "Concurrency": [
                    {
                        "AvailableSlots": 3,
                        "Channel": "CHAT",
                        "MaximumSlots": 3
                    },
                    {
                        "AvailableSlots": 1,
                        "Channel": "VOICE",
                        "MaximumSlots": 1
                    }
                ],
                "DefaultOutboundQueue": {
                    "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN",
                    "Channels": [
                        "VOICE"
                    ],
                    "Name": "OutboundQueue"
                },
                "InboundQueues": [
                    {
                        "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/agent/agent-ARN",
                        "Channels": [
                            "VOICE",
                            "CHAT"
                        ],
                        "Name": null
                    },
                    {
                        "ARN": "arn:aws:connect:us-west-2:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/queue-ARN",
                        "Channels": [
                            "CHAT",
                            "VOICE"
                        ],
                        "Name": "Omni-channel-queue"
                    }
                ],
                "Name": "AgentEventStreamProfile"
            },
            "Username": "aestest"
        },
        "Contacts": [ ]
    },
    "Version": "2017-10-01"
}
```

Determine how long an agent spends doing ACW

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

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

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

For example, in the following agent event stream output, the contact enters ACW state at "**StateStartTimestamp**": "2019-05-25T18:55:27.017Z".

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

```
{
    "AWSAccountId": "012345678901",
    "AgentARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent/agent-ARN",
    "CurrentAgentSnapshot": {
        "AgentStatus": {
            "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent-state/agent-state-ARN",
            "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.
            "StartTimestamp": "2019-05-25T18:43:59.049Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "(Removed)",
            "LastName": "(Removed)",
            "RoutingProfile": {
                "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/routing-profile/routing-profile-ARN",
                "DefaultOutboundQueue": {
                    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                    "Name": "BasicQueue"
                },
                "InboundQueues": [
                    {
                        "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                        "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",
                "ConnectedToAgentTimestamp": "2019-05-25T18:55:21.011Z",
                "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": {
                    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                    "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",
    "EventTimestamp": "2019-05-25T18:55:27.017Z",
    "EventType": "STATE_CHANGE",  //This shows that the state of the contact has changed;
 above we can see the conversation ENDED.
    "InstanceARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111",
    "PreviousAgentSnapshot": {
        "AgentStatus": {
            "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent-state/agent-state-ARN",
            "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.
            "StartTimestamp": "2019-05-25T18:43:59.049Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "(Removed)",
            "LastName": "(Removed)",
            "RoutingProfile": {
                "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/routing-profile/routing-profile-ARN",
                "DefaultOutboundQueue": {
                    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                    "Name": "BasicQueue"
                },
                "InboundQueues": [
                    {
                        "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                        "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.
                "ConnectedToAgentTimestamp": "2019-05-25T18:55:21.011Z",
                "ContactId": "ContactId-1",  //This shows the agent was working with a
 contact identified as "ContactId-1".
                "InitialContactId": null,
                "InitiationMethod": "OUTBOUND",
                "Queue": {
                    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                    "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.
            }
        ]
    },
    "Version": "2019-05-25"
}
```

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

1. Find where the `CurrentAgentSnapshot` has no contacts, and the state for the contact listed in the `PreviousAgentSnapshot` equals ENDED.

   Because a STATE_CHANGE event also occurs when the agent's configuration is changed, such as when they are assigned a different routing profile, this step confirms you have the right event.
2. Find where the `EventType` = "STATE_CHANGE".
3. View the `EventTimeStamp` for it.

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

```
{
    "AWSAccountId": "012345678901",
    "AgentARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent/agent-ARN",
    "CurrentAgentSnapshot": {
        "AgentStatus": {
            "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent-state/agent-state-ARN",
            "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.
            "StartTimestamp": "2019-05-25T18:43:59.049Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "(Removed)",
            "LastName": "(Removed)",
            "RoutingProfile": {
                "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/routing-profile/routing-profile-ARN",
                "DefaultOutboundQueue": {
                    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                    "Name": "BasicQueue"
                },
                "InboundQueues": [
                    {
                        "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                        "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-cd1a-4785-b1a8-97023dc1229d",
    "EventTimestamp": "2019-05-25T18:55:32.022Z",  //Here's the EventTimestamp for the
 STATE_CHANGE event. This is when
        the contact left ACW.
    "EventType": "STATE_CHANGE",  //Here's the STATE_CHANGE
    "InstanceARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111",
    "PreviousAgentSnapshot": {
        "AgentStatus": {
            "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent-state/agent-state-ARN",
            "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.
            "StartTimestamp": "2019-05-25T18:43:59.049Z"
        },
        "Configuration": {
            "AgentHierarchyGroups": null,
            "FirstName": "(Removed)",
            "LastName": "(Removed)",
            "RoutingProfile": {
                "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/routing-profile/routing-profile-ARN",
                "DefaultOutboundQueue": {
                    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                    "Name": "BasicQueue"
                },
                "InboundQueues": [
                    {
                        "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-
bbbb-cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                        "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",
                "ConnectedToAgentTimestamp": "2019-05-25T18:55:21.011Z",
                "ContactId": "ContactId-1",  //This is the ContactId of the customer the
 agent was working on previously.
                "InitialContactId": null,
                "InitiationMethod": "OUTBOUND",
                "Queue": {
                    "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-
cccc-dddd-111111111111/queue/queue-ARN-for-BasicQueue",
                    "Name": "BasicQueue"
                },
                "QueueTimestamp": null,
                "State": "ENDED", //The ACW for ContactId-1 has ended.
                "StateStartTimestamp": "2019-05-25T18:55:27.017Z"
            }
        ]
    },
    "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:

- Subtract the "**StateStartTimestamp**": "2019-05-25T18:55:27.017Z" from the "**EventTimestamp**": "2019-05-25T18:55:32.022Z".

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

Agent event streams data model

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

- LOGIN—An agent login to the contact center.
- LOGOUT—An agent logout from the contact center.
- STATE_CHANGE—One of the following changed:
  - The agent changed their status in the Contact Control Panel (CCP). For example, they changed it from Available to on Break.
  - The state of the conversation between the agent and contact changed. For example, they were connected and then on hold.
  - One of the following settings changed in the agent's configuration:
    - Their routing profile
    - The queues in their routing profile
    - Auto-accept call
    - Sip address
    - Agent hierarchy group
    - Language preference setting in the CCP
- HEART_BEAT—This event is published every 120 seconds if there are no other events published during that interval.

> **Note**
> These events continue to be published up to an hour after an agent has logged off.

Event Objects

AgentEvent

The `AgentEvent` object includes the following properties:

AgentARN

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

Type: ARN

AWSAccountId

The 12-digit AWS account ID for the AWS account associated with the Amazon Connect instance.

Type: String

CurrentAgentSnapshot

Contains agent configuration, such as username, first name, last name, routing profile, hierarchy groups, contacts, and agent status.

Type: `AgentSnapshot` object

EventId

Universally unique identifier (UUID) for the event.

Type: String

EventTimestamp

A time stamp for the event, in ISO 8601 standard format.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*:*sss*Z)

EventType

The type of event.

Valid values: `STATE_CHANGE` | `HEART_BEAT` | `LOGIN` | `LOGOUT`

InstanceARN

Amazon Resource Name for the Amazon Connect instance in which the agent's user account is created.

Type: ARN

PreviousAgentSnapshot

Contains agent configuration, such as username, first name, last name, routing profile, hierarchy groups), contacts, and agent status.

Type: `AgentSnapshot` object

Version

The version of the agent event stream in date format, such as 2019-05-25.

Type: String

AgentSnapshot

The `AgentSnapshot` object includes the following properties:

AgentStatus

Agent status data, including:

- ARN—The ARN for the agent's current agent status (not for the agent).
- Name—This is the status of the agent that they manually set in the CCP (p. 998), or that the supervisor manually changes in the real-time metrics report (p. 935).

  For example, their status might be **Available**, which means that they are ready for inbound contacts to be routed to them. Or it might be a custom status, such as Break or Training, which means that inbound contacts can't be routed to them BUT they can still make outbound calls.
- StartTimestamp—The timestamp in ISO 8601 standard format for the time at which the agent entered the status.

  Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*:*sss*Z)

Type: `AgentStatus` object.

NextAgentStatus

If the agent set a next agent status, the data appears here.

- ARN—The ARN of the agent status that the agent has set as their next status.
- Name—This is the name of the agent status that the agent has set as their next status.
- EnqueueTimestamp—The timestamp in ISO 8601 standard format for the time at which the agent set their next status and paused routing of incoming contacts.

  Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*:*sss*Z)

Type: `NextAgentStatus` object.

Configuration

Information about the agent, including:

- FirstName—The agent's first name.
- HierarchyGroups—The hierarchy group the agent is assigned to, if any.
- LastName—The agent's last name.
- RoutingProfile—The routing profile the agent is assigned to.
- Username—the agent's Amazon Connect user name.

Type: `Configuration` object

Contacts

The contacts

Type: `List of Contact Objects` object

Configuration

The `Configuration` object includes the following properties:

FirstName

The first name entered in the agent's Amazon Connect account.

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`, `CHAT`, `TASKS`

InitiationMethod

Indicates how the contact was initiated.

Valid values:

- `INBOUND`: The customer initiated voice (phone) contact with your contact center.
- `OUTBOUND`: An agent initiated voice (phone) contact with the customer, by using the CCP to call their number. This initiation method calls the StartOutboundVoiceContact API.
- `TRANSFER`: The customer was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new contact record being created.
- `CALLBACK`: The customer was contacted as part of a callback flow.

  For more information about the InitiationMethod in this scenario, see About queued callbacks in metrics (p. 1002).
- `API`: The contact was initiated with Amazon Connect by API. This could be an outbound contact you created and queued to an agent, using the StartOutboundVoiceContact API, or it could be a live chat that was initiated by the customer with your contact center, where you called the StartChatConnect API.
- `QUEUE_TRANSFER`: While the customer was in one queue (listening to Customer queue flow), they were transferred into another queue using a contact flow block.
- `DISCONNECT`: When a Set disconnect flow (p. 403) block is triggered, it specifies which contact flow to run after a disconnect event during a contact.

  A disconnect event is when:

- A call, chat, or task is disconnected by an agent.
- A task is disconnected as a result of a flow action.
- A task expires. The task is automatically disconnected if it is not completed in 7 days.

If a new contact is created while running a disconnect flow, then the initiation method for that new contact is DISCONNECT.

State

The state of the contact.

Valid values: `INCOMING` | `PENDING` | `CONNECTING` | `CONNECTED` | `CONNECTED_ONHOLD` | `MISSED` | `REJECTED` | `ERROR` | `ENDED`

> **Note**
> The `REJECTED` state does not apply to voice contacts. Rejected voice contacts appear as `MISSED`.

StateStartTimestamp

The time at which the contact entered the current state.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*:*sss*Z)

ConnectedToAgentTimestamp

The time at which the contact was connected to an agent.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*:*sss*Z)

QueueTimestamp

The time at which the contact was put into a queue.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*:*sss*Z)

Queue

The queue the contact was placed in.

Type: `Queue` object

HierarchyGroup object

The `HierarchyGroup` object includes the following properties:

ARN

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

Type: String

Name

The name of the hierarchy group.

Type: String

AgentHierarchyGroups object

The `AgentHierarchyGroups` object includes the following properties:

Level1

Includes details for Level1 of the hierarchy assigned to the agent.

Type: `HierarchyGroup` object

Level2

Includes details for Level2 of the hierarchy assigned to the agent.

Type: `HierarchyGroup` object

Level3

Includes details for Level3 of the hierarchy assigned to the agent.

Type: `HierarchyGroup` object

Level4

Includes details for Level4 of the hierarchy assigned to the agent.

Type: `HierarchyGroup` object

Level5

Includes details for Level5 of the hierarchy assigned to the agent.

Type: `HierarchyGroup` object

Queue object

The `Queue` object includes the following properties:

ARN

The Amazon Resource Name (ARN) for the queue.

Type: String

Name

The name of the queue.

Type: String

RoutingProfile object

The `RoutingProfile` object includes the following properties:

ARN

The Amazon Resource Name (ARN) for the agent's routing profile.

Type: String

Name

The name of the routing profile.

Type: String

InboundQueues

The `Queue` objects associated with the agent's routing profile.

Type: List of `Queue` object

DefaultOutboundQueue

The default outbound queue for the agent's routing profile.

Type: `Queue` object

Amazon Connect contact events

Amazon Connect allows you to subscribe to a near real-time stream of contact (voice calls, chat, and task) events (for example, call is queued) in your Amazon Connect contact center. These events include:

- INITIATED - A voice call, chat, or task is initiated or transferred.
- CONNECTED_TO_SYSTEM - The date and time the customer endpoint connected to Amazon Connect, in UTC time. For INBOUND, this matches InitiationTimestamp. For OUTBOUND, CALLBACK, and API, this is when the customer endpoint connected to Amazon Connect.

  Note
  CONNECTED_TO_SYSTEM event is generated for outbound calls (API only), Tasks, and Chats.
- QUEUED - A voice call, chat, or task is queued to be assigned to an agent.
- CONNECTED_TO_AGENT - A voice call, chat, or task is connected to an agent.
- DISCONNECTED - A voice call, chat, or task is disconnected.

  A disconnect event is when:
  - A call, chat, or task is disconnected by an agent.
  - A task is disconnected as a result of a flow action.
  - A task expires. The task is automatically disconnected if it is not completed in 7 days.

You can use contact events to create analytics dashboards to monitor and track contact activity, integrate into workforce management (WFM) solutions to better understand contact center performance, or to integrate applications that react to events (for example, call disconnected) in real-time.

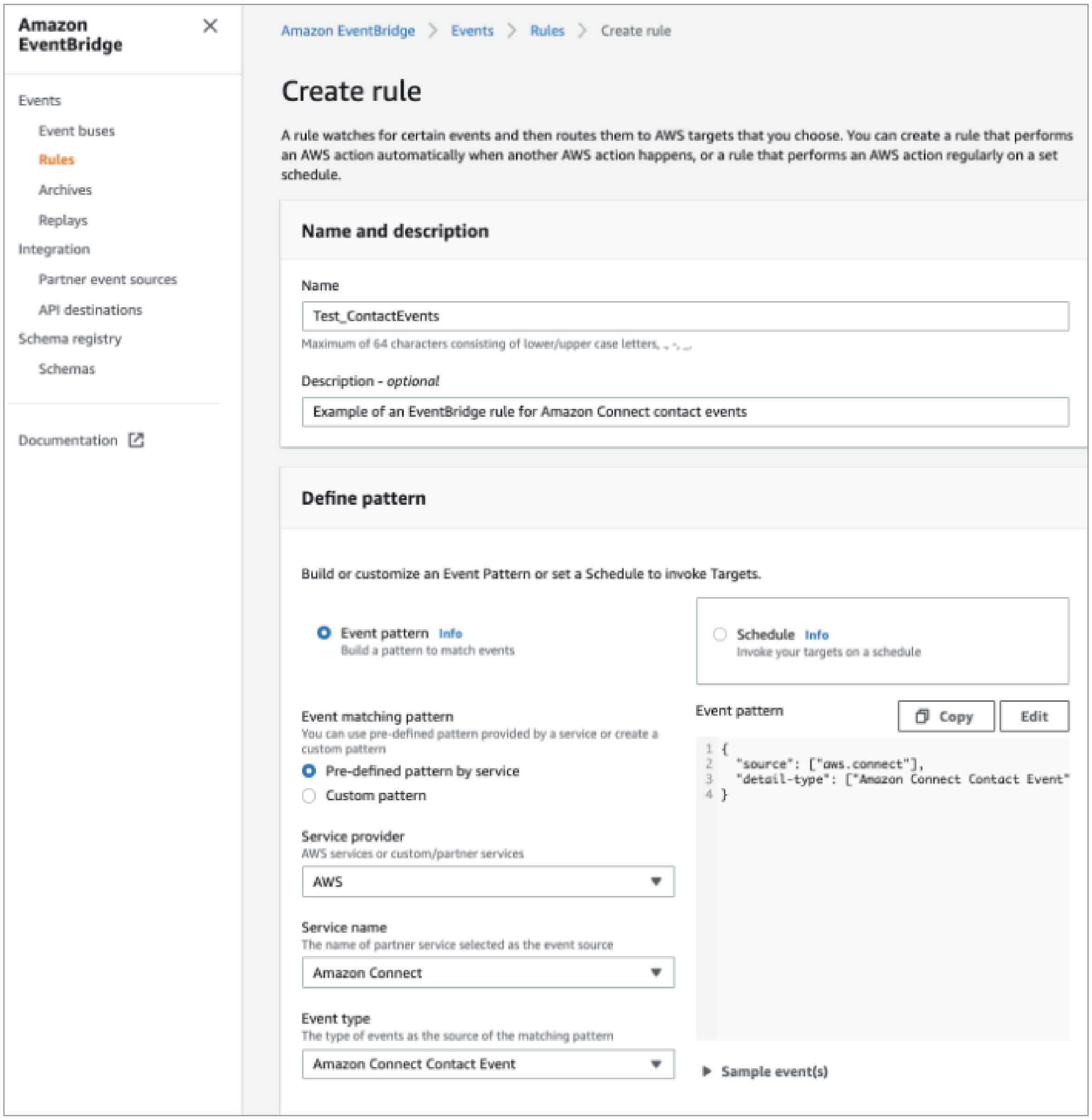
Subscribe to Amazon Connect contact events

Amazon Connect contact events are published using Amazon EventBridge, and can be enabled in a couple of steps for your Amazon Connect instance in the Amazon EventBridge console by creating a new rule. Although events are not ordered, they have a timestamp which enables you to consume the data.

Events are emitted on a best effort basis.

To subscribe to Amazon Connect contact events, go to Amazon EventBridge and create a new rule by selecting **Amazon Connect** as the service name, and **Amazon Connect contact event** as the event type. For more information about configuring rules, see Amazon EventBridge rules in the *Amazon EventBridge User Guide*.

The following image shows what this looks like in EventBridge:



Create rule

A rule watches for certain events and then routes them to AWS targets that you choose. You can create a rule that performs an AWS action automatically when another AWS action happens, or a rule that performs an AWS action regularly on a set schedule.

Name and description

Name: Test_ContactEvents

Maximum of 64 characters consisting of lower/upper case letters, ., -, _.

Description - *optional*: Example of an EventBridge rule for Amazon Connect contact events

Define pattern

Build or customize an Event Pattern or set a Schedule to invoke Targets.

● Event pattern Info
Build a pattern to match events

○ Schedule Info
Invoke your targets on a schedule

Event matching pattern
You can use pre-defined pattern provided by a service or create a custom pattern
● Pre-defined pattern by service
○ Custom pattern

Service provider
AWS services or custom/partner services
AWS

Service name
The name of partner service selected as the event source
Amazon Connect

Event type
The type of events as the source of the matching pattern
Amazon Connect Contact Event

Event pattern

```
{
  "source": ["aws.connect"],
  "detail-type": ["Amazon Connect Contact Event"
}
```

You can then select a target of your choice which includes a Lambda function, SQS queue, or SNS topic. For information about configuring targets, Amazon EventBridge targets.

Contact events data model

Contact events are generated in JSON. For each event type, a JSON blob is sent to the target of your choice, as configured in the rule. The following contact events are available:

- INITIATED - A voice call, chat, or task is initiated or transferred.
- QUEUED - A voice call, chat, or task is queued to be assigned to an agent.
- CONNECTED_TO_AGENT - A voice call, chat, or task is connected to an agent.
- CONNECTED_TO_SYSTEM - This identifies that the contact has established media (either answered by a live human voice or answering machine). This event has one of the following status codes in the response schema to identify what the actual disposition was in case the contact was connected

to Amazon Connect: HUMAN_ANSWERED, SIT_TONE-DETECTED, FAX_MACHINE_DETECTED, VOICEMAIL_BEEP, VOICEMAIL_NO_BEEP, AMD_UNRESOLVED, AMD_ERROR.

- DISCONNECTED - A voice call, chat, or task is disconnected. For outbound calls, the dial attempt is not successful, the attempt is connected but the call is not picked up, or the attempt results in a SIT tone.

  A disconnect event is when:
  - A call, chat, or task is disconnected by an agent.
  - A task is disconnected as a result of a flow action.
  - A task expires. The task is automatically disconnected if it is not completed in 7 days.

Event Objects

Contact event

The Contact object includes the following properties:

EventType

The type of event published.

Type: String

Valid values: INITIATED, QUEUED, CONNECTED_TO_AGENT, DISCONNECTED

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

PreviousContactId

The original identifier of the contact that was transferred.

Type: String

Length: 1-256

InstanceARN

Amazon Resource Name for the Amazon Connect instance in which the agent's user account is created.

Type: ARN

Channel

The type of channel.

Type: `VOICE`, `CHAT`, or `TASK`

QueueInfo

The queue the contact was placed in.

Type: `QueueInfo` object

AgentInfo

The agent the contact was assigned to.

Type: `AgentInfo` object

InitiationMethod

Indicates how the contact was initiated.

Valid values:

- INBOUND: The customer initiated voice (phone) contact with your contact center.
- OUTBOUND: Represents an agent-initiated outbound voice call from the Contact Control Panel (CCP). This initiation method calls the StartOutboundVoiceContact API.
- TRANSFER: The contact was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new contact record being created.
- CALLBACK: The customer was contacted as part of a callback flow. For more information about the InitiationMethod in this scenario, see About queued callbacks in metrics (p. 1002).
- API: The contact was initiated with Amazon Connect by API. This could be an outbound contact you created and queued to an agent, using the StartOutboundVoiceContact API, or it could be a live chat that was initiated by the customer with your contact center, where you called the StartChatContact API, or it could be a tasks initiated by the customer by calling the StartTaskContact API.
- QUEUE_TRANSFER: While the contact is one queue, and was then transferred into another queue using a contact flow block.
- DISCONNECT: When a Set disconnect flow (p. 403) block is triggered, it specifies which contact flow to run after a disconnect event.

  A disconnect event is when:

  - A call, chat, or task is disconnected by an agent.
  - A task is disconnected as a result of a flow action.
  - A task expires. The task is automatically disconnected if it is not completed in 7 days.

  When the disconnect event occurs, the corresponding content flow runs. If a new contact is created while running a disconnect flow, then the initiation method for that new contact is DISCONNECT.

QueueInfo

The `QueueInfo` object includes the following properties:

ARN

The Amazon Resource Name (ARN) for the queue.

Type: String

QueueType

The type of queue.

Type: String

AgentInfo

The `AgentInfo` object includes the following properties:

AgentARN

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

Type: ARN

RoutingProfileArn

The Amazon Resource Name (ARN) for the agent's routing profile.

Type: String

CustomerVoiceActivity

The `CustomerVoiceActivity` object includes the following properties:

GreetingStartTimestamp

The date and time that measures the beginning of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

GreetingEndTimestamp

The date and time that measures the end of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

Contact timestamps

InitiationTimestamp

The date and time this contact was initiated, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

ConnectedToSystemTimestamp

The date and time the customer endpoint connected to Amazon Connect, in UTC time.

EnqueueTimestamp

The date and time the contact was added to the queue, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

ConnectedToAgentTimestamp

The date and time the contact was connected to the agent, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

DisconnectTimestamp

The date and time that the customer endpoint disconnected from Amazon Connect, in UTC time

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

ScheduledTimestamp

The date and time when this contact was scheduled to trigger the flow to run, in UTC time. This is supported only for the task channel.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

GreetingStartTimestamp

The date and time that measures the beginning of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

GreetingEndTimestamp

The date and time that measures the end of the customer greeting from an outbound voice call, in UTC time.

Type: String (yyyy-MM-dd'T'HH:mm:ss.SSS'Z')

Sample contact event for when a voice call is connected to an agent

```
{
    "version": "0",
    "id": "abcabcab-abca-abca-abca-abcabcabcabc",
    "detail-type": "Amazon Connect Contact Event",
    "source": "aws.connect",
    "account": "111122223333",
    "time": "2021-05-01T18:43:48Z",
    "region": "us-west-1",
    "resources": [
        "arn:aws::...",
        "contactArn",
        "instanceArn"
    ],
    "detail": {
        "eventType": "CONNECTED_TO_AGENT",
        "contactId": "11111111-1111-1111-1111-111111111111",
        "initialContactId": "11111111-2222-3333-4444-555555555555",
        "previousContactId": "11111111-2222-3333-4444-555555555555",
        "channel": "Voice",
        "instanceArn": "arn:aws::connect:us-
west-2:123456789012:instance/12345678-1234-1234-1234-123456789012",
        "initiationMethod": "INBOUND",
        "initiationTimestamp":"2021-08-04T17:17:53.000Z",
        "connectedToSystemTimestamp":"2021-08-04T17:17:55.000Z",
        "queueInfo": {
            "queueArn": "arn",
            "queueType": "type",
            "enqueueTimestamp": "2021-08-04T17:29:04.000Z"
        },
        "AgentInfo": {
            "AgentArn" : "arn",
            "RoutingProfileArn": "",
            "connectedToAgentTimestamp":"2021-08-04T17:29:09.000Z"
        }
    }
}
```

Sample contact event for when a voice call is disconnected

```
{
    "version": "0",
    "id": "abcabcab-abca-abca-abca-abcabcabcabc",
    "detail-type": "Amazon Connect Contact Event",
    "source": "aws.connect",
    "account": "111122223333",
    "time": "2021-08-04T17:43:48Z",
    "region": "us-west-1",
    "resources": [
        "arn:aws:...",
        "contactArn",
        "instanceArn"
    ],
    "detail": {
        "eventType": "DISCONNECTED",
        "contactId": "11111111-1111-1111-1111-111111111111",
        "initialContactId": "11111111-2222-3333-4444-555555555555",
        "previousContactId": "11111111-2222-3333-4444-555555555555",
        "channel": "Voice",
        "instanceArn": "arn:aws::connect:us-
west-2:123456789012:instance/12345678-1234-1234-1234-123456789012",
        "initiationMethod": "OUTBOUND",
        "initiationTimestamp":"2021-08-04T17:17:53.000Z",
        "connectedToSystemTimestamp":"2021-08-04T17:17:55.000Z",
        "disconnectTimestamp":"2021-08-04T17:18:37.000Z",
        "queueInfo": {
            "queueArn": "arn",
            "queueType": "type",
            "enqueueTimestamp": "2021-08-04T17:29:04.000Z"
        },
        "AgentInfo": {
            "AgentArn": "arn",
            "connectedToAgentTimestamp":"2021-08-04T17:29:09.000Z"
        },
        "CustomerVoiceActivity": {
           "greetingStartTimestamp":"2021-08-04T17:29:20.000Z",
           "greetingEndTimestamp":"2021-08-04T17:29:22.000Z",
        }
    },
}
```

Contact records data model

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

For the contact record retention period and maximum size of the attributes section of a contact record, see Feature specifications (p. 1210).

For information about when a contact record is created (and thus can be exported or used for data reporting), see Events in the contact record (p. 1001).

> **Tip**
> Amazon Connect delivers contact records at least once. Contact records may be delivered again for multiple reasons, such as new information arriving after initial delivery. For example, when you use update-contact-attributes to update a contact record, Amazon Connect delivers a new contact record. This contact record is available for 24 months from the time the associated contact was initiated.
> If you're building a system that consumes contact record export streams, be sure to include logic that checks for duplicate contact records for a contact. Use the **LastUpdateTimestamp** property to determine if a copy contains new data than previous copies. Then use the **ContactId** property for deduplication.

Agent

Information about the agent who accepted the incoming contact.

AgentInteractionDuration

The time, in whole seconds, that an agent interacted with a customer.

Type: Integer

Min value: 0

AfterContactWorkDuration

The difference in time, in whole seconds, between `AfterContactWorkStartTimestamp` and `AfterContactWorkEndTimestamp`.

Type: Integer

Min value: 0

AfterContactWorkEndTimestamp

The date and time when the agent stopped doing After Contact Work for the contact, in UTC time.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

AfterContactWorkStartTimestamp

The date and time when the agent started doing After Contact Work for the contact, in UTC time.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

ARN

The Amazon Resource Name of the agent.

Type: ARN

ConnectedToAgentTimestamp

The date and time the contact was connected to the agent, in UTC time.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

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. 987)

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. 995)

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. 987)

Level2

The group at level two of the agent hierarchy.

Type: AgentHierarchyGroup (p. 987)

Level3

The group at level three of the agent hierarchy.

Type: AgentHierarchyGroup (p. 987)

Level4

The group at level four of the agent hierarchy.

Type: AgentHierarchyGroup (p. 987)

Level5

The group at level five of the agent hierarchy.

Type: AgentHierarchyGroup (p. 987)

ContactDetails

Contains user-defined attributes which are lightly typed within the contact.

This object is used only for task contacts. For voice or chat contacts, or for tasks that have contact attributes set with the flow block, check the ContactTraceRecord (p. 988) Attributes object.

ContactDetailsName

Type: String

Length: 1-128

ContactDetailsValue

Type: String

Length: 0-1024

ReferenceAttributeName

Type: String

Length: 1-128

ReferenceAttributesValue

Type: String

Length: 0-1024

ContactTraceRecord

Information about a contact.

Agent

If this contact successfully connected to an agent, this is information about the agent.

Type: Agent (p. 986)

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 contact reached your contact center.

Valid values: `VOICE`, `CHAT`, `TASK`

ConnectedToSystemTimestamp

The date and time the customer endpoint connected to Amazon Connect, in UTC time. For `INBOUND`, this matches InitiationTimestamp. For `OUTBOUND`, `CALLBACK`, and `API`, this is when the customer endpoint answers.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

ContactId

The ID of the contact.

Type: String

Length: 1-256

CustomerEndpoint

The customer endpoint.

Type: Endpoint (p. 992)

DisconnectTimestamp

The date and time that the customer endpoint disconnected from Amazon Connect, in UTC time.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

DisconnectReason

Indicates how the contact was terminated. This data is currently available in the Amazon Connect contact record stream only.

The disconnect reason may not be accurate when there are agent or customer connectivity issues. For example, if the agent is having connectivity issues, the customer might not be able to hear them ("Are you there?") and hang up. This would be recorded as CUSTOMER_DISCONNECT and not reflect the connectivity issue.

Type: String

Voice contacts can have the following disconnect reasons:

- CUSTOMER_DISCONNECT: Customer disconnected first.
- AGENT_DISCONNECT: Agent disconnected when the contact was still on the call.
- THIRD_PARTY_DISCONNECT: In a third-party call, after the agent has left, the third-party disconnected the call while the contact was still on the call.
- TELECOM_PROBLEM: Disconnected due to an issue with connecting the call from the carrier, network congestion, network error, etc.
- CONTACT_FLOW_DISCONNECT: Call was disconnected in a flow.
- OTHER: This includes any reason not explicitly covered by the previous codes. For example, the contact was disconnected by an API.

Tasks can have the following disconnect reasons:

- AGENT_DISCONNECT: Agent marked the task as complete.
- EXPIRED: Task expired automatically because it was not assigned or completed within 7 days.
- CONTACT_FLOW_DISCONNECT: Task was disconnected or completed by a flow.
- API: The StopContact API was called to end the task.
- OTHER: This includes any reason not explicitly covered by the previous codes.

InitialContactId

If this contact is related to other contacts, this is the ID of the initial contact.

Type: String

Length: 1-256

InitiationMethod

Indicates how the contact was initiated.

Valid values:

- INBOUND: The customer initiated voice (phone) contact with your contact center.
- OUTBOUND: An agent initiated voice (phone) contact with the customer, by using the CCP to call their number. This initiation method calls the StartOutboundVoiceContact API.
- TRANSFER: The customer was transferred by an agent to another agent or to a queue, using quick connects in the CCP. This results in a new CTR being created.
- CALLBACK: The customer was contacted as part of a callback flow.

  For more information about the InitiationMethod in this scenario, see About queued callbacks in metrics (p. 1002).
- API: The contact was initiated with Amazon Connect by API. This could be an outbound contact you created and queued to an agent, using the StartOutboundVoiceContact API, or it could be a live chat that was initiated by the customer with your contact center, where you called the StartChatConnect API.
- QUEUE_TRANSFER: While the customer was in one queue (listening to Customer queue flow), they were transferred into another queue using a contact flow block.
- DISCONNECT: When a Set disconnect flow (p. 403) block is triggered, it specifies which contact flow to run after a disconnect event during a contact.

A disconnect event is when:

- A call, chat, or task is disconnected by an agent.
- A task is disconnected as a result of a flow action.
- A task expires. The task is automatically disconnected if it is not completed in 7 days.

If a new contact is created while running a disconnect flow, then the initiation method for that new contact is DISCONNECT.

InitiationTimestamp

The date and time this contact was initiated, in UTC time. For `INBOUND`, this is when the contact arrived. For `OUTBOUND`, this is when the agent began dialing. For `CALLBACK`, this is when the callback contact was created. For `TRANSFER` and `QUEUE_TRANSFER`, this is when the transfer was initiated. For `API`, this is when the request arrived.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

InstanceARN

The Amazon Resource Name of the Amazon Connect instance.

Type: ARN

LastUpdateTimestamp

The date and time this contact was last updated, in UTC time.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

MediaStreams

The media streams.

Type: Array of MediaStream (p. 992)

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. 993)

Recording

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

Type: RecordingInfo (p. 993)

Recordings

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

Type: Array of RecordingsInfo (p. 994)

> **Note**
> The first recording for a contact will appear in both the Recording and Recordings sections of the contact record.

ScheduledTimestamp

The date and time when this contact was scheduled to trigger the flow to run, in UTC time. This is supported only for the task channel.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

SystemEndpoint

The system endpoint. For `INBOUND`, this is the phone number that the customer dialed. For `OUTBOUND`, this is the Outbound caller ID number assigned to the outbound queue that is used to dial the customer.

Type: Endpoint (p. 992)

TransferCompletedTimestamp

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

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

TransferredToEndpoint

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

Type: Endpoint (p. 992)

Endpoint

Information about an endpoint. In Amazon Connect, an endpoint is the destination for a contact, such as a customer phone number, or a phone number for your contact center.

Address

The value for the type of endpoint. For `TELEPHONE_NUMBER`, the value is a phone number in E.164 format.

Type: String

Length: 1-256

Type

The endpoint type. Currently, an endpoint can only be a telephone number.

Valid values: `TELEPHONE_NUMBER`

MediaStream

Information about the media stream used during the contact.

Type

Type: MediaStreamType

Valid values: `AUDIO`, `VIDEO`, `CHAT`

QueueInfo

Information about a queue.

ARN

The Amazon Resource Name of the queue.

Type: ARN

DequeueTimestamp

The date and time the contact was removed from the queue, in UTC time. Either the customer disconnected or the contact was connected to an agent.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

Duration

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

Type: Integer

Min value: 0

EnqueueTimestamp

The date and time the contact was added to the queue, in UTC time.

Type: String (*yyyy*-*mm*-*dd*T*hh*:*mm*:*ss*Z)

Name

The name of the queue.

Type: String

Length: 1-256

RecordingInfo

Information about a voice recording.

DeletionReason

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

Type: String

Location

The location, in Amazon S3, for the recording.

Type: String

Length: 0-256

Status

The recording status.

Valid values: `AVAILABLE` | `DELETED` | `NULL`

Type

The recording type.

Valid values: `AUDIO`

RecordingsInfo

Information about a voice recording or chat transcript.

DeletionReason

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

Type: String

FragmentStartNumber

The number that identifies the Kinesis Video Streams fragment where the customer audio stream started.

Type: String

FragmentStopNumber

The number that identifies the Kinesis Video Streams fragment where the customer audio stream stopped.

Type: String

Location

The location, in Amazon S3, for the recording/transcript.

Type: String

Length: 0-256

MediaStreamType

Information about the media stream used during the conversation.

Type: String

Valid values: `AUDIO`, `VIDEO`, `CHAT`

ParticipantType

Information about the conversation participant: whether they are an agent or contact.

Type: String

StartTimestamp

When the conversation started.

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

Status

The status of the recording/transcript.

Valid values: `AVAILABLE` | `DELETED` | `NULL`

StopTimestamp

When the conversation stopped.

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

StorageType

Where the recording/transcript is stored.

Type: String

Valid values: Amazon S3 | `KINESIS_VIDEO_STREAM`

References

Contains links to other documents that are related to a contact.

Reference Info

ReferenceType

ContentType

Location

RoutingProfile

Information about a routing profile.

ARN

The Amazon Resource Name of the routing profile.

Type: ARN

Name

The name of the routing profile.

Type: String

Length: 1-100

VoiceID

The latest Voice ID status.

AuthenticationEnabled

Was voice authentication enabled for the call?

Type: Boolean

GeneratedSpeakerId

The speaker identifier generated by Voice ID.

Type: String

Length: 25 characters

AuthenticationThreshold

The minimum authentication score required for a user to be authenticated.

Type: Integer

Min value: 0

Max value: 100

AuthenticationMinimumSpeechInSeconds

The number of seconds of speech used to authenticate the user.

Type: Integer

Min value: 5

Max value: 10

AuthenticationScore

The output of Voice ID authentication evaluation.

Type: Integer

Min value: 0

Max value: 100

AuthenticationResult

The string output of Voice ID authentication evaluation.

Type: String

Length: 1-32

Valid values: Authenticated, Not Authenticated, Not Enrolled, Opted Out, Inconclusive, Error

SpeakerEnrolled

Was the customer enrolled during this contact?

Type: Boolean

SpeakerOptedOut

Did the customer opt out during this contact?

Type: Boolean

FraudDetectionEnabled

Was detection of fraudsters in a watchlist enabled for the contact?

Type: Boolean

FraudDetectionThreshold

The threshold for detection of fraudsters in a watchlist that was set in the contact flow for the contact.

Type: Integer

Min value: 0

Max value: 100

FraudDetectionResult

The string output of detection of fraudsters in a watchlist.

Type: String

Valid values: High Risk, Low Risk, Inconclusive, Error

FraudDetectionReasons

Contains one fraud type: Known Fraudster.

Type: List of String

Length: 1-128

FraudRiskScoreKnownFraudster

The detection of fraudsters in a watchlist score for Known Fraudster category.

Type: Integer

Min value: 0

Max value: 100

FraudRiskScoreVoiceSpoofing

The detection of fraudsters in a watchlist score for Voice Spoofing, TTS, Audio Replay categories.

Type: Integer

Length: 3

FraudRiskScoreSyntheticSpeech

The detection of fraudsters in a watchlist score for Synthetic speech using TTS.

Type: Integer

Length: 3

GeneratedFraudsterID

The fraudster ID if the fraud type is Known Fraudster.

Type: String

Length: 25 characters

How to identify abandoned contacts

An abandoned contact refers to a contact that was disconnected by the customer while in queue. This means that they weren't connected to an agent.

The contact record for an abandoned contact has a **Queue**, and an **Enqueue Timestamp** because it was enqueued. It won’t have a **ConnectedToAgentTimestamp**, or any of the other fields that populate only after the contact has been connected to an agent.

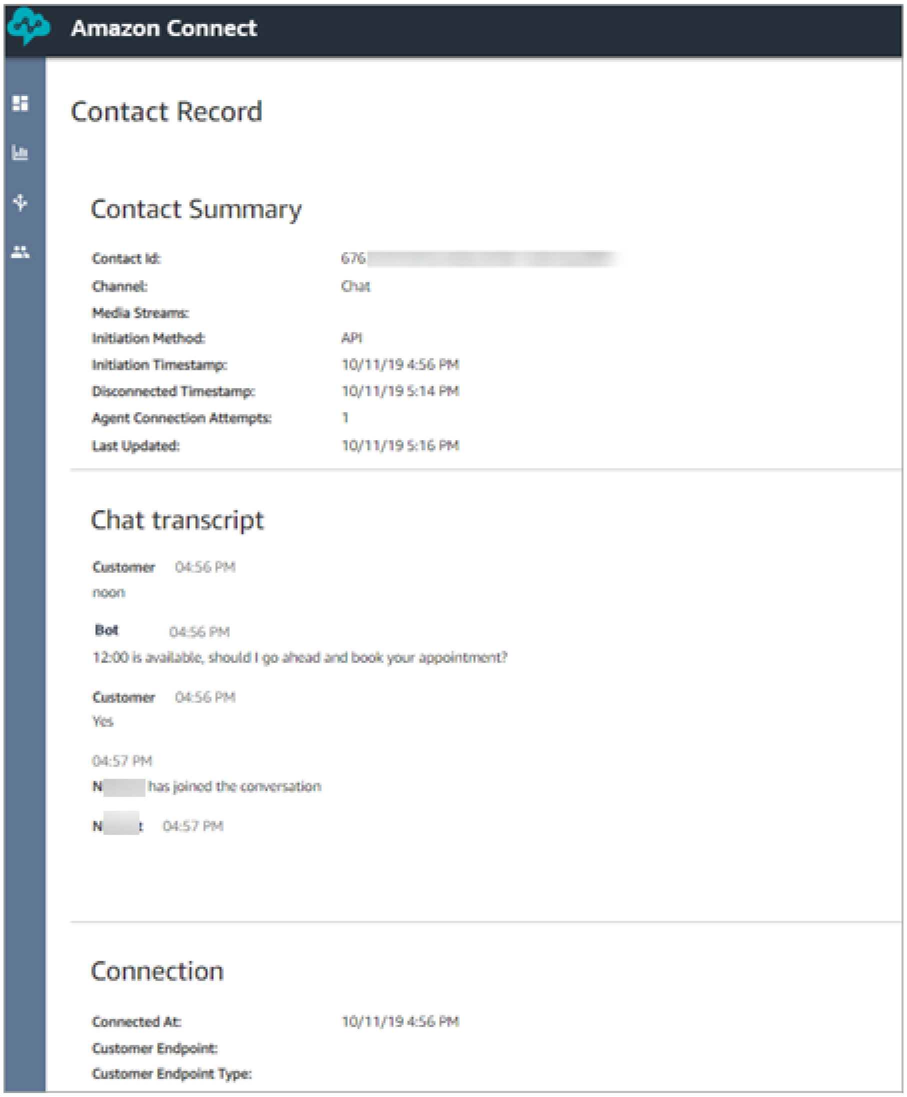
View a contact record in the UI

1. Do a contact search (p. 907). A list of contact IDs will be returned.

2. Choose an ID to view the contact record for the contact.

The following image shows part of a contact record in the UI, for a chat conversation. Note the following:

- For chats, the initiation method is always **API**.
- The chat transcript is visible in the UI.



Contact Record

Contact Summary

Contact Id:	676[redacted]
Channel:	Chat
Media Streams:	
Initiation Method:	API
Initiation Timestamp:	10/11/19 4:56 PM
Disconnected Timestamp:	10/11/19 5:14 PM
Agent Connection Attempts:	1
Last Updated:	10/11/19 5:16 PM

Chat transcript

Customer 04:56 PM
noon

Bot 04:56 PM
12:00 is available, should I go ahead and book your appointment?

Customer 04:56 PM
Yes

04:57 PM
N[redacted] has joined the conversation

N[redacted]t 04:57 PM

Connection

Connected At:	10/11/19 4:56 PM
Customer Endpoint:	
Customer Endpoint Type:	

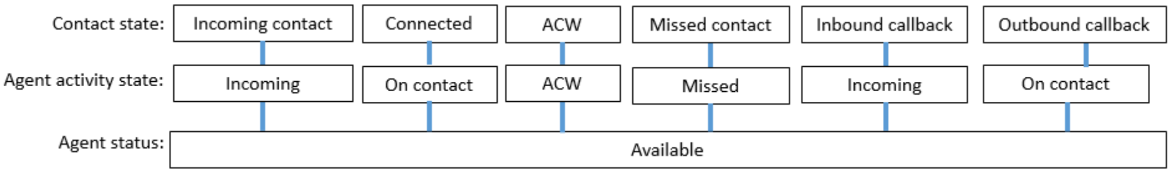
About agent status

Agents have a status. It's manually set in the Contact Control Panel (CCP).

- When they're ready to handle contacts, they set their status in the CCP to **Available**. This means inbound contacts can be routed to them.
- When agents want to stop taking inbound contacts, they set their status to a custom status that you create, such as **Break** or **Training**. They can also change their status to **Offline**.

> **Tip**
> Supervisors can manually change the agent's status in the real-time metrics report (p. 935).

The following diagram illustrates how the agent's status in the CCP stays constant while they are handling contacts, but in the real-time metrics report, the **Agent activity state** and the **Contact state** change.



For example, when the **Agent activity state** = **Incoming**, the **Contact state** = **Incoming contact**.

About custom agent statuses

It's possible for agents to make outbound calls when their status in the CCP is set to a custom status. Technically, agents can make an outbound call when their CCP is set to **Offline**.

For example, an agent wants to make an outbound call to a contact. Because they don't want contacts to be routed to them during this time, they set their status to a custom status. So when you look at your real-time metrics report, you'll see the agent is simultaneously on **NPT** (the metric that indicates a custom status) and **On contact**, for example.

About ACW (After contact work)

After a conversation between an agent and customer ends, the contact is moved into the ACW state.

When the agent finishes doing ACW for the contact, they click **Clear** to clear that slot so another contact can be routed to them.

To identify how long an agent spent on ACW for a contact:

- In the historical metrics report, **After contact work time** captures the amount of time each contact spent in ACW.
- In the agent event stream, you have to do some calculations. For more information, see Determine how long an agent spends doing ACW (p. 968).

How do you know when an agent can handle another contact?

The **Availability** metric tells you when agents are finished with a contact and ready to have another one routed to them.

What appears in the real-time metrics report?

To find out what the agent status is in the real-time metrics report, look at the **Agent Activity** metric.

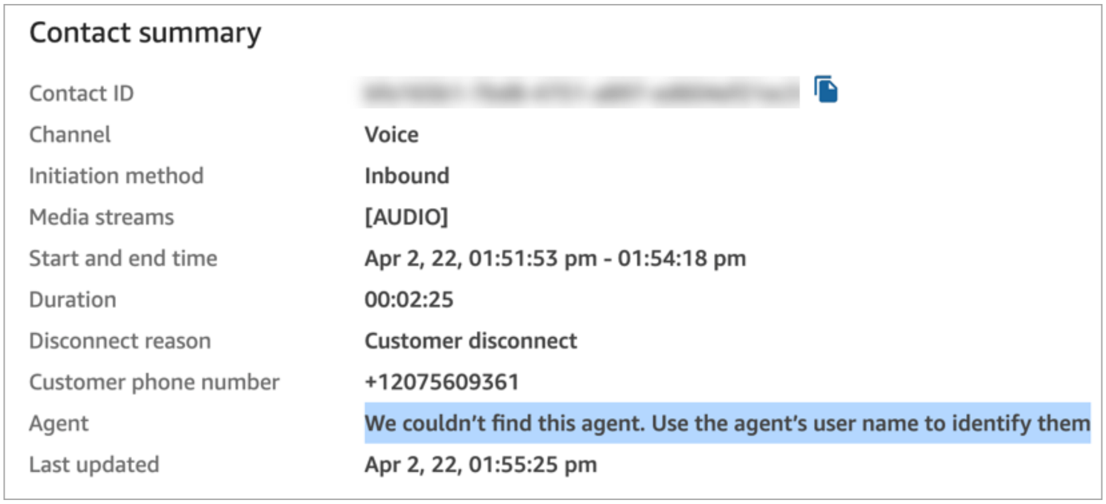
What appears in the agent event stream?

In the agent event stream you'll see the **AgentStatus**, for example:

```
{
 "AWSAccountId": "012345678901",
 "AgentARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent/agent-ARN",
  "CurrentAgentSnapshot": {
      "AgentStatus": {   //Here's the agent's status that they set in the CCP.
          "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/agent-state/agent-state-ARN",
          "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.
          "StartTimestamp": "2019-05-25T18:43:59.049Z"
      },
```

"We couldn't find this agent. Use the agent's user name to identify them."

On occassion, in the **Contact summary** the **Agent** field may say **"We couldn't find this agent. Use the agent's user name to identify them."**



Contact summary

Contact ID	[redacted]
Channel	Voice
Initiation method	Inbound
Media streams	[AUDIO]
Start and end time	Apr 2, 22, 01:51:53 pm - 01:54:18 pm
Duration	00:02:25
Disconnect reason	Customer disconnect
Customer phone number	+12075609361
Agent	We couldn't find this agent. Use the agent's user name to identify them
Last updated	Apr 2, 22, 01:55:25 pm

This is a generic message for contacts that did not get connected to an agent at the time. It usually means that the inbound call was not answered by the agent and the customer disconnected the call.

To confirm that the caller was never connected to an agent:

- **Disconnect reason** = **Customer disconnect**.
- No recording of the call is found for that contact ID.

To verify this behavior, call your contact center and disconnect after a period of time without an agent accepting the call.

About contact states

Contact states appear in two places: the real-time metrics reports and the agent event stream.

Contact states in the agent event stream

There are different events that can appear in the lifecycle of a contact. Each of these events appear in the agent event stream as a **State**. A contact can have the following states that appear in the agent event stream:

- INCOMING - This is specific to queued callbacks. The agent is presented with a callback.
- PENDING - This is specific to queued callbacks.
- CONNECTING - An inbound contact is being offered to the agent (it's ringing). The agent has not yet taken any action to accept or reject the contact, and they haven't missed it.
- CONNECTED - The agent has accepted the contact. Now the customer is in a conversation with the agent.
- CONNECTED_ONHOLD - They are in a conversation with the agent, and the agent has put the customer on hold.
- MISSED - The contact was missed by the agent.
- ERROR - This appears when, for example, the customer abandons the call during outbound whisper.
- ENDED - The conversation has ended, and the agent has started doing ACW for that contact.
- REJECTED - The contact was rejected by the agent or the customer abandoned the contact when it is connecting to the agent. This applies to chat and tasks.

Here's what the contact state looks like in the agent event stream:

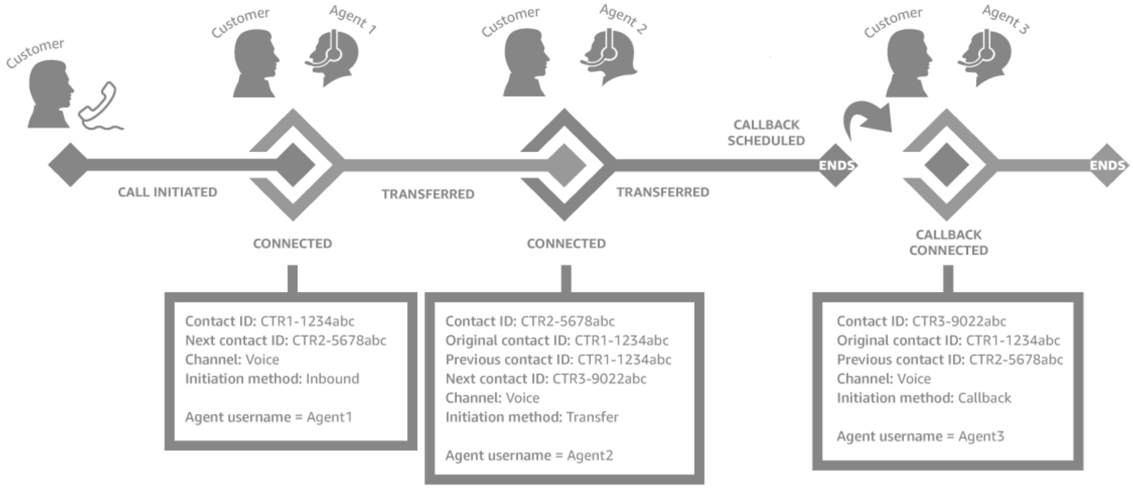
```
"Contacts": [
  {
    "Channel": "VOICE",  //This shows the agent and contact were talking on the phone.
    "ConnectedToAgentTimestamp": "2019-05-25T18:55:21.011Z",
    "ContactId": "ContactId-1",  //This shows the agent was working with a contact
 identified as "ContactId-1".
    "InitialContactId": null,
    "InitiationMethod": "OUTBOUND", //This shows the agent reached the customer by making
 an outbound call.
    "Queue": {
         "ARN": "arn:aws:connect:us-east-1:012345678901:instance/aaaaaaaa-bbbb-cccc-
dddd-111111111111/queue/queue-ARN-for-BasicQueue",
     },
    "QueueTimestamp": null,
    "State": "CONNECTED",  //Here's the contact state. In this case, it shows the contact
 was CONNECTED to the agent,
      instead of say, MISSED.
    "StateStartTimestamp": "2019-05-25T18:55:21.011Z"  //This shows when the contact was
 connected to the agent.
   }
  ]
```

Events in the contact record

A contact record captures events associated with the contact in your contact center. For example, how long the contact lasted, when it started and stopped. For a list of all data that's captured in the contact record, see Contact records data model (p. 985).

A contact record is opened for a customer when they are connected to your contact center. The contact record is completed when the interaction with the contact flow or agent ends (that is, the agent has completed the ACW and cleared the contact). This means it's possible for a customer to have multiple contact records.

The following diagram shows when a contact record is created for a contact.



Contact ID: CTR1-1234abc
Next contact ID: CTR2-5678abc
Channel: Voice
Initiation method: Inbound

Agent username = Agent1

Contact ID: CTR2-5678abc
Original contact ID: CTR1-1234abc
Previous contact ID: CTR1-1234abc
Next contact ID: CTR3-9022abc
Channel: Voice
Initiation method: Transfer

Agent username = Agent2

Contact ID: CTR3-9022abc
Original contact ID: CTR1-1234abc
Previous contact ID: CTR2-5678abc
Channel: Voice
Initiation method: Callback

Agent username = Agent3

Each time a contact is connected to an agent, a new contact record is created. The contact records for a contact are linked together through the contactId fields: original, next, and previous.

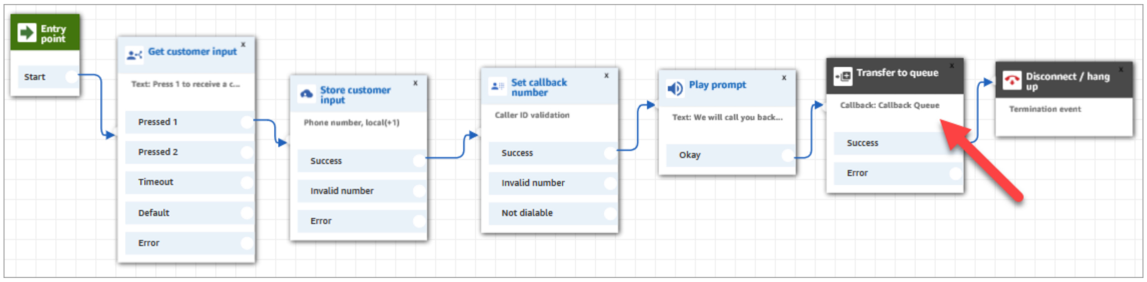
Tip
A contact is considered connected when a contact record is created. It's possible a contact record can be created before a call is finished ringing for the caller, due to network conditions and PSTN event propagation.

About queued callbacks in metrics

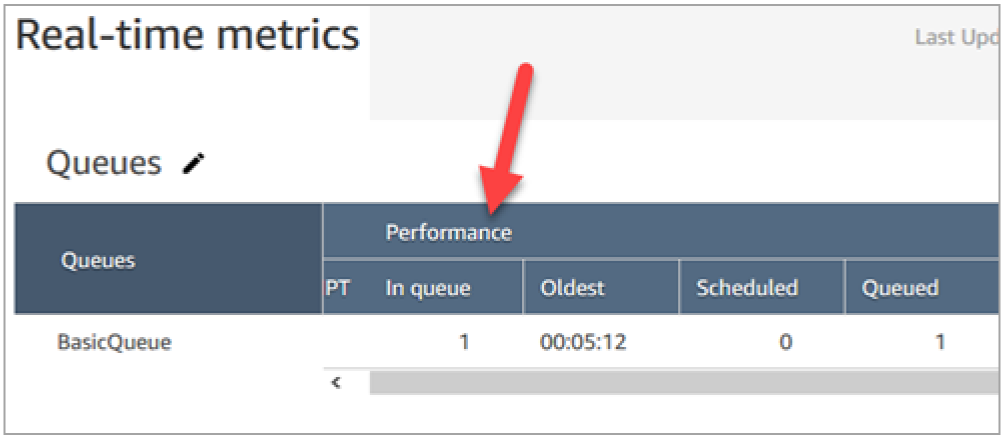
This topic explains how queued callbacks appear in your real-time metrics reports and the contact record.

Tip
To see only the number of customers who are waiting for a call back, you need to create a queue that only takes callback contacts. To learn how to do this, see Set up routing (p. 220). Currently there isn't a way to see the phone numbers of the contacts waiting for callbacks.

1. Callbacks are initiated when the Transfer to queue (p. 437) block is triggered to create the callback in a callback queue.



2. After any initial delay is applied, the callback is put into the queue. It remains there until an agent is available and can be offered the contact.

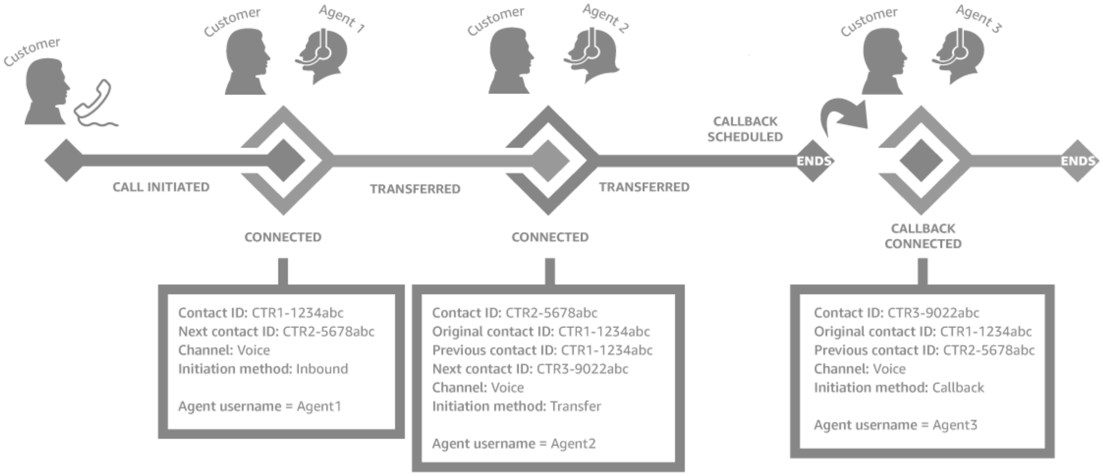


Real-time metrics

Queues

Queues	Performance				
	PT	In queue	Oldest	Scheduled	Queued
BasicQueue		1	00:05:12	0	1

3. When the callback is connected to the agent, a new contact record is created for the contact.



Contact ID: CTR1-1234abc
Next contact ID: CTR2-5678abc
Channel: Voice
Initiation method: Inbound

Agent username = Agent1

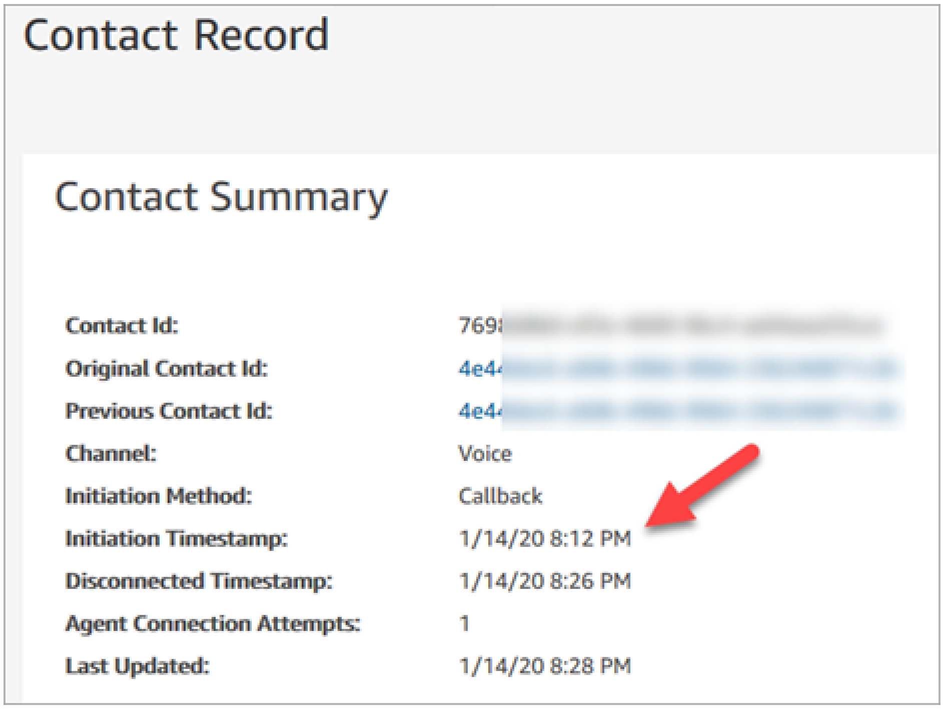
Contact ID: CTR2-5678abc
Original contact ID: CTR1-1234abc
Previous contact ID: CTR1-1234abc
Next contact ID: CTR3-9022abc
Channel: Voice
Initiation method: Transfer

Agent username = Agent2

Contact ID: CTR3-9022abc
Original contact ID: CTR1-1234abc
Previous contact ID: CTR2-5678abc
Channel: Voice
Initiation method: Callback

Agent username = Agent3

4. The **Initiation Timestamp** in the callback contact record corresponds to when the callback is initiated in the contact flow, shown in step 1.



Contact Record

Contact Summary

Contact Id:	769[redacted]
Original Contact Id:	4e4[redacted]
Previous Contact Id:	4e4[redacted]
Channel:	Voice
Initiation Method:	Callback
Initiation Timestamp:	1/14/20 8:12 PM
Disconnected Timestamp:	1/14/20 8:26 PM
Agent Connection Attempts:	1
Last Updated:	1/14/20 8:28 PM

How properties in the Transfer to Queue block affect this flow

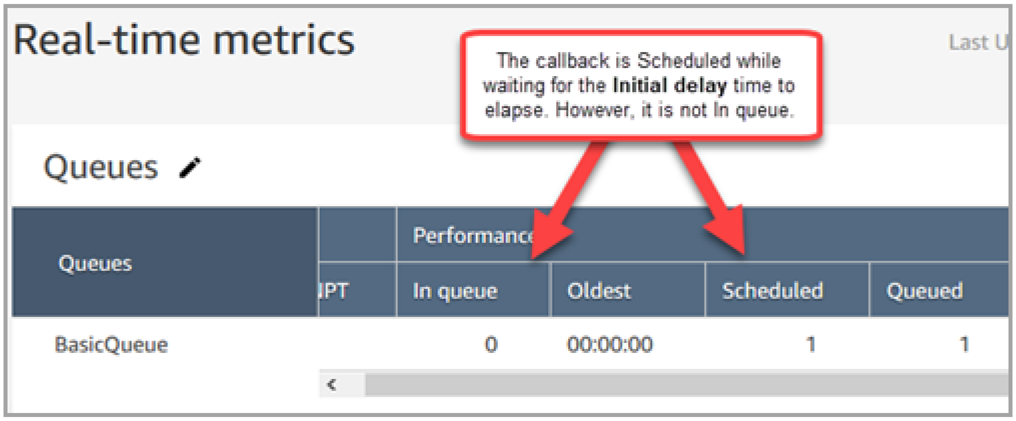
The Transfer to queue (p. 437) block has the following properties, which affect how Amazon Connect handles the callback:

- **Initial delay**: This property affects when a callback is put in queue. Specify how much time has to pass between a callback contact being initiated in the contact flow, and the customer being put in queue for the next available agent. For more information, see How Initial delay affects Scheduled and In queue metrics (p. 1004).
- **Maximum number of retries**: If this is set to 2, then Amazon Connect tries to call the customer at most three times: the initial callback, and two retries.
- **Minimum time between attempts**: If the customer doesn't answer the phone, this is how long to wait before trying again.

How Initial delay affects Scheduled and In queue metrics

In the Transfer to queue (p. 437) block, the **Initial delay** property affects when a callback is put in queue. For example, assume **Initial delay** is set to 30 seconds. Here's what appears in your real-time metrics report:

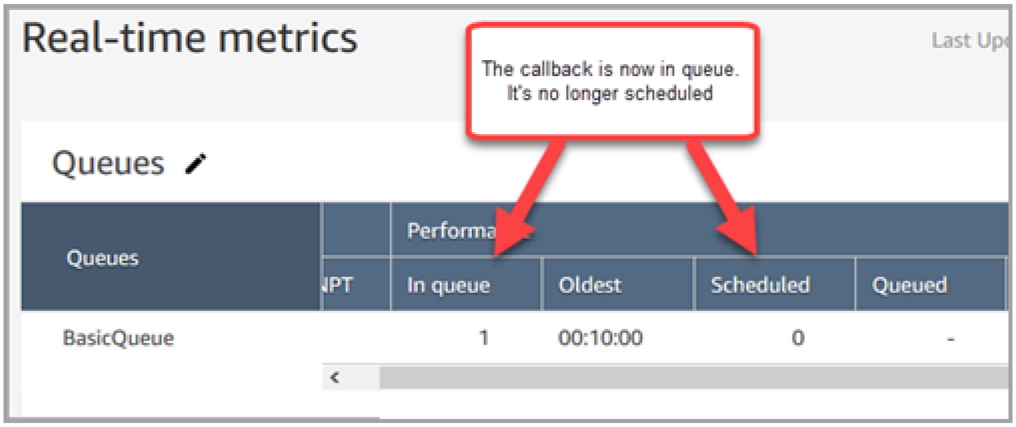
1. After 20 seconds, the callback has already been created, but it is not yet in queue because of the **Initial delay** setting.



The callback is Scheduled while waiting for the **Initial delay** time to elapse. However, it is not In queue.

Queues		Performance			
	PT	In queue	Oldest	Scheduled	Queued
BasicQueue		0	00:00:00	1	1

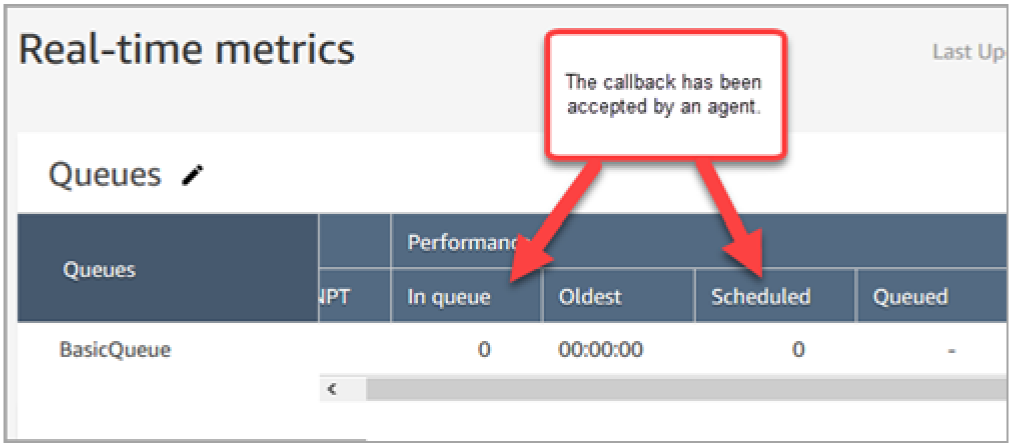
2. After 35 seconds, the callback contact has been placed in queue.



The callback is now in queue. It's no longer scheduled

Queues		Performa			
	PT	In queue	Oldest	Scheduled	Queued
BasicQueue		1	00:10:00	0	-

3. Assume that after 40 seconds, an agent accepts the callback.



The callback has been accepted by an agent.

Queues		Performanc			
	PT	In queue	Oldest	Scheduled	Queued
BasicQueue		0	00:00:00	0	-

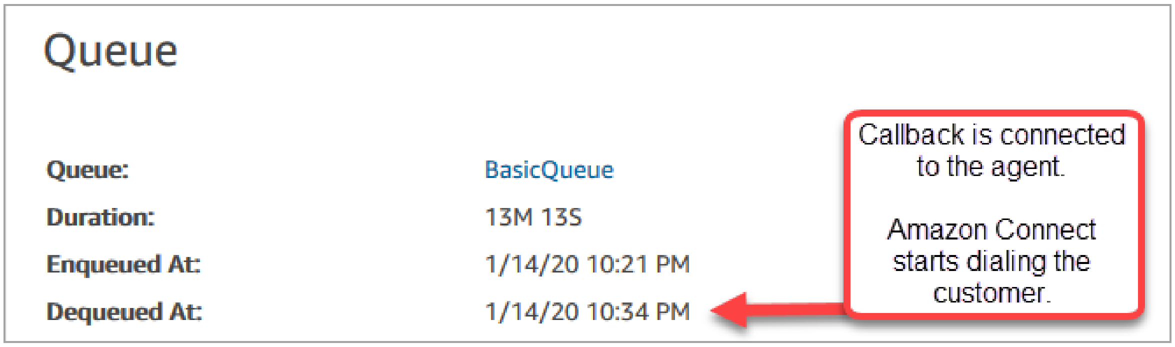
What counts as a "Failed Callback Attempt"

If an agent doesn't accept an offered callback, it doesn't count as an failed callback attempt. Rather, the routing engine offers the callback to the next available agent, until an agent accepts.

A failed callback attempt would be along the lines of: an agent accepts a callback but then something goes wrong between then and the agent being joined to the customer.

The contact is considered to be in the callback queue until an agent accepts the offered callback contact.

Amazon Connect removes the callback from the queue when it's connected to the agent. At that time, Amazon Connect starts dialing the customer. The following image shows what this looks like in a contact record:



Queue

Queue:	BasicQueue
Duration:	13M 13S
Enqueued At:	1/14/20 10:21 PM
Dequeued At:	1/14/20 10:34 PM

Callback is connected to the agent.

Amazon Connect starts dialing the customer.

The enqueued time on the contact record for a particular callback leg corresponds to the amount of time that the contact was in queue before that particular callback attempt was made. This is not the total enqueued time across all contact records.

For example, an inbound call could be in queue for 5 minutes before a callback is scheduled. Then, after an initial delay of 10 seconds, the callback contact could be in a callback queue for 10 seconds before an agent accepts it. In this case, you would see two contact records:

1. The first contact record, with InitiationMethod=INBOUND, would have an enqueued time of 5 minutes.
2. The second contact record, with InitiationMethod=CALLBACK, would have an enqueued time of 10 seconds.

Example: Metrics for a queued callback

This topic shows an example queued callback flow and reviews how the contact records and times are set for it.

Assume we have set up the following contact flows:

- **Inbound contact flow** -- Runs when the customer calls the customer service number.
- **Customer queue flow** – Runs when the customer is waiting in queue. In this example, we build a flow that offers a callback to the customer. If the customer selects yes, this contact flow executes the **Transfer to queue** block to transfer the contact to the callback queue named CallbackQueue, with an initial delay of 99 seconds, and then hangs up.
- **Outbound whisper flow** -- When a queued callback is placed, the customer hears this after they pick up and before they connect to the agent. For example, "Hello, this is your scheduled callback..."
- **Agent whisper flow** -- The agent hears this right after they accept the contact, before they are joined to the customer. For example, "You are about to be connected to Customer John, who requested a refund for..."

In this example, John calls customer service. Here's what happens:

1. Inbound contact flow creates contact record-1:
   a. John calls customer service at 11:35. The Inbound contact flow runs and puts him in queue at 11:35.
   b. The Customer queue flow runs. At 11:37, John chooses to schedule a callback, so Amazon Connect initiates a callback contact at 11:37, before the inbound contact is disconnected.
2. Callback contact flow creates contact record-2:

a. The callback contact was initiated at 11:37.
b. Because the initial delay is 99 seconds, the callback contact is placed into CallbackQueue at 11:38:39, after the 99 seconds pass. Now the callback contact is offered to an available agent.
c. After 21 seconds, an agent available at 11:39:00 and accepts the contact. The 10-second agent whisper flow is played to the agent.
d. After the agent whisper flow is complete, Amazon Connect calls John at 11:39:10. John picks up, and listens to the 15-second outbound whisper flow.
e. When the outbound whisper flow is complete, John is connected to the agent at 11:39:25. They talk until 11:45, and then John hangs up.

This scenario results in two contact records, which include the following metadata.

Contact record-1	Data	Notes
Initiation Method	Inbound	
Initiation Timestamp	11:35	The inbound contact is initiated in Amazon Connect.
ConnectedToSystem Timestamp	11:35	Because this is an inbound contact, InitiationTimestamp = ConnectedToSystemTimestamp.
Next Contact Id	points to contact record-2	
Queue	InboundQueue	
Enqueued Timestamp	11:35	The inbound contact is put in queue.
Dequeued Timestamp	11:37	Because no agent picked up, this is the same as DisconnectedTimestamp.
ConnectedToAgent Timestamp	N/A	John scheduled a callback before any agent could pick up.
Disconnected Timestamp	11:37:00	John was disconnected by contact flow.

contact record-2	Data	Notes
PreviousContactId	points to contact record-1	
Initiation Timestamp	11:37	The callback contact is created in Amazon Connect.
Queue	CallbackQueue	
Enqueued Timestamp	11:38:39	The contact was put into the CallbackQueue, after the 99-second initial delay completes.
Dequeued Timestamp	11:39:00	After 21 seconds, an agent accepts the contact.

contact record-2	Data	Notes
Queue Duration	120 seconds	This is the initial delay (99 seconds), plus any additional time sitting in queue waiting for an agent to become available (21 seconds).
ConnectedToSystem Timestamp	11:39:10	John is called after the 10 second agent whisper flow completes.
ConnectedToAgent Timestamp	11:39:25	John and the agent are connected, after the 15 second outbound whisper flow completes.
Disconnected Timestamp	11:45	John hangs up.

Save custom reports

You can create custom real-time, historical, and login/logout reports that include only the metrics you're interested in. For instructions, see Create a real-time metrics report (p. 932) and Create a historical metrics report (p. 952).

After you create a report, you can:

- Save (p. 1008) the custom report and return to it later.
- Share (p. 1010) a link to the custom report so only people in your organization who have the link AND who have the appropriate permissions (p. 1012) in their security profile can access the report.
- Publish (p. 1013) the report so everyone in your organization who has the appropriate permissions (p. 1013) in their security profile can view the report.

Personal saved reports count towards quota

Personal saved reports count towards your service quota of reports per instance. For example, if you save a report every day, it will count towards your organization's number of saved reports for the instance.

For more information about quotas, see Amazon Connect service quotas (p. 1205).

Create a naming convention

All saved reports in your Amazon Connect instance must have a unique name. We recommend creating a naming convention that indicates who the owner of the report is. For example, use the team name or owner alias as the report suffix: Agent Performance - *team name*. That way, if the report is published, others will know who owns it.

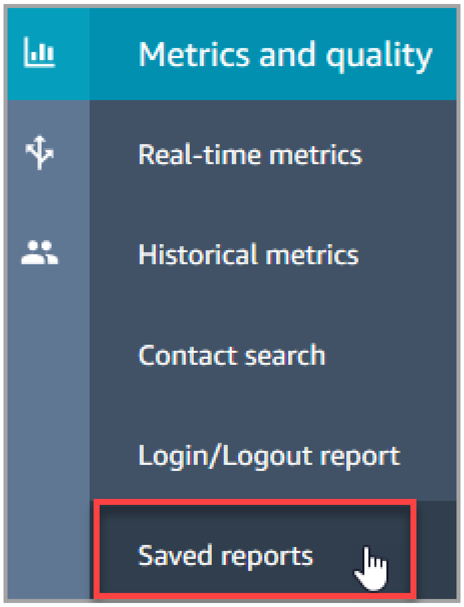
If your organization needs to delete reports because you've reached the service quota for reports for your instance, a naming convention that includes the team or owner alias will help you track down the report owners to find out if the report is still needed.

How to save reports

1. Customize a real-time, historical, or login/logout report to include the metrics you want.

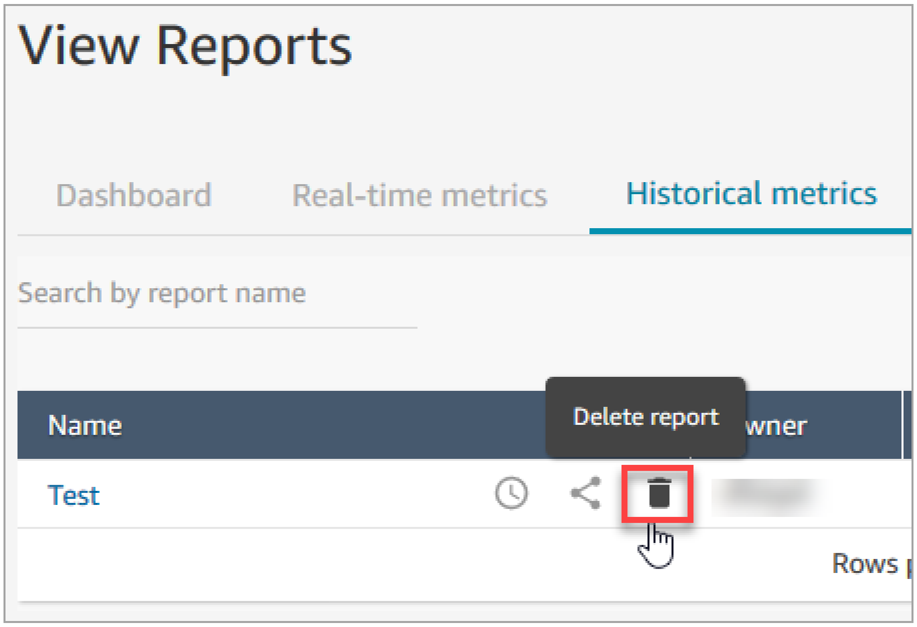
2. Choose **Save**. If you don't have permissions in your security profile to create reports, this button will be inactive.
3. Assign a unique name to the report.

   Tip
   We recommend establishing a naming convention for reports in your organization, especially published reports. This will help everyone identify who the owner is. For example, use the team name or owner alias as the report suffix: Agent Performance - *team name*.
4. To view to the report at a later time, go to **Analytics**, **Saved reports**.



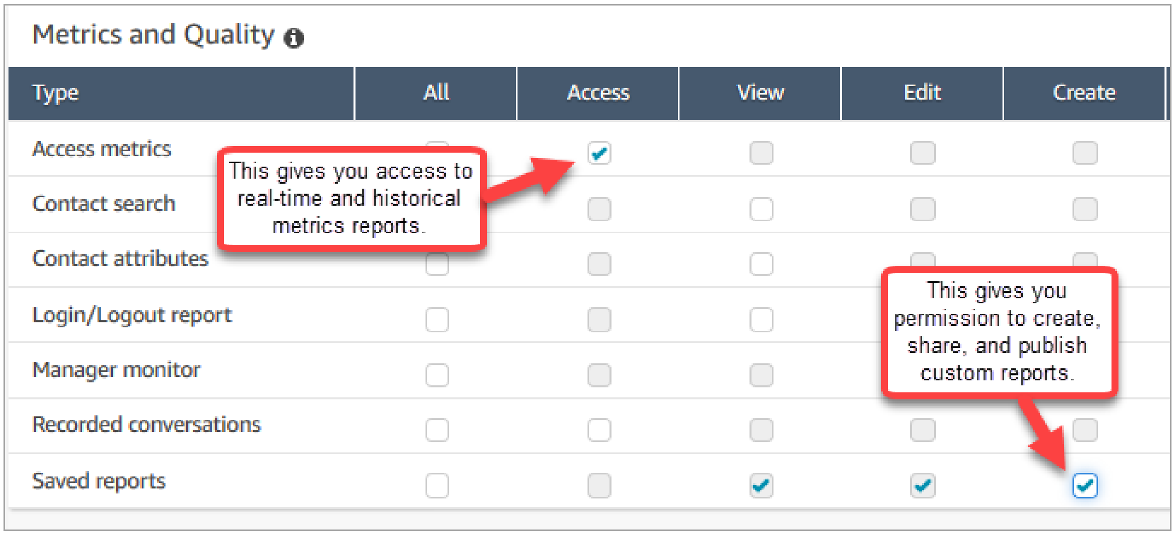
How to delete saved reports

1. On the navigation menu, choose **Analytics**, **Saved reports**.
2. Choose the **Historical metrics** tab.
3. Go to the row that has the report you want to delete, and choose the **Delete** icon. If you don't have permissions in your security profile to delete reports, this option won't be available.



Share custom reports

You can only share reports that you create and save. This means you need the following permissions in your security profile to share reports: **Access metrics** and **Create** saved reports.



Metrics and Quality

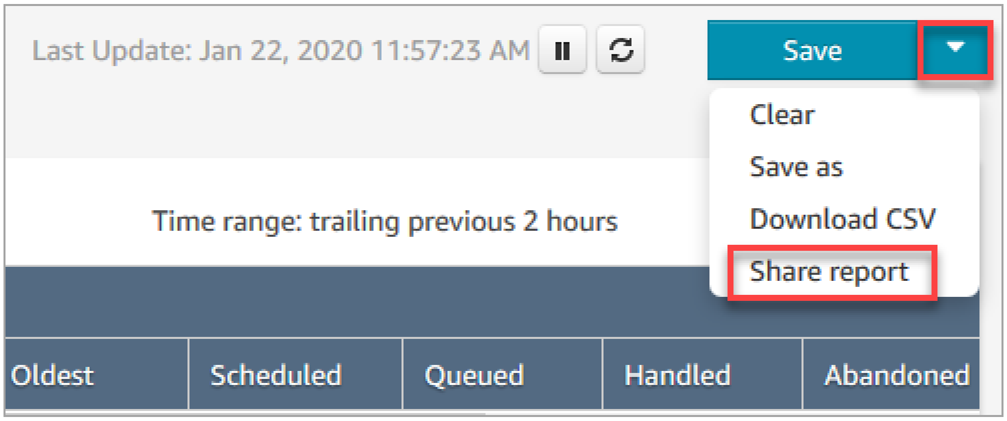
Type	All	Access	View	Edit	Create
Access metrics	□	☑	□	□	□
Contact search		□	□	□	□
Contact attributes	□	□	□	□	□
Login/Logout report	□	□	□		
Manager monitor	□	□	□		
Recorded conversations	□	□	□	□	□
Saved reports	□	□	☑	☑	☑

This gives you access to real-time and historical metrics reports.

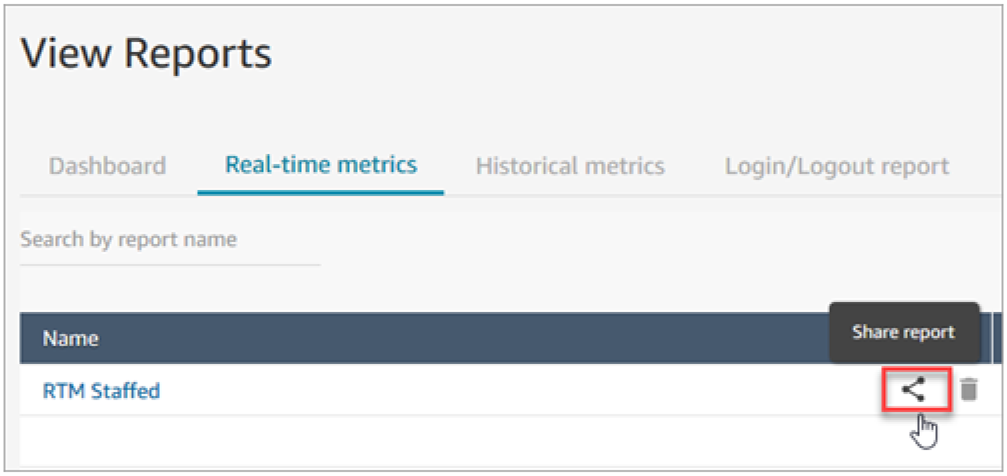
This gives you permission to create, share, and publish custom reports.

To share reports

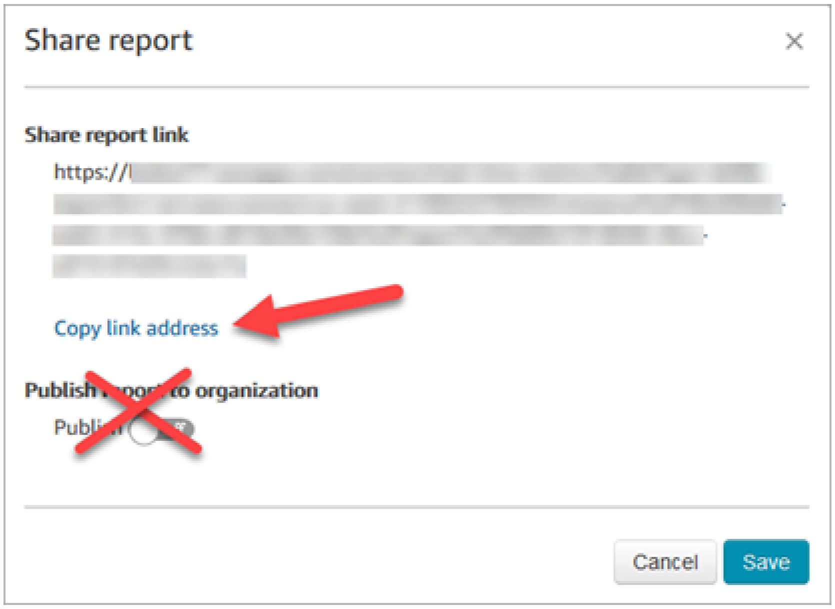
1. On the report page, choose **Share report**.



Or, from your list of saved reports, choose the **Share report** icon.



2. Choose **Copy link address** and choose **Save**. This saves the link to your clipboard. Paste this link into an email or other location to share the report.



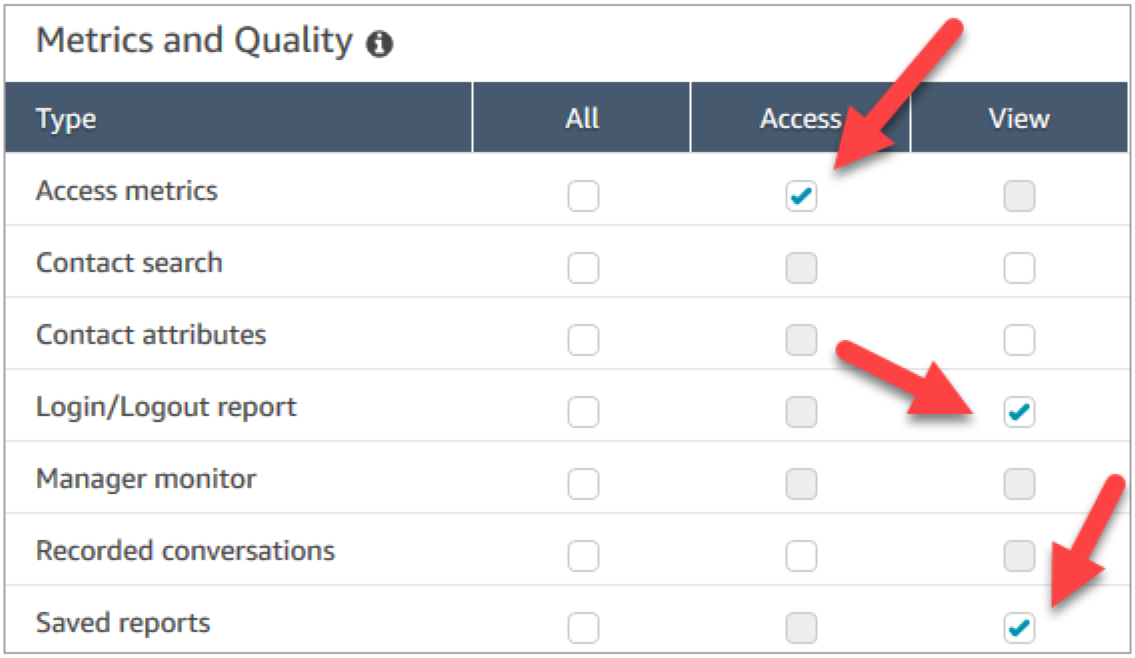
You don't need to publish the report to your organization in order to share the link with specific people.

> **Important**
> Anyone who has the link and the appropriate permissions can access the report.

View a shared report

To view a report that someone has shared with you, you need the following:

- A link to the report.
- Permissions in your security profile:
  - **Access metrics**, if the report is a real-time or historical metrics report
  - **View** Login/Logout report, if the report is a login/logout report
  - **View** Saved reports



Metrics and Quality

Type	All	Access	View
Access metrics	□	☑	□
Contact search	□	□	□
Contact attributes	□	□	□
Login/Logout report	□	□	☑
Manager monitor	□	□	□
Recorded conversations	□	□	□
Saved reports	□	□	☑

Tips for viewing a shared report

- Every time you want to view the shared report, you need to access it through the link that was shared with you.
- If you get a 505 error when you choose the link that was shared with you, it means you don't have permissions to view the report.
- There's no way to save the exact same report to your list of Saved reports. You can give the report a new name and save it to your list, but then it's a different report from the one that was shared with you. If the owner of original report makes changes, you won't see them in your renamed report.

Publish reports

After you create and save a custom report with the metrics you're interested in, you can publish it so everyone in your organization with the appropriate permissions (p. 1013) can access the report.

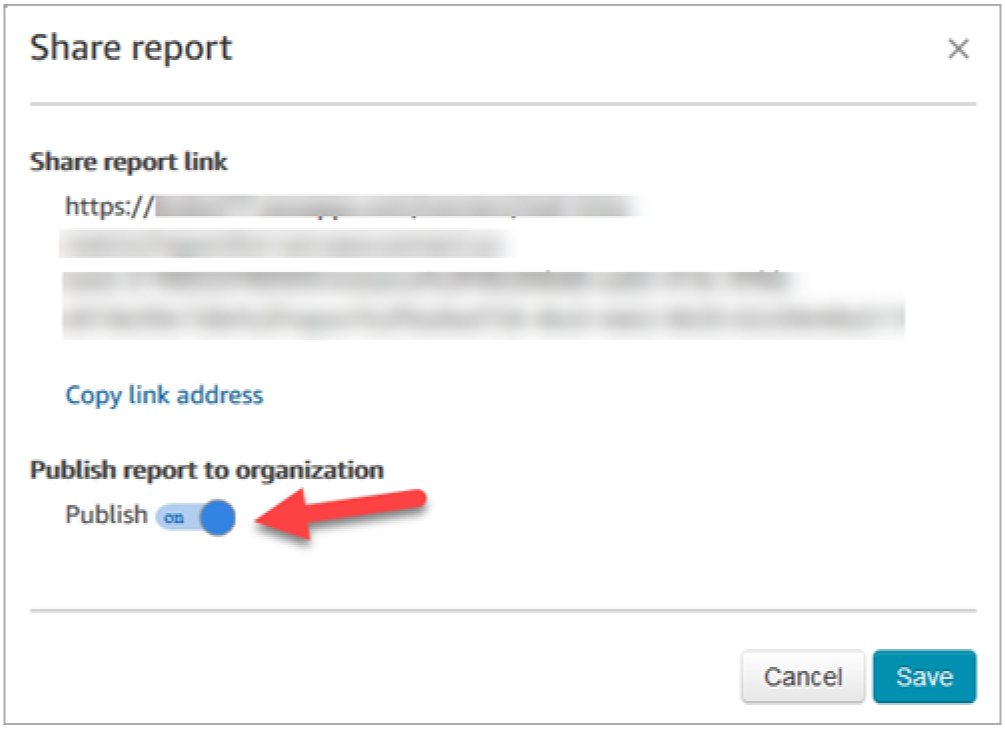
After a report is published, people will be able to see the report in their list of Saved reports.

> **Tip**
> We recommend establishing a naming convention for reports in your organization. When reports are published, this will help everyone identify who the owner is. For example, use the team name or owner alias as the report suffix: Agent Performance - *team name*.

Only people who have permissions in their security profile to **Create** saved reports will be able to change the published report and save their changes to the published version.

To publish a report

1. On the real-time metrics, historical metrics, login/logout report, or Saved reports page, choose **Share report**.
2. Toggle **Publish report** to **On**, and then choose **Save**.



Share report

Share report link

https://[redacted]

Publish report to organization

Publish on

The report appears in the list of Saved reports for everyone who has appropriate permissions in their security profile.

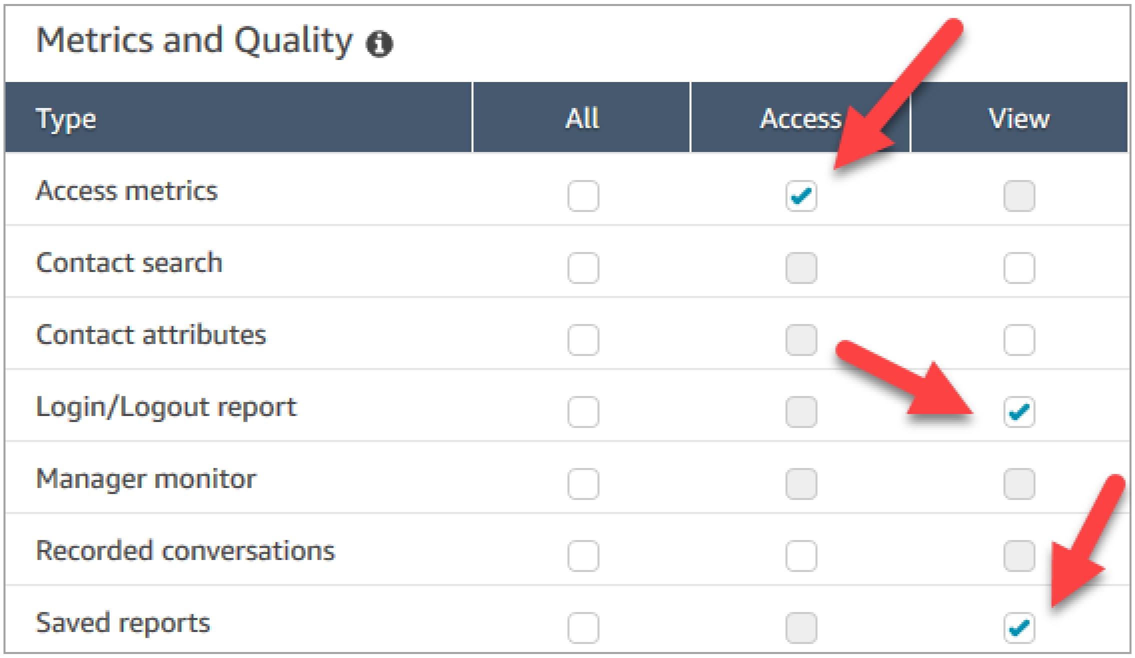
3. To unpublish the report, move the toggle to **Off**.

The report is removed from everyone's list of Saved reports.

View published reports

To view published reports, at minimum you need the following permissions in your security profile:

- **Access metrics**, if the report is a real-time or historical metrics report
- **View** Login/Logout report, if the report is a login/logout report
- **View** Saved reports



Metrics and Quality

Type	All	Access	View
Access metrics	□	☑	□
Contact search	□	□	□
Contact attributes	□	□	□
Login/Logout report	□	□	☑
Manager monitor	□	□	□
Recorded conversations	□	□	□
Saved reports	□	□	☑

To view published reports

- Go to **Analytics**, **Saved reports**.

  Published reports appear in your list automatically.

Monitoring your instance using CloudWatch

Amazon Connect sends data about your instance to CloudWatch metrics so that you can collect, view, and analyze CloudWatch metrics for your Amazon Connect virtual contact center. You can use this data to monitor key operational metrics and set up alarms. Data about your contact center is sent to CloudWatch every 1 minute.

When you view the CloudWatch metrics dashboard, you can specify the refresh interval for the data displayed. The values displayed in the dashboard reflect the values for the refresh interval you define. For example, if you set the refresh interval to 1 minute, the values displayed are for a minute period. You can select a refresh interval of 10 seconds, but Amazon Connect does not send data more often than every 1 minute. Metrics that are sent to CloudWatch are available for two weeks, and then discarded. To learn more about metrics in CloudWatch, see the Amazon CloudWatch User Guide.

> **Note**
> If your Amazon Connect instance was created on or before October 2018, you need to provide Amazon Connect with permission to begin publishing chat metrics to your CloudWatch account. To do so, create an IAM policy with the following permission and attach it to the Amazon Connect service role. You can find the Amazon Connect service role on the **Account overview** page for your Amazon Connect instance.

```
{
  "Effect": "Allow",
  "Action": "cloudwatch:PutMetricData",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "cloudwatch:namespace": "AWS/Connect"
    }
  }
}
```

Amazon Connect metrics sent to CloudWatch

The `AWS/Connect` namespace includes the following metrics.

Metric	Description
CallsBreachingConcurrencyQuota	The total number of voice calls that exceeded the concurrent calls quota for the instance. For the total number of calls that breach the quota, take a look at the Sum statistic. For example, assume your contact center experiences the following volumes, and your service quota is 100 concurrent calls: • 0:00 : 125 concurrent calls. This is 25 over the quota. • 0:04 : 135 concurrent calls. This is 35 over the quota. • 0:10 : 150 concurrent calls. This is 50 over the quota. CallsBreachingConcurrencyQuota = 110: the total number of voice calls that exceeded the quota between 0:00 and 0:10. Unit: Count Dimension: • **InstanceId**: The ID of your instance • **MetricGroup**: **VoiceCalls**
CallBackNotDialableNumber	The number of times a queued callback to a customer could not be dialed because the customer's number is in a country for which outbound calls are not allowed for the instance. The countries allowed for an instance are defined by the service quotas. 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:

Metric	Description
	- **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**
ChatsBreachingActiveChatQuota	The total number of valid requests made to start a chat that exceeded the concurrent active chats quota for the instance. For the total number of chats requests that breach the quota, take a look at the Sum statistic. For example, assume your contact center experiences the following volumes, and your service quota is 2500 concurrent active chats: - 0:00 : 2525 concurrent active chats. This is 25 over the quota. - 0:04 : 2535 concurrent active chats. This is 35 over the quota. - 0:10 : 2550 concurrent active chats. This is 50 over the quota. ChatsBreachingActiveChatsQuota = 110: the total number of chats that exceeded the quota between 0:00 and 0:10. Unit: Count Dimensions: - **InstanceId**: The ID of your instance - **MetricGroup**: **Chats**
ConcurrentActiveChats	The number of concurrent active chats (p. 1205) in the instance at the time the data is displayed in the dashboard. The value displayed for this metric is the number of concurrent active chats at the time the dashboard is displayed, and not a sum for the entire interval of the refresh interval set. All active chats are included, not only active tasks that are connected to agents. While all statistics are available in CloudWatch for concurrent active chats, you might be most interested in looking at the Maximum/Average statistic. The Sum statistic isn't as useful here. Unit: Count Dimensions: - **InstanceId**: The ID of your instance - **MetricGroup**: **Chats**

Metric	Description
ConcurrentActiveChatsPercentage	The percentage of the concurrent active chats service quota used in the instance. This is calculated by: • ConcurrentActiveChats / ConfiguredConcurrentActiveChatsLimit Where ConfiguredConcurrentActiveChatsLimit is the Concurrent active chats per instance configured for your instance. Unit: Percent (Output displays as an integer. For example, 1% of chats is shown as 1, not as 0.01.) Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **Chats**
ConcurrentCalls	The number of concurrent active voice calls in the instance at the time the data is displayed in the dashboard. The value displayed for this metric is the number of concurrent active calls at the time the dashboard is displayed, and not a sum for the entire interval of the refresh interval set. All active voice calls are included, not only active calls that are connected to agents. While all statistics are available in CloudWatch for concurrent voice calls you might be most interested in looking at the Maximum/Average statistic. The Sum statistic isn't as useful here. Unit: Count Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **VoiceCalls**
ConcurrentCallsPercentage	The percentage of the concurrent active voice calls service quota used in the instance. This is calculated by: • ConcurrentCalls / ConfiguredConcurrentCallsLimit Unit: Percent (output displays as a decimal) Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **VoiceCalls**

Metric	Description
ConcurrentTasks	The number of concurrent active tasks in the instance at the time the data is displayed in the dashboard. The value displayed for this metric is the number of concurrent active tasks at the time the dashboard is displayed, and not a sum for the entire interval of the refresh interval set. All active tasks are included, not only active tasks that are connected to agents. While all statistics are available in CloudWatch for concurrent tasks you might be most interested in looking at the Maximum/Average statistic. The Sum statistic isn't as useful here. Unit: Count Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **Tasks**
ConcurrentTasksPercentage	The percentage of the concurrent active tasks service quota used in the instance. This is calculated by: • ConcurrentTasks / ConfiguredConcurrentTasksLimit Where ConfiguredConcurrentTasksLimit is the Concurrent tasks per instance (p. 1205) configured for your instance. Unit: Percent (output displays as a decimal) Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **Tasks**
ContactFlowErrors	The number of times the error branch for a contact flow was run. 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

Metric	Description
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: Count 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

Metric	Description
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
SuccessfulChatsPerInterval	The number of chats successfully started in the instance for the defined interval. Unit: Count Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **Chats**
TasksBreachingConcurrencyQuota	The total number of tasks that exceeded the concurrent tasks quota for the instance. For the total number of tasks that breach the quota, take a look at the Sum statistic. For example, assume your contact center experiences the following volumes, and your service quota is 2500 concurrent tasks: • 0:00 : 2525 concurrent tasks. This is 25 over the quota. • 0:04 : 2535 concurrent tasks. This is 35 over the quota. • 0:10 : 2550 concurrent tasks. This is 50 over the quota. TasksBreachingConcurrencyQuota = 110: the total number of tasks that exceeded the quota between 0:00 and 0:10. Unit: Count Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **Tasks**
TasksExpired	Tasks which have expired after being active for 7 days. To monitor the total number of tasks that have expired in a given time period, take a look at the Sum statistic in CloudWatch. Unit: Count Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **Tasks** • **ContactId**: The ID of the task contact

Metric	Description
TasksExpiryWarningReached	Tasks that have been active for 6 days 22 hours and reached expiry warning limit. To monitor the total number of tasks that have reached expiry warning limit in a given time period, take a look at the Sum statistic in CloudWatch. Unit: Count Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **Tasks** • **ContactId**: The ID of the task contact
ThrottledCalls	The number of voice calls that were rejected because the rate of calls per second exceeded the maximum supported quota. To increase the supported rate of calls, request an increase in the service quota for concurrent active calls per instance. To monitor the total throttled calls in a given time period, take a look at the Sum statistic in CloudWatch. Unit: Seconds Unit: Count Dimensions: • **InstanceId**: The ID of your instance • **MetricGroup**: **VoiceCalls**
ToInstancePacketLossRate	The ratio of packet loss for calls in the instance, reported every 10 seconds. Each data point is between 0 and 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. When you view metrics in the dashboard, only metrics with data are displayed. If there is no activity during the refresh interval for which there is a metric, then no data from your instance is displayed in the dashboard.

The following dimensions are used in the CloudWatch dashboard for Amazon Connect metrics.

Contact flow metrics dimension

> **Note**
> If a contact flow has a dimension name in non-ASCII characters, you won't be able to see it in CloudWatch.

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

- ContactFlowErrors
- ContactFlowFatalErrors
- PublicSigningKeyUsage

Contact metrics dimension

Filters metric data by contacts. Includes the following metrics:

- TasksExpiryWarningReached
- TasksExpired

Instance metrics dimension

Filters meta data by instance. Includes the following metrics:

- CallsBreachingConcurrencyQuota
- CallsPerInterval
- CallRecordingUploadError
- ChatsBreachingActiveChatQuota
- ConcurrentActiveChats
- ConcurrentActiveChatsPercentage
- ConcurrentCalls
- ConcurrentCallsPercentage
- ConcurrentTasks
- ConcurrentTasksPercentage
- MisconfiguredPhoneNumbers
- MissedCalls
- SuccessfulChatsPerInterval
- TasksBreachingConcurrencyQuota
- ThrottledCalls

Instance ID, Participant, Stream Type, Type of Connection

Filters metric data by connection. Includes the following metrics:

- ToInstancePacketLossRate

Queue metrics dimension

> **Note**
> If a queue has a dimension name in non-ASCII characters, you won't be able to see it in CloudWatch.

Filters metric data by queue. Includes the following metrics:

- CallBackNotDialableNumber
- LongestQueueWaitTime
- QueueCapacityExceededError
- QueueSize

Amazon Connect Voice ID metrics sent to CloudWatch

The `VoiceID` namespace includes the following metrics.

RequestLatency

The elapsed time for the request.

Frequency: 1 minute

Unit: Milliseconds

Dimension: API

UserErrors

The number of Error counts due to bad requests from user.

Frequency: 1 minute

Unit: Count

Dimension: API

SystemErrors

The number of Error counts due to internal service error.

Frequency: 1 minute

Unit: Count

Dimension: API

Throttles

The number of requests that are rejected due to exceeding the max rate allowed for sending requests.

Frequency: 1 minute

Unit: Count

Dimension: API

ActiveSessions

The number of active sessions in the domain. Active sessions are sessions that are in pending or ongoing status.

Frequency: 1 minute

Unit: Count

Dimension: Domain

ActiveSpeakerEnrollmentJobs

The number of active Batch Enrollment Jobs in the domain. Active Jobs are those which are in Pending or InProgress status.

Frequency: 15 minutes

Unit: Count

Dimension: Domain

ActiveFraudsterRegistrationJobs

The number of active Batch Registration Jobs in the domain. Active Jobs are those which are in Pending or InProgress status.

Frequency: 15 minutes

Unit: Count

Dimension: Domain

Speakers

The number of Speakers in the domain.

Frequency: 15 minutes

Unit: Count

Dimension: Domain

Fraudsters

The number of Fraudsters in the domain.

Frequency: 15 minutes

Unit: Count

Dimension: Domain

Amazon Connect Voice ID metrics dimensions

The following dimensions are used in the CloudWatch dashboard for Amazon Connect Voice ID metrics. When you view metrics in the dashboard, only metrics with data are displayed. If there is no activity during the refresh interval for which there is a metric, then no data from your instance is displayed in the dashboard.

API metrics dimension

This dimension limits the data to one of the following Voice ID operations:

- DeleteFraudster
- EvaluateSession
- ListSpeakers
- DeleteSpeaker
- OptOutSpeaker

Domain metrics dimension

The Voice ID domain where the enrollment, authentication or registration is conducted.

Use CloudWatch metrics to calculate concurrent call quota

Here's how to calculate your quota for concurrent calls.

With calls active in the system, look at **ConcurrentCalls** and **ConcurrentCallsPercentage**. Calculate the quota:

- (ConcurrentCalls / ConcurrentCallsPercentage)

For example, if **ConcurrentCalls** is 20 and **ConcurrentCallsPercentage** is 50, your quota is calculated as (20/50) = 0.40 which is 40%.

Use CloudWatch metrics to calculate concurrent active chats quota

Here's how to calculate your quota for concurrent active chats.

With chats active in the system, look at **ConcurrentActiveChats** and **ConcurrentChatsPercentage**. Calculate the quota:

- (ConcurrentActiveChats / ConcurrentActiveChatsPercentage) * 100

For example, if **ConcurrentActiveChats** is 1000 and **ConcurrentActiveChatsPercentage** is 50, your quota is calculated as (1000/50)*100 = 2000.

Use CloudWatch metrics to calculate concurrent task quota

Here's how to calculate your quota for concurrent tasks.

With tasks active in the system, look at **ConcurrentTasks** and **ConcurrentTasksPercentage**. Calculate the quota:

- (ConcurrentTasks / ConcurrentTasksPercentage)*100

For example, if **ConcurrentTasks** is 20 and **ConcurrentTasksPercentage** is 50, your quota is calculated as (20/50)*100= 40.

Logging Amazon Connect API calls with AWS CloudTrail

Amazon Connect is integrated with AWS CloudTrail, a service that provides a record of the Amazon Connect API calls that a user, role, or AWS service makes. CloudTrail captures Amazon Connect API calls as events. All public Amazon Connect APIs support CloudTrail.

Using the information that CloudTrail collects, you can identify a specific request to an Amazon Connect API, the IP address of the requester, the requester's identity, the date and time of the request, and so on. If you configure a trail, you can enable continuous delivery of CloudTrail events to an Amazon S3 bucket. If you don't configure a trail, you can view the most recent events in **Event History** in the CloudTrail console.

For more information about CloudTrail, including how to configure and enable it, see Creating a Trail For Your AWS Account and AWS CloudTrail User Guide.

Amazon Connect information in CloudTrail

CloudTrail is enabled on your AWS account when you create the account. When supported event activity occurs in Amazon Connect, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see Viewing Events with CloudTrail Event History.

For an ongoing record of events in your AWS account, including events for Amazon Connect, create a trail. A *trail* enables CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all AWS Regions and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- Creating a trail for your AWS account
- CloudTrail supported services and integrations
- Configuring Amazon SNS notifications for CloudTrail
- Receiving CloudTrail log files from multiple Regions
- Receiving CloudTrail log files from multiple accounts

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.
- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the CloudTrail userIdentity Element.

Example: Amazon Connect log file entries

A trail is a configuration that enables delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `GetContactAttributes` action.

```
{
        "eventVersion": "1.05",
        "userIdentity": {
         "type": "AssumedRole",
         "principalId": "AAAAAAA1111111EXAMPLE",
         "arn": "arn:aws:sts::123456789012:assumed-role/John",
         "accountId": "123456789012",
         "accessKeyId": "AAAAAAA1111111EXAMPLE",
         "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2019-08-15T06:40:14Z"
            },
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAA1111111EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/John",
                "accountId": "123456789012",
                "userName": "John"
            }
        }
    },
    "eventTime": "2019-08-15T06:40:55Z",
    "eventSource": "connect.amazonaws.com",
    "eventName": "GetContactAttributes",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "205.251.233.179",
    "userAgent": "aws-sdk-java/1.11.590 Mac_OS_X/10.14.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.202-b08 java/1.8.0_202 vendor/Oracle_Corporation",
    "requestParameters": {
        "InitialContactId": "00fbeee1-123e-111e-93e3-11111bfbfcc1",
        "InstanceId": "00fbeee1-123e-111e-93e3-11111bfbfcc1"
    },
    "responseElements": null,
    "requestID": "be1bee1d-1111-11e1-1eD1-0dc1111f1ac1c",
    "eventID": "00fbeee1-123e-111e-93e3-11111bfbfcc1",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "recipientAccountId": "123456789012"
}
```

Example: Amazon Connect Voice ID log file entries

Just like Amazon Connect, Voice ID is integrated with CloudTrail. When enabled, the service emits events for the Voice ID API calls made by a user, role, or an AWS service. You can reuse the same CloudTrail resources created for Amazon Connect, including the trail and the S3 bucket, to receive CloudTrail logs for Voice ID as well.

For security reasons, the sensitive fields which might contain PII information in the API requests and responses are redacted in the events.

The following example shows a CloudTrail log entry that demonstrates the `CreateDomain` action.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROA5STZEFPSWCM4YHJB2:SampleUser",
    "arn": "arn:aws:sts::111122223333:assumed-role/SampleRole/SampleUser",
    "accountId": "111122223333",
    "accessKeyId": "AAAAAAA1111111EXAMPLE",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "EXAMPLEZEFPSWCM4YHJB2",
        "arn": "arn:aws:iam::111122223333:role/SampleRole",
        "accountId": "111122223333",
        "userName": "SampleRole"
      },
      "webIdFederationData": {},
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2021-08-17T01:55:39Z"
      }
    }
  },
  "eventTime": "2021-08-17T01:55:41Z",
  "eventSource": "voiceid.amazonaws.com",
  "eventName": "CreateDomain",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.251.233.179",
  "userAgent": "aws-sdk-java/1.11.590 Mac_OS_X/10.14.6 Java_HotSpot(TM)_64-
Bit_Server_VM/25.202-b08 java/1.8.0_202 vendor/Oracle_Corporation",
  "requestParameters": {
    "description": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "name": "HIDDEN_DUE_TO_SECURITY_REASONS",
    "serverSideEncryptionConfiguration": {
      "kmsKeyId": "alias/sample-customer-managed-key"
    }
  },
  "responseElements": {
    "domain": {
      "arn": "arn:aws:voiceid:us-west-2:111122223333:domain/ExampleOsAjzg9xoByUatN",
      "createdAt": "Aug 17, 2021, 1:55:40 AM",
      "description": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "domainId": "UcUuCPFOsAjzg9xoByUatN",
      "domainStatus": "ACTIVE",
      "name": "HIDDEN_DUE_TO_SECURITY_REASONS",
      "serverSideEncryptionConfiguration": {
        "kmsKeyId": "arn:aws:kms:us-west-2:111122223333:key/1111111-7741-44b1-
a5fe-7c6208589bf3"
      },
      "updatedAt": "Aug 17, 2021, 1:55:40 AM"
    }
  },
  "requestID": "11111111-b358-4637-906e-67437274fe4e",
  "eventID": "1111111-a4d1-445e-ab62-8626af3c458d",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "eventCategory": "Management",
  "recipientAccountId": "111122223333"
}
```

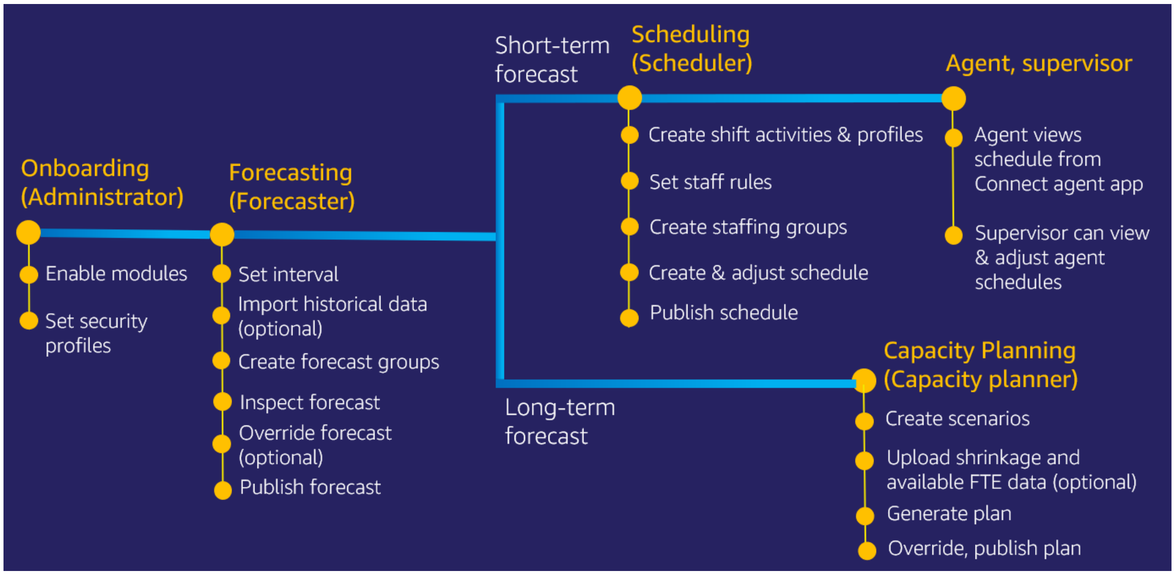
Forecasting, capacity planning, and scheduling (Preview)

To run a contact center, you need the right number of agents working at the right times to achieve your operational goals. It's critical to not overspend or overrun your workforce.

Amazon Connect provides a set of services powered by machine learning that help you optimize your contact center by offering the following:

- Forecasting (p. 1031). Analyze and predict contact volume based on historical data. What will future demand—the contact volume and handle time—look like? Amazon Connect forecasting provides accurate and auto-generated forecasts that are automatically updated daily.
- Scheduling (p. 1051). Generate agent schedules for day-to-day workloads that are flexible, and meet business and compliance requirements. Offer agents flexible schedules and work-life balance. How many agents are needed in each shift? Which agent works in which slot?
- Capacity planning (p. 1042). Predict how many agents your contact center will require. Optimize plans by scenarios, service level goals, and metrics, such as shrinkage.

The following diagram shows a typical end-to-end optimization workflow by persona: Amazon Connect administrator, forecaster, scheduler, capacity planner, and agent.



Enable forecasting, capacity planning, and scheduling (Preview)

You enable forecasting, capacity planning, and scheduling at the Amazon Connect instance level.

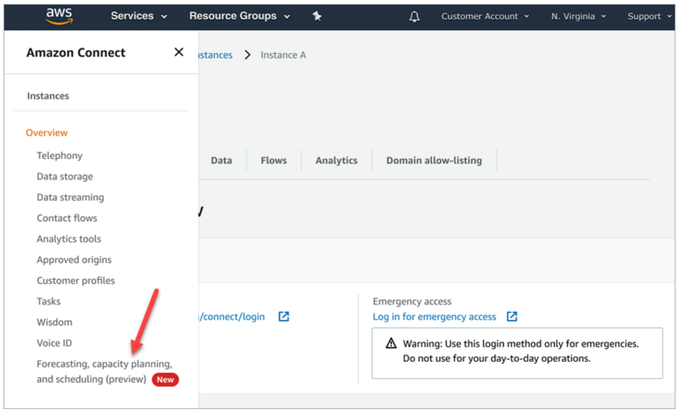
Requirements

The user must have the following permissions:

- `iam:CreateRole`
- `iam:CreatePolicy`
- `iam:AttachRolePolicy`
- `bayes-markov:*`

To enable forecasting, capacity planning, and scheduling

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.
3. In the navigation pane, choose **Forecasting, capacity planning, and scheduling**.



Warning: Use this login method only for emergencies. Do not use for your day-to-day operations.

4. On the **Forecasting, capacity planning, and scheduling** page, choose **Enable Forecasting, capacity planning, and scheduling**.

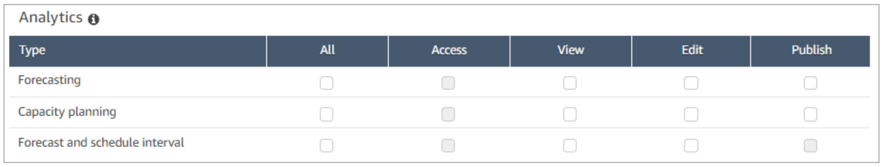
   Your users will have access to forecasting, capacity planning, and scheduling within 24 hours. After forecasting, capacity planning, and scheduling capabilities are enabled, continue setup as follows:

   a. Assign users the appropriate security profile permissions to access the features. For instructions, see Required permissions (p. 1030).

   b. Set the forecast and scheduling interval (p. 1032). This is a one-time activity typically done by forecasters. After it's set, it cannot be undone.

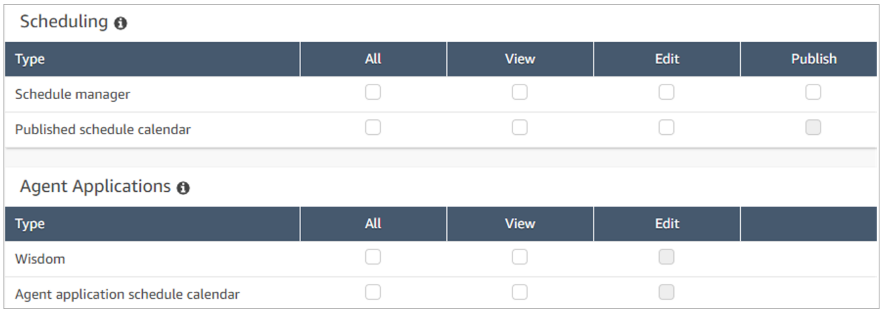
Security profile permissions for forecasting, capacity planning, and scheduling (Preview)

The following images show you the security profile permissions that apply to forecasting, capacity planning, and scheduling.



Analytics

Type	All	Access	View	Edit	Publish
Forecasting	☐	☐	☐	☐	☐
Capacity planning	☐	☐	☐	☐	☐
Forecast and schedule interval	☐	☐	☐	☐	☐



Scheduling

Type	All	View	Edit	Publish
Schedule manager	☐	☐	☐	☐
Published schedule calendar	☐	☐	☐	☐

Agent Applications

Type	All	View	Edit	
Wisdom	☐	☐	☐	
Agent application schedule calendar	☐	☐	☐	

Assign the following permissions as needed to use Amazon Connect forecasting, capacity planning, and scheduling features:

- **Forecasting**: This permission allows you to view and edit in forecasting pages. For example, you can create, view, publish, and delete forecast groups and forecasts, import historical data from external applications, and more.
- **Capacity planning**: This permission allows you to view and edit in capacity planning pages, including scenario and capacity plans. It also allows users to import future estimated shrinkage and available FTEs.
- **Schedule manager**: This permission allows you to view and edit generated schedules from the schedule manager.
- **Team schedule calendar**: After a schedule is published, this permission enables you to view or edit the published schedule. You can see the schedule calendar, but agents cannot.
- **Individual schedule calendar**: This permission allows agents to view their schedule in their agent application.

For information about how add more permissions to an existing security profile, see Update security profiles (p. 797).

By default, the **Admin** security profile already has permissions to perform all forecasting, capacity planning, and scheduling activities.

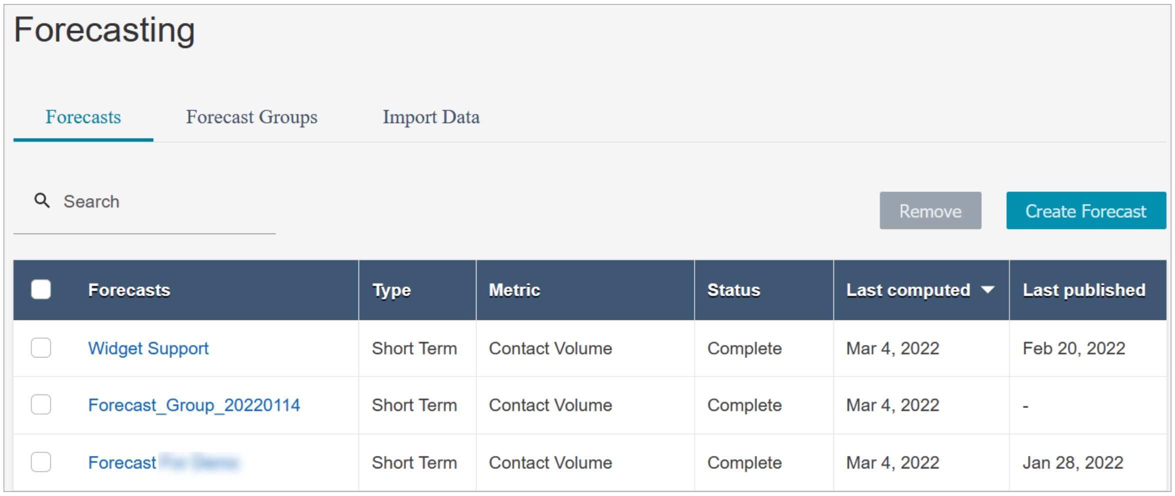
Forecasting in Amazon Connect (Preview)

Forecasting is the starting point for any scheduling and capacity planning activities. Before you can generate a schedule or capacity plan, you must create a corresponding forecast.

A *forecast* attempts to predict future contact volume and handle time. We use historical metrics to create the forecast.

Short term forecasts are automatically updated every day. When you come into work, you can review the forecast that was updated overnight with the most current data. You can publish the forecast to make it available to schedulers whenever you want. The **Forecasting** page displays when a forecast was last updated and published. Use short term forecasts for scheduling.

Long term forecasts are automatically updated every week, based on the day you created the forecast. For example, if you created the forecast on a Monday, it is updated every Monday. Use long term forecasts for hiring.



☐	Forecasts	Type	Metric	Status	Last computed ▼	Last published
☐	Widget Support	Short Term	Contact Volume	Complete	Mar 4, 2022	Feb 20, 2022
☐	Forecast_Group_20220114	Short Term	Contact Volume	Complete	Mar 4, 2022	-
☐	Forecast [redacted]	Short Term	Contact Volume	Complete	Mar 4, 2022	Jan 28, 2022

> **Important**
> Only the most current forecast is available. Because the forecast is updated every day, if you want to keep the current day's forecast, you must download it before Amazon Connect overwrites it.

Getting started with forecasting

Following is the order of steps for creating a forecast and sharing it with others.

1. Set the forecast and scheduling interval (p. 1032): This is a one-time activity typically set up by forecasters. It cannot be undone.
2. Create forecast groups (p. 1033)
3. Import historical data (p. 1035)
4. Create forecasts (p. 1037)
5. Inspect a forecast (p. 1039)
6. Publish a forecast (p. 1041)

There are other things you can do with a forecast, such as download to a .csv file for offline analysis (p. 1039) or override (p. 1040) it, but these steps will get you started.

Set the forecast and schedule interval (Preview)

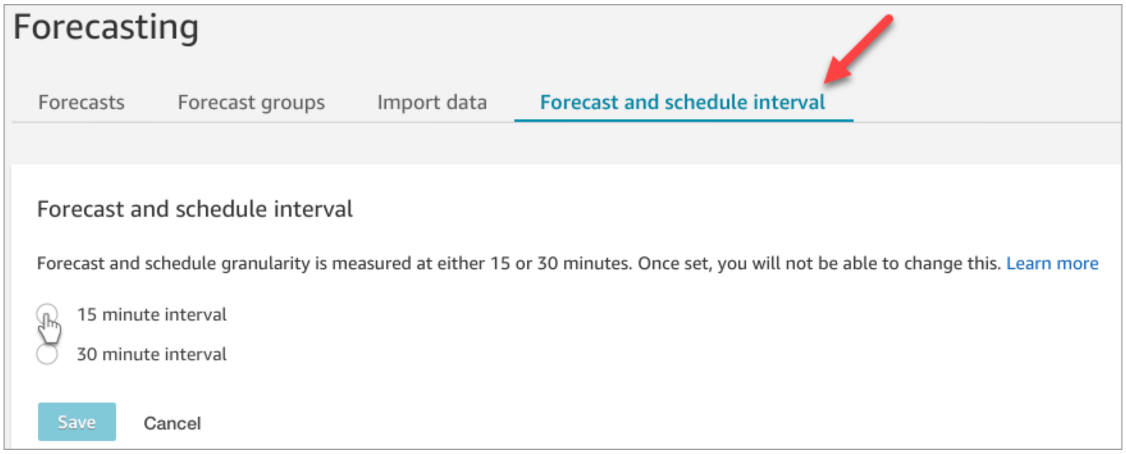
You can set the granularity for your short-term forecasts and your schedules.

Important things to know

- You must have security profile permissions for **Analytics**, **Forecast and schedule interval - Edit**. For more information, see Required permissions (p. 1030).
- You must specify an interval for short-term forecasting and scheduling.
- Amazon Connect supports 15- or 30-minute intervals. For example, if you select 30 minutes as the interval, your short-term forecasts are generated for 30-minute intervals (that is, 20 contacts between 9:00 AM-9:30 AM), and your schedules are computed for 30 minute intervals.
- You must set up a forecast and a schedule interval before you can generate forecasts or create forecast groups.
- After you set the forecast and schedule interval, you cannot change it.

To set the forecast and schedule interval

1. Log in to the Amazon Connect console.
2. On the Amazon Connect navigation menu, select **Analytics**, **Forecasting**.
3. Choose the **Forecast and schedule interval** tab. You'll see this tab only if you have the appropriate security profile permissions.



Forecast and schedule interval

Forecast and schedule granularity is measured at either 15 or 30 minutes. Once set, you will not be able to change this. Learn more

○ 15 minute interval
○ 30 minute interval

4. Choose one of the following options:

   - **15 minute interval** – Generates short-term forecasts in 15-minute intervals. For example, 20 contacts between 9:00 AM to 9:15 AM, and 30 contacts between 9:15 AM to 9:30 AM.
   - **30 minute interval** – Generates short-term forecasts in 30-minute intervals. For example, 20 contacts between 9:00 AM to 9:30 AM, 30 contacts between 9:30 AM to 10:00 AM.

Create forecast groups (Preview)

Forecast groups are a way for you to combine different queues into one forecast. This enables you to create a forecast from aggregated data from multiple queues, instead of from just one queue.

Important things to know

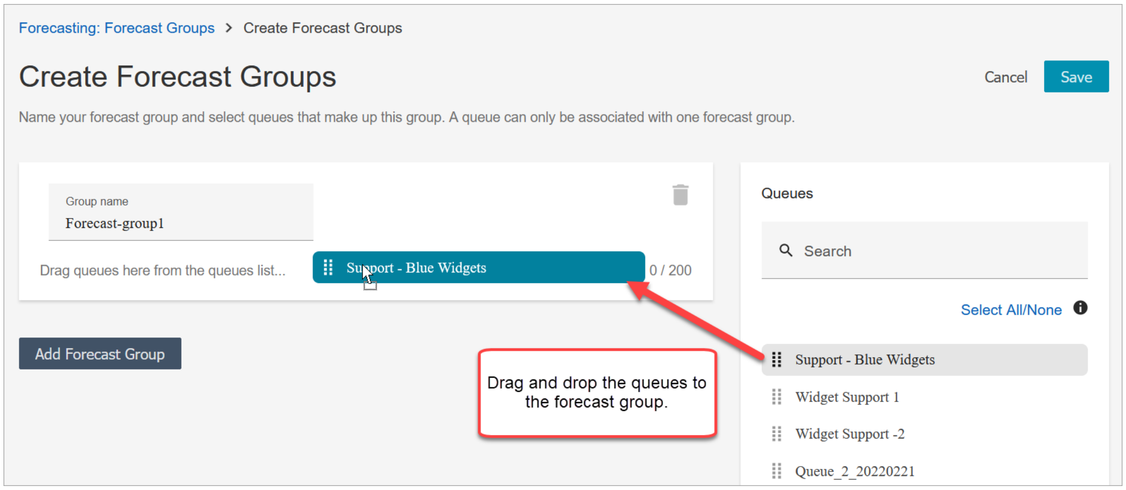
- Forecast groups are associated with a staffing group for scheduling purposes. Therefore, we recommend you group queues that share the same pool of staff (agents) under the same forecast group. It enables you to generate a more accurate forecast.
- Each queue can belong to only one forecast group. This prevents duplicates in the forecast.
- You must create at least one forecast group before you can generate any forecast.
- We strongly recommend that you create all forecast groups before creating any forecast.

  Amazon Connect uses historical data for queues included in all forecast groups to train your forecasting model. By creating forecasts after all forecast groups are created, you ensure historical data of all relevant queues are included in the training.
- If a queue is associated with a forecast group and is later disabled, it does not change the forecast group. The queue will still be included by the forecast group and the historical data associated with it will be included in the forecast. Over time, because no contact reaches the disabled queue, it stops impacting the forecast.

How to create forecast groups

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Forecasting - Edit**.

   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, select **Analytics**, **Forecasting**.
3. Select the **Forecast groups** tab, and then choose **Create forecast group**.
4. On the **Create Forecast Groups** page, under **Queues**, you'll see a list of queues that are not yet associated with a forecast group are listed. If no queues are listed, it means they are all associated with a forecast group already.
5. Drag and drop one or more queues to the forecast group. You can press and hold CTRL (COMMAND for macOS users) or SHIFT to select multiple queues at a time.



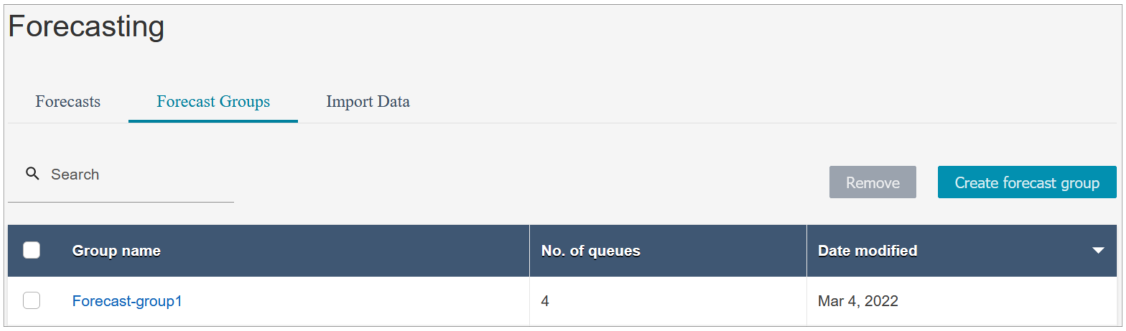
Create Forecast Groups

Name your forecast group and select queues that make up this group. A queue can only be associated with one forecast group.

Group name: Forecast-group1

Drag and drop the queues to the forecast group.

6. Choose **Save**. The new forecasting group appears, along with the number of queues in the group and the date it was last changed.



□	Group name	No. of queues	Date modified
□	Forecast-group1	4	Mar 4, 2022

7. After creating a forecast group, you can add or remove queues. However, doing so might initiate an immediate change in associated forecasts. It will also impact downstream capacity plans and schedules that are created based on the forecast group.

Next steps

Now you're ready to create a forecast. For instructions, see Create forecasts (p. 1037).

Import historical data for forecasting (Preview)

Amazon Connect requires sufficient historical data to learn the contact pattern and make good forecasts. By default, it uses historical contact data in Amazon Connect for forecasting. You can import historical data from external applications for Amazon Connect to use for forecasting. When you import data, Amazon Connect uses both its data and the imported data for forecasting. However, *the imported data takes precedence over the Amazon Connect data*.

When to import data

We recommend importing historical data from external applications in the following use cases:

- **Insufficient historical data in Amazon Connect**. If you have less than one year of historical data in Amazon Connect, we strongly recommend that you extract historical data from your legacy system and upload the data to Amazon Connect. For example, if you have nine months of historical in Amazon Connect (for example, from April to December 2021, we recommend importing three additional months of data (from January to March 2022).

  If you have less than six months of recent historical data in Amazon Connect, the forecast fails. You must import additional historical data to unblock forecasting. For more information, see Data requirements for forecasting (p. 1037).
- **Incorrect historical data in Amazon Connect**. If the historical contact pattern is incorrect (for example, the contact volume is abnormally low on the day of a wide-spread power outage in the contact center), you can import data that is more representative and correct for the anomaly.

If you have more than one year of historical data in Amazon Connect, you can choose to skip data import and start creating forecasts (p. 1037).

Important things to know

- The data file must be a .csv file and it must be in the required format. If the file format and data don't meet the requirements, the upload does not work. We recommend downloading and using the template provided through the user interface (see step 4 in How to import historical data (p. 1036)) to help you prepare the historical data.

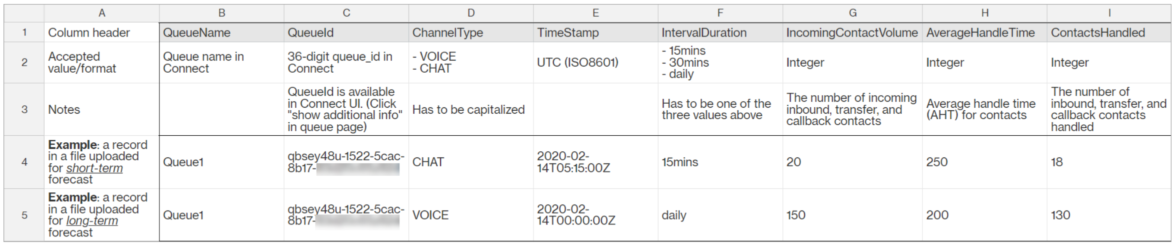
  Following are the requirements for imported data:
  - `QueueName`: Enter the Amazon Connect queue name.
  - `QueueId`: Enter the Amazon Connect queue ID. To find the queue ID in the Amazon Connect console, on the left navigation, go to **Routing**, **Queues**, choose the queue, select **Show additional queue information**. The queue ID is the last number after `/queue/`.
  - `ChannelType`: Enter `CHAT` or `VOICE`.
  - `TimeStamp`: Enter the timestamp in UTC (ISO8601) format.
  - `IntervalDuration`: Enter `15mins` or `30mins` for short-term forecast, depending on your forecast and schedule interval. Enter `daily` for long-term forecast.
  - `IncomingContactVolume`: Enter the number of inbound, transfer, and callback contacts as an integer.
  - `AverageHandleTime`: Enter the amount of average handle time (in seconds) as an integer.
  - `ContactsHandled`: Enter the number of inbound, transfer, and callback contacts handled as an integer.
- You can import multiple files. You do not have to consolidate all data in one big file. You can divide data by year, queue, interval duration types, and more, per your preference.

  If duplicate data are found across multiple files, the last uploaded records are used.

- You need to upload historical data for short-term and long-term forecast.
  - Data aggregated in 15- or 30-minute intervals is used for short-term forecasting.
  - Data aggregated at daily grain is used for long-term forecasting.

  For example, if you only upload data in 15- or 30-minute interval, you won't be able to generate long-term forecasts.
- The following special characters are allowed in the .csv file: -, _, ., (, and). Space is allowed.

The following table provides an example:

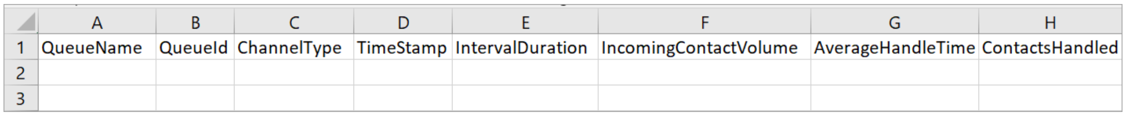


	A	B	C	D	E	F	G	H	I
1	Column header	QueueName	QueueId	ChannelType	TimeStamp	IntervalDuration	IncomingContactVolume	AverageHandleTime	ContactsHandled
2	Accepted value/format	Queue name in Connect	36-digit queue_id in Connect	- VOICE - CHAT	UTC (ISO8601)	- 15mins - 30mins - daily	Integer	Integer	Integer
3	Notes		QueueId is available in Connect UI. (Click "show additional info" in queue page)	Has to be capitalized		Has to be one of the three values above	The number of incoming inbound, transfer, and callback contacts	Average handle time (AHT) for contacts	The number of inbound, transfer, and callback contacts handled
4	**Example**: a record in a file uploaded for *short-term* forecast	Queue1	qbsey48u-1522-5cac-8b17-[redacted]	CHAT	2020-02-14T05:15:00Z	15mins	20	250	18
5	**Example**: a record in a file uploaded for *long-term* forecast	Queue1	qbsey48u-1522-5cac-8b17-[redacted]	VOICE	2020-02-14T00:00:00Z	daily	150	200	130

How to import historical data

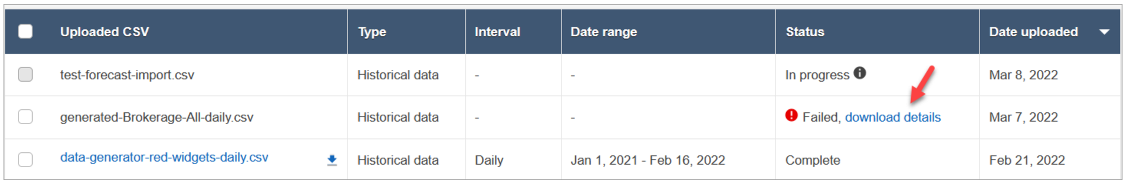
1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Forecasting - Edit**.

   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, select **Analytics**, **Forecasting**, and then choose the **Import Data** tab.
3. Choose **Upload data**.
4. On the **Upload historical data** dialog box, choose **download the CSV template for historical data**. You will receive a template that looks like the following image:



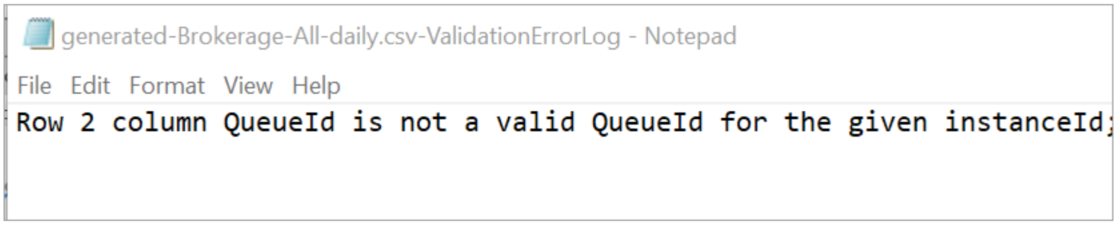
	A	B	C	D	E	F	G	H
1	QueueName	QueueId	ChannelType	TimeStamp	IntervalDuration	IncomingContactVolume	AverageHandleTime	ContactsHandled
2								
3								

5. Add historical data to the csv file, and then choose **Upload file** to upload it. Choose **Apply**.
6. If the upload fails, choose download details to view the error log message for more information.



□	Uploaded CSV	Type	Interval	Date range	Status	Date uploaded
□	test-forecast-import.csv	Historical data	-	-	In progress	Mar 8, 2022
□	generated-Brokerage-All-daily.csv	Historical data	-	-	Failed, download details	Mar 7, 2022
□	data-generator-red-widgets-daily.csv	Historical data	Daily	Jan 1, 2021 - Feb 16, 2022	Complete	Feb 21, 2022

Following is a sample message:



generated-Brokerage-All-daily.csv-ValidationErrorLog - Notepad
File Edit Format View Help

```
Row 2 column QueueId is not a valid QueueId for the given instanceId;
```

7. If the forecast was uploaded successfully, its **Status** = **Complete** and **Date uploaded** = today.

Data requirements for forecasting (Preview)

Amazon Connect generates forecasts using a machine-learning model tailored for contact center operations. It requires a sufficient amount of recent contact data to ensure the model is trained with relevant data and is able to generate high-quality forecasts.

Important things to know

- Amazon Connect generates forecasts using historical data for all queues included in all forecast groups.
- Amazon Connect performs a *data sufficiency* check (is there enough data) based on the aggregation of all queues included in all forecast groups.
  - At least 2,000 monthly contacts in the past six months are required to successfully generate a forecast.
    - Amazon Connect does not require 2,000 monthly contacts for every queue. All queues in all forecast groups must total to more than 2,000 monthly contacts.
  - While Amazon Connect can generate forecasts with six months of data, we recommend 12 months of recent contact data to ensure contact patterns (for example, seasonality) are properly captured.
- Amazon Connect performs a *data recency* check (is the data recent enough) based on the aggregation of all queues included in all forecast groups.
  - At least one data point in the past four weeks is required to successfully generate a forecast.

Do I have a sufficient amount of recent contact data?

- If you have been using Amazon Connect for more than 12 months, you do not need to provide any additional data.
- If you have been using Amazon Connect for more than six months but less than 12, we recommend providing additional historical data. You can import historical data from a source that is external to Amazon Connect. For instructions, see Import historical data (p. 1035).
- If you have been using Amazon Connect for less than six months, make sure it has at least six months of data. Otherwise, forecasting will fail.

For instructions about how to import more data, see Import historical data (p. 1035).

Create forecasts (Preview)

Forecasts are a projection of the workload in your contact center. Amazon Connect provides long-term and short-term forecasts for you to generate capacity plans and agent schedules. The forecasts include inbound, transfer, and callback contacts in both voice and chat channels.

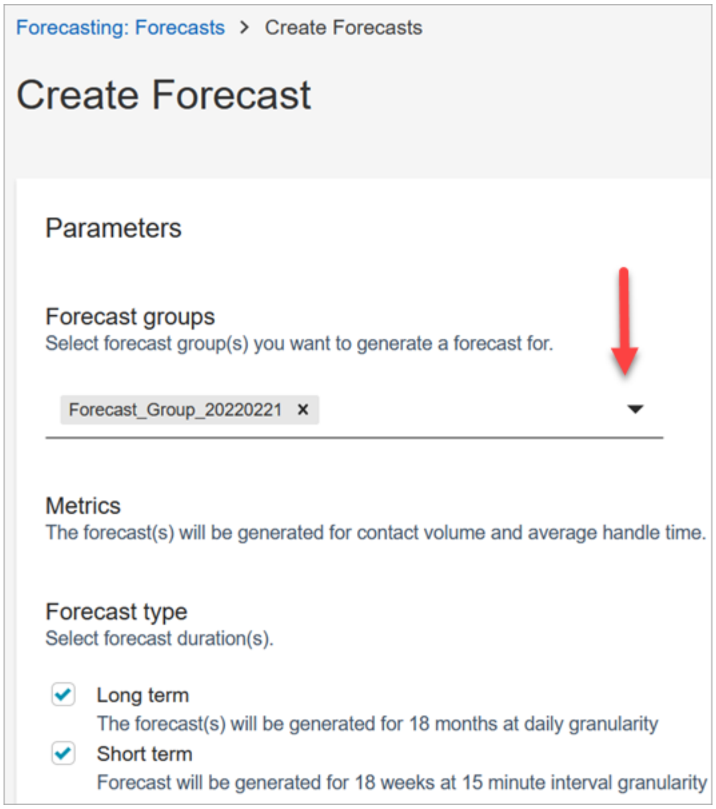
After creating a forecast, you will not need to generate it manually.

- Short-term forecasts are scheduled to run automatically every day.
- Long-term forecasts are scheduled to run automatically every week, starting from the day of onboarding. For example, if you enable Amazon Connect forecasting on Monday, long-term forecasts will be computed on the day of onboarding and automatically re-computed every Monday.
- Every forecast is computed using the most current contact data.
- The models for short-term and long-term forecasts are retrained on a weekly and monthly basis respectively to incorporate the latest contact pattern.
- You can delete forecasts. Downstream capacity plans and schedules created based on the forecasts will be impacted.

To create a forecast

1. Before creating a forecast, you must create at least one forecast group. If you haven't yet done that, see Create forecast groups (p. 1033). We strongly recommend creating all of your forecast groups before creating any forecast.
2. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Forecasting - Edit**.

   For more information, see Required permissions (p. 1030).
3. On the Amazon Connect navigation menu, select **Analytics**, **Forecasting**.
4. Select the **Forecast** tab, and then choose **Create Forecast**.
5. On the **Create Forecast** page, choose the forecast groups.



Forecasting: Forecasts > Create Forecasts

Create Forecast

Parameters

Forecast groups
Select forecast group(s) you want to generate a forecast for.

Forecast_Group_20220221 ×

Metrics
The forecast(s) will be generated for contact volume and average handle time.

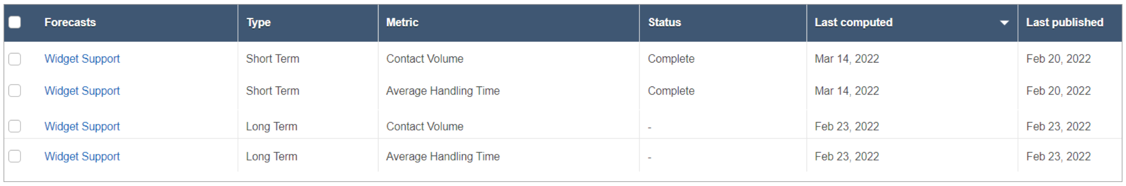
Forecast type
Select forecast duration(s).

☑ Long term
The forecast(s) will be generated for 18 months at daily granularity

☑ Short term
Forecast will be generated for 18 weeks at 15 minute interval granularity

6. Choose the forecast type. Amazon Connect creates a forecast for each type you select.
   - **Long term** forecasts are used for capacity planning. For example, how many agents you need to hire in the next few months, quarter, and year.
   - **Short term** forecasts are used for scheduling agents.
7. Choose **Save**. If the forecast group has already been included in a forecast, an error message is displayed.
8. If the forecast was created successfully, it's Status = **Scheduled**.

   The status is **Complete** when the computation finishes. You can use **Search** to find forecasts by forecast group name.
9. Amazon Connect creates a forecast for each forecast type, as shown in the following image:



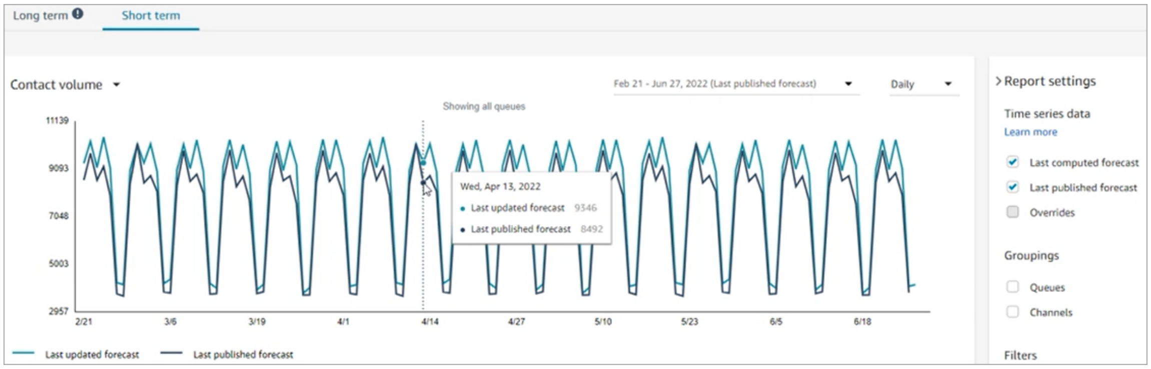
□ Forecasts	Type	Metric	Status	Last computed	Last published
□ Widget Support	Short Term	Contact Volume	Complete	Mar 14, 2022	Feb 20, 2022
□ Widget Support	Short Term	Average Handling Time	Complete	Mar 14, 2022	Feb 20, 2022
□ Widget Support	Long Term	Contact Volume	-	Feb 23, 2022	Feb 23, 2022
□ Widget Support	Long Term	Average Handling Time	-	Feb 23, 2022	Feb 23, 2022

Inspect a forecast (Preview)

You can inspect your forecasts before publishing them. You can do this in the online user interface, or download the forecasts (p. 1039) for offline analysis.

To help make it easier to inspect a forecast in the user interface, the forecast data is displayed in both a graph and a table. Use the controls on the report settings panel and calendar picker to adjust and filter the data for a more granular view. For example, you can:

- Use the calendar to change the horizon. You can zoom into specific dates.
- Choose 15 minute intervals if your date range is less than a week. This enables you to see the exact contact pattern of the day.
- Compare **Last computed forecast** and **Last published forecast** as shown in the following image.



Choose the **Override** setting to inspect the effect of any override you uploaded. The **Override** option is active only after an override has been uploaded. For more information, see Override a forecast (p. 1040).

- Filter by queues or channels to limit your forecast to one or more type.

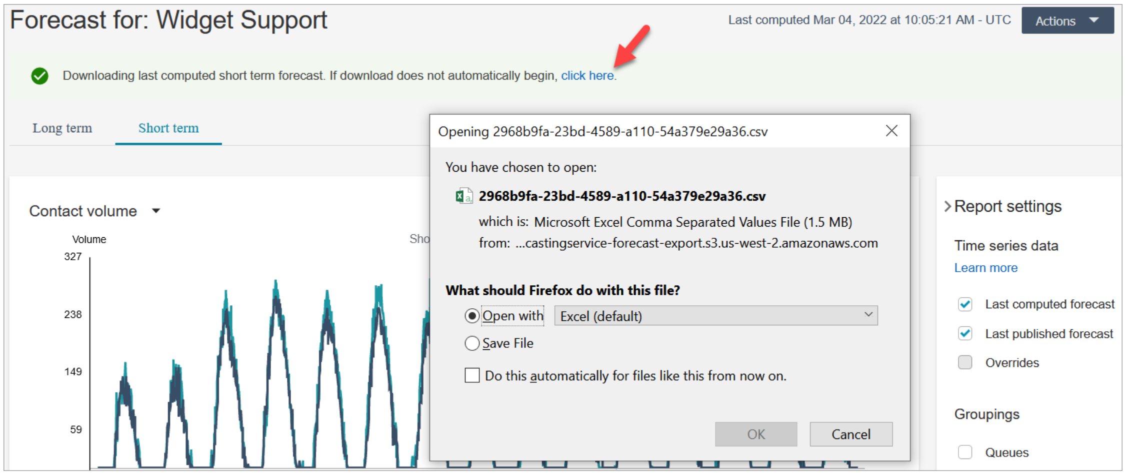
Download a forecast (Preview)

You can download a forecast so you can inspect it offline. A forecast is downloaded as a .csv file of the forecast data. It has the queue name, channel type, timestamp, incoming contact volume and average handle time data.

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Forecasting - Edit**.

   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, choose **Analytics**, **Forecasting**.
3. On the **Forecasts** tab, choose the forecast.
4. Choose **Actions**, and then download either the last computed forecast or the last published forecast.

5. We recommend clicking or tapping **click here** so that you can choose the name of the file download and where to save it. Otherwise, the file is saved to your **Downloads** folder and its name is a generated number.


Forecast for: Widget Support

Last computed Mar 04, 2022 at 10:05:21 AM - UTC

Downloading last computed short term forecast. If download does not automatically begin, click here.

Opening 2968b9fa-23bd-4589-a110-54a379e29a36.csv

You have chosen to open:

2968b9fa-23bd-4589-a110-54a379e29a36.csv

which is: Microsoft Excel Comma Separated Values File (1.5 MB)

from: ...castingservice-forecast-export.s3.us-west-2.amazonaws.com

What should Firefox do with this file?

● Open with Excel (default)

○ Save File

□ Do this automatically for files like this from now on.

Report settings

Time series data

☑ Last computed forecast

☑ Last published forecast

□ Overrides

Groupings

□ Queues

Override a forecast (Preview)

You can override the forecast at the queue channel level by uploading a .csv file. Override allows you to modify forecasts and make sure the forecasts reflect the contact pattern in special events (for example, a one-off marketing event that can increase volume by 10 percent in a given week).

You can also remove the override if the override is no longer applicable.

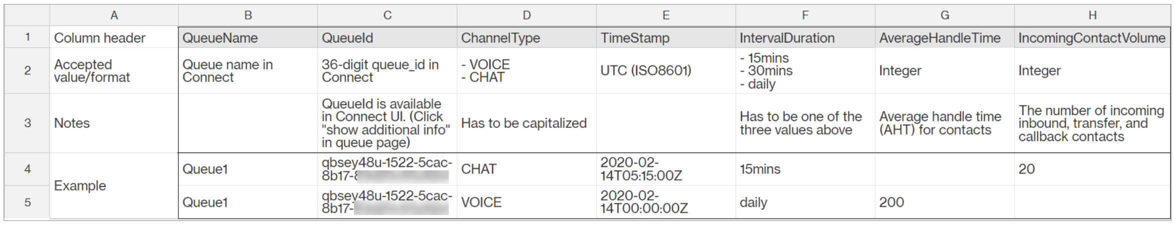
Important things to know

- To override a forecast, you need to prepare and upload a .csv file with your override data. Currently Amazon Connect does not support changing the values in forecasting user interface directly.
- The override data file be must a .csv file and it must be in the required format. If the file format and data don't meet the requirements, the upload does not work. We recommend downloading and using the template provided to help you prepare the historical data.

  Following are the requirements for imported data:
  - `QueueName`: Enter the Amazon Connect queue name.
  - `QueueId`: Enter the Amazon Connect queue ID. To find the queue ID in the Amazon Connect console, on the left navigation, go to **Routing**, **Queues**, choose the queue, select **Show additional queue information**. The queue ID is the last number after `/queue/`.
  - `ChannelType`: Enter `CHAT` or `VOICE`.
  - `TimeStamp`: Enter the timestamp in UTC (ISO8601) format.
  - `IntervalDuration`: Enter `15mins` or `30mins` for short-term forecast, depending on your forecast and schedule interval. Enter `daily` for long-term forecast.
  - `IncomingContactVolume`: Enter the number of inbound, transfer, and callback contacts as an integer.
  - `AverageHandleTime`: Enter the amount of average handle time (in seconds) as an integer.
- You can upload only one override file for a forecast group.
  - This means if you previously uploaded an override file (for example, with 120 lines of overrides), you must add new overrides to this override file (for example, add 50 new lines of overrides) and re-upload the file that now has 170 lines of overrides.

  - This also means you will need to include overrides for both short-term and long-term forecasts in one file.
- Both contact volume and Average Handle Time metrics are included in one override file. To override only one of them for a selected interval, leave the other metric blank.
- The following special characters are allowed in the .csv file: -, _, ., (, and). Space is allowed.

The following table provides an example:



	A	B	C	D	E	F	G	H
1	Column header	QueueName	QueueId	ChannelType	TimeStamp	IntervalDuration	AverageHandleTime	IncomingContactVolume
2	Accepted value/format	Queue name in Connect	36-digit queue_id in Connect	- VOICE - CHAT	UTC (ISO8601)	- 15mins - 30mins - daily	Integer	Integer
3	Notes		QueueId is available in Connect UI. (Click "show additional info" in queue page)	Has to be capitalized		Has to be one of the three values above	Average handle time (AHT) for contacts	The number of incoming inbound, transfer, and callback contacts
4	Example	Queue1	qbsey48u-1522-5cac-8b17-[redacted]	CHAT	2020-02-14T05:15:00Z	15mins		20
5		Queue1	qbsey48u-1522-5cac-8b17-[redacted]	VOICE	2020-02-14T00:00:00Z	daily	200	

How to override a forecast

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Forecasting - Edit**.

   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, select **Analytics**, **Forecasting**, and then choose the **Forecast** tab.
3. Choose the forecast.
4. Choose **Actions**, **Upload forecast override**.
5. Choose **Download the CSV template for override data**.

   > **Note**
   > Amazon Connect supports one, which would be the latest, override file per forecast group.
   >
   > - If you have never uploaded an override file, your template will contain headings but no data.
   > - If you have uploaded override file in the past, your template will be the previously uploaded file.

   You don't need values in all of the columns, but your csv file must include all column headings.

   If you don't want to override certain data, such as the **AverageHandleTime**, leave that column empty; it won't override the existing values. However, if you need to make changes to **AverageHandleTime** later on, you must download the last uploaded file, make your changes, and then upload the file. Amazon Connect only retains the last uploaded file.
6. Add override data, and then choose **Upload file** to upload it. Choose **Apply** to confirm forecast override.

Publish a forecast (Preview)

When you publish a forecast, you make it visible to other users, such as capacity planners and schedulers, so that they can use the forecasts for capacity planning and scheduling.

> **Important**
> Amazon Connect retains only the last published forecast. We strongly advise you to download the last published forecast before publishing a new one because the last forecast will be permanently replaced. For instructions, see Download last published forecast (p. 1042).

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Forecasting - View**.

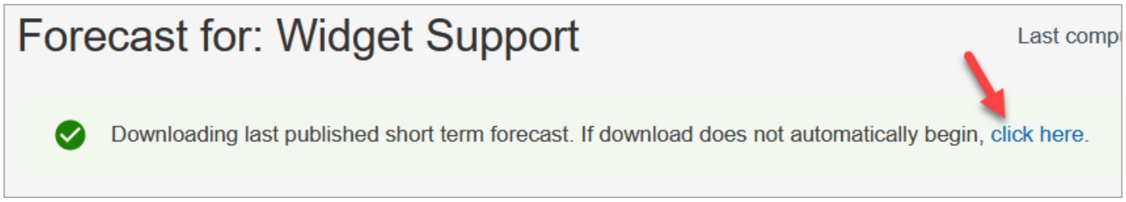
   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, select **Analytics**, **Forecasting**.
3. On the **Forecasts** tab, choose the forecast.
4. Choose **Actions**, **Publish forecast**.
5. Choose the forecasts.

   The status is **Complete** for successfully published forecasts. When publish fails, the status is **Publish failed**.

Download the last published forecast

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Forecasting - View**.

   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, select **Analytics**, **Forecasting**.
3. On the **Forecasts** tab, choose the forecast.
4. Choose **Actions**, **Download last published forecast**.
5. We recommend choosing **click here** so you can specify the name of the downloaded file and the location. Otherwise, the file is saved to your **Downloads** folder and its name is a generated number.



Forecast for: Widget Support

Last comp

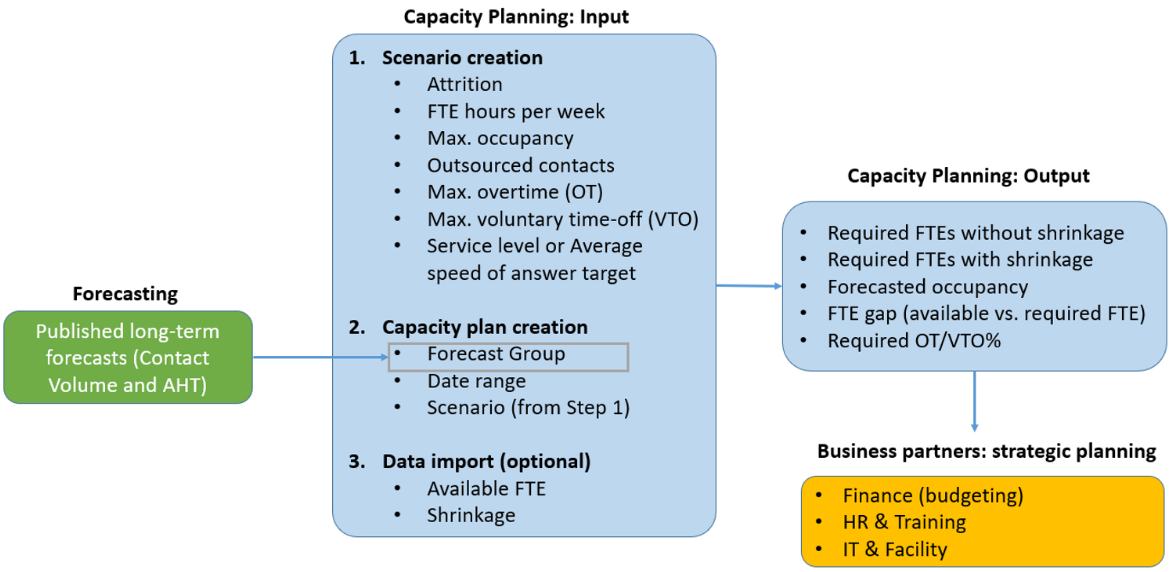
Downloading last published short term forecast. If download does not automatically begin, click here.

Capacity planning in Amazon Connect (Preview)

A capacity plan helps you estimate the long-term FTE (full-time equivalent) requirements for your contact center, up to 18 months. It specifies how many FTE agents are required to meet the service level target for a certain period of time.

After you generate long term FTE estimations, you can share this information with other stakeholders, such as Human Resources, Finance, and the Training Department, to help facilitate the hiring and training of staff. When a business launches a new product or extends into a new Region, staff hiring is needed to meet the customer service demand.

The capacity planning feature uses published long-term forecasts as input, along with scenario information that you provide. It then creates a long-term capacity plan that you can share with stakeholders. The following diagram illustrates this integration among published long-term forecasts, capacity planning, and capacity planning output.


Capacity Planning: Input
1. Scenario creation
Attrition
FTE hours per week
Max. occupancy
Outsourced contacts
Max. overtime (OT)
Max. voluntary time-off (VTO)
Service level or Average speed of answer target
2. Capacity plan creation
Forecast Group
Date range
Scenario (from Step 1)
3. Data import (optional)
Available FTE
Shrinkage
Forecasting
Published long-term forecasts (Contact Volume and AHT)
Capacity Planning: Output
Required FTEs without shrinkage
Required FTEs with shrinkage
Forecasted occupancy
FTE gap (available vs. required FTE)
Required OT/VTO%
Business partners: strategic planning
Finance (budgeting)
HR & Training
IT & Facility

Getting started

Following is the order of steps for creating a capacity plan and sharing it with others.

1. Create capacity planning scenarios (p. 1043)
2. ??? (p. 1045): This is an optional step but it can improve the accuracy of your capacity plan.
3. Create capacity plans using forecasts and scenarios (p. 1046)
4. Create capacity planning scenarios (p. 1047)
5. Review (p. 1047), override (p. 1048), re-run (p. 1049), or download (p. 1050) a capacity plan.
6. Publish a capacity plan (p. 1051)

Create capacity planning scenarios (Preview)

A scenario has two parts:

- Scenario inputs: The maximum occupancy, daily attrition, FTE hours per week. For example, you might enter data that represent your best case scenarios (everyone is at work) or worst case scenarios (a large number of people are out sick during winter months).
- Optimization inputs: The service level or average speed of answer (ASA). For example, 85% of calls are answered within 30 seconds of entering the queue.

You can then use this scenario to generate a capacity plan that represents how many people you need to hire accordingly to meet your business goals. The output includes the required FTE employees with and without shrinkage, forecasted occupancy rate, the gap between available required FTEs, and maximum overtime (OT) and voluntary time-off (VTO) rate allowed.

To create a capacity planning scenario

1. Before you can create a capacity plan, you must create and publish a long-term forecast. Amazon Connect uses the published long-term forecast as the input for creating the capacity plan. If you haven't yet created a forecast, see Getting started with forecasting (p. 1032).
2. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Capacity planning - Edit**.

For more information, see Required permissions (p. 1030).

3. On the Amazon Connect navigation menu, choose **Analytics**, **Capacity planning**.
4. On the **Planning Scenarios** tab, choose **Create a Scenario**.
5. On the **Create scenario** page, enter a name and description.
6. In the **Scenario inputs** section, enter the following information:

   a. **Max Occupancy (optional)**: The percentage of time agents will spend handling contact volume when they log in.

      i. **Daily attrition**: The percentage of staff leaving your contact center. The percentage of staff leaving your contact center.

         For example, if the annual attrition is 50%, the daily attrition would be 50%/250 working days per year = 0.2%.

      ii. **Full-time equivalent (FTE) hours per week**: How many hours each FTE employee will work per week.

   b. **Outsourced contacts (optional)**: You can outsource a percentage to a third-party.

   c. **Max overtime (OT) allowed (optional)**: Specify the maximum percent of overtime to plan for peaks. As a planner, you don't want to burn out your workforce.

      For example, you specify 40 as FTE hours per week, with 10 percent maximum overtime. The total work week would be up to 44 hours.

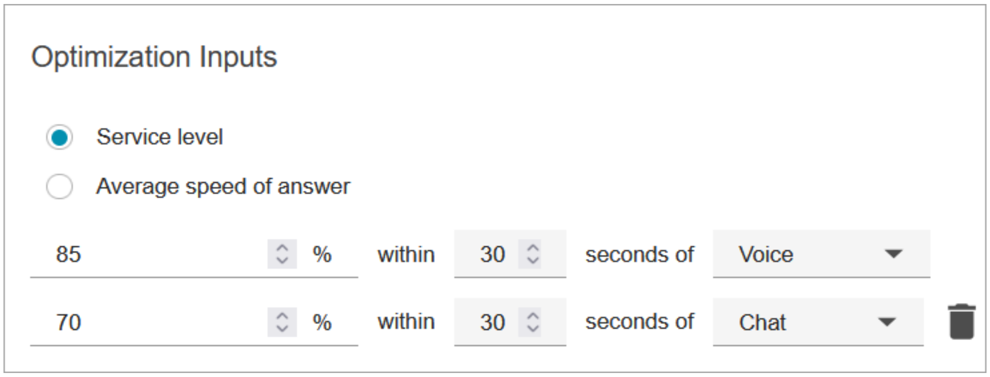
   d. **Max voluntary time off (VTO) allowed (optional)**: Specify the maximum percent of time off to plan for troughs, when there is a lull in contacts and you can save in costs. Be sure not to give too much time off in case traffic increases again.

      For example, you specify 40 as FTE hours per week, with 10 percent maximum time off. The total work week would be at least 36 hours.

7. In the **Optimization inputs** section, enter the operational goals for your organization:

   a. **Service level**: The percentage of contacts answered within a defined target time threshold.

      The following image shows service level targets where 80 percent of voice contacts and 70 percent of chat contacts will be answered within 30 seconds.



Optimization Inputs

● Service level

○ Average speed of answer

85 % within 30 seconds of Voice

70 % within 30 seconds of Chat

   b. **Average speed of answer** (ASA): The average amount of time it takes for contacts to be answered in a call center during a specific time period.

   c. You can create one goal per channel. Choose **Add another goal** to add another goal.

Import estimated future shrinkage and available full-time employees (Preview)

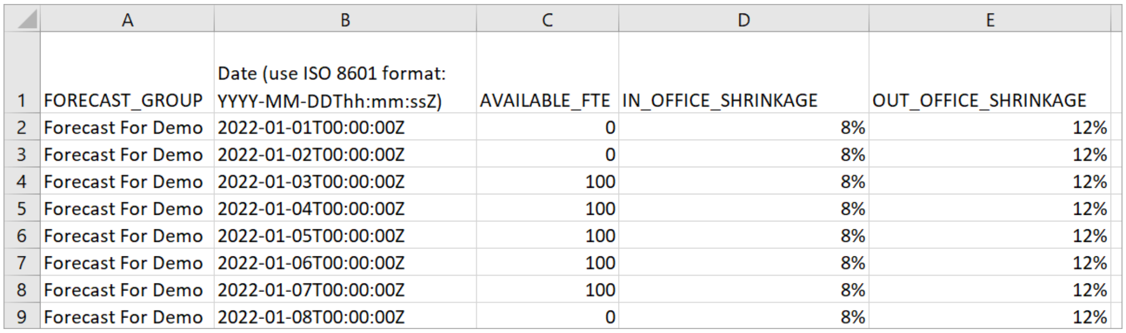
You can increase capacity planning accuracy by providing estimated future data (Available FTE and Shrinkage) for your existing forecast groups. Providing Available FTE and shrinkage data is optional. Amazon Connect can generate a capacity plan without it, but providing it improves the accuracy of your plan.

How to import data

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Capacity planning - Edit**.

   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, select **Analytics**, **Capacity Planning**.
3. On the **Import Data** tab, choose **Upload data**.

   The .csv file you upload must have the following headings:



	A	B	C	D	E
1	FORECAST_GROUP	Date (use ISO 8601 format: YYYY-MM-DDThh:mm:ssZ)	AVAILABLE_FTE	IN_OFFICE_SHRINKAGE	OUT_OFFICE_SHRINKAGE
2	Forecast For Demo	2022-01-01T00:00:00Z	0	8%	12%
3	Forecast For Demo	2022-01-02T00:00:00Z	0	8%	12%
4	Forecast For Demo	2022-01-03T00:00:00Z	100	8%	12%
5	Forecast For Demo	2022-01-04T00:00:00Z	100	8%	12%
6	Forecast For Demo	2022-01-05T00:00:00Z	100	8%	12%
7	Forecast For Demo	2022-01-06T00:00:00Z	100	8%	12%
8	Forecast For Demo	2022-01-07T00:00:00Z	100	8%	12%
9	Forecast For Demo	2022-01-08T00:00:00Z	0	8%	12%

4. Update values in this template, and then choose `Upload CSV` to upload it. Choose `Upload`.

It usually between 2 - 5 minutes for the .csv file to upload. If the upload fails, check if the `FORECAST_GROUP` name in the .csv file matches the name of the forecast group that you created.

Important things to know about your .csv file

- FORECAST_GROUP: Enter the EXACT name of the forecast group you created. You can add multiple forecast groups in this csv file.
- Date: Each row is one day. In the previous image, row 2 is January 1, row 3 is January 2, row 4 is January 3, and so on. Use ISO 8601 format ending with Z.
- AVAILABLE FTE: How many agents are available for working that day. In the previous image, 0 indicates no full-time agents are available on January 1 for the forecast group named **Forecast For Demo**. On January 3, 100 agents are available.
- IN_OFFICE_SHRINKAGE: Percentage of agents in the office but not in production mode. For example, they might be in training or in meetings.
- OUT_OFFICE_SHRINKAGE: Percentage of agents absent from work (for example, no show or personal time off).

> **Note**
> The latest uploaded .csv file always overrides the previous one you updated. Make sure errors aren't introduced to the uploaded .csv file accidentally. For example, don't press **Enter** and add

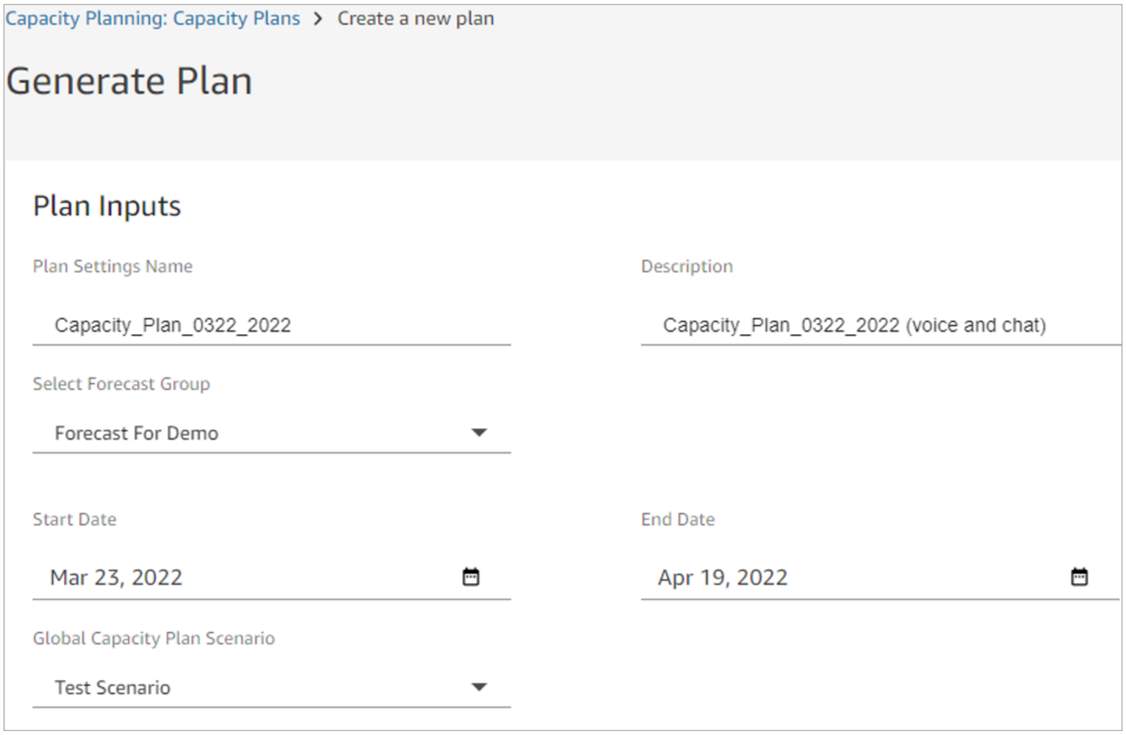
new rows to the end of the file. Otherwise, the data won't validate and an error message is displayed.

Create capacity plans using forecasts and scenarios (Preview)

Before you can create a capacity plan, you must create a planning scenario and publish a long-term forecast. Amazon Connect uses the forecasts and planning scenarios as inputs for creating the capacity plan. If you haven't yet created a forecast and planning scenario, see Getting started with forecasting (p. 1032) and Create capacity planning scenarios (Preview) (p. 1043).

How to create a capacity plan

1. Go to the **Capacity Plans** tab, and choose **Generate Plan**.
2. Provide the plan name, description, forecast group (which has published long-term forecasts), start/end date, and plan scenario. See the following image for an example:



Capacity Planning: Capacity Plans > Create a new plan

Generate Plan

Plan Inputs

Plan Settings Name: Capacity_Plan_0322_2022

Description: Capacity_Plan_0322_2022 (voice and chat)

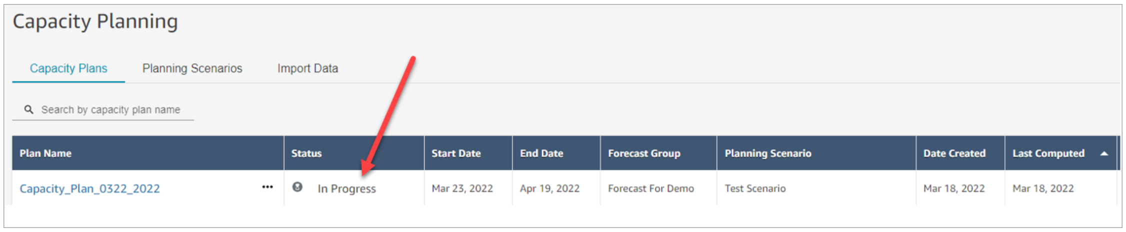
Select Forecast Group: Forecast For Demo

Start Date: Mar 23, 2022

End Date: Apr 19, 2022

Global Capacity Plan Scenario: Test Scenario

3. Choose **Generate Capacity Plan**.
4. To quickly identify the plan that is in processing, choose **Last Computed** to sort the table list. In the following example, the status of the plan is **In Progress**.



Capacity Planning

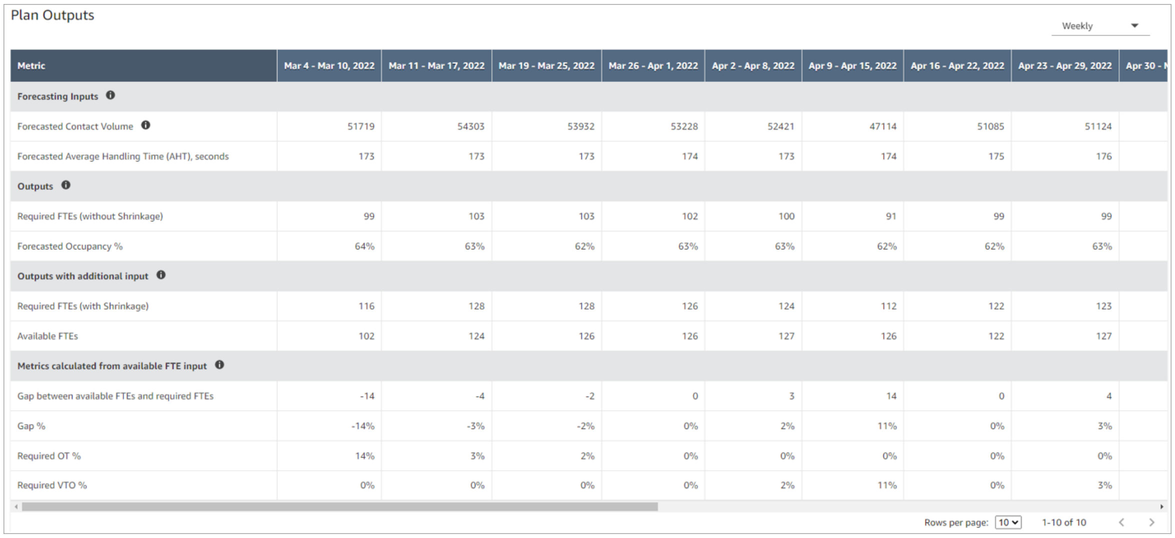
Plan Name	Status	Start Date	End Date	Forecast Group	Planning Scenario	Date Created	Last Computed
Capacity_Plan_0322_2022	In Progress	Mar 23, 2022	Apr 19, 2022	Forecast For Demo	Test Scenario	Mar 18, 2022	Mar 18, 2022

It usually takes between 5-10 minutes for the plan to be generated. If the plan generation fails, try publishing the selected long-term forecasts, and then generating the capacity plan again.

Review capacity plan output (Preview)

To review capacity plan output, choose the hyperlink for the plan you generated. The first half of the page summarizes the input you used in scenario and capacity plan generation.

The plan output shows a week-by-week or month-by-month calculation. To switch from weekly to monthly view, select **Monthly** from the dropdown, as shown in the following image.



Plan Outputs

Weekly

Metric	Mar 4 - Mar 10, 2022	Mar 11 - Mar 17, 2022	Mar 19 - Mar 25, 2022	Mar 26 - Apr 1, 2022	Apr 2 - Apr 8, 2022	Apr 9 - Apr 15, 2022	Apr 16 - Apr 22, 2022	Apr 23 - Apr 29, 2022	Apr 30 - M
Forecasting Inputs									
Forecasted Contact Volume	51719	54303	53932	53228	52421	47114	51085	51124	
Forecasted Average Handling Time (AHT), seconds	173	173	173	174	173	174	175	176	
Outputs									
Required FTEs (without Shrinkage)	99	103	103	102	100	91	99	99	
Forecasted Occupancy %	64%	63%	62%	63%	63%	62%	62%	63%	
Outputs with additional input									
Required FTEs (with Shrinkage)	116	128	128	126	124	112	122	123	
Available FTEs	102	124	126	126	127	126	122	127	
Metrics calculated from available FTE input									
Gap between available FTEs and required FTEs	-14	-4	-2	0	3	14	0	4	
Gap %	-14%	-3%	-2%	0%	2%	11%	0%	3%	
Required OT %	14%	3%	2%	0%	0%	0%	0%	0%	
Required VTO %	0%	0%	0%	0%	2%	11%	0%	3%	

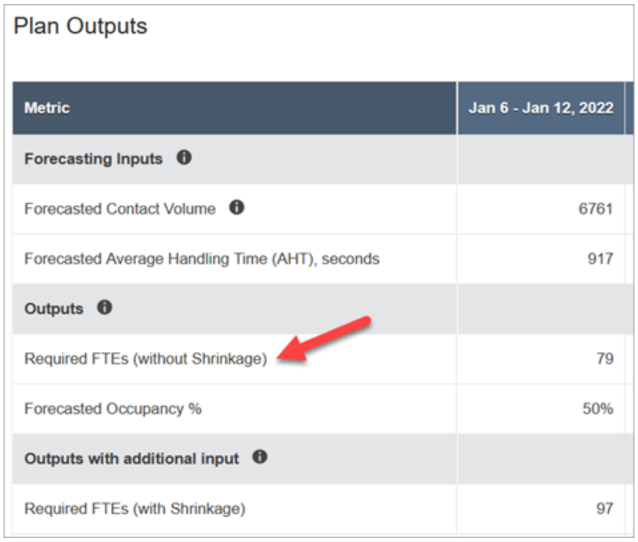
Following is a description of the metrics in the plan output:

- **Forecasting Inputs**
  - **Forecasted Contact Volume**: This metric is a sum of both voice and chat volume for the selected forecast group.
  - **Forecasted Average Handling Time (AHT), seconds**: This metric shows the aggregated AHT for the selected forecast group.
  - The forecasted contact volume and AHT in the plan output table reflects only the values from the selected forecast group. After there are newly published forecasts, consider re-running the capacity plan to reflect the latest published contact volume and AHT.
- **Outputs**
  - **Required FTEs (without Shrinkage)**: How many full-time equivalent agents need to be hired to meet the defined business goals (such as service level target), without considering shrinkage.
  - **Forecasted Occupancy %**: How much occupancy is for the agents.
- **Outputs with additional input**
  - **Required FTEs (with Shrinkage)**: How many full-time equivalent agents needed to be hired to meet the defined business goals (such as service level target), with considering shrinkage.
  - **Available FTEs**: How many agents are available for working that day. It can be uploaded in the **Import data** section.
- **Metrics calculated from available FTE input**
  - **Gap between available FTEs and required FTEs**: The difference between available FTEs and required FTEs.
  - **Gap %**: The percentage of the gap.
  - **Required OT %**: if there is a supply deficit (required FTEs higher than available FTEs), required OT% indicates how much overtime would be needed to cover the deficit.

- **Required OT %**: If there is a supply surplus (the number of required FTEs is lower than the available FTEs), required VTO % indicates how much voluntary time off could be used to lower the amount of agent idle time and thus lower costs.

Override a capacity plan (Preview)

You can upload a .csv file that overrides the **Required FTEs (without Shrinkage)** data in the **Plan outputs** section of a capacity plan. This section is shown in the following image.



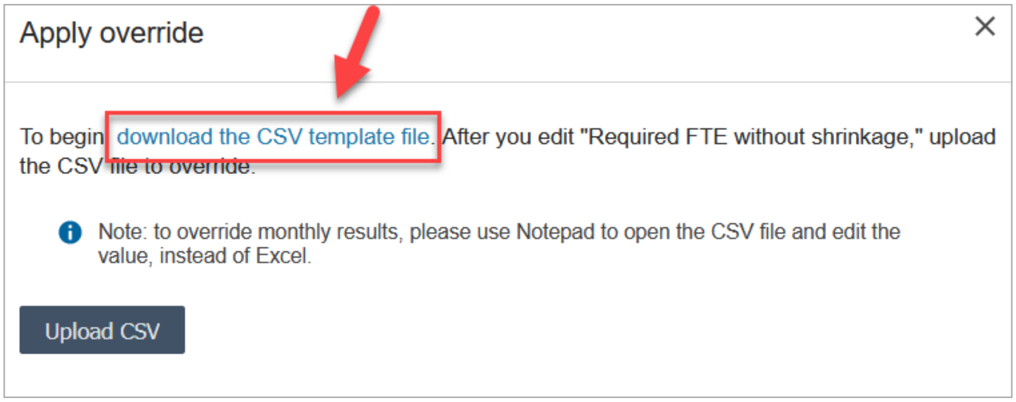
Plan Outputs

Metric	Jan 6 - Jan 12, 2022
Forecasting Inputs	
Forecasted Contact Volume	6761
Forecasted Average Handling Time (AHT), seconds	917
Outputs	
Required FTEs (without Shrinkage)	79
Forecasted Occupancy %	50%
Outputs with additional input	
Required FTEs (with Shrinkage)	97

You might want to do this, for example, to give your team of agents a buffer.

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Capacity planning - Edit**.

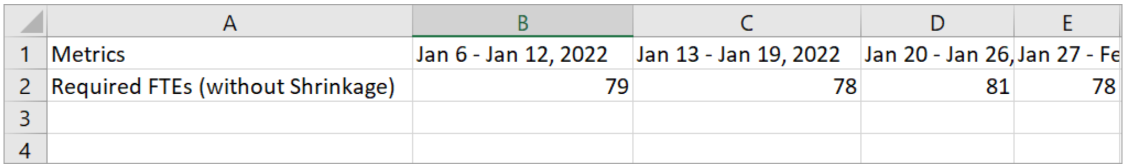
   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling (Preview) (p. 1030).
2. On the Amazon Connect navigation menu, select **Analytics**, **Capacity Planning**.
3. On the **Capacity Plans** tab, choose the plan.
4. On the detailed page for the capacity plan, choose **Actions**, **Upload plan override**, and then choose **download the CSV template file**.



To begin download the CSV template file. After you edit "Required FTE without shrinkage," upload the CSV file to override.

Note: to override monthly results, please use Notepad to open the CSV file and edit the value, instead of Excel.

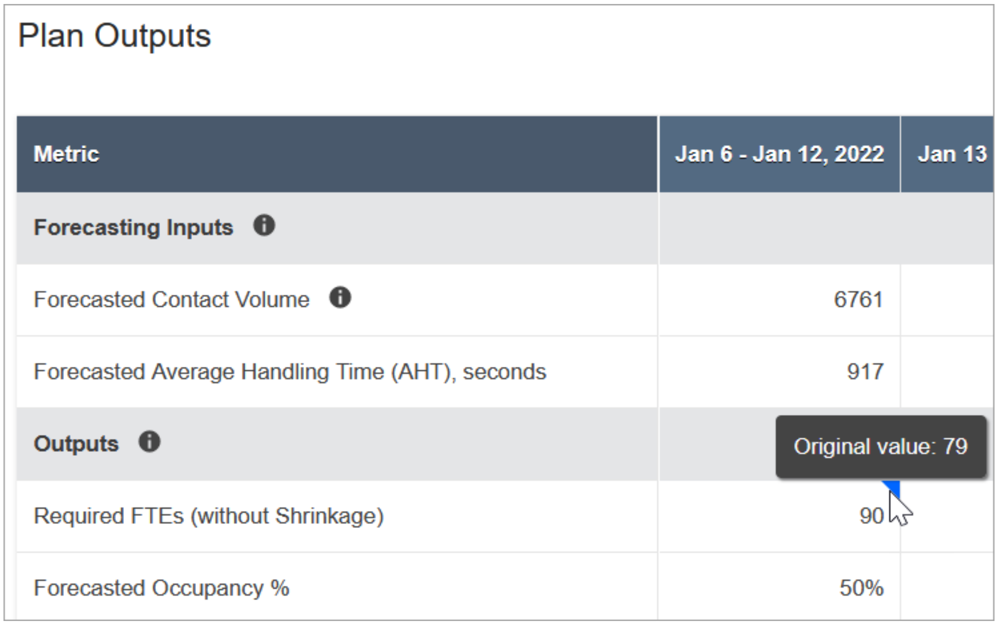
The .csv file template has one row, and it contains the values that were displayed in the **Required FTEs (with Shrinkage)** row of the **Plan outputs** table. The following image shows an example:



	A	B	C	D	E
1	Metrics	Jan 6 - Jan 12, 2022	Jan 13 - Jan 19, 2022	Jan 20 - Jan 26,	Jan 27 - Fe
2	Required FTEs (without Shrinkage)	79	78	81	78
3					
4					

5. Make your changes, and save the template file with a different name. Return to the **Upload override** dialog box (you might need to choose **Actions**, **Upload plan override** to redisplay the dialog box), choose **Upload CSV**, and then choose **Override**.

6. After you upload the .csv file, the metrics in the **Required FTEs (without Shrinkage)** row are automatically re-calculated and updated. Hover over the blue triangle to see the original value.



Plan Outputs

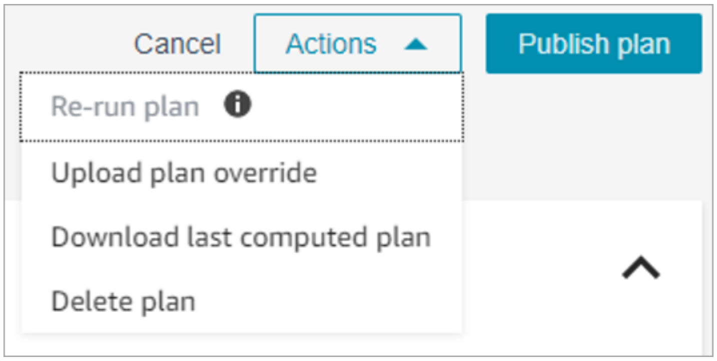
Metric	Jan 6 - Jan 12, 2022	Jan 13
Forecasting Inputs		
Forecasted Contact Volume	6761	
Forecasted Average Handling Time (AHT), seconds	917	
Outputs		
Required FTEs (without Shrinkage)	90	
Forecasted Occupancy %	50%	

Original value: 79

7. The rest of the metrics are updated automatically to reflect the latest change for **Required FTEs (without Shrinkage)**.

Re-run a capacity plan (Preview)

You can re-run capacity plans when you make any changes on the plan start and/or end date, or the scenario. When there are no changes to plan inputs or the scenario, the **Re-run plan** option is not active, as shown in the following image.

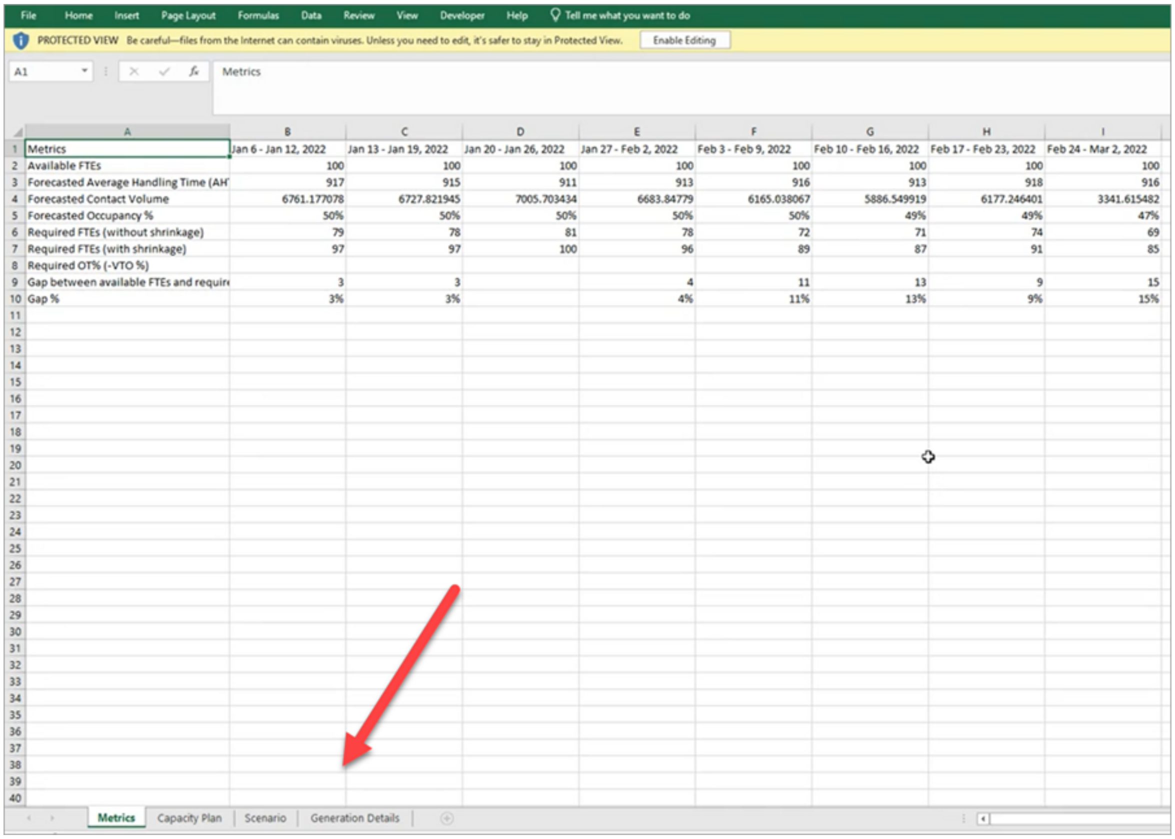


To re-run a plan

1. Go to the **Capacity Plans** tab, and choose the plan.
2. Change the start and/or end date, or select a different scenario.
3. Choose **Actions**, **Re-run plan**.

Download a capacity plan (Preview)

When you download a capacity plan file, it downloads as a .csv file type with multiple tabs. It's helpful to open this file using Excel.



PROTECTED VIEW Be careful—files from the Internet can contain viruses. Unless you need to edit, it's safer to stay in Protected View.

	A	B	C	D	E	F	G	H	I
1	Metrics	Jan 6 - Jan 12, 2022	Jan 13 - Jan 19, 2022	Jan 20 - Jan 26, 2022	Jan 27 - Feb 2, 2022	Feb 3 - Feb 9, 2022	Feb 10 - Feb 16, 2022	Feb 17 - Feb 23, 2022	Feb 24 - Mar 2, 2022
2	Available FTEs	100	100	100	100	100	100	100	100
3	Forecasted Average Handling Time (AH	917	915	911	913	916	913	918	916
4	Forecasted Contact Volume	6761.177078	6727.821945	7005.703434	6683.84779	6165.038067	5886.549919	6177.246401	3341.615482
5	Forecasted Occupancy %	50%	50%	50%	50%	50%	49%	49%	47%
6	Required FTEs (without shrinkage)	79	78	81	78	72	71	74	69
7	Required FTEs (with shrinkage)	97	97	100	96	89	87	91	85
8	Required OT% (-VTO %)								
9	Gap between available FTEs and requir	3	3		4	11	13	9	15
10	Gap %	3%	3%		4%	11%	13%	9%	15%

Following is a description of each tab:

- **Metrics**: The capacity plan output.
- **Capacity Plan**: The capacity plan metadata, such as name, starting date, and ending date of the plan.
- **Scenario**: The input defined for the capacity plan.
- **Generation Details**: The metadata indicating when someone last changed the capacity plan.

How to download capacity plan results

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Analytics**, **Capacity planning - Edit**.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling (Preview) (p. 1030).

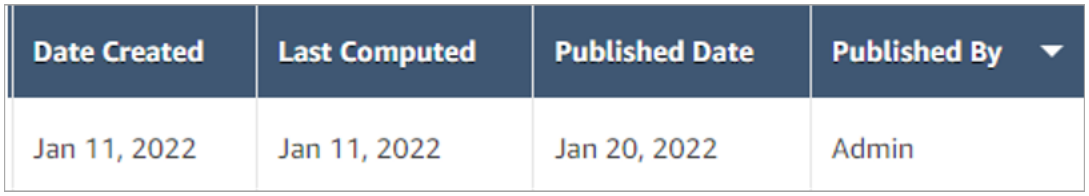
2. On the Amazon Connect navigation menu, select **Analytics**, **Capacity Planning**.
3. On the **Capacity Plans** tab, choose the plan.
4. On the detailed page for the capacity plan, choose **Actions**, **Download capacity plan**.

Publish a capacity plan (Preview)

When you are satisfied with the capacity plan outputs, choose **Publish plan** to finalize your plan.

> **Note**
> You cannot edit the plan after it is published.

Your login name and the published date is displayed on the list view of the capacity plans. For example, the following image shows a plan that was first created on January 11, 2022, and then it was published on January 20, 2022 by Admin.



Date Created	Last Computed	Published Date	Published By ▼
Jan 11, 2022	Jan 11, 2022	Jan 20, 2022	Admin

Scheduling in Amazon Connect (Preview)

Contact center schedulers or managers need to create agent schedules for day-to-day workloads that are flexible and meet business and compliance requirements. Amazon Connect helps you create efficient schedules that are optimized for per-channel Service Level or Average speed of answer targets. You can generate and manage agent schedules based on the following:

- A short-term published forecast
- Shift profiles (templates for weekly shifts)
- Staffing groups (agents that can handle specific types of contacts from a specific forecast group)
- Human resources and business rules

> **Note**
> Amazon Connect scheduling is not designed to ensure compliance with any particular laws. It is your responsibility to ensure that your actions and your use of scheduling comply with any applicable laws including employment regulations. You should confer with your legal counsel to determine your obligations.

Getting started

Following is the order of steps for creating a schedule and publishing it so supervisors and agents can view it.

1. Add users (p. 785) to your Amazon Connect instance.
2. Double-check with your Amazon Connect admin that users have the required security profile permissions to access scheduling features. The required permissions are described here (p. 1030).
3. Create staff scheduling rules (Preview) (p. 1053)
4. Create shift activities (Preview) (p. 1054)

5. Create shift profiles (Preview) (p. 1054)
6. Create staffing groups and rules (Preview) (p. 1055)
7. Generate, review, and publish a schedule by using Schedule Manager (Preview) (p. 1057)

To learn how supervisors and agents view schedules, see How supervisors view published schedules (Preview) (p. 1060) and How agents view their schedule (p. 1144).

Scheduling roles: Who does what (Preview)

There are a variety of roles for people who might create and manage schedules in a contact center, such as the following:

1. **Amazon Connect administrator** – Maintains user profiles, grants security profile permissions, sets up holiday hours for the contact center.
2. **Scheduler** – Creates manages staffing groups, creates staffing rules, configures shift components (such as creating shift activities and profiles), generates schedules, revises, and publishes schedules.

   After the scheduler publishes a schedule, the supervisors and agents receive an email notification that the schedule has been published and they can view it.
3. **Supervisor** – Manages agents and schedules, updates schedules, manages requests for time off, shift swaps, overtime (OT), and voluntary time off (VTO).
4. **Agent** – Answers contacts, views the generated schedule, manages requests for time off, shift swaps, overtime (OT), and voluntary time off (VTO).

Amazon Connect provides security profile permissions that you can assign to each role, so that you can manage access to specific features by role. For more information, see Security profile permissions for forecasting, capacity planning, and scheduling (Preview) (p. 1030).

Scheduling terminology (Preview)

Draft schedule

A collection of schedules for all agents in a set of staffing groups that the schedule is for.

Only schedulers can view and adjust draft schedules. Agents or their supervisors cannot view these schedules until published.

Overtime / Voluntary time off

- Requesting overtime to agents allows your contact center to handle a contact surge or agent shortages without hiring more employees. Requesting voluntary time off to agents allows your business to handle contacts without paying employees to be idle.
- Requesting voluntary time off to agents allows your business to handle contacts without paying employees to be idle.

Publish a schedule

An action taken by schedulers to make agent schedules formal and visible in agent and supervisor Schedule calendars (which are separate user interfaces).

Schedule

Multiple shifts tied together between the start and end dates for a specific agent.

Schedule adjustment

Before schedule publishing to supervisors or agents, the Scheduler or the person with permission can add, edit, remove, replace agent activities, or edit and remove shifts to orchestrate supply (that is, the number of agents and shift activities) vs demand (the number of contacts).

Schedule generation

The ability to generate and publish shift schedules for specific date range for a Forecast Group - Staff Group combination.

Shift activities

Daily activities that the agent does during their shift. For example, meetings, training, and lunch.

Shift profiles

The base structure of a shift, schedule window, daily shift activities that go into it.

Shift swap

Peer shift swap is a workflow for agents to have flexibility over their work hours by swapping shifts with each other.

Staffing groups

A group or team of agents who are skilled to take specific types of contacts. For example, you might create one staffing group named General Enquiry, and another named Tier 2 Support.

Create staff scheduling rules (Preview)

Use staff rules to specify details for individual agents and supervisors, such as their local time zone, start and end dates, and contract details. The individual staff rules you specify here override any staffing group rules when their schedule is generated.

For example, you might set up the staffing group to generate a schedule where everyone works 40 hours per week. In the staffing rules, you can choose specific employees to schedule for 20 hours per week.

To create staffing rules for individual users

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Scheduling**, **Schedule manager - Edit**.

   For more information, see Required permissions (p. 1030).
2. On the Amazon Connect navigation menu, select **Users**, **Scheduling**.
3. Choose the **Staff Rules** tab, and then search and choose one or more staff from the list.
4. Specify details such as:

   - Time zone: Render schedules in the local time zone of the agent.

   - Start and end dates: Schedule specific agent shifts based on start or end dates.
   - Working hours: Define the minimum and maximum working hours per day and per week. Working hours should include non-productive time, such as breaks and meals.
   - Consecutive days worked or days off: Schedule shifts based on the allowed range of consecutive days worked or days off.
5. Choose **Apply to Staff**. This saves the rules, and ensures they are applied during the next scheduling cycle.

Create shift activities (Preview)

Shift activities are daily activities that the staff (agents) does during their shift. For example:

- **Productive**: At work activities that agents do that are counted as productive work, such as answering contacts.
- **Non-Productive**: At work activities that agents do that are not counted as productive work, such as breaks and team meetings.
- **Leave**: Absent from work. Their status in the agent application is **Offline**.

You can create multiple shift activities to include as part of your staff shifts.

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Scheduling**, **Schedule manager - Edit**.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling (Preview) (p. 1030).
2. On the Amazon Connect navigation menu, select **Users**, **Scheduling**.
3. Choose the **Shift Activities** tab, and then choose **Add shift activities**. Fill in the details and choose **Save**.

   You can add multiple activities, and add and remove activities.
4. The next time a schedule is created as part of the scheduling cycle, the shift activities are applied.

   Tip
   Create shift profiles to ensure the desired sequence of the shift activities. For example, to schedule agents to go on their break two hours before lunch. For instructions, see Create shift profiles (Preview) (p. 1054).

Create shift profiles (Preview)

Use shift profiles to create templates for weekly shifts. The template includes the days of the week worked, the earliest start time and the latest end times the staff can be scheduled, and the activities they would do during their shift.

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Scheduling**, **Schedule manager - Edit**.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling (Preview) (p. 1030).
2. On the Amazon Connect navigation menu, select **Users**, **Scheduling**.
3. Choose the **Shift Profiles** tab, and then choose **Add shift profiles**.
4. Select days of the week staff will be scheduled for, earliest start time and the latest end time for each day. Ensure that these times are configured in UTC instead of local time.

Depending on the contact demand pattern forecast, Amazon Connect determines the best possible start and end times for shifts, while adhering to the minimum and maximum hours per day and week worked.

5. Choose **Add shift activities**. Select the shift activities the staff will do during their shift.
6. For each activity, set placement rules. The rules include:

   - The time duration from the beginning to end of the shift where the activities need to be placed.
   - The time window for Amazon Connect to pick the best spot to maximize efficiency of the generated schedules to meet the goals, such as the service level percent (SL%) targets.
7. After saving the shift profile, you can edit or remove it from the list view.

For example, if you set break to start 6 hours after the start of a shift and lunch to start 3 hours after the start of a shift, the lunch is scheduled to occur first.

Create staffing groups and rules (Preview)

A *staffing group* is a group or team of agents who are skilled to take specific types of contacts. You add agents who need a schedule generated for them, and supervisors who manage agent schedules. You can also add rules that apply at the staffing group level, such as the minimum staff required and the minimum working hours per day or week for the group.

For example, say your contact center opens at 9AM but the forecast says no contacts arrive between 9-9:30AM. You can add a rule that says, despite what the forecast predicts, there should be a minimum of one agent during this time.

If you don't have a shift start time rule, then the schedule is built using the predictions from the forecast.

Example

For example, you might create one staffing group named General Enquiry, and another named Tier 2 Support. Because you map one or more staffing groups to a forecast group, here's how you would create staffing groups in this case:

1. Group all General Enquiry queues to a General Enquiry forecast group.
2. Map the General Enquiry forecast group to multiple staffing groups that have agents who can take general enquiry contacts.

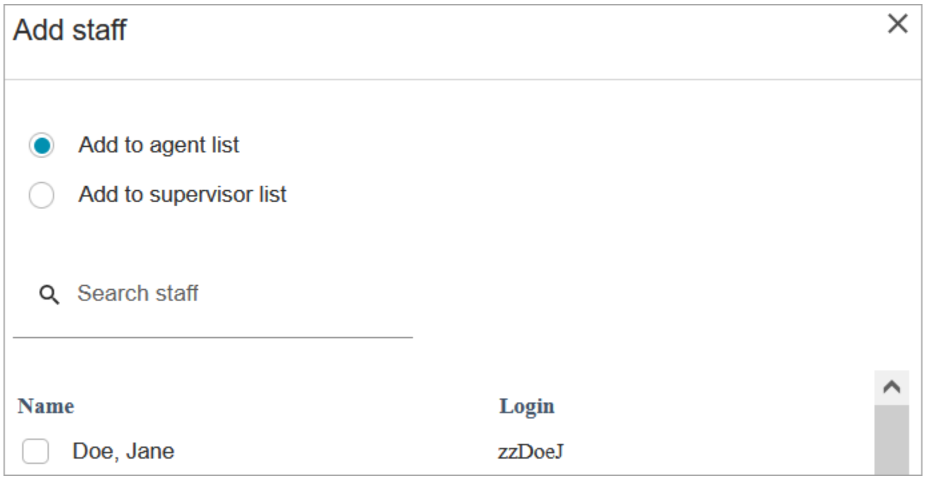
Create group and add staff

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Scheduling**, **Schedule manager - Edit**.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling (Preview) (p. 1030).
2. On the Amazon Connect navigation menu, select **Users**, **Scheduling**.
3. Choose the **Staffing Groups** tab, and then choose **Create staffing group**.
4. On the **Create Staffing Group** page, under **Associate to forecast group**, use the dropdown to choose the forecast group to associate with this staffing group.

   In the following example, contacts from the queues in the Forecast_Group_20220124 will be routed to the agents in this staffing group.

5. Choose **Add staff** to add agents and supervisors to this staffing group. A user must be added to Amazon Connect in order to appear in the list of staff.



Add staff

● Add to agent list

○ Add to supervisor list

Search staff

Name	Login
□ Doe, Jane	zzDoeJ

> **Tip**
> Every agent must be in a staffing group in order for a schedule to be generated for them. You can add and remove agents in between schedule cycles and manually add shifts.

Add rules

To generate a schedule, Amazon Connect uses information from the forecast group, which reflects the historical demand pattern for your contact center. Staffing rules enable you to specify conditions that must be accounted for in the schedule, regardless of what the forecast predicts.

For example, your contact center opens at 9AM but the forecast says no contacts arrive between 9AM-9:30AM. You can add a rule that, despite what the forecast predicts based on historical demand, there should be a minimum of one agent during this time. This forces Amazon Connect to keep one agent in the schedule from 9-9:30AM. In addition, you can add a rule to set the **Working Hours** to start at 9AM, even though the forecast would start it at 9:30AM.

To add rules

- In the **Rules** section, choose **+** and then use the dropdown to choose the type of rule to create for the staffing group. For example, you can specify:

  - **Minimum Staff Required**: Specify the minimum number of agents that should be available, despite what the forecast indicates. For example, if the forecast says that you do not need any agents in the first half hour that your contact center opens, you can ensure that there is a minimum of one agent during this time.
  - **Shift Start Time: Same Start Time**: This creates schedules with the same shift start time for all agents.
  - **Working Hours**: Specify the group's minimum and maximum working hours per day or week. This setting applies to all staff in the staffing group. You can override this setting for individual staff. For instructions, see Create staff scheduling rules (Preview) (p. 1053).

Generate, review, and publish a schedule by using Schedule Manager (Preview)

Amazon Connect is designed to generate the least number of shifts for agents based on the forecasted demand pattern and configured constraints to hit the optimization goal.

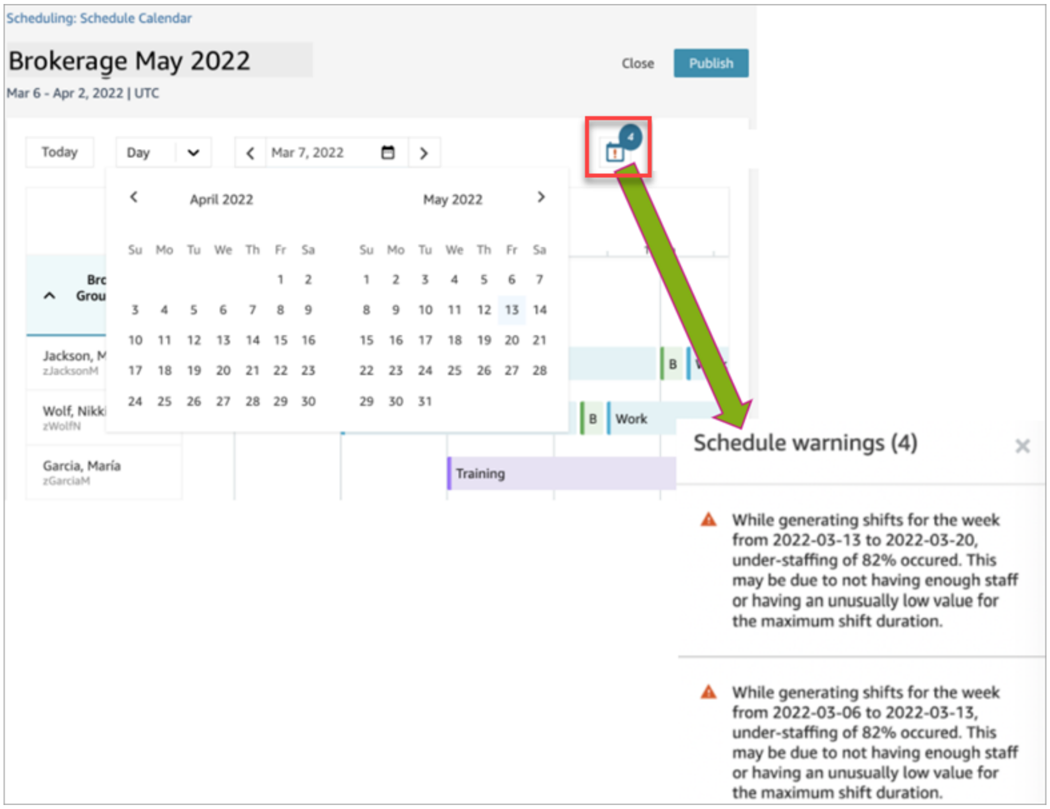
After you create shift activities, shift profiles, staffing groups and staffing group rules, you can generate a schedule.

1. Log in to the Amazon Connect console with an account that has security profile permissions for **Scheduling**, **Schedule manager - Edit**.

   For more information, see Security profile permissions for forecasting, capacity planning, and scheduling (Preview) (p. 1030).
2. On the Amazon Connect navigation menu, select **Users**, **Scheduling**.
3. Choose the **Schedule Manager** tab, and then choose **Generate schedule**.
4. Enter a name and description for the schedule.
5. In the **Schedule input** section, select the forecast group from the dropdown menu.

   Currently you cannot schedule for multiple forecast groups.
6. Specify the duration of the schedule - the start and end dates. You can schedule up to 18 weeks out.
7. Under **Optimize schedule for**, choose **Service level** or **Average speed of answer**.
8. Choose **Generate schedule**.

   > **Note**
   > Amazon Connect generates a draft schedule. It will not visible to agents or supervisors until you publish it.
9. In the list of schedules, the schedule you created shows a status of **In progress**. It takes 5-30 minutes to generate, depending on the number of agents, number of configured rules, schedule duration, and more. After the schedule is generated, it's status is **Complete** or **Failed**.
10. To view any warnings and breaches of rules or constraints breaches, choose the warnings icon to learn more.



Scheduling: Schedule Calendar

Brokerage May 2022

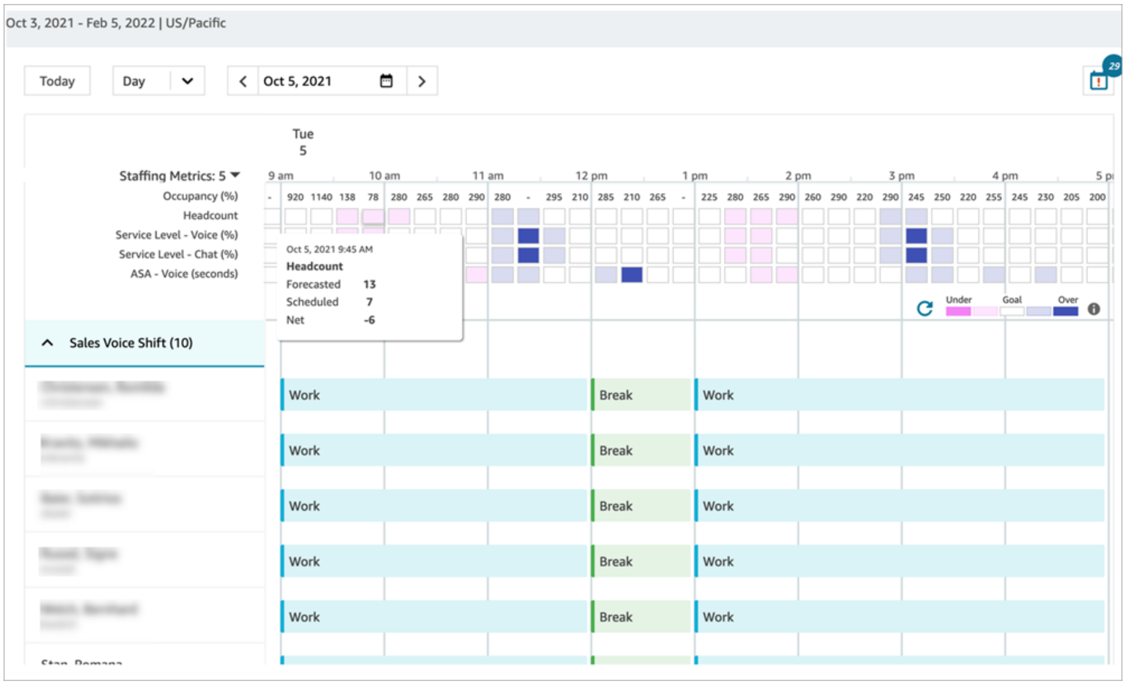
Mar 6 - Apr 2, 2022 | UTC

Schedule warnings (4)

While generating shifts for the week from 2022-03-13 to 2022-03-20, under-staffing of 82% occured. This may be due to not having enough staff or having an unusually low value for the maximum shift duration.

While generating shifts for the week from 2022-03-06 to 2022-03-13, under-staffing of 82% occured. This may be due to not having enough staff or having an unusually low value for the maximum shift duration.

11. When the status is **Complete**, choose the draft schedule to view it. The following image shows a sample schedule:



Oct 3, 2021 - Feb 5, 2022 | US/Pacific

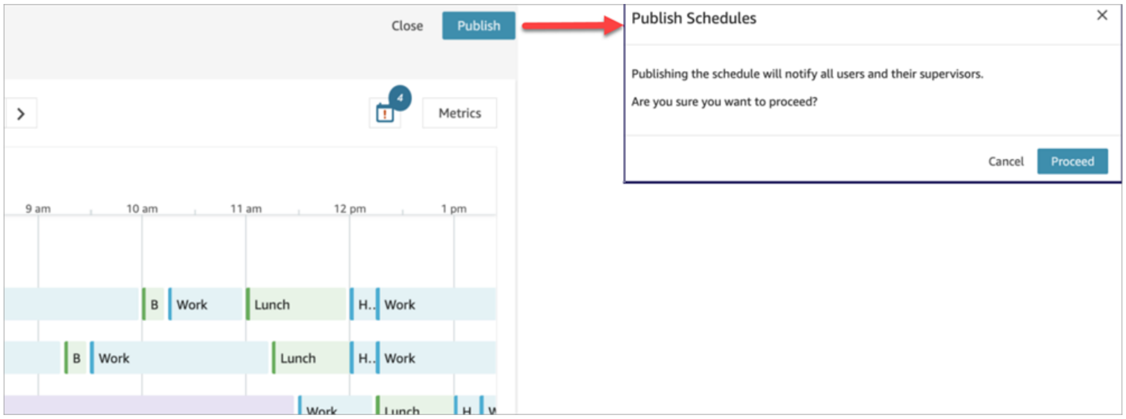
Oct 5, 2021 9:45 AM
Headcount
Forecasted 13
Scheduled 7
Net -6

Schedulers can:

- View schedules for all agents.

- Pick a date to view a specific shift.
- Navigate back to today's date.
- View failed rules and goals.

12. When you're satisfied with the schedule, choose **Publish**. You'll get a confirmation page. Choose **Proceed** to make the schedule official!



Publish Schedules

Publishing the schedule will notify all users and their supervisors.

Are you sure you want to proceed?

Staff (agents) and supervisors specified in the staffing groups can now view the schedule. See the following topics to learn about their experience:

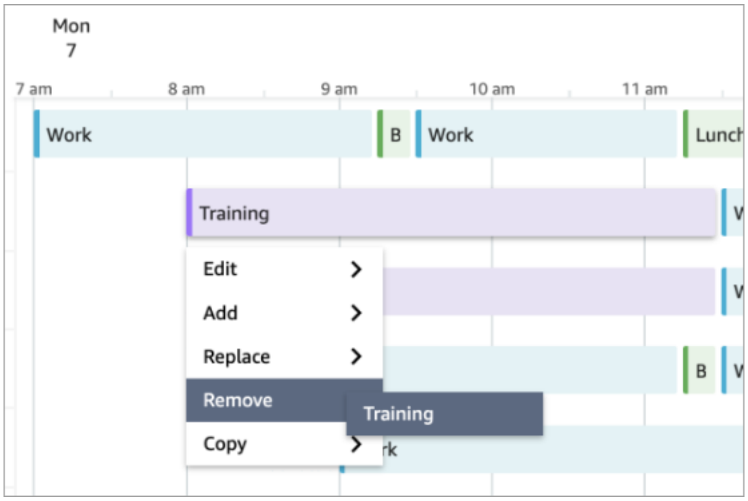
- How supervisors view published schedules (Preview) (p. 1060)
- How agents view their schedule (p. 1061)

Edit a schedule

Before publishing a schedule, you might want to edit it. For example, if you notice that all the agents are scheduled to be on break at the same time and no one is scheduled to take contacts.

You can:

- Change agent shift start and/or end time, duration.
- Change activity shift start and/or end time, duration.
- Add an activity to one or more agents shift.
- Remove or replace activity from an agent shift.
- Copy an entire shift from one agent to another.
- Recompute metrics to ensure schedule adjustments result in better service level (SL%) or occupancy.



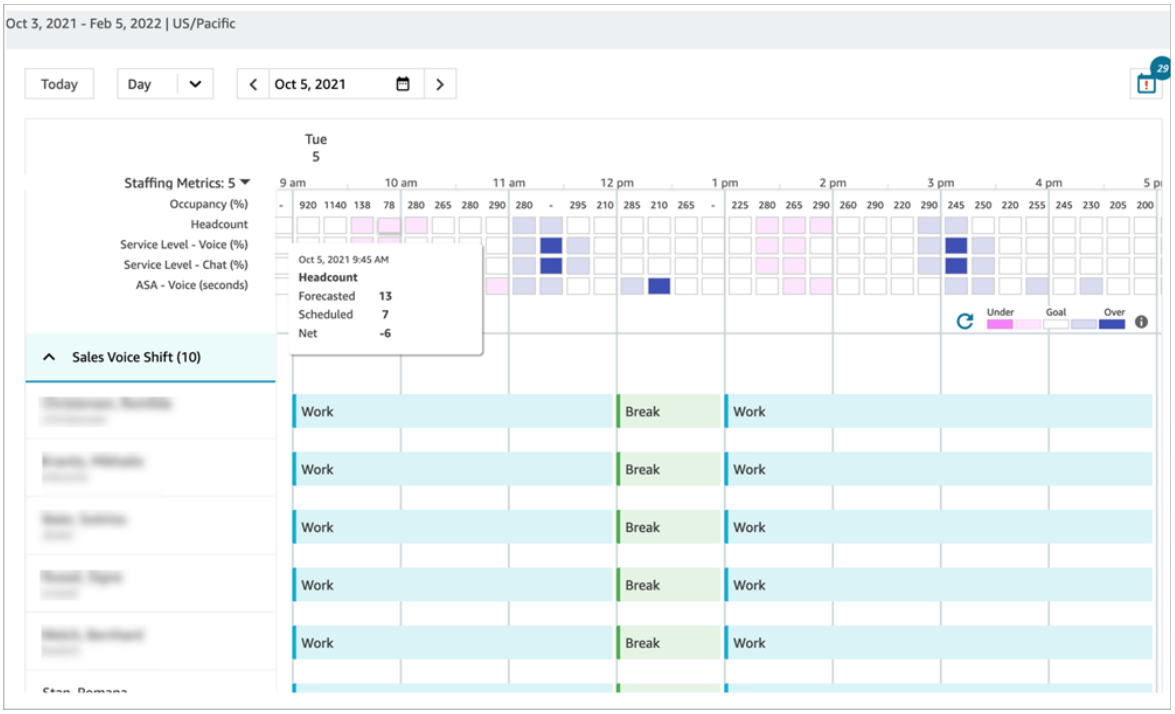
How supervisors view published schedules (Preview)

After a scheduler publishes a schedule, it's official. Agents can now view their individual scheduling using their agent application. Supervisors can also view their agents schedules using the Amazon Connect console.

Supervisors with **Scheduling**, **Schedule manager - Edit** permissions in their security profile can edit agent schedules.

> **Important**
> When a supervisor edits an agent schedule and publishes it, the change appears immediately to the agent. The agent receives an email notification that their schedule has been changed. They do not need to refresh their browser for the agent application to reflect the change.

The following image shows a sample schedule for a supervisor's team:



Oct 5, 2021 9:45 AM
Headcount
Forecasted 13
Scheduled 7
Net -6

How agents view their schedule

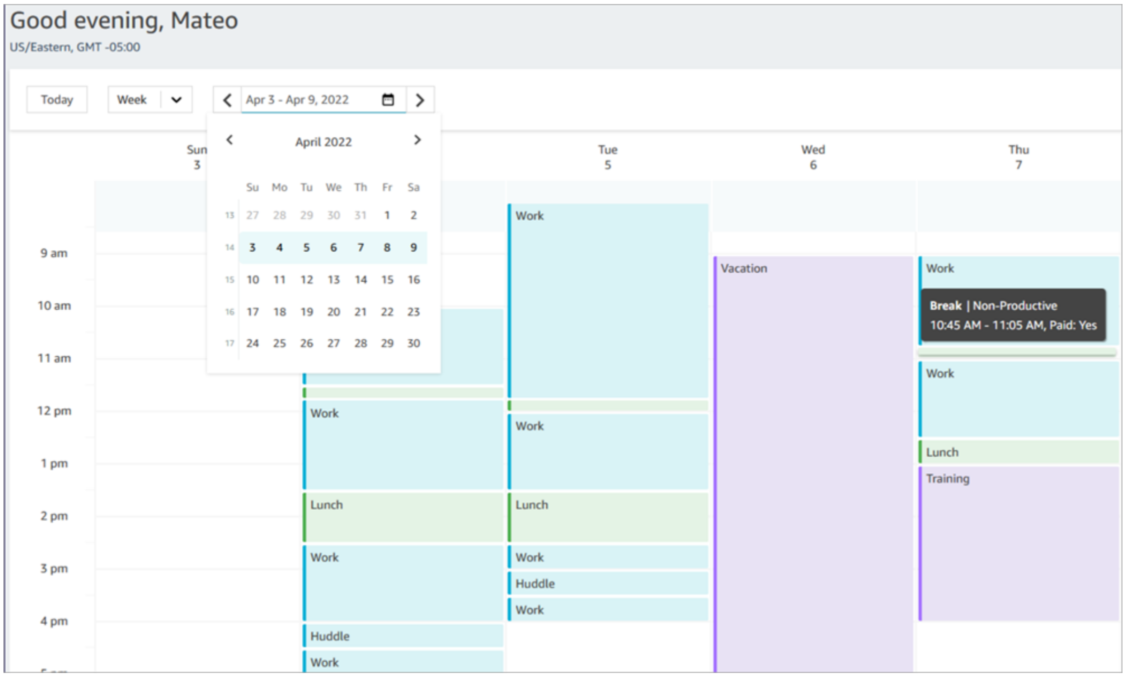
There are two ways agents can access their schedules:

- If your organization uses the Amazon Connect agent application, agents access their schedule by entering **https://*instance name*/connect/agent-app-v2/** into their browser and then choosing the calendar icon.
- If your organization uses the Contact Control Panel (CCPv1 or CCPv2), Salesforce CTI, or a custom-built agent desktop, agents access their schedule by entering **https://*instance name*/connect/agent-app-v2/scheduling** into their browser, logging into Amazon Connect, and then choosing the calendar icon.

Following are steps agents use to view their schedule in the agent application.

1. Log on to the agent application using the URL that your admin gives you.
2. Choose the Calendar icon on the application navigation bar to launch the staff schedule manager viewer. Otherwise, the staff schedule manager viewer launches automatically.

   The following image shows a sample schedule in the agent application:



You can see a daily or weekly view of your schedule.

Private optimization APIs (Preview)

Amazon Connect forecasting, capacity planning, and scheduling (preview) uses the following private API resources as actions in its IAM policy:

- `connect:BatchAssociateAnalyticsDataSet`. Grants access permissions and associates the specified datasets for the specified Amazon Connect instance with the specified AWS account.

- `connect:BatchDisassociateAnalyticsDataSet`. Revokes access permissions and disassociates the specified datasets for the specified Amazon Connect instance with the specified AWS account.

If you remove these actions from the preview role policy, the forecasting, capacity planning, and scheduling features won't work.

Security in Amazon Connect

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The shared responsibility model describes this as security *of* the cloud and security *in* the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the AWS compliance programs. To learn about the compliance programs that apply to Amazon Connect, see AWS Services in Scope by Compliance Program.
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations.

This documentation helps you understand how to apply the shared responsibility model when using Amazon Connect. The following topics show you how to configure Amazon Connect to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your Amazon Connect resources.

Contents

Data protection in Amazon Connect

The AWS shared responsibility model applies to data protection in Amazon Connect. As described in this model, AWS is responsible for protecting the global infrastructure that runs all of the AWS Cloud. You are responsible for maintaining control over your content that is hosted on this infrastructure. This content includes the security configuration and management tasks for the AWS services that you use. For more information about data privacy, see the Data Privacy FAQ. For information about data protection in Europe, see the AWS Shared Responsibility Model and GDPR blog post on the *AWS Security Blog*.

For data protection purposes, we recommend that you protect AWS account credentials and set up individual user accounts with AWS Identity and Access Management (IAM). That way each user is given only the permissions necessary to fulfill their job duties. We also recommend that you secure your data in the following ways:

- Use multi-factor authentication (MFA) with each account.
- Use SSL/TLS to communicate with AWS resources. We recommend TLS 1.2 or later.

- Set up API and user activity logging with AWS CloudTrail.
- Use AWS encryption solutions, along with all default security controls within AWS services.
- Use advanced managed security services such as Amazon Macie, which assists in discovering and securing personal data that is stored in Amazon S3.
- If you require FIPS 140-2 validated cryptographic modules when accessing AWS through a command line interface or an API, use a FIPS endpoint. For more information about the available FIPS endpoints, see Federal Information Processing Standard (FIPS) 140-2.

We strongly recommend that you never put confidential or sensitive information, such as your customers' email addresses, into tags or free-form fields such as a **Name** field. This includes when you work with Amazon Connect or other AWS services using the console, API, AWS CLI, or AWS SDKs. Any data that you enter into tags or free-form fields used for names may be used for billing or diagnostic logs. If you provide a URL to an external server, we strongly recommend that you do not include credentials information in the URL to validate your request to that server.

Contents

Data handled by Amazon Connect

Data held within Amazon Connect is segregated by the AWS account ID and the Amazon Connect instance ID. This ensures that data can be accessed only by the authorized users of a specific Amazon Connect instance.

Amazon Connect handles a variety of data related to the contact center, including but not limited to the following categories.

- **Resources and configurations** -- This includes queues, contact flows, users, routing profiles, and task templates.
- **Contact metadata**-- This includes connection time, handle time, source number (ANI), destination number (DNIS), and user defined contact attributes.
- **Agent-related performance data** -- This includes login time, status changes, and contacts handled.
- **Phone call audio streams** -- When enabled, this also includes call recordings.
- **Chat transcripts** – Included only if enabled.
- **Attachments** – Included only if enabled.
- **Integration configuration** – Includes user defined name, description and metadata when creating integration with external applications.
- **Knowledge documents** – This includes documents used by agents to handle contacts.
- **Voiceprints** – When Amazon Connect Voice ID is enabled, a voiceprint is created from the customer's voice for future authentication. Similarly, a voiceprint is created while registering a fraudster in the Voice ID system for future fraud detection.
- **Speaker and Fraudster Audio** – When Amazon Connect Voice ID is enabled, the audio used for enrolling speakers and registering fraudsters is stored so that Voice ID can re-enroll and reregister them in future when there is a need to do so.

Amazon Connect stores the following Personally Identifiable Information (PII) data related to your customers:

- The customer's phone number: ANI for inbound calls, and DNIS for outbound calls or transfers.
- If you are using Amazon Connect Customer Profiles, all this data could potentially be PII. This data is always encrypted at rest using either a customer-provided KMS key or a service-owned key. The Amazon Connect Customer Profiles data is segregated by the AWS account ID and the domain. Multiple Amazon Connect instances can share a single Customer Profiles domain.
- For high-volume outbound communications, Amazon Pinpoint passes customer phone numbers and relevant attributes to Amazon Connect. On the Amazon Connect side, these are always encrypted at rest using either a customer managed key or an AWS owned key. The high-volume outbound communications data is segregated by the Amazon Connect instance ID and are encrypted by instance-specific keys.

External application data

Amazon AppIntegrations enables you to integrate with external applications. It stores references to other AWS resources and client-service specified metadata. No data is stored other than incidentally while being processed. When syncing data periodically with an Amazon Connect service, data is encrypted using a customer managed key and stored temporarily for one month.

Phone call media

Amazon Connect is in the audio path for calls handled by the service. It is therefore responsible for relaying the call’s media stream between participants. This can include the audio between a customer and a contact flow / IVR, the audio between a customer and an agent, or mixing the audio between multiple parties in a conference or during a transfer. There are two types of phone calls:

- PSTN calls. This includes inbound customer calls, outbound calls placed by agents to customers, and calls to an agent’s physical phone, if this option has been enabled in the Contact Control Panel (CCP).
- Softphone calls placed to the agent’s browser.

PSTN calls are connected between Amazon Connect and various telecommunications carriers using either private circuits maintained between Amazon Connect and our providers or existing AWS internet connectivity. For PSTN calls routed over the public internet, signaling is encrypted with TLS and the audio media is encrypted with SRTP.

Softphone calls are established to the agent’s browser with an encrypted WebSocket connection using TLS. The audio media traffic to the browser is encrypted in transit using DTLS-SRTP.

Call recordings

Call recording is disabled by default in Amazon Connect. You can enable call recording in the contact flows, which allows for more detailed control over which calls are recorded.

The call recording feature has options for choosing whether to record the agent only, customer only, or agent and customer conversations. When call recording is enabled, the recording begins when the call is connected to an agent and stops when the agent disconnects. Any transfers to external numbers are not recorded after the agent leaves the call.

You can limit access to the call recordings based on user permissions. Recordings can be searched and played back within the Amazon Connect web interface.

Call recording storage

Call recordings are stored in two phases:

- Recordings intermediately held within Amazon Connect during and after the call, but before delivery.

- Recordings delivered to your Amazon S3 bucket.

The recordings that are stored in your Amazon S3 bucket are secured using a AWS KMS key that was configured when your instance was created.

At all times, you maintain full control over the security of call recordings delivered to your Amazon S3 bucket.

Call recording access

You can search and listen to call recordings in Amazon Connect. To determine which users can do this, assign them the appropriate security profiles. If AWS CloudTrail is enabled, access to specific recordings by Amazon Connect users is captured in CloudTrail.

The capabilities of Amazon S3, AWS KMS, and IAM put you in full control of who has access to call recording data.

In addition, you can track who listens to or deletes recordings; see Track who deleted or listened to recordings (p. 806).

Contact metadata

Amazon Connect stores metadata related to contacts that flow through the system and allows authorized users to access this information. The Contact Search feature allows you to search and view contact data, such as origination phone numbers or other attributes set by the contact flow, that are associated with a contact for diagnostics or reporting purposes.

Contact data classified as PII that is stored by Amazon Connect is encrypted at rest using a key that is time-limited and specific to the Amazon Connect instance. Specifically, the customer origination phone number is cryptographically hashed with a key that is specific to the instance to allow for use in contact search. For contact search, the encryption key is not time-sensitive.

The following data stored by Amazon Connect is treated as sensitive:

- Origination phone number
- Outbound phone number
- External numbers dialed by agents for transfers
- External numbers transferred to by a contact flow
- Contact name
- Contact description
- All contact attributes
- All contact references

Contact Lens real-time processing

Content processed by Contact Lens in real-time is encrypted at rest and in transit. Data is encrypted with keys owned by Contact Lens.

Voiceprints and Voice ID audio recordings

When you enable Amazon Connect Voice ID, it computes voiceprints out of your customer's speech for authenticating them in future, and stores the data. Similarly, when you enable fraud detection, it stores the voiceprint for each fraudster registered in Voice ID.

While enrolling a customer into Voice ID for authentication and fraud detection, you must specify a `CustomerSpeakerId` for them. Since Voice ID stores biometric information for each speaker, we strongly recommend that you use an identifier that does not contain PII in the `CustomerSpeakerId` field.

Speaker and Fraudster Audio

When you enable Amazon Connect Voice ID, it stores the necessary amount of audio it aggregated while enrolling a speaker or registering a fraudster into the system. The data is retained until the speaker/fraudster is deleted. This audio is used in the future whenever the voiceprints for the speakers and fraudsters need to be regenerated.

High-volume outbound communications

For high-volume outbound communications, Amazon Pinpoint passes customer phone numbers and relevant attributes to Amazon Connect. On Amazon Connect, these are always encrypted at rest using either a customer managed key or an AWS owned key. The high-volume outbound communications data is segregated by the Amazon Connect instance ID and are encrypted by instance specific keys.

Task templates

Any processing of task template resources in Amazon Connect is encrypted at rest and in transit. Data is encrypted with AWS KMS key.

Encryption at rest

Contact data classified as PII, or data that represents customer content being stored by Amazon Connect, is encrypted at rest (that is, before it is put, stored, or saved to a disk) using a key that is time-limited and specific to the Amazon Connect instance.

Amazon S3 server-side encryption is used to encrypt conversation recordings (voice and chat) and knowledge documents at rest with a AWS Key Management Service data key unique per customer account. Amazon AppIntegrations configuration data is encrypted the same way. For information about AWS KMS keys, see What is AWS Key Management Service? in the *AWS Key Management Service Developer Guide*.

Amazon Connect Voice ID stores customer voiceprints which cannot be reverse-engineered to obtain the enrolled customer's speech or identify a customer. These are encrypted using a customer managed key.

Integration configuration data is encrypted at rest using a key that is time-limited and specific to the user account.

External application data encryption at rest

When you create a DataIntegration encrypted with a customer managed key, Amazon AppIntegrations creates a grant on your behalf by sending a `CreateGrant` request to AWS KMS. Grants in AWS KMS are used to give Amazon AppIntegrations access to a KMS key in your account.

You can revoke access to the grant, or remove the access that Amazon AppIntegrations has to the customer managed key at any time. If you do, Amazon AppIntegrations can not access any of the data encrypted by the customer managed key, which affects operations that are dependent on that data.

External application data that Amazon AppIntegrations processes is encrypted at rest in an S3 bucket using the customer managed key that you provided during configuration.

Amazon AppIntegrations requires the grant to use the customer managed key for the following internal operations:

- Send `GenerateDataKeyRequest` to AWS KMS to generate data keys encrypted by your customer managed key.
- Send `Decrypt` requests to AWS KMS to decrypt encrypted data keys so that they can be used to encrypt your data.

Amazon Connect Customer Profiles encryption at rest

All user data stored in Amazon Connect Customer Profiles is encrypted at rest. Amazon Connect Customer Profiles encryption at rest provides enhanced security by encrypting all your data at rest using encryption keys stored in AWS Key Management Service (AWS KMS). This functionality helps reduce the operational burden and complexity involved in protecting sensitive data. With encryption at rest, you can build security-sensitive applications that meet strict encryption compliance and regulatory requirements.

Organizational policies, industry or government regulations, and compliance requirements often require the use of encryption at rest to increase the data security of your applications. Customer Profiles integrated with AWS KMS to enable its encryption at rest strategy. For more information, see AWS Key Management Service Concepts in the AWS Key Management Service Developer Guide.

When creating a new domain, you must provide a KMS key that the service will use to encrypt your data in transit and at rest. The customer managed key is created, owned, and managed by you. You have full control over the customer managed key (AWS KMS charges apply).

You can specify an encryption key when you create a new domain or profile object type or switch the encryption keys on an existing resources by using the AWS Command Line Interface (AWS CLI), or the Amazon Connect Customer Profiles Encryption API. When you choose a customer managed key, Amazon Connect Customer Profiles creates a grant to the customer managed key that grants it access to the customer managed key.

AWS KMS charges apply for a customer managed key. For more information about pricing, see AWS KMS pricing.

Amazon Connect Wisdom encryption at rest

All user data stored in Amazon Connect Wisdom is encrypted at rest using encryption keys stored in AWS Key Management Service. If you optionally provide a customer managed key, Wisdom uses it to encrypt knowledge content stored at rest outside of Wisdom search indices. Wisdom uses dedicated search indices per customer and they are encrypted at rest by using AWS owned keys stored in AWS Key Management Service. Additionally, you can use CloudTrail to audit any data access via the Wisdom APIs.

AWS KMS charges apply when using a key that you provide. For more information about pricing, see AWS KMS pricing.

Amazon Connect Voice ID encryption at rest

All user data stored in Amazon Connect Voice ID is encrypted at rest. When creating a new Voice ID domain, you must provide a customer managed key that the service uses to encrypt your data at rest. The customer managed key is created, owned, and managed by you. You have full control over the key.

You can update the KMS key in the Voice ID domain by using the `update-domain` command in AWS Command Line Interface (AWS CLI), or the UpdateDomain Voice ID API.

When you change the KMS key, an asynchronous process will be triggered to re-encrypt the old data with the new KMS key. After this process completes, all of your domain's data will be encrypted under the new KMS key, and you may safely retire the old key. For more information, see UpdateDomain.

Voice ID creates a grant to the customer managed key that grants it access to the key. For more information, see How Amazon Connect Voice ID uses grants in AWS KMS (p. 1069).

Following is a list of data that is encrypted at rest using the customer managed key:

- **Voiceprints**: The voiceprints generated while enrolling the speakers and registering fraudsters into the system.
- **Speaker and fraudster audio**: The audio data used for enrolling the speakers and registering the fraudsters.
- **CustomerSpeakerId**: The customer-provided SpeakerId while enrolling the customer into Voice ID.
- **Customer-provided metadata**: These include free-form strings such as `Domain Description`, `Domain Name`, `Job Name`, and more.

AWS KMS charges apply for a customer managed key. For more information about pricing, see AWS KMS pricing.

How Amazon Connect Voice ID uses grants in AWS KMS

Amazon Connect Voice ID requires a grant to use your customer managed key. When you create a domain, Voice ID creates a grant on your behalf by sending a see CreateGrant request to AWS KMS. The grant is required to use your customer managed key for the following internal operations:

- Send DescribeKey requests to AWS KMS to verify that the symmetric customer managed key ID provided is valid.
- Send GenerateDataKey requests to KMS key to create data keys with which to encrypt objects.
- Send Decrypt requests to AWS KMS to decrypt the encrypted data keys so that they can be used to encrypt your data.
- Send ReEncrypt requests to AWS KMS when the key is updated to re-encrypt a limited set of data using the new key.
- Store files in S3 using the AWS KMS key to encrypt the data.

You can revoke access to the grant, or remove the service's access to the customer managed key at any time. If you do, Voice ID won't be able to access any of the data encrypted by the customer managed key, which affects all the operations that are dependent on that data, leading to `AccessDeniedException` errors and failures in the asynchronous workflows.

Customer managed key policy for Voice ID

Key policies control access to your customer managed key. Every customer managed key must have exactly one key policy, which contains statements that determine who can use the key and how they can use it. When you create your customer managed key, you can specify a key policy. For more information, see Managing access to KMS keys in the *AWS Key Management Service Developer Guide*.

Following is an example key policy which gives a user the permissions they need to call all Voice ID APIs using the customer managed key:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "Allow key access to Amazon Connect VoiceID.",
            "Effect": "Allow",
            "Principal": {
                "AWS": "your_user_or_role_ARN"
            },
            "Action": [
                "kms:CreateGrant",
                "kms:Decrypt",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": [
                        "voiceid.region.amazonaws.com"
                    ]
                }
            }
        }
    ]
}
```

For information about specifying permissions in a policy, see Specifying KMS keys in IAM policy statements in the AWS Key Management Service Developer Guide.

For information about troubleshooting key access, see Troubleshooting key access in the AWS Key Management Service Developer Guide.

Voice ID encryption context

An encryption context is an optional set of key-value pairs that contain additional contextual information about the data. AWS KMS uses the encryption context as additional authenticated data to support authenticated encryption.

When you include an encryption context in a request to encrypt data, AWS KMS binds the encryption context to the encrypted data. To decrypt data, you include the same encryption context in the request.

Voice ID uses the same encryption context in all AWS KMS cryptographic operations, where the key is `aws:voiceid:domain:arn` and the value is the resource Amazon Resource Name (ARN) Amazon Resource Name (ARN).

```
"encryptionContext": {
   "aws:voiceid:domain:arn": "arn:aws:voiceid:us-west-2:111122223333:domain/sampleDomainId"
}
```

You can also use the encryption context in audit records and logs to identify how the customer managed key is being used. The encryption context also appears in logs generated by CloudTrail or Amazon CloudWatch Logs.

Using encryption context to control access to your customer managed key

You can use the encryption context in key policies and IAM policies as conditions to control access to your symmetric customer managed key. You can also use encryption context constraints in a grant.

Amazon Connect Voice ID uses an encryption context constraint in grants to control access to the customer managed key in your account or Region. The grant constraint requires that the operations that the grant allows use the specified encryption context.

The following are example key policy statements to grant access to a customer managed key for a specific encryption context. The condition in this policy statement requires that the grants have an encryption context constraint that specifies the encryption context.

```
{
    "Sid": "Enable DescribeKey",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:DescribeKey",
     "Resource": "*"
},
{
     "Sid": "Enable CreateGrant",
     "Effect": "Allow",
     "Principal": {
         "AWS": "arn:aws:iam::111122223333:role/ExampleReadOnlyRole"
     },
     "Action": "kms:CreateGrant",
     "Resource": "*",
     "Condition": {
         "StringEquals": {
             "kms:EncryptionContext:"aws:voiceid:domain:arn": "arn:aws:voiceid:us-
west-2:111122223333:domain/sampleDomainId""
          }
     }
}
```

Monitoring your encryption keys for Voice ID

When you use an AWS KMS customer managed key with Voice ID, you can use AWS CloudTrail or Amazon CloudWatch Logs to track requests that Voice ID sends to AWS KMS.

The following examples is a sample AWS CloudTrail event for `CreateGrant` operation called by Voice ID to access data encrypted by your customer managed key:

CreateGrant

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA5STZEFPSZEOW7NP3X:SampleUser1",
        "arn": "arn:aws:sts::111122223333:assumed-role/SampleRole/SampleUser",
        "accountId": "111122223333",
        "accessKeyId": "AAAAAAA1111111EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA5STZEFPSZEOW7NP3X",
                "arn": "arn:aws:iam::111122223333:role/SampleRole",
                "accountId": "111122223333",
                "userName": "SampleUser"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2021-09-14T23:02:23Z",
                "mfaAuthenticated": "false"
            }
        },
        "invokedBy": "voiceid.amazonaws.com"
    },
    "eventTime": "2021-09-14T23:02:50Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "CreateGrant",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "SampleIpAddress",
    "userAgent": "Example Desktop/1.0 (V1; OS)",
    "requestParameters": {
        "constraints": {
            "encryptionContextSubset": {
                "aws:voiceid:domain:arn": "arn:aws:voiceid:us-
west-2:111122223333:domain/sampleDomainId"
            }
        },
        "retiringPrincipal": "voiceid.amazonaws.com",
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/44444444-3333-2222-1111-
EXAMPLE11111",
        "operations": [
            "CreateGrant",
            "Decrypt",
            "DescribeKey",
            "GenerateDataKey",
            "GenerateDataKeyPair",
            "GenerateDataKeyPairWithoutPlaintext",
            "GenerateDataKeyWithoutPlaintext",
            "ReEncryptFrom",
            "ReEncryptTo"
        ],
        "granteePrincipal": "voiceid.amazonaws.com "
    },
    "responseElements": {
        "grantId": "0000000000000000000000000000cce47be074a8c379ed39f22b155c6e86af82"
    },
    "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
    "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
    "readOnly": false,
    "resources": [
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-999999999999"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

DescribeKey

```
{
    "eventVersion": "1.08",
    "userIdentity": {
      "type": "AWSService",
      "invokedBy": "voiceid.amazonaws.com"
    },
    "eventTime": "2021-10-13T15:12:39Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "DescribeKey",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "voiceid.amazonaws.com",
    "userAgent": "voiceid.amazonaws.com",
    "requestParameters": {
        "keyId": "alias/sample-key-alias"
    },
    "responseElements": null,
    "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
    "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
    "readOnly": true,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-9999999999999"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```

Decrypt

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "voiceid.amazonaws.com"
    },
    "eventTime": "2021-10-12T23:59:34Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "Decrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "voiceid.amazonaws.com",
    "userAgent": "voiceid.amazonaws.com",
    "requestParameters": {
        "encryptionContext": {
            "keyId": "arn:aws:kms:us-west-2:111122223333:key/44444444-3333-2222-1111-
EXAMPLE11111",
            "encryptionContext": {
                "aws:voiceid:domain:arn": "arn:aws:voiceid:us-
west-2:111122223333:domain/sampleDomainId"
            },
            "encryptionAlgorithm": "SYMMETRIC_DEFAULT"
        },
        "responseElements": null,
        "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
        "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
        "readOnly": true,
        "resources": [{
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-9999999999999"
        }],
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "sharedEventID": "35d58aa1-26b2-427a-908f-025bf71241f6",
        "eventCategory": "Management"
    }
```

GenerateDataKeyWithoutPlaintext

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "voiceid.amazonaws.com"
    },
    "eventTime": "2021-10-13T00:26:41Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "GenerateDataKeyWithoutPlaintext",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "voiceid.amazonaws.com",
    "userAgent": "voiceid.amazonaws.com",
    "requestParameters": {
        "keyId": "arn:aws:kms:us-west-2:111122223333:key/44444444-3333-2222-1111-
EXAMPLE11111",
        "encryptionContext": {
            "aws:voiceid:domain:arn": "arn:aws:voiceid:us-west-2:111122223333:domain/
sampleDomainId"
        },
        "keySpec": "AES_256"
    },
    "responseElements": null,
    "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
    "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
    "readOnly": true,
    "resources": [{
        "accountId": "111122223333",
        "type": "AWS::KMS::Key",
        "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-9999999999999"
    }],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "35d58aa1-26b2-427a-908f-025bf71241f6",
    "eventCategory": "Management"
}
```

ReEncrypt

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AWSService",
        "invokedBy": "voiceid.amazonaws.com"
    },
    "eventTime": "2021-10-13T00:59:05Z",
    "eventSource": "kms.amazonaws.com",
    "eventName": "ReEncrypt",
    "awsRegion": "us-west-2",
    "sourceIPAddress": "voiceid.amazonaws.com",
    "userAgent": "voiceid.amazonaws.com",
    "requestParameters": {
        "destinationEncryptionContext": {
            "aws:voiceid:domain:arn": "arn:aws:voiceid:us-west-2:111122223333:domain/
sampleDomainId"
        },
        "destinationKeyId": "arn:aws:kms:us-
west-2:111122223333:key/44444444-3333-2222-1111-EXAMPLE11111",
        "sourceEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "sourceAAD": "SampleSourceAAAD+JXBmH+ZJNM73BfHE/dwQALXp7Sf44VwvoJOrLj",
        "destinationAAD": "SampleDestinationAAAD+JXBmH+ZJNM73BfHE/
dwQALXp7Sf44VwvoJOrLj",
        "sourceEncryptionContext": {
            "aws:voiceid:domain:arn": "arn:aws:voiceid:us-west-2:111122223333:domain/
sampleDomainId"
        },
        "destinationEncryptionAlgorithm": "SYMMETRIC_DEFAULT",
        "sourceKeyId": "arn:aws:kms:us-west-2:111122223333:key/55555555-3333-2222-1111-
EXAMPLE22222"
    },
    "responseElements": null,
    "requestID": "ed0fe4ab-305b-4388-8adf-7e8e3a4e80fe",
    "eventID": "31d0d7c6-ce5b-4caf-901f-025bf71241f6",
    "readOnly": true,
    "resources": [{
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-999999999999"
        },
        {
            "accountId": "111122223333",
            "type": "AWS::KMS::Key",
            "ARN": "arn:aws:kms:us-
west-2:111122223333:key/00000000-1111-2222-3333-777777777777"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "sharedEventID": "35d58aa1-26b2-427a-908f-025bf71241f6",
    "eventCategory": "Management"
}
```

High-volume outbound communications

For high-volume outbound communications, Amazon Pinpoint passes customer phone numbers and relevant attributes to Amazon Connect. On Amazon Connect, these are always encrypted at rest using either a customer managed key or an AWS owned key. The high-volume outbound communications data is segregated by the Amazon Connect instance ID and are encrypted by instance specific keys.

You can provide your own customer managed key when onboarding to high-volume outbound communications.

The service use this customer managed key to encrypt sensitive data at rest. The customer managed key is created, owned, and managed by you. You have full control over the customer managed key

If you do not provide your own customer managed key, then high-volume outbound communications encrypts sensitive data at rest using a AWS owned key specific to your Amazon Connect instance.

AWS KMS charges apply for a customer managed key. For more information about pricing, see AWS KMS pricing.

Encryption in transit

All data exchanged with Amazon Connect is protected in transit between the user's web browser and Amazon Connect using industry-standard TLS encryption. Which version of TLS? (p. 1129)

External data is additionally encrypted while being processed by AWS KMS.

When Amazon Connect integrates with AWS services, such as AWS Lambda, Amazon Kinesis, or Amazon Polly, data is always encrypted in transit using TLS.

When event data is forwarded from external applications to Amazon Connect it is always encrypted in transit using TLS.

Key management

You can specify AWS KMS keys, including bring your own keys (BYOK), to use for envelope encryption with Amazon S3 input/output buckets. This also applies to data used stored in Amazon Connect Customer Profiles.

Amazon Connect Wisdom stores knowledge documents that are encrypted at rest in S3 using a BYOK or a service-owned key. The knowledge documents are encrypted at rest in Amazon OpenSearch Service using a service-owned key. Wisdom stores agent queries and call transcripts using a BYOK or a service-owned key.

Amazon AppIntegrations doesn't support BYOK for encryption of configuration data. When syncing external application data, periodically you are required to BYOK. Amazon AppIntegrations requires a grant to use your customer managed key. When you create a data integration, Amazon AppIntegrations sends a `CreateGrant` request to AWS KMS on your behalf. You can revoke access to the grant, or remove the service's access to the customer managed key at any time. If you do, Amazon AppIntegrations won't be able to access any of the data encrypted by the customer managed key, which affects Amazon Connect services that are dependent on that data.

The knowledge documents used by Amazon Connect Wisdom are encrypted by an AWS KMS key.

For using Amazon Connect Voice ID, it is mandatory to provide a customer managed key KMS key (BYOK) while creating a Amazon Connect Voice ID domain, which is used to encrypt all the customer data at rest.

High-volume outbound communications encrypts all sensitive data using an AWS owned key or a customer managed key. As the customer managed key is created, owned, and managed by the you, you have full control over the customer managed key (AWS KMS charges apply).

For information about AWS KMS keys see What is AWS Key Management Service? in the *AWS Key Management Service Developer Guide*.

Amazon Connect and interface VPC endpoints (AWS PrivateLink)

You can establish a private connection between your VPC and a subset of endpoints in Amazon Connect by creating an interface VPC endpoint. Following are the supported endpoints:

- Amazon AppIntegrations
- Customer Profiles
- High-volume outbound communications
- Voice ID
- Wisdom

The core Amazon Connect service does not support AWS PrivateLink or VPC endpoints.

Interface endpoints are powered by AWS PrivateLink, a technology that enables you to privately access Amazon Connect APIs without an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection. Instances in your VPC don't need public IP addresses to communicate with the Amazon Connect APIs that integrate with AWS PrivateLink.

For more information, see the AWS PrivateLink Guide.

Creating an interface VPC endpoint for Amazon Connect

You can create an interface endpoint using either the Amazon VPC console or the AWS Command Line Interface (AWS CLI). For more information, see Create an interface endpoint in the *AWS PrivateLink Guide*.

Amazon Connect supports the following service names:

- com.amazonaws.*region*.app-integrations
- com.amazonaws.*region*.profile
- com.amazonaws.*region*.connect-campaigns
- com.amazonaws.*region*.voiceid
- com.amazonaws.*region*.wisdom

If you enable private DNS for an interface endpoint, you can make API requests to Amazon Connect using the default DNS name for the Region. For example, voiceid.us-east-1.amazonaws.com. For more information, see DNS hostnames in the *AWS PrivateLink Guide*.

Creating a VPC endpoint policy

You can attach an endpoint policy to your VPC endpoint that controls access. The policy specifies the following information:

- The principal that can perform actions.
- The actions that can be performed.
- The resources on which actions can be performed.

For more information, see Control access to services using endpoint policies in the *AWS PrivateLink Guide*.

Example: VPC endpoint policy

The following VPC endpoint policy grants access to the listed Amazon Connect Voice ID actions for all principals on all resources.

```
{
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                "voiceid:CreateDomain",
                "voiceid:EvaluateSession",
                "voiceid:ListSpeakers"
            ],
            "Resource":"*",
            "Principal":"*"
        }
    ]
}
```

Following is another example. In this one, the VPC endpoint policy grants access to the listed high-volume outbound communications actions for all principals on all resources.

```
{
    "Statement":[
        {
            "Effect":"Allow",
            "Action":[
                 "connect-campaigns:CreateCampaign",
                "connect-campaigns:DeleteCampaign",
                "connect-campaigns:ListCampaigns"
            ],
            "Resource":"*",
            "Principal":"*"
        }
    ]
}
```

Identity and access management for Amazon Connect

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be *authenticated* (signed in) and *authorized* (have permissions) to use Amazon Connect resources. IAM is an AWS service that you can use with no additional charge.

Topics

Audience

How you use AWS Identity and Access Management (IAM) differs, depending on the work that you do in Amazon Connect.

Service user – If you use the Amazon Connect service to do your job, then your administrator provides you with the credentials and permissions that you need. As you use more Amazon Connect features to do your work, you might need additional permissions. Understanding how access is managed can help you request the right permissions from your administrator. If you cannot access a feature in Amazon Connect, see Troubleshooting Amazon Connect identity and access (p. 1118).

Service administrator – If you're in charge of Amazon Connect resources at your company, you probably have full access to Amazon Connect. It's your job to determine which Amazon Connect features and resources your employees should access. You must then submit requests to your IAM administrator to change the permissions of your service users. Review the information on this page to understand the basic concepts of IAM. To learn more about how your company can use IAM with Amazon Connect, see How Amazon Connect works with IAM (p. 1098).

IAM administrator – If you're an IAM administrator, you might want to learn details about how you can write policies to manage access to Amazon Connect. To view example Amazon Connect identity-based policies that you can use in IAM, see Amazon Connect identity-based policy examples (p. 1101).

Authenticating with identities

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see Signing in to the AWS Management Console as an IAM user or root user in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 signing process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing access keys for IAM users in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

An *IAM group* is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see When to create an IAM user (instead of a role) in the *IAM User Guide*.

IAM roles

An *IAM role* is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by switching roles. You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see Using IAM roles in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated users and roles in the *IAM User Guide*.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
  - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see Actions, Resources, and Condition Keys for Amazon Connect in the *Service Authorization Reference*.
  - **Service role** – A service role is an IAM role that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see Creating a role to delegate permissions to an AWS service in the *IAM User Guide*.
  - **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.
- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see Using an IAM role to grant permissions to applications running on Amazon EC2 instances in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see When to create an IAM role (instead of a user) in the *IAM User Guide*.

Managing access using policies

You control access in AWS by creating policies and attaching them to IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see Overview of JSON policies in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as an IAM user, group of users, or role. These policies control what actions users and roles can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see Creating IAM policies in the *IAM User Guide*.

Identity-based policies can be further categorized as *inline policies* or *managed policies*. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see Choosing between managed policies and inline policies in the *IAM User Guide*.

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified principal can perform on that resource and under what conditions. You must specify a principal in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see Permissions boundaries for IAM entities in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see How SCPs work in the *AWS Organizations User Guide*.

- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see Session policies in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see Policy evaluation logic in the *IAM User Guide*.

Required permissions for using custom IAM policies to manage access to the Amazon Connect console

If you're using custom IAM policies to manage access to the Amazon Connect console, your users need some or all of the permissions listed in this article, depending on the tasks they need to do.

> **Note**
> Using **connect:*** in a custom IAM policy grants your users all of the Amazon Connect permissions listed in this article.

> **Note**
> Certain pages on the Amazon Connect console, such as Tasks (p. 1090) and Customer Profiles (p. 1092), require that you add permissions to your inline policies.

AmazonConnect_FullAccess policy

To allow full read/write access to Amazon Connect, you must attach two policies to your IAM users, groups, or roles. Attach the **AmazonConnect_FullAccess** policy and a custom policy with the following contents:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AttachAnyPolicyToAmazonConnectRole",
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
        }
    ]
}
```

To allow an IAM user to create an instance, ensure that they have the permissions granted by the AmazonConnect_FullAccess policy.

When you use AmazonConnect_FullAccess policy, note the following:

- Additional privileges are required to create a Amazon S3 bucket with a name of your choosing, or use an existing bucket while creating or updating an instance from the Amazon Connect console. If you choose default storage locations for your call recordings, chat transcripts, call transcripts, etc, they are now prefixed with "amazon-connect-".
- The aws/connect KMS key is available to use as a default encryption option. To use a custom encryption key, assign users additional KMS privileges.

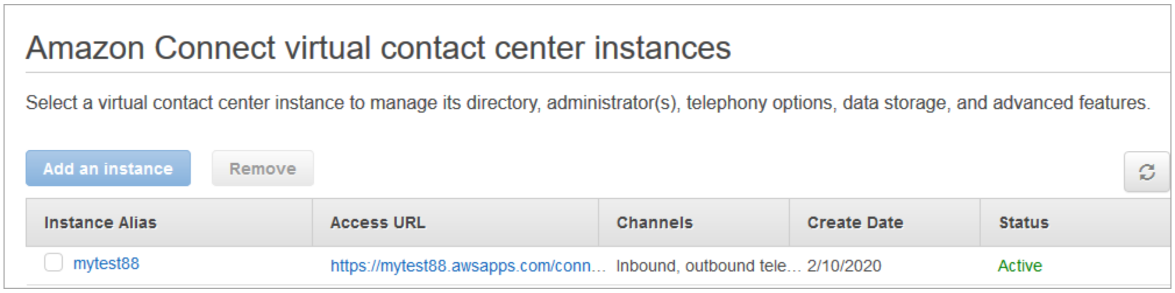
- Assign users additional privileges to attach other AWS resources like Amazon Polly, Live Media Streaming, Data Streaming, and Lex bots to their Amazon Connect instances.

AmazonConnectReadOnlyAccess policy

To allow read-only access, you need to attach only the **AmazonConnectReadOnlyAccess** policy.

Amazon Connect console home page

The following image shows a sample Amazon Connect console home page.



Amazon Connect virtual contact center instances

Select a virtual contact center instance to manage its directory, administrator(s), telephony options, data storage, and advanced features.

Instance Alias	Access URL	Channels	Create Date	Status
□ mytest88	https://mytest88.awsapps.com/conn…	Inbound, outbound tele…	2/10/2020	Active

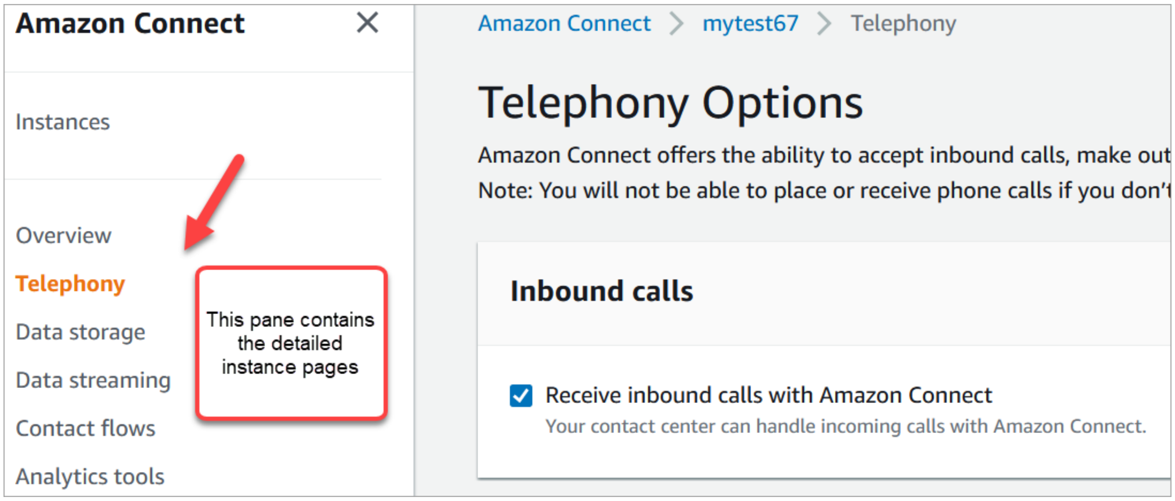
Use the permissions listed in the following table to manage access to this page.

Action/Use case	Permissions needed
List instance	connect:ListInstances ds:DescribeDirectories
Describe instance: View the details of the instance/ current settings	connect:DescribeInstance connect:ListLambdaFunctions connect:ListLexBots connect:ListInstanceStorageConfigs connect:ListApprovedOrigins connect:ListSecurityKeys connect:DescribeInstanceAttributes connect:DescribeInstanceStorageConfig ds:DescribeDirectories
Create instance	connect:CreateInstance connect:DescribeInstance connect:ListInstances connect:AssociateInstanceStorageConfig connect:UpdateInstanceAttribute ds:CheckAlias

Action/Use case	Permissions needed
	ds:CreateAlias ds:AuthorizeApplication ds:UnauthorizeApplication ds:CreateIdentityPoolDirectory ds:CreateDirectory ds:DescribeDirectories iam:CreateServiceLinkedRole kms:CreateGrant kms:DescribeKey kms:ListAliases kms:RetireGrant logs:CreateLogGroup s3:CreateBucket s3:GetBucketLocation s3:ListAllMyBuckets servicequotas:GetServiceQuota profile:ListAccountIntegrations profile:GetDomain profile:ListDomains profile:GetProfileObjectType profile:ListProfileObjectTypeTemplates
Delete instance	connect:DescribeInstance connect:DeleteInstance connect:ListInstances ds:DescribeDirectories ds:DeleteDirectory ds:UnauthorizeApplication

Detailed instance pages

The following image shows how you navigate to each of the detailed instance pages:


Amazon Connect
Instances
Overview
Telephony
Data storage
Data streaming
Contact flows
Analytics tools
This pane contains the detailed instance pages
Amazon Connect > mytest67 > Telephony
Telephony Options
Amazon Connect offers the ability to accept inbound calls, make out
Note: You will not be able to place or receive phone calls if you don't
Inbound calls
☑ Receive inbound calls with Amazon Connect
Your contact center can handle incoming calls with Amazon Connect.

To access the detailed instance pages, you need permissions to the Amazon Connect console home page (describe/list). Or, use the **AmazonConnectReadOnlyAccess** policy.

The following tables list the granular permissions for each detailed instance page.

> **Note**
> To perform **Edit** actions, users also need **List** and **Describe** permissions.

Overview page

Action/Use case	Permissions needed
Create service-linked role	connect:DescribeInstance connect:ListInstances connect:DescribeInstanceAttribute connect:UpdateInstanceAttribute connect:ListIntegrationAssociations profile:ListAccountIntegrations ds:DescribeDirectories iam:CreateServiceLinkedRole iam:PutRolePolicy

Telephony page

Action/Use case	Permissions needed
View telephony options	connect:DescribeInstance
Enable/Disable telephony options	connect:UpdateInstanceAttribute
View high-volume outbound communications	connect-campaigns:GetConnectInstanceConfig

Action/Use case	Permissions needed
	connect-campaigns:GetInstanceOnboardingJobStatus connect:DescribeInstance connect:DescribeInstanceAttribute kms:DescribeKey
Enable/disable high-volume outbound communications	connect-campaigns:GetConnectInstanceConfig connect-campaigns:GetInstanceOnboardingJobStatus connect-campaigns:StartInstanceOnboardingJob connect-campaigns:DeleteInstanceOnboardingJob connect-campaigns:DeleteConnectInstanceConfig connect:DescribeInstance connect:DescribeInstanceAttribute connect:UpdateInstanceAttribute iam:CreateServiceLinkedRole iam:DeleteServiceLinkedRole iam:AttachRolePolicy iam:PutRolePolicy iam:DeleteRolePolicy events:PutRule events:PutTargets events:DeleteRule events:RemoveTargets events:DescribeRule events:ListTargetsByRule ds:DescribeDirectories kms:DescribeKey kms:ListKeys kms:CreateGrant kms:RetireGrant

Data storage page

Call recording section

Action/Use case	Permissions needed
View call recording	connect:DescribeInstance connect:ListInstanceStorageConfigs connect:DescribeInstanceStorageConfig
Edit call recording	connect:AssociateInstanceStorageConfig connect:UpdateInstanceStorageConfig connect:DisassociateInstanceStorageConfig s3:ListAllMyBuckets s3:GetBucketLocation s3:GetBucketAcl s3:CreateBucket kms:CreateGrant kms:DescribeKey kms:ListAliases kms:RetireGrant

Chat transcripts section

Action/Use case	Permissions needed
View chat transcripts	connect:DescribeInstance connect:DescribeInstanceStorageConfig connect:ListInstanceStorageConfigs
Edit chat transcripts	connect:AssociateInstanceStorageConfig connect:UpdateInstanceStorageConfig connect:DisassociateInstanceStorageConfig s3:ListAllMyBuckets s3:GetBucketLocation s3:GetBucketAcl s3:CreateBucket kms:CreateGrant

Action/Use case	Permissions needed
	kms:DescribeKey kms:ListAliases kms:RetireGrant

Attachments section

Action/Use case	Permissions needed
View chat attachments	connect:DescribeInstance connect:DescribeInstanceStorageConfig connect:ListInstanceStorageConfigs
Edit chat attachments	connect:AssociateInstanceStorageConfig connect:UpdateInstanceStorageConfig connect:DisassociateInstanceStorageConfig s3:ListAllMyBuckets s3:GetBucketLocation s3:CreateBucket s3:GetBucketAcl kms:CreateGrant kms:DescribeKey kms:ListAliases kms:RetireGrant

Live media streaming section

Action/Use case	Permissions needed
View live media streaming	connect:DescribeInstance connect:ListInstanceStorageConfigs connect:DescribeInstanceStorageConfig
Edit live media streaming	connect:AssociateInstanceStorageConfig connect:UpdateInstanceStorageConfig connect:DisassociateInstanceStorageConfig kms:CreateGrant

Action/Use case	Permissions needed
	kms:DescribeKey kms:RetireGrant

Exported reports section

Action/Use case	Permissions needed
View exported reports	connect:DescribeInstance connect:ListInstanceStorageConfigs connect:DescribeInstanceStorageConfig
Edit exported reports	connect:AssociateInstanceStorageConfig connect:UpdateInstanceStorageConfig connect: DisassociateInstanceStorageConfig s3:ListAllMyBuckets s3:GetBucketLocation s3:CreateBucket kms:DescribeKey kms:ListAliases kms:RetireGrant kms:CreateGrant

Data streaming page

Contact records section

Action/Use case	Permissions needed
View data streaming - Contact records	connect:DescribeInstance connect:ListInstanceStorageConfigs connect:DescribeInstanceStorageConfig
Edit contact record	connect:AssociateInstanceStorageConfig connect:UpdateInstanceStorageConfig connect:DisassociateInstanceStorageConfig firehose:ListDeliveryStreams firehose:DescribeDeliveryStream

Action/Use case	Permissions needed
	kinesis:ListStreams kinesis:DescribeStream

Agent events section

Action/Use case	Permissions needed
View data streaming - Agent events	connect:DescribeInstance connect:ListInstanceStorageConfigs connect:DescribeInstanceStorageConfig
Edit agent events	connect:AssociateInstanceStorageConfig connect:UpdateInstanceStorageConfig connect:DisassociateInstanceStorageConfig kinesis:ListStreams kinesis: DescribeStream

Application integration page

Action/Use case	Permissions needed
View approved origins	connect:DescribeInstance connect:ListApprovedOrigins
Edit approved origins	connect: AssociateApprovedOrigin connect:ListApprovedOrigins connect:DisassociateApprovedOrigin

Tasks page

Action/Use case	Permissions needed
View Tasks integrations	app-integrations:GetEventIntegration connect:ListIntegrationAssociations
Edit Tasks integrations	app-integrations:CreateEventIntegration app-integrations:GetEventIntegration app-integrations:ListEventIntegrations app-integrations:DeleteEventIntegrationAssociation

Action/Use case	Permissions needed
	app-integrations:CreateEventIntegrationAssociation appflow:CreateFlow appflow:CreateConnectorProfile appflow:DescribeFlow appflow:DeleteFlow appflow:DeleteConnectorProfile appflow:DescribeConnectorEntity appflow:ListFlows appflow:ListConnectorEntities appflow:StartFlow connect:ListIntegrationAssociations connect:DeleteIntegrationAssociation connect:ListUseCases connect:DeleteUseCase events:ActivateEventSource events:CreateEventBus events:DescribeEventBus events:DescribeEventSource events:ListEventSources events:ListTargetsByRule events:PutRule events:PutTargets events:DeleteRule events:RemoveTargets kms:CreateGrant kms:DescribeKey kms:ListAliases kms:ListKeys kms:ListGrants

Customer profiles page

Action/Use case	Permissions needed
View customer profiles	appflow:DescribeFlow appflow:DescribeConnectorEntity appflow:ListFlows appflow:ListConnectorEntities appflow:ListConnectorProfiles kms:ListKeys profile:ListDomains profile:ListAccountIntegrations sqs:ListQueues
Edit customer profiles	appflow:CreateFlow appflow:CreateConnectorProfile appflow:DescribeFlow appflow:DeleteFlow appflow:DescribeConnectorEntity appflow:ListFlows appflow:ListConnectorEntities appflow:ListConnectorProfiles appflow:StartFlow appflow:StopFlow kms:ListKeys profile:CreateDomain profile:DeleteIntegration profile:DeleteDomain profile:ListDomains profile:ListAccountIntegrations profile:PutIntegration profile:UpdateDomain kms:ListGrants kms:DescribeKey

Action/Use case	Permissions needed
	kms:ListAliases kms:ListKeys sqs:ListQueues

Voice ID page

Action/Use case	Permissions needed
View Voice ID integrations	voiceid:DescribeDomain voiceid:ListDomains voiceid:RegisterComplianceConsent voiceid:DescribeComplianceConsent connect:ListIntegrationAssociations
Edit Voice ID integrations	voiceid:DescribeDomain voiceid:ListDomains voiceid:RegisterComplianceConsent voiceid:DescribeComplianceConsent voiceid:UpdateDomain voiceid:CreateDomain connect:ListIntegrationAssociations connect:CreateIntegrationAssociation connect:DeleteIntegrationAssociation events:PutRule events:DeleteRule events:PutTargets events:RemoveTargets

Contact flows page

Contact flows security keys section

Action/Use case	Permissions needed
View contact flow security keys	connect:DescribeInstance connect:ListSecurityKeys

Action/Use case	Permissions needed
Add/remove contact flow security keys	connect:AssociateSecurityKey connect:DisassociateSecurityKey

Lex bots section

Action/Use case	Permissions needed
View Lex bots	connect:ListLexBots connect:ListBots
Add/remove Lex bots	lex:GetBots lex:GetBot lex:CreateResourcePolicy lex:DeleteResourcePolicy lex:UpdateResourcePolicy lex:DescribeBotAlias lex:ListBotAliases lex:ListBots connect:AssociateBot connect:DisassociateBot connect:ListBots connect:AssociateLexBot connect:DisassociateLexBot connect:ListLexBots

Lambda functions section

Action/Use case	Permissions needed
View Lambda functions	connect:ListLambdaFunctions
Add/remove Lambda functions	connect:ListLambdaFunctions connect:AssociateLambdaFunction connect:DisassociateLambdaFunction lambda:ListFunctions lambda:AddPermission

Action/Use case	Permissions needed
	lambda:RemovePermission

Contact flow logs section

Action/Use case	Permissions needed
View contact flow log config	connect:DescribeInstance connect:DescribeInstanceAttribute
Enable/disable contact flow log	logs:CreateLogGroup

Amazon Polly section

Action/Use case	Permissions needed
View Amazon Polly option	connect:DescribeInstance connect:DescribeInstanceAttribute
Update Amazon Polly option	connect:UpdateInstanceAttribute

Federations

SAML federation

Action/Use case	Permissions needed
SAML federation	connect:GetFederationToken

Admin/Emergency federation

Action/Use case	Permissions needed
Admin/Emergency federation	connect:GetFederationTokens

Restrict AWS resources that can be associated with Amazon Connect

Each Amazon Connect instance is associated with an IAM service-linked role when the instance is created. Amazon Connect can integrate with other AWS services for use cases such as call recording storage (Amazon S3 bucket), natural language bots (Amazon Lex bots), and data streaming (Amazon Kinesis Data Streams). Amazon Connect assumes the service-linked role to interact with these other services. The policy is first added to the service-linked role as part of corresponding APIs on the Amazon Connect service (that are in turn called by the AWS console). For example, if you want to use a certain Amazon S3 bucket with your Amazon Connect instance, the bucket must be passed to the AssociateInstanceStorageConfig API.

For the set of IAM actions defined by Amazon Connect, see Actions defined by Amazon Connect.

Following are some examples of how to restrict access to other resources that may be associated with an Amazon Connect instance. They should be applied to the IAM User or Role that is interacting with Amazon Connect APIs or the Amazon Connect console.

> **Note**
>
> A policy with an explicit `Deny` would override the `Allow` policy in these examples.

For more information about what resources, condition keys, and dependent APIs you can use to restrict access, see Actions, resources, and condition keys for Amazon Connect.

Example 1: Restrict which Amazon S3 buckets can be associated with an Amazon Connect instance

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "connect:UpdateInstanceStorageConfig",
        "connect:AssociateInstanceStorageConfig"
      ],
      "Resource": "arn:aws:connect:region:account-id:instance/instance-id",
      "Condition": {
        "StringEquals": {
          "connect:StorageResourceType": "CALL_RECORDINGS"
        }
      }
    },
    {
      "Sid": "VisualEditor1",
      "Effect": "Allow",
      "Action": [
        "iam:PutRolePolicy",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation"
      ],
      "Resource": [
        "arn:aws:iam::account-id:role/aws-service-role/connect.amazonaws.com/*",
        "arn:aws:s3:::s3-bucket-name"
      ]
    },
    {
      "Sid": "VisualEditor2",
      "Effect": "Allow",
      "Action": "s3:ListAllMyBuckets",
      "Resource": "*"
    }
  ]
}
```

This example allows an IAM principal to associate an Amazon S3 bucket for call recordings for the given Amazon Connect instance ARN, and a specific Amazon S3 bucket named `my-connect-recording-bucket`. The `AttachRolePolicy` and `PutRolePolicy` actions are scoped to the Amazon Connect service-linked role (a wildcard is used in this example, but you can provide the role ARN for the instance if needed).

Note

To use an AWS KMS key to encrypt recordings in this bucket, an additional policy is needed.

Example 2: Restrict which AWS Lambda functions can be associated with an Amazon Connect instance

AWS Lambda functions are associated with an Amazon Connect instance, but the Amazon Connect service-linked role is not used to invoke them, and so is not modified. Instead, a policy is added to the function through the `lambda:AddPermission` API that allows the given Amazon Connect instance to invoke the function.

To restrict which functions can be associated with an Amazon Connect instance, you specify the Lambda function ARN that a user can use to invoke `lambda:AddPermission`:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "connect:AssociateLambdaFunction",
                "lambda:AddPermission"
            ],
            "Resource": [
                "arn:aws:connect:region:account-id:instance/instance-id",
                "arn:aws:lambda:*:*:function:my-function"
            ]
        }
    ]
}
```

Example 3: Restrict which Amazon Kinesis Data Streams can be associated with an Amazon Connect instance

This example follows a similar model to the Amazon S3 example. It restricts which specific Kinesis Data Streams may be associated with a given Amazon Connect instance for delivering contact records.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "connect:UpdateInstanceStorageConfig",
                "connect:AssociateInstanceStorageConfig"
            ],
            "Resource": "arn:aws:connect:region:account-id:instance/instance-id",
            "Condition": {
                "StringEquals": {
                    "connect:StorageResourceType": "CONTACT_TRACE_RECORDS"
                }
            }
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "kinesis:DescribeStream",
                "iam:PutRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::account-id:role/aws-service-role/connect.amazonaws.com/*",
                "arn:aws:kinesis:*:account-id:stream/stream-name"
            ]
        },
        {
            "Sid": "VisualEditor2",
            "Effect": "Allow",
            "Action":  "kinesis:ListStreams",
            "Resource": "*"
        }
    ]
}
```

How Amazon Connect works with IAM

Before you use IAM to manage access to Amazon Connect, you should understand what IAM features are available to use with Amazon Connect. To get a high-level view of how Amazon Connect and other AWS services work with IAM, see AWS Services That Work with IAM in the *IAM User Guide*.

Topics

Amazon Connect identity-based policies

With IAM identity-based policies, you can specify allowed or denied actions and resources as well as the conditions under which actions are allowed or denied. Amazon Connect supports specific actions, resources, and condition keys. To learn about all of the elements that you use in a JSON policy, see IAM JSON Policy Elements Reference in the *IAM User Guide*.

Actions

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Action` element of a JSON policy describes the actions that you can use to allow or deny access in a policy. Policy actions usually have the same name as the associated AWS API operation. There are some exceptions, such as *permission-only actions* that don't have a matching API operation. There are also some operations that require multiple actions in a policy. These additional actions are called *dependent actions*.

Include actions in a policy to grant permissions to perform the associated operation.

Policy actions in Amazon Connect use the following prefix before the action: `connect:`. Policy statements must include either an `Action` or `NotAction` element. Amazon Connect defines its own set of actions that describe tasks that you can perform with this service.

To specify multiple actions in a single statement, separate them with commas as follows:

```
"Action": [
      "connect:action1",
      "connect:action2"
```

You can specify multiple actions using wildcards (*). For example, to specify all actions that begin with the word `Describe`, include the following action:

```
"Action": "connect:Describe*"
```

To see a list of Amazon Connect actions, Actions, Resources, and Condition Keys for Amazon Connect.

Resources

Amazon Connect supports resource-level permissions (specifying a resource ARN in an IAM policy). Following is a list of Amazon Connect resources:

- Instance
- Contact
- User
- Routing profile
- Security profile
- Hierarchy group
- Queue
- Contact flow
- Hours of operation
- Phone number
- Task templates
- Customer profile domain
- Customer profile object type
- High-volume outbound campaigns

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Resource` JSON policy element specifies the object or objects to which the action applies. Statements must include either a `Resource` or a `NotResource` element. As a best practice, specify a resource using its Amazon Resource Name (ARN). You can do this for actions that support a specific resource type, known as *resource-level permissions*.

For actions that don't support resource-level permissions, such as listing operations, use a wildcard (*) to indicate that the statement applies to all resources.

```
"Resource": "*"
```

The Amazon Connect instance resource has the following ARN:

```
arn:${Partition}:connect:${Region}:${Account}:instance/${InstanceId}
```

For more information about the format of ARNs, see Amazon Resource Names (ARNs) and AWS Service Namespaces.

For example, to specify the `i-1234567890abcdef0` instance in your statement, use the following ARN:

```
"Resource": "arn:aws:connect:us-east-1:123456789012:instance/i-1234567890abcdef0"
```

To specify all instances that belong to a specific account, use the wildcard (*):

```
"Resource": "arn:aws:connect:us-east-1:123456789012:instance/*"
```

Some Amazon Connect actions, such as those for creating resources, cannot be performed on a specific resource. In those cases, you must use the wildcard (*).

```
"Resource": "*"
```

Many Amazon Connect; API actions involve multiple resources. For example,

To specify multiple resources in a single statement, separate the ARNs with commas.

```
"Resource": [
      "resource1",
      "resource2"
```

To see a list of Amazon Connect resource types and their ARNs, see Actions, Resources, and Condition Keys for Amazon Connect. The same article explains with which actions you can specify the ARN of each resource.

Condition keys

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

The `Condition` element (or `Condition` *block*) lets you specify conditions in which a statement is in effect. The `Condition` element is optional. You can create conditional expressions that use condition operators, such as equals or less than, to match the condition in the policy with values in the request.

If you specify multiple `Condition` elements in a statement, or multiple keys in a single `Condition` element, AWS evaluates them using a logical `AND` operation. If you specify multiple values for a single condition key, AWS evaluates the condition using a logical `OR` operation. All of the conditions must be met before the statement's permissions are granted.

You can also use placeholder variables when you specify conditions. For example, you can grant an IAM user permission to access a resource only if it is tagged with their IAM user name. For more information, see IAM policy elements: variables and tags in the *IAM User Guide*.

AWS supports global condition keys and service-specific condition keys. To see all AWS global condition keys, see AWS global condition context keys in the *IAM User Guide*.

Amazon Connect defines its own set of condition keys and also supports using some global condition keys. To see all AWS global condition keys, see AWS Global Condition Context Keys in the *IAM User Guide*.

All Amazon EC2 actions support the `aws:RequestedRegion` and `ec2:Region` condition keys. For more information, see Example: Restricting Access to a Specific Region.

To see a list of Amazon Connect condition keys, see Actions, Resources, and Condition Keys for Amazon Connect.

Examples

To view examples of Amazon Connect identity-based policies, see Amazon Connect identity-based policy examples (p. 1101).

Authorization based on Amazon Connect tags

You can attach tags to Amazon Connect resources or pass tags in a request to Amazon Connect. To control access based on tags, you provide tag information in the condition element of a policy using the `connect:ResourceTag/key-name`, `aws:RequestTag/key-name`, or `aws:TagKeys` condition keys.

To view an example identity-based policy for limiting access to a resource based on the tags on that resource, see Describe and update Amazon Connect users based on tags (p. 1104).

Amazon Connect IAM roles

An IAM role is an entity within your AWS account that has specific permissions.

Using temporary credentials with Amazon Connect

You can use temporary credentials to sign in with federation, assume an IAM role, or to assume a cross-account role. You obtain temporary security credentials by calling AWS STS API operations such as AssumeRole or GetFederationToken.

Amazon Connect supports using temporary credentials.

Service-linked roles

Service-linked roles allow AWS services to access resources in other services to complete an action on your behalf. Service-linked roles appear in your IAM account and are owned by the service. An IAM administrator can view but not edit the permissions for service-linked roles.

Amazon Connect supports service-linked roles. For details about creating or managing Amazon Connect service-linked roles, see Use service-linked roles for Amazon Connect (p. 1120).

Choosing an IAM role in Amazon Connect

When you create a resource in Amazon Connect, you must choose a role to allow Amazon Connect to access Amazon EC2 on your behalf. If you have previously created a service role or service-linked role, then Amazon Connect provides you with a list of roles to choose from. It's important to choose a role that allows access to start and stop Amazon EC2 instances.

Amazon Connect identity-based policy examples

By default, IAM users and roles don't have permission to create or modify Amazon Connect resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to perform specific API operations on the specified resources they need. The administrator must then attach those policies to the IAM users or groups that require those permissions.

To learn how to create an IAM identity-based policy using these example JSON policy documents, see Creating Policies on the JSON Tab in the *IAM User Guide*.

Topics

- Create and view Amazon Connect Wisdom Assistants (p. 1105)
- Manage high-volume outbound communications resources (p. 1105)

Policy best practices

Identity-based policies are very powerful. They determine whether someone can create, access, or delete Amazon Connect resources in your account. These actions can incur costs for your AWS account. When you create or edit identity-based policies, follow these guidelines and recommendations:

- **Get started using AWS managed policies** – To start using Amazon Connect quickly, use AWS managed policies to give your employees the permissions they need. These policies are already available in your account and are maintained and updated by AWS. For more information, see Get started using permissions with AWS managed policies in the *IAM User Guide*.
- **Grant least privilege** – When you create custom policies, grant only the permissions required to perform a task. Start with a minimum set of permissions and grant additional permissions as necessary. Doing so is more secure than starting with permissions that are too lenient and then trying to tighten them later. For more information, see Grant least privilege in the *IAM User Guide*.
- **Enable MFA for sensitive operations** – For extra security, require IAM users to use multi-factor authentication (MFA) to access sensitive resources or API operations. For more information, see Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.
- **Use policy conditions for extra security** – To the extent that it's practical, define the conditions under which your identity-based policies allow access to a resource. For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also write conditions to allow requests only within a specified date or time range, or to require the use of SSL or MFA. For more information, see IAM JSON policy elements: Condition in the *IAM User Guide*.

Allow IAM users to view their own permissions

This example shows how you might create a policy that allows IAM users to view the inline and managed policies that are attached to their user identity. This policy includes permissions to complete this action on the console or programmatically using the AWS CLI or AWS API.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Grant "View User" permissions

When you create an IAM user or group in your AWS account, you can associate an IAM policy with that group or user, which specifies the permissions that you want to grant.

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

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

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

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

Allow IAM users to integrate with external applications

This example shows how you might create a policy that allows IAM users to interact with their external application integrations.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllAppIntegrationsActions",
            "Effect": "Allow",
            "Action": [
                "app-integrations:ListEventIntegrations",
                "app-integrations:CreateEventIntegration",
                "app-integrations:GetEventIntegration",
                "app-integrations:UpdateEventIntegration",
                "app-integartions:DeleteEventIntegration",
                "app-integrations:ListDataIntegrations",
                "app-integrations:CreateDataIntegration",
                "app-integrations:GetDataIntegration",
                "app-integrations:UpdateDataIntegration",
                "app-integartions:DeleteDataIntegration"
            ],
            "Resource": "*"
 }
 ]
}
```

Describe and update Amazon Connect users based on tags

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

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

The following sample policy allows the "describe" and "update" actions for users with specific tags.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "connect:DescribeUser",
                "connect: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.

Create Amazon Connect users based on tags

The following sample policy allows the create actions for users with specific request tags.

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

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

Create and view Amazon AppIntegrations resources

The following sample policy allows event integrations to be created, listed, and fetched.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "app-integrations:CreateEventIntegration",
                "app-integrations:GetEventIntegration",
                "app-integrations::ListEventIntegrations",
            ],
            "Resource": "*"
        }
    ]
}
```

Create and view Amazon Connect Wisdom Assistants

The following sample policy allows Wisdom assistants to be created, listed, fetched, and deleted.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wisdom:CreateAssistant",
                "wisdom:GetAssistant",
                "wisdom:ListAssistants",
                "wisdom:DeleteAssistant",
            ],
            "Resource": "*"
        }
    ]
}
```

Manage high-volume outbound communications resources

Onboarding permissions: The following sample policy allows Amazon Connect instances to be onboarded to high-volume outbound communications.

```
"Sid": "VisualEditor0",
             "Effect": "Allow",
             "Action": [
                 "kms:DescribeKey",
                 "kms:CreateGrant"
             ],
             "Resource": [
                 "arn:aws:kms:region:account-id:key/key-id"
                   ]
        },
        {
             "Sid": "VisualEditor1",
             "Effect": "Allow",
             "Action": [
                 "connect:DescribeInstance"
             ],
             "Resource": [

                 "arn:aws:connect:region:account-id:instance/instance-id"
             ]
        },
        {
             "Sid": "VisualEditor2",
             "Effect": "Allow",
             "Action": [
                 "events:PutTargets",
                 "events:PutRule",
                 "iam:CreateServiceLinkedRole",
                 "iam:AttachRolePolicy",
                 "iam:PutRolePolicy",
                 "ds:DescribeDirectories",
                 "connect-campaigns:StartInstanceOnboardingJob",
                 "connect-campaigns:GetConnectInstanceConfig",
                 "connect-campaigns:GetInstanceOnboardingJobStatus",
                 "connect-campaigns:DeleteInstanceOnboardingJob",
                 "connect:DescribeInstanceAttribute",
                 "connect:UpdateInstanceAttribute",
                 "connect:ListInstances",
                 "kms:ListAliases"
             ],
             "Resource": "*"
        }
```

To disable high-volume outbound communications for an instance, add the following permissions:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "kms:DescribeKey",
                "kms:RetireGrant"
            ],
            "Resource": [
                 "arn:aws:kms:region:account-id:key/key-id"
            ]
        },
        {
            "Sid": "VisualEditor1",
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:DescribeRule",
                "iam:DeleteRolePolicy",
                "events:ListTargetsByRule",
                "iam:DeleteServiceLinkedRole",
                "connect-campaigns:DeleteConnectInstanceConfig"
            ],
            "Resource": "*"
        }
    ]
```

Management permissions: The following sample policy allows all read and write operations on high-volume outbound campaigns.

```
{
    "Sid": "AllowConnectCampaignsOperations",
    "Effect": "Allow",
    "Action": [
        "connect-campaigns:CreateCampaign",
        "connect-campaigns:DeleteCampaign",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:UpdateCampaignName",
        "connect-campaigns:GetCampaignState"
        "connect-campaigns:UpdateOutboundCallConfig",
        "connect-campaigns:UpdateDialerConfig",
        "connect-campaigns:PauseCampaign",
        "connect-campaigns:ResumeCampaign",
        "connect-campaigns:StopCampaign",
        "connect-campaigns:GetCampaignStateBatch",
        "connect-campaigns:ListCampaigns"
    ],
    "Resource": "*"
}
```

ReadOnly permissions: The following sample policy allows read-only access to the campaigns.

```
{
    "Sid": "AllowConnectCampaignsReadOnlyOperations",
    "Effect": "Allow",
    "Action": [
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:GetCampaignState",
        "connect-campaigns:GetCampaignStateBatch",
        "connect-campaigns:ListCampaigns"
     ],
    "Resource": "*",
}
```

Tag-based permissions: The following sample policy restricts access to the campaigns integrated with a particular Amazon Connect instance using tags. More permissions can be added based on the use case.

```
{
    "Sid": "AllowConnectCampaignsOperations",
    "Effect": "Allow",
    "Action": [
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:GetCampaignState"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
             "aws:ResourceTag/owner":
 "arn:aws:connect:region:customer_account_id:instance/connect_instance_id"
         }
    }
}
```

Note

`connect-campaigns:ListCampaigns` and `connect-campaigns:GetCampaignStateBatch` operations cannot be restricted by Tag.

Amazon Connect resource-level policy examples

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

Deny the "delete" and "update" actions

This following sample policy denies the "delete" and "update" actions for users in one Amazon Connect instance. It uses a wild card at the end of the Amazon Connect user ARN so that "delete user" and "update user" are denied on the full user ARN (that is, all Amazon Connect users in the provided instance, such as arn:aws:connect:us-east-1:123456789012:instance/00fbeee1-123e-111e-93e3-11111bfbfcc1/agent/00dtcddd1-123e-111e-93e3-11111bfbfcc1).

```
{
    "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/*"
        }
    ]
}
```

Allow actions for integrations with specific names

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowAllAppIntegrationsActions",
            "Effect": "Allow",
            "Action": [
                "app-integrations:ListEventIntegrations",
                "app-integrations:CreateEventIntegration",
                "app-integrations:GetEventIntegration",
                "app-integrations:UpdateEventIntegration",
                "app-integartions:DeleteEventIntegration"
            ],
"Resource":"arn:aws:appintegrations:*:*:event-integration/MyNamePrefix-*"
 }
    ]
}
```

Allow "create users" but deny if you're assigned to a specific security profile

The following sample policy allows "create users" but explicitly denies using arn:aws:connect:us-west-2:123456789012:instance/00fbeee1-123e-111e-93e3-11111bfbfcc1/security-profile/11dtcggg1-123e-111e-93e3-11111bfbfcc17 as the parameter for security profile in CreateUser request.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "connect:CreateUser"
```

```
             ],
            "Resource": "*",
        },
        {
            "Effect": "Deny",
            "Action": [
                "connect:CreateUser"
             ],
            "Resource": "arn:aws:connect:us-
west-2:123456789012:instance/00fbeee1-123e-111e-93e3-11111bfbfcc17/security-
profile/11dtcggg1-123e-111e-93e3-11111bfbfcc17",
        }
    ]
}
```

Allow recording actions on a contact

The following sample policy allows "start contact recording" on a contact in a specific instance. Since contactID is dynamic, * is used.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
          "connect:StartContactRecording"
      ],
      "Resource": "arn:aws:connect:us-west-2:accountID:instance/instanceId/contact/*",
      "Effect": "Allow"
    }
  ]
}
```

Set up a trusted relationship with *accountID*.

The following actions are defined for the recording APIs:

- "connect:StartContactRecording"
- "connect:StopContactRecording"
- "connect:SuspendContactRecording"
- "connect:ResumeContactRecording"

Allow more contact Actions in the same role

If the same role is used to calling other contact APIs, you can list the following contact actions:

- GetContactAttributes
- ListContactFlows
- StartChatContact
- StartOutboundVoiceContact
- StopContact
- UpdateContactAttributes

Or use a wildcard to allow all contact actions, for example: "connect:*"

Allow more resources

You can also use a wildcard to allow more resources. For example, here's how to allow all connect actions on all contact resources:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "connect:*"
            ],
            "Resource": "arn:aws:connect:us-west-2:accountID:instance/*/contact/*",
            "Effect": "Allow"
        }
    ]
}
```

View specific Amazon AppIntegrations resources

The following sample policy allows a specific event integrations to be fetched.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "app-integrations:GetEventIntegration"
            ],
            "Resource": "arn:aws:app-integrations:us-west-2:accountID:event-integration/
Name"
        }
    ]
}
```

Grant access to Amazon Connect Customer Profiles

Amazon Connect Customer Profiles use `profile` as the prefix for actions instead of `connect`. The following policy grants full access to a specific domain in Amazon Connect Customer Profiles.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
          "profile:*"
      ],
      "Resource": "arn:aws:profile:us-west-2:accountID:domains/domainName",
      "Effect": "Allow"
    }
  ]
}
```

Set up a trusted relationship with accountID to domain domainName.

Grant read-only access to Customer Profiles data

Following is an example for granting read access to the data in Amazon Connect Customer Profiles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "profile:SearchProfiles",
                "profile:ListObjects"
            ],
            "Resource": "arn:aws:profile:us-west-2:accountID:domains/domainName",
            "Effect": "Allow"
        }
    ]
}
```

Query Amazon Connect Wisdom only for a specific Assistant

The following sample policy allows querying only a specific Assistant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "wisdom:QueryAssistant "
            ],
            "Resource": "arn:aws:wisdom:us-west-2:accountID:assistant/assistantID"
        }
    ]
}
```

Grant full access to Amazon Connect Voice ID

Amazon Connect Voice ID uses `voiceid` as the prefix for actions instead of connect. The following policy grants full access to a specific domain in Amazon Connect Voice ID:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
          "voiceid:*"
      ],
      "Resource": "arn:aws:voiceid:us-west-2:accountID:domain/domainName",
      "Effect": "Allow"
    }
  ]
}
```

Set up a trusted relationship with accountID to domain domainName.

Grant access to High-volume outbound communications resources

High-volume outbound communications uses `connect-campaign` as the prefix for actions instead of `connect`. The following policy grants full access to a specific high-volume outbound campaign.

```
{
    "Sid": "AllowConnectCampaignsOperations",
    "Effect": "Allow",
    "Action": [
        "connect-campaigns:DeleteCampaign",
        "connect-campaigns:DescribeCampaign",
        "connect-campaigns:UpdateCampaignName",
        "connect-campaigns:GetCampaignState"
        "connect-campaigns:UpdateOutboundCallConfig",
        "connect-campaigns:UpdateDialerConfig",
        "connect-campaigns:PauseCampaign",
        "connect-campaigns:ResumeCampaign",
        "connect-campaigns:StopCampaign"
    ],
    "Resource": "arn:aws:connect-campaigns:us-west-2:accountID:campaign/campaignId",
    }
```

AWS managed policies for Amazon Connect

To add permissions to users, groups, and roles, it is more efficient to use AWS managed policies than to write policies yourself. It takes time and expertise to create IAM customer managed policies that provide your team with only the permissions that they need. To get started quickly, you can use AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see AWS managed policies in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the ReadOnlyAccess AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see AWS managed policies for job functions in the *IAM User Guide*.

AWS managed policy: AmazonConnect_FullAccess

To allow full read/write access to Amazon Connect, you must attach two policies to your IAM users, groups, or roles. Attach the `AmazonConnect_FullAccess` policy and a custom policy with the following contents:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AttachAnyPolicyToAmazonConnectRole",
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
        }
    ]
}
```

To allow an IAM user to create an instance, ensure that they have the permissions granted by the `AmazonConnect_FullAccess` policy.

When you use `AmazonConnect_FullAccess` policy, note the following:

- The `iam:PutRolePolicy` allows the user who gets that policy to configure any resource in the account to work with the Amazon Connect instance. Because it grants such broad permissions, only assign it when necessary. Instead, create the service-linked role with access to the necessary resources and let the user have access to pass the service-linked role to Amazon Connect (which is granted by the `AmazonConnect_FullAccess` policy).
- Additional privileges are required to create a Amazon S3 bucket with a name of your choosing, or use an existing bucket while creating or updating an instance from the Amazon Connect console. If you choose default storage locations for your call recordings, chat transcripts, call transcripts, etc, they are now prefixed with "amazon-connect-".
- The aws/connect KMS key is available to use as a default encryption option. To use a custom encryption key, assign users additional KMS privileges.
- Assign users additional privileges to attach other AWS resources like Amazon Polly, Live Media Streaming, Data Streaming, and Lex bots to their Amazon Connect instances.

For more information and detailed permissions, see Required permissions for using custom IAM policies to manage access to the Amazon Connect console (p. 1082).

AWS managed policy: AmazonConnectReadOnlyAccess

To allow read-only access, you need to attach only the `AmazonConnectReadOnlyAccess` policy.

AWS managed policy: AmazonConnectVoiceIDFullAccess

To allow full access to Amazon Connect Voice ID, you must attach two policies to your IAM users, groups, or roles. Attach the `AmazonConnectVoiceIDFullAccess` policy and the following custom policy contents to access Voice ID through the Amazon Connect console:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AttachAnyPolicyToAmazonConnectRole",
            "Effect": "Allow",
            "Action": "iam:PutRolePolicy",
            "Resource": "arn:aws:iam::*:role/aws-service-role/connect.amazonaws.com/
AWSServiceRoleForAmazonConnect*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "connect:CreateIntegrationAssociation",
                "connect:DeleteIntegrationAssociation",
                "connect:ListIntegrationAssociations"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "events:DeleteRule",
                "events:PutRule",
                "events:PutTargets",
                "events:RemoveTargets"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "events:ManagedBy": "connect.amazonaws.com"
                }
            }
        }
    ]
}
```

The manual policy configures the following:

- The `iam:PutRolePolicy` allows the user who gets that policy to configure any resource in the account to work with the Amazon Connect instance. Because it grants such broad permissions, only assign it when necessary.
- To attach a Voice ID domain with an Amazon Connect instance, you need additional Amazon Connect and Amazon EventBridge privileges. You need privileges to call Amazon Connect APIs to create, delete, and list integration associations. You need EventBridge permissions to create and delete EventBridge rules which are used to provide contact records related to Voice ID.

Since there is no default encryption option, to use your customer managed key with your Amazon Connect Voice ID, the following API operations must be permitted in the key policy. Also, you must add these permissions on the relevant key. They are not included in the managed policy.

- `kms:Decrypt` to access or store encrypted data.
- `kms:CreateGrant` – when creating or updating a domain, used to create a grant to the customer managed key for the Voice ID domain. The grant controls access to the specified KMS key which allows access to grant operations Amazon Connect Voice ID requires. For more information about using grants, see Using grants in the *AWS Key Management Service Developer Guide*.
- `kms:DescribeKey` – when creating or updating a domain, allows determining the ARN for KMS key you provided.

For more about creating domains and KMS keys, see Enable Voice ID (p. 862) and Encryption at rest (p. 1067).

Amazon Connect updates to AWS managed policies

View details about updates to AWS managed policies for Amazon Connect since this service began tracking these changes. For automatic alerts about changes to this page, subscribe to the RSS feed on the Amazon Connect Document history (p. 1258) page.

Change	Description	Date
AmazonConnectServiceLinkedRolePolicy (p. 1120) – Added actions for Amazon CloudWatch	Added the following action to publish usage Amazon Connect metrics for an instance to your account. • `cloudwatch:PutMetricData`	Februrary 22, 2022
AmazonConnect_FullAccess (p. 1112) – Added permissions for managing Amazon Connect Customer Profiles domains	Added all permissions for managing Amazon Connect Customer Profiles domains that are created for new Amazon Connect instances. • `profile:ListAccountIntegrations` - Lists all the integrations associated with a specific URI in the AWS account.	November 12, 2021

Change	Description	Date
	- `profile:ListDomains` - Returns a list of all the domains for an AWS account that have been created. - `profile:GetDomain` - Returns information about a specific domain. - `profile:ListProfileObjectTypeTemplates` - Allow the Amazon Connect console to display a list of templates that you can use to create your data mappings. - `profile:GetObjectTypes` - Allow you to view all the current Object Types (data mappings) that you've created. The following permissions are allowed to be performed on domains with a name that is prefixed with `amazon-connect-`: - `profile:AddProfileKey` - Allows you to associate a new key value with a specific profile - `profile:CreateDomain` - Allows you to create new domains - `profile:CreateProfile` - Allows you to create new profiles - `profile:DeleteDomain` - Allows you to delete domains - `profile:DeleteIntegration` - Allows you to delete integrations with a domain - `profile:DeleteProfile` - Allows you to delete a profile - `profile:DeleteProfileKey` - Allows you to delete a profile key - `profile:DeleteProfileObject` - Allows you to delete a profile object - `profile:DeleteProfileObjectType` - Allows you to delete a profile object type - `profile:GetIntegration` - Allows you to retrieve	

Change	Description	Date
	information about an integration • `profile:GetMatches` - Allows you to retrieve possible profile matches • `profile:GetProfileObjectType` - Allows you to retrieve profile object types • `profile:ListIntegrations` - Allows you to list integrations • `profile:ListProfileObjects` - Allows you to list profile objects • `profile:ListProfileObjectTypes` - Allows you to list profile object types • `profile:ListTagsForResource` - Allows you to list tags for a resource • `profile:MergeProfiles` - Allows you to merge profile matches • `profile:PutProfileObject` - Allows you to create and update objects • `profile:PutProfileObjectType` - Allows you to create and update object types • `profile:SearchProfiles` - Allows you to search profiles • `profile:TagResource` - Allows you to tag resources • `profile:UntagResource` - Allows you to untag resources • `profile:UpdateDomain` - Allows you to update domains • `profile:UpdateProfile` - Allows you to update profiles	

Change	Description	Date
AmazonConnectServiceLinkedRolePolicy (p. 1120) – Added actions for Amazon Connect Customer Profiles	Added the following actions so Amazon Connect contact flows and the agent experience can interact with the profiles in your default Customer Profiles domain: • `profile:SearchProfiles` • `profile:CreateProfile` • `profile:UpdateProfile` • `profile:AddProfileKey` Added the following action so Amazon Connect contact flows and the agent experience can interact with the profile objects in your default Customer Profiles domain: • `profile:ListProfileObjects` Added the following action so Amazon Connect contact flows and the agent experience can determine whether Customer Profiles is enabled for your Amazon Connect instance: • `profile:ListAccountIntegrations`	November 12, 2021
AmazonConnectVoiceIDFullAccess (p. 1113) – Added new AWS managed policy	Added a new AWS managed policy so you can set up your users to use Amazon Connect Voice ID. This policy provides full access to Amazon Connect Voice ID through the AWS console, SDK, or other means.	September 27, 2021
AmazonConnectCampaignsServiceLinkedRolePolicy (p. 1123) – Added new service-linked role policy	Added a new service-linked role policy for high-volume outbound communications. The policy provides access to retrieve all the high-volume outbound campaigns.	September 27, 2021

Change	Description	Date
AmazonConnectServiceLinkedRolePolicy (p. 1120) – Added actions for Amazon Lex	Added the following actions for the all bots created in the account across all Regions. These actions were added to support integration with Amazon Lex. • `lex:ListBots` - Lists all the bots available in a given Region for your account. • `lex:ListBotAliases` - Lists all the aliases for a given bot.	June 15, 2021
AmazonConnect_FullAccess (p. 1082) – Added actions for Amazon Lex	Added the following actions for the all bots created in the account across all Regions. These actions were added to support integration with Amazon Lex. • `lex:ListBots` • `lex:ListBotAliases`	June 15, 2021
Amazon Connect started tracking changes	Amazon Connect started tracking changes for its AWS managed policies.	June 15, 2021

Troubleshooting Amazon Connect identity and access

Use the following information to help you diagnose and fix common issues that you might encounter when working with Amazon Connect and IAM.

Topics

I am not authorized to perform iam:PassRole

If you receive an error that you're not authorized to perform the `iam:PassRole` action, then you must contact your administrator for assistance. Your administrator is the person that provided you with your user name and password. Ask that person to update your policies to allow you to pass a role to Amazon Connect.

Some AWS services allow you to pass an existing role to that service, instead of creating a new service role or service-linked role. To do this, you must have permissions to pass the role to the service.

The following example error occurs when an IAM user named `marymajor` tries to use the console to perform an action in Amazon Connect. However, the action requires the service to have permissions granted by a service role. Mary does not have permissions to pass the role to the service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform: iam:PassRole
```

In this case, Mary asks her administrator to update her policies to allow her to perform the `iam:PassRole` action.

I want to view my access keys

After you create your IAM user access keys, you can view your access key ID at any time. However, you can't view your secret access key again. If you lose your secret key, you must create a new access key pair.

Access keys consist of two parts: an access key ID (for example, `AKIAIOSFODNN7EXAMPLE`) and a secret access key (for example, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). Like a user name and password, you must use both the access key ID and secret access key together to authenticate your requests. Manage your access keys as securely as you do your user name and password.

> **Important**
> Do not provide your access keys to a third party, even to help find your canonical user ID. By doing this, you might give someone permanent access to your account.

When you create an access key pair, you are prompted to save the access key ID and secret access key in a secure location. The secret access key is available only at the time you create it. If you lose your secret access key, you must add new access keys to your IAM user. You can have a maximum of two access keys. If you already have two, you must delete one key pair before creating a new one. To view instructions, see Managing access keys in the *IAM User Guide*.

I'm an administrator and want to allow others to access Amazon Connect

To allow others to access Amazon Connect, you must create an IAM entity (user or role) for the person or application that needs access. They will use the credentials for that entity to access AWS. You must then attach a policy to the entity that grants them the correct permissions in Amazon Connect.

To get started right away, see Creating your first IAM delegated user and group in the *IAM User Guide*.

I want to allow people outside of my AWS account to access my Amazon Connect resources

You can create a role that users in other accounts or people outside of your organization can use to access your resources. You can specify who is trusted to assume the role. For services that support resource-based policies or access control lists (ACLs), you can use those policies to grant people access to your resources.

To learn more, consult the following:

- To learn whether Amazon Connect supports these features, see How Amazon Connect works with IAM (p. 1098).
- To learn how to provide access to your resources across AWS accounts that you own, see Providing access to an IAM user in another AWS account that you own in the *IAM User Guide*.
- To learn how to provide access to your resources to third-party AWS accounts, see Providing access to AWS accounts owned by third parties in the *IAM User Guide*.
- To learn how to provide access through identity federation, see Providing access to externally authenticated users (identity federation) in the *IAM User Guide*.
- To learn the difference between using roles and resource-based policies for cross-account access, see How IAM roles differ from resource-based policies in the *IAM User Guide*.

Use service-linked roles for Amazon Connect

What are service-linked roles (SLR) and why are they important?

Amazon Connect uses AWS Identity and Access Management (IAM) service-linked roles. A service-linked role is a unique type of IAM role that is linked directly to an Amazon Connect instance.

Service-linked roles are predefined by Amazon Connect and include all the permissions (p. 1120) that Amazon Connect requires to call other AWS services on your behalf.

You need to enable service-linked roles so you can use new features in Amazon Connect, such as tagging support, the new user interface in **User management** and **Routing profiles**, and queues with CloudTrail support.

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

Service-linked role permissions for Amazon Connect

Amazon Connect uses the service-linked role with the prefix **AWSServiceRoleForAmazonConnect_***`unique-id`* – Grants Amazon Connect permission to access AWS resources on your behalf.

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

- `connect.amazonaws.com`

The 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-linked 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 Connect Customer Profiles `profile:SearchProfiles`, `profile:CreateProfile`, `profile:UpdateProfile`, `profile:AddProfileKey`, `profile:ListProfileObjects`, `profile:ListAccountIntegrations` to use your default Customer Profiles domain (including profiles and all object-types in domain) with the Amazon Connect contact flows and agent experience applications.
- Action: Amazon Kinesis Data Firehose `firehose:DescribeDeliveryStream` and `firehose:PutRecord`, and `firehose:PutRecordBatch` for the delivery stream defined for agent event streams and contact records.
- Action: Amazon Kinesis Data Streams `kinesis:PutRecord`, `kinesis:PutRecords`, and `kinesis:DescribeStream` for the stream specified for agent event streams and contact records.
- Action: Amazon Lex `lex:PostContent` for the bots added to your instance.
- Action: Amazon Lex `lex:ListBots`, `lex:ListBotAliases` for all bots created in the account across all Regions.

- Action: Amazon CloudWatch Logs `logs:CreateLogStream`, `logs:DescribeLogStreams`, and `logs:PutLogEvents` to the CloudWatch Logs group specified for contact flow logging.
- Action: Amazon CloudWatch Metrics `cloudwatch:PutMetricData` to publish Amazon Connect usage metrics for an instance to your account.
- Action: Amazon Connect Voice-ID `voiceid:*` for the Voice ID domains associated with your instance.
- Action: EventBridge `events:PutRule` and `events:PutTargets` for the Amazon Connect managed EventBridge rule for publishing CTR records for your associated Voice ID domains.
- Action: high-volume outbound communications
  - `connect-campaigns:CreateCampaign`
  - `connect-campaigns:DeleteCampaign`
  - `connect-campaigns:DescribeCampaign`
  - `connect-campaigns:UpdateCampaignName`
  - `connect-campaigns:GetCampaignState`
  - `connect-campaigns:GetCampaignStateBatch`
  - `connect-campaigns:ListCampaigns`
  - `connect-campaigns:UpdateOutboundCallConfig`
  - `connect-campaigns:UpdateDialerConfig`
  - `connect-campaigns:PauseCampaign`
  - `connect-campaigns:ResumeCampaign`
  - `connect-campaigns:StopCampaign` for all operations related to high-volume outbound campaigns.

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

Create a service-linked role for Amazon Connect

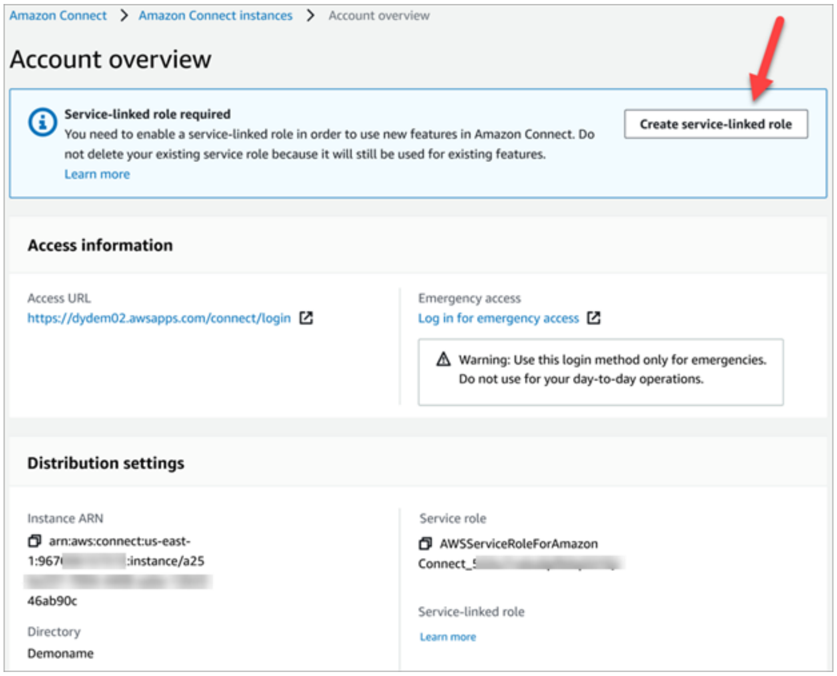
You don't need to manually create a service-linked role. When you create a new instance in Amazon Connect in the AWS Management Console, Amazon Connect creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create a new instance in Amazon Connect, Amazon Connect creates the service-linked role for you again.

You can also use the IAM console to create a service-linked role with the **Amazon Connect - Full access** use case. In the IAM CLI or the IAM API, create a service-linked role with the `connect.amazonaws.com` service name. For more information, see Creating a service-linked role in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

For instances created before October 2018

If your Amazon Connect instance was created before October 2018, you don't have service-linked roles set up. To create a service-linked role, on the **Account overview** page, choose **Create service-linked role**.



Amazon Connect > Amazon Connect instances > Account overview

Account overview

Service-linked role required
You need to enable a service-linked role in order to use new features in Amazon Connect. Do not delete your existing service role because it will still be used for existing features.
Learn more

Create service-linked role

Access information

Access URL
https://dydem02.awsapps.com/connect/login

Emergency access
Log in for emergency access

⚠ Warning: Use this login method only for emergencies. Do not use for your day-to-day operations.

Distribution settings

Instance ARN
arn:aws:connect:us-east-1:967[redacted]:instance/a25[redacted]46ab90c

Directory
Demoname

Service role
AWSServiceRoleForAmazonConnect_[redacted]

Service-linked role
Learn more

For a list of the IAM permissions required to create the service-linked role, see Overview page (p. 1085) in the Required permissions for using custom IAM policies to manage access to the Amazon Connect console (p. 1082) topic.

Edit a service-linked role for Amazon Connect

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

Checking a service-linked role has permissions for Amazon Lex

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

Delete a service-linked role for Amazon Connect

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

Supported Regions for Amazon Connect service-linked roles

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

Use service-linked roles for high-volume outbound communications

High-volume outbound communications uses AWS Identity and Access Management service-linked roles. When an Amazon Connect instance is enabled to use high-volume outbound communications, it creates a unique service linked role that allows it to perform actions on the Amazon Connect instance.

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

For information about other services that support service-linked roles, see AWS services that work with IAM in the *IAM User Guide*. Look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for high-volume outbound communications

High-volume outbound communications uses the service-linked role prefixed `AWSServiceRoleForConnectCampaigns`—Grants high-volume outbound communications permission to access AWS resources on your behalf.

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

- `connect-campaigns.amazonaws.com`

The role permissions policy allows high-volume outbound communications to complete the following actions on the specified resources:

- Action: High-volume outbound communications `connect-campaigns:ListCampaigns` for the AWS account.
- Action: Amazon Connect `connect:StartOutboundVoiceContact` `connect:GetMetricData` and `connect:GetCurrentMetricData` for the Amazon Connect instance specified.

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

Create a service-linked role for high-volume outbound communications

You don't need to manually create a service-linked role. When you associate an Amazon Connect instance with high-volume outbound communications by invoking the `StartInstanceOnboardingJob` API, high-volume outbound communications creates the service-linked role for you.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you associate a new Amazon Connect instance with high-volume outbound communications, Amazon Connect creates the service-linked role for you again.

Edit a service-linked role for high-volume outbound communications

High-volume outbound communications does not allow you to edit the `AWSServiceRoleForConnectCampaigns` service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see Editing a service-linked role in the *IAM User Guide*.

Delete a service-linked role for high-volume outbound communications

If you no longer need high-volume outbound communications, we recommend that you delete the associated service-linked role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

To delete high-volume outbound communications resources used by the `AWSServiceRoleForConnectCampaigns`

- Delete all campaigns setup for the AWS account.
- For this public preview, contact AWS support to delete all configuration so the service-linked role can be deleted safely.

To manually delete the service-linked role using IAM

- Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForConnectCampaigns` service-linked role. For more information, see Deleting a service-linked role in the *IAM User Guide*.

Supported Regions for high-volume outbound communications service-linked roles

High-volume outbound communications supports using service-linked roles in all of the Regions where the service is available. For more information, see AWS Regions and Endpoints.

Logging and monitoring Amazon Connect

Monitoring is important for maintaining the reliability, availability, and performance of your contact center.

You should collect monitoring data from all of the parts of your AWS solution so that you can more easily debug a multipoint failure if one occurs. But before you start monitoring Amazon Connect, you should create a monitoring plan that includes answers to the following questions:

- What are your monitoring goals?
- What data about your Amazon Connect instance will you monitor?
- How often will you monitor your instance?
- What monitoring tools will you use?
- Who will perform the monitoring tasks?

- Who should be notified when something goes wrong?

See the following topics to learn how to use Amazon CloudWatch Logs and AWS CloudTrail to monitor Amazon Connect and describes the Amazon Connect metrics sent to CloudWatch:

- Monitoring your instance using CloudWatch (p. 1014)
- Logging Amazon Connect API calls with AWS CloudTrail (p. 1025)

Tagging resources in Amazon Connect

A *tag* is a custom metadata label that you can add to a resource in order to make it easier to identify, organize, and find in a search. Tags are comprised of two individual parts: A tag key and a tag value. This is referred to as a key:value pair.

A *tag key* typically represents a larger category, while a tag value represents a subset of that category. For example you could have *tag key=Color* and *tag value=Blue*, which would produce the key:value pair `Color:Blue`. Note that you can set the value of a tag to an empty string, but you can't set the value of a tag to null. Omitting the tag value is the same as using an empty string.

Tag keys can be up to 128 characters in length and tag values can be up to 256 characters in length; both are case sensitive. For more information, see:

- Amazon Connect TagResource
- Amazon Connect Customer Profiles TagResource
- Amazon Connect Voice ID TagResource: You can add tags to the Voice ID domain.
- Amazon AppIntegrations TagResource

Amazon Connect services support up to 50 tags per resource. For a given resource, each tag key must be unique with only one value.

> **Note**
> Your tags cannot begin with `aws:` because AWS reserves this prefix for system-generated tags. You cannot add, modify, or delete `aws:*` tags, and they don't count against your tags-per-resource limit.

The following table describes the Amazon Connect resources that can be tagged using the AWS CLI or an AWS SDK.

Tagging support for Amazon Connect resources

Resource	Supports tags	Supports tagging on creation
Agent	Yes	Yes
Agent group	Yes	Yes
Agent group level	No	No
Agent state	Yes	Yes
Task template	Yes	No
Contact	No	No

Resource	Supports tags	Supports tagging on creation
Contact flow	Yes	Yes
Flow module	Yes	Yes
Instance	No	No
Integration association	Yes	Yes
Operating hours	Yes	Yes
Phone number	Yes	Yes
Prompt	No	No
Queue	Yes	Yes
Queue agent	No	No
Routing Profile	Yes	Yes
Security profile	Yes	Yes
Transfer destination	Yes	Yes
Use case	Yes	Yes
Vocabulary	Yes	Yes

> **Note**
> Tagging of Amazon Connect resources is currently only available using the AWS CLI or an AWS SDK.

To learn more about tagging, including best practices, see Tagging AWS resources in the *AWS General Reference*.

Tag-based access control

To use tags to control access to resources within your AWS accounts, you need to provide tag information in the condition element of an IAM policy. For example, to control access to your Voice ID domain based on the tags you've assigned to it, use the `aws:ResourceTag/key-name` condition key to specify which tag key:value pair must be attached to the domain, in order to allow given actions for it.

For more detailed information on tag-based access control, see Controlling access to AWS resources using tags in the *IAM User Guide*

Compliance validation in Amazon Connect

Third-party auditors assess the security and compliance of AWS services as part of multiple AWS compliance programs, such as SOC, PCI, FedRAMP, and HIPAA.

To learn whether or other AWS services are within the scope of specific compliance programs, see AWS Services in Scope by Compliance Program. For general information, see AWS Compliance Programs.

You can download third-party audit reports using AWS Artifact. For more information, see Downloading Reports in AWS Artifact.

Your compliance responsibility when using AWS services is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- Security and Compliance Quick Start Guides – These deployment guides discuss architectural considerations and provide steps for deploying baseline environments on AWS that are security and compliance focused.
- Architecting for HIPAA Security and Compliance on Amazon Web Services – This whitepaper describes how companies can use AWS to create HIPAA-eligible applications.

  Note
  Not all AWS services are HIPAA eligible. For more information, see the HIPAA Eligible Services Reference.
- AWS Compliance Resources – This collection of workbooks and guides might apply to your industry and location.
- Evaluating Resources with Rules in the *AWS Config Developer Guide* – The AWS Config service assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- AWS Security Hub – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.
- AWS Audit Manager – This AWS service helps you continuously audit your AWS usage to simplify how you manage risk and compliance with regulations and industry standards.

Best practices for PII compliance in Amazon Connect

Following this list of best practices can help you ensure your Amazon Connect contact center is PII (Personally Identifiable Information) compliant.

- Conduct compliance eligibility audits for all services used in your contact center, as well as any third party integration points.
- AWS Key Management Service (KMS) encrypts Amazon S3 contents at the object level, which covers recordings, logs, and saved reports by default for Amazon S3. Make sure encryption in transit and at rest rules apply downstream or to third party apps.
- Use encryption in the **Store customer input** block for sensitive DTMF information.
- Use your own KMS key when ingesting data in Amazon Connect Customer Profile domains.
- Do not upload content containing customer PII to Amazon Connect Wisdom.
- When using Amazon Connect Voice ID, do not use PII in the `CustomerSpeakerId`.
- As with any AWS service, we strongly recommend that you not use sensitive information to name resources.

Best practices for PCI compliance in Amazon Connect

Following this list of best practices can help you ensure your Amazon Connect contact center is PCI-compliant.

- Conduct compliance eligibility audits for all services used in your contact center, as well as any third party integration points.
- Payment card information (PCI) should be collected via encrypted DTMF.
- If PCI is captured in call recordings, the PCI data must be scrubbed from the recording and obfuscated from any logs or transcriptions. We recommend working with an Amazon Solution Architect if you need help doing this.

- Use encryption in transit and at rest for any downstream integration points.
- Enable multi-factor authentication (MFA) for any access to PCI as Amazon Connect is a public endpoint.
- For a detailed walkthrough that explains how to encrypt PCI, see Creating a secure IVR solution with Amazon Connect.
- AWS Key Management Service (KMS) encrypts Amazon S3 contents at the object level, which covers recordings, logs, and saved reports by default for Amazon S3. Make sure encryption in transit and at rest rules apply downstream or to third party apps.
- Use encryption in the **Store customer input** block for sensitive DTMF information.
- Use your own KMS key when ingesting data in Amazon Connect Customer Profile domains.
- Do not upload content containing PCI to Amazon Connect Wisdom.
- For more information, see https://www.pcisecuritystandards.org.

Best practices for HIPAA compliance in Amazon Connect

Note
Amazon Connect Wisdom is currently not HIPAA compliant.

Note
Amazon Connect Voice ID is not currently HIPAA compliant.

Following this list of best practices can help you ensure your Amazon Connect contact center is HIPAA compliant.

- Conduct compliance eligibility audits for all services used in your contact center, as well as any third party integration points.
- AWS Key Management Service (KMS) encrypts Amazon S3 contents at the object level, which covers recordings, logs, and saved reports by default for Amazon S3. Make sure encryption in transit and at rest rules apply downstream or to third party apps.
- Use encryption in the **Store customer input** block for sensitive DTMF information.
- Do not upload content subject to HIPAA to Amazon Connect Wisdom.
- For more information about HIPAA compliance, see https://www.hipaacompliance.org/.

Resilience in Amazon Connect

The AWS global infrastructure is built around AWS Regions and Availability Zones. AWS Regions provide multiple physically separated and isolated Availability Zones, which are connected with low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between Availability Zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see AWS Global Infrastructure.

In addition to the AWS global infrastructure, Amazon Connect offers the following features to help support your data resiliency and backup needs:

- Contact flow versioning (p. 452)
- Ability to export your contact record data to Kinesis. This way, you can back up the contact record data across Availability Zones.

To backup call recordings, use the cross-region replication (CRR) feature to copy the call recordings to Amazon S3 buckets in different AWS Regions.

Infrastructure security in Amazon Connect

As a managed service, Amazon Connect is protected by the AWS global network security procedures that are described on the Best Practices for Security, Identity, and Compliance page.

You use AWS published API calls to access Amazon Connect through the network.

Supported versions of TLS

Clients must support Transport Layer Security (TLS) 1.2 or later.

Amazon Connect offers a new website access model with a new domain (instance name.my.connect.aws) that supports TLS 1.2 or newer versions only. It is available by default for instances created after March 2021. Existing customers can opt in to using the new domain using the following methods:

- For non-SAML Amazon Connect instances, change your access URL from **.awsapps.com/connect** to **.my.connect.aws** and log in again.
- For SAML-enabled instances, specify an extra query parameter new_domain=true in the relay state URL and log in again. For more information, see Use a destination in your relay state URL (p. 130).

Other requirements

Clients must support cipher suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

Additionally, requests must be signed by using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

You can call these API operations from any network location, but Amazon Connect does support resource-based access policies, which can include restrictions based on the source IP address.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in resource policies to limit the permissions that Amazon Connect gives another service to the resource. If you use both global condition context keys, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

The most effective way to protect against the confused deputy problem is to use the exact Amazon Resource Name (ARN) of the resource you want to allow. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcards (`*`) for the unknown portions of the ARN. For example, `arn:aws:`*`servicename`*`::`*`region-name`*`::`*`your AWS account ID`*`:*`.

Amazon Connect Customer Profiles cross-service confused deputy prevention

The following examples show policies that apply to cases where someone else is set up as the administrator for Amazon Connect Customer Profiles. Use these policies to prevent the confused deputy problem.

Example Amazon Connect Customer Profiles policy to create Customer Profile domains

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "profile.amazonaws.com"
    },
    "Action": ["kms:GenerateDataKey", "kms:CreateGrant", "kms:Decrypt"],
    "Resource": [
      "arn:aws:kms:your region-name:your AWS account ID:key/your key ARN"
    ],
    "Condition": {
      "ArnEquals": {
        "aws:SourceArn": "arn:aws:profile:your region name:your AWS account ID:domains/your
 Customer Profiles domain name"
      },
      "StringEquals": {
        "aws:SourceAccount": "your AWS account ID"
      }
    }
  }
}
```

Example Amazon Connect Customer Profiles policy to create Customer Profiles object types

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "profile.amazonaws.com"
    },
    "Action": ["kms:GenerateDataKey", "kms:CreateGrant", "kms:Decrypt"],
    "Resource": [
      "arn:aws:kms:your Region:your AWS account ID:key/your key ARN"
    ],
    "Condition": {
      " ArnEquals": {
        "aws:SourceArn": "arn:aws:profile:your region name:your AWS account ID:domains/your
 Customer Profiles domain name/objects/your object type"
      },
      "StringEquals": {
        "aws:SourceAccount": "your AWS account ID"
      }
    }
  }
}
```

Example Amazon Connect Customer Profiles policy to create and update dead-letter queues

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow Amazon Connect Customer Profiles to publish messages to your queue",
      "Effect": "Allow",
      "Principal": {
        "Service": "profile.amazonaws.com"
      },
      "Action": "sqs:SendMessage",
      "Resource": "your dead-letter queue ARN",

      "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "your AWS account ID",
          "aws:SourceArn": "arn:aws:profile:your region name:your AWS account
 ID:domains/your Customer Profiles domain name"
        }
      }
    }
  ]
}
```

Example Amazon Connect Customer Profiles policy to protect the Amazon S3 bucket used as part of the Identity Resolution process

```
{
    "Sid": "Allow Amazon Connect Customer Profiles to put S3 objects to your bucket",
    "Effect": "Allow",
    "Principal": {
        "Service": "profile.amazonaws.com"
    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::your S3 bucket name/*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "your AWS account ID"
        },
        "ArnEquals": {
            "aws:SourceArn": "arn:aws:profile:your region name:your AWS account ID:domains/
*"
        }
    }
}
```

Amazon Connect Voice ID cross-service confused deputy prevention

The following Voice ID example shows a resource policy to apply to prevent the confused deputy problem.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "voiceid.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnEquals": {
        "aws:SourceArn": "arn:aws:voiceid:your region name:your AWS account ID:domain/your
 Voice ID domain name"
      },
      "StringEquals": {
        "aws:SourceAccount": "your AWS account ID"
      }
    }
  }
}
```

Amazon Connect chat message streaming cross-service confused deputy prevention

The following Amazon Connect example shows a resource policy to apply to prevent the confused deputy problem.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"connect.amazonaws.com"
         },
         "Action":"sns:Publish",
         "Resource":"your SNS topic ARN",
         "Condition":{
            "StringEquals":{
               "aws:SourceAccount":"your AWS account ID"
            },
            "ArnEquals":{
               "aws:SourceArn":"your Amazon Connect instance ARN"
            }
         }
      }
   ]
}
```

Security Best Practices for Amazon Connect

Amazon Connect provides a number of security features to consider as you develop and implement your own security policies. The following best practices are general guidelines and don’t represent a complete security solution. Because these best practices might not be appropriate or sufficient for your environment, treat them as helpful considerations rather than prescriptions.

Contents

- Amazon Connect Detective Security Best Practices (p. 1134)

Amazon Connect Preventative Security Best Practices

- Ensure that all profile permissions are as restrictive as possible. Allow access to only those resources absolutely required for the user's role. For example, don't give agents permissions to create, read, or update users in Amazon Connect.
- Ensure that multi-factor authentication (MFA) is set up through your SAML 2.0 identity provider, or Radius server, if that's more applicable for your use case. After MFA is set up, a third text box becomes visible on the Amazon Connect login page to provide the second factor.
- If you use an existing directory through AWS Directory Service or SAML-based authentication for identity management, ensure that you follow all security requirements appropriate for your use case.
- Use the **Log in for emergency access** URL on the instance page of the AWS console only in emergency situations, not for daily use. For more information, see Emergency admin login (p. 146).

Use Service Control Policies (SCPs)

Service control policies (SCPs) are a type of organization policy that you can use to manage permissions in your organization. An SCP defines a guardrail, or sets limits, on the actions that the account's administrator can delegate to the IAM users and roles in the affected accounts. You can use SCPs to protect critical resources associated with your Amazon Connect workload.

Set a Service Control Policy to prevent the deletion critical resources

If you're using SAML 2.0-based authentication and delete the AWS IAM Role that is used for authenticating Amazon Connect users, users won't be able to login to the Amazon Connect instance. You will need to delete and recreate users to be associated with a new Role. This results in the deletion of all data associated with those users.

To prevent the accidental deletion of critical resources and to protect the availability of your Amazon Connect instance, you can set a Service Control Policy (SCP) as an additional control.

Following is an example SCP that can be applied at the AWS Account, Organizational Unit, or Organizational Root to prevent the deletion of the Amazon Connect instance and associated Role:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AmazonConnectRoleDenyDeletion",
      "Effect": "Deny",
      "Action": [
        "iam:DeleteRole"
      ],
      "Resource": [
        "arn:aws:iam::*:role/Amazon Connect user role"
      ]
    },
    {
      "Sid": "AmazonConnectInstanceDenyDeletion",
      "Effect": "Deny",
      "Action": [
        "connect:DeleteInstance"
      ],
      "Resource": [
        "Amazon Connect instance ARN"
      ]
    }
  ]
}
```

Amazon Connect Detective Security Best Practices

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

Define log retention requirements and lifecycle policies early on, and plan to move log files to cost-efficient storage locations as soon as practical. Amazon Connect public APIs log to CloudTrail. Review and automate actions based on CloudTrail logs.

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

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

You can implement fraud detection and prevention for incoming contacts by customizing Amazon Connect contact flows per your requirements. For example, you can check incoming contacts against previous contact activity in Dynamo DB and then take actions such as disconnecting a contact who is on a deny list.

Agent training guide

CCP

You use the Amazon Connect Contact Control Panel (CCP) to interact with customer contacts. It's how you receive calls, chat with contacts, transfer them to other agents, put them on hold, and perform other key tasks.

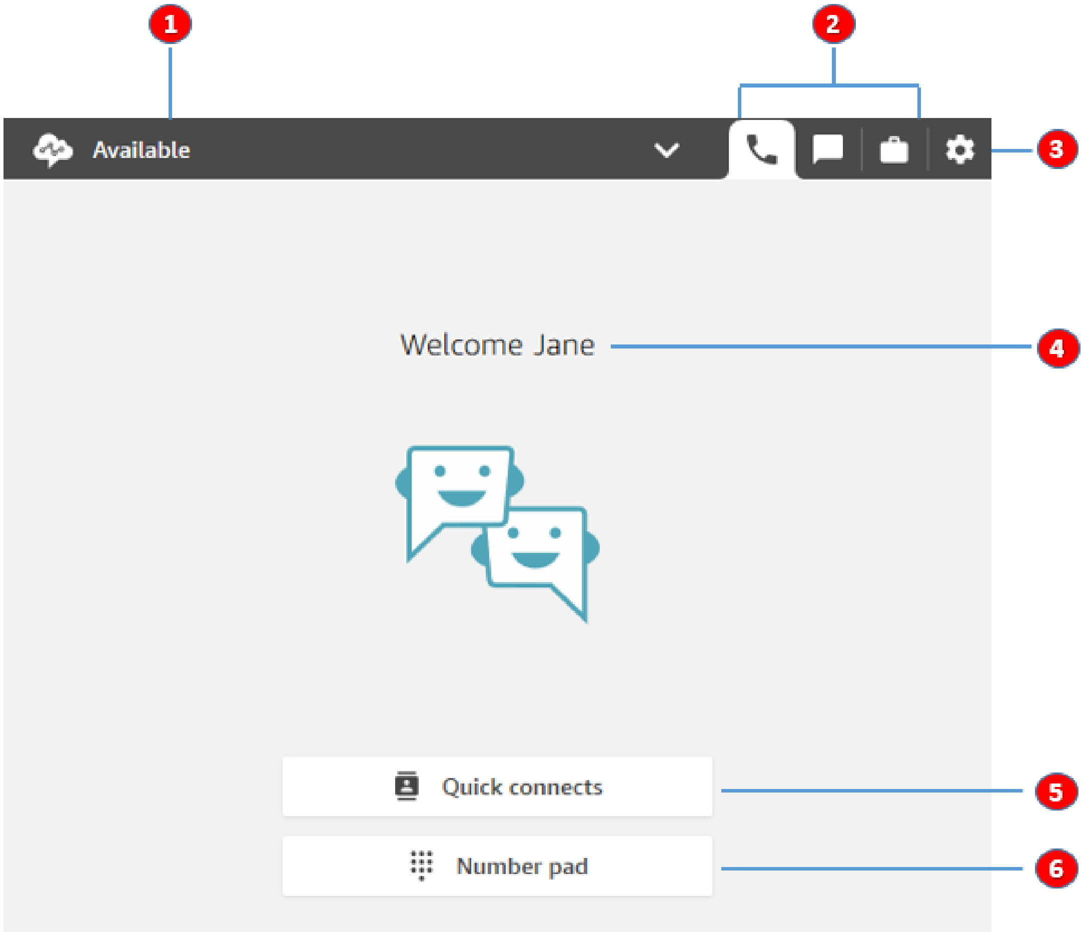
The URL to launch the CCP is:

- https://*instance name*.my.connect.aws/ccp-v2/

Where *instance name* is provided by your IT department or the individuals that set up Amazon Connect for your business.

Large businesses often choose to customize their CCP. For example, they might want to integrate it with a CRM. However, this section describes how CCP works before it is customized.

The following image shows the CCP.



1. Set your status.
2. The channels enabled for your agent routing profile.
3. Log in and out. Set your language preferences, device settings (if enabled), and phone type.

4. Name of the agent that's currently signed in.
5. Choose a predefined destination to transfer the contact. Or call an external number.
6. Call a number or enter digits into an IVR menu.

Agent application

With the agent application you can access all Amazon Connect features in a single application. You can:

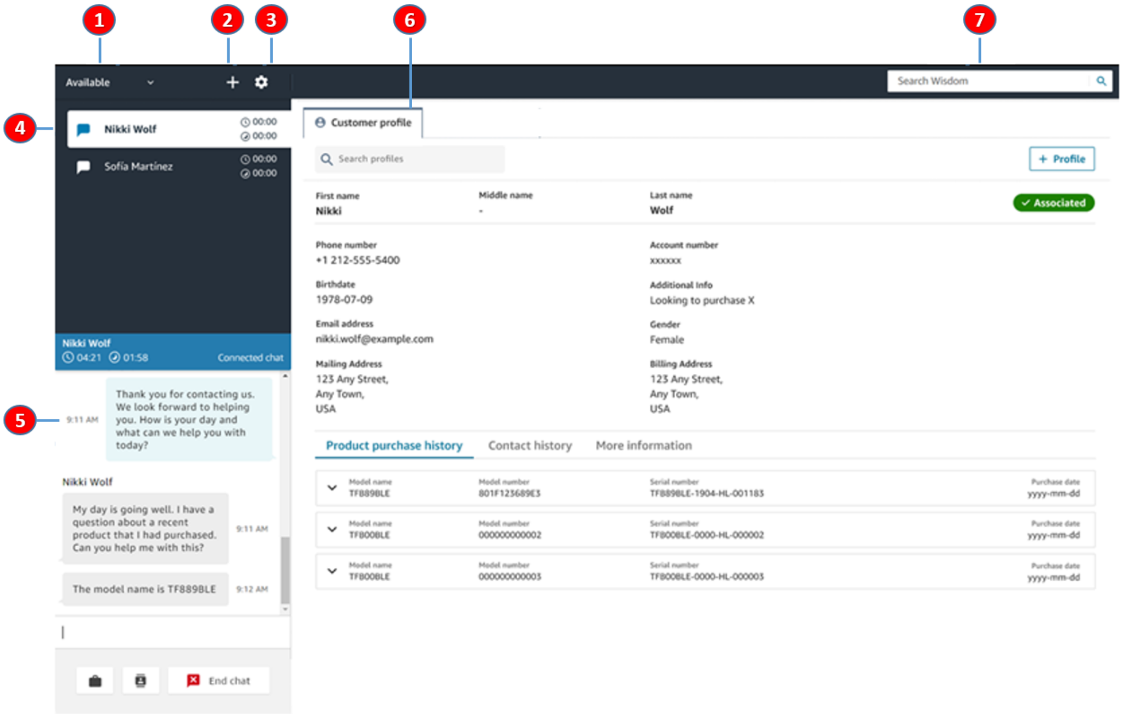
- Use the Contact Control Panel (CCP) to interact with customer contacts.
- Use Customer Profiles to view customer information.
- Use Amazon Connect Wisdom to obtain the information you need from your company knowledge base.

To access the agent application use the following URL:

- https://*instance name*.my.connect.aws/agent-app-v2/

Where *instance name* is provided by your IT department or the individuals that set up Amazon Connect for your business.

The following image shows the agent application with the CCP, Customer Profiles, and Wisdom.



9:11 AM Thank you for contacting us. We look forward to helping you. How is your day and what can we help you with today?

Nikki Wolf

My day is going well. I have a question about a recent product that I had purchased. Can you help me with this? 9:11 AM

The model name is TF889BLE 9:12 AM

First name: Nikki
Middle name: -
Last name: Wolf

Phone number: +1 212-555-5400
Account number: xxxxxx
Birthdate: 1978-07-09
Additional Info: Looking to purchase X
Email address: nikki.wolf@example.com
Gender: Female
Mailing Address: 123 Any Street, Any Town, USA
Billing Address: 123 Any Street, Any Town, USA

Model name	Model number	Serial number	Purchase date
TF889BLE	801F123689E3	TF889BLE-1904-HL-001183	yyyy-mm-dd
TF800BLE	000000000002	TF800BLE-0000-HL-000002	yyyy-mm-dd
TF800BLE	000000000003	TF800BLE-0000-HL-000003	yyyy-mm-dd

1. Set your status.
2. Access to the number pad, quick connects, and task creation.
3. Log in and out. Set your language preferences, device settings (if enabled), and phone type.
4. Inbox of inbound calls, chats, and tasks.
5. Based on the channel of the contact that is in focus in your inbox, the appropriate content shows here; for example, when a chat is selected, the chat interface appears.

6. View customer information for the contact that is in focus in your inbox.
7. Search for knowledge articles to solve customer issues.

Training video: How to use the CCP

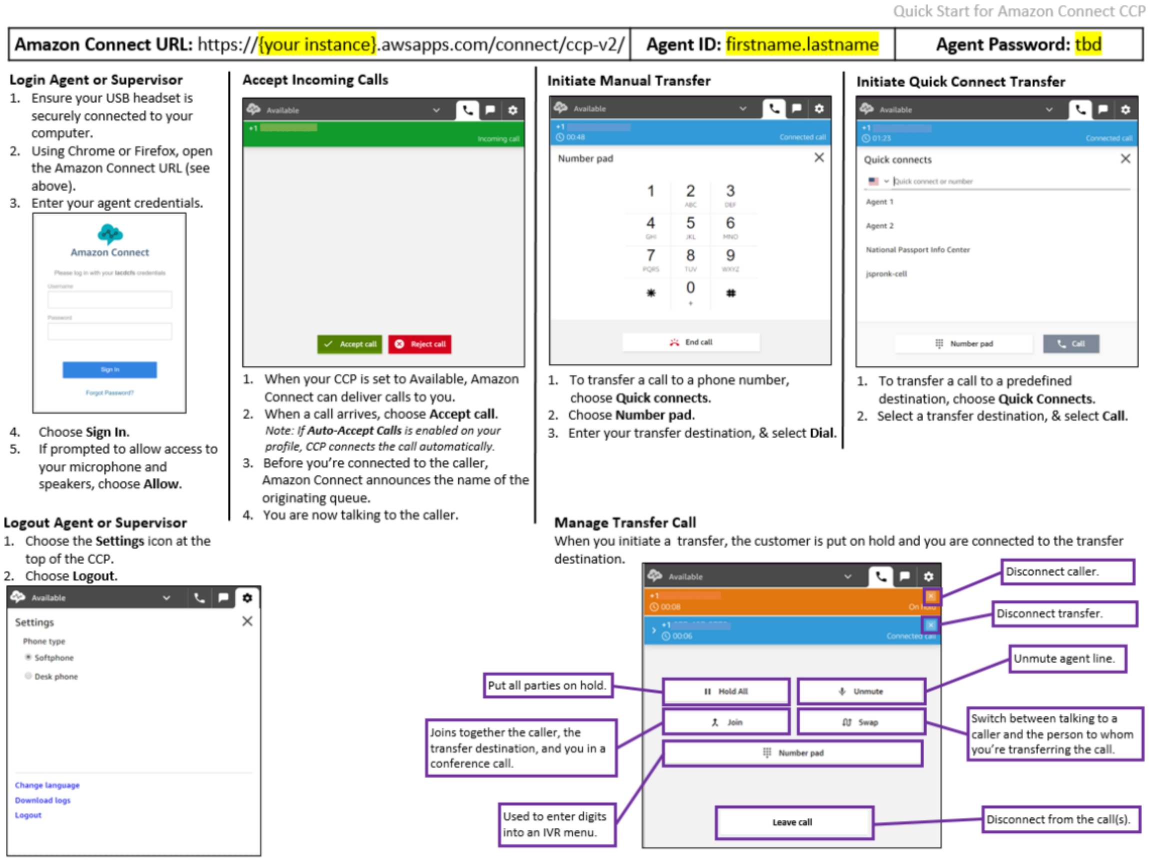
The following video introduces you to the Contact Control Panel (CCP). It shows how to perform common tasks, such as login and setup, accept incoming calls, place calls, transfer calls, accept chat, and more.

Quick start cheat sheet for training agents

The following image shows a one-page cheat sheet to help agents learn the most common tasks in the CCP.

Click here to download a Microsoft PowerPoint slide of this image.

Your manager or IT administrator provides you with the name of your instance, agent ID, and password.



Quick Start for Amazon Connect CCP

Amazon Connect URL: https://{your instance}.awsapps.com/connect/ccp-v2/	Agent ID: firstname.lastname	Agent Password: tbd

Login Agent or Supervisor

1. Ensure your USB headset is securely connected to your computer.
2. Using Chrome or Firefox, open the Amazon Connect URL (see above).
3. Enter your agent credentials.
4. Choose **Sign In**.
5. If prompted to allow access to your microphone and speakers, choose **Allow**.

Logout Agent or Supervisor

1. Choose the **Settings** icon at the top of the CCP.
2. Choose **Logout**.

Accept Incoming Calls

1. When your CCP is set to Available, Amazon Connect can deliver calls to you.
2. When a call arrives, choose **Accept call**.
   Note: If ***Auto-Accept Calls*** *is enabled on your profile, CCP connects the call automatically.*
3. Before you're connected to the caller, Amazon Connect announces the name of the originating queue.
4. You are now talking to the caller.

Initiate Manual Transfer

1. To transfer a call to a phone number, choose **Quick connects**.
2. Choose **Number pad**.
3. Enter your transfer destination, & select **Dial**.

Initiate Quick Connect Transfer

1. To transfer a call to a predefined destination, choose **Quick Connects**.
2. Select a transfer destination, & select **Call**.

Manage Transfer Call

When you initiate a transfer, the customer is put on hold and you are connected to the transfer destination.

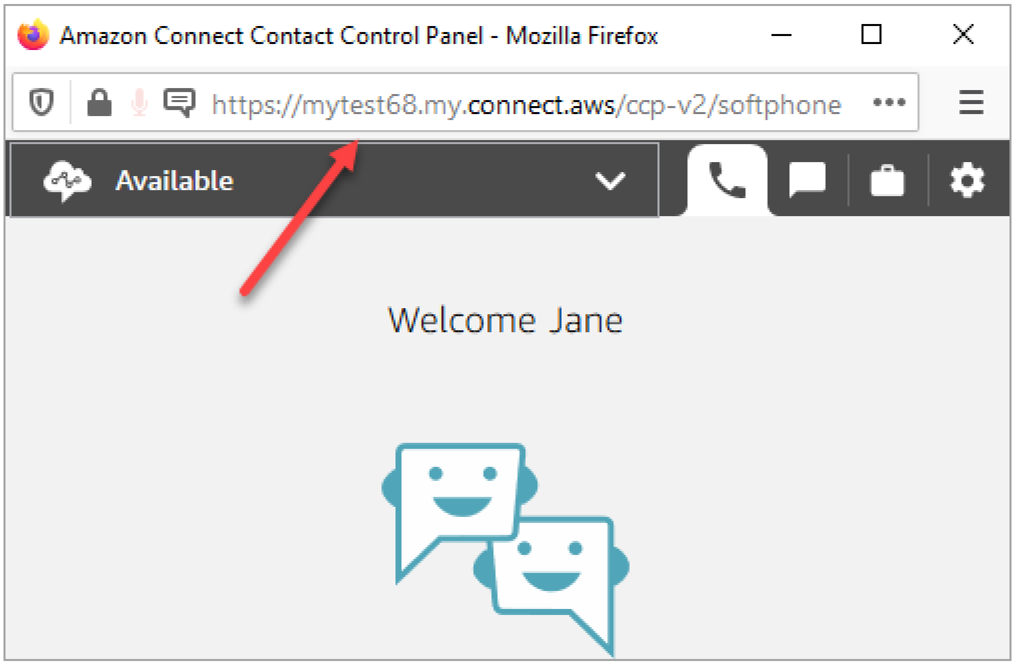
Available
+1 [redacted]
00:08
On hold
+1 [redacted]
00:06
Connected call
Hold All
Unmute
Join
Swap
Number pad
Leave call
Disconnect caller.
Disconnect transfer.
Unmute agent line.
Put all parties on hold.
Switch between talking to a caller and the person to whom you're transferring the call.
Joins together the caller, the transfer destination, and you in a conference call.
Used to enter digits into an IVR menu.
Disconnect from the call(s).

Launch the CCP

The URL to launch the CCP is:

- https://*instance name*.my.connect.aws/ccp-v2/

Where *instance name* is provided by your IT department or whoever set up Amazon Connect for your business. The following image shows an example URL for the CCP.


Amazon Connect Contact Control Panel - Mozilla Firefox
https://mytest68.my.connect.aws/ccp-v2/softphone
Available
Welcome Jane

With this updated CCP, your agents can manage voice, chat, and tasks from this single interface.

As the administrator, you can also launch the CCP directly from the Amazon Connect console. Just choose the phone icon in the upper right corner.

To provide agents the ability to launch the CCP from their desktop and start handling contacts, there are a few things you need to do:

- Add agents as users to the instance. For more information, see Manage users in Amazon Connect (p. 785).
- Configure permissions for the agents. By default, agents assigned to the Agent security profile can access the CCP and make outbound calls. But you can create a custom security profile and add additional permissions. For more information, see Security profiles (p. 789).
- 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. 291).

Log in and log out of the Amazon Connect CCP

Before you can log in to the Contact Control Panel (CCP), your administrator must give you the following information:

- The URL to launch the CCP:
  - https://*instance name*.my.connect.aws/ccp-v2/

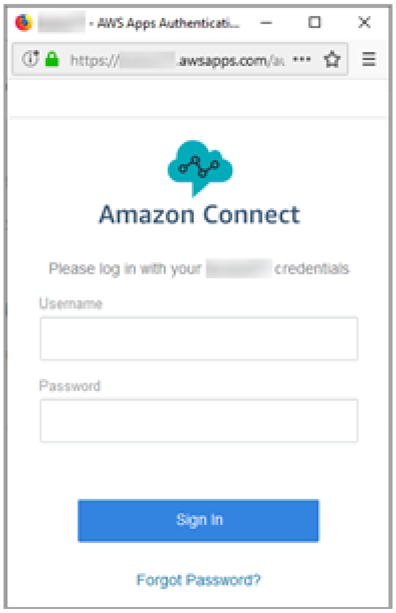
  Where *instance name* is provided by your IT department or whoever set up Amazon Connect for your business.

- Your agent ID.
- Your agent password.

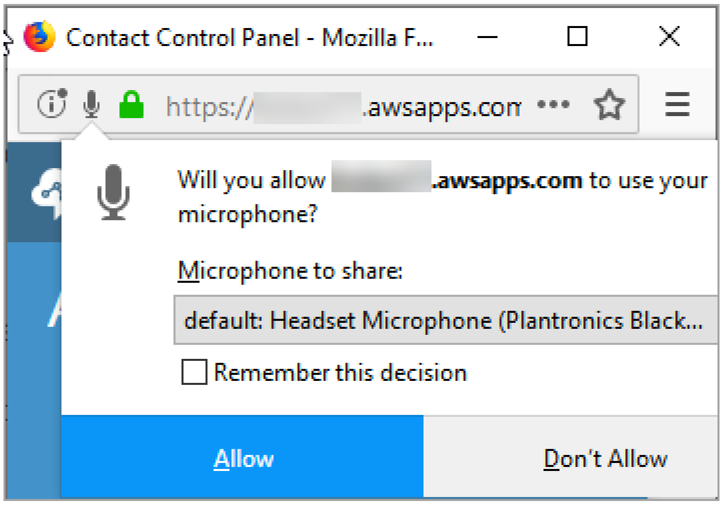
To log in

After you have that information, here's how to log in and get started.

1. Ensure that your USB headset is securely connected to your computer.
2. Using Chrome or Firefox, open the CCP by using the URL that you received from your administrator.
3. Enter your agent ID and password, and then choose **Sign In**.


[redacted] - AWS Apps Authenticati...
https://[redacted].awsapps.com/a
Amazon Connect
Please log in with your [redacted] credentials
Username
Password
Sign In
Forgot Password?

4. If you are prompted to allow access to your microphone and speaker, choose **Allow**.


Contact Control Panel - Mozilla F...
https://[redacted].awsapps.com

Will you allow [redacted]**.awsapps.com** to use your microphone?

Microphone to share: default: Headset Microphone (Plantronics Black...

□ Remember this decision

You're all set to go!

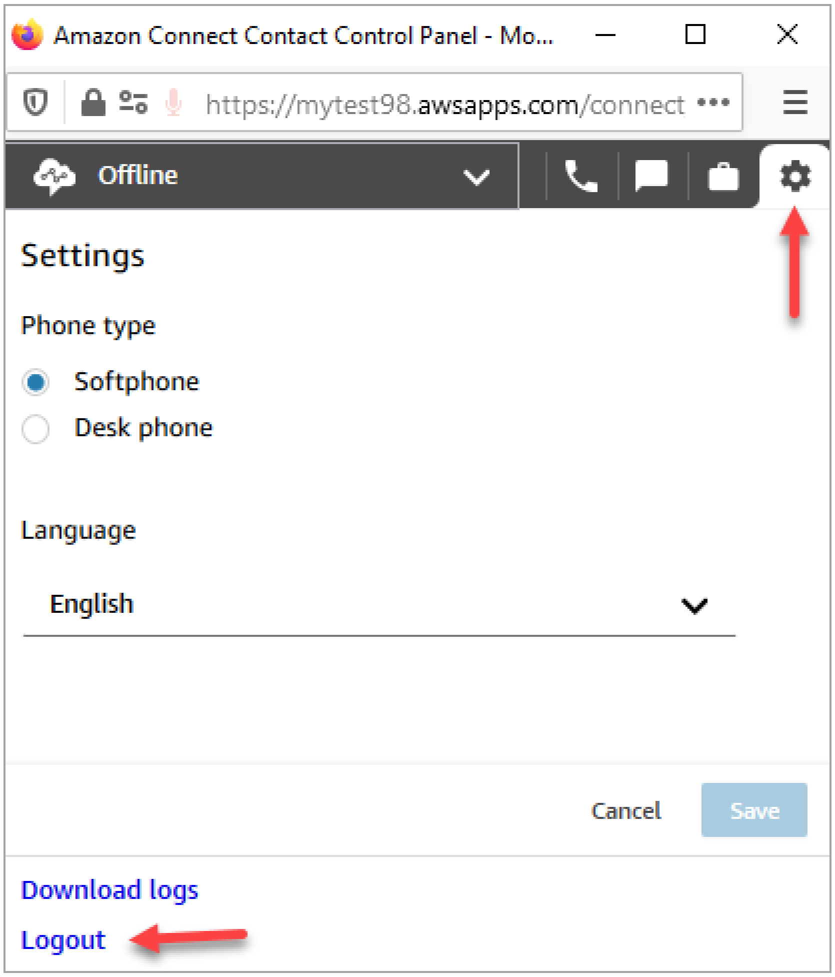
Problems logging in?

If you have problems logging in to the CCP, contact your manager for help, or the IT Department for your organization.

Log out of the Amazon Connect CCP

> **Important**
> Closing the CCP doesn't automatically sign out an agent. Amazon Connect still tries to route contacts to them. To change this behavior, a developer can customize CCP for your contact center. For instructions, see CCPv1: Log out agents automatically when they close their CCP (p. 235).

1. At the top of the CCP, choose **Settings**.
2. Choose **Log out**.


Amazon Connect Contact Control Panel - Mo...
https://mytest98.awsapps.com/connect
Offline

Settings

Phone type

● Softphone
○ Desk phone

Language

English

Cancel
Save
Download logs
Logout

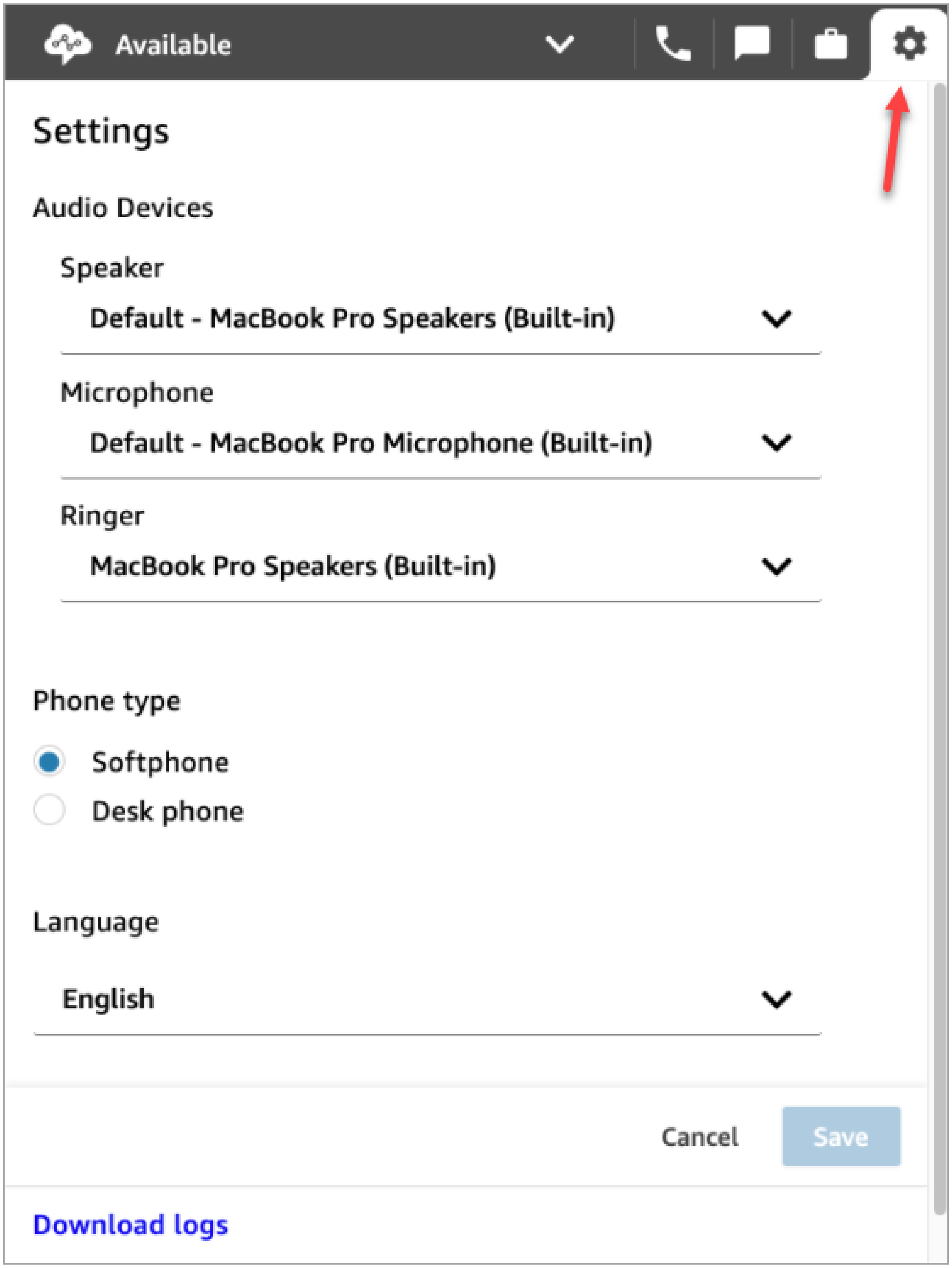
Change your audio device settings

If your organization is using a customized version of the Contact Control Panel (CCP), you can use it to change your audio device settings.

Tip
Developers: for more information about enabling this feature, see the Amazon Connect Streams documentation on GitHub.

To change your audio settings

1. In your CCP, choose **Settings**. The **Settings** dialog box appears, similar to the following image.



Settings

Audio Devices

Speaker

Default - MacBook Pro Speakers (Built-in)

Microphone

Default - MacBook Pro Microphone (Built-in)

Ringer

MacBook Pro Speakers (Built-in)

Phone type

● Softphone

○ Desk phone

Language

English

2. Under **Audio devices**, use the dropdown to select your **Speaker**, **Microphone**, and **Ringer**.

   Note
   If you use Firefox, you can change your **Microphone** device setting. To change your speaker and ringer, use your computer settings.

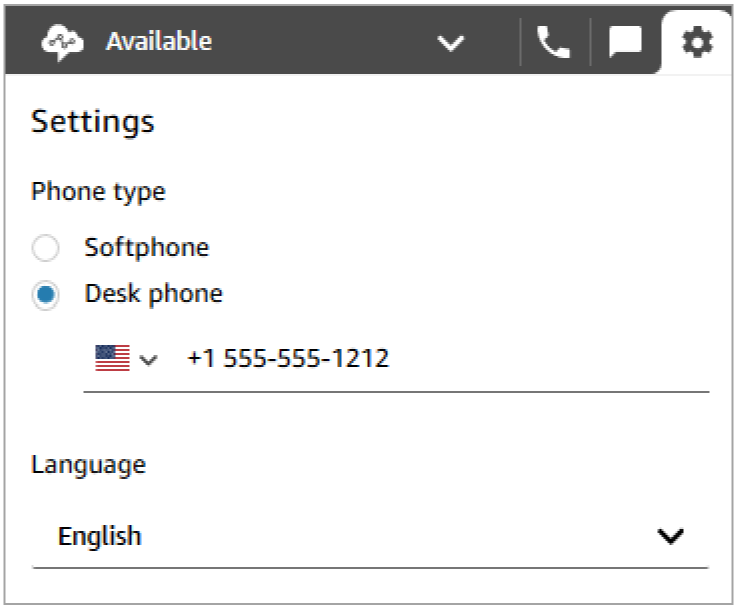
Change your ringtone

You can change your ringtone if your organization uses a custom CCP. **Developers**: for more information, see Amazon Connect Streams.

Forward calls to a mobile device (iPhone, Android)

You can take the audio portion of a call on your mobile device, and at the same time use your computer to access the Contact Control Panel. This topic explains how to forward calls to your mobile device.

1. In your Contact Control Panel (CCP), open Settings.
2. Under **Phone type**, choose **Desk phone**.
3. Enter the phone number for your mobile device, and choose **Save**.



Settings

Phone type

○ Softphone

● Desk phone

+1 555-555-1212

Language

English

When a contact calls, the audio portion of the call goes to your mobile device. At the same time, on your computer you can manage the call using the CCP.

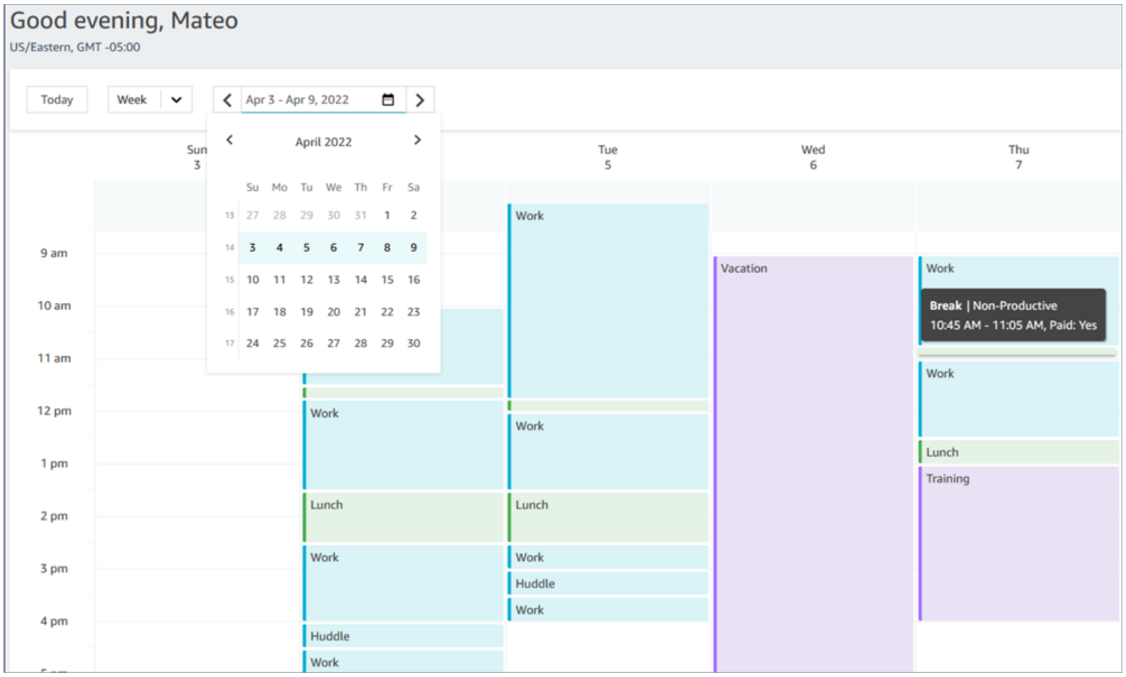
View your schedule

If your organization uses the forecasting, capacity planning, and scheduling features of Amazon Connect you can view your schedule in the agent application, the Contact Control Panel (CCPv1 or CCPv2), the Salesforce CTI, or a custom-built agent desktop.

Following are steps you use to view your schedule in the agent application.

1. Log on to the agent application using the URL that your admin gives you (for example, **https://[instance name].my.connect.aws/ccp-v2/**).
2. Choose the Calendar icon on the application navigation bar to launch the staff schedule manager viewer. Otherwise, the staff schedule manager viewer launches automatically.

   The following image shows a sample schedule in the agent application:



You can see a daily or weekly view of your schedule.

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. 227) to determine which contacts to route to them.

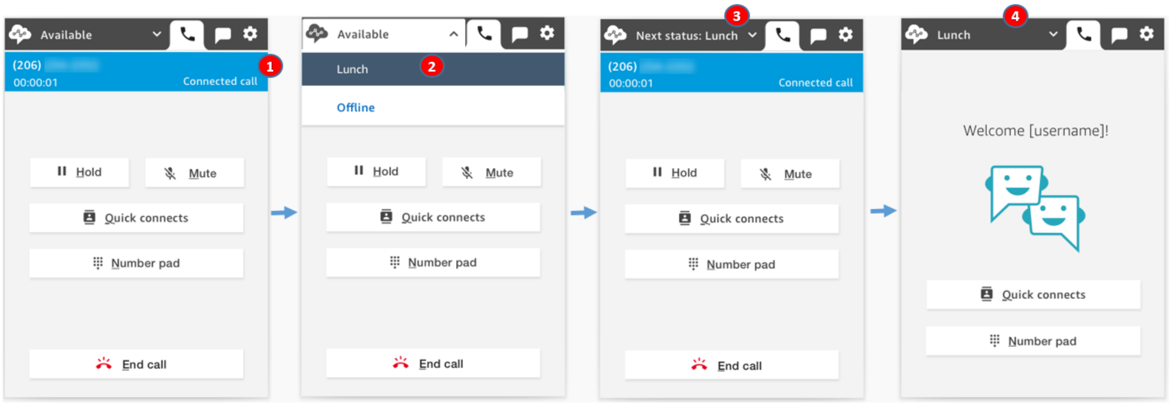
For more information about agent statuses, see About agent status (p. 998). For information about how Amazon Connect counts the Available status in the real-time metrics report, see Available (p. 919).

Set your "Next status"

> **Note**
> "Next status" is available only to customers who are using the latest Contact Control Panel (CCP). The URL for the latest CCP ends with **ccp-v2**.
> **IT administrators**: For more information about the **Next status** feature, such as changes to the agent event stream, see July 2021 Updates (p. 1230) in the *Release notes*.

Use the **Next status** feature to pause new contacts being routed to you, while you finish your current contacts. When all your slots are cleared, Amazon Connect automatically sets your CCP to the next status, such as **Lunch**.

The following images of the Contact Control Panel (CCP) show how to use this feature.

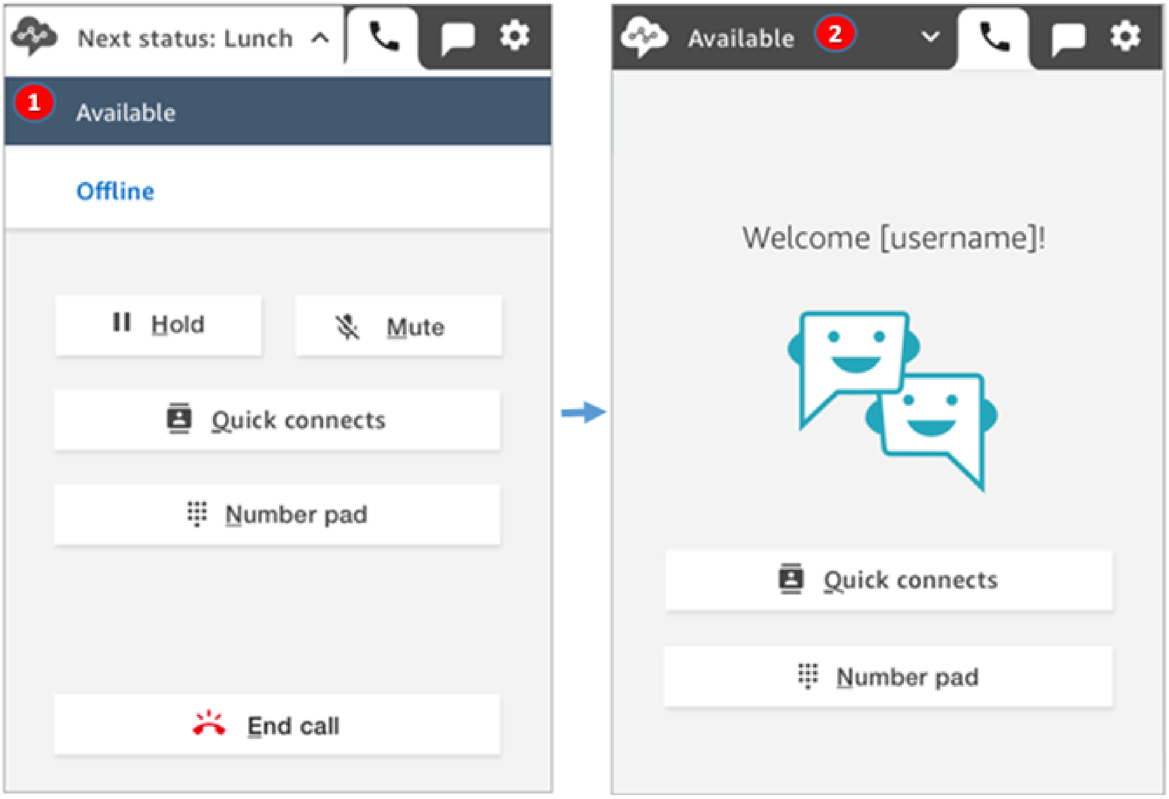


1. The agent is on a contact.
2. The agent chooses their next status, such as **Lunch**. They can choose only a custom (NPT (p. 923)) status, or **Offline**.
3. The agent is in **Next status: Lunch**. They are still on contact. No new contacts can be routed to them.
4. The contact ends. The agent finishes ACW, and chooses **Clear contact**. Instead of going back to **Available**, their CCP is automatically set to **Lunch**.

How to cancel "Next status"

You can easily switch from **Next status** back to **Available**. The ability to switch your status is useful, for example, if you accidentally choose **Next status: Lunch**, or if you decide not to go to **Lunch** before Amazon Connect automatically sets to that status.

The following images show this workflow.



1. While working on the same contact, the agent cancels **Next status: Lunch** and goes back to **Available**.
2. The contact ends and the agent is still **Available** for new contacts to be routed to them.

Example 1: Set "Next status" while handling only ACW contacts

Let's say an agent is finishing after contact work (ACW) for one or more contacts, such as a voice contact or multiple chats. They are not on contact with anyone.

Instead of choosing **Clear contact** when the agent finishes ACW, they choose **Lunch**. This puts them in **Next status: Lunch** only briefly.

Here's what happens in this scenario:

1. Agent finishes ACW and chooses **Lunch** instead of **Clear contact**.
2. Amazon Connect stops routing new contacts to them.
3. All their slots are cleared. This is so the agent doesn't have to choose **Clear contact** to end the ACW.
4. Because all the ACWs have been cleared, Amazon Connect immediately starts the automatic transition that sets the agent's status to **Lunch**.

   Agents were put into **Next status - Lunch** only briefly (milliseconds!). They might even see it in the CCP if they look fast enough.

This order of events mirrors how the CCP works when agents change their status while working on ACW. For example, an agent is finishing ACW and they set their status to **Lunch**. Here's what happens next:

1. Amazon Connect stops routing new contacts to them.
2. The ACW slot is cleared for the agent so they don't have to choose **Clear contact**.
3. The agent is set to **Lunch**.

Example 2: Set "Next status" while managing some chats on contact and other chats in ACW

Let's say an agent is managing two chats:

- Customer 1 is in ACW.
- Customer 2 is on contact.

While still on a contact, the agent sets their status to **Offline**. This puts them in the **Next status: Offline** state.

Here's what happens in this scenario:

1. The agent sets their status to **Offline**.
2. Amazon Connect stops routing new contacts to them.
3. The contact that is in ACW is cleared so the agent doesn't have to choose **Clear contact**. Only the connected chat remains.
4. The agent's status is **Next status: Offline**, and they continue working on their connected chat.
5. After they finish work on that contact, the agent chooses **Clear contact** to end the ACW.
6. Amazon Connect automatically sets the agent's status to **Offline**.

Chat with contacts

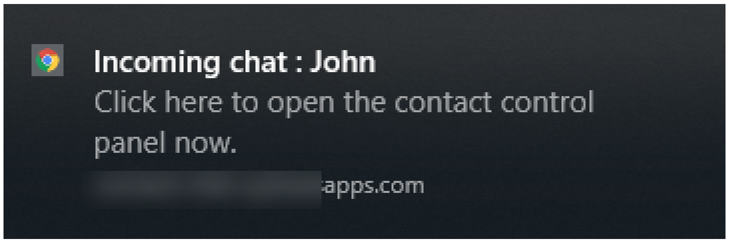
When you set your status in the CCP to **Available**, Amazon Connect delivers calls or chats to you, based on the settings in your routing profile (p. 227). An administrator can specify that up to 10 chat conversations can be routed to you at the same time.

You can't initiate chat conversations from the CCP.

> **Note**
> IT Administrators: To enable customers and agents to send attachments, such as files, through the chat interface, see Enable attachments to share files using chat (p. 142).
>
> **Tip**
> Amazon Connect routes contacts to you for only one channel at a time. When you're on a call, you won't be routed a chat conversation. And when you're handling chat conversations, you won't be routed a call.

When a chat contact arrives, here's how you are notified:

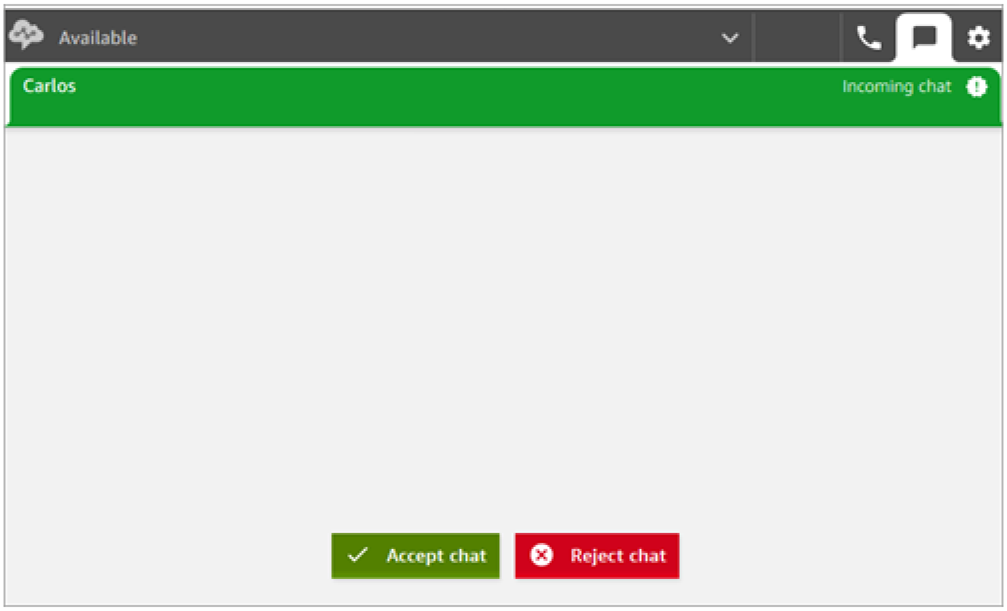
1. If you enabled notifications in your browser, you'll get a pop-up notification at the bottom of your screen, like this:



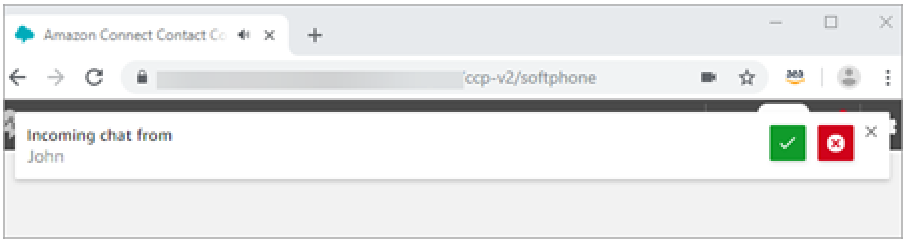
Incoming chat : John

Click here to open the contact control panel now.

2. If you're on the chat tab, the page displays the name of the contact and a button for you to connect to the chat.

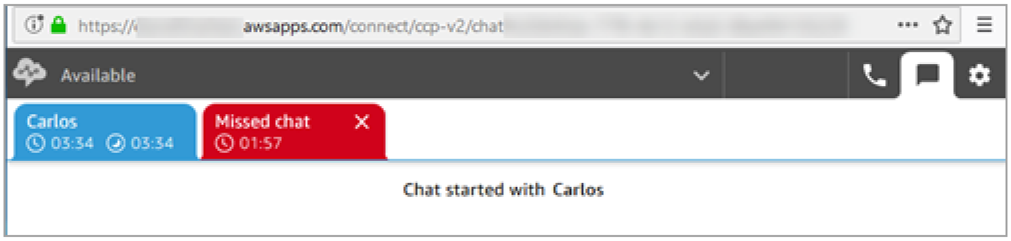


3. If you're on the phone tab, a banner displays the name of the contact and a button for you to connect to the chat.



Incoming chat from
John

4. You have 20 seconds to accept or reject a contact. If you're on a chat, and another comes in but you don't accept it, a tab appears indicating the chat was missed.



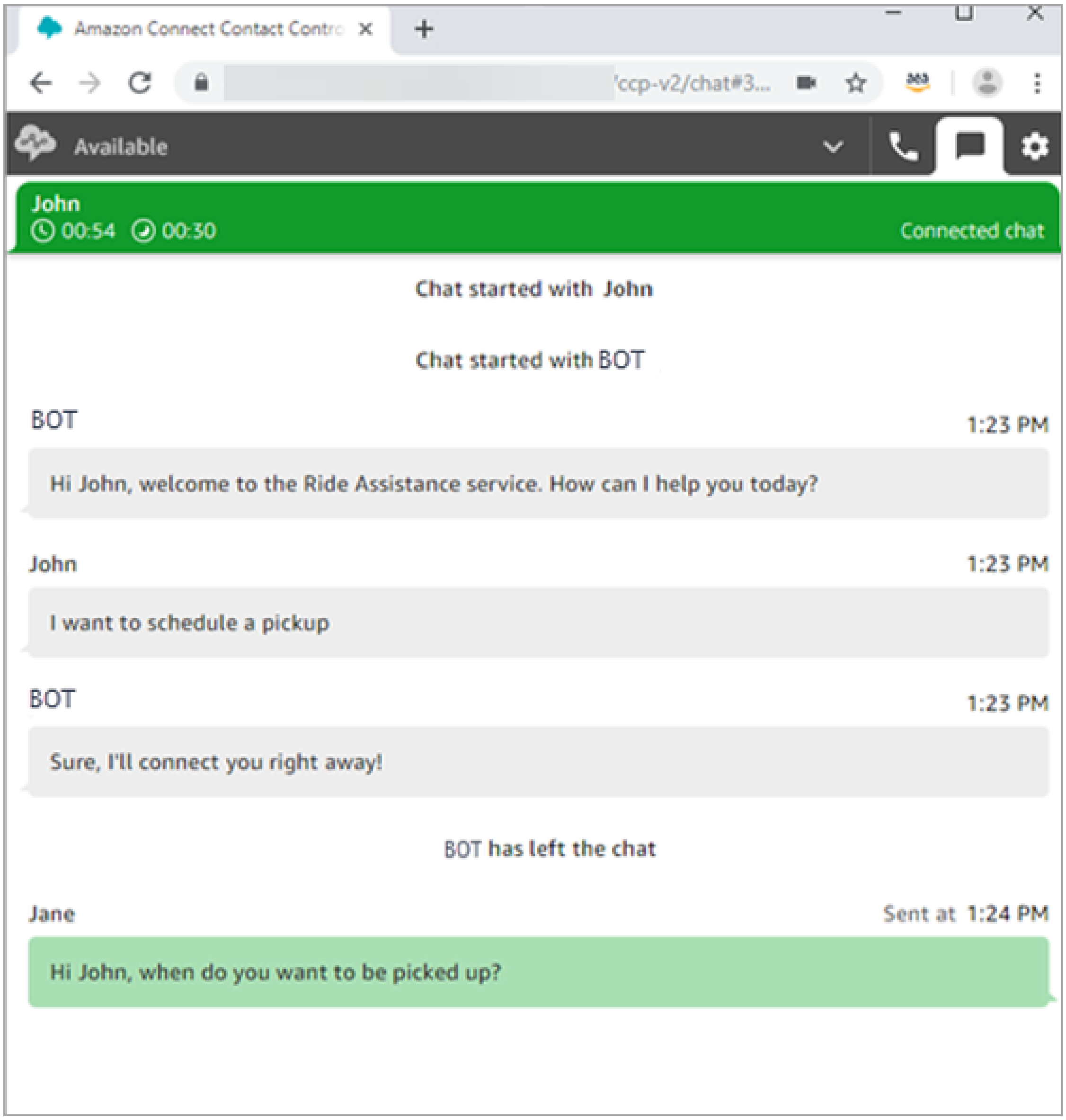
Chat started with Carlos

5. Choose **Accept chat** to connect to the contact.

   Note

   Chat conversations must be accepted manually. There's no auto-accept for these conversations.

6. You'll see the full transcript of what the contact has already typed. If applicable, you'll also see what a bot or another agent has entered. In the following image, **John** is the name of the customer, **BOT** is the Amazon Lex bot, and **Jane** is the name of the agent.



Chat started with John

Chat started with BOT

BOT 1:23 PM

Hi John, welcome to the Ride Assistance service. How can I help you today?

John 1:23 PM

I want to schedule a pickup

BOT 1:23 PM

Sure, I'll connect you right away!

BOT has left the chat

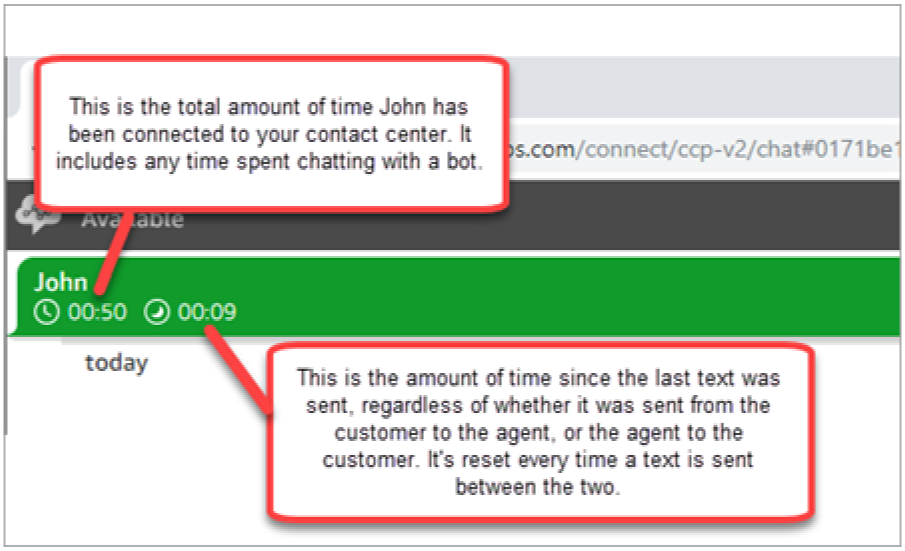
Jane Sent at 1:24 PM

Hi John, when do you want to be picked up?

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:

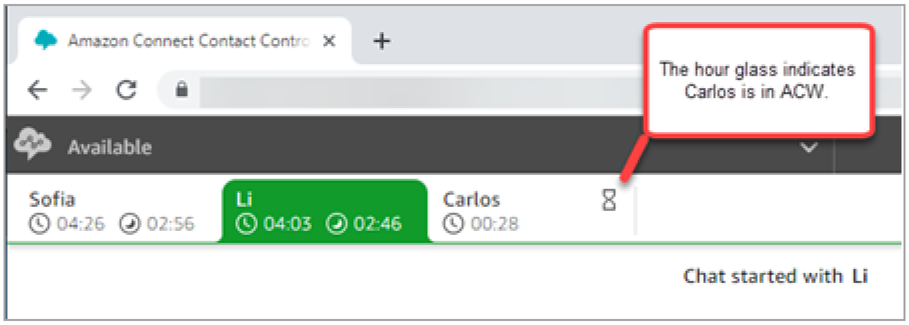
- How long the contact has been connected to your contact center. This includes the time spent with the bot, if you're using one.
- How long since the last text was sent. This can be either from the customer to the agent, or from the agent to the customer. the timer is reset with each text message.



This is the total amount of time John has been connected to your contact center. It includes any time spent chatting with a bot.

This is the amount of time since the last text was sent, regardless of whether it was sent from the customer to the agent, or the agent to the customer. It's reset every time a text is sent between the two.

If you have multiple chat tabs open, an hour glass appears letting you know which ones are in an After Contact Work (ACW) state. The timer indicates how long the contact has been in ACW.



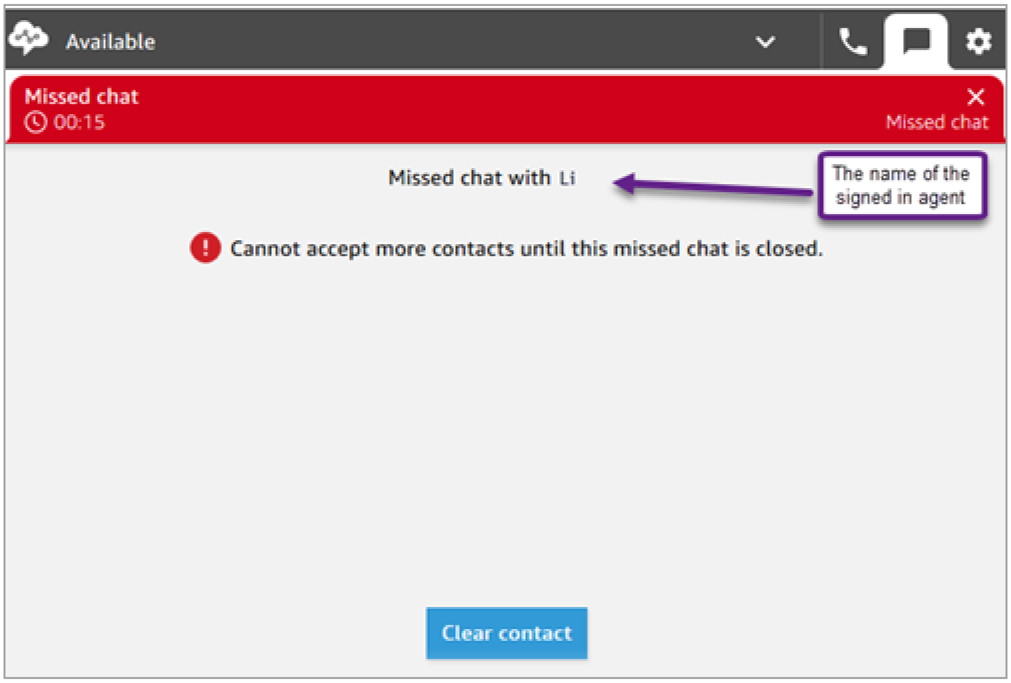
The hour glass indicates Carlos is in ACW.

What happens to missed chats?

Let's say you take a break but forget to change your status in the CCP from **Available** to **Break**. Amazon Connect tries to route a chat to you for 20 seconds. Keep in mind that your admin can't configure this amount of time.

After 20 seconds, the contact is counted as Agent non-response (p. 918) 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.



Missed chat 00:15

Missed chat

Missed chat with Li

The name of the signed in agent

Cannot accept more contacts until this missed chat is closed.

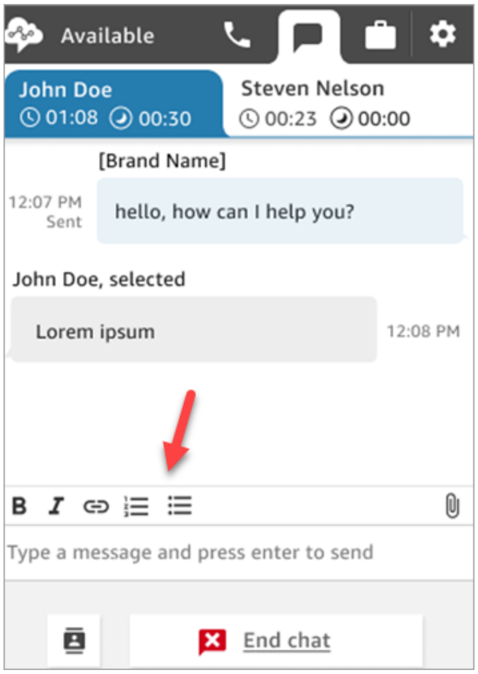
You can clear the slots so that chats are routed to you again. For each missed contact, choose the banner, and then choose **Clear contact**.

How to format messages

When composing a chat message, you have the ability to format your message. This enables you to add structure and clarity to your support messages. You can add the following formatting:

- Bold
- Italic
- Bulleted list
- Numbered list
- Hyperlinks
- Attachments

To get started, highlight the text you want to format, and then select a the formatting options from the toolbar. You can see exactly what the message looks like before sending it.



[Brand Name]

12:07 PM Sent

hello, how can I help you?

John Doe, selected

Lorem ipsum

12:08 PM

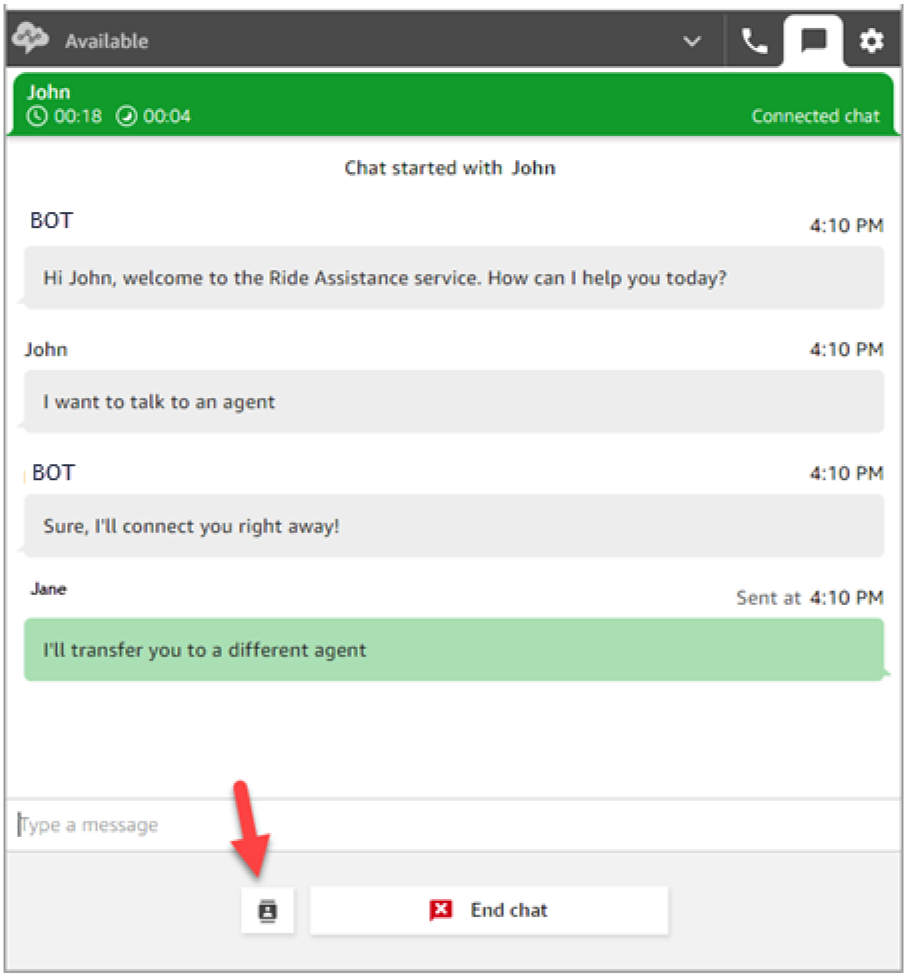
Tip
Developers: Enable this feature from the chat user interface. For instructions, see Enable text formatting for your customer's chat experience (p. 257).

Transfer chats to another queue

When a chat is transferred from a bot to an agent, or from an agent to another queue, all context is preserved. This context lets the next agent read all previous messages in that contact.

To transfer a customer to another queue

1. Choose the **Quick Connect** button at the bottom of the CCP page.



Chat started with John

BOT 4:10 PM

Hi John, welcome to the Ride Assistance service. How can I help you today?

John 4:10 PM

I want to talk to an agent

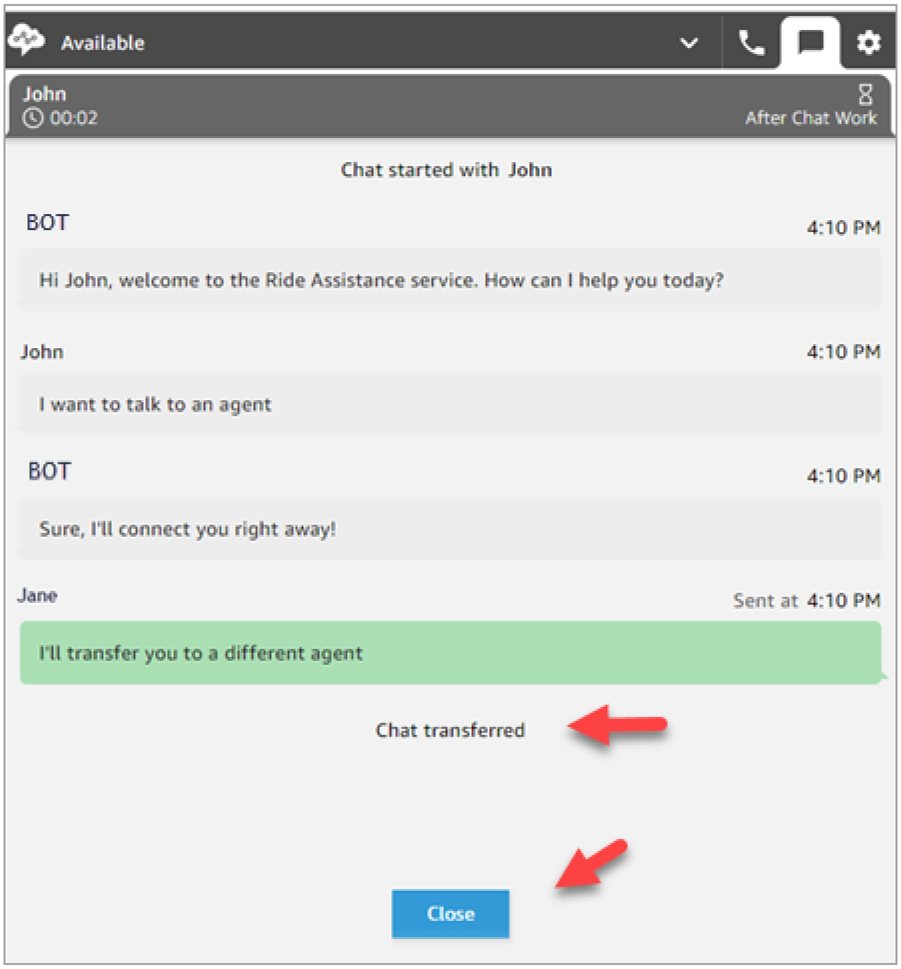
BOT 4:10 PM

Sure, I'll connect you right away!

Jane Sent at 4:10 PM

I'll transfer you to a different agent

2. Choose or search for the queue you want to transfer to, and then choose the transfer button.
3. You'll see a confirmation message. You're now doing After Contact Work (ACW) for the customer. Choose **Close** to end the contact.



Available

John
00:02

After Chat Work

Chat started with John

BOT 4:10 PM

Hi John, welcome to the Ride Assistance service. How can I help you today?

John 4:10 PM

I want to talk to an agent

BOT 4:10 PM

Sure, I'll connect you right away!

Jane Sent at 4:10 PM

I'll transfer you to a different agent

Chat transferred

Make a call while on a chat

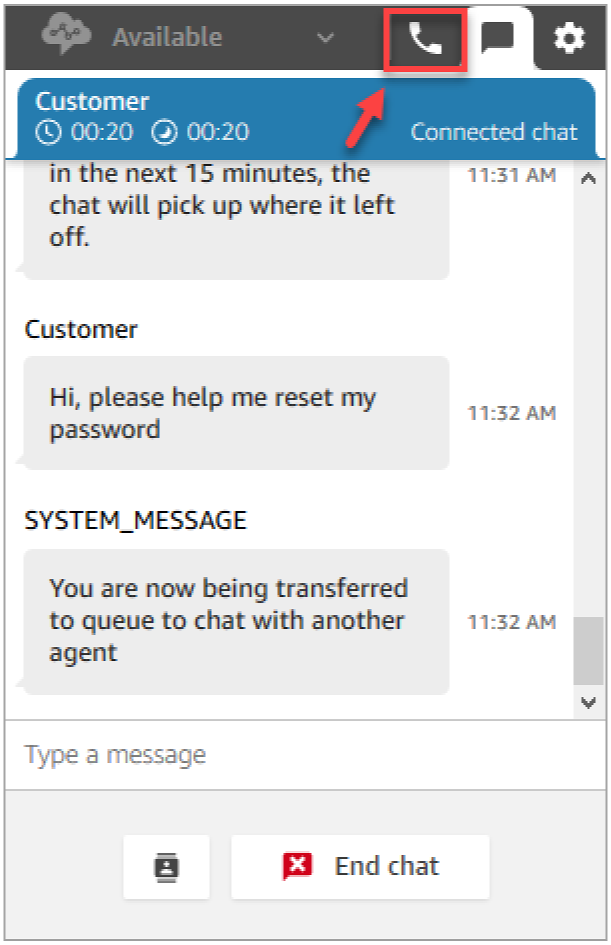
Let's say you're chatting with a contact and you want to consult with someone else. While you're on a chat, you can use the updated CCP to make outbound calls using the number pad and external quick connects (p. 466).

Note the following limitations:

- You can't access agent quick connects while you're on a chat.
- Agents can't receive calls while on a chat.

To make an external call while you're on a chat

1. In the CCP, choose the phone tab.



in the next 15 minutes, the chat will pick up where it left off. 11:31 AM

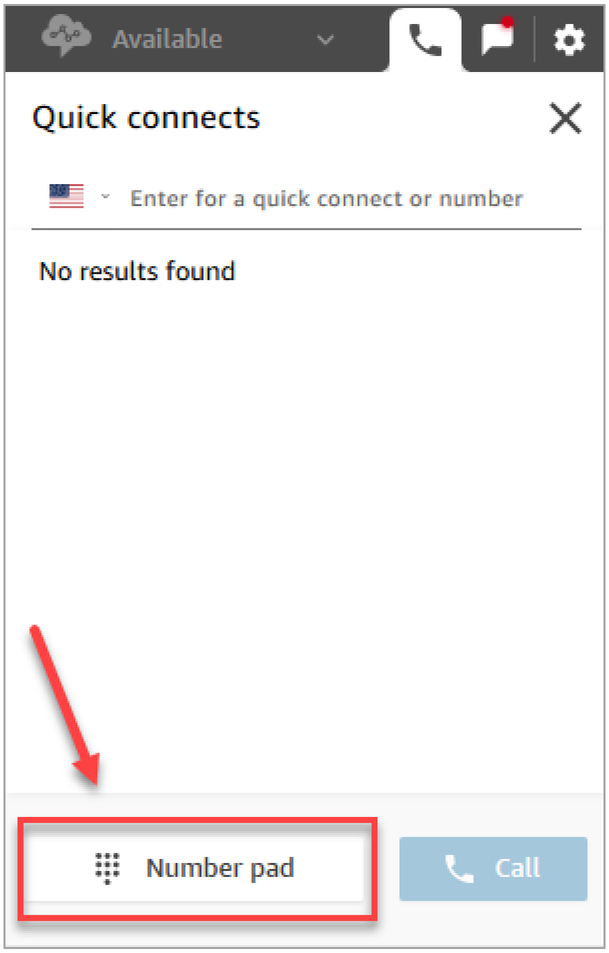
Customer

Hi, please help me reset my password 11:32 AM

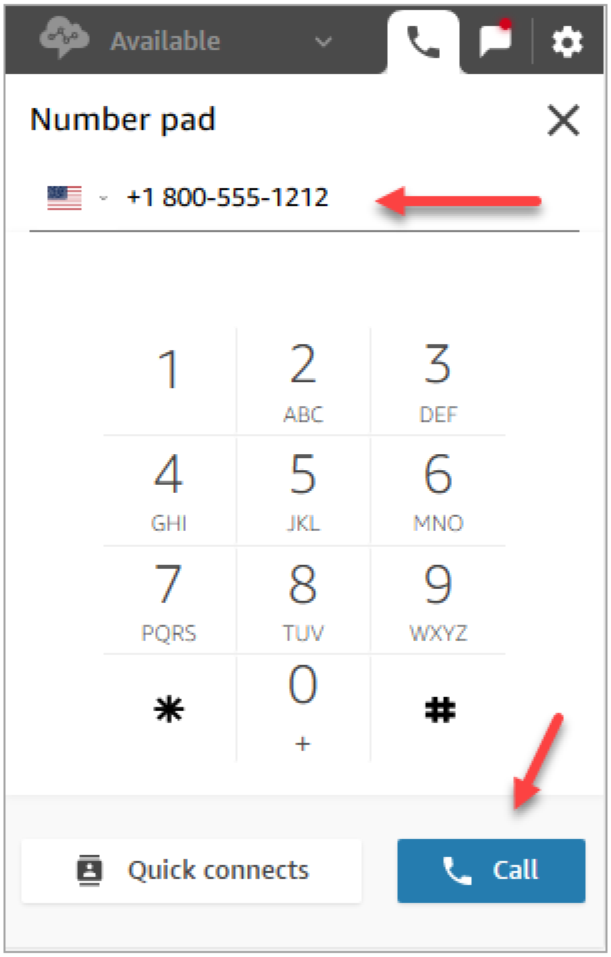
SYSTEM_MESSAGE

You are now being transferred to queue to chat with another agent 11:32 AM

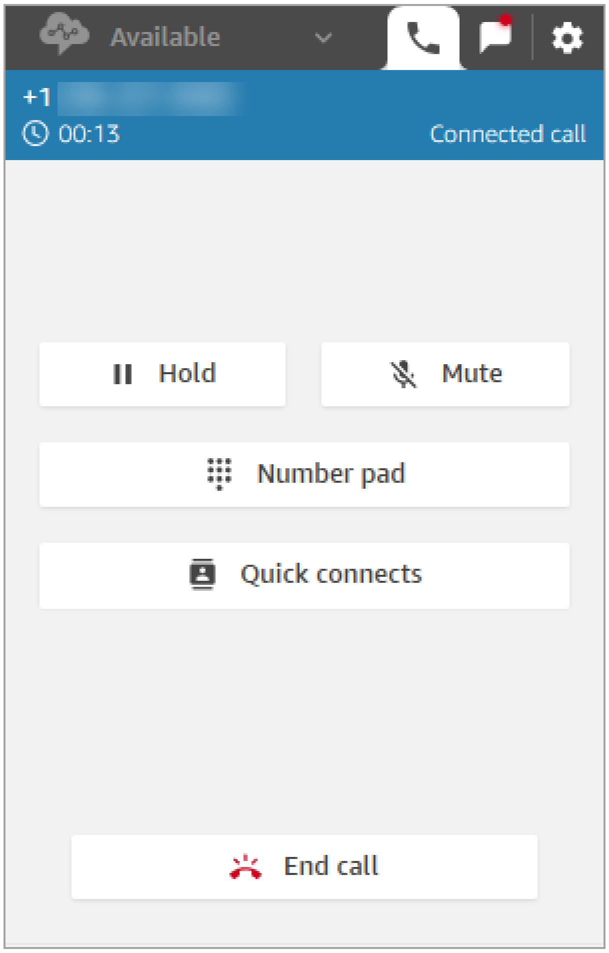
2. Choose **Number pad**.



3. Enter the external number you want to call, and then choose **Call**.



4. You'll be connected to the call at the same time the chat is still ongoing, as shown in the following image.



5. To go to the chat conversation while you're on the phone, choose the chat tab.
6. To end the phone conversation, choose the phone tab, choose **End call**, and then choose **Clear contact**. You're still connected to the chat conversation.

Can't make outbound call to another agent

If you're on a chat and having trouble making an outbound call to another agent, that agent may be handling a chat conversation. They can't receive a call while on a chat.

Can't see external quick connects in the CCP

Agent quick connects (p. 466) are not visible in the CCP while you're on a chat.

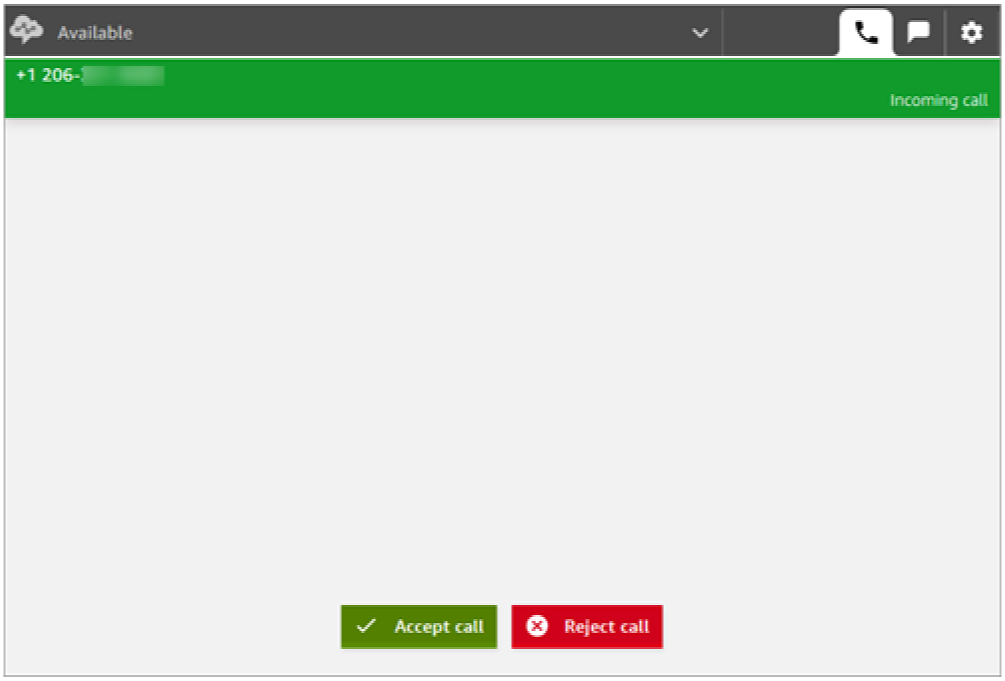
If you can't see external quick connects (p. 466) in your CCP, however, check that the external quick connect has been added to your queue as described in Step 2: Enable agents to see quick connects (p. 466).

Enable agent quick connects for calls during a chat

To enable agents to consult over the phone with each other while they are on chats, your Amazon Connect administrator needs to set up a direct dial number (DID) that routes to the agent. This configuration incurs additional costs.

Accept incoming calls

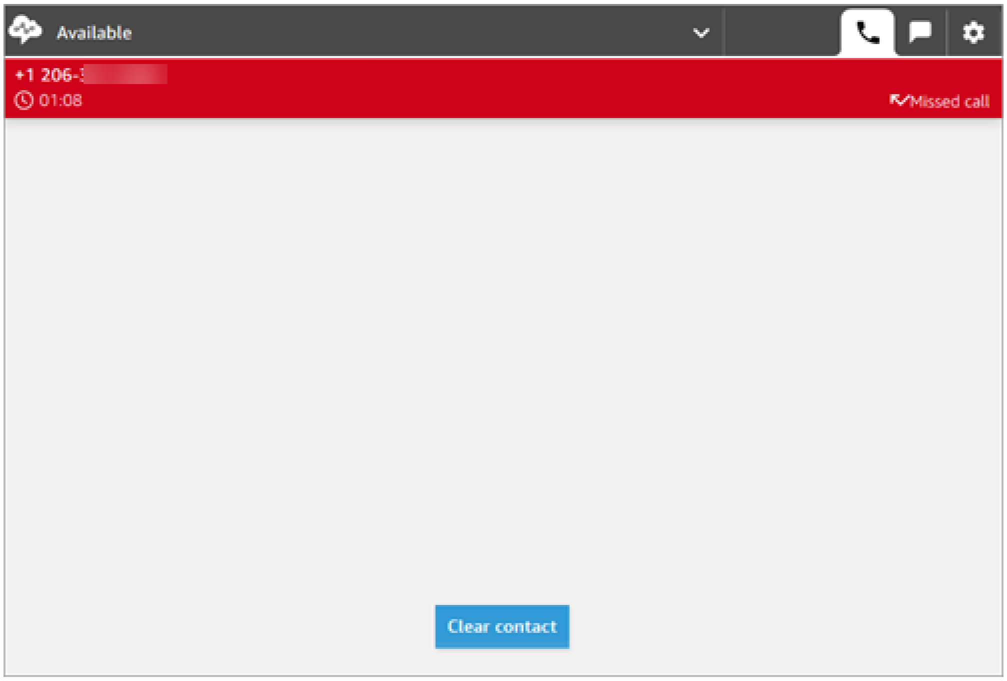
1. Whenever you set your status in the CCP to **Available**, Amazon Connect can deliver calls to you, based on the settings in your routing profile (p. 227).



2. When a call arrives, choose the **Accept call** button.

   Note
   The **Accept call** button does not appear if your admin has configured your user profile for Auto-Accept Call (p. 234).

3. Before you're connected to the contact, Amazon Connect announces the name of the originating queue.
4. You're now talking to the contact.
5. You have 20 seconds to accept or reject a contact. If you miss a call, it will look similar to the following image. Choose **Clear contact** so you can accept another call.

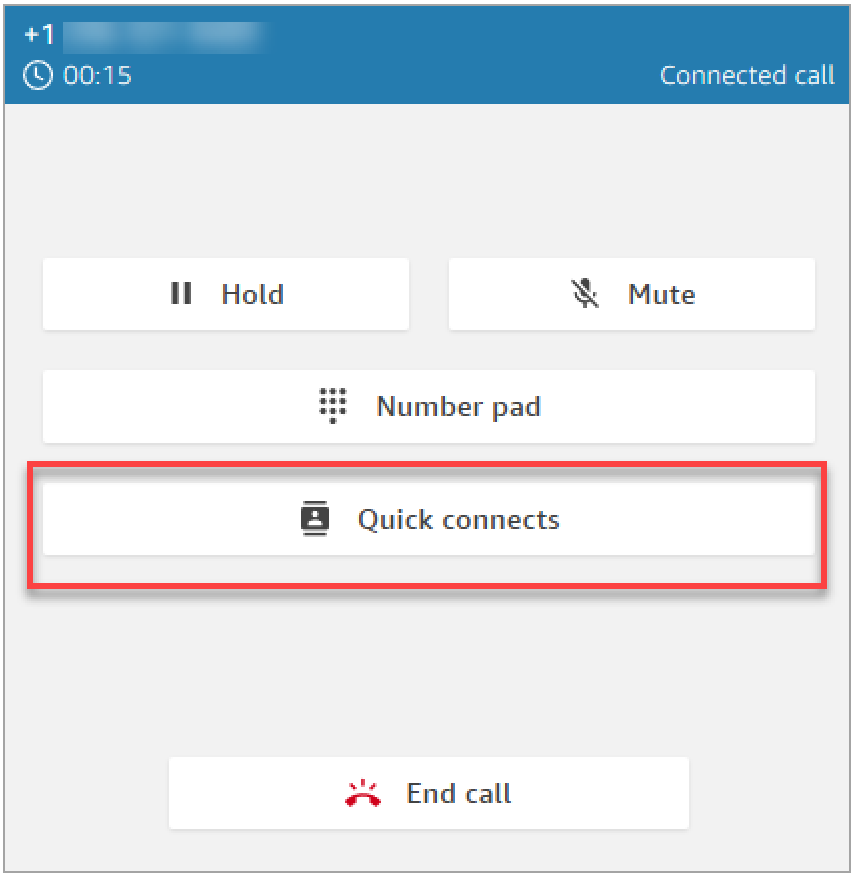


Transfer calls to a quick connect or external number

You can transfer calls to people in a predefined list, called quick connects. You can also transfer calls to external phone numbers that you enter.

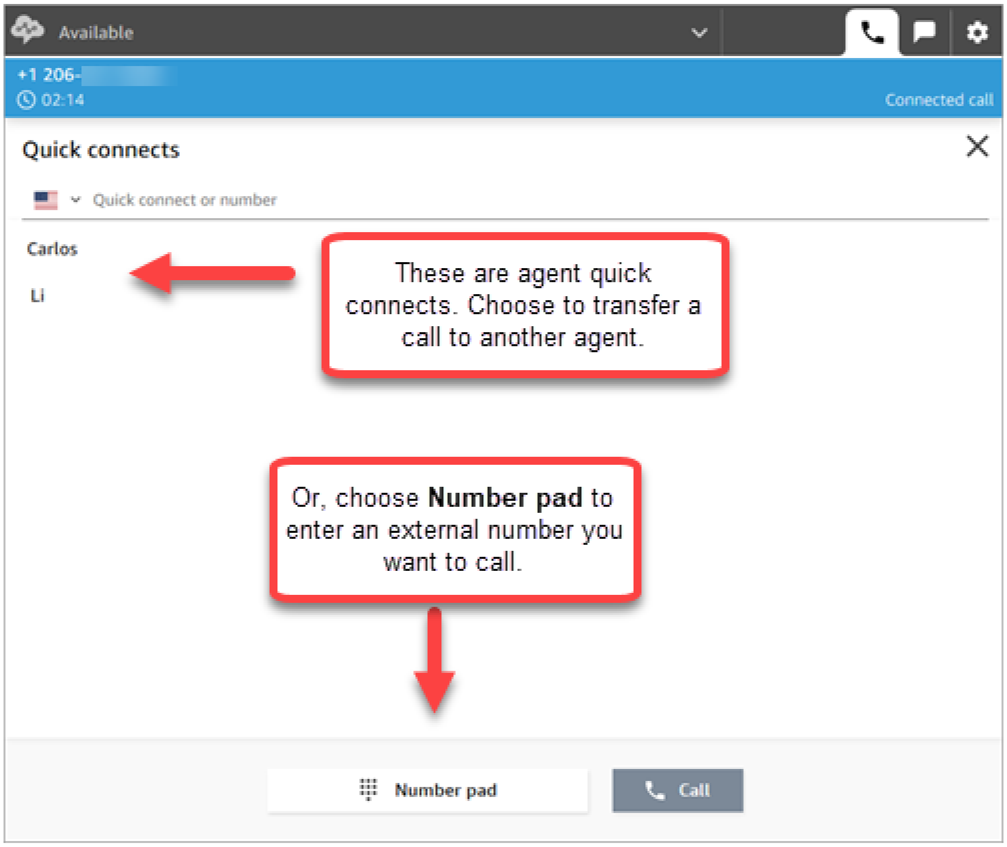
To transfer to a quick connect or to an external number

1. While you're connected to the contact, choose **Quick connects** on the CCP.



2. From the list of quick connects, choose the name of another agent to transfer the call to. (Your Amazon Connect administrator adds the names of agents to the list of quick connects.)

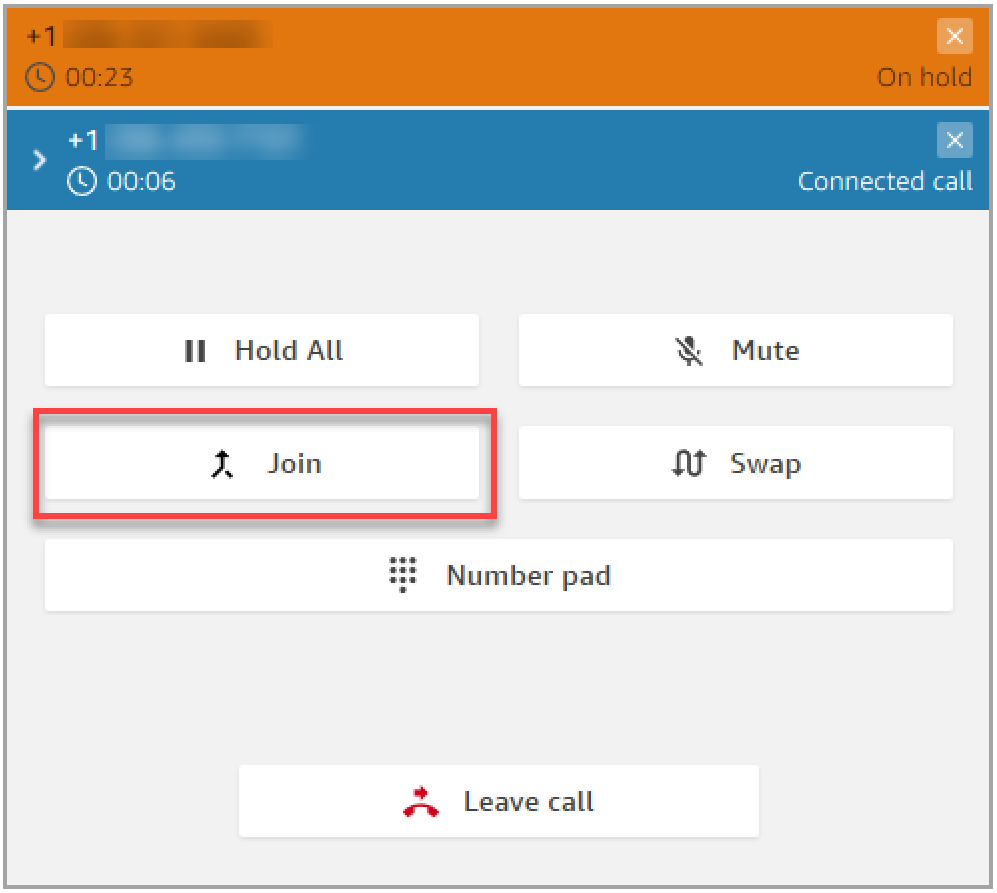
   Or, to call an external number, choose **Number pad**, enter the number you want to call, and then choose **Call**.



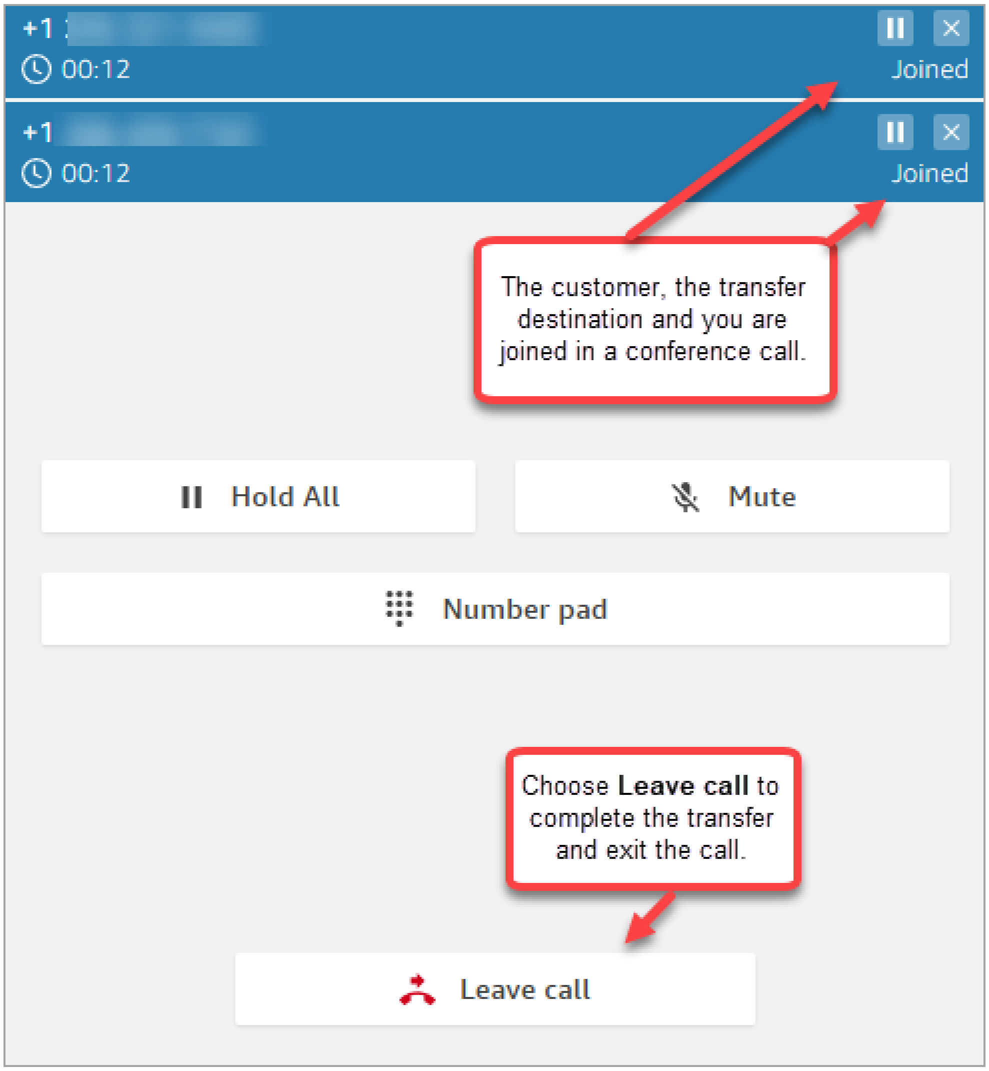
These are agent quick connects. Choose to transfer a call to another agent.

Or, choose **Number pad** to enter an external number you want to call.

3. After the call is connected to the transfer destination, you can choose **Join** so the caller, the transfer destination, and you are in a conference call.



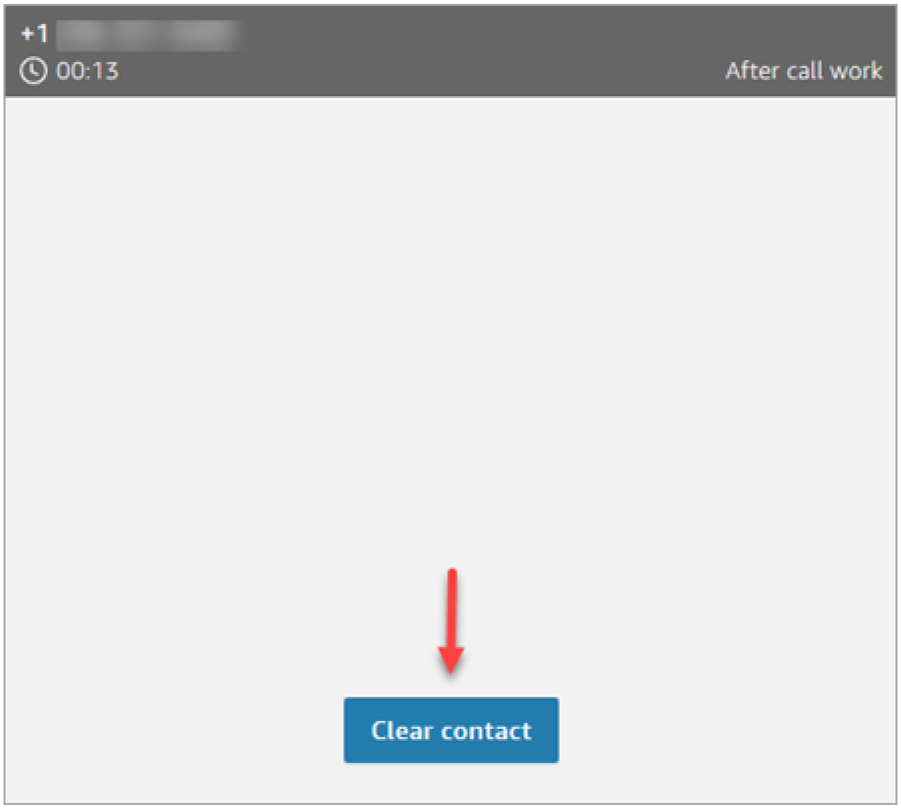
4. When the call is joined, the three of you can talk. Choose **Leave** to complete the transfer and exit the call.



The customer, the transfer destination and you are joined in a conference call.

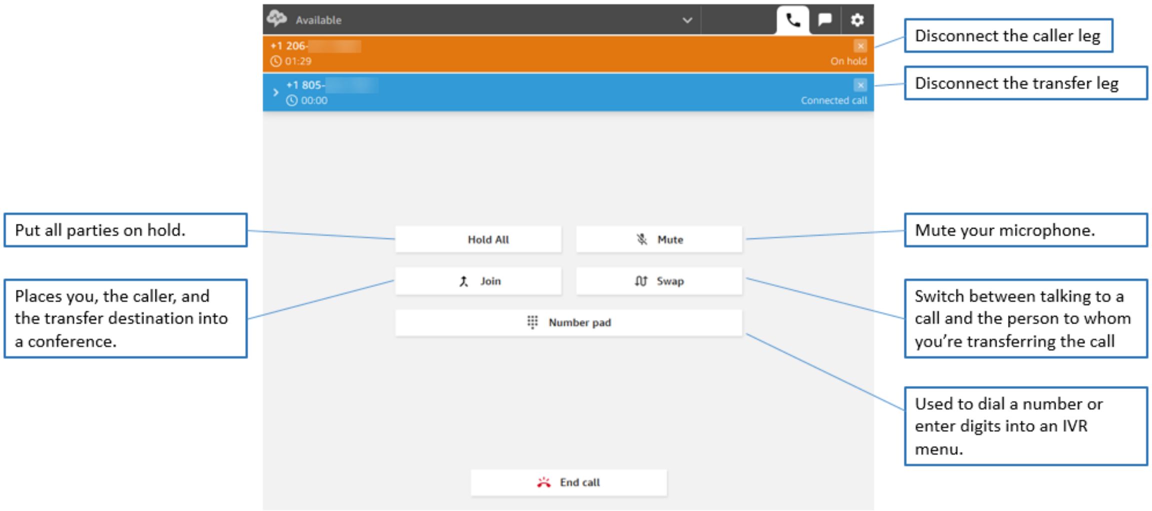
Choose **Leave call** to complete the transfer and exit the call.

5. Complete the after contact work and then choose **Clear contact**.



Manage transfer a call

After you initiate a transfer, the customer is placed on hold and you are connected to the transfer destination. The following image shows what actions you can take at this point.



Disconnect the caller leg

Disconnect the transfer leg

Put all parties on hold.

Mute your microphone.

Places you, the caller, and the transfer destination into a conference.

Switch between talking to a call and the person to whom you're transferring the call

Used to dial a number or enter digits into an IVR menu.

Multi-party calls: Add additional participants to an ongoing call

You can add up to **4** additional participants to an ongoing customer service call, for a total of **6** participants.

By using quick connects or your number pad, you can add other agents, supervisors, or external participants.

For example, to help close a mortgage transaction, an agent at a financial services company can add a mortgage broker, the customer's spouse, a translator, and a supervisor to the call to help resolve any issues quickly.

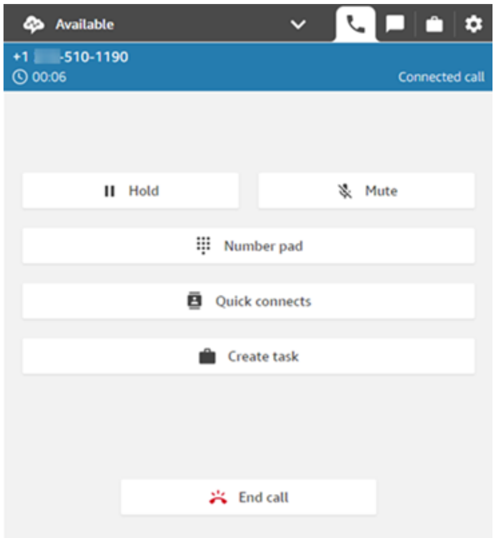
For information about how multi-party calls differs from the default three-party calls, see Comparison: Three-party and multi-party calls (p. 1224).

Important things to know

- This feature is only available in CCPv2 and custom CCP using Amazon Connect Streams.js.
  - **IT administrators**:
    - Before enabling the multi-party calls feature, if you are using Contact Lens or planning to do so in the future, see Multi-party calls and Contact Lens (p. 818).
    - By default, there can be three participants on a call (for example, two agents and a caller, or an agent, a caller, and an external party). Before enabling multi-party calling, see Comparison: Three-party and multi-party calls (p.). To enable agents to connect up to six parties on a call, see Update telephony options (p. 140).
  - **Developers**: In custom CCPs, use the updated Amazon Connect Streams API to enable multi-party calling, up to six parties. See the Amazon Connect Streams documentation on GitHub. Before enabling multi-party calling, see Comparison: Three-party and multi-party calls (p.).
- **AWS GovCloud (US-West)**: You can't enable this feature using the console user interface. Instead, use the UpdateInstanceAttribute API or contact AWS Support.

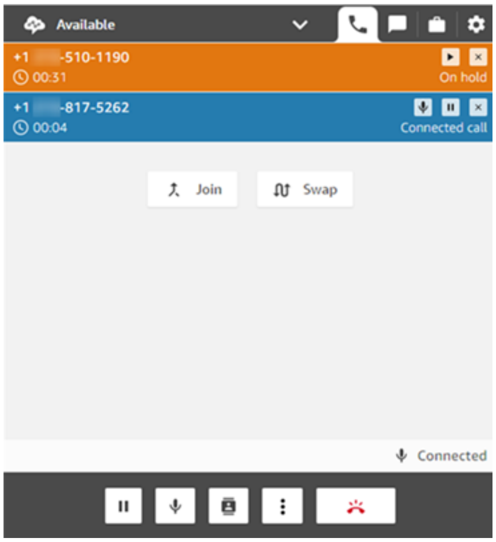
How to add participants to a multi-party call

1. The following image shows the contact and you (the agent) on a call. The customer always appears at the top.



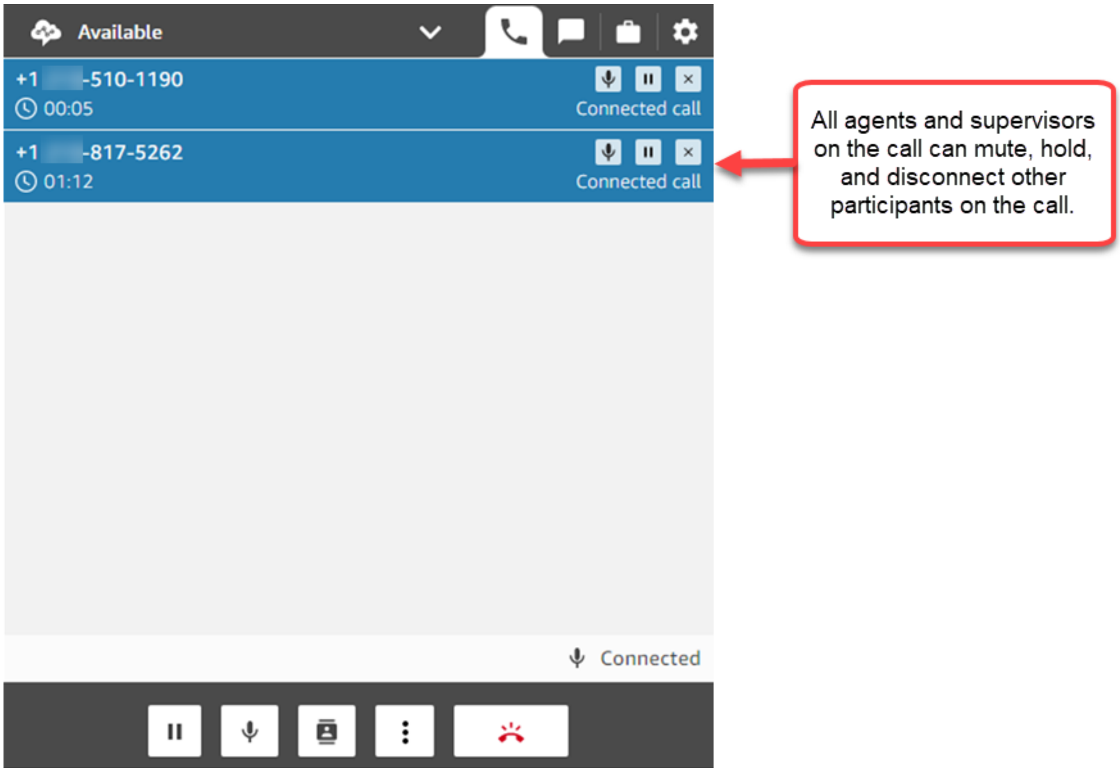
2. While you're connected to the contact, choose **Quick connects** to add another agent or the **Number pad** to make an external call. The caller is put on hold while you do this.
3. When you add the third participant to the call, you can greet and talk to them before adding them to the call (for example, tell them why you are adding them to the call).

   The following image shows what the CCP looks like when you add a third participant to the call. The contact is on hold, and you're talking to the third party. Choose **Join** to take all parties off hold. Or, choose **Swap** to toggle between the parties on hold and the party you just called.



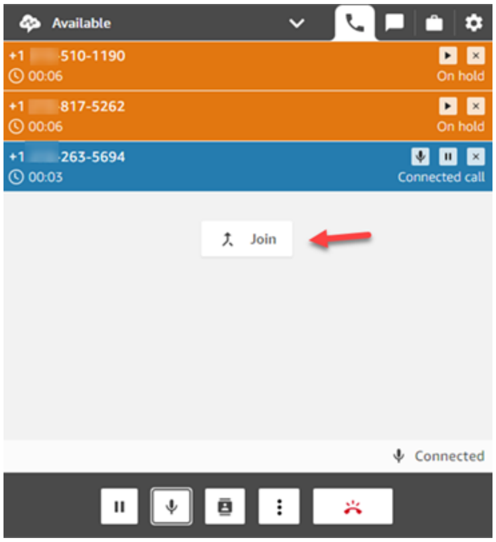
   Note
   Swap is only available when there are three parties on a call (for example, you, the caller, and another agent or external party). It is not available when there are more than three parties on the call.

4. When there are multiple agents on the call (for example, three agents and a caller), all agents on the call can view all parties and have the option to put any participant or another agent on hold, mute, and disconnect participants from the call.



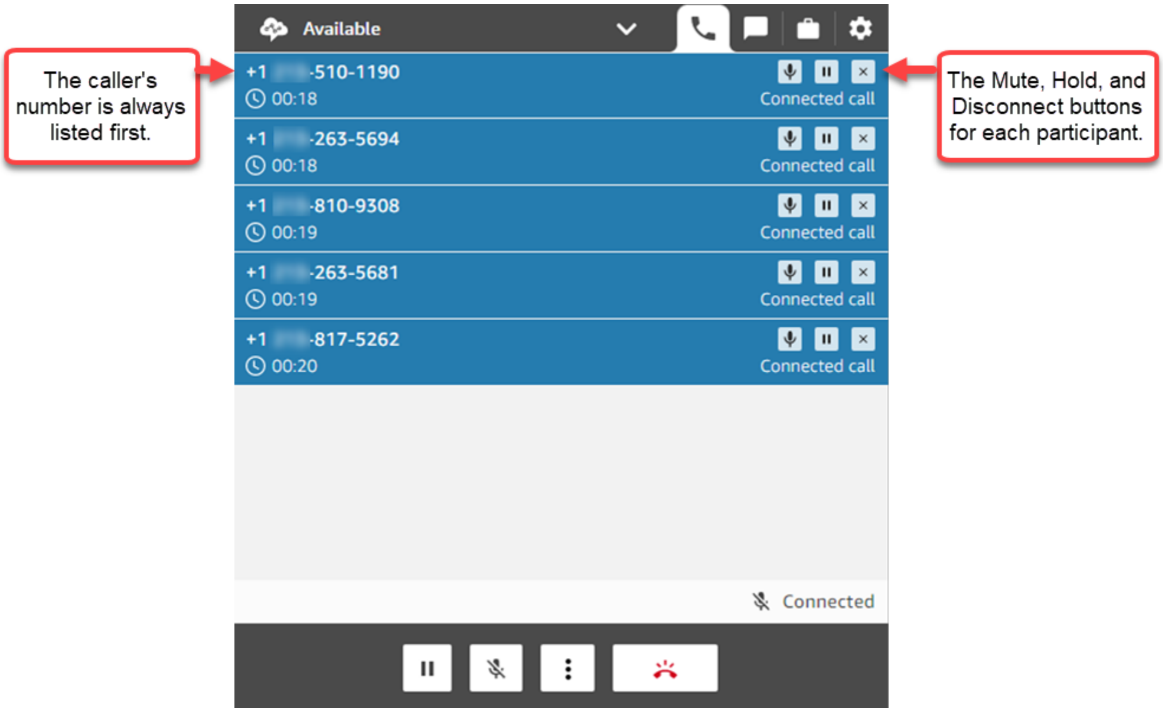
All agents and supervisors on the call can mute, hold, and disconnect other participants on the call.

5. Every time you add a new participant to the call, you are prompted to greet and talk to them before adding them to the call. Choose **Join** to take all parties off hold.



How to manage participants

Every agent on the call has access to the controls next to each participant's number to mute, hold, or disconnect individual participants.

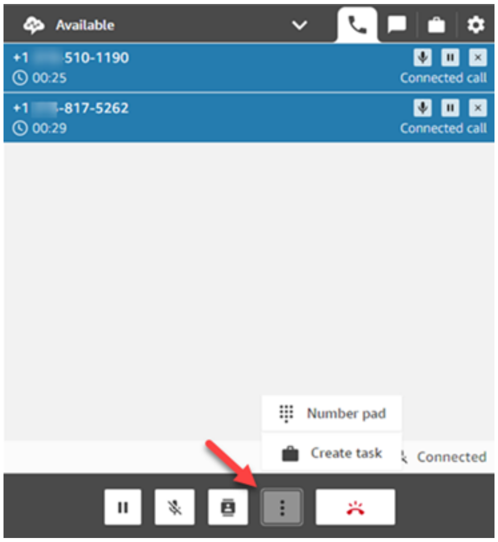


The caller's number is always listed first.

The Mute, Hold, and Disconnect buttons for each participant.

You can transfer a multi-party call to another agent, or disconnect yourself from the ongoing call.

Choose the **More** button to open the number pad and to create a task:



When do multi-party calls end?

A multi-party call stays up as long as the caller or the agent is on the call. For example, add an external party to a call and then you disconnect. The caller and external party continue the call.

If only third-parties are left on the line, the contact is terminated. However, as the agent you can choose to disconnect and allow only the caller and the third-party participants to remain on the call.

Make outbound calls

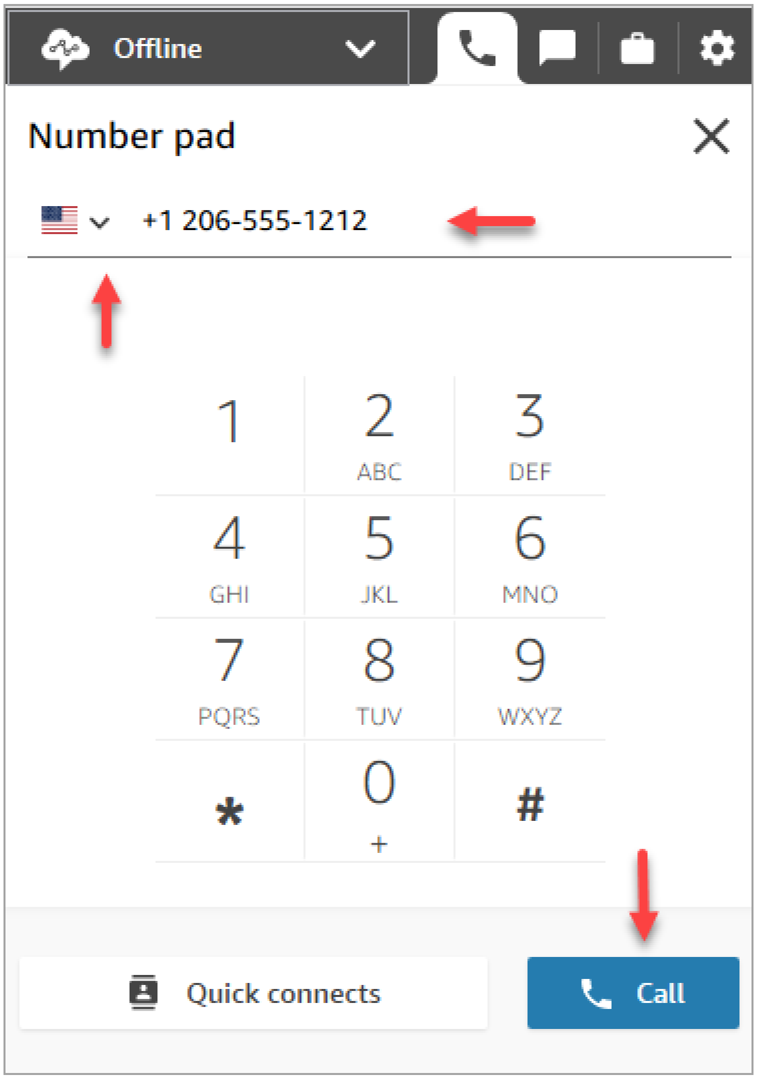
Before you can make an outbound call, your contact center must be set up to allow agents to make calls. For more information, see Step 3: Set telephony (p. 137) in Create an Amazon Connect instance (p. 135).

For information about the caller ID that's displayed when you make an outbound call, see Set up outbound caller ID (p. 212).

> **Note**
> **IT administrators**: For a list of countries available for outbound calls based on the Region of your instance, see Amazon Connect pricing. If a country is not available in your dropdown menu, open a ticket to add it to your allow list. For more information, see Countries you can call (p. 1214).

To make an outbound call

1. In your Contact Control Panel, choose **Number pad**.
2. Use the dropdown menu to choose the country, then enter the number.

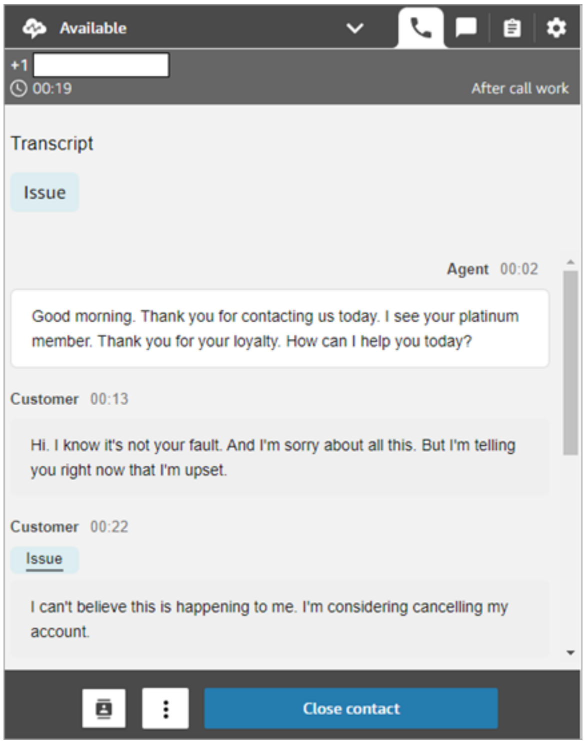


3. Choose **Call**.

View a call transcript during ACW

At the end of a call, you can see an unredacted transcript of your conversation in the CCP or agent application. You can view the entire transcript for reference, and copy any useful text into your notes.

The call transcript displays any categories (p. 580) identified by Contact Lens. For example, in the following image, an issue has been identified at 22 seconds.



Agent 00:02

Good morning. Thank you for contacting us today. I see your platinum member. Thank you for your loyalty. How can I help you today?

Customer 00:13

Hi. I know it's not your fault. And I'm sorry about all this. But I'm telling you right now that I'm upset.

Customer 00:22

Issue

I can't believe this is happening to me. I'm considering cancelling my account.

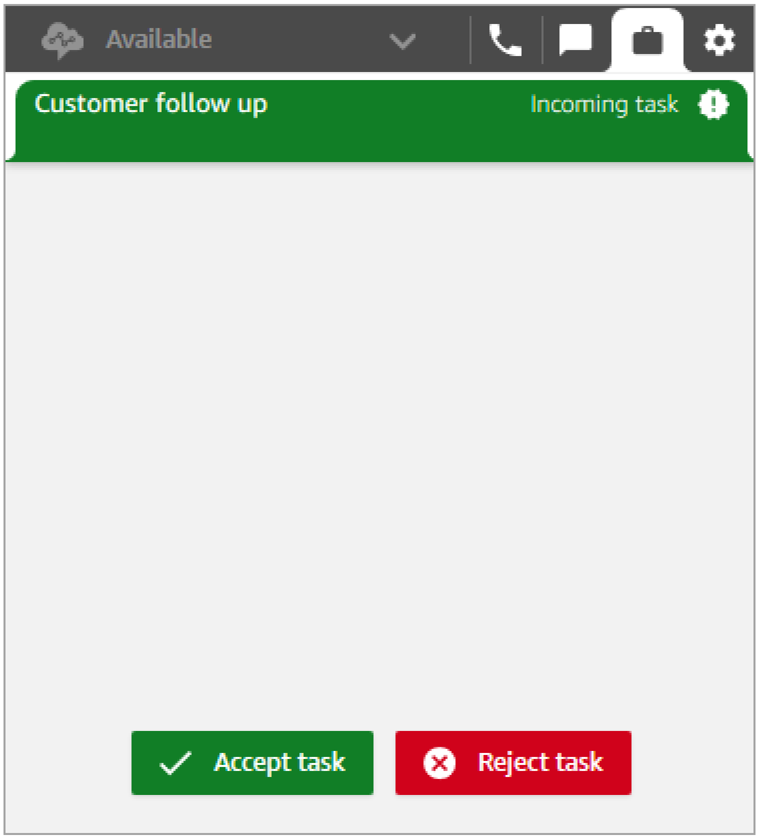
If a call is transferred to you from another agent, you will see an unredacted transcript of their conversation with the customer.

Customer sentiment score is not included in the CCP or agent application.

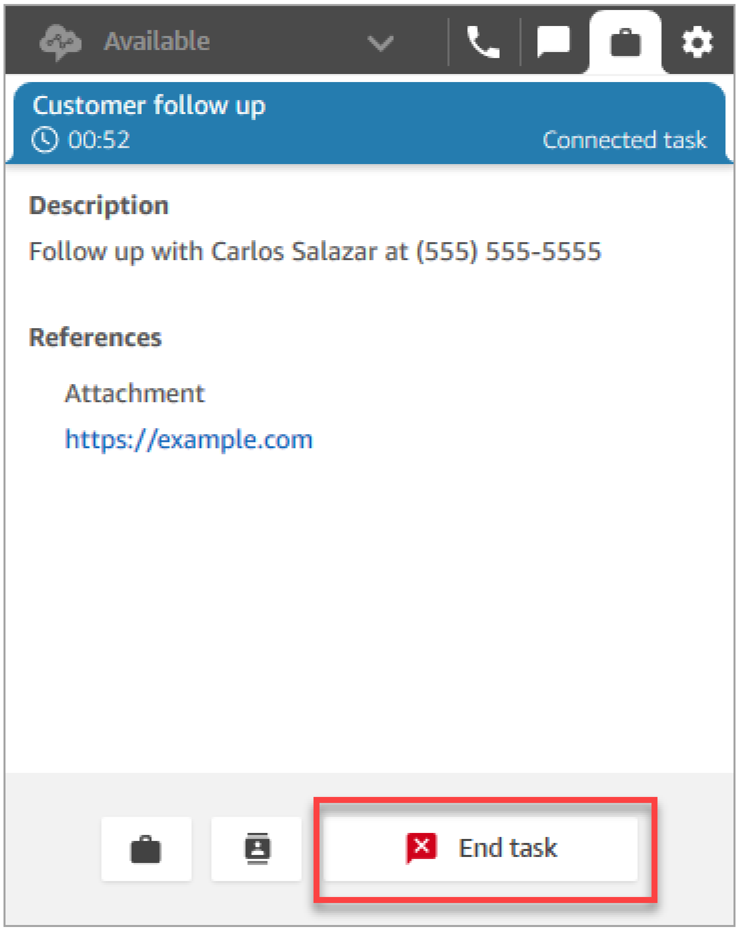
> **Note**
> **IT administrators**: This feature is available in the CCP and the agent application. To make this feature available to agents:
>
> 1. Enable Contact Lens (p. 812) for your Amazon Connect instance.
> 2. Add the following permissions to the agent's security profile:
>   - **Analytics** - **Contact Lens - speech analytics**
>   - **Analytics** - **Recorded Conversations - unredacted (access)**
>   - **Contact Control Panel (CCP)** - **Contact Lens data**

Accept a task

1. Whenever you set your status in the CCP to **Available**, Amazon Connect can deliver tasks to you, based on the settings in your routing profile (p. 227).



2. When a task arrives, choose **Accept task**.
3. Review the description of the task, and choose the links as needed to complete the task.



Description

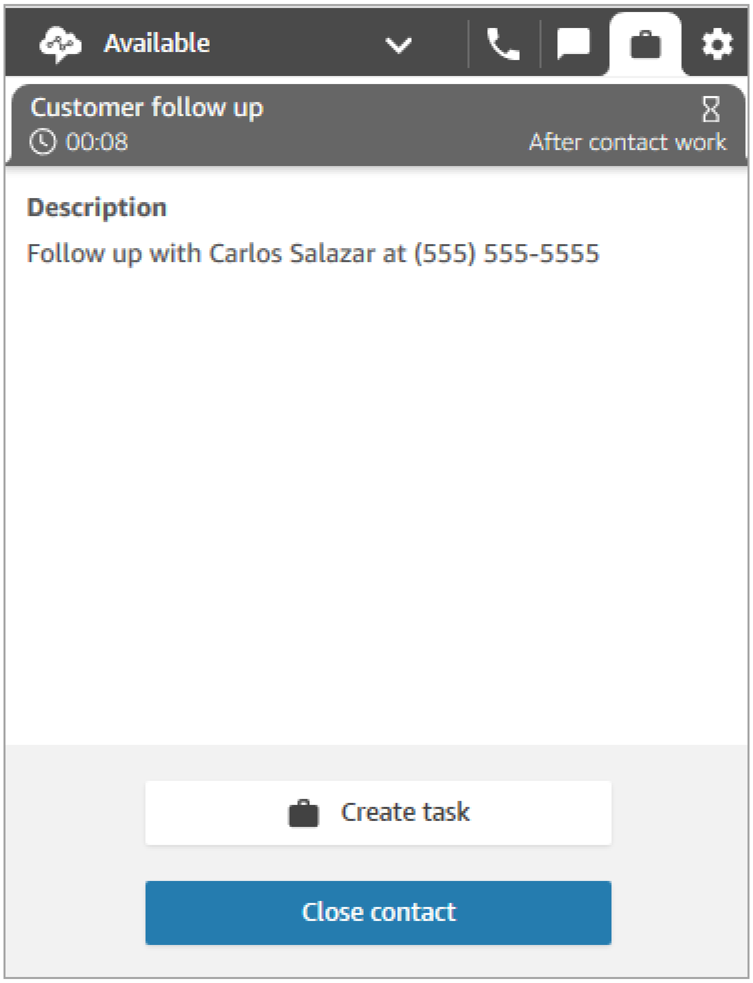
Follow up with Carlos Salazar at (555) 555-5555

References

Attachment

https://example.com

4. When you've completed the task, choose **End task**.
5. You will then be in ACW. When finished, choose **Close contact**.



Description

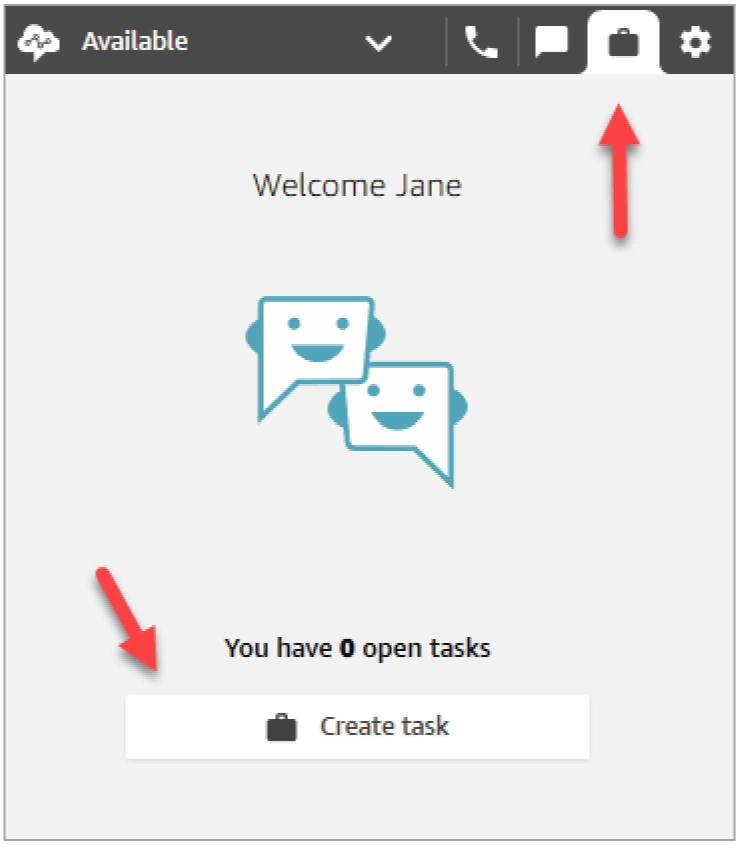
Follow up with Carlos Salazar at (555) 555-5555

Create a new task

You can create a task any time, even when your status is Offline. And you can assign a task to anyone who has a quick connect, including yourself.

You can create a task, which starts the task immediately. Or you can schedule the task to start on a future date and time.

1. Open the CCP. Select the **Task** tab, and then choose **Create task**.

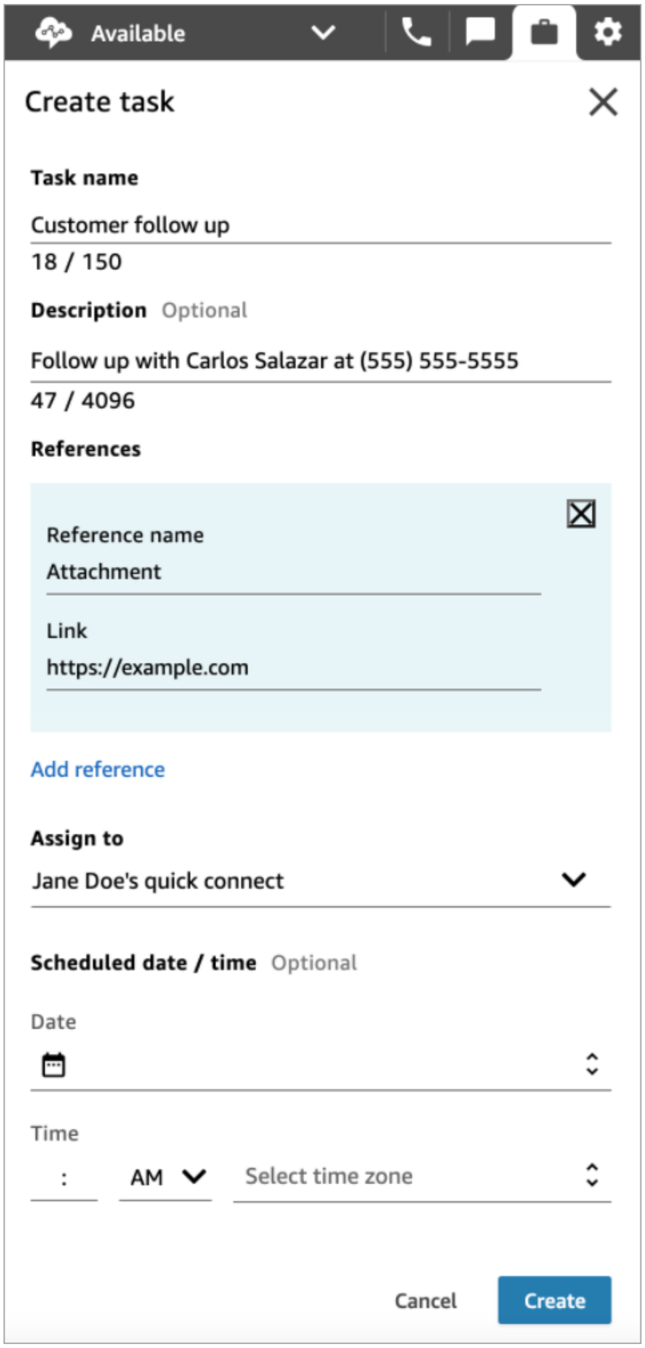


2. Complete the **Create task** page. When you choose **Assign to**, you can assign a task only to someone or a queue that has quick connect.

   Choose **Create**.

   CCP only

   The following image shows the option to create a task in the CCP.



Task name
Customer follow up
18 / 150

Description Optional
Follow up with Carlos Salazar at (555) 555-5555
47 / 4096

References

Reference name
Attachment

Link
https://example.com

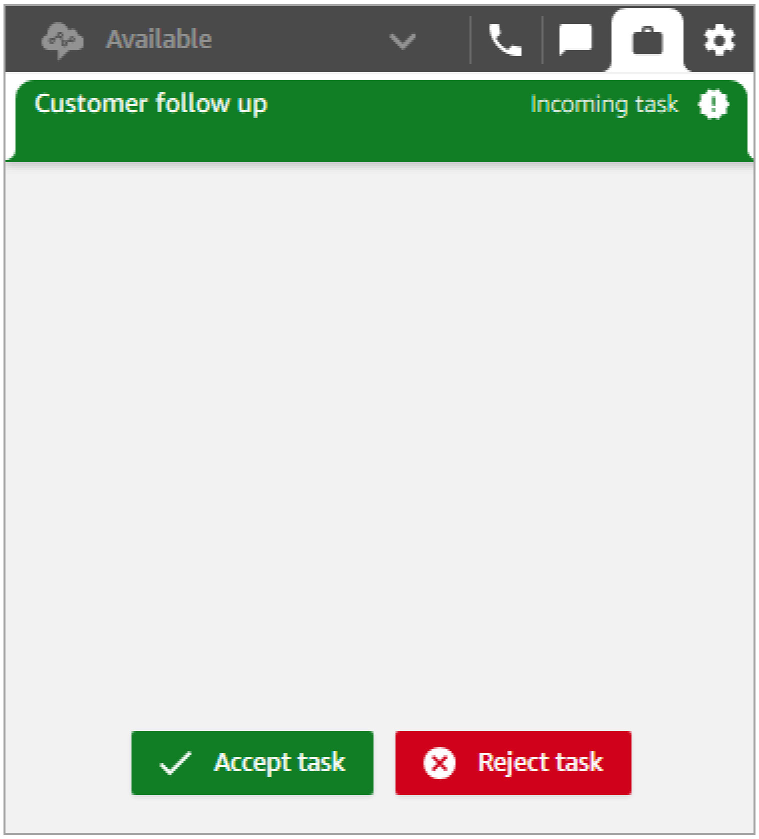
Assign to
Jane Doe's quick connect

Scheduled date / time Optional

Date

Time
: AM Select time zone

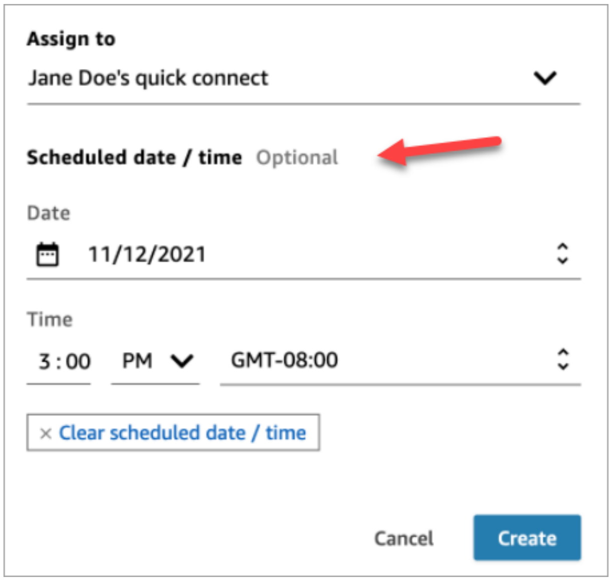
3. If you chose yourself, the task is routed to you. Choose **Accept task**.



Create a scheduled task

You can schedule a task to start on a future date and time.

1. Complete the steps to create a task. For example, add a **Task name** and **Assign to** a quick connect.
2. In the **Scheduled date / time** section, choose a future date and time, and specify the timezone. You can schedule a task up to six days in future.
3. If you want to clear all values in the **Scheduled date / time** section and start over, choose **Clear scheduled date / time**.



Assign to

Jane Doe's quick connect

Scheduled date / time Optional

Date

11/12/2021

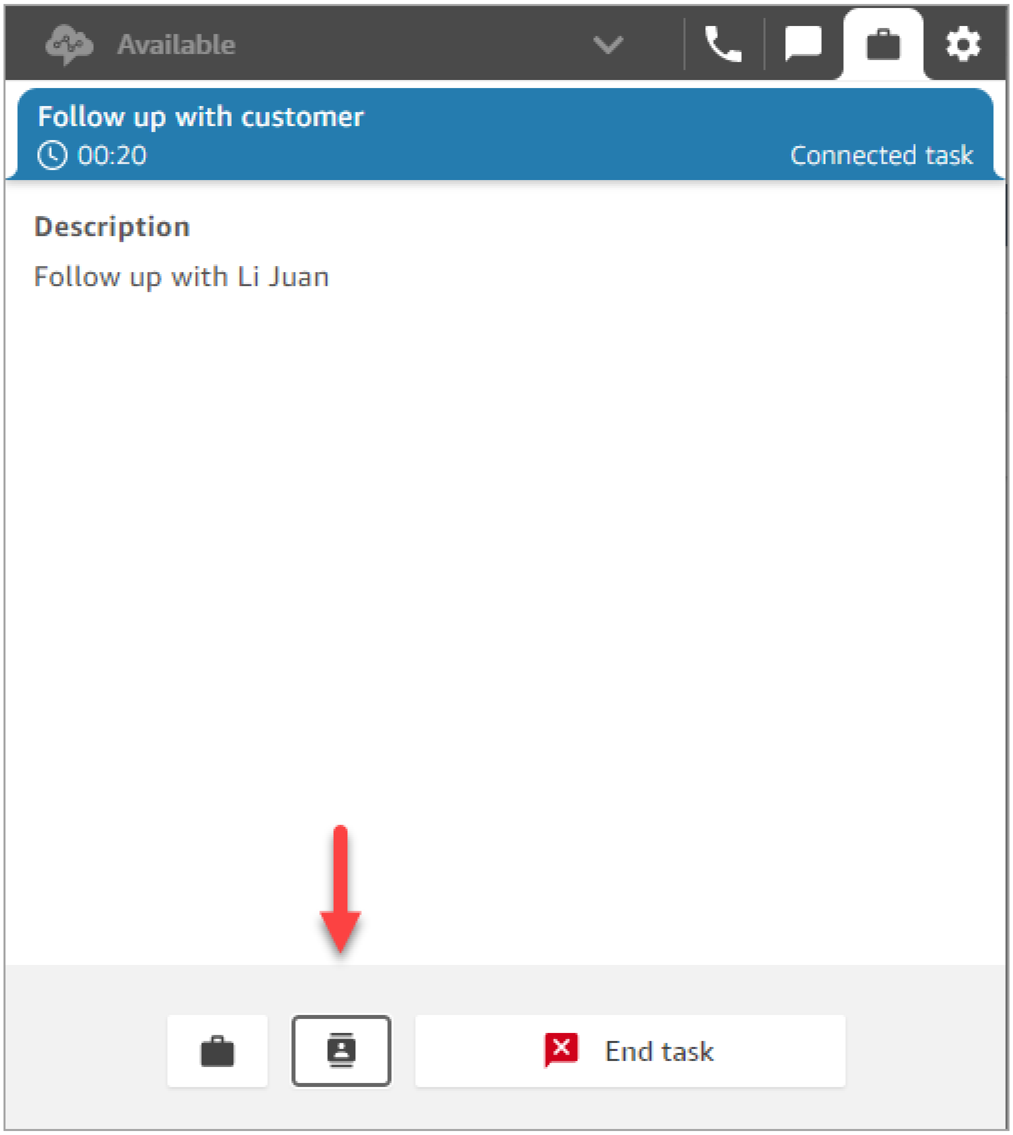
Time

3:00 PM GMT-08:00

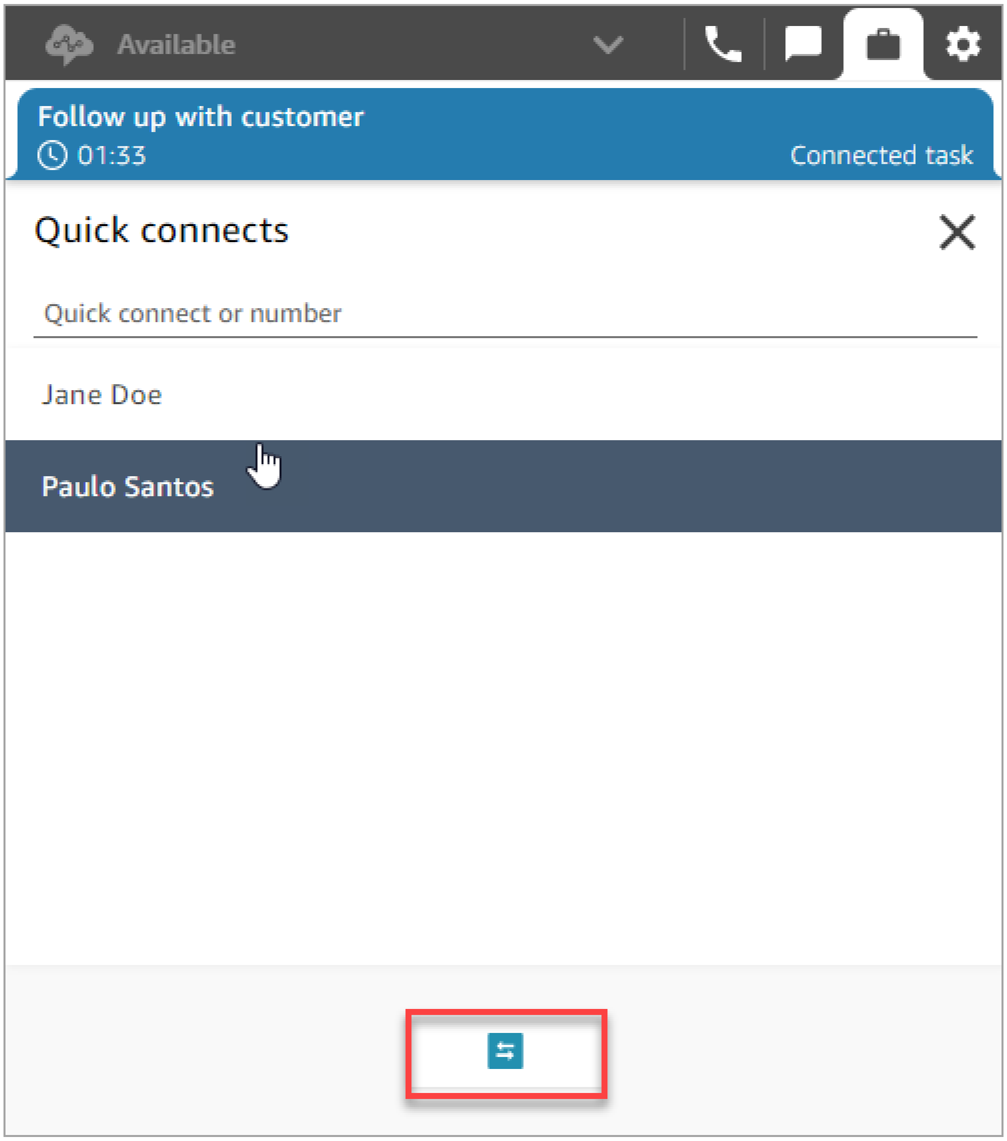
Transfer a task

You can transfer a task that's assigned to you to another agent or queue.

1. Open the task you want to transfer, and then choose the quick connect icon.



2. Choose from the list of people or destinations listed under **Quick connects**, and then choose the transfer icon.



Accept incoming contacts with Customer Profiles

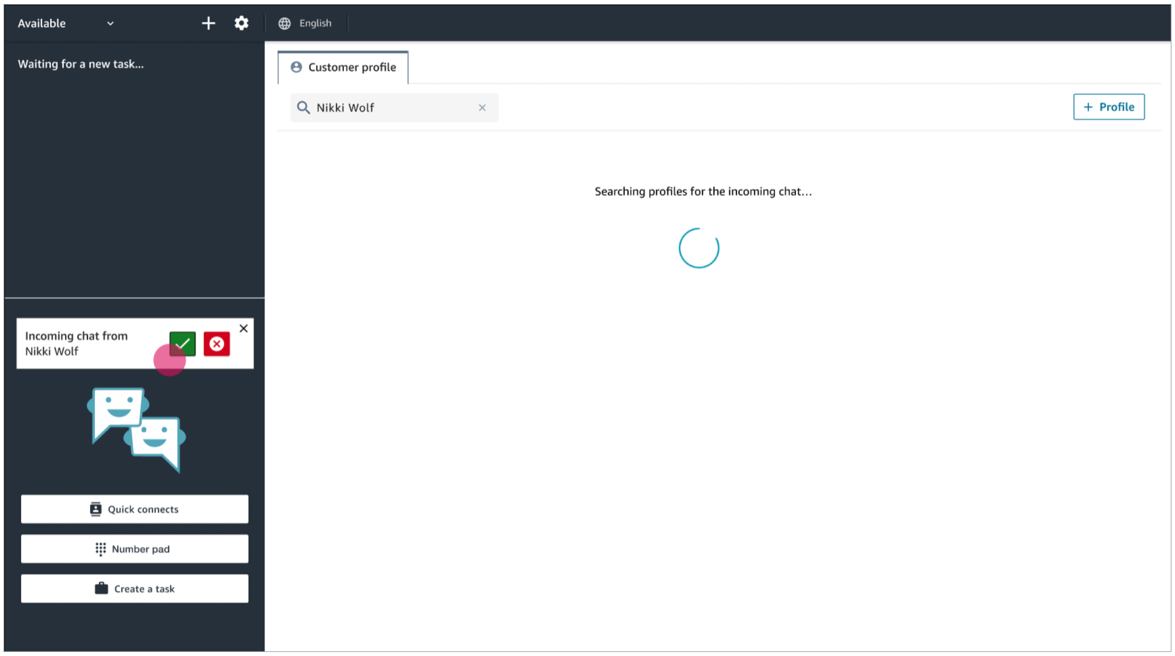
When a call or chat is connected to your Contact Control Panel (CCP), Amazon Connect, in the same browser window, automatically displays customer profiles that may match the incoming phone number.

Before agents can access customer profiles, the Amazon Connect administrator must enable the Customer Profiles feature, grant agents the appropriate permissions, and integrate Customer Profiles into your agent application. For more information, see Enable Customer Profiles for your instance (p. 641).

Example 1: Auto-populate the customer profile

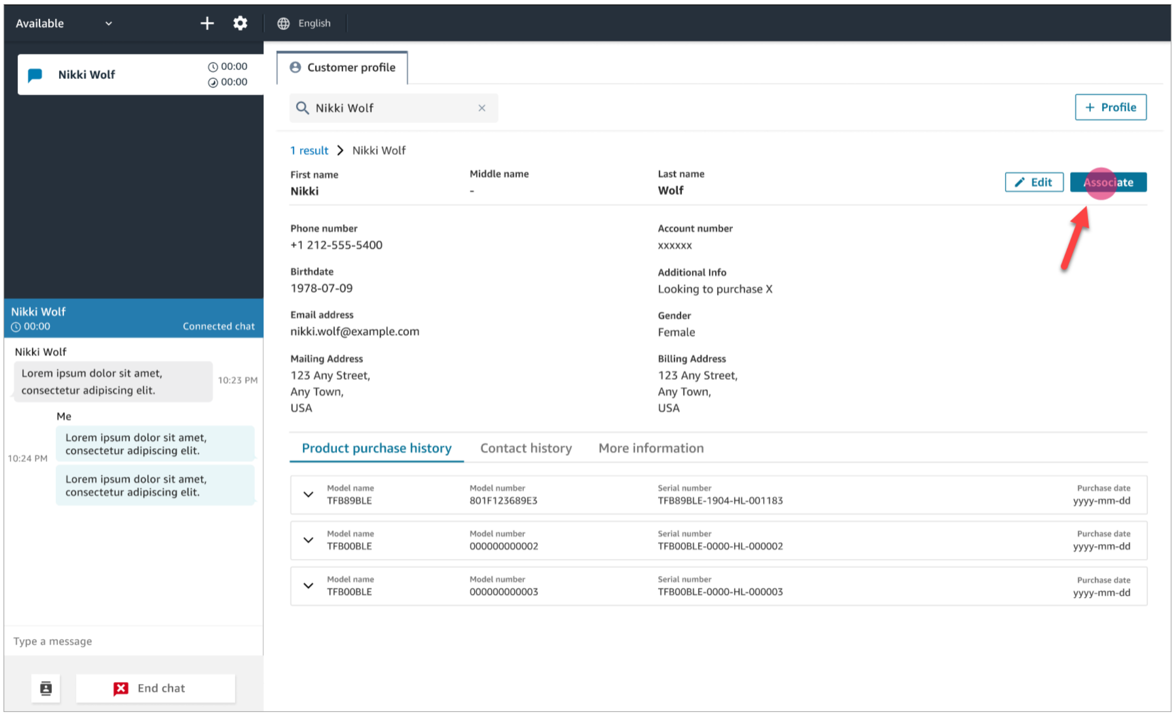
As soon as Amazon Connect matches the phone number (voice) or email address (chat) with an existing customer profile, it automatically displays the profile even though you may not have accepted the contact yet.

The following image shows what your Contact Control Panel (CCP) may look like when there's an incoming chat. A customer profile has been found that matches the customer, and Amazon Connect is loading the data.



Searching profiles for the incoming chat...

This next example shows what it might look like after you've accepted and joined the chat, and Amazon Connect displays the customer's profile. In this case, Amazon Connect found the customer's profile based on their email address. If this were a voice call, by default Amazon Connect would match the customer's profile based on their phone number. Your IT department can customize (p. 658) this behavior to search for the profile based on other information about the contact.



Nikki Wolf

Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:23 PM

Me

10:24 PM Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

First name: Nikki
Middle name: -
Last name: Wolf

Phone number: +1 212-555-5400
Account number: xxxxxx

Birthdate: 1978-07-09
Additional Info: Looking to purchase X

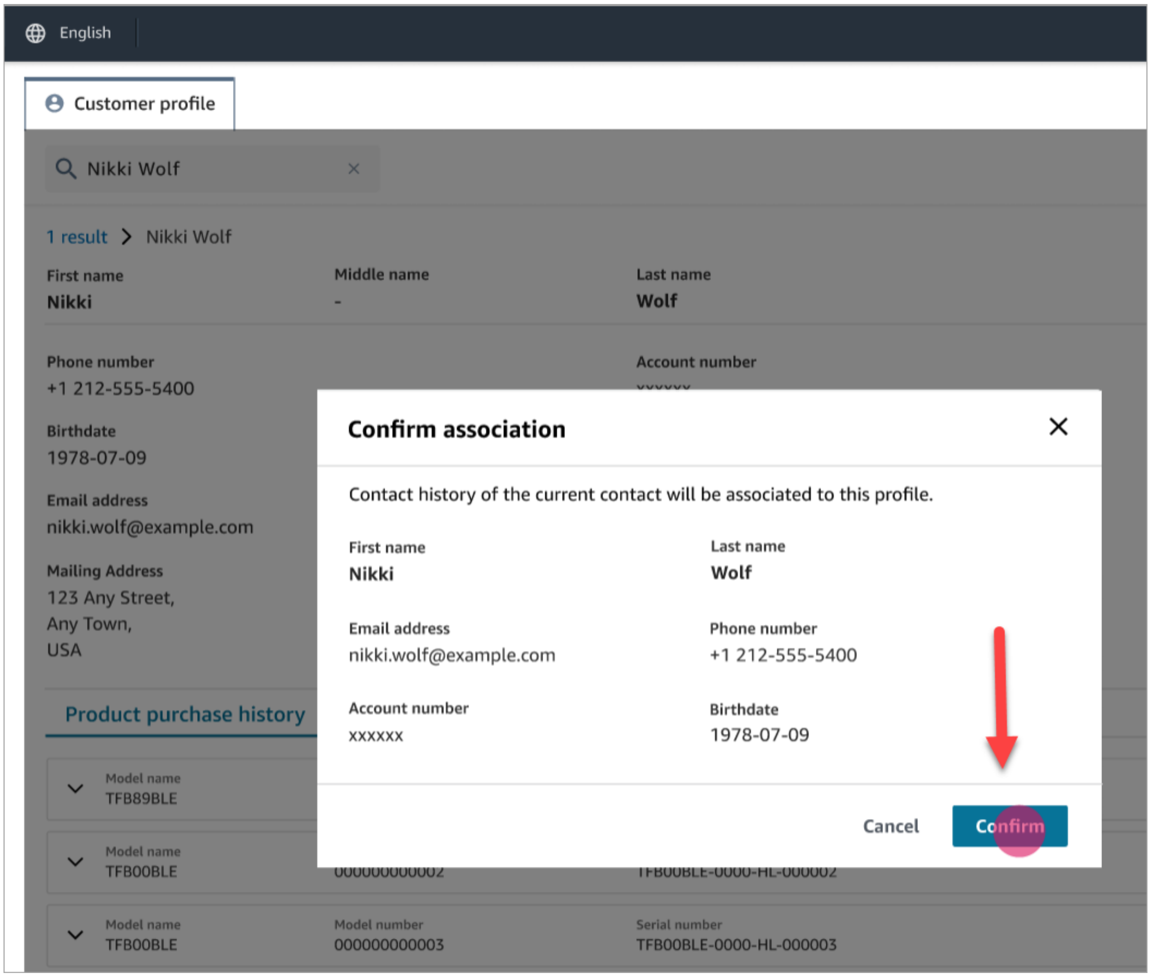
Email address: nikki.wolf@example.com
Gender: Female

Mailing Address
123 Any Street,
Any Town,
USA

Billing Address
123 Any Street,
Any Town,
USA

Model name	Model number	Serial number	Purchase date
TFB89BLE	801F123689E3	TFB89BLE-1904-HL-001183	yyyy-mm-dd
TFB00BLE	000000000002	TFB00BLE-0000-HL-000002	yyyy-mm-dd
TFB00BLE	000000000003	TFB00BLE-0000-HL-000003	yyyy-mm-dd

- Choose **Associate** to associate the contact record of the current contact with the customer profile, and then choose **Confirm**.



First name: Nikki
Middle name: -
Last name: Wolf
Phone number: +1 212-555-5400
Account number: xxxxxx
Birthdate: 1978-07-09
Email address: nikki.wolf@example.com
Mailing Address: 123 Any Street, Any Town, USA

Model name: TFB89BLE
Model name: TFBOOBLE, 000000000002, TFBOOBLE-0000-HL-000002
Model name: TFBOOBLE, Model number: 000000000003, Serial number: TFBOOBLE-0000-HL-000003

Confirm association

Contact history of the current contact will be associated to this profile.

First name Nikki	Last name Wolf
Email address nikki.wolf@example.com	Phone number +1 212-555-5400
Account number xxxxxx	Birthdate 1978-07-09

- If you choose **Associate** by mistake, you can continue to browse other customer profiles, and associate the contact with a different customer profile. Or, if you have been assigned Create permission (p. 661), you can create a new profile.

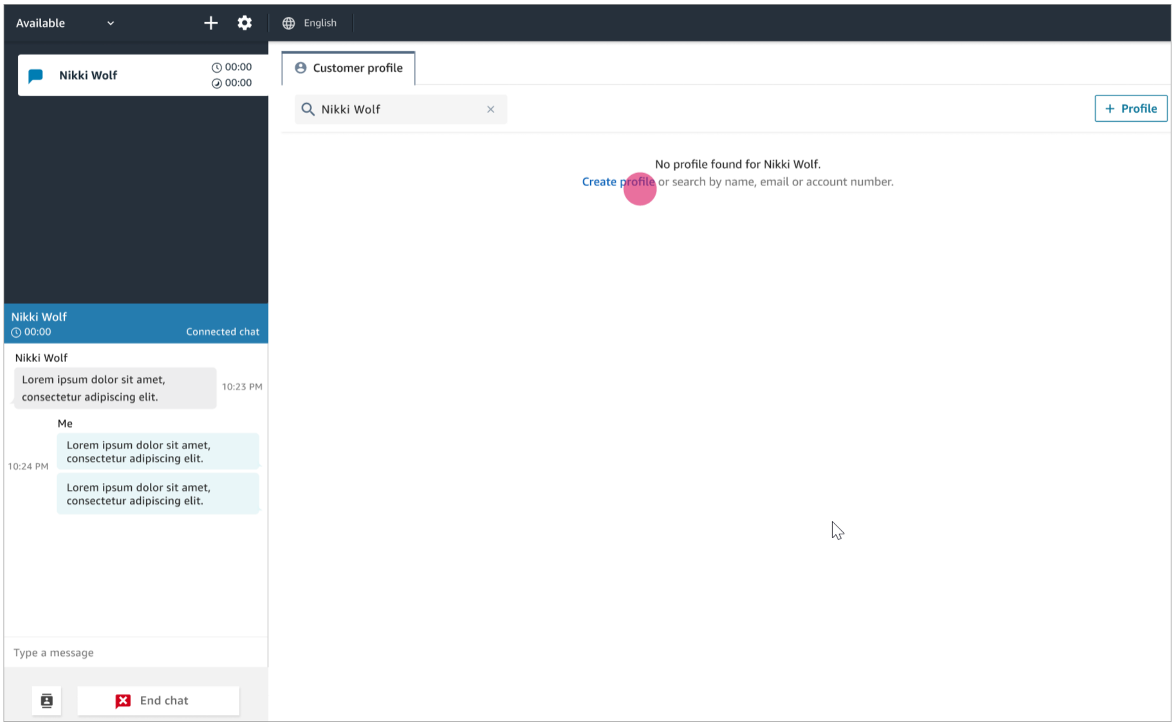
  You can associate a contact with customer profile multiple times during an interaction, including during After Contact Work (ACW) time. Only the most recent association remains, before you clear the contact.

Example 2: Accept incoming contact, no customer profile found

If no results are returned when a call or chat comes in, do the following:

1. Search for the customer's profile using their email address, name, or account number. An *account number* is a unique identifier for the customer in your business, such as a member number or a customer relationship number.
2. If no customer profile is found, create a new profile (p. 1185) for the contact. The only required information is first name.

In the following image, the agent searched for **John Doe**. No matches were found so they chose **Create profile**.



No profile found for Nikki Wolf.
Create profile or search by name, email or account number.

Nikki Wolf

Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:23 PM

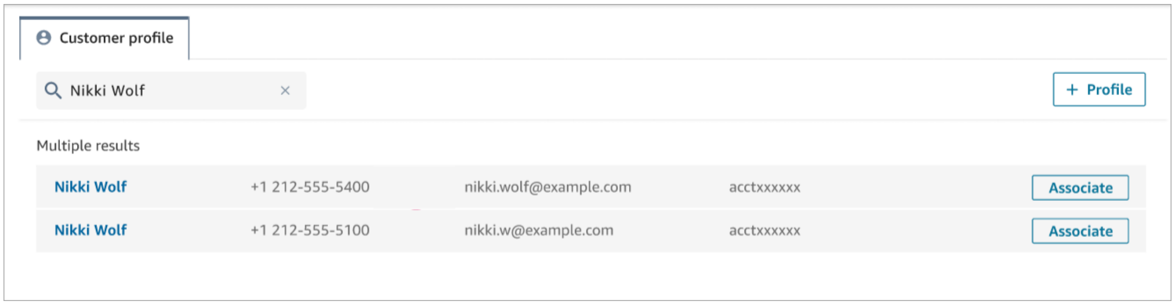
Me

Lorem ipsum dolor sit amet, consectetur adipiscing elit.

Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:24 PM

Example 3: Accept incoming contact, multiple customer profiles found

In some cases, multiple profiles may be returned for the same call or chat. Use the summary information to verify the customer's identity. For example, ask the customer to verify their email address or account number, and then associate the contact with the right customer profile.

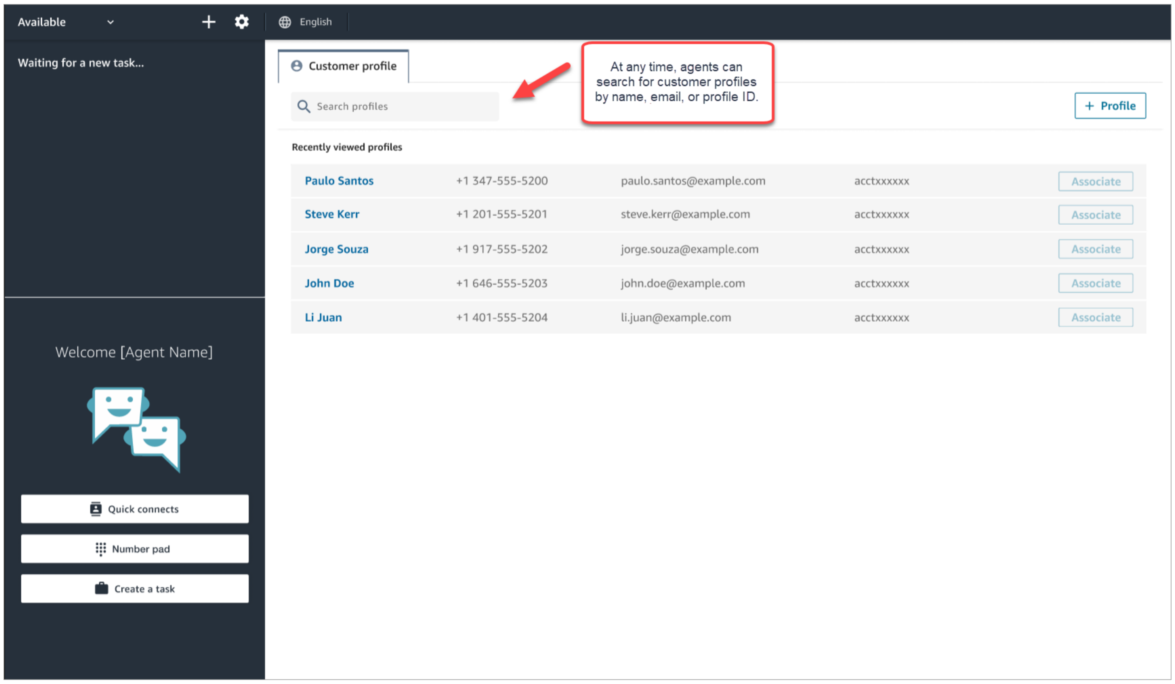


Multiple results

Nikki Wolf	+1 212-555-5400	nikki.wolf@example.com	acctxxxxxx	Associate
Nikki Wolf	+1 212-555-5100	nikki.w@example.com	acctxxxxxx	Associate

Example 4: Search when not on contact

When there are no incoming contacts, you can search for customer profiles using phone number, name, email address, or profile ID. For example, you might want to use this time to search for previous contacts, or completing a profile.



At any time, agents can search for customer profiles by name, email, or profile ID.

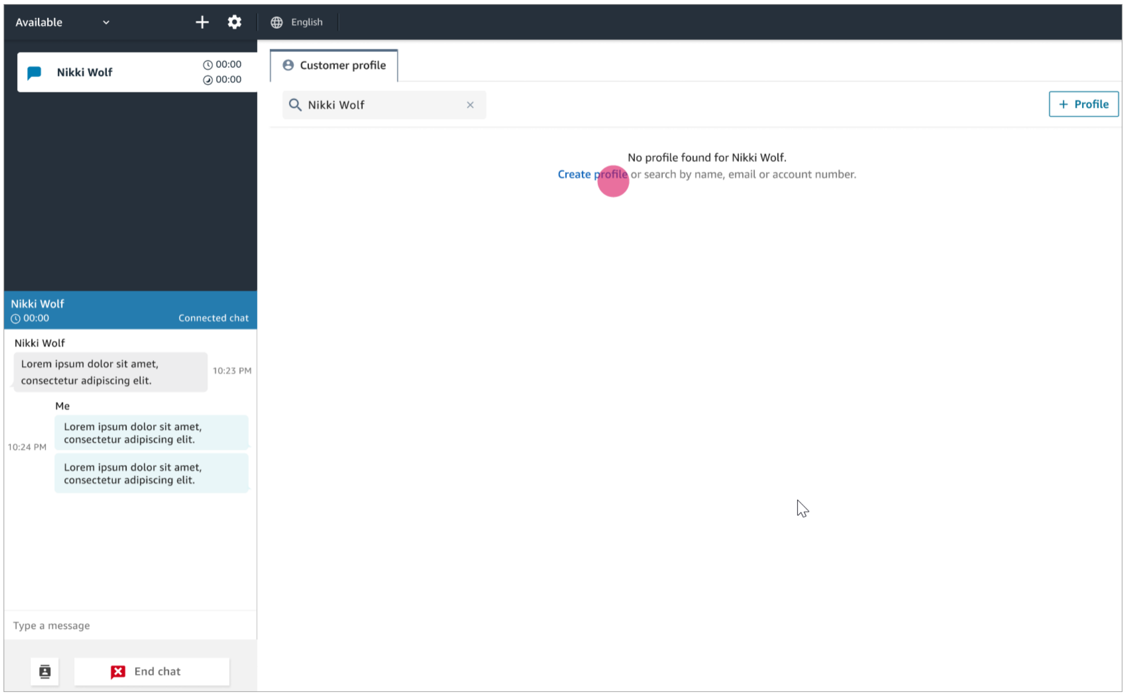
Recently viewed profiles

Paulo Santos	+1 347-555-5200	paulo.santos@example.com	acctxxxxxx	Associate
Steve Kerr	+1 201-555-5201	steve.kerr@example.com	acctxxxxxx	Associate
Jorge Souza	+1 917-555-5202	jorge.souza@example.com	acctxxxxxx	Associate
John Doe	+1 646-555-5203	john.doe@example.com	acctxxxxxx	Associate
Li Juan	+1 401-555-5204	li.juan@example.com	acctxxxxxx	Associate

Create a new customer profile

Let's say you're on a chat and there's no customer profile for the contact. You can create a new customer profile for them.

1. Choose **Create profile**.



No profile found for Nikki Wolf.
Create profile or search by name, email or account number.

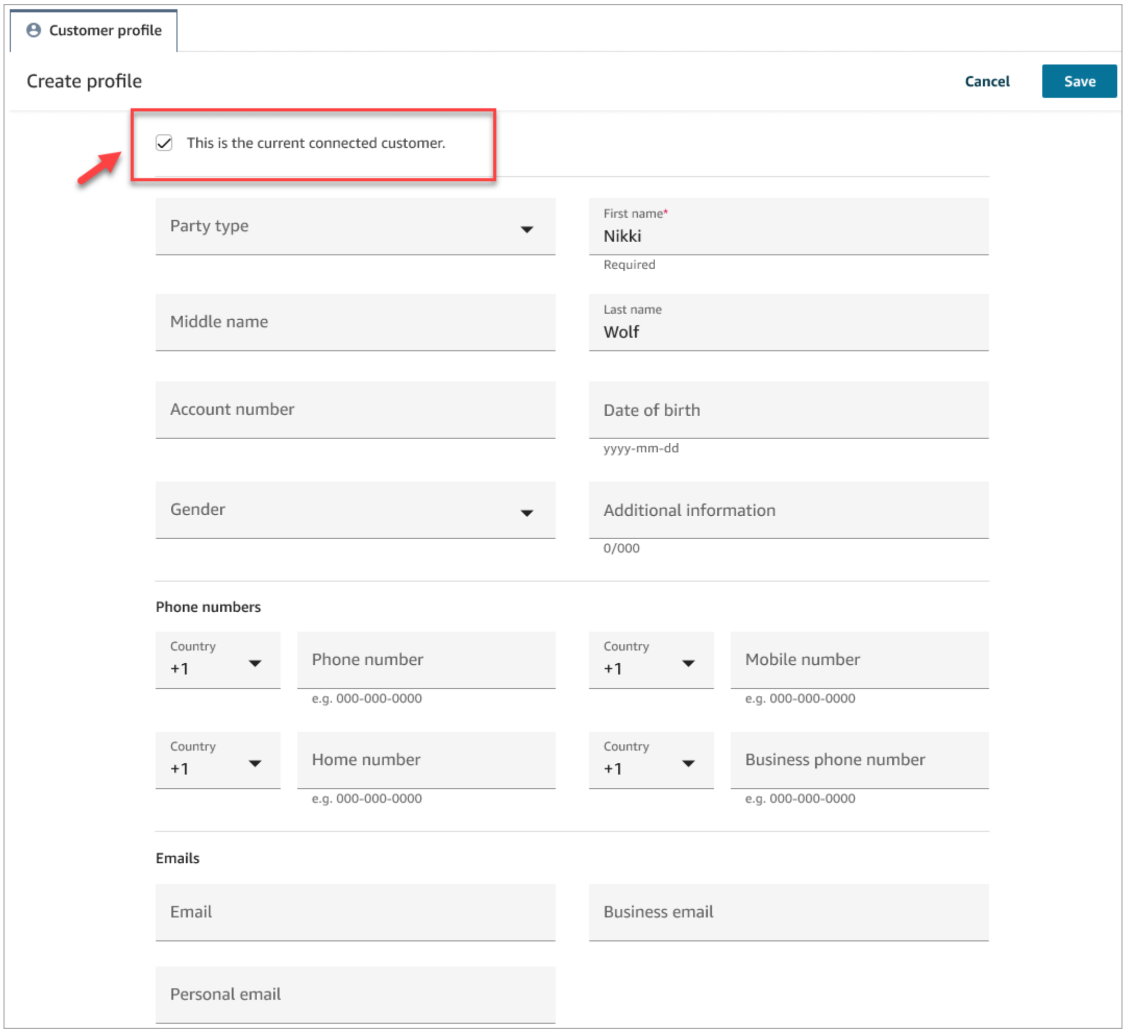
Nikki Wolf
Lorem ipsum dolor sit amet, consectetur adipiscing elit. 10:23 PM

Me
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
10:24 PM
Lorem ipsum dolor sit amet, consectetur adipiscing elit.

2. Choose **This is the current connected customer**. This tells Amazon Connect to link the customer profile to the contact ID for the current customer.

   If you don't select this check box, the profile isn't associated with the current contact. This is useful when a contact is calling from someone else's number.

   Enter information in the required boxes, and then choose **Save**.

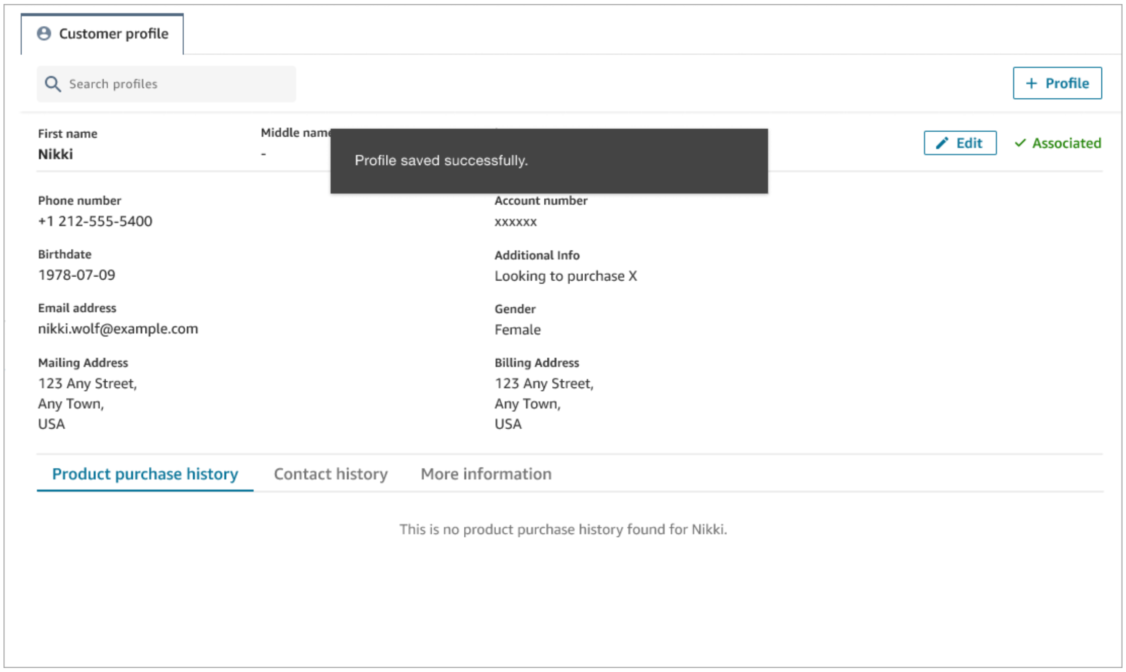
   Create profile

   ☑ This is the current connected customer.

   First name* Nikki

   Last name Wolf

3. You'll receive a verification page that the contact has been created.



Profile saved successfully.

First name: Nikki
Middle name: -

Phone number: +1 212-555-5400
Account number: xxxxxx
Birthdate: 1978-07-09
Additional Info: Looking to purchase X
Email address: nikki.wolf@example.com
Gender: Female
Mailing Address: 123 Any Street,
Any Town,
USA
Billing Address: 123 Any Street,
Any Town,
USA

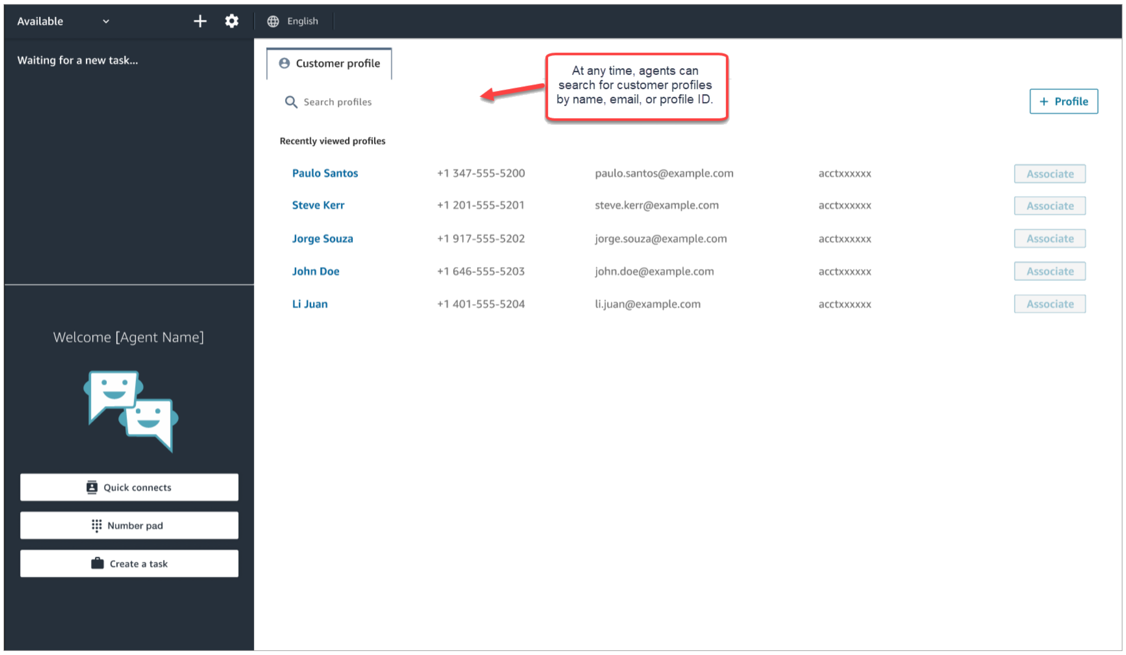
This is no product purchase history found for Nikki.

4. You can continue the conversation with the customer.

Search for a customer profile

Even when you're not on a contact you can search customer profiles. This is helpful in cases where, for example, you want to return to a customer profile.

1. In the **Search** box, type the customer phone number, name, email, or profile ID.



At any time, agents can search for customer profiles by name, email, or profile ID.

Recently viewed profiles

Paulo Santos	+1 347-555-5200	paulo.santos@example.com	acctxxxxxx	Associate
Steve Kerr	+1 201-555-5201	steve.kerr@example.com	acctxxxxxx	Associate
Jorge Souza	+1 917-555-5202	jorge.souza@example.com	acctxxxxxx	Associate
John Doe	+1 646-555-5203	john.doe@example.com	acctxxxxxx	Associate
Li Juan	+1 401-555-5204	li.juan@example.com	acctxxxxxx	Associate

2. If more than one result is returned, you can review the summary information to identify the contact that you want.

3. Choose **View details** to see profile information and the contact history for that customer.

Search for content using Amazon Connect Wisdom

You can search and find content across multiple repositories, such as frequently asked questions (FAQs), wikis, articles, and step-by-step instructions for handling different customer issues.

For example, you can type questions or phrases in the search box (such as, "how long after purchase can handbags be exchanged?") without having to guess which keywords will work. Wisdom searches the connected sources, and returns relevant information adjacent to your Contact Control Panel (CCP).

You can search for content at any time: while on a contact, on After Contact Work, or between contacts.

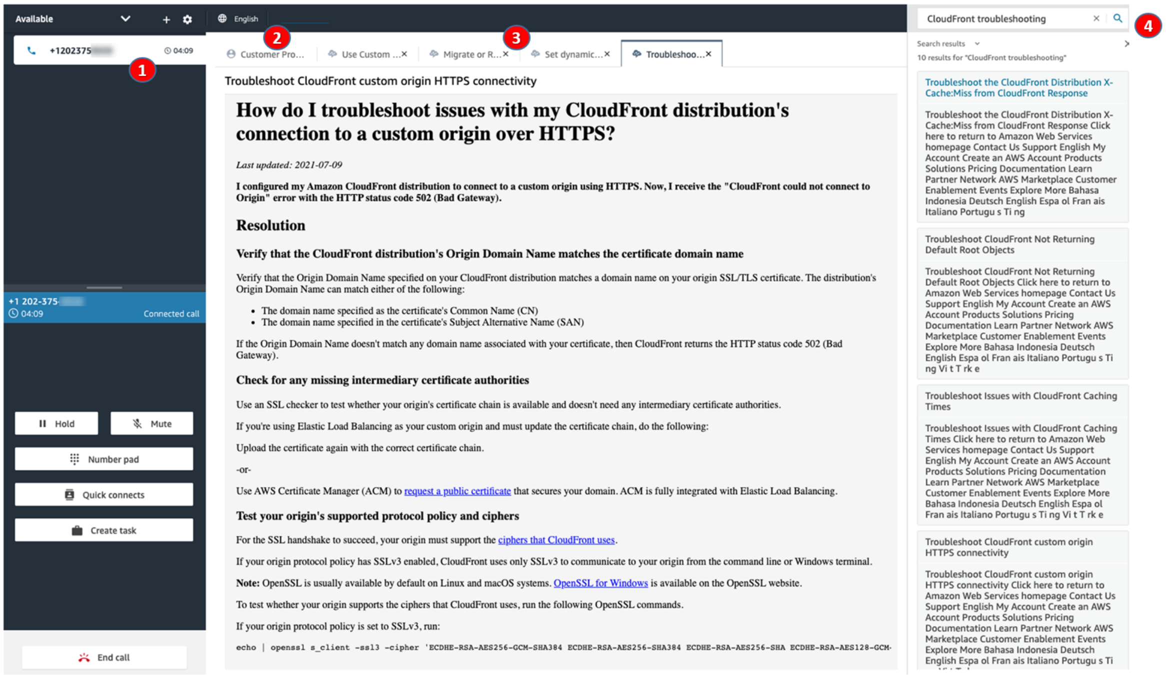
To search for content

1. In the search box, type words or phrases.
2. Choose the article that you want to view.
3. The article appears in a new tab.
4. The list of search results is cleared only after you complete ACW and choose **Clear contact**, or select the **Close** icon next to the search box.

Use real-time recommendations

If your organization uses Contact Lens for Amazon Connect, you may get real-time recommendations that point you to information related to the current conversation with the customer.

The following image shows how an article may appear in the agent application when you're on a call.



Troubleshoot CloudFront custom origin HTTPS connectivity

How do I troubleshoot issues with my CloudFront distribution's connection to a custom origin over HTTPS?

Last updated: 2021-07-09

I configured my Amazon CloudFront distribution to connect to a custom origin using HTTPS. Now, I receive the "CloudFront could not connect to Origin" error with the HTTP status code 502 (Bad Gateway).

Resolution

Verify that the CloudFront distribution's Origin Domain Name matches the certificate domain name

Verify that the Origin Domain Name specified on your CloudFront distribution matches a domain name on your origin SSL/TLS certificate. The distribution's Origin Domain Name can match either of the following:

- The domain name specified as the certificate's Common Name (CN)
- The domain name specified in the certificate's Subject Alternative Name (SAN)

If the Origin Domain Name doesn't match any domain name associated with your certificate, then CloudFront returns the HTTP status code 502 (Bad Gateway).

Check for any missing intermediary certificate authorities

Use an SSL checker to test whether your origin's certificate chain is available and doesn't need any intermediary certificate authorities.

If you're using Elastic Load Balancing as your custom origin and must update the certificate chain, do the following:

Upload the certificate again with the correct certificate chain.

-or-

Use AWS Certificate Manager (ACM) to request a public certificate that secures your domain. ACM is fully integrated with Elastic Load Balancing.

Test your origin's supported protocol policy and ciphers

For the SSL handshake to succeed, your origin must support the ciphers that CloudFront uses.

If your origin protocol policy has SSLv3 enabled, CloudFront uses only SSLv3 to communicate to your origin from the command line or Windows terminal.

Note: OpenSSL is usually available by default on Linux and macOS systems. OpenSSL for Windows is available on the OpenSSL website.

To test whether your origin supports the ciphers that CloudFront uses, run the following OpenSSL commands.

If your origin protocol policy is set to SSLv3, run:

```
echo | openssl s_client -ssl3 -cipher 'ECDHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES256-SHA384 ECDHE-RSA-AES256-SHA ECDHE-RSA-AES128-GCM-
```

10 results for "CloudFront troubleshooting"

Troubleshoot the CloudFront Distribution X-Cache:Miss from CloudFront Response

Troubleshoot the CloudFront Distribution X-Cache:Miss from CloudFront Response Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti ng

Troubleshoot CloudFront Not Returning Default Root Objects

Troubleshoot CloudFront Not Returning Default Root Objects Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti ng Vi t T rk e

Troubleshoot Issues with CloudFront Caching Times

Troubleshoot Issues with CloudFront Caching Times Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti ng Vi t T rk e

Troubleshoot CloudFront custom origin HTTPS connectivity

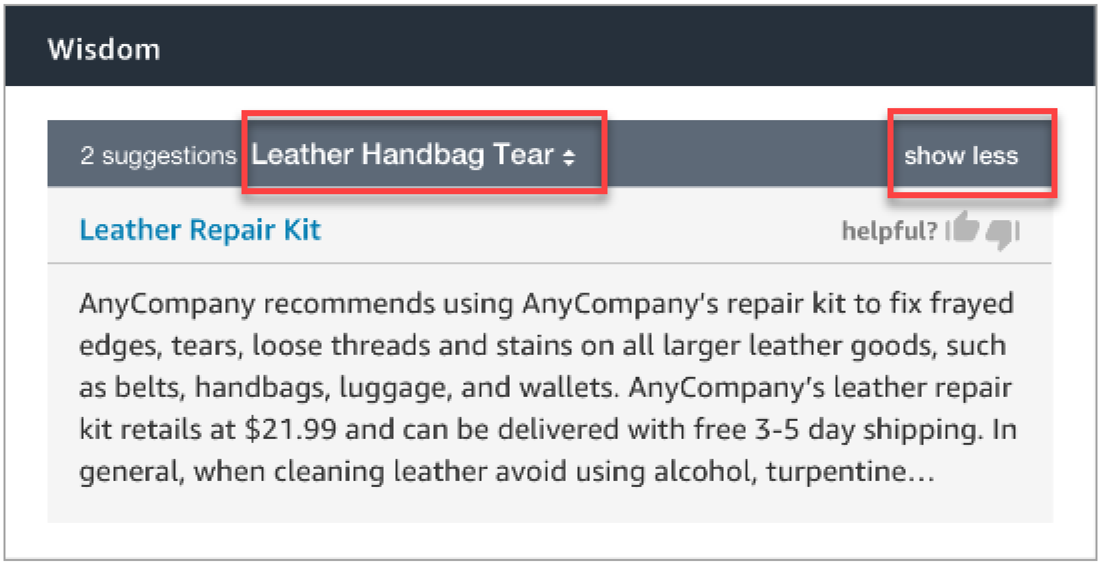
Troubleshoot CloudFront custom origin HTTPS connectivity Click here to return to Amazon Web Services homepage Contact Us Support English My Account Create an AWS Account Products Solutions Pricing Documentation Learn Partner Network AWS Marketplace Customer Enablement Events Explore More Bahasa Indonesia Deutsch English Espa ol Fran ais Italiano Portugu s Ti

1. You're on a call.

2. The **Customer profile** tab is available.
3. You can have multiple articles open at the same time.
4. You can search for articles.

You can select the recommendation to view the entire article, or choose **Show less** to close the details of the recommendation.

As more recommendations are sent, you can toggle through them and choose those you want to read.



Wisdom

2 suggestions Leather Handbag Tear ⬍ show less

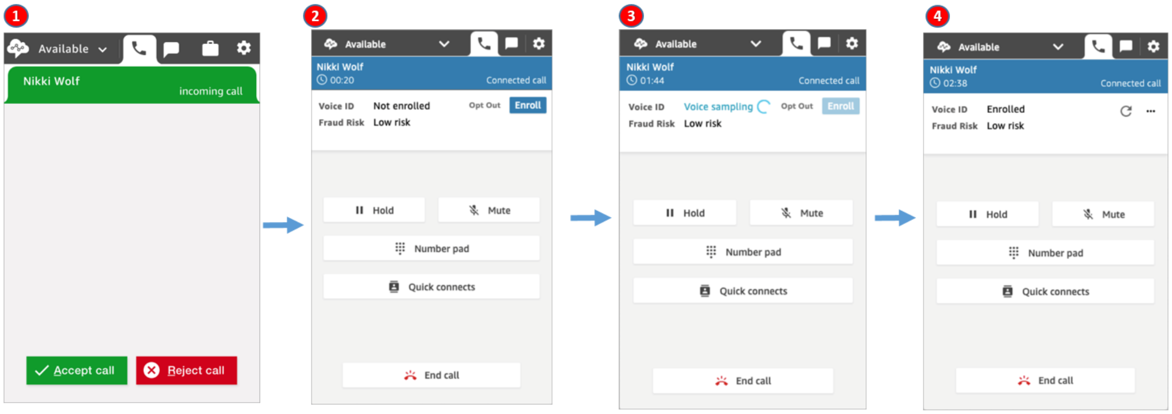
Leather Repair Kit helpful?

AnyCompany recommends using AnyCompany's repair kit to fix frayed edges, tears, loose threads and stains on all larger leather goods, such as belts, handbags, luggage, and wallets. AnyCompany's leather repair kit retails at $21.99 and can be delivered with free 3-5 day shipping. In general, when cleaning leather avoid using alcohol, turpentine…

Use Voice ID

This topic shows how Voice ID features appear in your Contact Control Panel (CCP).

Enroll a caller in Voice ID



1
Available
Nikki Wolf
incoming call
Accept call
Reject call

2
Available
Nikki Wolf
00:20
Connected call
Voice ID Not enrolled Opt Out Enroll
Fraud Risk Low risk

3
Available
Nikki Wolf
01:44
Connected call
Voice ID Voice sampling Opt Out Enroll
Fraud Risk Low risk

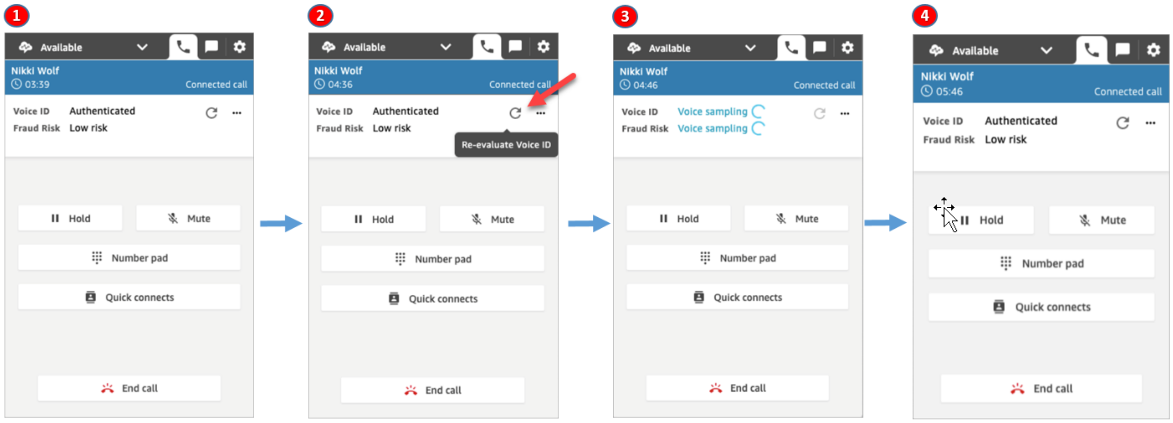
4
Available
Nikki Wolf
02:38
Connected call
Voice ID Enrolled
Fraud Risk Low risk

1. You receive an incoming call.
2. The caller is not yet enrolled in Voice ID so you choose **Enroll**.
3. A message is displayed that Voice ID is sampling the caller's voice. It requires 30 seconds of speech (excluding silence).

4. The caller is now enrolled in Voice ID. This example also shows the caller's **Fraud risk** as lower than the threshold.

Verification of an enrolled caller

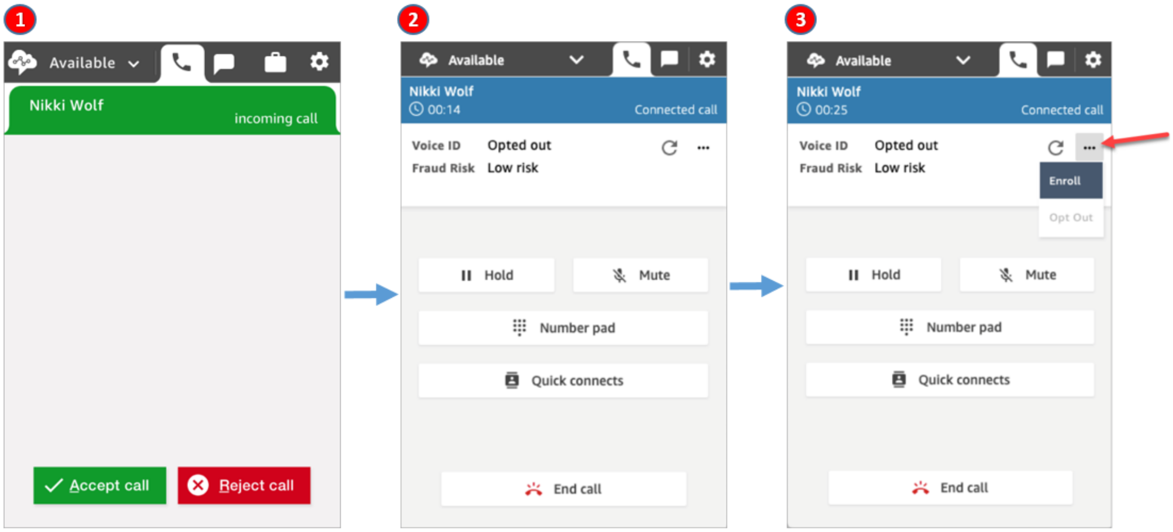
After a customer is enrolled in Voice ID, when they call your contact center again, you can verify they are who they say they are.



1. You receive an incoming call.
2. The caller is already enrolled in Voice ID, and their status is **Authenticated**. You can choose to re-evaluate authentication using Voice ID.
3. A message is displayed that Voice ID is evaluating the caller's speech. It requires 10 seconds of speech, not including silence.
4. The caller has been authenticated by Voice ID. This example also shows the caller's **Fraud risk** is lower than the threshold.

Caller has opted out

The following image shows what appears in your CCP when a caller has opted out of Voice ID.

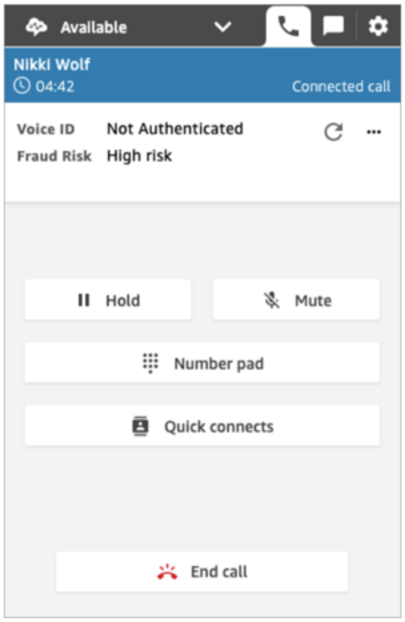


1. You receive an incoming call.

2. The caller has previously opted out of Voice ID.
3. You have the option to enroll them.

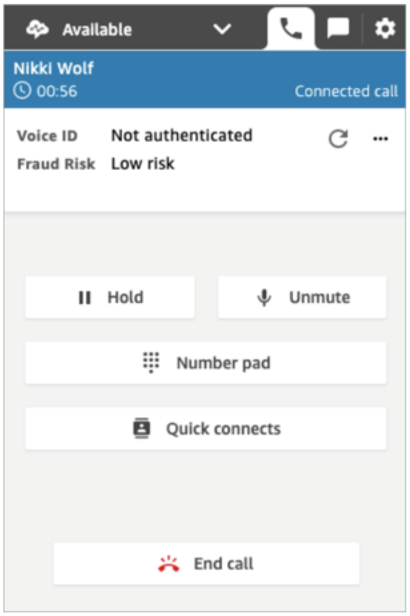
Authentication status = Not authenticated

When an enrolled caller calls your contact center, Voice ID may return a result of **Not authenticated**. This means Voice ID was unable to authenticate a caller's speech. The authentication score for the caller is lower than the configured threshold.



Nikki Wolf
04:42
Connected call

Voice ID Not Authenticated
Fraud Risk High risk



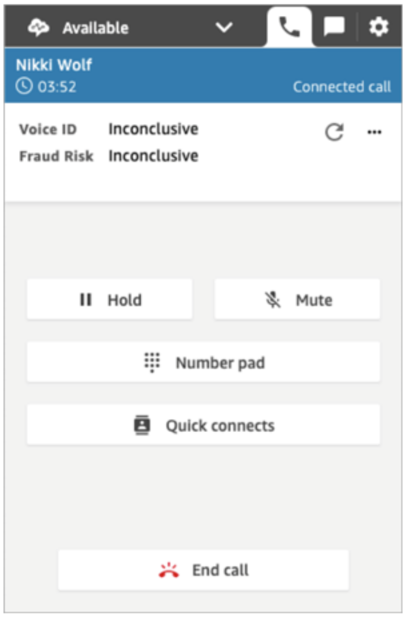
Nikki Wolf
00:56
Connected call

Voice ID Not authenticated
Fraud Risk Low risk

The previous images show that the **Fraud risk** can be **High** or **Low**, independent of whether the caller is authenticated.

Authentication status: Inconclusive

When an enrolled customer calls your contact center, Voice ID may return a result of **Inconclusive**: Voice ID was unable to analyze a caller's speech for authentication. This is usually because Voice ID did not get the required 10 seconds to provide a result for verification.



Voice ID Inconclusive

Fraud Risk Inconclusive

Troubleshooting Issues with the Contact Control Panel (CCP)

Troubleshooting Contact Control Panel (CCP) issues requires support from your network operations, system administrator, and virtual desktop (VDI) solution teams to collect the appropriate level of information to identify root cause and drive resolution. To help determine the appropriate resources to engage, it's important to break issues down into those with similar symptoms. The following guidance has been helpful in assisting Amazon Connect customers in resolving CCP issues with their operations support teams.

Contents

Use the Endpoint Test Utility

To validate connectivity to Amazon Connect, or when your agents are experiencing problems with the Contact Control Panel (CCP), we recommend using the Amazon Connect Endpoint Test Utility.

The Amazon Connect Endpoint Test Utility performs the following checks:

- Validates that the browser being used supports WebRTC.
- Determines if the browser has appropriate access to media devices (microphone, speakers, etc).
- Performs latency tests for all active Amazon Connect Regions.
- Performs latency tests to a specific Amazon Connect instance, if provided.
- Validates network connectivity across required ports for media streams.

The complete results are available for download as a JSON file. You can copy the results to include in a support ticket. You can also load the results file into the tool by selecting the **Load previous results** option. This option displays the contents of the file visually and makes it easier to analyze the results. Additionally, you can download a bookmark specifically for the provided instance to make future tests easier to run.

Parameters to customize the Endpoint Test Utility

You can use the Endpoint Test Utility as is without any customizations. However, if you want to customize it, use the following URL parameters:

- **lng**: Change the language of the tool. Currently supported languages are English, Spanish, and French. It accepts the following values:
  - en (default)
  - es
  - fr
- **autoRun**: Run the tool automatically. It accepts the following values:
  - true
  - false (default)
- **connectInstanceUrl**: Not used by default. You can specify the Amazon Connect instance in the URL. It must start with **https**.

Example customized URL:

```
https://a.co/4pBJMng?lng=es&autoRun=true&connectInstanceUrl=https://
myinstance.awsapps.com/connect/login
```

Previous Check Connectivity Tool

The previous version of the tool is available here: Amazon Connect Check Connectivity Tool.

This tool checks which web browser the agent is running, and whether the microphone has required permissions. Click the **Test** buttons to check the ports and latency.

Common Contact Control Panel (CCP) Issues

The following are common issues encountered when using the Amazon Connect CCP.

- **CCP does not initialize/connect**—The most common causes are missing port/IP allow list entries, not allowing browser microphone access, or not answering your external device. Be sure that you have added to the allow list all IPs covered in the Set up your network (p. 605) 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. 605) section of this guide.
- **Missed calls, state change delays, and CCP unresponsive**—In most cases, this is intermittent and directly correlated with resource contention in the agent's workstation, network, or both. This can be made worse, or caused directly, by a poor, unstable, or strained connection to AWS resources at the private WAN/LAN, public WAN levels, or local workstation resource contention.

The following are common issues with call quality when using the CCP. Call quality encompasses a large range of potential causes and is best approached by first identifying the types of issues that you're having.

- **Latency/cross-talk**—in a voice connection manifests as a delay between when something is said and when the person on the other end hears it. In some use cases that require a lot of conversation, high latency can create situations in which both parties are talking over each other. The PSTN (public switched telephone network) and agent latency need to be calculated in this scenario to identify contributing factors and take action to reduce PSTN latency, agent latency, or both. For more information, see the PSTN and agent connection latency section of this documentation.

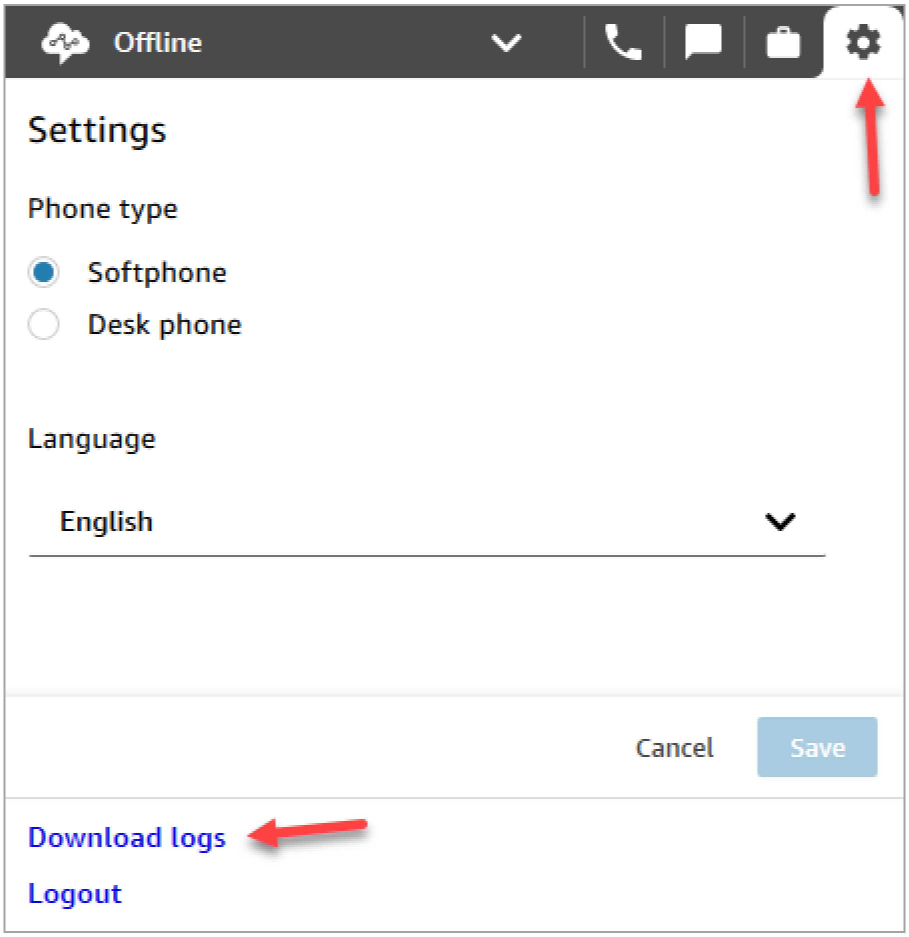
- **One way audio**—is when the agent can't hear the caller or the caller can't hear them. This is normally indicative of an issue with the agent's workstation at the hardware, network, resource levels, or all three. It and can also be related to browser microphone permissions or headset issues. For more information, see the How to determine whether a workstation is the source of problems (p. 293) section of this guide.
- **Volume increase or decrease**— can happen at the beginning or intermittently during the call, and it's important to differentiate the two for troubleshooting purposes. Typically, this relates to forwarding calls to or from Amazon Connect that inherit this from an issue with the third party transfer.
- **Audio choppy, cutting out, echo, reverb, or other signal noise**—could also manifest as a robotic sound or other distortion making it difficult for either the agent, caller, or both parties to understand what’s being said. This is normally indicative of an issue with the agent's workstation at the hardware, network, resource levels, or all three. For more information, see the How to determine whether a workstation is the source of problems (p. 293) section of this guide.
- **Wobble**—is the effect that media codecs can have on audio that manifests as the slowing down and speeding up of audio to combat high jitter and latency. This is normally indicative of an issue with the agent's workstation at the hardware, network, resource levels, or all three. For more information, see the How to determine whether a workstation is the source of problems (p. 293) section of this guide.
- **Disconnects**—can happen at any point in the call. It is important to note when during the call that the disconnections occur to identify a pattern. For example, disconnects on call transfers to a specific external number typically relate to forwarding calls to or from Amazon Connect that inherit this from an issue with the third party transfer. They can also be related to circular transfers, which means transferring calls out of Amazon Connect and back in the same call.

Download CCP logs

The Contact Control Panel logs store agent actions and timing.

To download CCP logs

1. On the agent's desktop, in their CCP, choose **Settings**, **Download logs**.



Offline

Settings

Phone type

● Softphone

○ Desk phone

Language

English

Cancel Save

Download logs

Logout

2. The `agent-log.txt` file is saved to your browser's default directory. After the file is downloaded, you can change the name of the file the same way you rename any other file on your computer. You can't customize the file name before the file it downloaded.

Troubleshooting Tools and Information

The following tools and information can be helpful with troubleshooting issues with Amazon Connect.

- **Instance ARN**—Provide your instance ARN (Amazon Resource Name) when you contact AWS support so that they can see the activity in your Amazon Connect instance. You can find the ARN for your instance on the Overview page that you access by choosing the alias of the instance from the Amazon Connect console.
- **Call recordings**—are very useful, not only to illustrate and determine reported behavior, but also to rule out audio issues from the agent's side. Recordings in Amazon Connect are done at the instance side of the interaction, before the audio traverses the agent connection. This allows you to determine if the audio issue was isolated to the agent's side of the interaction or if it existed in the audio received by the agent. You can find call recordings associated with a contact in the Contact Search report.
- **Contact IDs from the contact record** —Provide when you contact AWS support.
- **Agent desktop performance/process logs**—can help rule out local resource/network contention.
- **Contact Control Panel (CCP) logs**—to track agent actions and timing. To download CCP logs, choose the settings cogwheel in the CCP, and then choose **Download logs**. The logs are saved to your browser's default download directory.

- **Network utilization logging/monitoring**—specifically for latency and dropped packets on the same network segment as your agents.
- **Private WAN/LAN network diagram**—outlining connection paths to the edge router to AWS to explain network traversal.
- **Firewall 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. 605).
- **Audio capturing and analytic tools**—for latency calculations from the agent's workstation.
- **AWS region latency test tools**—use the Endpoint Test Utility tool (p. 1193).

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 outbound call with large impact).
- 6:34PM agentName MI3 (missed inbound call with large impact).

Analyzing the Data

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

- Use the Contact record / Contact search report to identify the contact IDs for the contacts during which call quality issues occurred. The contact record includes a link to the associated call recording, and additional details that you can use for symptom verification and to provide to your AWS support representative.
- Use the agent name and timestamp in the contact record to get a sense of the types of issues you're experiencing and their prevalence by agent, symptom, scenario, and severity over time. This will allow you to see if issues are happening around the same time, surround a specific event, or are isolated to specific agents or agent actions. You can also easily identify and access associated call recordings and associated contact IDs available if you need to engage support.
- Correlate data sources, such as local network logs, CPU/disk/memory utilization and process monitor logs from the operating system on the client workstation. This lets you correlate events by agent over time to rule out local resource contention as a cause or contributor.
- Analyze data by symptom and scenario reported per minute or per hour to create heat maps of an issue by type and severity by agent over time. Doing this is especially helpful in environmental troubleshooting as you may find clustered impacts associated with scheduled activity like backups or large file transfers.
- If you can't find any evidence of local resource contention or derive any noteworthy correlations, you can use the contact IDs collected to open a support case. If issues experienced are intermittent in nature, they most likely relate to issues with the agent's workstation, network connectivity, or both.

Validation Testing

Voice quality issues can have many contributing sources. It's important to run controlled tests and monitor the same environment or workstation as those reporting the issue, and be able to reproduce the same use cases. Consider the following general testing recommendations for measuring and gathering data to investigate voice quality issues.

PSTN and Agent Connection Latency

For troubleshooting cross-talk issues, you need to differentiate and measure agent and raw PSTN latency contributions, as they require different remediation efforts.

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

Amazon Connect leverages CloudFront for connectivity. Not all CloudFront ranges are advertised over AWS Direct Connect. This means not all URLs generated by Amazon Connect are reachable over a Public Virtual Interface.

- [redirect_latency] is the latency resulting in redirecting audio to an external device. This latency can be calculated by measuring [overall_latency] once with redirect and once without and take the difference between the two.
- [forward_latency] is the latency resulting in forward calls to or from Amazon Connect. This latency can be calculated by measuring [overall_latency], once with forward and once without, and take the difference between the two.

Measuring Latency

In addition to the steps below, see Measure latency for validation testing and troubleshooting in Amazon Connect).

- Reproduce your use case. Any deviations need to be measured and accounted for, because they skew test results.
- Match production controls and environment as much as possible. Use the same flows, phone numbers, and endpoint locations.
- Note the geographical locations of your callers, agents, and external transfer destinations, where applicable. If you are servicing multiple countries, each country should be tested individually to provide the same test coverage that your agents experience in production.
- Note mobile and land line use in your tests. Mobile networks can add latency and need to be measured and considered for customer, agent, and transfer endpoints, where applicable.
- Reproduce the business use case. If the agents use conference and transfer, be sure to test those scenarios. If circular transfers occur, which are not recommended, be sure to test those as well.
- Reproduce the agent environment by including the workstation environment, located on the same network segment, and using equipment your agents would use.

Requirements for Testing Latency

To perform effective testing for latency, the following are required:

- Call recording enabled to capture [agent_latency]. Without call recording, you can calculate only [overall_latency].
- A customer phone source. For testing, confirm call quality on an actual call from a customer.
- An agent phone, if redirecting audio to an external device. You must be able to record the input and output of this device.
- A third-party transfer endpoint, if applicable. Testing is best when performed on actual calls or transfers from a third party.
- An agent workstation with sound recording or analysis software.
- Reproducible use cases. Troubleshooting can be difficult for issues that cannot be reproduced.
- NTP or other method to sync timestamps to facilitate identifying specific contacts and when they occurred, especially when activity is occurring across multiple time zones.

Testing Inbound Calls Using a Soft Phone

This process allows you to complete a latency test scenario in about 15 seconds. Analyzing the results and marking timestamps takes approximately 1-2 minutes per recording.

1. Go to a quiet location.

2. Configure agent workstation to play audio from external speakers and make sure they are turned up.
3. Use the agent workstation to log in to the CCP.
4. Start recording using an audio capturing tool on the agent workstation.
5. From the customer's phone source, use a speaker phone to call the incoming number for your Amazon Connect instance. This could really just be any external phone source to simulate a customer call.
6. Answer the incoming call using the soft phone on the agent workstation.
7. Make sure that the customer phone is not muted.
8. On the customer side, use an object or your hand, tap loudly on the desk or table, and then immediately mute the customer phone.
9. Wait 3 or more seconds. Repeat steps 7-8 at least 3 times.
10. Stop recording on the agent workstation.
11. Open the recording in your audio analysis tool. You should be able to see both the initial tapping sound that you made on the desk, and the tapping sound on the agent line on the other end. Take the three deltas and average for your [overall_latency].
12. Optionally, to calculate [agent_latency], open the associated Amazon Connect call recording in your audio analysis tool. You should be able to see both the initial tapping sound and the sound when it arrives to the agent at the other end. Take the three deltas and average for your [recording_latency]. [agent_latency] = [overall_latency] - [recording_latency]. Repeat as needed.

Modify the test plan as necessary to fit your use case. As the steps change, the process of recording and analyzing the audio is the same. If you need to test conferences and transfers, take measurements as normal, and then take another measurement when the conference is active with the third party transfer endpoint.

Interpreting the Test Results

The impact of increasing [overall_latency] begins to be noticeable at approximately 300ms and can result in crosstalk above 500ms. The impact, and what level of latency is considered acceptable, depends on your use case. For recommended remediation efforts for decreasing latency, see the PSTN and Agent Connection Latency (p. 1198).

Mobile phones (iPhone, Android) and iPads are not supported

The default version of the Contact Control Panel (CCP) does not work with mobile devices such as iPhones and iPads.

You can set up your CCP to forward the audio portion of the call to your mobile device. For instructions, see Forward calls to a mobile device (iPhone, Android) (p. 1144).

Microsoft Edge is not supported

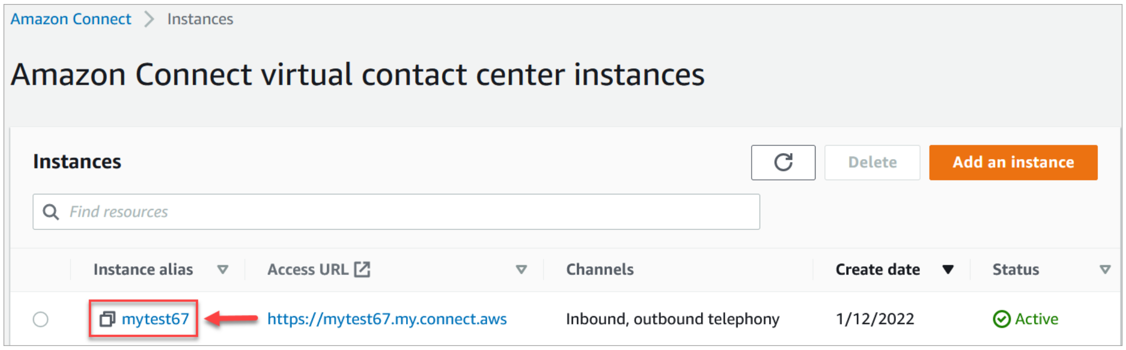
Using Microsoft Edge or Edge Chromium with the Contact Control Panel is not supported. For a list of supported browsers, see Browsers supported by Amazon Connect (p. 4).

Can't make an outbound call from the CCP

The top reason most agents can't make outbound calls from the CCP is because their instance of Amazon Connect has not been set up to make outbound calls.

To enable agents to make outbound calls

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. On the instances page, choose the instance alias. The instance alias is also your **instance name**, which appears in your Amazon Connect URL.



Amazon Connect > Instances

Amazon Connect virtual contact center instances

Instances

	Instance alias	Access URL	Channels	Create date	Status
○	mytest67	https://mytest67.my.connect.aws	Inbound, outbound telephony	1/12/2022	Active

3. In the navigation pane, choose **Telephony**.
4. To enable outbound calling from your contact center, choose **I want to make outbound calls with Amazon Connect**.
5. Choose **Save**.

Attachments are not appearing in chats

The following issues may cause attachments to not display for your agents using chat.

Internal firewall settings are preventing access

Check that your firewall isn't preventing agents from accessing the files in your Amazon S3 bucket. You may need to add the Amazon S3 bucket where your files are stored to your domain allow list. For more information, see Set up your network (p. 605).

Attachments are too large, too many, or don't meet file type requirements

Check that the attachments meet the size, number, and file type requirements. For more information, see Feature specifications (p. 1210).

To calculate the size of an attachment (artifactSizeInBytes), use a third-party tool such as File.size.

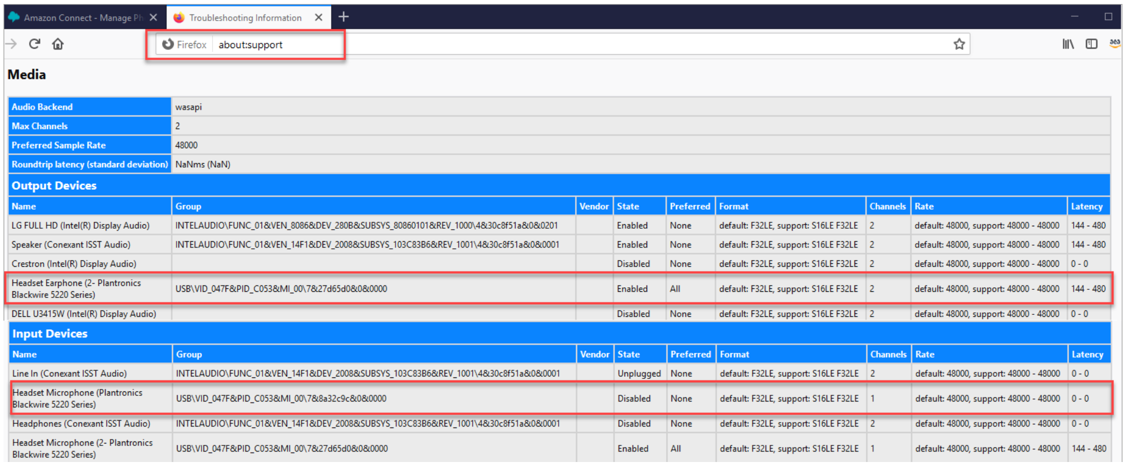
Humming sound in headset: Verify the headset and browser sample rates

If the agent's audio device does not support up to 48khz and the browser asserts a sample rate of 48khz, audio issues such as an audible humming sound may be present in the agent's outgoing audio. This has been seen with Firefox but not with Chrome.

Perform the following steps to verify your headset and browser sample rates.

Verify Firefox sample rate

1. Open the agent's CCP in FireFox, and set their status to **Available**.
2. Accept a call.
3. Open a second Firefox tab, and type **about:support** in the Search box.
4. Scroll down the page to **Media**.
5. Verify that the sample rates for the input and output devices are **48000**, as shown in the following image.



Media

Audio Backend	wasapi
Max Channels	2
Preferred Sample Rate	48000
Roundtrip latency (standard deviation)	NaNms (NaN)

Output Devices

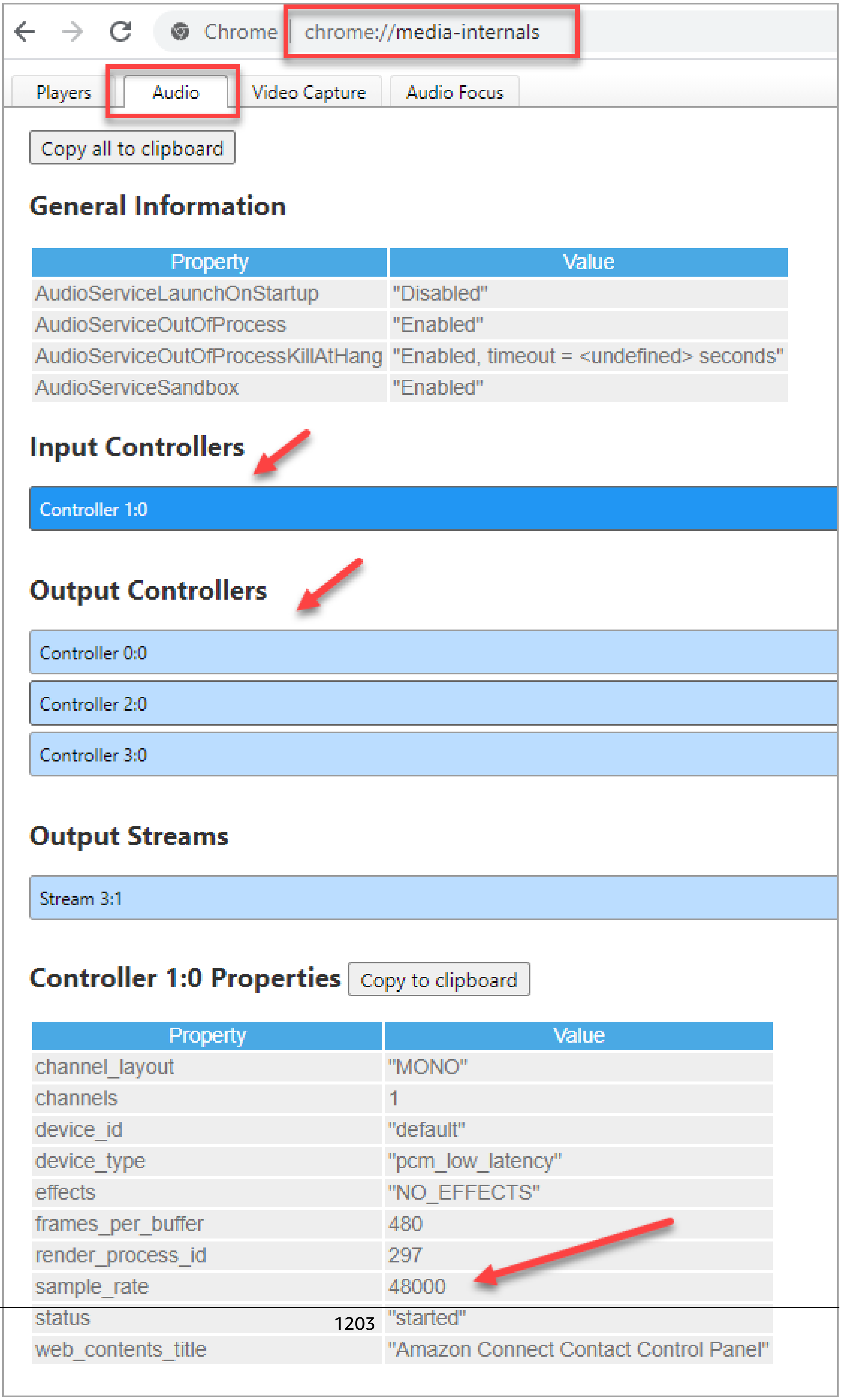
Name	Group	Vendor	State	Preferred	Format	Channels	Rate	Latency
LG FULL HD (Intel(R) Display Audio)	INTELAUDIO\FUNC_01&VEN_8086&DEV_280B&SUBSYS_80860101&REV_1000\4&30c8f51a&0&0201		Enabled	None	default: F32LE, support: S16LE F32LE	2	default: 48000, support: 48000 - 48000	144 - 480
Speaker (Conexant ISST Audio)	INTELAUDIO\FUNC_01&VEN_14F1&DEV_2008&SUBSYS_103C83B6&REV_1001\4&30c8f51a&0&0001		Enabled	None	default: F32LE, support: S16LE F32LE	2	default: 48000, support: 48000 - 48000	144 - 480
Crestron (Intel(R) Display Audio)			Disabled	None	default: F32LE, support: S16LE F32LE	2	default: 48000, support: 48000 - 48000	0 - 0
Headset Earphone (2- Plantronics Blackwire 5220 Series)	USB\VID_047F&PID_C053&MI_00\7&27d65d0&0&0000		Enabled	All	default: F32LE, support: S16LE F32LE	2	default: 48000, support: 48000 - 48000	144 - 480
DELL U3415W (Intel(R) Display Audio)			Disabled	None	default: F32LE, support: S16LE F32LE	2	default: 48000, support: 48000 - 48000	0 - 0

Input Devices

Name	Group	Vendor	State	Preferred	Format	Channels	Rate	Latency
Line In (Conexant ISST Audio)	INTELAUDIO\FUNC_01&VEN_14F1&DEV_2008&SUBSYS_103C83B6&REV_1001\4&30c8f51a&0&0001		Unplugged	None	default: F32LE, support: S16LE F32LE	2	default: 48000, support: 48000 - 48000	0 - 0
Headset Microphone (Plantronics Blackwire 5220 Series)	USB\VID_047F&PID_C053&MI_00\7&8a32c9c&0&0000		Disabled	None	default: F32LE, support: S16LE F32LE	1	default: 48000, support: 48000 - 48000	0 - 0
Headphones (Conexant ISST Audio)	INTELAUDIO\FUNC_01&VEN_14F1&DEV_2008&SUBSYS_103C83B6&REV_1001\4&30c8f51a&0&0001		Disabled	None	default: F32LE, support: S16LE F32LE	2	default: 48000, support: 48000 - 48000	0 - 0
Headset Microphone (2- Plantronics Blackwire 5220 Series)	USB\VID_047F&PID_C053&MI_00\7&27d65d0&0&0000		Enabled	All	default: F32LE, support: S16LE F32LE	1	default: 48000, support: 48000 - 48000	144 - 480

Verify Chrome sample rate

1. Open the agent's CCP in Chrome, and set their status to **Available**.
2. Accept a call.
3. Open a second Chrome tab, and type **chrome://about** in the Search box.
4. Scroll down the page and choose **chrome://media-internals**.
5. On the **Audio** tab, choose the **Input Controllers** and verify that the sample rate is **48000**. Then verify the sample rate for the Output Controllers.



General Information

Property	Value
AudioServiceLaunchOnStartup	"Disabled"
AudioServiceOutOfProcess	"Enabled"
AudioServiceOutOfProcessKillAtHang	"Enabled, timeout = <undefined> seconds"
AudioServiceSandbox	"Enabled"

Input Controllers

Controller 1:0

Output Controllers

Controller 0:0

Controller 2:0

Controller 3:0

Output Streams

Stream 3:1

Controller 1:0 Properties

Property	Value
channel_layout	"MONO"
channels	1
device_id	"default"
device_type	"pcm_low_latency"
effects	"NO_EFFECTS"
frames_per_buffer	480
render_process_id	297
sample_rate	48000
status	"started"
web_contents_title	"Amazon Connect Contact Control Panel"

One-way audio from customers?

If an agent can hear the customer, but the customer can't hear the agent, this may be the result of an application taking exclusive control of agent's mic/speaker.

For instructions about how to disable it, see How do I turn off Exclusive-Mode for a Windows audio playback device?

Troubleshoot problems pausing, rewinding, or fast-fowarding recordings

If you are unable to pause, rewind or fast-forward recordings on the **Contact search** page, one possible reason could be that your network is blocking HTTP range requests. See HTTP range requests on the MDN Web Docs site. Work with your network administrator to unblock HTTP range requests.

Amazon Connect service quotas

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

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

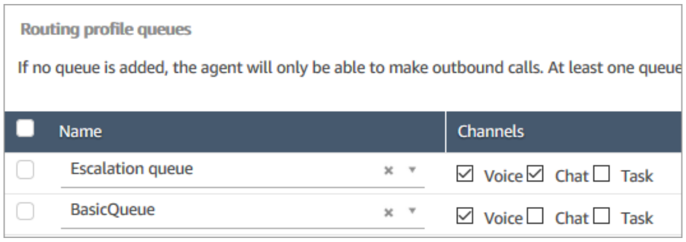
To request a quota increase, see Requesting a quota increase in the *Service Quotas User Guide*. If the quota is not yet available in Service Quotas, use the Amazon Connect service quotas increase form. You must be signed in to your AWS account to access the form.

Considerations

- You must create your instance before you can request a service quota increase.
- It can take up to a few weeks to increase your service quota. If you're increasing your quotas as part of a larger project, be sure to add this time to your plan.
- Use the same form to submit a request to port your US phone number from your current carrier to Amazon Connect. For more information about porting phone numbers, see Port your current phone number (p. 157).
- This documentation describes the default quotas for new accounts. Because the quotas have been adjusted over time, the default values for your account might be different than the default values described here.

Amazon Connect quotas

Name	Default	Adjustable
AWS Lambda functions per instance	35	Yes
Agent status per instance	50	No
Amazon Connect instances per account	2	Yes
Amazon Lex bots per instance	70	Yes
Amazon Lex V2 bot aliases per instance	100	Yes
Concurrent active calls per instance	10 For more information, see the section called “How contacts are counted” (p. 1214).	Yes
Concurrent active chats per instance	100 This includes chats that are waiting. If this quota is exceeded, the API call fails with a quota exceeded error.	Yes

Name	Default	Adjustable
Concurrent active tasks per instance	2500 concurrent active tasks All tasks that have not yet ended are considered active and are counted as concurrent tasks: tasks that are being routed in flows, waiting in a queue for an agent, being handled by agents, or being run in After Contact Work (ACW).	Yes
Contact flows per instance	100	Yes
Hours of operation per instance	100	Yes
Maximum duration that a task can be scheduled in future	6 days	No
Modules per instance	200	No
Phone numbers per instance	5 It's possible to get an error message that "You've reached the limit of Phone Numbers," even if it's the first time you've claimed a phone number. All the issues that cause this error message require help from AWS Support to resolve.	Yes
Prompts per instance	500	Yes
Queues per instance	50	Yes
Queues per routing profile per instance	50 This quota refers to number of queue/channel combinations per routing profile. For example, in the following image there are two queues, but there are three queue-channel combinations: Escalation queue Voice, Escalation queue Chat, and BasicQueue Voice. This counts three towards the service limit of 50.  Routing profile queues If no queue is added, the agent will only be able to make outbound calls. At least one queue □ Name | Channels □ Escalation queue | ☑ Voice ☑ Chat □ Task □ BasicQueue | ☑ Voice □ Chat □ Task	Yes
Quick connects per instance	100	Yes
Rate of API requests	See Amazon Connect API throttling quotas (p. 1216).	Yes

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

Amazon Connect Customer Profiles service quotas

Name	Default	Adjustable
Amazon Connect Customer Profiles domains count	100	Yes
Keys per object type	10	Yes
Maximum expiration in days	1,096 (3 years) This is the expiration of objects and profiles.	Yes
Maximum number of integrations	50	Yes

Name	Default	Adjustable
Maximum size of all objects for a profile	50MB	Yes
Object and profile maximum size	250KB	No
Object types per domain	100	Yes
Objects per profile	1000 This is the maximum number of objects that can be attached to a profile.	Yes
Maximum number of Identity Resolution Jobs each week for a domain	3	No
Maximum number of consolidation rules in an Identity Resolution Job	10	No
Maximum number of attributes in each consolidation rule	20	No

Amazon Connect Cases service quotas (Preview)

For this preview release, please contact AWS Support for any changes to Case quotas.

Name	Default	
Cases domains per AWS account	2	
Fields in a Cases domain	50	
Field options per single-select field in the Cases domain	100	
Layouts in a Cases domain	25	
Templates in a Cases domain	25	

Name	Default	
Related items that can be attached to a case	50	
Case fields per case template	30 (cannot be increased)	

High-volume outbound communications quotas

Name	Default	Adjustable
Amazon Connect campaigns	25	Yes

Amazon Connect Voice ID service quotas

Item	Default quotas
Domains	3 This quota applies per account.
Concurrent active sessions per domain	50 See the following table (p. 1209) for information about how to derive your **Concurrent active sessions** quota based on your Amazon Connect call volume.
Maximum number of fraudsters per domain	500
Maximum number of speakers per domain	100,000
Active Batch Speaker Enrollment Jobs per domain	1
Active Batch Fraudster Registration Jobs per domain	1
Speakers per Batch Speaker Enrollment Job	10,000
Fraudsters per Batch Fraudster Registration Job	500

Derive Concurrent active sessions based on your Amazon Connect call volume

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

Amazon Connect Voice Contacts (Calls)/Hour*	Voice ID Concurrent active sessions
1,000	50
5,000	250
10,000	500
20,000	1,000
50,000	2,500

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

Amazon Connect Wisdom service quotas

Item	Default quotas
Assistants	5
Knowledge bases	10
Maximum size of a knowledge base	5GB per knowledge base
Content per knowledge base	10,000
Maximum size per document	1MB
RateLimit for all APIs	50TPS

Feature specifications

The following table lists feature specifications.

> **Note**
> Feature specifications cannot be increased.

Item	Feature Specification
Maximum size of a real-time metrics report	200KB
File types supported for chat attachments	.csv, .doc, .docx, .jpeg, .jpg, .pdf, .png, .ppt, .pptx, .txt, .wav, .xls, .x
Max file size for a chat attachment	20MB
Attachments per chat conversation	35
People who can listen in on the same agent call at the same time	5 For example, you can have a group of 5 people listen in to a call at the same time, and then a different group of 5 people listen in to a different call at the same time, and so on.

Item	Feature Specification
Quick connects you can assign to a queue	700
Participants on a conference call	6 The participants are the customer, agent, and others who can be agents or external third-parties.
Contact record retention	24 months from the time the associated contact was initiated. You can choose to stream contact records to Kinesis so you can manage retention and perform advanced analysis.
Max size of the contact record attributes section	32KB
Active chats per agent	10
Total duration per chat	Up to 7 days, including wait time • The default is 25 hours. You configure the chat duration using StartChatContact API and add the `ChatDurationInMinutes` parameter. • Minimum configurable chat duration is 1 hour (60 minutes). • Maximum configurable chat duration is 7 days (10,080 minutes).
Characters per chat message	1024
Open websocket connections per chat participant	5
Chat Amazon Lex bot integration timeout	6 seconds The maximum time within which the Amazon Lex bot must respond to the chat customer's prompt.
Task templates per instance	50
Task template customized fields per instance	50
Maximum duration of a task	7 days
Maximum number of transfers for a task	11 transfers
Maximum number of linked tasks on an existing contact	11

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

Contact Lens for Amazon Connect feature specifications

To request changes to the following specifications, use the Amazon Connect service quotas increase form. You must be signed in to your AWS account to access the form.

Item	Feature Specification
Concurrent real-time calls with analytics	50 100 for US East (N. Virginia)
Concurrent post-call analytics jobs	200 See the following table (p. 1212) for information about how to derive your concurrent post-call analytics jobs based on your Amazon Connect call volume.
Custom vocabularies	20
Contact Lens rules	200

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

A post-call analytics job is kicked off after the completion of each call with Contact Lens enabled. The time to complete a post-call analytics job is about 40% of the call length. To calculate concurrent post-call analytics jobs, use the following formula:

```
(average call duration in minutes) * (0.4) * (calls per hour) / (60)
```

The following table shows some examples.

Average call duration (in minutes)	Calls per hour*	Approximate Concurrent post-call jobs
5	1000	33
10	500	33
10	1000	67
10	3000	200

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

Amazon Connect Rules feature specifications

The following table lists feature specifications.

> **Note**
> Feature specifications cannot be increased.

Item	Feature Specification
Published rules per instance	200
Draft rules per instance	50
Conditions in a rule	20

Condition type	Number of entries or selections	Post-call	Real-time
Words or phrases - Exact match	100	Yes	Yes
Words or phrases - Semantic match	4	Yes	Not supported
Words or phrases - Pattern match	100	Yes	Yes
Queue condition	100	Yes	Yes
Agent condition	100	Yes	Yes
Custom attributes	5	Yes	Yes
Sentiment - Time period	5	Yes	Yes
Sentiment - Entire contact	5	Yes	Not supported
Interruptions	5	Yes	Not supported

Condition type	Number of entries or selections	Post-call	Real-time
Non-talk time	5	Yes	Not supported

How contacts are counted

The following contacts are counted:

- Handled by a contact flow
- Waiting in queue
- Handled by an agent
- Outbound call

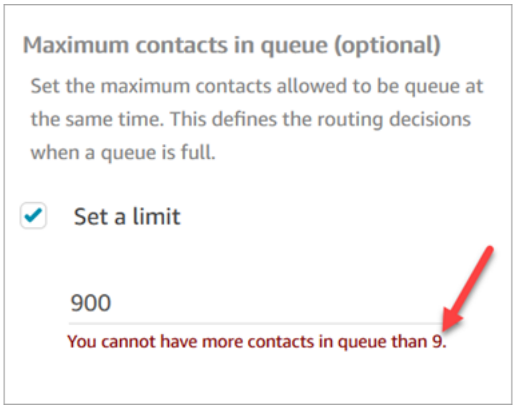
The following contacts are not counted:

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

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

You can calculate your configured quota using CloudWatch metrics. For instructions, see Use CloudWatch metrics to calculate concurrent call quota (p. 1025).

If you're only taking calls you can also determine your concurrent calls quota by editing a queue and entering an exceptionally large number for the contact limit. The resulting error message displays your quota for concurrent calls. For example, in the following image, it shows the call quota for that instance is 9.



Maximum contacts in queue (optional)

Set the maximum contacts allowed to be queue at the same time. This defines the routing decisions when a queue is full.

☑ Set a limit

900

You cannot have more contacts in queue than 9.

Countries you can call

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

Submit a service quota increase request to allow calling to additional countries, or to limit the countries that you can call from. You must be signed in to your AWS account to access the form.

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

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

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

You can call the following countries by default:

- United States
- Canada
- Mexico
- Puerto Rico
- United Kingdom: See Prefixes that are not allowed by default (p. 1216)

Instances created in Africa (Cape Town)

You can call the following countries by default:

- South Africa
- United Kingdom
- United States

Instances created in Asia Pacific (Seoul)

You can call the following countries by default:

- South Korea
- United Kingdom
- United States

Instances created in Asia Pacific (Singapore)

You can call the following countries by default:

- Singapore
- Australia
- Hong Kong
- United States
- United Kingdom: See Prefixes that are not allowed by default (p. 1216)

Instances created in Asia Pacific (Sydney)

You can call the following countries by default:

- Australia
- New Zealand
- Philippines
- United States

Instances created in Asia Pacific (Tokyo)

You can call the following countries by default:

- Japan: See Prefixes that are not allowed by default (p. 1216)
- Vietnam
- United States

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

You can call the following countries by default:

- United Kingdom: See Prefixes that are not allowed by default (p. 1216)
- Italy
- France
- Ireland
- United States

Prefixes that are not allowed by default

UK numbers with the following prefixes are not allowed by default:

- +447 +44111 +44118 +44119 +448 +44826 +449

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

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

- +8170, 8180, and 8190

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

Amazon Connect API throttling quotas

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

- If different 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.

  Note
  The rate limit cannot be increased for GetMetricData and GetCurrentMetricData.

- For StartChatContact, StartContactStreaming, StopContactStreaming, a RateLimit of 5 requests per second, and a BurstLimit of 8 requests per second.
- For all other operations, a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.

Amazon Connect Participant Service API throttling quotas

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

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

- CreateParticipantConnection: a RateLimit of 6 requests per second, and a BurstLimit of 9 requests per second.
- DisconnectParticipant: a RateLimit of 3 requests per second, and a BurstLimit of 5 requests per second.
- GetTranscript: a RateLimit of 8 requests per second, and a BurstLimit of 12 requests per second.
- SendEvent and SendMessage: a RateLimit of 10 requests per second, and a BurstLimit of 15 requests per second.
- StartAttachmentUpload: a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.
- CompleteAttachmentUpload: a RateLimit of 2 requests per second, and a BurstLimit of 5 requests per second.
- GetAttachment: a RateLimit of 8 requests per second, and a BurstLimit of 12 requests per second.

Amazon Connect Contact Lens Service API throttling quotas

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

- If different 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 Contact Lens API, the number of requests per second is limited to the following:

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

Amazon Connect Cases API throttling quotas (Preview)

API	Default TPS throttling limits
CreateCase, SearchCases, UpdateCase, AssociateContact, ListTemplates, CreateRelatedItem, SearchRelatedItems	10
CreateField, ListFields, CreateDomain, GetDomain,CreateTemplate, BatchPutFieldOptions, CreateLayout, UpdateLayout, UpdateTemplate, UpdateField	5
BatchGetField	25
GetCase	15
GetTemplate, GetLayout	20
ListFieldOptions	15

Amazon Connect Voice ID Service API throttling quotas

API	Default TPS throttling limits
EvaluateSession	60
Domain APIs: CreateDomain, DescribeDomain, UpdateDomain, DeleteDomain, ListDomains Batch APIs: StartSpeakerEnrollmentJob, DescribeSpeakerEnrollmentJob, ListSpeakerEnrollmentJobs, StartFraudsterRegistrationJob, DescribeFraudsterRegistrationJob, ListFraudsterRegistrationJobs	2
ListSpeakers	5
DescribeSpeaker, OptOutSpeaker, DeleteSpeaker, DescribeFraudster, DeleteFraudster	10
CreateIntegrationAssociation, DeleteIntegrationAssociation, ListIntegrationAssociation	2
TagResource, UnTagResource, ListTagsForResource	2

Additional resources for Amazon Connect

In addition to using the contents of this guide, you can learn more about Amazon Connect by using the following resources.

Resources

Amazon Connect API Reference

The Amazon Connect API Reference describes the API actions that are used to set up and manage your contact center.

Amazon Connect Participant Service API Reference

The Amazon Connect Participant Service API Reference describes the API actions that are used to manage chat participants, such as agents and customers.

Amazon AppIntegrations Service API Reference

The Amazon AppIntegrations Service API Reference describes the API actions that you can use to configure connections to external applications.

Contact Lens for Amazon Connect API Reference

The Amazon Connect Contact Lens API Reference describes the API actions that you can use to access an up-to-date transcript, along with all the associated conversation characteristics while a call is still in progress. This helps to reduce the need for agents to write detailed call summaries and enables a seamless handoff from one agent to another during a call transfer.

Amazon Connect Customer Profiles API

The Amazon Connect Customer Profiles API Reference describes the API actions that you can use to manage domains and profiles.

Amazon Connect Voice ID API Reference

The Amazon Connect Voice ID API Reference describes the API actions that provide real-time caller authentication and fraud screening.

Amazon Connect Wisdom API Reference

The Amazon Connect Wisdom API Reference describes the API actions that deliver information to agents to help them solve customer issues.

Amazon Connect Streams

The Amazon Connect Streams documentation describes how to integrate your existing web applications with Amazon Connect. Streams gives you the power to embed the Contact Control Panel (CCP) UI components into your page, and/or handle agent and contact state events directly giving you the power to control agent and contact state through an object oriented event driven interface. You can use the built in interface or build your own from scratch: Streams gives you the power to choose.

Amazon Connect Chat UI Examples

The Amazon Connect Chat SDK and Sample Implementations provides examples of how to enable your app to engage with Amazon Connect chat.

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

July 2022 Updates

Search for contacts by using the agent's first or last name

You can search for contacts using the agent's first or last name. The filter name is **Agent**. To view an image of this experience, see Search contacts by agent's first or last name (p. 907).

Released updates for rich text format rendering

On the **Contact Search** and **Contact Detail** pages, you can now view chat transcripts that have rich text formatting, such as bold or italic font, bullet points, numbered lists, and hyperlinks. For more information about getting started with Amazon Connect Chat, see Set up your customer's chat experience.

View call transcript using the CCP or agent application

Agents can view call unredacted transcripts in the CCP and agent application. For more information, see View a call transcript during ACW.

June 2022 Updates

Support for Lex intent confidence scores and sentiment analysis

You can further personalize the automated self-service customer experience using Amazon Lex intent confidence scores and sentiment analysis as a branch within your flows. For more information, see the Get customer input block. For a list of new contact attributes, see Amazon Lex contact attributes.

Released Amazon Connect Cases (Preview)

Amazon Connect Cases (Preview) allows your agents to quickly track and manage customer issues that require multiple interactions, follow-up tasks, and teams in your contact center. For more information, see Amazon Connect Cases (Preview) and Amazon Connect Cases API Reference (Preview).

GA for High-volume outbound communications

Released Amazon Connect High-volume outbound communications for General Availability. This release includes a set of APIs for creating and managing high-volume outbound campaigns. For more information, see Enable high-volume outbound communications and Amazon Connect High-Volume Outbound Communications API Reference.

Released GetCurrentUserData API

Released the GetCurrentUserData API. It enables you to return the real-time active user data from the specified Amazon Connect instance.

Released task templates

You can now create custom task templates, making it easy for agents to consistently capture the relevant and required information to create or complete tasks. For more information, see Create task templates. For information about using the API to programmatically create and manage task templates, see the Amazon Connect API Reference and the Amazon Connect Resource Type Reference in the *AWS CloudFormation User Guide*.

New API to transfer contacts

Added a new API that you can use to transfer contacts from one agent or queue to another agent or queue at any point after a contact is created. You can transfer a contact to another queue by providing the contact flow which orchestrates the contact to the destination queue. This gives you more control over contact handling and helps you adhere to the service level agreement (SLA) guaranteed to your customers.

For information, see TransferContact in the *Amazon Connect API Reference*.

May 2022 Updates

Updated workflow for high-volume outbound communications

Updated the workflow for onboarding to high-volume outbound communications using the Amazon Connect and Amazon Pinpoint user interface. For more information, see Enable high-volume outbound communications.

Voice ID expires speakers

For BIPA Compliance, Amazon Connect Voice ID automatically expires speakers that have not been accessed for enrollment, re-enrollment, or successful authentication for three years. You can see a speaker's last access time by looking at the `lastAccessedAt` attribute returned by the DescribeSpeaker and ListSpeakers APIs.

For more information, see What data is stored? in the Use real-time caller authentication with Voice ID topic.

April 2022 Updates

New API to change an agent's current status

Amazon Connect provides an API to programmatically change the current status of an agent. Agent statuses (p. 998) are used to determine when an agent is **Available** to be routed contacts in Amazon Connect, versus when they are set to **Offline** or a custom status such as **Lunch** or **Break** and should not be routed contacts. For more information, see PutUserStatus in the Amazon Connect API Reference.

New API to search for users by name, agent hierarchies, and tags

Added API to search for user records in your Amazon Connect instance. This new API provides a programmatic and flexible way to search for users by first name, last name, username, routing profile, security profile, agent hierarchies or tags. For example, you can now use this API to search for all users tagged with a Department:key value pair. You can also quickly find a list of all users assigned to a specific security profile, routing profile, or agent hierarchy. For more information, see the Amazon Connect API Reference.

New APIs to claim and configure phone numbers

Added new APIs to claim new phone numbers and configure them programmatically. Using these APIs, you can programmatically search for and claim available phone numbers, associate phone numbers to contact flows, or release phone numbers that are no longer needed. Additionally, the phone number APIs come with support for AWS CloudFormation. For more information, see the Amazon Connect API Reference and the Amazon Connect Resource Type Reference in the *AWS CloudFormation User Guide*.

Telephony: Multi-party calls

You can enable Amazon Connect to allow up to six parties on a call: the agent, the caller, and four more participants. (By default, Amazon Connect allows agents to have up to three parties on a call: the agent, and caller, and another participant.) For more information, see Update instance settings. For more information, see Host multi-party calls (p. 1167).

For information about new functionality on the existing Connection and Contact API in Amazon Connect Streams, see the Amazon Connect Streams Readme.

The following sections describes how managing multi-party calls differs from managing three-party calls.

Contents

New behavior with multi-party calls

- All agents see all of the connections in a call.
- All agents have exactly the same capabilities as any other agent on the call. This takes into affect the moment an agent accepts the invitation to join the call.
- Before a warm transfer is complete, an agent can start talking to the caller as well as disconnect any other agent on the call.

Comparison: Three-party and multi-party calls

The following table summarizes the differences between the agent's experience using the Contact Control Panel (CCP) for three-party calls and multi-party calls.

- Primary agent: the first agent on the call.
- Secondary agent: any agent other than the first agent on the call.

Three-party calls	Multi-party calls
Agent can control hold, resume, and disconnect only the parties they added.	All agents are have the same call control capabilities.
Agent can add one other participant to an existing call, for a total of three participants (the agent, the caller, and another participant).	Any agent on the call can add additional participants, as long as the total number of participants on the call, including themselves, does not exceed six.
Agent can put only the party they added on hold.	Any agent on the call can put any party on hold.
When a primary agent places a secondary agent on hold, the secondary agent can't take themselves off hold.	Any agent on the call can take themselves off hold.

Three-party calls	**Multi-party calls**
Secondary agent can talk to the primary agent during hold.	Secondary agents cannot talk to each other until they are taken off hold.
Primary agent can only mute themselves. Secondary agent can only mute themselves.	Any agent on the call can mute any other participant on the call.
When an agent disconnects (leaves or is disconnected), call control continues to be available to the remaining agent(s) on the call.	When an agent disconnects, control of the call is transferred to the remaining agents.
Only the primary agent can disconnect a party on the call. The secondary agent can disconnect the caller only if the primary agent has disconnected.	All agents have the capability to disconnect any other party.
The primary agent can see two connections (caller and another party), while a secondary agent sees only the transfer connection.	All agents can see all connections.
An agent only sees **internal transfer** for another agent on the call.	An agent sees the quick connect ID for other agents, instead of just **internal transfer**.
Not applicable.	When an party is being dialed, an agent on a multi-party call cannot add another party until the prior dial operation is completed (party added or call leg terminated).

Play prompts from an Amazon S3 bucket

Added the ability to source prompts from an Amazon S3 bucket. You can store as many voice prompts as needed in Amazon S3 and access them in real time by using contact attributes in the following contact blocks that play prompts: Get customer input (p. 366), Loop prompts (p. 390), Play prompt (p. 393), and Store customer input (p. 426).

For more information, see the Play prompt (p. 393) block. For information about the policy required for Amazon Connect to access the Amazon S3 bucket, see Set up prompts to play from an S3 bucket (p. 461).

CloudTrail support for queues and routing profiles

Amazon Connect records all changes made to users, routing profiles, and queues as events in AWS CloudTrail. For example, you can identify who took which action, what resources were acted upon, and when an event occurred. For more information, see the section called “Logging service API calls” (p. 1025).

March 2022 Updates

Rich messaging for chat

Added support for rich messaging for your customer's chat experience. Agents and customers can use bold, italics, bulleted lists, numbered lists, hyperlinks, and attachments. For more information, see Enable text formatting for your customer's chat experience.

Customer Profiles: Object type mapping user interface

Added a user interface for creating object type mapping by using the Amazon Connect admin console. For more information, see Create an object type mapping.

February 2022 Updates

Added bulk ingestion of data for Customer Profiles

Added support for the bulk ingestion of data for Customer Profiles. For more information, see *Bulk ingestion of data* in the Set up integration for Salesforce, ServiceNow, Marketo, or Zendesk topic.

New CloudWatch metrics for chat

Added the following Amazon CloudWatch metrics for chat: **ConcurrentActiveChats**, **ConcurrentActiveChatsPercentage**, **ChatBreachingActiveChatQuota**, and **SuccessfulChatsPerInterval**. For more information, see Monitoring your instance using CloudWatch (p. 1014).

January 2022 Updates

Configure maximum chat duration up to 7 days

You can configure the maximum chat duration to last up to 7 days. For more information, see the `ChatDurationInMinutes` parameter in the StartChatContact API.

Add custom vocabularies to Contact Lens

Improve the accuracy of speech recognition for product names, brand names, and domain-specific terminology, by expanding and tailoring the vocabulary of the speech-to-text engine in Contact Lens. For more information, see Add custom vocabularies (p. 823).

December 2021 Updates

Chat widget supports browser notifications

The chat widget supports browser notifications for desktop devices. For more information, see Browser notifications (p. 254).

Ingest data into Customer Profiles from Segment and Shopify

For more information, see Set up integration for Segment and Set up integration for Shopify.

November 2021 Updates

Released unified agent application

Amazon Connect released the unified agent application to improve the agent experience and customer interactions. For more information, see Agent training guide.

Released call summarization

Contact Lens for Amazon Connect provides the option for you to view a transcript summary. The summary shows only those lines where Contact Lens has identified an issue, outcome, or action item in the transcript. For more information, see View call summary.

Released Identity Resolution to consolidate similar profiles

Amazon Connect Customer Profiles offers Identity Resolution, a feature that is designed to automatically detect similar customer profiles by comparing name, email address, phone number, date of birth, and address. For example, two or more profiles with spelling mistakes, such as "John Doe" and "Jhn Doe," can be detected as belonging to the same customer "John Doe" using clustering and matching machine learning (ML) algorithms. Once a group of profiles are detected to be similar, admins can configure how profiles should be merged together by setting up consolidation rules by using the Amazon Connect admin console or Amazon Connect Customer Profiles APIs.

Amazon Connect Customer Profiles stores contact history at no charge

Amazon Connect Customer Profiles now provides contact history and customer information together in unified customer profiles at no charge, helping contact center managers personalize the contact center experience. In new instances, Customer Profiles is enabled by default. For more information, see Step 4: Data Storage in the *Create an Amazon Connect instance* topic.

Added modular flows to help you create common functions

Contact flow modules are reusable sections of a contact flow. You can create them to extract repeatable logic across your flows, and create common functions. For more information, see Contact flow modules for reusable functions.

New APIs to archive/unarchive and delete contact flows

Added new APIs that provide a programmatic and flexible way to manage your library of contact flows at scale. For example, contact flows used only during certain times of the year can be archived when not in use and then unarchived when needed. You can now also delete a contact flow so it is no longer available for use. For more information, see the Amazon Connect API Reference.

Search contacts by custom contact attributes

Added support for searching contacts by custom contact attributes (also called user-defined attributes). For more information, see Search by custom contact attributes.

Added Customer profiles block

Added the Customer profiles block. It enables you to retrieve, create, and update a customer profile.

Released Contact APIs

Added APIs so you can get and update contact details programmatically. For example, you can describe contact details such as queue information, chat attachments, task references, and update contact information such as task name. For more information, see DescribeContact, UpdateContact, and ListReferences in the *Amazon Connect API Reference*.

Released scheduled tasks

Added the ability to schedule tasks up to six days in the future to follow-up on customer issues when promised. You can also update the scheduled date and time using the UpdateContactSchedule API. For more information, see the Create task block and the Create a task topic in the *Agent training guide*.

Released security profiles APIs

Added APIs so you can create and manage security profiles programmatically. Security profiles help you manage who can access the Amazon Connect dashboard and Contact Control Panel (CCP), and who can perform specific tasks. For more information, see the Amazon Connect API Reference.

Changes to real-time metrics agent tables

We are rolling out a new service to maintain the high availability from metrics that you expect from Amazon Connect. Due to this change, the agent tables will now be sorted by availability status by default, rather than by agent login.

Additionally, the queues and routing profiles table will sort by agents online by default instead of queue or routing profile name.

Added new metrics

Added following new historical metrics: **Contacts transferred in by agent** and **Contacts transferred out by agent**. Added new real-time metrics: T**ransferred in by agent** and **Transferred out by agent**. For more information, see Historical metrics definitions and Real-time metrics definitions.

October 2021 Updates

Released real-time chat message streaming

You can subscribe to a real-time stream of chat messages. For more information, see Enable real-time chat message streaming.

Released `HoursOfOperation` APIs for General Availability

Released the Amazon Connect `HoursOfOperation` APIs for general availability (GA). Also launched AWS CloudFormation support for Users, User Hierarchies, and Hours of Operation. For more information, see the Amazon Connect API Reference and the AWS CloudFormation User Guide.

September 2021 Updates

Released Amazon Connect Wisdom General Availability

For more information, see Deliver information to agents using Amazon Connect Wisdom and the Amazon Connect Wisdom API Reference.

Amazon Connect Voice ID - General Availability

For more information, see Use real-time caller authentication with Voice ID and the Amazon Connect Voice ID API Reference.

Preview release of high-volume outbound communications

Added content for the preview release of high-volume outbound communications. By using Amazon Pinpoint Journeys and Amazon Connect, you can now create high-volume outbound campaigns for voice, SMS, and email. For more information, see Enable high-volume outbound communications.

New Amazon AppIntegrations Service APIs

New DataIntegration APIs for the Amazon AppIntegrations Service: `CreateDataIntegration`, `DeleteDataIntegration`, `GetDataIntegration`, `ListDataIntegrationAssociations`, `ListDataIntegrations`, `UpdateDataIntegration`.

For more information, see Amazon AppIntegrations Service API Reference.

Display name and contact attributes in chat

You can now personalize the chat experience, as you can specify the name of your customer that interacts using the chat user interface. You can also securely pass the contact attributes to capture information about the contact which can be used in the contact flow to further personalize the experience. For more information, see Pass the customer display name when a chat initializes and Pass contact attributes when a chat initializes.

Preview of agent application

Launched an updated UI for the agent application preview that combines Customer Profiles and the Contact Control Panel (CCP). For more information, see Access Customer Profiles in the agent application.

Added Create task block

Added the **Create task** block. It creates a new task, sets the tasks attributes, and initiates a contact flow to start the task. For more information, see Contact block: Create task.

August 2021 Updates

Improved user interface for Amazon Connect console

Released a redesigned and improved user interface for the Amazon Connect console, making it easier and faster to manage Amazon Connect instances. For more information, see Create an Amazon Connect instance (p. 135).

APIs for Hours of Operation and Agent Status (Preview)

Released for ungated preview new APIs for managing hours of operation and agent status. For more information, see Amazon Connect Service API Reference.

Contact Lens: Build rules that generate tasks and EventBridge events

Contact Lens rules now allow you to automatically generate tasks and EventBridge events based on uttered keywords, sentiment scores, customer attributes, and other criteria. For more information, see Create rules with Contact Lens (p. 577).

Networking: Allow AWS Global Accelerator

When using SAML Sign-In to your Amazon Connect instance, you now need to add the AWS Global Accelerator domain, ***. awsglobalaccelerator.com**, to your allow list. For more information, see Set up your network (p. 605).

July 2021 Updates

"Next status" feature for the CCP

In busy contact centers, it can be difficult for agents to take a break or go offline when contacts are being quickly routed to them. To help agents manage their time, we have released a feature that lets agents pause new contacts being routed to them while they finish their current contacts. When all their slots are cleared, Amazon Connect automatically sets agents to the next status, such as **Lunch**.

For details about how agents use this feature, see Set your "Next status" (p. 1145).

Metrics: No changes due to "Next status"

When an agent is in **Next status**, their metrics are the same as when their status is **Available**.

For example, an agent is handling one contact and chooses **Next status**. Here's what you'll see in the real-time metrics report:

- Agent Activity state = On Contact
- Agent - Staffed = 1

Non-productive time (NPT) is not incremented when an agent is in **Next status** because the agent is still **Available**. NPT increments only when the agent actually enters the non-productive status, such as **Lunch**.

Agent event stream has new NextAgentStatus field

When an agent sets their status to **Next status**, Amazon Connect populates a new `NextAgentStatus` field with the next status selected by the agent.

At the same time, the `AgentStatus` field continues to display `Available`.

The following code snippet shows what the agent event stream looks like when an agent has set their CCP to **Next status: Lunch**.

```
"CurrentAgentSnapshot":
{
    "AgentStatus": {
            "ARN": "example-ARN",
            "Name": "Available",
            "StartTimestamp": "2019-08-13T20:52:30.704Z"
        },
     "NextAgentStatus": {
            "Name": "Lunch",
            "ARN": "example-ARN2",
            "EnqueueTimestamp": "2019-08-13T20:58:00.004Z",
        }
}
```

When an agent has not selected a **Next status**, the field is `null`, as shown in the following snippet:

```
"CurrentAgentSnapshot": {
    "AgentStatus": {
            "ARN": "example-ARN",
            "Name": "Available",
            "StartTimestamp": "2019-08-13T20:52:30.704Z"
        },
     "NextAgentStatus": null
}
```

Amazon Connect Streams API and "Next status"

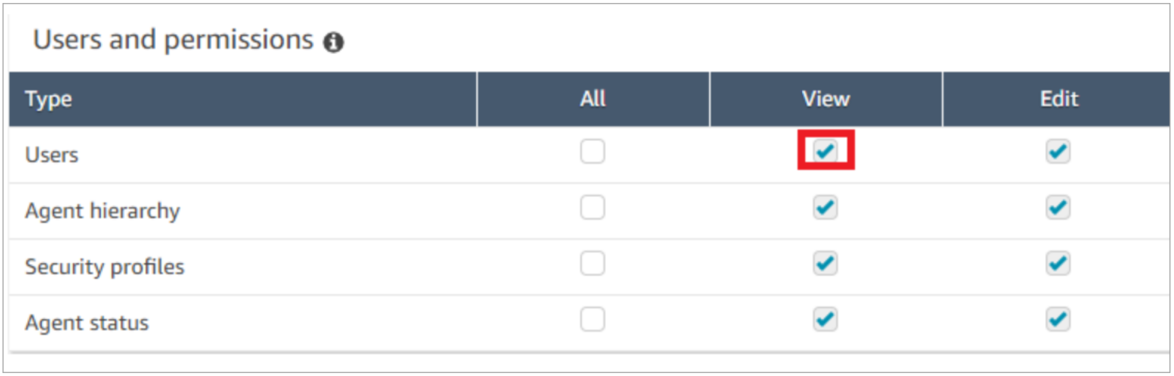
The feature has the following effect:

- If you integrate with Amazon Connect Streams API and your agents interact directly with the native CCP user interface, your agents will start using this new feature immediately.
- If you integrate with Amazon Connect Streams API but your agents don't interact directly with the native CCP user interface, your contact center will continue to have the previous behavior when agent.setState() is called: an agent will not be able to select an NPT or Offline status while connected to at least one contact.

  If you are handling state change logic yourself from Amazon Connect Streams, you will need to make additional changes explained in the Amazon Connect Streams README.

Contact search: To search contacts by Agent login requires Users - View permissions in your security profile

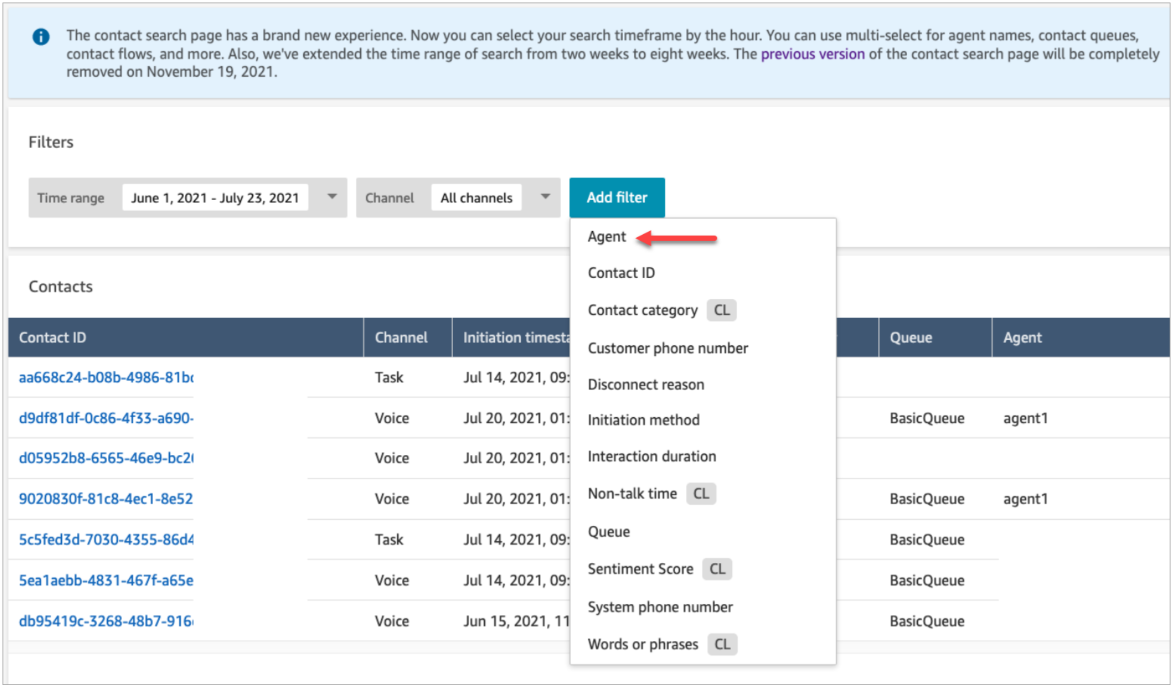
To use the **Agent** filter on the **Contact search** page, in your Amazon Connect security profile you must have **Users - View** permissions, as shown in the following image:



Users and permissions

Type	All	View	Edit
Users	□	☑	☑
Agent hierarchy	□	☑	☑
Security profiles	□	☑	☑
Agent status	□	☑	☑

When you have **Users - View** permissions, on the **Contact search** page the **Agent** filter appears, as shown in the following image:



The contact search page has a brand new experience. Now you can select your search timeframe by the hour. You can use multi-select for agent names, contact queues, contact flows, and more. Also, we've extended the time range of search from two weeks to eight weeks. The previous version of the contact search page will be completely removed on November 19, 2021.

Filters

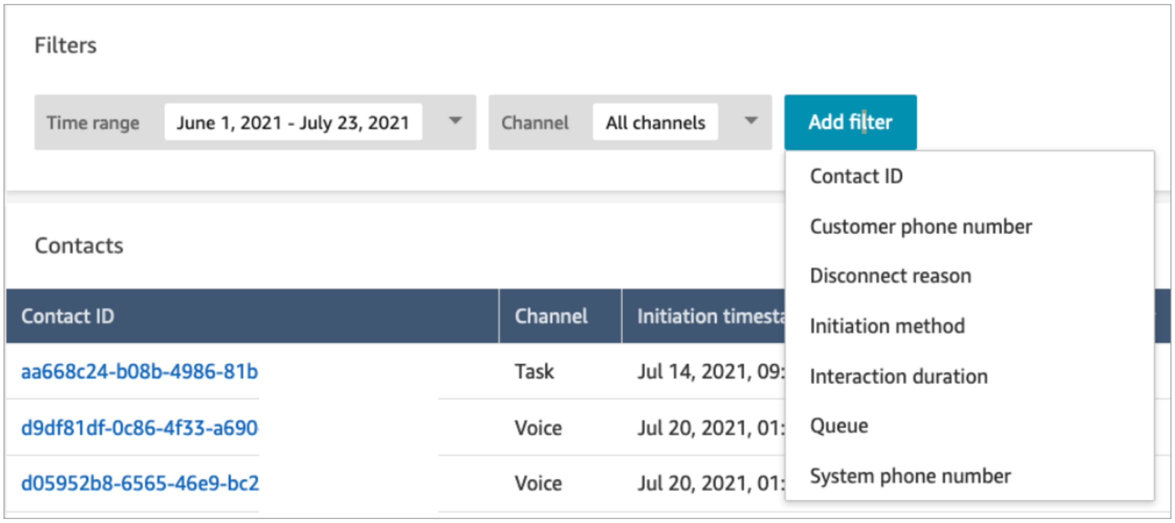
Time range: June 1, 2021 - July 23, 2021

Channel: All channels

Contacts

Contact ID	Channel	Initiation timesta	Queue	Agent
aa668c24-b08b-4986-81b	Task	Jul 14, 2021, 09:		
d9df81df-0c86-4f33-a690-	Voice	Jul 20, 2021, 01:	BasicQueue	agent1
d05952b8-6565-46e9-bc2	Voice	Jul 20, 2021, 01:		
9020830f-81c8-4ec1-8e52	Voice	Jul 20, 2021, 01:	BasicQueue	agent1
5c5fed3d-7030-4355-86d4	Task	Jul 14, 2021, 09:	BasicQueue	
5ea1aebb-4831-467f-a65e	Voice	Jul 14, 2021, 09:	BasicQueue	
db95419c-3268-48b7-916	Voice	Jun 15, 2021, 11	BasicQueue	

Without **User - View** permissions, the **Agent** filter is not visible, and searching contacts by Agent login is not supported, as shown in the following image:



Filters

Time range: June 1, 2021 - July 23, 2021

Channel: All channels

Contacts

Contact ID	Channel	Initiation timesta
aa668c24-b08b-4986-81b	Task	Jul 14, 2021, 09:
d9df81df-0c86-4f33-a690	Voice	Jul 20, 2021, 01:
d05952b8-6565-46e9-bc2	Voice	Jul 20, 2021, 01:

June 2021 Updates

Apple Messages for Business GA

Released Apple Messages for Business for general availability (GA). For more information, see Enable Apple Messages for Business (p. 259).

Quick connects management API GA

Released Amazon Connect quick connects management API for general availability (GA). For more information, see Amazon Connect Service API Reference. The quick connects API also supports AWS CloudFormation. For more information, see Amazon Connect Resource Type Reference in the AWS CloudFormation User Guide.

Support for Amazon Lex V2 console and APIs

For more information on using the Amazon Lex V2 console with Amazon Connect, see Add an Amazon Lex bot. Added these three APIs: AssociateLexBot, DisassociateLexBot, and ListLexBots. See the Amazon Connect Service API Reference.

Chat: Increase to chat agent concurrency

Chat agents can now handle up to 10 concurrent chat contacts. For more information, see Create a routing profile.

May 2021 Updates

Added contact events

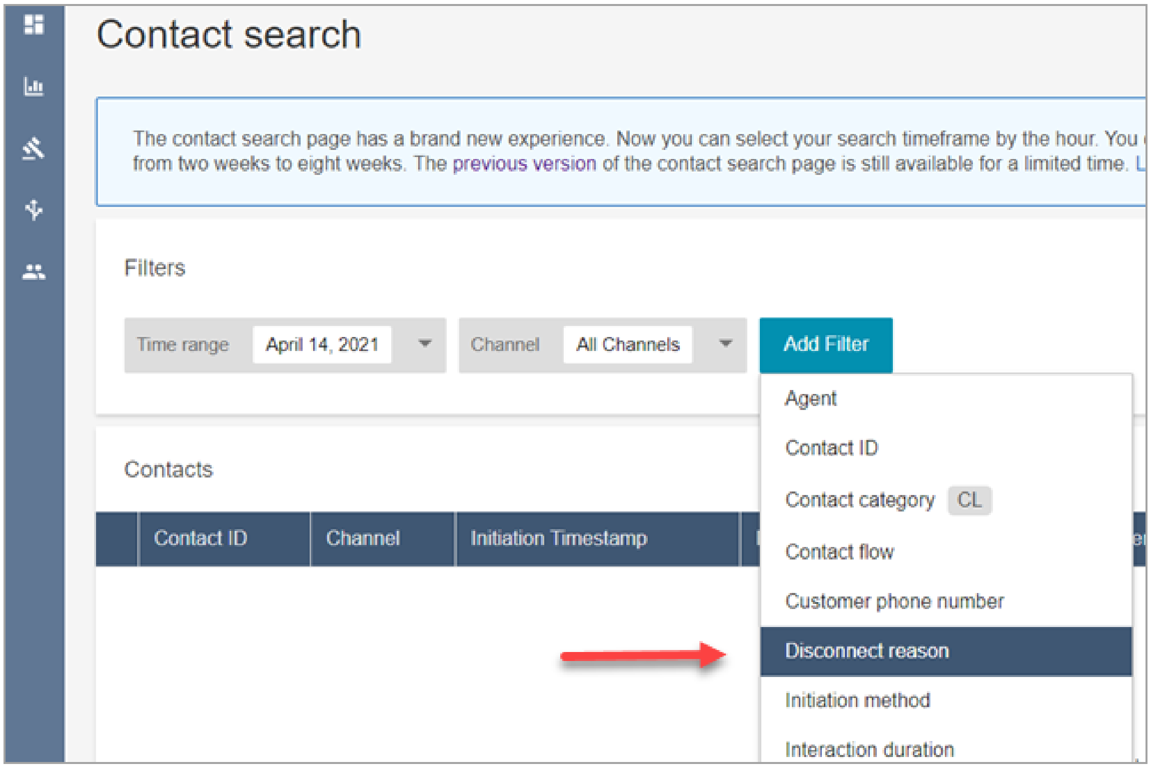
Subscribe to a near real-time stream of contact events (for example, call is queued) in your Amazon Connect contact center. For more information, see Amazon Connect contact events (p. 979).

Contact search

The following changes were release for Contact search:

- Download increase: You are able to download 3,000 rows of search results to a CSV file, instead of 1,000 rows. This increase applies to contacts that occurred after Dec 01, 2020.
- Contact search supports Disconnect Reason as a new filter on the **Contact search** page.

  The following image shows how **Disconnect reason** appears in the user interface as a filter.



Contact search

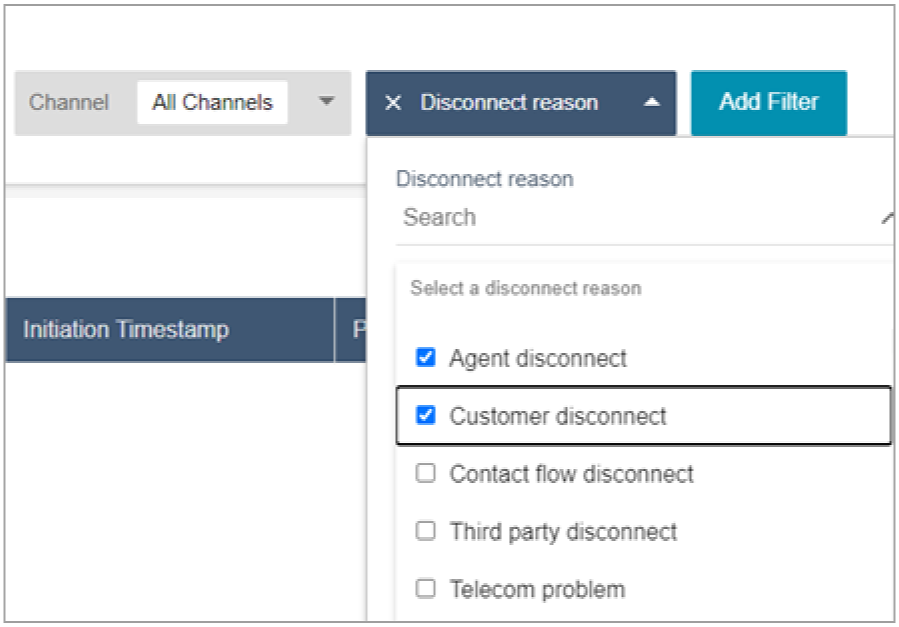
The contact search page has a brand new experience. Now you can select your search timeframe by the hour. You
from two weeks to eight weeks. The previous version of the contact search page is still available for a limited time. L

Filters

Time range: April 14, 2021

Channel: All Channels

  The following image shows how you can filter by type of disconnect reason. For a definition of each disconnect reason, see the ContactTraceRecord (p. 988) section of the *Contact records data model* topic.



Disconnect reason

Search

Select a disconnect reason

☑ Agent disconnect

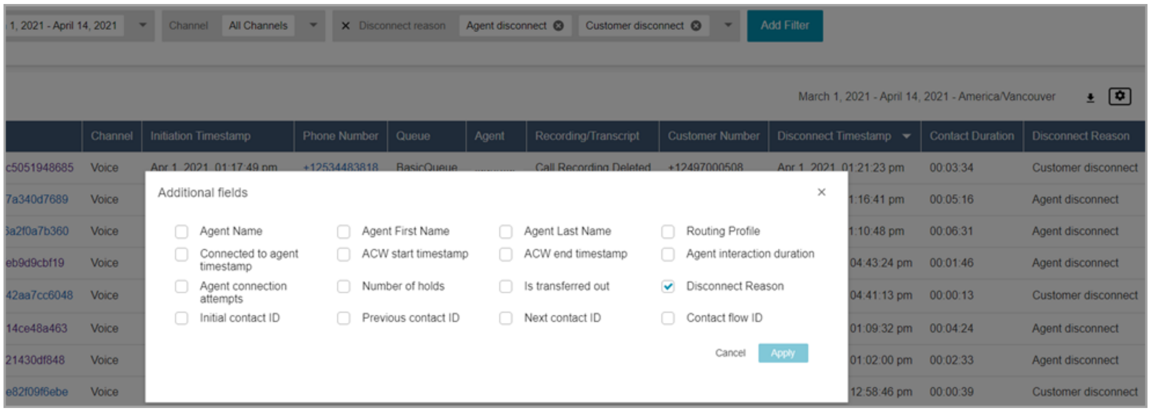
☑ Customer disconnect

☐ Contact flow disconnect

☐ Third party disconnect

☐ Telecom problem

The following image shows how you add **Disconnect reason** as a column to your search results.



	Channel	Initiation Timestamp	Phone Number	Queue	Agent	Recording/Transcript	Customer Number	Disconnect Timestamp	Contact Duration	Disconnect Reason
c5051948685	Voice	Apr 1, 2021, 01:17:49 pm	+12534483818	BasicQueue	--------	Call Recording Deleted	+12497000508	Apr 1, 2021, 01:21:23 pm	00:03:34	Customer disconnect
7a340d7689	Voice							1:16:41 pm	00:05:16	Agent disconnect
3a2f0a7b360	Voice							1:10:48 pm	00:06:31	Agent disconnect
eb9d9cbf19	Voice							04:43:24 pm	00:01:46	Agent disconnect
42aa7cc6048	Voice							04:41:13 pm	00:00:13	Customer disconnect
14ce48a463	Voice							01:09:32 pm	00:04:24	Agent disconnect
21430df848	Voice							01:02:00 pm	00:02:33	Agent disconnect
e82f09f6ebe	Voice							12:58:46 pm	00:00:39	Customer disconnect

Additional fields

☐ Agent Name ☐ Agent First Name ☐ Agent Last Name ☐ Routing Profile

☐ Connected to agent timestamp ☐ ACW start timestamp ☐ ACW end timestamp ☐ Agent interaction duration

☐ Agent connection attempts ☐ Number of holds ☐ Is transferred out ☑ Disconnect Reason

☐ Initial contact ID ☐ Previous contact ID ☐ Next contact ID ☐ Contact flow ID

Cancel Apply

April 2021 Updates

Customer Profiles: Identity resolution

Added identity resolution APIs to Customer Profiles. For more information, see the GetMatches and MergeProfiles APIs in the Amazon Connect Customer Profiles API reference.

Contact Lens: Use category tags to navigate transcript

For more information, see Tap or click category tags to navigate through transcript (p. 832).

Fixes for chat metrics

We released fixes for the following issues identified in chat metrics:

- Amazon Connect incorrectly reported that chat contacts that were created from disconnect flows were created from transfer flows.
- When these fixes, Amazon Connect correctly reflects in the contact records and agent event stream that these chat contacts were created from disconnect flows.

There is no impact to voice or task contacts.

Chat contacts created through disconnect flows no longer increment the following metrics:

- Contact flow time (p. 945)
- Contacts incoming (p. 947)
- Contacts handled incoming (p. 946)
- Contacts transferred in (p. 948)

In addition, note the following fixes for contact records and the agent event stream for chat contacts:

- Contact records: There was an issue in the Attributes section of a chat contact record where the initiation method is **API** for both disconnect and transfer contacts. With this fix, the initiation method correctly reflects **Disconnect** and **Transfer**, respectively.
- Agent event stream: Chat contacts created from disconnect flows now have **Disconnect** as the initiation method.

March 2021 Updates

Amazon Connect is now available in the Canada (Central) Region

Amazon Connect is now available in the Canada (Central) Region. You can claim toll-free and local telephone numbers from Canadian telephony suppliers. For a list of countries were the Canada (Central) Region is supported, see Region requirements for phone numbers. For a list of Contact Lens features available in the Canada (Central) Region, see Availability of Contact Lens features by Region.

Domain for new Amazon Connect instances is "my.connect.aws"

The domain for the Amazon Connect access URL has changed to **my.connect.aws**.

For example:

- Current: https://[*instance name*].**awsapps.com**/connect/
- New: https://[*instance name*].**my.connect.aws/**

How does this change impact logging in to Amazon Connect?

The current access URL continues to work for Amazon Connect instances created before the release of the **my.connect.aws** domain. Any Amazon Connect instances created after the release automatically use the new domain.

Also, if you create new Amazon Connect instances after the release of the new domain, you must add new domains to your allow list. These domains are **in addition** to the ones that are currently required.

Currently required domains added to your allow list:

- {myInstanceName}.awsapps.com/connect/ccp-v2
- {myInstanceName}.awsapps.com/connect/api
- *.cloudfront.net

New additional domains to add to your allow list:

- {myInstanceName}.my.connect.aws/ccp-v2
- {myInstanceName}.my.connect.aws/api
- *.static.connect.aws

For more information, see Set up your network (p. 605).

Schedule for domain change

The change has been rolled out to all Regions.

Chat: Add a chat user interface your website

Added a chat widget that you can customize and secure so it can only be launched from your widget. For more information, see Set up your customer's chat experience (p. 243).

Provided an open source example. For more information, see Download and customize our open source example (p. 253).

Amazon Connect Endpoint Test Utility

To help you validate connectivity to Amazon Connect, or troubleshoot when your agents are experiencing problems with the Contact Control Panel (CCP), we've added the Amazon Connect Endpoint Test Utility. For more information, see Use the Endpoint Test Utility (p. 1193).

February 2021 Updates

Contact Lens: Availability of real-time analytics

Content Lens real-time analytics is available in Europe (London), Europe (Frankfurt), and Asia (Tokyo). For more information, see Availability of Contact Lens features by Region (p. 818).

Ingest data into Customer Profiles using Amazon S3

Added the ability to create and ingest data from Amazon S3. For more information, see Create and ingest customer data into Customer Profiles by using Amazon S3 (p. 730).

Disconnect reason in contact record stream

The Amazon Connect contact records stream now includes **DisconnectReason** for voice calls and tasks. **DisconnectReason** indicates whether an agent or customer disconnected the call, or whether a telecom or network issue caused a call to disconnect. You can also determine whether a task was completed by an agent or an automatic flow, or it expired. For more information, see ContactTraceRecord (p. 988).

Custom service levels

Added the ability to create custom service levels. For details, see New metric groupings and categories (p. 896).

January 2021 Updates

CCP: Change your audio settings

Added the ability to change audio settings from the Contact Control Panel (CCP). This applies to organizations using a customized CCP. For more information, see Change your audio device settings (p. 1141).

Queue APIs (Preview)

Added APIs so you can programmatically create and manage queues. For more information, see Amazon Connect Service API Reference.

Amazon AppIntegrations APIs - GA

Released Amazon AppIntegrations APIs for general availability (GA). For more information, see Amazon AppIntegrations Service API Reference.

December 2020 Updates

Quick Connect APIs (Preview)

Added APIs so you can programmatically create and manage quick connects. For more information, see Amazon Connect Service API Reference.

Chat: Support for attachments

Added support for chat attachments. For more information, see Enable attachments to share files using chat (p. 142).

Added the following APIs:

- CompleteAttachmentUpload
- GetAttachment
- StartAttachmentUpload

Configurable DTMF timeouts for Lex bots

For more information, see Configurable fields for DTMF input (p. 374).

Tasks

Added support for tasks, allowing you to prioritize, assign, track, and even automate tasks across the disparate tools agents use to support customers. For more information, see Tasks (p. 16).

Amazon Connect APIs

Added an Amazon Connect API that provides the ability to create tasks (`StartTaskContact`), and a set of preview APIs.

Preview APIs:

- `CreateIntegrationAssociation`
- `DeleteIntegrationAssociation`
- `ListIntegrationAssociations`
- `CreateUseCase`
- `DeleteUseCase`
- `ListUseCases`

Amazon AppIntegrations APIs (Preview)

Added the Amazon AppIntegrations APIs (Preview), which enables you to configure and reuse connections to external applications. For more information, see Amazon AppIntegrations Service API Reference (Preview).

Customer Profiles

Added Amazon Connect Customer Profiles, enabling agents to create a customer profile for every new contact that comes in. You can also integrate with external applications that provide customer profile data. For more information, see Use Customer Profiles (p. 640) and the Amazon Connect Customer Profiles API Reference.

Real-time analytics using Contact Lens

Added real-time analytics for Contact Lens so you can detect and resolve customer issues more proactively while the call is in progress. For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 811) and the Amazon Connect Contact Lens API Reference.

Amazon Connect Voice ID (Preview)

Added Amazon Connect Voice ID (Preview), which provides for real-time caller authentication. For more information, see Use real-time caller authentication with Voice ID (p. 858).

Amazon Connect Wisdom (Preview)

Added Amazon Connect Wisdom (Preview), which enables agents to search and find content across multiple repositories, such as frequently asked questions (FAQs), wikis, articles, and step-by-step instructions for handling different customer issues. For more information, see Deliver information to agents using Amazon Connect Wisdom (p. 881).

Amazon Connect with Apple Messages for Business (Preview)

Added support for using Amazon Connect with Apple Messages for Business. For more information, see Enable Apple Messages for Business (p. 259).

November 2020 Updates

Contact search

- Made several improvements to contact search. For more information, see What's new in contact search (p. 907).

Telephony call metadata attributes

- Added call attributes to improve fraud detection and routing. For more information, see Telephony call metadata attributes (call attributes) (p. 524).

View historical changes

- The ability to **View historical changes** on the resource configuration pages is now available for the London Region. The following differences appear as the changes are rolled out to other Regions.
  - Total results: The number feature in the **View historical changes** search page, and page numbers, are replaced with **Previous** and **Next** icons.
  - The Username filter requires the entire login name.

Chat

- Added interactive message templates. For more information, see Add interactive messages to chat (p. 633).

APIs

- Added APIs so you can programmatically manage your agent hierarchies and agent groups. For more information, see Amazon Connect Service API Reference.
- Added the following APIs (in an ungated preview release):
  - CreateInstance
  - DescribeInstance
  - ListInstances
  - DeleteInstance
  - UpdateInstanceAttribute
  - UpdateInstanceStorageConfig

Earlier Updates

October 2020 Updates

The following updates were released in October 2020:

Contact flows

- Added chat support for whisper flows. For more information, see Contact block: Set whisper flow (p. 418).

Metrics

- Released the following real-time metrics:
  - Avg callback connecting time (p. 920)
  - Avg incoming connecting time (p. 920)
  - Avg outbound connecting time (p. 921)

  Released the following historical metrics:
  - Agent API connecting time (p. 939)
  - Agent callback connecting time (p. 940)
  - Agent incoming connecting time (p. 940)
  - Agent outbound connecting time (p. 941)
  - Average agent API connecting time (p. 942)
  - Average agent callback connecting time (p. 942)
  - Average agent incoming connecting time (p. 942)
  - Average agent outbound connecting time (p. 943)
- In real-time metrics reports, added one-click drill-downs. These allow you to drill down into queue and routing profile data in one click. For more information, see Use one-click drill-downs for Routing profiles and Queues tables (p. 927).
- Added the **Restrict contact access** permission which enables you to manage a user's access to results on the **Contact search** page based on their agent hierarchy group. For more information, see Search for contacts (p. 907).
- Added **ContactDetails** and **References** to the contact record. For more information, see Contact records data model (p. 985).

September 2020 Updates

The following updates were released in September 2020:

Service quotas

- Updated the service quotas for the following Amazon Connect Participant Service APIs:
  - CreateParticipantConnection (p. 1217)
  - DisconnectParticipant (p. 1217)
  - GetTranscript (p. 1217)

Contact flows

- Added the Amazon Connect Flow language, a JSON-based representation of a series of flow actions, and the criteria for moving between them. For more information, see Amazon Connect Flow language (p. 543).

APIs

Added the following APIs for contact flows:

- CreateContactFlow
- DescribeContactFlow
- UpdateContactFlowContent
- UpdateContactFlowName

Added the following API to list prompts:

- ListPrompts

Added the following APIs for routing profiles:

- AssociateRoutingProfileQueues
- CreateRoutingProfile
- DeleteRoutingProfile
- DescribeRoutingProfile
- DisassociateRoutingProfileQueues
- ListRoutingProfileQueues
- UpdateRoutingProfileConcurrency
- UpdateRoutingProfileName
- UpdateRoutingProfileQueues

August 2020 Updates

The following updates were released in August 2020:

Contact flows

- Added the ability to automatically use the best sounding voice available from Amazon Polly for text-to-speech. For more information, see Amazon Polly best sounding voice (p. 457).
- Added the ability to select, cut, copy, and paste contact flows. For more information, see Copy and paste contact flows (p. 452).

Telephony

- Added the ability for all customers to enable/disable media support for outbound phone calls. For more information, see Step 3: Set telephony (p. 137) in the Create an Amazon Connect instance (p. 135) topic.

Monitoring

- Added logging of Amazon Connect Participant Service calls with AWS CloudTrail. For more information, see Logging Amazon Connect API calls with AWS CloudTrail (p. 1025).

Contact Lens for Amazon Connect

- Updated the security profile permissions for the redaction feature. For more information, see Security profile permissions for Contact Lens (p. 818).

July 2020 Updates

The following updates were released in July 2020:

Contact flows

- The **Set voice** block supports speaking styles with neural text-to-speech (TTS) voices. For more information, see Contact block: Set voice (p. 415).

APIs

- Added StartContactRecording, StopContactRecording, SuspendContactRecording, ResumeContactRecording to the Amazon Connect Service API.

Contact Lens for Amazon Connect

- Updated Contact Lens for Amazon Connect for general availability. This feature lets you analyze customer-agent conversations, by using speech transcription, natural language processing, and intelligent search capabilities. For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 811).

Metrics

- Fixed content that was added in June 2020 that said **Agent idle time**, **Agent on contact time**, and **Occupancy** had been deprecated. That was incorrect. Rather, they are no longer available for queue groupings only. For more information, see What's new in metrics (p. 892).
- Corrected how **Occupancy** is calculated. The correct calculation is:

  (Agent on contact (wall clock time) / (Agent on contact (wall clock time) + Agent idle time))

June 2020 Updates

The following updates were released in June 2020:

Metrics

- The following historical metrics no longer appear in queue groupings:
  - Agent idle time
  - Agent on contact time
  - Occupancy
- Added upcoming metric changes: new real-time and historical metrics for inbound and outbound contact time. For more information, see What's new in metrics (p. 892).

Contact Control Panel (CCP)

- Released the following improvements:
  - DTMF input is passed to all lines in a three-way call. Any party can enter DTMF input.
  - Resolved an issue where the DTMF tone degraded when agents interacted with Quick connect and/ or Number pad during a session.
  - Resolved an issue where quick connects sometimes did not appear on a page, even after an agent refreshed it.
  - Improved the experience when a manager "listens in" to multiple chat conversations. Updated the unread message count on the CCP to include messages sent by the customer and those sent by the agent. Previously, the unread message count only included messages sent by the customer.
- Published instructions for upgrading to the latest CCP. For more information, see Upgrade to the latest CCP (p. 277).
- Published a training video that explains how to use the CCP. For more information, see Training video: How to use the CCP (p. 1137).

Contact flows

- The **Set disconnect flow** block supports voice conversations. For more information, see Contact block: Set disconnect flow (p. 403).
- The **Set Voice** block supports Amazon Polly Neural Text-to-Speech (NTTS) voices. For more information, see Contact block: Set voice (p. 415).
- The **Get queue metrics** block can return metrics by channel, for example, by voice or chat. For more information, see Contact block: Get queue metrics (p. 378).

May 2020 Update

The following updates were released in May 2020:

Contact flows

- Added the ability to select multiple blocks at the same time and rearrange them as a group within a contact flow. For more information, see Create an inbound contact flow (p. 447).

April 2020 Update

The following updates were released in April 2020:

Telephony

- Added early media support for outbound phone calls. Enabled by default, an agent hears tones and audio messages played by phone companies—such as busy signals, failure to connect errors, or other informational messages—through their headset or audio device. For more information, see Step 3: Set telephony (p. 137) in the Create an Amazon Connect instance (p. 135) topic.
- Added the `barge-in-enabled` session attribute to the Get customer input (p. 366) block so customers can interrupt Amazon Lex bots with their voice.

March 2020 Update

The following updates were released in March 2020:

Contact flows

- Updated the Store customer input (p. 426) block to allow you to specify a custom terminating keypress.

Metrics

- Announced June 2020: Changes for omnichannel support (p. 901).

Networking

- Updated softphone requirements in Set up your network (p. 605).

February 2020 Update

The following updates were released in February 2020:

Service Quotas

- Adjusted Amazon Connect service quotas (p. 1205) for new accounts.

Contact Flows

Updated the following blocks so you can set contact attributes:

- Set customer queue flow (p. 402)
- Set hold flow (p. 405)
- Set whisper flow (p. 418)

January 2020 Update

The following updates were released in January 2020:

Contact Control Panel (CCP)

The following updates were made to the updated Contact Control Panel (ccp-v2):

- Agents can now transfer a contact by double-clicking a quick connect. For more information, see Transfer calls to a quick connect or external number (p. 1161).
- The number pad now retains the previously selected country flag so agents don't need to select it every time.
- All strings in the CCP user interface are now localized in available languages.
- Resolved an issue where the color of the call status bar incorrectly displayed as green during a conference call when the call was in the Joined state. It is now blue.

- Resolved an issue where the agent's name was displayed in error messages for missed chats, rather than the customer's name.

Networking

- Updated Set up your network (p. 605) to include requirements for the updated Contact Control Panel (ccp-v2).

December 2019 Update

The following update was released in December 2019:

Monitoring

- Added Contact Lens for Amazon Connect for preview. This feature enables you search conversations for keywords, sentiment scores, and non-talk time. For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 811).
- Added logging of Amazon Connect API calls with AWS CloudTrail. For more information, see Logging Amazon Connect API calls with AWS CloudTrail (p. 1025).

November 2019 Update

The following updates were released in November 2019:

Omnichannel Support

- Added support for chat communications. For more information, see Concepts (p. 10).

Metrics

- For a description of changes, see What's new in metrics (p. 892).

Contact Flows

Added the following contact flow blocks:

- the section called "Wait"
- the section called "Set disconnect flow"

Updated the following contact flow blocks for chat:

- the section called "Play prompt"
- the section called "Get customer input"
- the section called "Store customer input"
- the section called "Set recording and analytics behavior"

User Management

- Added that you can use AWS Identity and Access Management (IAM) with Amazon Connect. For more information, see Identity and access management for Amazon Connect (p. 1078).

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. 775).

API

- Added StartChatContact, ListTagsForResource, TagResource, UntagResource to the Amazon Connect Service API.
- Added the Amazon Connect Participant Service API. These APIs are used chat participants, such as agents and customers.

Contact Control Panel (CCP)

- Updated the CCP so it supports chat. For more information, see Agent training guide (p. 1135).

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. 965).

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. 932)

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

- 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 record for callback contacts.
- Resolved an issue where **InitiationTimestamp** for callback contacts did not match the time that the callback was created.
- Resolved an issue where users were given an incorrect message when they did not have permissions to edit a report.

Contact Control Panel (CCP)

- Resolved an issue where callbacks were not ringing in the CCP.

January 2019 Updates

The following updates were released in January 2019:

Updates by category

Contact Routing

- 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

- Resolved an issue where agent event streams were missing agent snapshots during login and logout events.
- Resolved an issue where the contact record detail page displayed timestamps using the timezone selected on the search page.
- Resolved an issue where the AfterContactWork status was overridden.
- Resolved an issue where the timestamps are incorrect if an agent accidentally disconnects while placing a customer on hold.

Contact Control Panel (CCP)

- Resolved an intermittent issue with initialization when an agent configuration is corrupted or null.
- Resolved an issue where pressing Enter to transfer a call did not work.

November 2018 Updates

The following updates were released in November 2018:

Updates by category

General

- 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

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

Metrics and Reporting

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

API

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

September 2018 Updates

The following updates were released in September 2018:

Updates by category

- General (p. 1252)
- API (p. 1252)

General

- Improved page loading times for the **User management** page.
- Resolved an issue that sometimes caused issues loading the **Queues** page when there were a large number of quick connects associated with a queue.

API

- Released the UpdateContactAttributes operation for the Amazon Connect API.

August 2018 Updates

The following updates were released in August 2018:

Updates by category

- General (p. 1252)
- Contact Routing (p. 1252)
- Metrics and Reporting (p. 1253)

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

- Caller ID number: Set in the queue or Call phone number block (p. 213)
- Add an Amazon Lex bot (p. 617)
- User Management APIs
- Manage contacts in a queue (p. 476)

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

- 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 Caller ID number: Set in the queue or Call phone number block (p. 213).
- Released contact attributes for system metrics, including a new **Get metrics** block in contact flows. For more information, see Route based on number of contacts in a queue (p. 533).

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

- 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 in to reports. Previously, in some cases, report data for the final 15 minute period during the scheduled report interval did not get included in scheduled reports. This applies to all report types.
- In metric calculations, the time that an incoming call rings is attributed to idle time if the agent is in idle state before an incoming call.
- The metric **Agent on contact time** now includes time that an agent spent in an auxiliary busy state.
- Published new documentation about metrics.

Contact Control Panel (CCP)

- Added a **Save** button to the settings menu for the CCP when an agent is using a desk phone. The **Save** button saves the deskphone configuration between sessions.

- Agent username is now available as part of agent configuration data in the Amazon Connect Streams API.
- Contact attributes are now available when using the streams.js (Streams API) for screenpops after queued callbacks.
- Fixed issue where for some auto-accept calls, the agent continued to hear ringing after accepting and joining the call.

Get administrative support for Amazon Connect

If you are an administrator and need to contact support for Amazon Connect, choose one of the following options:

- If you have an AWS Support account, go to Support Center and submit a ticket.
- Otherwise, open the AWS Management Console and choose **Amazon Connect**, **Support**, **Create case**.

It's helpful to provide the following information:

- Your contact center instance ID/ARN. To find your instance ARN, see Find your Amazon Connect instance ID/ARN (p. 139).
- Your region.
- A detailed description of the issue.

Amazon Connect Document history

The following table describes important changes in each release of the Amazon Connect Admininstrator Guide. For notification about updates to this documentation, you can subscribe to an RSS feed.

update-history-change	update-history-description	update-history-date
Attachments per chat conversation now at 35 (p. 1258)	Updated the limit for attachments per chat conversations from 5 to 35. See Feature specifications.	July 20, 2022
Added Voice ID Flow language actions (p. 1258)	Added topics for the following Voice ID Flow language actions: CheckOutboundCallStatus, CheckVoiceId, and StartVoiceIdStream.	July 19, 2022
Search for contacts by using the agent's first or last name (p. 1258)	You can search for contacts using the agent's first or last name. The filter name is **Agent**. To view an image of this experience, see Search for contacts by using the agent's first or last name.	July 15, 2022
Released updates for rich text format rendering (p. 1258)	On the **Contact Search** and **Contact Detail** pages, you can now view chat transcripts that have rich text formatting, such as bold or italic font, bullet points, numbered lists, and hyperlinks. For more information about getting started with Amazon Connect Chat, see Set up your customer's chat experience.	July 13, 2022
View call transcript in CCP or agent application (p. 1258)	For more information, see View a call transcript during ACW.	July 7, 2022
Added feature specifications for Contact Lens (p. 1258)	For more information, see Contact Lens for Amazon Connect feature specifications.	July 1, 2022
Support for Lex intent confidence scores and sentiment analysis (p. 1258)	You can further personalize the automated self-service customer experience using Amazon Lex intent confidence scores and sentiment analysis as a branch within your flows. For more information, see the Get customer input block. For a list of new contact attributes see Amazon Lex contact attributes.	June 29, 2022

GA for High-volume outbound communications (p. 1258)	Released Amazon Connect High-volume outbound communications for General Availability. This release includes a set of APIs for creating and managing high-volume outbound campaigns. For more information, see Enable high-volume outbound communications and Amazon Connect High-Volume Outbound Communications API Reference.	June 20, 2022
Amazon Connect Cases (Preview) (p. 1258)	Amazon Connect Cases (Preview) allows your agents to quickly track and manage customer issues that require multiple interactions, follow-up tasks, and teams in your contact center. For more information, see Amazon Connect Cases (Preview) and Amazon Connect Cases API Reference (Preview).	June 20, 2022
Updated Amazon Lex bot per instance quota (p. 1258)	Updated the Amazon Lex bot per instance quota from 50 to 70. For more information, see Amazon Connect service quotas.	June 7, 2022
New GetCurrentUserData API (p. 1258)	Released the GetCurrentUserData API. It enables you to return the real-time active user data from the specified Amazon Connect instance.	June 6, 2022
Released task templates (p. 1258)	You can now create custom task templates, making it easy for agents to consistently capture the relevant and required information to create or complete tasks. For more information, see Create task templates. For information about using the API to programmatically create and manage task templates, see the Amazon Connect API Reference and the Amazon Connect Resource Type Reference in the *AWS CloudFormation User Guide*.	June 2, 2022

New API to transfer contacts (p. 1258)	Added a new API that you can use to transfer contacts from one agent or queue to another agent or queue at any point after a contact is created. For information, see TransferContact in the *Amazon Connect API Reference*.	June 2, 2022
Updated workflow for high-volume outbound communications (p. 1258)	Updated the workflow for onboarding to high-volume outbound communications using the Amazon Connect and Amazon Pinpoint user interface. For more information, see Enable high-volume outbound communications.	May 27, 2022
Voice ID expires speakers (p. 1258)	For BIPA Compliance, Amazon Connect Voice ID automatically expires speakers that have not been accessed for enrollment, re-enrollment, or successful authentication for three years. You can see a speaker's last access time by looking at the `lastAccessedAt` attribute returned by the DescribeSpeaker and ListSpeakers APIs, and the What data is stored? section of the Amazon Connect Admin Guide.	May 25, 2022
Search Voice ID results (p. 1258)	Added topic Search and review Voice ID results.	April 28, 2022
New API to change agent's current status (p. 1258)	Amazon Connect provides an API to programmatically change the current status of an agent. Agent statuses are used to determine when an agent is **Available** to be routed contacts in Amazon Connect, versus when they are set to **Offline** or a custom status such as **Lunch** or **Break** and should not be routed contacts. For more information, see PutUserStatus in the Amazon Connect API Reference.	April 28, 2022

New APIs (p. 1258)	Added API to search for user records by first name, last name, username, routing profile, security profile, agent hierarchies or tags. Added API to claim new phone numbers and configure them programmatically. For more information, see the Amazon Connect API Reference.	April 25, 2022
Multi-party calls (p. 1258)	You can enable Amazon Connect to allow up to six parties on a call: the agent, the caller, and four more participants. For more information, including a comparison of how multi-party calling differs from the default three-party calling, see Telephony: Multi-party calls.	April 6, 2022
Play prompts from an Amazon S3 bucket (p. 1258)	Added the ability to source prompts from an Amazon S3 bucket. This enables you to store as many voice prompts as needed in Amazon S3 and access them in real time using contact attributes in the following contact blocks that play prompts: Get customer input, Loop prompts, Play prompt, and Store customer input.	April 5, 2022
Real-time contact analysis segment streams (p. 1258)	Added support for accessing Contact Lens analytics in near real-time. For more information, see Use streaming for real-time contact analysis.	March 28, 2022
Rich messaging for chat (p. 1258)	Added support for rich messaging for your customer's chat experience. Agents and customers can use bold, italic, bulleted lists, numbered list, hyperlinks, and attachments. For more For more information, see Enable text formatting for your customer's chat experience.	March 13, 2022
Object type mapping user interface (p. 1258)	Added a user interface for creating object type mapping by using the Amazon Connect admin console. For more information, see Create an object type mapping.	March 8, 2022

Updates to `AmazonConnectServiceLinkedRolePolicy` (p. 1258)	Added actions for Amazon CloudWatch metrics. For more information, see Amazon Connect updates to AWS managed policies.	February 22, 2022
Added bulk ingestion of data for Customer Profiles (p. 1258)	For more information, see *Bulk ingestion of data* in the Set up integration for Salesforce, ServiceNow, Marketo, or Zendesk topic.	February 21, 2022
New quotas for APIs (p. 1258)	For StartChatContact , StartContactStreaming , StopContactStreaming , a RateLimit of 5 requests per second, and a BurstLimit of 8 requests per second.	February 11, 2022
New CloudWatch metrics for chat (p. 1258)	Added the following Amazon CloudWatch metrics for chat: **ConcurrentActiveChats**, **ConcurrentActiveChatsPercentage**, **ChatBreachingActiveChatQuota**, and **SuccessfulChatsPerInterval**. For more information, see Monitoring your instance using CloudWatch.	February 11, 2022
Documented Rules feature specifications (p. 1258)	Documented the feature specifications for Amazon Connect Rules. For more information, see Amazon Connect Rules feature specifications.	January 28, 2022
Documented Identity Resolution quotas (p. 1258)	Documented three quotas for Identity Resolution. For more information, see Customer Profiles quotas.	January 28, 2022
Configure maximum chat duration (p. 1258)	You can configure the total duration per chat to be up to 7 days, including wait time. For more information, see the `ChatDurationInMinutes` parameter in the StartChatContact API.	January 27, 2022
Contact Lens supports custom vocabularies (p. 1258)	For more information, see Add custom vocabularies.	January 25, 2022
Released tagging support for UserHierarchyGroup resource (p. 1258)	For more information, see CreateUserHierarchyGroup.	January 20, 2022
Chat widget supports browser notifications (p. 1258)	For more information, see Browser notifications.	December 21, 2021

Integrate Customer Profiles with Segment and Shopify (p. 1258)	For more information, see Set up integration for Segment and Set up integration for Shopify.	December 20, 2021
Updated compliance for tasks (p. 1258)	Tasks is in compliance with GDPR, and is approved for SOC, PIC, HITRUST, ISO, and HIPAA.	December 17, 2021
Released unified agent application (p. 1258)	Amazon Connect released the unified agent application to improve the agent experience and customer interactions. For more information, see Agent training guide.	November 30, 2021
Released call summarization (p. 1258)	Contact Lens for Amazon Connect provides the option for you to view a transcript summary. The summary shows only those lines where Contact Lens has identified an issue, outcome, or action item in the transcript. For more information, see View call summary.	November 30, 2021
Documented Average API Connecting Time (p. 1258)	Documented the real-time metric **Average API Connecting Time**. For more information, see Average API Connecting Time.	November 26, 2021
Released Identity Resolution to consolidate similar profiles (p. 1258)	Amazon Connect Customer Profiles offers Identity Resolution, a feature that is designed to automatically detect similar customer profiles by comparing name, email address, phone number, date of birth, and address. For more information, see Use Identity Resolution to consolidate similar profiles and the Amazon Connect Customer Profiles API Reference.	November 24, 2021
Updated Customer Profiles service quotas (p. 1258)	Amazon Connect Customer Profiles now supports 1000 objects per profile (increased from 100), and 50MB Maximum size of all objects for a profile (increased from 5MB). For more information, see Amazon Connect Customer Profiles service quotas.	November 23, 2021

Amazon Connect Customer Profiles stores contact history at no charge (p. 1258)	Amazon Connect Customer Profiles now provides contact history and customer information together in unified customer profiles at no charge, helping contact center managers personalize the contact center experience. In new instances, Customer Profiles is enabled by default. For more information, see Step 4: Data Storage in the *Create an Amazon Connect instance* topic.	November 23, 2021
New APIs to archive/unarchive and delete contact flows (p. 1258)	Added new APIs that provide a programmatic and flexible way to manage your library of contact flows at scale. For example, contact flows used only during certain times of the year can be archived when not in use and then unarchived when needed. You can now also delete a contact flow so it is no longer available for use. For more information, see the Amazon Connect API Reference.	November 22, 2021
Added modular flows to help you create common functions (p. 1258)	Contact flow modules are reusable sections of a contact flow. You can create them to extract repeatable logic across your flows, and create common functions. For more information, see Contact flow modules for reusable functions.	November 22, 2021
Search contacts by custom contact attributes (p. 1258)	Added support for searching contacts by custom contact attributes (also called user-defined attributes). For more information, see Search by custom contact attributes.	November 15, 2021
Added **Customer profiles** block (p. 1258)	Added the Customer profiles block. It enables you to retrieve, create, and update a customer profile.	November 15, 2021
Updated `AmazonConnect_FullAccess` (p. 1258)	Added permissions for managing Amazon Connect Customer Profiles. See Amazon Connect updates to AWS managed policies.	November 12, 2021

Released security profiles APIs (p. 1258)	Added APIs so you can create and manage security profiles programmatically. For more information, see the Amazon Connect API Reference.	November 12, 2021
Released scheduled tasks (p. 1258)	Added the ability to schedule tasks up to six days in the future to follow-up on customer issues when promised. You can also update the scheduled date and time using the UpdateContactSchedule API. For more information, see the Create task block and the Create a task topic in the *Agent training guide*.	November 12, 2021
Released Contact APIs (p. 1258)	Added APIs so you can get and update contact details programmatically. For example, you can describe contact details such as queue information, chat attachments, task references, and update contact information such as task name. For more information, see DescribeContact, UpdateContact, and ListReferences in the *Amazon Connect API Reference*.	November 12, 2021
Changes to real-time metrics agent tables (p. 1258)	We are rolling out a new service to maintain the high availability from metrics that you expect from Amazon Connect. Due to this change, the agent tables will now be sorted by availability status by default, rather than by agent login. Additionally, the queues and routing profiles table will sort by agents online by default instead of queue or routing profile name.	November 12, 2021
Added actions to `AmazonConnectServiceLinkedRolePolicy` (p. 1258)	Added actions for Amazon Connect Customer Profiles. See Amazon Connect updates to AWS managed policies.	November 12, 2021
Added new metrics (p. 1258)	Added following new historical metrics: **Contacts transferred in by agent** and **Contacts transferred out by agent**. Added new real-time metrics: **Transferred in by agent** and **Transferred out by agent**. See Historical metrics definitions and Real-time metrics definitions.	November 9, 2021

Released real-time chat message streaming (p. 1258)	You can subscribe to a real-time stream of chat messages. For more information, see Enable real-time chat message streaming.	October 29, 2021
Cross-service confused deputy prevention for Customer Profiles (p. 1258)	Updated Cross-service confused deputy prevention with more sample policies you can apply for Amazon Connect Customer Profiles.	October 26, 2021
GA for HoursOfOperation APIs (p. 1258)	Released the Amazon Connect `HoursOfOperation` APIs for general availability (GA). Also launched AWS CloudFormation support for Users, User Hierarchies, and Hours of Operation. For more information, see the Amazon Connect API Reference and the AWS CloudFormation User Guide.	October 22, 2021
Example: Programmatically integrate S3 with Customer Profiles (p. 1258)	Added a topic that shows how to programmatically integrate S3 with Customer Profiles.	October 21, 2021
Cross-service confused deputy prevention (p. 1258)	Added a topic with example policies you can apply for Cross-service confused deputy prevention.	October 18, 2021
How long unanswered callbacks stay in queue (p. 1258)	In the Set up queued callback topic, clarified that unanswered queued callbacks stay in queue at least 7 days and up to 14 days before Amazon Connect automatically removes them.	October 13, 2021
Updated endpoint for client-side metrics (p. 1258)	In the Set up your network topic, changed the endpoint for client-side metrics from `*.execute-api.{region}.amazonaws.com` to `*.telemetry.connect.{region}.amazonaws.com`.	October 11, 2021

Corrected errors in Service quota topic (p. 1258)	Corrected errors in the Service quotas topic: For Amazon Connect Wisdom, **Maximum size per document** is 1MB not 10MB. For Amazon Connect Customer Profiles, the name of the quota is **Object Types per domain** not Objects per domain. Updated the Amazon Connect Voice ID quotas table with correct information.	October 8, 2021
Preview release of high-volume outbound communications (p. 1258)	Added content for the preview release of high-volume outbound communications. By using Amazon Pinpoint Journeys and Amazon Connect, you can now create high-volume outbound campaigns for voice, SMS, and email. For more information, see Enable high-volume outbound communications.	September 27, 2021
New Amazon AppIntegrations Service APIs (p. 1258)	New DataIntegration APIs for the Amazon AppIntegrations Service: `CreateDataIntegration`, `DeleteDataIntegration`, `GetDataIntegration`, `ListDataIntegrationAssociations`, `ListDataIntegrations`, `UpdateDataIntegration`. For more information, see Amazon AppIntegrations Service API Reference.	September 27, 2021
Amazon Connect Wisdom - General Availability (p. 1258)	For more information, see Deliver information to agents using Amazon Connect Wisdom and the Amazon Connect Wisdom API Reference.	September 27, 2021
Amazon Connect Voice ID - General Availability (p. 1258)	For more information, see Use real-time caller authentication with Voice ID and the Amazon Connect Voice ID API Reference.	September 27, 2021

Added new service-linked role policy (p. 1258)	Added `AmazonConnectVoiceIDFullAccess`. Use this AWS managed policy so you can set up your users to use Voice ID. This policy provides full access to Amazon Connect Voice ID through the AWS console, SDK, or other means. For more information, see AWS managed policy: AmazonConnectVoiceIDFullAccess.	September 27, 2021
Added new service-linked role policy (p. 1258)	Added `AmazonConnectCampaignsServiceLinkedRolePolicy`, a new service-linked role policy for high-volume outbound communications. The policy provides access to retrieve all the high-volume outbound campaigns. For more information, see Enable high-volume outbound communications.	September 27, 2021
Display name and contact attributes in chat (p. 1258)	You can now personalize the chat experience, as you can specify the name of your customer that interacts using the chat user interface. You can also securely pass the contact attributes to capture information about the contact which can be used in the contact flow to further personalize the experience. For more information, see Pass the customer display name when a chat initializes and Pass contact attributes when a chat initializes.	September 17, 2021
Preview of agent application (p. 1258)	Launched an updated UI for the agent application preview that combines Customer Profiles and the Contact Control Panel (CCP). For more information, see Access Customer Profiles in the agent application.	September 16, 2021
Added Create task block (p. 1258)	Added the **Create task** block. It creates a new task, sets the tasks attributes, and initiates a contact flow to start the task. For more information, see Contact block: Create task.	September 16, 2021

More languages for Contact Lens (p. 1258)	Contact Lens now supports the following languages for post-call and real-time analytics: Japanese, Korean, and Mandarin. The following languages are supported for real-time analytics: French (Canada), French (France), Portuguese (Brazil), German (Germany), and Italian (Italy). For more information, see Contact Lens for Amazon Connect in the *Languages supported by Amazon Connect* topic.	September 13, 2021
Updated historical metrics definitions (p. 1258)	Updated the definitions of **Contacts transferred in** and **Contacts transferred out**. For more information, see Historical metrics definitions.	September 10, 2021
Improved user interface for Amazon Connect console (p. 1258)	Released a redesigned user interface for the Amazon Connect console, making it easier and faster to manage Amazon Connect instances. For more information, see Create an Amazon Connect instance.	August 27, 2021
Customer Profiles is HIPAA compliant (p. 1258)	Customer Profiles is now HIPAA compliant. Removed note stating it is not.	August 23, 2021
Porting numbers in Singapore (p. 1258)	Updated documentation requirements. For more information, see Singapore in the *Region requirements for ordering and porting phone numbers* topic.	August 10, 2021
APIs for hours of operation and agent status (p. 1258)	Released for ungated preview new APIs for managing hours of operation and agent status. For more information, see Amazon Connect Service API Reference.	August 6, 2021
Contant Lens rules create tasks and EventBridge events (p. 1258)	Contact Lens rules now allow you to generate tasks and EventBridge events based on uttered keywords, sentiment scores, customer attributes, and other criteria. For more information, see Build rule with Contact Lens.	August 5, 2021

Countries you can call by default (p. 1258)	We have updated the list of countries you can call by default when you create a new instance in a given Region. For more information, see Countries you can call.	August 4, 2021
Add AWS Global Accelerator to your allowlist (p. 1258)	When using SAML Sign-In to your Amazon Connect instance, you now need to add the AWS Global Accelerator domain, ***. awsglobalaccelerator.com**, to your allow list. For more information, see Set up your network.	August 3, 2021
New "Next status" feature (p. 1258)	To help agents manage their time, we have released a feature that lets agents pause new contacts being routed to them while they finish their current contacts. For more information, see "Next status" feature for the CCP.	July 30, 2021
Update to Contact search functionality (p. 1258)	To use the **Agent** filter on the **Contact search** page, in your Amazon Connect security profile you must have **Users - View** permissions. For more information, see Contact search: To search contacts by Agent login requires Users - View permissions in your security profile.	July 23, 2021
Added two task metrics sent to CloudWatch (p. 1258)	Amazon Connect sends the following two new metrics to CloudWatch: ConcurrentTasks and ConcurrentTasksPercentage. For more information, see Monitoring your instance using CloudWatch.	July 7, 2021
Updated required permissions for custom IAM policies (p. 1258)	Added permissions for Amazon Lex. For more information, see Amazon Connect updates to AWS managed policies.	June 29, 2021
Apple Messages for Business GA (p. 1258)	Released Apple Messages for Business for general availability (GA). For more information, see Enable Apple Messages for Business.	June 28, 2021

Quick connects management API GA (p. 1258)	Released Amazon Connect quick connects management API for general availability (GA). For more information, see Amazon Connect Service API Reference. The quick connects API also supports AWS CloudFormation. For more information, see Amazon Connect Resource Type Reference in the AWS CloudFormation User Guide.	June 24, 2021
Added service quota for Amazon Lex V2 bot aliases per instance = 100 (p. 1258)	For more information about service quotas, see Amazon Connect service quotas.	June 17, 2021
Support for Amazon Lex V2 console and APIs (p. 1258)	For information on using the Amazon Lex V2 console, see Add an Amazon Lex bot. Added these three APIs: AssociateLexBot, DisassociateLexBot, and ListLexBots. See the Amazon Connect Service API Reference.	June 15, 2021
Coming soon: Faster load times for Real-time metrics page (p. 1258)	Rollout to all Regions July 19, 2021, to September 19, 2021, subject to change. For more information, see Upcoming change: Faster reload times for the Real-time metrics page.	June 11, 2021
Coming soon: New DataIntegration APIs (p. 1258)	On May 20, 2021, we published that new DataIntegration APIs were added to the Amazon AppIntegrations service. These APIs are not yet available.	June 8, 2021
Chat agent concurrency increased (p. 1258)	Increased chat agent concurrency from 5 to 10. For more information, see Create a routing profile.	June 7, 2021
Object type mapping for Customer Profiles (p. 1258)	Added object type mapping for the Customer Profiles standard profile. For more information, see the Object type mapping for the standard profile.	June 1, 2021
Channels supported by blocks (p. 1258)	Added a topic that lists all the blocks and which channels each one supports. For more information, see the Channels each block supports.	May 18, 2021
Added contact events (p. 1258)	For more information, see the Amazon Connect contact events.	May 12, 2021

Announced upcoming change to Agent audit report (p. 1258)	In a future release, you'll be able to download the Agent audit report. For more information, see the Upcoming changes: Download the Agent audit report.	May 4, 2021
Added identity resolution APIs (preview) to Customer Profiles. (p. 1258)	For more information, see the GetMatches and MergeProfiles APIs in the Amazon Connect Customer Profiles API reference.	April 30, 2021
Added topic on how to apply permissions that restrict which AWS resources can be associated with Amazon Connect. (p. 1258)	For more information, see Restrict AWS resources that can be associated with Amazon Connect.	April 28, 2021
Added chapter on architectural guidance, authored by AWS Solution Architects (p. 1258)	For more information, see Architectural guidance for Amazon Connect.	April 28, 2021
Announced upcoming fix to agent event stream (p. 1258)	For more information, see Upcoming change: Fix for agent event stream.	April 27, 2021
Revised the topics on porting phone numbers (p. 1258)	For more information, see Port your phone number.	April 24, 2021
Using Customer Profiles with CCP out-of-the-box is in ungated preview (p. 1258)	For more information, see Access the Customer Profiles Agent UI.	April 22, 2021
Announced upcoming changes for Contact search (p. 1258)	For more information, see Upcoming changes: Contact search.	April 20, 2021
Added NLB endpoint for Canada (Central) Region (p. 1258)	Updated Set up your network with the NLB endpoint for Canada (Central) Region.	April 15, 2021
Amazon Connect is now available in the Canada (Central) Region (p. 1258)	You can claim toll-free and local telephone numbers from Canadian telephony suppliers. For a list of countries that support the Canada (Central) Region, see Region requirements for phone numbers. Also see Availability of Contact Lens features by Region.	March 31, 2021

Announced upcoming fixes for chat metrics (p. 1258)	Currently Amazon Connect incorrectly reports that chat contacts that were created from disconnect flows were created from transfer flows. When the fixes are released, Amazon Connect will correctly reflect in the contact records and agent event stream that these chat contacts were created from disconnect flows. For more information, see Upcoming change: Fixes for chat metrics in the Release notes.	March 25, 2021
Completed release of new domain name (p. 1258)	The domain for the Amazon Connect access URL has changed to **my.connect.aws**. For more information, see March 2021 Updates in the Release notes.	March 22, 2021
Default service quota for reports per instance (p. 1258)	Updated the default service quota for reports per instance to 2000. This default applies to accounts created in October, 2020 or later. For more information, see Amazon Connect service quotas.	March 16, 2021
Identification requirements for ordering and porting phone numbers (p. 1258)	Added identification requirements for ordering phone numbers. Added requirements for ordering and porting phone numbers from Argentina, Chile, Mexico, Peru, and Puerto Rico. For more information, see Region requirements for phone numbers.	March 11, 2021
Use the Amazon Connect Endpoint Test Utility (p. 1258)	To help you validate connectivity to Amazon Connect, or troubleshoot when your agents are experiencing problems with the Contact Control Panel (CCP), we added the Amazon Connect Endpoint Test Utility. For more information, see Use the Endpoint Test Utility.	March 5, 2021
Add a chat user interface to your website. (p. 1258)	Added a chat widget that you can customize and add to your website. Also provided an open source example to help you get started with adding chat to your website. For more information, see Set up your customer's chat experience.	March 5, 2021

Content Lens real-time analytics is available in Europe (London), Europe (Frankfurt), and Asia (Tokyo). (p. 1258)	For more information, see Availability of Contact Lens features by Region.	February 26, 2021
Added ability to create and ingest data into Customer Profiles from Amazon S3 (p. 1258)	For more information, see Create and ingest data into Customer Profiles from Amazon S3.	February 25, 2021
Added DisconnectReason to the contact record stream (p. 1258)	The Amazon Connect contact records stream now includes **DisconnectReason** for voice calls and tasks. For more information, see ContactTraceRecord.	February 19, 2021
Added custom service levels (p. 1258)	Added the ability to create custom service levels, and update the metrics user interface. For details, see New metric groups and categories.	February 16, 2021
Change audio device settings from the CCP (p. 1258)	Added the ability to change audio settings from the Contact Control Panel (CCP). This applies to organizations using a customized CCP. CCP: Change audio device settings.	January 30, 2021
Queue APIs (Preview) (p. 1258)	Added APIs so you can programmatically create and manage queues. Queue APIs (Preview).	January 29, 2021
Amazon AppIntegrations APIs - GA (p. 1258)	Released Amazon AppIntegrations APIs for general availability (GA). For more information, see Amazon AppIntegrations APIs - GA.	January 29, 2021
New Contact search page (p. 1258)	Updated the **Contact search** page. For more information, see Search for contacts.	January 5, 2021
Amazon Connect Service API Reference (p. 1258)	Added APIs so you can programmatically create and manage quick connects. For more information, see Amazon Connect Service API Reference.	December 22, 2020
Chat: Support for sharing attachments (p. 1258)	Added support for sharing chat attachments. For more information, see Chat: Support for attachments.	December 21, 2020

Configurable DTMF timeouts for Lex bots (p. 1258)	Added support for configurable DTMF timeouts for Lex bots. For more information, see Configurable DTMF timeouts for Lex bots.	December 4, 2020
Amazon Connect with Apple Messages for Business (Preview) (p. 1258)	Added support for using Amazon Connect with Apple Messages for Business. For more information, see Amazon Connect with Apple Messages for Business (Preview)	December 3, 2020
Tasks (p. 1258)	Added support for tasks, allowing you to prioritize, assign, track, and even automate tasks across the disparate tools agents use to support customers. For more information, see Tasks.	December 1, 2020
Real-time analytics using Contact Lens for Amazon Connect (p. 1258)	Added real-time analytics for Contact Lens so you can detect and resolve customer issues more proactively while the call is in progress. For more information, see Analyze Conversations with Contact Lens for Amazon Connect.	December 1, 2020
Amazon Connect Wisdom (Preview) (p. 1258)	Added Amazon Connect Wisdom (Preview), which enables agents to search and find content across multiple repositories, such as frequently asked questions (FAQs), wikis, articles, and step-by-step instructions for handling different customer issues. For more information, see Amazon Connect Wisdom (Preview).	December 1, 2020
Amazon Connect Voice ID (Preview) (p. 1258)	Added Amazon Connect Voice ID (Preview), which provides for real-time caller authentication. For more information, see Amazon Connect Voice ID (Preview).	December 1, 2020
Amazon Connect Customer Profiles (p. 1258)	Added Amazon Connect Customer Profiles, enabling agents to create a customer profile for every new contact that comes in. You can also integrate with external applications that provide customer profile data. For more information, see Amazon Connect APIs.	December 1, 2020

Amazon Connect APIs (p. 1258)	Added an Amazon Connect API that provides the ability to create tasks (`StartTaskContact`), and added a set of preview APIs. For more information, see Amazon Connect APIs.	December 1, 2020
Amazon Connect supports interact messages for chat (p. 1258)	Added interactive message templates. For more information, see Add interactive messages to chat.	November 24, 2020
Telephony call metadata attributes (p. 1258)	Added call attributes to improve fraud detection and routing. For more information, see Telephony call metadata attributes (call attributes).	November 20, 2020
APIs to manage user hierarchies (p. 1258)	Added APIs so you can programmatically manage your agent hierarchies and agent groups. For more information, see Amazon Connect Service API Reference.	November 18, 2020
Service quotas (p. 1258)	Noted that up to 700 quick connects can be added to a queue. See Feature specifications. (This update was published erroneously and has since been removed.)	October 5, 2020
Security (p. 1258)	Added new topic on Required permissions for managing access to the Amazon Connect console.	September 24, 2020
Quick filters (p. 1258)	Added new topic that explains how to use quick filters in real-time metrics reports. For more information, see Use quick filters to drill into Routing profiles and Queues tables.	September 23, 2020
Service quotas (p. 1258)	Updated the service quotas for the following Amazon Connect Participant Service APIs: `CreateParticipantConnection`, `DisconnectParticipant`, and `GetTranscript`. For more information, see Amazon Connect Participant Service API throttling quotas.	September 22, 2020

Show agent queues in a Queues table. (p. 1258)	By default, agent queues don't appear in a Queues table in a historical metrics report. You can choose to show them. For more information, see Show agent queues in a Queues table.	September 18, 2020
Migrate contact flows to a different instance (p. 1258)	You can migrate hundreds of contact flows using a set of contact flow APIs. For more information, see Migrate contact flows to a different instance.	September 18, 2020
Languages supported by Amazon Connect (p. 1258)	Learn about which languages are supported in the Amazon Connect console, Contact Control Panel, Contact Lens, Amazon Lex, and Amazon Polly. For more information, see Languages supported by Amazon Connect.	September 18, 2020
Amazon Connect Flow language (p. 1258)	You can use the Amazon Connect Flow language to efficiently update contact flows that you're migrating from one instance to another, and Write contact flows rather than drag blocks onto the contact flow designer. For more information, see Amazon Connect Flow language.	September 18, 2020
Option 2 (not recommended): Allow IP address ranges (p. 1258)	Removed tip from *Option 2: Allow IP address ranges*, that said if you don't see an entry for your region, use GLOBAL. For more information, see Option 2 (not recommended): Allow IP address ranges.	September 11, 2020
Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list (p. 1258)	Updated Option 1, second row of table, with a line break between {myInstanceName}.awsapps.com/connect/api and *.cloudfront.net. For more information, see Option 1 (recommended): Replace Amazon EC2 and CloudFront IP range requirements with a domain allow list.	September 11, 2020

Amazon Connect resource-level policy examples (p. 1258)	Changed title of "Amazon Connect resource-based policy examples" topic to "Amazon Connect resource-level policy examples." For more information, see Amazon Connect resource-level policy examples.	September 8, 2020

Earlier updates

Change	Description	Date
Updated the **Consult** and **Contact consulted** metrics to indicate they were deprecated May 2019.	For more information, see Consult (p. 921) and Contacts consulted (p. 946).	August 27, 2020
Added topic on setting up agent-to-agent transfers.	For more information, see Set up agent-to-agent transfers (p. 472).	August 19, 2020
Added section on requirements for custom termination points.	For more information, see Request numbers, international numbers, or termination points (p. 169).	August 18, 2020
Removed the "Known differences" section from I use the Amazon Connect Streams API (p. 289).	For more information, see I use the Amazon Connect Streams API (p. 289).	August 3, 2020
Changed the name of the **Metrics** chapter to **Monitor metrics & run reports**.	For more information, see Monitor metrics and run reports (p. 892).	July 16, 2020
Clarified that the following metrics are no longer supported in queue grouping: Agent on contact time, Agent idle time, Occupancy. Previously we stated that these metrics had been deprecated.	For more information, see June 2020: Changes for omnichannel support (p. 901).	July 8, 2020
Updated the Set disconnect flow (p. 403) block, which now supports voice conversations.	For more information, see Set disconnect flow (p. 403).	June 29 2020
Added upcoming metric changes: new real-time and historical metrics for inbound and outbound contact time	For more information, see What's new in metrics (p. 892).	June 26, 2020
Added how to upgrade CCP	For more information, see Upgrade to the latest CCP (p. 277).	June 16, 2020

Change	Description	Date
Added video on using CCP	For more information, see Training video: How to use the CCP (p. 1137).	June 16, 2020
Deprecated metrics: Agent on contact time, Agent idle time, Occupancy.	For more information, see June 2020: Changes for omnichannel support (p. 901).	June 12, 2020
Added topic on quick connects work	For more information, see How quick connects work (p. 470).	May 21, 2020
Added how to get administrative support, and added a topic on inherited permissions	For more information, see Get administrative support for Amazon Connect (p. 1257) and About inherited permissions (p. 790).	April 16, 2020
Added how to customize your CCP to log out agents automatically when they close the CCP window	For more information, see CCPv1: Log out agents automatically when they close their CCP (p. 235).	April 16, 2020
Updated the **Get customer input** block to support timeout values for voice input	For more information, see Get customer input (p. 366).	April 8, 2020
Added terminating keypress	For more information, see Store customer input (p. 426).	March 31, 2020
Added NLB endpoints and required domain for softphones	For more information, see Set up your network (p. 605).	March 23, 2020
Announced upcoming changes for metrics	For more information, see June 2020: Changes for omnichannel support (p. 901).	March 23, 2020
Added topic on region requirements for phone numbers	For more information, see Region requirements for ordering and porting phone numbers (p. 171).	March 11, 2020
Added tutorials	For more information, see Tutorials: An introduction to Amazon Connect (p. 31).	March 6, 2020
Added topic on tracking who deleted recordings	For more information, see Track who deleted or listened to recordings (p. 806).	March 5, 2020
Added topic on emergency admin access	For more information, see Emergency admin login (p. 146).	March 3, 2020
Added topics on saving, sharing, and publishing reports	For more information, see Save custom reports (p. 1008), Share custom reports (p. 1010), View a shared report (p. 1012), and Publish reports (p. 1013).	January 22, 2020

Change	Description	Date
Updated contact block definitions	For more information, see .	January 17, 2020
Added a section about queued callbacks in metrics reporting.	For more information, see About queued callbacks in metrics (p. 1002).	January 17, 2020
Updated networking guidance for the updated CCP (ccp-v2)	For more information, see Set up your network (p. 605).	January 15, 2020
Add a topic on logging Amazon Connect API calls with AWS CloudTrail	For more information, see Logging Amazon Connect API calls with AWS CloudTrail (p. 1025).	December 13, 2019
Added a section on analyzing conversations	For more information, see Analyze conversations using Contact Lens for Amazon Connect (p. 811).	December 02, 2019
Added information about live media streaming	For more information, see Capture customer audio: live media streaming (p. 775).	November 21, 2019
Added information about chat	For more information, see Chat (p. 13). Also added these topics: Best practices for Amazon Connect (p. 29), About agent status (p. 998), About contact states (p. 1000), and Additional resources for Amazon Connect (p. 1219).	November 21, 2019
Added topic on using IAM	For more information, see Identity and access management for Amazon Connect (p. 1078).	November 14, 2019
Added dimensions	Added dimensions to the Amazon Connect metrics sent to CloudWatch. See Monitoring your instance using CloudWatch (p. 1014).	October 22, 2019
Added a networking topic	Consolidated networking content into Set up your network (p. 605). 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
Updated historical metrics report section	Added categories to the historical metrics definitions.	August 27, 2019

Change	Description	Date
Re-organized the content	Re-organized the content so it's task-based.	July 19, 2019
Added information about the updated **Transfer to phone number** block	You can use the updated **Transfer to phone number** block to transfer callers to a phone number external to your Amazon Connect instance, and then optionally resume the contact flow after the call with the external party ends. For more information, see Resume a contact flow after transfer (p. 475).	February 18, 2019
Adding information about live media streaming for customer audio streams	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. 775).	December 21, 2018
Added content about agent queues	You can use agent queues to route calls directly to a specific agent. For more information, see Transfer contacts to a specific agent (p. 477).	December 21, 2018
Added information about using Amazon Connect in the Asia Pacific (Tokyo) Region.	For more information, Claim phone numbers for Amazon Connect in the Asia Pacific (Tokyo) Region (p. 168).	December 10, 2018
Added information about how to determine agent ACW time from agent event streams	For more information, see Determine how long an agent spends doing ACW (p. 968).	October 30, 2018
Added troubleshooting and best practices	Troubleshooting Issues with the Contact Control Panel (CCP) (p. 1193) covers best practices for agent connectivity using the CCP and troubleshooting connectivity and call quality issues in Amazon Connect.	October 18, 2018
Added information about service-linked roles in Amazon Connect	For more information, see Use service-linked roles for Amazon Connect (p. 1120).	October 17, 2018

Change	Description	Date
Added information about queue to queue transfers	You can use the new options of the **Transfer to queue** block to enable transferring calls that are already in a queue to another queue. For more information, see Manage contacts in a queue (p. 476).	July 31, 2018
Added information about the **Call phone number** block	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 Caller ID number: Set in the queue or Call phone number block (p. 213).	July 2, 1018
Added information about contact attributes and the **Get queue metrics** block	For more information, see Use Amazon Connect contact attributes (p. 515).	June 18, 2018
Added information about new metrics sent to Amazon CloudWatch Logs.	Monitoring your instance using CloudWatch (p. 1014) includes additional metrics.	April 19, 2018
Added information about using SAML for identity management	You can configure your instance to use SAML for identity management. You can also use SAML to enable single sign-on. For more information, see Configure SAML with IAM for Amazon Connect (p. 124).	March 30, 2018
Added information about agent call transfers	You can enable call transfers from an agent to another agent, to a queue, or to an external number.	December 10, 2017
Added information about manager listen-in	You can configure and enable a manager to listen in on agent calls. For more information, see Monitor live conversations (p. 798).	December 10, 2017
Added information about contact flow logs	For more information, see Enable contact flow logs (p. 511).	November 16, 2017
Added information about contact flow import/export	For more information, see Import/export contact flows (p. 487).	November 16, 2017
Added information about agent event streams	For more information, see Amazon Connect agent event streams (p. 965).	November 16, 2017

Change	Description	Date
Added information about porting your current phone number to Amazon Connect	For more information, see Port your current phone number (p. 157).	November 10, 2017
Added information about Login/ Logout reports	For more information, see Login/Logout reports (p. 960).	November 1, 2017
Initial release	Initial release of the *Amazon Connect Administrator Guide*.	March 28, 2017

Amazon Connect Glossary

Channel

How a customer contacts your business: voice (a phone call), chat (a web site or app), and task.

Contact attribute

A piece of data about a contact. You can use this data to personalize the customer experience, make routing decisions about contacts as they progress through your contact center or retrieve real-time metrics about the queues and agents in your contact center to dynamically route contacts based on queue and agent availability.

Flow

Flows define the experience your customers have when they interact with your contact center. These are similar in concept to Interactive Voice Response (IVR). Contact flows are comprised of blocks, with each block defining a step or interaction in your contact center. For example, there are blocks to play a prompt, get input from a customer, branch based on customer input, or invoke an Lambda function or Amazon Lex bot.

Instance

A virtual contact center. It is 100% cloud-based and can scale to support any sized business. An Amazon Connect instance is not aligned to an EC2 instance or any other hardware concept.

Letter of Authorization

Letter of Authorization (LOA) is a legal document in which you assert to the carrier for Amazon Connect that you have the authority to port phone numbers from your current carrier to the carrier for Amazon Connect. Traditionally, this is a paper document requiring an actual signature.

Losing carrier

Also the customer’s current carrier. This is the carrier that currently owns the telephone number. The losing carrier will review all information presented on the Letter of Authorization (LOA) and will validate if it matches the information that they have on file for the customer.

Mutually agreed date and time

After the LOA has been approved by the losing carrier, the losing and winning carriers agree upon a date and time to perform the porting activity.

Omnichannel

A unified contact experience across multiple communication channels, such as voice and chat. Admins can build experiences once, and enable them for voice and chat. Managers monitor and adjust queues from one dashboard. Agents handle all customers using one interface.

Phone number portability

Number portability allows telephone customers to transfer their numbers to other carriers. Carriers and countries may have unique processes and procedures required.

Queue

A waiting area that holds contacts to be answered by agents.

Winning carrier

Also the carrier for Amazon Connect. This is the carrier that the phone number is being ported to, and will own the phone number after the porting is completed.