Amazon Connect

Administrator Guide

Amazon Connect: Administrator Guide

Table of Contents

What Is Amazon Connect?

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

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

How Amazon Connect Works

An Amazon Connect contact center resides in an instance, which contains all the resources and settings you need to launch, run, and scale your contact center. These instances provide both the ability to configure settings such as data storage options, and a user interface to manage and use your contact center.

To get started with Amazon Connect, ensure that you have either a user directory or a list of users. These users can range from administrators to agents.

It's important to understand the underlying functions of your Amazon Connect configuration. These need to be set up correctly to ensure that your contact center doesn't encounter any issues.

> **Note**
> You can have multiple instances, but information such as user directories cannot be shared across instances.

Directories for Identity Management

Amazon Connect requires a directory to store user information and permissions for the instance. As a first step to setting up an Amazon Connect instance, you select the directory you want to use for identity management. You can choose to manage users in Amazon Connect, or to use an existing directory that is set up in AWS Directory Service. An existing directory must be associated with your AWS account, and active in the AWS region in which you create your instance. You can choose to use a Microsoft Active Directory, Active Directory Connector, or Simple Active Directory. You can associate an AWS Directory Service directory with only one Amazon Connect instance at a time.

You cannot change the directory you select for identity management 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. For information about the costs associated with using AWS Directory Service, see AWS Service Pricing Overview.

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

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

- Directories cannot be shared across multiple Amazon Connect instances.

Administrators

Administrators set permissions, manage and generate metrics, add users, and configure all aspects of contact management. Administrators can be granted different types of permissions—this is done in Amazon Connect.

Secure Storage and Data Integrity

Secure storage and data integrity are an important part of managing recorded calls. Customer calls are recorded in real time and can contain sensitive information.

By default, AWS creates a new Amazon S3 bucket during the configuration process, with built-in encryption. You can also use existing S3 buckets. There are separate buckets for call recordings and exported reports, and they are configured independently. There is full access through Amazon Connect and control over recordings, allowing for custom retention policies. Customizable metrics reports published into Amazon S3 can be processed using the Amazon S3 API or AWS Lambda to integrate with external systems such as workforce management and business intelligence tools.

Note
We recommend that you keep the default settings for encryption.

The following security measures are supported:

- AWS Key Management Service—AWS KMS is a powerful, managed service that gives you complete control over your encryption keys. A default AWS KMS key is provided.
- ARN/ID—You can use an ARN/ID instead of an AWS KMS master key. This is an advanced option and should be attempted only if you are confident of the changes that you're going to make.

Supported Browsers

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

Browser	Version	Check your version
Google Chrome	Latest 3 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	Latest 3 versions	Open Firefox. On the menu, choose the Help icon and then choose **About Firefox**. The version number is listed underneath the Firefox name.
Mozilla Firefox	Latest 3 versions	Open Firefox. On the menu, choose the Help icon and then choose **About Firefox**. The version number is listed underneath the Firefox name.

Service Limits

The following table provides the default limits for new Amazon Connect instances. You can create two instances per AWS account to start, but if you need more instances it is easy to request an increase. You can also request an increase for any of the limits using the Amazon Connect service limits increase form. You need to be signed in to your AWS account to access the form.

Item	Default limit
Amazon Connect instances per account	2
Users per instance	500
Phone numbers per instance	10
Queues per instance	50
Queues per routing profile	50
Routing profiles per instance	100
Hours of operation per instance	100
Quick connects per instance	100
Prompts per instance	500
Agent status per instance	50
Security profiles per instance	100
Contact flows per instance	100
Groups per level	50
Reports per instance	500
Scheduled reports per instance	50
Concurrent active calls per instance	10

Related Services

The following services are used with Amazon Connect:

- **AWS Directory Service**—AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. Amazon Connect user and identity management is based on this service.
- **Amazon S3**—Amazon Simple Storage Service (Amazon S3) is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web. Amazon Connect uses Amazon S3 as a primary data storage service/platform for call recordings and metrics reports delivered into your AWS account.
- **AWS Lambda**—Lambda allows you to build and run code quickly without provisioning or managing servers. Amazon Connect contact flows (IVR flows) are integrated with Lambda so you can build a highly personalized and dynamic IVR experience. You can build Lambda functions that communicate

with CRM systems or custom services for data dips that influence customer IVR experience (such as customer segmentation and dynamic IVR menus, or account and last contact look ups). Lambda functions can also be used as notification mechanisms to external systems during specific points in the contact flow.

- **Amazon Lex**—Amazon Connect integrates with Amazon Lex to build conversational interfaces using voice and text. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable you to build applications with highly engaging user experiences and lifelike conversational interactions. For more information, see the Amazon Lex Developer Guide.
- **Kinesis**—Amazon Connect integrates with Kinesis as the platform for streaming contact trace records (CTR) and agent event streams data. The data is published to Kinesis in JSON format, and include details about contacts and agent activities in your contact center. You can use this data stream to optionally process and publish them into Amazon Redshift (an AWS data warehouse service) or your custom data warehouse systems, enabling detailed analytics and reporting on your contact center data. You can leverage Amazon QuickSight (a cloud-powered business analytics service) or your own BI tools to build powerful visualizations on top of synthesized data. Additionally, this data can be streamed to Elasticsearch to query on this data using a convenient visual interface. For more information, see the Amazon Kinesis Data Streams Developer Guide.

  Note
  Amazon Connect does not support publishing data to streams for which server-side encryption is enabled.
- **Amazon CloudWatch**—Amazon Connect integrates with CloudWatch to provide you with real-time operational metrics for your contact center, such as total calls per second, calls rejected and throttled, percentage of concurrent calls, failed / missed calls count (errors, bad number/address, busy/line engaged), and contact flow errors. You can set up monitors on these metrics in order to stay on top of the health of your contact center. For more information, see Monitoring Amazon Connect Using Amazon CloudWatch Metrics (p. 13).
- **AWS Identity and Access Management**—The AWS Management Console requires your username and password so that any service you use can determine whether you have permission to access its resources. We recommend that you avoid using AWS account root user credentials to access AWS because root user credentials cannot be revoked or limited in any way. Instead, we recommend that you create an IAM user and add the user to an IAM group with administrative permissions. You can then access the console using the IAM user credentials. For more information, see the IAM User Guide.

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

Getting Started with Amazon Connect

An Amazon Connect instance is the starting point for your contact center. When your instance has launched, you can edit the resource configuration settings, which include data storage, integration with CRM systems, and analytics. Then, you can launch your instance from the AWS Management Console, follow the onboarding steps, and begin using your contact center.

Part of this tutorial refers to the Amazon Connect Contact Control Panel (CCP). The CCP is built in to the Amazon Connect Contact Center Manager (CCM). After you have claimed and tested your number, you can start using the CCP immediately. For more information, see Using the Contact Control Panel in the *Amazon Connect User Guide*.

To get started with using Amazon Connect, you first create an instance, which is the basis of your contact center. You can edit your instance's resource settings in the AWS Management Console. After your instance has been created, it is accessible through a unique URL, which is used by agents, administrators, and managers to open the CCM and access the CCP. For more information, see How Amazon Connect Works (p. 1).

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.

If you have an AWS account already, skip to the next task. If you don't have an AWS account, use the following procedure to create one.

To create an AWS account

1. Open https://aws.amazon.com/, and then choose **Create an AWS Account**.

   Note
   This might be unavailable in your browser if you previously signed into the AWS Management Console. In that case, choose **Sign in to a different account**, and then choose **Create a new AWS account**.
2. Follow the online instructions.

   Part of the sign-up procedure involves receiving a phone call and entering a PIN using the phone keypad.

Create an Amazon Connect Instance

You can create or add an instance as follows. These steps are intended to help you get started quickly; some advanced settings are not included.

To create an Amazon Connect instance

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

2. Do one of the following:
   - If you have not previously created an Amazon Connect instance, choose **Get started**.
   - If you have previously created an instance, choose **Add an instance**.
3. For **Step 1: Identity management** step, do one of the following:
   - If you want to manage your users within Amazon Connect, choose **Store users within Amazon Connect**.
   - If you want to use an existing directory where you users are managed, choose **Link to an existing directory**.
4. Enter an instance alias for your instance in the **Access URL** field, and then choose **Next step**.

   The name you enter is displayed as the instance alias in the AWS console, and is used as the domain in the access URL to access your contact center. The alias must be globally unique, meaning that an alias can be used only once across all Amazon Connect instances and regions. You cannot change the alias URL once your instance is created.
5. For **Step 2: Administrator**, do one of the following:
   - If you chose **Store users with Amazon Connect** for identity management, enter the user details for an admin account, and then choose **Next step**.
   - If you chose **Link to an existing directory** for identity management, enter the user name for the account you want to use as the admin account for your instance, and then choose **Next step**.

     If the user name you enter does not exist in your directory, you can add it later.
   - Choose **Skip this** if you want to create an admin account later. To create an admin later, you can log in to your instance as an administrator from the Amazon Connect console.
6. For **Step 3: Telephony options**, indicate whether you'd like your contact center to accept calls, make calls, or both. You can set the user permissions within the Amazon Connect web application. The telephone number options are provided after setup.
7. For **Step 4: Data storage**, you can keep the default settings or choose **Customize settings** in order to modify settings. For more information, see Data Storage (p. 9).
8. For **Step 5: Review and create**, review your settings and then choose **Create instance**.

   Important
   This is the only time you can change the directory and domain name settings—you can edit any other setting later on.
9. After your instance is created, choose **Get started** to claim and test a phone number. Amazon Connect automatically configures your instance to use the phone number that you select.

   Note
   For information about how to use your current phone number with Amazon Connect, see Port Your Current Phone Number (p. 6).
10. (Optional) Continue to configure your instance. For more information, see Configuring Your Amazon Connect Instance (p. 9).

Port Your Current Phone Number

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

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

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

To port your current phone number to Amazon Connect

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Log in with the account used to create the Amazon Connect instance to which to port your current number, and choose **Support**, **Support Center**.
3. On the **Support Center** page, choose **Create Case**.
4. For **Regarding**, select **Service Limit Increase**.
5. For **Limit Type**, select **Connect**.
6. For **Region**, select the region in which you created your Amazon Connect instance.
7. For **Limit**, select **Phone Number Porting**.
8. For **New limit value**, enter the number of phone numbers to port.
9. For **Use Case Description**, include as much information as possible about your request, including whether the numbers are Direct Inward Dial or toll-free, your current carrier, and the contact information for the person authorized to make changes to your current phone service. If you do not know all of these details, you may leave information out.
10. Fill in the rest of the form, and choose **Submit**.

About Porting Phone Numbers

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

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

The steps in the porting process are as follows:

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

   On the LOA form, include the numbers to port; information about your current carrier, such as a phone bill; and contact information for the person authorized to make changes to your phone service.
4. To get the port started, the Amazon Connect team submits the LOA to the carrier for Amazon Connect on your behalf. The new carrier works with your current carrier to move your current number over to their service. This step typically takes 3–5 business days.

If your current carrier is able to validate and approve your request, they provide a date for the number to be ported to Amazon Connect.

If your current carrier rejects the request to port your number due to the LOA not having correct or complete information, the Amazon Connect team contacts you and requests a new LOA to submit to the carrier.

When we receive a date from your current carrier, we start adding the numbers to your Amazon Connect instance about a day before the scheduled date.

Integrate with Your CRM

You can integrate Amazon Connect with the Salesforce and Zendesk CRMs. Integration allows you to launch your contact center in your CRM of choice, maintain your existing user base, and use the Amazon Connect cloud-based infrastructure.

To integrate the Contact Control Panel (CCP) into your CRM, see Amazon Connect Contact Streams. When completed, add the origin URLs to your instance settings. This enables communication between Amazon Connect and your CRM. For more information, see Application Integration (p. 11).

Delete Your Amazon Connect Instance

If you no longer wish to use an Amazon Connect instance, you can delete it. Any directories, buckets, or administrators that are associated with the instance are also deleted.

Important
This operation cannot be canceled or undone.

To delete an Amazon Connect instance

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

Configuring Your Amazon Connect Instance

You can configure your Amazon Connect instance using the AWS Management Console. To access instance settings, choose the name of the instance in the **Instance Alias** column.

Settings

Overview

The **Overview** section displays the following information about your Amazon Connect instance.

- **Instance ARN**—the ARN for the instance. The instance ID for the instance is included in the ARN, and is the value after the instance/. For example, the instance ID in the following instance ARN is df9e742b-310b-4eb2-a062-31bc99177ed4. `arn:aws:connect:us-east-1:361814831152:instance/df9e742b-310b-4eb2-a062-31bc99177ed4`
- **Directory**—The instance alias for the instance.
- **Login URL**—The URL to use in a browser to log in directly to the contact center for your instance.

  If your agents (users that are assigned only the Agent security profile) try to use this URL to log in to Amazon Connect, "Error 403! (Forbidden) is displayed on the page. The agent can still open the Contact Control Panel (CCP) by selecting the phone icon in the top-right corner of the page.

You can use the **Login as administrator** button to log in to the instance using your AWS account with full admin permissions. This can be helpful if you ever forgot the password for the admin account, or need to update Amazon Connect settings.

Telephony

Select whether to accept incoming calls to, or allow outbound calls from, your Amazon Connect instance. You can use security profiles to set permissions to enable or disable outbound calling.

Data Storage

Data, such as call recordings and reports, is stored securely in an Amazon S3 bucket. During setup, a default Amazon S3 bucket is created and encrypted using AWS Key Management Service. This bucket and key are used for both calling recordings and reports. Alternatively, you can use separate buckets and keys for call recordings and reports.

Before updating the data storage settings, ensure that you are familiar with Amazon S3 and AWS KMS.

To update data storage settings

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 **Data storage**.
4. To update the settings for call recordings, do the following:
   a. For **Call recordings**, choose **Edit**.
   b. (Optional) To disable call recordings, clear **Enable call recording**.
   c. (Optional) If call recordings are enabled, you can create a new S3 bucket or select an S3 bucket that you've already created.
   d. (Optional) If call recordings are enabled, you can update the encryption settings as needed. To disable encryption, clear **Enable encryption**. To update the KMS key, specify a key from the same region as your S3 bucket.
   e. To save your changes, choose **Save**.
5. To update the settings for exported reports, do the following:
   a. For **Exported reports**, choose **Edit**.
   b. (Optional) To disable exported reports, clear **Enable exported reports**.
   c. (Optional) If exported reports are enabled, you can create a new S3 bucket or select an S3 bucket that you've already created.
   d. (Optional) If exported reports are enabled, you can update the encryption settings as needed. To disable encryption, clear **Enable encryption**. To update the KMS key, specify a key from the same region as your S3 bucket.
   e. To save your changes, choose **Save**.

Data Streaming

You can export contact trace records (CTRs) and agent events from Amazon Connect and perform real-time analysis on contacts. Data streaming uses the Amazon Kinesis platform to support data streaming.

To set up data streaming

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 **Data streaming**.
4. Choose **Enable data streaming**.
5. Select **Kinesis** or **Kinesis Data Firehose**, and then do one of the following:
   - To use an existing Amazon Kinesis stream or Kinesis Data Firehose, select the resource in the drop-down list.
   - To create a new resource, choose **Create a new Amazon Kinesis stream** (or Kinesis Data Firehose).

     This opens the Amazon Kinesis console where you can create the stream or firehose to use with Amazon Connect. Wait until the stream or firehose is created, then return to the Amazon Connect console.

     Reload the page so that the stream or firehose you created is displayed in the resource selection, then select the stream or firehose.

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

6. Choose **Save**.

Application Integration

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

To whitelist a domain URL

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

Contact Flows

A contact flow defines the customer experience with the contact center from start to end. You can configure your contact flow using the AWS Management Console as follows.

Security Keys

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

Note
You can have up to two signing keys active at one time to facilitate rotation.

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

To add a security key

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the name of the instance from **Instance Alias**.
3. In the navigation pane, choose **Contact flows**.
4. Choose **Add key**.
5. Paste the contents of your public key in **Public key contents** and choose **Add**.

Amazon Lex

With Amazon Lex, you can build conversational interactions (bots) that feel natural to your customers, giving you access to the same speech recognition and natural language understanding technology that powers Alexa. After you create a Lex bot, you can integrate it into your contact flows.

To integrate an Lex bot

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 **Contact flows**.
4. Choose **Add Lex Bot**.
5. Choose your Lex bot from **Lex bots** and choose **Save Lex Bots**.

Contact flow logs

Select the **Enable Contact flow logs** check box to start sending your contact flow logs to Amazon CloudWatch. To learn more about Contact flow logs, see Contact flow logs.

Monitoring Amazon Connect Using Amazon CloudWatch Metrics

Amazon Connect integrates with CloudWatch so that you can collect, view, and analyze CloudWatch metrics for your Amazon Connect virtual contact center. Using this data, you can monitor key operational metrics and set up alarms. The metrics that you configure are automatically collected and pushed to CloudWatch every five minutes. Metrics are archived for two weeks; after that period, the data is discarded.

VoiceCalls Metrics

Metric	Description
`MissedCalls`	Represents the number of voice calls that were missed by the agents (not answered within 20 seconds).
`ThrottledCalls`	Represents the number of voice calls that were throttled by the Amazon Connect Voice Service due to TPS/Callrate going beyond configured threshold for the Amazon Connect instance.
`CallsBreachingConcurrencyQuota`	Represents the number of voice calls that breached the `Concurrency Quota` configured threshold for the Amazon Connect instance.
`ConcurrentCalls`	Represents the number of concurrent voice calls.
`ConcurrentCallsPercentage`	Represents the percentage of concurrent voice calls. `ConcurrentCalls/ConfiguredConcurrentCallsLimit * 100`.
`CallsPerInterval`	Represents the rate at which voice calls (both inbound, outbound) are coming.

CallRecordings Metrics

Metric	Description
`CallRecordingUploadError`	Represents the number of call recordings that failed to be uploaded to the customer's S3 bucket.

ContactFlow Metrics

Metric	Description
`MisconfiguredPhoneNumbers`	Represents the number of calls that failed because the phone number is not configured to a **Contact flow**.

Metric	Description
`ContactFlowFatalErrors`	Represents **Contact flow** execution failures.
`ContactFlowErrors`	Represents the number of times the **Contact flow** branched to an `ERROR` label in the instruction.

Queue Metrics

Metric	Description
`QueueCapacityExceededError`	Represents the number of calls rejected due to the queue being full.
`QueueCallBackNonDialableNumber`	Represents an error when the queue call back to a customer number is not dialable due to dialing profile restrictions.

Other Metrics

Metric	Description
`PublicSigningKeyUsage`	Usage count of the public sign-in key for CCIVR contact flows in Amazon Connect.

Metric Dimensions

To filter the metrics for Amazon Connect, use the following dimensions.

Metric	Description
`InstanceId`	The Amazon Connect instance ID. This is currently not the complete ARN, just the ID.
`QueueName`	The name of the queue. This dimension is relevant only for queue metrics.
`ContactFlowName`	The name of the ContactFlow. This dimension is relevant only for ContactFlow metrics.
`MetricGroup`	The category group. The following category groups are supported: `CallRecordings`, `ContactFlow`, `Queue`, and `VoiceCalls`.

Using AWS Lambda Functions with Amazon Connect

Amazon Connect can interact with your own systems and take different paths in contact flows dynamically. To achieve this, invoke Lambda functions, fetch results in an contact flow, and call your own services or interact with other AWS data stores or services.

To learn more about AWS Lambda, see the AWS Lambda Developer Guide.

Invoking a Lambda Function from a Contact Flow

The steps required to invoke a Lambda function from Amazon Connect include the following:

1. Create a Lambda function and define its trigger policy to allow Amazon Connect to invoke the function.
2. Use the ARN of the Lambda function in an **Invoke AWS Lambda function** block in your contact flow.
3. Configure the Lambda function code to parse the JSON event sent from the contact flow, and define the business logic to execute.
4. Test the configuration to confirm that the Lambda function returns the correct JSON response.
5. Consume the attribute values returned from Lambda to use in your contact flow.

Create a Lambda Function and Configure a Trigger Policy

Amazon Connect can successfully invoke a Lambda function in an AWS account when a resource policy has been set on the Lambda function. For more information, see Using Resource-Based Policies for AWS Lambda in the *AWS Lambda Developer Guide*.

To begin, create a Lambda function, and then note down the function name. For more information about creating a Lambda function, see Create a Simple Lambda Function.

Use the following add-permission command to create a resource policy using this information:

```
aws lambda add-permission --function-name function:my-lambda-function --statement-id 1 \
--principal connect.amazonaws.com  --action lambda:InvokeFunction --source-
account 123456789012 \
--source-arn arn:aws:connect:us-east-1:123456789012:instance/def1a4fc-ac9d-11e6-
b582-06a0be38cccf \
```

This command uses the following input:

- The name of the Lambda function (for example, **my-lambda-function**)
- The ARN of a Amazon Connect instance (for example, **arn:aws:connect:us-east-1:123456789012:instance/def1a4fc-ac9d-11e6-b582-example**)

To find the ARN for your instance, open the Amazon Connect console, and then choose the **Instance Alias** to open the **Overview** page.

- The AWS account ID for the Lambda function (for example, **123456789012**)

Invoke the Lambda Function in Your Contact Flow

To invoke a Lambda function from your contact flow, add an **Invoke AWS Lambda function** block to the flow, and then add the ARN for the function you created as the value for the **Function ARN** in the contact flow properties. You can view the ARN for the function in the AWS Lambda console at https://console.aws.amazon.com/lambda/.

You can also run the following command in the AWS Command Line Interface to view the function ARN:

```
aws lambda get-function --function-name my-lambda-function
```

In the **Invoke AWS Lambda function** block, you can add **Function input parameters**, which are key-value pairs that are sent to the Lambda function when invoked. You can also specify a **Timeout** value for the function.

On every Lambda function invocation from a contact flow, you pass a default set of information related to ongoing contact, as well as any additional attributes defined in the **Function input parameters** for the **Invoke AWS Lambda function** block added to your contact flow.

The following is an example JSON request to a Lambda function:

```
{
    "Details": {
        "ContactData": {
            "Attributes": {},
            "Channel": "VOICE",
            "ContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXXX",
            "CustomerEndpoint": {
                "Address": "+1234567890",
                "Type": "TELEPHONE_NUMBER"
            },
            "InitialContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXX",
            "InitiationMethod": "INBOUND | OUTBOUND | TRANSFER | CALLBACK",
            "InstanceARN": "arn:aws:connect:aws-region:1234567890:instance/
c8c0e68d-2200-4265-82c0-XXXXXXXXXX",
            "PreviousContactId": "4a573372-1f28-4e26-b97b-XXXXXXXXXX",
            "Queue": "QueueName",
            "SystemEndpoint": {
                "Address": "+1234567890",
                "Type": "TELEPHONE_NUMBER"
            }
        },
        "Parameters": {
            "sentAttributeKey": "sentAttributeValue"
        }
    },
    "Name": "ContactFlowEvent"
}
```

The request is divided into three parts:

- Contact data—This is always passed by Amazon Connect for every contact. Some parameters are optional.

- User attributes—These are attributes that have been previously associated with a contact, such as when using a **Set contact attributes** block in a contact flow. This map may be empty if there aren't any saved attributes.
- Parameters—These are parameters specific to this call that were defined when you created the Lambda function.

The Lambda function response should be a simple Map *`String String`*. 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. The following code is an example Python Lambda function:

Configure Your Lambda Function

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

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

Verify the Function Response

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) {

var resultMap = {
    Name:'CustomerName',
    Address:'1234 Main Road',
    CallerType:'Patient'
}

callback(null, resultMap);
}
```

And this example shows an example response using Python:

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

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

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

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

Using the Lambda Function Response

There are two ways to use the function response in your contact flow. You can either directly reference the variables returned from Lambda, or store the values returned from the function as contact attributes and then reference the stored attributes. When you use an external reference to a response from a Lambda function, the reference will always receive the response form the most recently invoked function. To use the response from a function before a subsequent function is invoked, the response must be saved as a contact attribute, or passed as a parameter to the next function.

Access Lambda attributes directly

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

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

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

Store Lambda variables as contact attributes

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

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

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

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

Amazon Connect and Salesforce Integration

The Amazon Connect CTI Adapter provides a WebRTC browser-based Contact Control Panel (CCP) within Salesforce. This integration enables your agents to leverage both inbound caller ID screen pop and outbound click to call/transfer/conferencing.

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. This configuration is a XML file that you import into your call center. It provides all the details required to enable the CTI.

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

Prerequisites

- Salesforce Classic, Salesforce Console, or Lightning Experience
- An Amazon Connect instance with a user account assigned only the Agent security role. The user accounts for Salesforce and Amazon Connect are separate accounts. You should log in to Amazon Connect with your user account that is assigned the Agent security role. You should also log in to Salesforce using a Salesforce user account that has been granted access to the CCP in Salesforce.

  For information about how to assign security profiles, see the Amazon Connect User Guide
- A Firefox or Chrome browser

To integrate with Salesforce

1. In your Salesforce sandbox, install the following managed package: Amazon Connect CTI Adapter.
2. Edit the call center configuration as follows:
   - For **CTI Adapter URL**, type the one of the following, based on your Salesforce interface:
     - **`/apex/amazonconnect__ACSFCCP_Classic`**
     - **`/apex/amazonconnect__ACSFCCP_Console`**
     - **`/apex/amazonconnect__ACSFCCP_Lightning`**
   - For **Salesforce Compatibility Mode**, choose **Classic** for the Salesforce Classic and Salesforce Console or **Lightning** for Lightning Experience.
   - For **Amazon Connect CCP URL**, type the CCP URL for your instance (for example, https://*instance*.awsapps.com/connect/ccp).
   - For **Phone Number Formatting**, **Country**, specify the appropriate 2-digit ISO country code.
   - To provide Salesforce users with access to the Amazon Connect CCP, on the **Setup Call Centers** page, choose **Manage Call Center Users**. Add the Salesforce users you want to enable for using these call features. Be sure to add your own Salesforce user account if you plan to these features.
3. Whitelist your Salesforce Visualforce domain URL using the directions in Application Integration (p. 11). This URL usually has the following format:

   ```
   https://amazonconnect.instance.visual.force.com
   ```

   To verify the URL, open the Visualforce page in setup.

4. Log in to your Amazon Connect instance.
5. Launch Salesforce. You should see the integrated CCP in the side panel (Salesforce Classic) or the phone toolbar (Salesforce Classic and Lightning Experience).

Troubleshooting Common Issues

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

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

  {"OPF":"0","NPF":"*2 digit dialing code*","Country":"*2 digit country code*","NF":"International_plaintext","TNF":"(555) 123-4567"}
- Confirm that the Salesforce user can access the call center. To check a user's status, choose **Manage Call Center Users**.
- Under **Softphone Layout**, **Screen Pop**, confirm that **Single-matching record** is set to **Pop detail page** and **Multiple-matching record** is set to **Pop to search page**.
- If you are using Salesforce Lightning Experience and do not see a phone toolbar icon, confirm that you have enabled console navigation. To enable console navigation, in the **Salesforce Setup Console**, choose **App Manager**, **Service Console (Lightning)**, **Edit**. On the **Edit** page, choose **App Options**, **App Navigation**, **Console Navigation**.

Document History

The following table describes the documentation for this release of Amazon Connect.

Change	Description	Date
Updated topic on using AWS Lambda functions with Amazon Connect	Replaced existing content with new information and examples to make the topic current with the technology. For more information, see Using AWS Lambda Functions with Amazon Connect (p. 15)	January 05, 2018
Added Port Your Current Phone Number	Added information about how to port your current telephone number to Amazon Connect. For more information, see Port Your Current Phone Number (p. 6)	November 10, 2017
Updated Salesforce integration information	Updated the steps to integrate Amazon Connect with Salesforce to clarify settings. For more information, see Amazon Connect and Salesforce Integration (p. 19)	October 27, 2017
Initial release	Initial release of the *Amazon Connect Administrator Guide*.	March 28, 2017