# Table of Contents

What Is Amazon Connect? ......................................................................................................................... 1
Amazon Connect Instances .......................................................................................................................... 1
Identity Management ................................................................................................................................. 1
Amazon Connect Administrator .................................................................................................................. 1
Secure Storage and Data Integrity ............................................................................................................. 1
Supported Browsers .................................................................................................................................. 2
Service Limits ........................................................................................................................................... 2
Related Services ...................................................................................................................................... 3
Get Started ............................................................................................................................................. 5
Before You Begin ................................................................................................................................... 5
Plan for User and Identity Management ................................................................................................. 5
Create an Amazon Connect Instance ..................................................................................................... 6
Use an Existing Directory for Amazon Connect Identity Management .................................................. 7
Configure SAML for Identity Management in Amazon Connect ............................................................ 8
  Overview of Using SAML with Amazon Connect .............................................................................. 8
  Enabling SAML-based Authentication for Amazon Connect ............................................................. 9
  Select SAML 2.0-based Authentication During Instance Creation .................................................. 9
  Enable SAML Federation Between Your Identity Provider and AWS .............................................. 9
  Use a Destination in Your Relay State URL ...................................................................................... 11
  Add users to Your Amazon Connect Instance .................................................................................. 11
  SAML User Log in and Session Duration ....................................................................................... 12
Port Your Current Phone Number .......................................................................................................... 13
About Porting Phone Numbers ............................................................................................................... 13
Integrate with Your CRM ....................................................................................................................... 14
Remove Your Amazon Connect Instance .............................................................................................. 14
Configuring Your Instance ..................................................................................................................... 16
Overview ................................................................................................................................................ 16
Telephony ............................................................................................................................................... 16
Data Storage .......................................................................................................................................... 16
Data Streaming ..................................................................................................................................... 17
Application Integration ........................................................................................................................... 18
Contact Flows ....................................................................................................................................... 18
  Security Keys .................................................................................................................................... 18
  Amazon Lex ...................................................................................................................................... 18
  Contact flow logs ............................................................................................................................ 19
Monitoring Amazon Connect in Amazon CloudWatch Metrics ............................................................ 20
  Amazon Connect Metrics Sent to CloudWatch .............................................................................. 20
  Amazon Connect CloudWatch Metrics Dimensions .................................................................. 21
Granting Access to Lambda Functions ................................................................................................... 23
  Invoking a Lambda Function from a Contact Flow ....................................................................... 23
    Create a Lambda Function and Configure a Trigger Policy .......................................................... 23
    Invoke the Lambda Function in Your Contact Flow ................................................................... 24
  Configure Your Lambda Function ...................................................................................................... 25
  Verify the Function Response .......................................................................................................... 25
  Using the Lambda Function Response ............................................................................................. 26
Salesforce Integration ............................................................................................................................. 27
Troubleshooting Common Issues .......................................................................................................... 28
Document History ................................................................................................................................. 29
Amazon Connect Administrator Guide

Amazon Connect Instances

What Is Amazon Connect?

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

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

Amazon Connect Instances

To create an Amazon Connect contact center, you create an Amazon Connect instance. Each instance contains all of the resources and settings related to your contact center. You can manage settings for your instance from the Amazon Connect console. You can manage settings for your contact center from within your contact center. You can create multiple instances, but each instance functions only within the AWS region in which you create it. Settings, users, metrics, and reporting are not shared between Amazon Connect instances.

Identity Management

When you create an Amazon Connect instance, you must choose how you want to manage your Amazon Connect users. Permissions to access Amazon Connect features and resources, such as opening the contact control panel (CCP), placing calls, or creating reports, are assigned to user accounts within Amazon Connect. You can choose from the following three options for identity management:

- Store users in Amazon Connect.
- Link to an existing directory using AWS Directory Service.
- Use SAML 2.0-based authentication to federate with your Amazon Connect instance and enable single sign-on.

To learn more about identity management in Amazon Connect, see Plan for User and Identity Management (p. 5).

Amazon Connect Administrator

Amazon Connect administrators set permissions, manage and generate metrics, add users, and configure all aspects of your contact center. You can grant or deny different types of permissions by assigning security profiles 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. The customizable metrics reports published into Amazon S3 can be processed using the Amazon S3 API or AWS Lambda. Integrate the reports 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.

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

### 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 must be signed in to your AWS account to access the form.

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

**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 in Amazon CloudWatch Metrics (p. 20).

- **AWS Identity and Access Management**—The AWS Management Console requires your user name 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. After you create an instance, you can edit the settings for it, which include telephony, data storage, data streaming, application integration, and contact flows. You can then launch your instance from the AWS Management Console and start using your contact center.

After you create an Amazon Connect instance, you can claim a phone number to use for your contact center. After you claim a number, you can place a test call into your contact center to confirm that it is working correctly. Calls are handled in the contact center using the Contact Control Panel (CCP). The CCP is built into the Amazon Connect Contact Center Manager (CCM). For more information about how agents use the CCP, see Using the Contact Control Panel in the Amazon Connect User Guide.

You can edit the settings for your instance in the AWS Management Console. After you create your instance, you can access it by using the URL in the Access URL column. The access URL is the URL your agents, administrators, and managers use to log in to and access the CCM and the CCP. For more information, see Amazon Connect Instances (p. 1).

Note
If you use SAML-based authentication for identity management, your users must log in to your instance through your identity provider instead of using the access URL for your instance.

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.

Plan for User and Identity Management

Before you set up your Amazon Connect instance, you should decide how you want to manage your Amazon Connect users. You cannot change the option you select for identity management after you
create the instance. If you decide to change the option or directory you selected, you can delete the instance and create a new one. When you delete an instance, you lose all configuration settings and metrics data for it.

You can choose from one of the following supported identity management solutions supported in Amazon Connect:

- **Store users with Amazon Connect**—Choose this option if you want to create and manage user accounts within Amazon Connect. When you manage users in Amazon Connect, the user name and password for each user is specific to Amazon Connect. Users must remember a separate user name and password to log in to Amazon Connect.

- **Link to an existing directory**—Choose this option to use an existing directory. The directory must be associated with your account, set up in AWS Directory Service, and be active in the same Region in which you create your instance. If you plan to choose this option, you should prepare your directory before you create your Amazon Connect instance. For more information, see Use an Existing Directory for Amazon Connect Identity Management (p. 7).

- **SAML 2.0-based authentication**—Choose this option if you want to use your existing network identity provider to federate users with Amazon Connect. Users can only log in to Amazon Connect by using the link configured through your identity provider. If you plan to choose this option, you should configure your environment for SAML before you create your Amazon Connect instance. For more information, see Configure SAML for Identity Management in Amazon Connect (p. 8).

## Create an Amazon Connect Instance

You can create or add an instance as follows.

### To create an Amazon Connect instance

1. Open the Amazon Connect console at [https://console.aws.amazon.com/connect/](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:
   - To manage your users within Amazon Connect, choose **Store users within Amazon Connect**.
   - To use an existing directory where your users are managed, choose **Link to an existing directory**. For more information about using an existing directory, see Use an Existing Directory for Amazon Connect Identity Management (p. 7).
   - To use SAML-based authentication with your identity provider to federate users with Amazon Connect, choose **SAML 2.0-based authentication**. For more information about using SAML with Amazon Connect, see Configure SAML for Identity Management in Amazon Connect (p. 8).
4. For **Access URL**, enter an instance alias for your instance, and choose **Next step**.
   
   The name that you enter is displayed as the instance alias in the AWS Management 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 one time across all Amazon Connect instances and Regions. You cannot change the alias URL after 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 choose **Next step**.
   - If you chose **Link to an existing directory** for identity management, enter the user name for the account to use as the admin account for your instance, and choose **Next step**.

   If the user name that you enter does not exist in your directory, you can add it later.
• Choose **Skip this** to create an admin account later. To create an admin later, 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**. For more information, see [Data Storage](p. 16).

8. For **Step 5: Review and create**, review your settings and 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 keep your current phone number and use it with Amazon Connect, see [Port Your Current Phone Number](p. 13).

10. (Optional) Continue to configure your instance. For more information, see [Configuring Your Amazon Connect Instance](p. 16).

---

**Use an Existing Directory for Amazon Connect Identity Management**

If you are already using a [AWS Directory Service](https://aws.amazon.com/directoryservice/) 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 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 in Amazon Connect. For information about the costs associated with using AWS Directory Service, see [AWS Service Pricing Overview](https://aws.amazon.com/pricing/).

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

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

Configure SAML for Identity Management in Amazon Connect

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

Steps for configuring SAML include:

- Overview of Using SAML with Amazon Connect (p. 8)
- Enabling SAML-based Authentication for Amazon Connect (p. 9)
- Select SAML 2.0-based Authentication During Instance Creation (p. 9)
- Enable SAML Federation Between Your Identity Provider and AWS (p. 9)
- Use a Destination in Your Relay State URL (p. 11)
- Add users to Your Amazon Connect Instance (p. 12)
- SAML User Log in and Session Duration (p. 12)

Overview of Using SAML with Amazon Connect

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

SAML requests go through the following steps:

1. The user browses to an internal portal that includes a link to log in to Amazon Connect. The link is defined in the identity provider.
2. The federation service requests authentication from the organization's identity store.
3. The identity store authenticates the user and returns the authentication response to the federation service.
4. When authentication is successful, the federation service posts the SAML assertion to the user’s browser.
5. The user's browser posts the SAML assertion to the AWS Sign-In SAML endpoint (https://signin.aws.amazon.com/saml). AWS Sign-In receives the SAML request, processes the request, authenticates the user, and forwards the authentication token to the Amazon Connect service.
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 users to your Amazon Connect instance. Use the admin account created when you created your instance to log in and add users. The user names must exactly match the user name in your network directory and your identity provider.
4. Configure your identity provider for the SAML assertions, authentication response, and relay state. Users log in to your identity provider. When successful, they are redirected to your Amazon Connect instance and then federated through an IAM role, which allows access to use the Amazon Connect console or CCP.

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 an administrator user 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 admin user because passwords are managed through your existing directory. The admin user is created in Amazon Connect and assigned the Admin security profile.

You can log in to your Amazon Connect instance through your identity provider with the admin account specified to add additional users, assign security profiles, and manage configurations settings after you create your instance.

If you encounter an error and are unable to log in to your instance through your identity provider, you can log in as an administrator through the AWS Management Console to modify the admin user account.

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, except that for step 7 in the flow diagram in the topic, the client is sent to your Amazon Connect instance instead of landing at 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. You only need to create one IAM role for federation. The IAM role determines which permissions the users that log in through your identity provider have in AWS. In this case, the permissions are for accessing Amazon Connect. You can control the permissions to features of Amazon Connect by using security profiles in Amazon Connect. For more information, see Creating a Role for SAML 2.0 Federation (Console).

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

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

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

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

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

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

      ```json
      {
        "Version": "2012-10-17",
        "Statement": [
          {
            "Sid": "Statement2",
            "Effect": "Allow",
            "Action": "connect:GetFederationToken",
            "Resource": "*",
            "Condition": {
              "StringEquals": {
                "connect:InstanceId": "2fb42df9-78a2-2e74-d572-c8af67ed289b"
              }
            }
          }
        ]
      }
      ```
Use this policy to enable federation for multiple instances. Note the brackets around the listed instance IDs.

```json
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement2",
      "Effect": "Allow",
      "Action": "connect:GetFederationToken",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "connect:InstanceId": [
            "2fb42df9-78a2-2e74-d572-c8af67ed289b",
            "1234567-78a2-2e74-d572-c8af67ed289b"
          ]
        }
      }
    }]
}
```

4. After you create the policy, choose **Next:Review**, and then return to step 10 in the *To create a role for SAML-based federation* procedure in the Creating a Role for SAML 2.0 Federation (Console) topic.

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

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

5. Configure the relay state of your identity provider to point to your Amazon Connect instance. For the private preview release, 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.

## 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, such opening the CCP directly when an agent logs in, or displaying the real time metrics page when a call center manager logs in. The user must be assigned a security profile that grants access to that page in the instance. For example, if you want to send agents directly to the CCP when they log in, you can use a URL similar to the following for the relay state to go directly to the CCP when an agent logs in. You must use **URL encoding** for the destination value used in the URL:

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 attempts to log in to Amazon Connect and successfully 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](image)

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 also import all of your users by adding their information to a CSV file, and then using the import feature within Amazon Connect. If you plan to add users by uploading a CSV file, make sure that you use the template for SAML users, which 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 Log in and Session Duration

When you are using SAML for identity management in Amazon Connect, users must log in to Amazon Connect by first logging in to the identity provider you have configured in your network to use with Amazon Web Services. After authentication by the identity provider, a token for their session is created, and the user is redirected to your Amazon Connect instance and automatically logged in to Amazon Connect using single sign-on.

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

About Session Expiration

Amazon Connect sessions expire 10 hours after a user logs in. After 10 hours, users are automatically logged out, even if they are currently on a call. If you plan to have agents stay logged in for more than 10 hours, you should consider having agents log out of Amazon Connect and your identity provider, and then log in again through your identity provider before the session expires. 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.
Port Your Current Phone Number

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

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

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

To port your current phone number to Amazon Connect

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

About Porting Phone Numbers

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

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

The steps in the porting process are as follows:

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

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

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

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

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

**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. 18).

**Remove Your Amazon Connect Instance**

If you no longer want to use an Amazon Connect instance, you can delete it. If you delete an instance, the phone number claimed for the instance is released. You lose all settings, data, metrics, and reports associated with the instance.
Important
You cannot undo the deletion of an instance or restore settings or data from the instance after it is deleted.

To delete an 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 (p. 16)
- Telephony (p. 16)
- Data Storage (p. 16)
- Data Streaming (p. 17)
- Application Integration (p. 18)
- Contact Flows (p. 18)

**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.
Amazon Connect Administrator Guide
Application Integration

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 Amazon 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.
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 in Amazon CloudWatch Metrics

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 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 What is Amazon CloudWatch?

Amazon Connect Metrics Sent to CloudWatch

The following Amazon Connect metrics are sent to CloudWatch:

- **CallsBreachingConcurrencyQuota**—The number of voice calls that exceeded the concurrent active calls limit for the instance. This is a count of the number of calls that exceeded the limit, not the number of concurrent calls in excess of the limit.
- **CallBackNotDialableNumber**—The number of times a queued call back to a customer could not be dialed because the customer's number is in a country for which outbound calls are not allowed for the instance. The countries allowed for an instance are defined by the service limits.
- **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.
- **CallsPerInterval**—The number of voice calls, both inbound and outbound, received or placed per second in the instance.
- **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.
- **ConcurrentCallsPercentage**—The percentage of the concurrent active voice calls service limit used in the instance. This is calculated by ConcurrentCalls/ConfiguredConcurrentCallsLimit * 100.
- **ContactFlowErrors**—The number of times the error branch for a contact flow was executed.
- **ContactFlowFatalErrors**—The number of times a contact flow failed to execute due to a system error.
- **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.
- **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.
- **MisconfiguredPhoneNumbers**—The number of calls that failed because the phone number is not associated with a contact flow.
- **PublicSigningKeyUsage**—The number of times a contact flow security key (public signing key) was used to encrypt customer input in a contact flow.
• **QueueCapacityExceededError**—The number of calls that were rejected because the queue was full.
• **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.
• **ThrottledCalls**—The number of voice calls that were throttled by the Amazon Connect service because the rate of calls per second (Callrate) exceeded the configured limit for the instance.
• **ToInstancePacketLossRate**—The ratio of packet loss for calls in the instance, reported every 10 seconds. Each data point is between 0 and 1, which represents the ratio of packets lost for the instance.

Amazon Connect CloudWatch Metrics Dimensions

In CloudWatch, a dimension is a name/value pair that uniquely identifies a metric. In the dashboard, metrics are grouped under dimensions. The following dimensions are used in the CloudWatch dashboard for Amazon Connect metrics. When you view metrics, only metrics for which there is data are displayed in the dashboard. If there is no activity during the refresh interval for which there is a metric, then no data from your instance is displayed in the dashboard. The following dimensions are used for Amazon Connect metrics in CloudWatch.

**Instance ID, Participant, Stream Type, Type of Connection**

This dimension contains metrics about connections to your instance, and includes:

• **ToInstancePacketLossRate**

**Contact Flow Metrics Dimension**

This dimension contains metrics about contact flows in your instance, and includes:

• **CallRecordingUploadError**
• **ContactFlowErrors**
• **ContactFlowFatalErrors**
• **MisconfiguredPhoneNumbers**
• **PublicSigningKeyUsage**

**Queue Metrics Dimension**

This dimension contains metrics about queues in your instance, and includes:

• **CallBackNotDialableNumber**
• **LongestQueueWaitTime**
• **QueueCapacityExceededError**
• **QueueSize**

**Instance metrics Dimension**

This dimension contains metrics about voice calls and call recordings in your instance, and includes:
• CallsBreachingConcurrencyQuota
• CallsPerInterval
• ConcurrentCalls
• ConcurrentCallsPercentage
• MissedCalls
• ThrottledCalls
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:

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

The request is divided into three parts:

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

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:

```javascript
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:

```javascript
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:

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

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

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

```json
{
    "Name": "CustomerName",
    "Address": "1234 Main Road",
    "CallerType": "Patient"
}
```
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 from the most recently invoked function. To use the response from a function before a subsequent function is invoked, the response must be saved as a contact attribute, or passed as a parameter to the next function.

**Access 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 use these features.

3. Whitelist your Salesforce Visualforce domain URL using the directions in Application Integration (p. 18). 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:
  
  ```json
  {"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 update history for Amazon Connect.

<table>
<thead>
<tr>
<th>Change</th>
<th>Description</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Updated topic about metrics sent to Amazon CloudWatch Logs.</td>
<td>Updated the topic Monitoring Amazon Connect in Amazon CloudWatch Metrics (p. 20) to include additional metrics and update the descriptions for all metrics.</td>
<td>April 19, 2018</td>
</tr>
<tr>
<td>Added content for using SAML for identity management.</td>
<td>New content added that describes how to configure your instance to use SAML for identity management to enable single sign-on. For more information, see Configure SAML for Identity Management in Amazon Connect (p. 8).</td>
<td>March 30, 2018</td>
</tr>
<tr>
<td>Updated topic on using AWS Lambda functions with Amazon Connect</td>
<td>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. 23).</td>
<td>January 05, 2018</td>
</tr>
<tr>
<td>Added Port Your Current Phone Number</td>
<td>Added information about how to port your current telephone number to Amazon Connect. For more information, see Port Your Current Phone Number (p. 13).</td>
<td>November 10, 2017</td>
</tr>
<tr>
<td>Updated Salesforce integration information</td>
<td>Updated the steps to integrate Amazon Connect with Salesforce to clarify settings. For more information, see Amazon Connect and Salesforce Integration (p. 27).</td>
<td>October 27, 2017</td>
</tr>
<tr>
<td>Initial release</td>
<td>Initial release of the Amazon Connect Administrator Guide.</td>
<td>March 28, 2017</td>
</tr>
</tbody>
</table>