Get Started with Service Cloud Voice with Partner Telephony from Amazon Connect

Salesforce, Spring '24

Last updated: March 22, 2024

CONTENTS

SERVICE CLOUD VOICE WITH PARTNER TELEPHONY FROM AMAZON CONNECT

Service Cloud Voice with Partner Telephony from Amazon Connect lets you integrate your own Amazon Connect instance with Service Cloud Voice. This document is for customers who set up Service Cloud Voice with Partner Telephony from Amazon Connect before Spring '22.

Tip: For the best end-to-end Voice experience and to ensure you always have the latest Voice features, use a new Amazon Connect Instance or use an existing Amazon Connect instance integrated by Salesforce.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

SEE ALSO:

Set Up Service Cloud Voice with Partner Telephony from Amazon Connect

Before You Start

Review these tips so setup and configuration go smoothly.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

Important: Service Cloud Voice with Partner Telephony from Amazon Connect is different from the default Service Cloud Voice product. In the default Voice product, Salesforce handles some of the configuration tasks for you. If that's what you want to set up, we've got you covered—see Set Up Service Cloud Voice with Amazon Connect.

Important: This document is for customers who set up Service Cloud Voice with Partner Telephony from Amazon Connect before Spring '22. If you're setting up Service Cloud Voice with the Spring '22 release or later, use the simplified process that is described in Set Up Service Cloud Voice with Partner Telephony from Amazon Connect in Salesforce Help.

First, complete the Service Cloud Voice Planning Checklist on page 3.

We strongly suggest that you print out and read through this entire guide before starting the setup process. Keep a notepad handy where you can copy and paste the values for some of the instructions. You need the values for later setup steps. We mention where to write down certain information.

This guide assumes that you're familiar with Amazon Web Services (AWS) services, including Amazon Connect, AWS Lambda, and Amazon Identity and Access Management (IAM). The guide walks you through the basic steps to configure Amazon Connect to work with Voice and provides links to AWS's product documentation. For comprehensive info about how to set up Amazon Connect and other AWS services, see the AWS Documentation: https://docs.aws.amazon.com/.

This guide assumes that you're familiar with Salesforce Service Cloud and Omni-Channel. For comprehensive documentation on Salesforce, see https://help.salesforce.com/.

This guide assumes that you already have:

- An AWS account
- An AWS root user or administrator privileges. You need administrative access to configure AWS and Amazon Connect.
- An Amazon Connect instance
- A Salesforce org where Service Cloud is enabled
- Salesforce administrator privileges. You need administrative access to configure Salesforce.

Now that you have your Salesforce org, Service Cloud Voice Partner license, and AWS account with an Amazon Connect instance ready, let's get started.

SEE ALSO:

Salesforce Help: Voice Limits and Limitations

Salesforce Help: Plan Your Voice Contact Center

External Link: AWS Documentation

Service Cloud Voice Planning Checklist

Before you begin setting up Service Cloud Voice with Partner Telephony from Amazon Connect, take care of these essential planning steps. They highlight best practices for using Voice and help you understand what to expect during your Voice rollout.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

Step	Where to Learn More
Step 1: Review Voice's key concepts and limitations. Understand the terms we use when talking about telephony, and read through the Voice limits and limitations.	*Salesforce Help:* Voice Key Concepts *Salesforce Help:*: Voice Limits and Limitations Not all Voice concepts, like connected apps or limitations, apply to Service Cloud Voice with Partner Telephony from Amazon Connect. For a walkthrough of key AWS settings for Service Cloud Voice, check the onboarding wizard
Step 2: Learn about your telephony model. Know where to find documentation for Amazon Connect.	*Amazon Help:* Amazon Connect Administrator Guide
Step 3: Consider your service quotas. If your contact center uses Amazon Connect telephony, decide whether to increase your Amazon service quotas. These quotas control things such as: • The maximum number of concurrent active calls • The maximum number of transcription jobs • The list of countries that can be called in outbound calls If you're not sure whether to adjust your quotas, ask an AWS Solution Architect for help.	*Salesforce Help:*: Increase Amazon Service Quotas *Amazon Help:*Amazon Connect Service Quotas For the default list of countries supported for outbound calls, see the section named "Countries you can call."
Step 4: Plan your phone number porting. Decide whether and how to use your existing phone number or numbers in your new contact center. Phone number porting is highly regulated, can't be rushed, and requires you to submit a porting request with your telephony provider many weeks in advance. To avoid any anxiety about the porting timeline, we recommend taking this approach: • Claim a new phone number for testing and production. • Forward traffic to that number from your original production phone number until testing is complete.	*Amazon Help:* Port Your Current Phone Number

Step	Where to Learn More
- Port the original production phone number from your previous telephony provider to your new one.	
Step 5: Design your environment and testing strategy. Decide how many sandbox orgs you need. If applicable, decide how many Amazon Connect test instances you need. Then, develop a plan to migrate data between production and test environments.	*Salesforce Help:* Test Your Voice Implementation
Step 6: Review AWS networking requirements. To avoid blocking important ports, review Amazon's networking guidance.	*Amazon Help:* Set Up Your Network
Step 7: Plan your routing requirements. Your interactive voice response (IVR) determines how customers navigate your phone support and get routed to agents. Consider: - Your current routing logic - How you want to improve it using Amazon Connect routing profiles and queues, or equivalent features from your telephony provider. - Available pre-built solutions We recommend starting simple by using the contact flows provided by Salesforce. These contact flows demonstrate good IVR practices. You can then build them out to move toward your ideal IVR, testing each change that you make.	*Service Cloud Voice Implementation Guide:* Using Service Cloud Voice Contact Flows

After you complete these planning steps, it's time to start your setup.

Configure Your Amazon Connect Instance for Voice

Follow these steps to configure your Amazon Connect instance to work with Service Cloud Voice. The majority of these steps take place in the AWS Console or in Amazon Connect. These instructions are for customers who are providing their own Amazon Connect instance.

1. Generate a Self-Signed Certificate with OpenSSL

   Use OpenSSL to generate an RSA private key and two certificates. You need one certificate to set up a secure connection between Amazon Connect and Salesforce and another certificate for the REST API integration. Repeat the steps to create both certificates.

2. Connect Your Amazon Connect Instance to Salesforce

   Configure your Amazon Connect instance and Salesforce org so they can connect with each other. Set up single sign-on (SSO) so agents can log in to the Amazon Connect instance through Service Cloud Voice. Configure data streaming and services so agents can see real-time transcription.

3. Configure Users in Amazon Connect

   Add users to your Voice contact center in Salesforce and in your Amazon Connect instance. This task assumes that you already have users in your Salesforce org that you want to add to the Amazon Connect contact center. If not, create some users in Salesforce.

4. Configure the Lambda Functions and Contact Flows for Voice
   Follow these steps to use the Salesforce-provided Lambda functions in your Amazon Connect instance. After setting up the Lambda functions, import the Service Cloud Voice sample contact flows to your Amazon Connect instance.
5. Turn On AWS Streaming Services
   Enable Contact Trace Records (CTR) data streaming and live media streaming to use real-time transcription in Salesforce. If you already have CTR enabled, it's not necessary to recreate these resources.
6. Configure Contact Lens Transcription
   Complete these steps to ensure your voice calls are transcribed.
7. Configure Call Recording
   Optionally, follow these steps to turn on automatic call recording and to allow support agents to pause call recording.

Generate a Self-Signed Certificate with OpenSSL

Use OpenSSL to generate an RSA private key and two certificates. You need one certificate to set up a secure connection between Amazon Connect and Salesforce and another certificate for the REST API integration. Repeat the steps to create both certificates.

Important: OpenSSL v1.1.1 must be used.

Important: The certificate expires after 1 year by default. You can change the expiration date. When the certificate expires, AWS services can't talk with your Voice contact center. To ensure uninterrupted service, generate and upload a new certificate before the old certificate expires.

1. Create a folder for holding the generated certificate:

```
$ mkdir certificates
```

2. Change the current directory to the certificates folder:

```
$ cd certificates
```

3. In the certificates folder, specify a password and generate an RSA private key. Where it says `<your_password>`, specify your own password.

```
$ openssl genrsa -des3 -passout pass:<your_password> -out server.pass.key 2048
```

4. Create a key file from the `server.pass.key` file using the password that you created in the previous step:

```
$ openssl rsa -passin pass:<your_password> -in server.pass.key -out server.key
```

5. Delete the `server.pass.key`:

```
$ rm server.pass.key
```

6. Request and generate the certificate:

```
$ openssl req -new -key server.key -out server.csr
```

7. Enter the required information.
   a. Enter your company details.
   b. When prompted for the challenge password, press **Enter**.

The Certificate Authorities use this password to authenticate the certificate owner when they want to revoke their certificate. You can't revoke it via the Certificate Revocation List (CRL) because it's a self-signed certificate.

8. Generate the SSL certificate:

```
$ openssl x509 -req -sha256 -days 365 -in server.csr -signkey server.key -out server.crt
```

Connect Your Amazon Connect Instance to Salesforce

Configure your Amazon Connect instance and Salesforce org so they can connect with each other. Set up single sign-on (SSO) so agents can log in to the Amazon Connect instance through Service Cloud Voice. Configure data streaming and services so agents can see real-time transcription.

Important: This guide assumes that you already have an AWS account. If you don't, create one. You need an AWS account before you can create and configure an Amazon Connect database instance.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

Create an Amazon Connect Instance

If you don't already have an Amazon Connect instance to use with Voice, log in to your AWS account and create an Amazon Connect instance.

Configure Salesforce as Your Identity Provider

Let Salesforce act as your identity provider for the telephony system. This step creates a metadata file that you need in order to configure the AWS Identity and Access Management settings. You need your custom domain name for this step.

Configure AWS Identity and Access Management (IAM) for Voice

AWS Identity and Access Management (IAM) lets you manage access to AWS services. You need the metadata XML file that you created for the identity provider and the Amazon Resource Name (ARN) for your Amazon Connect instance. These instructions are for customers who set up Service Cloud Voice with Partner Telephony from Amazon Connect before Spring '22.

Add Your Domain to the Approved Origins List in Amazon Connect

The approved origins list tells Amazon Connect the URL to connect to.

Create an Amazon Connect Relay State URL

Create an Amazon Connect Relay State URL that your Salesforce org can use to set up single sign-on (SSO).

Create a Connected App for Amazon Connect

In Salesforce, create a connected app that connects Salesforce to Amazon Connect. Then, set up single sign-on (SSO) so that your agents can log in to the Amazon Connect instance via the Salesforce Omni-Channel utility.

Save Your Private Key to the AWS Parameter Store

Add the private key from your self-signed certificate to the AWS parameter store.

Create an Amazon Connect Instance

If you don't already have an Amazon Connect instance to use with Voice, log in to your AWS account and create an Amazon Connect instance.

The *Get Started with Service Cloud Voice for Partner Telephony from Amazon Connect* guide is intended for customers who already have an Amazon Connect instance that they want to use with Voice. This guide explains the basic steps to configure a Connect instance to work with Voice, but it doesn't provide comprehensive instructions for configuring Amazon Connect. For detailed documentation on Amazon Connect, see the *Amazon Help:* Amazon Connect Administrator Guide.

Important: The Amazon Connect instance must use SAML 2.0 based authentication. If your existing Connect instance already is configured to use SAML 2.0, you can skip this step. If your existing Connect instance *doesn't* use SAML 2.0, create another instance because you can't change the authentication setting after the instance is created.

This guide assumes that you already have an AWS account. If not, create one. You need an AWS account before you can create and configure an Amazon Connect database instance.

1. Log in to the AWS Management Console.
2. In the search bar, enter Amazon Connect, then select Amazon Connect.
3. Click **Add an instance**.
4. In the top-right corner, select the region where you want the instance to be created. Select a region closest to where your contact center is physically located.

   For example, if your contact center is in Los Angeles, select the *US-West (Oregon) us-west-2* region. Regions where Amazon Connect isn't available are grayed out.

5. For Identity Management, select **SAML 2.0-based authentication**.
6. In the **Access URL** field, enter a unique name for your instance, then click **Next**.
7. For the Administrator, optionally create an admin or skip this step. You can create or add an admin later.
8. For Telephony Options, select **I want to handle incoming calls with Amazon Connect** and **I want to make outbound calls with Amazon Connect**, then click **Next**.
9. For Data Storage, optionally customize where to store call recordings and exported reports. To accept the default values, click **Next**.
10. For Review and Create, check the details of your Amazon Connect instance and click **Create Instance**.

    A confirmation is displayed when the instance is created.

SEE ALSO:

External Link: Amazon Connect Administrator Guide: Create an Amazon Connect instance

Configure Salesforce as Your Identity Provider

Let Salesforce act as your identity provider for the telephony system. This step creates a metadata file that you need in order to configure the AWS Identity and Access Management settings. You need your custom domain name for this step.

1. Log in to Salesforce with your custom domain name.
2. From Setup, in the Quick Find box, enter *`Identity Provider`*, then select **Identity Provider**.
3. Click **Enable Identity Provider**.
4. Select a certificate from the dropdown menu.
5. Save your changes.
6. Click **Download Metadata**, and then save the metadata XML file to your computer.

   Tip: You need the metadata file later when you configure AWS identity and access management settings.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

Define and modify identity providers and service providers:

- Customize Application

Configure AWS Identity and Access Management (IAM) for Voice

AWS Identity and Access Management (IAM) lets you manage access to AWS services. You need the metadata XML file that you created for the identity provider and the Amazon Resource Name (ARN) for your Amazon Connect instance. These instructions are for customers who set up Service Cloud Voice with Partner Telephony from Amazon Connect before Spring '22.

Before you start, review the AWS IAM Best Practices Guide at https://aws.amazon.com/iam/.

Tip: You need the ARN for your Amazon Connect instance so you can create a policy:

1. Go to Amazon Connect and select your instance.
2. Click **Overview**.
3. The ARN is shown in the Overview section. Copy and paste this value to your notepad.

To configure access to AWS, follow these steps:

1. Create a policy to manage access to AWS services.
   a. Go to Identity and Access Management (IAM) in AWS.
   b. Under Access management, select **Policies**.
   c. Click **Create policy**.
      The Create policy page opens.
   d. Click the JSON tab.
   e. Copy and paste the following JSON policy, but replace **YOUR ARN** with your Amazon Connect instance's ARN.

      Don't change the userid string.

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
          "Sid": "Statement1",
          "Effect": "Allow",
          "Action": "connect:GetFederationToken",
          "Resource": ["**YOUR ARN**/user/${aws:userid}"
          ]

       }
    ]
}
```

f. Click **Next: Tag**. then click **Next: Permission**.

g. Click **Next: Review**.

h. For Name, enter a name such as *`AmazonConnectSFDCPolicy`*. Optionally enter a description.

i. Click **Create policy**.

The policy is created.

2. Add an identity provider.

   a. Under Access management, select **Identity Providers**.

   b. Click **Add Provider**.

   c. Fill out the fields as follows:

      - For **Provider Type**, select *`SAML`*.
      - For **Provider Name**, enter *`AmazonConnectSFDC`*
      - For **Metadata Document**, click **Choose File** and select the Salesforce identity provider metadata file.

   d. Click **Add provider**.
   A banner is displayed asking you to assign a role.

3. Create a new role to assign to the identity provider.

   a. Click **Assign role**.
   A window is displayed asking you to create a role or use an existing role.

   b. Click **Create a new role**.

      - In the **Select type of trusted entity** section, select *`SAML 2.0 federation`*.
      - Select **Allow programmatic and AWS Management Console access**. The Attribute and Value fields are automatically populated.

   c. Click **Next: Permissions**.

   d. Attach the policy to the role.

      - In the search box, enter the name of the policy that you created in Step 1.
      - Select the policy.

   e. Click **Next: Tags**, and then click **Next: Review**.

   f. In the **Role name** field, enter a name such as *`MyCallCenter1-ConnectCallRole`*. Use the following name format:`{contact center internal name}-ConnectCallRole`.

   g. In the **Description** field, optionally enter a description.

   h. Click **Create role**.

The role is created. You need this role to set up the connected app in Salesforce.

SEE ALSO:

External Link: AWS Identity and Access Management: Best practices

Set Up Service Cloud Voice with Partner Telephony from Amazon Connect

Add Your Domain to the Approved Origins List in Amazon Connect

The approved origins list tells Amazon Connect the URL to connect to.

You need your My Domain URL and the Lightning Domain URL.

To find your My Domain domain name, log in to Salesforce. From Setup, in the Quick Find box, enter *`My Domain`*, and then select **My Domain**. Your My Domain name is the value for the `Current My Domain URL` field. For example, *`https://[YourDomainName].my.salesforce.com`*.

To find your Lightning Domain name, log in to Salesforce. Your Lightning domain name is the URL host name in your browser. For example, *`https://[YourDomainName].lightning.force.com`*.

1. Log in to Amazon Connect.
2. Select your instance.
3. Click **Approved origins**.
4. In the **Application integration** section, click **+ Add origin**.
5. Enter your My Domain URL, and then click **Add**.

   For example, *`https://[YourDomainName].my.salesforce.com`*.

6. Enter your Lightning Domain URL, and then click **Add**.

   For example, *`https://[YourDomainName].lightning.force.com`*.

Create an Amazon Connect Relay State URL

Create an Amazon Connect Relay State URL that your Salesforce org can use to set up single sign-on (SSO).

The Relay State URL uses this format, where *`**instanceId**`* is replaced with your Amazon Connect instance Id and *`**regionId**`* is replaced with your Amazon region Id: `https://**regionId**.console.aws.amazon.com/connect/federate/**instanceId**`.

1. Replace the **instanceId** with your instance Id.

   To find your Amazon Connect instance ARN:

   a. Open a tab in your browser and navigate to the Amazon Connect Console.

   b. Click the name (alias) of your instance.

   c. From the Instance ARN, copy the portion after 'instance/'.

2. Replace **regionId** with your region Id.

   To find your region, look at the ARN for your Connect instance. For example: `arn:aws:connect:us-east-1:xxxxxxx:instance/<instanceid>`. Alternatively, you can find your region on the AWS console page in the overview section.

3. After you replace the `**instanceId**` and the `**regionId**`, the updated Relay State URL looks like this: `https://region-id.console.aws.amazon.com/connect/federate/instance-id`.

   Tip: Copy and paste the Relay State URL to your notepad. You need the Relay State URL later on for the Amazon Connect Call Center Configuration.

Create a Connected App for Amazon Connect

In Salesforce, create a connected app that connects Salesforce to Amazon Connect. Then, set up single sign-on (SSO) so that your agents can log in to the Amazon Connect instance via the Salesforce Omni-Channel utility.

Tip: Before you start, get the Amazon Resource Names (ARN) for the AmazonConnectSFDC and AmazonConnectSSO_SFDC role from the AWS Identity and Access Management console.

1. Go to Identity and Access Management in AWS.
2. Under Access management, click **Identity providers**, and then select `AmazonConnectSFDC`.
3. The ARN is shown in the Summary section. Copy and paste this value to your notepad.
4. Click **Identity providers**, and then select the `AmazonConnectSSO_SFDC` role.
5. The ARN is shown in the Summary section. Copy and paste this value to your notepad.

After you have the ARNs, follow these steps to create the connected app and SSO URL.

1. Create the connected app in Salesforce.
   - a. From Setup, in the Quick Find box, enter `App Manager`, and then select **App Manager**.
   - b. Click **New Connected App**.
   - c. In the Basic Information section, specify the **Connected App Name**, **API Name** (this field is automatically populated), and **Contact Email**.
   - d. In the Web App Settings section, leave the **Start URL** field empty.
   - e. Select **Enable SAML**.
   - f. In the **Entity ID** field, enter `AmazonConnectSFDC`.
   - g. In the **ACS URL** field, enter `https://signin.aws.amazon.com/saml`.
   - h. In the **Subject Type** field, select **Persistent ID**.
   - i. In the **Name ID Format** field, select `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
   - j. Save your work.
     The connected app is created.
2. Create a custom attribute for the attribute key.
   - a. In the **Custom Attributes** section, click **New**.
   - b. In the **Key** field, enter `https://aws.amazon.com/SAML/Attributes/RoleSessionName`.
   - c. In the **Value** field, enter `$User.Id & '@' & $Organization.Id`.
   - d. Save your work.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To read, create, update, or delete connected apps:

- Customize Application AND either

  Modify All Data OR Manage Connected Apps

To update Profiles, Permission Sets, and Service Provider SAML Attributes:

- Customize Application AND Modify All Data AND Manage Profiles and Permission Sets

To install and uninstall connected apps:

- Customize Application AND either

  Modify All Data OR Manage Connected Apps

3. To create another customer attribute, click **New**.
   a. In the Key field, enter `https://aws.amazon.com/SAML/Attributes/Role`.
   b. In the Value field, enter the AmazonConnectSFDC IdP ARN and the AmazonConnectSSO_SFDC role ARN, separated by a comma.

      For example, `'{AmazonConnectSFDC IdP ARN}' &',' &'{AmazonConnectSSO_SFDC role ARN}'`.

      It's easiest to copy and paste these values. Make sure to include the apostrophes and to remove the curly brackets.
   c. Save your work.
      Now there are two attributes listed in the Custom Attributes section.
4. Click **Manage**. A page opens that contains the SAML Login Information section.

   Tip: Copy and paste the value in the IdP-Initiated Login URL field into your notepad.
5. Click **Manage Profiles**.
   a. Select a profile from the list. For example, select System Administrator.
   b. Save your work.
6. Test that your IdP settings are working.
   a. Open a new tab in your browser and navigate to the IdP-Initiated Login URL that you created in Step 4. The browser redirects to the AWS Console.
   b. To expand your identity, click the dropdown arrow at the top-right corner of the page.

      Tip: Write down your federated login in your notepad. The federated login consists of the role name—here, AmazonConnectSSO_SFDC—and the email address that you use to log in to Salesforce. You need this information later to use to create an Amazon Connect user.
7. To set up OAuth between AWS Lambda and Salesforce, create another connected app by following these steps. However, it's not necessary to create another private key or certificate. You already did that earlier in the flow.

Your Amazon Connect instance and Salesforce org are connected. Now that you set up Salesforce SSO with a relay state, you can use Salesforce SSO to open the AWS Console.

SEE ALSO:

Salesforce Help: Connected Apps

Save Your Private Key to the AWS Parameter Store

Add the private key from your self-signed certificate to the AWS parameter store.

Tip: Copy the private key from your notepad so it's easy to paste it into AWS.

1. In the AWS Management Console, search for Systems Manager, and then click **Systems Manager**.
2. Under Application Management, click **Parameter Store**.
3. Click **Create parameter**.
4. For Name, enter a name such as `telephony-integration-auth-private-key`.
5. For Tier, select **Standard**.
6. For Type, select **SecureString**.

7. For KMS key source, select **My current account**.
8. For KMS Key ID, if you have another KMS key, this field is automatically populated.
9. For Value, paste the `server.key` private key from the self-signed certificate that you created at the beginning of this guide.
10. Click **Create parameter**.

Configure Users in Amazon Connect

Add users to your Voice contact center in Salesforce and in your Amazon Connect instance. This task assumes that you already have users in your Salesforce org that you want to add to the Amazon Connect contact center. If not, create some users in Salesforce.

You can use the Salesforce Data Loader to export existing Salesforce users to a CSV file that you can use to upload users to Amazon Connect.

Important: Amazon Connect and Salesforce use email addresses as usernames. Amazon calls these "user logins," while Salesforce uses the term "username."

When you modify the CSV file, make sure that the value for Amazon Connect is the same for Salesforce. The email address that an agent uses to log in to Amazon Connect must be the same as the email address that the agent uses to log in to Salesforce.

Next, create a routing profile in Amazon Connect. Upload the users to Amazon Connect, and then apply the routing profile to the users.

1. In Salesforce, export the user records via the Data Loader.
2. In the AWS Management Console, click **Log in for emergency access** on the Overview tab to go to the Amazon Connect Console.
3. Create a routing profile. This profile is used to route calls to users.
   a. In the navigation bar, hover over **Users**, and then select **Routing profiles**.
   b. Click **Add new profile**, and then create a routing profile.

      The routing profile name can only contain underscores and alphanumeric characters. It must be unique, begin with a letter, not include spaces, not end with an underscore, and not contain two consecutive underscores.
4. Upload the Salesforce users to Amazon Connect.
   a. Click **Users**.
   b. Click **User management**.
   c. Click **Add new users**.
   d. Select **Upload my users from a template (csv)**, and then click the template hyperlink. A CSV template file is downloaded. Then click **Next**.

      Edit the CSV template:

      a. In the CVS file, create a column for the userName that uses this format: `$User.Id & '@' & $Organization.Id`.
      b. Copy the user information from the exported user records to the CSV file.

         Note: Enter the 15-character, case-sensitive user ID.
      c. In the CSV template, specify these settings:

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To export records using the Salesforce Data Loader:
- Read on the records

To export all records using the Salesforce Data Loader:
- Read on the records

a. Make sure that the Salesforce username is matched to the correct Amazon Connect login name. For details, see the preceding note.

b. For Set Routing Profile, you can select the default `Basic Routing Profile` or select the routing profile that you created in the previous steps.

c. For Set Security Profile, you can select `Agent` or `Admin`.

e. Click **Choose file**, and then select the CSV to upload.

f. Click **Upload and verify**.

g. Click **Create users**.

You're not done adding users yet. When you finish configuring Amazon Connect and start the Voice setup process in Salesforce, there are a few more steps to add users to the Voice contact center.

SEE ALSO:

Salesforce Help: Data Loader

Salesforce Help: Exporting Data

Assign Contact Center Permission Sets for Partner Telephony

Add and Remove Users in Your Partner Telephony Contact Center

Configure the Lambda Functions and Contact Flows for Voice

Follow these steps to use the Salesforce-provided Lambda functions in your Amazon Connect instance. After setting up the Lambda functions, import the Service Cloud Voice sample contact flows to your Amazon Connect instance.

Create an Execution Role for the Voice Lambda Functions

The execution role gives the Service Cloud Voice Lambda functions permission to access AWS services and resources.

Deploy the Service Cloud Voice Lambda Functions in Your Amazon Connect Instance

To deploy the Lambda functions, install the ServiceCloudVoiceLambdas serverless application, add the Lambda functions to the Connect instance, and select the execution role for the Lambda function.

Set the AWS Lambda Environment Variables

Specify the AWS Lambda function environment variables with these values. Environment variables adjust the Lambda function's behavior using a key-value string pair.

Import the Voice Contact Flows into Amazon Connect

Contact flows define the user experience for callers. Salesforce provides sample Amazon Connect contact flows that use the AWS Lambda functions you configured in the previous section. Salesforce provides these sample contact flows for you to use as a starting point to build your interactive voice response (IVR) experiences.

Create an Execution Role for the Voice Lambda Functions

The execution role gives the Service Cloud Voice Lambda functions permission to access AWS services and resources.

1. In AWS, log in to the Identity and Access Management console.
2. Go to **Roles**.
3. Click **Create Roles**.

4. In the `Select type of trusted entity` section, click **AWS Service**.
5. In the `Choose the service that will use this role` section, click **Lambda**.
6. Click **Next: Permissions**.
7. Search for and attach the *`AmazonSSMReadOnlyAccess`* and *`AWSLambdaENIManagementAccess`* permission policies.
8. Click **Next: Tags**.
9. Click **Next: Review page** and enter a role name such as *`SCV_Lambda_Execution`*.
10. Click **Create role**.

Deploy the Service Cloud Voice Lambda Functions in Your Amazon Connect Instance

To deploy the Lambda functions, install the ServiceCloudVoiceLambdas serverless application, add the Lambda functions to the Connect instance, and select the execution role for the Lambda function.

Gather this information:

- Your Salesforce org Id
- The CallCenter API Name, which is the internal name of the partner telephony contact center you created.
- The telephony integration private key that you created in Generate a Self-Signed Certificate with OpenSSL on page 5

Note: When Salesforce publishes a new version of the serverless application, a notification is shown in the AWS console.

1. Install the service-cloud-voice serverless application in AWS:
   a. Go to the **Serverless Application Repository**.
   b. Click **Available applications**.
   c. Enter *`ServiceCloudVoiceLambdas`* as the application name.
   d. Click **ServiceCloudVoiceLambdas**, and view and modify these application settings:
      - SalesforceOrgId: Add your Salesforce Organization ID that you want to connect to the service-cloud-voice serverless application.
      - CallCenterApiName: Update this value to the name of the Call Center in your Salesforce org.
      - TelephonyIntegrationAuthPrivateKeySSMParamName: Update this value to the name of the private key.

      Other settings don't require any updates or changes.
   e. Click **Deploy**. Before moving on, wait until your Lambda functions are deployed. This process can take a couple minutes.
2. Add the Lambda functions to your Amazon Connect instance:
   a. Go to your Amazon Connect instance page.
   b. From the navigation bar on the left, select **Contact flows**, and then scroll down to the AWS Lambda section.
   c. For the **Function** field, open the dropdown menu, select a function, and then click **+Add Lambda Function**.

      These functions appear in the list:
      - *`<Contact Center Name>-CTRDataSyncFunction`*
      - *`<Contact Center Name>-kvsConsumerTrigger`*
      - *`<Contact Center Name>-kvsTranscriber`*
      - *`<Contact Center Name>-InvokeSalesforceRestApiFunction`*
      - *`<Contact Center Name>-InvokeTelephonyIntegrationApiFunction`*

   d. Repeat step 2c for *<Contact Center Name>-kvsConsumerTrigger*, *<Contact Center Name>-InvokeSalesforceRestApiFunction*, and *<Contact Center Name>-InvokeTelephonyIntegrationApiFunction*. Not all Lambda functions are required for contact flows.

3. Edit the permissions for the InvokeTelephonyIntegrationApiFunction Lambda function:
   a. Go to AWS Lambda.
   b. In the **Functions** list, select the *<Contact Center Name>-InvokeTelephonyIntegrationApiFunction*.
   c. Click the **Configuration** tab.
   d. Click **Permissions**.
   e. In the **Execution role** section, click **Edit**.
4. In the **Existing role** field, select the role called *SCV_Lambda_Execution*, and then save your work.

Set the AWS Lambda Environment Variables

Specify the AWS Lambda function environment variables with these values. Environment variables adjust the Lambda function's behavior using a key-value string pair.

To set the environment variables in the AWS Lambda console, follow these steps:

1. In the AWS Management Console, go to the Lambda console.
2. Click **Functions**.
3. Update each function.
   a. Select a function.
   b. Under Environment variables, click **Edit**.
   c. Click **Add environment variable**.
   d. Enter a key and value as specified in the tables.
   e. Save your work.
4. To set the environmental variables for each Lambda function, repeat steps 3a–3e.

Table 1: InvokeTelephonyIntegrationApiFunction Environment Variables

Key	Value
CALL_CENTER_API_NAME	Internal name of your call center
PRIVATE_KEY_PARAM_NAME	*telephony-integration-auth-private-key*
SALESFORCE_ORG_ID	Your Salesforce org Id You can find the org Id on the Company information page in Salesforce.
SCRT_ENDPOINT_BASE	*https://{Org my domain}.my.salesforce-scrt.com/telephony/v1* Where *{Org my domain}* is your custom domain

Table 2: CTRDataSyncFunction Environment Variables

Key	Value
INVOKE_TELEPHONY_INTEGRATION_API_ARN	ARN for the InvokeTelephonyIntegrationApiFunction

Table 3: kvsConsumerTrigger Environment Variables

Key	Value
transcriptionFunction	ARN for the kvsTranscriber function

Table 4: kvsTranscriber Environment Variables

Key	Value
APP_REGION	Your Amazon Connect instance's region code
AUDIENCE	*https://scrt.salesforce.com*
CALL_CENTER_API_NAME	Internal name of your call center
PRIVATE_KEY_PARAM_NAME	*telephony-integration-auth-private-key*
SALESFORCE_ORG_ID	Your Salesforce org Id You can find the org Id on the Company information page in Salesforce.
SCRT_ENDPOINT_BASE	*https://{Org my domain}.my.salesforce-scrt.com/telephony/v1* Where *{Org my domain}* is your custom domain
START_SELECTOR_TYPE	NOW
TRANSCRIBE_REGION	Transcription region code

Table 5: InvokeSalesforceRestAPIFunction Environment Variables

Key	Value
ACCESS_TOKEN_PARAM_NAME	*salesforce-rest-api-access-token*
AUDIENCE	If production org, enter: *https://login.salesforce.com*. If sandbox, enter: *https://test.salesforce.com*.
CONSUMER_KEY_PARAM_NAME	*salesforce-rest-api-auth-consumer-key* Where the consumer key is imported from the connected app's digital signature
PRIVATE_KEY_PARAM_NAME	*salesforce-rest-api-auth-private-key* This private certificate is the second one you created in the setup.

Key	Value
SALESFORCE_AUTH_ENDPOINT	*https://voicetest.my.stmfa.stm.salesforce.com/services/oauth2/token*
SCRT_ENDPOINT_BASE	*https://{Org my domain}.my.salesforce-scrt.com/telephony/v1* Where *{Org my domain}* is your custom domain
SALESFORCE_REST_API_ENDPOINT_BASE	*https://{My Domain URL}/services/data/v49.0* Note: To use versions newer than v49.0, update the end of the URL with the version number.
SUBJECT	Salesforce userName or Salesforce UserId that triggers the InvokeSalesforceRestAPIFunction

Import the Voice Contact Flows into Amazon Connect

Contact flows define the user experience for callers. Salesforce provides sample Amazon Connect contact flows that use the AWS Lambda functions you configured in the previous section. Salesforce provides these sample contact flows for you to use as a starting point to build your interactive voice response (IVR) experiences.

1. Download the latest contact flows from Github:
   a. Go to the Service Cloud Voice Github repo: `https://github.com/service-cloud-voice/examples-from-doc` .
   b. Click **Download ZIP**.

      All the folders in the repo are downloaded. You only need the files in the Contact Flows directory.

2. Add the contact flows to your contact center:
   a. Log in to the AWS Console, and then select **Amazon Connect**.
   b. Select your instance.
   c. Click the **Contact flows** tab.
   d. In the AWS Lambda section, select these lambda functions from the **Function** menu:
      - Lambda function name that contains InvokeTelephonyIntegrationAPIFunction
      - Lambda function name that contains kvsConsumerTrigger
   e. Click **Add Lambda Function**.

3. Create contact flows and configure Lambda blocks for inbound calls:
   a. In the left navigation bar, hover over **Routing**, and then click **Contact flows**.
   b. Click **Create contact flow**.
   c. Click **Import flow (beta)**, and then select *`Sample_SCV_Inbound_Flow_With_Transcription`* from your download folder.
   d. Click Invoke AWS Lambda function block.
   e. In the **Select a function** menu on the right panel, select the function that contains *`InvokeTelephonyIntegrationApiFunction`*.
   f. Click **Save**. The right panel closes.

   g. Click **Save**, and then click **Publish**.
   h. In the left navigation bar, hover over **Routing**, and then click **Phone numbers**.
   i. Select the desired phone number.
   j. In the **Contact flow/IVR** dropdown menu, select the contact flow that you created.
   k. Save your changes.

4. Create contact flows and configure Lambda blocks for outbound calls:
   a. In the Contact flows page, click **Create outbound whisper flow**.
   b. Click **Import flow (beta)**, and then select `Sample SCV Outbound Flow With Transcription` from your download folder.
   c. Click **Invoke AWS Lambda function** block.
   d. In the **Select a function** menu on the right panel, select the function that contains `InvokeTelephonyIntegrationApiFunction`.
   e. Click **Save**. The right panel closes.
   f. Click **Save**, and then click **Publish**.
   g. In the left navigation bar, hover over **Routing**, and then click **Queues**.
   h. Select the default queue for your routing profile.
   i. For Outbound whisper flow (optional), select **Sample SCV Outbound Flow with Transcription**.
   j. Save your work.

5. Create contact flows and configure Lambda blocks for transferred calls:
   a. In the Contact flows page, click **Create transfer to agent flow**.
   b. Click **Import flow (beta)**, and then select `Sample SCV Transfer Flow for Agent Transfers` from your download folder.
   c. Click **Invoke AWS Lambda function** block.
   d. In the **Select a function** menu on the right panel, select the function that contains `InvokeTelephonyIntegrationApiFunction`.
   e. Click **Save**. The right panel closes.
   f. Click **Save**, and then click **Publish**.
   g. In the Contact flows page, click **Create transfer to queue flow**.
   h. Click **Import flow (beta)**, and then select `Sample SCV Transfer Flow for Queue Transfers` from your download folder.
   i. Click **Invoke AWS Lambda function** block.
   j. In the **Select a function** menu on the right panel, select the function that contains `InvokeTelephonyIntegrationApiFunction`.
   k. Click **Save**. The right panel closes.
   l. Click **Save**, and then click **Publish**.

Your contact flows were updated so that end-to-end call flows with agent screen pops and real-time transcription are ready to go.

Turn On AWS Streaming Services

Enable Contact Trace Records (CTR) data streaming and live media streaming to use real-time transcription in Salesforce. If you already have CTR enabled, it's not necessary to recreate these resources.

Enable the Contact Trace Records (CTR) Data Stream

CTR Data streams let you see agent activity in the Amazon Connect instance.

Enable Live Media Streaming

Enable live media streaming in Amazon Connect so call transcriptions are streamed to Voice.

Enable the Contact Trace Records (CTR) Data Stream

CTR Data streams let you see agent activity in the Amazon Connect instance.

1. Log in to the AWS Console, select **Amazon Connect**, and then select your instance.
2. Click **Data streaming**.
3. Select **Enable data streaming**.
4. Click **Kinesis Stream**.
5. Select your instance's CTRStream Kinsesis Stream.
6. Save your work.

Enable Live Media Streaming

Enable live media streaming in Amazon Connect so call transcriptions are streamed to Voice.

1. Log in to the AWS Console, select **Amazon Connect**, and then select your instance.
2. Click the **Data storage** tab.
3. Click **Edit** for live media streaming.
4. Select **Enable live media streaming**.
5. Enter a prefix that you can use with the contact center name.
6. For Encryption, choose **Select KMS key by name**, and then select your KMS key from the dropdown menu.
7. Under Data retention period, select **No data retention**.
8. Save your work.

Configure Contact Lens Transcription

Complete these steps to ensure your voice calls are transcribed.

Associate the Voice-Provisioned Kinesis Stream with Your Amazon Connect Instance

To enable transcription, Service Cloud Voice reads events from the Voice-provisioned Kinesis stream associated with your existing Amazon Connect instance. If you installed the ServiceCloudVoiceLambdas serverless application version 11.0 or earlier, verify the association between this Kinesis stream and your instance. If you created the serverless application with version 11.1 or later, the association is configured for you when you create or update your contact center.

Verify that Contact Lens is Enabled in Your Contact Flows

Enable speech analytics in each contact flow so that Contact Lens generates real-time transcripts during a call and post-call analytics after the conversation has ended. By default, speech analytics is enabled for some Salesforce-provided contact flows and subflows. Verify this setting in case things have changed or you're using your own contact flows. Repeat these steps for each contact flow and subflow for which you want to enable speech analytics.

Associate the Voice-Provisioned Kinesis Stream with Your Amazon Connect Instance

To enable transcription, Service Cloud Voice reads events from the Voice-provisioned Kinesis stream associated with your existing Amazon Connect instance. If you installed the ServiceCloudVoiceLambdas serverless application version 11.0 or earlier, verify the association between this Kinesis stream and your instance. If you created the serverless application with version 11.1 or later, the association is configured for you when you create or update your contact center.

Tip: Service Cloud Voice supports both KVS transcription and Contact Lens transcription. If Contact Lens transcription isn't supported in your region, use KVS transcription. Otherwise, we recommend that you use Contact Lens transcription. Contact Lens transcription doesn't have the 15-minute transcription limitation like KVS transcription. Also Contact Lens can generate intelligence signals such as sentiments.

1. Open the AWS CLI.
2. To see which stream with the REAL_TIME_CONTACT_ANALYSIS_SEGMENTS resource type is associated with your Amazon Connect instance, run the list-instance-storage-configs AWS CLI command.

   ```
   aws connect list-instance-storage-configs   list-instance-storage-configs
   --instance-id <your Amazon Connect instance ID>
   --resource-type REAL_TIME_CONTACT_ANALYSIS_SEGMENTS
   ```

3. If your Amazon Connect instance is associated with a different Kinesis stream, to remove the association, run the disassociate-instance-storage-config AWS CLI command.

   ```
   aws connect disassociate-instance-storage-config
   --instance-id <your Amazon Connect instance ID>
   --association-id <association ID>
   --resource-type REAL_TIME_CONTACT_ANALYSIS_SEGMENTS
   ```

4. To associate the Voice-provisioned Kinesis stream with your Amazon Connect instance, run the associate-instance-storage-config AWS CLI command.

   ```
   aws connect associate-instance-storage-config
   --instance-id <your Amazon Connect instance ID>
   --resource-type REAL_TIME_CONTACT_ANALYSIS_SEGMENTS
   --storage-config 'StorageType=KINESIS_STREAM,KinesisStreamConfig={StreamArn=<the ARN
   of your Kinesis stream>}'
   ```

The Kinesis stream ARN can be found on the Kinesis Instance page. After you successfully run the command to associate the stream, the command returns an association ID.

SEE ALSO:

Amazon Documentation: Enable Real-Time Contact Analysis Segment Streams

Verify that Contact Lens is Enabled in Your Contact Flows

Enable speech analytics in each contact flow so that Contact Lens generates real-time transcripts during a call and post-call analytics after the conversation has ended. By default, speech analytics is enabled for some Salesforce-provided contact flows and subflows. Verify this setting in case things have changed or you're using your own contact flows. Repeat these steps for each contact flow and subflow for which you want to enable speech analytics.

To enable Contact Lens in a contact flow, add a Set Recording and Analytics Behavior block to the flow and set these Contact Lens settings.

Field	Setting
Call Recording	Select these options. • On • Agent and Customer If you don't enable it, call recording won't work.
Analytics	Check these options only. • Enable Contact Lens Conversational Analytics • Enable Speech Analytics If you don't enable these options, real-time transcription won't work.

SEE ALSO:

Amazon Documentation: Enable Contact Lens for Amazon Connect

Configure Call Recording

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

Optionally, follow these steps to turn on automatic call recording and to allow support agents to pause call recording.

Enable Call Recording in Amazon Connect

There are a few high-level steps to configure automatic call recording. In Amazon Connect, enable call recording, and select where recordings are stored. Then give agents permission to listen to call recordings. In Salesforce, add the Call Audio Player to the Voice Call page. If call recording is already enabled for your instance, it's not necessary to make any changes.

Let Agents Pause and Resume Call Recordings

Some organizations automatically record calls for training and quality purposes. Your customers and your company might prefer not to record certain information for privacy and legal compliance reasons. Honor your customer's privacy and protect your company when a call is recorded by allowing agents to pause the recording when sensitive information is exchanged. Agents can resume the recording when it's appropriate.

Create a Call Connect Role and IAM Policy

To create a Call Connect role and an Identity and Access Management (IAM) policy, create a policy and a role, and then attach the role to the policy.

Enable Call Recording in Amazon Connect

There are a few high-level steps to configure automatic call recording. In Amazon Connect, enable call recording, and select where recordings are stored. Then give agents permission to listen to call recordings. In Salesforce, add the Call Audio Player to the Voice Call page. If call recording is already enabled for your instance, it's not necessary to make any changes.

1. Log in to Amazon Connect, and then select your instance.
2. Create an S3 Bucket for storing call recordings:
   a. Click **Data Storage**.
   b. Select **Enable call recording**.
   c. Select the option **Select an existing S3 bucket**.
   d. Optionally, enable encryption.
   e. Save your work.
3. To let agents listen to call recordings, update the agent security profile:
   a. Log in to your Amazon Connect instance.
   b. In the left navigation bar, hover over Users, and then click **Security profiles**.
   c. Select the security profile for Agent.
   d. In the Metrics and Quality section, select **Access** for Record conversations (unredacted) and Record conversations (redacted).
   e. Save your work.

When you configure the Voice Call record page in Salesforce, add the Call Audio Player component to the page so users can listen to recorded calls.

Let Agents Pause and Resume Call Recordings

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To assign permission sets:
- Assign Permission Sets

Some organizations automatically record calls for training and quality purposes. Your customers and your company might prefer not to record certain information for privacy and legal compliance reasons. Honor your customer's privacy and protect your company when a call is recorded by allowing agents to pause the recording when sensitive information is exchanged. Agents can resume the recording when it's appropriate.

For more information about how agents can pause call recording while on a call, see Pause Call Recording to Honor Customer Privacy.

To let agents suspend and resume call recording, complete these high-level steps:

1. In Amazon Connect, create a call connect role and an IAM policy in your contact center definition file.
2. In Salesforce, clone the Contact Center Agent (Partner Telephony) user permission set and add the Control Call Recording user permission to the permission set.

SEE ALSO:

Create a Call Connect Role and IAM Policy

Create a Call Connect Role and IAM Policy

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

To create a Call Connect role and an Identity and Access Management (IAM) policy, create a policy and a role, and then attach the role to the policy.

Tip: You need the Amazon Resource Name (ARN) for your Amazon Connect instance so you can create a policy:

1. From the AWS Console, go to Amazon Connect and select your instance.
2. Click **Overview**.
3. The ARN is shown in the Overview section. Copy and paste this value to your notepad.

To configure access to AWS, follow these steps:

1. Create a policy to manage access to AWS services.
   a. Go to Identity and Access Management in AWS.
   b. Under Access management, select **Policies**.
   c. Click **Create policy**.
      The Create policy page opens.
   d. Click the JSON tab.
   e. Copy and paste this JSON policy, but replace the “Resource” with your Amazon Connect instance's ARN.

Don’t change the userid string.

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "connect:ResumeContactRecording",
                    "connect:SuspendContactRecording"
                ],
                "Resource":
"arn:aws:connect:YOUR_REGION:YOUR_ACCOUNT:instance/YOUR_INSTANCE_ID/contact/*"
            }
        ]
      }
```

f. Click **Next: Tag**, and then click **Next: Permission**.

g. Click **Next: Review**.

h. For Name, enter a name such as *`ConnectCallRecordingPolicy`*. Optionally, enter a description.

i. Click **Create policy**.

The policy is created.

2. Add an identity provider.

   a. Under Access management, select **Identity Providers**.

   b. Click **Add Provider**.

   c. Fill out the fields:

      - For **Provider Type**, select *`SAML`*.
      - For **Provider Name**, enter *`ConnectCallRecording`*.
      - For **Metadata Document**, click **Choose File**, and then select the Salesforce identity provider metadata file.

   d. Click **Add provider**.
      A banner is displayed asking you to assign a role.

3. Create a new role to assign to the identity provider.

   a. Click **Assign role**.
      A window is displayed asking you to create a role or use an existing role.

   b. Click **Create a new role**.

      - In the **Select type of trusted entity** section, select *`SAML 2.0 federation`*.
      - Select **Allow programmatic and AWS Management Console access**. The Attribute and Value fields are automatically populated.

   c. Click **Next: Permissions**.

   d. Attach the policy to the role.

      - In the search box, enter the name of the policy that you created in Step 1.
      - Select the policy.

   e. Click **Next: Tags**, and then click **Next: Review**.

f. In the **Role name** field, enter a name such as `ConnectCallRole`.

g. Optionally, in the **Description** field, enter a description.

h. Click **Create role**.
The role is created. You need this role to set up the connected app in Salesforce.

4. Update your new ConnectCallRole's trust relationship.

a. From the ConnectCallRole summary, click the **Trust relationships** tab.

b. Click **Edit trust relationship**.

c. Copy and paste this JSON string.

```
{
      "Version": "2012-10-17",
      "Statement": [
        {
          "Effect": "Allow",
          "Principal": {
            "AWS": "arn:aws:iam::793525387755:root"
          },
          "Action": "sts:AssumeRole"
        }
      ]
    }
```

d. Click **Update Trust Policy**.

Set Up Service Cloud Voice for Partner Telephony

After you configure your Amazon Connect instance, follow these steps to set up Service Cloud Voice in Salesforce.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

1. Enable Prerequisite Services in Salesforce
   My Domain and Omni-Channel must be enabled before you can turn on Service Cloud Voice. If you already completed the previous steps to configure Amazon Connect and SSO, then My Domain is already turned on. Enable Omni-Channel in your org. If Omni-Channel already is enabled in your org, skip this step.
2. Turn on Service Cloud Voice with Partner Telephony
   Enable Voice for your org.
3. Create Your Partner Telephony from Amazon Connect Contact Center
   To create a contact center for Service Cloud Voice with Partner Telephony from Amazon Connect, create an XML contact center definition file and import it into Voice. Use the sample contact center definition file as a model. And use the Self-Signed Certificate that you created earlier.
4. Create a Phone Channel
   To configure call routing for voice calls, including Omni-Channel flows and queue routing, and to determine when to create an End User record, create a phone channel. After you create a phone channel, you can set up a caller ID tool to create or reuse an End User record and choose whether to associate the End User record with the number dialed.

5. Enable Universal Call Recording in an Existing Contact Center

   By default, the Universal Call Recording feature is disabled in Amazon Connect contact centers. To enable this feature in a Partner Telephony from Amazon Connect contact center that was created before Spring '22, update the XML contact center definition file. Then import the XML file into your Salesforce org using the Metadata API to update the contact center setting.

6. Configure Omni-Channel for Service Cloud Voice

   Follow these steps to configure Omni-Channel so agents can use it to accept and make calls. Create a contact center agent permission set, and then create a presence status and assign it to users. Add the Omni-Channel utility to the Lightning Service Console so agents can use the Omni-Channel softphone. Optionally, configure the After Conversation Work setting and add the After Conversation Component component to the Voice Call record page.

7. Assign Contact Center Permission Sets for Partner Telephony

   Use permission sets to control access to your Voice contact center. Give at least one user, such as yourself, the Contact Center Admin (Partner Telephony) permission set so they can set up the contact center. Give agents and supervisors the Contact Center Agent (Partner Telephony) permission set so they can make and receive voice calls and listen to call recordings.

8. Add and Remove Users in Your Partner Telephony Contact Center

   After you create a contact center for Service Cloud Voice with Partner Telephony or Service Cloud Voice with Partner Telephony from Amazon Connect, add users to your contact center. You can add Service Cloud Users who have the Contact Center Admin (Partner Telephony) permission set or the Contact Center Agent (Partner Telephony) permission set. Remove users who no longer need access.

Enable Prerequisite Services in Salesforce

My Domain and Omni-Channel must be enabled before you can turn on Service Cloud Voice. If you already completed the previous steps to configure Amazon Connect and SSO, then My Domain is already turned on. Enable Omni-Channel in your org. If Omni-Channel already is enabled in your org, skip this step.

If My Domain and Omni-Channel aren't enabled in your org, the Turn On Service Cloud Voice setting isn't available. After you enable My Domain and Omni-Channel, the setting is available so you can turn on Voice.

1. From Setup, enter `Omni-Channel Settings` in the Quick Find box, then select **Omni-Channel Settings**.
2. Select **Enable Omni-Channel**.
3. Click **Save**.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To set up Omni-Channel:

- Customize Application

Turn on Service Cloud Voice with Partner Telephony

Enable Voice for your org.

This task applies to this telephony model.

Service Cloud Voice with Amazon Connect	Service Cloud Voice with Partner Telephony from Amazon Connect	Service Cloud Voice with Partner Telephony
✕	✕	✓

USER PERMISSIONS

To view the Partner Telephony Setup page:

- Customize Application

To turn on Voice:

- Customize Application

If you have the Service Cloud Voice for Partner Telephony license, you see the Partner Telephony Setup page in the Setup menu.

1. From Setup, enter `Partner Telephony Setup` in the Quick Find box, then select **Partner Telephony Setup**.
2. Select **Turn On Service Cloud Voice**.
   The Partner Telephony Contact Centers page appears in the Setup menu.

After you turn on Voice, it's time to install the managed package from your telephony provider.

Create Your Partner Telephony from Amazon Connect Contact Center

To create a contact center for Service Cloud Voice with Partner Telephony from Amazon Connect, create an XML contact center definition file and import it into Voice. Use the sample contact center definition file as a model. And use the Self-Signed Certificate that you created earlier.

Before you start, make sure that you created the Self-Signed Certificate with OpenSSL from earlier in the setup.

Download the sample contact center definition file from the Service Cloud Voice Github repository and customize it for your contact center.

To download files from Github, go to the top-level directory https://github.com/service-cloud-voice/examples-from-doc, click **Code**, and then click **Download zip**. The entire repository is downloaded as a zipped file.

For Partner Telephony from Amazon Connect, use the sample file `amazon_connect_partner_telephony_cc_import.xml` shown at https://github.com/service-cloud-voice/examples-from-doc/blob/main/callcenter/amazon_connect_partner_telephony_cc_import.xml.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To view the Partner Telephony Setup page:

- Customize Application

To view the Partner Telephony Contact Centers page:

- Customize Application AND Manage Call Centers

To create and manage a contact center:

- Contact Center Admin (Partner Telephony)

Edit the file and replace the generic values with the values for your contact center.

1. Set `reqDisplayName` to be the name of your contact center.
2. The `reqInternalName` autopopulates and is referred to in the Lambda section as the `CALL_CENTER_API_NAME`.
3. Leave `reqVendorInfoApiName` unchanged.
4. Set the `reqRelayState` to the Relay State URL created earlier in the setup.
5. Copy and paste the Self-Signed Certificate into `reqTelephonyIntegrationCertificate` section.
6. Leave `reqLongDistPrefix` unchanged.
7. Set `reqInstanceName` to be your Amazon Connect instance alias.
8. Set `reqInstanceRecordingRole` to be the ARN your created earlier in the setup.

9. Save the file as an XML file.

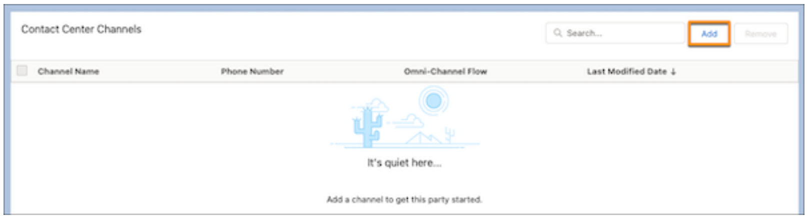
Create a Phone Channel

To configure call routing for voice calls, including Omni-Channel flows and queue routing, and to determine when to create an End User record, create a phone channel. After you create a phone channel, you can set up a caller ID tool to create or reuse an End User record and choose whether to associate the End User record with the number dialed.

Before you create a phone channel:

- Service Cloud Voice Planning Checklist on page 3
- Create Your Partner Telephony from Amazon Connect Contact Center on page 29

1. From Setup, in the Quick Find box, enter `Partner Telephony Contact Centers`, then select **Partner Telephony Contact Centers**.
2. Select the contact center you want to create a phone channel for.
3. In the Contact Center Channels section, click **Add**.



It's quiet here...

Add a channel to get this party started.

4. Enter a channel name and the contact center phone number.
5. Optional: Set up routing configurations for your contact center.
   a. To route this phone channel's calls to a specific queue, select **Queue** in the Routing Type field, and then enter the name of the Salesforce queue you want to route calls to.
   b. To route this phone channel's calls with an Omni-Channel flow, select **Omni-Channel Flow** in the Routing Type field, and then enter the names of the Omni-Channel flow and fallback queue.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To view the Amazon Contact Centers page:

- Customize Application AND Manage Call Centers

To create and manage a contact center:

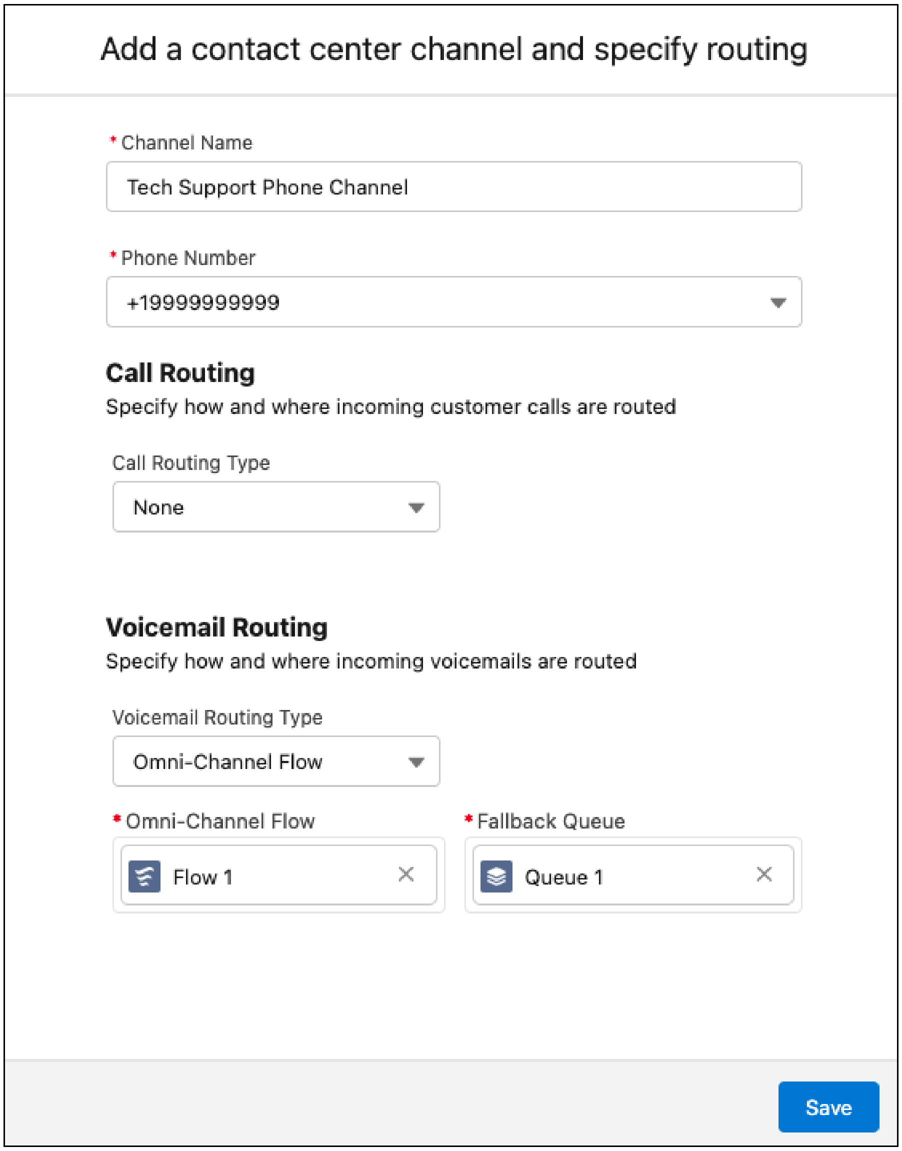
- Contact Center Admin

To view the Partner Telephony Contact Centers page:

- Customize Application AND Manage Call Centers

To create and manage a contact center:

- Contact Center Admin (Partner Telephony)



Add a contact center channel and specify routing

* Channel Name

Tech Support Phone Channel

* Phone Number

+19999999999

Call Routing

Specify how and where incoming customer calls are routed

Call Routing Type

None

Voicemail Routing

Specify how and where incoming voicemails are routed

Voicemail Routing Type

Omni-Channel Flow

* Omni-Channel Flow

Flow 1

* Fallback Queue

Queue 1

6. Save your changes.

To make it easier to identify callers, configure your End User record settings for your phone channel. You can choose to either match callers to End User records or override your phone channel number settings.

Enable Universal Call Recording in an Existing Contact Center

By default, the Universal Call Recording feature is disabled in Amazon Connect contact centers. To enable this feature in a Partner Telephony from Amazon Connect contact center that was created before Spring '22, update the XML contact center definition file. Then import the XML file into your Salesforce org using the Metadata API to update the contact center setting.

1. Use the retrieve() call in the Metadata API to get the XML contact center definition file.
2. Open the XML file in a text editor.
3. In the section that contains the Amazon Connect contact center details, add the Universal Call Recording Access parameters as shown here.

```
<sections>
    <items>
        <label>Telephony Provider</label>
        <name>reqTelephonyProvider</name>
        <value>AMAZON_CONNECT</value>
    </items>
    <items>
        <label>Instance Name</label>
        <name>reqInstanceName</name>
        <value>testhvcc00DS70000000SmT</value>
    </items>
    <items>
        <label>Universal Call Recording Access</label>
        <name>reqUniversalCallRecordingAccess</name>
        <value>true</value>
    </items>
...
</sections>
```

4. Save the XML file.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To manage a contact center:

- Contact Center Admin (Partner Telephony) AND Customized Application AND Manage Call Center

5. Use the deploy() call in the Metadata API to deploy the updated XML file and update the contact center.

SEE ALSO:

Listen to and Collaborate on Call Recordings

Configure Omni-Channel for Service Cloud Voice

Follow these steps to configure Omni-Channel so agents can use it to accept and make calls. Create a contact center agent permission set, and then create a presence status and assign it to users. Add the Omni-Channel utility to the Lightning Service Console so agents can use the Omni-Channel softphone. Optionally, configure the After Conversation Work setting and add the After Conversation Component component to the Voice Call record page.

1. Clone the Contact Center Agent permission set.
    a. From Setup, in the Quick Find box, enter *`Permission Sets`*, and then select **Permission Sets**.
    b. Find the Contact Center Agent permission set, and then click **Clone**.
    c. Enter *`Contact Center Agent (SFDC)`* as the permission set name.
    d. Save your changes.
2. Create a presence status so agents can indicate when they're available for phone calls.
    a. From Setup, in the Quick Find box, enter *`Presence`*, and then select **Presence Statuses**.
    b. Click **New**.
    c. For `Status Name`, enter *`Available`*.
    d. For `Status Options`, select *`Online`*.
    e. Add the **Phone** service channel to the Available Channels list.
    f. Save your changes.

       To add more statuses, repeat the steps. For example, you can create a "Busy" presence status.
3. Assign the presence status to agents so they can indicate when they're available to accept calls.
    a. From Setup, in the Quick Find box, enter *`Permission Sets`*, and then select **Permission Sets**.
    b. Find the permission set that you cloned.
    c. Click **Service Presence Statuses Access**.
    d. Click **Edit**.
    e. In the Available Service Presences list, select the presence status that you created, and then click **Add** to associate it with permission set.

       Agents who are assigned to this permission set can sign in to Omni-Channel with any of the presence statuses that you make available to them.
    f. Save your changes.
4. Add the Omni-Channel utility to your Lightning Service Console.
    a. From Setup, in the Quick Find box, enter *`Apps`*, and then select **App Manager**.
    b. Click the dropdown next to the Service Console app that you want to add Omni-Channel to, and then click **Edit**.
    c. Under App Settings, click **Utility Items (Desktop Only)**.
    d. Click **Add Utility Item**.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To set up Omni-Channel and to create presence statuses:
- Customize Application

To create permission sets:
- Manage Profiles and Permission Sets

To assign permission sets:
- Assign Permission Sets

EDITIONS

Available in: Service Cloud Voice with Amazon Connect

Available in: Service Cloud Voice with Partner Telephony

Available in: Service Cloud Voice with Partner Telephony from Amazon Connect

  e. In the window, search for Omni-Channel.
  f. Click **Omni-Channel**.
  g. Click **Save**, and then exit the App Manager.

5. Optionally, give agents a set amount of time after a call ends to wrap up their work.
   a. From the Service Channels page in Setup, edit or create a channel based on Voice or Messaging. Alternatively, from the Presence Configurations page in Setup, edit or create configuration.

   The Voice service channel is automatically created when you turn on Voice.

   a. In the After Conversation Work Time section, select **Give agents wrap-up time after conversations**.
   b. In the Duration (seconds) field (required), enter the number of seconds that agents have to complete their closing work after a conversation. The value must be from 30 to 3,600 seconds.
   c. To let agents extend their ACW time, select **Let agent extend timer** and add the extension duration in seconds. Also, choose the maximum number of times agents can extend their ACW.
   d. Save your changes.

   Important: Make sure that the After Conversation Work component is added to the Voice Call page layout. Otherwise, agents don’t see the countdown.

Service Cloud Voice is now set up so that Connect agents can log in to Omni-Channel.

Assign Contact Center Permission Sets for Partner Telephony

Use permission sets to control access to your Voice contact center. Give at least one user, such as yourself, the Contact Center Admin (Partner Telephony) permission set so they can set up the contact center. Give agents and supervisors the Contact Center Agent (Partner Telephony) permission set so they can make and receive voice calls and listen to call recordings.

Note: The Contact Center Agent (Partner Telephony) permission set includes the View Call Recordings user permission. Agents need this user permission to listen to call recordings.

1. From Setup, enter `Partner Telephony Setup` in the Quick Find box, then select **Partner Telephony Setup**.
2. In the Set Up Your Contact Center section, click **Assign Permissions**. The Permission Sets page opens.
3. Click either Contact Center Admin (Partner Telephony) or Contact Center Agent (Partner Telephony).
4. Click **Manage Assignments**.
5. Click **Add Assignments**.
6. Select the users that need the permission set.
7. Click **Assign**.

After assigning permission sets, create your contact center.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To assign permission sets:
- Assign Permission Sets

Add and Remove Users in Your Partner Telephony Contact Center

After you create a contact center for Service Cloud Voice with Partner Telephony or Service Cloud Voice with Partner Telephony from Amazon Connect, add users to your contact center. You can add Service Cloud Users who have the Contact Center Admin (Partner Telephony) permission set or the Contact Center Agent (Partner Telephony) permission set. Remove users who no longer need access.

1. In your telephony provider's system, add the users to the call center. Salesforce and the telephony provider don't automatically sync users, so you must manually create users and then add them to your telephony provider's call center and the Voice contact center.

   Important: If you want to use single sign-on (SSO) to authenticate support agents, the username must be the same for both Salesforce and the telephony partner.

2. In Salesforce, add the users to your Voice contact center.
   a. From Setup, in the Quick Find box, enter `Partner Telephony Contact Centers`, then select **Partner Telephony Contact Centers**.
   b. Select the contact center that you want to modify.
   c. In the Contact Center Users section, click **Add**.
   d. Select the users that you want to add to this contact center. Add only one or two users at a time.

      The list shows only users who have the Contact Center Admin (Partner Telephony) or Contact Center Agent (Partner Telephony) permission sets. If you don't see the users that you want to add, make sure that they have the right permission sets, and then try adding them again.
   e. Click **Done**.

If a user no longer needs access to your contact center, remove them. Removing a user only takes away their ability to access the contact center. It doesn't delete the user or change their ability to access other parts of Salesforce.

1. In the Contact Center Users section, select the user that you want to remove.
2. Click **Remove** > **OK**.
3. Work with your telephony provider to remove the user from their telephony system.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

USER PERMISSIONS

To view the Partner Telephony Contact Centers page:
- Customize Application AND Manage Call Centers

To create and manage a contact center:
- Contact Center Admin (Partner Telephony)

Report on Your Contact Center

Create a CRM Analytics App to report on your contact center's key performance indicators (KPIs).

Track Contact Center KPIs with the CRM Analytics App

Let support supervisors view key performance indicators (KPIs) and see graphs and data about your company's Service Cloud Voice contact centers. Supervisors can track call volume, average handle time, average speed to answer, and more. Customize how contact center data is displayed so supervisors see relevant and actionable information.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

Track Contact Center KPIs with the CRM Analytics App

Let support supervisors view key performance indicators (KPIs) and see graphs and data about your company's Service Cloud Voice contact centers. Supervisors can track call volume, average handle time, average speed to answer, and more. Customize how contact center data is displayed so supervisors see relevant and actionable information.

This feature is available with these telephony models.

Service Cloud Voice with Amazon Connect	Service Cloud Voice with Partner Telephony from Amazon Connect	Service Cloud Voice with Partner Telephony
✓	✓	✓

For help assigning permission sets, see Set Up Permissions for the Service Analytics.

1. Navigate to Analytics Studio.
2. Click **Create**, and then select **App**.
3. Click **Create App from Template**.
4. Select **Service Cloud Voice Reporting Dashboard**.
5. Click **Continue**.
6. Click **Create a brand new app**.
7. Answer the questions to determine how the data appears in your dashboard.
8. Click **Looks good, next**.
9. Enter a name for your app. For example, `<Your Company> Voice Analytics`.

USER PERMISSIONS

To create and manage CRM Analytics apps:

- Manage Analytics Templated Apps AND Edit Analytics Dataflows

To set up the Contact Center Reporting Dashboard:

- CRM Analytics Plus Admin permission set AND Service Analytics Admin permission set

To view the Contact Center Reporting Dashboard:

- CRM Analytics Plus User permission set AND Service Analytics User permission set

10. Click **Create**. It can take a few minutes for the app to be created. Check your email; Salesforce sends a notification email when the app is ready.

After the CRM Analytics app is created, customize how it displays data. Open the app and customize the location, call resolution, and sharing settings.

- Select a location to use to filter agents by geography. For example, to show agents from California, select the **State** field on the User object.
- Show how many calls were resolved by selecting the Call Resolution field values that indicate that a call was resolved. You can select multiple field values. Companies use different values to mean that a call is resolved. For example, the values *Closed* and *Resolved* both can mean that the customer issue was solved. All unselected values are used to calculate the number of unresolved calls.
- Determine how users see information in your contact center. Select one of the following sharing settings:
  - Use the Salesforce role hierarchy to control data access. Users see data that they own and that subordinate users own. This sharing setting is the most restrictive.
  - Let users see data that they own, that other users at their same level own, and that subordinate users own.
  - Users see all data. This sharing setting is the least restrictive.

The following graphs are available.

Graph	Description
Call Volume	Shows the number of inbound calls versus outbound calls.
Average Handle Time	Shows the average amount of time an agent spends on a call.
Average Speed To Answer	Shows the average amount of time a customer is waiting before an agent answers the call.
First Call Resolution (FCR)	Shows the resolution for the first call that a customer makes to the contact center.
Abandonment Rate	Shows the percentage of calls where the customer hangs up before the agent answers the call.
Calls to Cases	Shows the number of calls that result in opening a case. Your contact center's metrics depend on your company's policies about how calls are managed. For example, some companies open a case for every call. Other companies open a case only when the issue isn't resolved during the call and is escalated.

Maintain Your Contact Center

Follow these steps to keep your contact center and contact flows up to date.

EDITIONS

Available in: Lightning Experience

Available in: **Enterprise** and **Unlimited** Editions

Available in: Sales Cloud, Service Cloud, and Government Cloud as an add-on license. Government Cloud is supported only on Service Cloud Voice with Partner Telephony from Amazon Connect and Service Cloud Voice with Partner Telephony.

Update Your Contact Flows
From time to time, Salesforce releases updates to contact flows for Service Cloud Voice. Download the contact flows from Github and import them into Amazon Connect.

Update Your Contact Center with the AWS Serverless Application
From time to time, Salesforce releases updates to the AWS serverless application that runs the contact centers. When an update is available, a notification is shown in the AWS Management Console.

Update Your Contact Flows

From time to time, Salesforce releases updates to contact flows for Service Cloud Voice. Download the contact flows from Github and import them into Amazon Connect.

Important: If you customized your contact flows, export them so you can reapply the changes to the updated contact flows. Importing the contact flows overwrites old flows with the same name.

1. Download the latest contact flows from https://github.com/service-cloud-voice/examples-from-doc/tree/main/ContactFlows.
   a. Go to https://github.com/service-cloud-voice/examples-from-doc.
   b. Click Download ZIP. All of the folders in the repo are downloaded. You only need the files in the Contact Flows directory.
2. Import the contact flows into Amazon Connect.

Update Your Contact Center with the AWS Serverless Application

From time to time, Salesforce releases updates to the AWS serverless application that runs the contact centers. When an update is available, a notification is shown in the AWS Management Console.

1. Log in to the AWS Management Console and navigate to the **Serverless Application Repository**.
2. Click **Available applications**.
3. Click **Private applications**.
4. Select **Show apps that create custom IAM roles or resource policies**.
5. Select the latest **service_cloud_voice_application**.
6. Click **Deploy**.

Train Your Agents on Service Cloud Voice

Use these resources to help your agents become familiar with Voice's softphone and features. Some features may differ depending on what features your telephony provider offers.

This feature is available with these telephony models.

Service Cloud Voice with Amazon Connect	Service Cloud Voice with Partner Telephony from Amazon Connect	Service Cloud Voice with Partner Telephony
✓	✓	✓

To enable agents to help customers on the phone, teach them how to:

- Answer inbound calls and make outbound calls using the Phone tab in the Omni-Channel utility
- Add a caller to a conversation
- Transfer a call to an agent or a queue
- Honor customer privacy when recording calls
- Listen to and collaborate on call recordings
- Link calls with customer contact records
- Report on your contact center