

---

# Einstein Conversation Insights Amazon Connect Configuration Guide

Salesforce, Spring '24





# CONTENTS

<a href="#">Configure Amazon Connect with Einstein Conversation Insights</a>	<a href="#">1</a>
Set Up the Amazon Connect CTI Adapter and Test the Salesforce Lambda Core Functionality	<a href="#">2</a>
Log In as the Integration User	<a href="#">6</a>
Set Up Amazon Connect Settings	<a href="#">7</a>
Identify Users as Call Owners	<a href="#">8</a>
Add Amazon Connect Named Credentials	<a href="#">10</a>
Set Up the Connected App	<a href="#">10</a>
Add ECI as an Authorized Provider	<a href="#">12</a>
Set Up the Salesforce Site	<a href="#">12</a>
Add ECI Named Credentials	<a href="#">13</a>
Assign the Guest User Permission Set	<a href="#">13</a>
Make Phone Calls with Amazon Connect	<a href="#">14</a>



# CONFIGURE AMAZON CONNECT WITH EINSTEIN CONVERSATION INSIGHTS

Follow these tasks to integrate Amazon Connect with Einstein Conversation Insights (ECI).

Amazon Connect when used with Service Cloud Voice with Amazon Connect was supported, but the provider is now supported without Service Cloud Voice.

Complete these steps after installing and launching the Voice Connector app.

Additional steps are required to complete the integration process and turn on the feature. See the [ECI Voice Connector Guide](#) for more details.

## [Set Up the Amazon Connect CTI Adapter and Test the Salesforce Lambda Core Functionality](#)

Prior to configuring Amazon Connect with Einstein Conversation Insights (ECI), the CTI adapter needs to be set up. Additional permissions need to be added before testing the Salesforce Lambda core functionality and proceeding with the configuration.

## [Log In as the Integration User](#)

Before you can set up the integration between the voice connector and Einstein Conversation Insights (ECI), a user with Salesforce admin permissions is required to be available for the integration. This user is typically a separate user created for the purpose of integrations. Make sure you're logged in as this user for the configuration tasks.

## [Set Up Amazon Connect Settings](#)

Amazon Connect object settings and fields must be updated in order for the Voice Connector app to work effectively.

## [Identify Users as Call Owners](#)

When a new call is conducted, some settings must be in place to identify the correct Salesforce user as the call owner. Otherwise, the phone number is used instead (from/to number) and is matched to the Salesforce user (Phone) field in their user profile.

## [Add Amazon Connect Named Credentials](#)

Add the named credentials for the voice provider from the Setup menu.

## [Set Up the Connected App](#)

To call the Einstein Conversation Insights (ECI) web service, create a connected app. If you've configured another voice connector, skip the remaining configuration tasks.

## [Add ECI as an Authorized Provider](#)

Add Einstein Conversation Insights (ECI) as an authorized provider from the Setup menu.

## [Set Up the Salesforce Site](#)

If a site isn't created, set up an active Salesforce site.

## [Add ECI Named Credentials](#)

Add the named credentials for ECI from the Setup menu.

## [Assign the Guest User Permission Set](#)

Assign the guest user permission set from Setup.

## [Make Phone Calls with Amazon Connect](#)

After you've finished setting up Amazon Connect with Einstein Conversation Insights, connect to the Amazon Connect control panel to start making phone calls.

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

# Set Up the Amazon Connect CTI Adapter and Test the Salesforce Lambda Core Functionality

Prior to configuring Amazon Connect with Einstein Conversation Insights (ECI), the CTI adapter needs to be set up. Additional permissions need to be added before testing the Salesforce Lambda core functionality and proceeding with the configuration.

1. Make sure the Amazon Connect CTI Adapter and Salesforce Lambdas are installed using either the [Amazon Connect help content](#) or Guided Setup.

The process for using the in-app Guided Setup is also outlined on the [Amazon Connect site](#).

2. Add the AmazonS3ReadOnlyAccess permission to the sfExecuteAwsServiceIamUser IAM user. Make sure the sfExecuteAwsServiceIamUser user is already created in your AWS account before you continue with this step.

- a. Navigate to the [AWS Console](#).
- b. Make sure you're working in the same region as your Amazon Connect instance. You can set the region by expanding the region selector in the upper right corner of the AWS Console and choosing the appropriate region.
- c. In the AWS Console, navigate to the IAM (Identity and Access Management) service by clicking on **Services** in the top left corner, then selecting IAM under the Security, Identity, & Compliance section.
- d. In the IAM dashboard, click on **Users** in the left navigation pane. From the list, click **sfExecuteAwsServiceIamUser**.
- e. Click the **Permissions** tab.
- f. Click **Add Permissions**.
- g. Select the **Attach policies directly** option. This allows you to directly attach AWS managed policies to the user.
- h. In the search box, enter `AmazonS3ReadOnlyAccess` and select the policy.
- i. Click **Next: Review**.
- j. Click **Add permissions**.

The AmazonS3ReadOnlyAccess permission is added to the sfExecuteAwsServiceIamUser IAM user.

3. Copy the Amazon Resource Name (ARN) of the serverlessrepo-AmazonConnectSa-sfExecuteAWSService-XXXX function. If you already have the ARN, proceed to the next step.

- a. Navigate to the [AWS Console](#).
- b. Click **Services** in the top left corner and select **Lambda** under the Compute section.
- c. In the Lambda dashboard, click on **Functions**.
- d. In the search box, enter `sfExecuteAWS` and select the **serverlessrepo-AmazonConnectSa-sfExecuteAWSService-XXXX** function.
- e. Copy the Function ARN.

This ARN uniquely identifies the function and can be used for various purposes, including setting up permissions.

4. Add the lambda:InvokeFunction permission to the sfExecuteAwsServiceIamUser IAM user.

- a. In the AWS Console, navigate to the IAM (Identity and Access Management) service by clicking on **Services** in the top left corner, then selecting IAM under the Security, Identity, & Compliance section.

## EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

## USER PERMISSIONS

To enable Einstein Conversation Insights:

- Customize Application

- b. In the IAM dashboard, click on **Users** in the left navigation pane. From the list, click **sfExecuteAwsServiceIamUser**.
- c. Click the **Permissions** tab.
- d. Click **Add Permissions**.
- e. Select the **Create inline policy** option. This allows you to create a custom policy.
- f. From the Specify permissions page, click on the **JSON** tab.
- g. In the JSON policy editor, locate the Action key, and add `lambda:InvokeFunction` as its value. This action grants permission to invoke Lambda functions.
- h. For the Resource key paste the ARN value you copied earlier.
- i. Click **Next: Review**.
- j. Click **Create policy**.

```

1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Action": [
6-         "lambda:InvokeFunction"
7-       ],
8-       "Resource": "arn:aws:lambda:us-east-2:XXXXXXXXXX:function:serverlessrepo-AmazonConnectSa-sfExecuteAWSService
9-         -0u82INNe4Vmn",
10-      "Effect": "Allow"
11-    }
12-  ]

```

5. Copy the Amazon Resource Name (ARN) of `SalesforceCredentialsSecretsManagerKey` in AWS Secrets Manager. If you already have this ARN, proceed to the next step.
  - a. Navigate to the [AWS Console](#).
  - b. Click **Services** in the top left corner and select **Secrets Manager** under the Security, Identity, & Compliance section.
  - c. Make sure you are working in the same region as your Amazon Connect instance. You can set the region by expanding the region selector in the upper right corner of the AWS Console and choosing the appropriate region.
  - d. In the Secrets Manager dashboard, click **SalesforceCredentials**.
  - e. Copy the ARN of the secret.
6. Add additional permissions to the `sfInvokeAPI` Lambda function.
  - a. Navigate to the [AWS Console](#).
  - b. Enter **Lambda** in the search box to access the AWS Lambda service.
  - c. In the Lambda dashboard, click on **Functions**.
  - d. In the search box, enter `sfInvokeAPI` and select the **serverlessrepo-AmazonConnectSalesforce-sfInvokeAPI-2XHzCTUoEZhA** function.
  - e. Go to Configuration and click on **Permissions**.
  - f. Click on the role name associated with the `sfInvokeAPI` function. It should be something like `serverlessrepo-AmazonConnectSale-sfLambdaBasicExec-xxxxx`.
  - g. Click the **Permissions** tab.
  - h. Click **Add Permissions**.
  - i. Select the **Create inline permission** option.

- j. Click on the **JSON** tab.
- k. In the JSON policy editor, locate the Action key, and add the following actions:

```
"kms:Decrypt",  
"kms:Encrypt",  
"kms:ReEncrypt*",  
"kms:GenerateDataKey"
```

- l. For the Resource key paste the ARN value from the AWS Secrets Manager.
- m. Click **Next**.
- n. Enter a policy name, such as KMSPolicy.
- o. Click **Create policy**.  
The policy should look like this.

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "VisualEditor0",  
      "Effect": "Allow",  
      "Action": [  
        "kms:Decrypt",  
        "kms:Encrypt",  
        "kms:ReEncrypt*",  
        "kms:GenerateDataKey"  
      ],  
      "Resource": "arn:aws:kms:us-west-2:xxxxxxx:key/xxxxxxxxxxx"  
    }  
  ]  
}
```

- 7. Give the Lambda function access to the Secret Manager.
  - a. Navigate to the [AWS Console](#).
  - b. Enter **Lambda** in the search box to access the AWS Lambda service.
  - c. In the Lambda dashboard, click on **Functions**.
  - d. Click the **Permissions** tab.
  - e. Click **Add Permissions**.
  - f. Select the **Create inline permission** option.
  - g. Click on the **JSON** tab.
  - h. In the JSON policy editor, locate the Action key, and add the following actions:

```
"secretsmanager:GetSecretValue",  
"secretsmanager:PutSecretValue"
```

- i. For the Resource key paste the ARN value from the AWS Secrets Manager you want to access.
- j. Click **Next**.
- k. Enter a policy name, such as SecretManagerPolicy.



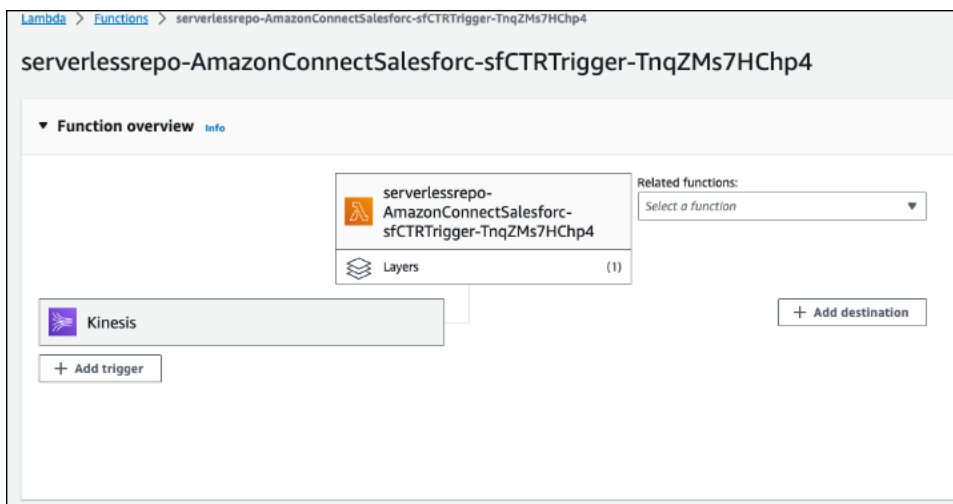
I. Click **Create policy**.

The policy should look like this.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:PutSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-west-2:xxxxx"
    }
  ]
}
```

8. Configure the sfCTRTrigger Lambda function to work with a Kinesis stream.

- a. Navigate to the [AWS Console](#).
- b. Enter **Lambda** in the search box to access the AWS Lambda service.
- c. In the Lambda dashboard, click on **Functions**.
- d. In the search box, enter *sfCTRTrigger* and select the **sfCTRTrigger** function.
- e. In the function overview page, click **Add trigger**.
- f. In the trigger configuration select **Kinesis** as the source.
- g. Under the expanded input values, locate the "Kinesis stream" option and choose the Kinesis stream that was created as part of the AC Guided Setup.  
Leave all other fields with their default values unless you have specific customization requirements.
- h. Click **Add**.



9. Add necessary permissions to the role associated with the sfCTRTrigger Lambda function.

- a. Navigate to the [AWS Console](#).
  - b. Enter **Lambda** in the search box to access the AWS Lambda service.
  - c. In the Lambda dashboard, click on **Functions**.
  - d. In the search box, enter `sfCTRTrigger` and select the **sfCTRTrigger** function.
  - e. Go to Configuration and click **Permissions**.
  - f. Under Role, click on the role name.
  - g. On the role detail page, navigate to Permission and click **Add permissions**.
  - h. Select the **Attach policies** option.
  - i. In the search box, enter `AmazonKinesisAnalyticsFullAccess` and click the adjacent **+** to select the policy.
  - j. Click **Add permissions**
10. Test the Salesforce Lambda core functionality using the steps described in the [Amazon Connect help content](#).  
If everything is configured correctly, the test will be successful and you can proceed with the configuration.

## Log In as the Integration User

Before you can set up the integration between the voice connector and Einstein Conversation Insights (ECI), a user with Salesforce admin permissions is required to be available for the integration. This user is typically a separate user created for the purpose of integrations. Make sure you're logged in as this user for the configuration tasks.

An integration user is assigned the custom access necessary to complete integrations between ECI and your voice provider. It's a Salesforce best practice to use a separate user for this purpose and to dedicate this user to this integration.

1. Add a user as an integration user by following the standard process to set up a user. See [Add a Single User](#).  
Make sure **System Administrator** is selected for the Profile. The user also needs **API Enabled** enabled, access to the Voice Call object, an ECI access permission set, and the Conversation Insights Integration User permission set assigned.
2. Log in as the integration user, and open the Voice Connector app.
3. Use the integration user to complete the configuration tasks.

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

To enable Einstein Conversation Insights:

- Customize Application

# Set Up Amazon Connect Settings

Amazon Connect object settings and fields must be updated in order for the Voice Connector app to work effectively.

1. From Setup, enter *Object Manager* in the Quick Find box, and then select **Object Manager**.
2. Select **AC Contact Trace Record**.  
If you don't see an AC Contact Trace Record, then the Amazon Connect CTI is not properly installed. See the earlier CTI topic or the Amazon help for more information.
3. Select **Page Layouts**, and then select the default page layout.
4. Add these fields.

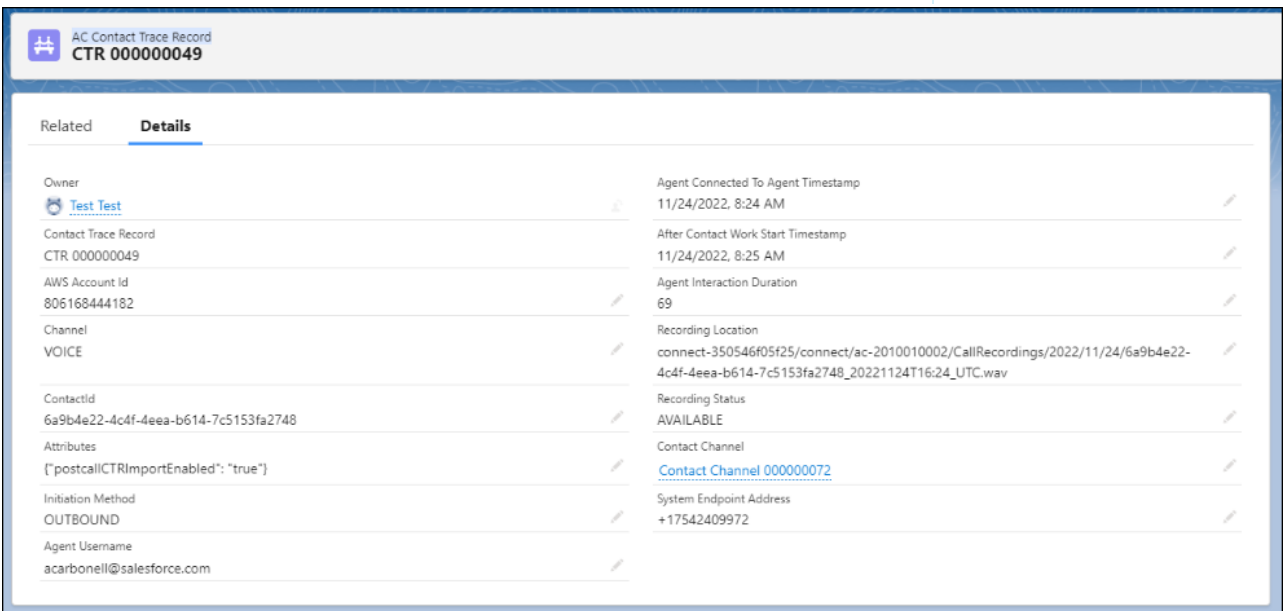
## EDITIONS

Available in: Lightning Experience

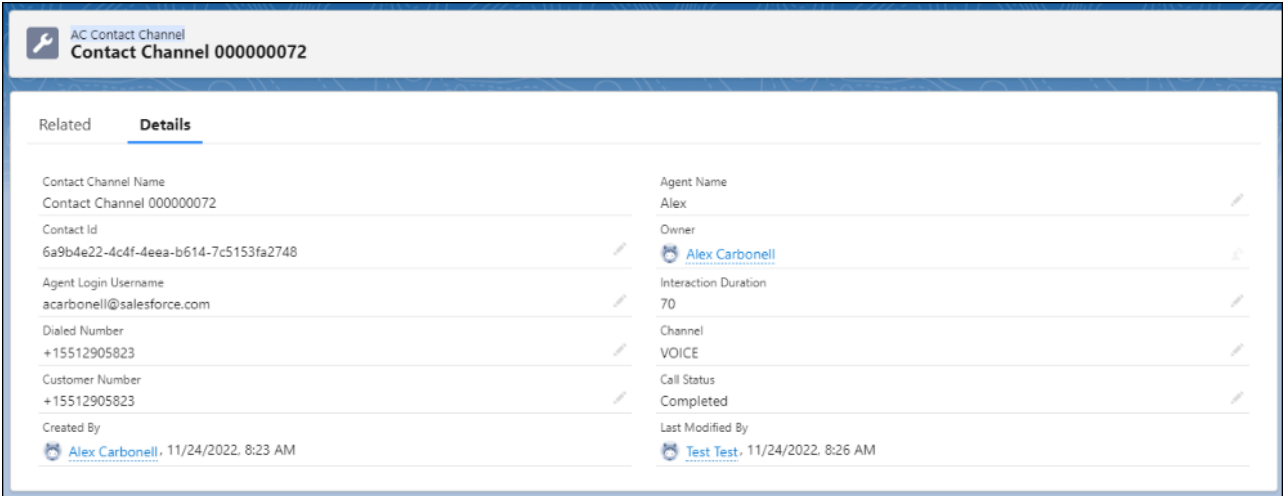
Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

## USER PERMISSIONS

- To enable Einstein Conversation Insights:
- Customize Application



5. Click **Save**.
6. From the Object Manager page, select **AC Contact Channel**.
7. Select **Page Layouts**, and then select the default page layout.
8. Add these fields.



9. Click **Save**.

## Identify Users as Call Owners

When a new call is conducted, some settings must be in place to identify the correct Salesforce user as the call owner. Otherwise, the phone number is used instead (from/to number) and is matched to the Salesforce user (Phone) field in their user profile.

1. Update the `amazonconnect_Amazon_Connect_Username_c` field in each Salesforce user profile. You can use a rule for adding users to a call center. The value of this field must reflect what is shown on the Contact Channel Trace record in the next step.

### EDITIONS

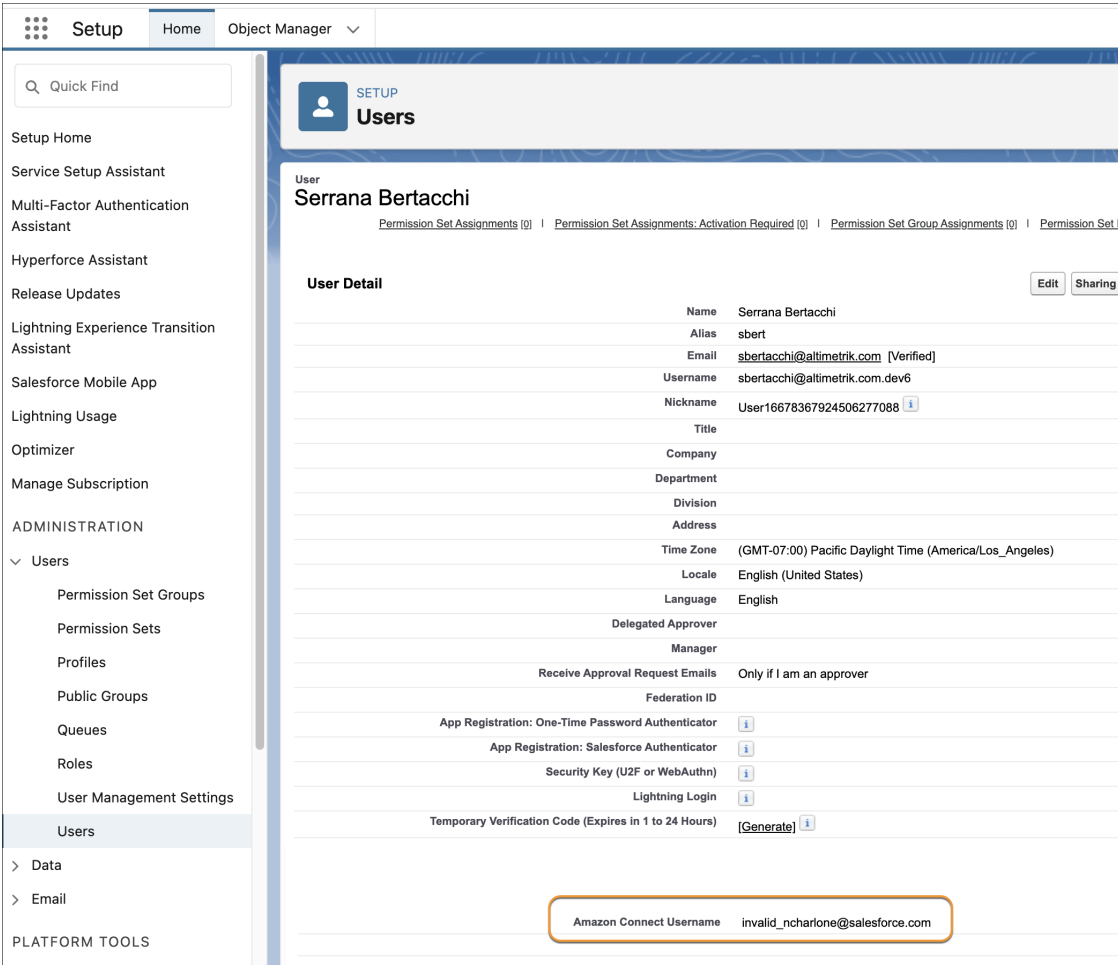
Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

To enable Einstein Conversation Insights:


- Customize Application



2. Configure the Contact Channel Trace object to use the Agent Login UserName field to update the appropriate call owner user. This field should match the value from amazonconnect\_Amazon\_Connect\_Username\_c for each user, if specified. Otherwise it's matched to the Phone Number or Email field.

## Add Amazon Connect Named Credentials

Add the named credentials for the voice provider from the Setup menu.

1. From Setup, enter *Named Credentials* in the Quick Find box, and then select **Named Credentials**.
2. Click the dropdown next to New and select **New Legacy**.
3. Complete these fields with the specified information.
  - Label: *Amazon Connect*
  - Name: *Amazon\_Connect*
  - URL: *https://{bucketName}.{service}.{region}.amazonaws.com*
    -  **Note:** Replace the curly brackets with your Amazon Connect details. (Example: <https://connect-350546f05f25.s3.us-east-1.amazonaws.com>)
  - Identity Type: *Named Principal*
  - Authentication Protocol: *AWS Signature Version 4*
  - ASW Access Key ID: *(Your access key ID from your AWS root user or IAM user)*
  - AWS Secret Access Key: *(Your secret access key generated at the moment of create the access key in your AWS root user or IAM user)*
  - AWS Region: *(The region where you have your bucket created, such as us-east-1)*
  - AWS Service: *(The AWS service you are using, such as s3)*
  - Generate Authorization Header: selected
4. Click **Save**.

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS


To enable Einstein Conversation Insights:

- Customize Application

## Set Up the Connected App

To call the Einstein Conversation Insights (ECI) web service, create a connected app. If you've configured another voice connector, skip the remaining configuration tasks.

 **Note:** The remaining tasks in this guide have been completed if you've configured another connector.

1. From Setup, enter *App Manager* in the Quick Find box, and then select **App Manager**.
2. Click **New Connected App**.
3. Complete these fields in the Basic Information section.
  - Connected App Name: *ECI Connected App*
  - API Name: *ECI\_Connected\_App*
    -  **Important:** Use this exact name.
  - Contact Email: [the email address you want to use]
4. Select **Enable OAuth Settings** and complete these fields.
  - Callback URL: [https://dummy\\_url/services/authcallback/ECI\\_Auth\\_Provider](https://dummy_url/services/authcallback/ECI_Auth_Provider)

### EDITIONS


Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

To enable Einstein Conversation Insights:

- Customize Application

 **Note:** This URL is obtained after you create the Auth Provider in the next section.

- Selected OAuth Scopes:
  - Access content resources (content)
  - Manage user data via APIs (api)
  - Manage user data via Web browsers (web)
  - Perform requests at any time (refresh\_token, offline\_access)
- Require Secret for Web Server Flow: selected
- Require Secret for Refresh Token Flow: selected

**5. Click **Save**.**

Changes can take up to 10 minutes to take effect. Deleting a parent org deletes all connected apps with OAuth settings enabled.

**6. After the ECI Connected App is created, return to the App Manager page. Click the dropdown in the ECI Connected App row, and then click **Manage**.**

**7. Click **Edit Policies**.**

**8. Complete these fields.**

- Permitted Users: *Admin approved users are pre-authorized*
- IP Relaxation: *Relax IP restrictions*
- Refresh Token Policy *Expire refresh token after 365 days*

It's not necessary to select **High assurance session required** even though the checkbox is marked as required.

**9. Click **Save**.**

**10. From the ECI Connected App Setup page, click **Manage Profiles** in the Profiles section.**

**11. Select the profiles you want to give access to, and then click **Save**.**

We recommend selecting Standard User, System Administrator, and any other profiles that use the connected app.

**12. From the App Manager page, select the dropdown in the ECI Connected App row, and then click **View**.**

**13. Click **Manage Consumer Details** to see the Consumer Key and the Consumer Secret.**

A new window opens.

**14. Enter the verification code sent to you over email.**

**15. The Consumer Key and Consumer Secret values are shown. Keep this window open, because these values are required to create the Auth Provider for the ECI Connected App.**

## Add ECI as an Authorized Provider

Add Einstein Conversation Insights (ECI) as an authorized provider from the Setup menu.

1. From Setup, enter *Identity* in the Quick Find box, and then select **Auth. Providers**.
2. Click **New**.
3. Select **Salesforce** for the Provider Type.
4. Complete these fields with the specified information.
  - Name: *ECI Auth Provider*
  - URL Suffix: *ECI\_Auth\_Provider*
5. Click **Save**.
6. Copy the Callback URL, and replace the dummy one in the ECI Connected App.
7. From the App Manager page, go to the ECI Connected App and replace the dummy Callback URL value with the copied one.
8. Click **Save**.

 **Important:** Use this exact name.

- Consumer Key: Add the Consumer Key from the previous task here.
- Consumer Secret: Add the Consumer Secret from the previous task here.

The Callback URL can be obtained.

Changes can take up to 10 minutes to take effect. Deleting a parent org also deletes all connected apps with OAuth settings enabled.

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

To enable Einstein Conversation Insights:

- Customize Application

## Set Up the Salesforce Site

If a site isn't created, set up an active Salesforce site.

1. From Setup, enter *Sites* in the Quick Find box, and then select **Sites**.
2. Select the checkbox, and then select **Register My Salesforce Site Domain**.
3. Click **New**.
4. Complete these fields with the specified information.
  - Site Label: *VoiceConnector*
  - Site Name: *VoiceConnector*
  - Site Contact: [the email address you want to use]
  - Default Record Owner: a Salesforce admin is recommended
  - Active: selected
  - Active Site Home Page: *SiteLogin*
  - Clickjack Protection Level: *Allow framing by the same origin only (Recommended)*
5. Leave the other options as default, and then click **Save**.

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

To enable Einstein Conversation Insights:

- Customize Application



## Add ECI Named Credentials

Add the named credentials for ECI from the Setup menu.

1. From Setup, enter *Named Credentials* in the Quick Find box, and then select **Named Credentials**.
2. Click the dropdown next to New and select **New Legacy**.
3. Complete these fields with the specified information.
  - Label: *ECI Named Credential*
  - Name: *ECI\_Named\_Credential*
  - URL: *https://your\_domain/* Replace "your\_domain" with your actual domain that is obtained from the Domains page in Setup. It's labeled My Domain under the Current HTTPS Option column.
  - Identity Type: *Named Principal*
  - Authentication Protocol: *OAuth 2.0*
  - Authentication Provider: *ECI Auth Provider*
  - Scope: *refresh\_token web api content*
  - Start Authentication Flow on Save: selected
  - Generate Authorization Header: selected
4. Click **Save**.
5. A login and an authorization page are shown. Follow the process to validate the account, and then click **Authorize**.
6. Return to the Named Credentials page and verify that the Authentication Status now reads Authenticated with [your integration user with admin permissions].

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

To enable Einstein Conversation Insights:

- Customize Application

## Assign the Guest User Permission Set

Assign the guest user permission set from Setup.

1. From the Search box at the top of Setup, enter *Guest User* and select **Voice Connector Guest User**.
2. Make sure this user is marked Active.
3. Click **Permission Sets**.
4. Click **Edit Assignments**.
5. Add **Voice Connector Permission**.
6. Add **Conversation Insights Integration User**.
7. Click **Save**.

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

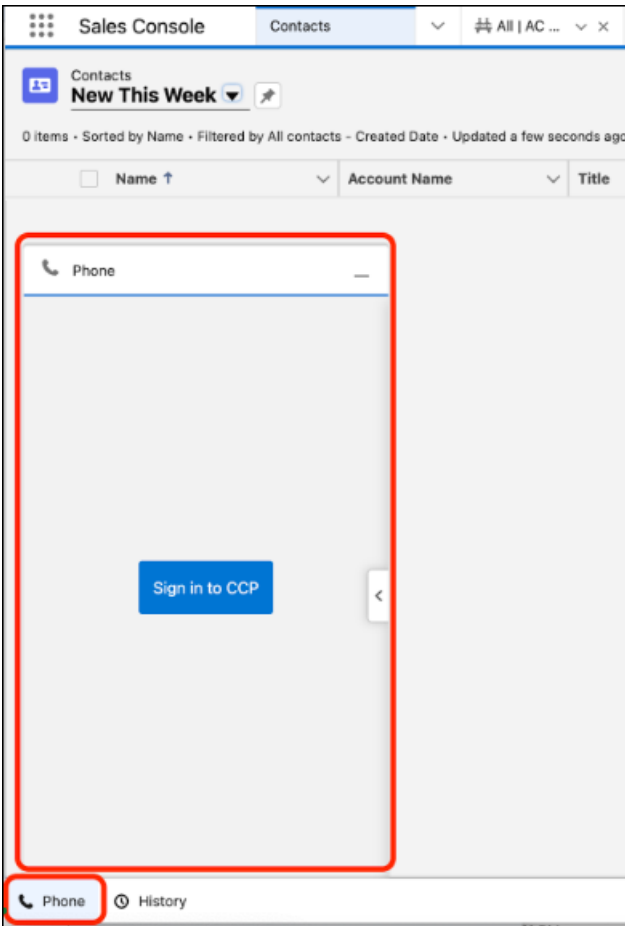
To enable Einstein Conversation Insights:

- Customize Application

## Make Phone Calls with Amazon Connect

After you've finished setting up Amazon Connect with Einstein Conversation Insights, connect to the Amazon Connect control panel to start making phone calls.

1. Navigate to Service Console Home.  
You can also make calls from Sales Console.
2. Click the Phone icon in the bottom left.
3. Connect to the Amazon Connect Control Panel.



You can make outbound calls or receive inbound calls. You will receive an AC Contact Trace if the Amazon Connect CTI was set up correctly.

### EDITIONS

Available in: Lightning Experience

Available in Einstein Conversation Insights, which is available in **Performance** and **Unlimited** Editions, and for an additional cost in **Enterprise Edition**

### USER PERMISSIONS

To enable Einstein Conversation Insights:

- Customize Application