Amazon Connect

Administrator Guide

Amazon Connect: Administrator Guide

Table of Contents

What Is Amazon Connect?

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

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

How Amazon Connect Works

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

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

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

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

Directories

As a first step to setting up an Amazon Connect instance, you can choose either an existing directory in your AWS account/region, or create a new directory. AWS Microsoft AD (or optionally AD Connector) can

integrate with your on-premises AD and users through a trust relationship. You can import individual users from your directory or do a batch upload.

Amazon Connect requires a directory to store user and contact center configuration information. The directory stores all user information and permissions for the instance. Each individual Amazon Connect instance that you create can use the same directory or a unique directory.

> **Note**
> An AWS directory can be used for and associated with a single Amazon Connect instance at a time. Set up the directory in the same region as the Amazon Connect instance.

After a directory has been associated with your Amazon Connect instance, it cannot be changed. You can delete the instance and create a new one. You will have to re-create any buckets and telephone numbers that you had claimed.

- You can use an existing Microsoft Active Directory.
- You can use a proprietary directory. For more information, see Active Directory Connector.
- We can create one for you.

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

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

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

Administrators

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

Secure Storage and Data Integrity

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

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

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

The following security measures are supported:

- AWS Key Management Service—AWS KMS is a powerful, managed service that gives you complete control over your encryption keys. A default AWS KMS key is provided.

- ARN/ID—You can use an ARN/ID instead of an AWS KMS master key. This is an advanced option and should be attempted only if you are confident of the changes that you're going to make.

Supported Browsers

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

Browser	Version	Check your version
Google Chrome	Most recent version	Open Chrome and type chrome://version in your address bar. The version is in the Google Chrome field at the top of the results.
Mozilla Firefox ESR	Most recent version	Open Firefox. On the menu, choose the Help icon and then choose **About Firefox**. The version number is listed underneath the Firefox name.
Mozilla Firefox	Most recent version	Open Firefox. On the menu, choose the Help icon and then choose **About Firefox**. The version number is listed underneath the Firefox name.

Service Limits

The following table provides the default limits per virtual contact center instance. An AWS account can have a maximum of three virtual contact center instances. To request a limit increase, use the Amazon Connect Limits form.

Item	Default limit
Amazon Connect instances per account	10
Users per instance	500
Phone numbers per instance	10
Queues per instance	50
Queues per routing profile	50
Routing profiles per instance	100
Hours of operation per instance	100
Quick connects per instance	100
Prompts per instance	500

Item	Default limit
Agent status per instance	50
Security profiles per instance	100
Contact flows per instance	100
Groups per level	50
Reports per instance	500
Scheduled reports per instance	50
Active calls per instance	100

Related Services

The following services are used with Amazon Connect:

- **AWS Directory Service**—AWS Directory Service for Microsoft Active Directory (Enterprise Edition), also known as Microsoft AD, enables your directory-aware workloads and AWS resources to use managed Active Directory in the AWS Cloud. Amazon Connect user and identity management is based on this service.
- **Amazon S3**—Amazon Simple Storage Service (Amazon S3) is object storage with a simple web service interface to store and retrieve any amount of data from anywhere on the web. Amazon Connect uses Amazon S3 as a primary data storage service/platform for call recordings and metrics reports delivered into your AWS account.
- **AWS Lambda**—Lambda allows you to build and run code quickly without provisioning or managing servers. Amazon Connect contact flows (IVR flows) are integrated with Lambda so you can build a highly personalized and dynamic IVR experience. You can build Lambda functions that communicate with CRM systems or custom services for data dips that influence customer IVR experience (such as customer segmentation and dynamic IVR menus, or account and last contact look ups). Lambda functions can also be used as notification mechanisms to external systems during specific points in the contact flow.
- **Amazon Lex**—Amazon Connect integrates with Amazon Lex to build conversational interfaces using voice and text. Amazon Lex provides the advanced deep learning functionalities of automatic speech recognition (ASR) for converting speech to text, and natural language understanding (NLU) to recognize the intent of the text, to enable you to build applications with highly engaging user experiences and lifelike conversational interactions. For more information, see the Amazon Lex Developer Guide.
- **Kinesis**—Amazon Connect integrates with Kinesis as the platform for streaming contact trace records (CTR), a raw (JSON formatted) output of detailed metadata about a call, in near real time. You can use this data stream to optionally process and publish them into Amazon Redshift (an AWS data warehouse service) or your custom data warehouse systems, enabling detailed analytics and reporting on your contact center data. You can leverage Amazon QuickSight (a cloud-powered business analytics service) or your own BI tools to build powerful visualizations on top of synthesized data. Additionally, this data can be streamed to Elasticsearch to query on this data using a convenient visual interface. For more information, see the Amazon Kinesis Streams Developer Guide.
- **Amazon CloudWatch**—Amazon Connect integrates with CloudWatch to provide you with real-time operational metrics for your contact center, such as total calls per second, calls rejected and throttled, percentage of concurrent calls, failed / missed calls count (errors, bad number/address, busy/line engaged), and contact flow errors. You can set up monitors on these metrics in order to stay on top of the health of your contact center. For more information, see Monitoring Amazon Connect Using Amazon CloudWatch Metrics (p. 12).

- **AWS Identity and Access Management**—The AWS Management Console requires your username and password so that any service you use can determine whether you have permission to access its resources. We recommend that you avoid using AWS account root user credentials to access AWS because root user credentials cannot be revoked or limited in any way. Instead, we recommend that you create an IAM user and add the user to an IAM group with administrative permissions. You can then access the console using the IAM user credentials. For more information, see the IAM User Guide.

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

Getting Started with Amazon Connect

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

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

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

Before You Begin

When you sign up for Amazon Web Services (AWS), your AWS account is automatically signed up for all services in AWS, including Amazon Connect. You are charged only for the services that you use.

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

To create an AWS account

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

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

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

Create an Amazon Connect Instance

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

To create an Amazon Connect instance

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose **Add an instance**.
3. For the **Identity management** step, choose **Store users within Amazon Connect** and type a domain name to complete **Access URL**. This domain is used in your contact center URL and cannot be changed. Choose **Next step**.
4. For the **Administrator** step, you can choose to add an administrator from your directory, create a new administrator, or skip this step for now and add an administrator later on.
5. For the **Telephony options** step, indicate whether you'd like your contact center to accept calls, make calls, or both. You can set the user permissions within the Amazon Connect web application. The telephone number options are provided after setup.
6. For the **Data storage** step, you can keep the default settings or choose **Advanced settings** in order to customize settings. For more information, see Data Storage (p. 9).
7. For the **Review and create** step, review your settings and then choose **Create instance**.

   Important
   This is the only time you can change the directory and domain name settings—you can edit any other setting later on.
8. After your instance is created, choose **Get started** to select and test a phone number. Users can access Amazon Connect using the provided URL.
9. Provide your users with their usernames and passwords so that they can log in and begin accepting and making calls. For more information, see the Amazon Connect User Guide.
10. (Optional) Continue to configure your instance. For more information, see Configuring Your Amazon Connect Instance (p. 9).

Integrate with Your CRM

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

Visit Amazon Connect Contact Streams to integrate the Contact Control Panel (CCP) into your CRM. When completed, add the origin URLs to your instance settings. This enables communication between Amazon Connect and your CRM. For more information, see Application Integration (p. 10).

Delete Your Amazon Connect Instance

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

Important
This operation cannot be canceled or undone.

To delete an Amazon Connect instance

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

Configuring Your Amazon Connect Instance

You can configure your Amazon Connect instance using the AWS Management Console.

Settings

Data Storage

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

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

To update data storage settings

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the name of the instance from **Instance Alias**.
3. In the navigation pane, choose **Data storage**.
4. To update the settings for call recordings, do the following:

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

5. To update the settings for exported reports, do the following:

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

Data Streaming

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

To set up data streaming

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the name of the instance from **Instance Alias**.
3. In the navigation pane, choose **Data streaming**.
4. Choose **Enable data streaming**
5. Select an existing resource from Amazon Kinesis Streams or Amazon Kinesis Firehose, or choose **Create a new Kinesis Firehose**.
6. Choose **Save**.

Application Integration

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

To whitelist a domain URL

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

Contact Flows

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

Security Keys

Amazon Connect can encrypt sensitive data collected by contact flows using public-key cryptography. Provide an X.509 certificate within your contact flow to encrypt data captured using the stored customer

input system attribute. You must upload a signing key in `.pem` format in order to use this feature. The signing key is used to verify the signature of the certificate used within the contact flow.

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

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

To add a security key

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

Amazon Lex

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

To integrate an Lex bot

1. Open the Amazon Connect console at https://console.aws.amazon.com/connect/.
2. Choose the name of the instance from **Instance Alias**.
3. In the navigation pane, choose **Contact flows**.
4. Choose **Add Lex Bot**.
5. Choose your Lex bot from **Lex bots** and choose **Save Lex Bots**.

Monitoring Amazon Connect Using Amazon CloudWatch Metrics

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

VoiceCalls Metrics

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

CallRecordings Metrics

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

ContactFlow Metrics

Metric	Description
`MisconfiguredPhoneNumbers`	Represents the number of calls that failed because the phone number is not configured to a **Contact flow**.
`ContactFlowFatalErrors`	Represents **Contact flow** execution failures.
`ContactFlowErrors`	Represents the number of times the **Contact flow** branched to an `ERROR` label in the instruction.

Queue Metrics

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

Other Metrics

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

Metric Dimensions

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

Metric	Description
`InstanceId`	The Amazon Connect instance ID. This is currently not the complete ARN, just the ID.

Metric	Description
`QueueName`	The name of the queue. This dimension is relevant only for queue metrics.
`ContactFlowName`	The name of the ContactFlow. This dimension is relevant only for ContactFlow metrics.
`MetricGroup`	The category group. The following category groups are supported: `CallRecordings`, `ContactFlow`, `Queue`, and `VoiceCalls`.

Granting Amazon Connect Access to AWS Lambda Functions

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

Environment variables indicate where to store output and logging settings, and specify the correct directory for files to be installed. By separating these settings from the application logic, you don't need to update your function code when you need to change the function behavior based on different settings.

Environment variables for Lambda functions enable you to pass settings dynamically to your function code and libraries, without making changes to your code. Environment variables are key-value pairs that you create and modify as part of your function configuration. Lambda makes these key-value pairs available to your Lambda function code.

Lambda Function Invocation from IVR

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

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

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

This command uses the following input:

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

Lambda Interaction Model

On every Lambda function invocation from a contact flow, you pass a default set of information related to ongoing contact as well as parameters specified by the user during contact flow creation.

Request

When you invoke a Lambda function, the set of parameters passed can be seen in the model definition. Below is an example request JSON which will be present in the `event` input of the Lambda function.

```
"event" : {
   "Name":"ContactFlowExecution",
   "Details":{
      "Parameters":{
         /* These are parameters that are specified by a user while configuring the contact
 flow */
         "key1":"value1",
         "key2":"value2"
      },
      "ContactData":{
         /* Unique contact Id */
         "ContactId":"ASDAcxcasDFSSDFs",
         /* Optional: Original id is present in cases like transfer */
         "OriginalContactId":"Acxsada-asdasdaxA",
         "PreviousContactId":"Acxsada-agdasdaxA",
         "Channel":"Voice",
         "InstanceARN": organization ARN
         "InitiationMethod":"Inbound/Outbound/Transfer/Callback",
         /* Optional: Will be missing for outbound calls */
         "SystemEndpoint":{
            "Type":"TELEPHONE_NUMBER",
             /* DNIS to which call came in */
            "Address":"01234567",
         },
         "CustomerEndpoint":{
            "Type":"TELEPHONE_NUMBER",
            /* Customer's phone number */
            "Address":"+12065555555"
         },
          /* Optional: May not be present for outbound calls.*/
         "Queue" : {
             /* Name of queue */
             "Name":"PrimaryPhoneQueue",
              /* Arn of the queue. */
              "ARN" : "",
         },
            /* Map of all contact attributes. These are set using the Set contact attribute
 block in the contact flow. */
         "Attributes":{
            "key1":"value",
            "key2":"value"
         }
      }
   }
}
```

The request is divided into three parts:

- Contact data—This is always passed by Amazon Connect for every contact. Some parameters are optional.
- User attributes—These are attributes saved in a contact flow based on previous **Set attributes** blocks in the contact flow. This map may be empty if there aren't any saved attributes.
- Parameters—These are parameters specific to this call.

The Lambda function response should be a simple Map *String String*. This map can be up to 32k. If you fail to reach Lambda, the function throws an exception, the response is not understood, or the Lambda function takes more time than the limit, the contact flow jumps to the `Error` label. The following code is an example Python Lambda function:

```
def lambda_handler(event, context):
     resultMap = {"lambdaResult":"Success"};
     return resultMap;
```

Sample NodeJS lambda function

```
exports.handler = (event, context, callback) => {
    console.log("Received event from Lily");
    callback(null, buildResponse());
};

function buildResponse() {
    return {
        foo: "bar",
        lambdaResult:"Success"
    };
}
```

The Lambda key being returned in this example is `State`. The return from the Lambda function must be a flat object of key/value pairs (no nested or complex objects) where the values are numbers, strings, or booleans. The properties available to access using JsonPath is the full `ContactData` object sent to your Lambda function as well as an `External` object that holds all of the properties returned by the last Lambda invocation. For example, you can access `$.External.key` or `$.CustomerEndpoint.Address`. You can also use attributes returned via Lambda in certain blocks using the **Use attributes** option.

Contact Flow External Invocation

You can use the following definition for an external contact flow:

```
def lambda_handler(event, context):

    customerPhoneNumber =
 event.get('Details').get('ContactData').get('CustomerAddress').get('Value');

    if authenticateCustomer(customerPhoneNumber) == "true":
        resultMap = {"isCustomerAuthenticated": "true" }
        return resultMap;
    else :
        resultMap = {"isCustomerAuthenticated": "false" }
        return resultMap;

def authenticateCustomer(customerPhoneNumber) :
    #We hardcode list of authenticated numbers. In production, make an external web service
 call to figure out if a customer is authenticated.
    customer_list = ["+12065555555"];
    if (customerPhoneNumber in customer_list) :
        return "true";
    else :
        return "false";
```

Amazon Connect and Salesforce Integration

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

We recommend that you initially install the package into your Salesforce sandbox. After the package is installed, you can configure your Salesforce Call Center configuration within Salesforce. This configuration is a XML file that you import into your call center. It provides all the details required to enable the CTI.

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

Prerequisites

- Salesforce Classic, Salesforce Console, or Lightning Experience
- An Amazon Connect instance
- A Firefox or Chrome browser

To integrate with Salesforce

1. In your Salesforce sandbox, install the following managed package: Amazon Connect CTI Adapter.
2. Download the AmazonConnectCallCenterConfig.xml file and import it into your Salesforce call center configuration.
3. Edit the call center configuration as follows:
   - For **CTI Adapter URL**, type the one of the following, based on your Salesforce interface:
     - **`/apex/amazonconnect__ACSFCCP_Classic`**
     - **`/apex/amazonconnect__ACSFCCP_Console`**
     - **`/apex/amazonconnect__ACSFCCP_Lightning`**
   - For **Salesforce Compatibility Mode**, choose **Classic** for the Salesforce Classic and Salesforce Console or **Lightning** for Lightning Experience.
   - For **Amazon Connect CCP URL**, type the CCP URL for your instance (for example, https://*instance*.awsapps.com/connect/ccp).

- For **Phone Number Formatting**, **Country**, specify the appropriate 2-digit ISO country code.
- To provide users with access to the CCP, choose **Manage Call Center Users**.

4. Whitelist your Salesforce Visualforce domain URL using the directions in Application Integration (p. 10). This URL usually has the following format:

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

   To verify the URL, open the Visualforce page in setup.
5. Log in to your Amazon Connect instance.
6. Launch Salesforce. You should see the integrated CCP in the side panel (Salesforce Classic) or the phone toolbar (Salesforce Classic and Lightning Experience).

Document History

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

Change	Description	Date
Initial release	Initial release of the *Amazon Connect Administrator Guide*.	March 28, 2017