

# Amazon Connect Connected System

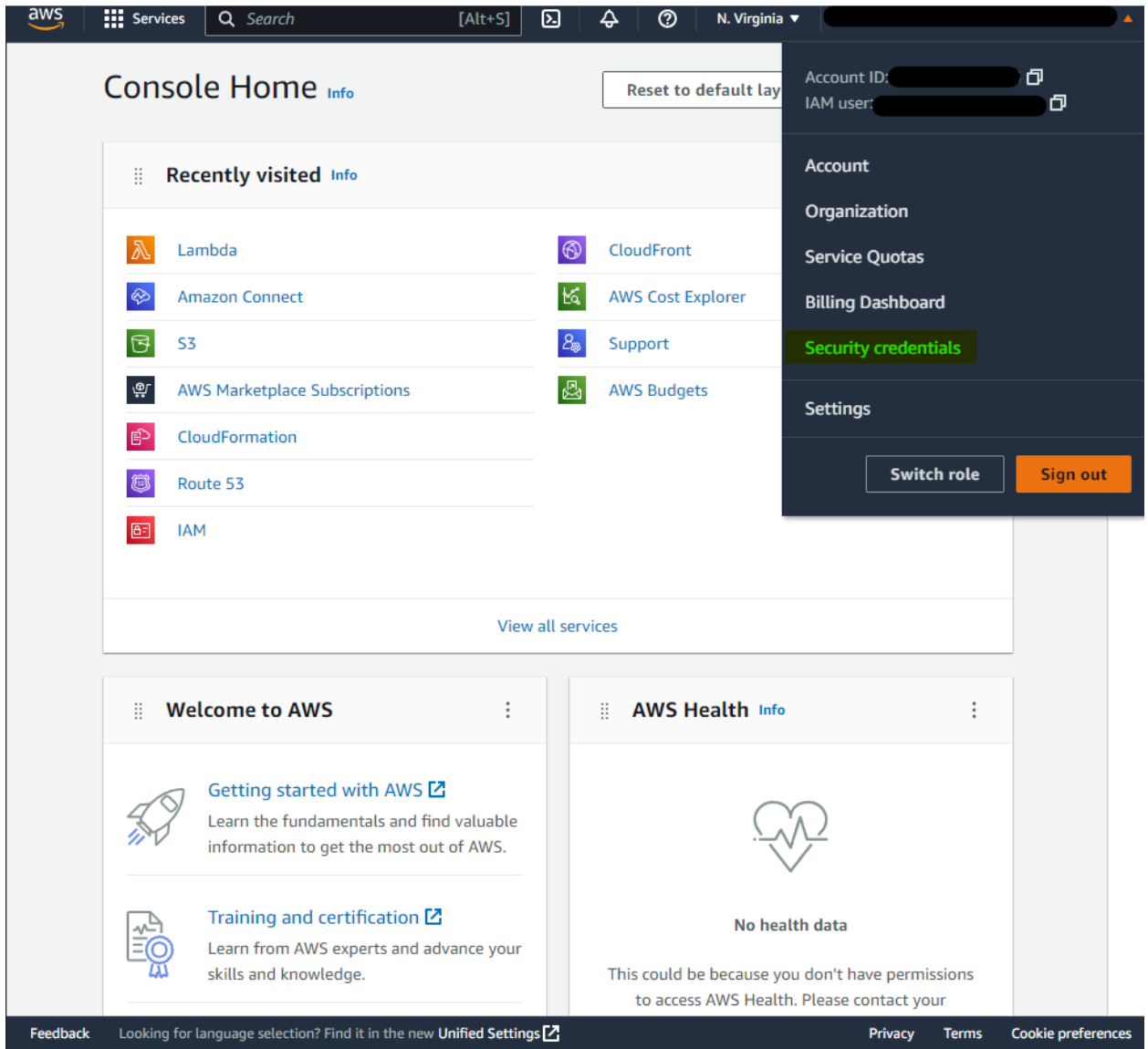
## Overview

The Amazon Connect Connected System plugin provides the integrations to retrieve the contact analysis, reports and recordings stored by the Amazon Connect Instance in the Amazon S3 storage bucket.

## Creating an Access Key in AWS Instance

1. Login to your AWS Console.

2. Click on your username and in the appearing pop up select Security Credentials.



3. In the Security credential window, scroll down to the Access keys section and click on the Create Access Key button to create a new one.

The screenshot displays the AWS IAM console interface. On the left is a navigation sidebar for 'Identity and Access Management (IAM)' with sections for 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings) and 'Access reports' (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). Below the sidebar is a 'Related consoles' section with a link to 'IAM Identity Center' marked as 'New'. The main content area is divided into three sections: 1. 'MFA devices' section with a message 'No MFA devices. Assign an MFA device to improve the security of your AWS environment' and an 'Assign MFA device' button. 2. 'Access keys (1)' section with a description of access keys and a 'Create access key' button. Below this is a table with one entry: Description: [redacted], Status: Active, Last used: 18 hours ago, Created: 92 days ago, Last used region: [redacted], Last used service: lambda. 3. 'Signing certificates (X.509) (0)' section with a description and buttons for 'Actions', 'Upload', and 'Create X.509 certificate'.

Device type	Identifier	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment		

[Assign MFA device](#)

**Access keys (1)**  
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

[Create access key](#)

		Actions
Description	-	Status Active
Last used	18 hours ago	Created 92 days ago
Last used region	[redacted]	Last used service lambda

**Signing certificates (X.509) (0)**  
Use X.509 certificates to make secure SOAP-protocol requests to some AWS services. You can have a maximum of two X.509 certificates (active or inactive) at a time. [Learn more](#)

[Actions](#) [Upload](#) [Create X.509 certificate](#)

4. In the appearing list of options, select Third-party service and click on Next.

IAM > Security credentials > Create access key

Step 1 of 3

## Access key best practices & alternatives

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

- Command Line Interface (CLI)**  
You plan to use this access key to enable the AWS CLI to access your AWS account.
- Local code**  
You plan to use this access key to enable application code in a local development environment to access your AWS account.
- Application running on an AWS compute service**  
You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.
- Third-party service**  
You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.
- Application running outside AWS**  
You plan to use this access key to enable an application running on an on-premises host, or to use a local AWS client or third-party AWS plugin.
- Other**  
Your use case is not listed here.

Cancel **Next**

5. In the next window, provide a description tag. This is an optional step. Click on Create Access key to proceed.

The screenshot shows the AWS IAM console interface. On the left is a navigation sidebar for 'Identity and Access Management (IAM)' with a search bar and a list of categories: 'Access management' (User groups, Users, Roles, Policies, Identity providers, Account settings) and 'Access reports' (Access analyzer, Archive rules, Analyzers, Settings, Credential report, Organization activity, Service control policies (SCPs)). At the bottom of the sidebar is a 'Related consoles' section with a link to 'IAM Identity Center' marked as 'New'. The main content area is titled 'IAM > Security credentials > Create access key' and shows 'Step 2 of 3' with the heading 'Set description tag - optional'. A sub-heading explains: 'The description for this access key will be attached to this user as a tag and shown alongside the access key.' Below this is a form for 'Description tag value' with a text input field and a note: 'Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.' A second note specifies: 'Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: \_ . : / = + - @'. At the bottom of the form are three buttons: 'Cancel', 'Previous', and 'Create access key'.

6. The Access Key ID and the Secret access key will be displayed. The credentials can also be downloaded as a CSV file by clicking on the Download .csv file button. Please make sure that the credentials are noted which will not be visible again once the Done button

is clicked.

**Identity and Access Management (IAM)**

Search IAM

Dashboard

▼ Access management

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access analyzer
  - Archive rules
  - Analyzers
  - Settings
- Credential report
- Organization activity
- Service control policies (SCPs)

Related consoles

IAM Identity Center [New](#)



**Access key created**  
This is the only time that the secret access key can be viewed or downloaded. You cannot recover it later. However, you can create a new access key any time.

IAM > Security credentials > Create access key

Step 3 of 3

## Retrieve access keys

**Access key**  
If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
 [Redacted]	 ***** <a href="#">Show</a>

**Access key best practices**

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [Best practices for managing AWS access keys](#).

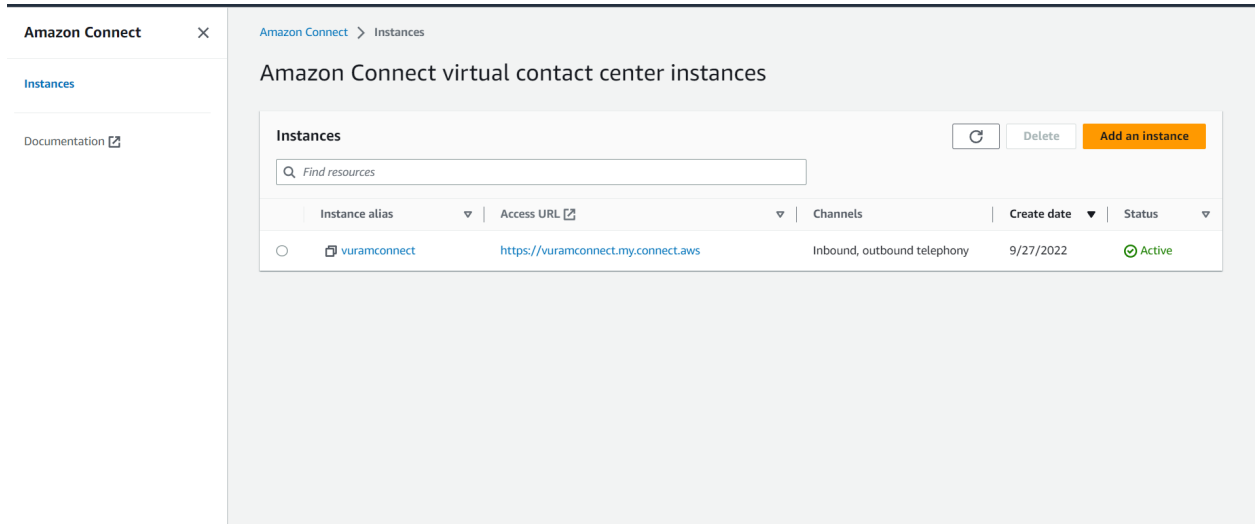
[Download .csv file](#) [Done](#)

7. Make sure that the Access key is active.

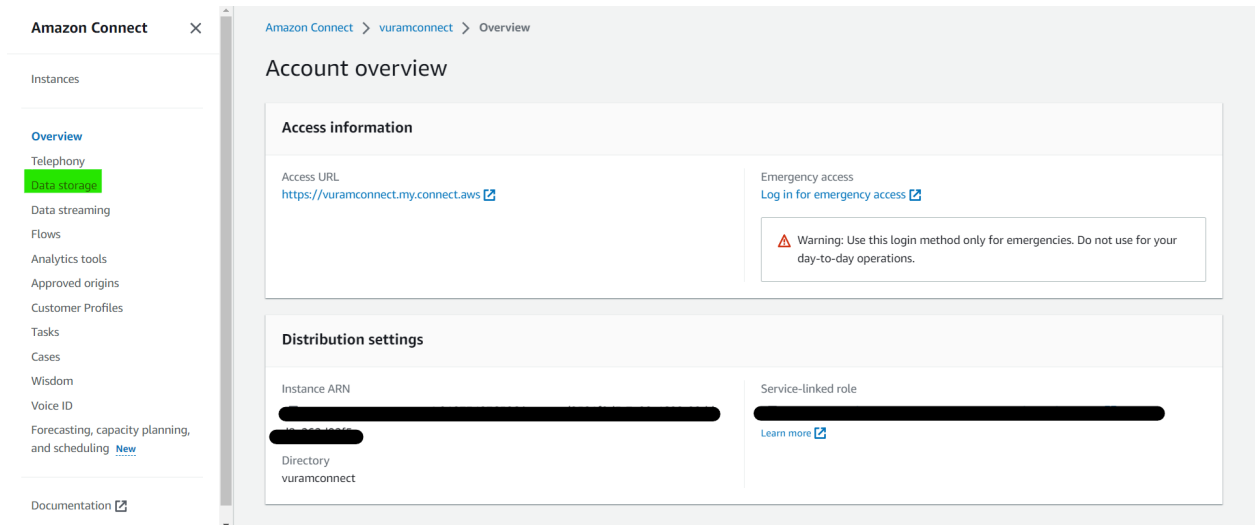
## Getting the Storage Bucket Name

1. Login to the AWS Console.

2. Select Amazon Connect. And the instances page will be opened, click on the instance.



3. Select data storage and navigate to the Exported Reports section.



4. The part of the url before the first '/'(forward slash) is the bucket name. The folders can be retrieved by navigating to the S3 bucket.

The screenshot displays the Amazon Connect console interface. On the left is a navigation sidebar with the following menu items: Instances, Overview, Telephony, **Data storage**, Data streaming, Flows, Analytics tools, Approved origins, Customer Profiles, Tasks, Cases, Wisdom, Voice ID, Forecasting, capacity planning, and scheduling (with a 'New' tag), and Documentation. The main content area is titled 'Amazon Connect' and contains four settings cards:

- Live media streaming**: Not enabled. Edit button.
- Exported reports**: Not enabled. Edit button. Below the title, it states: 'Exported reports will be stored in this S3 bucket' followed by a redacted bucket name 'amazon-connect-8196d473568' and 'Encrypted using this key' followed by a redacted key.
- Attachments**: Not enabled. Edit button.
- Contact evaluations**: Not enabled. Edit button.

Connected System



# Connected System Properties



## Amazon Connect

Authenticates the AWS account with the provided access keys and exposes client APIs to get the contact information stored in the S3 bucket configured in the Amazon Connect instance.

Version: 1

### Name \*

### Description

### Amazon Connect Configuration

#### Access Key

\*\*\*\*\* [\(Clear\)](#)

Provide the AWS Access Key.

#### Secret Key

\*\*\*\*\* [\(Clear\)](#)

Provide the AWS Secret Key

#### S3 Storage Bucket \*

Provide the S3 bucket where the recordings and transcripts will be stored.

#### Region \*

Select the region where the AWS instance is located.

**TEST CONNECTION**

CANCEL

USE IN NEW INTEGRATION

SAVE

Provide the access key, secret key values generated from AWS Security Console. Use the S3 storage bucket name as obtained by the steps discussed in the previous section. Choose the region of your S3 instance from the list and press the Test Connection button to check whether the connection is established without any errors.

## Available Integrations

1. Get Contact Report
2. Get Contact Analysis
3. Get Contact Recording

## Get Contact Report

Retrieves the generated contact transcripts from the S3 storage location. Available only for chat contact types.

The screenshot displays the configuration for the 'Get Contact Report' operation in the Amazon Connect console. The 'Operation' is set to 'Get Contact Report (Reads Data)'. The 'Folder Name' is 'connect/Vuramconnect/ChatTranscripts/'. The 'Contact Information' is provided as a JSON object:

```
1  altoJson(  
2  {  
3    id: "37b21506-4ff2-4f3b-8bc8-3b7d2fe359f7",  
4    contactType: "chat",  
5    contactDuration: 49,  
6    contactStartTime: "2023-04-24T08:06:32.266Z",  
7    contactQueue: {  
8      queueARN: "arn:aws:connect:us-east-1:910734276586:in",  
9      name: "BasicQueue",  
10     queueId: "arn:aws:connect:us-east-1:910734276586:ins",  
11   },  
12   isInbound: true  
13 }  
14 )
```

The 'altoJson' function is used to convert the contact information into a JSON string. The 'TEST REQUEST' button is visible at the bottom.

The right side of the screenshot shows the 'Result' tab, indicating a successful operation:

- Success!**
- Time:** 140 ms
- Prepare:** < 1 ms - **Execute:** 139 ms (Send/Wait/Receive: 136 ms) - **Transform:** 1 ms
- Value:**
  - Dictionary: success **true** (Boolean)
  - result Dictionary:
    - InitialContactId "37b21506-4ff2-4f3b-8bc8-3b7d2fe359f7" (Text)
    - Transcript List of Dictionary - 13 Items
    - AWSAccountid "910734276586" (Text)
    - Version "2019-08-26" (Text)
    - InstanceId "0581f9d5-7a99-4602-82dd-d8e262d02f5c" (Text)
    - Contactid "37b21506-4ff2-4f3b-8bc8-3b7d2fe359f7" (Text)
  - Participants List of Dictionary - 3 items
    - Dictionary: Participantid "5c3f889a-74a5-46d8-888c-ea29de8a135e" (Text)
    - Dictionary: Participantid "b8c5bb4f-6512-41f2-9908-e3d43a5ee952" (Text)
    - Dictionary: Participantid "920d85ee-90be-4240-8a7e-ba6a460d848e" (Text)
  - error **null** (Null)
  - authType Diagnostic

## Parameters

1. **Folder Name** - The S3 bucket URL substring where the contact reports are stored. (\*Required)
2. **Contact Information** - The contact information dictionary as obtained from the *onContactEnded save-into* of the *Amazon Connect Component*. Must be provided as a *JSON formatted string*.

## Get Contact Analysis

Retrieves the generated contact analysis reports from the S3 storage location. Analysis reports are generated shortly after the contact ends and hence there will be delays. It supports both chat and voice contact types.

The screenshot displays the AWS Lambda console interface for the 'AC CS Amazon Connect' function. The 'Configuration' tab is active, showing the following details:

- Operation:** Get Contact Analysis (Reads Data)
- Folder Name:** Analysis/
- Contact Information:** A JSON object is provided in the `altoJson` parameter, containing contact details such as `id`, `contactType`, `contactDuration`, `contactStartTime`, and `contactQueue`.

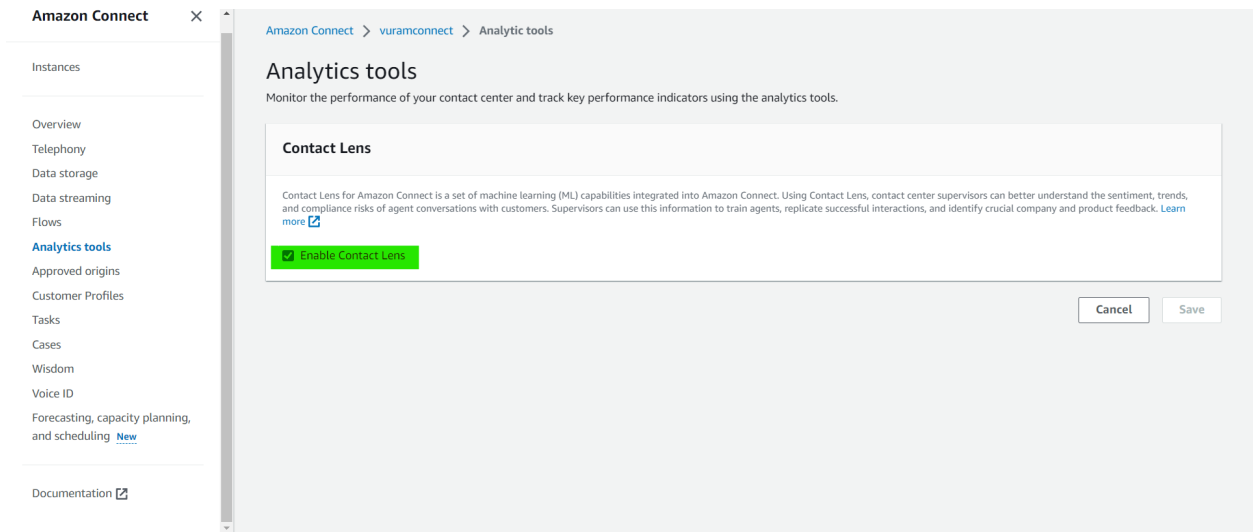
The 'Execution' tab on the right shows a successful result with a status of 'Success!'. The execution time is 210 ms. The response value is a dictionary containing:

- `success`: true (Boolean)
- `result`: Dictionary
  - `JobStatus`: "COMPLETED" (Text)
  - `LanguageCode`: "en-US" (Text)
  - `Transcript`: List of Dictionary - 19 items
  - `AccountId`: "910734276586" (Text)
  - `Version`: "1.1.0" (Text)
  - `Categories`: Dictionary
  - `CustomModels`: List of Variant - 0 items
  - `Channel`: "VOICE" (Text)
  - `Participants`: List of Dictionary - 2 items
  - `ConversationCharacteristics`: Dictionary
  - `CustomerMetadata`: Dictionary
  - `ContentMetadata`: Dictionary
    - `Output`: "Raw" (Text)
  - `error`: null (Null)
  - `authType`: Diagnostic

## Parameters

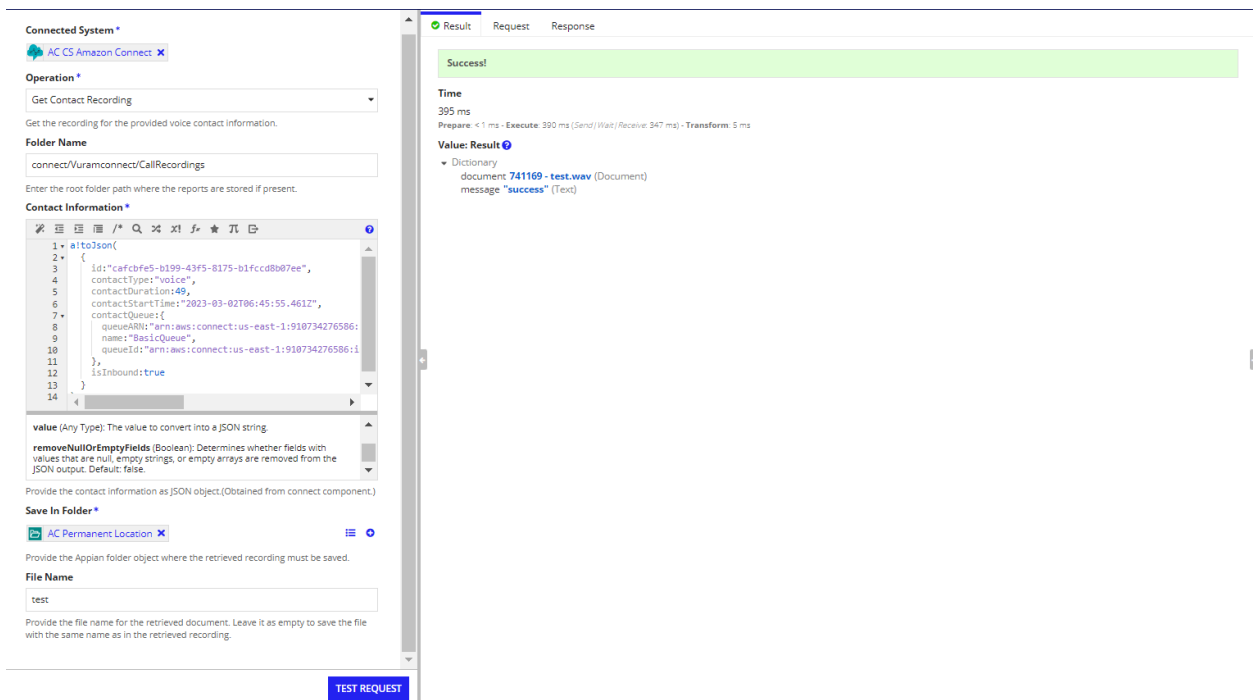
- Folder Name** - The S3 bucket URL substring where the contact reports are stored. (\*Required)
- Contact Information** - The contact information dictionary as obtained from the `onContactEnded save-into` of the *Amazon Connect Component*. Must be provided as a *JSON formatted string*.

**Note:** In order to enable contact analysis, Contact Lens feature must be enabled in the instance page of Amazon Connect in the AWS console.



## Get Contact Recording

Retrieves the recording of the given voice contact from the S3 storage location and saves it to the specified Appian folder. Available only for voice contact type.



## Parameters

1. **Folder Name** - The S3 bucket URL substring where the contact reports are stored. (\*Required)
2. **Contact Information** - The contact information dictionary as obtained from the *onContactEnded save-into* of the *Amazon Connect Component*. Must be provided as a *JSON formatted string*.
3. **Save In Folder** - The Appian folder object where the retrieved recording must be saved. (\*Required)
4. **File Name** - The name with which the retrieved recording has to be saved. (Optional)

**Note: The Amazon Connect Connected System plugin requires the Amazon Connect Component plugin to function.**

**Note: Amazon connect is available only in certain regions. Please refer to the [link](#) to know more.**