Amazon SQS Connector Documentation

Last Modified on 03/18/2024 11:49 am EDT

On this page:

Authentication Prerequisites

The Amazon SQS connector uses the OAuth 2.0 authentication workflow. Before you can authenticate an instance of the Amazon SQS connector, you need the following:

Provider sandbox

A trial Amazon SQS account and sandbox are required.

Create an Amazon SQS App

To create an Amazon SQS app and register it with your Amazon SQS account, follow these steps:

1. Navigate to the site.
2. Create app.
3. Register app.

Generate Oauth Credentials

After creating and registering your app, you can generate the necessary Oauth credentials for ≠authentication.

1. Click **Credentials.**
2. Select **Generate**.
3. Note your AWS Access Key and Secret Keyk which you will need for authentication.

Required Authentication Parameters

You can authenticate a connector instance using the UI or via API calls. For detailed information on how to authenticate an instance, see our related documentation:

- Authenticate a Connector Instance (UI)
- Authenticate a Connector Instance (API)

To authenticate an instance of the Amazon SQS connector, you will need the following parameters:

Parameter Name/UI Value	API Value	Description	Source
Name	name	The name of your connector instance	n/a
AWS Access Key	sqs.access_key	The API access key for your AWS account.	Generated as part of the credentials for your app; see **Generate Oauth Credentials above.**
AWS Secret Key	sqs.secret_key	The API secret key for your AWS account.	Generated as part of the credentials for your app; see **Generate Oauth Credentials above.**
AWS Region	sqs.region_name	The name of the region where your tenant server is hosted.	Found in your tenant URL; for example, https://[URL].amazon.sqs.fakesite, eg .fakesite
Visibility Timeout	sqs.message_visibility_timeout	How soon your messages and functions are removed from the interface, measured in seconds.	Determined by your account administrator.

Sample Configuration JSON

```
{
  "name": "myCoolInstance",
  "configuration": {
    "synchronous.bulk.notification": "true",
    "sqs.access_key": "******",
    "sqs.secret_key": "******",
    "sqs.region_name": "myRegion",
    "sqs.message_visibility_timeout": "180"
  }
}
```

Connector Fact Sheet and Reference

Authentication and Configuration Parameters

To see all authentication parameters for the Amazon SQS connector, follow these steps:

1. Sign in to SAP Open Connectors and navigate to Connectors.
2. Hover over the card for a connector, and then click My Resources.
3. In the top navigation toolbar, click Setup.
4. From the **Setup** page, you can view a complete list of the connector's authentication and configuration parameters.

Events and Supported Resources

The Amazon SQS connector supports events via webhooks. For detailed information about our Events framework and

how to configure a connector instance with events, see our documentation:

- Authenticate a Connector Instance with Events (UI)
- Authenticate a Connector Instance with Events (API)

You can set up polling events for the following resources of the Amazon SQS connector:

- [LIST_OF_EVENT_CONFIG_PARAMETERS]

Objects and Supported Operations

Object	Operations	Bulk Support (y/n)
[OBJECT_1]	GET /accounts POST /accounts GET /accounts/{id}	Y
[OBJECT_2]	GET /contacts POST /contacts GET /contacts/{id}	Y
[OBJECT_3]	GET /credit-notes POST /credit-notes GET /credit-notes/{id}	Y
ETC		

Queryable Endpoints

You can use OCNQL to query the following endpoints of the Amazon SQS connector:

- GET /{objectName}
- GET /endpoint2
- GET /endpoint3/{id}

API Documentation

Provider Documentation

- Amazon SQS API Reference
- API Documentation