AWS Single Sign-On

User Guide

Documentation - This Guide

Search

[Documentation](#) » [AWS Single Sign-On](#) » [User Guide](#) » [Manage Your Identity Source](#) » [Connect to Your External Identity Provider](#) » [Supported Identity Providers](#) » Okta

This prerelease documentation is confidential and is provided under the terms of your nondisclosure agreement with Amazon Web Services (AWS) or other agreement governing your receipt of AWS confidential information.

Okta

AWS SSO supports automatic provisioning (synchronization) of user and group information from Okta into AWS SSO using the System for Cross-domain Identity Management (SCIM) v2.0 protocol. You configure this connection in Okta using your SCIM endpoint for AWS SSO and a bearer token that is created automatically by AWS SSO. When you configure SCIM synchronization, you create a mapping of your user attributes in Okta to the named attributes in AWS SSO. This causes the expected attributes to match between AWS SSO and your IdP.

Okta supports the following provisioning features when connected to AWS SSO via SCIM:

- Create users – Users assigned to the AWS SSO application in Okta will be provisioned in AWS SSO.
- Update user attributes – Attribute changes for users assigned to the AWS SSO application in Okta will be updated in AWS SSO.
- Deactivate users – Users unassigned from the AWS SSO application in Okta will be disabled in AWS SSO.
- Group push – Groups (and their members) in Okta will be synchronized to AWS SSO.

The following steps walk you through how to enable automatic provisioning of users and groups from Okta to AWS SSO using the SCIM protocol.

> **Note**
>
> Before you begin deploying SCIM, we recommend that you first review the [Considerations for Using Automatic Provisioning](#). Then continue reviewing additional considerations in the next section.

Topics

Additional Considerations

The following are important considerations about Okta that can impact how you implement provisioning with AWS SSO.

- Using the same Okta group for assignments and also for group push is not currently supported. To maintain consistent group memberships between Okta and AWS SSO, you need to create a separate group and configure it to push groups to AWS SSO.
- If you update a user’s address you must have **streetAddress**, **city**, **state**, **zipCode** and the **countryCode** value specified. If any of these values are not specified for the Okta user at the time of synchronization, the user or changes to the user will not be provisioned.
- Entitlements and role attributes are not supported and cannot be synced to AWS SSO.

Prerequisites

You will need the following before you can get started:

- An Okta account (free trial) with Okta's AWS Single Sign-on application installed.
- A SAML connection from your Okta account to AWS SSO, as described in How to Configure SAML 2.0 for AWS Single Sign-On.
- An AWS SSO-enabled account (free). For more information, see Enable AWS SSO.

Step 1: Enable Provisioning in AWS SSO

In this first step, you will use the AWS SSO console to enable automatic provisioning.

To enable automatic provisioning in AWS SSO

1. Open the AWS SSO console.

2. Choose **Settings** in the left navigation pane.

3. On the **Settings** page, under **Identity source**, choose **Enable automatic provisioning**. This immediately enables automatic provisioning in AWS SSO and displays the necessary endpoint and access token information.
4. In the **Inbound automatic provisioning** dialog box, copy each of the values for the following options. You will need to paste these in later when you configure provisioning in Okta.
    a. **SCIM endpoint**
    b. **Access token**
5. Choose **Close**.

Now that you have set up provisioning in the AWS SSO console, you need to do the remaining tasks using the Okta user interface as described in the procedures below.

Step 2: Configure Provisioning in Okta

Use the following procedure in the Okta admin portal to enable integration between AWS SSO and the AWS Single Sign-On app.

To configure provisioning in Okta

1. In a separate browser window, login to the Okta admin portal and navigate to the AWS Single Sign-On app.
2. In the AWS Single Sign-On app page, select the **Provisioning** tab, and then choose **Integration**.
3. Choose **Configure API Integration**, then select the check box next to **Enable API integration** to enable provisioning.
4. In the previous procedure you copied the **SCIM endpoint** value in AWS SSO. Paste that value into the **Base URL** field in Okta. Make sure to remove the trailing forward slash at the end of the URL. Paste that value into the **API Token** field in Okta.
5. Choose **Test API Credentials** to verify the credentials entered are valid.
6. Choose **Save**.
7. Under **Settings**, select **To App**, choose **Edit**, and then for each of the **Provisioning Features** you want to enable check the box next to **Enable**.
8. Choose **Save**.

By default, no users or groups are assigned to your Okta AWS Single Sign-On app so you will need to complete the next procedure to begin synchronizing users and groups to AWS SSO.

Step 3: Assign Access for Users and Groups in Okta

Use the following procedures in Okta to assign access to your users and groups. All Okta users that belong to groups that you assign here will also be synchronized automatically to AWS SSO. To minimize administrative overhead in both Okta and AWS SSO, we recommend that you assign and *push* groups instead of individual users.

After you complete this step and the first synchronization with SCIM has completed, the users and groups you've assigned will appear in AWS SSO, and will be able to access the AWS SSO user portal using their Okta credentials.

To assign access for users in Okta

1. In the **AWS Single Sign-On app** page, select the **Assignments** tab.
2. In the **Assignments** page, select **Assign**, then choose **Assign to People**.
3. Choose the Okta user or users you want to assign access to the AWS Single Sign-On app, choose **Assign**, choose **Save and Go Back**, and then choose **Done**. This will start the process of provisioning the user or users into AWS SSO.

To assign access for groups in Okta

1. In the **AWS Single Sign-On app** page, select the **Assignments** tab.
2. In the **Assignments** page, select **Assign**, then choose **Assign to Groups**.
3. Choose the Okta group or groups you want to assign access to the AWS Single Sign-On app, choose **Assign**, choose **Save and Go Back**, and then choose **Done**. This will start the process of provisioning the users in the group into AWS SSO.
4. Select the **Push Groups** tab, choose the Okta group or groups you just selected in the previous step, and then choose **Save**. The group status will change to **Active** once the group and its members have successfully been pushed to AWS SSO.

To grant your Okta users access to AWS accounts and cloud applications, complete the following applicable procedures using the AWS SSO console:

- To grant access to AWS accounts, see Assign User Access.
- To grant access to cloud applications, see Assign User Access.

Troubleshooting

The following can help you troubleshoot some common issues you might encounter while setting up automatic provisioning with Okta.

Base URL: Does not match required pattern

The SCIM endpoint URL you pasted into **Base URL** likely contains a trailing forward slash (/). Remove the forward slash from the SCIM endpoint URL before pasting into **Base URL**. For example, https://scim.us-east-2.amazonaws.com/xxxxxxxx-xxxx-xxxxx-xxxxxx-xxxx/scim/v2.

Error during synchronization

After you have started synchronization, you might see the following error:

```
Automatic profile push of <user> to app AWS Single Sign-on failed: Error while trying to
push profile update for <user>@Corp.Example.com: Bad Request. Errors reported by remote
server: Request is unparsable, syntactically incorrect, or violates schema.
```

For SCIM synchronization to work:

- Every user must have a **First name**, **Last name**, **Username** and **Display name** value specified. If any of these values are missing from a user, that user will not be provisioned.
- If you update a user’s address you must have **streetAddress**, **city**, **state**, **zipCode** and the **countryCode** value specified. If any of these values are not specified for the Okta user at the time of synchronization, the user or changes to the user will not be provisioned.