



# How to Configure SAML 2.0 for AWS Single Sign-on

## Contents

- [Supported Features](#)
  - [Configuration Steps](#)
  - [Notes](#)
- 

## Supported Features

The Okta/AWS Single Sign-on SAML integration currently supports the following features:

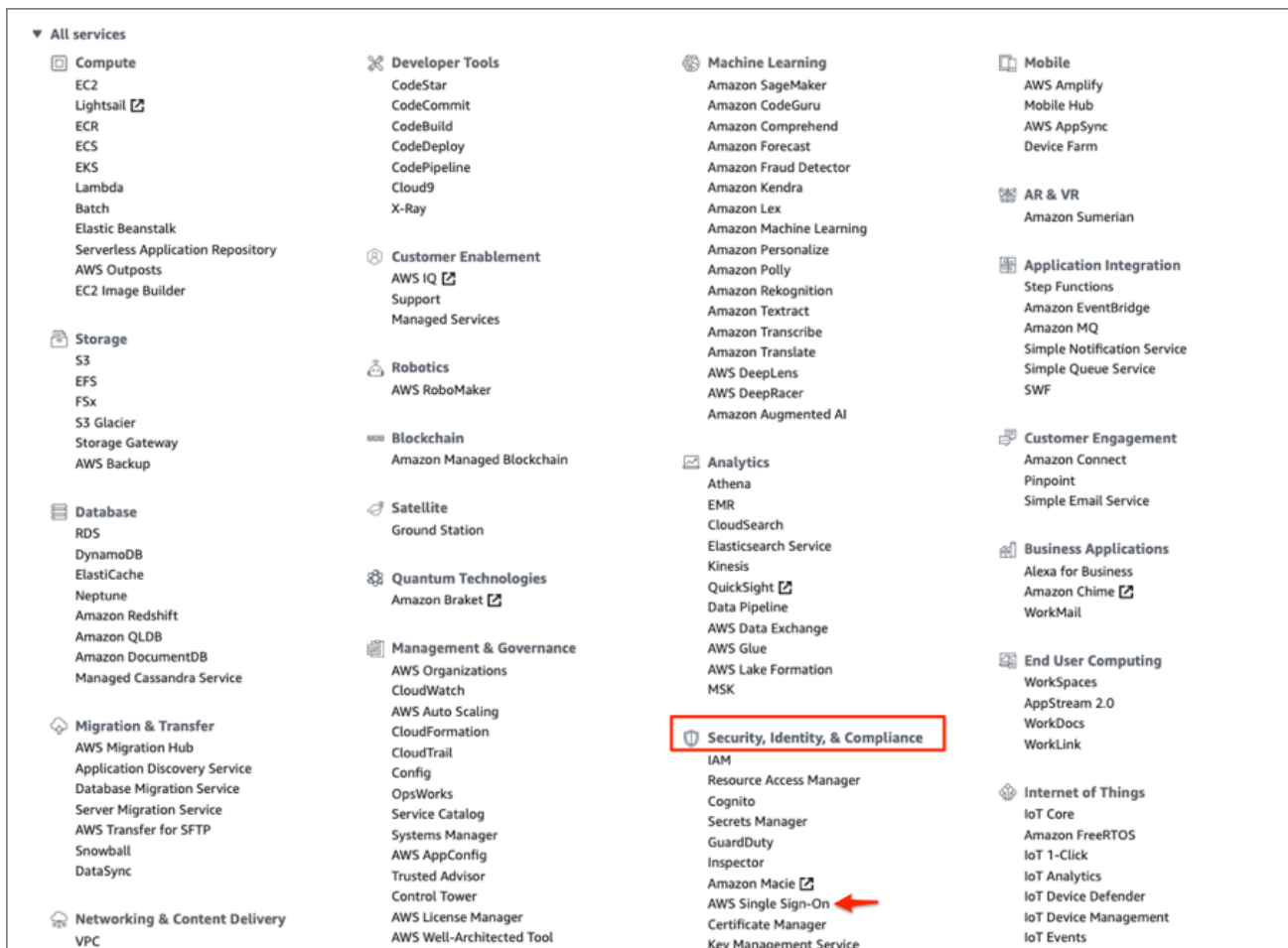
- SP-initiated SSO
- IdP-initiated SSO

For more information on the listed features, visit the [Okta Glossary](#).

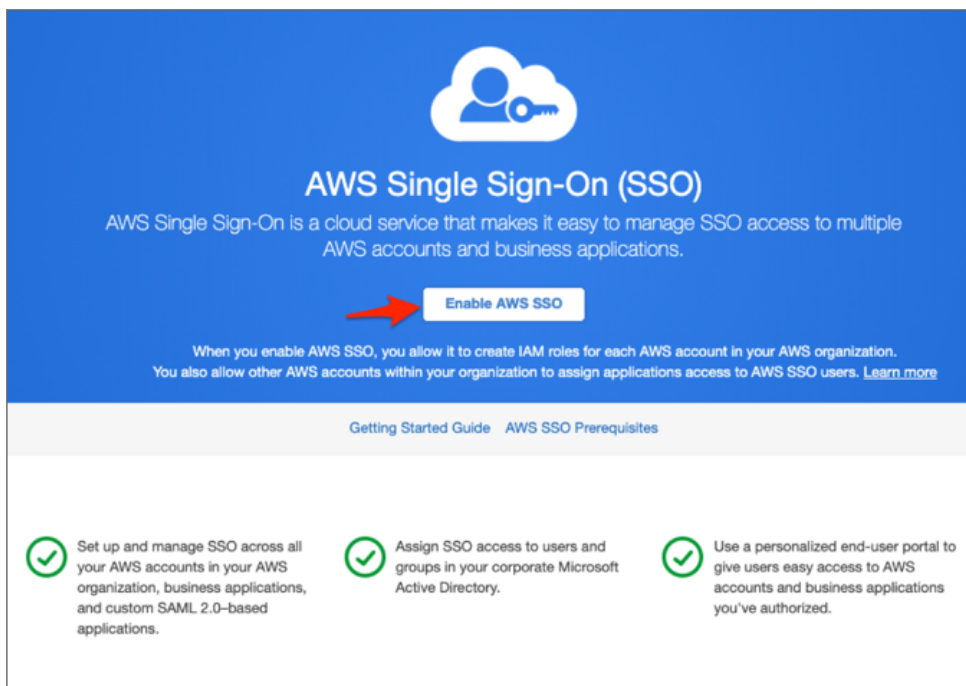
---

## Configuration Steps

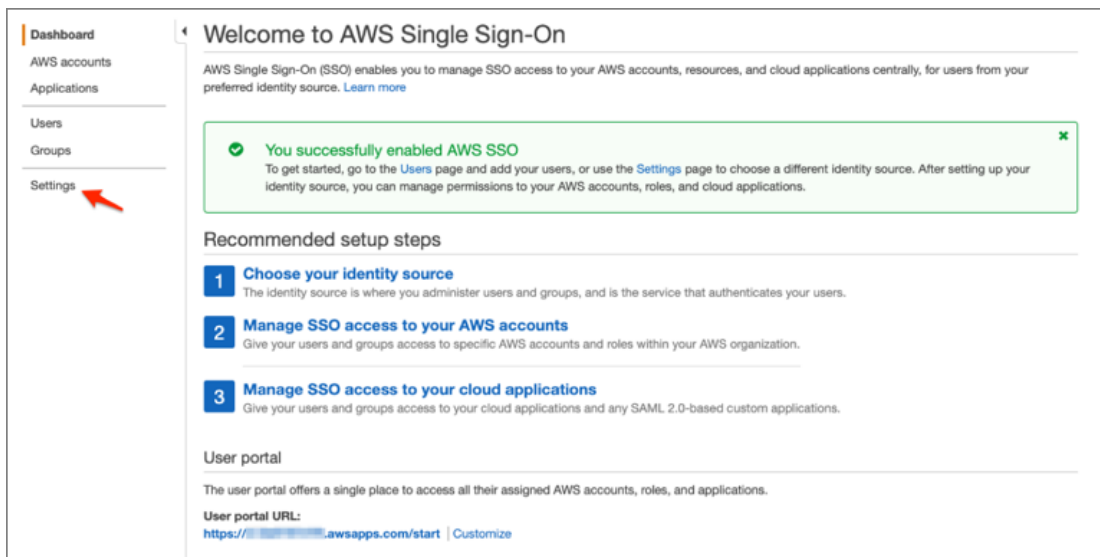
- 1 Log in to the AWS Management Console.
- 2 Navigate to **Security, Identity, & Compliance > AWS Single Sign-On**:



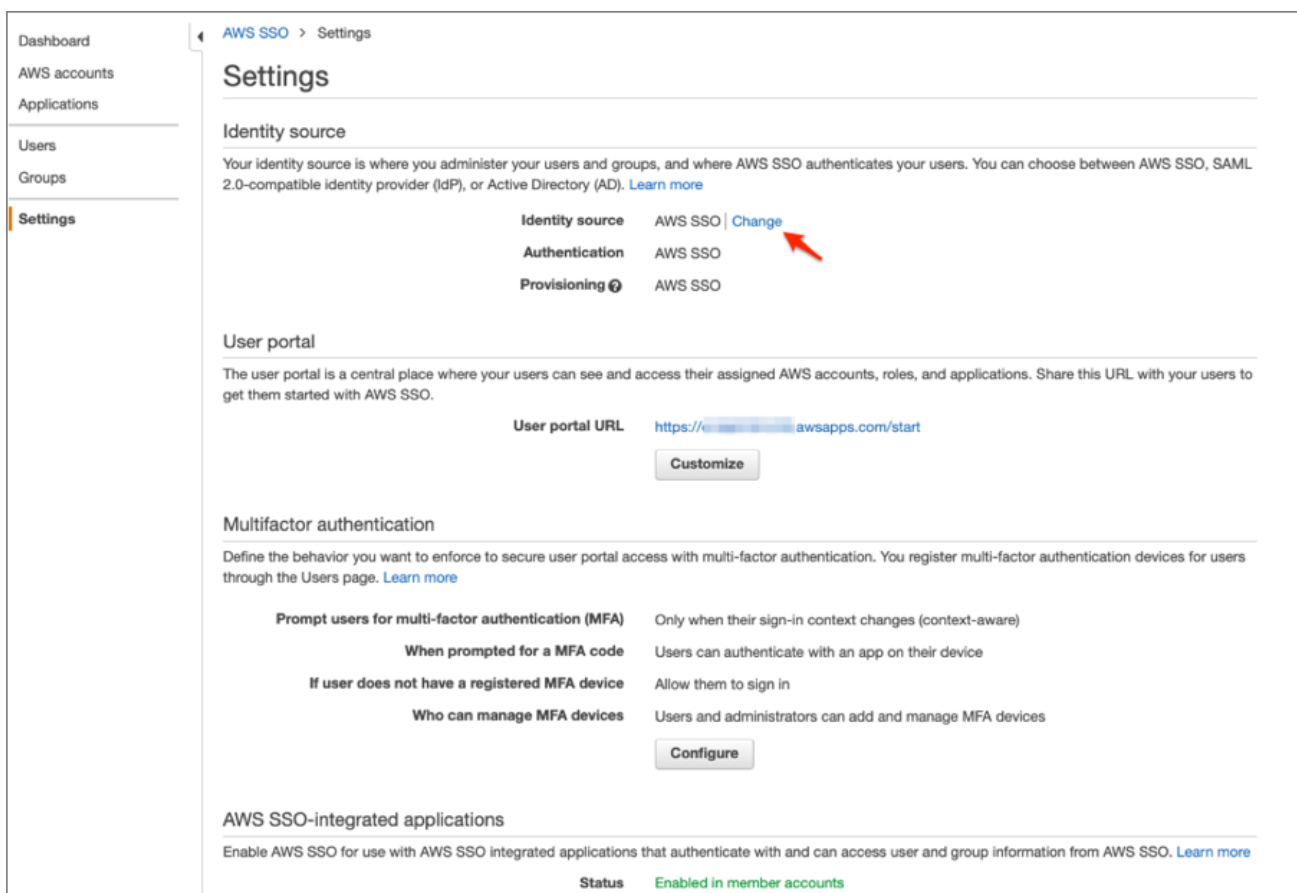
3 Click **Enable AWS SSO**:



4 Select **Settings**:



5 Under **Identity source**, select **Change**:



6 Enter the following:

- Select **External identity provider**.
- Click **Show individual metadata values**.

# Change identity source

1

Choose directory

2

Review

## Choose where your identities are sourced

Your identity source is the place where you administer and authenticate identities. You use AWS SSO to manage permissions for identities from your identity source to access AWS accounts, roles, and applications. [Learn more](#)

☐ **AWS SSO**

You will administer all users, groups, credentials, and multi-factor authentication assignments in AWS SSO. Users sign in through the AWS SSO user portal.

☐ **Active Directory**

You will administer all users, groups, and credentials in AWS Managed Microsoft AD, or you can connect AWS SSO to your existing Active Directory using AWS Managed Microsoft AD or AD Connector. Users sign in through the AWS user portal.

☒ **External identity provider**

You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.

## Configure external identity provider

AWS SSO works as a SAML 2.0 compliant service provider to your external identity provider (IdP). To configure your IdP as your AWS SSO identity source, you must establish a SAML trust relationship by exchanging meta data between your IdP and AWS SSO. While AWS SSO will use your IdP to authenticate users, the users must first be provisioned into AWS SSO before you can assign permissions to AWS accounts and resources. You can either provision users manually from the Users page, or by using the automatic provisioning option in the Settings page after you complete this wizard. [Learn more](#)

### Service provider metadata

Your IdP requires the following AWS SSO certificate and metadata details to trust AWS SSO as a service provider. You may copy and paste, or type this information into your IdP's service provider configuration interface, or you may download the AWS SSO metadata file and upload it into your IdP.

**AWS SSO SAML metadata**

[Download metadata file](#)

[Show individual metadata values](#)

### Identity provider metadata

AWS requires specific metadata provided by your IdP to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.

**IdP SAML metadata\***

**Browse...**

[If you don't have a metadata file, you can manually type your metadata values](#)

**Cancel**

**Next: Review**

- Make a copy of the **AWS SSO Sign-in URL**, **AWS SSO ACS URL**, and **AWS SSO issuer URL** values. These values will be used later on.
- **IdP SAML metadata**: Save the following file as **metadata.xml**, then upload it into AWS.

Individual data will be generated here

- Click **Next: Review**.

**Important:** Changing your source to or from Active Directory removes all existing user and group assignments. You must manually reapply assignments after you have successfully changed your source.

## ● External identity provider

You will administer all users, groups, credentials, and multi-factor authentication in an external identity provider (IdP). Users sign in through your IdP sign-in page to access the AWS SSO user portal, assigned accounts, roles, and applications.

### Configure external identity provider

AWS SSO works as a SAML 2.0 compliant service provider to your external identity provider (IdP). To configure your IdP as your AWS SSO identity source, you must establish a SAML trust relationship by exchanging meta data between your IdP and AWS SSO. While AWS SSO will use your IdP to authenticate users, the users must first be provisioned into AWS SSO before you can assign permissions to AWS accounts and resources. You can either provision users manually from the Users page, or by using the automatic provisioning option in the Settings page after you complete this wizard. [Learn more](#)

#### Service provider metadata

Your IdP requires the following AWS SSO certificate and metadata details to trust AWS SSO as a service provider. You may copy and paste, or type this information into your IdP's service provider configuration interface, or you may download the AWS SSO metadata file and upload it into your IdP.

##### AWS SSO SAML metadata

##### Download metadata file

AWS SSO Sign-in URL

https://[redacted].awsapps.com/start



AWS SSO ACS URL

https://us-east-2.signin.aws.amazon.com/platform/saml/acs



AWS SSO issuer URL

https://us-east-2.signin.aws.amazon.com/platform/saml/[redacted]



[Hide individual metadata values](#)

#### Identity provider metadata

AWS requires specific metadata provided by your IdP to establish trust. You may copy and paste from your IdP, type the metadata in manually, or upload a metadata exchange file that you download from your IdP.


IdP SAML metadata\*

metadata\_amazon\_aws\_sso.xml

Browse...

[If you don't have a metadata file, you can manually type your metadata values](#)

Cancel

 Next: Review

- 7 Review the list of changes. Once you are ready to proceed, type **CONFIRM**, then click Change identity source.

## Change identity source

**1**

Choose directory

**2**

Review

### Review and confirm



#### Review list of changes

You are changing your source of identity to use an external identity provider. Please review the list of changes

- You must complete the SAML federation between AWS SSO and your IdP for your users to be able to federation in.
- AWS SSO will preserve your existing users and assignments.
- Existing users in AWS SSO that are not in IdP will be retained in AWS SSO, but will be unable to sign in to AWS SSO. You may add these users in the IdP or may remove the user from AWS SSO.
- Users from IdP that do not exist in AWS SSO will be provisioned in AWS SSO.
- You must configure provisioning via SCIM to auto provision your users from IdP to AWS SSO. Alternatively, you may manually provision users in AWS SSO without SCIM.
- With SCIM enabled, Your IdP will be authoritative source of identity. You may only provision new user or edit existing user attributes in your IdP.
- All existing MFA configurations will be deleted when customer switches from AWS SSO to IdP. MFA policy controls will be managed on IdP.
- With SCIM disabled, you can provision new users and/or edit existing users in AWS SSO. User Email Id must match in AWS SSO and your IdP in order for user to be able to sign in to AWS SSO.

Type "CONFIRM" to confirm changing the identity source

Cancel

Previous

Change identity source

8 In Okta select the **Sign On** tab for the AWS Single Sign-On SAML app, then click **Edit**:

- Enter your **AWS SSO ACS URL** and **AWS SSO issuer URL** values you made a copy of in step 6 into the corresponding fields.
- **Application username format**: Select one of the options from the dropdown menu.

**Note:** All users in AWS SSO require a unique username, so the mapped value should be unique within your organization.

- Click **Save**:

General

Sign On

Mobile

Import

Assignments

Settings

Cancel

SIGN ON METHODS

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. [Configure profile mapping](#)

1

SAML 2.0 is the only sign-on option currently supported for this application.

SAML 2.0

Default Relay State

All IDP-initiated requests will include this RelayState.

Disable Force Authentication

☒

Never prompt user to re-authenticate.

SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

Identity Provider metadata is available if this application supports dynamic configuration.

ADVANCED SIGN-ON SETTINGS

These fields may be required for a AWS Single Sign-on proprietary sign-on option or general setting.

AWS SSO ACS URL

https://us-east-2.signin.aws.amazon.com/platform/saml

Enter your AWS SSO ACS URL. Refer to the Setup Instructions above to obtain this value.

AWS SSO Issuer URL

https://us-east-2.signin.aws.amazon.com/platform/saml/acs.

Enter your AWS SSO issuer URL. Refer to the Setup Instructions above to obtain this value.

CREDENTIALS DETAILS

Application username format

Email

9 Done!

## SP-initiated SSO

Go to the **AWS SSO Sign-in URL** you made a copy of in step 6.