okta

How to Configure SAML 2.0 for IAM Identity Center

Contents

Supported Features

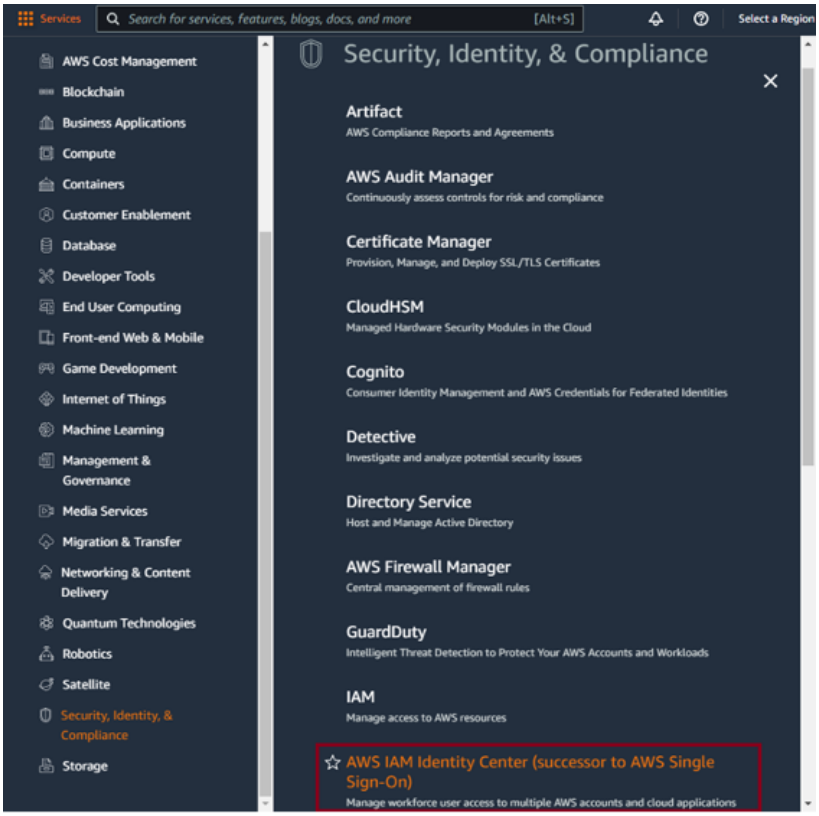
The Okta/IAM Identity Center SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO

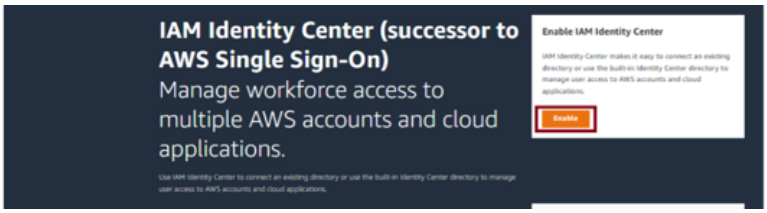
For more information on the listed features, visit the Okta Glossary.

Configuration Steps

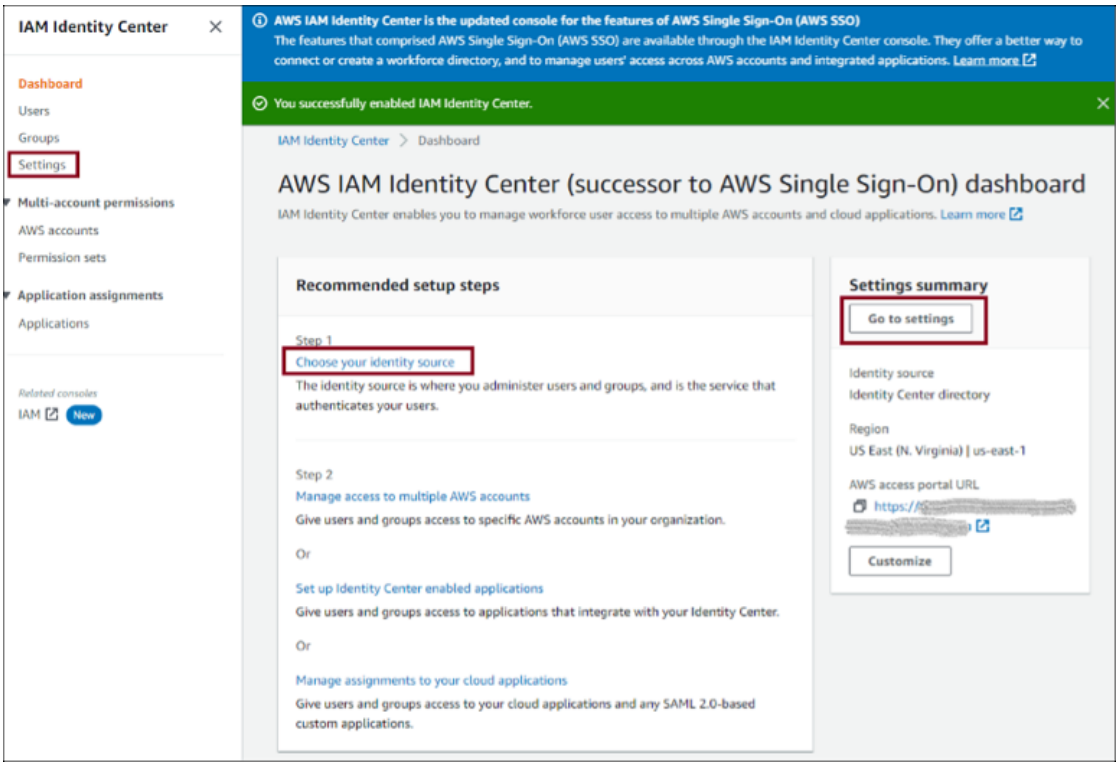
1. Save Okta's IdP SAML metadata:
   - Sign in to the Okta admin dashboard, add the AWS IAM Identity Center app.
   - Select the **Sign On** tab.
   - Under **SAML Signing Certificates**, select **View IdP Metadata** from the **Actions** drop-down menu.
   - Save the contents as **metadata.xml**.
2. Sign in to the AWS Management Console.
3. Go to **Security, Identity, & Compliance > IAM Identity Center**:



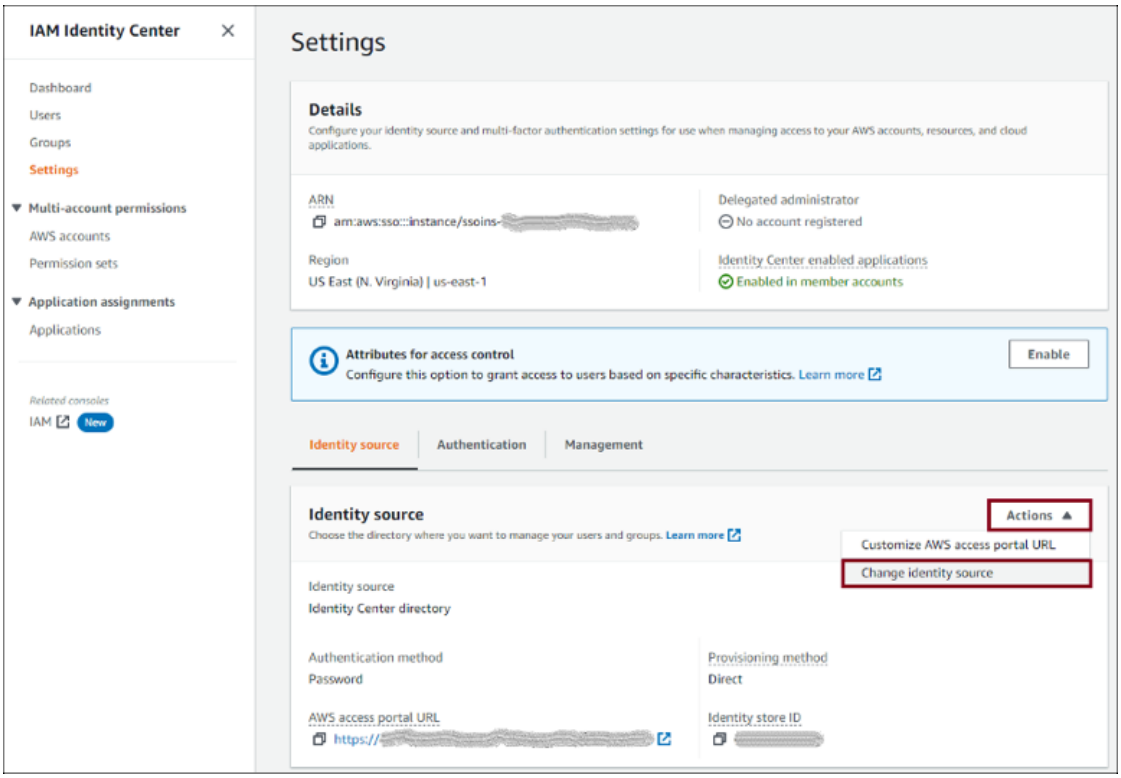
4 Click **Enable** in the upper right:



5 Select **Settings** (on the left), **Go to settings** on the right, or **Choose your identity source** (in the middle). All three take you to the **Settings** page where you can choose your identity source:



6 Under **Identity source**, select **Change identity source** from the **Actions** drop-down menu:

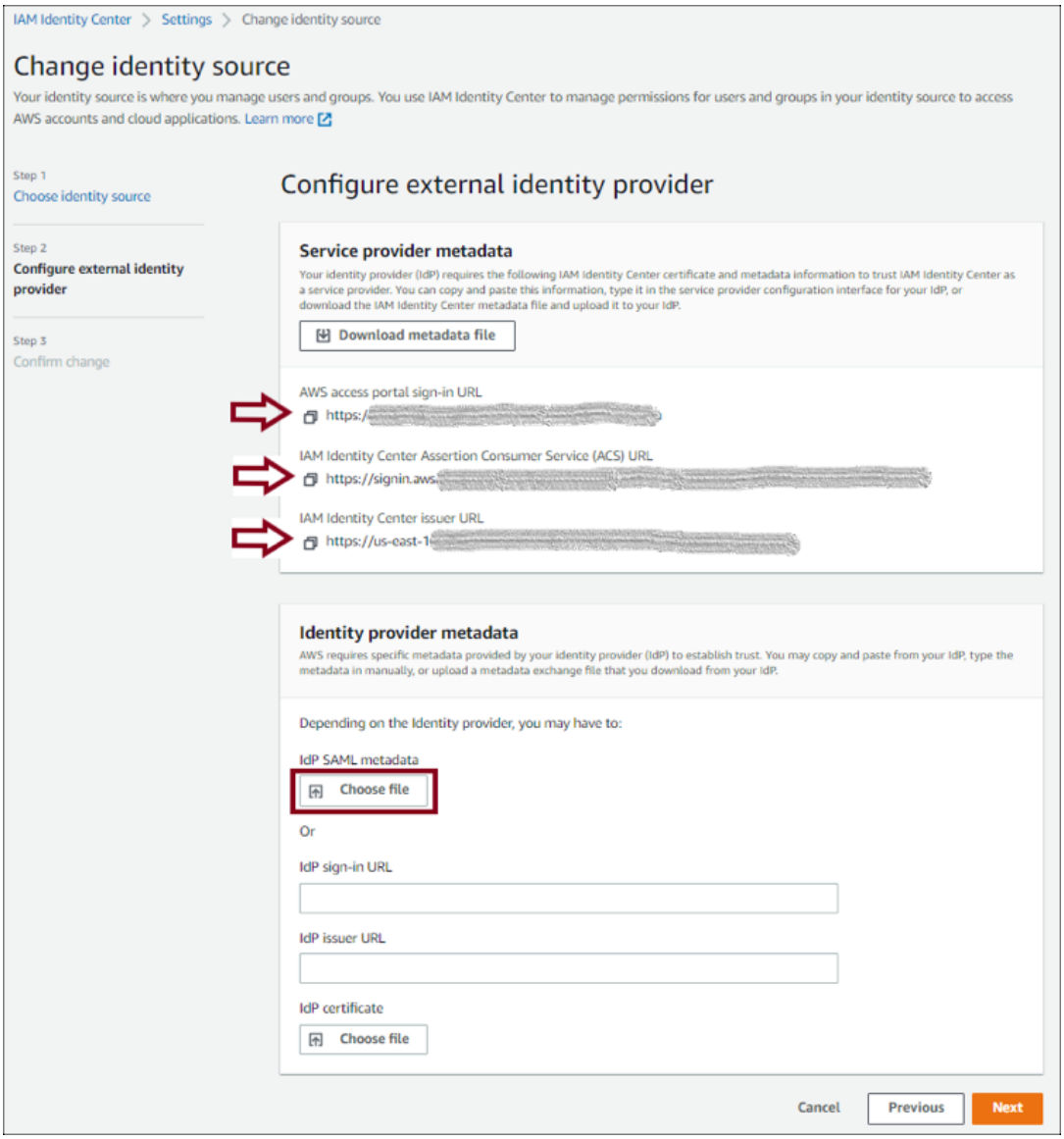


7 On the next page select **External identity provider**, then click **Next**.

8 Configure the external identity provider.

- **IdP SAML metadata**: Click **Choose file** to upload Okta's IdP SAML metadata you saved in step 1.
- Make a copy of the **AWS access portal sign-in URL**, **IAM Identity Center ACS URL**, and **IAM Identity Center issuer URL** values. You'll need these values later on.
- Click **Next**.

  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.



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

10 In Okta, select the **Sign On** tab IAM Identity Center SAML app, then click **Edit**:

- Enter your **AWS IAM Identity Center SSO ACS URL** and **AWS IAM Identity Center SSO issuer URL** values (step 8) into the corresponding fields.
- **Application username format**: Select one of the options from the drop-down menu.

  Note: All users in AWS IAM Identity Center SSO require a unique username, so the mapped value should be unique within your organization.
- Click **Save**.

11 Done!

SP-initiated SSO

Go to the **AWS IAM Identity Center Sign-in URL** (step 8).