How to Configure SAML 2.0 for AWS Single Sign-on

Contents

Supported Features

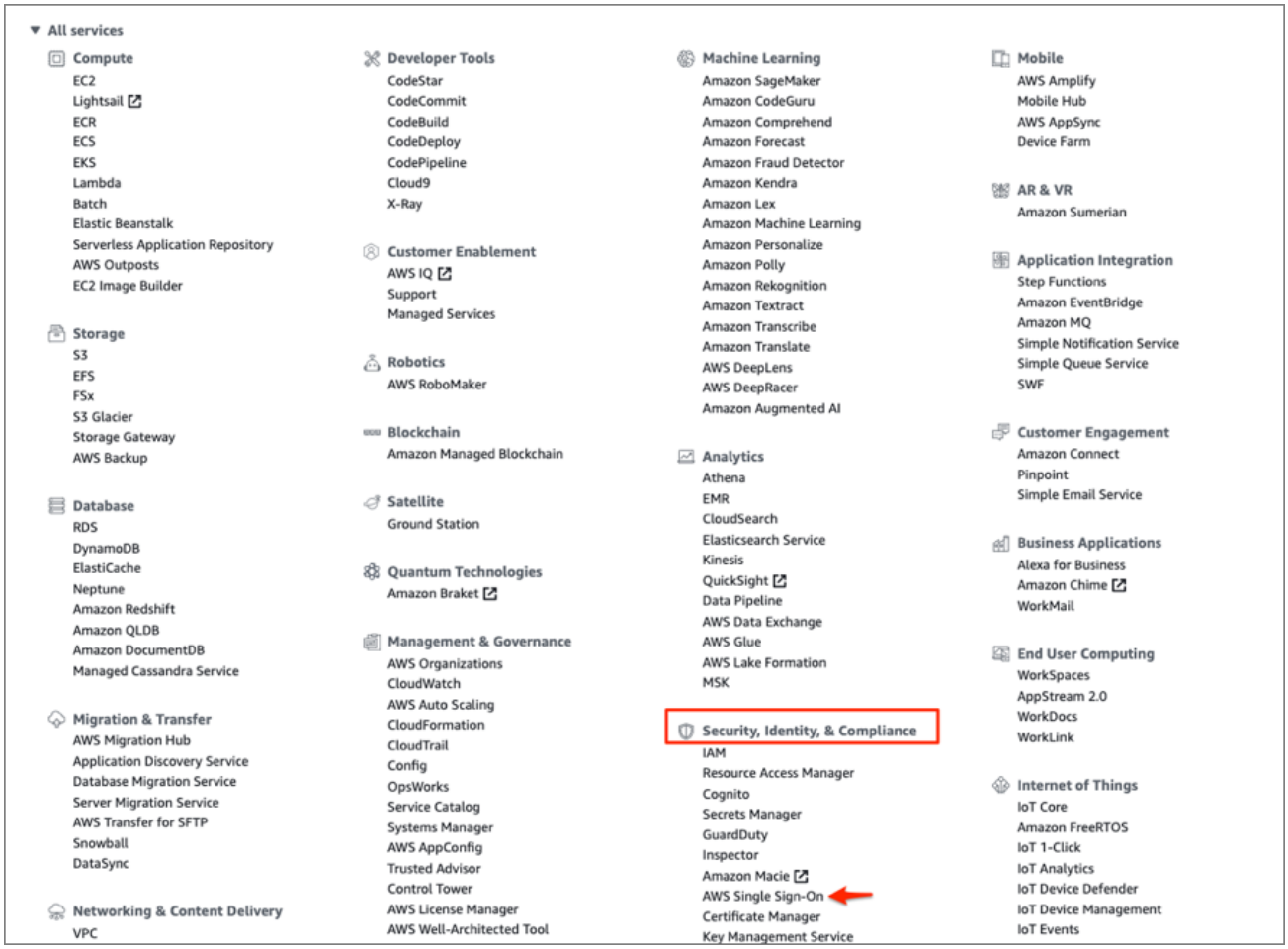
The Okta/AWS Single Sign-on SAML integration currently supports the following features:

- SP-initiated SSO
- IdP-initiated SSO

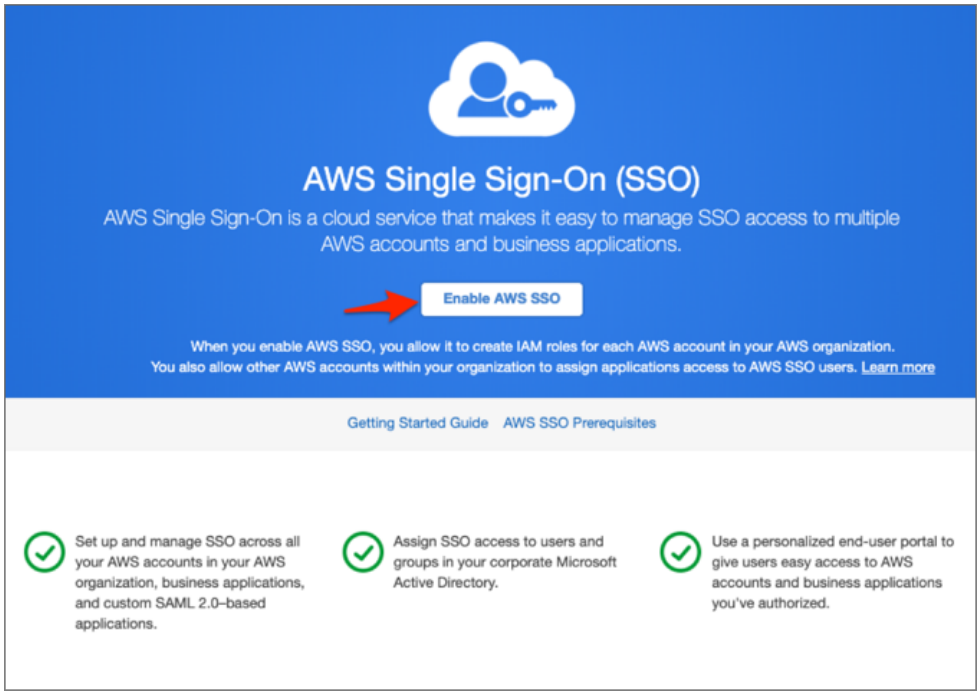
For more information on the listed features, visit the Okta Glossary.

Configuration Steps

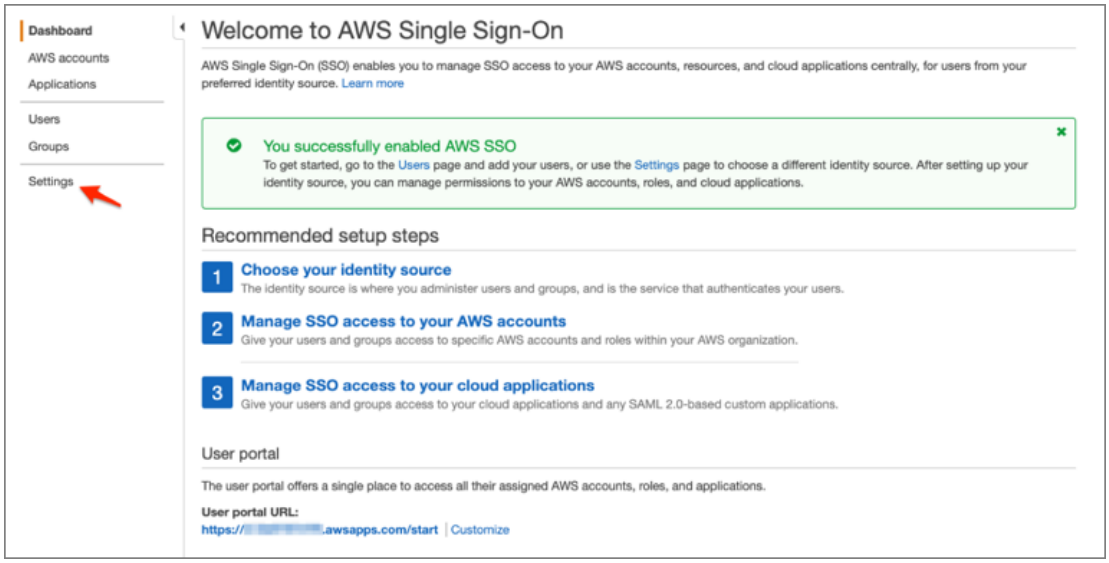
1. Log in to the AWS Management Console.
2. Navigate to **Security, Identity, & Compliance > AWS Single Sign-On**:



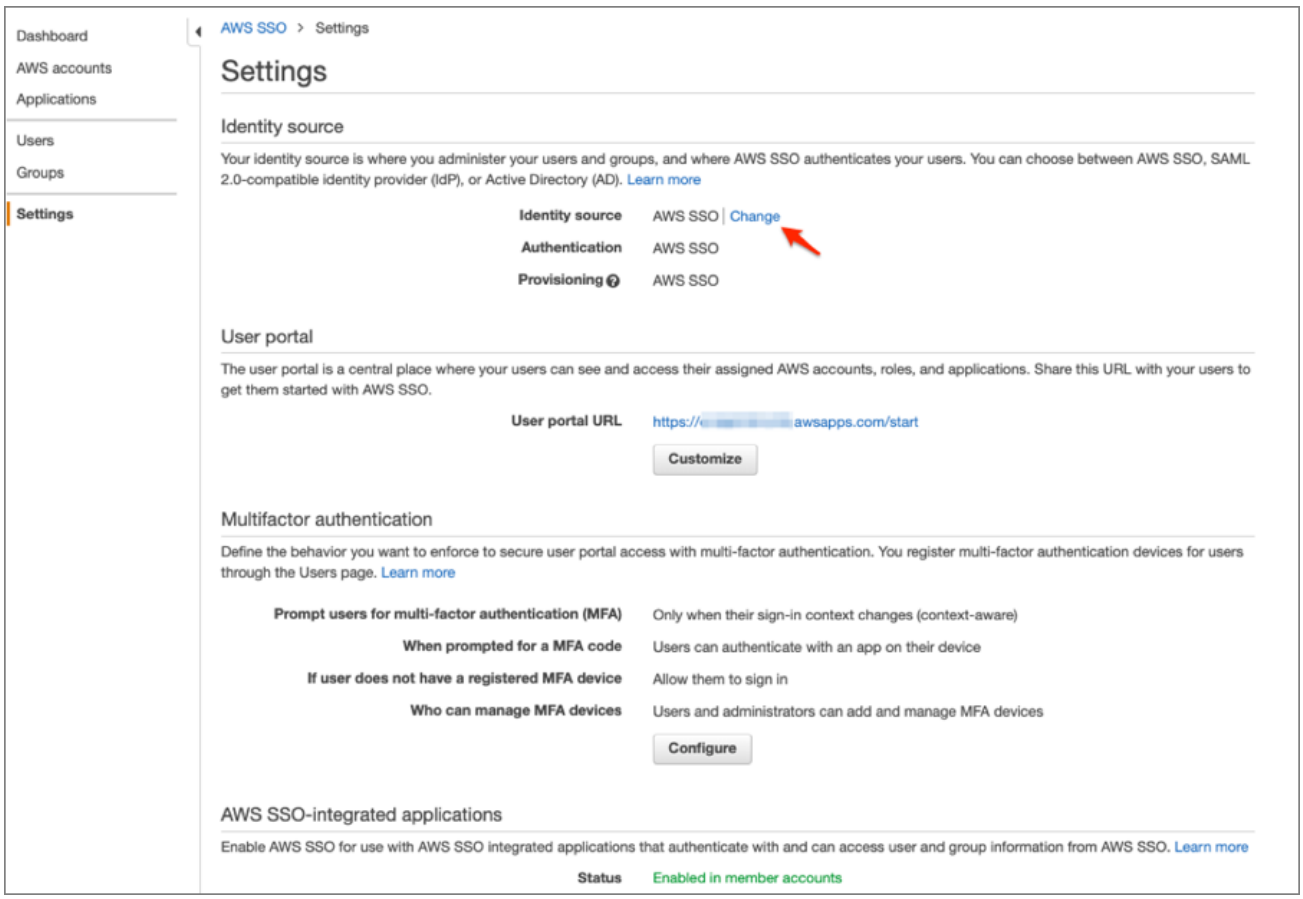
3 Click **Enable AWS SSO**:



4 Select **Settings**:

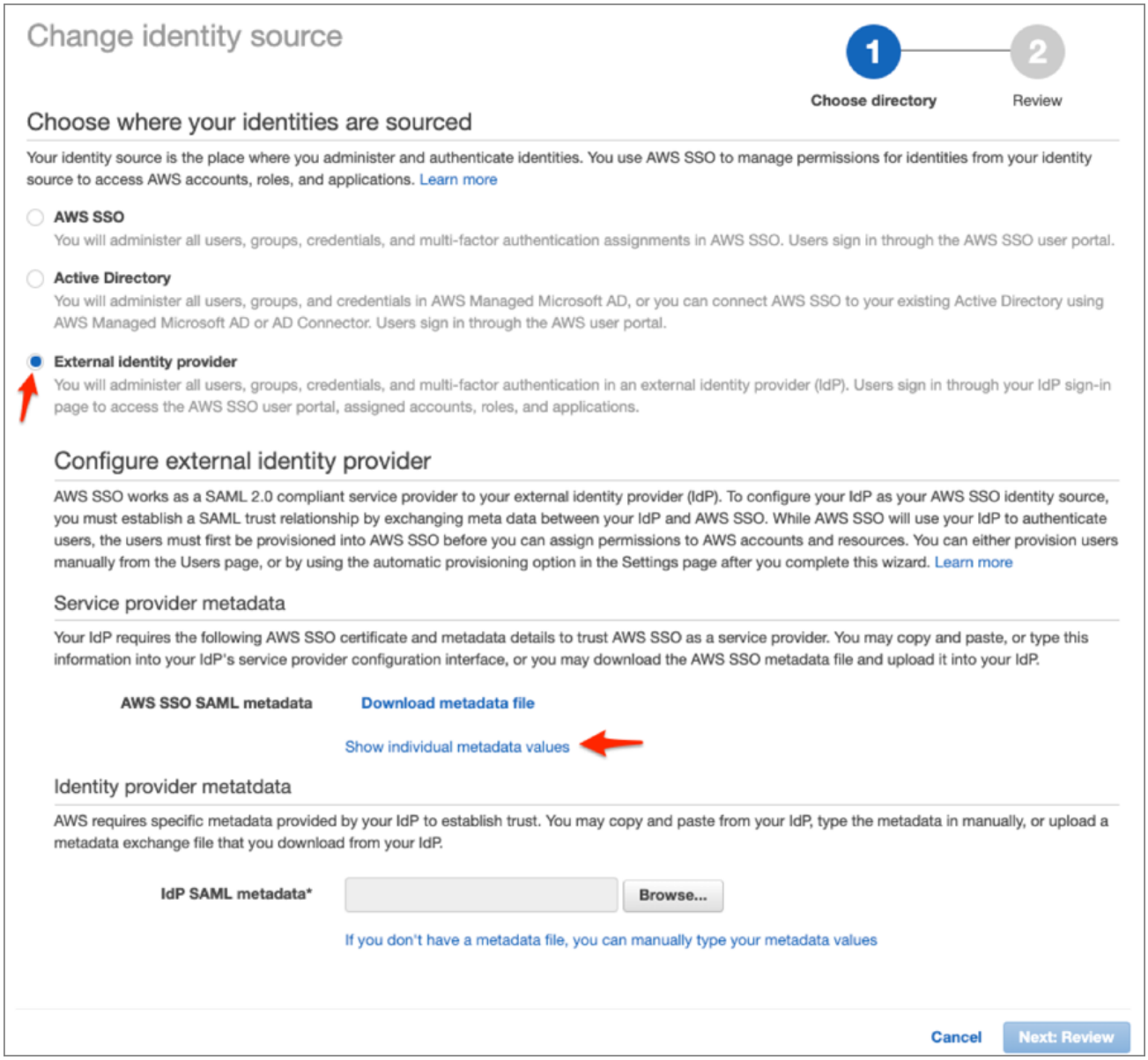


5 Under **Identity source**, select **Change**:



6 Enter the following:

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

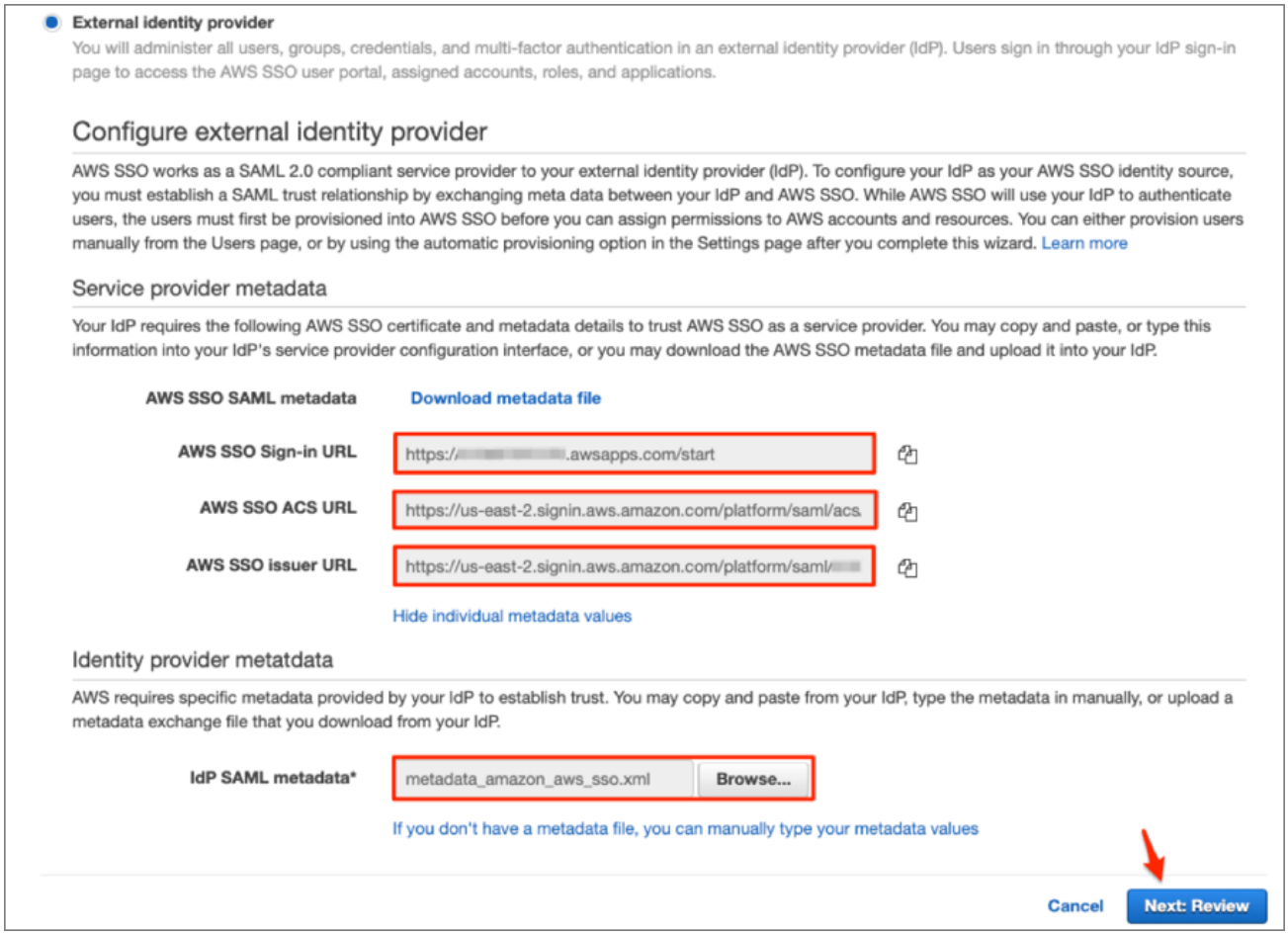


- Make a copy of the **AWS SSO Sign-in URL**, **AWS SSO ACS URL**, and **AWS SSO issuer URL** values. These values will be used later on.
- **IdP SAML metadata**: Save the following file as **metadata.xml**, then upload it into AWS.

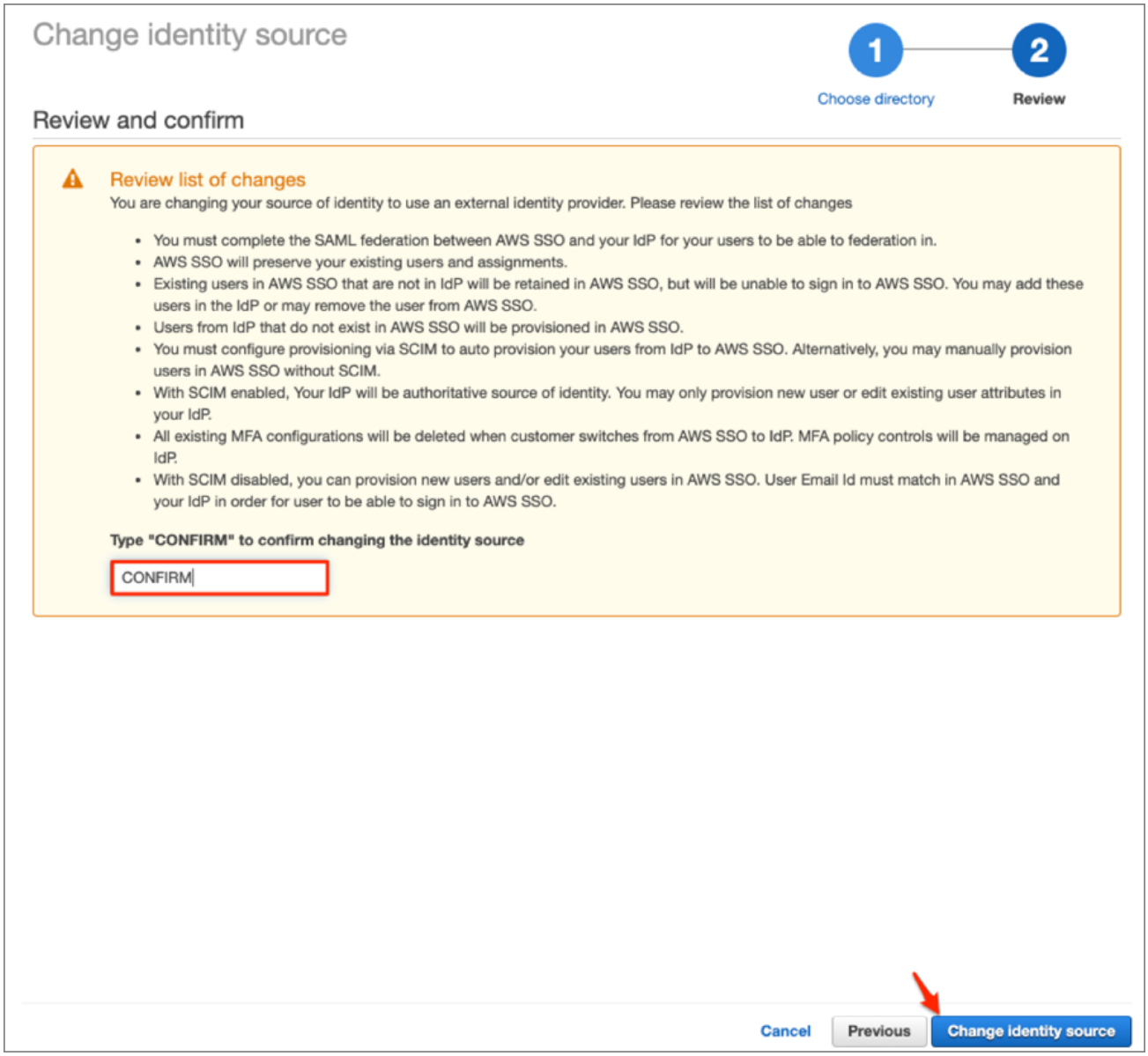
  Individual data will be generated here

- 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.



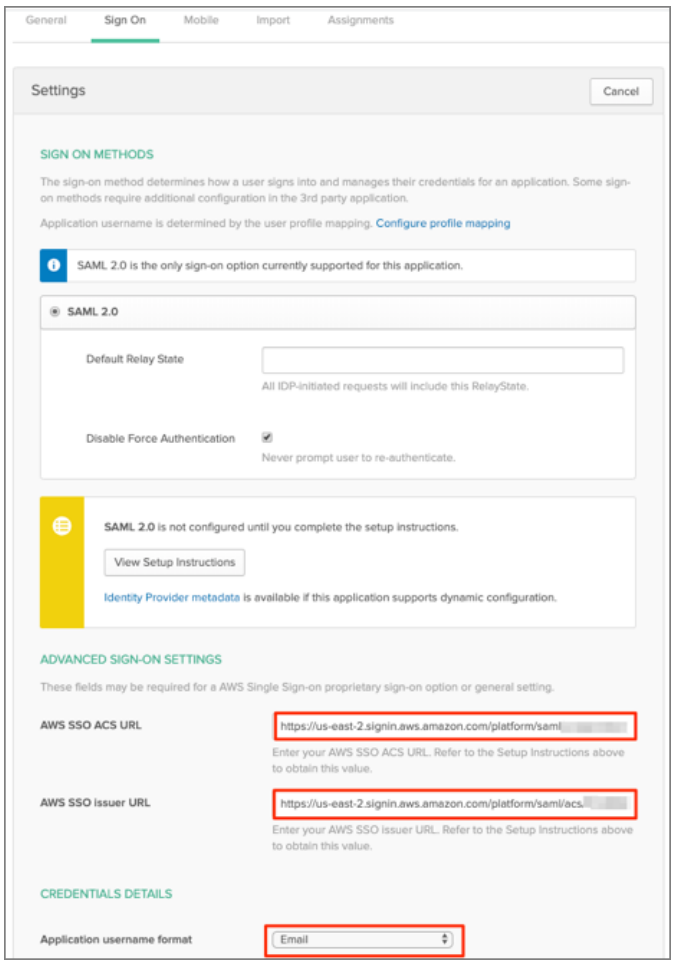
7 Review the list of changes. Once you are ready to proceed, type **CONFIRM**, then click Change identity source.



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**:



9 Done!

SP-initiated SSO

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