Configuring your SAML 2.0 IdP with relying party trust and adding claims

PDF (iam-ug.pdf#id_roles_providers_create_saml_relying-party) | **RSS (aws-iam-release-notes.rss)**

When you create an IAM identity provider and role for SAML access, you are telling AWS about the external identity provider (IdP) and what its users are allowed to do. Your next step is to then tell the IdP about AWS as a service provider. This is called adding *relying party trust* between your IdP and AWS. The exact process for adding relying party trust depends on what IdP you're using. For details, see the documentation for your identity management software.

Many IdPs allow you to specify a URL from which the IdP can read an XML document that contains relying party information and certificates. For AWS, use `https://` *`region-code`* `.signin.aws.amazon.com/static/saml-metadata.xml` or `https://signin.aws.amazon.com/static/saml-metadata.xml` . For a list of possible *`region-code`* values, see the **Region** column in AWS Sign-In endpoints (https://docs.aws.amazon.com/general/latest/gr/signin-service.html) .

If you can't specify a URL directly, then download the XML document from the preceding URL and import it into your IdP software.

You also need to create appropriate claim rules in your IdP that specify AWS as a relying party. When the IdP sends a SAML response to the AWS endpoint, it includes a SAML *assertion* that contains one or more *claims*. A claim is information about the user and its groups. A claim rule maps that information into SAML attributes. This lets you make sure that SAML authentication responses from your IdP contain the necessary attributes that AWS uses in IAM policies to check permissions for federated users. For more information, see the following topics:

- Overview of the role to allow SAML-federated access to your AWS resources (./id_roles_providers_saml.html#CreatingSAML-configuring-role) . This topic discusses using SAML-specific keys in IAM policies and how to use them to restrict permissions for SAML-federated users.
- Configuring SAML assertions for the authentication response (./id_roles_providers_create_saml_assertions.html) . This topic discusses how to configure SAML claims that include information about the user. The claims are bundled into a SAML assertion and included in the SAML response that is sent to AWS. You must ensure that the information

needed by AWS policies is included in the SAML assertion in a form that AWS can recognize and use.

- Integrating third-party SAML solution providers with AWS (./id_roles_providers_saml_3rd-party.html) . This topic provides links to documentation provided by third-party organizations about how to integrate identity solutions with AWS.