Creating a role for SAML 2.0 federation (console)

PDF (iam-ug.pdf#id_roles_create_for-idp_saml) | RSS (aws-iam-release-notes.rss)

You can use SAML 2.0 federation instead of creating IAM users in your AWS account. With an identity provider (IdP), you can manage your user identities outside of AWS and give these external user identities permissions to access AWS resources in your account. For more information about federation and identity providers, see Identity providers and federation (./id_roles_providers.html) .

Prerequisites for creating a role for SAML

Before you can create a role for SAML 2.0 federation, you must first complete the following prerequisite steps.

To prepare to create a role for SAML 2.0 federation

1. Before you create a role for SAML-based federation, you must create a SAML provider in IAM. For more information, see Creating IAM SAML identity providers (./id_roles_providers_create_saml.html) .
2. Prepare the policies for the role that the SAML 2.0–authenticated users will assume. As with any role, a role for the SAML federation includes two policies. One is the role trust policy that specifies who can assume the role. The other is the IAM permissions policy that specifies the AWS actions and resources that the federated user is allowed or denied access to.

   When you create the trust policy for your role, you must use three values to ensure that only your application can assume the role:

   - For the `Action` element, use the `sts:AssumeRoleWithSAML` action.
   - For the `Principal` element, use the string `{"Federated":` *`ARNofIdentityProvider`*`}` . Replace *`ARNofIdentityProvider`* with the ARN of the SAML identity provider (./id_roles_providers_saml.html) that you created in Step 1 (#idpsamlstep1) .
   - For the `Condition` element, use a `StringEquals` condition to test that the `saml:aud` attribute from the SAML response matches the SAML federation endpoint for

AWS.

The following example trust policy is designed for a SAML federated user:

```
{
    "Version": "2012-10-17",
    "Statement": {
      "Effect": "Allow",
      "Action": "sts:AssumeRoleWithSAML",
      "Principal": {"Federated": "arn:aws:iam::account-id:saml-
provider/PROVIDER-NAME"},
      "Condition": {"StringEquals": {"SAML:aud":
"https://signin.aws.amazon.com/saml"}}
    }
  }
```

Replace the principal ARN with the actual ARN for the SAML provider that you created in IAM. It will have your own account ID and provider name.

Creating a role for SAML

After you complete the prerequisite steps, you can create the role for SAML-based federation.

To create a role for SAML-based federation

1. Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam/ (https://console.aws.amazon.com/iam/) .
2. In the navigation pane of the IAM console, choose **Roles** and then choose **Create role**.
3. Choose the **SAML 2.0 federation** role type.
4. For **Select a SAML provider**, choose the provider for your role.
5. Choose the SAML 2.0 access level method.
   - Choose **Allow programmatic access only** to create a role that can be assumed programmatically from the AWS API or AWS CLI.
   - Choose **Allow programmatic and AWS Management Console access** to create a role that can be assumed programmatically and from the AWS Management Console.

   The roles created by both are similar, but the role that can also be assumed from the console includes a trust policy with a particular condition. That condition explicitly ensures that the

SAML audience (SAML:aud attribute) is set to the AWS sign-in endpoint for SAML (https://signin.aws.amazon.com/saml).

6. If you're creating a role for programmatic access, choose an attribute from the **Attribute** list. Then, in the **Value** box, enter a value to include in the role. This restricts role access to users from the identity provider whose SAML authentication response (assertion) includes the attributes that you specify. You must specify at least one attribute to ensure that your role is limited to a subset of users at your organization.

   If you're creating a role for programmatic and console access, the SAML:aud attribute is automatically added and set to the URL of the AWS SAML endpoint (https://signin.aws.amazon.com/saml).

7. To add more attribute-related conditions to the trust policy, choose **Condition (optional)**, select the additional condition, and specify a value.

   > **Note**
   >
   > The list includes the most commonly used SAML attributes. IAM supports additional attributes that you can use to create conditions. For a list of the supported attributes, see Available Keys for SAML Federation (https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_iam-condition-keys.html#condition-keys-saml) . If you need a condition for a supported SAML attribute that's not in the list, you can manually add that condition. To do that, edit the trust policy after you create the role.

8. Review your SAML 2.0 trust information and then choose **Next**.
9. IAM includes a list of the AWS managed and customer managed policies in your account. Select the policy to use for the permissions policy, or choose **Create policy** to open a new browser tab and create a new policy from scratch. For more information, see Creating IAM policies (./access_policies_create-console.html#access_policies_create-start) . After you create the policy, close that tab and return to your original tab. Select the check box next to the permissions policies that you want web identity users to have. If you prefer, you can select no policies at this time, and then attach policies to the role later. By default, a role has no permissions.
10. (Optional) Set a permissions boundary (./access_policies_boundaries.html) . This is an advanced feature.

    Open the **Permissions boundary** section and choose **Use a permissions boundary to control the maximum role permissions**. Select the policy to use for the permissions boundary.
11. Choose **Next**.
12. Choose **Next: Review**.

13. For **Role name**, enter a role name. Role names must be unique within your AWS account. They are not distinguished by case. For example, you cannot create roles named both `PRODROLE` and `prodrole`. Because other AWS resources might reference the role, you cannot edit the name of the role after it has been created.
14. (Optional) For **Description**, enter a description for the new role.
15. Choose **Edit** in the **Step 1: Select trusted entities** or **Step 2: Add permissions** sections to edit the use cases and permissions for the role.
16. (Optional) Add metadata to the role by attaching tags as key–value pairs. For more information about using tags in IAM, see Tagging IAM resources (./id_tags.html) .
17. Review the role and then choose **Create role**.

After you create the role, you complete the SAML trust by configuring your identity provider software with information about AWS. This information includes the roles that you want your federated users to use. This is referred to as configuring the relying party trust between your IdP and AWS. For more information, see Configuring your SAML 2.0 IdP with relying party trust and adding claims (./id_roles_providers_create_saml_relying-party.html) .