Creating IAM SAML identity providers

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

An IAM SAML 2.0 identity provider is an entity in IAM that describes an external identity provider (IdP) service that supports the SAML 2.0 (Security Assertion Markup Language 2.0) (https://wiki.oasis-open.org/security) standard. You use an IAM identity provider when you want to establish trust between a SAML-compatible IdP such as Shibboleth or Active Directory Federation Services and AWS, so that users in your organization can access AWS resources. IAM SAML identity providers are used as principals in an IAM trust policy.

For more information about this scenario, see About SAML 2.0-based federation (./id_roles_providers_saml.html) .

You can create and manage an IAM identity provider in the AWS Management Console or with AWS CLI, Tools for Windows PowerShell, or AWS API calls.

After you create a SAML provider, you must create one or more IAM roles. A role is an identity in AWS that doesn't have its own credentials (as a user does). But in this context, a role is dynamically assigned to a federated user that is authenticated by your organization's IdP. The role permits your organization's IdP to request temporary security credentials for access to AWS. The policies assigned to the role determine what the federated users are allowed to do in AWS. To create a role for SAML federation, see Creating a role for a third-party Identity Provider (federation) (./id_roles_create_for-idp.html) .

Finally, after you create the role, you complete the SAML trust by configuring your IdP with information about AWS and the roles that you want your federated users to use. This is referred to as configuring relying party trust between your IdP and AWS. To configure relying party trust, see Configuring your SAML 2.0 IdP with relying party trust and adding claims (./id_roles_providers_create_saml_relying-party.html) .

Topics

- Creating and managing an IAM SAML identity provider (AWS API) (#idp-create-identityprovider-API)
- Configuring your SAML 2.0 IdP with relying party trust and adding claims (./id_roles_providers_create_saml_relying-party.html)
- Integrating third-party SAML solution providers with AWS (./id_roles_providers_saml_3rd-party.html)
- Configuring SAML assertions for the authentication response (./id_roles_providers_create_saml_assertions.html)

Creating and managing an IAM identity provider (console)

You can use the AWS Management Console to create and delete IAM SAML identity providers.

To create an IAM SAML identity provider (console)

1. Before you can create an IAM SAML identity provider, you need the SAML metadata document that you get from the IdP. This document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that are received from the IdP. To generate the metadata document, use the identity management software your organization uses as its IdP. For instructions on how to configure many of the available IdPs to work with AWS, including how to generate the required SAML metadata document, see Integrating third-party SAML solution providers with AWS (./id_roles_providers_saml_3rd-party.html) .

   > ⚠ **Important**
   >
   > This metadata file includes the issuer name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) received from the IdP. The metadata file must be encoded in UTF-8 format without a byte order mark (BOM). To remove the BOM, you can encode the file as UTF-8 using a text editing tool, such as Notepad++.
   >
   > The x.509 certificate included as part of the SAML metadata document must use a key size of at least 1024 bits. Also, the x.509 certificate must also be free of any repeated extensions. You can use extensions, but the extensions can only appear once in the certificate. If the x.509 certificate does not meet either condition, IdP creation fails and returns an "Unable to parse metadata" error.

2. 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/) .
3. In the navigation pane, choose **Identity providers** and then choose **Add provider**.
4. For **Configure provider**, choose **SAML**.
5. Type a name for the identity provider.
6. For **Metadata document**, choose **Choose file**, specify the SAML metadata document that you downloaded in Step 1 (#samlstep1) .
7. (Optional) For **Add tags** you can add key–value pairs to help you identify and organize your IdPs. You can also use tags to control access to AWS resources. To learn more about tagging SAML identity providers, see Tagging IAM SAML identity providers (./id_tags_idps_saml.html) .

   Choose **Add tag**. Enter values for each tag key-value pair.
8. Verify the information that you have provided. When you are done, choose **Add provider**.
9. Assign an IAM role to your identity provider to give external user identities managed by your identity provider permissions to access AWS resources in your account. To learn more about creating roles for identity federation, see Creating a role for a third-party Identity Provider (federation) (./id_roles_create_for-idp.html) .

To delete a SAML provider (console)

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, choose **Identity providers**.
3. Select the radio button next to the identity provider that you want to delete.
4. Choose **Delete**. A new window opens.
5. Confirm that you want to delete the provider by typing the word `delete` in the field. Then, choose **Delete**.

Creating and managing an IAM SAML Identity Provider (AWS CLI)

You can use the AWS CLI to create and manage SAML providers.

Before you can create an IAM identity provider, you need the SAML metadata document that you get from the IdP. This document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that are received from the IdP. To generate the metadata document, use the identity management software your organization uses as its IdP. For instructions on how to configure many of the available IdPs to

work with AWS, including how to generate the required SAML metadata document, see Integrating third-party SAML solution providers with AWS (./id_roles_providers_saml_3rd-party.html) .

> **Important**
>
> This metadata file includes the issuer name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) received from the IdP. The metadata file must be encoded in UTF-8 format without a byte order mark (BOM). To remove the BOM, you can encode the file as UTF-8 using a text editing tool, such as Notepad++.
>
> The x.509 certificate included as part of the SAML metadata document must use a key size of at least 1024 bits. Also, the x.509 certificate must also be free of any repeated extensions. You can use extensions, but the extensions can only appear once in the certificate. If the x.509 certificate does not meet either condition, IdP creation fails and returns an "Unable to parse metadata" error.

To create an IAM identity provider and upload a metadata document (AWS CLI)

- Run this command: `aws iam create-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/create-saml-provider.html)

To upload a new metadata document for an IAM identity provider (AWS CLI)

- Run this command: `aws iam update-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/update-saml-provider.html)

To tag an existing IAM identity provider (AWS CLI)

- Run this command: `aws iam tag-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/tag-saml-provider.html)

To list tags for existing IAM identity provider (AWS CLI)

- Run this command: `aws iam list-saml-provider-tags` (https://docs.aws.amazon.com/cli/latest/reference/iam/list-saml-provider-tags.html)

To remove tags on an existing IAM identity provider (AWS CLI)

- Run this command: `aws iam untag-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/untag-saml-provider.html)

To tag an existing IAM identity provider (AWS CLI)

- Run this command: `aws iam tag-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/tag-saml-provider.html)

To list tags for existing IAM identity provider (AWS CLI)

- Run this command: `aws iam list-saml-provider-tags` (https://docs.aws.amazon.com/cli/latest/reference/iam/list-saml-provider-tags.html)

To remove tags on an existing IAM identity provider (AWS CLI)

- Run this command: `aws iam untag-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/untag-saml-provider.html)

To delete an IAM SAML identity provider (AWS CLI)

1. (Optional) To list information for all providers, such as the ARN, creation date, and expiration, run the following command:
   - `aws iam list-saml-providers` (https://docs.aws.amazon.com/cli/latest/reference/iam/list-saml-providers.html)
2. (Optional) To get information about a specific provider, such as the ARN, creation date, and expiration, run the following command:
   - `aws iam get-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/get-saml-provider.html)
3. To delete an IAM identity provider, run the following command:
   - `aws iam delete-saml-provider` (https://docs.aws.amazon.com/cli/latest/reference/iam/delete-saml-provider.html)

Creating and managing an IAM SAML identity provider (AWS API)

You can use the AWS API to create and manage SAML providers.

Before you can create an IAM identity provider, you need the SAML metadata document that you get from the IdP. This document includes the issuer's name, expiration information, and keys that can be used to validate the SAML authentication response (assertions) that are received from the IdP. To generate the metadata document, use the identity management software your organization uses as its IdP. For instructions on how to configure many of the available IdPs to work with AWS, including how to generate the required SAML metadata document, see Integrating third-party SAML solution providers with AWS (./id_roles_providers_saml_3rd-party.html) .

> **⚠ Important**
>
> The metadata file must be encoded in UTF-8 format without a byte order mark (BOM). Also, the X.509 certificate that is included as part of the SAML metadata document must use a key size of at least 1024 bits. If the key size is smaller, the IdP creation fails with an "Unable to parse metadata" error. To remove the BOM, you can encode the file as UTF-8 using a text editing tool, such as Notepad++.

To create an IAM identity provider and upload a metadata document (AWS API)

- Call this operation: `CreateSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_CreateSAMLProvider.html)

To upload a new metadata document for an IAM identity provider (AWS API)

- Call this operation: `UpdateSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_UpdateSAMLProvider.html)

To tag an existing IAM identity provider (AWS API)

- Call this operation: `TagSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_TagSAMLProvider.html)

To list tags for an existing IAM identity provider (AWS API)

- Call this operation: `ListSAMLProviderTags` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_ListSAMLProviderTags.html)

To remove tags on an existing IAM identity provider (AWS API)

- Call this operation: `UntagSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_UntagSAMLProvider.html)

To tag an existing IAM identity provider (AWS API)

- Call this operation: `TagSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_TagSAMLProvider.html)

To list tags for an existing IAM identity provider (AWS API)

- Call this operation: `ListSAMLProviderTags` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_ListSAMLProviderTags.html)

To remove tags on an existing IAM identity provider (AWS API)

- Call this operation: `UntagSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_UntagSAMLProvider.html)

To delete an IAM identity provider (AWS API)

1. (Optional) To list information for all IdPs, such as the ARN, creation date, and expiration, call the following operation:
   - `ListSAMLProviders` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_ListSAMLProviders.html)
2. (Optional) To get information about a specific provider, such as the ARN, creation date, and expiration, call the following operation:
   - `GetSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_GetSAMLProvider.html)
3. To delete an IdP, call the following operation:
   - `DeleteSAMLProvider` (https://docs.aws.amazon.com/IAM/latest/APIReference/API_DeleteSAMLProvider.html)
