

Configure for AWS SAML Passthrough Authentication

Contents:

- *Pre-requisites*
 - *Enable*
 - *Configure*
 - *List of Roles*
 - *Per-User Assignments*
 - *Assignment per API*
-

Optionally for single sign-on, the Trifacta® platform can leverage the AWS user/role mappings that are managed by a SAML authentication provider. In this authentication scenario:

- The Trifacta platform uses its native SAML support for SSO authentication.
- Access to AWS resources is governed by the set of permissions and IAM roles that are managed by your AWS admins. The Trifacta platform does not allow editing of the list of available IAM roles for use.
- Authentication to AWS is governed by a third-party SAML provider, which has access to this set of IAM roles and underlying permissions.
- Users of the Trifacta platform are mapped to one or more IAM roles. These IAM roles can be selected at the workspace (admin) or individual user level.

Usage:

When this feature is enabled, a user's available IAM roles are automatically synched via SAML. When a user signs in to the Trifacta application, the user can select their default role to use.

Pre-requisites

- Per-user authentication to AWS has been enabled. For more information, see *Configure AWS Per-User Authentication*.
- This feature is supported only for the SAML authentication method of SSO authentication native to the Trifacta platform. It is not supported for any other SSO auth method. For more information, see *Configure SSO for SAML*.
- AWS permissions must be defined via IAM role and made available to an identity provider that adheres to SAML standards. The SAML identity provider must be configured with a list of SAML assertions containing the IAM roles that an external user may assume.

NOTE: When this feature is enabled and the platform is restarted, users of the Trifacta platform cannot authenticate to AWS resources until IAM roles have been assigned to their accounts. Where possible, you should enable this feature on an unused instance of the platform.

Enable

To enable, the following configuration change must be applied.

Steps:

1. You can apply this change through the *Admin Settings Page* (recommended) or `trifacta-conf.json`.
For more information, see *Platform Configuration Methods*.
2. Locate the following parameter, and set it to `true`:

```
"feature.importAwsRoles.saml.enabled": true,
```

3. Save your changes and restart the platform.

Configure

After the feature has been assigned, roles must be assigned to users.

List of Roles

The list of available roles is passed from the SAML identity provider to the Trifacta platform. From this list of roles, each user can select the one to apply to the account.

Per-User Assignments

Individual users must select the IAM role ARN to assume from the list exposed by Trifacta administrator.

NOTE: Before a user is permitted to complete login to the application, the user must select a role from the provided list.

For more information, see *Configure Your Access to S3*.

Assignment per API

You can use the platform APIs to create platform AWS roles and assign them to users. For more information, see *API Workflow - Manage AWS Configurations*.