Configuring SAML SSO Authentication

Security Assertion Markup Language (SAML) enables web-based, cross-domain single sign-on (SSO) to the AtScale Design Center. After you set up integration with SAML for an AtScale organization, users in that organization sign into AtScale using single sign-on instead of a username and password.

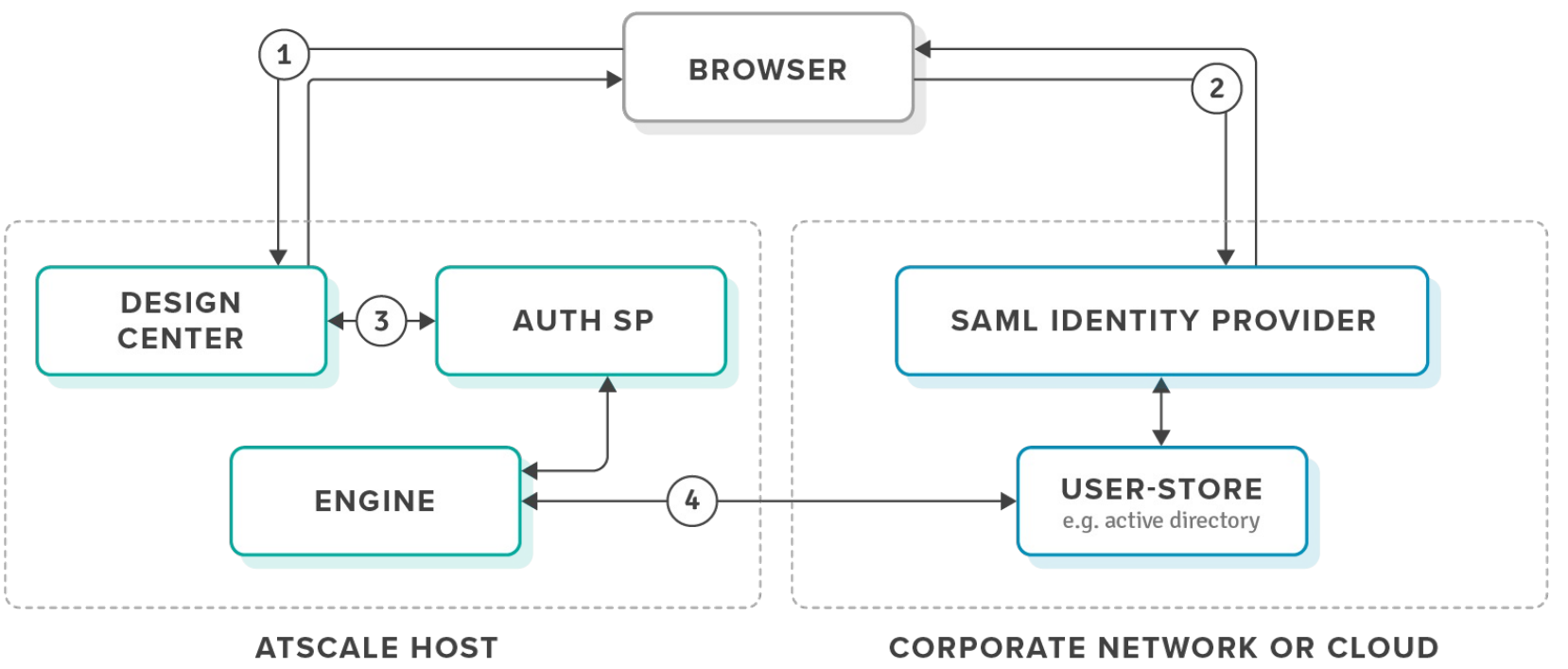
The configuration procedure establishes a trust relationship between AtScale and your Identity Provider (IdP), which allows the IdP to authenticate users and log them into AtScale.

- When SAML SSO is enabled, Basic authentication for AtScale APIs is disabled. Scripts using AtScale APIs must be reconfigured to use a SAML JWT endpoint. See "Next Steps" in this topic.
- To use SAML SSO authentication, you must be operating on a secured (TLS-enabled) AtScale environment.

How Login Works

Once you have configured SAML for an AtScale organization, SAML enables user SAML login to AtScale through the Design Center. Logging into the Design Center follows the flow illustrated in Figure 1 for any user who is part of that organization.

Figure 1. Design Center SAML Authentication Process Flow



1. When a user is directed to the Design Center login page, they select their AtScale organization and click the login button.
2. AtScale redirects the browser to the IdP you configured, which authenticates the user when they provide their

login information.

3. The browser redirects back to AtScale, which verifies the user's SAML authentication and grants the user access to the landing page for their organization.
4. The AtScale engine looks up the user's group membership in the directory with the service account you are using with AtScale.

Logging out of AtScale only logs a user out of the AtScale session. AtScale does not log the user out of the IdP.

Before You Begin

Carefully review the prerequisites and restrictions before configuring SAML.

Prerequisites:

- Permissions to edit an AtScale organization
- AtScale roles and groups configured, connection to an external directory service, and the directory mapped to AtScale roles (See the documents in Using External Authentication)
- A SAML 2.0-based Identity Provider (IdP)
- A metadata XML file from your IdP
- Service Provider (SP) encryption certificate and encryption private key
- (Optional) SP signing certificate and signing private key
- Ensure that the certificate chain for each certificate used in your SAML configuration is valid. For example, ensure that each intermediate and root certificate authority specified in your AtScale SAML certificates and SSL certificate is imported into your identity provider's key store. You must do this if you are using self-signed certificates for testing purposes.

Restrictions:

- AtScale only supports SAML 2.0 POST bindings. GET bindings are not supported.
- Some IdPs do not accept certificates generated from PKCS1 keys. To ensure your IdP accepts the certificates provided to it, generate it from a PKCS8 key that contains a PKCS1 key. For example, using OpenSSL:

```
openssl genpkey -algorithm RSA -out [privateKeyFileName].pem
openssl req -new -x509 -key [privateKeyFileName].pem -out [pubKeyFileName].pem -days [numDaysValid]
```

About This Task

To configure SAML authentication, you will upload IdP metadata and required certificates and private keys to AtScale. AtScale then generates a metadata file for you to provide to the IdP.

Follow this procedure separately for each AtScale organization for which you would like to enable SAML authentication.

Procedure

1. In the Design Center, go to **Security** > **SAML Configuration**.
2. Enter information in the following fields:

    1. **Name**: The name of the Identity Provider. This name will be displayed to users on the login screen's authentication button.
    2. **User ID Attribute Mapping to UID**: Enter the name of the attribute in the SAML Assertion that will contain the user's unique ID. (This is configurable at your IdP.) The value contained by this attribute should match whatever the directory considers the user's unique ID. To see the label for this value according to the directory, go the directory. If these values do not match, user lookup will fail. AtScale directory setup. (To see this value in directory setup, in the Security tab go to Directory > Setup. The value is listed under User Schema Settings, in the field User Unique ID Attribute.)

3. Upload the following files to AtScale:

    1. **Identity Provider Metadata**: The XML file provided by the IdP.
    2. **Service Provider Key Pairs**: The encryption certificate and private key. Optionally, also upload the signing certificate and signing private key. If you do not upload the signing certificate and private key, AtScale uses the encryption certificate and private key.

4. Select **Require Assertion Signing** if you need AtScale to require valid signatures on respones from the IdP.
5. Select the **Save** button (or **Update**, if you have configured SAML integration before).
6. Select the **Download** icon to download the AtScale metadata file. AtScale generates a new version of this file whenever you save your SAML configuration changes on this page.
7. After downloading the generated metadata file, you must securely share the file with your IdP. To do so, go to your IdP dashboard or contact your IdP.
8. After sharing the AtScale metadata file with your IdP, test to ensure the setup is working:

    1. Return to the SAML Configuration page and select the **Test Authentication** button. A new browser tab opens that prompts you for your IdP credentials.
    2. Enter your IdP credentials. If SAML configuration was successful, the browser redirects you to the AtScale landing page.

9. Once you have tested the configuration successfully, enable SAML authentication. Return to the SAML Configuration page, select the **Enable** option under Login Preference,then select **Update**.

After SAML setup for an organization, users in that organization can no longer log in locally. Only the local system administrator can log in with a username and password instead of SAML authentication.

Next Steps

When SAML SSO is enabled, Basic authentication for AtScale APIs is disabled, unless using administrator credentials to get a JWT token through the Basic authentication endpoint.

Scripts using AtScale APIs without administrator credentials must use a SAML JWT endpoint at `/org/:orgId/SAML2/ConstructAndRedirectSAMLRequest`.

This endpoint initiates a redirect to the IdP's login page. The script needs to input credentials, POST the credentials, follow the redirect back to AtScale, and read the response from AtScale. The response is a plaintext JWT in the success case, and an error otherwise.

Using Azure Active Directory (Azure AD) As The LDAP Server And SAML Identity Provider

As of AtScale version 2020.2.0, AtScale supports using Azure AD as both the LDAP Server and SAML Identity Provider. If Azure AD is your SSO Authentication method, read the following sections to configure Microsoft Azure AD with AtScale.

About This Task

To configure Azure AD SAML authentication, you will upload IdP metadata and required certificates and private keys to AtScale. AtScale then generates a metadata file for you to provide to the IdP.

Follow this procedure separately for each AtScale organization for which you would like to enable SAML authentication.

Procedure

Begin with steps one and two if you are starting from scratch and configuring a non-gallery application for SSO within Azure AD. Start with step three if the AtScale non-gallery application is already configured for SSO within Microsoft Azure AD.

1. In the Azure AD application, follow the steps to configure a non-gallery application (AtScale) found in Add an enterprise application.
2. Configure the newly registered application for SAML SSO by following the instructions in View enterprise applications. The Microsoft Azure AD SAML Configurations are as follows:

- **Entity ID**: Entity ID from Service Provider (AtScale) metadata.
- **Reply URL**: Assertion Consumer Service url in the AtScale metadata.
- **Sign on URL**: `https://hostname:port/org/:orgId/`
- **User Attributes and Claims**: The Unique User Id attribute must be present in the **Additional Claims** section. To ensure this is true, look to the value of the **unique user identifier** (name id) within the Additional Claims section and ensure that same value is being used for another claim in the **Additional claims** section. Record the claim name associated with the value in the additional claims section, as this name will be used on the AtScale SAML configuration page in the **Attribute Mapping** section.

3. In the Design Center, go to **Security** > **SAML Configuration**.
4. Enter information in the following fields:

    1. **Name**: The name of the Identity Provider. This name will be displayed to users on the login screen's authentication button.
    2. **User ID Attribute Mapping to UID**: Enter the name of the attribute in the SAML Assertion that will contain the user's unique ID. (This is configurable at your IdP, see step 2.) This value should correspond to the LDAP attribute specified for the **User Unique ID Attribute** on the AtScale Custom Directory Setup page. To access the AtScale Directory Setup page select **Security** > **Directory: Setup** and then select **Custom Directory** as the type of directory service.

5. Upload the following files to AtScale:

    1. The **Identity Provider Metadata**: Navigate to the SAML Signing Certification section here to download the Federation Metadata XML. Once downloaded, upload the file to AtScale on the SAML Configuration page..
    2. **Service Provider Key Pairs**: The encryption certificate and private key. Optionally, also upload the signing certificate and signing private key. If you do not upload the signing certificate and private key, AtScale uses the encryption certificate and private key.

6. Select **Require Identity Provider assertion signing** if you need AtScale to require valid signatures on responses from the IdP.
7. **Login Preference**. Dictates whether the SAML login option will be present on the AtScale login page.
8. Select the **Download** icon to download the AtScale metadata file once the SAML configuration is complete. AtScale generates a new version of this file whenever you save your SAML configuration changes on this page.
9. After downloading the generated metadata file, you must securely share the file with Azure AD (You will see a warning about authentication requests not being signed. This is expected behavior). For more details on uploading the file to Microsoft Azure AD, click here.
10. After sharing the AtScale metadata file with Azure AD, test to ensure the setup is working:

1. Return to the SAML Configuration page and select the **Test Authentication** button. A new browser tab opens that prompts you for your IdP credentials.
2. Enter your credentials from a valid user account that the AD will recognize. If SAML configuration was successful, the browser redirects you to the AtScale landing page.

11. Once you have tested the configuration successfully, enable SAML authentication. Return to the SAML Configuration page, select the **Enable** option under Login Preference,then select **Update**.

After SAML setup for an organization, users in that organization can no longer log in locally. Only the local system administrator can log in with a username and password instead of SAML authentication.