aspera
an IBM® company

SAML Single Sign-On (SSO) for Aspera Web Applications

AT A GLANCE

Key Features

- Built in support for SAML 2.0 to enable single sign-on (SSO) for Aspera web applications: *faspex*, Shares, and Console.
- Federated Identity across Aspera web applications and third party web applications that share the same Identity Provider.
- Utilize existing Identity Provider to authenticate with Aspera web applications.
- New users to Aspera web application can be provisioned in real time through SAML just-in-time provisioning.

Key Benefits

- Reduce repetitive sign-on across Aspera and third party web applications.
- Reuse existing Identity Providers to centrally manage user credentials.
- Streamline access to Aspera web applications.
- Automatically provision new users and grant access to Aspera web application.

SAML (Security Assertion Markup Language) 2.0 is a popular open standard data format that supports Single Sign-On (SSO) among multiple applications. By utilizing SAML, users can sign into one Aspera application and simultaneously have access to any of the other Aspera web applications.

With SAML, Aspera enables web browser single sign-on (SSO) for Aspera *faspex*, Shares, and Console web applications. Once authenticated through SAML, users can seamlessly utilize any authorized Aspera web applications without having to reenter their credentials for access – thus providing federated identity.

FEDERATED IDENTITY

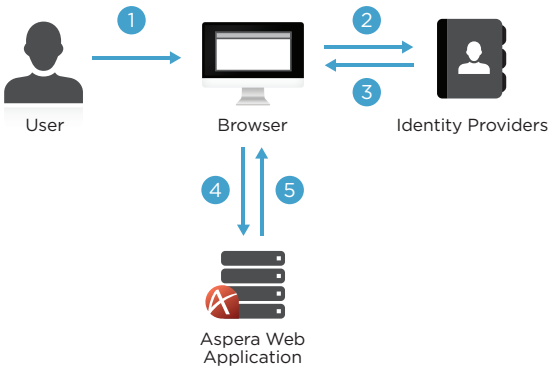
SAML uses two main actors in its specification, the Service Provider and the Identity Provider. Under the SAML model, each of the Aspera web applications is a Service Provider from the end user's perspective. The customer also utilizes an Identity Provider to authorize and authenticate the end users to the Aspera (or other) Service Provider. An Identity Provider can utilize existing user credentials – such as Microsoft Active Directory or other LDAP to authenticate users and send a SAML response to the Service Provider.

By utilizing SAML, users can sign into any application supported by the customer Identity Provider, including any Aspera web application. As a result SAML federates identity across the *faspex*, Shares and Console web applications.

HOW SAML WORKS

When a user attempts to log into an Aspera web application, the Aspera application functions as a SAML Service Provider, generating a SAML request to the Identity Provider. The Identity Provider will parse the SAML request and authenticate the user to the customer's other existing backend user stores. Upon authentication, the Identity Provider sends a SAML response back to the Aspera application. Assuming the user was authorized to access the web application, Aspera will then take the user to the page they requested.

SAML SINGLE SIGN-ON PROCESS



1. User connects to the Aspera web application (*faspex*, Shares, Console) via its URL.
   - If the user has not already authenticated with another Aspera or third party web application within the single sign-on (SSO) system, the user will be prompted to enter their credentials.
   - If the user has already been authenticated through another web application, the information provided previously will be used to authenticate and authorize the user for this particular Aspera web application.
2. A SAML request is sent to the Identity Provider.
3. The Identity Provider authenticates the user based on the information provided and sends a SAML response back to the browser.
4. The browser sends the SAML response to the Aspera web application.
5. The Aspera web application will now take the appropriate action depending on the SAML response received.
   - A user takes no additional steps and will be able to see the requested page, if authorized for the Aspera web application.
   - If the user is authorized and has never used the Aspera web application before, the Aspera web application will provision the user before showing the user the requested page.
   - If the user is not authorized, the user will not be able to see the content available from the Aspera web application.

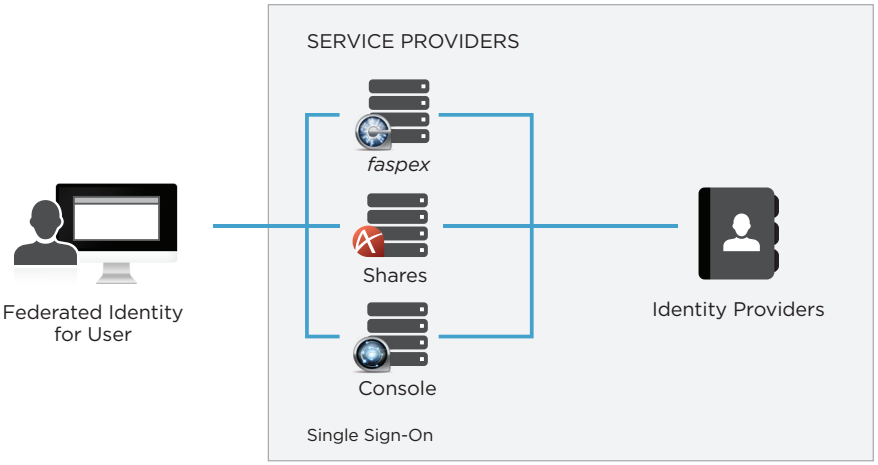
SAML Single Sign-On (SSO) for Aspera Web Applications

TESTED IDENTITY PROVIDERS

- ForgeRock OpenAM
- Microsoft ADFS
- PingIdentity PingFederate
- Shibboleth

SUPPORTED ASPERA SOFTWARE VERSIONS

- Aspera *faspex* 3.5.5+
- Aspera Shares 1.6.3+
- Aspera Console 2.3.0+



SAML CONFIGURATION

SAML is easily configured and is completed in three distinct steps:

STEP 1: IDENTITY PROVIDER CONFIGURATION

The purpose of this step is to have an existing Identity Provider recognize the Aspera web application as a trusted Service Provider. The Identity Provider will learn about the Aspera web application though the Aspera web application's details such as the entity ID, Assertion Consumer Service, and the base URL. This enables the Identity Provider to send the SAML request back to the Aspera web applications.

The Identity Provider will also be configured with the SAML attributes needed by the Aspera web application. These SAML attributes can include information such as username, email, first name, and last name.

The final step to configure the Identity Provider is to extract the Identity Provider's certificate fingerprint (SHA1) or actual certificate for the Aspera web application. This enables the Service Provider to properly send SAML request to the Identity Provider.

STEP 2: ASPERA WEB APP CONFIGURATION

In the second step, the administrator will configure the Aspera web application to accept user authentication validated by the Identity Provider. This allows the Aspera web application to properly send and receive SAML requests to and from the Identity Provider.

The Aspera web application will be configured with the Identity Provider's single sign-on URL and SSL certificates, among other common configuration data.

STEP 3: USER PROVISIONING

When the Identity Provider and the Aspera web application are configured, users can access the Aspera web application [assuming the user account has been configured in the Aspera web application]. If the user account was not created or imported into the Aspera web application, the Aspera web application supports just-in-time provisioning for the user.

In the case of just-in-time provisioning, there will be a normal exchange between the Identity Provider and the Aspera web application. Once Aspera learns that the user has been authenticated, the Aspera web application will create the user account. From the user perspective, he or she will not know that their account has just been created and will just be logged into the Aspera web application.

About Aspera

The creator of next-generation transport technologies that move the world's data at maximum speed regardless of file size, transfer distance and network conditions. Based on its patented FASP™ protocol, Aspera software fully utilizes existing infrastructures to deliver the fastest, most predictable file-transfer experience. Aspera's core technology delivers unprecedented control over bandwidth, complete security and uncompromising reliability. Organizations across a variety of industries on six continents rely on Aspera software for the business-critical transport of their digital assets.

Learn more at www.asperasoft.com