Recast

SAML 2.0

Last Modified on 04.22.26

Security Assertion Markup Language 2.0 (SAML 2.0) is an industry standard for exchanging identification, authentication and authorization data between trusted parties. Application Workspace implements a SAML 2.0 Identity Provider that can federate with SAML 2.0 Service Providers (SP) for exchanging data.

Settings screen

Metadata section

Allow metadata queries – If enabled, external parties can receive the metadata of this identity provider. In most cases, it's recommended to allow it, so that federations can be performed quickly and easily. This option can always be disabled after setting up a federation; it's important to remember that some service providers can monitor the metadata to automatically pick up changes like Active Directory Federation Service (AD FS).
Metadata URL – The URL where the metadata is published. Note that even if the **Allow metadata queries** option is disabled, an administrator can always download the metadata by using the **Download** button.

Single sign in/logout sections

Allow post requests (recommended) – If enabled, the identity provider allows incoming authentication/logout request messages by HTTP POST.
Allow redirect requests – If enabled, the identity provider allows incoming authentication/logout request messages by HTTP REDIRECT.
Require signing – If enabled, the authentication/logout messages must be signed by a trusted certificate. If disabled, any signing will be ignored.

> Recommendations
> We recommend you use the POST method over REDIRECT, especially when **Require signing** is enabled.
> Note that in the case of HTTP REDIRECT, the size of the messages can exceed the limit of the browser URL and also HTTP REDIRECT is less secure than HTTP POST.
> We also recommend activating the **Require signing** option for logout messages, otherwise it could be possible for a third-party to start the logout process for any known username.

Session section

Insert the number of seconds you want a SAML session to be valid for, without being refreshed. If you insert the value of zero, SAML sessions will never expire.

Service Providers screen

Service providers contains the definition and settings of the trusted third-parties that are federated with this identity provider.

If you click **Create service provider** in the table toolbar of the **Service Providers** tab, a dialog box with the same name will open.

Create service provider type

You can create a service provider manually. Find below the description of the most important elements of a *Create service provider* type of provider.

General tab

General section
Name – Provide the name of the service provider. It will be visible for users when they log out.
Entity ID – The SAML 2.0 Entity ID for this service provider.
Signing Certificate – The certificate used for verifying the SAML message signatures.
Profile – The profile that will be used to send additional information with a successful authentication response.

Name Identifier section
Format – The format of the unique identifier used for the authenticated user:

- *Transient* – an identifier that is only valid within a SAML session. If a user authenticates again through SAML, another newly created identifier will be used.
- *Persistent* – an identifier that is always valid for the same user. If a user authenticates again through SAML, the same identifier will be used.
- *Unspecified* – an identifier that is agreed upon between the two parties and that is not defined within the SAML specifications.
- *Windows Domain Qualified Name* – The authentication name as used for Active Directory.
- *Email Address* – The email address of the user.

Attribute – Specify the value of the name identifier.

End points tab

Single sign in/logout sections
Post URL – The service provider's URL to which SAML 2.0 POST authentication/logout messages should be sent.
Redirect URL – The service provider's URL to which SAML 2.0 REDIRECT authentication/logout messages should be sent.

Import Service provider from Metadata type

You can also create a service provider based on the metadata of that SP. The metadata can be provided by URL, file or plain XML text.

Edit service provider dialog box

To view the details of a service provider or edit it, double click its entry.

Access conditions tab

With access control you can limit which users can make use of this service provider. When the access is denied for a user, the user will be redirected to the requesting web application where an access denied error message will be displayed.

The filters available are the same as those for contexts.

Advanced tab

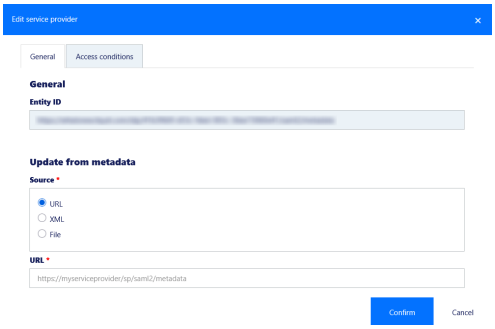
Advanced section
Use consumer URL if provided in an authentication request – If the service provider requests an authentication, it can also provide a consumer URL optionally. A consumer URL can be used to deep redirect the user into the service provider application. We recommend enabling this option when the signing of authentication messages is required, as this can leak potentially user data to untrusted third parties. No domain restriction is applied.
Do full logout of the workspace if this service provider request a logout – If enabled, when the service provider requests a

logout, a full logout of the Application Workspace will execute. Otherwise, the logout will apply only for the service provider that requested it.
The service provider supports that the logout action is embedded (iframe) – Enable this option if the client supports being logged out within an HTML iframe. If there are problems with logging out, we recommend you disable this option.

Custom Logout section
Overrule logout action – If enabled, the logout action will ignore the SAML configuration and will use a custom logout page. This is especially handy for service providers that don't support SAML Single Logout.
Logout URL field – If the logout page supports redirect after logout, then use "${slo.return.url}" as variable to generate a URL back to the Application Workspace that will report the logout status to the logout page.
Does the custom logout report status back – If enabled, the logout page will wait for the status report. Otherwise, the logout page assumes a successful logout after a few seconds.
Does the custom logout use a secure connection – If enabled, the logout URL and redirects on the service provider are considered secure. A secure connection is important especially in scenarios where embedded content is supported by specific browsers.

Metadata tab

The **URL** and **XML** fields in this tab cannot be edited here, they just display the existing information. To import metadata from URL, XML or a local file you must first click **Update from metadata** and the following dialog will be displayed:



Here you can choose to enter the URL where the IdP SAML configuration is stored, copy the content of the metadata XML or import the metadata XML from a local folder on your computer.

After you click **Confirm** all the options that can be derived from the metadata will be updated.

Profiles screen

When a user authenticates to a service provider, the identity provider can send additional information about the user: group membership, company information etc.
Define a profile for every different set of information that should be sent.