saml-metadata-idp-sso-settings

Jump to:

SingleSignOnService endpoint requirements | Should I configure a SingleLogoutService endpoint? | Should I configure a ArtifactResolutionService endpoint?

The IdP SSO Settings section in Federation Manager is where a Site Administrator configures all the key Identity Provider (IdP) service endpoints found in the SAML metadata's `IDPSSODescriptor` element. These include Single Sign-On Service endpoints (`<SingleSignOnService>`), Single Logout Service endpoints (`<SingleSignOnService>`), and Artifact Resolution Services endpoints (`<ArtifactResolutionService>`). Single n Federation Manager og into the Federation Manager as a Site Administrator (SA). To configure:

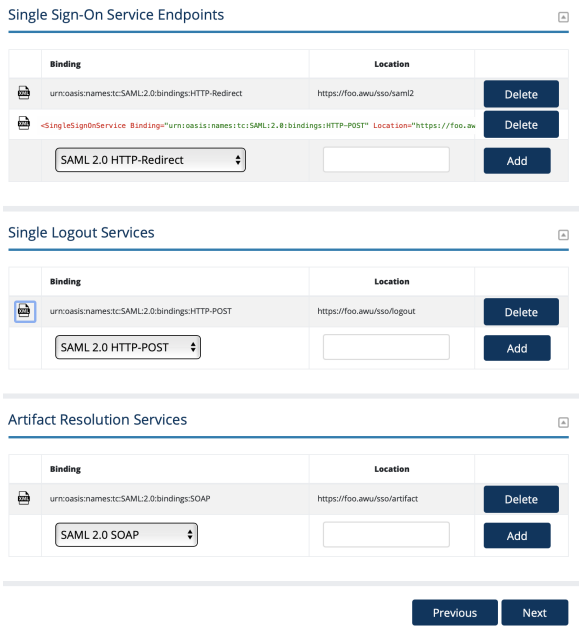
Login to Federation as a Site Administrator

Click on the entity you wish to update to bring up the View/Edit page.

On the left navigation, click "IdP SSO Settings".

Enter the location of your service end points in their respective sections shown in the "IdP SSO Settings" section.

Click the XML toggle icon to preview your endpoint as shown in SAML.



SingleSignOnService endpoint requirements

All `<SingleSignOnService>` endpoints **MUST** begin with **https://**, that is, a SingleSignOnService endpoint must be encrypted with modern, supported TLS encryption.

An IdP in the Incommon Federation **MUST** include a `<SingleSignOnService>` endpoint with a SAML2 `HTTP-Redirect` binding.

An IdP **SHOULD** include a `<SingleSignOnService>` endpoint with a SAML 2.0 `HTTP-POST` binding to maintain compatibility with SAML Service Provider (SP) deployments that prefer a SAML 2.0 HTTP-POST binding.

We **STRONGLY RECOMMEND** an IdP registered in the Incommon Federation support both bindings.

DO NOT register any SAML1 endpoints. SAML1 is deprecated. The option is available for legacy support only.

As a general rule, configure the least number of SingleSignOnService endpoint you need to interoperate. A typical new IdP should only configure two SingleSignOnService endpoints: one each with SAML 2.0 `HTTP-Redirect and SAML 2.0 HTTP-POST` respectively. Add additional endpoints only when necessary.

Working with SAML metadata

- Manage metadata export options
- Qualifications and Capabilities (Entity Attributes, etc.)
- SAML Representation of InCommon Metadata
- Requested Attributes
- Entity ID
- Scope
- Contacts information
- IdP SSO Settings (IDPSSODescriptor)
- SP SSO Settings (SPSSODescriptor)
- Signaling Encryption Method Support for a Service Provider

Related content

- Requirements to use Federation Manager
- What's New in Federation Manager
- Review and submit metadata
- Understanding the Endpoint Encryption Score
- Reset your Federation Manager user password
- Federation Manager
- Assign metadata management to a Delegated Administrator
- Prepare for Delegated Administration assignment
- Assign access to a Delegated Administrator
- Add an identity provider

Get help

Can't find what you are looking for?

help Ask the community

See Section 5.1 Web Browser SSO Profile in the Security Assertion Markup Language (SAML) V2.0 Technical Overview.

Should I configure a SingleLogoutService endpoint?

Although supported in Federation Manager, an IdP operator should take care when configuring an single logout (SLO) endpoint:

An IdP that introduces an SLO endpoint in its metadata is inviting an SP to send a logout request. If a SP does so but does not configure its own SLO endpoint in the published metadata, an error will occur on the IdP side when the IdP attempts to process the single logout request.

For example, a Shibboleth SP is configured to send SLO requests out-of-the-box. If the SP operator register its SLO endpoint in its published metadata, all is well. Otherwise, when that Shibboleth SP interacts with an IdP that advertises an SLO endpoint during a user logout, the SP detects the IdP's SLO endpoint and automatically sends a SLO request to the IdP. The IdP attempts to respond to the SLO request. However, with no SLO endpoint in the published SP metadata, the IdP fails because it doesn't know how to send the response back to the SP.

Should I configure a ArtifactResolutionService endpoint?

As a general rule, don't. This style of SAML message exchange has largely fallen out of favor in InCommon and is not preferred.

Configure an `<ArtifactResolutionService>` endpoint only if you know you will be integrating with a SP that insists on using the SP-initiated SSO / Artifact Binding exchange. If you do configure a `<ArtifactResolutionService>` endpoint, make sure to also configure a `<SingleSignOnService>` endpoint with a `SAML 2.0 SOAP` binding.

See Section 5.1.3 of the Security Assertion Markup Language (SAML) V2.0 Technical Overview.

Also see https://wiki.shibboleth.net/confluence/display/SP3/ArtifactResolutionService.