saml-metadata-sp-sso-settings

Jump to:

AssertionConsumerService endpoint (ACS URL) requirements | Configuring Requested Attributes | Should I configure a SingleLogout endpoint?

The SP SSO Settings section in Federation Manager is where a Site Administrator configures the key Service Provider (SP) service endpoints found in the SAML metadata's `SPSSODescriptor` element. These include:

- Assertion Consumer Service endpoints (`<AssertionConsumerService>`),also known as ACS URLs
- Discovery Response locations (`<SingleSignOnService>`)
- Requested Attributes (`<RequestedAttribute>` elements within `<AttributeConsumingService>`)
- Single Logout Service endpoints(`<SingleLogoutService>`).

To configure:

Login to Federation as a Site Administrator

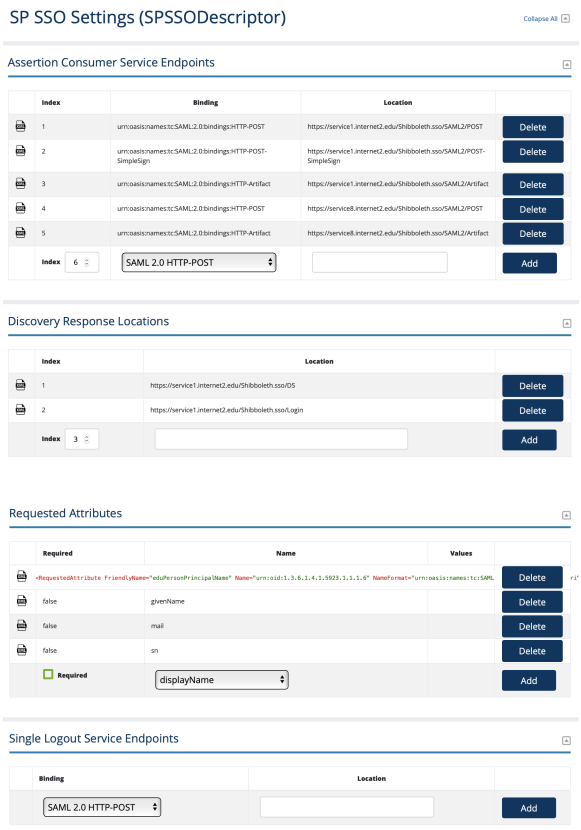
Click on the entity you wish to update to bring up the View/Edit page.

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

Enter information as directed as shown in the "SP SSO Settings" section.

Click the XML toggle icon to preview the data you've entered as shown in SAML.

Use the toggle in the Index column to manually order your ACS URLs and Discovery Response endpoints.



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

AssertionConsumerService endpoint (ACS URL) requirements

All `<AssertionConsumerService>` endpoints **MUST** begin with **https://**, that is, an Assertion Consumer Service endpoint, or ACS URL, must be encrypted with modern, supported TLS encryption.

A SP in the Incommon Federation **MUST** include at least one `<AssertionConsumerService>` endpoint with a SAML2 `HTTP-POST` binding.

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

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

Should I configure a DiscoveryResponse location?

If you have configured your SP to use a home organization discovery service via the *SAML V2.0 Identity Provider Discovery Protocol*, you **MUST** include at least one `<DiscoveryResponse>` endpoint in your SP metadata. The discovery service will redirect the user back to you at the designated endpoint once they have selected their preferred identity provider. InCommon Wayfinder is InCommon Federation's default home organization discovery service.

Related: What is InCommon Wayfinder?

Configuring Requested Attributes

Configuring Requested Attributes is optional.

Federation Manager lets you select from a list of commonly supported attributes in the Incommon Federation when configuring Requested Attributes.

To learn more, see Requested Attributes.

Should I configure a SingleLogout endpoint?

If you have configured your SP to send single logout (SLO) requests to an IdP advertising a SingleLogoutService endpoint, you must publish your SP's SingleLogoutService endpoint in your published metadata. Failing to do so will cause an error when the IdP attempts to respond to your SP's SLO request.

Shibboleth SP software is by default configured to send SLO requests.