

SP Endpoints

Endpoints in SP Metadata


This page gives guidance and recommendations regarding SAML endpoints in SP metadata. [Endpoints in Metadata](#) are crucial to the overall security and interoperability of SAML protocol exchanges.

An *endpoint in metadata* signals support for a specific profile of SAML. In particular, all SPs in InCommon metadata MUST support *SAML2 Web Browser SSO* by including certain browser-facing SSO endpoints in metadata. Support for any other profile is strictly OPTIONAL.

Endpoint Requirements

The most important endpoint in SP metadata is the `<md:AssertionConsumerService>` endpoint. Every SP MUST have at least one such endpoint in metadata.

An SP that supports SAML V2.0 Web Browser SSO MUST include at least one `AssertionConsumerService` endpoint that supports the SAML V2.0 HTTP-POST binding. Occasionally an IdP will prefer to respond with an artifact, and therefore an `AssertionConsumerService` endpoint that supports the SAML V2.0 HTTP-Artifact binding MAY also be included in SP metadata. Note: An SP that supports artifact resolution MUST have at least one signing certificate in metadata.

 **Single Logout Endpoints**
A single topic covering [Single Logout Endpoints](#) in both IdP and SP metadata will be found elsewhere in this wiki.

Discovery Service Endpoints in SP Metadata

If your SP is configured to use the [SAML V2.0 Identity Provider Discovery Protocol](#), you MUST configure your SP's metadata to include one or more `<idpdisc:DiscoveryResponse>` extension elements. (In practice, the actual number of such endpoints is implementation-dependent.) A discovery service will redirect the unauthenticated user back to the SP at the designated endpoint once the user has selected their preferred identity provider.

Technical Details

Support for *SAML V2.0 Web Browser SSO* is REQUIRED:

- SPs MUST include an SSL/TLS-protected `<md:AssertionConsumerService>` endpoint that supports the SAML V2.0 HTTP-POST binding.
- SPs MAY include an SSL/TLS-protected `<md:AssertionConsumerService>` endpoint that supports the SAML V2.0 HTTP-Artifact binding.
- SPs MAY include an SSL/TLS-protected `<idpdisc:DiscoveryResponse>` endpoint that supports the *SAML V2.0 Identity Provider Discovery Protocol*.

SAML Endpoints in SP Metadata
<pre><!-- SAML V2.0 --> <md:AssertionConsumerService index="1" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://sp.example.org/sso/SAML2/POST"/> <md:AssertionConsumerService index="2" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Artifact" Location="https://sp.example.org/sso/SAML2/Artifact"/></pre>
Discovery Service Endpoints in SP Metadata
<pre><!-- SAML V2.0 --> <idpdisc:DiscoveryResponse index="1" xmlns:idpdisc="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" Binding="urn:oasis:names:tc:SAML:profiles:SSO:idp-discovery-protocol" Location="https://sp.example.org/sso/Login"/></pre>

Note that all of the above endpoints are browser-facing endpoints that run on the default SSL/TLS port (443).

Other Issues

- [SP Endpoints for SAML1](#)