Static Analysis of IdP Endpoints

> ⚠ **Deprecated**
>
> Note that this page has been deprecated. The information it contains is no longer current.

Static Analysis of IdP Endpoints in Metadata

The results of the latest *static analysis of IdP endpoints in metadata* are summarized below:

```
Static Analysis of IdP Endpoints in Metadata

   2 IdPs with 1 endpoints
  20 IdPs with 2 endpoints
  24 IdPs with 3 endpoints
   9 IdPs with 4 endpoints
  12 IdPs with 5 endpoints
 106 IdPs with 6 endpoints
  41 IdPs with 7 endpoints
 120 IdPs with 8 endpoints
   8 IdPs with 9 endpoints
   2 IdPs with 10 endpoints
   1 IdPs with 12 endpoints

 345 total IdPs in metadata

 556 ArtifactResolutionService endpoints in IdP metadata
 477 AttributeService endpoints in IdP metadata
  29 SingleLogoutService (SLO) endpoints in IdP metadata
1135 SingleSignOnService (SSO) endpoints in IdP metadata

2197 total endpoints in IdP metadata

  12 SLO endpoints with HTTP-POST binding
  13 SLO endpoints with HTTP-Redirect binding
   4 SLO endpoints with SOAP binding

 310 SSO endpoints with AuthnRequest binding
 323 SSO endpoints with HTTP-POST binding
 163 SSO endpoints with HTTP-POST-SimpleSign binding
 327 SSO endpoints with HTTP-Redirect binding
  12 SSO endpoints with SOAP binding (ECP)

-----IdPs with issues-----

  11 SAML1-only IdPs with no SAML2 SSO endpoints
   9 SAML2 IdPs with no HTTP-Redirect binding
   8 IdPs with duplicate bindings
 181 IdPs with SAML2 AttributeService endpoints

-----IdP endpoints with possible issues-----

  15 IdP endpoint locations with unexpected port
  97 IdP endpoint locations with missing port

-----
http://md.incommon.org/InCommon/InCommon-metadata.xml
Thu Apr 3 06:27:48 EDT 2014
```

The raw endpoint data used to compile the above statistics are attached to this wiki page.

Static Properties of Endpoints

At the bottom of the output shown above, you'll notice some special categories of IdPs and endpoints:

1. SAML1-only IdPs with no SAML2 bindings (see idps-no-saml2-sso.txt)

2. SAML2 IdPs with no HTTP-Redirect binding (see idps-no-http-redirect.txt)
3. IdPs with duplicate bindings (see idps-duplicate-bindings.txt)
4. IdPs with SAML2 AttributeService endpoints (see idps-saml2-attribute-service.txt)
5. IdP endpoint locations with unexpected port (see idp-endpoints-unexpected-port.txt)
6. IdP endpoint locations with missing port (see idp-endpoints-missing-port.txt)

Each of these IdP categories is discussed below.

SAML1-only IdPs

The OASIS SAML V2.0 standard is more than nine years old. By now, every IdP in the InCommon Federation should support SAML V2.0. If yours doesn't, and you don't have a plan to migrate to SAML V2.0 in the near future, please develop such a plan now.

In the future, any new services introduced into the Federation will require SAML V2.0. Many already do. Don't miss out, migrate to SAML V2.0 as soon as possible.

No HTTP-Redirect Binding

Every SAML2 IdP in the InCommon Federation must support the HTTP-Redirect binding. If you don't, we will be contacting you and asking you to support HTTP-Redirect.

Duplicate Bindings

An IdP must not have two browser-facing endpoints (`SingleSignOnService` or `SingleLogoutService`) with the same binding. For example, two `SingleSignOnService` endpoints that claim to support the HTTP-Redirect binding are not allowed. Either you support a binding or you don't, but it doesn't make sense to support a binding twice. Please remove all duplicate endpoints from your metadata.

SAML2 AttributeService Endpoints

If your SAML2 IdP pushes attributes on the front channel, that back-channel SAML2 AttributeService endpoint you have in metadata may be serving no purpose. Depending on your default attribute release policy, SPs may be querying your AttributeService endpoint unnecessarily.

Unexpected Port Number

A port number is expected (but not required) on any SAML1 or SAML2 SOAP endpoint. Anything else is unexpected and therefore flagged.

Just because your IdP has never exhibited an error doesn't mean your metadata is correct. If, for example, all your SP partners send requests to one your SAML2 browser-facing endpoints (HTTP-Redirect or HTTP-POST), you would never know you had a problem since all your SOAP endpoints would go unused in that case.

Missing Port Number

A port number is expected (but not required) on any SAML1 or SAML2 SOAP endpoint. If you expose such an endpoint in metadata *without a port number*, it is flagged. That doesn't mean its wrong but it is *likely* to be wrong (depending on your deployment characteristics).

As in the previous section, SOAP endpoints are often a ticking time bomb (which is a bit of an over-dramatization, I know, but you get the idea) 🙂

File	Modified
Text File idps-redundant-bindings.txt Historical data, please IGNORE	Apr 03, 2014 by trscavo@internet2.edu
Text File non-http-redirect-entities.txt Historical data, please IGNORE	Apr 03, 2014 by trscavo@internet2.edu
Text File non-saml2-entities.txt Historical data, please IGNORE	Apr 03, 2014 by trscavo@internet2.edu
Text File idp-endpoints-unexpected-port.txt IdP endpoints with unexpected port	Apr 03, 2014 by trscavo@internet2.edu
Text File all-idp-endpoints-summary.txt All IdP endpoint summary	Apr 03, 2014 by trscavo@internet2.edu
Text File all-idp-endpoints.txt All IdP endpoints (RAW DATA)	Apr 03, 2014 by trscavo@internet2.edu
Text File idp-endpoints-missing-port.txt IdP endpoints with a missing port	Apr 03, 2014 by trscavo@internet2.edu
Text File idps-duplicate-bindings.txt IdPs with duplicate SAML bindings	Apr 03, 2014 by trscavo@internet2.edu
Text File idps-no-http-redirect.txt IdPs with no HTTP-Redirect binding	Apr 03, 2014 by trscavo@internet2.edu
Text File idps-no-saml2-sso.txt IdPs with no support for SAML2 Web Browser SSO	Apr 03, 2014 by trscavo@internet2.edu
Text File idp-endpoints-saml2-attribute-service.txt Historical data, please IGNORE	Apr 03, 2014 by trscavo@internet2.edu
Text File idps-saml2-attribute-service.txt IdPs with SAML2 AttributeService endpoints	Apr 03, 2014 by trscavo@internet2.edu

Download All