

New IdPs in Metadata

Planning for a New IdP in Metadata

Are you planning to register an IdP in the InCommon Federation? This document addresses a set of topics that are best considered in advance, before registering the actual IdP metadata.



A [Checklist for IdPs](#) deployed in the InCommon Federation

Contents:

- [Designated Site Administrators](#)
- [Metadata Refresh](#)
- [Key Generation](#)
- [Use of Primary Domain](#)
 - [Entity ID](#)
 - [Scope](#)
 - [Endpoint Locations](#)
- [Protocol Support](#)

Designated Site Administrators

One of the first things a prospective Federation participant should do is designate *at least two Site Administrators* to manage metadata. Beyond the obvious advantages of having a trained administrator for backup purposes, multiple Site Administrators has security advantages as well. Like password changes, metadata updates generate email notifications to **all** designated Site Administrators, which helps prevent both honest mistakes and malicious activity.

Metadata Refresh

The importance of *a secure, automated metadata refresh process* can not be over-emphasized. All participants are strongly encouraged to configure their software to *refresh and verify metadata at least daily*. An optimal process will attempt to refresh metadata every hour and intelligently short-circuit that attempt if the metadata file has not changed on the server. The latter is accomplished using a technique called [HTTP Conditional GET](#).


 Read more about [Metadata Consumption...](#)

Key Generation

A secure web server typically protects its browser-facing resources with TLS. To obtain a trusted TLS certificate, an administrator issues a Certificate Signing Request (CSR) to a trusted CA. In doing so, a private TLS key is generated. This key must be generated securely and kept safe for the entire lifetime of the server.

 Read more about [TLS Server Certificates...](#)

A SAML IdP is a secure web server that issues SAML assertions to SPs upon request. Assertions are signed by the IdP for authenticity and integrity. The IdP administrator generates a private signing key for this purpose. (The corresponding public key is bound to a long-lived, self-signed certificate published in SAML metadata.) Like the TLS key, the signing key must be generated securely and kept safe indefinitely. A compromised IdP signing key is the absolute worst thing that can happen in a federated context.

 Read more about [IdP Key Handling...](#)

Develop *a strategy for securing your private keys* before you generate them. Avoid unnecessary exposure by generating the keys on the IdP in the first place. Strictly control access to the IdP system on which the keys are stored. Keep the IdP software and the underlying operating system software patched and up to date.

Use of Primary Domain

An organization's *primary domain* is a critical piece of information used repeatedly in metadata.

 Read more about an organization's [Primary DNS Domain...](#)

Entity ID

The entityID is an identifier for your IdP. Although it is almost always a URL, an entityID is a name (not a location). One of your first (and perhaps most important) tasks is to choose a permanent entityID in a namespace you control. Thus the host part of the chosen URL must be rooted in a DNS name you control (as indicated in the whois database or via a Domain Control Validation process administered by the Registration Authority (InCommon)). This is almost always the primary domain of your organization.

Example. `https://sso.example.edu/idp` where the primary domain is `example.edu`

Choose your entityID carefully—you may not get a second chance. Once an entityID is released into the wild, it will be difficult to change, at least not without a lot of pain.

 Read more about [Entity IDs](#) in metadata...

Scope

A Scope is a suffix appended to so-called *scoped attributes* (such as eduPersonPrincipalName). The attribute's Scope indicates the asserting IdP, which is why the best Scope value is the primary domain of the organization.. Since scoped attributes are typically used for access control at the SP, they are likewise difficult to change once released into the wild.



Avoid multiple Scopes in metadata.



Read more about [Scope in Metadata...](#)

Endpoint Locations

Each of the SAML endpoints published in metadata has a location. Some of these endpoints are browser-facing, and so you should choose a logical hostname that makes sense to the user. This hostname need not agree with your entityID (which is a name, not a location) but in any case, the chosen hostname should be rooted in your primary domain for security, usability, and stability.



Read more about [IdP Endpoints](#) in metadata...

Protocol Support

The following deployment strategy forces all protocol traffic over the front channel, which is easier to troubleshoot, manage, and maintain.



Recommended Protocol Support for New IdPs

- **DO** support SAML2 Web Browser SSO on the front channel
- **DO NOT** support back-channel SAML protocols



Read more about recommended [Protocol Support for New IdPs...](#)