IdP Endpoint Locations

Deprecated

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 The information it contains is no longer current.

Endpoint Locations in IdP Metadata

This topic focuses on the *protocol endpoint locations* in IdP metadata. The parent topic discusses IdP Endpoints more generally.

Consider your endpoint locations to be permanent!

Choose your endpoint locations with care. Once published, it will be difficult to change the endpoint locations in metadata without adversely affecting interoperability.

TLS Requirements

Policy: *All endpoint locations in IdP metadata MUST be HTTPS-protected.* (This policy is enforced by the Federation Manager software.) In particular, all browser-facing endpoint locations MUST be protected with TLS to preserve the confidentiality of secrets and other sensitive information in transit.

Test your TLS configuration

Use SSL Labs to test the browser-facing TLS configuration on your IdP server.

Domain Requirements

Policy: *All domains in IdP endpoint locations SHOULD be controlled by the organization associated with the IdP.* This policy is self-enforced by the IdP owner.

The remainder of this document outlines the advantages of controlling the domains in IdP endpoint locations.

As a hypothetical example, IdP metadata submitted by an organization in control of the **example.edu** domain might contain the following elements:

IdP metadata example #1

1. Entity ID: https://websso.**example.edu**/idp
2. Scope: **example.edu**
3. Endpoint location prefix: https://login.**example.edu**/…

In the above example, a single domain (**example.edu**) is used in all three metadata elements (which is typical). For comparison, if the following metadata were submitted, it too would be accepted:

IdP metadata example #2

1. Entity ID: https://websso.**example.edu**/idp
2. Scope: **example.edu**
3. Endpoint location prefix: https://login.**cloudservice.com**/…

Although the domain **cloudservice.com** is not owned by the organization that owns domain **example.edu**, the metadata is allowed. However, InCommon does not recommend this practice.

Domains in IdP endpoint locations

It is strongly RECOMMENDED that all domains in IdP endpoint locations be controlled by the organization associated with the IdP. Such an endpoint is much more likely to be stable. This is important since changing an endpoint location can affect both interoperability and end-user trust.

Since a browser-facing SSO endpoint location appears in the browser address bar, it contributes to the login interface by definition. A trusted login interface will incorporate design elements that are easily recognized by the user. An SSO endpoint location is one of those elements, so choose your endpoint locations with care. Most importantly, choose a domain that the user recognizes. Most often this will be the primary domain controlled by the organization (such as **example.edu** above) or a subdomain rooted in the primary domain.

> **An SSO endpoint location contributes to user trust**
>
> An SSO endpoint location SHOULD contain a domain that the user recognizes (and therefore trusts).

In any case, once the endpoint location is chosen, it should never change. If you must change an SSO endpoint location in metadata, be sure to let your users know that this change is coming. Doing so helps manage user trust.

> **Stabilize the login interface**
>
> A trusted login interface SHOULD NOT be changed without ample advanced notice to end users. To put it another way: Train your users to expect a stable, consistent login interface. This helps minimize the risk of phishing.

Be aware that changing an endpoint location will disrupt SSO interoperability unless certain precautions are taken. While migrating from one endpoint location to another, an IdP owner may have to run two nearly identical IdPs in production for a time to avoid down time.

> **It's in the best interest of the IdP owner to own the domains!**
>
> The best way to avoid having to change your endpoint locations is to *control the domains on the endpoint locations in metadata*.