saml-metadata-entityid

Jump to:

How to choose a good Entity ID | Examples of well formed entity IDs | About those URN-based entity ID's | References

An ***Entity ID*** is a globally unique name for a SAML entity, i.e., your Identity Provider (IdP) or Service Provider (SP). It is how other services identify your entity. Like any other unique identifiers you share to interoperate with others, making sure your identifier is clear, unique, and permenant is critical for successful continued operation of your service(s). Choose your entity ID carefully and deliberately.

How to choose a good Entity ID

An Entity ID **MUST** be globally unique

To ensure your Entity ID is globally unique, the Incommon Federation asks that your Entity ID be in the form of a universal resource locator (URL). The DNS domain in the URL needs to be a domain for which you can demonstrate control, typically one belonging to your organization. InCommon will perform domain control validation on a domain you use in your entity ID to verify control.

Make every effort to choose an entity ID that will persist indefinitely

Services that interoperate with you use your entity ID to look up your metadata. Changing an entity ID once your service (IdP or SP) is in operation leads to complicated change management efforts spanning multiple organizations. Choose your identifier carefully to guard against identifier changes because you've switched out technology, network topology, product versions, cloud service providers, or any criteria that will likely change over time.

Tips for creating a clear, meaningful entity ID

- An entityID SHOULD be an absolute URL starting with “https://” or “http://”; an URL-based entity ID starting with "https://" is more flexible than one starting with "http://"
- The URL SHOULD NOT contain a port number, a query string, or a fragment identifier
- The host part of the URL SHOULD NOT contain the substring “www”
- The URL SHOULD NOT end with a slash (/)
- An entityID SHOULD NOT be more than 30 characters in length
- Include the substring "idp" in an IdP entity ID
- Include the substring "sp" in an SP entity ID
- Do not include the substring "incommon" in an entity ID
- Do not include the name of your SAML software in an entity ID ("shibboleth", "adfs", "php", etc.)

Additional notes

An entity ID is a name. It need not be a resolvable web location. SAML entity IDs must be a Universal Resource Identifier (URI). Because an URL if a more familiar form of URI, we adopt URL as the preferred format for an entity ID. Although a URL, it's important to note that an entity ID is a persistent identifier, not a web location. An entity ID need not resolve to an actual web resource. If you do make your entity ID a resolvable web link, the link should point to a web page describing your service and mention that the location is an identifier for your service.

The domain in the entity ID need not match those in the endpoint locations in metadata. A common misconception is that the entity ID must match the endpoint locations for the deployment. This is not required. The entity ID should accurately reflect the organization that owns the entity. Endpoint locations, on the other hand, are resolvable DNS names.

Examples of well formed entity IDs

IdP names:

- https://exampleuniverstiy.edu/idp
- https://cloudcompany.com/idp

SP names:

- https://comanage.example.edu/sp
- https://wiki.cs.example.org/sp
- https://intranet.math.example.edu/sp

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

- https://myapp.example.com/sp

About those URN-based entity ID's

In the early days of the Federation, InCommon assigned an URN (Uniform Resource Name) to all new IdPs, based on the IdP's primary DNS domain name:

```
<EntityDescriptor entityID="urn:mace:incommon:example.edu">
```

You may see those in the InCommon metadata. They are legal and you should accept them as valid entity IDs. However, InCommon no longer issues URNs to IdPs. We also no longer allow URNs as entity IDs for newly registered entities.

References

- General discussion of entity naming in the Shibboleth wiki
- InCommon Federation's domain control validation procedure