Hide from Discovery category

Jump to:

[Why use the Hide from Discovery category?](#)

The "Hide from Discovery" entity category is a category of Identity Providers that are intended **not to be shown on discovery interfaces** by default.

> ⚠️ **Hide From Discovery Category Specification**
>
> InCommon's implementation of the *Hide from Discovery category* and the use of the `hide-from-discovery` entity attribute (described below) conform to the [REFEDS Hide from Discovery category specification](#).

The `hide-from-discovery` entity attribute is self-asserted by IdP operators but InCommon Operations may insert the `hide-from-discovery` entity attribute into any IdP entity descriptor at its discretion.

Why use the Hide from Discovery category?

By and large, participants register an IdP for one or more of the following reasons:

1. To interoperate with providers of commercial vendor services called *Sponsored Partners*
2. To interoperate with *Enterprise Services* (co-located in the same security domain as the IdP)
3. To interoperate with cross-domain *Federation Services* such as [Research & Scholarship Category](#) services and other collaborative services

To interoperate with Sponsored Partners and Enterprise Services, a bilateral arrangement is often needed, whereas cross-domain Federation Services are "promiscuous" in the sense that they are willing and able to interoperate with **any** IdP. This gives rise to *IdP Discovery*, a user-driven process (or interface) to discover the federated user's preferred IdP.

An IdP that interoperates solely with Sponsored Partners and/or Enterprise Services may not need (or want) to be exposed on arbitrary discovery interfaces, in which case the IdP should declare the `hide-from-discovery` entity attribute in metadata. Federation Services can (and should) filter such IdPs from their discovery interfaces.

Be aware that InCommon Operations reserves the right to insert the `hide-from-discovery` entity attribute into any IdP entity descriptor at its discretion. Possible reasons include, but are not limited to:

- The IdP is known not to consume InCommon metadata on a daily basis.
- The IdP is in a domain name that is not public.
- The IdP has endpoints that are behind a firewall.

Asserting Hide from Discovery

An IdP calls out its desire to *Hide From Discovery* by asserting the following entity attribute in metadata (whitespace added for readability):

```
<mdattr:EntityAttributes
    xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute">
  <saml:Attribute
      xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
      Name="http://macedir.org/entity-category">
    <saml:AttributeValue>
      http://refeds.org/category/hide-from-discovery
    </saml:AttributeValue>
  </saml:Attribute>
</mdattr:EntityAttributes>
```

To assert the `hide-from-discovery` entity attribute in IdP metadata, a Site Administrator signs into the Federation Manager to make the updates. See the [Hide an identity provider from discovery](#) topic to learn how.

For More Information

Get help

Can't find what you are looking for?

[help Ask the community](#)

- https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPMetadataProvider