

configure-shib-sp

Jump to:

[Version requirement](#) | [Configuring Shibboleth SP v3](#) | [Configuring Shibboleth SP V2](#) | [Obtaining metadata signing key](#)

Version requirement

The per-entity metadata service works with both Shibboleth v2 and v3. There are some limitations:

- You will need at least Shibboleth SP v2.1 to specify a maximum Cache Duration.
- You will need at least Shibboleth SP v2.4 to specify a minimum cache duration.

Further, you should consider upgrading to Shibboleth SP V3 as soon as possible. Shibboleth v2 has already reached end of life. The service also works with other federating software that supports the protocol.

Configuring Shibboleth SP v3

This example configures a [Shibboleth SP](#) to use the InCommon Per-Entity Metadata Distribution Service for all entities. The SP will query the service when it needs metadata for a specific IdP. It will also cache the result.

Shibboleth SP v3 introduces a specific MDQ metadata provider which allows for slightly simpler configuration. We recommend that you enable a metadata cache duration of at least one hour, but no longer than one day, in your Shibboleth SP. In both examples, we set the minimum cache duration to one minute and the maximum cache duration to one day. A short minimum cache duration is recommended in order to prevent failed lookups from being cached for an extended period of time. Note that Shibboleth does not refresh at the minimum cache duration value, so it is okay to have a low minimum cache duration set.

Information on the Shibboleth SPv3 MDQ Metadata Provider is available [here](#).

```
<!-- InCommon Per-Entity Metadata Distribution Service -->
<MetadataProvider type="MDQ" id="incommon" ignoreTransport="
true" cacheDirectory="inc-mdq-cache"

    maxCacheDuration="86400" minCacheDuration="60"

    baseUrl="https://mdq.incommon.org/">

    <MetadataFilter type="Signature" certificate="inc-md-cert-
mdq.pem" />

    <MetadataFilter type="RequireValidUntil"
maxValidityInterval="1209600" />

</MetadataProvider>
```

Configuring with multiple metadata providers

If you have more than one metadata provider, you will want to put the InCommon Per-Entity Metadata Distribution Service **after** any statically configured metadata providers. If you do not do this, Shibboleth will try to fetch your static entities from InCommon each time it is requested before falling back to your static metadata providers.

Configuring Shibboleth SP V2

This example configures a Shibboleth v2 SP to use the InCommon Per-Entity Metadata Distribution Service for all entities. Information on the Shibboleth SPv2 Dynamic Metadata Provider is available [here](#).

```
<!-- InCommon Per-Entity Metadata Distribution Service -->
<MetadataProvider type="Dynamic" ignoreTransport="true"
maxCacheDuration="86400" minCacheDuration="60">

    <Subst>https://mdq.incommon.org/entities/$entityID<
/Subst>
```

Related content

- [Migrating to the MDQ Service](#)
- [Metadata Distribution Service Documentation](#)
- [Introducing per-entity metadata service](#)
- [Configure Shibboleth service provider](#)
- [Configure other software](#)
- [Prefetch an entity with Shibboleth](#)
- [Locating the production metadata](#)
- [Metadata signing key for the Production environment](#)
- [Metadata Service](#)
- [Configure Shibboleth identity provider](#)

Get help

Can't find what you are looking for?

[help](#) [Ask the community](#)

```
<MetadataFilter type="RequireValidUntil"
maxValidityInterval="1209600"/>

<MetadataFilter type="Signature" certificate="inc-md-
cert-mdq.pem"/>

</MetadataProvider>
```

Obtaining metadata signing key

Download and place the metadata signing key in the credentials folder of the SP and name it *inc-md-cert-mdq.pem*.

Available Keys

- [Metadata signing key for the Production environment](#)