configure-shib-idp-for-preview-mdq

This is documentation for the Preview MDQ environment

The information on this page is for the Preview environment of the MDQ Service. For production configuration instruction, see Configure Shibboleth identity provider.

Additional Note: The public key and its certificate for the *Preview environment* of the MDQ service may change with little notice. The production version of the public key and its certificate are long-lived and stable.

Versions 3.0 and higher of the Shibboleth IdP support the MDQ protocol. If you are not running Shibboleth IdP V3 or higher, or other software that supports the protocol., you should upgrade as soon as possible. Also note that the requiredSignedRoot property is new as of v3.2.0. Upgrading to the most recent version of the Shibboleth IdP and enabling this feature will protect your deployment against man in the middle attacks.

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.

Example IdP configuration

```
<!-- InCommon Per-Entity Metadata Distribution Service -->
<MetadataProvider id="incommon" xsi:type="DynamicHTTPMetadataProvider"
                  maxCacheDuration="PT24H" minCacheDuration="PT10M">
  <!-- Verify the signature on the root element (i.e., the
EntityDescriptor element) -->
  <MetadataFilter xsi:type="SignatureValidation" requireSignedRoot="true"
                  certificateFile="%{idp.home}/credentials/inc-md-cert-mdq.
pem" />

  <!-- Require a validUntil XML attribute no more than 14 days into the
future -->
  <MetadataFilter xsi:type="RequiredValidUntil" maxValidityInterval="P14D"
/>

  <!-- The MetadataQueryProtocol element specifies the base URL for the
query protocol -->
  <MetadataQueryProtocol>https://mdq-preview.incommon.org/<
/MetadataQueryProtocol>
</MetadataProvider>
```

In this example, we configured a one minute minimum cache duration and one day maximum cache duration, but we did not configure any timeouts. 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. The Shibboleth IdP documentation provides more information on all of the options available with the DynamicHTTPMetadataProvider.

It is strongly recommended that you enable a metadata cache duration of at least one hour, but no longer than one day, in your Shibboleth IdP.

You will need to get the new signing key certificate here: **Metadata signing key for the Preview environment**. In this case the certificate was downloaded and placed into the credentials folder of the IdP and named incommon-mdq.pem.

Related content

- Configure Shibboleth SP for the Preview MDQ environment
- Locating the preview metadata
- Configure Shibboleth IdP for Preview MDQ environment
- Prefetch an entity with Shibboleth in the Preview MDQ environment
- Introducing per-entity metadata service
- Metadata Distribution Service Documentation
- Prefetch an entity with Shibboleth
- Metadata signing key for the Production environment
- Configure other software
- Configure Shibboleth service provider

Get help

Can't find what you are looking for?

help Ask the community