

IdP Configuration

Shibboleth 2 Identity Provider Configuration

The Shibboleth 2 IdP uses the following configuration files to control various aspects of its operation:

- *attribute-filter.xml*. Configures the release of attributes to SP's.
- *attribute-resolver.xml*. Configures attribute collection, transformation, and encoding.
- *handler.xml*. Configures how the IdP receives and responds to various message types.
- *relying-party.xml*. Configures how the IdP processes messages that are received.
- *logging.xml*. Configuration of the IdP's logging system. You might want to use this to debug problems.
- *login.config*. Configuration for the [Username/Password authentication mechanism](#).
- *service.xml*. Configuration for coarse grained IdP components. Most people will never edit this.
- *internal.xml*. Low-level IdP configuration file. Most people will never edit this.
- *tc_config.xml*. Terracotta clustering configuration. Added in 2.1.

It also relies on configuration of the web environment for some features.

Basic Configuration Tasks

The following tasks are basic configuration operations performed by most deployers.

Communicate with a Service Provider	Describes how to communicate with a new Service Provider.
Configure Loaded Metadata	Describes how to read a new source of metadata information and how to apply filters to a source.
Customize User Authentication	Describes how to configuration the IdP's authentication mechanism.
Define a New Attribute	Describes how to read in and prepare a new attribute that may be released to a service provider.
Define a New Attribute Filter	Describes how to define a new attribute filter policy in order to control the release of a configured attribute.
Get the Status of the IdP	Describes how to use the IdP's status page.
Customize the IdP Logs	Describes how to customize the IdP's logging files and describes the format of the Audit and Access logs.
Determine IdP Version	Describes how to determine the IdP version number.
Renew IdP Certificate	Describes how to generate a new key/certificate pair for the IdP.

Intermediate Configuration Tasks

The following tasks are usually not necessary for many IdP deployments and are more complicated than the basic configuration tasks and as such should not be done without a good understanding of how the IdP operates.

Specialized Relying Party Configuration	Describes how to customize configurations on a per relying party basis.
Support a new Name Identifier	Describes how to add support for a new name identifier type either for the entire IdP or for a given service provider.
Define a New Cryptographic Credential	Describes how to read in new cryptographic credentials (e.g. private keys, certificates) and make them available for cryptographic operations.
Configure XML Signature & Encryption	Describes how to enable configure XML signing and encryption support.
Enable IdP Clustering Support	Describes how to configure multiple running instances of an IdP to share state.
Enable ECP	Describes how to enable the ECP profile handler included with the V2.3+ IdP.
Error Handling with Velocity	Describes how to use Velocity instead of JSP for error handling.

Advanced Configuration Tasks

The following tasks are rarely needed for an IdP deployment. They can be quite complicated and should not be attempted without an excellent understanding on how the operation operates. Mistakes in these configurations can leave the IdP inoperable or insecure.

Configure a new Trust Engine	Describes how to configure a new trust engine that may be used to validate signatures and client certificates.
--	--

Customize IdP Configuration Loading	Describes how to customize the manner in which the IdP loads its configuration information. This includes loading configuration from URLs, enabling configuration reloading, etc.
---	---

Deployer Contributed Tasks

The following tasks are descriptions contributed by IdP deployers. They are generally tasks that span multiple configuration locations (i.e. authentication and attribute management). The content of these documents are not watched as closely by the Shibboleth development team and may fall out of date as new releases are made. If this occurs please contact the development on the [user's mailing list](#)

Use Two or More LDAP Directories	Use multiple separate LDAP directories and user bases with a single IdP.
Active Directory Configuration Issues	Issues that arise when configuring the Identity Provider to communicate with an Active Directory server.