Installation

Before You Begin

Refer to the SystemRequirements page for details on supported software platforms.

If you use Java 8 (which you should), be aware that it relies on a blocking PRNG by default, and the IdP may be observed to start up very slowly if there is insufficient entropy available. There are various workarounds or ways to install better sources of entropy by altering jre/lib/security/java.security or using system properties, but they are platform-specific.

See the SecurityAndNetworking page for introductory help in understanding the use of network ports, keys, and certificates.

> *A nice cross-platform GUI for manipulating Java keystores, PKCS#12 files, viewing certificates, etc., is Keystore Explorer.*

Before you begin you should collect the following items and information:

- a TLS key/certificate that you'll use to secure your browser-facing HTTP(S) connection on port 443

Assuming you plan to use the IdP for SAML support (as opposed to CAS support for example), you will need:

- the entityID URL you want to use to name your IdP (the installer will suggest one from your hostname, but this may not be a good choice)
- the second- or third-level DNS subdomain to append to any "scoped" attributes, often the same as your organization's email domain
- a source of SAML Metadata for the service providers your IdP needs to support (this could come from a "federation" of organizations you've joined, directly from the SP owners, or created and maintained by hand)

If you don't have any SAML metadata to give the IdP, you won't have an easy time making it do anything useful without changing a lot of defaults, so please take the time and start by acquiring or creating that metadata **first** if you're just starting out. If you have nothing else to use, the SAMLtest.ID site can help you get started, but if you're using it longer than a couple of weeks, you should rethink what you're trying to accomplish.

The installation process will suggest or generate the following information for you:

- the IdP's entityID (which you can override as noted above)
- separate self-signed key/certificate pairs for:
    - message signing
    - securing web service connections, generally on port 8443
    - encryption of data by other systems for decryption by the IdP
- a secret key and key version file for securing cookies and other data produced by the IdP for its own use (this is a special Java keystore of type "JCEKS")
- some initial sample metadata describing the IdP for use by partner SPs, once it's reviewed and supplemented
- a default set of IdP configuration files based on this information

Windows Installation

A specially packaged installer is available for Microsoft Windows that ensures files will have the correct line endings and optionally provides automated support for the use of Jetty and configuration against Active Directory. See the WindowsInstallation topic for instructions.

Non-Windows Installation

As noted, the IdP is a standard Java web application based on the Servlet 3.0 specification and should run for the most part in any compatible servlet container, but official support is provided only for Jetty and Tomcat. Jetty is the strongly recommended option and is used by the primary team members in their production environments.

Containers for which we have specific installation guidance are shown in step 1 below, including some that we do not officially support. Material specific to any container is provided as a convenience, and is not a substitute for the container's own documentation.

1. Prepare your Servlet container. Linux deployers may want to take a look at IdPLinuxNonRoot, which documents one way of using privileged ports. Some containers, such as Jetty, include alternatives. The links below are to (imperfect) examples provided by the project or by deployers. The list below is **not** reflective of the specific containers and versions we support, which is explicitly and only available on the SystemRequirements page.
    - Jetty 9.2
    - Jetty 9.3
    - Jetty 9.4
    - Apache Tomcat 8.0
2. Download the latest Identity Provider software package (the zip file has Windows line endings, the tarball Unix line endings).
3. Unpack the archive you downloaded to a convenient location. It will not be needed after installation.
4. Change into the newly created distribution directory, *shibboleth-identityprovider-VERSION*
5. Run either **./bin/install.sh** (on non-Windows systems) or **.\bin\install.bat** (on Windows systems).
    - The installation directory you provide will be referred to as `idp.home` throughout this documentation.
6. Deploy the IdP WAR file, located in *idp.home/war/idp.war*. See the Servlet container preparation notes for examples on how to do this.

Controlling Generated Key Size 3.4

In V3.4 the default key size has been increased. This could fail because of restrictions imposed by version of Java and the JCE "jusrisdiction policy" in use governing cryptographic strength.

This can be fixed by installing the unlimited strength Unlimited Strength Jurisdiction Policy or by updating to a supported version of Java, all of which have begun defaulting to the unlimited policy.

If this is impossible (or if you want a different key size) you can specify the `idp.keysize` parameter on the command line during the install process:

Setting generated key size on non-Windows system

```
./bin/install.sh -Didp.keysize=2048
```

Setting generated key size on Windows systems

```
.\bin\install.bat -Didp.keysize=2048
```

A Quick Test

You can test that the IdP is properly installed and is at least running successfully in the container with the status command line utility (**idp.home/bin/status.sh** or **idp.home\bin\status.bat**).

If everything is working correctly, you should see output summarizing the environment and information about the IdP's state. This doesn't mean that you will be able to log into anything yet as you have not yet configured the IdP to use your organization's infrastructure, added metadata, etc.

Typical Next Steps

1. Review the top of the Configuration page to get some basic familiarity with the installation tree and how to use it.
2. Load SAML metadata for the service provider(s) with which you will interact.
3. Configure authentication.
4. Configure attribute resolution and attribute release policy.
5. Customize your login UI, error handling, etc.

Rebuilding the WAR file

To rebuild the WAR file, run the build command line utility (**idp.home/bin/build.sh** or **idp.home\bin\build.bat**) from the installation directory `idp.home`.