Shibboleth Service Provider (SP)

1. Introduction

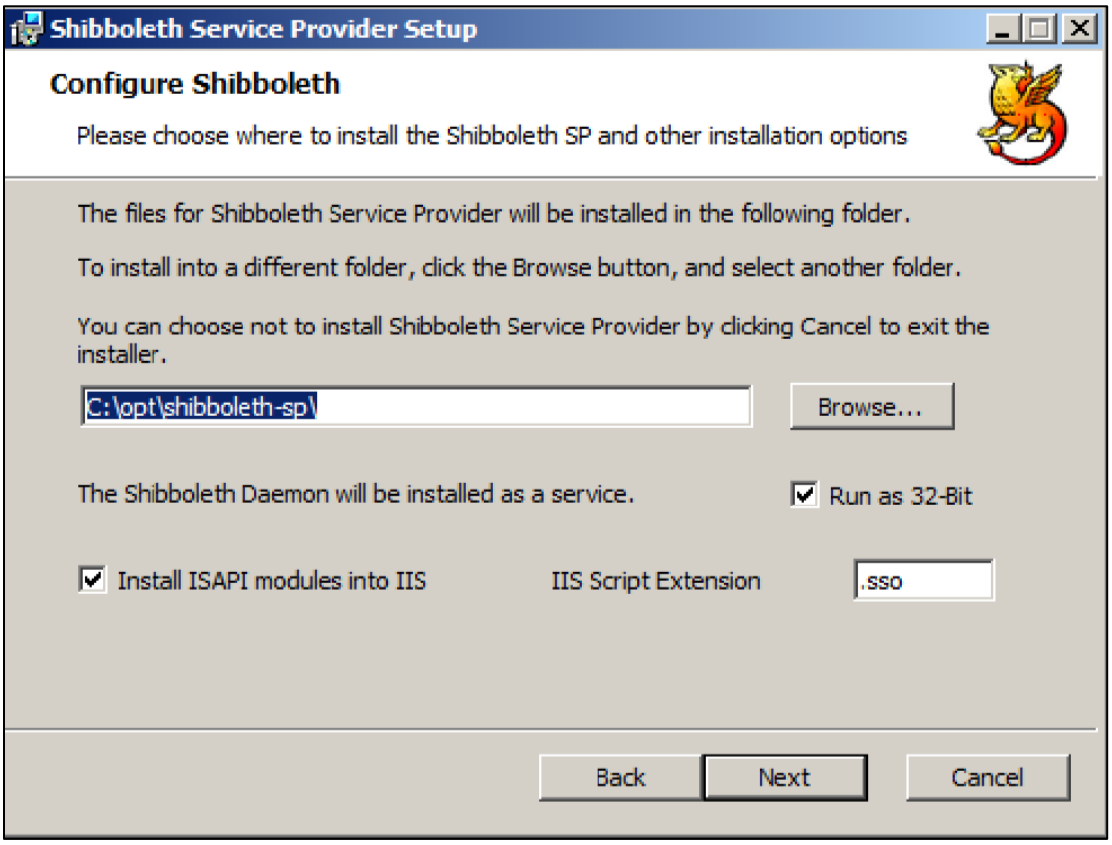
This guide describes the installation of a Shibboleth Service Provider (SP)

2. Download Windows Installer file

Download the Shibboleth Service Provider .msi file from the Shibboleth software repository. Chose the 64 bit version.

Run the installer

1. Confirm the dialog to run the software
2. Click "Next"
3. Accept the license agreement
4. The setup should look like on the screenshot below.



5. Install the Service Provider into the default location to C:\opt\shibboleth-sp

Click "Run as 32-Bit" as Shibboleth is used with a 32-bit application pool.

"Install ISAPI modules into IIS" should be checked. IIS Script Extension should be the default ".sso"

6. Click "Next", then "Install", then "Finish" 7. Click "Yes" to restart the system
7. Click "Yes" to restart the system

3. Verify Shibboleth Service settings

In order to check whether the installation was successful, open Administrative Tools > Services. The Shibboleth service (Shibboleth 2 Daemon) should have Status=Started, Startup Type=Automatic, Logon As=Local System

4. IIS settings

Open Internet Information Server (IIS) Manager

1. At **Web Server level**, select the ISAPI and CGI Restrictions tab.
2. Add a Shibboleth restriction entry from ccc\lib\shibboleth\isapi-shib.dll
3. At **Web Site level** open Properties, select the ISAPI Filters tab.
4. Add a Shibboleth filter entry from C:\opt\shibboleth-sp\lib\shibboleth\isapi-shib.dll

** Shibboleth will not do anything to protect the site unless this filter is in place. It is worth knowing this as removing the filters is a good way to force access in an emergency. With the filter removed the normal Elements login page will be displayed which will allow access to any locally authenticated user (e.g. the system account).*

5. Result

The Service Provider should now be installed on the system. Of particular interests are the directories:

C:\opt\shibboleth-sp\etc\shibboleth

Configuration directory of Shibboleth. The main configuration file is shibboleth2.xml.

C:\opt\shibboleth-sp\var\log\shibboleth

Log directory where logs are written to. The most important log file is the shibd.log file that should be consulted in case of problems.

6. Service Provider Configuration

Most of the native service provider's configuration options are found in shibb**oleth2.xml**, located in the SP's main configuration directory. This location varies by installation, but will commonly be **/etc/shibboleth/shibboleth2.xml** or **/opt/shibboleth-sp/etc/shibboleth/shibboleth2.xml**.

6.1 SP Configuration for a single Elements instance on one server

Edit in **shibboleth2.xml** file the following:

<InProcess> section

```
<InProcess logger="native.logger">
   <ISAPI normalizeRequest="true" safeHeaderNames="true">
      <Site id="1" name="sp.example.org" scheme="https" port="443"/>
  </ISAPI>
</InProcess>
```

- The 'name' is just a name that we'll reference in the <RequestMapper> section later
- The 'Site id' is the ID in IIS, Default website is usually 1, followed sequentially for each new site

<RequestMapper> section

```
<RequestMapper type="Native">
    <RequestMap>
        <Host name="sp.example.org" scheme="https" port="443" authType="shibboleth" requireSession="true">
            <Path name="login.html" authType="shibboleth" requireSession="true"/>
        </Host>
    </RequestMap>
</RequestMapper>
```

- Should contain something like the above, name is the same as the reference in the <InProcess> section
- This will trap all references to the login.html and redirect to the Shib server
- Without scheme="https" it's possible that Shibboleth will intercept the http request before Elements can flip it to http

<ApplicationDefaults> section

Application Defaults

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
                     REMOTE_USER="eppn persistent-id targeted-id">
```

- The entityID is an unique URL that describes the SP (most are just the main URL plus /shibboleth)

SSO

```
<SSO entityID="https://idp.example.org/idp/shibboleth"
     discoveryProtocol="SAMLDS"
     discoveryURL="https://ds.example.org/DS/WAYF" >
SAML2 SAML1
</SSO>
```

- The IdP location (URL)
- It is best practice, although not always required, that a full URL is added here

Metadata Provider

```
<MetadataProvider type="XML" file="idp-metadata.xml"/>
```

For the MetadataProvider please see 7.1 Metadata IdP

6.2 SP Configuration for 2 or more Elements instances on one server

https://wiki.cam.ac.uk/raven/Virtual_hosting_issues_with_Shibboleth

Keypair

Get a single Shibboleth instance working as you normally would, then:

1. Rename the key pairs created on install and update the Shib2.xml file to match this name change.
2. Run the keygen.bat utility from the Shibboleth folder C:\opt\shibboleth-sp\etc\shibboleth to create another keypair with the -h argument supplying the second virtual host's host name
3. Rename these for the second instance **example**: sp-key-prod.pem and sp-cert-prod.pem
4. Edit in **shibboleth2.xml** file the following:

<InProcess> section

```
<InProcess logger="native.logger">
    <ISAPI normalizeRequest="true" safeHeaderNames="true">
        <!-- prod -->
        <Site id="2" name="example-prod.symplectic.co.uk" scheme="https" port="443" />
        <!-- dev -->
        <Site id="3" name="example-dev.symplectic.co.uk" scheme="https" port="443" />
    </ISAPI>
</InProcess>
```

- Add another <Site> section to the <InProcess>section
- The 'name' are the names that we'll reference in the <RequestMapper> section
- The 'Site id' are the IDs in IIS, each Elements instance has its own id. Configure with the appropriate IIS site ID number

<RequestMapper> section

```
<RequestMapper type="Native">
    <RequestMap>
        <!-- prod -->
        <Host name="example-prod.symplectic.co.uk" scheme="https" port="443" authType="shibboleth" requireSession="true">
            <Path name="login.html" authType="shibboleth" requireSession="true"/>
        </Host>
        <!-- dev -->
        <Host name="example-dev.symplectic.co.uk" applicationId="dev" scheme="https" port="443" authType="shibboleth" requireSession="true">
            <Path name="login.html" authType="shibboleth" requireSession="true"/>
        </Host>
    </RequestMap>
</RequestMapper>
```

- Add another <Host>section in the <RequestMapper> section
- This second Host needs an extra attribute called "**applicationId**" adding with a string value

<ApplicationDefaults> section

Application Defaults

```
<ApplicationDefaults entityID="https://sp.example.org/shibboleth"
                     REMOTE_USER="eppn persistent-id targeted-id">
```

- The entityID is an unique URL that describes the SP (most are just the main URL plus /shibboleth)

SSO

```
<SSO entityID="https://idp.example.org/idp/shibboleth"
     discoveryProtocol="SAMLDS"
     discoveryURL="https://ds.example.org/DS/WAYF" >
SAML2 SAML1
</SSO>
```

- The IdP location (URL)
- It is best practice, although not always required, that a full URL is added here

Metadata Provider

```
<MetadataProvider type="XML" uri="https://edugate.heanet.ie/rr3/sigmedmetadata/provider/aHR0cHM6Ly91Y2QuZWxlbWVudHMuc3ltcGxlY3RpY5vcmc~/metadata.xml"
    backingFilePath="federation-metadata.xml" reloadInterval="7200">
   <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
   <MetadataFilter type="Signature" certificate="metadata-signer-2012.crt"/>
   <DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"
    attributeName="http://macedir.org/entity-category"
    attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    attributeValue="http://refeds.org/category/hide-from-discovery" />
</MetadataProvider>
```

ApplicationOverride

Add an ApplicationOverride section just before the end of the </ApplicationDefaults> section.

```
<ApplicationOverride id="dev" entityID="example-dev.symplectic.co.uk">
    <CredentialResolver type="File" key="sp-key-dev.pem" certificate="sp-cert-dev.pem" />
</ApplicationOverride>
```

- The id attribute in here, must match the **applicationId** attribute entered in the host section before.

7. Metadata

7.1 Metadata IdP

NOTE: Shibboleth uses SAML 2.0 Metadata

Locally stored

- Open the url to the IdP Metadata, save this file to the same folder as the Shibboleth2.xml file

Then reference this in the Shibboleth2.xml file:

```
<MetadataProvider type="XML" file="idp-metadata.xml"/>
```

<MetadataProvider type="XML" file="idp-metadata.xml"/>

Note that if you put the whole absolute path (c:\shib... etc.) it doesn't work.

Remotely configured

- This is usually for a fedorated system, InCommon, etc.
- You also need a link to a Certificate that is used to verify the online Metadata, this needs to be stored in the same folder as the Shibbolth2.xml file

```
<MetadataProvider type="XML" uri="https://edugate.heanet.ie/rr3/sigmedmetadata/provider/aHR0cHM6Ly91Y2QuZWxlbWVudHMuc3ltcGxlY3RpYy5vcmc~/metadata.xml"
    backingFilePath="federation-metadata.xml" reloadInterval="7200">
  <MetadataFilter type="RequireValidUntil" maxValidityInterval="2419200"/>
  <MetadataFilter type="Signature" certificate="metadata-signer-2012.crt"/>
  <DiscoveryFilter type="Blacklist" matcher="EntityAttributes" trimTags="true"
    attributeName="http://macedir.org/entity-category"
    attributeNameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
    attributeValue="http://refeds.org/category/hide-from-discovery" />
</MetadataProvider>
```

7.2 Metadata SP

This is an overview of how to create metadata **about** an SP, which you will **give** to an IdP.

The Metadata is a text file containing Entity IDs, Service URLs and an SSL Cert.

It's obtained by entering the following URL:

https://<base_url>/Shibboleth.sso/Metadata

If nothing loads, Shibboleth isn't protecting the URLs, check the filters, etc. in IIS.

NOTE: For 2 or more Elements instances on one server you need to generate a metadata file for each instance