UM Shibboleth Setup

FOR WINDOWS

CONTENTS

SET UP AND CONFIGURE A UM-PARTNER SHIBBOLETH SERVICE PROVIDER

This documentation will review the installation and configuration of a Shibboleth Service Provider against UM's Identity Provider. The Service Provider is usually configured on our Test Identity Provider first. Then, once Shibboleth Authentication has been successfully tested, your SP will be configured on our Production Identity Provider.

You can have your Service Provider communicating with other Identity Providers in addition of UM's. Please refer to Shibboleth Wiki for more information on this subject.

In addition of handling user authentication, Shibboleth also sends back sets of user attributes for your application to use. Please refer to the Configuration section of the documentation for more information.

PRE-REQUISITES

It is usually recommended to install Shibboleth Service Provider on the machine where runs the Web server front-ending the application you want to protect with Shibboleth.

In this documentation, we assume that you already have a fully functional web server in front of the application you want to Shibbolize.

This documentation will cover Apache 2.X and IIS 7 web servers' configuration.

Please also note that this documentation will use the default paths set during Shibboleth installation:

- For Windows: C:\opt\shibboleth-sp\

PRE INSTALLATION

Please note that depending on whether your system is a 32 or 64-bit system, files to install will differ.

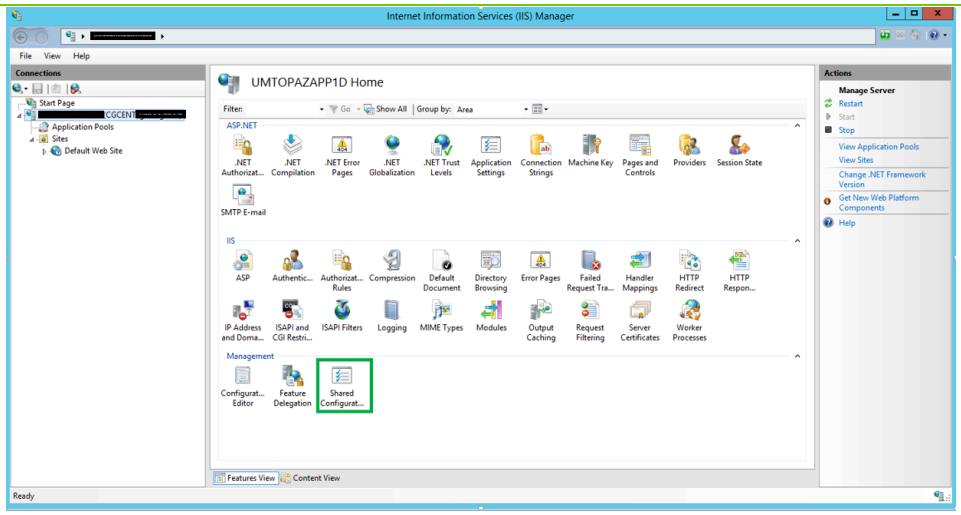
APACHE

Make sure that you have SSL enabled on your web server.

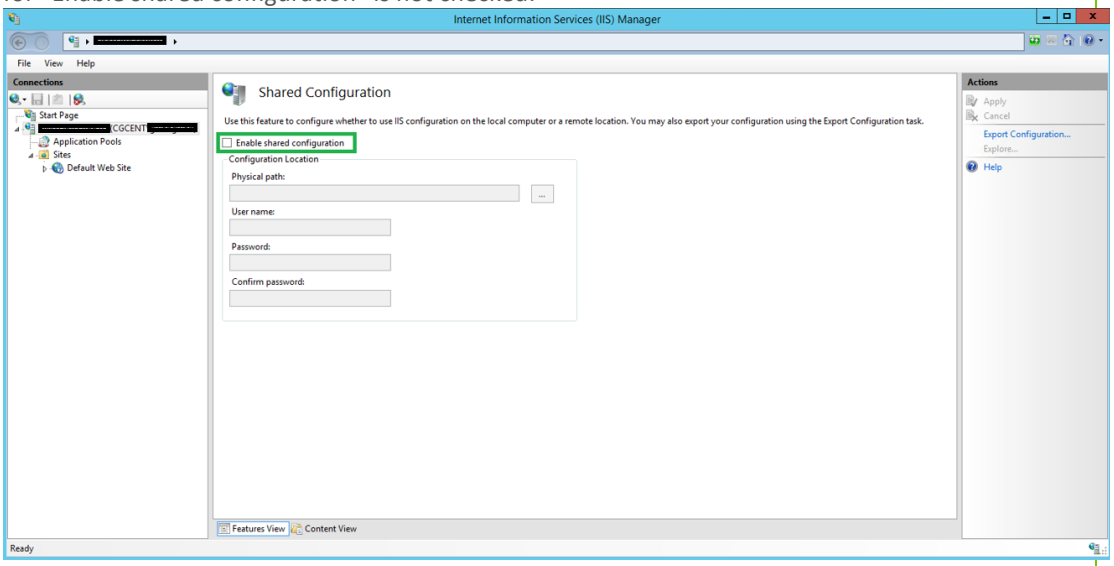
IIS

You will need to disable IIS "Shared Configuration" option for the Service provider installation.

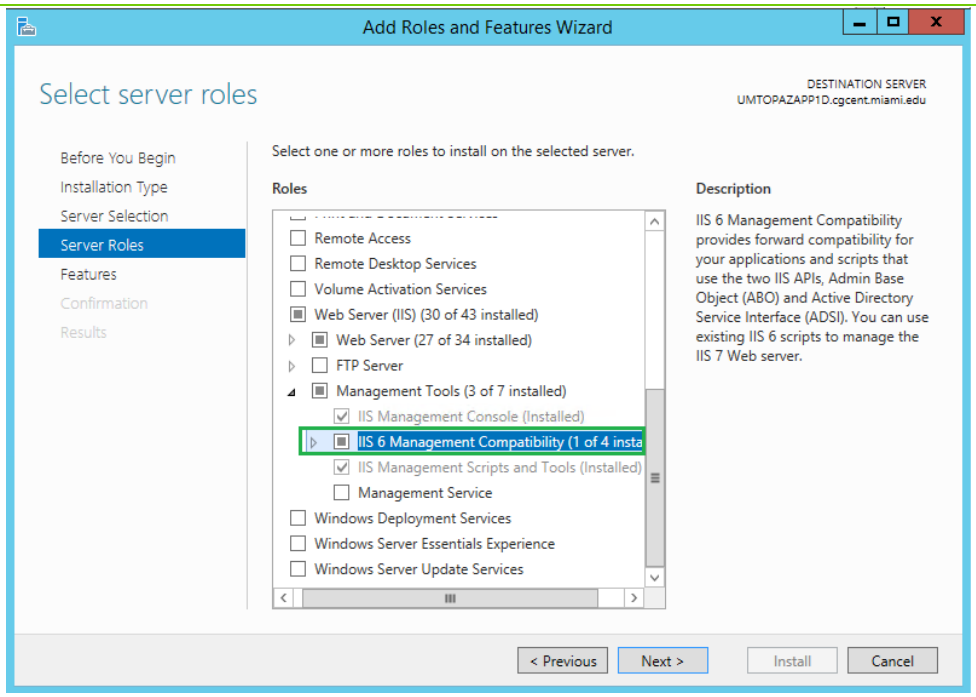
1. In IIS, click on the Server name (example, UMITSERVERPROD). On the center panel, under Management, you will find the "Shared Configuration" option:



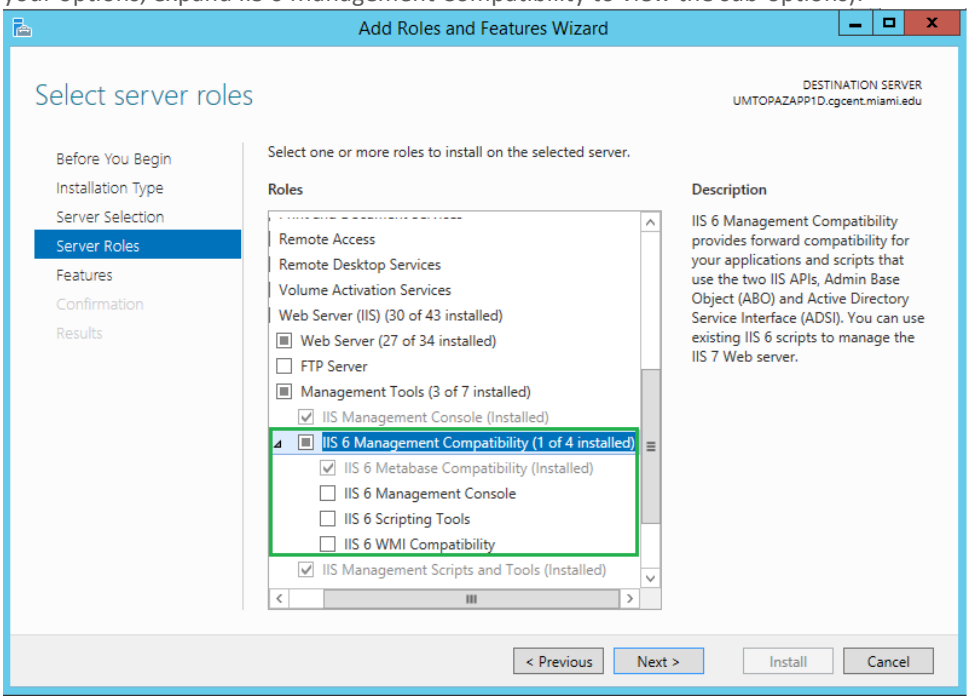
2. Double click on “Shared Configuration”, and on the resulting screen, and ensure that the checkbox for “Enable shared configuration” is not checked:



3. You may also need to install the IIS6 management compatibility role services and the ISAPI filters and extensions. If so:
    a. Under Windows Features, select “Server Roles” on the left
    b. Expand Web Server (IIS)
    c. Expand Management Tools
    d. Ensure that IIS Management Compatibility is checked:

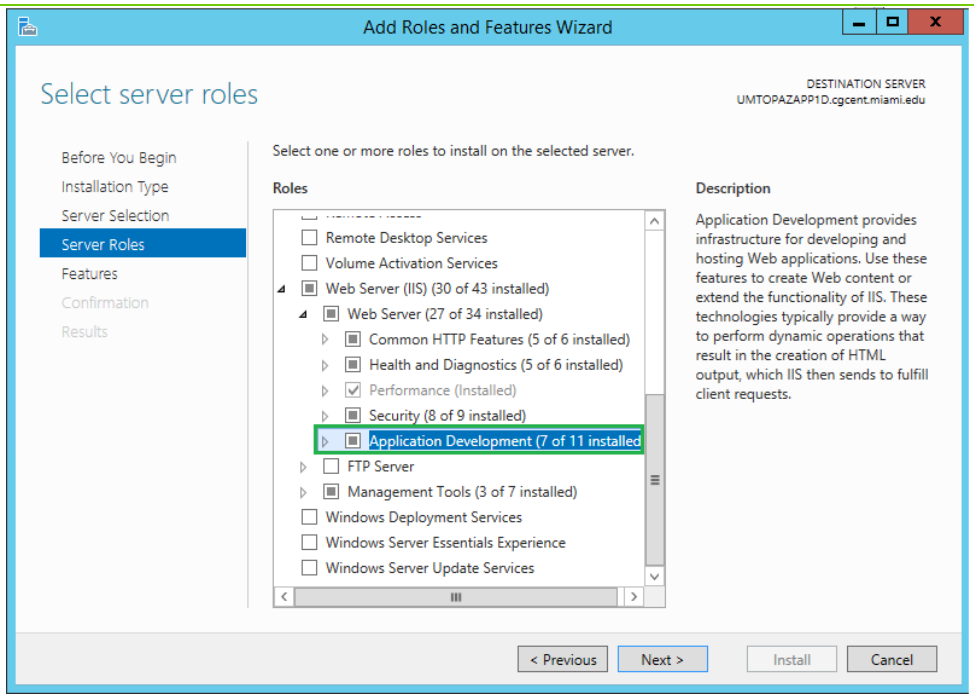


4. No other options under IIS 6 Management Compatibility needs to be checked (to double-check your options, expand IIS 6 Management Compatibility to view the sub-options):

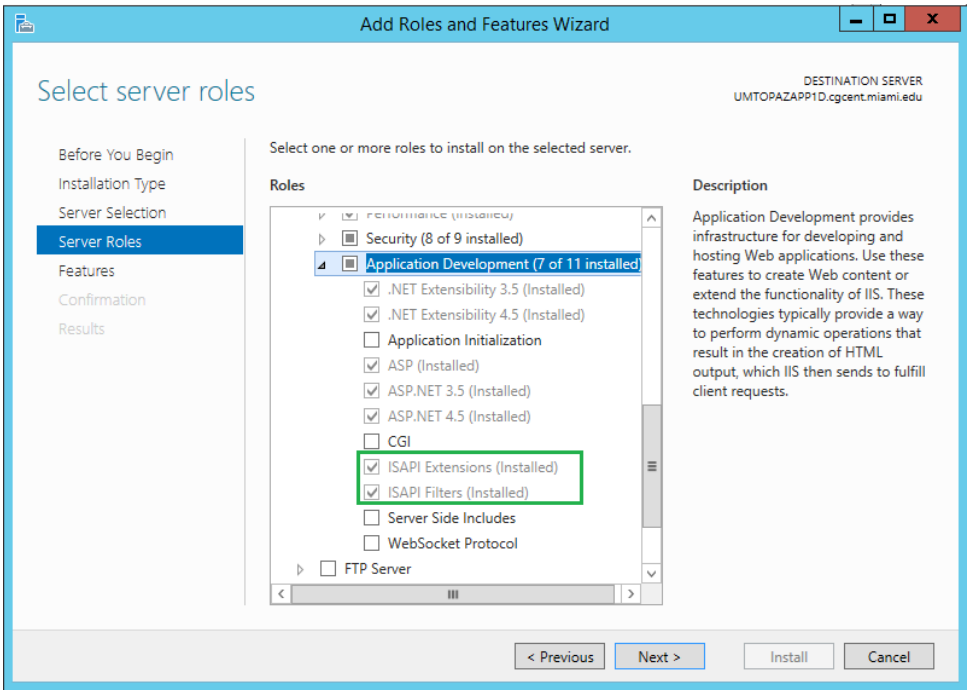


5. Under Windows Features, ensure that “Server Roles” on the left is still selected
6. Expand Web Server (IIS)

7. Expand Application Development:



8. Ensure that ISAPI Extensions and ISAPI Filters are selected:



9. If any changes were made, click on Next, and install the features.

Install the Shibboleth Service Provider

Windows

Download the appropriate .msi file (win32 or win64) from http://shibboleth.net/downloads/service-provider/latest/ and run the installer.

The installer can take care of basic IIS configuration for you, if you checked the option and installed IIS 6 compatibility services.

Post-install configuration

Apache

After the installation of Shibboleth Service Provider, there is some quick configuration that needs to be done on Apache.

- Add the content of /etc/shibboleth/apacheXX.xml (or C:\opt\shibboleth-sp\etc\shibboleth\apachexx.xml for Windows) file to your Apache's **httpd.conf** file.

  In **apacheXX.xml**, please pay attention to the **<Location /secure>** element: you must add the content of this element into the definition of your web application, in Apache configuration.

- In Apache **httpd.conf**, add the following: **UseCanonicalName On** and make sure that the **ServerName** directive is properly set.

- You'll also have to give read access to Apache to the whole installation directory as well as write access to the **/var/log** folder.

Then restart Apache and start shibd daemon: **/sbin/service shibd restart**

(or via Windows Service interface for Windows-based installations).

IIS

Add read access for the IIS user on the whole Shibboleth installation folder, except Shibboleth's private key file: **C:\opt\shibboleth-sp\etc\shibboleth\sp-key.pem**

And grant him write access to **C:\opt\shibboleth-sp\var\log\shibboleth\native.log**

If the basic configuration of IIS by the installer failed, follow the instructions at https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPWindowsIIS7Installer

The IIS user name can sometimes be found using "machine name\IIS_IUSRS", but differs depending on the installation.

To remove Read access for the IIS user, once inside the properties window for the file, you may have to click on the "Change permissions" button in the Advanced Security Settings for the sp-key.pem file. In this Dialog button, select the IIS user, click the "Disable inheritance" button, select the "Convert inherited permissions into explicit permissions on this object" option, and finally click on the "Remove" button to remove the access.

In order for IIS to be aware of which application requires Shibboleth authentication, you need to define a **RequestMapper** element in **C:\opt\shibboleth-sp\etc\shibboleth\shibboleth2.xml:**

- In the ISAPI filter part, change the Site id to the IIS site Identifier and the site name to site's host name
  To find out what is your site identifier, use IIS Manager Tool, select your application in the folder tree and look at the identifier column on the right.

- In the **RequestMapper** part, add a **Host** child element :

```
<RequestMapper type="Native">
    <RequestMap>
      <Host name="<Host name>" scheme="<http/https>">
            <Path name="<Site URL>" authType="shibboleth" requireSession="true"/>
      </Host>
    </RequestMap>
  </RequestMapper>
```

For example, fill in with the information that pertains to you, this is to protect with Shib the folder "secure" in "cwwwdev.miami.edu":

```
<RequestMapper type="Native">
    <RequestMap>
      <Host name="ummyserverapp1t.cgcent.miami.edu" scheme="https" >
        <Path name="secure" authType="shibboleth" requireSession="true"/>
      </Host>
    </RequestMap>
  </RequestMapper>
```

For more information on RequestMapper:
https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMapper
https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPRequestMap

Then restart IIS and start shibd (Shibboleth 2 Daemon) service via the Windows Service interface.

The shibboleth2.xml file might be found in C:\opt\shibboleth-sp\etc\shibboleth\ folder, if the C:\opt folder (default) was used during installation.

The host name needs to be fully qualified – example: ummyserverapp1t.cgcent.miami.edu

If there is an issue with restarting the Shibboleth service, try opening the Shibboleth2.xml file in XML Notepad. If the file cannot be opened, this application may pinpoint the location of the issue, if it's within the file.

CONFIGURE SP TO RECEIVE ATTRIBUTES FROM UM IDP

Shibboleth SP configuration files are located in:

- **C:\opt\shibboleth-sp\etc** for Windows

Edit **shibboleth2.xml**:

- In the **ApplicationDefaults** tag, set the **entityID** and the **homeURL** of your SP :

  <ApplicationDefaults entityID="https://<yourServerURL>/shibboleth-sp"
  homeURL="https://<yourServerURL>/index.html" REMOTE_USER="eppn">

The **homeURL** is a standard page to which a request is being redirected when there's nothing that can be done with it.

REMOTE_USER is the server variable used to pass the primary identifier of a user browser.

Examples of this tag:
<ApplicationDefaults entityID="https://ummyserverapp1t.cgcent.miami.edu/shibboleth-sp" REMOTE_USER="eppn">

<ApplicationDefaults entityID="https://ummyserverapp1t.cgcent.miami.edu/shibboleth-sp"
homeURL="https://ummyserverapp1t.cgcent.miami.edu/index.html" REMOTE_USER="eppn">

- Update the **Sessions, SSO** part of the file by setting the **entity ID of** UM Test IDP:

  <SSO entityID="https://cas.cgcent.miami.edu/idp/shibboleth">
  SAML2 SAML1
  </SSO>

- Uncomment the **MetadataProvider** and set the URI to the IDP's metadata URL.

  <MetadataProvider type="XML" uri="http://cas.cgcent.miami.edu/idp/profile/Metadata/SAML"
  backingFilePath="um-test-idp-metadata.xml" reloadInterval="180000">
  </MetadataProvider>

- You can also customize the various HTML error templates specified in the **<Errors>** element.

Edit **attribute-map.xml:**

The attributes the SP will gather are the ones specified in **attribute-map.xml**, all other attributes will be ignored. For an attribute to be decoded by the SP, add an entry in **attribute-map.xml.** Example with "eduPersonPrincipalName" attribute:

```
<Attribute name="urn:mace:dir:attribute-def:eduPersonPrincipalName" id="eppn">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>
<Attribute name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" id="eppn">
    <AttributeDecoder xsi:type="ScopedAttributeDecoder"/>
</Attribute>
```

We recommend uncommenting at least the OID and SAML2 definitions of the following attributes: targeted-id, persistent-id and eppn (or employeeNumber)

Please refer to the list of attributes released by UM IDP by default, to configure additional attributes.

TEST

Once the basic SP installation is complete, try accessing https://localhost/Shibboleth.sso/Status from your web server's machine.

Try logging in to your site/web application. You should be redirected to a SSO login screen, and once authenticated, to your web application.

Go to https://<your server URL>/Shibboleth.sso/Session to see the attributes being sent by Shibboleth.

Once we are up and running, go to https://<localhost>/Shibboleth.sso/Metadata and this should generate the metadata file to configure into our IdP.
Let us know when this step is done so the IdP can be configured based on this metadata file.

TROUBLESHOOT

Try to run shibd daemon from the command line with "**-check**" option

Or check the log files for errors.

LOGS

WINDOWS

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

MOVE TO OUR PRODUCTION IDP

Once Shibboleth Authentication has been successfully tested on Um Test IDP, you can migrate to the production Shibboleth.

Coordinate with the Shibboleth admins, so that they configure the production IDP to communicate with your Service provider. You'll need to provide your entity ID and your SP Metadata.

In your SP configuration, replace all references to **cas.cgcent.miami.edu** by **caneid.miami.edu**

And replace the IDP metadata file by the one you can get at
http://caneid.miami.edu/idp/profile/Metadata/SAML.

Then restart shibd daemon.

Perform a search on the shibboleth2.xml file to ensure that all entries with "cas.cgcent.miami" have been replaced.

To minimize any (future) confusion the backingFilePath value in the MetadataProvider tag can be updated from "um-test-idp-metadata.xml" to "um-idp-metadata.xml".

Completed tag:
<MetadataProvider type="XML"
Uri="http://caneid.miami.edu/idp/profile/Metadata/SAML"
BackingFilePath="um-idp-metadata.xml" reloadInterval="180000">
</MetadataProvider>

Create the um-idp=metadata.xml file in the opt\shibboleth-sp\etc\shibboleth folder, and copy the contents of the http://caneid.miami.edu/idp/profile/Metadata/SAML into the file.

In some IIS cases, restarting the shibd daemon service wasn't enough, and IIS also needed to be restarted as well, before everything worked as expected.

Follow test cases suggestions that will test login, access control if any, and SSO logout