# **Shibboleth Service Provider**

This guide will help in installing Shibboleth Service Provider on Windows machine and help it configure with Shibboleth Identity Provider. Also it helps is configuring a Web Application with Shibboleth Service Provider.

## Prerequisites

1. Requires Administrator rights
2. May Require Machine Restart

**To install and run Shibboleth SP, we need to install Apache Httpd Web server first.**

## Apache Httpd Configuration on Windows for Http

1. Download the Apache httpd-2.4.7-winXX.zip for windows from following locations:

64bit OS: http://www.apachelounge.com/download/win64/

32bit OS: http://www.apachelounge.com/download/win32/

1. Extract the zip file and note the extracted path of the containing Apache24 folder.

PATH\_ APACHE\_HTTPD\_HOME= E:/Development/httpd-2.4.7-win64/Apache24

1. Locate the httpd.conf file at the below path and replace the "C:\Apache24" path to the location which we refer as PATH\_ APACHE\_HTTPD\_HOME.

PATH\_ APACHE\_HTTPD\_HOME\conf\httpd.conf

The below lines in the httpd.conf file will be needed to be changed.

ServerRoot "E:/Development/httpd-2.4.7-win64/Apache24"

..

DocumentRoot "E:/Development/httpd-2.4.7-win64/Apache24/htdocs"

..

<Directory "E:/Development/httpd-2.4.7-win64/Apache24/htdocs">

..

ScriptAlias /cgi-bin/ "E:/Development/httpd-2.4.7-win64/Apache24/cgi-bin/"

..

<Directory "E:/Development/httpd-2.4.7-win64/Apache24/cgi-bin">

AllowOverride None

1. [Optional] Change the listen port and server name in httpd.conf file to the desired port number and the desired server name. Here we have configured the port as 9000 and the server name as M.Y.I.P. Make sure you change the port and server name in the whole file wherever it is referred.

The below lines in the httpd.conf files will be needed to be changed.

Listen 9000

..

ServerName M.Y.I.P:9000

1. Check if the installation is working fine by starting the htttpd.exe on command prompt

E:\Development\httpd-2.4.7-win64\Apache24\bin>httpd.exe

The process should be waiting and should not be terminated automatically.

If the process gets terminated, error logs can be checked from the below path and errors need to be resolved before proceeding further.

PATH\_ APACHE\_HTTPD\_HOME\logs\error.log

1. Check if the installation is working fine by hitting the URL in browser.

http://M.Y.I.P:9000/

1. Process can be safely terminated by pressing ^C on the prompt and we can go further.

## Apache Httpd Configuration on Windows for Https (SSL)

1. Locate the httpd-ssl.conf or httpd-sni.conf file at the below path and replace the "C:\Apache24" path to the location which we refer as PATH\_ APACHE\_HTTPD\_HOME.

PATH\_ APACHE\_HTTPD\_HOME\conf\extra\httpd-ssl.conf

The below lines in the httpd.conf file will be needed to be changed.

SSLSessionCache "shmcb:E:/Development/httpd-2.4.7-win64/Apache24/logs/ssl\_scache(512000)"

..

DocumentRoot "E:/Development/httpd-2.4.7-win64/Apache24/htdocs"

..

ErrorLog "E:/Development/httpd-2.4.7-win64/Apache24/logs/error.log"

TransferLog "E:/Development/httpd-2.4.7-win64/Apache24/logs/access.log"

..

<Directory "E:/Development/httpd-2.4.7-win64/Apache24/cgi-bin">

SSLOptions +StdEnvVars

</Directory>

..

CustomLog "E:/Development/httpd-2.4.7-win64/Apache24/logs/ssl\_request.log" \

"%t %h %{SSL\_PROTOCOL}x %{SSL\_CIPHER}x \"%r\" %b"

1. [Optional] Change the listen secure port and server name in httpd-ssl.conf file to the desired secure port number and the desired server name. Here we have configured the secure port as 9001 and the server name as M.Y.I.P. Make sure you change the secure port and server name in the whole file wherever it is referred.

The below lines in the httpd-ssl.conf files will be needed to be changed.

Listen 9001

..

<VirtualHost M.Y.I.P:9001>

..

ServerName M.Y.I.P:9001

1. Specify the Certificate and Certificate Key path in the httpd-ssl.conf. You can refer APPENDIX-A to configure the Certificate and Certificate Path.

The below lines in the httpd-ssl.conf files will be needed to be changed.

SSLCertificateFile "E:/Development/keystore/org\_name\_sp\_public.cer"

SSLCertificateKeyFile "E:/Development/keystore/org\_name\_sp\_private.key "

1. Enable the use of SSL configuration in the httpd.conf file.

The below lines in the httpd-ssl.conf files will be needed to be changed/uncommented.

LoadModule ssl\_module modules/mod\_ssl.so

..

Include conf/extra/httpd-ssl.conf

..

LoadModule proxy\_module modules/mod\_proxy.so

..

LoadModule proxy\_html\_module modules/mod\_proxy\_html.so

..

LoadModule proxy\_http\_module modules/mod\_proxy\_http.so

..

LoadModule xml2enc\_module modules/mod\_xml2enc.so

..

LoadModule headers\_module modules/mod\_headers.so

1. Check if the installation is working fine by starting the htttpd.exe on command prompt

E:\Development\httpd-2.4.7-win64\Apache24\bin>httpd.exe

The process should be waiting and should not be terminated automatically.

If the process gets terminated, error logs can be checked from the below path and errors need to be resolved before proceeding further.

PATH\_ APACHE\_HTTPD\_HOME\logs\error.log

1. Check if the installation is working fine by hitting the URL in browser.

https://M.Y.I.P:9001/

1. Process can be safely terminated by pressing ^C on the prompt and we can go further.

## Apache Httpd Configuration as a Service on Windows

1. Install Apache Httpd Service in Windows Services.msc. Note the process will get terminated regardless of success or failure.

E:\Development\httpd-2.4.7-win64\Apache24\bin>httpd.exe –k install

Error log can be checked from below to confirm.

PATH\_ APACHE\_HTTPD\_HOME\logs\error.log

1. To start the Apache Httpd Service. Note the process will get terminated regardless of success or failure.

E:\Development\httpd-2.4.7-win64\Apache24\bin>httpd.exe –k start

Error log can be checked from below to confirm.

PATH\_ APACHE\_HTTPD\_HOME\logs\error.log

1. Check if the installation is working fine by hitting the below URLs in browser.

http://M.Y.I.P:9000/

https://M.Y.I.P:9001/

1. To stop the Apache Httpd Service.

E:\Development\httpd-2.4.7-win64\Apache24\bin>httpd.exe –k stop

**Once the Apache web server is installed, perform following steps to configure Shibboleth SP.**

## Shibboleth SP Installation on Windows

1. Download the shibboleth-sp-2.5.2-winXX.msi for windows from following locations:

64bit OS: http://www.apachelounge.com/download/win64/

32bit OS: http://www.apachelounge.com/download/win32/

1. Install the setup to a specific location of your choice. Note the installed path of the shibboleth-sp folder.

PATH\_SHIBBOLETH\_SP\_HOME= E:\Development\Shibboleth\opt\shibboleth-sp

The installation will also add the service in Windows Services.msc.

1. Locate the apache24.config file at the below path and replace the "C:\opt\shibboleth-sp" path to the location which we refer as PATH\_SHIBBOLETH\_SP\_HOME.

PATH\_SHIBBOLETH\_SP\_HOME\etc\shibboleth\apache24.config

The below lines in the apache24.config file will be needed to be changed.

LoadModule mod\_shib E:/Development/Shibboleth/opt/shibboleth-sp/lib64/shibboleth/mod\_shib\_24.so

..

Alias /shibboleth-sp/main.css E:/Development/Shibboleth/opt/shibboleth-sp/doc/shibboleth/main.css

1. Update the apache24.config file elements as below

<Location /Shibboleth.sso>

AuthType None

Require all granted

ShibUseHeaders On

require valid-user

</Location>

..

<IfModule mod\_alias.c>

<Location /shibboleth-sp>

AuthType None

Require all granted

</Location>

Alias /shibboleth-sp/main.css E:/Development/Shibboleth/opt/shibboleth-sp/doc/shibboleth/main.css

</IfModule>

..

<Location /secure>

AuthType shibboleth

ShibRequestSetting requireSession 1

require valid-user

ShibUseHeaders On

</Location>

1. Locate the shibboleth2.xml file at the below path and change the host name and secure port corresponding to the one given in Apache Httpd.

PATH\_SHIBBOLETH\_SP\_HOME\etc\shibboleth\shibboleth2.xml

The below lines in the shibboleth2.xml file will be needed to be changed.

<Site id="1" name="M.Y.I.P:9001"/>

..

<Host name=" M.Y.I.P:9001">

..

<ApplicationDefaults entityID="https:// M.Y.I.P:9001/shibboleth"

..

<Sessions lifetime="28800" timeout="3600" relayState="ss:mem" exportLocation="https:// M.Y.I.P:9001/Shibboleth.sso/GetAssertion"

1. Specify the Certificate and Certificate Key path in shibboleth2.xml. These path will be same as configured in httpd-ssl.conf.

The below lines in the httpd-ssl.conf files will be needed to be changed.

<CredentialResolver type="File" key="E:/Development/keystore/org\_name\_sp\_private.key" certificate="E:/Development/keystore/org\_name\_sp\_public.cer"/>

1. Restart the Shibboleth and Apache24 services from Windows services.msc
2. Check if the installation is working fine by hitting the below URLs in browser.

http://M.Y.I.P:9000/Shibboleth.sso/Metadata

https://M.Y.I.P:9001/Shibboleth.sso/Metadata

This should ask to download the file. Save it as Org\_Name\_Sp\_Metadata.xml

Org\_Name\_Sp\_Metadata.xml

## IdP Configuration in Shibboleth SP

1. Get the Idp-Metadata.xml from your Identity Provider. Save this file in your Shibboleth location in a new folder IdP as below.

PATH\_SHIBBOLETH\_SP\_HOME \IdP\Org\_Name\_IdP\_Metadata.xml

1. Update the path of Org\_Name\_IdP\_Metadata.xml and the URL of your IdP mentioned in that file, in your Shibboleth2.xml file.

Following lines will have to be changed in Shibboleth2.xml file.

<SSO entityID="https://MY.IDP.I.P:7002/idp/shibboleth">

..

<SessionInitiator type="Chaining" Location="/Login" isDefault="true" id="Login" entityID="https://172.20.65.53:7002/idp/shibboleth" >

..

<MetadataProvider type="XML" file=" PATH\_SHIBBOLETH\_SP\_HOME \IdP\Org\_Name\_IdP\_Metadata.xml"/>

1. Restart the Shibboleth and Apache24 services from Windows services.msc

## Attribute Release Configuration in Shibboleth SP

1. Get the list of attributes from your Identity Provider which they will be sharing as a part of SAML response.

They will be as below:

<Attribute name="urn:oid:0.9.2342.19200300.100.1.1" id="username"></Attribute>

<Attribute name="urn:oid:0.9.2342.19200300.100.1.2" id="fname"></Attribute>

<Attribute name="urn:oid:0.9.2342.19200300.100.1.3" id="mname"></Attribute>

<Attribute name="urn:oid:0.9.2342.19200300.100.1.4" id="lname"></Attribute>

<Attribute name="urn:oid:0.9.2342.19200300.100.1.5" id="dob"></Attribute>

<Attribute name="urn:oid:0.9.2342.19200300.100.1.6" id="ucrn"></Attribute>

<Attribute name="urn:oid:0.9.2342.19200300.100.1.7" id="uprn"></Attribute>

1. Locate the attribute-map.xml file at the below path and add the above attributes inside its <Attributes></Attributes> section

PATH\_SHIBBOLETH\_SP\_HOME\etc\shibboleth\ attribute-map.xml

1. Restart the Shibboleth and Apache24 services from Windows services.msc

## Web Application Integration with Shibboleth SP

1. Locate the shibboleth2.xml file at the below path and provide the url of your Web Application, which should be accessible only after Single Sign On, as below:

PATH\_SHIBBOLETH\_SP\_HOME\etc\shibboleth\shibboleth2.xml

The below lines in the shibboleth2.xml file will be needed to be changed.

<ApplicationDefaults entityID="https://M.Y.I.P:9001/shibboleth" homeURL="https://MY.WEB.APP.IP:9001/samlAttrTest/samlAttrServlet"

1. Enable AJP port configuration in your shibboleth2.xml

<ApplicationDefaults entityID="https://M.Y.I.P:9001/shibboleth" homeURL="https://MY.WEB.APP.IP:9001/samlAttrTest/samlAttrServlet"

REMOTE\_USER="eppn username persistent-id targeted-id" attributePrefix="AJP\_">

1. Locate the apache24.config file at the below path and add your web application location as below under Shibboleth.sso location

PATH\_SHIBBOLETH\_SP\_HOME\etc\shibboleth\apache24.config

The below lines in the apache24.config file will be needed to be changed.

<Location /Shibboleth.sso>

AuthType None

Require all granted

ShibUseHeaders On

require valid-user

</Location>

<Location /samlAttrTest/samlAttrServlet>

AuthType shibboleth

ShibRequestSetting requireSession 1

ShibUseHeaders On

require valid-user

</Location>

1. Enable AJP port configuration in your Web Application Web Server.

If your Web Application is deployed on Apache Tomcat, you can configure AJP port in its server.xml file as below:

<Connector port="9009" protocol="AJP/1.3" redirectPort="9443" tomcatAuthentication="false" packetSize="65536"/>

Please note down the AJP port and the redirect HTTPS port and restart your Web Application Server.

1. Locate the httpd.conf file at the below path and replace the "C:\Apache24" path to the location which we refer as PATH\_ APACHE\_HTTPD\_HOME.

PATH\_ APACHE\_HTTPD\_HOME\conf\httpd.conf

The below lines in the httpd.conf file will be needed to be added/changed as per your Web Application Server AJP port and HTTPS port.

ProxyIOBufferSize 65536

SSLProxyEngine on

ProxyRequests on

ProxyPass /home https://MY.WEB.APP.IP:9443/samlAttrTest

ProxyPass /samlAttrTest ajp://MY.WEB.APP.IP:9009/samlAttrTest

ProxyPassReverse /home https:/ MY.WEB.APP.IP:9443/samlAttrTest

ProxyPassReverse /samlAttrTest ajp://MY.WEB.APP.IP:9009/samlAttrTest

1. The Attributes Released by IdP in Saml Response, can be fetched in your Web Application from AJP headers in Http Request as below:

final String authType = request.getHeader("AJP\_username");

System.out.println("authType");

final String fname = request.getHeader("AJP\_fname");

System.out.println("fname");

1. Download your SP-Medata.xml file and share it with your Identity Provider. Ask them to add your SP in their relying parties.

http://M.Y.I.P:9000/Shibboleth.sso/Metadata

https://M.Y.I.P:9001/Shibboleth.sso/Metadata

This should ask to download the file. Save it as Org\_Name\_Sp\_Metadata.xml and share this file.

Org\_Name\_Sp\_Metadata.xml

1. Restart the Shibboleth and Apache24 services from Windows services.msc

## APPENDIX-A: Key Store and Self Signed Certificate Generation

1. Generate a keystore for Shibboleth Service Provider. The below command will generate a keystore with a Public-Private Key Pair inside it with the alias CECDEMO.

E:\Development\keystore>keytool -genkeypair -alias CECDEMO -keystore CecDemo.keystore -ext san=ip:M.Y.I.P

Enter keystore password:

Re-enter new password:

What is your first and last name?

[Unknown]: CEC Demo

What is the name of your organizational unit?

[Unknown]: IS

What is the name of your organization?

[Unknown]: IS

What is the name of your City or Locality?

[Unknown]: EDB

What is the name of your State or Province?

[Unknown]: SL

What is the two-letter country code for this unit?

[Unknown]: SL

Is CN=CEC Demo, OU=IS, O=IS, L=EDB, ST=SL, C=SL correct?

[no]: y

Enter key password for <CECDEMO>

(RETURN if same as keystore password):

Re-enter new password:

1. Export the Public key corresponding to your Private key as below

E:\Development\keystore>keytool -exportcert -alias CECDEMO -keystore CecDemo.keystore -file CECDEMO.cer

Enter keystore password:

Certificate stored in file <CECDEMO.cer>

1. Generate the PKCS12 type keystore from the above keystore.

E:\Development\keystore>keytool -v -importkeystore -srckeystore CECDEMO.keystore -srcalias CECDEMO -destkeystore CECDEMO\_PKCS12.keystore -deststoretype PKCS12

Enter destination keystore password:

Re-enter new password:

Enter source keystore password:

[Storing CECDEMO\_PKCS12.keystore]

1. Print the PKCS12 public certificate from PKCS12 type keystore.

E:\Development\keystore>openssl pkcs12 -in CECDEMO\_PKCS12.keystore -nocerts -nodes

Enter Import Password:

MAC verified OK

Bag Attributes

friendlyName: cecdemo

localKeyID: \*CONTENT\_DELETED\*

Key Attributes: <No Attributes>

-----BEGIN PRIVATE KEY-----

\*CONTENT\_DELETED\*

-----END PRIVATE KEY-----

Save the content printed content in CECDEMO.key

1. Import your Public certificate in your Java Trust Store.

E:\Development\keystore>keytool -importcert -alias CECDEMO -keystore E:\Development\servers\jdk7\jre\lib\security\cacerts -file CECDEMO.cer

Enter keystore password:

Owner: CN=CEC Demo, OU=IS, O=IS, L=EDB, ST=SL, C=SL

Issuer: CN=CEC Demo, OU=IS, O=IS, L=EDB, ST=SL, C=SL

Serial number: \*CONTENT\_DELETED\*

Valid from: Thu Feb 06 22:51:29 GMT 2014 until: Wed May 07 23:51:29 BST 2014

Certificate fingerprints:

MD5: \*CONTENT\_DELETED\*

SHA1: \*CONTENT\_DELETED\*

SHA256: \*CONTENT\_DELETED\*

Signature algorithm name: SHA1withDSA

Version: 3

Extensions:

#1: ObjectId: 2.5.29.17 Criticality=false

SubjectAlternativeName [

IPAddress: M.Y.I.P

]

#2: ObjectId: 2.5.29.14 Criticality=false

SubjectKeyIdentifier [

KeyIdentifier [

\*CONTENT\_DELETED\*]

]

Trust this certificate? [no]: y

Certificate was added to keystore

E:\Development\keystore>

1. [OPTIONAL] If required you can export the Public key of your keystore in PEM format as below

keytool -exportcert -alias CECDEMO -keystore CECDEMO.keystore -rfc -file CECDEMO.pem