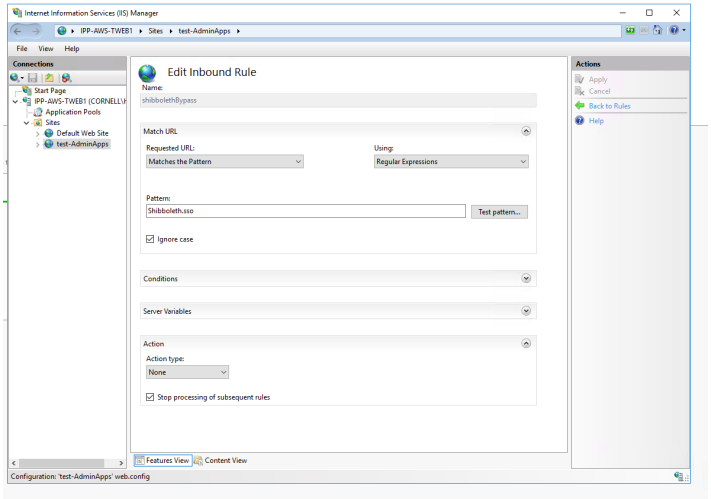
Install Shibboleth Service Provider(SP) 3.x on Windows and IIS

This document describes the procedure used to install Shibboleth Service Provider (SP) software on Windows Server and Internet Information Server (IIS), and to configure it to work with the Cornell Shibboleth Identity Provider (IdP).

Prerequisites

- Shibboleth Service Provider 3.x software supports Windows Server 2008 and later, and installers are available for both 32-bit and 64-bit systems. Shibboleth 3.x supports the versions of the IIS web server that are provided with the supported Windows versions.
- The IIS website must have an appropriate SSL certificate installed and SSL enabled. To request a SSL certificate: https://it.cornell.edu/ssl/renew-or-request-ssl-certificate
- If you have any **URL rewrite rules** defined in IIS, make sure those rules do not apply to Shibboleth.sso path. Or you can add this rule at the top of all the other rules that will stop redirecting any request for /Shibboleth.sso
- 

Installation

These links may break at some point, but for now the 32-bit and 64-bit run times can be found at:

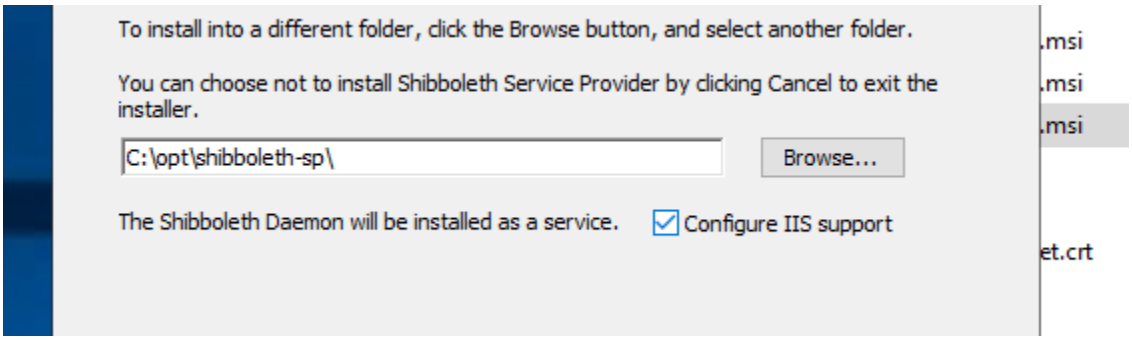
https://aka.ms/vs/15/release/VC_redist.x86.exe

https://aka.ms/vs/15/release/VC_redist.x64.exe

The top-level link to find them is https://visualstudio.microsoft.com/downloads/ via Other Tools
1 Download the latest version of the Windows installer package from the Shibboleth download site at https://shibboleth.net/downloads/service-provider/latest/. Select either the win32/ or win64/ directory as appropriate to your 32-bit or 64-bit system. Then download .msi file.

2 Run the installer package. It is recommended that you accept all defaults, as follows:

1. Accept the license agreement
2. Install to C:\opt\shibboleth-sp (this is the default location. You may change it to other location.)
3. **Make sure 'Configure IIS Support' checkbox is checked**



1. Click Next, then Install, then Finish
2. Click Yes to restart your system

On the *Administrative Tools* menu, click *Services*. Find *Shibboleth Daemon* in the list and double-click it. Verify that *Service Status* is "Running", *Startup type* is "Automatic", and on the *Log On* tab, verify that "Local System" is selected.

Configuration

Go to your SP installation directory(`C:\opt\shibboleth-sp` if you use the default) . All the SP configuration files are in the \etc\shibboleth directory.

Save a copy of attribute-map.xml to attribute-map.xml.orig or similar. Download our **sample attribute-map.xml** and replace your attribute-map.xml with downloaded file. Our attribute-map.xml defines all commonly used attributes.

All attributes except groups are released by default to all SP. Attribute "groups" is released on demand. Submit group membership requirement when you submit shibboleth integration request form. Find all the default attributes released by Cornell IDP from Shibboleth at Cornell Page. Edit attribute-map.xml as needed.
Save a copy of `shibboleth2.xml` to `shibboleth2.xml.orig` or similar. Download our **sample shibboleth2.xml** and replace your shibboleth2.xml with downloaded file. Open shibboleth2.xml in a text editor.

- Update the site ID and name:

  Find *<ISAPI...>...<Site id="1" name="shibtest.cit.cornell.edu"/>*. Change the "site id" to match the id assigned to your site by IIS. You can find your site id in Internet Services (IIS) Manager by clicking on "Sites". In this same location, change the site name to your website domain name. Our example defined two sites. Delete or add more as needed.

> **HTTP Header Variables**
>
> It is not safe to use HTTP header variables. Shibboleth SP 3 do not pass attributes as HTTP headers by default. If your applications look up attributes from HTTP headers, it is recommended switching to use server variables.
>
> If you have to use HTTP header variables, refer to https://wiki.shibboleth.net/confluence/display/SP3/ISAPI for instruction.

- Update the host name:

  Find *<RequestMap>...<Host name="shibtest.cit.cornell.edu">*. Change the "Host name" to the site name you defined in step above. In this example file, we defined two hosts and specifies different authorization rules for each site and location. Please modify it to meet your site requirement. If your site supports both http and https, add redirectToSSL="443" in Host element because shibboleth SP doesn't work with http connection.

> If you use group for authorization, please note group membership is not released by default. Please specify your group names in Shibboleth Integration Request form. Shibboleth IDP doesn't support nested groups(for example group B is a member of group A, user C is a member of group B, IDP doesn't know user C is a member of group A) . If you have to use nested group, you need to convert nested group to dynamic group.

Example: Entire website require authentication and allow valid-user

```
<Host name="xxx" authType="shibboleth" requireSession="true" redirectToSSL="443" />
```

Example: certain path require authentication and allow valid-user

```
<Host name="xxx"  redirectToSSL="443" />
        <Path name="special" authType="shibboleth" requireSession="true" />
</Host>
```

Example: different authorizaiton rules

```
<Host name="xxx"  redirectToSSL="443" />
     <!-- authorization by NetID -->
     <Path name="special" authType="shibboleth" requireSession="true">
              <AccessControl>
            <Rule require="uid">jy98 mop29</Rule>
         </AccessControl>
    </Path>
    <!-- authorization by group/permit -->
    <!-- Group Name is CASE SENSITIVE -->
    <Path name="students" authType="shibboleth" requireSession="true">
              <AccessControl>
            <Rule require="groups">cit.idm CIT-IDM-test</Rule>
         </AccessControl>
    </Path>
    <!-- authorization by user's affiliation.Possible value of affiliation: affiliate, alum, faculty, employee,
staff, student -->
    <Path name="students" authType="shibboleth" requireSession="true">
              <AccessControl>
            <Rule require="affiliations">employee student</Rule>
         </AccessControl>
    </Path>

</Host>
```

Example: sub level path has different authorization rule

```
<!-- /secure require certain netID. /special/doc require group cit.idm -->
<Path name="secure" authType="shibboleth" requireSession="true">
          <AccessControl>
        <Rule require="uid">jy98 mop29</Rule>
    </AccessControl>
    <Path name="doc">
        <AccessControl>
            <Rule require="groups">cit.idm</Rule>
        </AccessControl>
    </Path>
</Path>
```

Example: Force Everyone with TwoFactor

```
<Host name="xxxx" authType="shibboleth" authnContextClassRef="https://refeds.org/profile/mfa" requireSession="
true" >
    <AccessControl>
        <Rule require="authnContextClassRef">https://refeds.org/profile/mfa</Rule>
    </AccessControl>
</Host>
```

- Update SP entityID**:**

  Find <*ApplicationDefaults entityID="https://shibtest.cit.cornell.edu/shibboleth" ...*>. EntityID is the unique identifier for your SP. Cornell Shibboleth Identity Provider(IDP) provides service to many applications. This entityID will help Cornell IDP to identify your SP. We recommend you follow shibboleth convention named it "https://yourDomainName/shibboleth". It's better not include space or special characters in it(/ or : are fine).

  You can use one entityID for all your sites hosted in the same IIS.

- Update the support contact:

  Find < *Errors supportContact ="root@localhost" helpLocation ="/about.html" styleSheet ="/shibboleth-sp/main.css"* /> . Change the email address to your application's support email address.

- Update IDP info if you are configuring a test/dev site(skip this if you are configuring production site)

Find <*SSO entityID=" https://shibidp.cit.cornell.edu/idp/shibboleth "*>. Replace our production IDP's entityID with test IDP's entityID: https://shibidp-test.cit.cornell.edu/idp/shibboleth

Find <*MetadataProvider ... url=" https://shibidp.cit.cornell.edu/idp/shibboleth " ..*>. This is production IDP's metadata url. Comment out this block for your test site. Then un-comment MetadataProvider for Cornell test IDP.

- If your site also support Weill Cornell Medicine CWID login, follow instruction:https://confluence.cornell.edu/display/SHIBBOLETH/Login+with+Cornell+NetID+and+Weill+Cornell+CWID

Go to your SP installation directory(`default C:\opt\shibboleth-sp`), cd to /sbin64 or /sbin directory as appropriate to your 64-bit or 32-bit system. Running the code below from the command line:

```
shibd.exe -check
```

If the last line of the output is the following message, everything is as expected:

"overall configuration is loadable, check console for non-fatal problems"

If there is error, check log for detail. All the log files are in SP installation directory\var\log\shibboleth

Whenever you make changes to SP's configuration file, save the file. You can wait for the Shibboleth Daemon to pick up the changes or you can restart the Shibboleth Daemon to make the changes take effect right away. Some changes may require IIS restart.

Register Service Provider with Cornell IDP

- Restart IIS and the Shibboleth Daemon. The Shibboleth Daemon can be restarted using the *Administrative Tools* > *Services* navigation.
- Navigate to *https://yoursiteDomain/Shibboleth.sso/Metadata* and download it. Open your downloaded file with text editor. Make sure the entityID is the same as your defined in shibboleth2.xml. If there are multiple sites in IIS require Shibboleth authentication and you define them in shibboleth2.xml, you need to manually add consumer service url for each site in your SP's metadata.

Example

```
In our example, SP's metadata can be obtained from https://shibtest.cit.cornell.edu/Shibboleth.sso/Metadata. In
the metadata there should be a line:
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://shibtest.cit.cornell.edu/Shibboleth.sso/SAML2/POST" index="1"/>

Our example also have shibtest1.cit.cornell.edu defined in shibboleth2.xml, another AssertionConsumerService
url for shibtest1.cit.cornell.edu need to be manually added in the metadata:
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://shibtest1.cit.cornell.edu/Shibboleth.sso/SAML2/POST" index="2"/>
```

- Save your metadata file. You'll need to submit your SP's metadata in shibboleth integration request form.

Submit your shibboleth integration request from https://shibrequest.cit.cornell.edu. On the second page of request form, select 'No' for question "Has the application service provider's metadata been published with InCommon?". Use text editor open your SP's metadata, copy the content of the metadata and paste it in the "Service Provider's metadata field. Once the form is submitted, Identity Management get a Remedy case. We'll configure your SP in prod IDP in 1 - 2 business day. We'll notify you when the configuration is complete.

Test SP integration with IdP

Confirm that you are able to log in with your netID and user's attributes are properly released.

1. Using a web browser, visit the **/secure** directory (or other protected location) of your SP.
2. If you are prompted to log in, that means that your SP is properly integrated with Cornell IdP.
3. After you log in, open a new tab of the same browser and point your web browser to https://<your dns name>/Shibboleth.sso/Session. Your browser should return a status page that show you all the attributes and values released to your SP.

FAQ

"Looping" refers to a situation in which an attempt to login to the SP results in a rapid cycle of redirections between the IdP and the SP with a new session created every time around. Please follow the instructions from Shibboleth WIKI page to troubleshoot.
If possible snap shot your Windows server before you make any changes.

When integrating your website with Shibboleth, you will need to submit a Shibboleth integration request form. After IDM receive the request, your SP's metadata will be configured in Cornell Identity Provider(IDP). It may take as long as one business day for IDM to complete your request. Before your SP's metadata is loaded in IDP, shibboleth authentication won't work. To avoid the long down time of your production website, we recommend you make the transition in two steps and make the changes during maintenance hours.
1. Prepare your Windows server for Shibboleth authentication: Follow our instruction to install and configure shibboleth SP. After you get your SP's metadata, copy shibboleth2.xml to shibboleth2-good.xml. Then edit shibboleth2.xml, comment out all your Site define inside <ISAPI > block, save the file. Restart shibboleth daemon and IIS server. This change will disable shibboleth authentication for your site. Submit your shibboleth integration request form.

```
<ISAPI normalizeRequest="true" safeHeaderNames="true">

    <! – <Site id="1" name="shibtest1.cit.cornell.edu"/ > --><! – <Site id="2" name="shibtest2.cit.cornell.edu"/ >

</ISAPI>
```

2. After IDM load your SP's metadata in IDP, go back to your server. Copy shibboleth2-good.xml to shibboleth.xml, delete CUWebAuth config from IIS handler mapping. Restart shibboleth daemon and IIS.

By default, Shibboleth attributes that released to your shibboleth SP are available to your application as server variables, not available in HTTP headers. But not all the server/module expose custom server variables to application, for example .asp. It's dangerous using HTTP headers. If you have to get Shibboleth attributes from HTTP header, you could enable it by adding useHeaders="true" in <ISAPI tag>. In your application, you should always get authenticated user's netID from server variable REMOTE_USER.

Detail and examples about attribute access

https://wiki.shibboleth.net/confluence/display/SP3/AttributeAccess

SpoofChecking if using HTTP headers

https://wiki.shibboleth.net/confluence/display/SP3/SpoofChecking

Need Help?

contact idmgmt@cornell.edu