Shib4MOSS
Installation & configuration
Documentation

Author: Jean Marie THIA
Version: 1.0

Université Pierre et Marie CURIE
4 Place Jussieu
75252 Paris cedex 5
FRANCE

Step 1 – Install Shibboleth 2.x Service Provider (SP)

Shib4MOSS rely on Internet2 Shibboleth service provider for IIS. The first step is installing this component. This document will not go deeper in Shibboleth installation, but you can get an excellent help with this SWITCH document:

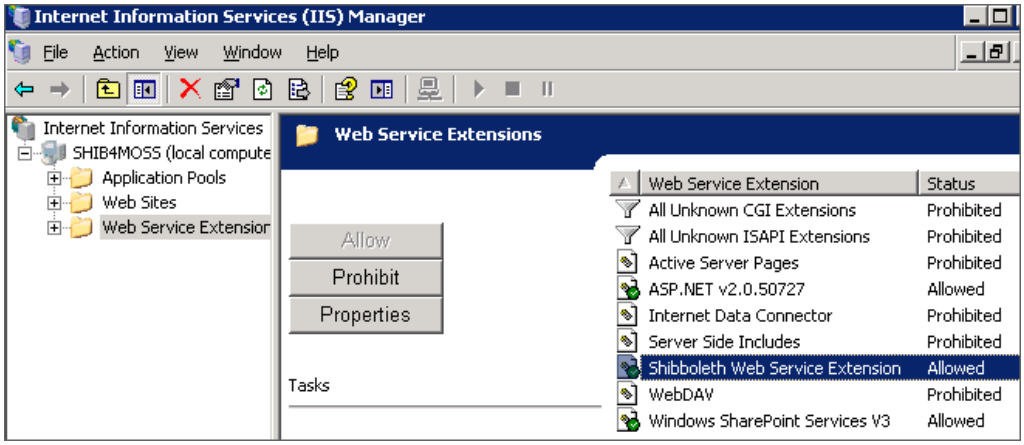
DEPLOYMENT OF SHIBBOLETH SERVICE PROVIDER (SP) 2.1 ON WINDOWS WITH IIS (https://www.switch.ch/aai/docs/shibboleth/SWITCH/2.1/sp/deployment/windows-iis.html).

And the provider installation file can be downloaded at:

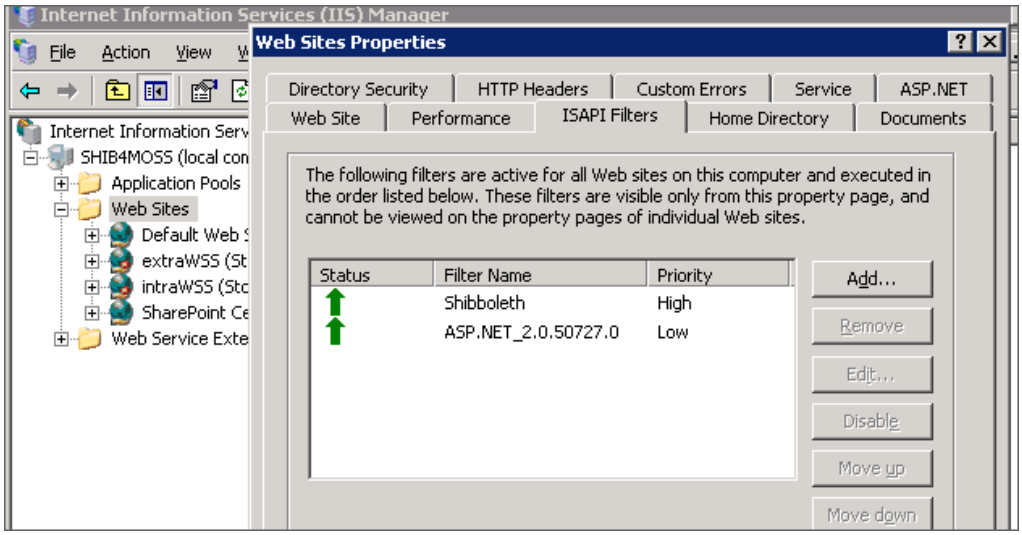
- http://shibboleth.internet2.edu/downloads/shibboleth/cppsp/latest/win32/shibboleth-sp-2.2-win32.msi,
- http://shibboleth.internet2.edu/downloads/shibboleth/cppsp/latest/win64/shibboleth-sp-2.2-win64.msi.

To check if the installation is fine, open the IIS manangement console:

- The ISAPI extension should be installed and allowed within the Web Service Extension.



- The ISAPi filter should be installed and up at the Web Sites level.



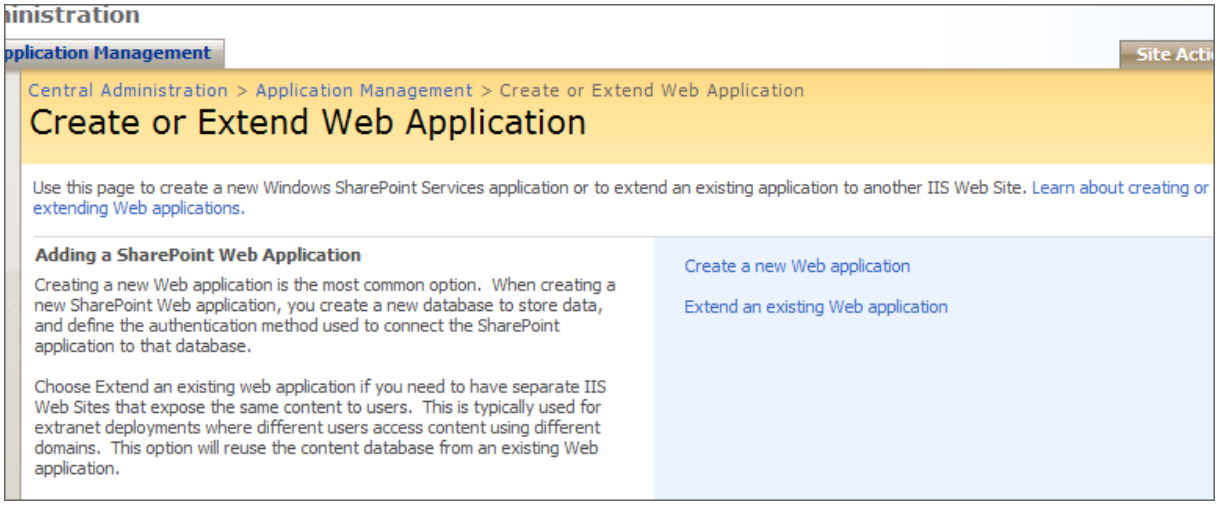
If any of these two point is not fine, reinstall the program and reboot the server.

Step 2 – Extend the web application

Sharepoint installation creates a default site which uses windows authentication. This site will be use to set authorization other sites. The extranet site has to be created by extending the web application.

1. In the application management page from the central administration site, follow select create or extend an existing web application

2. Click on extend an existing web application



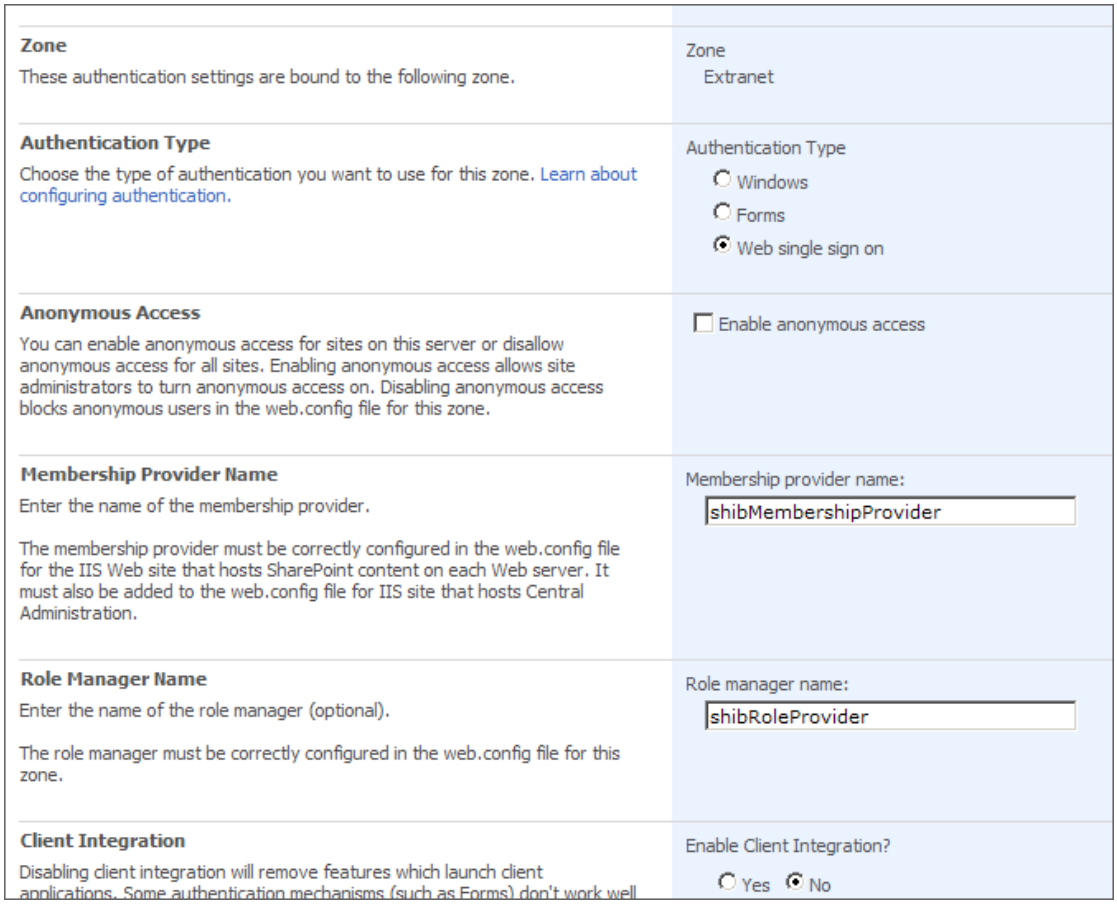
3. Fill in the fields as usual, except the zone that should be set to Extranet.

Step 3 – Configure Sharepoint

This step focuses on the configuration of the extranet zone for Web single sign on with Shibboleth identity federation through shib4MOSS.

Configure the extranet zone for web single sign on

1. Configure the authentication provider for the *Extranet* zone :



   a. On the application tab of the Sharepoint Central administration site, follow the authentication provider link.

   b. Within the list of zone mapped to the web application (both should be Windows), click on the *Windows* of the *Extranet* zone.

   c. In the *authentication type* section, select *web single sign on*.

   d. In the *membership provider* field, enter *ShibMembershipProvider*.

   e. In the *role provider* field, enter *ShibRoleProvider*.

   f. Make sure the *activate client integration* option is set to no.

2. Use a text editor to open the *web.config* file of the *Extranet* site and add the following entry in the *<configSections>*.

```
<!-- Registers the Umpc configuration section -->
<sectionGroup name="shibboleth">
   <section name="addOn"
            type="Umpc.Shibboleth.ShibConfigurationHandler,
                 Shib4MOSS, Version=1.0.0.0, Culture=neutral,
                 PublicKeyToken=F20DC168DFD54966"/>
   </sectionGroup>
</configSections>
```

3. Add the next entry at the end of the *<httpModules>* section.

```
  <!-- Registers the ShibAuthenticationModule in classic ASP.NET applications -->
  <add name="ShibAuthenticationModule"
       type="Umpc.Shibboleth.ShibAuthenticationModule, Shib4MOSS,
       Version=1.0.0.0, Culture=neutral, PublicKeyToken=F2ODC168DFD54966"/>
```

4. Add the following sections right after *<authentication mode>* in the *<system.web>*.

```
<!-- Validate the user with the ShibMembershipProvider membership provider -->
<membership defaultProvider="ShibMembershipProvider">
   <providers>
       <add name="ShibMembershipProvider"
            type="Umpc.Shibboleth.ShibMembershipProvider,
                 Shib4MOSS, Version=1.0.0.0, Culture=neutral,
                 PublicKeyToken=F2ODC168DFD54966"
            applicationName="/"/>
   </providers>
</membership>

<!-- Fetches roles for the user from the ShibRoleProvider role provider -->
<roleManager enabled="true" defaultProvider="ShibRoleProvider">
   <providers>
       <add name="ShibRoleProvider"
            type="Umpc.Shibboleth.ShibRoleProvider, Shib4MOSS,
                 Version=1.0.0.0, Culture=neutral, PublicKeyToken=F2ODC168DFD54966"
            applicationName="/"
            roleHttpHeaders ="<look at step 4: Configure shib4MOSS>"
            roleValues ="< look at step 4: Configure shib4MOSS >" />
   </providers>
</roleManager>

<!-- Logs web events from the Umpc.Shibboleth.ShibAuthenticationModule authentication module -->
<healthMonitoring enabled="true">
<!-- Event types the custom auth module exposes -->
   <eventMappings>
      <!-- authentication failure -->
      <add name="ShibAuthenticationFailureEvent"
           type="Umpc.Shibboleth.ShibAuthenticationFailureEvent,
                Shib4MOSS, Version=1.0.0.0, Culture=neutral,
                PublicKeyToken=F2ODC168DFD54966"/>
       <!-- authentication failure -->
       <add name="ShibAuthenticationSuccessEvent"
            type="Umpc.Shibboleth.ShibAuthenticationSuccessEvent,
                 Shib4MOSS, Version=1.0.0.0, Culture=neutral,
                 PublicKeyToken=F2ODC168DFD54966"/>
   </eventMappings>
   <rules>
      <!-- Forward all custom basic authentication events to the event log -->
      <add name="ShibAuthenticationFailureToEventLog"
           eventName="ShibAuthenticationFailureEvent"
           profile="Critical"
           provider="EventLogProvider" />
      <add name="ShibAuthenticationSuccessToEventLog"
           eventName="ShibAuthenticationSuccessEvent"
           profile="Critical"
           provider="EventLogProvider" />
     </rules>
   </healthMonitoring>
 <compilation debug="true" defaultLanguage="c#"/>
```

5. Add the following section after *<system.web>* section.

```
<shibboleth>
   <addOn enabled="true" audit="true" >
     <userAttribute header="Shib-InetOrgPerson-mail" />
     <roleAttributes headers="Shib-EP-PrimaryAffiliation|Shib-Application-ID|Shib-EP-UnscopedAffiliation"
                     valueSeparator=";"/>

   </addOn>
</shibboleth>
```

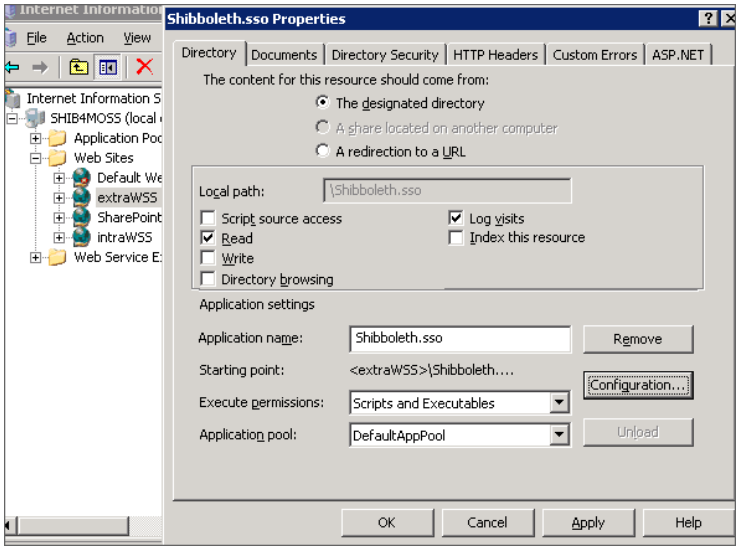
6. Add a new entry in *<securitypolicy>* section

```
    <trustLevel name="CustomTrust" policyFile="web_customtrust.config" />
```

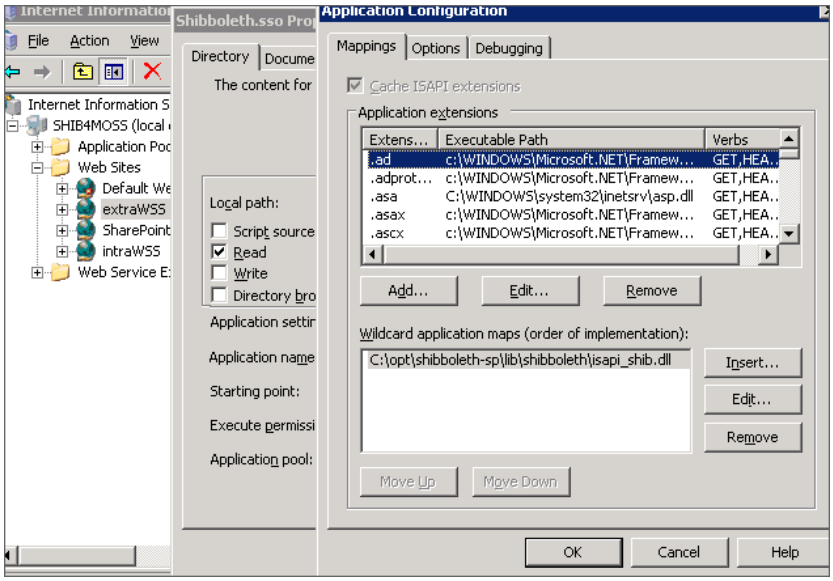
7. Change the trust level by modifying the *<trust>* by the following value.

```
    <trust level="CustomTrust" originUrl="" processRequestInApplicationTrust="true" />
```

8. Copy the *web_customtrust.config* in the root folder of the web site.
9. Copy the *shi4moss.dll* file in the *bin* directory of the web site.
10. Add an empty folder named *Shibboleth.sso* in the root folder of the site.
11. In IIS manager, select *Extranet* (in my case extraWSS) in the left panel. Right click on *Shibboleth.sso* folder and select properties in the context menu.



The folder should be change to an application in order to access the configuration button.



Now remove the wildcard mapping to asp.Net. Insert a new mapping by broswing to Shibboleth filter's dll. In the default installation of shibboleth, the ddl in located in: *C:\opt\shibboleth-sp\lib\shibboleth\isapi_shib.dll*.

> **Note :**
>
> *Wilcard mapping take precedence over the application extension. And we have to handle a Shibboleth.sso page request when the user gets back from the Shibboleth IDP. The trick is simply a real folder that is map to the Shibboleth extension. This thread* http://forums.iis.net/p/1157801/1904390.aspx#1904390 *on the IIS.Net forum gave the solution. The directory name should be change accordingly with the Shobboleth call back page.*

The Extranet web site is now configured for federated web Single Sign On. But the site is still not reachable as no permission has been set yet for the federated users. The next step is to configure the default site to be aware of the federated roles.

> **Important note :**
>
> *When selecting Web Sigle Sign On, anonymous authentication is autmatically set for the site in IIS.*

Set authorization on the Extranet site

In order to allow someone to access the *Extranet* site, rights should be set for the site by adding a shibboleth attribute value, for example: student, the visitor's group of the site. To do so, the *shibRoleProvider* provider has to be set for the default site.

1. Use your prefered text editor to open *web.config* file of the *Default* zone. This site is configured for NTLM authentication.
2. Add the following sections after the *<authentication mode>* section.

```
<membership>
    <providers>
        <add name="ShibMembershipProvider"
             type="Umpc.Shibboleth.ShibMembershipProvider,
                  Shib4MOSS, Version=1.0.0.0, Culture=neutral,
                  PublicKeyToken=F20DC168DFD54966"
             applicationName="/"/>

 </membership>

 <!-- Fetches roles for the user from the ShibRoleProvider role provider -->
 <roleManager enabled="true" defaultProvider="AspNetWindowsTokenRoleProvider">
   <providers>
     <remove name="AspNetSqlRoleProvider" />
     <add name="ShibRoleProvider"
          Type="Upmc.Shibboleth.ShibRoleProvider, Shib4MOSS,
               Version=1.0.0.0, Culture=neutral, PublicKeyToken=F20DC168DFD54966"
          applicationName="/"
          roleHttpHeaders ="<A définir,Cf. section Configurer l'extension Web SSO fédéré Shibboleth>"
          roleValues ="<A définir,Cf. section Configurer l'extension Web SSO fédéré Shibboleth>" />
   </providers>
 </roleManager>
```

3. Add this entry the *<securitypolicy>* section.

```
<trustLevel name="CustomTrust" policyFile="web_customtrust.config" />
```

4. Change the trust level by changing *<trust> key* by the following.

```
<trust level="CustomTrust" originUrl="" />
```

5. Copy *web_customtrust.config* in the root directory of the *default* web site.
6. Copy *shi4moss.dll* file in the *bin* directory of the default web site.
7. Open your browser, navigate to default web site and log in as the site's administrator.
8. Click on *site's actions* to open the menu, select *site parameters* and finally click click on *Persons and groups*.
9. Click on *Add* and then click on *Add users*. Add one of the roles values that have been declared in the web.config file. The possible values of this section are explained in *step 4: configure shib4MOSS*.
10. Set the permission as needed.

11. Click on *OK*.

The extranet site is now configure for shibboleth identity federation and only persons with the right attribute value can access the site.

But the one more step, the *shibboleth2.xml* file has to be modified to allow the shibboleth filtering on the *Extranet* site.

> **Note :**
>
> *The central admnistration site can be configured the same way to set permission based on shibboleth attribtes. But it is not a good pattern.*

Step 4 - Configure Shib4MOSS

This part describes the attributes use and value that should be set in the *web.config* file of the Sharepoint site.

Configure the http module

The http module is the piece of code that transforms the shibboleth identity in a .Net standard identity object. The module should know where to get the user's id and where to get the user's roles.

The http module uses his own configuration section as shown below:

```
<shibboleth>
  <addOn enabled="true" audit="true">
    <userAttribute header="uid"/>
    <roleAttributes headers="Shib-EP-PrimaryAffiliation|Shib-Application-ID|Shib-EP-UnscopedAffiliation"
                    valueSeparator=";"/>
  </addOn>
</shibboleth>
```

addOn attributes are:

Attribute	Description
enabled	Optional. Tells if shib4MOSS http module is enabled. The default value is: *false*.
audit	Optional. Tell shib4MOSS http module should log authentication events. The default value is *false*.

addOn child elements are :

Element	Description
userAttribute	Tells which Shibboleth header attribute to use for the user id.
roleAttributes	Tell which Shibboleth header attribute to use as role value container.

userAttribute comes with this mandatory attribute:

Attribute	Description
header	Defines the Shibboleth header attribute that contains the user id. Only **one** value is allowed. The default value is: *Shib-InetOrgPerson-mail*.

roleAttributes have the following mandatory attributes :

Attributs	Description
headers	Defines the Shibboleth headers that should be use to harvest the user's roles transferred by the IDP. The value separator is the | character. The attribute should have at least **one** value.
valueSeparator	Defines the separator value within each header.

Configure the membership provider

The membership provider is mandatory when enabling Web single sign on in Sharepoint. Shib4Moss comes with *ShibMembershipProvider* witch in fact does not do anything.

In a federated scenario it is, it should, be impossible for the service provider to interact with the identity provider.

Configure the role provider

The configuration of the ShibRoleProvider is done in the declaration of the provider in the *<roleManager>* section.

```
  <roleManager defaultProvider="ShibRoleProvider" enabled="true" cacheRolesInCookie="true">
    <providers>
      <add name="ShibRoleProvider"
           type="Upmc.Shibboleth.ShibRoleProvider, Shib4MOSS, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=F20DC168DFD54966"
           applicationName="/"
           roleHttpHeaders="primary-affiliation|unscoped-affiliation|supannRoleGenerique"
           roleValues="member|student|affiliate|etudiant"/>
    </providers>
  </roleManager>
```

All the attributes are mandatory and their use is:

attribute	Description
roleHttpHeaders	Mandatory. Defines the http headers that will be use to create the user role. The same as the headers of the http module. The values must be separated by the PIPE character. Ex. : *primary-affiliation|unscoped-affiliation|supannRoleGenerique*
roleValues	Mandatory. Defines the roles that will use by Sharepoint's people picker. These values are the groups that Sharepoint will use. They should be found in one of the http header used as role container. Ex. : *member|student|affiliate|etudiant*

Step 5 – Configure Shibboleth

The shibboleth filter needs to know the sites that it should filters; to do this you should customize the Shibbileth2.conf. The <site> element should contain the IIS id number of site and is name. In the example below, the name of my extranet site is devwss.dmz.net

```
<InProcess logger="native.logger">
    <ISAPI normalizeRequest="true">
        <!--
        Maps IIS Instance ID values to the host scheme/name/port/sslport. The name is
        required so that the proper <Host> in the request map above is found without
        having to cover every possible DNS/IP combination the user might enter.
        The port and scheme can usually be omitted, so the HTTP request's port and
        scheme will be used.
         <Site id="308250845" name="devwss.dmz.net"/>
         <Site id="1" name="devwss.dmz.net"/>
        -->

        <Site id="5396735" name="devwss.dmz.net"/>
    </ISAPI>
</InProcess>
```

The IIS site id can be found in the IIS management console when the web server is selected.