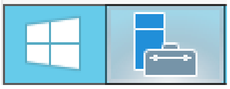
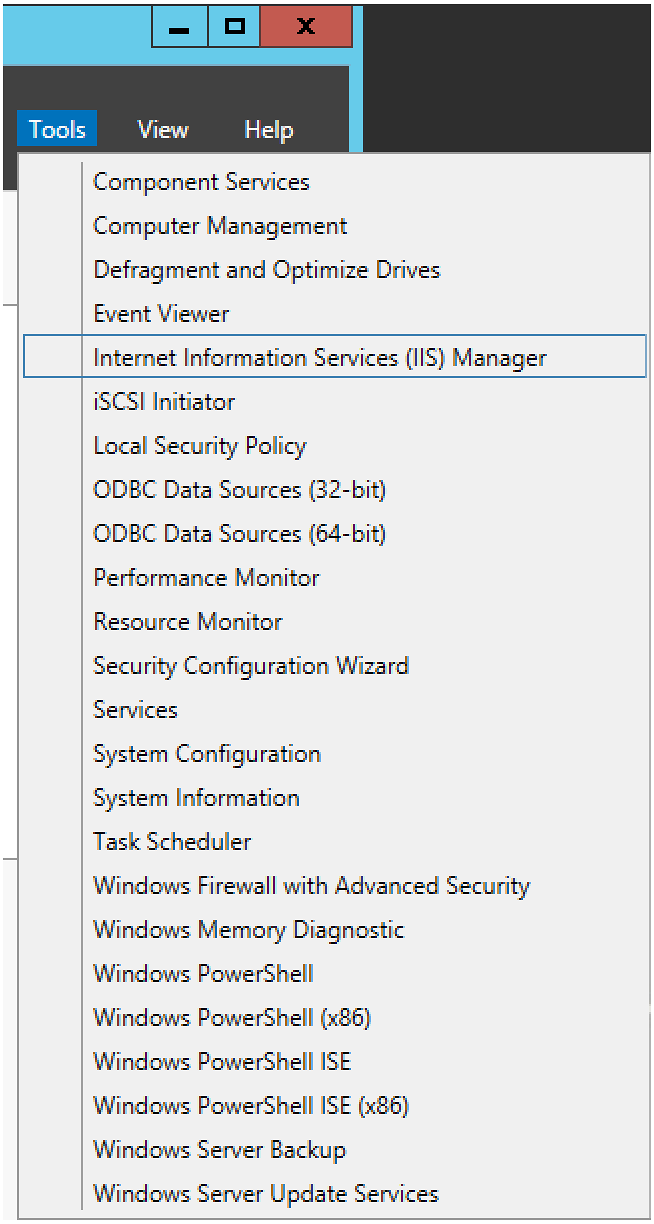
# Jack Stromberg

A site about stuff

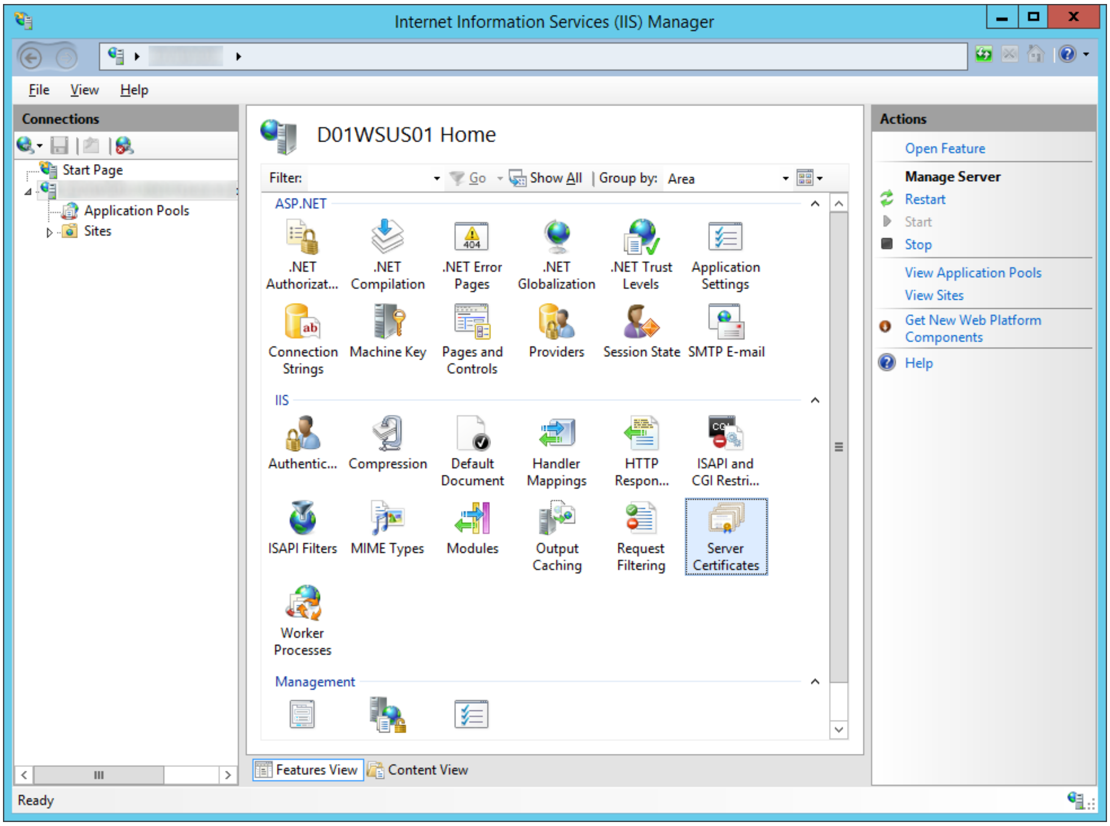
## Enabling SSL on Windows Server Update Services (WSUS)

Here are the steps to configure SSL on your servers running the Windows Server Update Services.  This guide was written using Server 2012 R2, however it should be the same steps for Windows Server 2008 R2 as well.  This guide also assumes you have a working instance of WSUS installed and configured, using default ports.

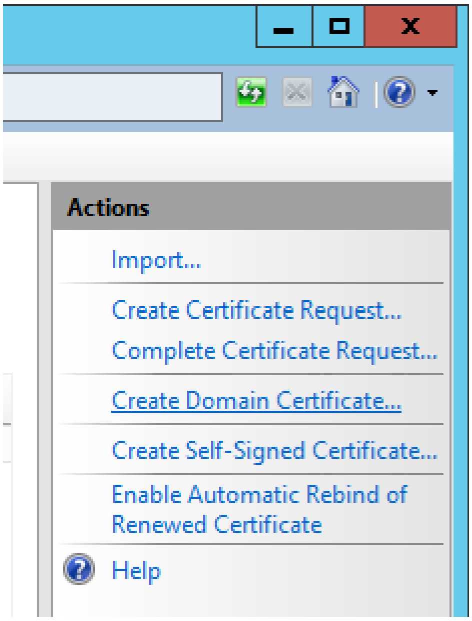
1. Login to your WSUS server
2. Open up **Server Manager**

3. Select **Tools** -> **Internet Information Services (IIS) Manager**



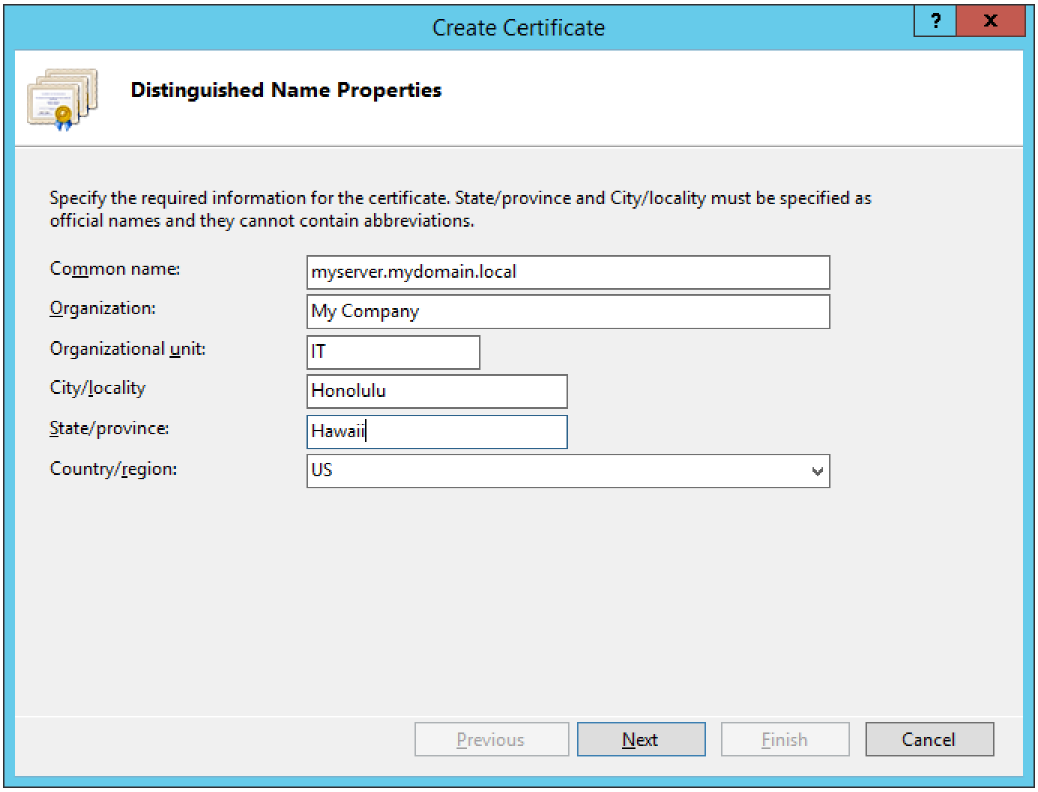
4. Generate a SSL certificate
    1. Click on your Server and select **Server Certificates**



2. If you have your own PKI environment, follow these steps, if not, jump to step three
    1. Click **Create Domain Certificate** on the right side


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

    2. Fill in the requested information on the Distinguished Name Properties page and click **Next**

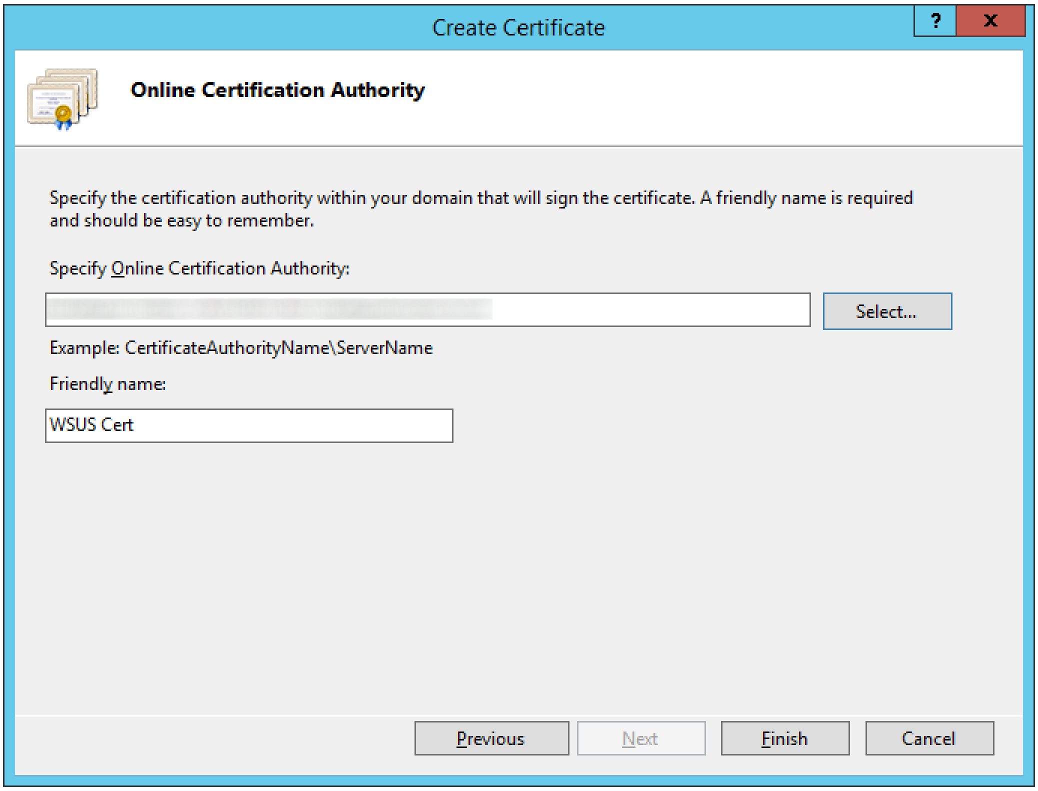


Distinguished Name Properties

Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: myserver.mydomain.local
Organization: My Company
Organizational unit: IT
City/locality Honolulu
State/province: Hawaii
Country/region: US

3. Select your certificate authority and enter a friendly name (this can be anything), and then click **Finish**

4. 

Online Certification Authority

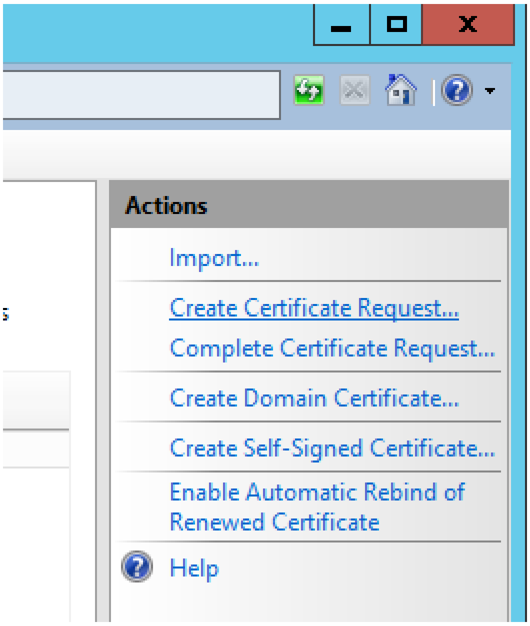
Specify the certification authority within your domain that will sign the certificate. A friendly name is required and should be easy to remember.

Specify Online Certification Authority: [redacted]

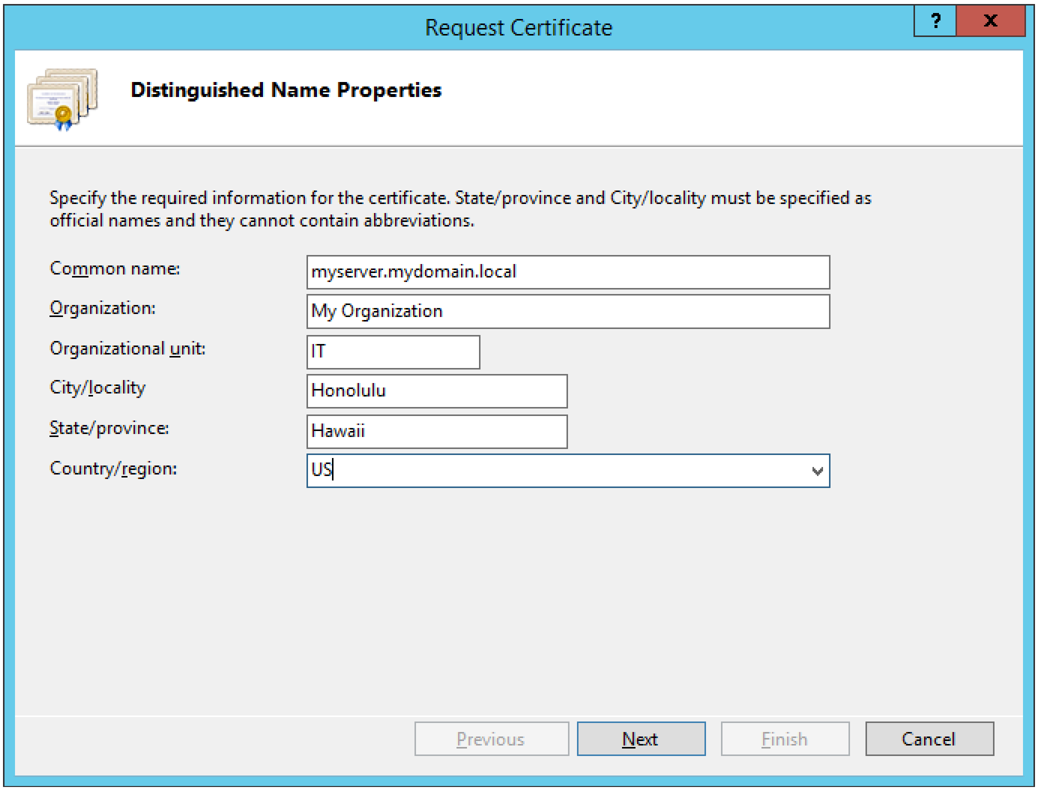
Example: CertificateAuthorityName\ServerName

Friendly name: WSUS Cert

3. If you need to submit a certificate request to an external certificate authority like Goaddy, Verisgn, Comodo; follow these steps
    1. Click **Create Certificate Request** on the right side


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

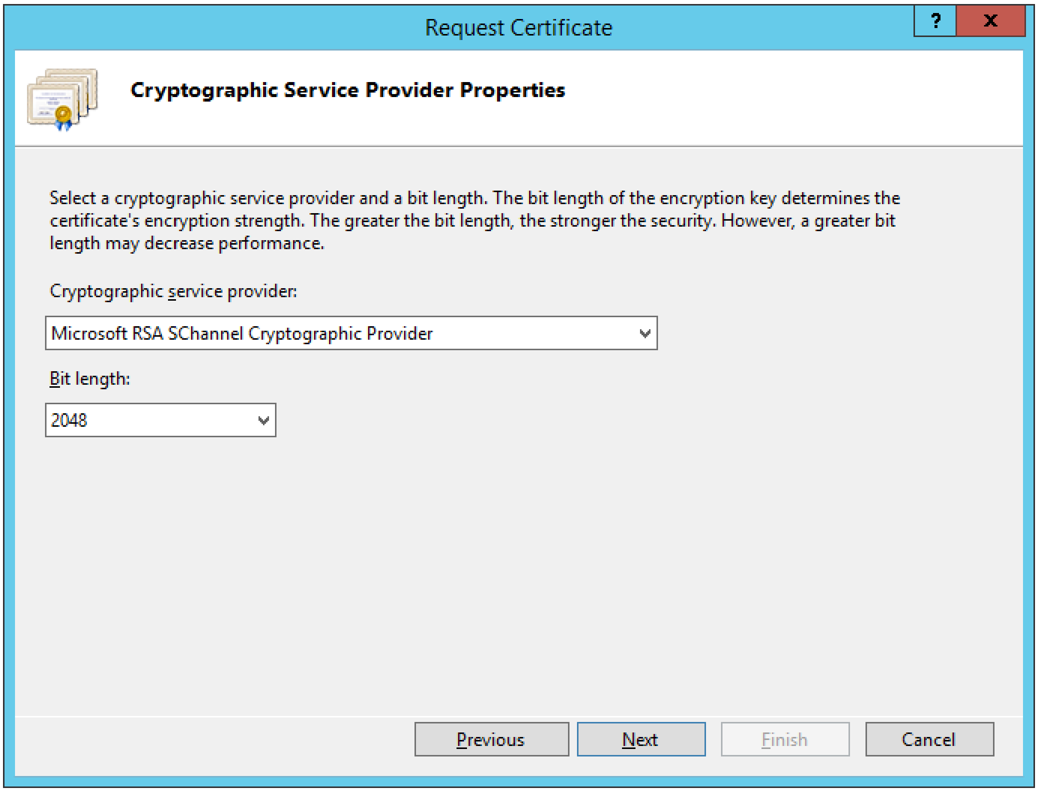
2. Fill out the **Distinguished Name Properties** and click **Next**



Specify the required information for the certificate. State/province and City/locality must be specified as official names and they cannot contain abbreviations.

Common name: myserver.mydomain.local
Organization: My Organization
Organizational unit: IT
City/locality Honolulu
State/province: Hawaii
Country/region: US

3. Change the **Bit length** to **2048** and click **Next**



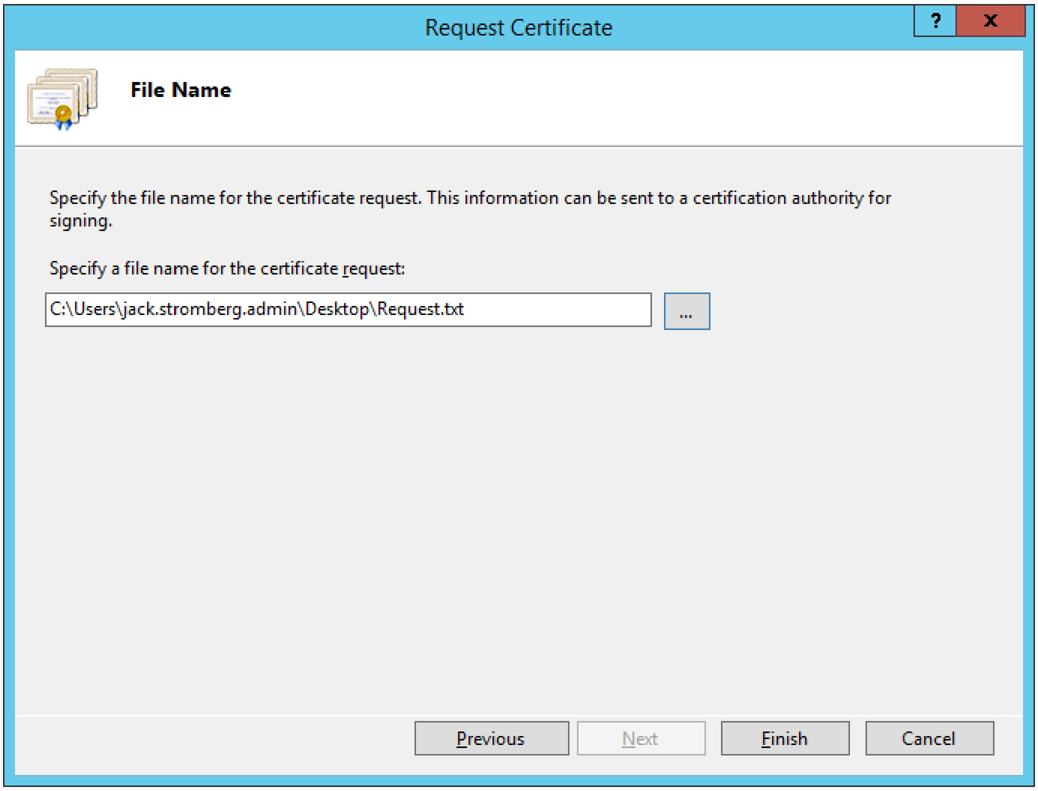
Cryptographic Service Provider Properties

Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

Cryptographic service provider: Microsoft RSA SChannel Cryptographic Provider

Bit length: 2048

4. Select a location on where to place the CSR file that will be generated by the wizard and click **Finish**

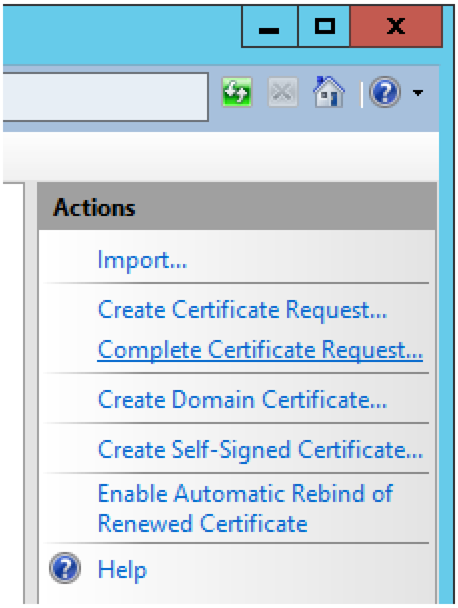


File Name

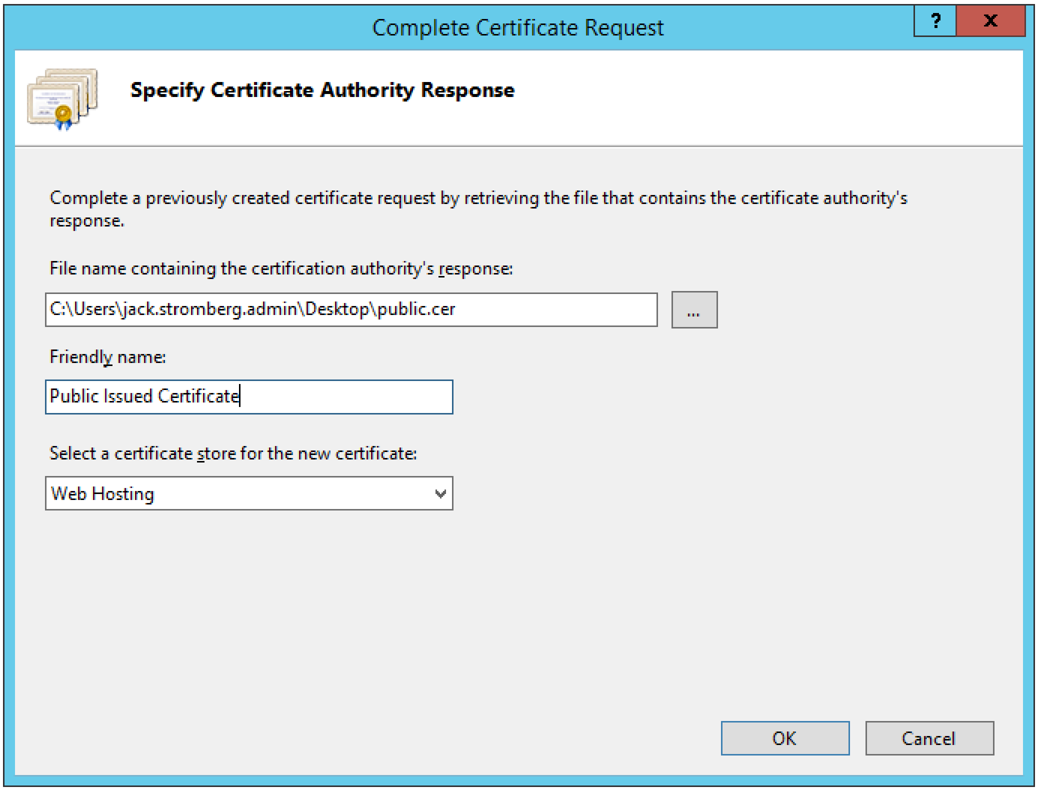
Specify the file name for the certificate request. This information can be sent to a certification authority for signing.

Specify a file name for the certificate request: C:\Users\jack.stromberg.admin\Desktop\Request.txt

5. At this point, send the request to your certificate authority (like GoDaddy, Verisign, or your own internal certificate authority). You should receive back a .cer file once the claim has been fulfilled.
6. Click on **Complete Certificate Request** on the right side


Actions
Import...
Create Certificate Request...
Complete Certificate Request...
Create Domain Certificate...
Create Self-Signed Certificate...
Enable Automatic Rebind of Renewed Certificate
Help

7. Select the .cer file that your public certificate authority provided you, type in a **friendly name** (this can be anything), select **Web Hosting** for the certificate store, and click **OK**



Specify Certificate Authority Response

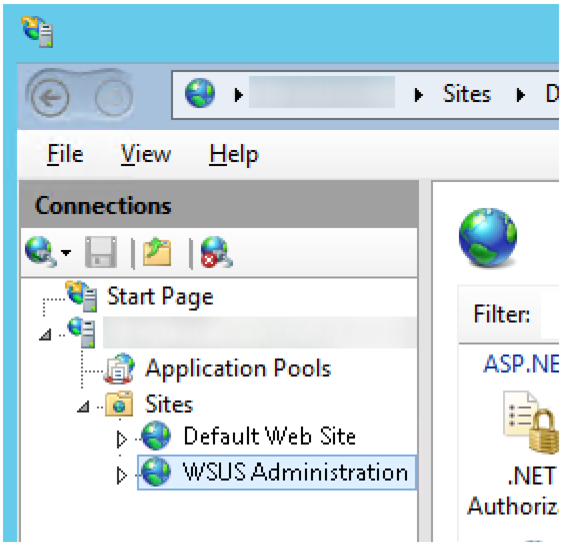
Complete a previously created certificate request by retrieving the file that contains the certificate authority's response.

File name containing the certification authority's response: C:\Users\jack.stromberg.admin\Desktop\public.cer

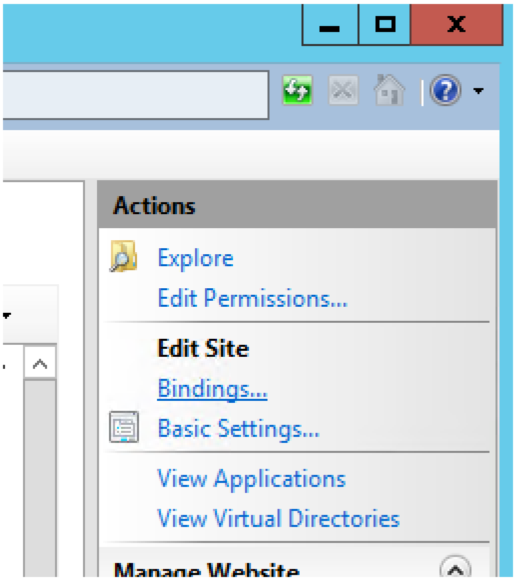
Friendly name: Public Issued Certificate

Select a certificate store for the new certificate: Web Hosting

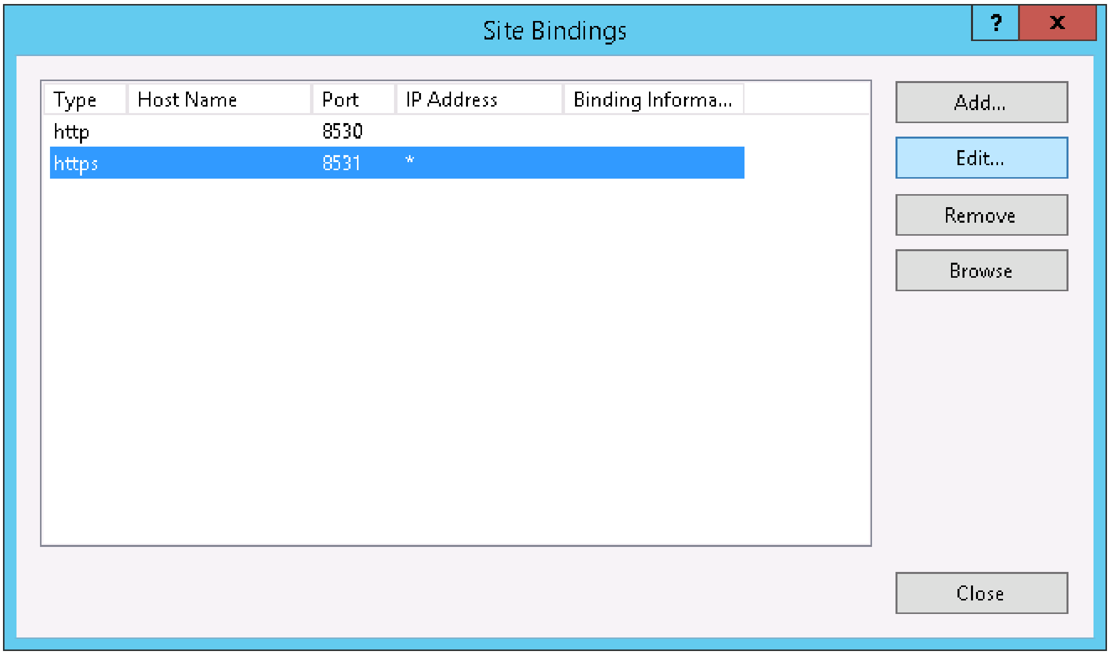
5. Next, we need to bind the SSL certificate to your network adapter.
   1. Expand your server, expand **Sites**, and select **WSUS Administration**



2. Select **Bindings...** on the right side

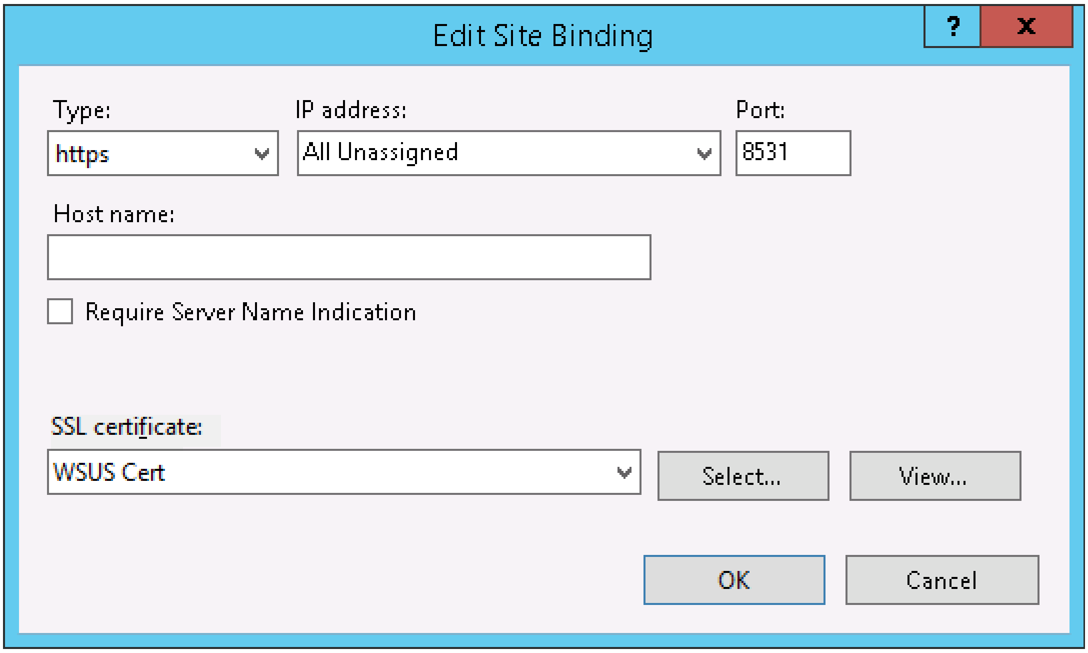


3. Select the **https** site and hit the **Edit...** button


Site Bindings

| Type | Host Name | Port | IP Address | Binding Informa... |
|---|---|---|---|---|
| http |  | 8530 |  |  |
| https |  | 8531 | * |  |

4. Select **https** for the type, select the **SSL certificate** you created above, and click **OK**



Edit Site Binding

Type: https

IP address: All Unassigned

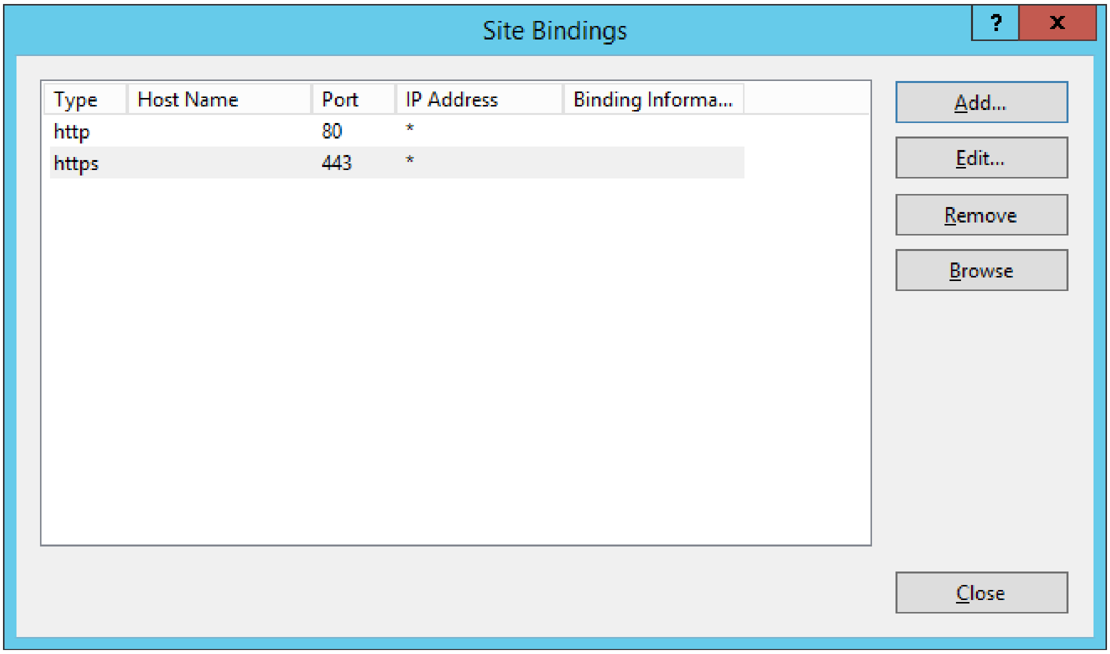
Port: 8531

Host name:

□ Require Server Name Indication

SSL certificate: WSUS Cert

5. Click **Close** on the Site Bindings window

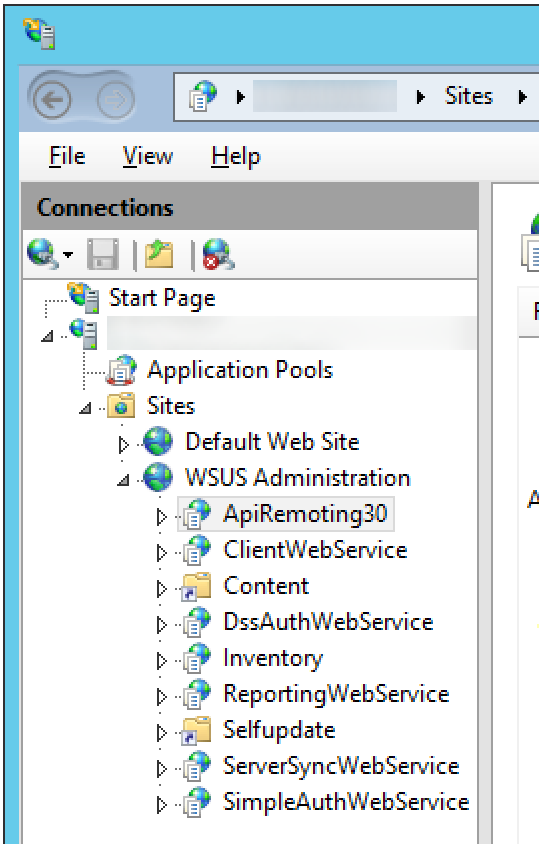


Site Bindings

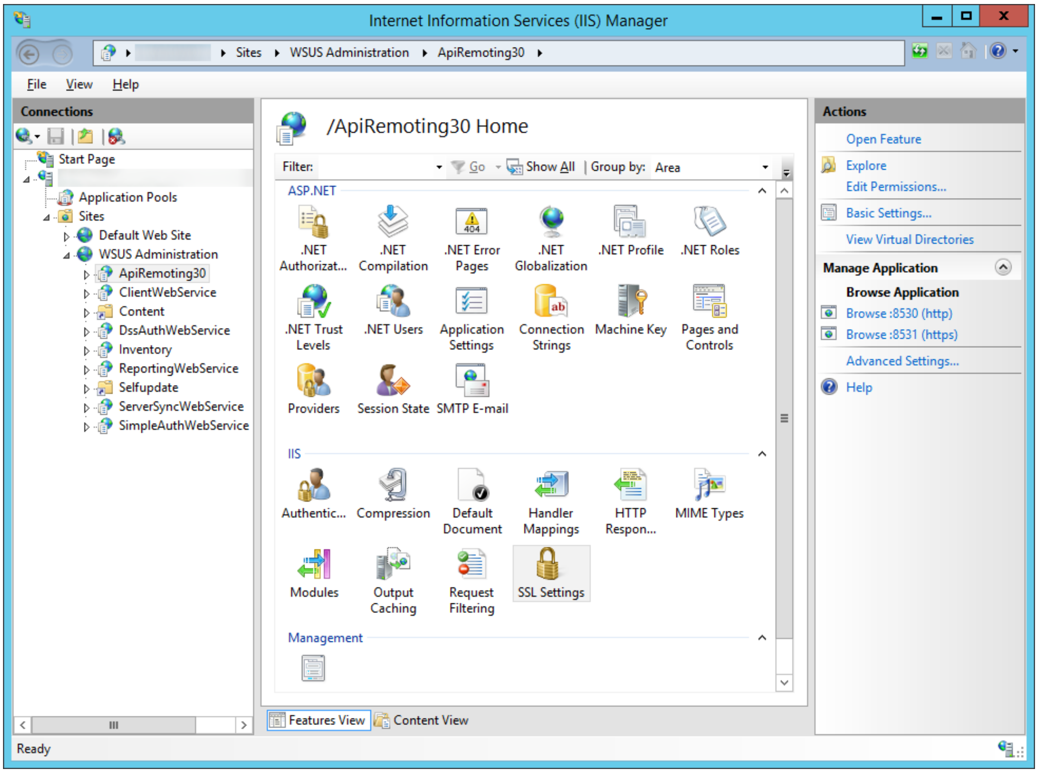
| Type | Host Name | Port | IP Address | Binding Informa... |
|---|---|---|---|---|
| http | | 80 | * | |
| https | | 443 | * | |

6. Next, we need to enforce SSL encryption on the following virtual roots
   - ApiRemoting30
   - ClientWebService
   - DSSAuthWebService
   - ServerSyncWebService
   - SimpleAuthWebService

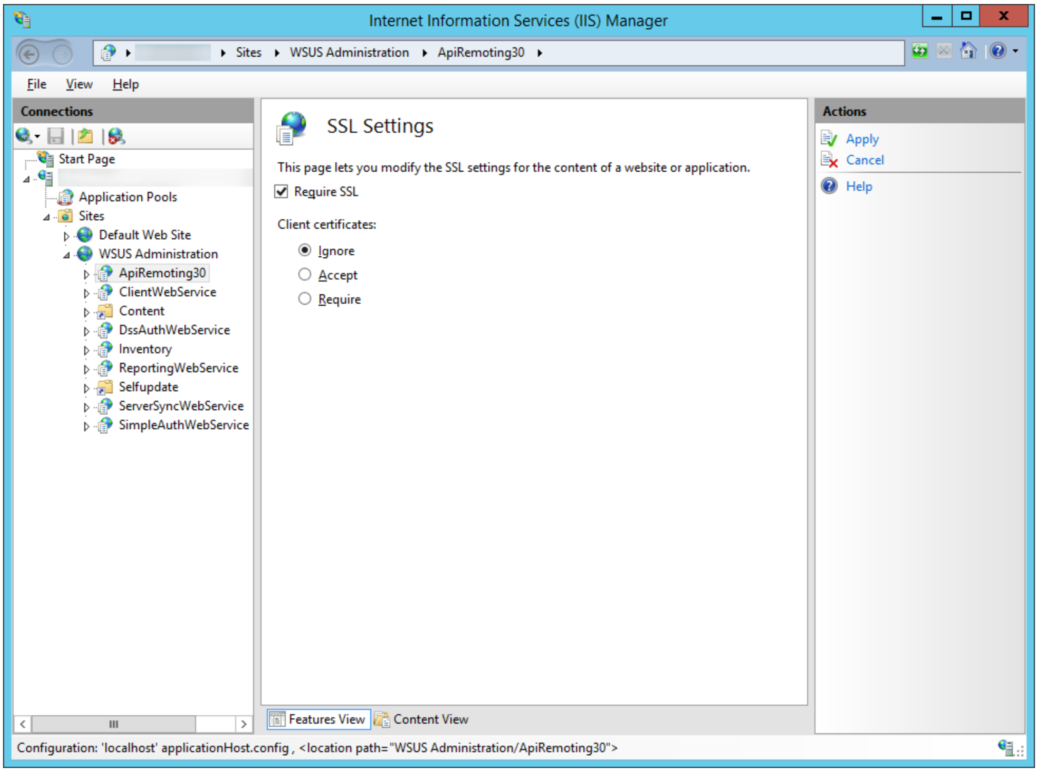
   1. Expand **WSUS Administration** and foreach of the directories above, complete the following steps
      1. Select the virtual site



2. Double click on **SSL Settings**



3. Check **Require SSL** and leave client certificates to **ignore**



SSL Settings

This page lets you modify the SSL settings for the content of a website or application.

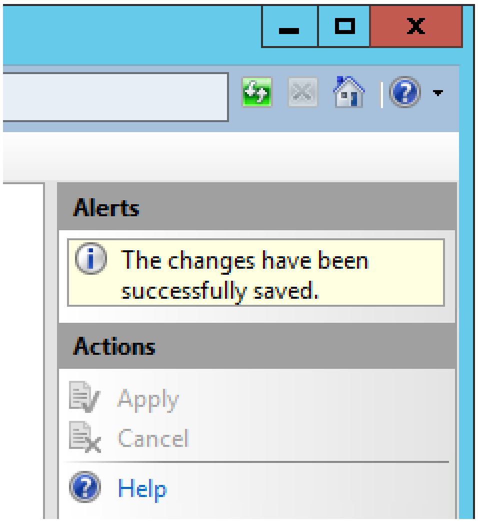
☑ Require SSL

Client certificates:

● Ignore
○ Accept
○ Require

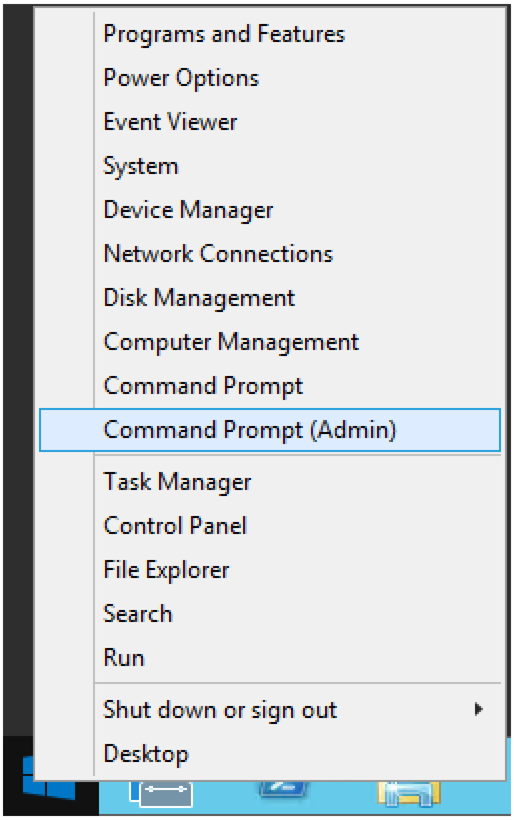
Configuration: 'localhost' applicationHost.config , <location path="WSUS Administration/ApiRemoting30">

4. Click **Apply** in the top right corner

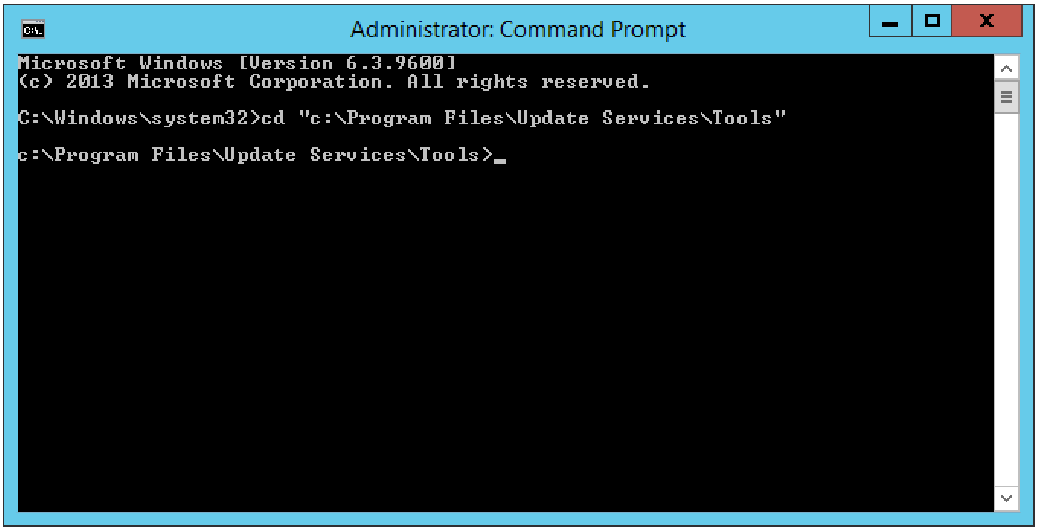


The changes have been successfully saved.

7. Next, we need to execute a command to tell WSUS to use ssl
   1. Open up an elevated command prompt

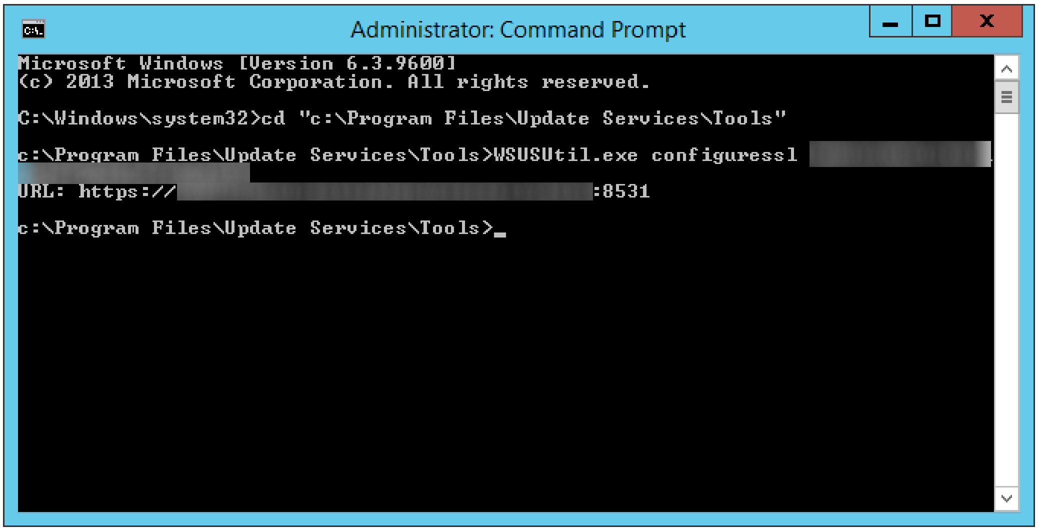


2. Navigate to your WSUS installation folder
    1. **cd "c:\Program Files\Update Services\Tools"**



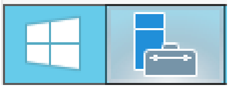
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "c:\Program Files\Update Services\Tools"

c:\Program Files\Update Services\Tools>_
```

3. Execute the following command (replace your server with the correct FQDN)
    1. **WSUSUtil.exe configuressl myserver.mydomain.local**

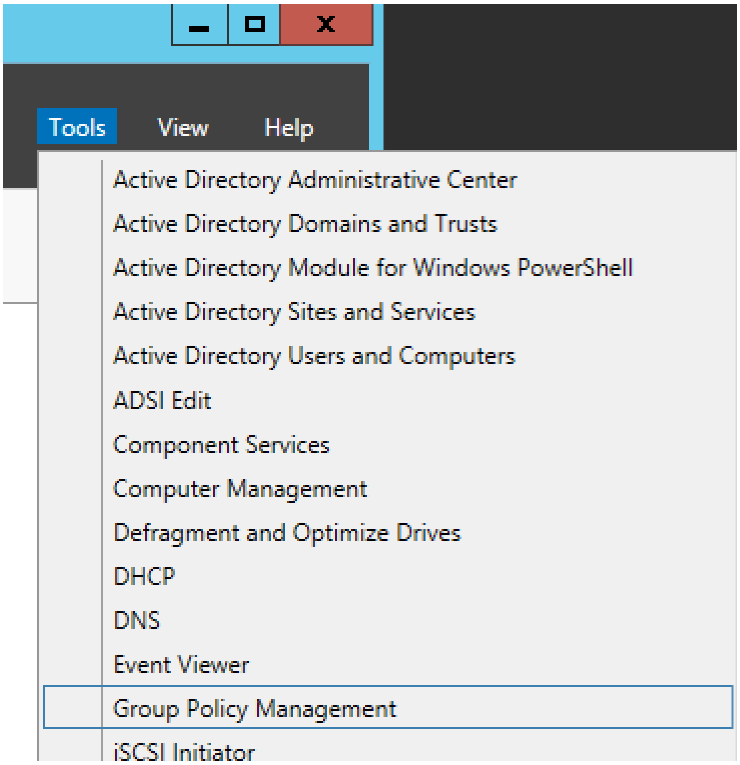


```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd "c:\Program Files\Update Services\Tools"

c:\Program Files\Update Services\Tools>WSUSUtil.exe configuressl [redacted]

URL: https://[redacted]:8531

c:\Program Files\Update Services\Tools>_
```

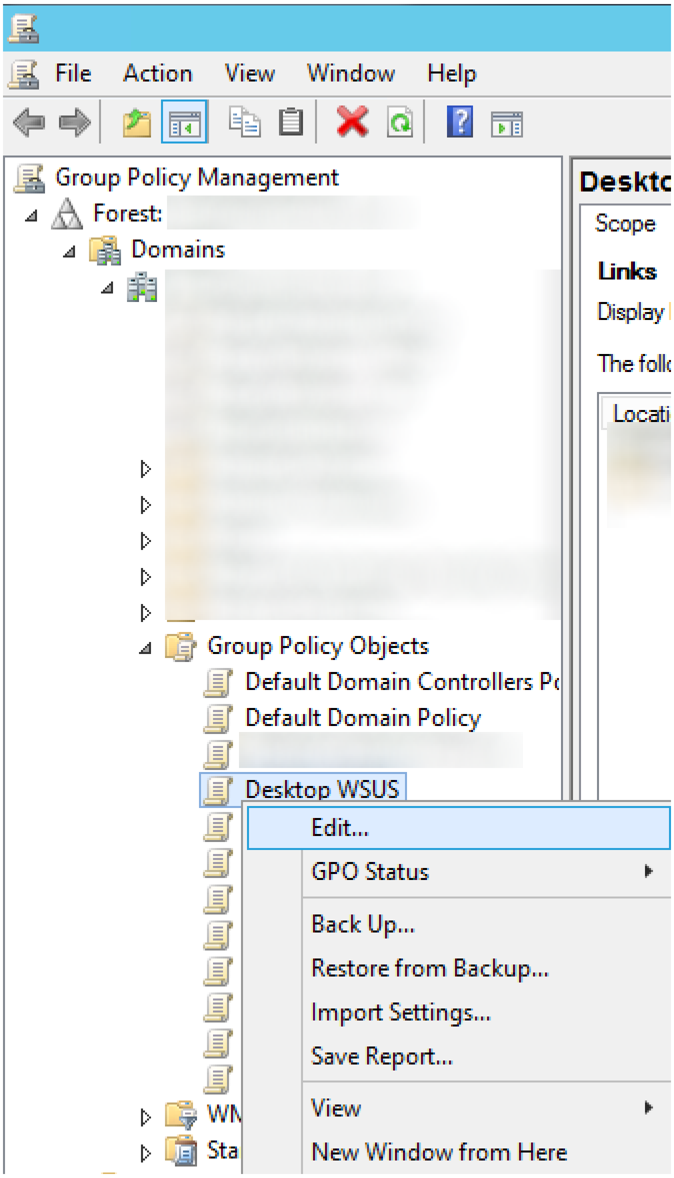
8. Restart the WSUS server to make sure all changes take effect.  You should be able to bring up the WSUS management console if all went well.
9. Configure your clients to connect via SSL to the WSUS server via Group Policy
   1. Login to your domain controller
   2. Open up Server Manager



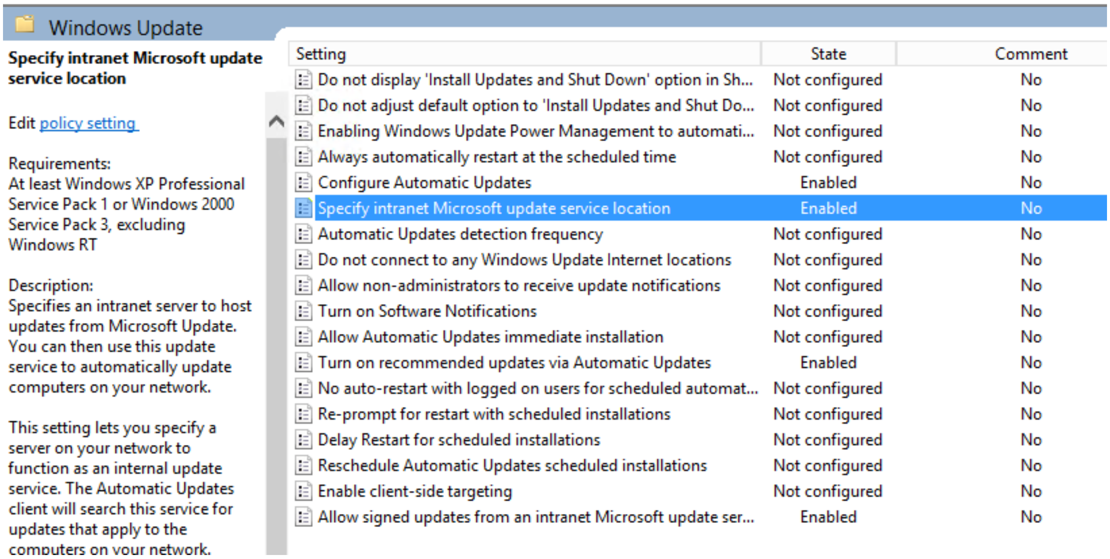
   3. Open up Group Policy Management


Tools
View
Help
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
DHCP
DNS
Event Viewer
Group Policy Management
iSCSI Initiator

   4. Right click on the policy you want to edit and select **Edit**



5. Expand **Computer Configuration** -> **Polices** -> **Administrative Templates** -> **Windows Components** -> **Windows Update**
6. Double click on **Specify intranet Microsoft update service location**



**Specify intranet Microsoft update service location**

Edit policy setting

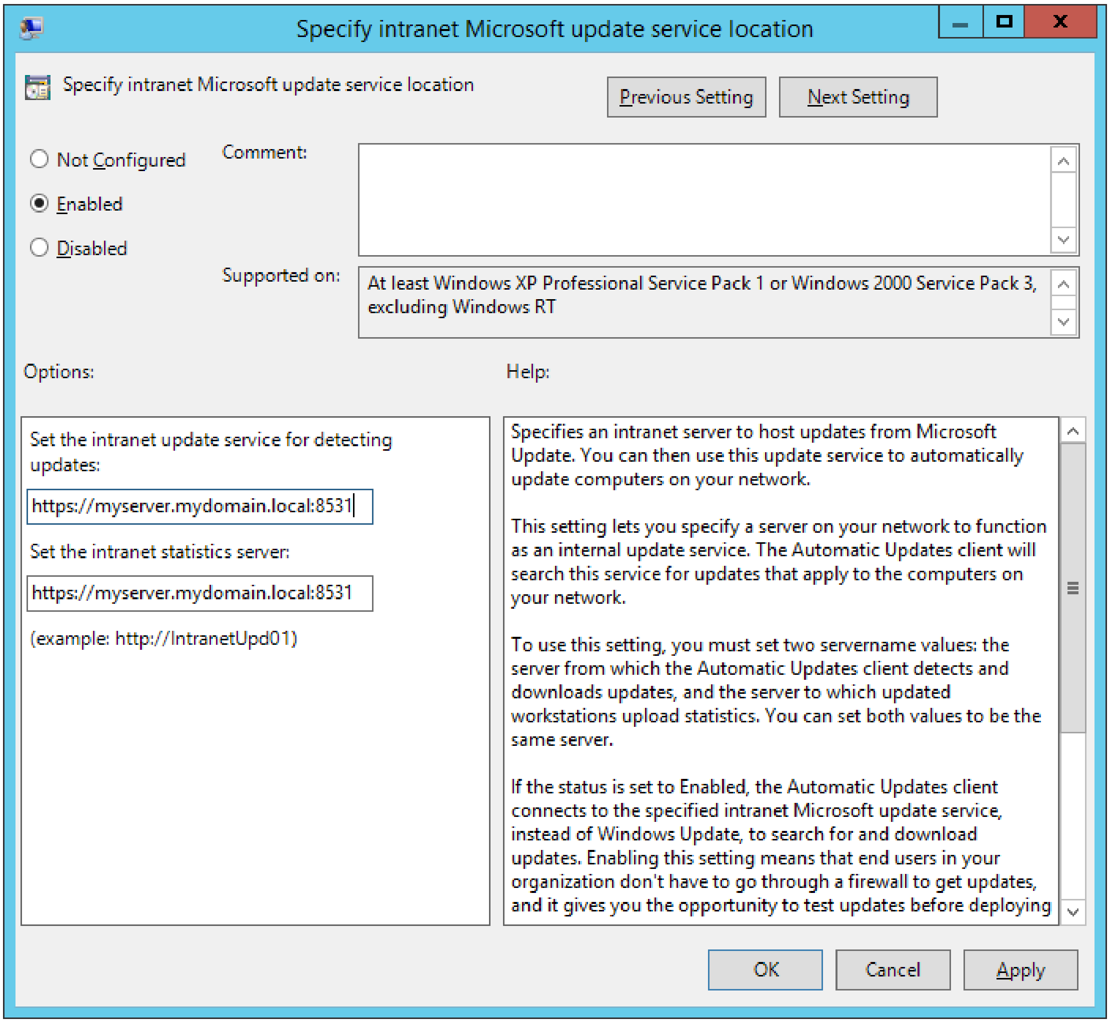
Requirements:
At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Description:
Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

| Setting | State | Comment |
|---|---|---|
| Do not display 'Install Updates and Shut Down' option in Sh... | Not configured | No |
| Do not adjust default option to 'Install Updates and Shut Do... | Not configured | No |
| Enabling Windows Update Power Management to automati... | Not configured | No |
| Always automatically restart at the scheduled time | Not configured | No |
| Configure Automatic Updates | Enabled | No |
| Specify intranet Microsoft update service location | Enabled | No |
| Automatic Updates detection frequency | Not configured | No |
| Do not connect to any Windows Update Internet locations | Not configured | No |
| Allow non-administrators to receive update notifications | Not configured | No |
| Turn on Software Notifications | Not configured | No |
| Allow Automatic Updates immediate installation | Not configured | No |
| Turn on recommended updates via Automatic Updates | Enabled | No |
| No auto-restart with logged on users for scheduled automat... | Not configured | No |
| Re-prompt for restart with scheduled installations | Not configured | No |
| Delay Restart for scheduled installations | Not configured | No |
| Reschedule Automatic Updates scheduled installations | Not configured | No |
| Enable client-side targeting | Not configured | No |
| Allow signed updates from an intranet Microsoft update ser... | Enabled | No |

7. Change the intranet update service url to **https** and specify port **8531** and then click **Apply**.



Specify intranet Microsoft update service location

Specify intranet Microsoft update service location

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Set the intranet update service for detecting updates: https://myserver.mydomain.local:8531

Set the intranet statistics server: https://myserver.mydomain.local:8531

(example: http://IntranetUpd01)

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying

That should do it! Try doing a gpupdate /force on your local machine and the check for windows updates. If windows successfully completes checking for updates, you should be good to go! 🙂

**Notes**: Official documentation from Microsoft in regards to using SSL and WSUS can be found here: http://technet.microsoft.com/en-us/library/hh852346.aspx#conssWSUS

This entry was posted in Uncategorized and tagged Server 2008 R2, server 2012 r2, ssl, Windows Server Update Services, wsus on November 6, 2013 [http://jackstromberg.com/2013/11/enabling-ssl-on-windows-server-update-services-wsus/] by Jack.

## 15 thoughts on “Enabling SSL on Windows Server Update Services (WSUS)”

Mark
February 18, 2014 at 10:26 pm

There is an error in your doco. You have in Step5 assigning the cert to the default website, instead of the WSUS Administration website

**Jack** Post author
February 20, 2014 at 11:59 am

Hey Mark,

Thank you for pointing this out! I have updated the document to reflect the correct settings.

Appreciate the feedback!
Jack

Anwar
June 13, 2014 at 11:19 am

Hi Jack,

Thanks for providing these instructions – very helpful!
Does this also provide client authentication? In other words, does the WSUS server require WSUS clients to authenticate themselves to the WSUS server by providing a computer certificate?

Thanks in advance,
Anwar

Post author

**Jack**
June 16, 2014 at 7:26 am

This requires the client to use SSL to communicate with WSUS but does not require the client to authenticate itself with their computer certificate. I believe you can achieve this by checking Require in IIS instead of Ignore (as shown in step 6-3).

Hope this helps,
Jack

Lasse
August 18, 2015 at 6:24 am

Exelent write-up.
Maybe add that wildcard certificates are a NO-GO.
And add the command for moving to port 443 / 80 instead of the 853x ports 🙂

Jordan Cobb
February 1, 2016 at 9:39 am

Why cant you use a wildcard cert?

**Jack** Post author
February 2, 2016 at 9:57 pm

There is no documentation by Microsoft stating that WSUS v3.0 supports or doesn't support. In this case, based on forums and the blog, it appears there are issues with the WSUS service understanding wildcard certs properly.

Pingback: Migrer un serveur WSUS en SSL - TechSpaceTechSpace

**Jack** Post author
December 15, 2016 at 10:44 am

Thank you for a version in French 🙂

Mark
May 19, 2017 at 1:59 pm

How would you create a certificate to work with an external FQDN and internal FQDN using an internal root CA?

**Jack** Post author
May 29, 2017 at 3:10 pm

Use a SAN certificate. See here: https://blogs.technet.microsoft.com/sus/2011/05/09/how-to-create-an-internet-facing-wsus-server-that-uses-different-internal-and-external-names/

Jack

gaurav pandey
September 1, 2017 at 7:50 am

At Step 6, by mistake I have applied “Require SSL” and “Ignore” on all subdirectories and the main directory “WSUS Administration” which broke something and WSUS is not showing the page and showing error with “Reset Server Node” button. Can you please guide, what setting I should choose for all those directory and subdirectories?

**Jack** Post author
September 1, 2017 at 8:00 am

Please see the following article for the correct permissions: https://technet.microsoft.com/en-us/library/bb633246.aspx#procedureSection1

Perform the following steps on the APIRemoting30, ClientWebService, DSSAuthWebService, Server-SyncWebService, and SimpleAuthWebService virtual directories that reside under the WSUS Web site.
-On the SSL Settings page, select the Require SSL checkbox. Ensure that Client certificates is set to Ignore.

---

**gaurav pandey**
September 1, 2017 at 8:42 am

I did same but I want to revert because this setting broke something.

---

Simon
March 5, 2018 at 8:13 am

Great doc – to the point – very helpful

---

This site uses Akismet to reduce spam. Learn how your comment data is processed.