Fusion Installer Instructions

This is the installation guide for the Fusion NaviLine installer. This guide provides instructions for installing, updating, and maintaining your Fusion REST web service. Each of these actions: installing, updating, or maintaining, has its own set of steps and instructions to follow. This guide explains what each of these actions does, and then guides and directs you to the steps you need to do for the action. iis

Contents

Configuration Checklist

Before you start the installation, go through the configuration checklist below and fill out all the values. You will be prompted to enter this information during the install. You should also print this list and keep a copy for your records. If your configuration checklist is complete, click here:

Prerequisites to move to the next section.

Item	Configuration Info	Customer's Value
1	**Application ID and Key**	
1a	Your App ID and App Key **Note:** Contact CentralSquare support to receive this value. This is a paired key consisting of a short (App ID) and long (App Key) encoded value.	**AppID1:**_____ **AppKey1:** _____
2	***iSeries Server Settings***	
2a	Local iSeries user name	**User:** _____
2b	Local iSeries password	**Password:**_____
2c	Fully qualified local iSeries server name or IP	_____
2d	iSeries database name	_____
2e	iSeries program library	_____
2f	iSeries data library	_____
2g	iSeries environment label (if used)	_____
2h	iSeries registered library (defaults to program library)	_____
3	Configuration Settings	
3a	***NaviLine Server Name*** ***Domain name*** This is the domain name used to access the site externally. I.e., Fusion.myCity.gov	_____ _____

Prerequisites

This section goes over prerequisites of other programs that must be installed before running the Fusion installation. The installation will not be able to install without these already installed on the server.

Go through the following checklist before starting any installation. For instructions, press **CTRL+Click** on the underlined portion of the text, and it will guide you to the section for that requirement.

Pre-Start Checklist

Item	Check	Confirmation
1	***NaviLine Version*** is 9.1.14.5 or higher	**[ ] NaviLine Version: _____**
2	***Hardware Specifications***	
2a	2 GHz processor	**[ ] Processor**
2b	6 GB RAM	**[ ] RAM**
2c	60 GB disk space	**[ ] Disk Space**
3	***Windows Server and IIS Manager***	
3a	Windows 2019 Server with IIS 10 Windows 2016 Server with IIS 10	**[ ] Windows 2019 / IIS 10** **[ ] Windows 2016 / IIS 10**
3b	***Web Platform Installer*** must be installed	**[ ] Web Platform Installer**
3c	*Error! Reference source not found.* must be installed	**[ ] Web Deploy**
4	***Configure IIS with SSL***	
4a	Symantec/DigiCert SSL certificate. Extended Validation (EV) is not required.	**[ ] SSL certificate**
5	***Firewall*** access	
5a	The server must be externally accessible, unless being queried by internal only resources.	**[ ] DMZ or NAT**
5b	See the Firewall Access section for a list of ports to open to/from iSeries	**[ ] iSeries Ports**
5c	Open ports 443 to the Internet	**[ ] Internet Ports**
6	***Microsoft.NET Framework 4.5*** or higher	**[ ] .NET 4.5**
7	***IBM I Access Client Solutions*** or IBM Client Access V7R1	**[ ] IBM Access Client Solution** **[ ] IBM Client Access**
8	Payments	
8a	*Error! Reference source not found.* package must be installed on the IBM iSeries for payments	**[ ] Web Enablement**

8b	***Cash Receipts*** batch must be configured to accept payments from Fusion	**[ ] Cash Receipt Batch**
8c	***Agnostic Payment Listener*** must be installed on POS machines accepting credit card payments	**[ ] Payment Listener**

Completed? If all the above checks are completed, click here: *Installation Options* to continue to the next steps.

NaviLine Version

Fusion requires NaviLine version 9.1.14.5 or higher. However, changes are only supported for the prior two NaviLine versions. Support issues for older versions will be made on a 'best effor' basis.

Hardware Specifications

NOTE: Due to port conflicts with WebLogic, Fusion cannot be on the same server as C2G3.

Recommended hardware specifications:

- Windows 2016 or 2019, 64 bit
- 2 GHz processor (2 processors)
- 6 GB RAM
- 60 GB disk space

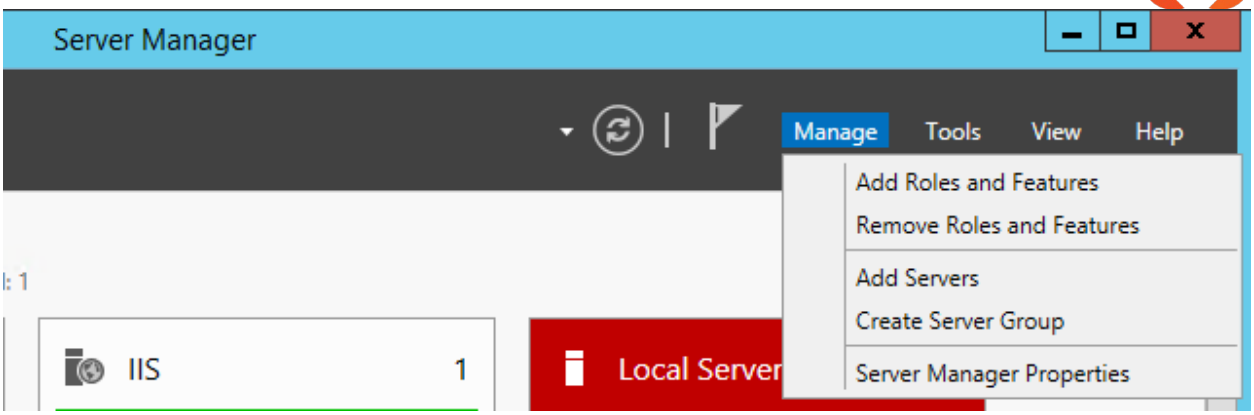
Windows Server and IIS Manager

IIS Manager must be installed on the Windows Server. The table below lists the supported operating systems (OS) and IIS version required.

Windows OS	IIS version
Windows Server 2019	**IIS 10**
Windows Server 2016	**IIS 10**

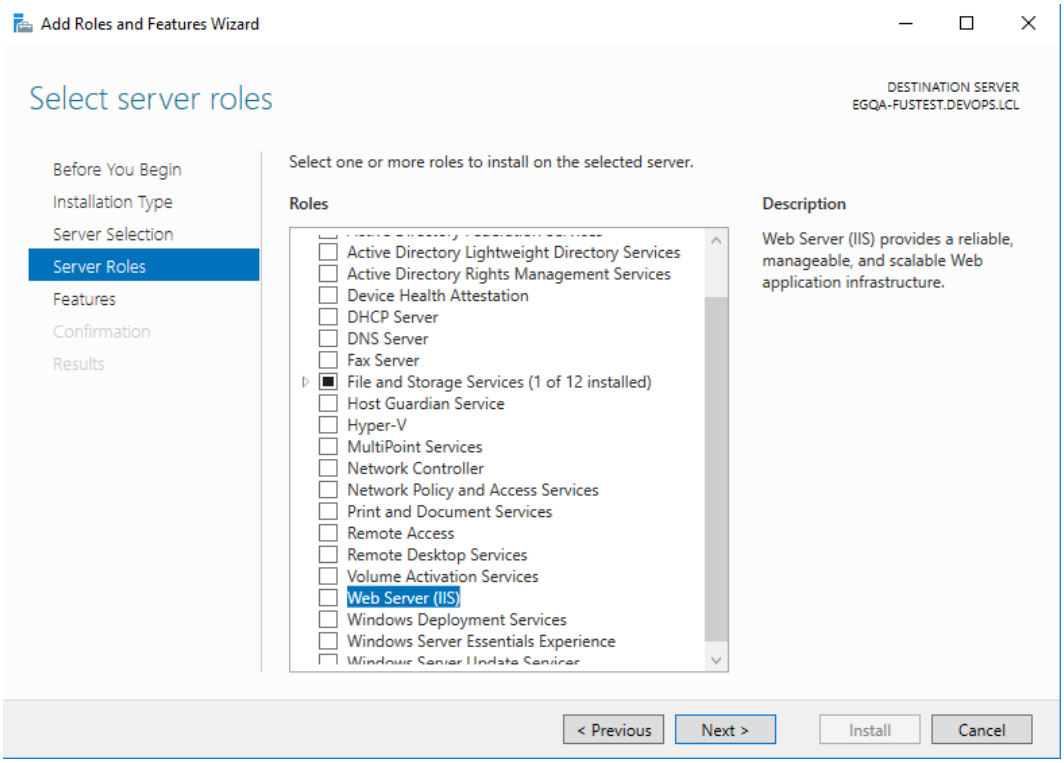
These instructions are for installing IIS 10 on Windows Server 2016. See ***Appendix 1: IIS installation for Windows 2012*** for similar instructions and screen shots using Windows Serveer 2012

Use the **Server Manager > Manage > Add Roles and Features** to enable the IIS Manager roles and features. If IIS was previously installed, some options may be already checked. Please step through the roles and features to make sure all the items below are set.

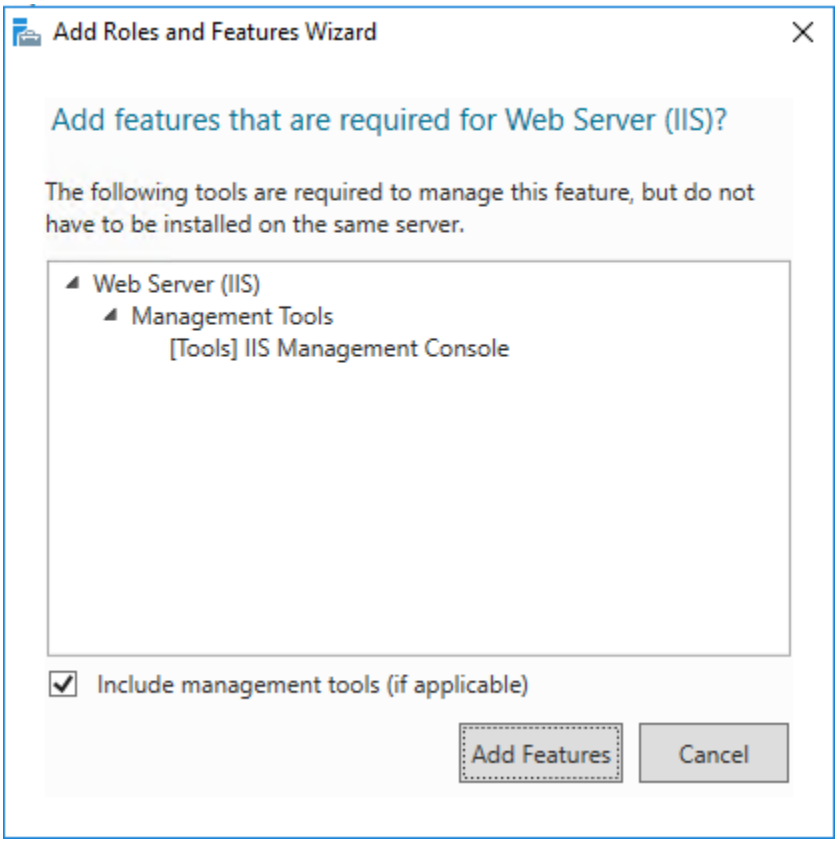


Select the Web Server role.

- Roles: Web Server



Checking the **Web Server (IIS)** prompts you with:

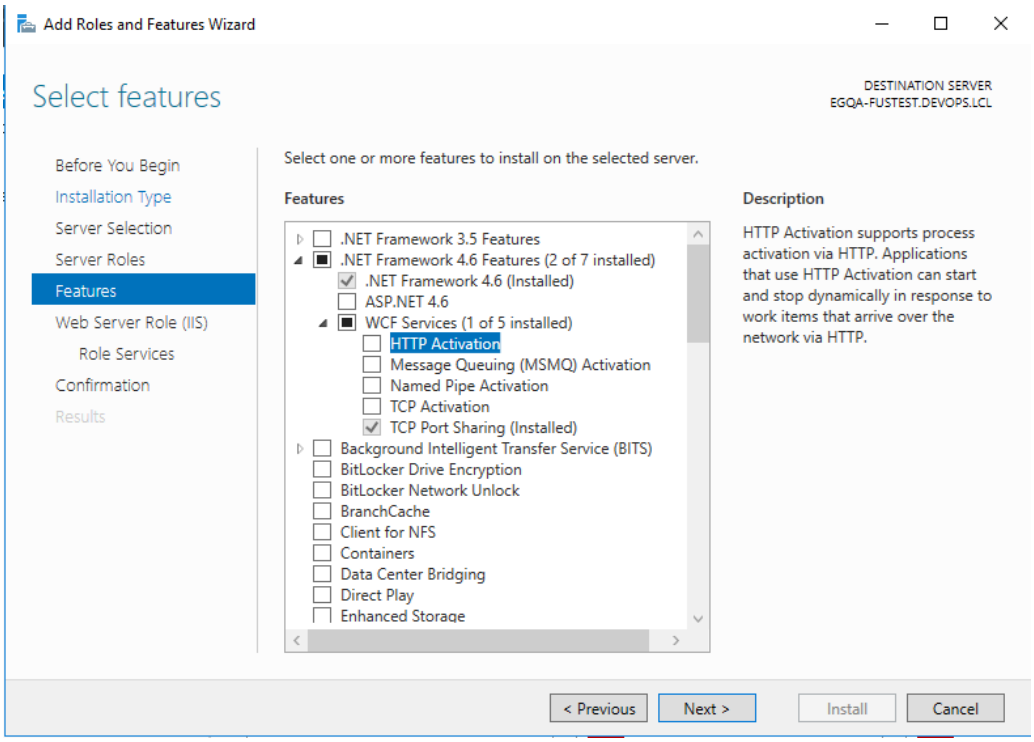


1. Click **Add Features**
2. Click **Next**

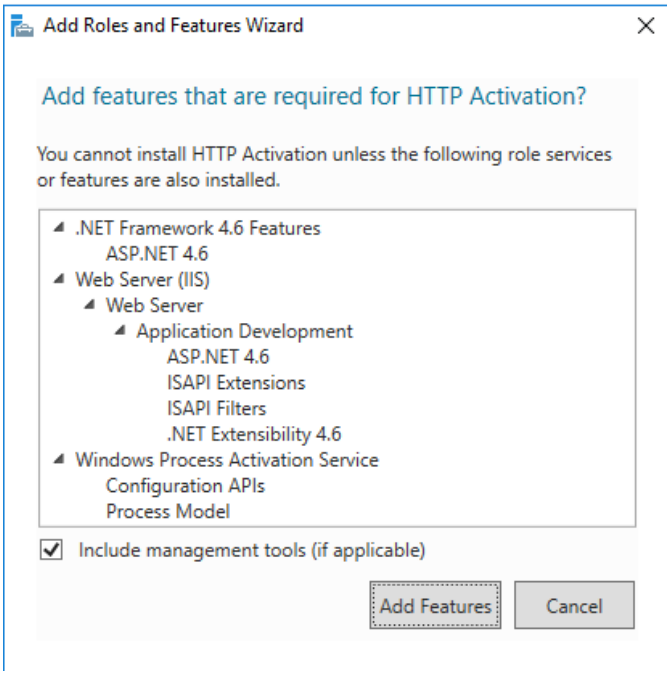
This continues to Features.

Set the Features options under Web Server.

- Features: **.NET Framework 4.6 Features > WCF Services > HTTP Activation**



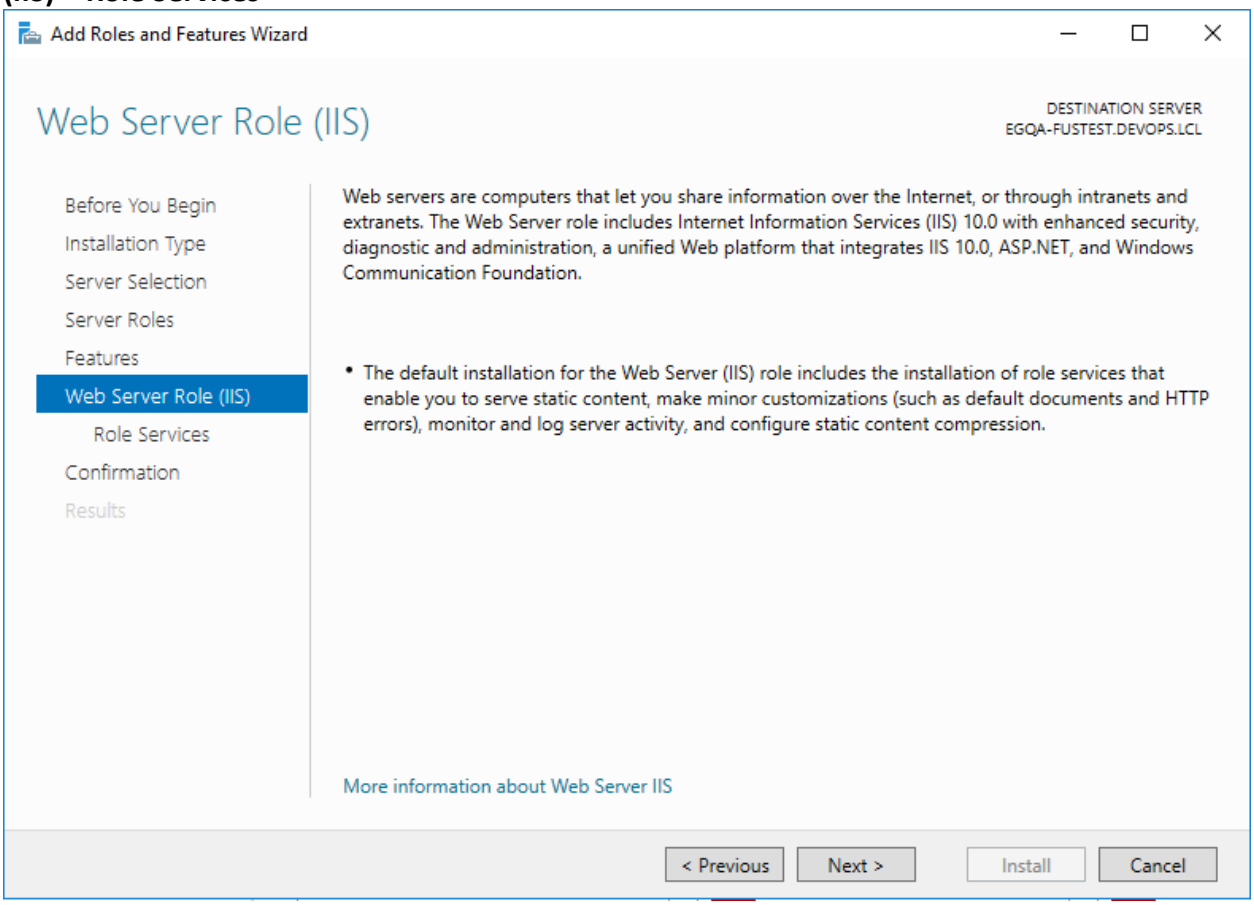
It prompts with:



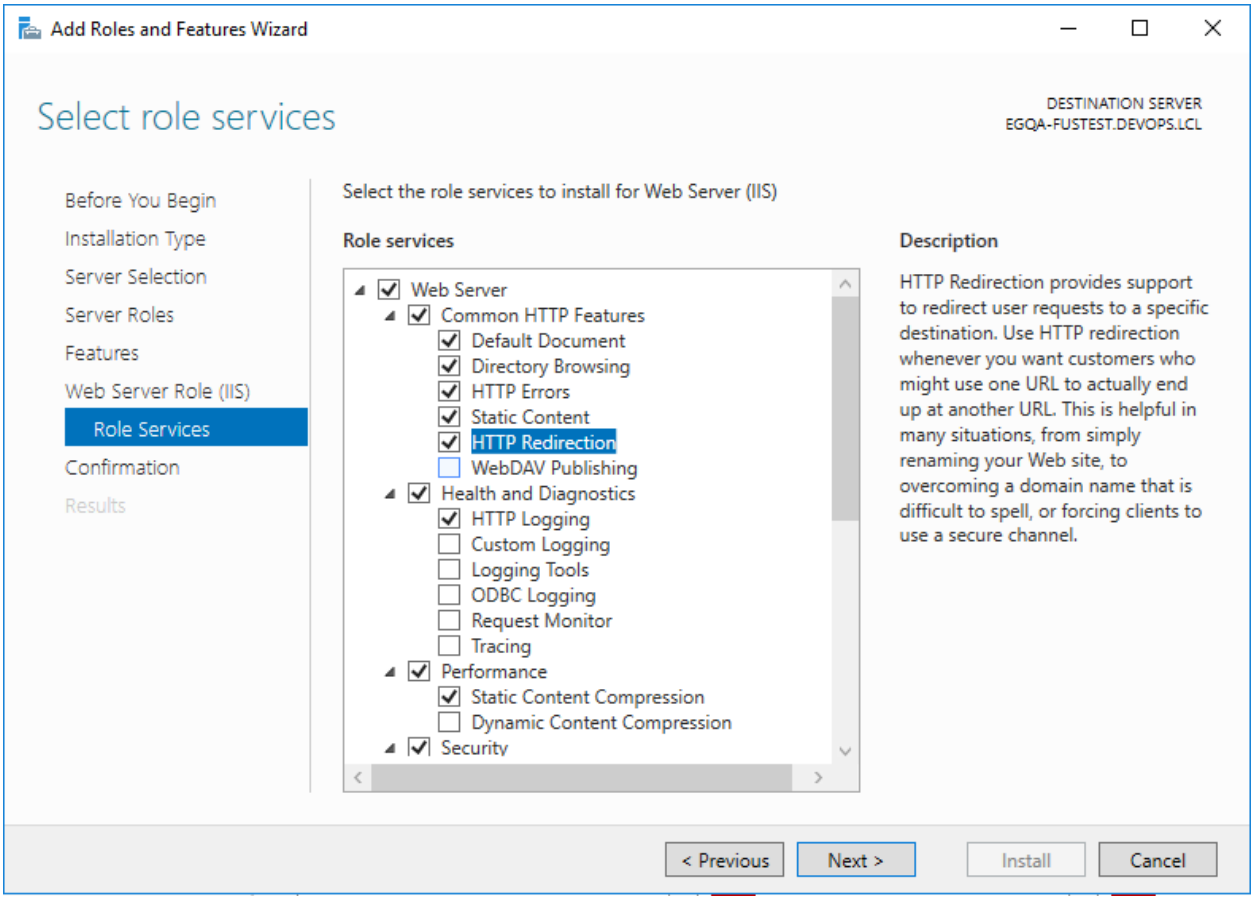
Click **Add Features**. Click **Next**.

Set the Web Server Role options

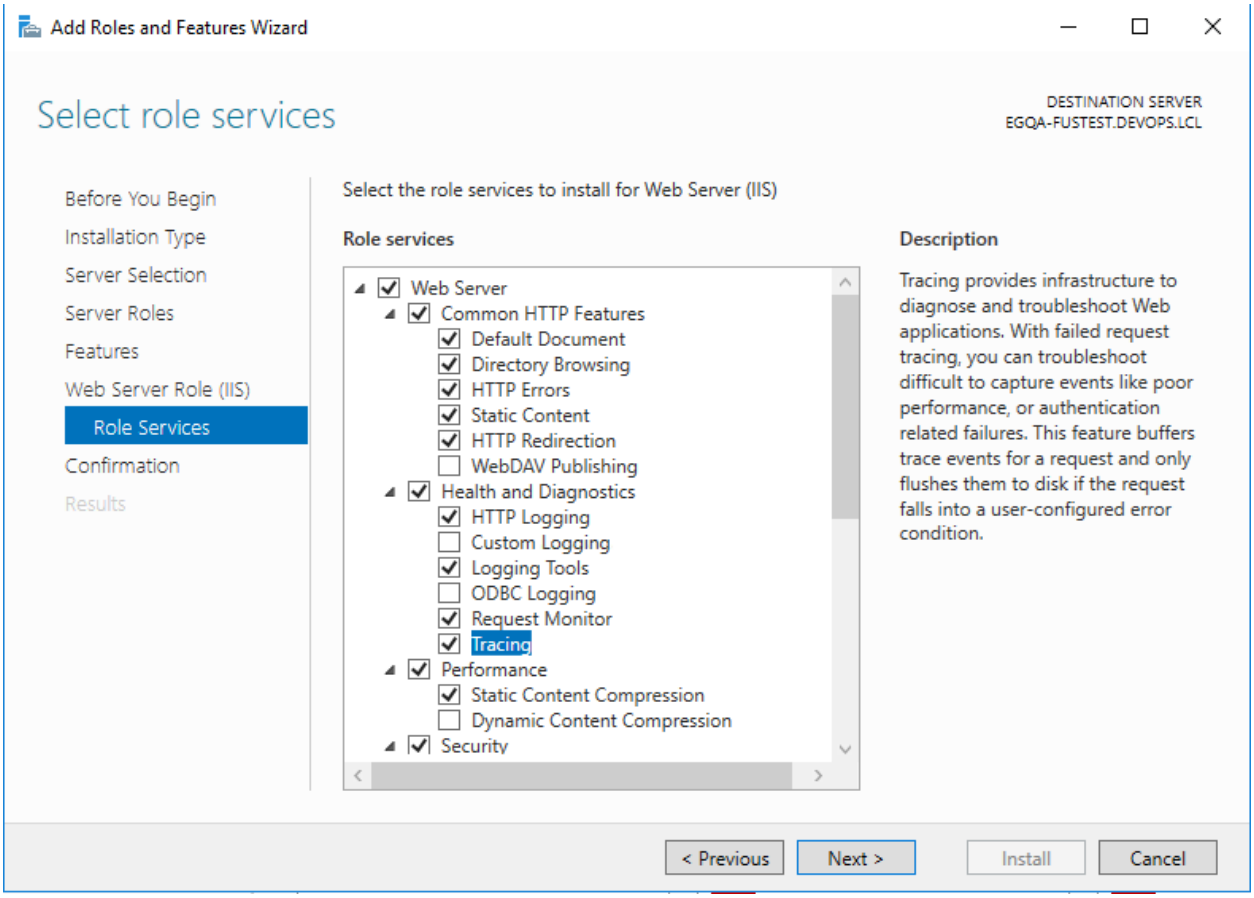
After enabling the Web Server role and features, it continues with settings for **Web Server Role (IIS) > Role Services**



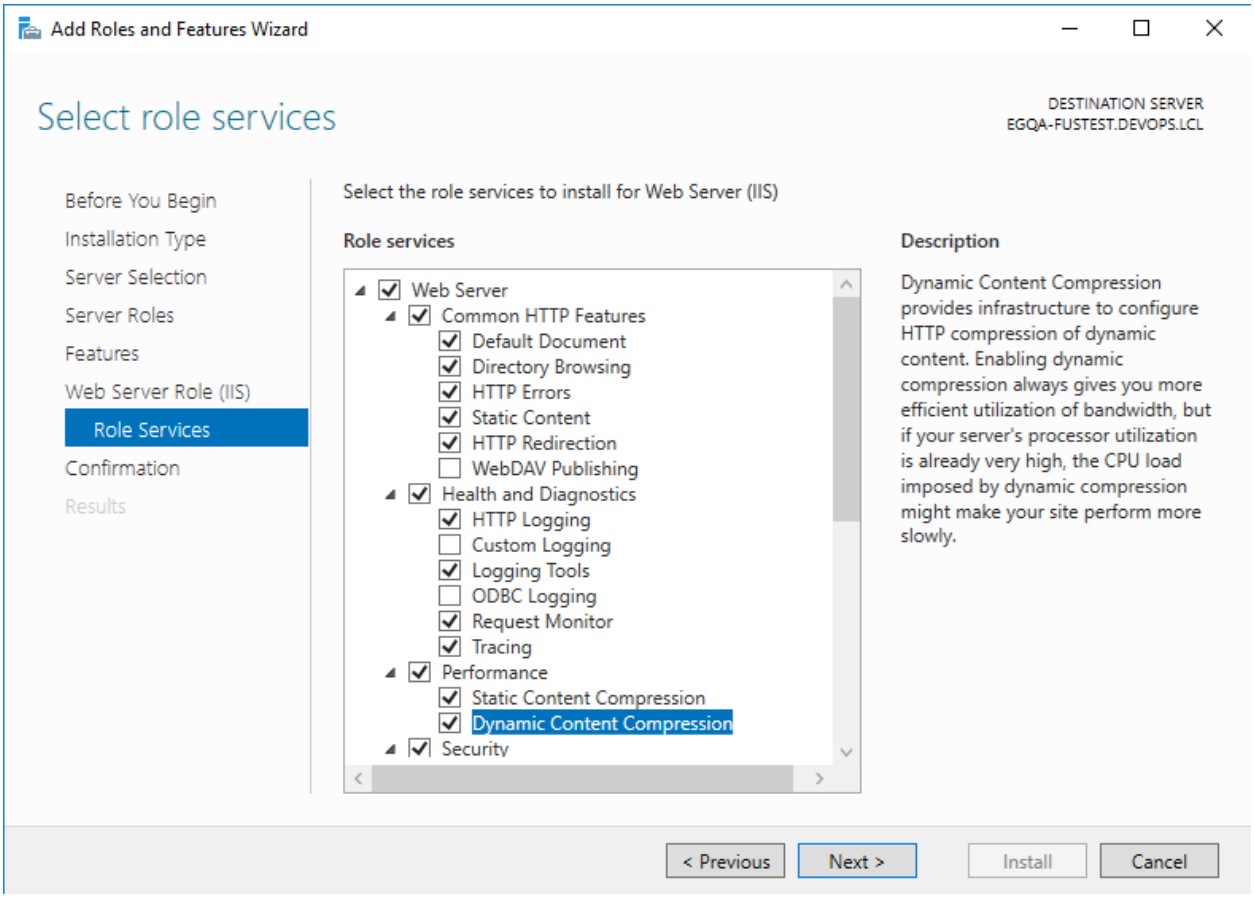
- Roles: **Web Server > Common HTTP Features**
    - Default Document
    - Directory Browsing
    - HTTP Errors
    - Static Content
    - HTTP Redirection



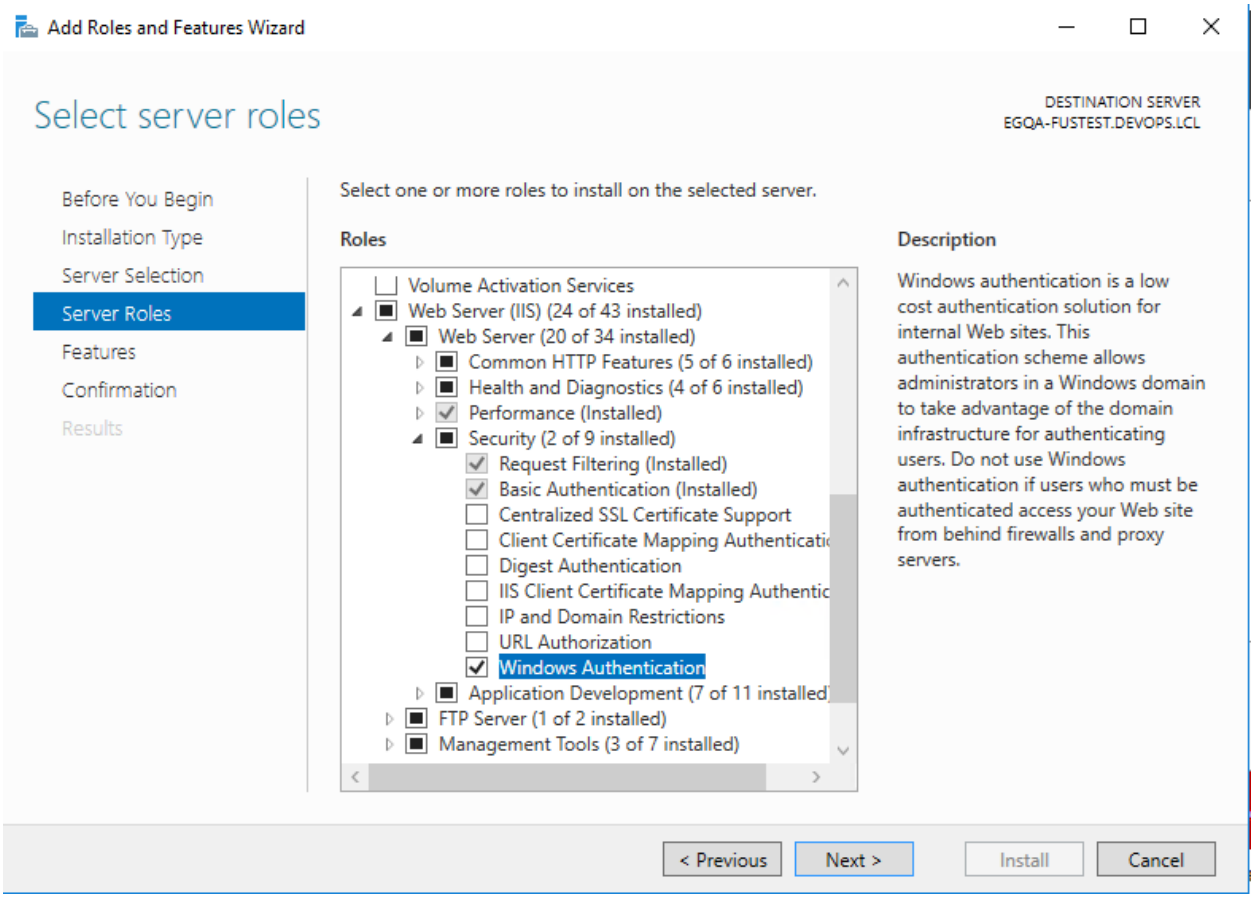
- Roles: **Web Server > Health and Diagnostics**
  - HTTP Logging
  - Logging Tools
  - Request Monitor
  - Tracing



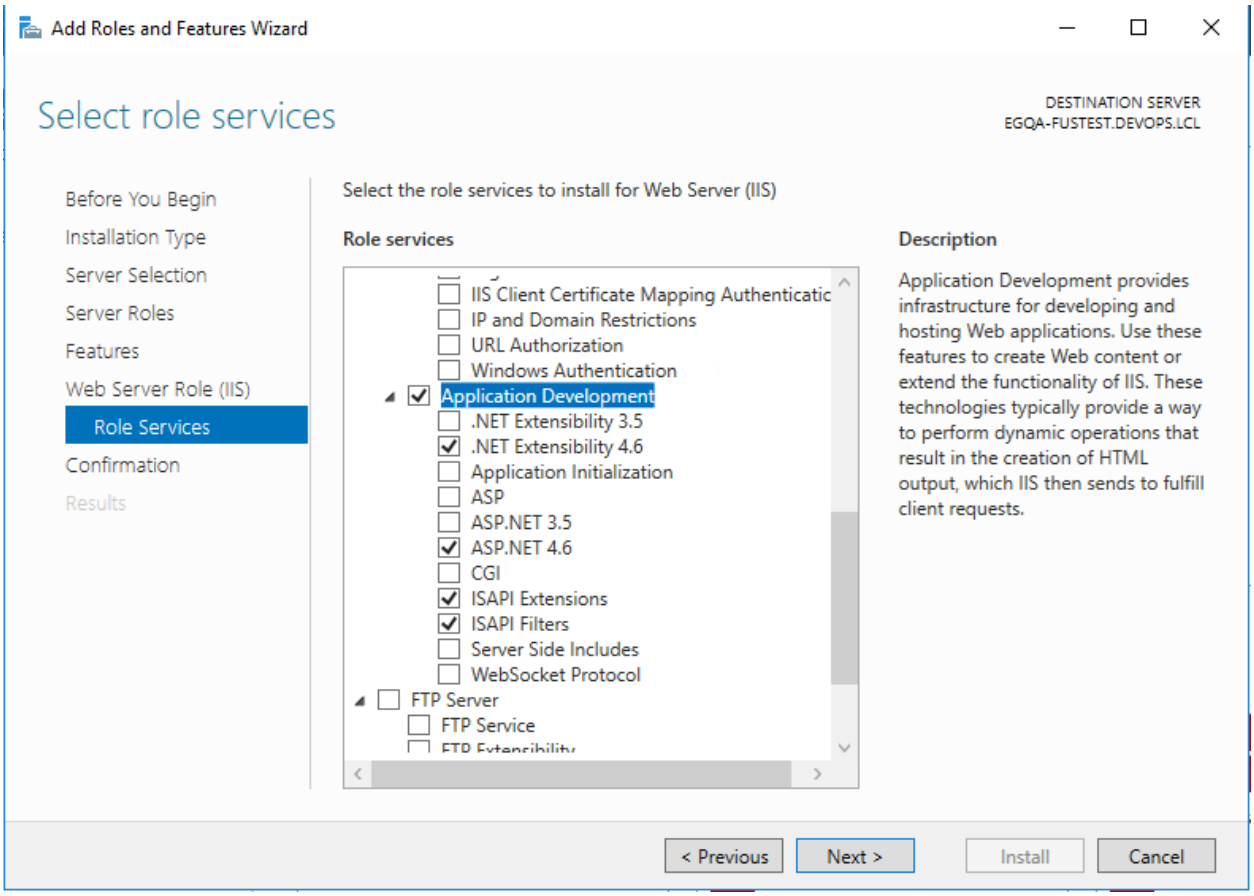
- Roles: **Web Server > Performance**
    - Static Content Compression
    - Dynamic Content Compression



- Roles: **Web Server > Security**
    - Request Filtering
    - Basic Authentication
    - Windows Authentication



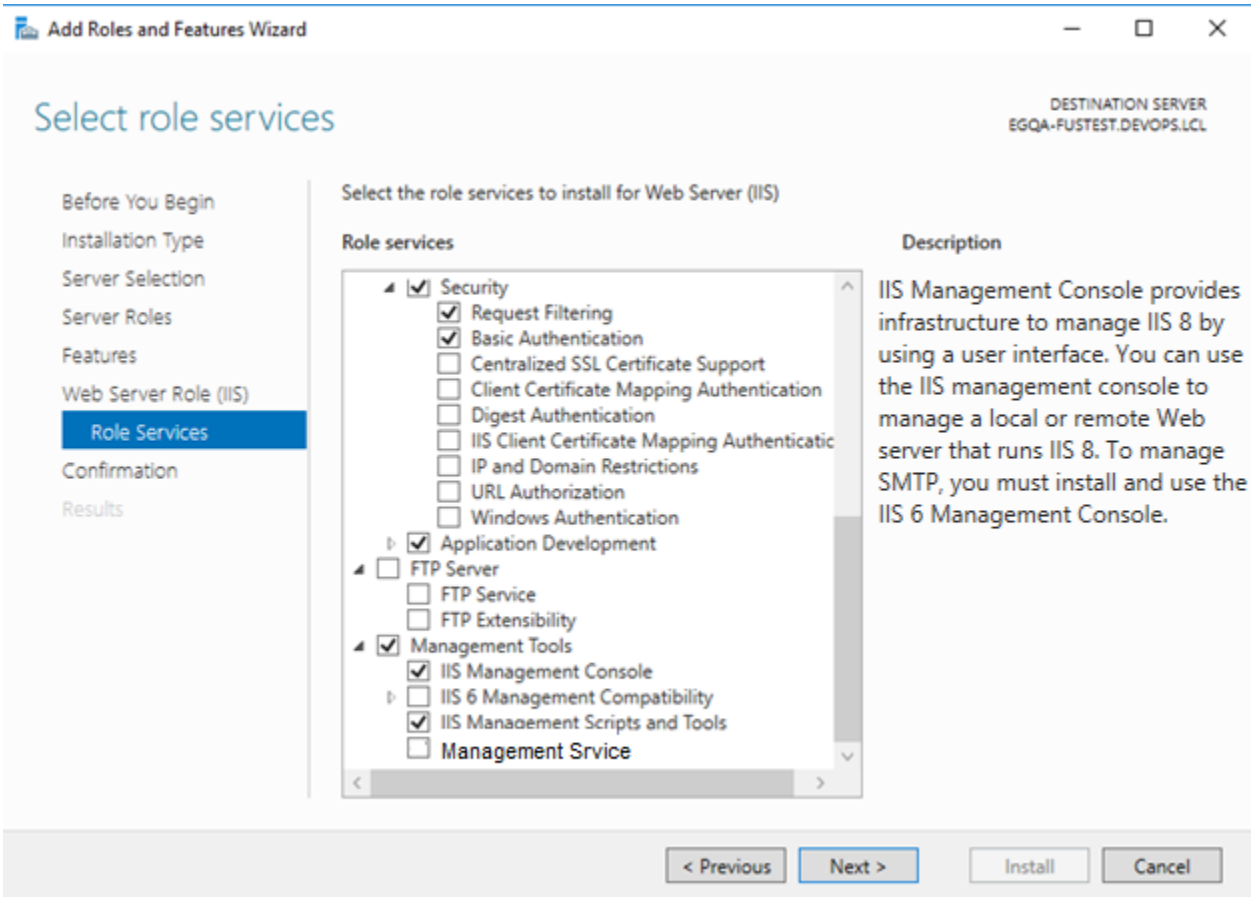
- Roles: **Web Server > Application Development**
  - .NET Extensibility 4.6
  - ASP.NET 4.6
  - Checking ASP.NET 4.6 will prompt to include the following pre-requisites
    - .NET Extensibility 4.6
    - ISAPI Extenstions
    - ISAPI Filters
  - CGI
  - ISAPI Extensions
  - ISAPI Filters



.NET Extensibility 3.5 and ASP.NET 3.5 are not required.

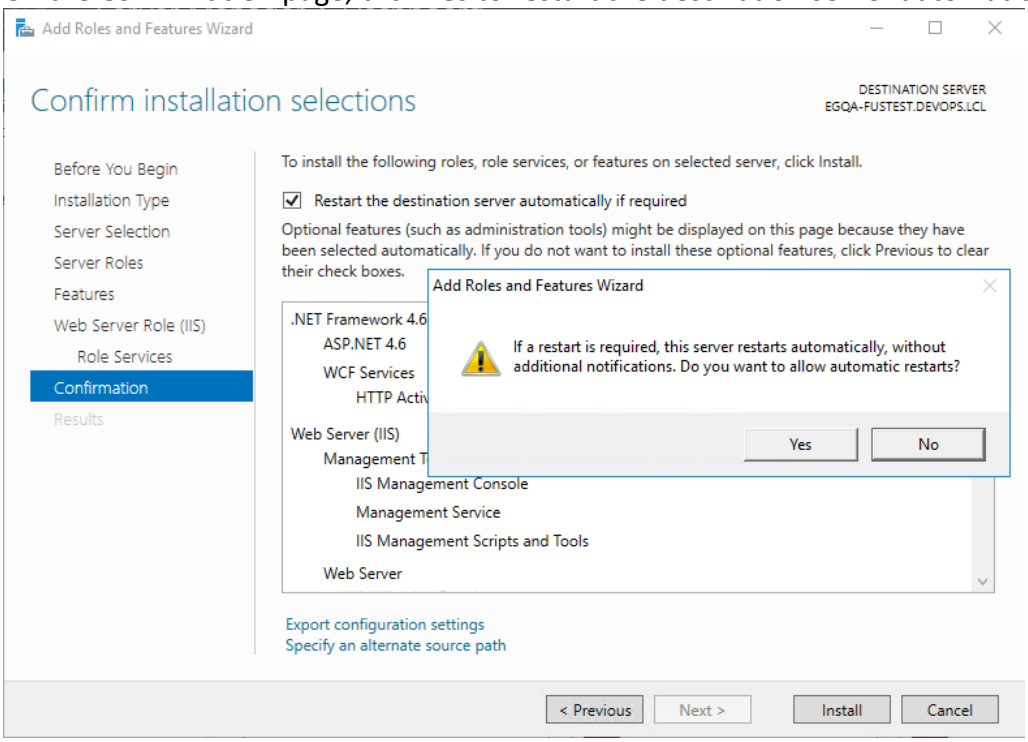
- Roles: **Web Server (IIS) > Management Tools**
    - IIS Management Console
    - IIS Management Scripts and Tools

    IIS 6 Management Compatibility is NOT requrired

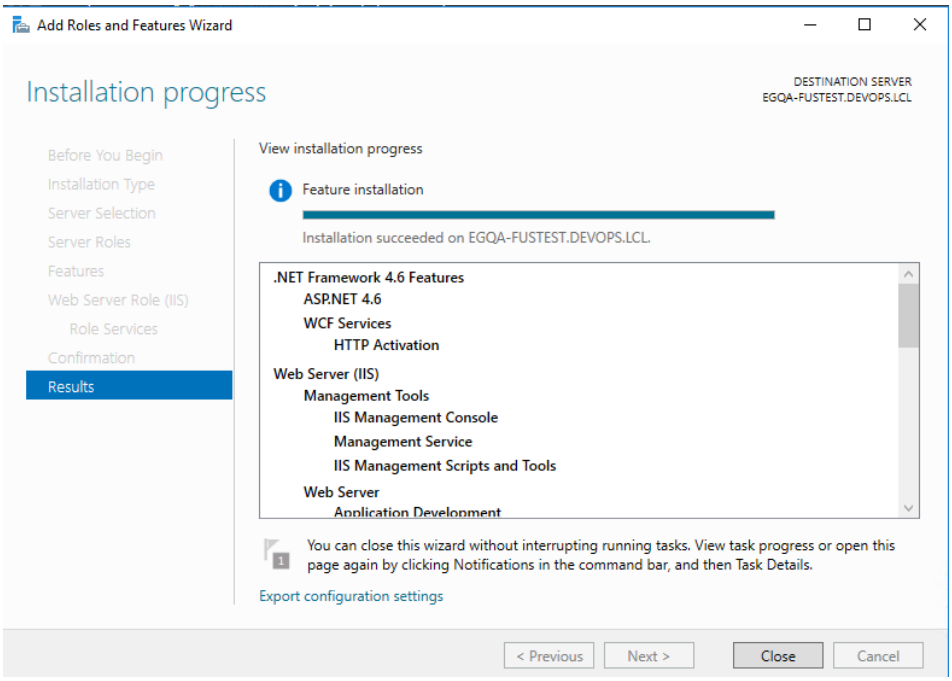


Click **Next** to continue.

On the **Confirmation** page, click **Yes** to restart the destination server automatically if required.



Click **Install.**

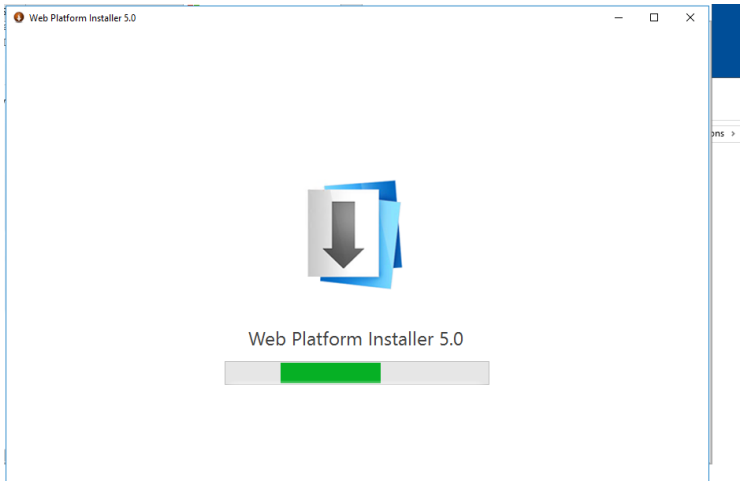


When the installation finishes, click **Close**.

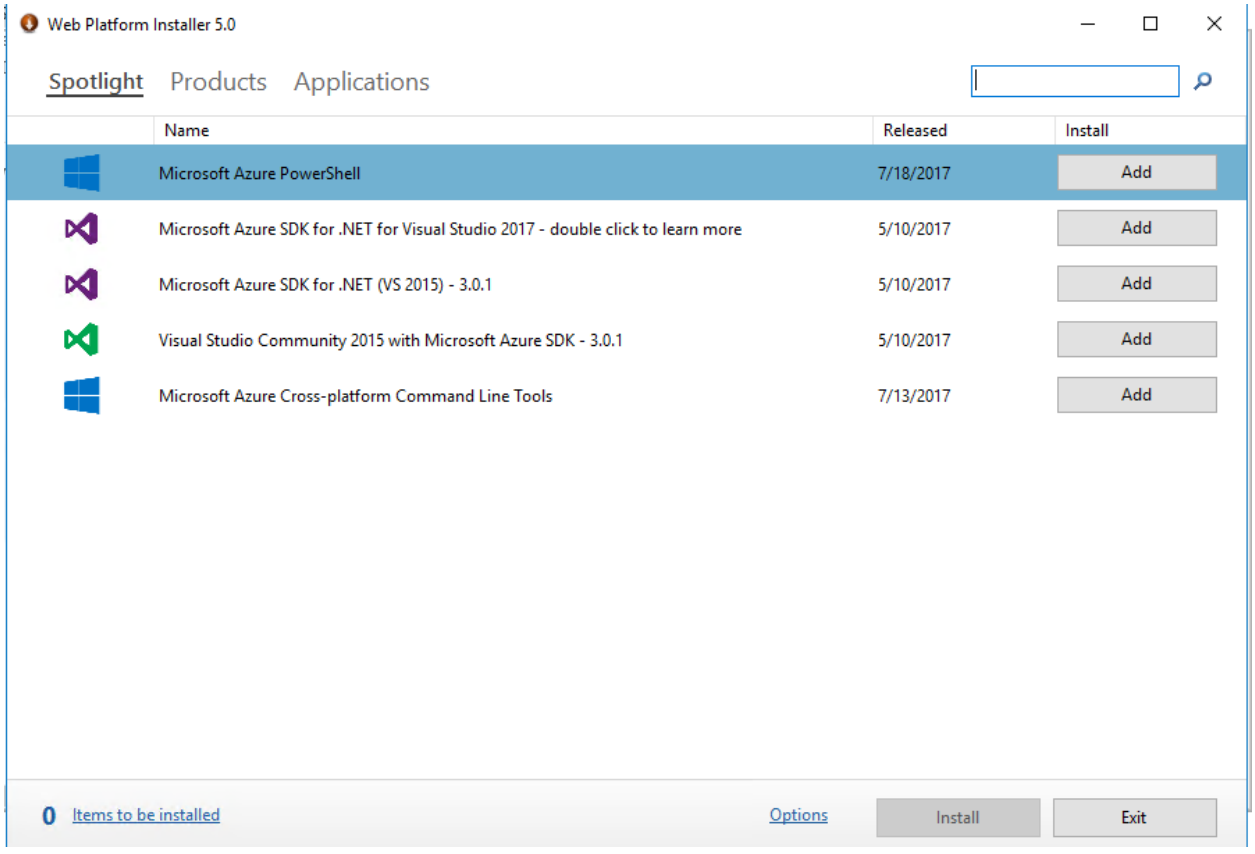
Web Platform Installer

The Web Platform Installer is used to download additional IIS components.

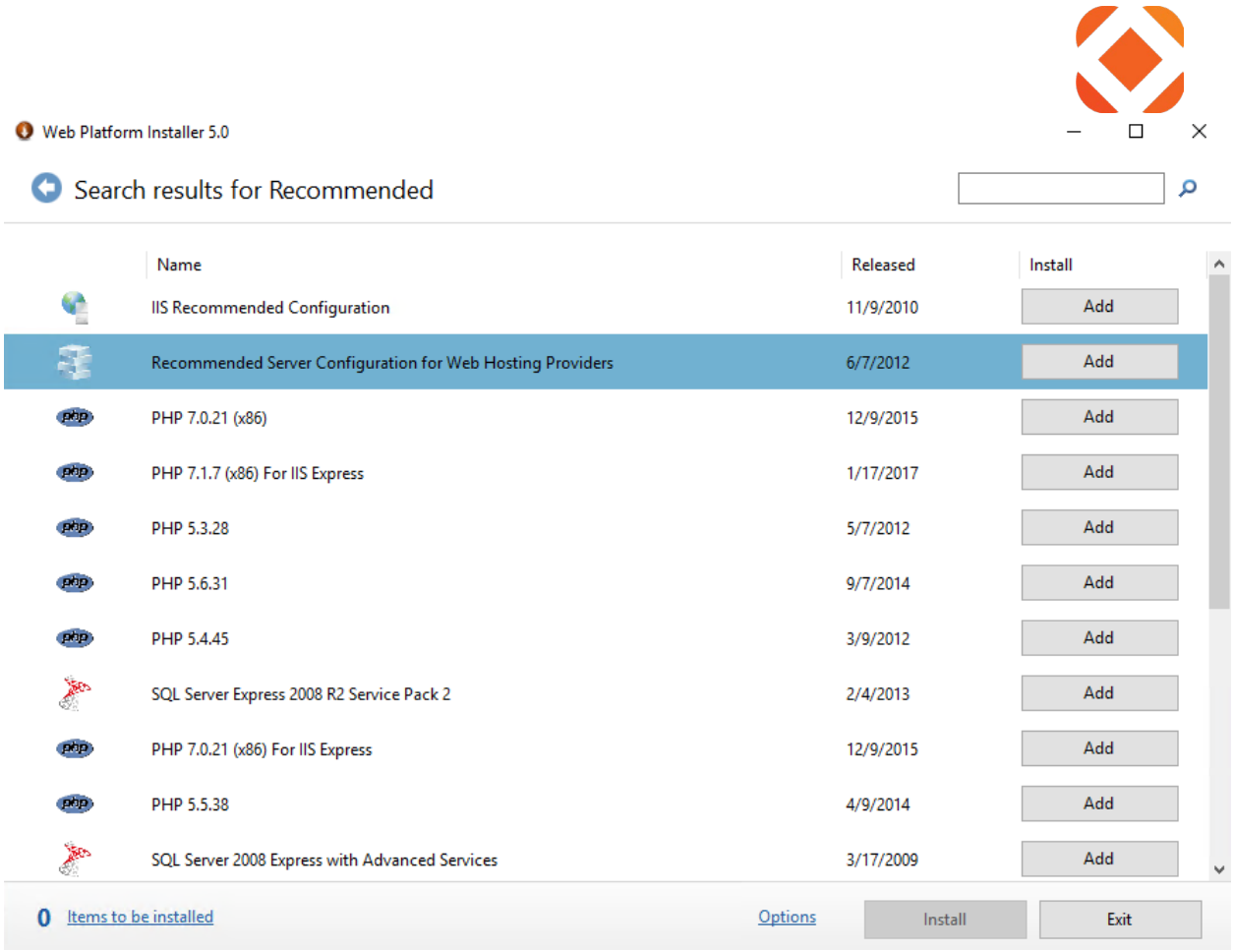
1. Click to download the Web Platform Installer



2. Web Platform Installer will open after installed.



3. Click in the search bar in the upper-right corner, enter “Recommended” in **Search**, and press **Enter**.



4. Select **Recommended Server Configuration for Web Hosting Prov**iders and click **Add**
5. Click **Install**
6. On the Prerequisites page, click **I accept.**

Web Deploy

Web Deploy (msdeploy.exe) is used to deploy web applications to IIS. It is an IIS extension that is downloaded and installed separately. It should be located in one of the folders below if it is installed on your machine.

C:\Program Files\IIS\Microsoft Web Deploy V3\msdeploy.exe
C:\Program Files (x86)\IIS\Microsoft Web Deploy V3\ msdeploy.exe

Use this link to install Web Deploy
https://download.microsoft.com/download/0/1/D/01DC28EA-638C-4A22-A57B-4CEF97755C6C/WebDeploy_amd64_en-US.msi

For more information, go to
https://www.iis.net/downloads/microsoft/web-deploy

URL Rewrite

URL Rewrite is an IIS module used for redirecting http calls to https for OWASP security settings. It needs to be downloaded and installed in IIS through the Web Platform Installer.

Use this link to install URL Rewrite
https://www.iis.net/downloads/microsoft/url-rewrite.

Configure IIS with SSL

To use SSL security, you will need to configure certificates in IIS. The sections below allow you to create a temp certificate to initially set up SSL and test that you can browse to the site using the https protocol. Once you obtain a valid certificate from a CA, you can install the certificate on your IIS server and set it to use SSL only.

CentralSquare supports Symantec/DigiCert certificates. Extended Validation (EV) certificates are not required. Pricing can be found here:
https://www.digicert.com/compare-and-buy-ssl-certificates/

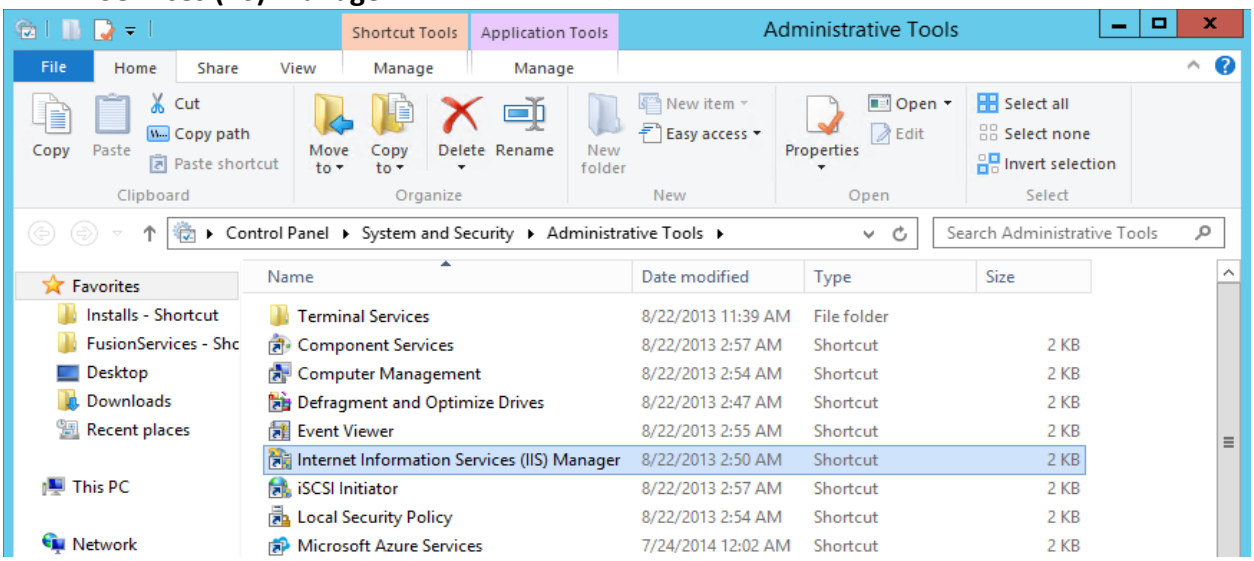
The Fusion installer will create the FusionServices under the Default Web Site. It will use the http / https settings from the Default Web Site. You can configure the SSL settings before or after installing Fusion.

Click the link below for the latest instructions on how to create a SSL Certificate for IIS.
http://www.iis.net/learn/manage/configuring-security/how-to-set-up-ssl-on-iis

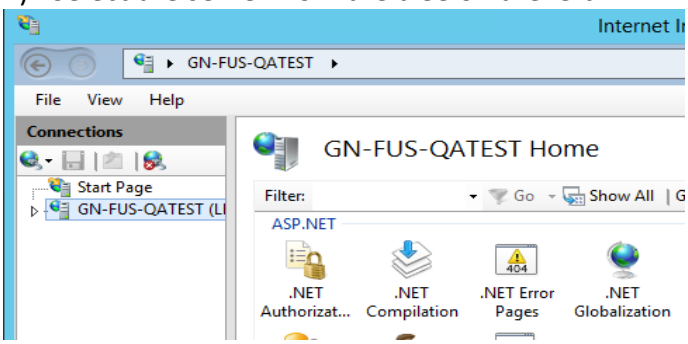
Create a temp certificate

These steps create a temporary SSL certificate so you can set up SSL and test it locally.

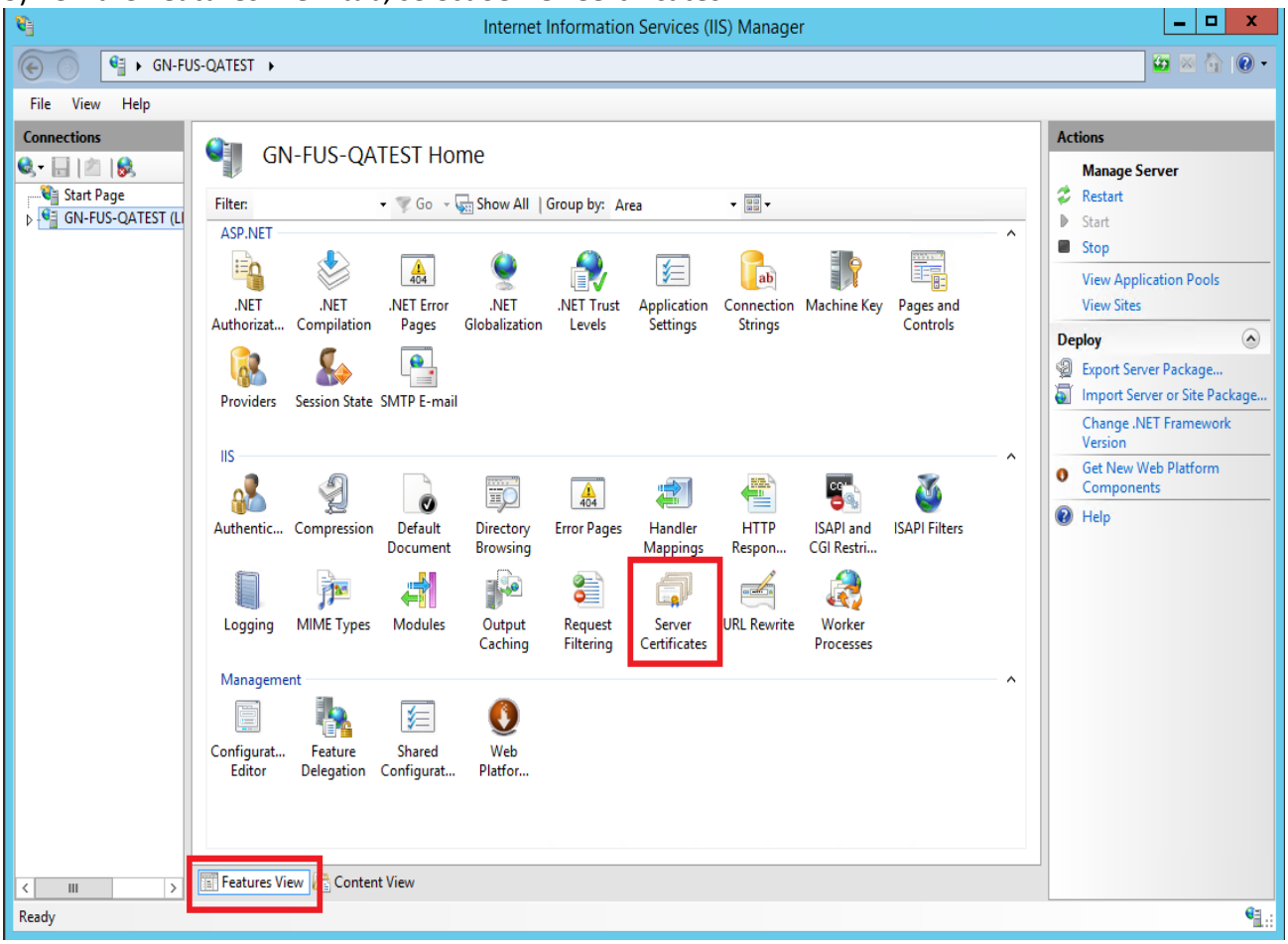
1) Open IIS Manager
   a) **Start** > **Control Panel** > **System Security** > **Administrative Tools > Internet Information Services (IIS) Manager**



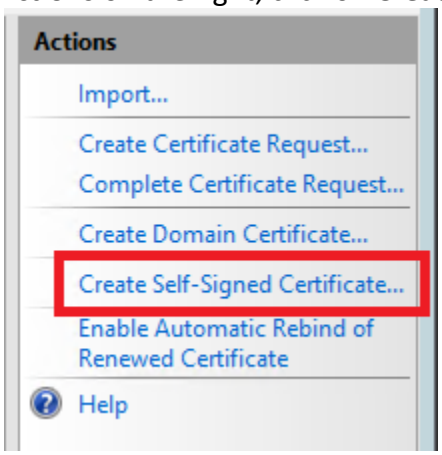
2) Select the server from the tree on the left



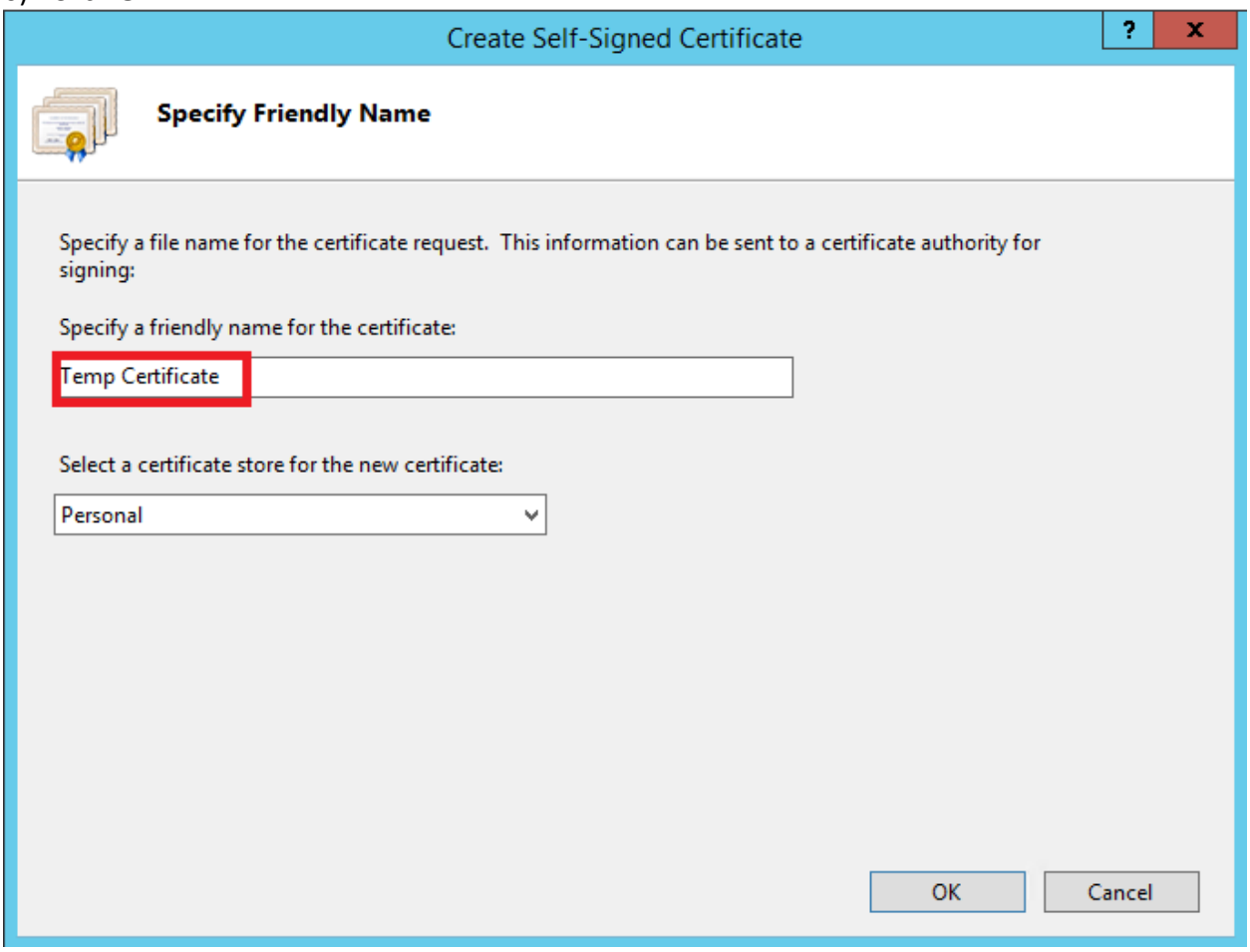
3) On the **Features View** tab, select **Server Certificates**



4) Under **Actions** on the right, click on **Create Self-Signed Certificate**



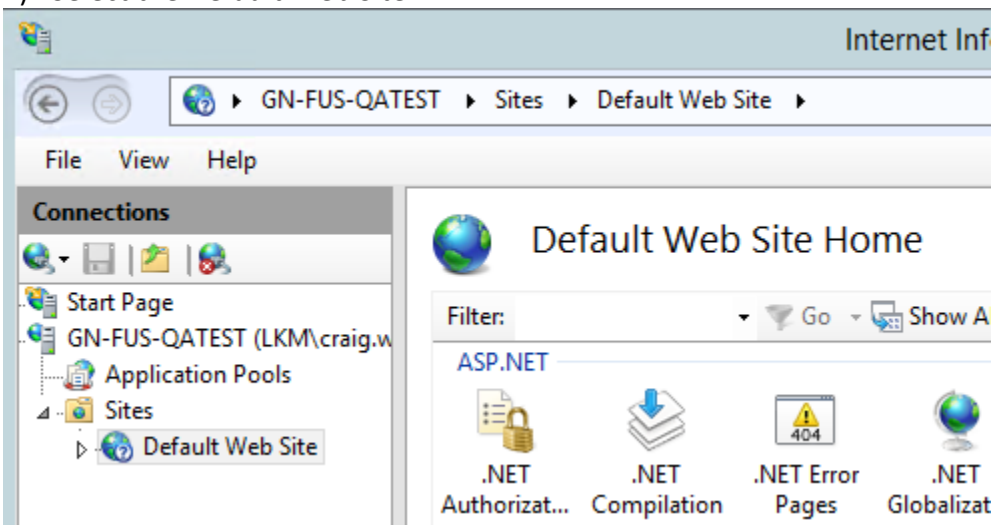
5) Give the certificate a **name**, such as Temp Certificate.
6) Click **OK**.



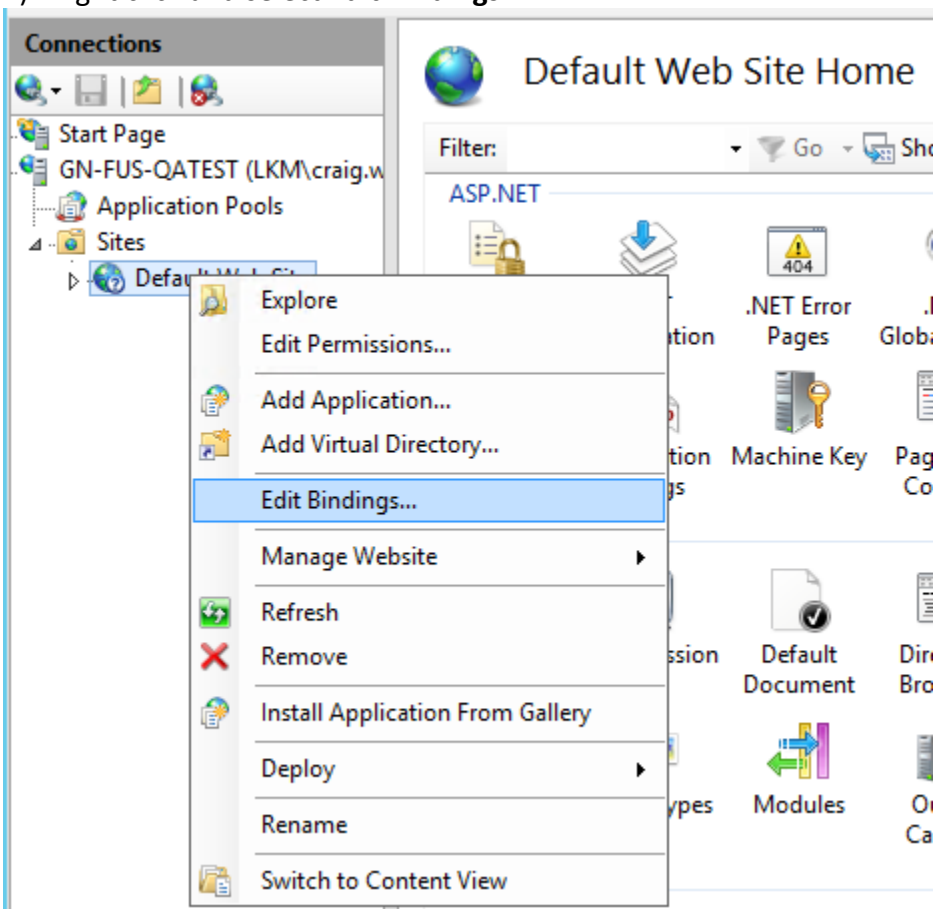
Add Https Binding

These steps tell the IIS Manager to accept URLs using the https protocol.

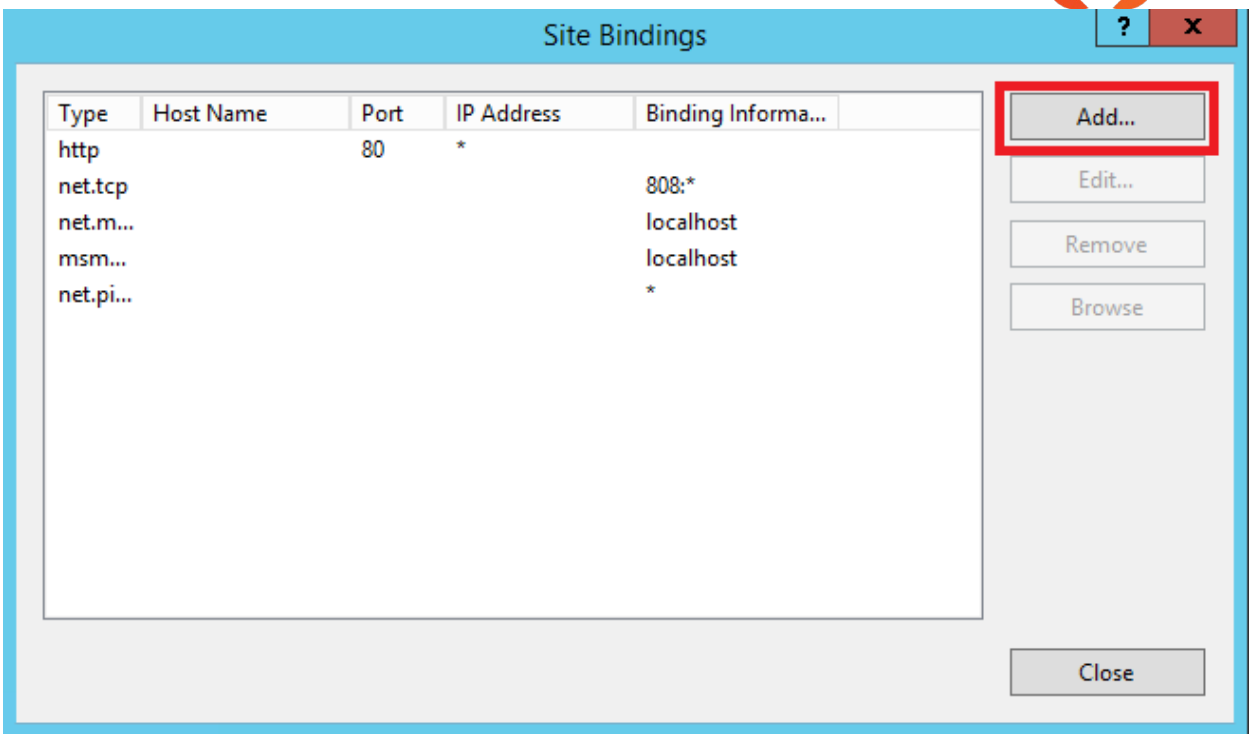
1) Select the Default Web Site



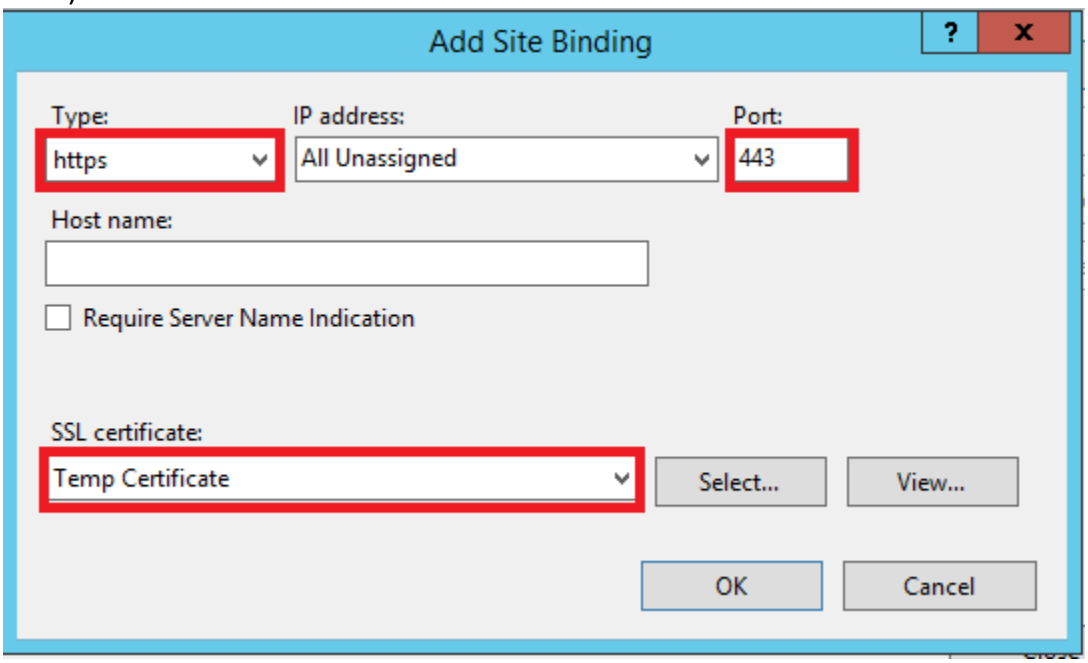
2) Right click and select **Edit Bindings…**



3) On the **Site Bindings** dialog, click **Add**.



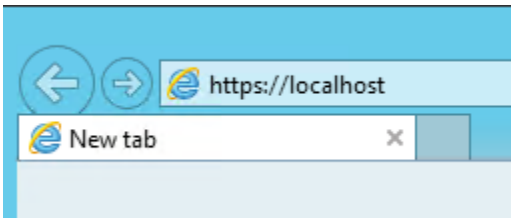
4) In the **Add Site Binding** dialog
   a) Set the **Type** to **https**
   b) You can leave the **Port** number as the default of 443 or change it to a different port number
   c) Select the temp certificate you added in the steps above.
   d) Click OK



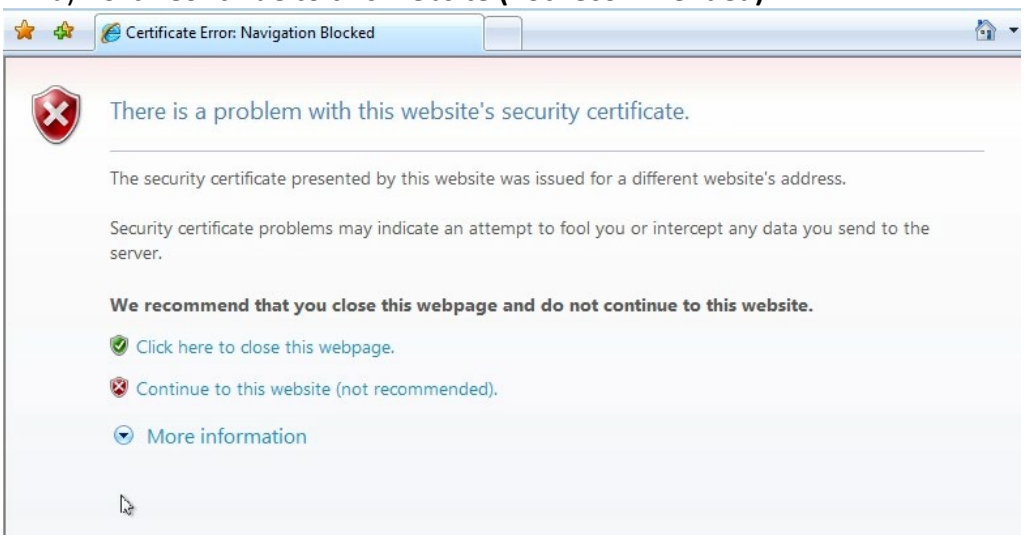
Test the https://localhost URL

You can now test the localhost URL using https to validate the SSL connection.

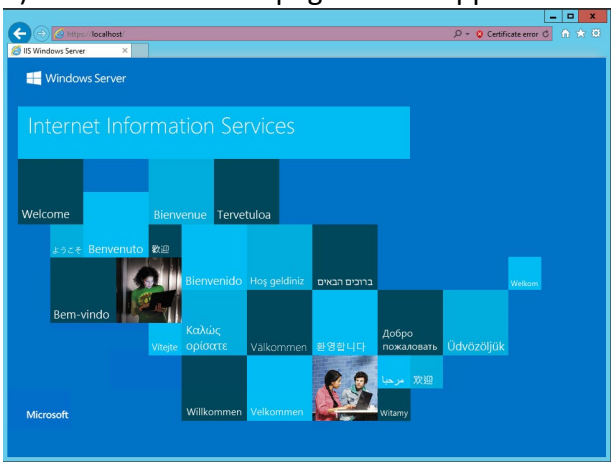
1) In Internet Explorer or other web browser, enter https://localhost into the address bar.



2) It will come up with a page showing a certificate error. This is because it is using a temporary certificate and not one from an authorized certificate authority (CA).
   a) Click **Continue to this website (not recommended)**



3) The IIS Welcome page should appear



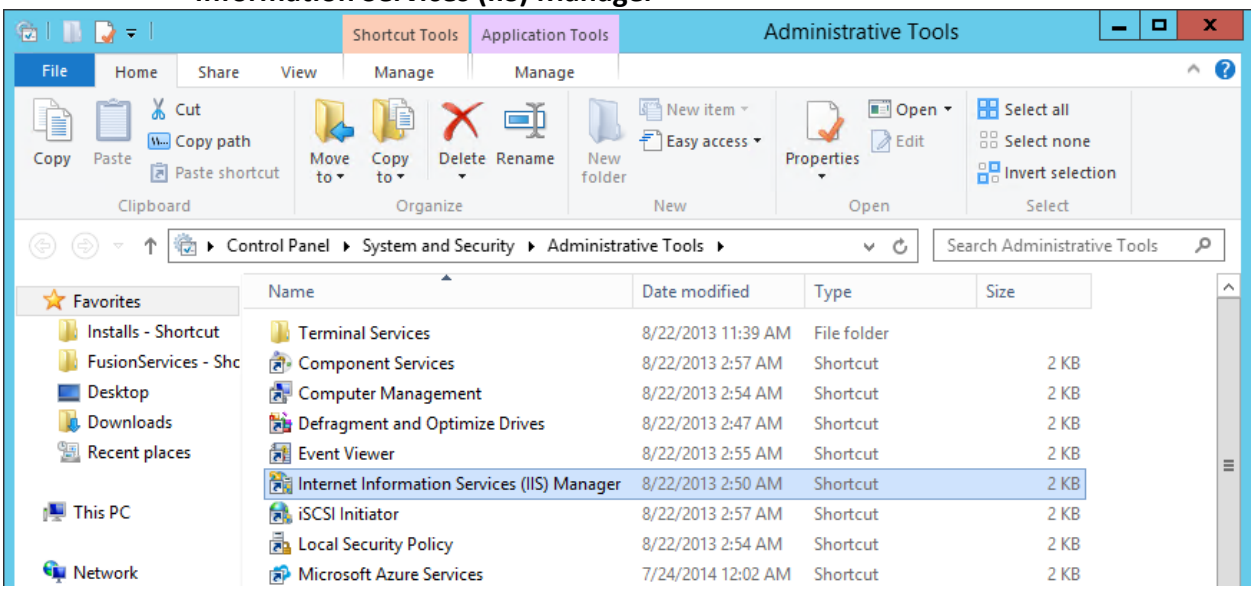
Domain name

This is your domain name as it will appear in the URL to your site, and used in your SSL Certificate. Do not include https or www. Example: Fusion.myCity.gov.

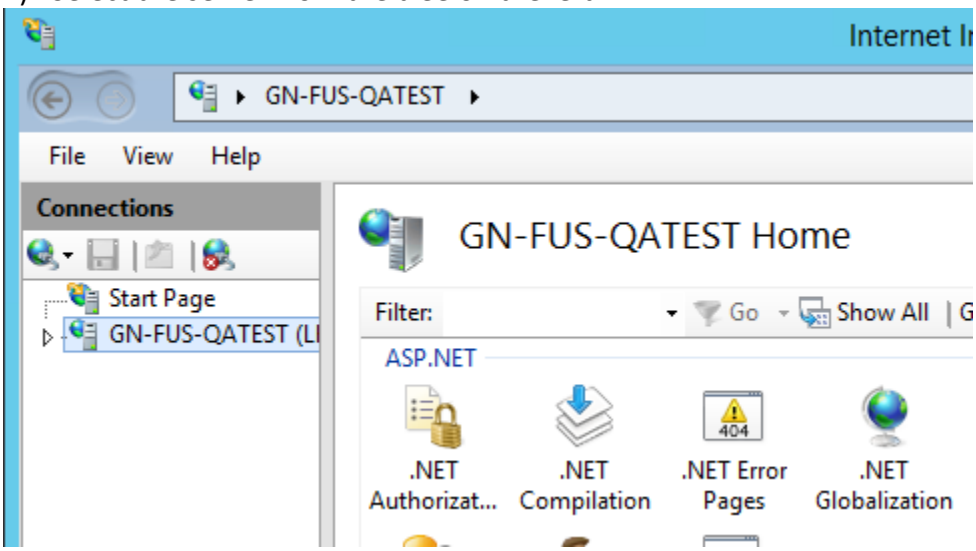
Request an Internet Server Certificate

These are the steps to request a certificate from a CA vendor.
The latest steps for this process can be found online at:
https://technet.microsoft.com/en-us/library/cc732906(v=ws.10).aspx

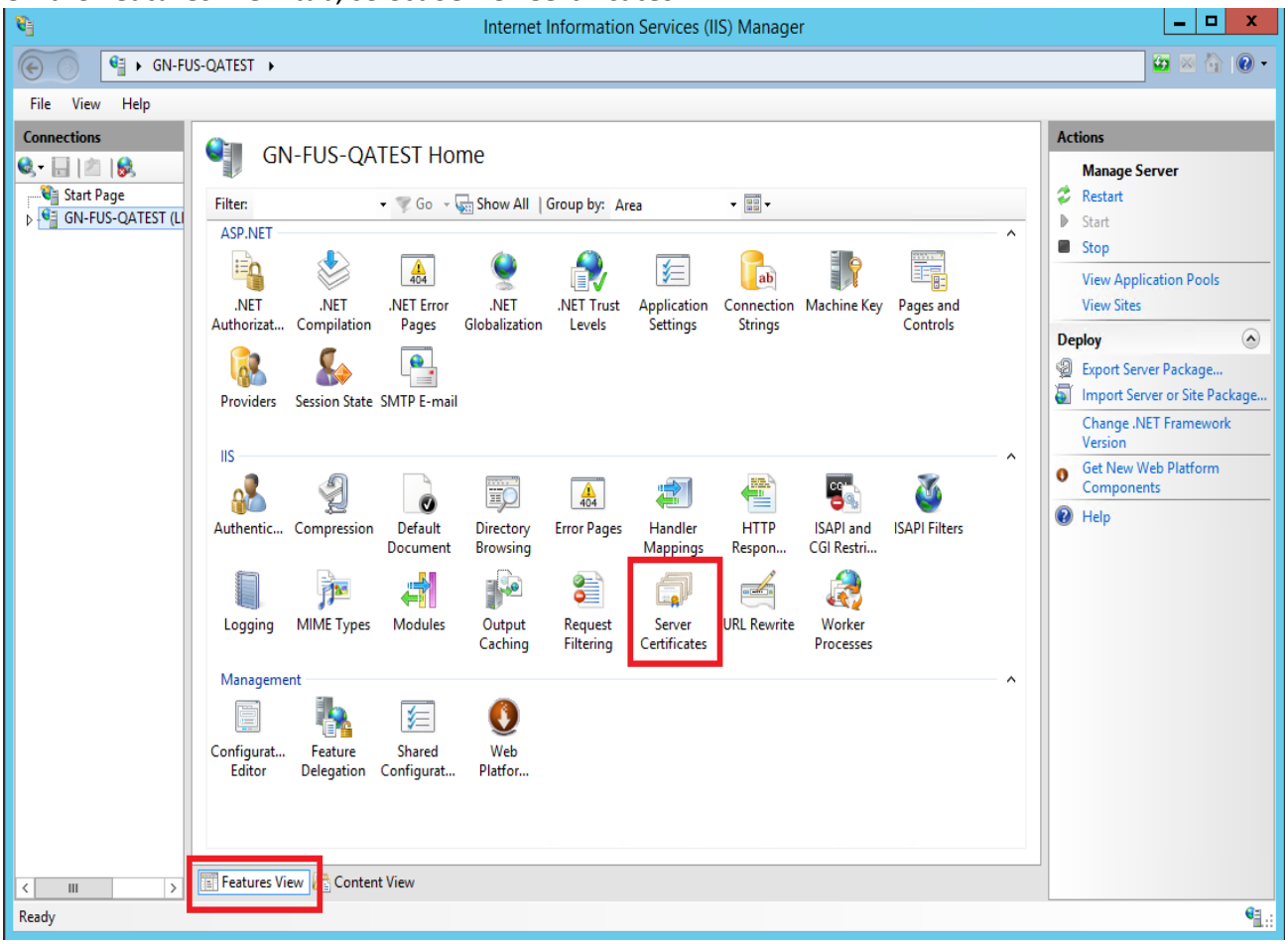
1) Open IIS Manager
   a) **Start** > **Control Panel** > **System Security** > **Administrative Tools** > **Internet Information Services (IIS) Manager**



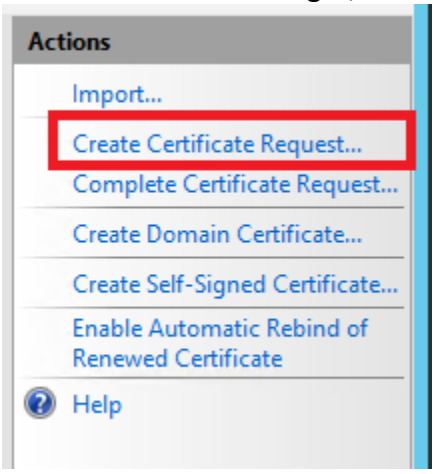
2) Select the server from the tree on the left



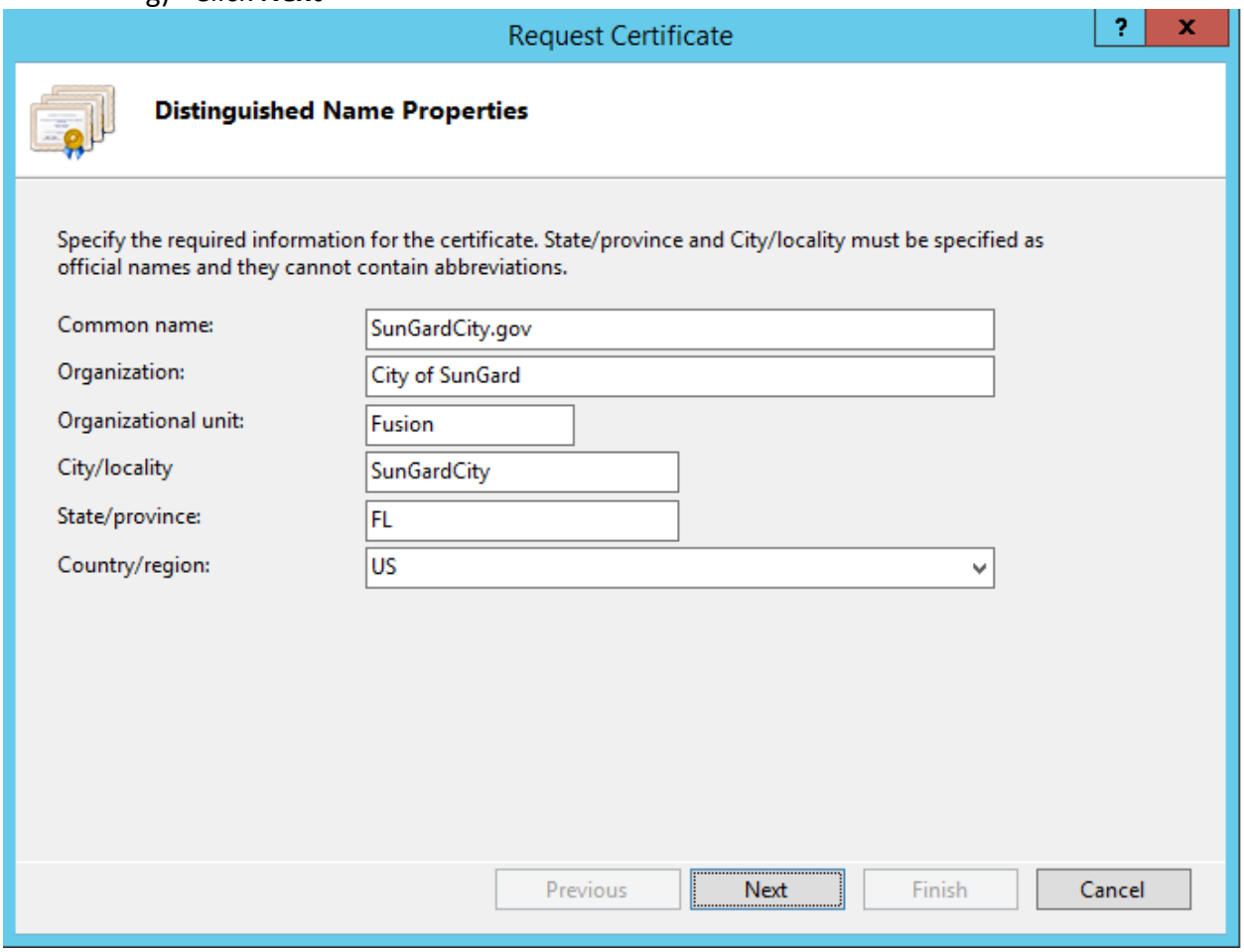
On the **Features View** tab, select **Server Certificates**



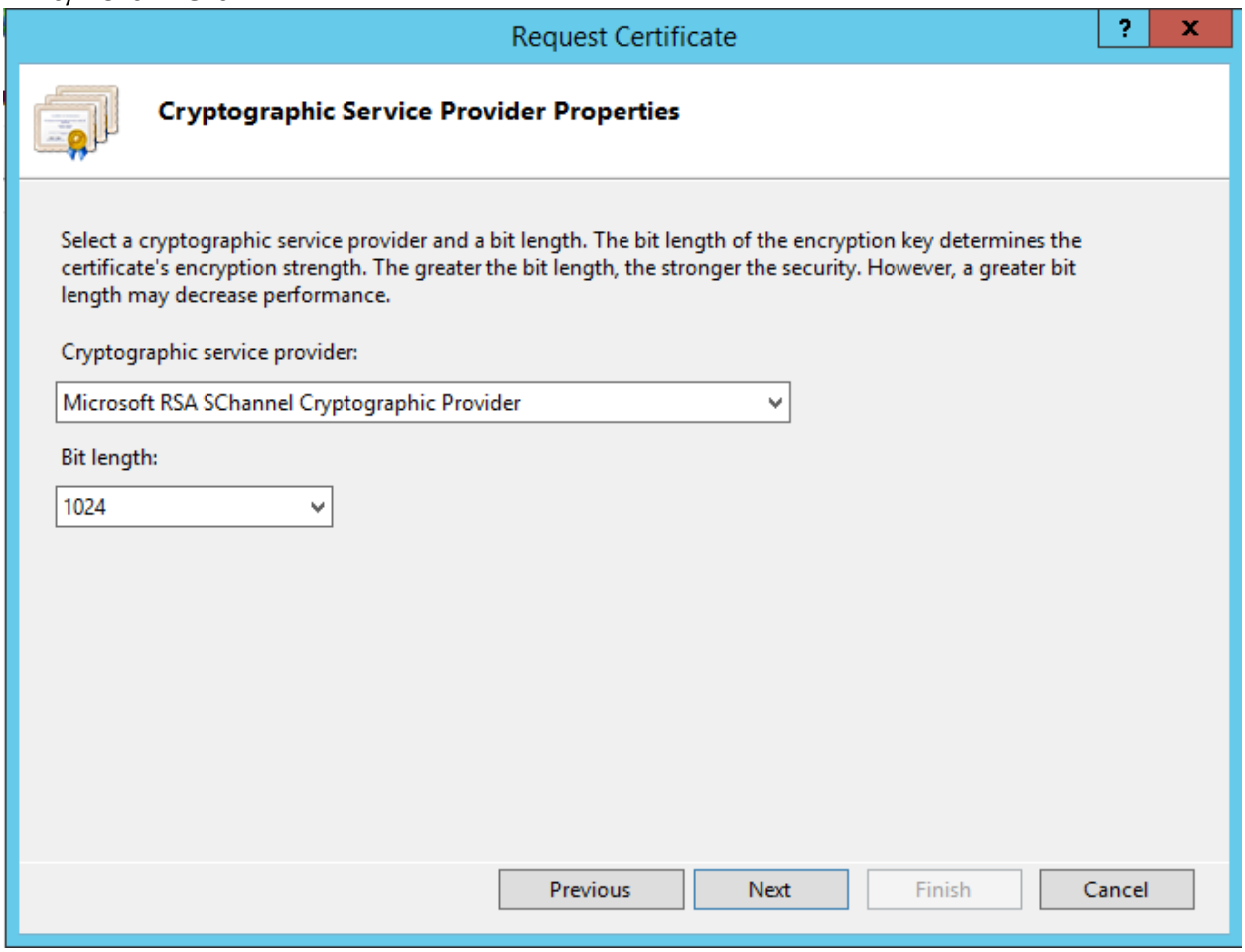
3) Under **Actions** on the right, click on **Create Certificate Request**



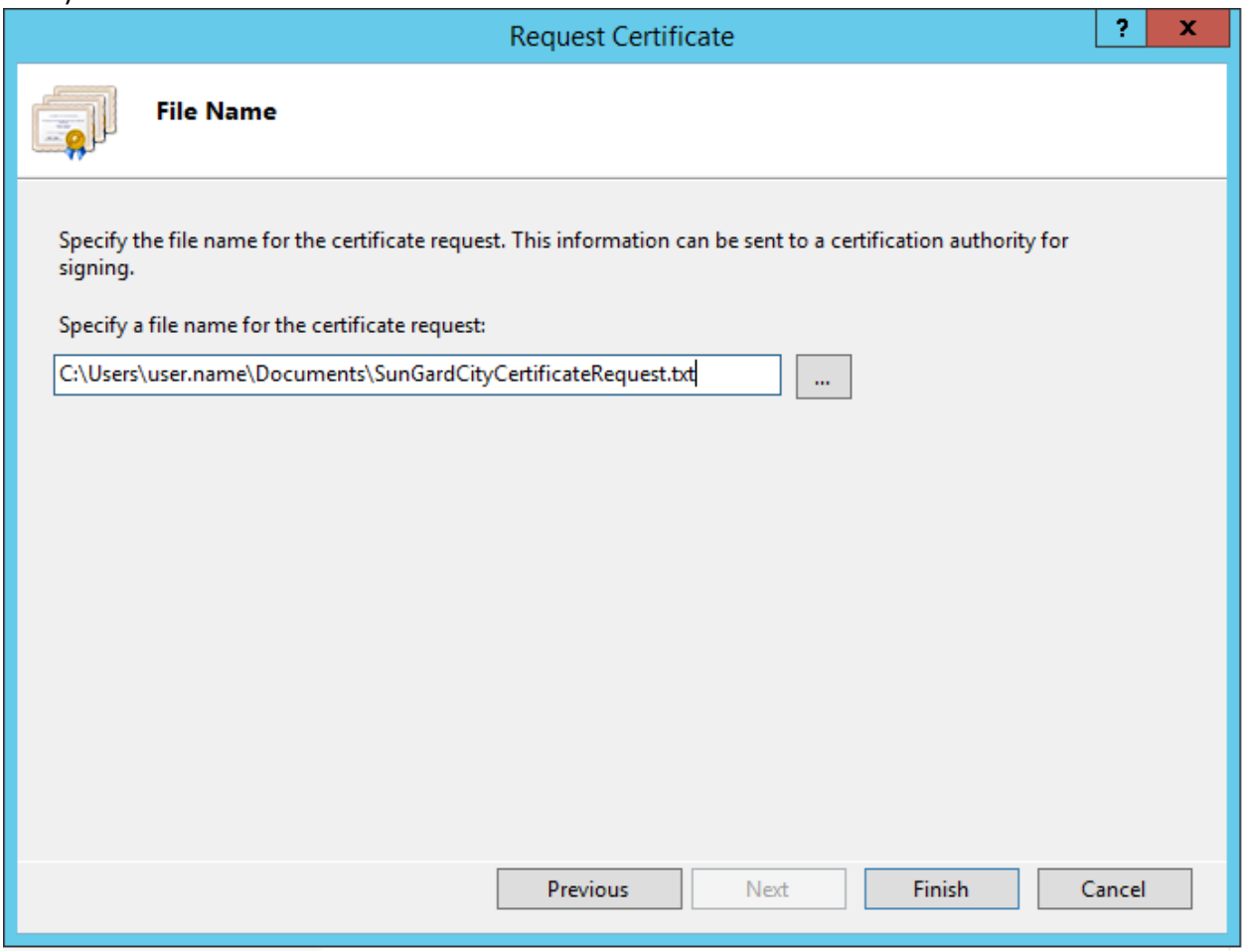
4) On the **Distinguished Name Properties** page of the **Request Certificate** wizard, type the following information, and then click **Next**.
   a) In the **Common name** text box, type in your domain name as it will appear in the URL to your site. Do not include https or www.
   b) In the **Organization** text box, type the name of the organization in which the certificate will be used.
   c) In the **Organizational unit** text box, type the name of the organizational unit in the organization in which the certificate will be used.
   d) In the **City/locality** text box, type the unabbreviated name of the city or locality where your organization or organizational unit is located.
   e) In the **State/province** text box, type the name of the state or province where your organization or organizational unit is located.
   f) In the **Country/region** text box, type the name of the country or region where your organization or organizational unit is located.
   g) Click **Next**



5) On the **Cryptographic Service Provider Properties** page
   a) select either **Microsoft RSA SChannel Cryptographic Provider** or **Microsoft DH SChannel Cryptographic Proveder** from the **Cryptographic service provider** drop-down list. By default, IIS 7 uses the Microsoft RSA SChannel Cryptographic Provider.
   b) In the **Bit length** drop-down list, select a bit length that can be used by the provider. By default, the RSA SChannel provider uses a bit length of 1024. The DH SChannel provider uses a bit length of 512. A longer bit length is more secure, but it can affect performance.
   c) Click **Next**



6) On the File Name page, type in a file name or click the browse button (…) to locate a file.
   a) Selecting your Documents folder to save it to will ensure you have permission to write the file to the folder.
   b) Use the .txt extension to save it as a plain text file. The information will be encrypted within the text file, but will allow you to copy and paste the information when sending it to the certificate authority (CA).
   c) Click **Finish**



7) Send the certificate request to a public CA

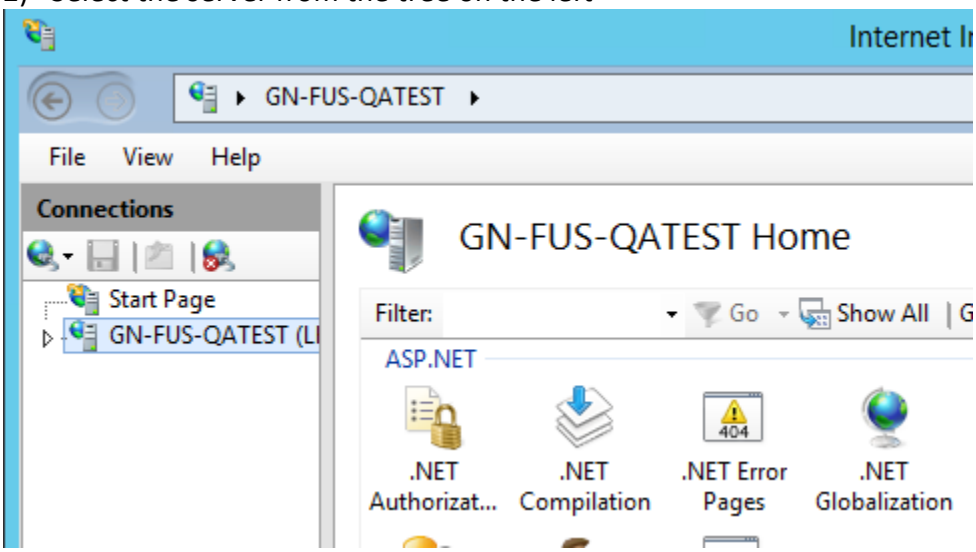
Install an Internet Server Certificate

When you receive a response from a public certification authority (CA) to whom you sent a certificate request, you must complete the process by installing the server certificate on your web server. You can install the server certificate only on the computer from which you sent the certificate request.

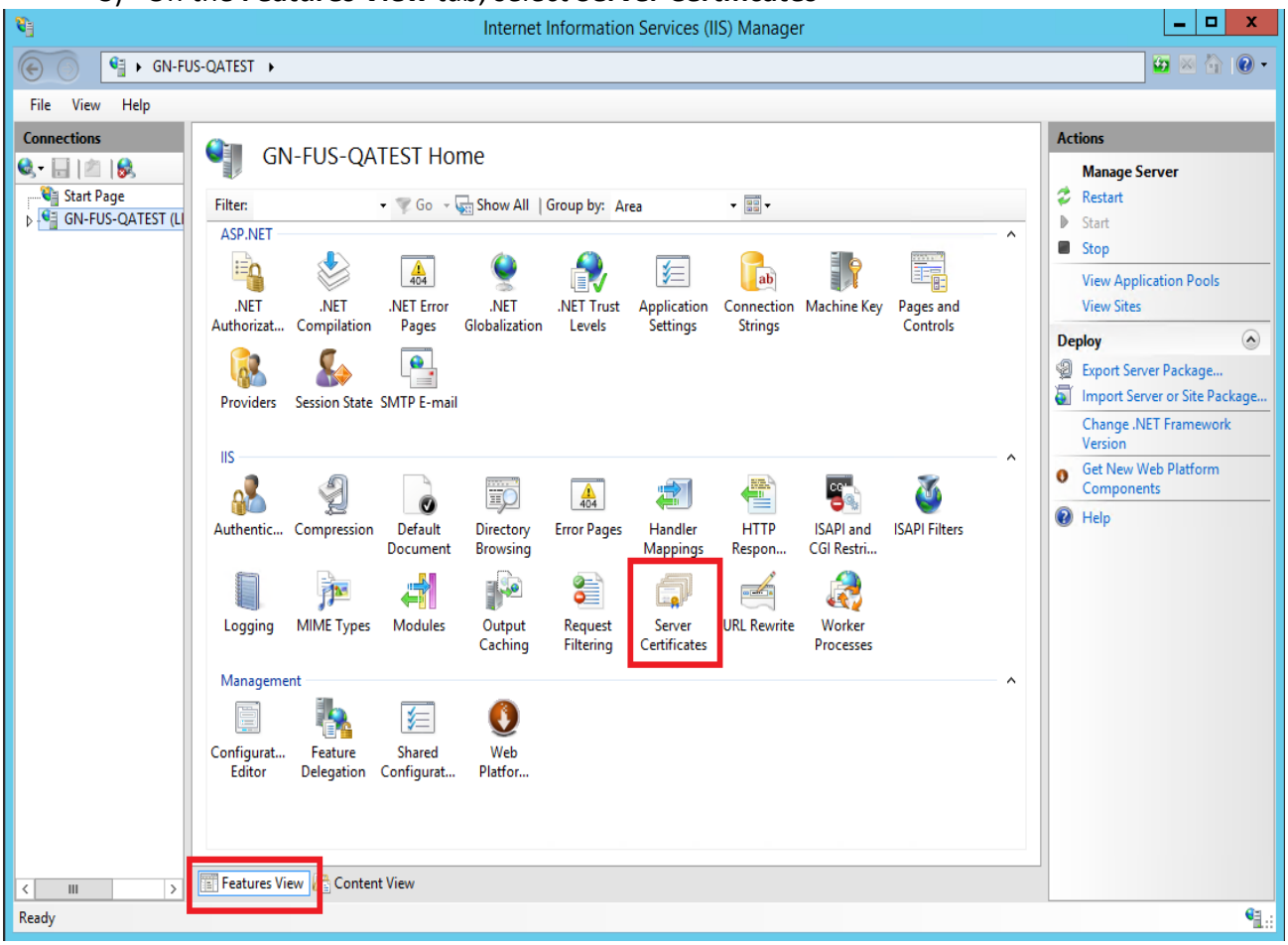
The latest steps for this process can be found online at:
https://technet.microsoft.com/en-us/library/cc771816(v=ws.10).aspx

1) Open IIS Manager
   a) **Start** > **Control Panel** > **System Security** > **Administrative Tools > Internet Information Services (IIS) Manager**

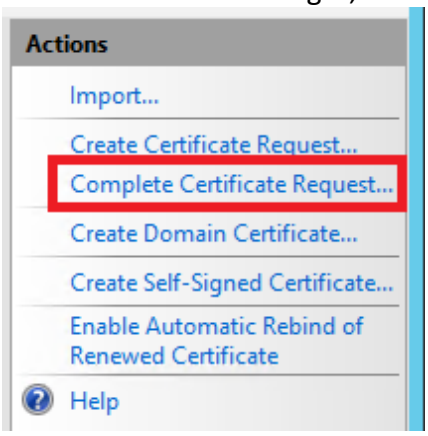
2) Select the server from the tree on the left



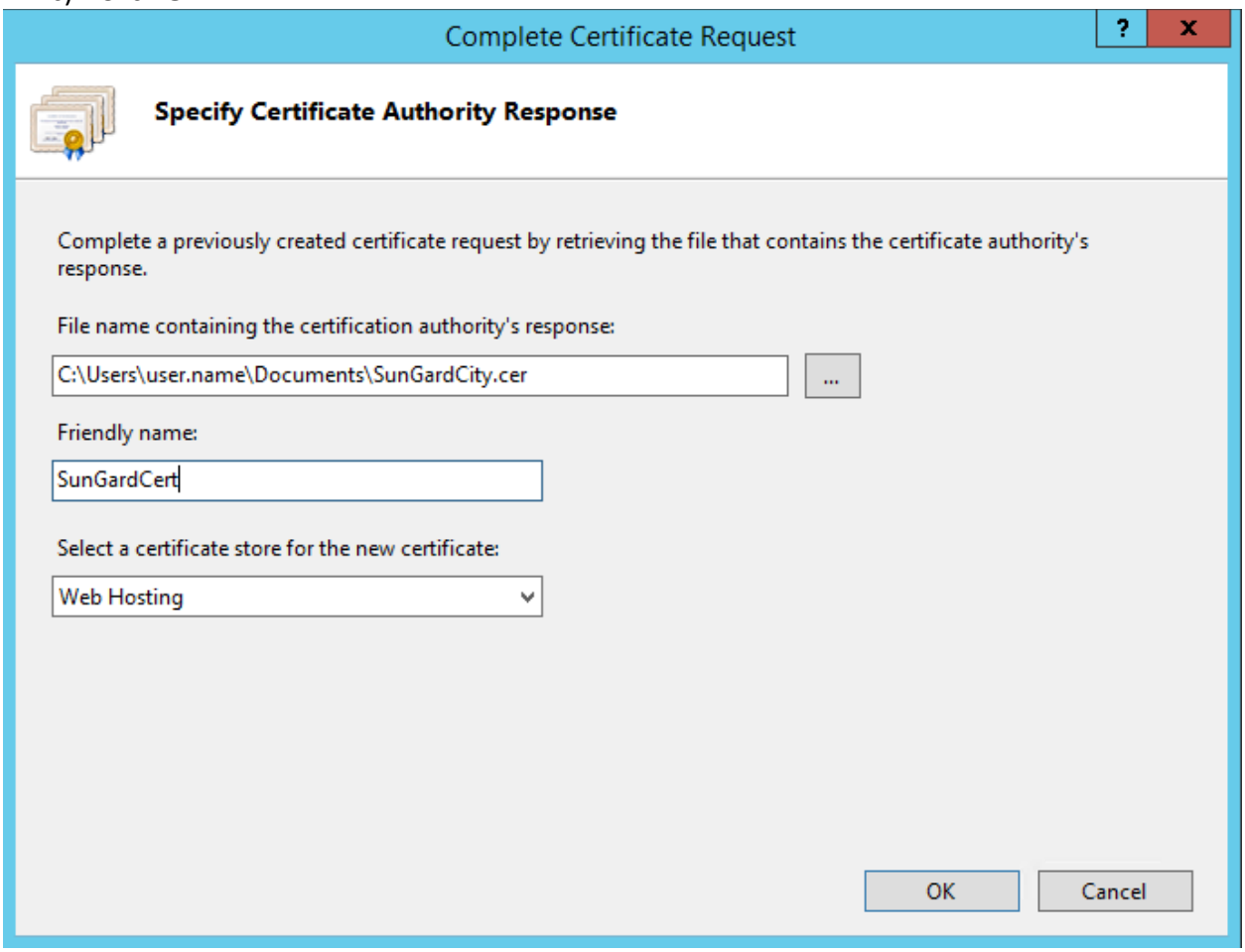
3) On the **Features View** tab, select **Server Certificates**



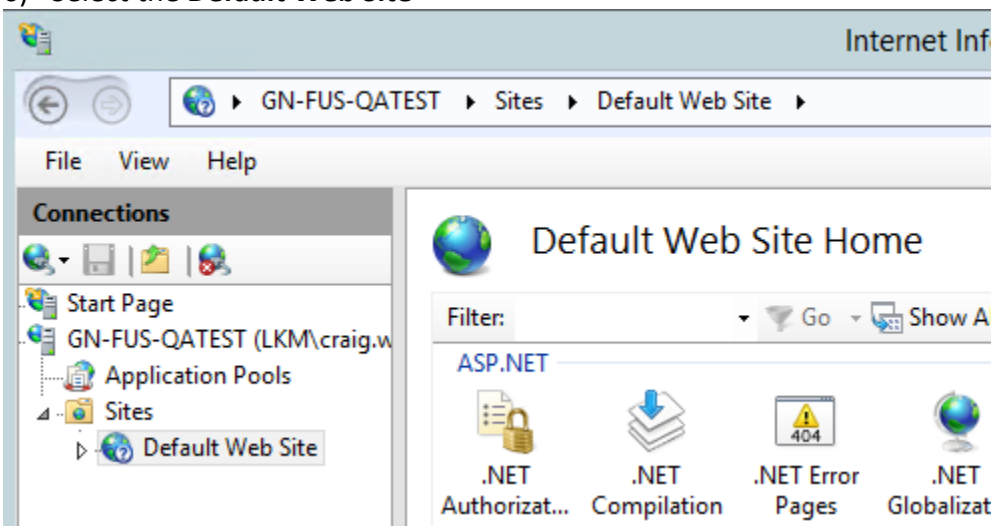
4) Under **Actions** on the right, click on **Create Certificate Request**



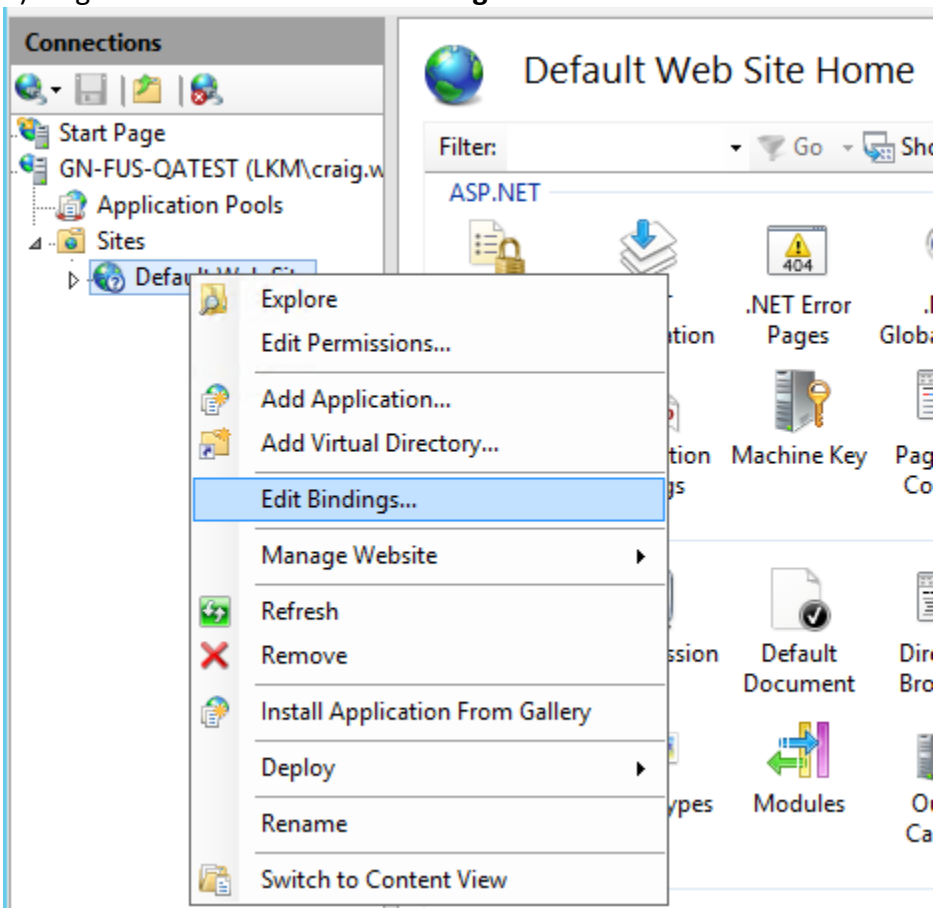
5) On the **Complete Certificate Request** page,
   a) In the **File name containing the certification authority's response** text box, click the browse button (…) to select the response file from the CA.
   b) Type a friendly name for the certificate in the **Friendly name** text box
   c) Click **OK**.



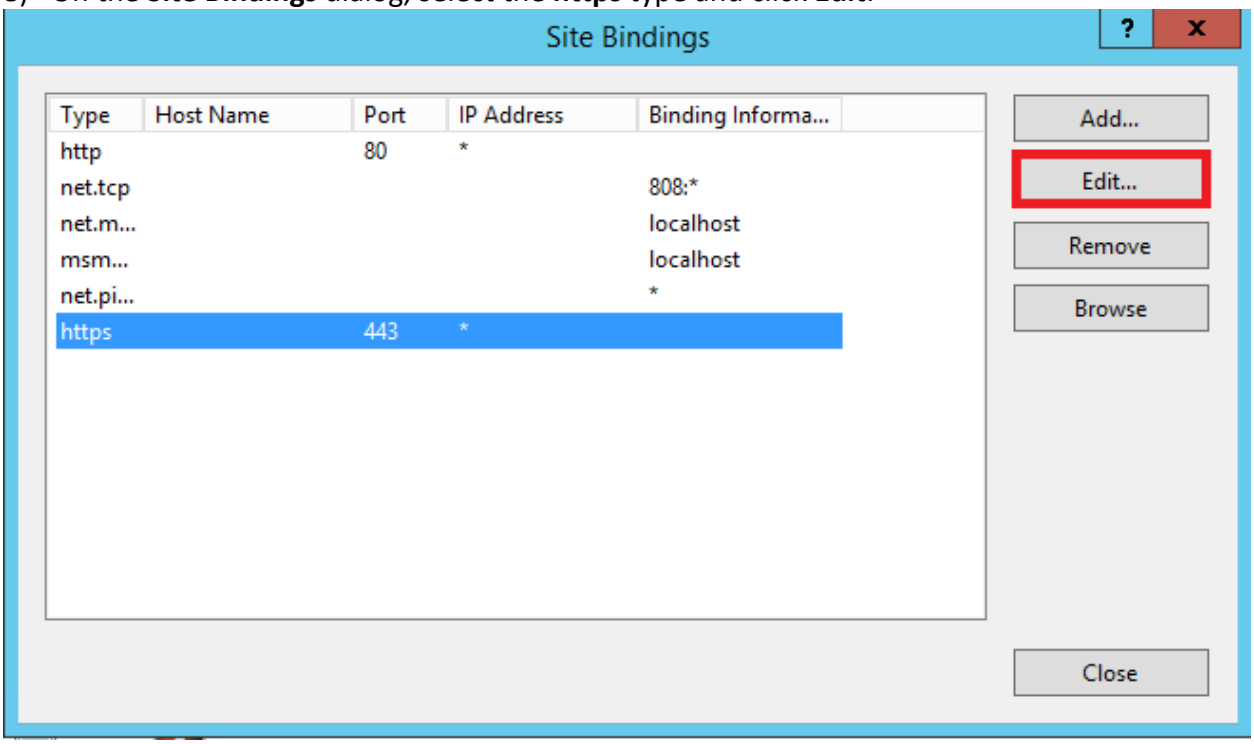
6) Select the **Default Web Site**



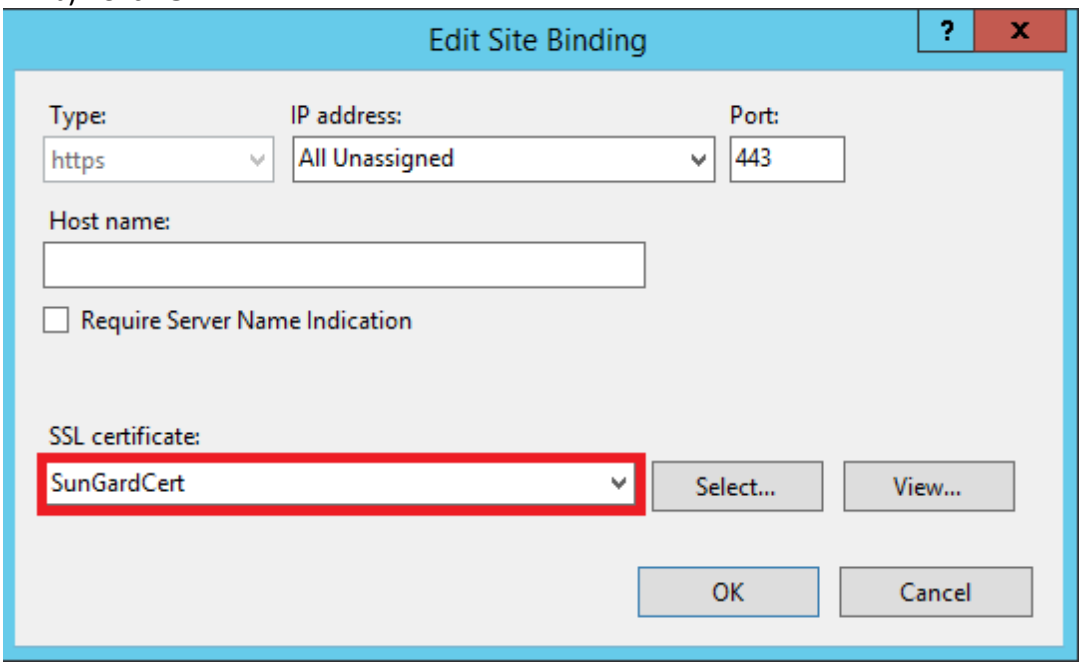
7) Right click and select **Edit Bindings…**



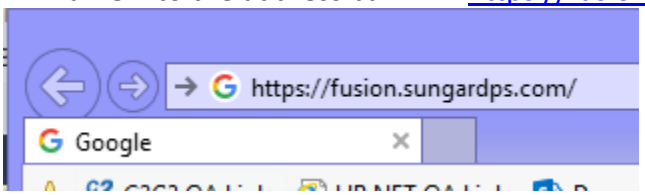
8) On the **Site Bindings** dialog, select the **https** type and click **Edit**.



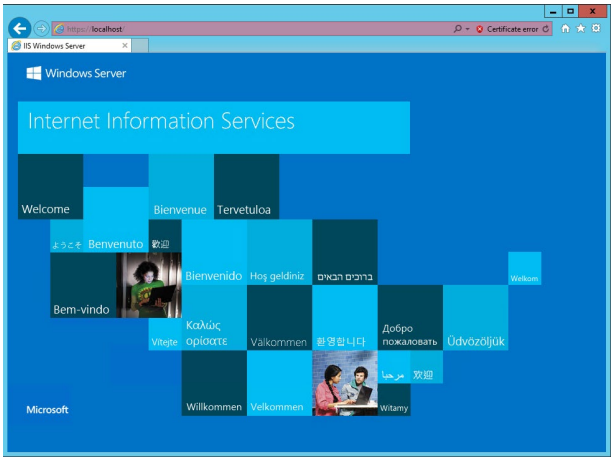
9) In the **Edit Site Binding** dialog
   a) Select the certificate you added in the steps above.
   b) Click **OK**



10) In Internet Explorer or other web browser, enter https:// followed by your domain name into the address bar. Ex. https://fusion.myCity.com

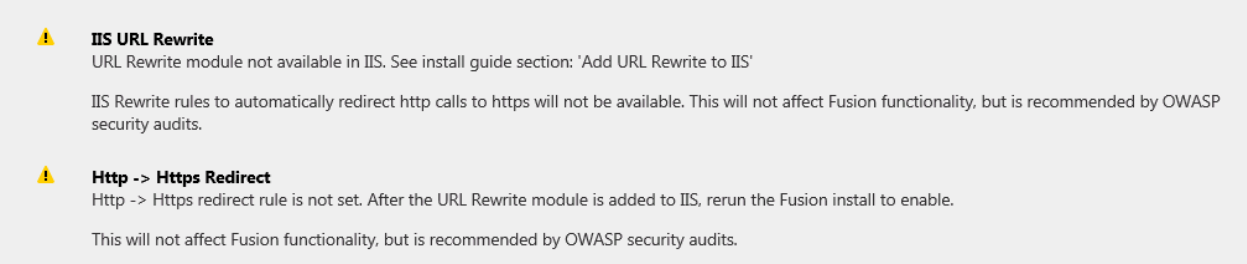


11) The IIS Welcome page should appear without a waning about the website's security certificate.



Add URL Rewrite to IIS

URL Rewrite allows the Fusion service to force a redirect from http to https. This is required for OWASP security compliance. If this is not installed, Fusion functionality will not be affected, but the Fusion diagnostics page will show a warning under HTTPS Security.

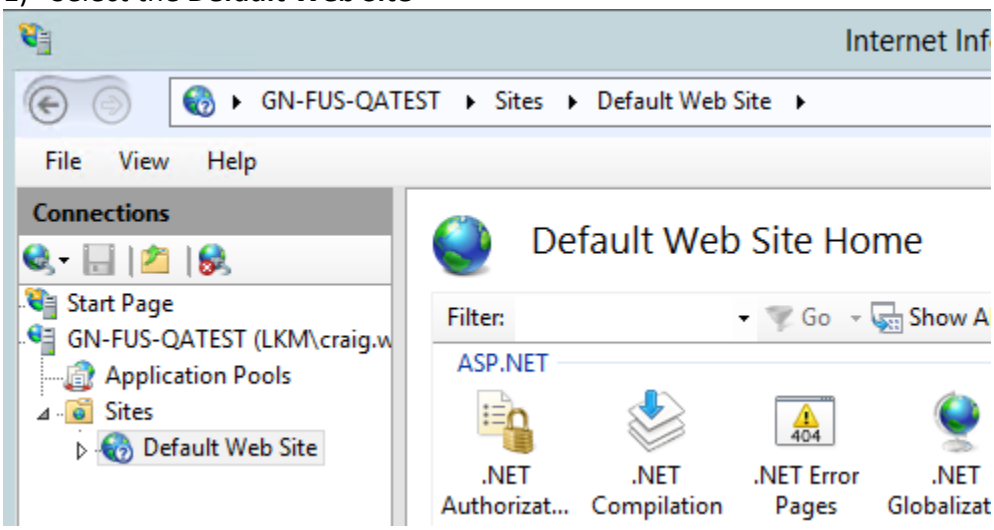


URL Rewrite is an IIS module that needs to be downloaded and installed through the IIS Web Platform installer. See the sections ***Use Web Platform Installer to install Web Deploy*** for adding URL Rewrite into IIS

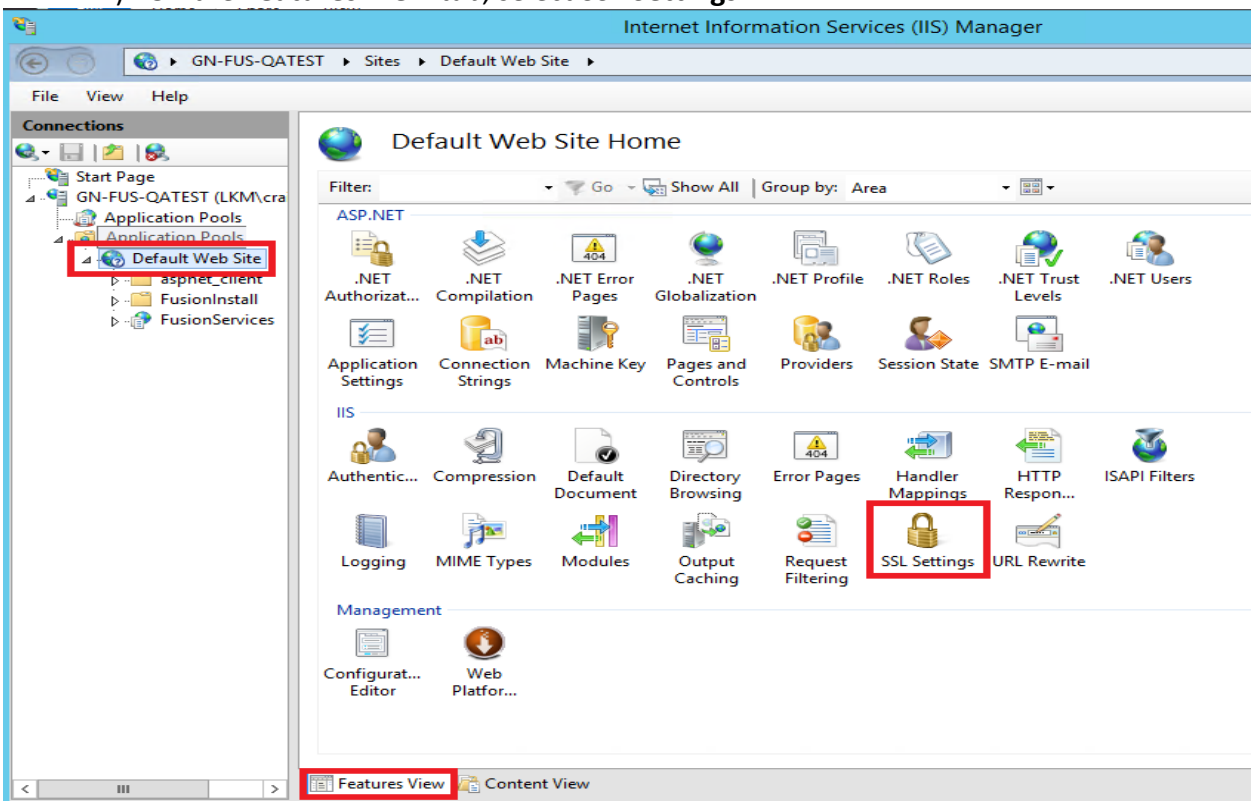
Set IIS to use SSL only

Once you are done testing your site and have a valid CA certificate, you can set IIS to only use the https protocol, and disable the http protocol.

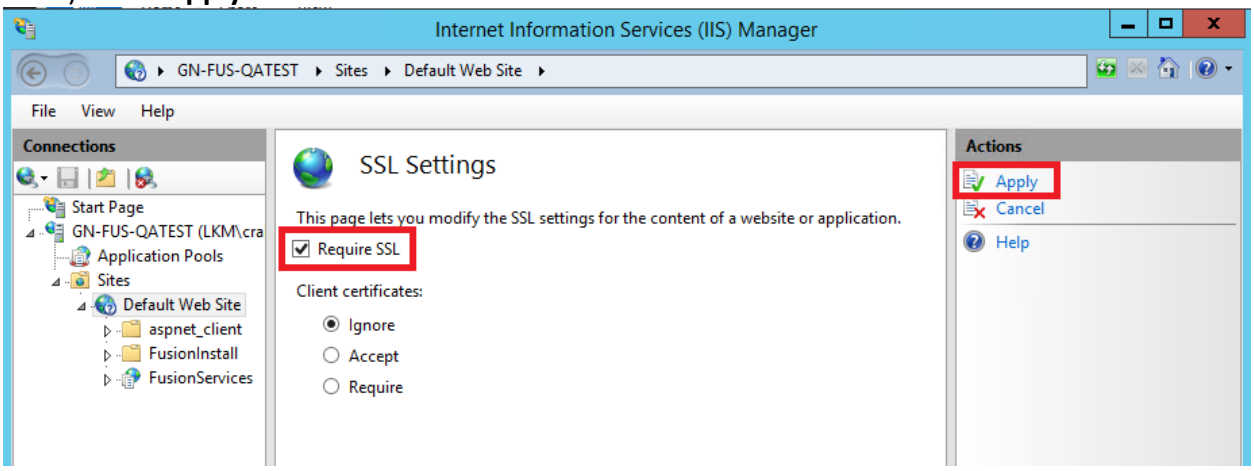
1) Select the **Default Web Site**



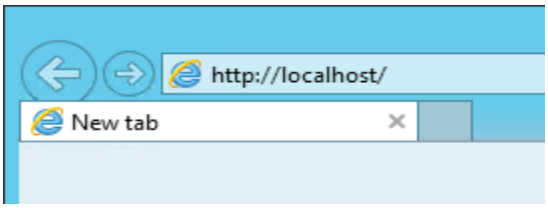
2) On the **Features View** tab, select **SSL Settings**



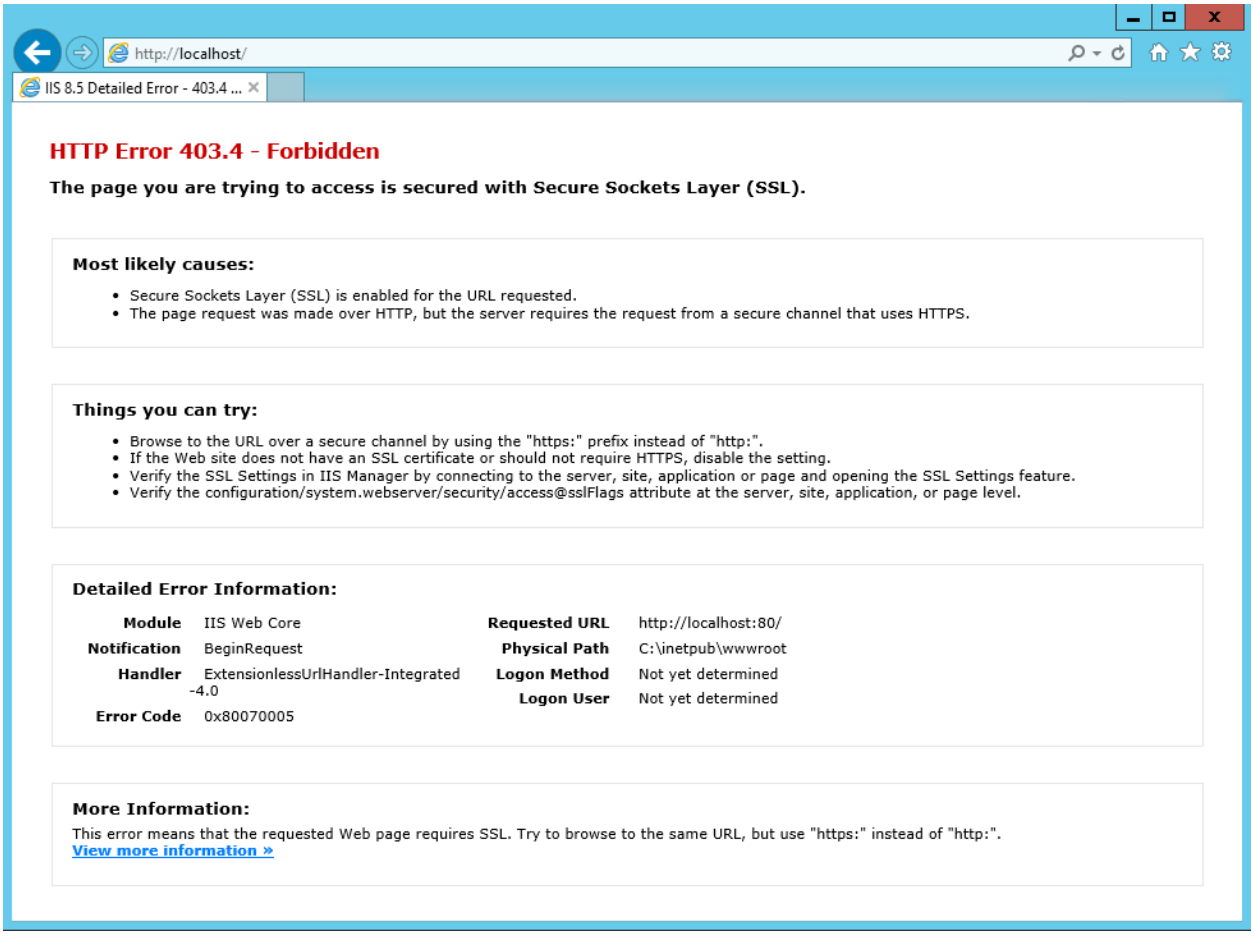
3) On the **SSL Settings** page,
   a) check the **Require SSL** checkbox
   b) Click **Apply**



4) In Internet Explorer or other web browser, enter http://localhost into the address bar.



5) It will come up with a page showing a HTTP 403 – forbidden error. This is because it now requires the https protocol to be used.



All applications accessing your site will now need to use https instead of http in the url to access your Fusion services. I.e. it would now use: https://yourcity.gov/FusionServices
You may need to contact CentralSquare support to change the url for your Converge applications

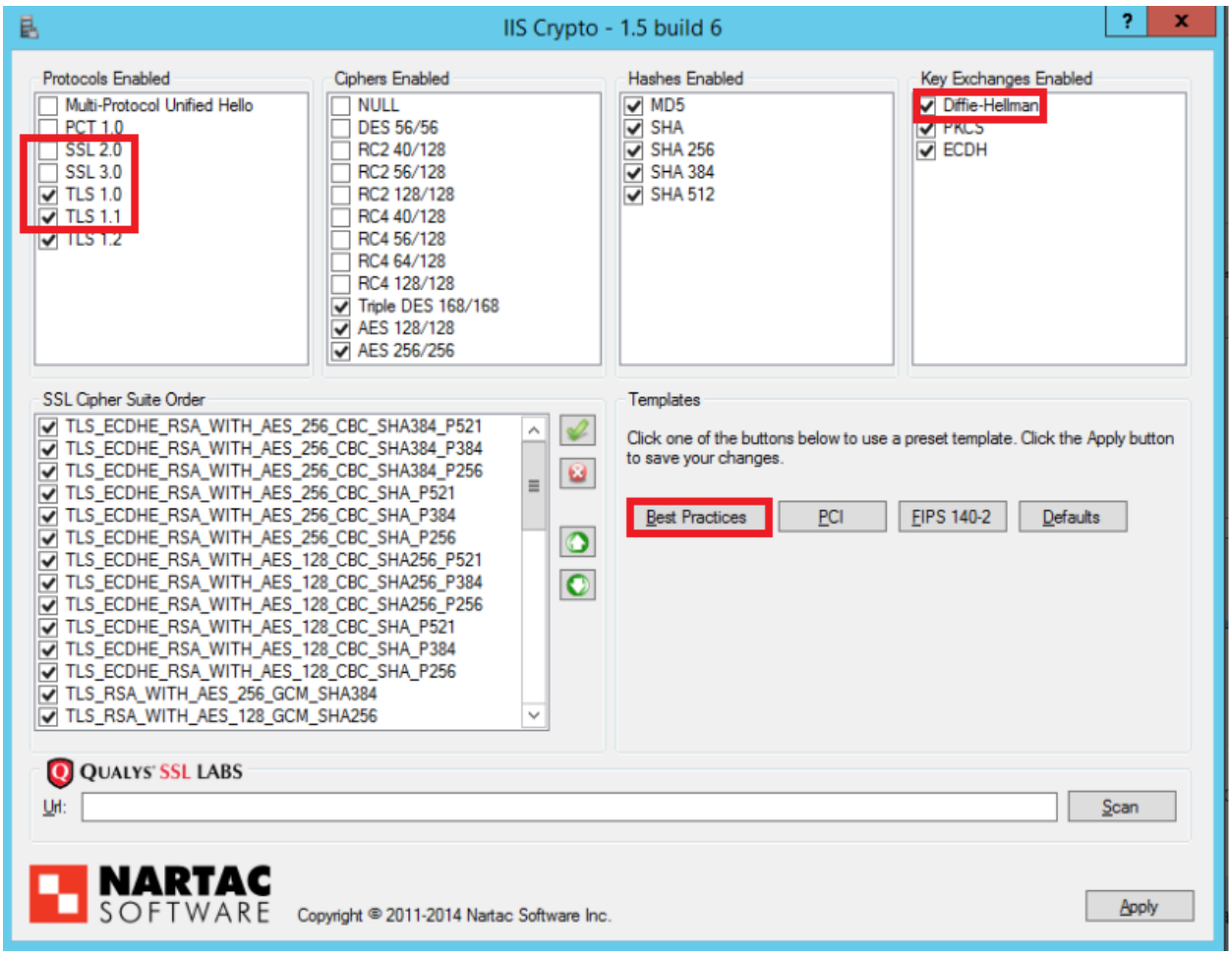
PCI compliance

For IIS to meet PCI compliance you will need to take the following steps.

Run IIS Crypto

The latest PCI security standards requires SSL v3 and TLS 1.0 protocols to not be used. IIS should be using TLS 1.2.
Download IIS Crypto from NarTac. It's a free download, (but we cannot endorse or support it).

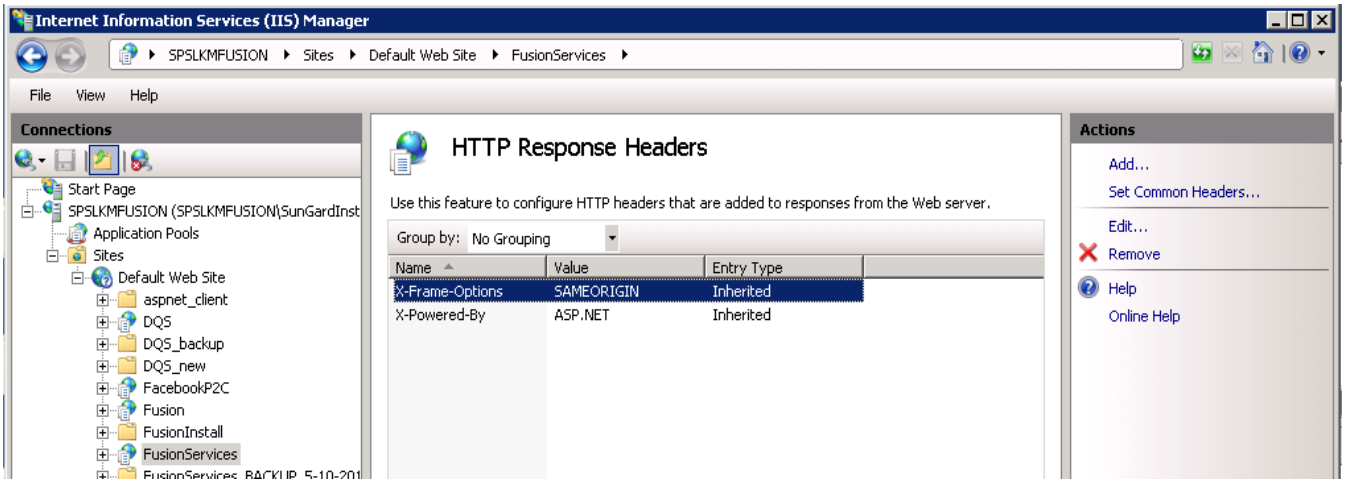
1. Select Best Practices
2. Disable DH
3. Disable all but TLS 1.2



Add X-Frame-Options

The X-Frame-Options header can be used to prevent framesniffing techniques. See https://support.microsoft.com/en-us/kb/2694329 for more information.

1. Open Internet Information Services **(IIS) Manager.**
2. In the **Connections** pane on the left side, expand the **Sites** folder and select **FusionServices**
3. Double-Click the **HTTP Response Headers** icon in the feature list in the middle.
4. In the **Actions** pane on the right side, click **Add**.
5. In the dialog box that appears, type **X-Frame-Options** in the Name field, and type **SAMEORIGIN** in the Value field.
6. Click **OK** to save your changes.



Firewall access

Clients will need to open the identified ports on their server. This is used by the applications to talk to the iSeries and to access the services over the internet.

Network Topology (Organized by Product Type or Category)				
Please confirm the below ports will be opened for <u>bi-directional</u> TCP communication between the devices specified.				
<u>Description</u>	**<u>Port(s)</u>**	**<u>From</u>**	**<u>To</u>**	**<u>Confirm?</u>**
General:				
http/https Internet Communication	80 and 443	Outside Internet	Fusion Web Server	Yes
Note: You can disable http after installing certificates for SSL.				
Payment-related functions:				
Payment Communication	81	Fusion Web Server	iSeries (AS/400)	
iSeries Data Communication (NaviLine / Select):				
IBM Client Access	8470 – 8476, 9471	Fusion Web Server	iSeries (AS/400)	Yes
Distributed Relational Data Manager / Distributed Data Management (DRDM / DDM) Communication	446-449	Fusion Web Server	iSeries (AS/400)	Yes
SSL Communication with iSeries	443	Fusion Web Server	iSeries (AS / 400)	Yes
File upload / download:				
NaviLine Server communication	80 and 443	Fusion Web Server	NaviLine Server	Yes

Please perform a standard network communication test (PING, TRACERT, TELNET, etc., to confirm the following devices can communicate with each other successfully:		
FROM	**TO**	**SUCCESS?**
iSeries Server(s)	Fusion Web Server	Yes
Fusion Web Server	iSeries Server(s)	Yes

Fusion Web Server	NaviLine Server	Yes

Microsoft.NET Framework 4.5

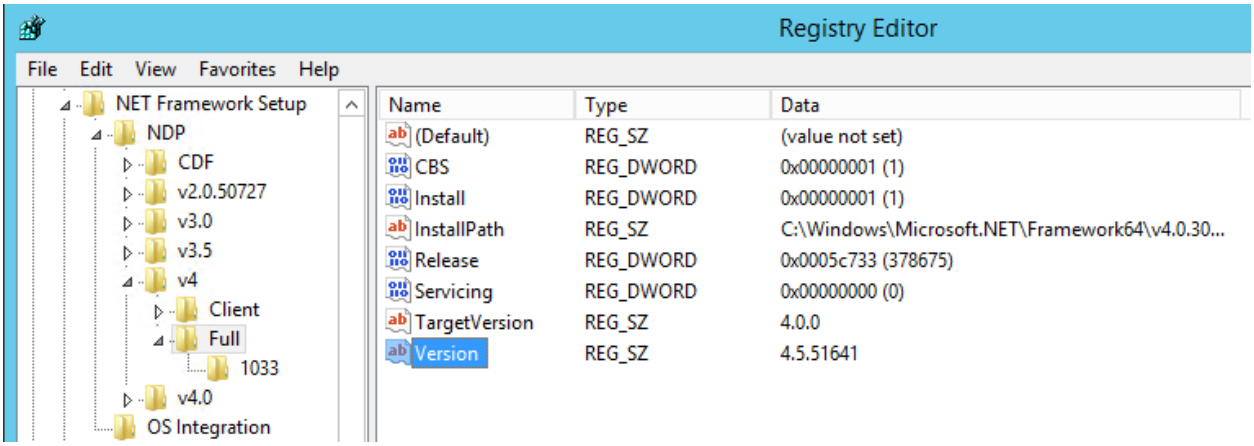
Microsoft .NET Framework 4.5 or higher is required. This is installed through **Server Manager > Add Roles and Features**. The instructions are included as part of the ***Windows Server and IIS Manager*** instructions for adding the roles and features for IIS.

Alternatively, you can also download Microsoft .NET Framework 4.5.1 from the Microsoft Download Center: Microsoft .NET 4.5.1 Download

You can verify what .NET version you have installed by checking the registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\net Framework Setup\NDP\v4\Full\Version

Any 4.5 version or higher should be sufficient.



IBM I Access Client Solutions

The IBM I Access Client Solutions – Windows Application Package is required for access to NaviLine.

This software should come with your iSeries setup and installation package. See the IBM iAccess site or call the IBM Support Line at 1-800-IBM-SERV (1-800-426-7378) for more assistance.

http://www-03.ibm.com/systems/power/software/i/access/solutions.html

The Windows Application Package is an add-on package to the IBM I Access Client Solutions that includes the IBM.Data.DB2.iSeries.dll .NET Data Provider needed for .NET applications to connect to the iSeries.

The install order for the required IBM components is:

1. Download and install latest Java Runtime from: https://www.java.com/en/
2. Install IBM i Access Client Solutions

3. Install the Windows Application Package

All versions of the IBM i Access Client Solutions are supported, as they should be installing version 7 of the .NET Data Provider. IBM Client Access V7R1, the predecessor to IBM i Access Client Solutions, will work but is no longer being supported by IBM. See

Appendix 2: IBMi Client Access if you are using the IBM Client Access version.

iSeries Server Settings

You will need information about the iSeries server in order for Fusion to connect to it. You can retrieve this information from the **System I Navigator**.

iSeries user / password

This is an iSeries account that the Fusion service will use to connect to iSeries. No special permissions are needed. It will use the same permissions as any NaviLine or Select user.

To create a profile from scratch for Fusion, use the following command and parameters:

CRTUSRPRF USRPRF(FUSION) PASSWORD() INLMNU(*SIGNOFF) LMTCPB(*YES) TEXT('Fusion Service Profile') SPCAUT(*NONE) PWDEXPITV(*NOMAX)

Explanation:

1. For the usrprf parameter, the user name is: FUSION
2. INLMNU is the Initial Menu: We use *SIGNOFF to prevent someone from successfully logging into the IBMi profile interactively.
3. LMTCPB stands for Limited Capabilities: This reduces the capabilities of the profile which is very important to also use SPCAUT (Special Authority of *NONE).
4. PWDEXPITV stands for Password Expiration Interval: Always use *NOMAX.

If this is an existing Click2Gov3 customer, you can copy the profile using the “WRKUSRPRF” IBMi command as illustrated below and change the appropriate parameters:

Hit enter

Use option 3 to Copy the existing profile, then change the parameters as indicated above, making sure you use PgDn for more parameters and change the Password Expiration Interval.

```
                          Work with User Profiles

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display
  12=Work with objects by owner

     User
Opt  Profile     Text

__   __________
3    SPSEGOV     Click2Gov3 Default Profile **DO NOT DELETE**
```

User Profile

The Fusion user profile must have QPGMR specified in the Group profile (GRPPRF) or Supplemental groups (SUPGRPPRF) parameter:

```
                        Change User Profile (CHGUSRPRF)

Type choices, press Enter.

Group profile  . . . . . . . . . GRPPRF          QPGMR
Owner  . . . . . . . . . . . . . OWNER           *USRPRF
Group authority  . . . . . . . . GRPAUT          *NONE
Group authority type . . . . . . GRPAUTTYP       *PRIVATE
Supplemental groups  . . . . . . SUPGRPPRF       *NONE
                          + for more values
Accounting code  . . . . . . . . ACGCDE          *BLANK
Document password  . . . . . . . DOCPWD          *SAME
Message queue  . . . . . . . . . MSGQ            FUSION
  Library  . . . . . . . . . . .                   QUSRSYS
Delivery . . . . . . . . . . . . DLVRY           *NOTIFY
Severity code filter . . . . . . SEV             0
Print device . . . . . . . . . . PRTDEV          *WRKSTN
Output queue . . . . . . . . . . OUTQ            *WRKSTN
  Library  . . . . . . . . . . .
```

- or -

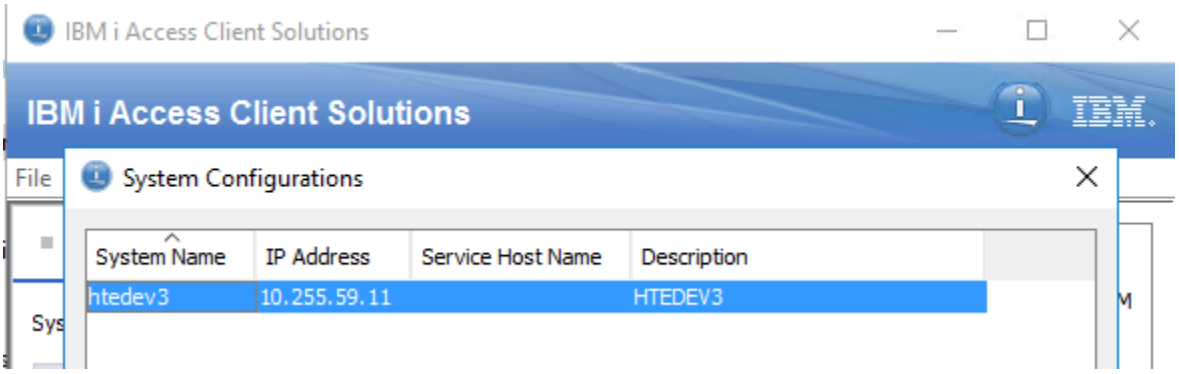
```
                     Change User Profile (CHGUSRPRF)

Type choices, press Enter.

Group profile  . . . . . . . . . GRPPRF          GRPALL
Owner  . . . . . . . . . . . . . OWNER           *USRPRF
Group authority  . . . . . . . . GRPAUT          *ALL
Group authority type . . . . . . GRPAUTTYP       *PRIVATE
Supplemental groups  . . . . . . SUPGRPPRF       GRPMOD
                          + for more values      QPGMR
Accounting code  . . . . . . . . ACGCDE          'GRPC2G'
Document password  . . . . . . . DOCPWD          *SAME
Message queue  . . . . . . . . . MSGQ            FUSION
  Library  . . . . . . . . . . .                   QUSRSYS
Delivery . . . . . . . . . . . . DLVRY           *BREAK
Severity code filter . . . . . . SEV             0
Print device . . . . . . . . . . PRTDEV          *WRKSTN
Output queue . . . . . . . . . . OUTQ            QPRINT
  Library  . . . . . . . . . . .                   QGPL
```

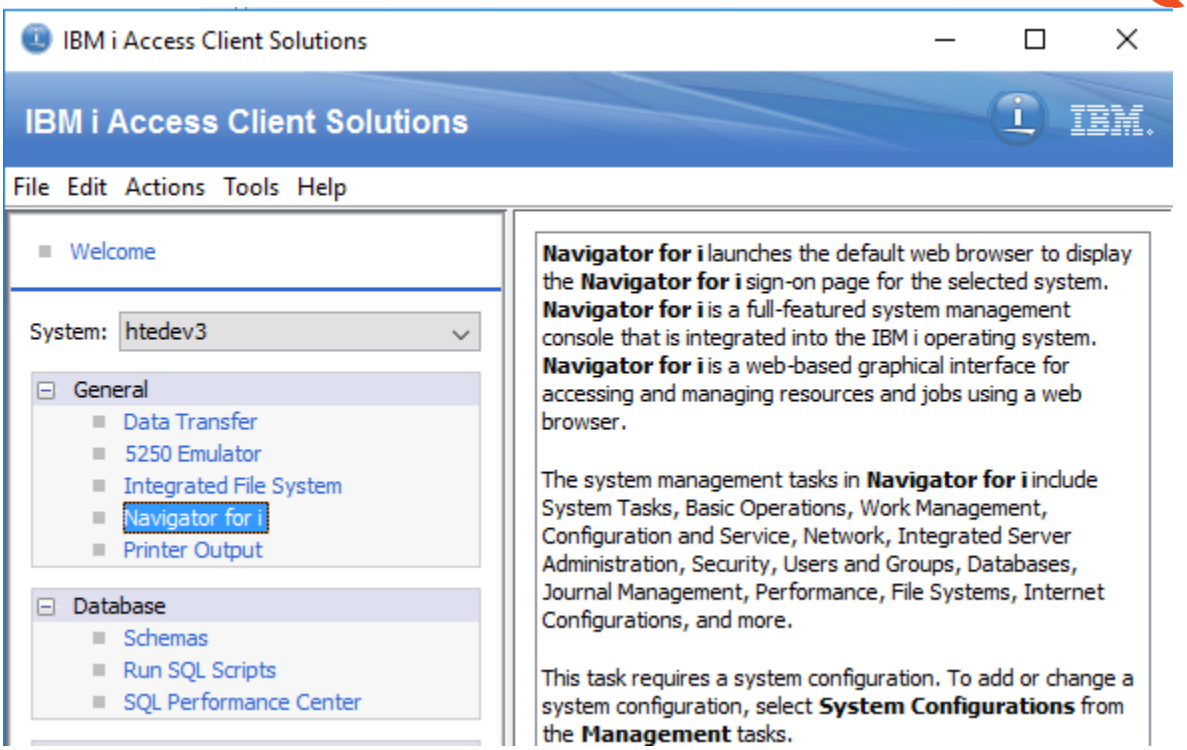
iSeries server

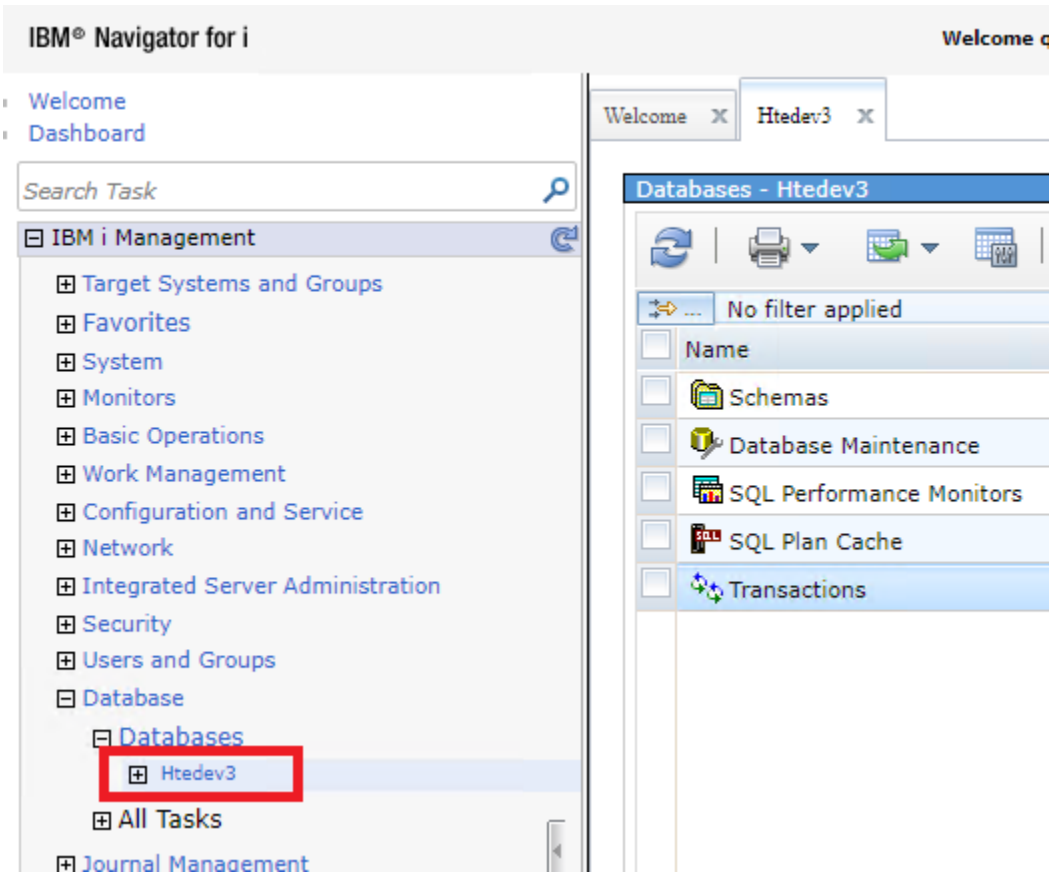
This is the fully qualified domain name or the IP address of your iSeries server.
This is the name of the server as it appears in **IBM I Access Client Solutions** under **System Configurations**.



iSeries database

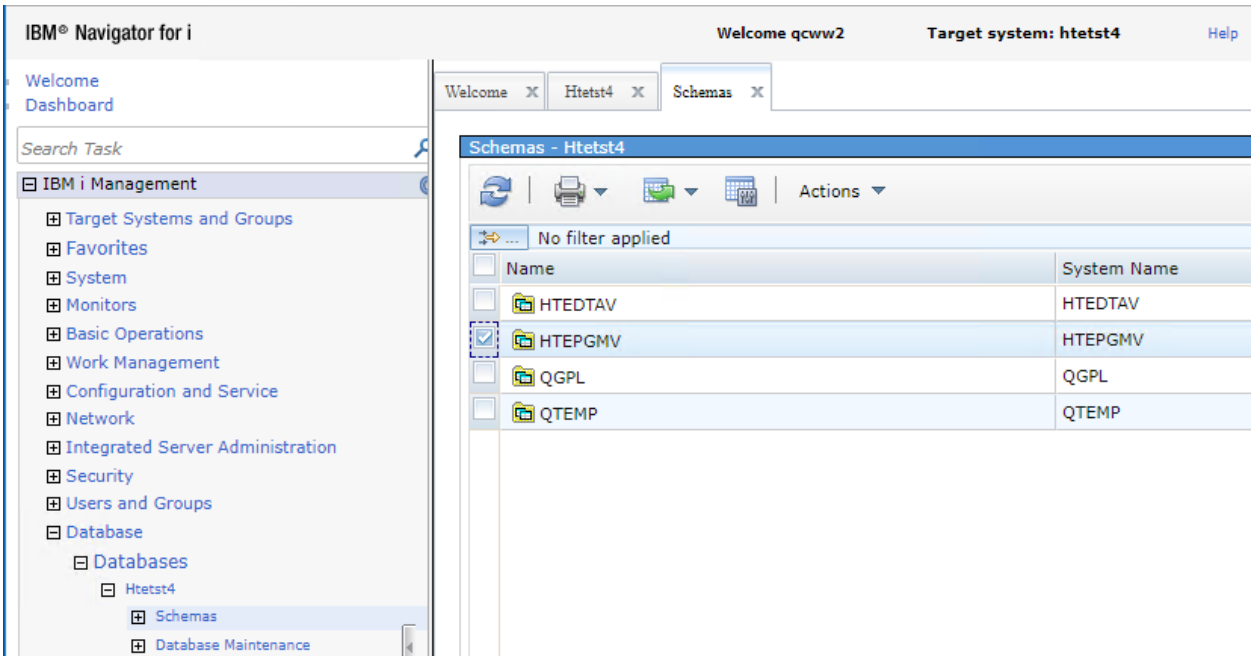
This is the name of the database as it appears in **IBM I Access Client Solutions** under **Navigator for I** > **Database > Databases**


IBM i Access Client Solutions
IBM i Access Client Solutions
File Edit Actions Tools Help
Welcome
System: htedev3
General
Data Transfer
5250 Emulator
Integrated File System
Navigator for i
Printer Output
Database
Schemas
Run SQL Scripts
SQL Performance Center
Navigator for i launches the default web browser to display the Navigator for i sign-on page for the selected system. Navigator for i is a full-featured system management console that is integrated into the IBM i operating system. Navigator for i is a web-based graphical interface for accessing and managing resources and jobs using a web browser.
The system management tasks in Navigator for i include System Tasks, Basic Operations, Work Management, Configuration and Service, Network, Integrated Server Administration, Security, Users and Groups, Databases, Journal Management, Performance, File Systems, Internet Configurations, and more.
This task requires a system configuration. To add or change a system configuration, select System Configurations from the Management tasks.


IBM® Navigator for i
Welcome
Dashboard
Search Task
IBM i Management
Target Systems and Groups
Favorites
System
Monitors
Basic Operations
Work Management
Configuration and Service
Network
Integrated Server Administration
Security
Users and Groups
Database
Databases
Htedev3
All Tasks
Journal Management
Welcome
Htedev3
Databases - Htedev3
No filter applied
Name
Schemas
Database Maintenance
SQL Performance Monitors
SQL Plan Cache
Transactions

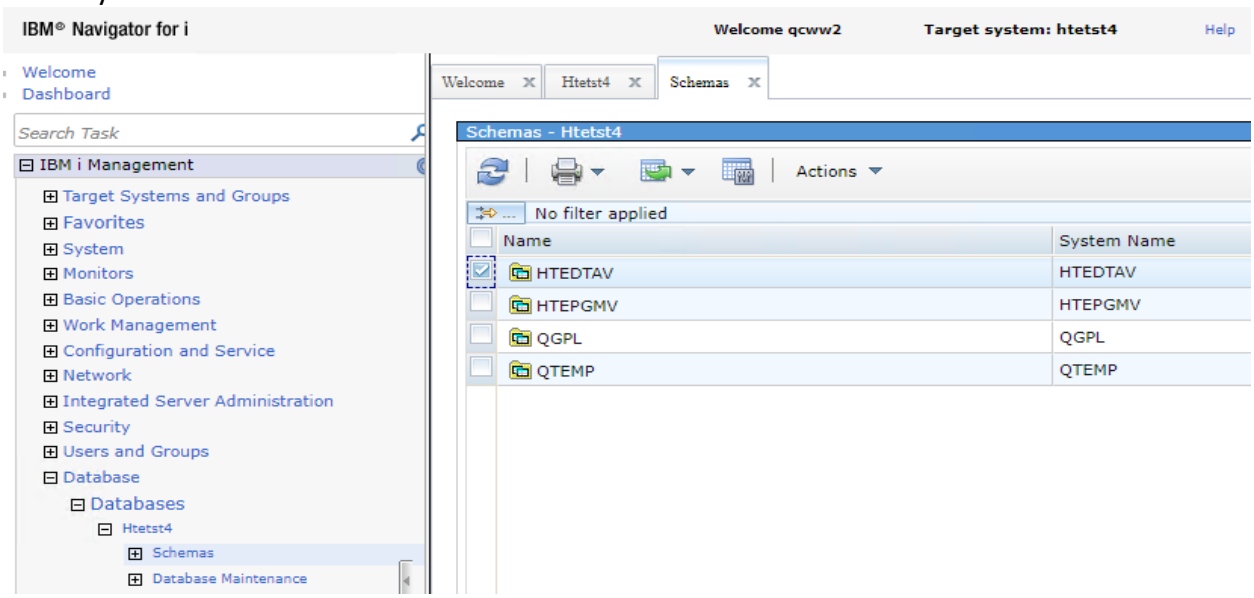
iSeries program libray

This is the name of the PGM library as it appears in **IBM I Access Client Solutions** under **Navigator for I** > **Database > Databases** > **[DatabaseName] > Schemas.** The default is HTEPGM, but may be different for a TEST environment.



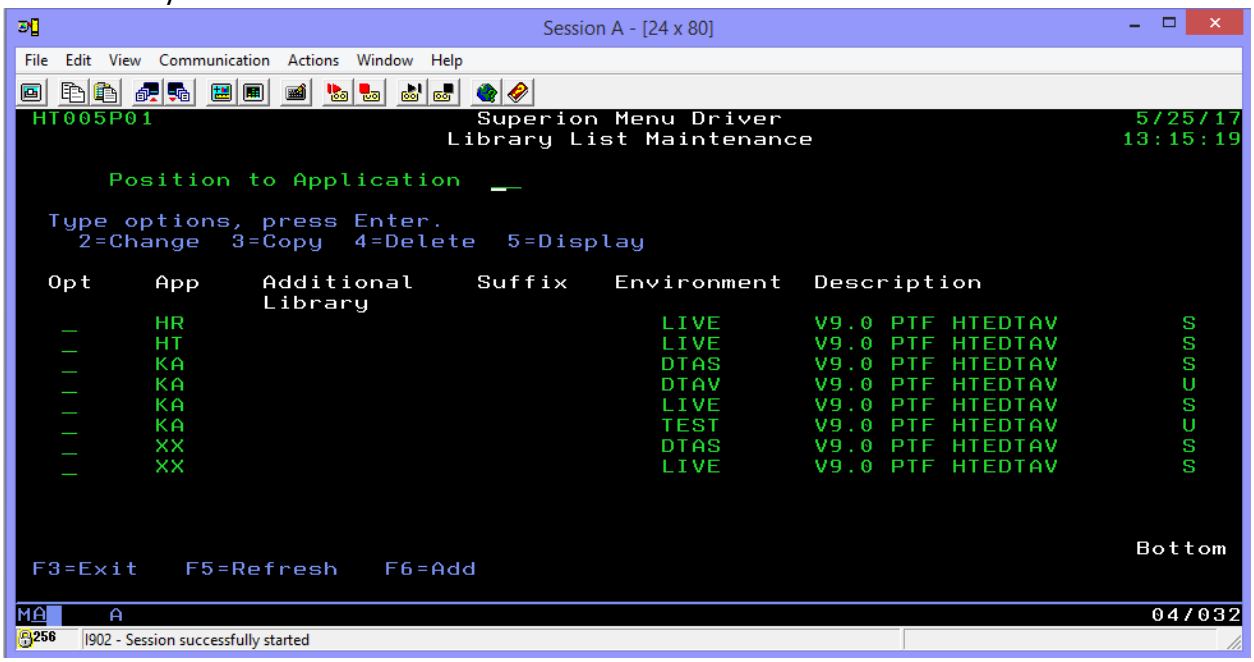
iSeries data libray

This is the name of the DTA library as it appears in **IBM I Access Client Solutions** under **Navigator for I** > **Database > Databases** > **[DatabaseName] > Schemas.** The default is HTEDTA, but may be different for a TEST environment.



iSeries environment

If you have multiple environments set up on iSeries, such as for LIVE and TEST, then you need to enter the environment name. If you sign in to either NaviLine or Select and get an environment screen, then this would be the environment you normally select on that screen. If you do not normally get the environment screen, then there isn't an environment and you can leave the environment blank. You can further check for environment names in either NaviLine or Select by using a **F9 command line > strsql > CALL HT005P**. This will bring up an environment list if there are any available.



NaviLine Server Name

You will need the fully qualified server name, i.e. NLServer.domain.com or IP address of the NaviLine server. This is used by methods that upload or retrieve file attachments. These methods require NaviLine 9.1.16.2 or higher.

Payments

Fusion payments require additional setup on the iSeries and Point of Sale (POS) servers for payments to be fully processed.
See the Payment Setup page for additional installation and setup guides.

NaviLine Web Enablement

The NaviLine Web Enablement package needs to be loaded on the NaviLine IBM iSeries server. Separate install instructions for installing the package on the iSeries should be sent to you when you order this package. Additional licensing and configuration instructions are on the Payment Setup page.

Cash Receipts

The Fusion payment methods require a Cash Receipt Batch to be configured on the IBM iSeries server for payment processing. See the Cash Receipts Setup instructions for how to setup and configure the batch.

Agnostic Payment Listener

This is required to be installed on any POS machine taking credit card payments. See the Payment Setup page for installation and setup guides.

Cloud Installs ONLY

For Cloud Installs that access a premise database, you will have to edit the web.config files (in both c:\inetpub\wwwroot and d:\inetpub\wwwroot if they exist there) to include the database server IP address in order for Web Service Payments via Fusion to work.

The file contents look like this….

```
<?xml version="1.0" encoding="UTF-8"?>

<configuration>

<system.net>

  <defaultProxy>

   <proxy proxyaddress="http://172.30.20.55:8080" bypassonlocal="true" />

       <bypasslist>

              <add address="172.30.2.54" />

              <add address="172.30.2.52" />
```

```
                <add address="172.30.2.129" />
                <add address="172.30.2.55" />
                <add address="172.30.2.62" />
                <add address="172.30.2.71" />
                <add address="172.30.2.75" />
                <add address="172.30.2.142" />
                <add address="172.30.2.92" />
                <add address="172.30.2.95" />
            </bypasslist>
        </defaultProxy>
    </system.net>
        <system.web>
            <identity impersonate="true" />
        </system.web>
</configuration>
```

Installation Options

Follow the guide link for your action. You may skip over sections for other actions you are not currently doing.

Click here: *To install for the first time*
Use this option if this is the first time you are installing Fusion on the server.

Click here: *To upgrade to a new version*
Use this option if you already have a version of Fusion installed, and you want to upgrade it to a new version.

Click here: *To change configuration information*
Use this option to change the configuration values after Fusion is already installed. I.e., changing the iSeries password or adding an AppID.

Click here: *To uninstall*
Use this option to uninstall and remove all Click2Gov applications. This removes all applications from WebLogic and deletes the files from your server.

To install for the first time

If you are installing Fusion for the first time on the server, this section guides you through the steps required.

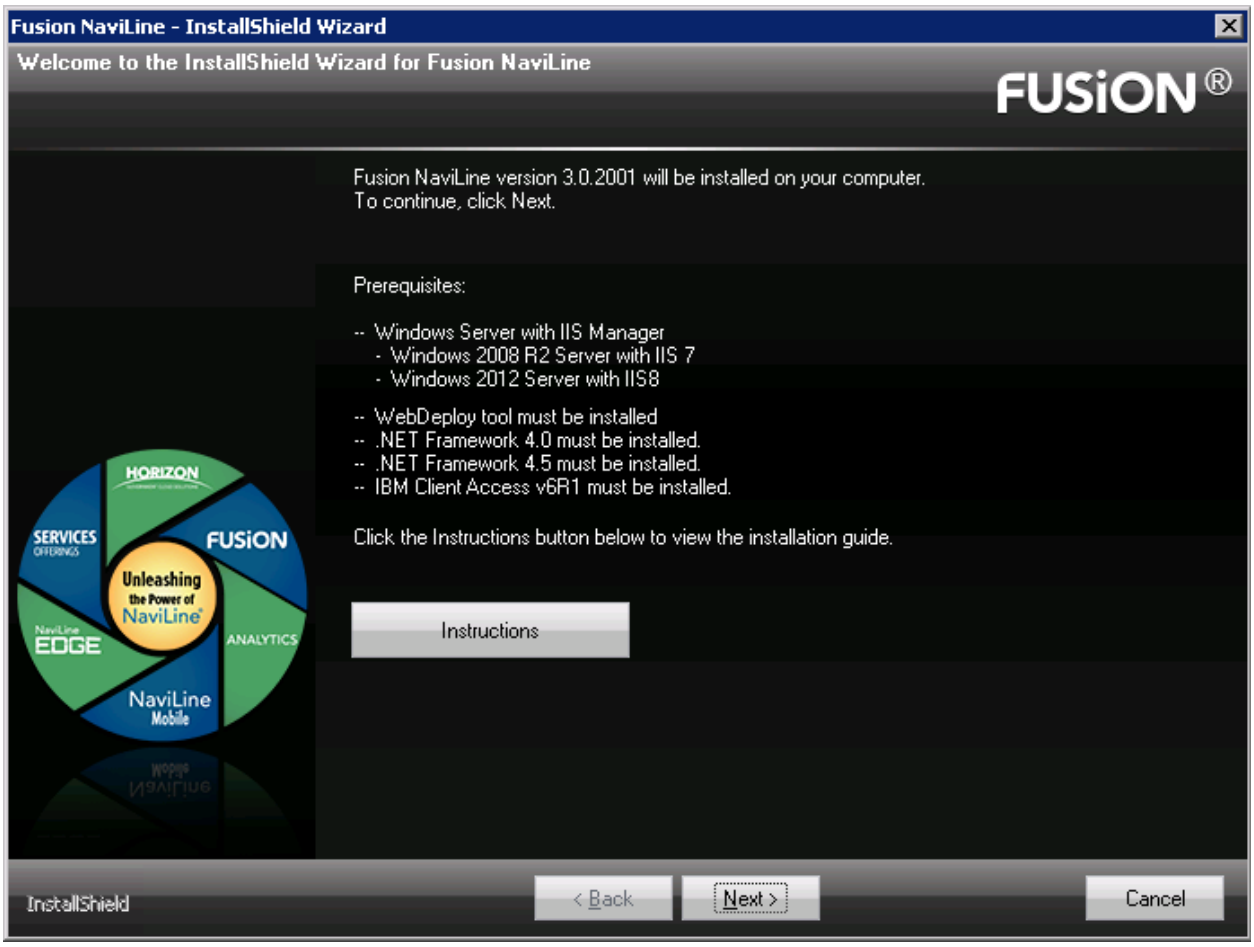
Install questions

The installer displays screens prompting you for the information you gathered in your configuration checklist.
This section guides you through the screens and instructs you about how to provide the required information.

Welcome

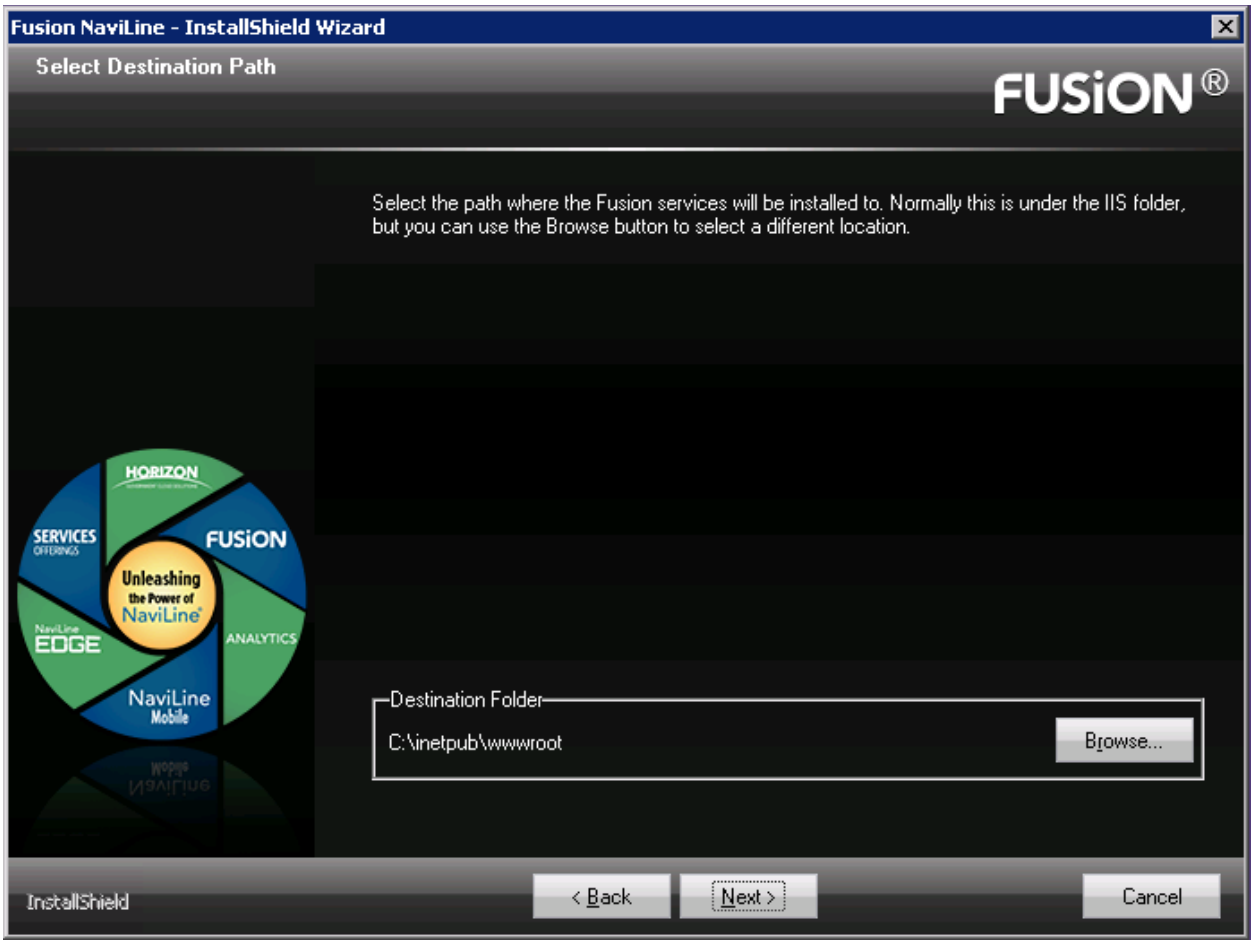
This screen states general information and requirements about the installer. See the section

Prerequisites for information about installing the prerequisites. When you click Next, the installer verifies that the prerequisites are installed. Click the **Instructions** button to display the installation instructions where you will find a list of the prerequisites and instructions on how to install them.



Destination Folder

Select the directory to install the Fusion services to. By default, this is your IIS folder. You can change it to install to a different location if you prefer by clicking the **Browse** button. The install will create a folder called FusionServices under the selected folder where the service files will be installed.



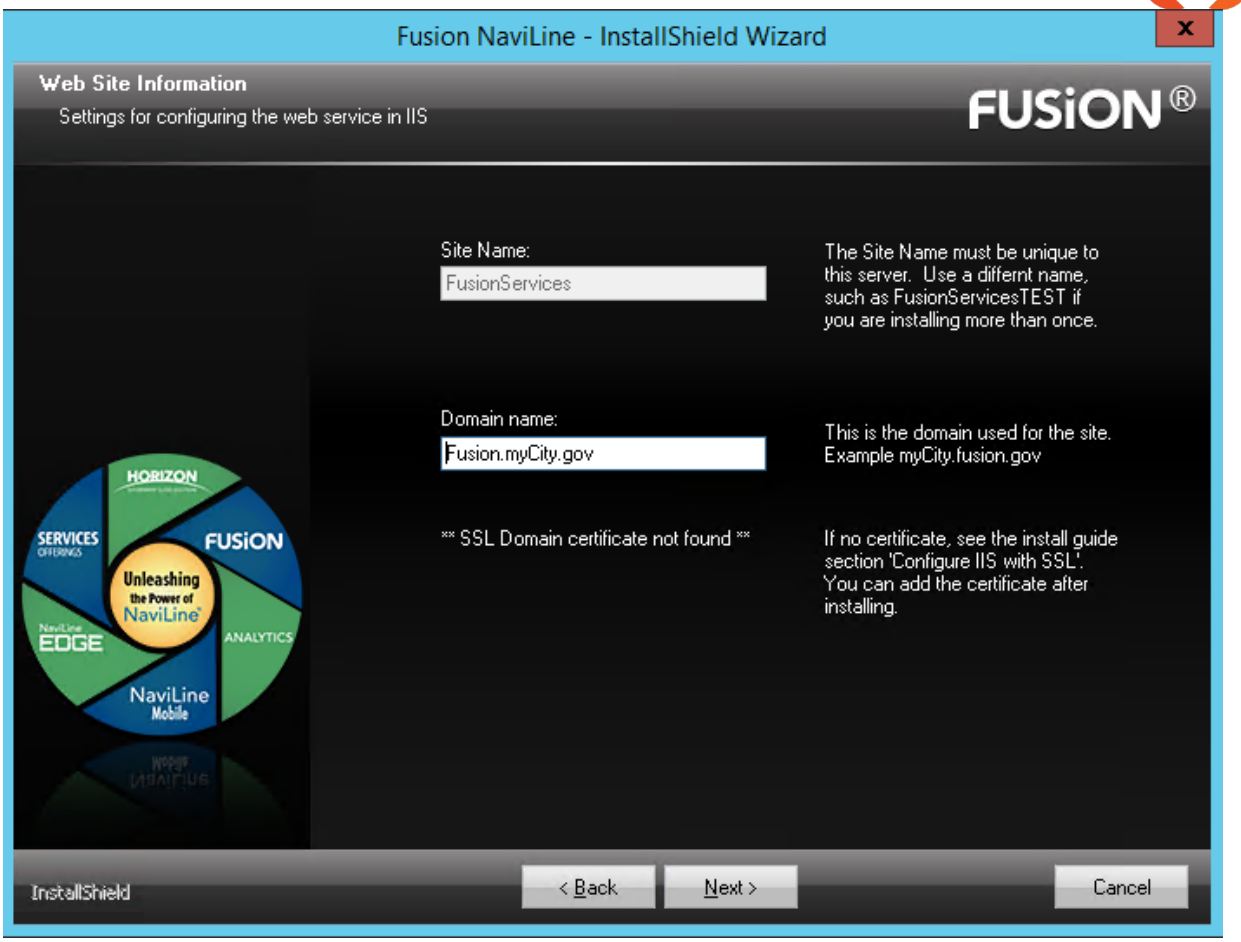
Site Information

Enter the **Site Name** to use as the name of the web service. This will determine the URL needed to access the fusion services. By default, this is FusionServices, and the resulting URL would be http://localhost/FusionServices

You can install the fusion services more than once on the same server. Each site requires you to enter a unique Site Name. This is used, for example, if you want to set up a second site going to your iSeries TEST server. You would enter FusionServicesTest as the Site Name to make it unique and to indicate it is going to the TEST server. Then you would access the Fusion services test site by using the URL: http://localhost/FusionServicesTEST

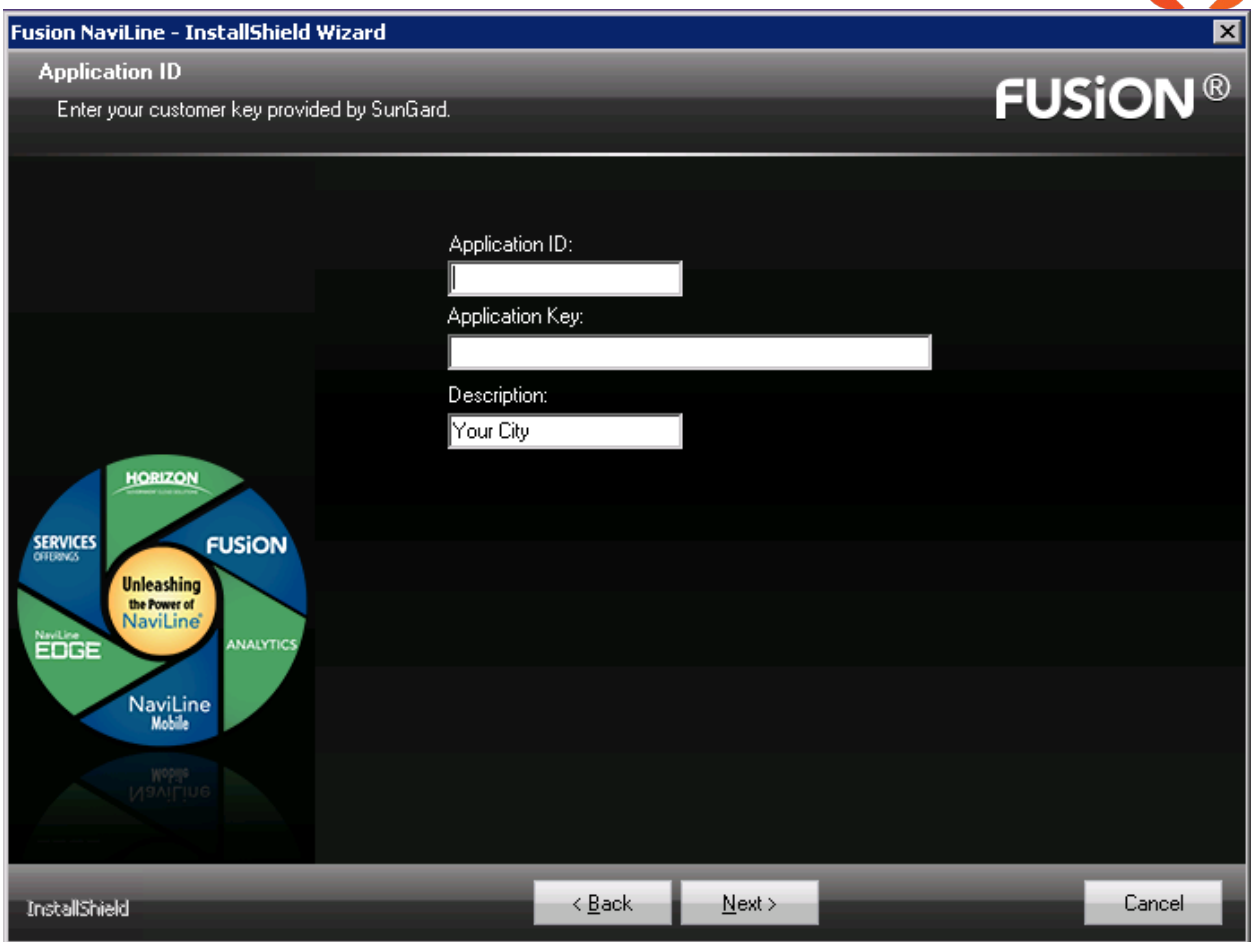
Enter the **Domain Name** used by your site's SSL certificate. This will determine the URL needed to externally access the fusion services. By default, this is Fusion.myCity.gov, and the resulting URL would be https://Fusion.myCity.gov/FusionServices. This needs to be changed to your domain name.

Under the domain name, is a message indicating if the SSL Domain certificate is available or not. It will re-check for a SSL certificate after you enter the domain name above. If the certificate is not found, see the section ***Configure IIS with SSL*** to add an SSL Certificate. If you do not have your domain name or Https enabled, you can leave the default domain name and change it after you receive your certificate. It is used for HTTPS security settings required for OWASP compliance. The Fusion diagnostic page will show a warning that Https security is not enabled, but you will still be able to use the Fusion services. To change the domain name and Https security settings after getting your certificate, see the section ***To change configuration information***.



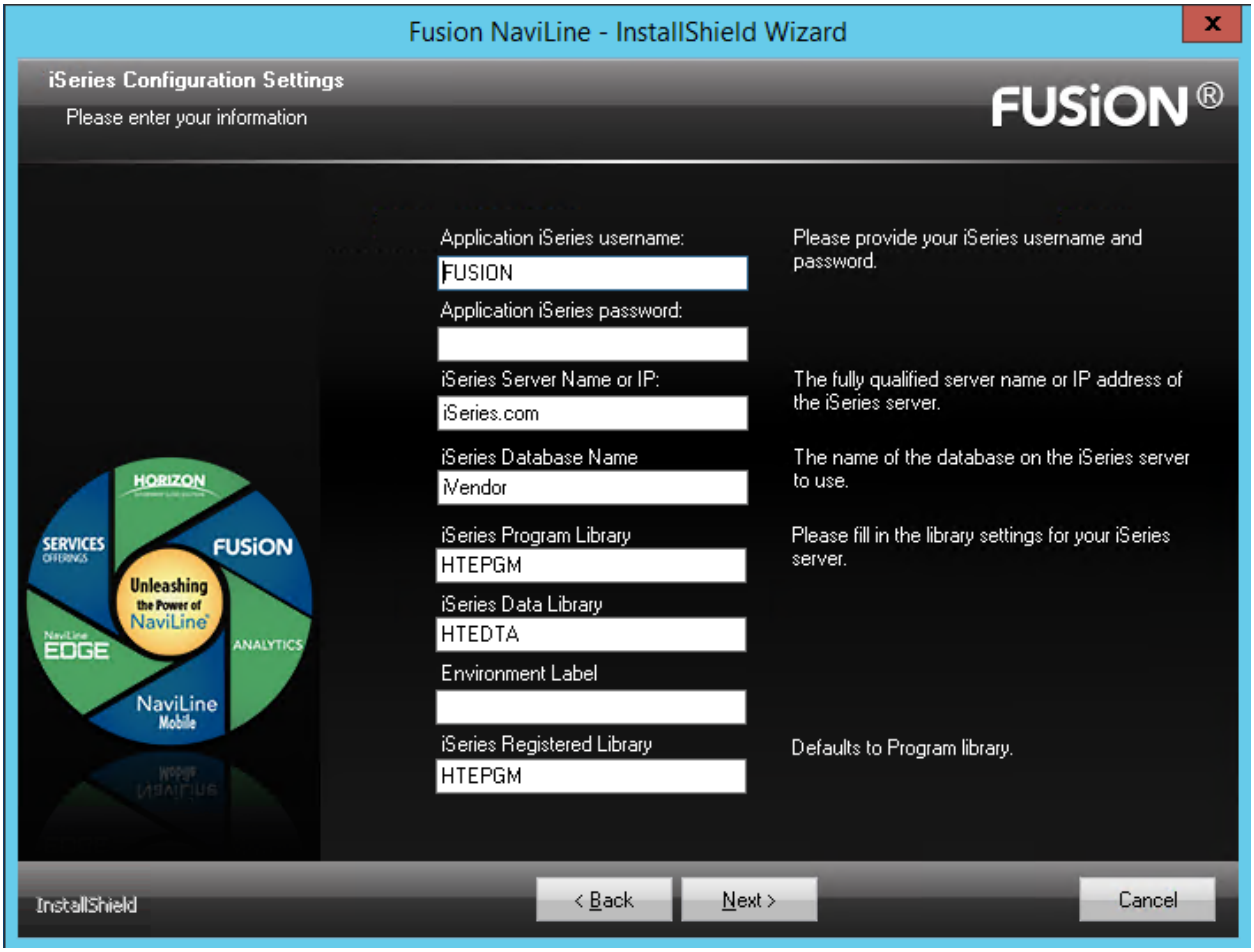
Application ID

An application ID and application key will be provided to you when you purchase Fusion through CentralSquare. This information is from item 1 in your configuration checklist. The **ID** and **Key** are required, enter your city name in the **Description.**


Fusion NaviLine - InstallShield Wizard
Application ID
Enter your customer key provided by SunGard.
FUSION®
Application ID:
Application Key:
Description:
Your City
HORIZON
SERVICES
FUSION
Unleashing the Power of NaviLine
NaviLine EDGE
ANALYTICS
NaviLine Mobile
InstallShield
< Back
Next >
Cancel

iSeries Configuration Settings

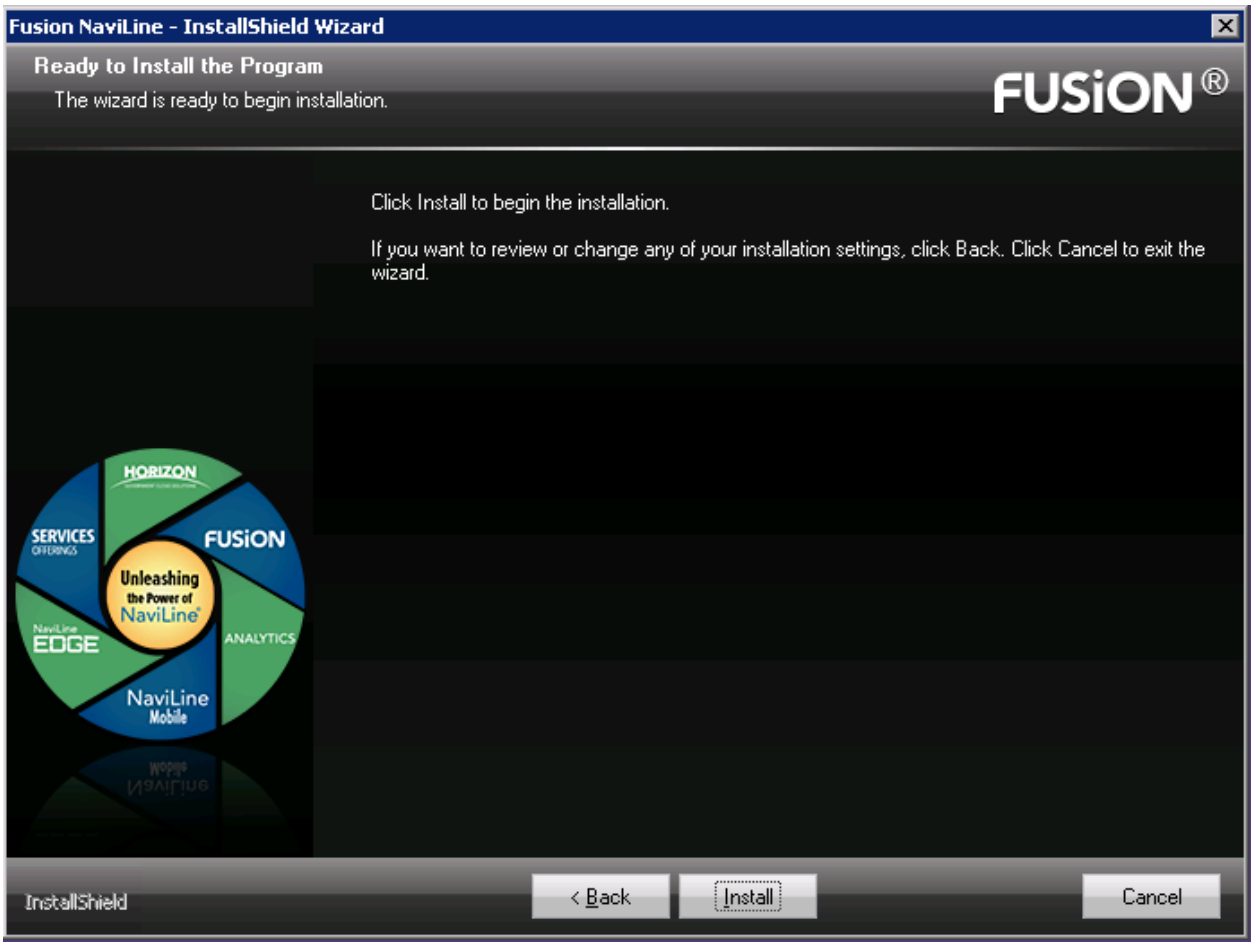
Enter the iSeries information from items 2a-2h in your configuration checklist.
This information is used to configure the Fusion services to communicate with the iSeries. All fields are required except the environment label. If your iSeries requires an environment label, fill it in.



Configuration Settings

Enter the NaviLine server information from item 3a in your configuration checklist. This information is used to configure the Fusion services to communicate with the NaviLine server for file attachments. If you do not have a NaviLine server, just enter localhost to continue.

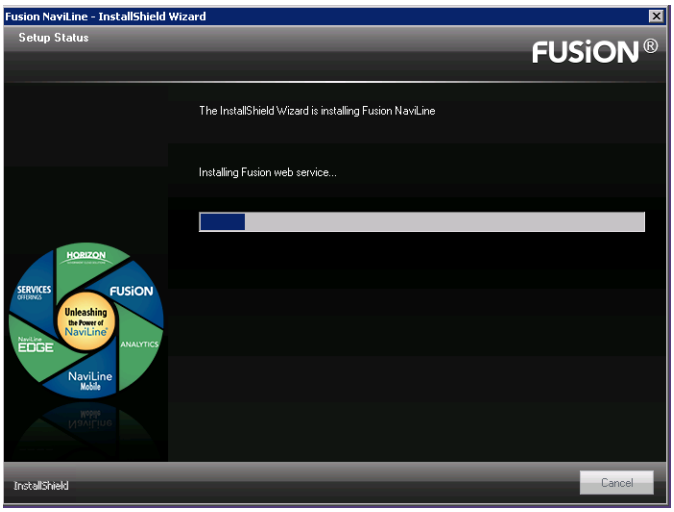
Ready to Install



Click **Install** to start the installation.

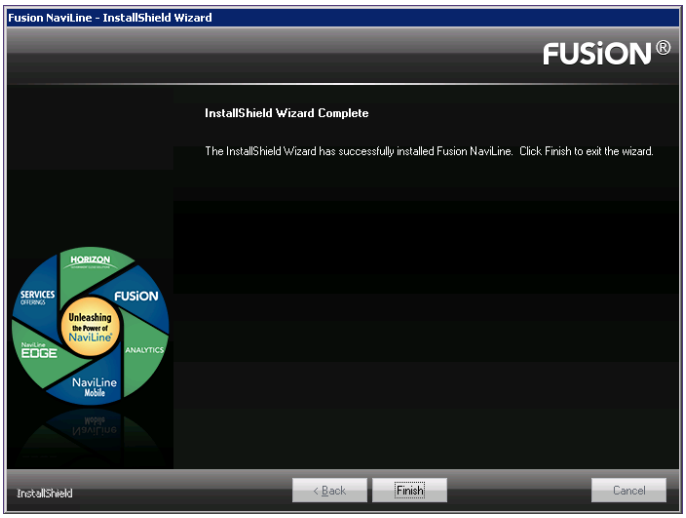
Installation

The installer will deploy the latest Fusion service files to IIS, then set the configuration values. If this is an upgrade or maintenance, then it will back up the previous files before making any changes. The installer displays what it's doing above the status bar. This should only take a few minutes.



Complete

This screen displays once the installer has completed installation and configuration.



Click **Finish** to end the installation. Click here: *Verify the installation* to continue to the post-install instructions.

To upgrade to a new version

If you are running the install in order to upgrade Fusion to the latest version, this section guides you through the steps required.

Install questions

The installer displays screens to indicate it is upgrading to a new version. It does not allow you to change any of the configuration during update mode.

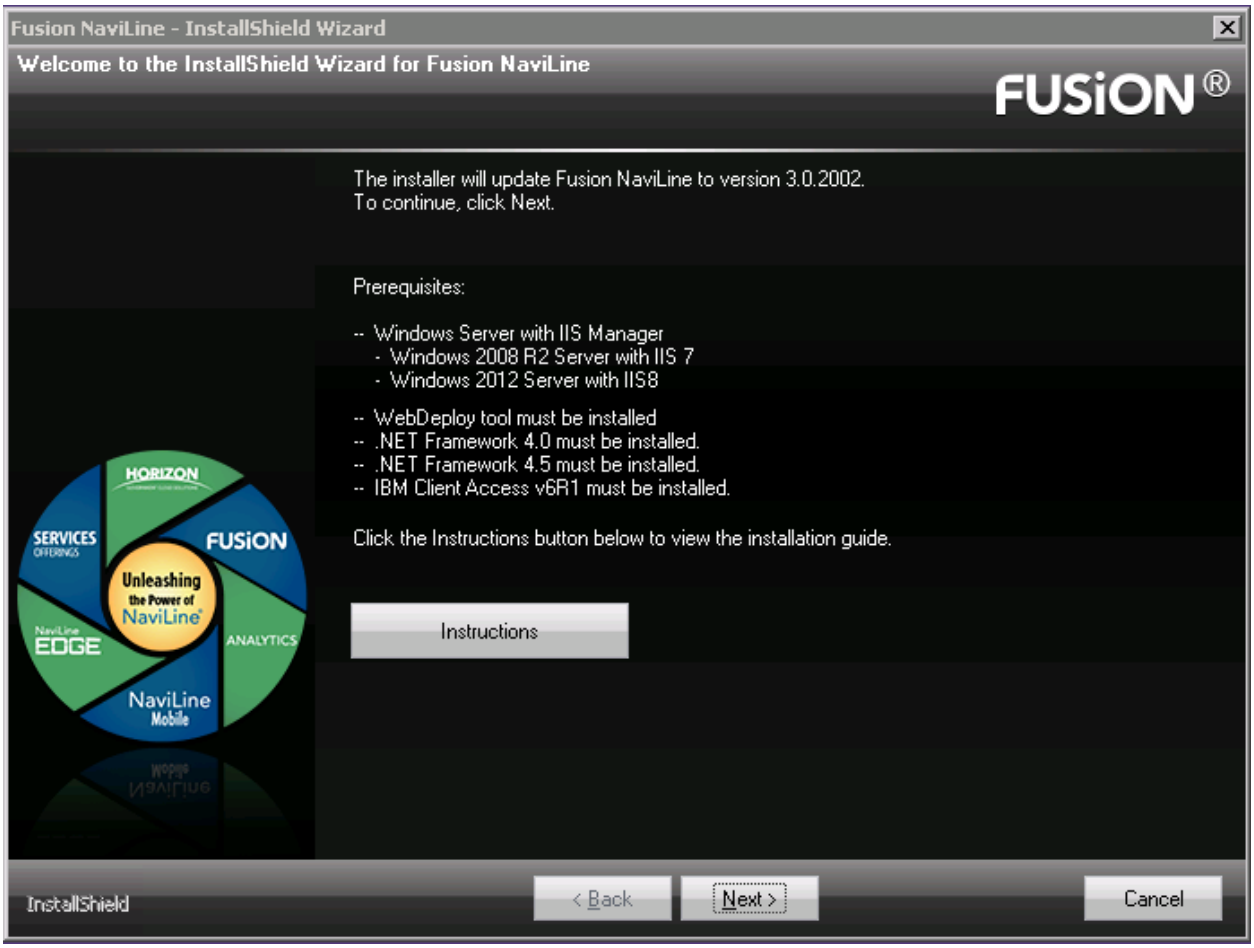
Multi-Instance Screen

The installation will first display the instance selection dialog shown below.

Choose the **Maintain or update the instance of this application selected below** radio button. Then select the Fusion application with the Site Name you want to update.

Welcome

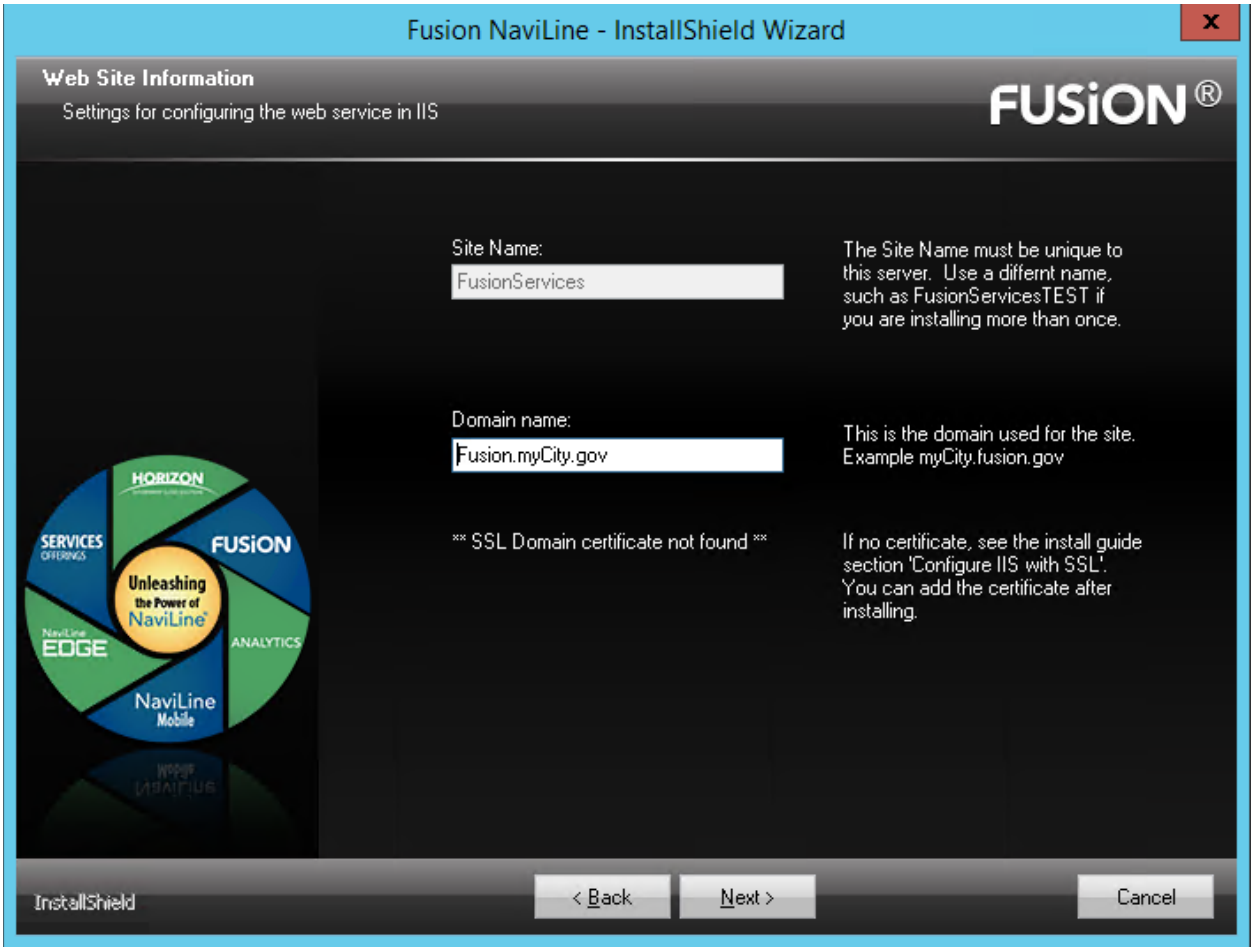
This screen simply states that it will update Fusion and show the version being upgraded to.



Site Information

Confirm that the **Site Name** is the correct one for the site you are trying to upgrade.

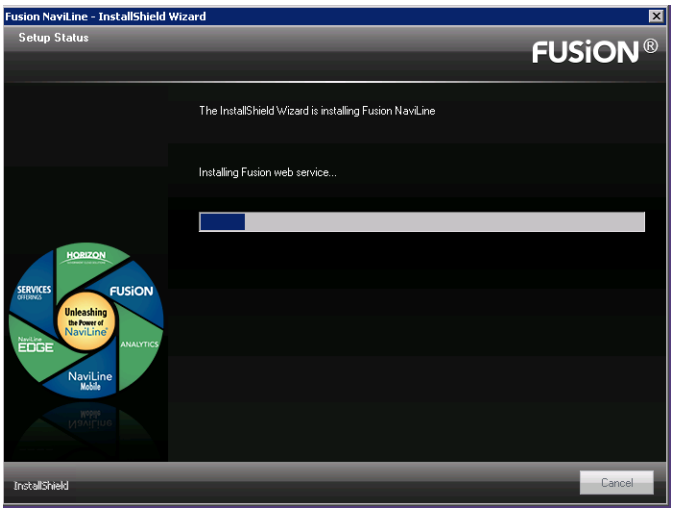
If you have not previously entered a **Domain name**, then you can enter it now, as this was not required in previous versions.



Click **Next** to start the installation.

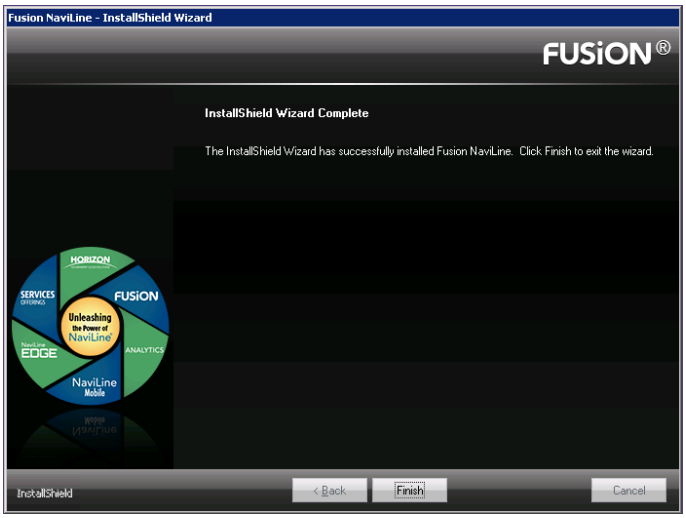
Installation

The installer will deploy the latest Fusion service files to IIS, then set the configuration values. If this is an upgrade or maintenance, then it will back up the previous files before making any changes. The installer displays what it's doing above the status bar. This should only take a few minutes.



Complete

This screen displays once the installer has completed installation and configuration.



Click **Finish** to end the installation. Click here: *Verify the installation* to continue to the post-install instructions.

To change configuration information

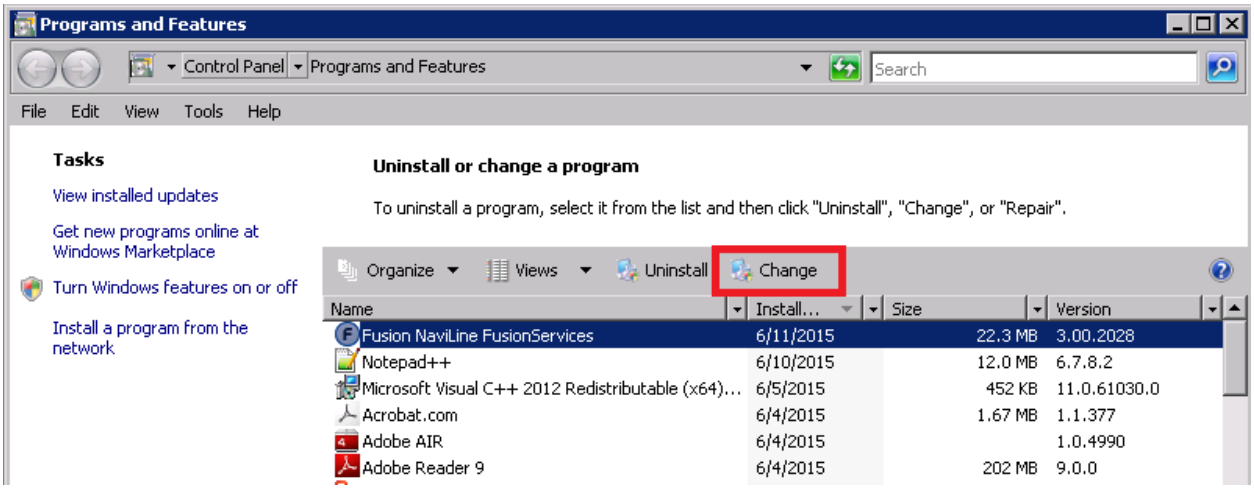
If you need to change any of the configuration values from the configuration checklist such as changing the iSeries password, this section guides you through the steps required.
Examples where you would use this option:

- The iSeries password has expired, and you need to reset it.
- You have the latest version installed on your TEST environment and want to switch it over to PRODUCTION.
- You want to add an App ID.

Starting the installer

You do not need the Fusion install package available to change the applications. Simply go to the **Programs and Features** option in Windows Control Panel. On the Windows **Start** menu, select **Control Panel**. Then select **Programs and Features.**

In the Programs and Features window, select the Fusion application, then click **Change**. This starts the installer.

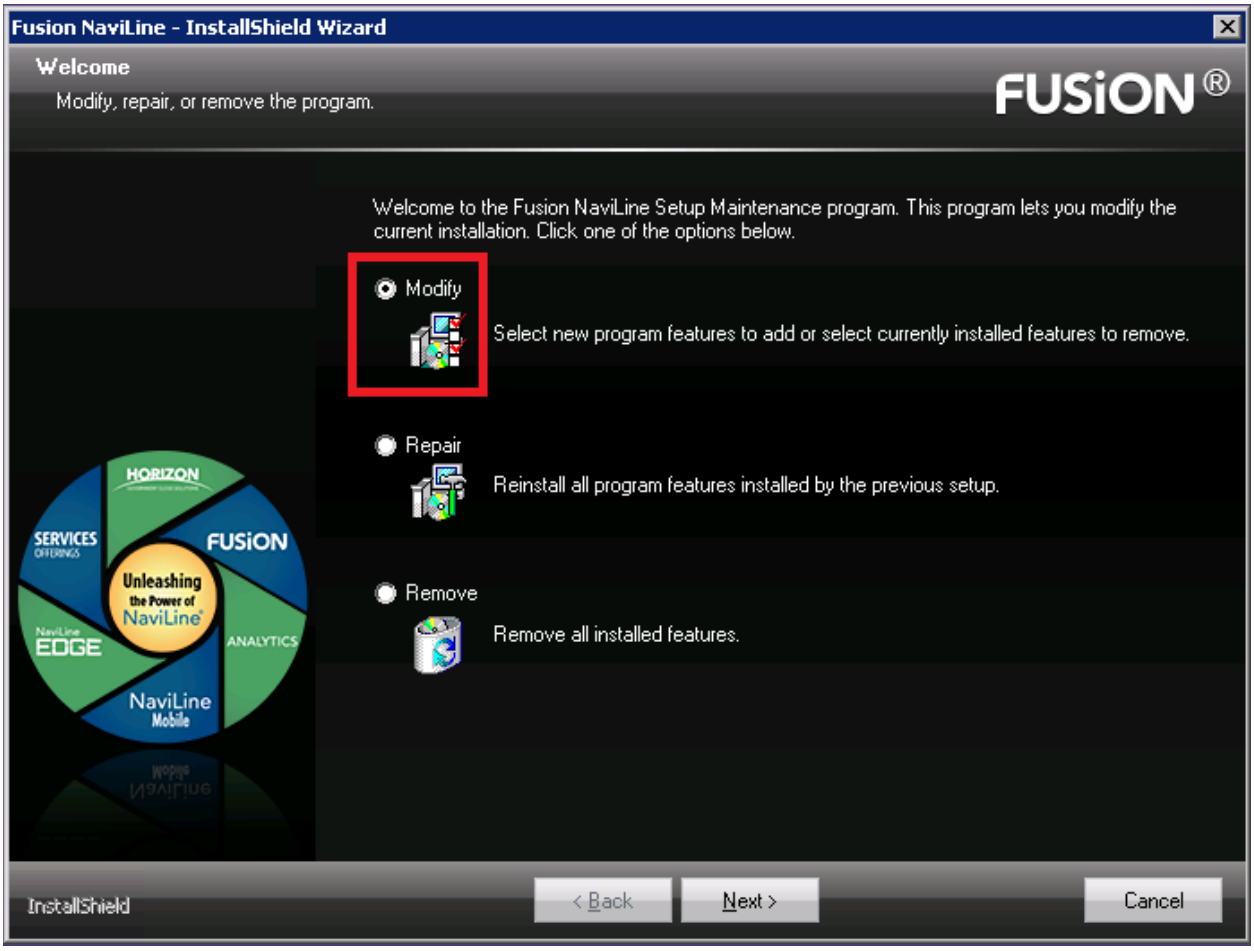


Install Questions

The installer displays screens prompting you for the information you gathered in your configuration checklist. This section guides you through the screens presented and instructs you about how to provide the required information.

Modify / Repair / Remove

The Modify / Repair / Remove screen displays first and asks you which of these options you want to do. Choose the first option, **Modify,** to change the configuration values for the currently installed applications.

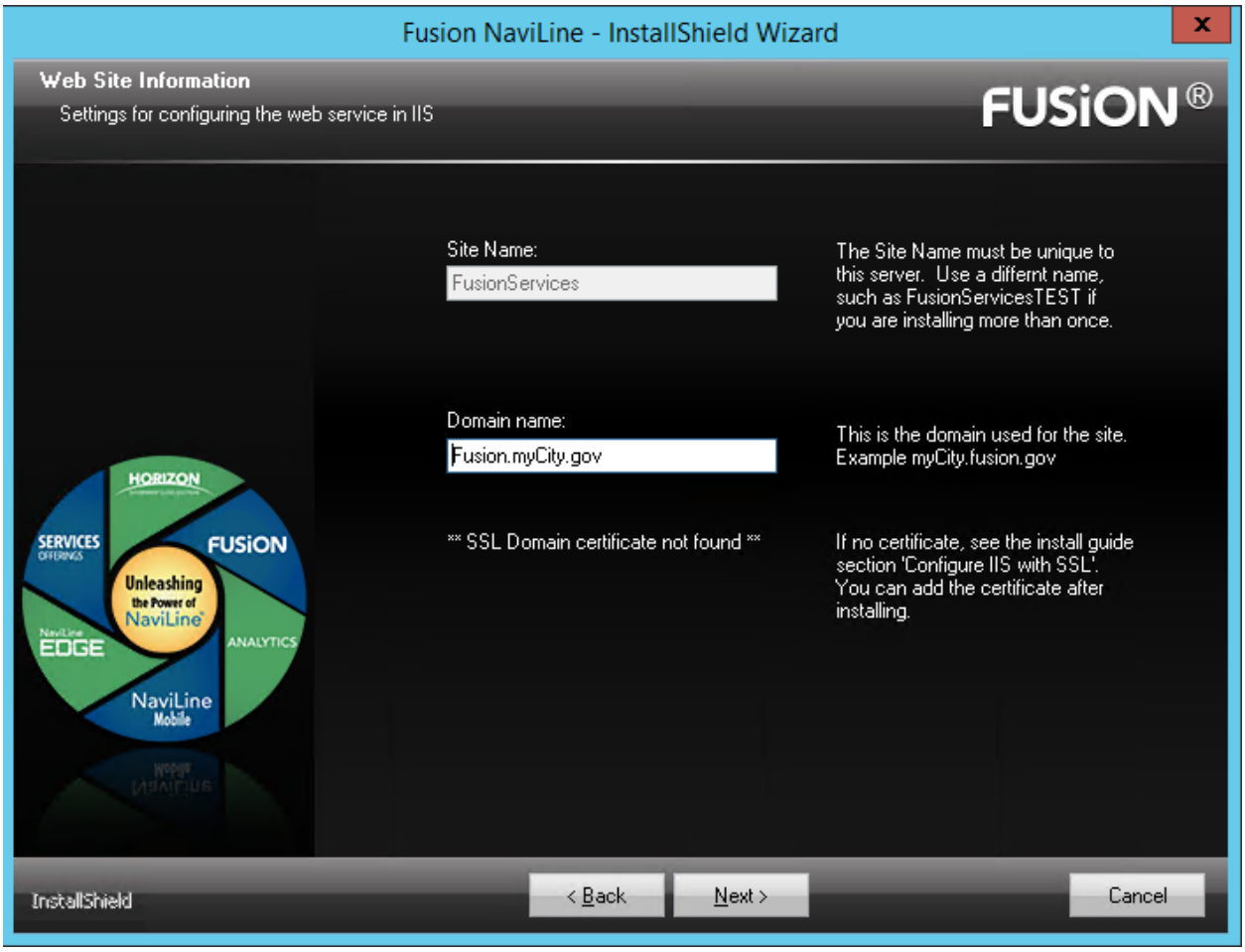


Site Information

Confirm that the **Site Name** is the correct one for the site you are trying to change.

Enter the **Domain Name** used by your site's SSL certificate. This will determine the URL needed to externally access the fusion services. By default, this is myCity.Fusion.gov, and the resulting URL would be https://myCity.fusion.gov/FusionServices. This needs to be changed to your domain name.

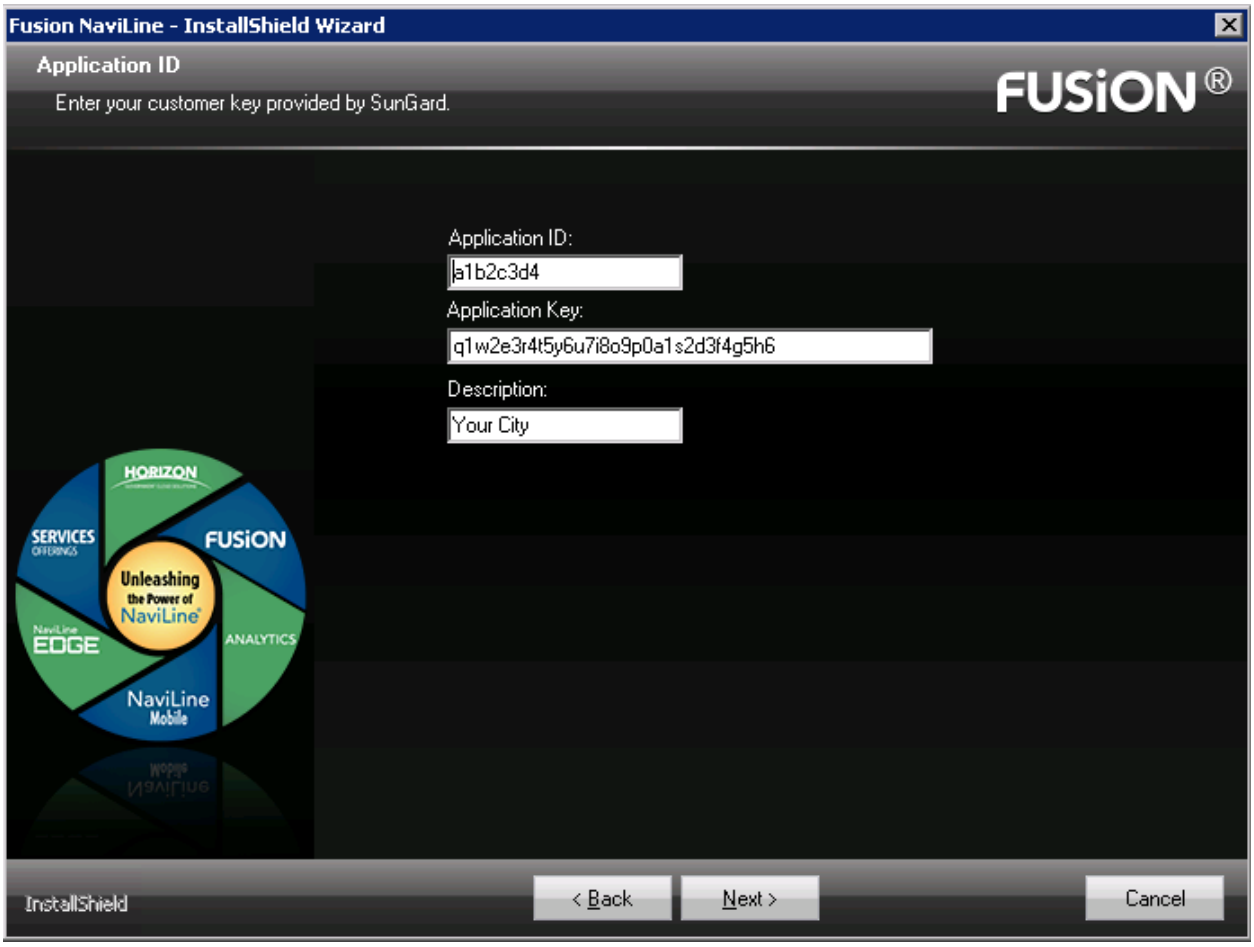
The **SSL Domain Certificate** message wil indicate if it found the certificate in IIS or not. If the certificate is not found after you entered the domain name, see the section ***Install an Internet Server Certificate*** to enable it for Https security.



Click **Next** to continue.

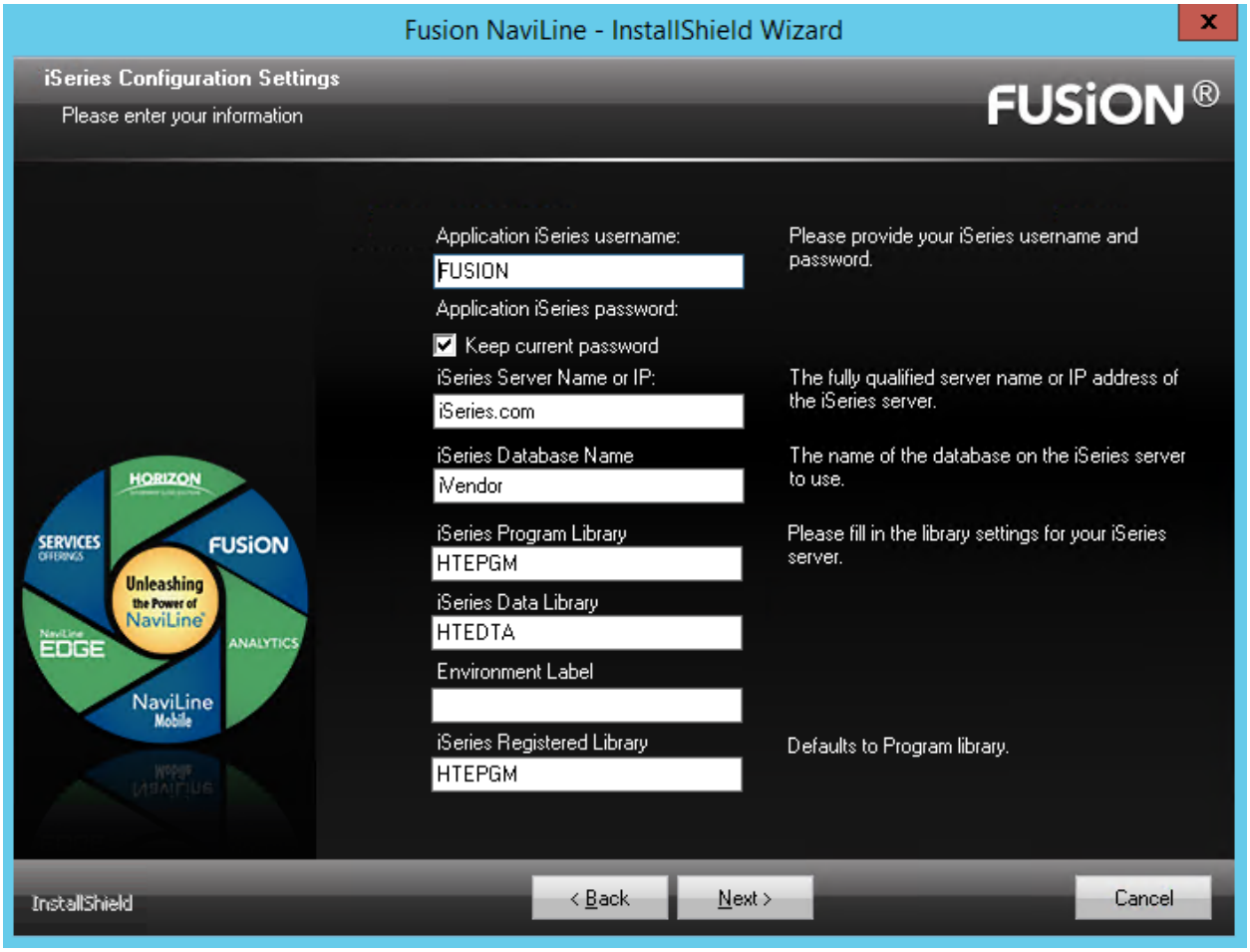
Application ID

An application ID and application key will be provided to you when you purchase Fusion through CentralSquare. This information is from item 1 in your configuration checklist. Both fields are required.



iSeries Configuration Settings

The iSeries Configuration Settings dialog displays the iSeries information that is read from the currently installed applications. This should match the iSeries information from items 2a-2h in your configuration checklist.
If the information is not correct, change it so that the applications will be set to the correct iSeries settings. To change the password, uncheck the **Keep current password** checkbox and the password field will appear instead. This information is used to configure the Fusion services to communicate with the iSeries. All fields are required except the environment label. If your iSeries requires an environment label, fill it in.

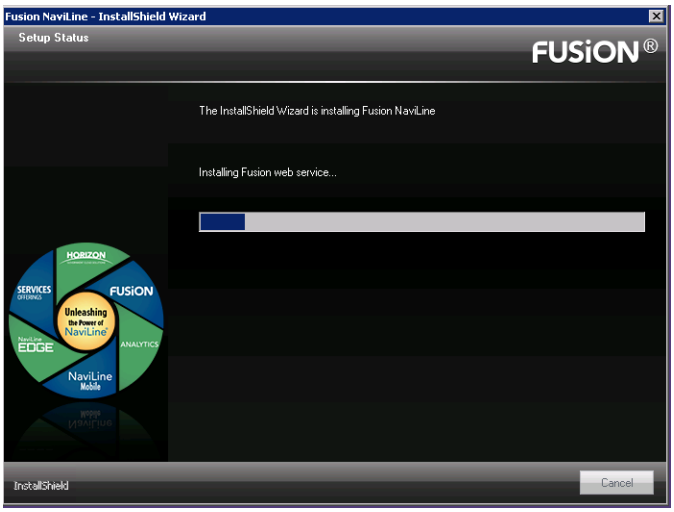


Configuration Settings

Enter the NaviLine server information from item 3a in your configuration checklist. This information is used to configure the Fusion services to communicate with the NaviLine server for file attachments. If you do not have a NaviLine server, enter localhost to continue.

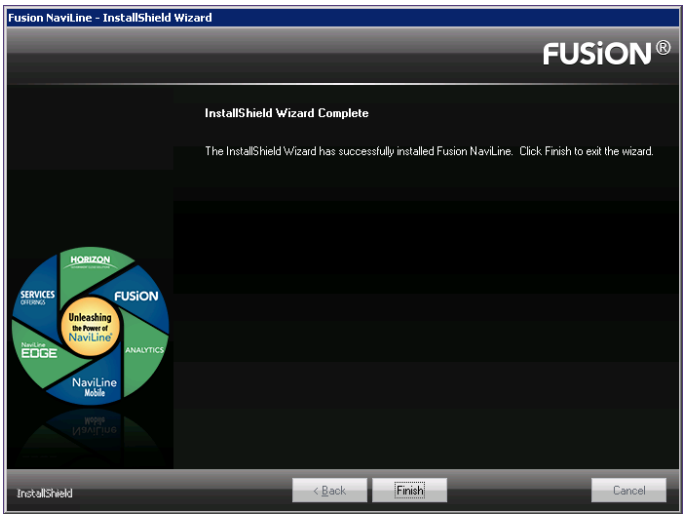
Installation

The installer will deploy the latest Fusion service files to IIS, then set the configuration values. If this is an upgrade or maintenance, then it will back up the previous files before making any changes. The installer displays what it's doing above the status bar. This should only take a few minutes.



Complete

This screen displays once the installer has completed installation and configuration.



Click **Finish** to end the installation. Click here: *Verify the installation* to continue to the post-install instructions.

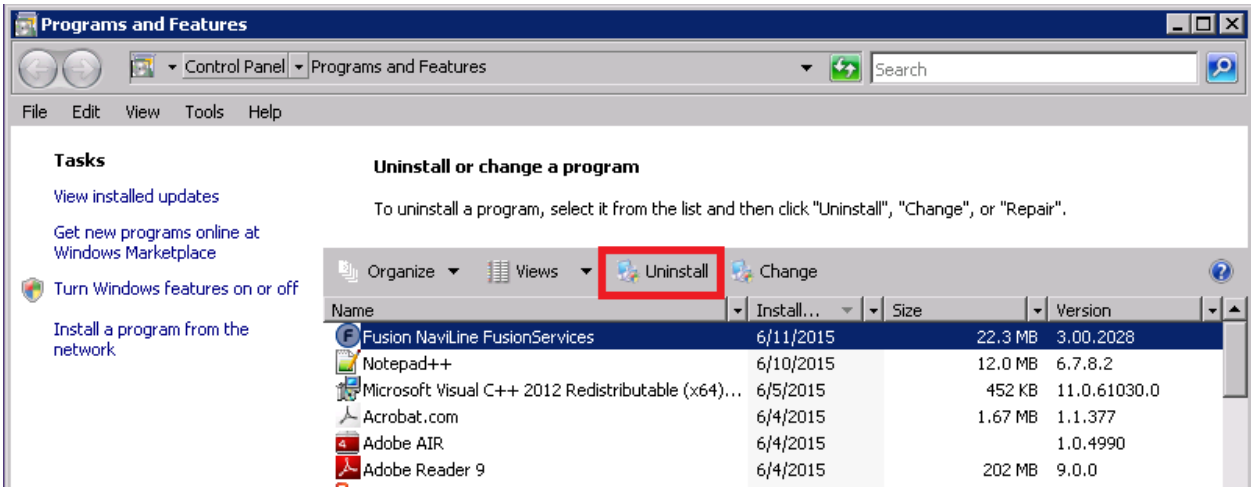
To uninstall

If you want to uninstall the Fusion services, this section guides you through the steps required.

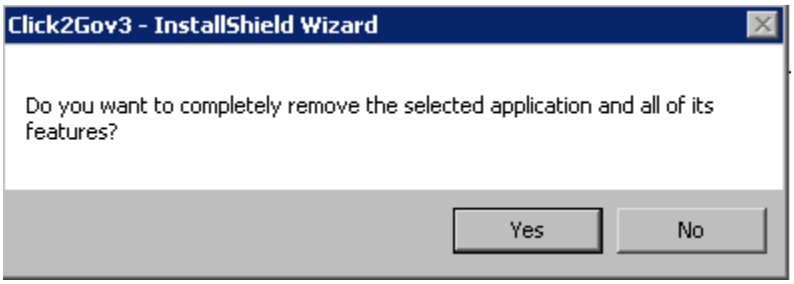
Starting the installer

You do not need the Fusion install package to change the applications. Simply go to the **Programs and Features** option in Windows Control Panel. On the Windows **Start** menu, select **Control Panel**. Then select **Programs and Features.**

In the Programs and Features window, select the Fusion application, then click **Uninstall**. This starts the installer.



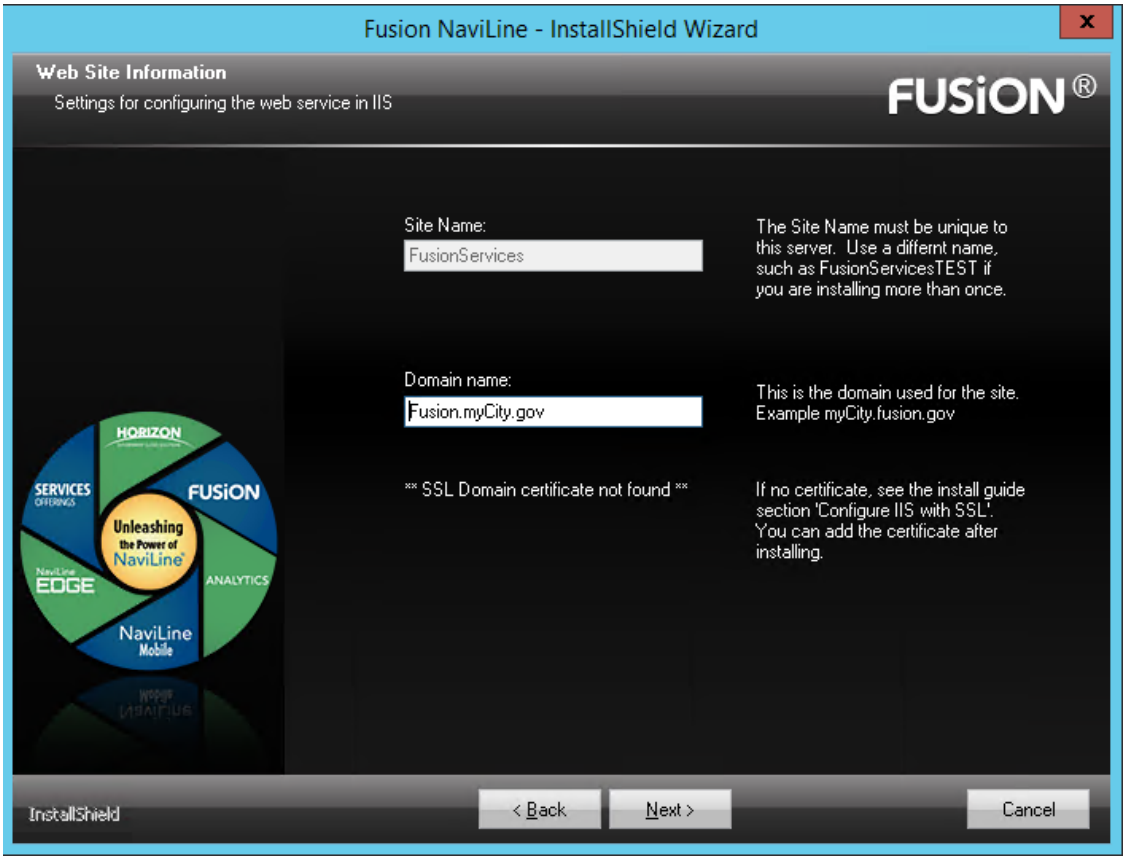
Click **Yes** to confirm that you want to uninstall Fusion.



Install Questions

Site Information

Confirm that the **Site Name** is the correct one for the site you are trying to remove.

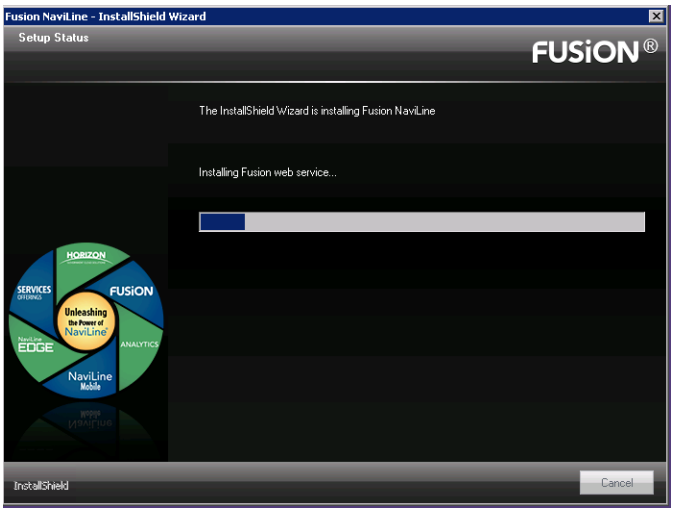


Click **Next** to continue.

The installer will immediately begin the uninstalling after you click **Next** to confirm. It will show the progress as it is uninstalling the files.

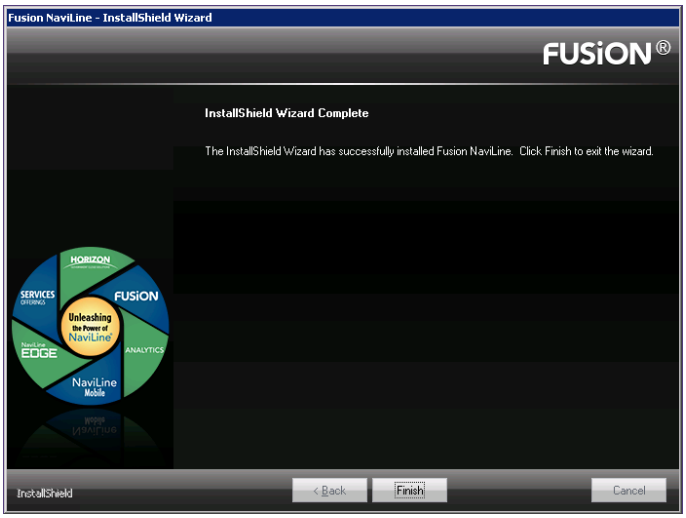
Installation

The installer will deploy the latest Fusion service files to IIS, then set the configuration values. If this is an upgrade or maintenance, then it will back up the previous files before making any changes. The installer displays what it's doing above the status bar. This should only take a few minutes.



Complete

This screen displays once the installer has completed uninstallation.



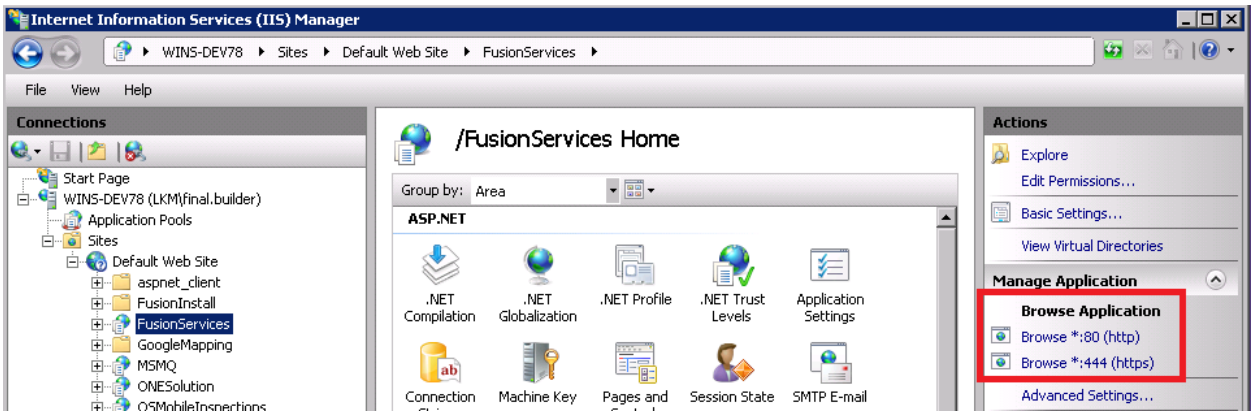
Click **Finish** to end the installation.

Verify the installation

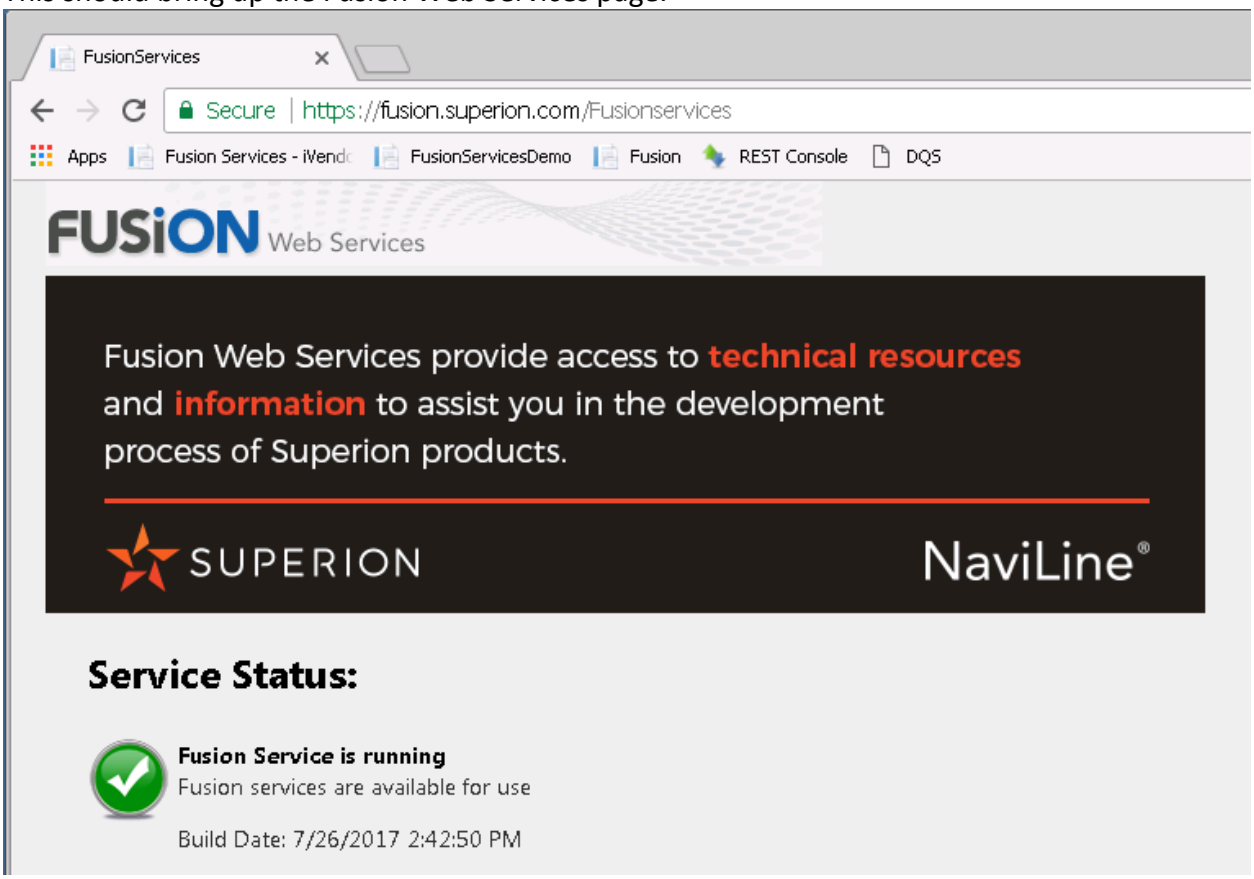
Verify the Fusion service

You can test that the Fusion service is installed by browsing it through IIS.

In IIS, select **FusionServices** under **Default Web Site**, and click **Browse** to browse the application using either http or https.

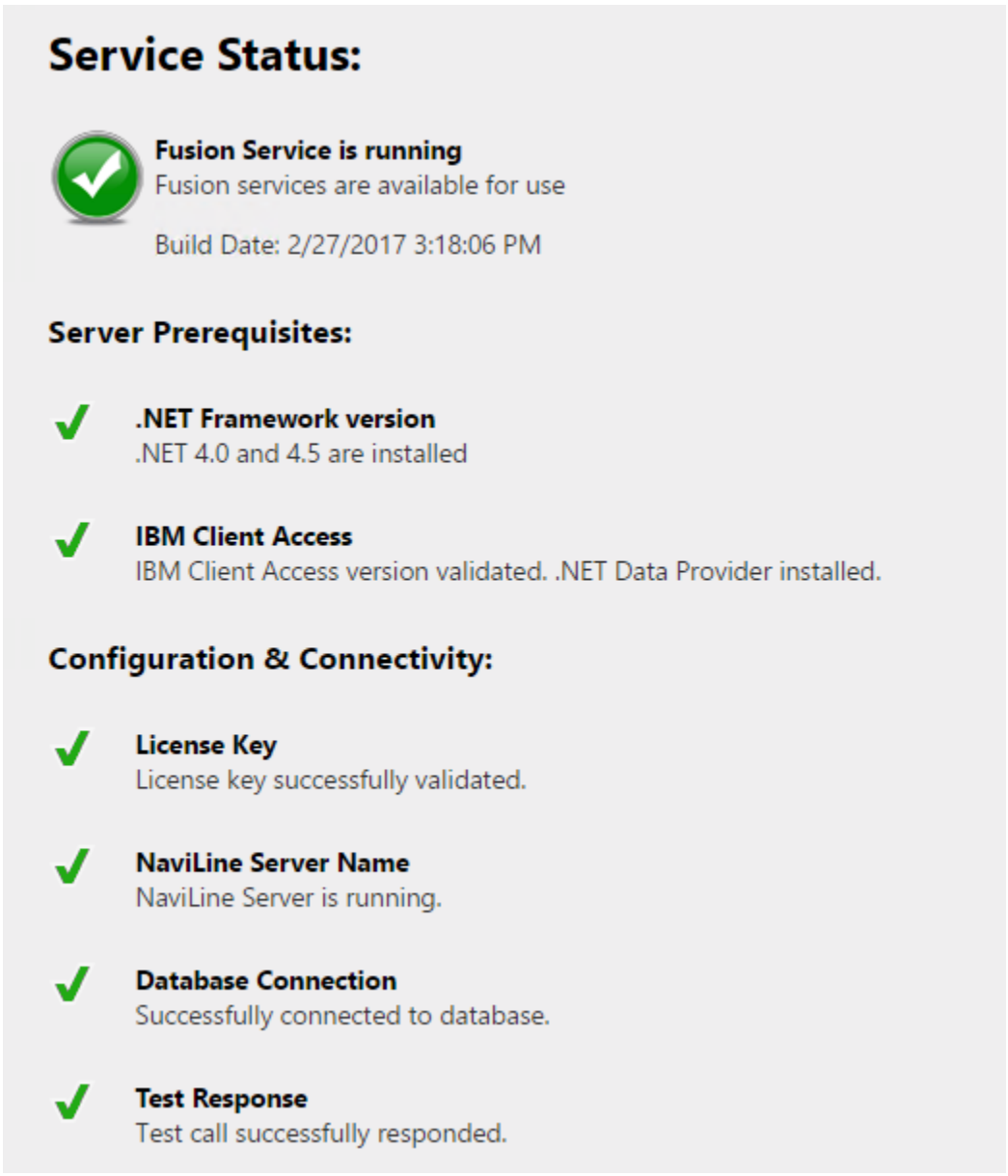


This should bring up the Fusion Web Services page.



Under the logo, there is a Service Status section. This page runs some basic test to verify that the pre-requisites are installed, and the configuration information is correct. If any of these show an error, review the configuration information you entered during the install, or see the

Prerequisites section for how to install missing prerequisites.



Verify https and the SSL certificate

You can test that the Fusion service is able to respond through the https URL by entering the URL below into an IE browser. This should bring up the diagnostics page shown above.

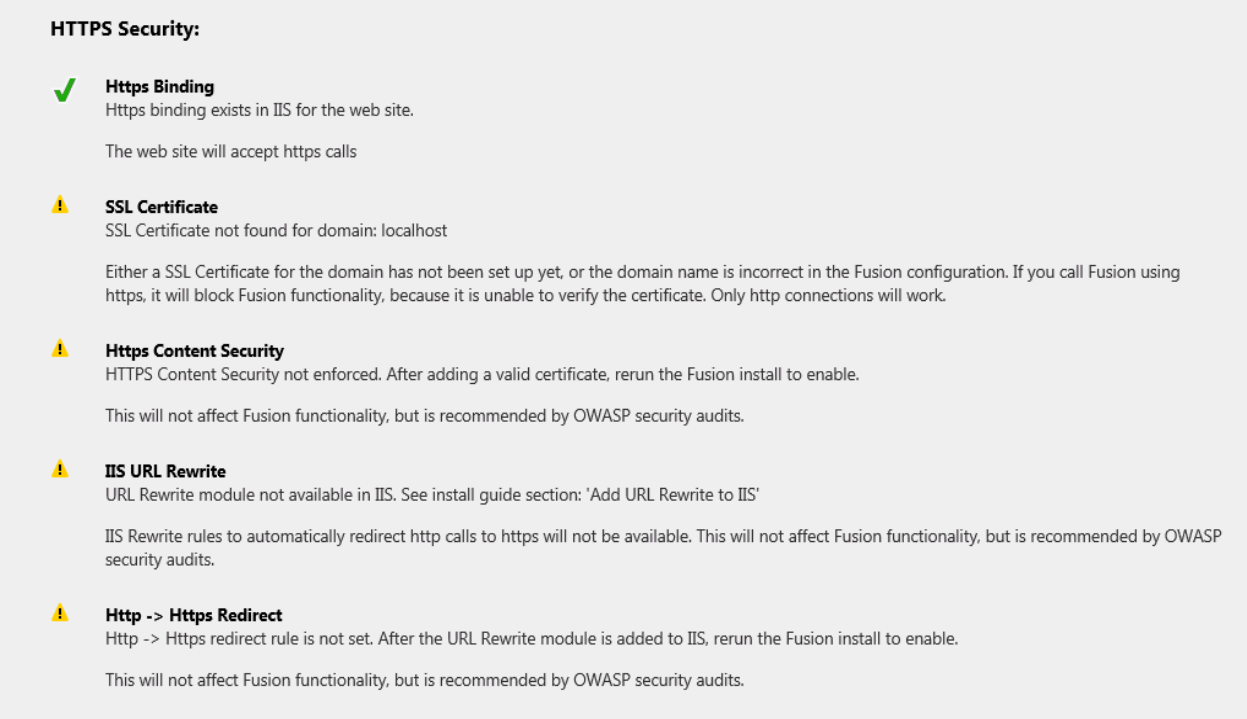
https://servername:443/FusionServices

Once you have your SSL certificate installed, you can test that the Fusion service is able to respond through the https URL by entering the URL below into an IE browser. This should bring up the diagnostics page shown above.

https://domainname.com/FusionServices

HTTPS Security

The Fusion service page will test for the HTTPS Security status. This checks if https and the SSL certificates are setup in IIS, along with other OWASP security standards.



Https Binding

On the Default Web Site in IIS, you have to add a Binding for https. It will not respond to https calls without the binding. Only http calls will work. See ***Add Https Binding***.

SSL Certificate

In IIS, you have to add the SSL certificate for your domain. Without the SSL certificate, if you call Fusion using https it will block Fusion functionality because it is unable to verify the

certificate. Only http connections will work. See ***Domain name*** and ***Install an Internet Server Certificate***.

Https Content Security

Https Content Security prevents external malicious scripts from being displayed on the Fusion service page. This is an OWASP security standard. It will not affect Fusion functionality.

To remove the warning, once you have added the SSL certificate for your domain, rerun the Fusion install ***To change configuration information***. Make sure the **Domain name** is entered, and that it finds the SSL Certificate. Continuing with the install will add the Https Content Security settings.

IIS URL Rewrite

URL Rewrite is a plug-in to IIS. You have to download and install it. See ***Add URL Rewrite to IIS.*** This is used to redirect http calls to https for OWASP security. This will not affect Fusion functionality.

Http -> Https Redirect

This automatically redirects any Http calls to use Https security. It requires the URL Rewrite plug-in above. This is an OWASP security standard. It will not affect Fusion functionality.

To remove the warning, once you have added the SSL certificate for your domain and installed the URL Rewrite plug-in, rerun the Fusion install ***To change configuration information***. Make sure the **Domain name** is entered, and that it finds the SSL Certificate. Continuing with the install will add the Https Content Security settings.

Verify the services are responding

To verify and test that the Fusion services are responding, see the ***REST Console Extension*** instructions in the next section.

You will NOT be able to browse any of the method URLs directly. I.e. entering: http://localhost/FusionServices/v2/Naviline/Utilities/NotificationSettings

into a browser will give you a page not found error. This is by design. Since this is a web service, and not a viewable application, it does not have viewable pages for each URL. As a service, it handles and processes the URL calls internally, which is why you need either the REST Console or your code sample to call the method.

REST Console Extension

This is a free web application available in Google Chrome that you can Download and use to test sending the service calls and see the JSON output that the services return.

The application presents a page that allows you to enter information that would normally be sent as part of the JSON request. The sections you will need to fill in values for are explained below.

Target

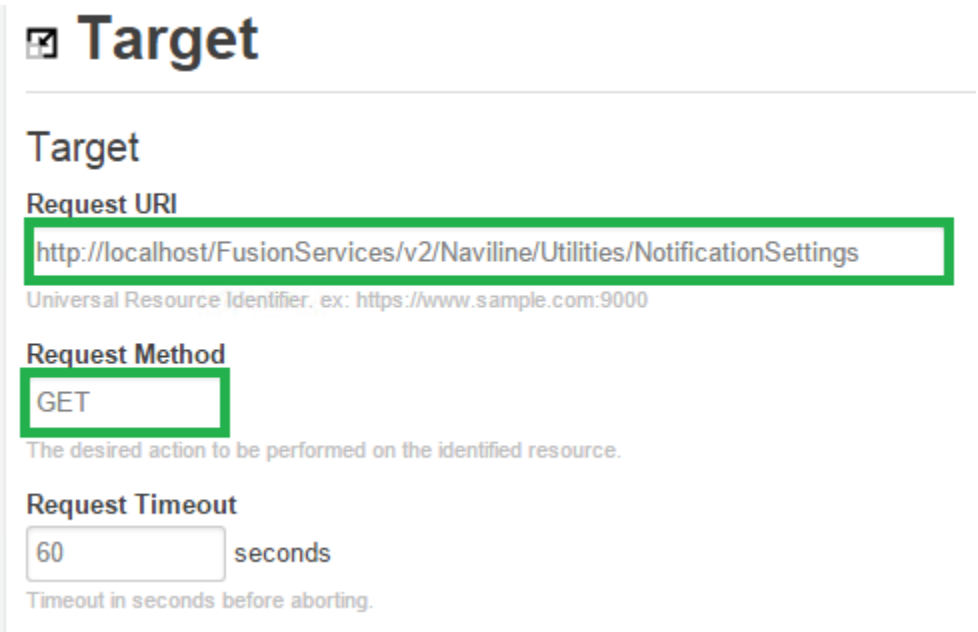
In the target section, you will fill in the URI for the service, and selecting either GET or POST as the Request method. The URL for each service is found in the Example section for the method on the Fusion documentation site http://fusion.CentralSquare.com/Fusion/. It also indicates if it is a GET or POST method.

From Fusion documentation:

Example

GET http://localhost/FusionServices/v2/Naviline/Utilities/NotificationSettings

In the REST Console:



Request URI

In the **Target** section, enter the URL into the **Request URI** field. Some of the service methods require values, such as account numbers, to be entered as part of the URL. If so, make sure the values are valid for your database, and that they are entered in the proper order.

Request Method

Select either **GET** or **POST**. The example in the Fusion documentation will indicate if it is a GET or POST method.

Body

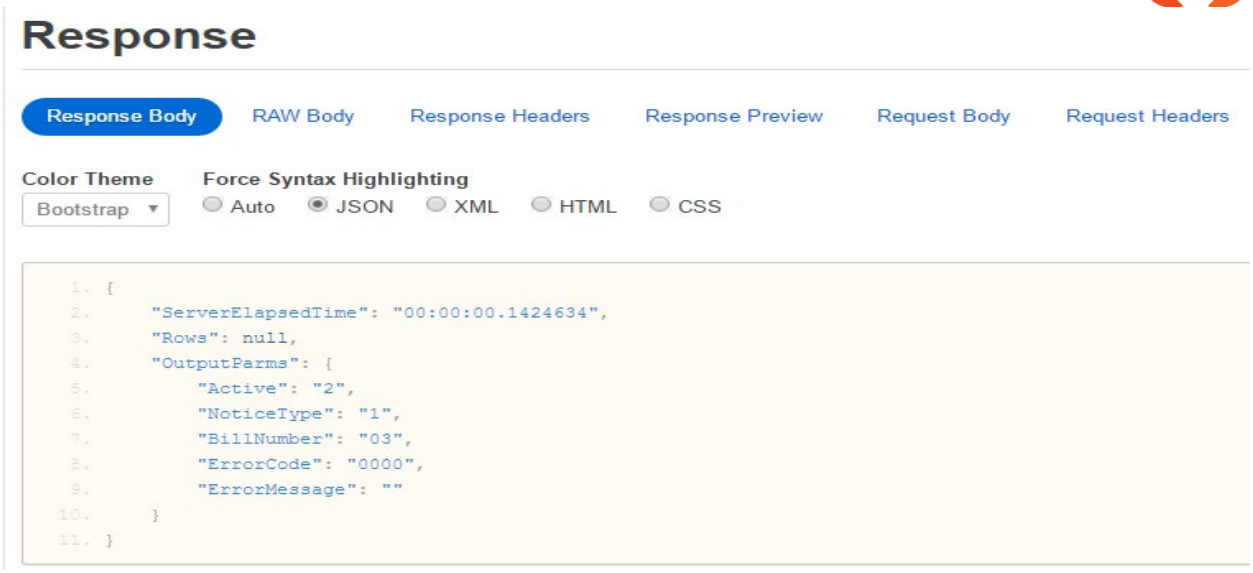
In the body section, you will fill in your APP ID and APP KEY, along with any other data to be passed to the method.

Custom Headers

You will need to enter your APP ID and APP KEY into the header information. The services require this to validate your license. Click the + button to add a new field to the Custom Headers section.
Enter X-APPID as the header name, and enter your APP-ID (short code) to the right.
Enter X-APPKEY as the header name, and enter your APP-KEY (long code) to the right.
You can enter these in any order.

Send

Click on the **Send** button to submit the request. The response will be returned at the bottom of the page.



Passing input paramaters

Services that use a **POST** request require paramaters to be sent to the service. These are listed as **Input Paramaters** in the method's documentation page. Some of the fields will be marked as **[Required]** and must be sent. The rest are optional.

Method PostSearchByAddress

Summary

Searches open permits by Street Number and Street Name

Remarks

This searches for open building permits by the street address. It will match any address that contains the street name.

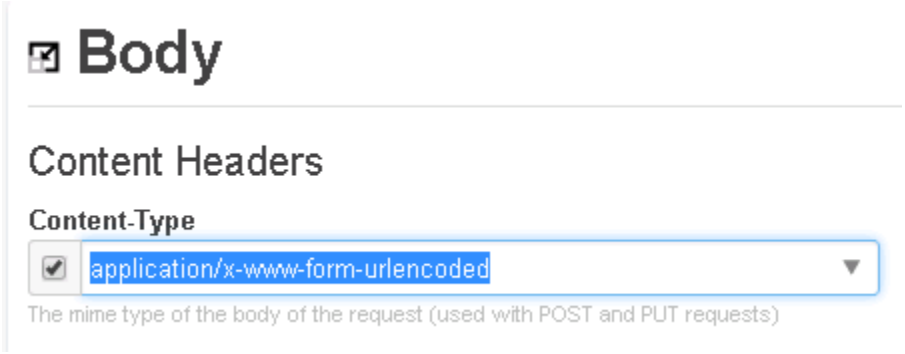
Input Parameters

Name	Type	Description
StreetName	System.String	[Required] Match street names beginning with this name.
StreetNumber	numeric	House or building number to search for.
StreetDirection	System.String	2 digit code indicating street direction: N, S, E, W, NE, NW, SE, SW
StreetSuffix	System.String	4 character street suffix. I.e. Bay, Dr, Lane, Rd, Way

To send the input parameters in the REST Console, you will need to enter the following fields:

Content Type

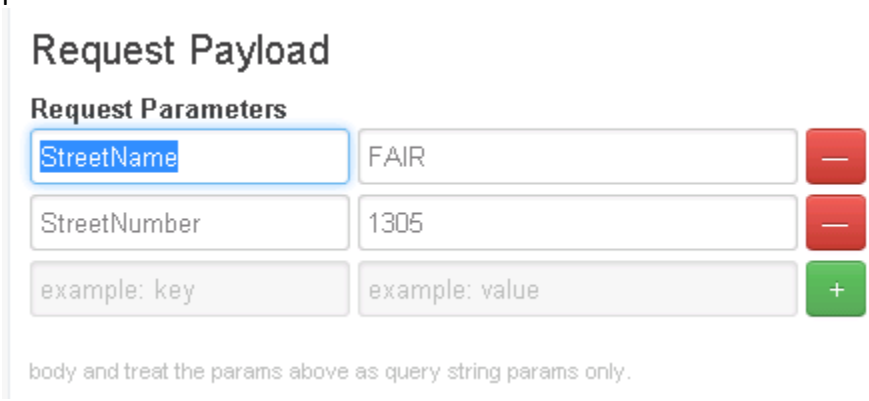
Set the **Content-Type** to **application/x-www-form-urlencoded**



Request Parameters

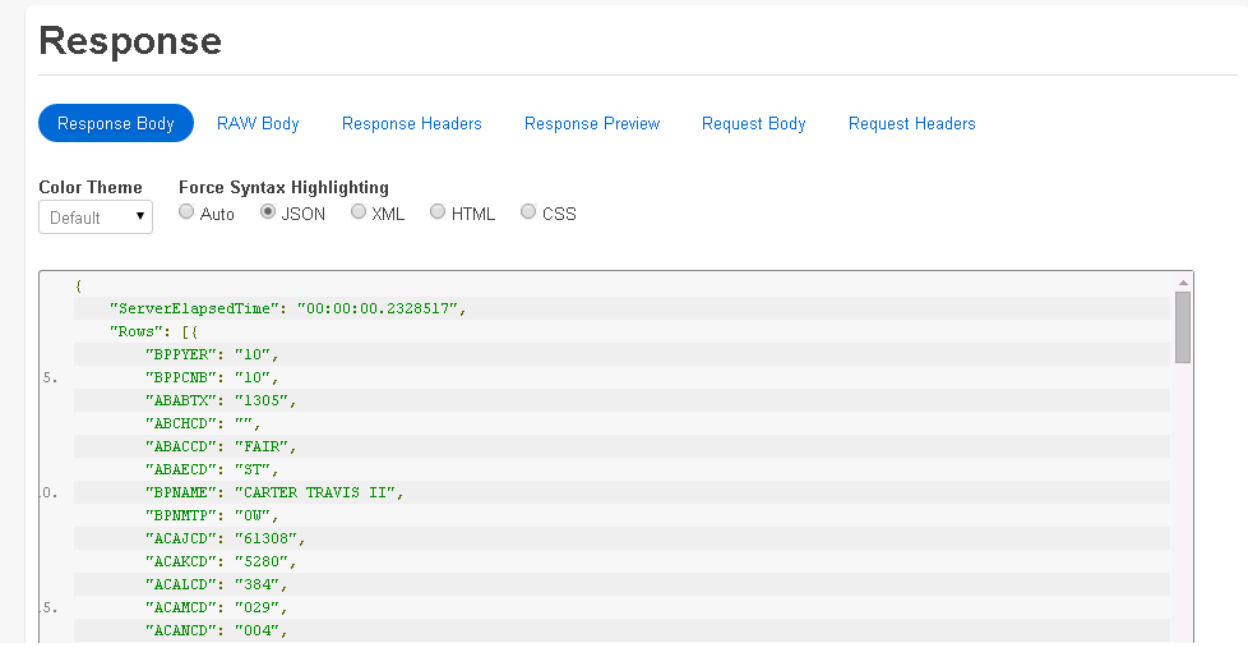
Under **Request Payload** > **Request Paramaters**, click on the add button + to add parameters.
Enter the name of the **Input Parameter** on the left, and the value on the right. The parameter name is not case sensitive, and the order the parameters are entered does not matter. The parameter value may be case sensitive depending on the method.

Click the add button to add more. Use the subtract button — to remove any unused parameters.



Send

Click on the **Send** button to submit the request. The response will be returned at the bottom of the page.

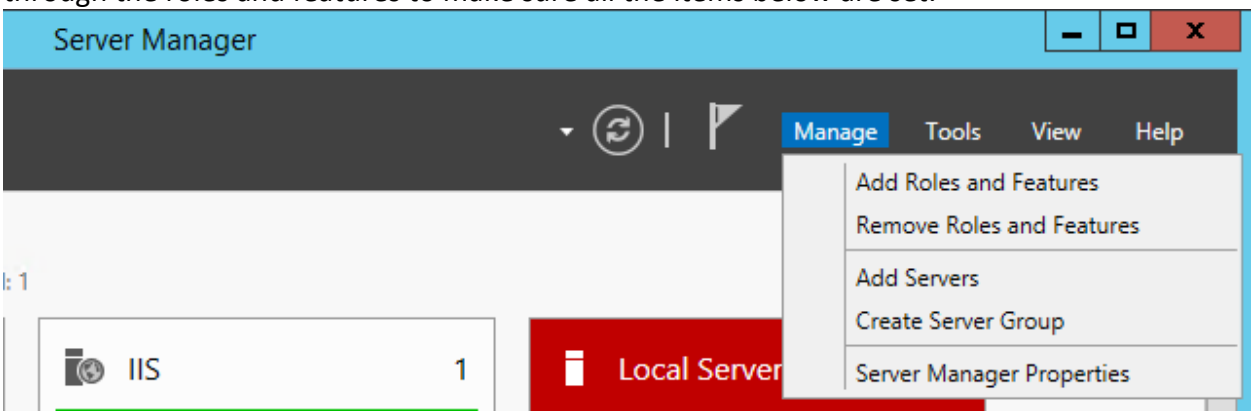

Response
Response Body
RAW Body
Response Headers
Response Preview
Request Body
Request Headers
Color Theme
Default
Force Syntax Highlighting
Auto
JSON
XML
HTML
CSS
{
"ServerElapsedTime": "00:00:00.2328517",
"Rows": [{
"BPPYER": "10",
"BPPCNB": "10",
"ABABTX": "1305",
"ABCHCD": "",
"ABACCD": "FAIR",
"ABAECD": "ST",
"BPNAME": "CARTER TRAVIS II",
"BPNMTP": "0W",
"ACAJCD": "61308",
"ACAKCD": "5280",
"ACALCD": "384",
"ACAMCD": "029",
"ACANCD": "004",

Appendix 1: IIS installation for Windows 2012

This appendix guides you through setting up the IIS, Web Deploy, and Microsoft .NET 4.5 prerequisites. These are installed by adding Roles and Features through Server Manager, or the the Web Platform Installer in IIS.

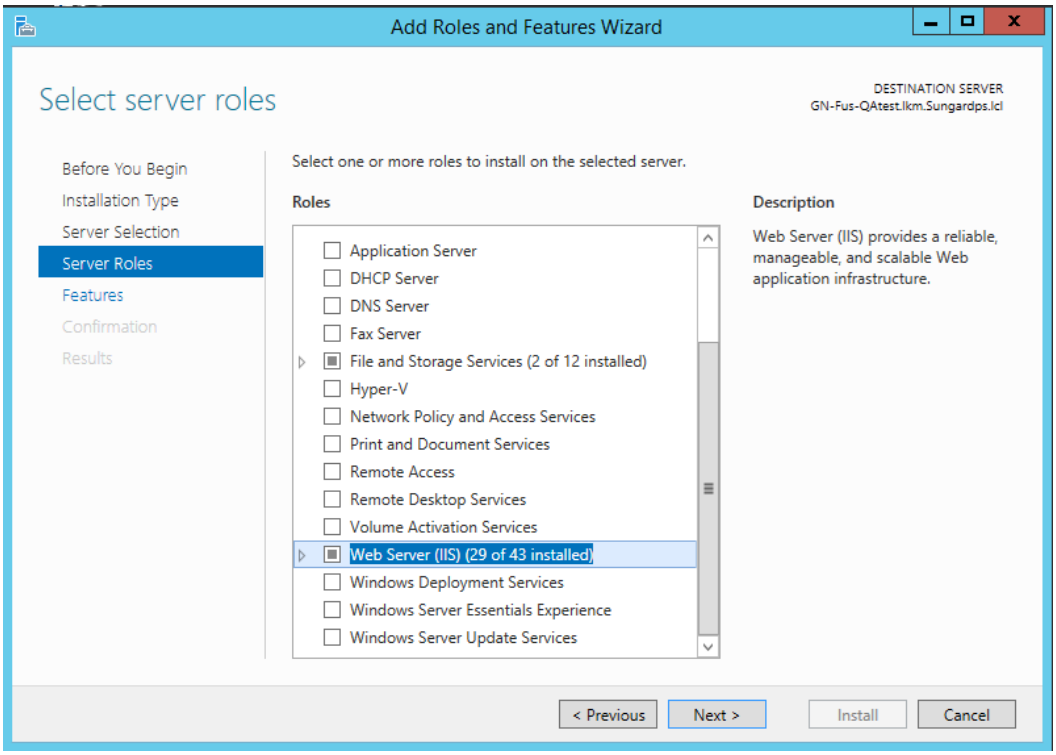
IIS Manager Roles and Features

Use the **Server Manager > Manage > Add Roles and Features** to enable the following roles and features. If IIS was previously installed, some options may be already checked. Please step through the roles and features to make sure all the items below are set.



Select the Web Server role.

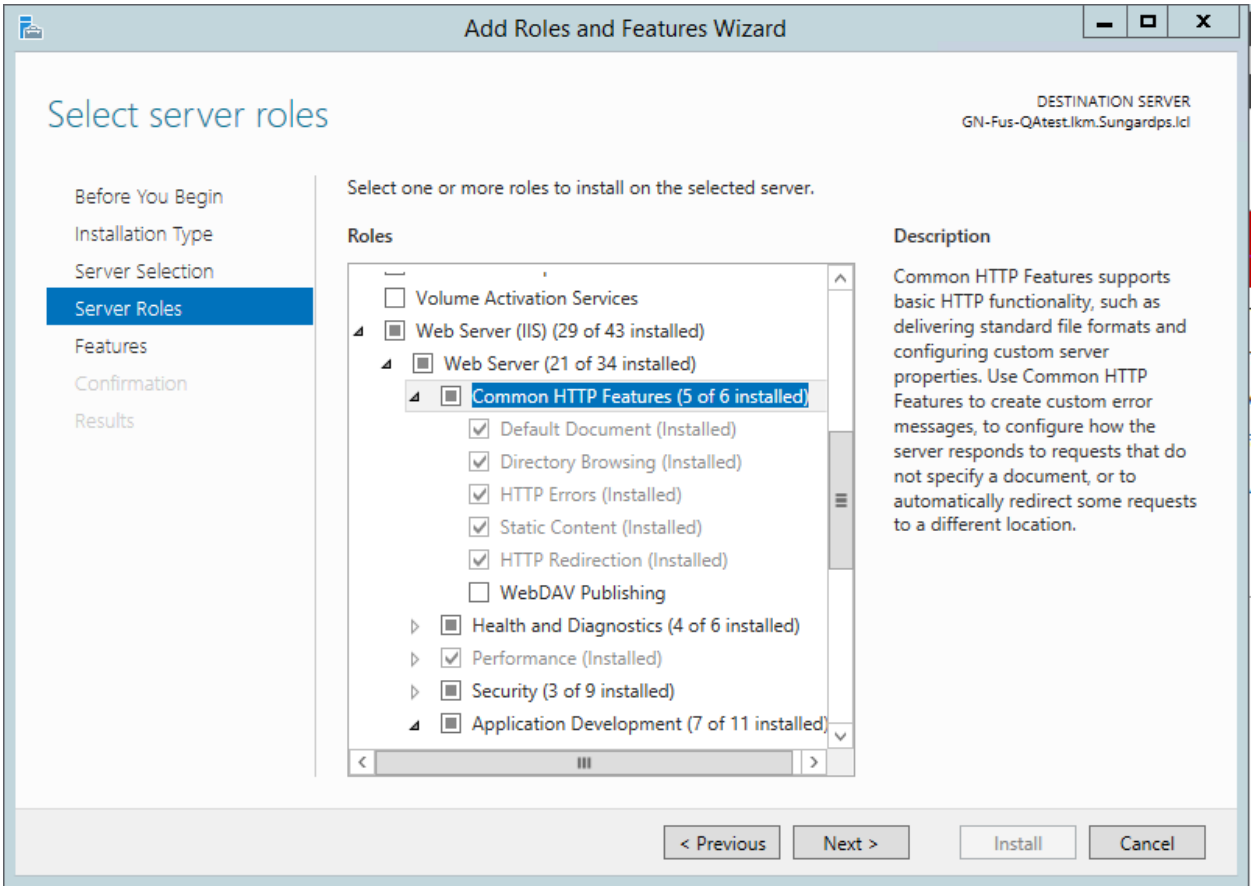
- Roles: Web Server



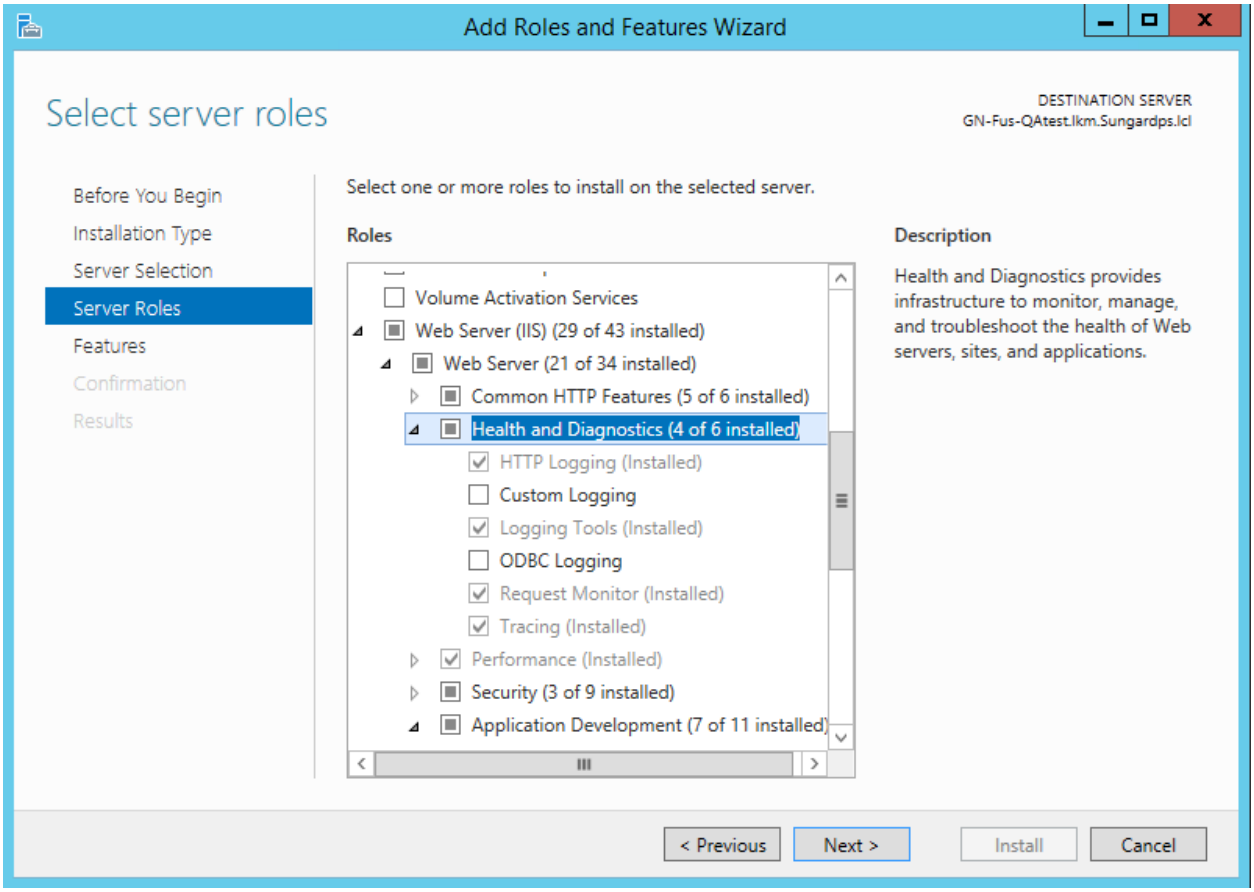
Set the Server Role options under Web Server.

Note: If this is the first time you are installing IIS, these options may not be available until after the Features dialog, which comes next. After selecting the features, it will prompt you to select the Web Server settings that are displayed here.

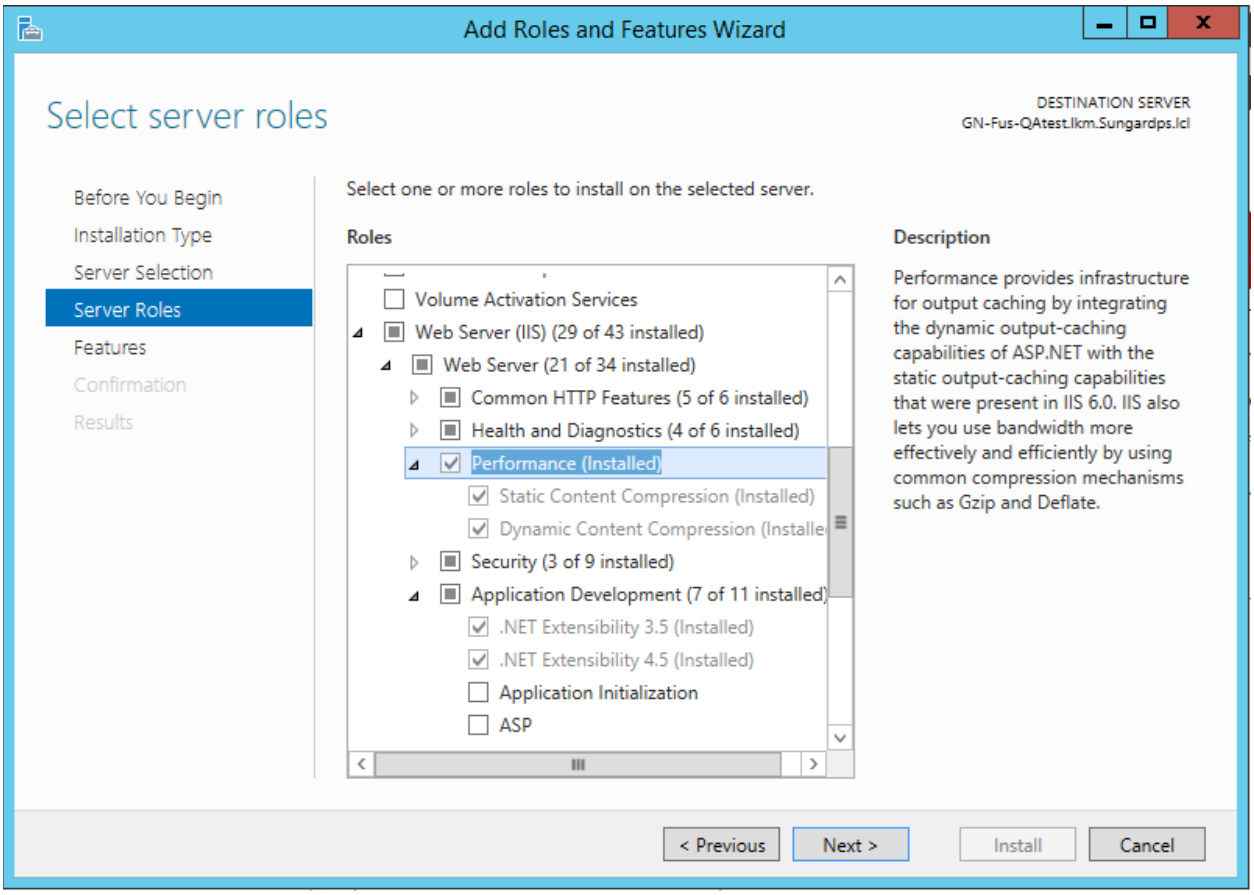
- Roles: **Web Server (IIS) > Web Server > Common HTTP Features**
  - Default Document
  - Directory Browsing
  - HTTP Errors
  - Static Content
  - HTTP Redirection



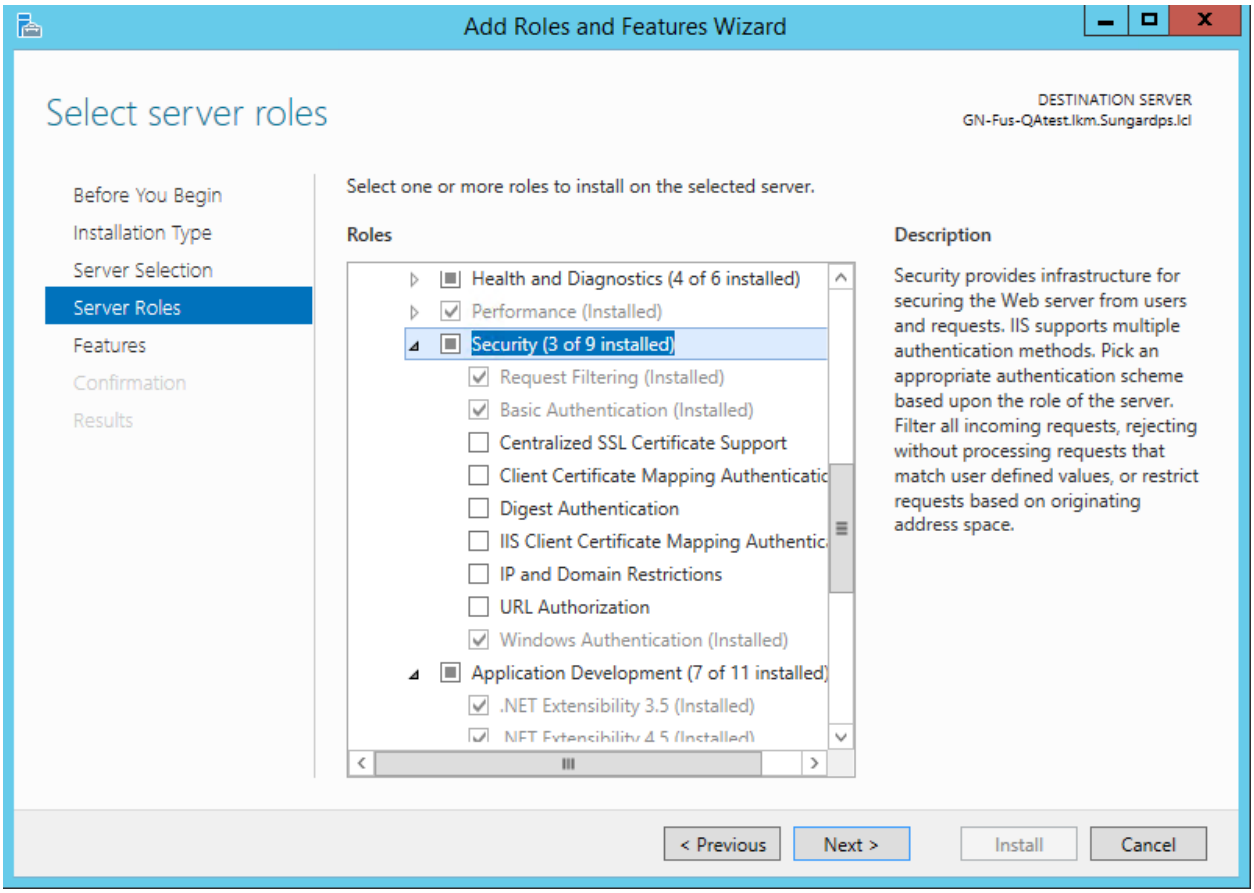
- Roles: **Web Server (IIS) > Web Server > Health and Diagnostics**
    - HTTP Logging
    - Logging Tools
    - Request Monitor
    - Tracing



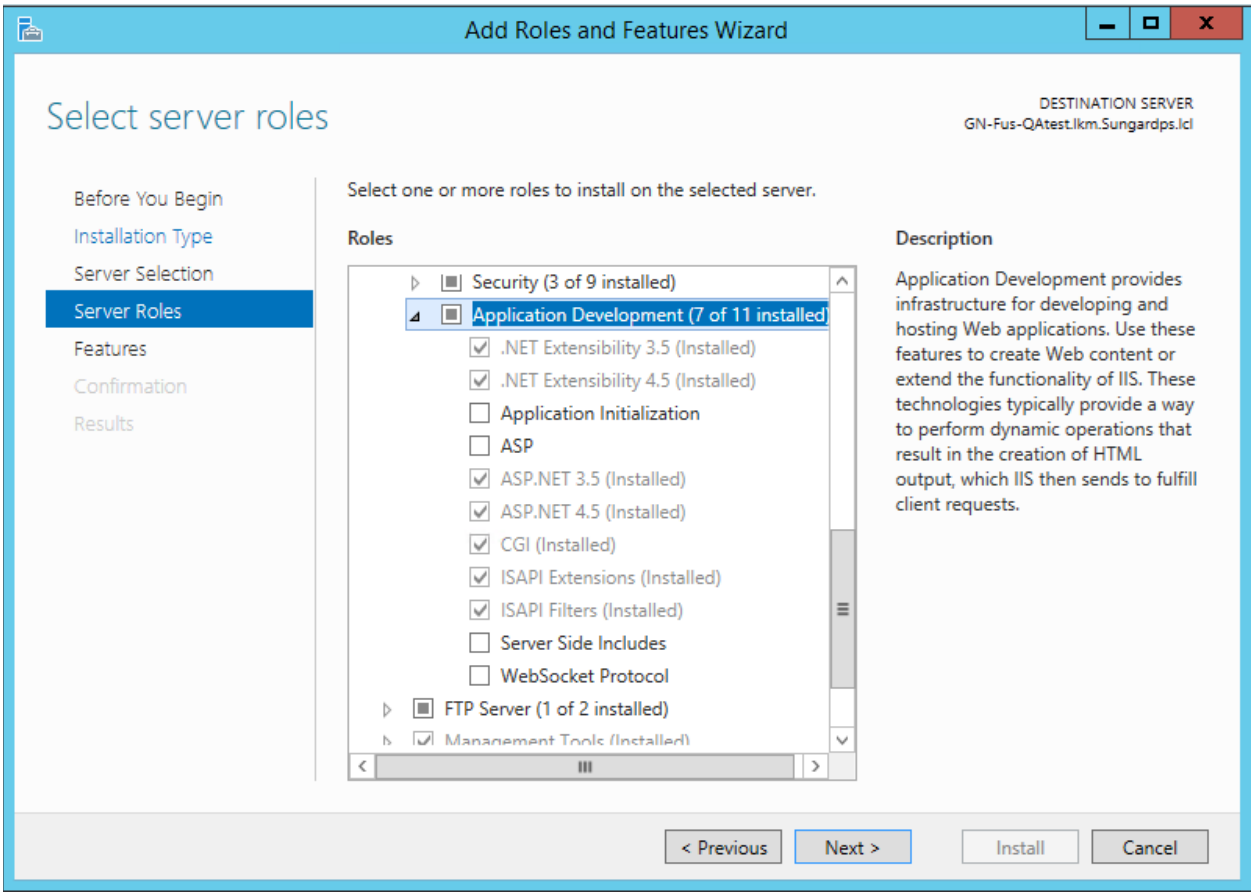
- Roles: **Web Server (IIS) > Web Server > Performance**
    - Static Content Compression
    - Dynamic Content Compression



- Roles: **Web Server (IIS) > Web Server > Security**
    - Request Filtering
    - Basic Authentication
    - Windows Authentication



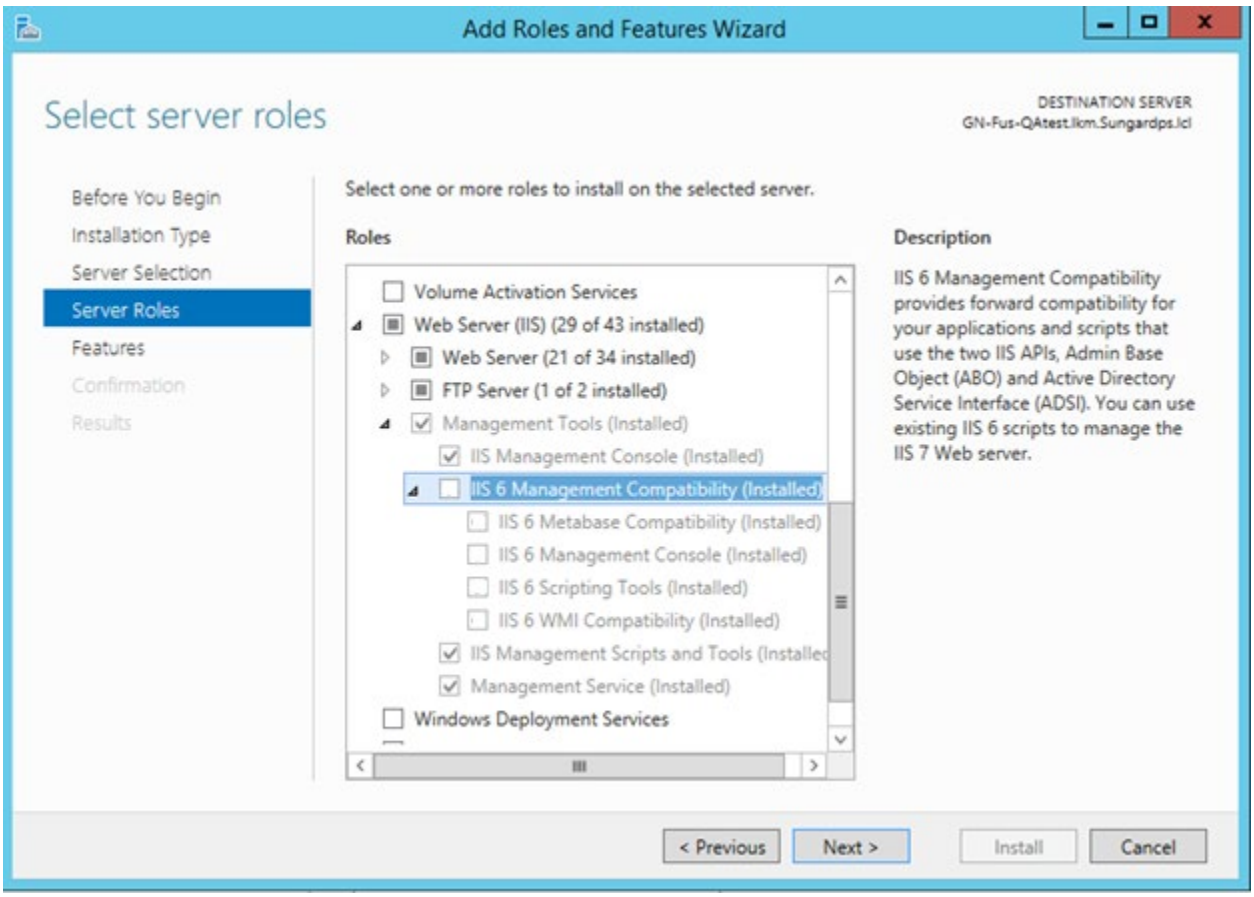
- Roles: **Web Server (IIS) > Web Server > Application Development**
  - .NET Extensibility 4.5
  - ASP.NET (Windows Server 2008)
  - ASP.NET 4.5 (Windows Server 2012)
  - Checking ASP.NET 4.5 will prompt to include the following pre-requisites
    - .NET Extensibility 4.5
    - ISAPI Extenstions
    - ISAPI Filters
  - CGI
  - ISAPI Extensions
  - ISAPI Filters



.NET Extensibility 3.5 and ASP.NET 3.5 are not required.

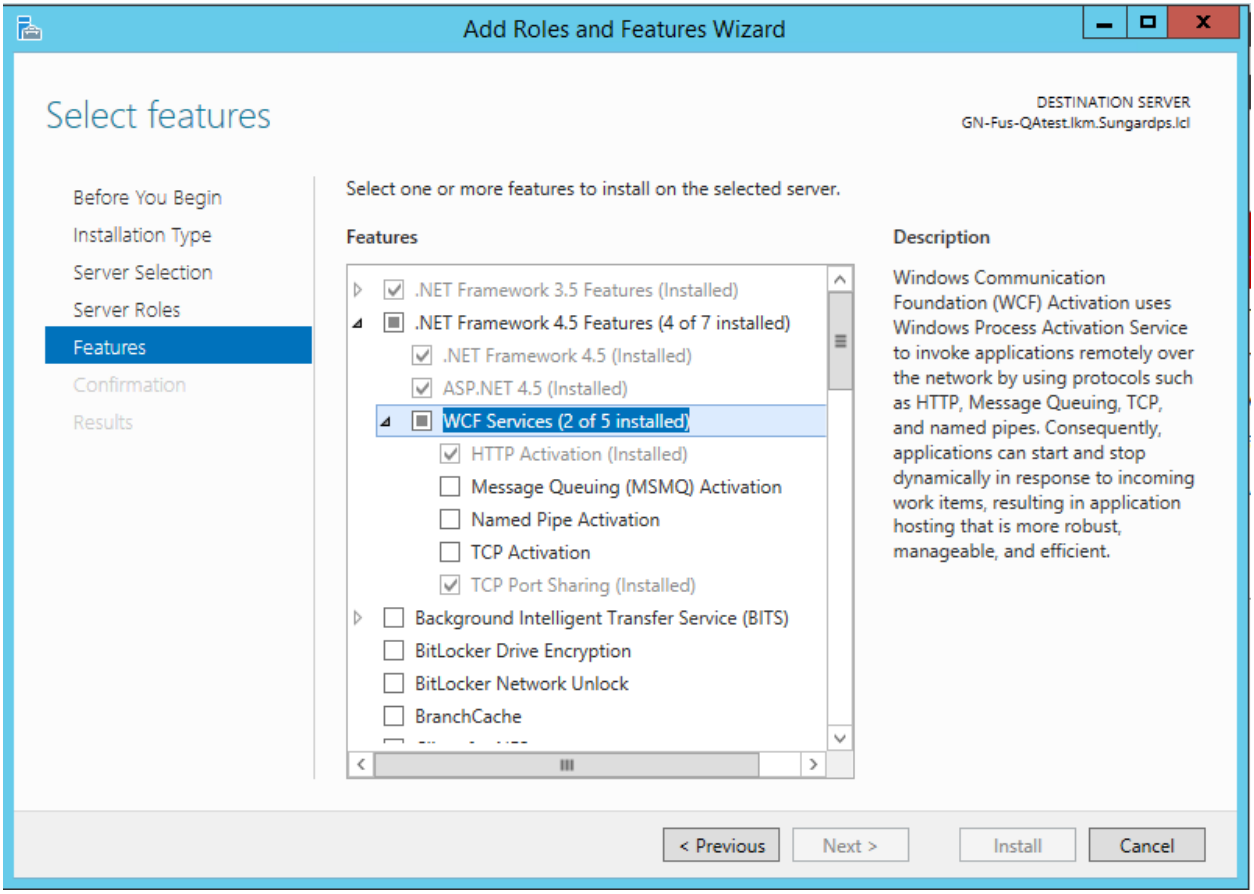
- Roles: **Web Server (IIS) > Management Tools**
  - IIS Management Console
  - IIS Management Scripts and Tools
  - Management Service

  IIS 6 Management Compatibility is NOT requrired



Set the Features options under Web Server.

- Features: **.NET Framework 4.5 Features > WCF Services > HTTP Activation**



Web Deploy

Web Deploy (msdeploy.exe) is used to deploy web applications to IIS. It is an IIS extension that is downloaded and installed separately. It should be located in one of the folders below if it is installed on your machine.

For Windows Server 2012

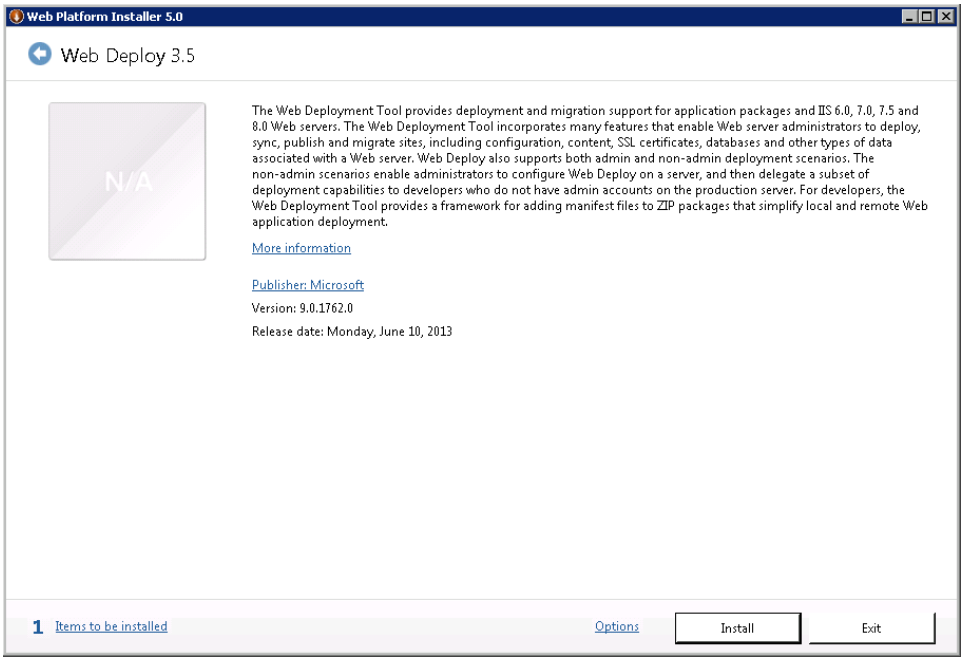
C:\Program Files\IIS\Microsoft Web Deploy V3\msdeploy.exe
C:\Program Files (x86)\IIS\Microsoft Web Deploy V3\ msdeploy.exe

Use Web Platform Installer to install Web Deploy along with its dependencies like the Web Management Service (WMSvc)

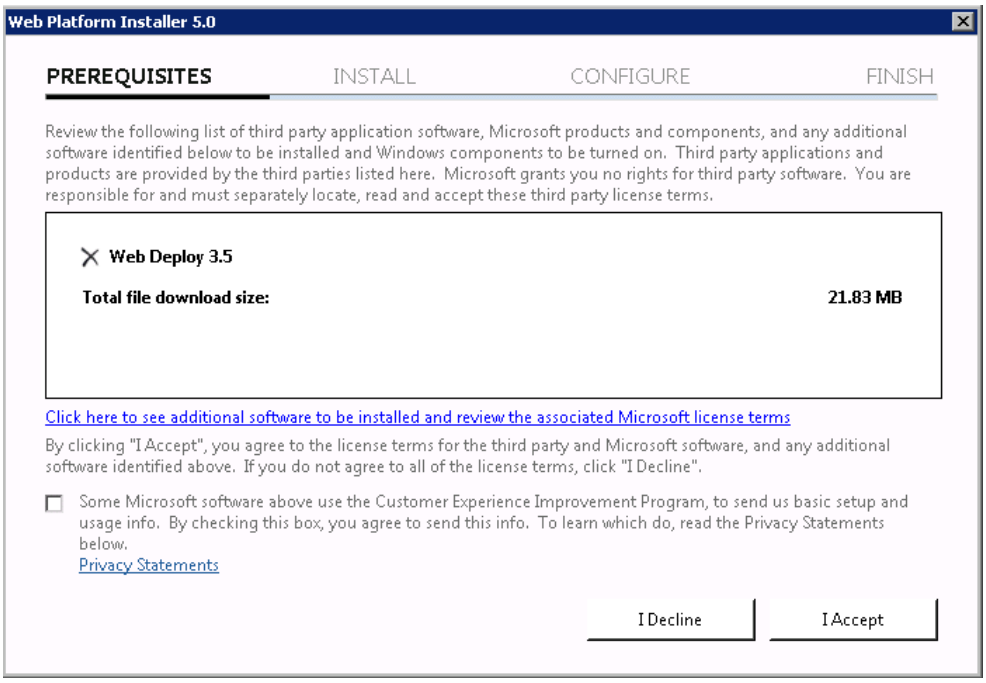
1. Click on the link below to go to the IIS Web Deploy download page.

   http://www.iis.net/downloads/microsoft/web-deploy
2. Click on the **Install this extension** button.
3. At the bottom of the browser, it will prompt you asking if you want to run or save the WDeploy.exe. Click **Run**.

4. The Web Platform Installer will come up.



5. Click on **Install**.
6. Click on I Accept to agree to the license agreements.

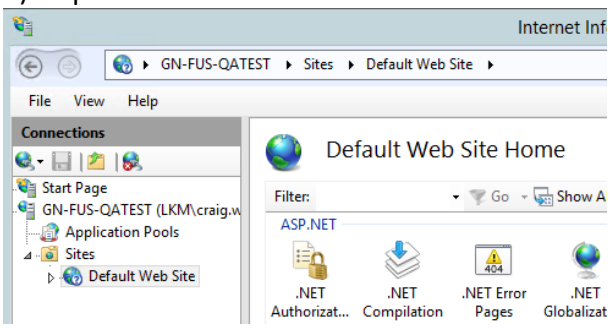


7. A progress dialog will appear. Click **Finish** when done.

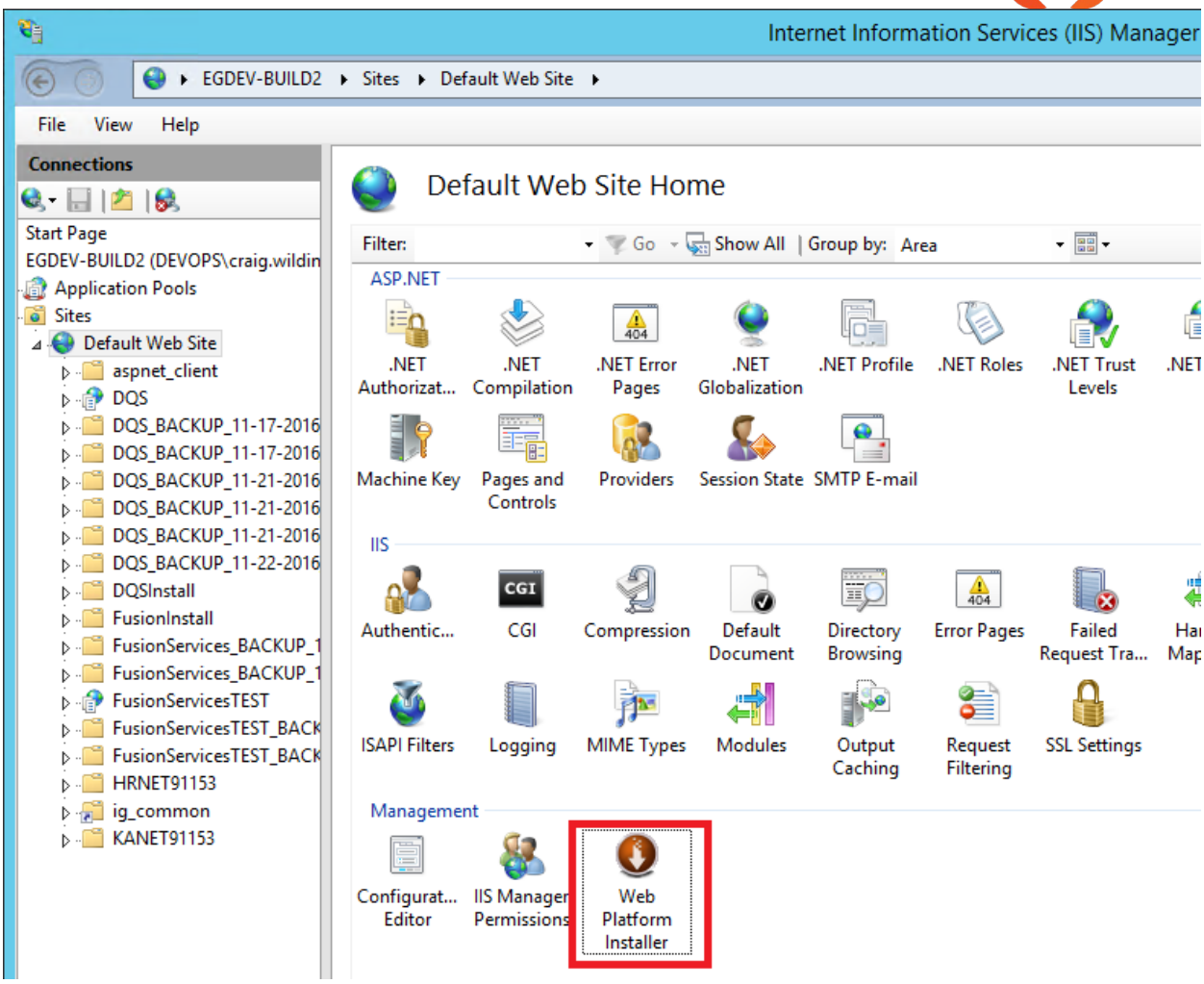
URL Rewrite

URL Rewrite is an IIS module that first needs to be downloaded and installed in IIS.

1) Open IIS and select the **Default Web Site**

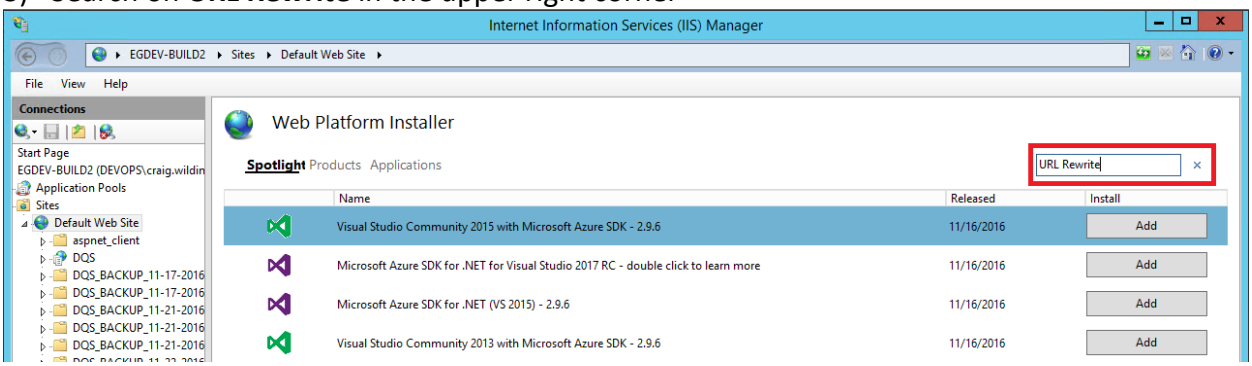


2) On the **Features View** tab, select **Web Platform Installer**

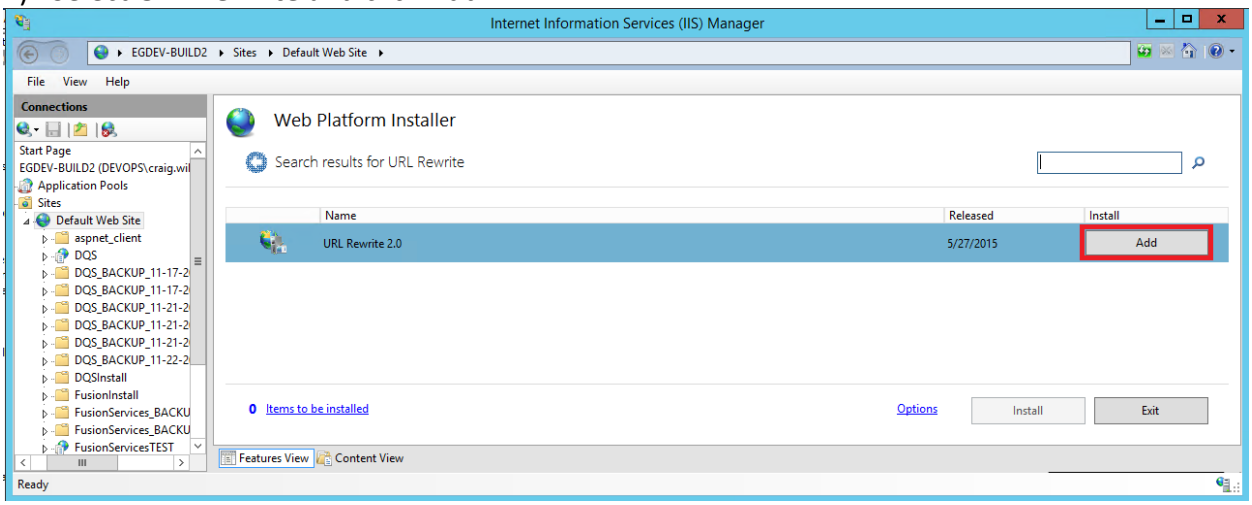


a) If you do not have the Web Platform Installer shown, you can download it here: https://www.microsoft.com/web/downloads/platform.aspx

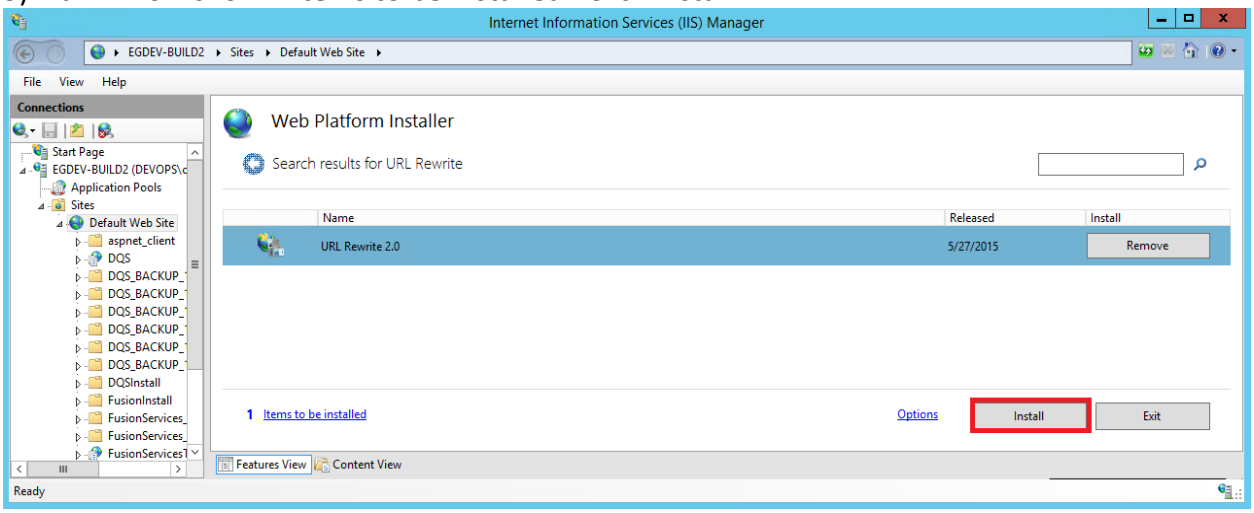
3) Search on **URL Rewrite** in the upper right corner



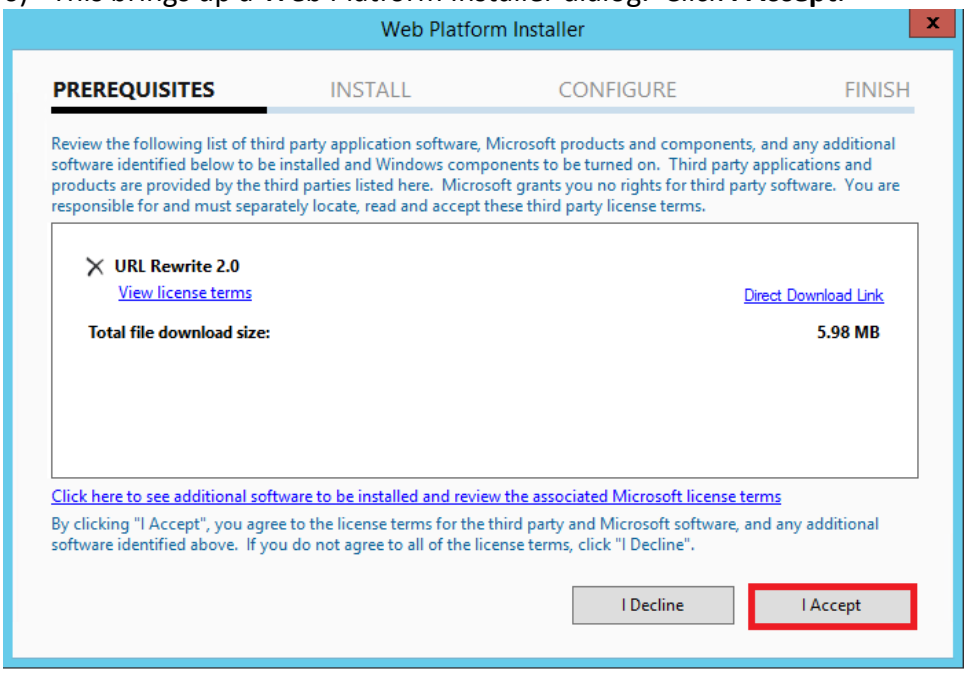
4) Select **URL Rewrite** and click **Add**



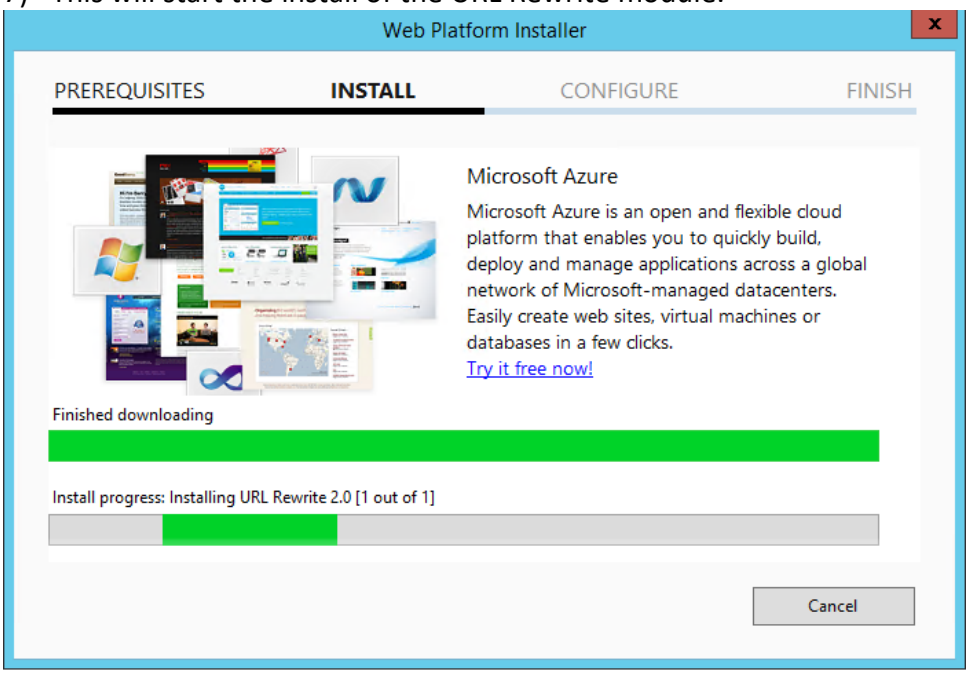
5) It will now show **1 items to be installed**. Click **Install**.



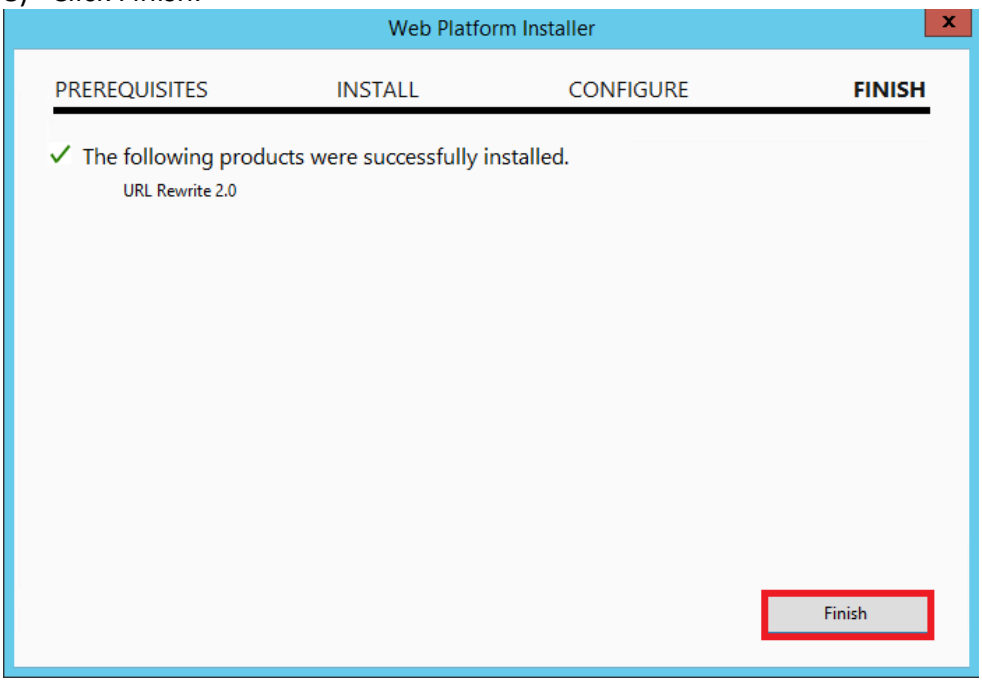
6) This brings up a Web Platform Installer dialog. Click **I Accept**.



7) This will start the install of the URL Rewrite module.



8) Click Finish.



Appendix 2: IBMi Client Access

IBM Client Access has been replaced with IBM Access Client Solutions. However, Fusion will still run with IBM Client Access V7R1. This section has instructions for installing IBM Client Access v7, and for obtaining the user, server, database, and library names from System Navigator.

IBM Client Access V7R1

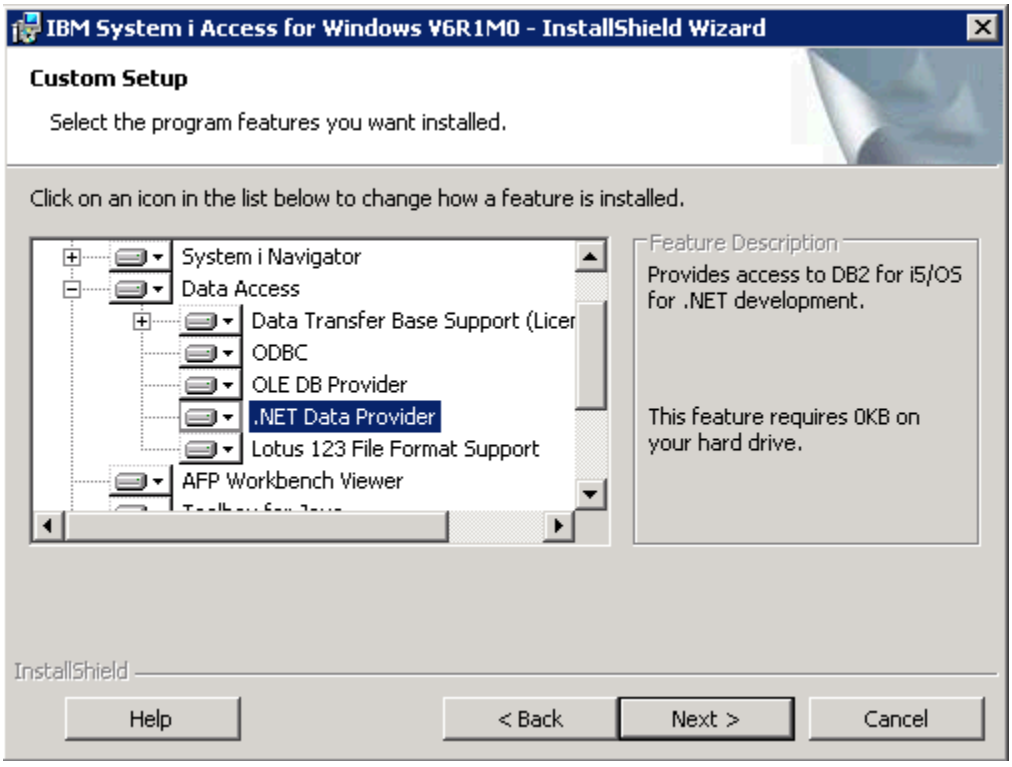
IBM Client Access is required for access to NaviLine. V7R1 is preferred as it resolves an error with the machine.config file noted below. If you use V6R1 be sure to install the latest v6 service patch. Fusion will not work with just the base v6 version.

This software should come with your iSeries setup and installation package. You can download the latest service pack from:

http://www-03.ibm.com/systems/power/software/i/access/windows_sp.html

Call the IBM Support Line at 1-800-IBM-SERV (1-800-426-7378) for more assistance.

During the IBM Client Access installation, the **.NET Data Provider** feature must be selected. This is selected by default if you select the 'Complete' option.



NOTE: If the IBM Client Access V6R1 is installed after IIS is installed, it may remove the permissions to the machine.config files. See the section ***Troubleshooting: HTTP Error 503. The service is unavailable***

iSeries Server Settings

You will need information about the iSeries server in order for Fusion to connect to it. You can retrieve this information from the **System I Navigator**.

iSeries user / password

This is an iSeries account that the Fusion service will use to connect to iSeries. No special permissions are needed. It will use the same permissions as any NaviLine or Select user.

To create a profile from scratch for Fusion, use the following command and parameters:

CRTUSRPRF USRPRF(FUSION) PASSWORD() INLMNU(*SIGNOFF) LMTCPB(*YES) TEXT('Fusion Service Profile') SPCAUT(*NONE) PWDEXPITV(*NOMAX)

Explanation:

5. For the usrprf parameter, the user name is: FUSION
6. INLMNU is the Initial Menu: We use *SIGNOFF to prevent someone from successfully logging into the IBMi profile interactively.
7. LMTCPB stands for Limited Capabilities: This reduces the capabilities of the profile which is very important to also use SPCAUT (Special Authority of *NONE).
8. PWDEXPITV stands for Password Expiration Interval: Always use *NOMAX.

If this is an existing Click2Gov3 customer, you can copy the profile using the “WRKUSRPRF” IBMi command as illustrated below and change the appropriate parameters:

Hit enter

Use option 3 to Copy the existing profile, then change the parameters as indicated above, making sure you use PgDn for more parameters and change the Password Expiration Interval.

```
                          Work with User Profiles

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display
  12=Work with objects by owner

     User
Opt  Profile     Text

__   __________
3    SPSEGOV     Click2Gov3 Default Profile **DO NOT DELETE**
```

User Profile

The Fusion user profile must have QPGMR specified in the Group profile (GRPPRF) or Supplemental groups (SUPGRPPRF) parameter:

```
                        Change User Profile (CHGUSRPRF)

Type choices, press Enter.

Group profile  . . . . . . . . . GRPPRF          QPGMR
Owner  . . . . . . . . . . . . . OWNER           *USRPRF
Group authority  . . . . . . . . GRPAUT          *NONE
Group authority type . . . . . . GRPAUTTYP       *PRIVATE
Supplemental groups  . . . . . . SUPGRPPRF       *NONE
                          + for more values
Accounting code  . . . . . . . . ACGCDE          *BLANK
Document password  . . . . . . . DOCPWD          *SAME
Message queue  . . . . . . . . . MSGQ            FUSION
  Library  . . . . . . . . . . .                   QUSRSYS
Delivery . . . . . . . . . . . . DLVRY           *NOTIFY
Severity code filter . . . . . . SEV             0
Print device . . . . . . . . . . PRTDEV          *WRKSTN
Output queue . . . . . . . . . . OUTQ            *WRKSTN
  Library  . . . . . . . . . . .
```

- or -

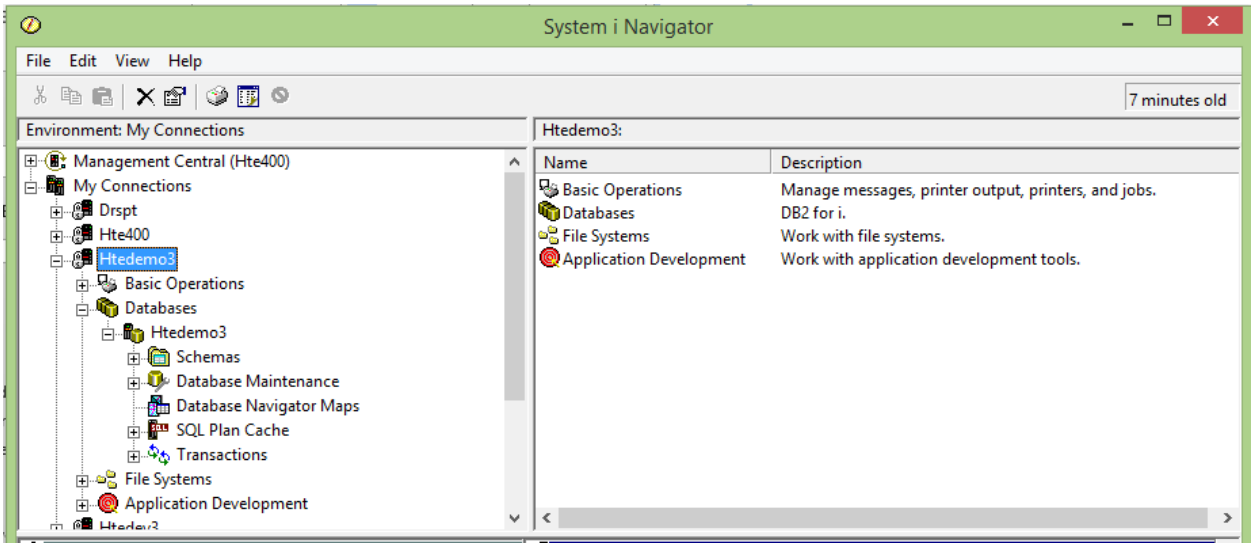
```
                    Change User Profile (CHGUSRPRF)

Type choices, press Enter.

Group profile  . . . . . . . . . GRPPRF          GRPALL
Owner  . . . . . . . . . . . . . OWNER           *USRPRF
Group authority  . . . . . . . . GRPAUT          *ALL
Group authority type . . . . . . GRPAUTTYP       *PRIVATE
Supplemental groups  . . . . . . SUPGRPPRF       GRPMOD
                          + for more values      QPGMR
Accounting code  . . . . . . . . ACGCDE          'GRPC2G'
Document password  . . . . . . . DOCPWD          *SAME
Message queue  . . . . . . . . . MSGQ            FUSION
  Library  . . . . . . . . . . .                   QUSRSYS
Delivery . . . . . . . . . . . . DLVRY           *BREAK
Severity code filter . . . . . . SEV             0
Print device . . . . . . . . . . PRTDEV          *WRKSTN
Output queue . . . . . . . . . . OUTQ            QPRINT
  Library  . . . . . . . . . . .                   QGPL
```

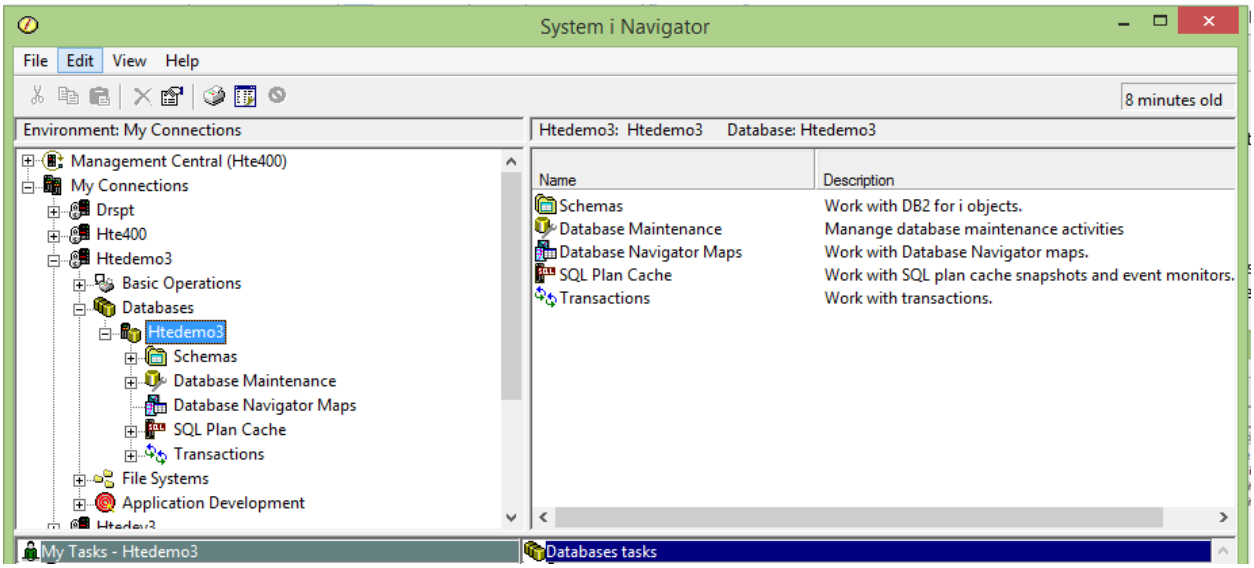
iSeries server

This is the fully qualified domain name or the IP address of your iSeries server.
This is the name of the server as it appears in **System I Navigator** under **My Connections**.



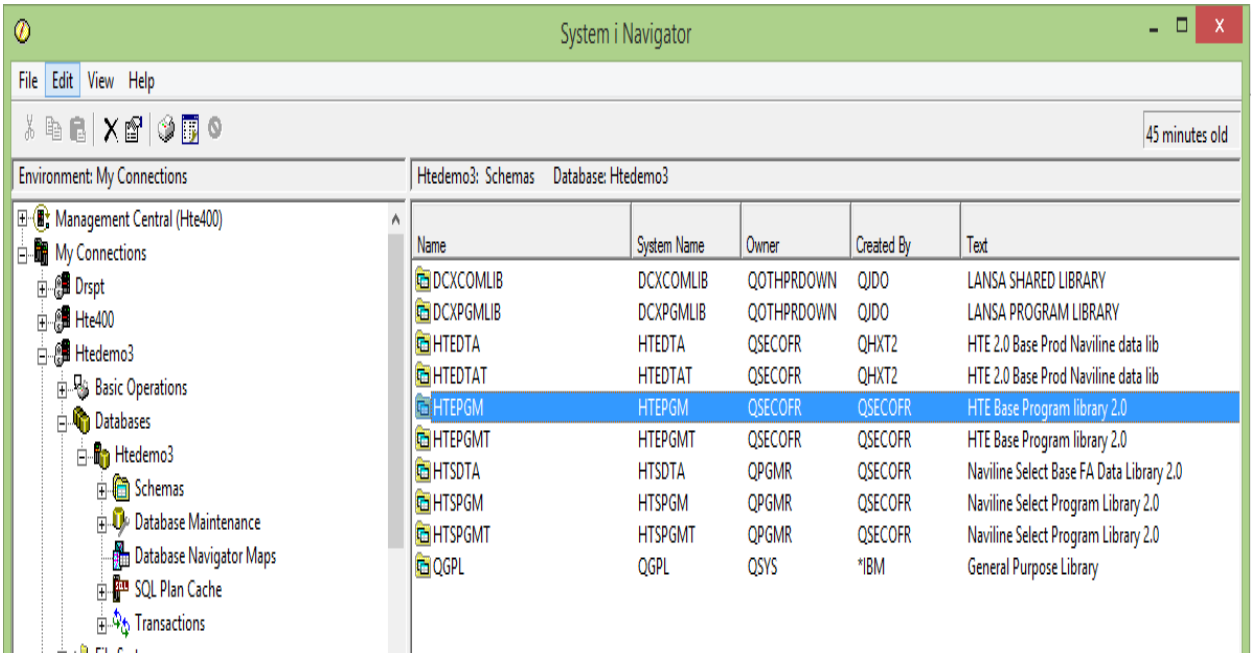
iSeries database

This is the name of the database as it appears in **System I Navigator** under **[Server] > Databases**



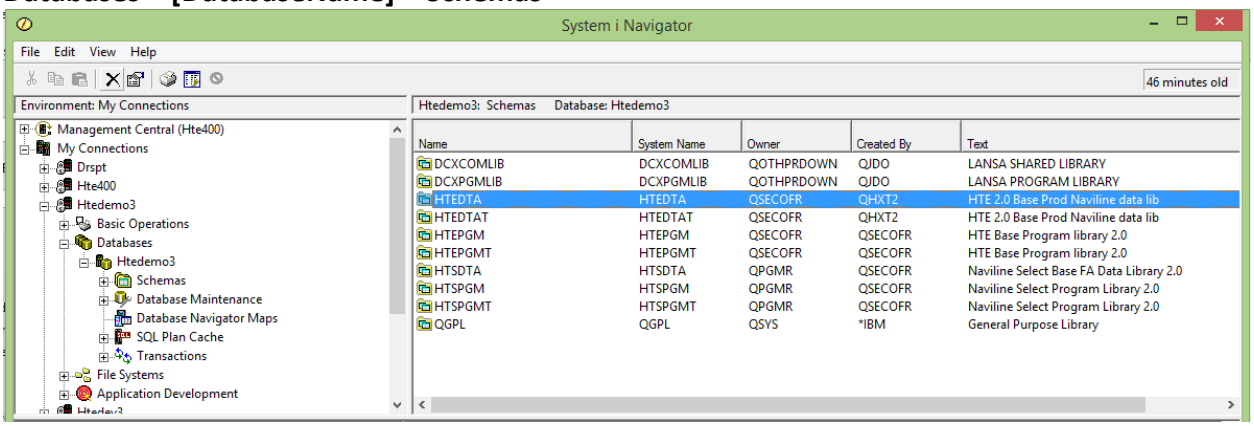
iSeries program libray

This is the name of the PGM library as it appears in **System I Navigator** under **[Server] > Databases > [DatabaseName] > Schemas**



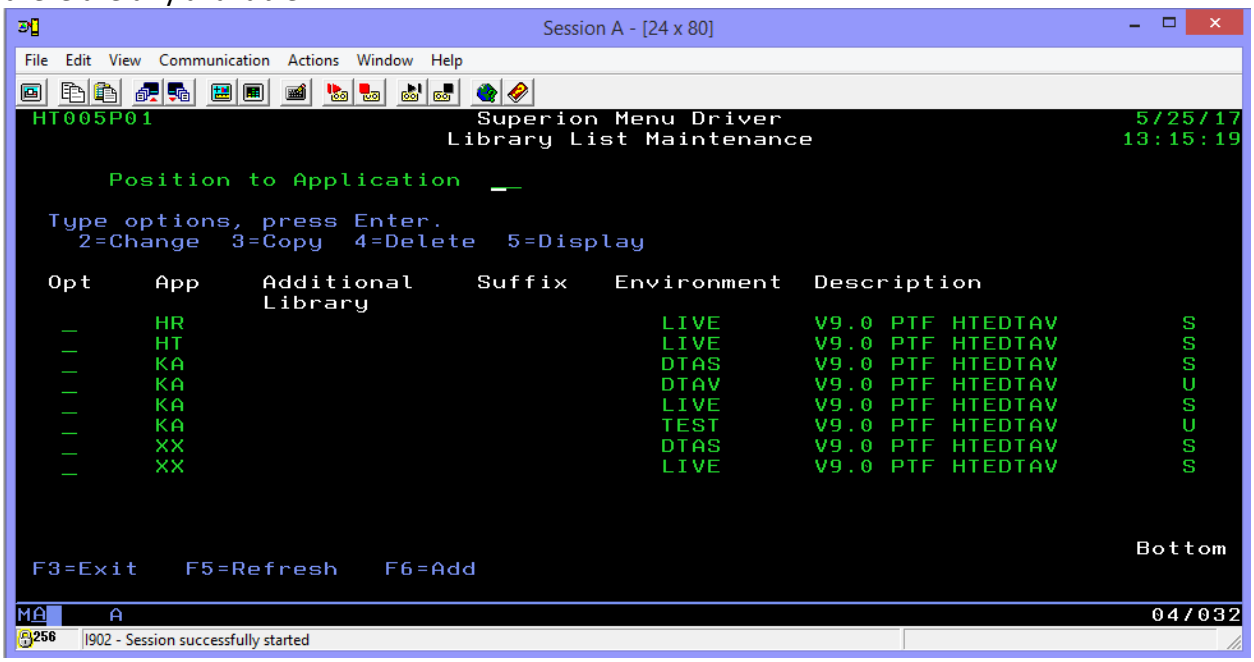
iSeries data libray

This is the name of the DTA library as it appears in **System I Navigator** under **[Server] > Databases > [DatabaseName] > Schemas**



iSeries environment

If you have multiple environments set up on iSeries, such as for LIVE and TEST, then you need to enter the environment name. If you sign in to either NaviLine or Select and get an environment screen, then this would be the environment you normally select on that screen. If you do not normally get the environment screen, then there isn't an environment and you can leave the environment blank. You can further check for environment names in either NaviLine or Select by using a **F9 command line > strsql > CALL HT005P**. This will bring up an environment list if there are any available.



Troubleshooting: Manually setting configuration values

If the install gives errors that it cannot write or save values to one of the configuration files, then it can be edited manually after the install. The install log should indicate what file it was unable to write to. This section lists the files and values that need to be set. You can open the named and manually set the value if needed.

The tables below list the configuration checklist items to get your values from, and in the **Key/Value** column it gives the section of code for where to set that value in the file. Searching on the keyword highlighted in light blue will help you find the section in the file. Replace the value highlighted in yellow with the value from your configuration checklist.

Web.config

This is the configuration file for the Fusion web service. This file is located at:

C:\inetpub\wwwroot\FusionServices\Web.config

The key values highlighted in blue are the names to search for to find them in the web.config file. The values highlighted in yellow are what you would change to reconfigure it to your configuration values.

Configuration Item	Key/Value
iSeries URL Configuration List: 2c	`<add key="SPS:Server" value="iVendor.com"/>`
iSeries Database Configuration List: 2c	`<add key="SPS:Database" value="iVendor"/>`
iSeries Program Lib Configuration List: 2d	`<add key="SPS:ProgramLibrary" value="HTEPGM"/>`
iSeries Data Lib Configuration List: 2e	`<add key="SPS:DataLibrary" value="HTEDTA"/>`
iSeries Registered Lib Configuration List: 2g	`<add key="SPS:RegisteredLibrary" value="HTEPGM"/>`
iSeries Environment Configuration List: 2f	`<add key="SPS:Environment" value="ENV"/>`
NaviLine Server Configuration List: 3a	`<add key="SPS:NaviLineServerName" value="NLSErver.domain.com"/>`
App ID Configuration List: 1a	`<add key="SPS:AppID1" value="yourAppID"/>`
App Key Configuration List: 1a	`<add key="SPS:AppKey1" value="yourAppKey"/>`
Key Desc Configuration List: 1a	`<add key="SPS:KeyDesc1" value="yourCityName"/>`

Troubleshooting: HTTP Error 503. The service is unavailable

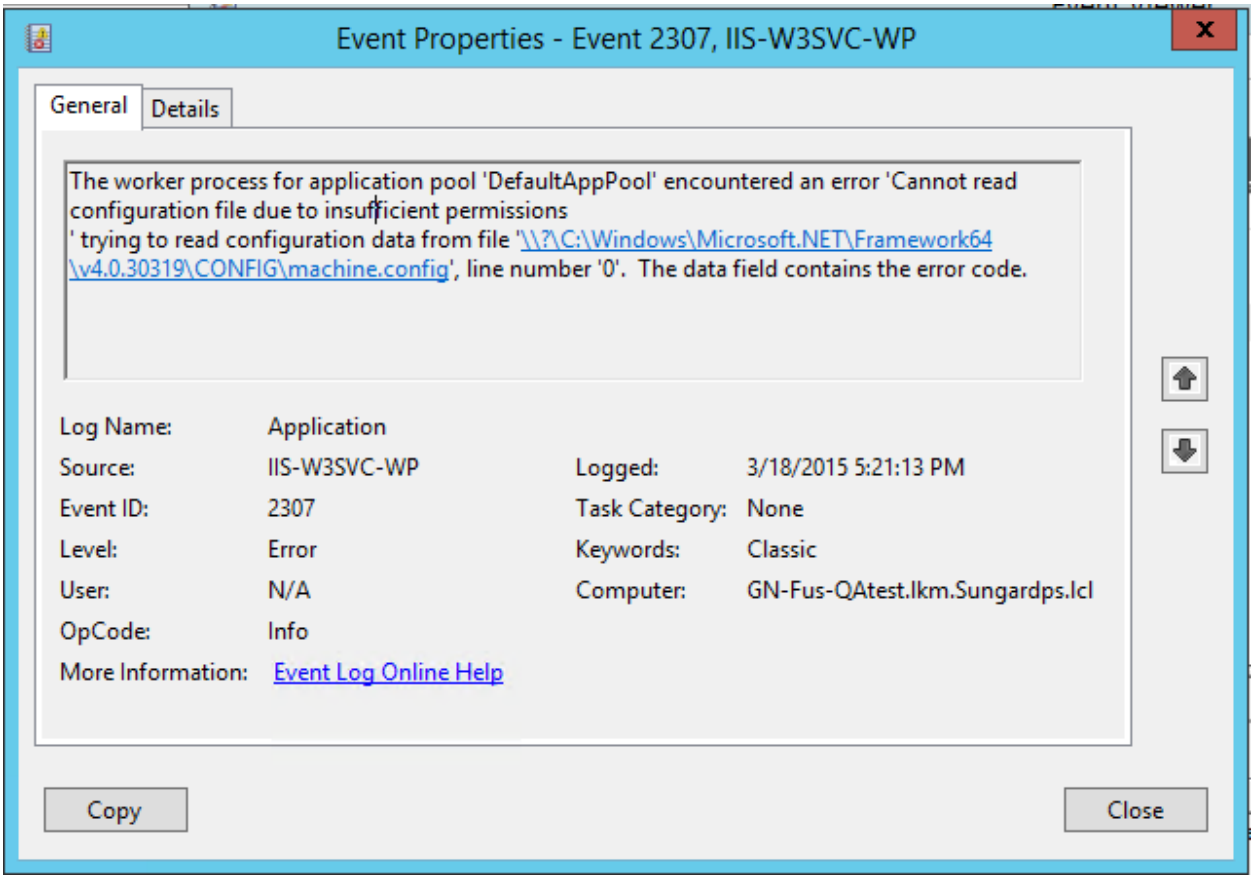
NOTE: If the IBM Client Access is installed after IIS is installed, it may remove the permissions to the machine.config files. You will get this error if you try to browse the FusionServices page, or even from browsing the Default Web Service page. This section tells you how to reset the file permission.

Machine.config

After installing the IBM Client Access, you may receive an error when you browse the FusionService page:

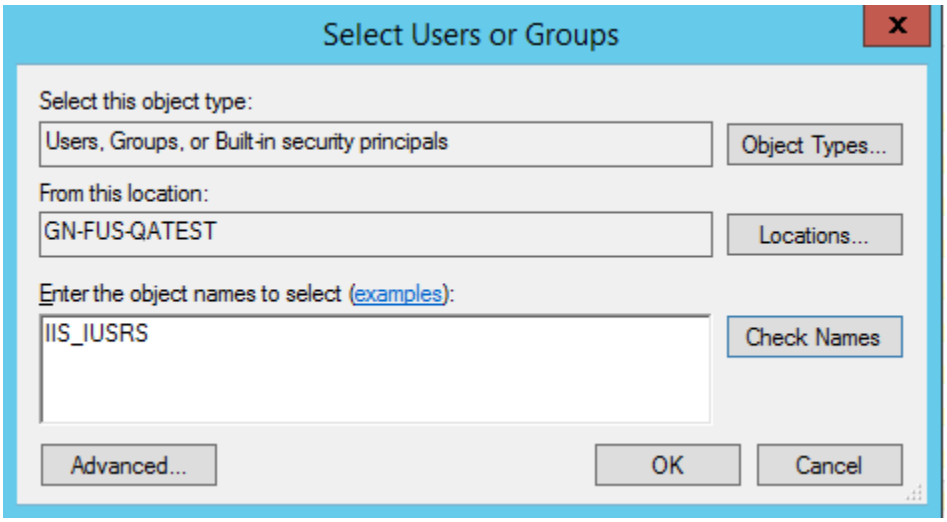
HTTP Error 503. The service is unavailable.

IIS requires read access to your machine.config file. Read permissions may have been removed when installing the IBM System I Access. You would see the following message in the Event Viewer if it does not have access:

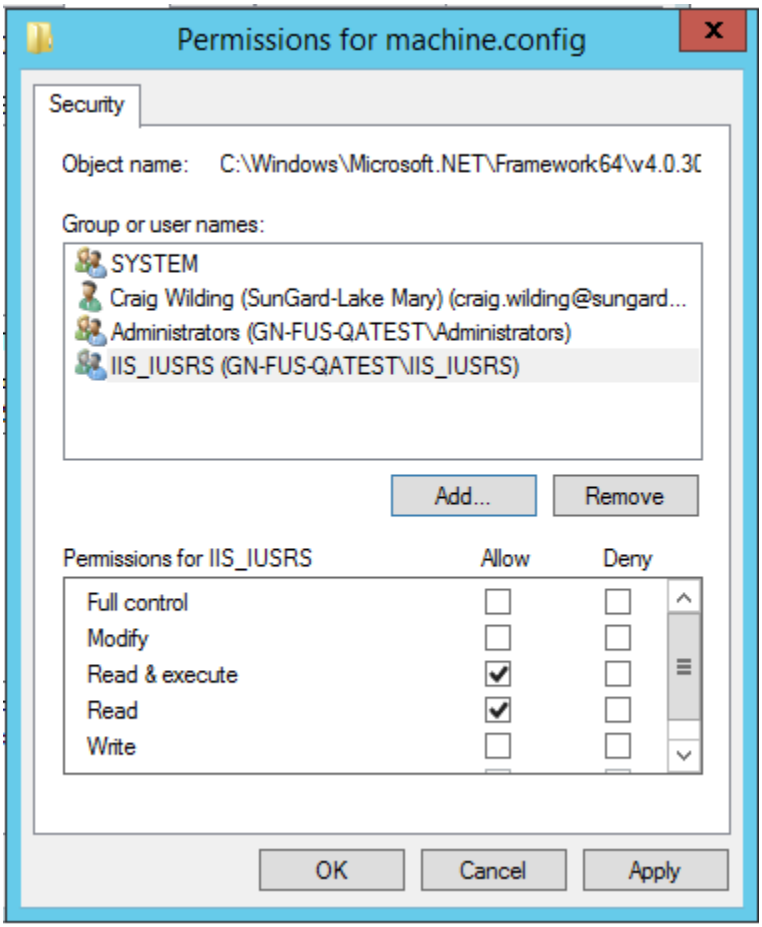


To fix the error, grant Read access permission to the file:
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config

Right click on the file and select **Properties** > **Security** > **Edit**



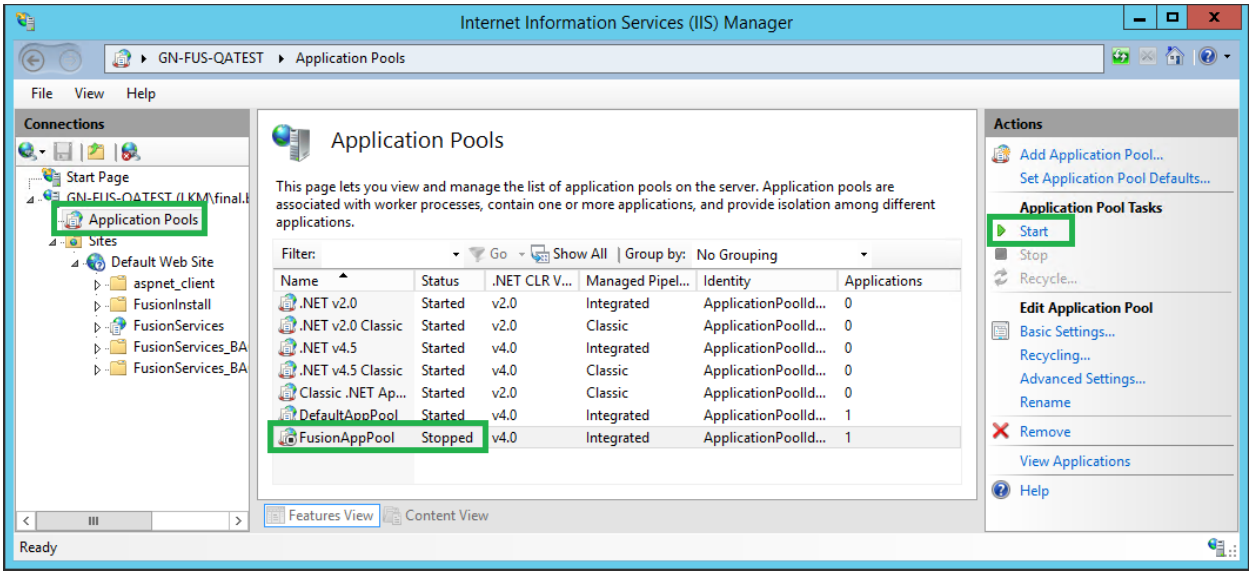
Click on the **Locations** button to change it from your domain name to the local machine name. Enter **IIS_IUSRS** at the bottom and click **OK**.



It should have the **Read & execute** and **Read** permissions selected. Make sure they are checked, and click **OK**.

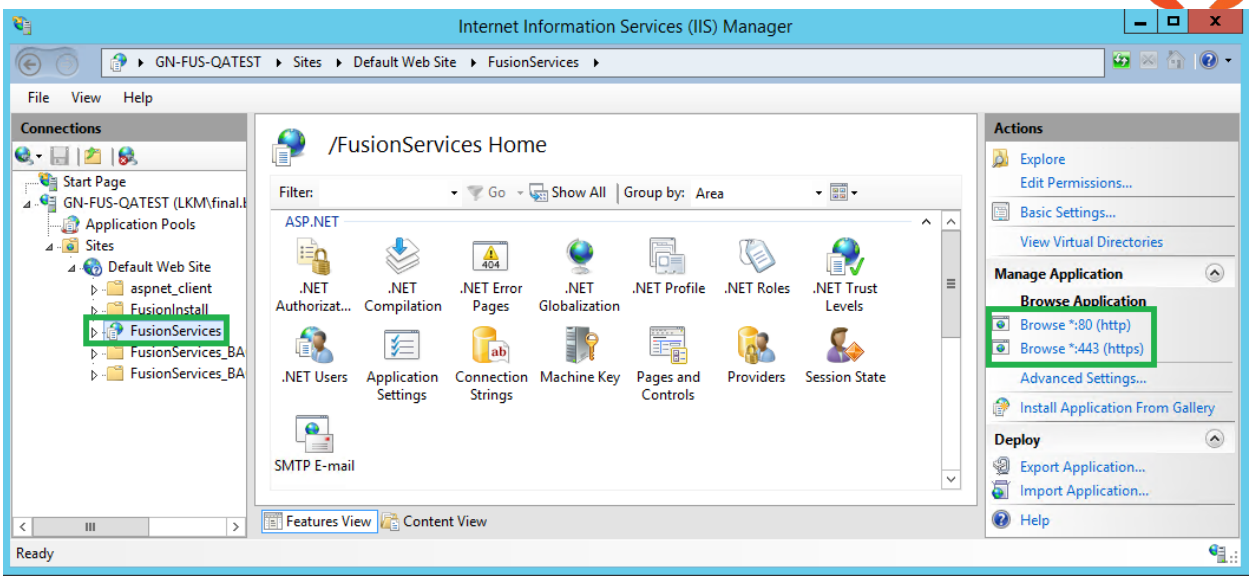
If you have already installed Fusion, make sure the Fusion App Pool in IIS is started. This may have been stopped if you received the 503 error due to the machine.config files.

In IIS Manager, select **Application Pools** in the tree view on the left. Select **FusionAppPool** from the list, then click the **Start** button on the right side.



You should now be able to browse the Fusion Service site.

In IIS Manager, expand the **Sites** > **Default Web Site** in the tree view on the left. Select **FusionServices** from the list, then click the **Browse** button on the right side. There is one Browse button for using http, and one if you are using https.



The Fusion Web Services page should come up in your web browser.