Using SSL With QilkView: An Introduction

Version: 2

Date: 2012-11-12

QV11

**Disclaimer:**

**Please be aware that this document is not supported and meant only as a guide. Individual environments may require adjustments for things to work correctly. Recommend contacting QlikView Expert Services for help with configuration**.

Table of Contents

[1 Introduction 4](#_Toc340495802)

[1.1 Prerequisites 4](#_Toc340495803)

[2 Installation Of QlikView 5](#_Toc340495804)

[3 Creating Self-Signed SSL Certificate 9](#_Toc340495805)

[3.1 Configuring IIS To Use SSL 14](#_Toc340495806)

[3.2 Testing SSL (port 443) HTTPS:// 17](#_Toc340495807)

[4 Using QlikView Web Server and SSL 21](#_Toc340495808)

[4.1 Configuration 21](#_Toc340495809)

[4.2 Configuring QlikView Web Server To Use SSL 24](#_Toc340495810)

[4.3 Testing SSL (port 443) HTTPS:// 26](#_Toc340495811)

[5 Configuring QlikView Web Services To Use SSL 29](#_Toc340495812)

# Introduction

This document will outline the steps:

* Creating a self-signed certificate using IIS.
* Assumes using version 11 SR2
* Setting up QlikView to use SSL
  + Using IIS as Web Server
  + Using QlikView Web Server (QVWS)
  + Configure QlikView Services to use SSL

The purpose is to show how to setup an environment for various testing purposes.

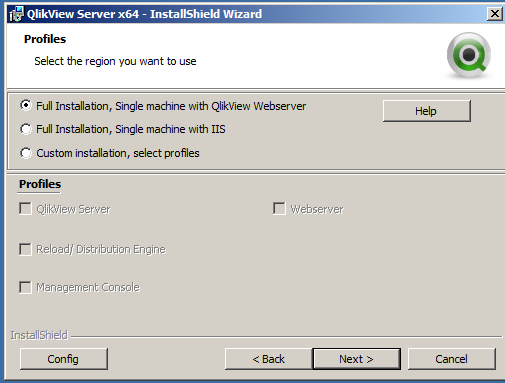
## Prerequisites

This document assumes that IIS has been installed based on the requirements documented in the Qlikview Server Reference Manual and that the user is familiar with installing QlikView to use IIS or QlikView Web Server. In this case all components of QlikView will be installed on the same machine (IIS components and QVWS). This is done for ease of use. Having the QlikView Settings and Web Server resources installed concurrently is not a typical setup. Normally either IIS or QVWS is used as the web server; both cannot be used at the same time.

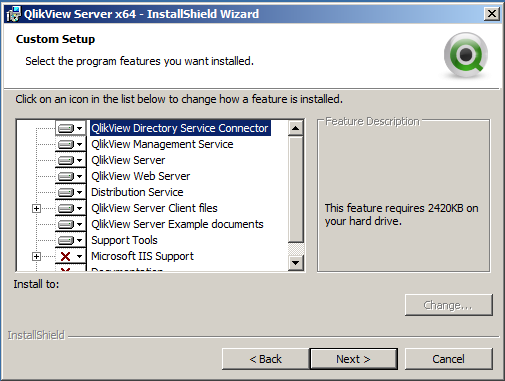
# Installation Of QlikView

This will just outline what is installed with QlikView and things to watch out for.

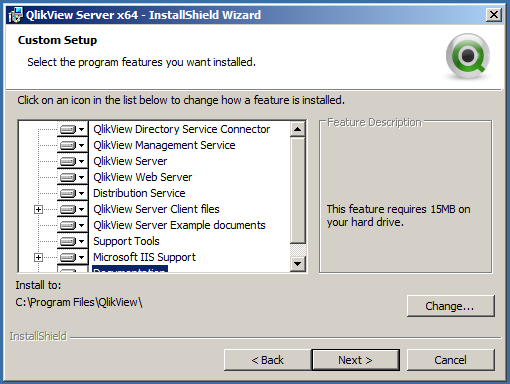
1. Start a QlikView Server Installation
2. When asked what to install, click the Config Button in the bottom lower left of the Profiles Screen



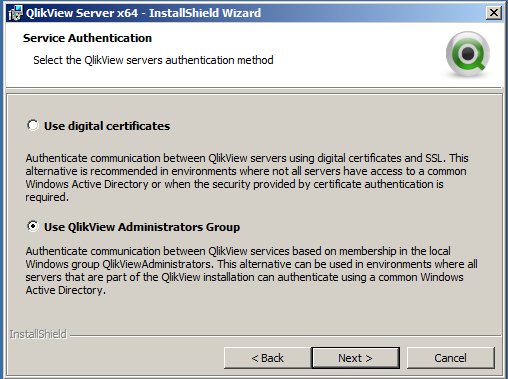
1. This will open a dialog where the user may manually choose what to install.



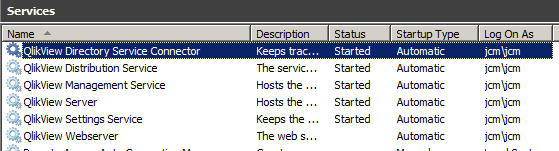
1. For the purpose of this install, the user will select anything that has a red **X** and in the drop down next to each, select “This Feature, and all sub features , will be installed on the local hard drive.” Your screen will resemble the figure below.



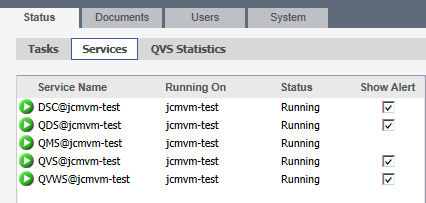
1. Keep in mind that IIS must be configured and running for the install to succeed.
2. When presented with the Service Authentication Dialog, ensure “Use QlikView Administrators Group” is selected (default)



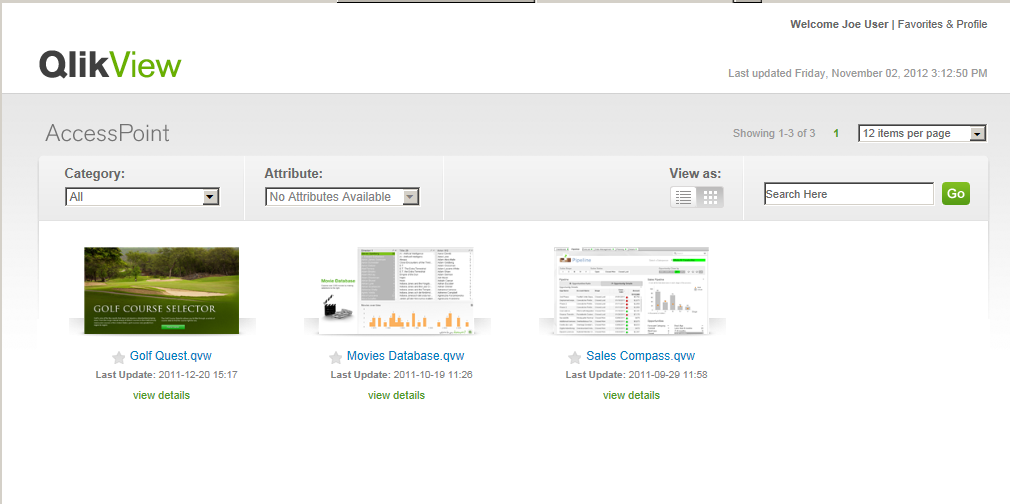
1. Use of Digital Certificates is intended for a different purpose. Read more in the QlikView Server Reference Manual.
2. Finish the installation and reboot the server.
3. Once the server is back up and the services have had a chance to start, notice that there is a service called the QlikView Settings Service; this service needs to run when using IIS. If using QVWS then the QlikView Webserver service is used. Also, notice that the Settings Service is running and the QlikView Webserver service is not, even though it is set to automatic. This is by design, when one is running the other cannot be started.

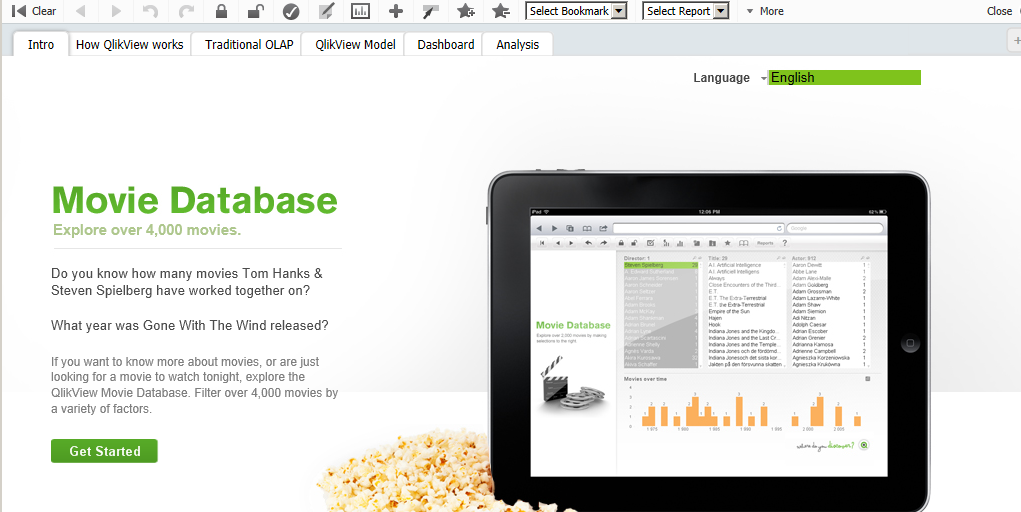


1. IIS will be the first configuration, so ensure the QlikView Settings Service is running.
2. If desired, the QlikView Web Service may be set to Manual.
3. Proceed with licensing the QlikView Server (and Publisher if so desired).
4. Ensure all services have a status of Running



1. Ensure that the AccessPoint opens, presents documents, and a document can be opened using the regular <http://<servername>/qlikview/index.htm> URL.

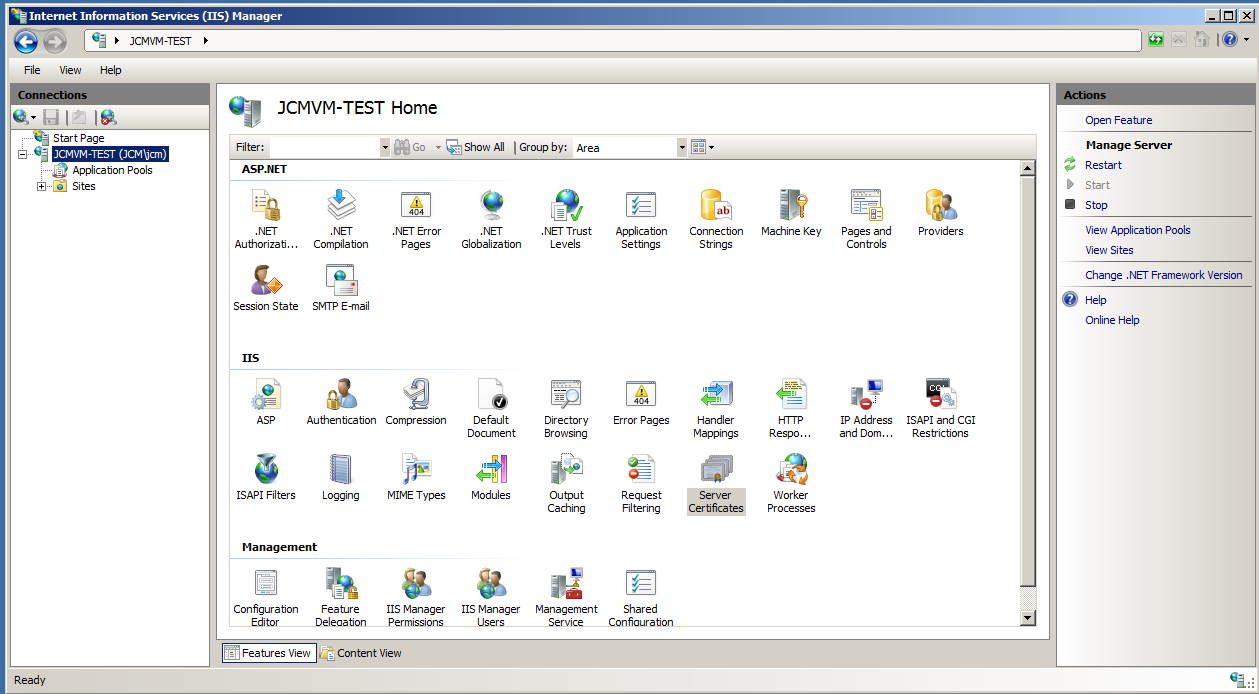




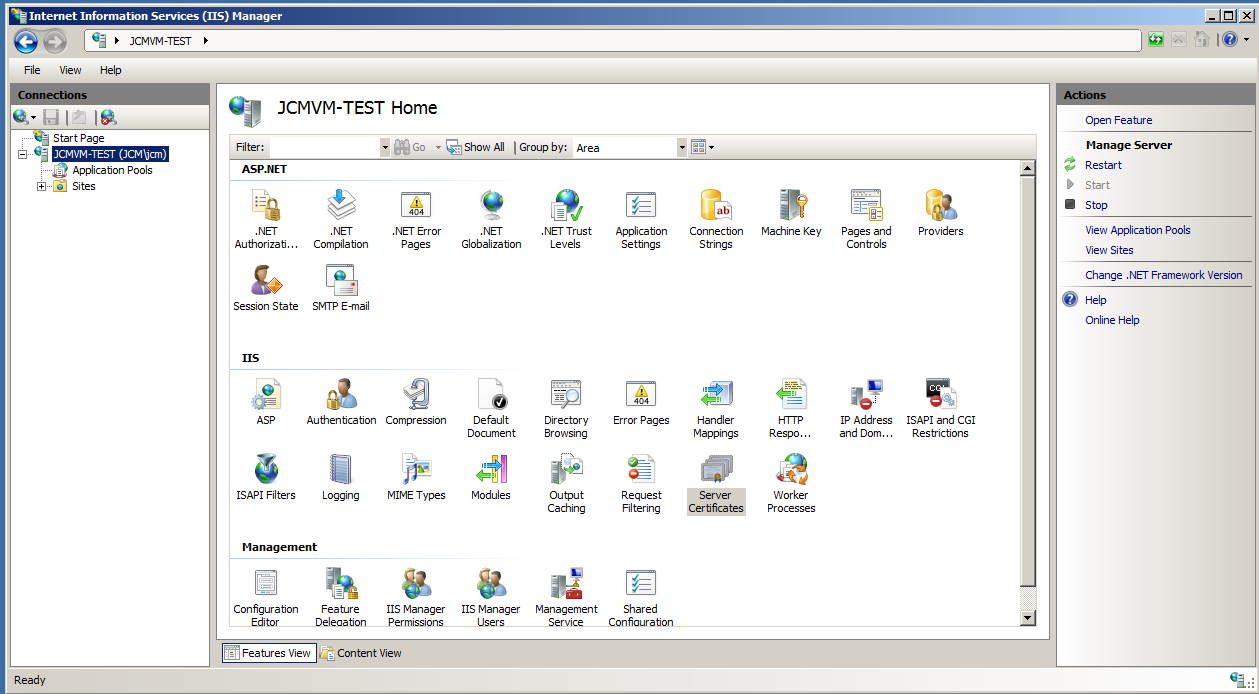
1. This is now a working QlikView Server

# Creating Self-Signed SSL Certificate

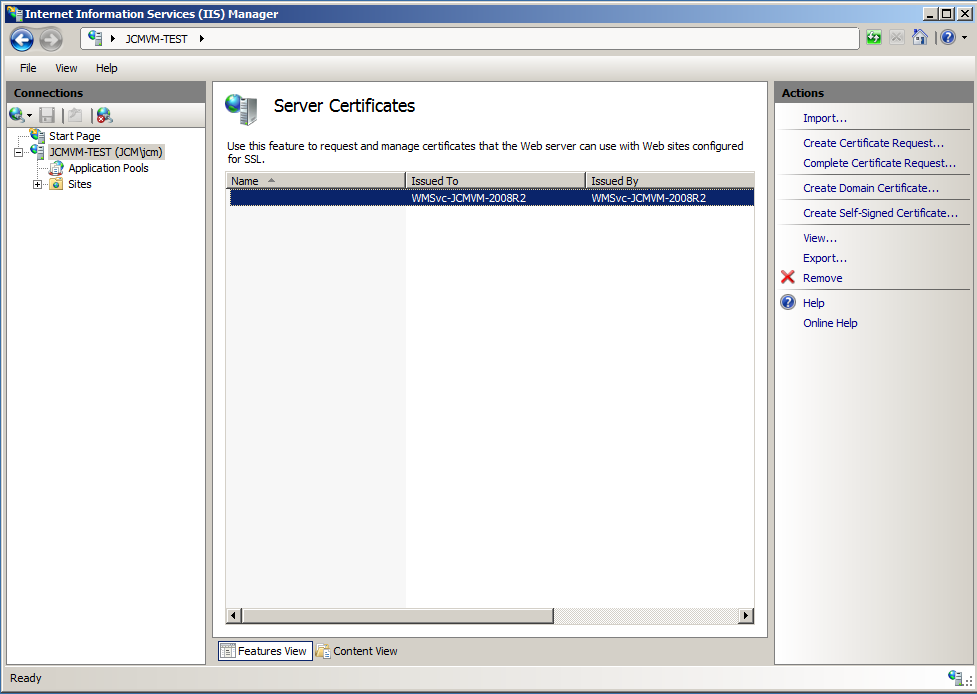
1. Open the IIS Manager
2. Click on the server at the top level in the leftmost pane



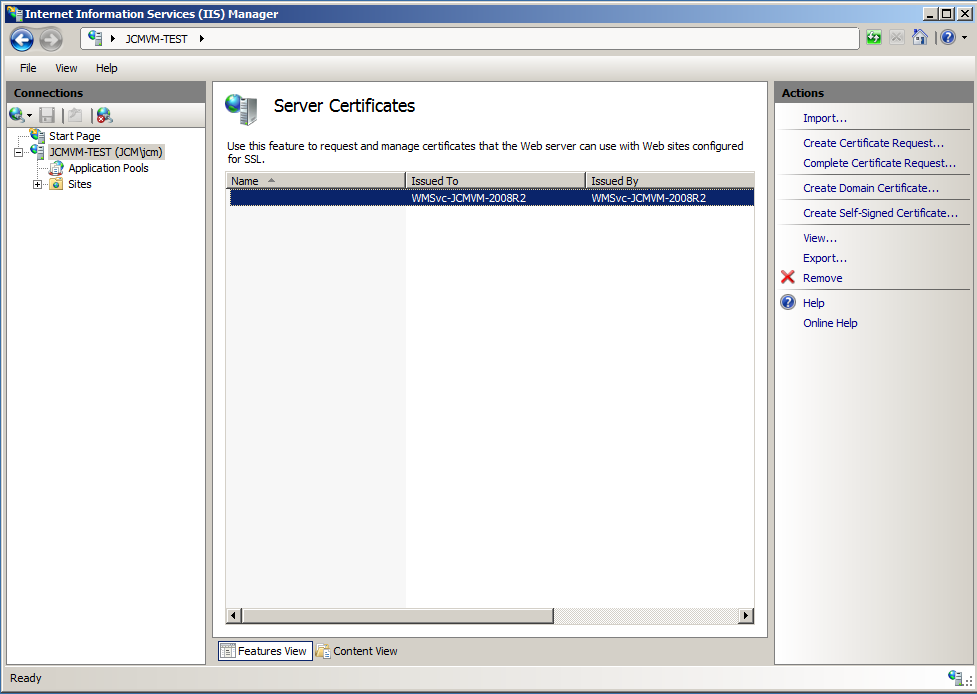
1. In the center panel, under the IIS section. Double-click Server Certificates.



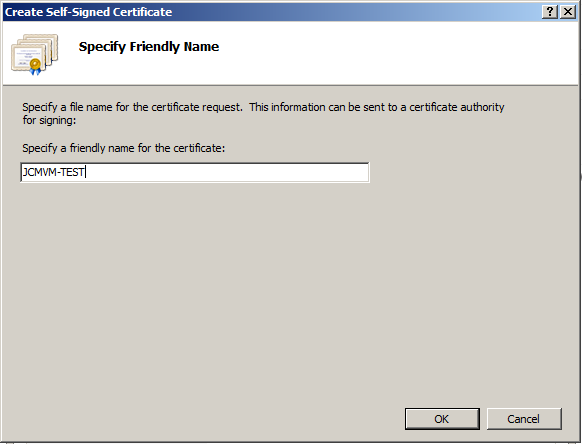
1. Once open, the user is presented with the following.



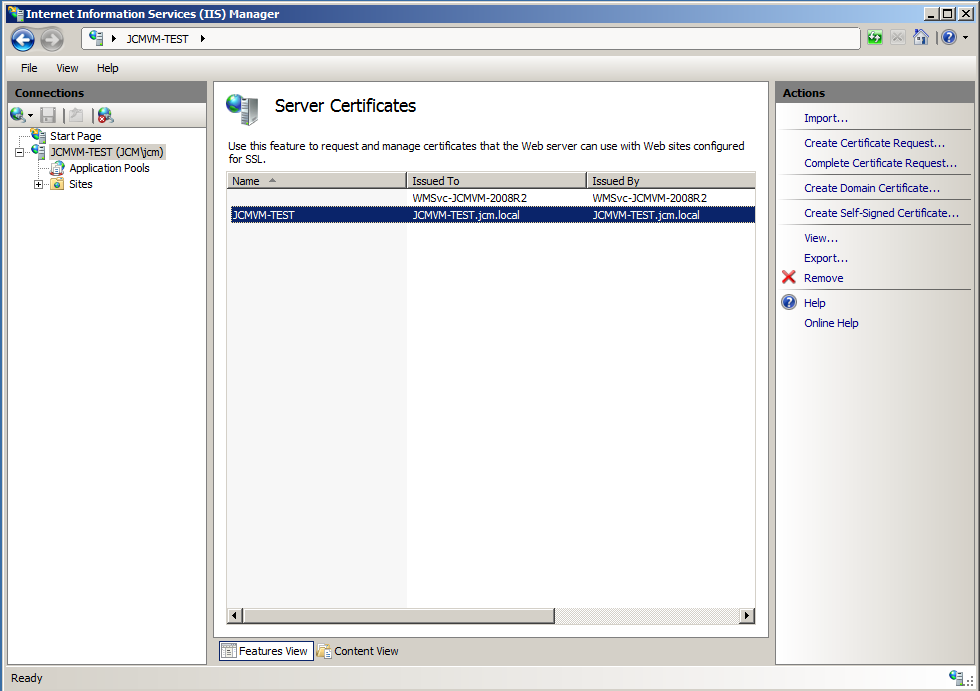
1. Click on Create Self Signed Certificate in the right hand (Actions) panel



1. Specify a friendly name. In most cases, use the name of the server.



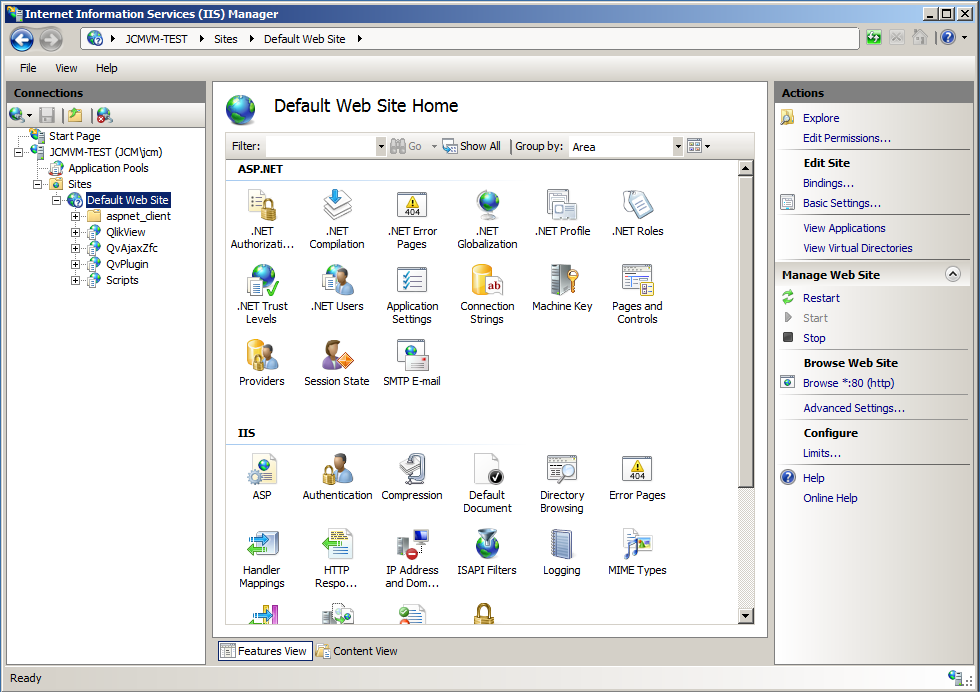
1. Click OK
2. The Certificate is created



1. Double clicking the line will open the certificate and the contents may be explored.

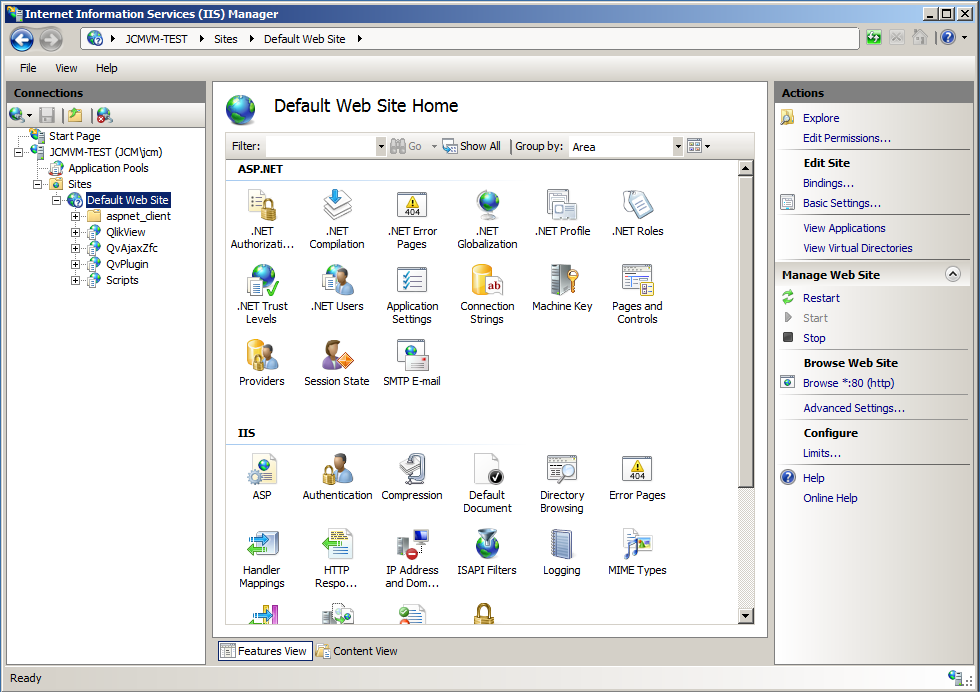


1. In the left hand panel of the IIS Manager, click and expand Sites. Select the Default site (or the site) selected during installation.

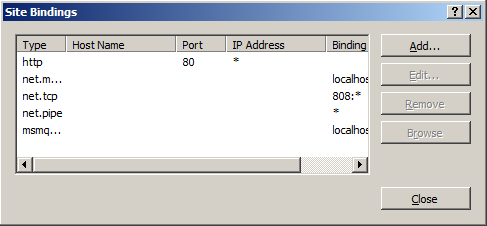


## Configuring IIS To Use SSL

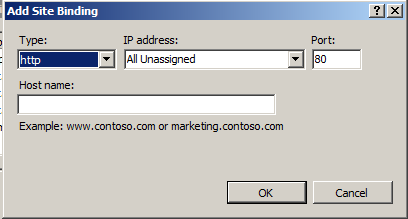
1. In the right hand panel (Actions) click on Bindings (Edit Site).



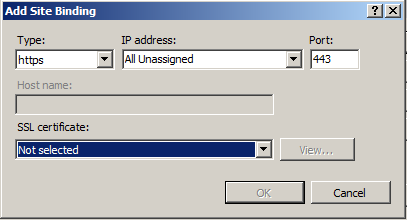
1. The following dialog should appear: Site Bindings.



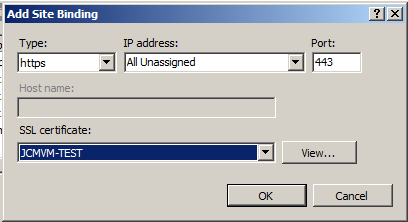
1. Click the Add button and the following should appear.



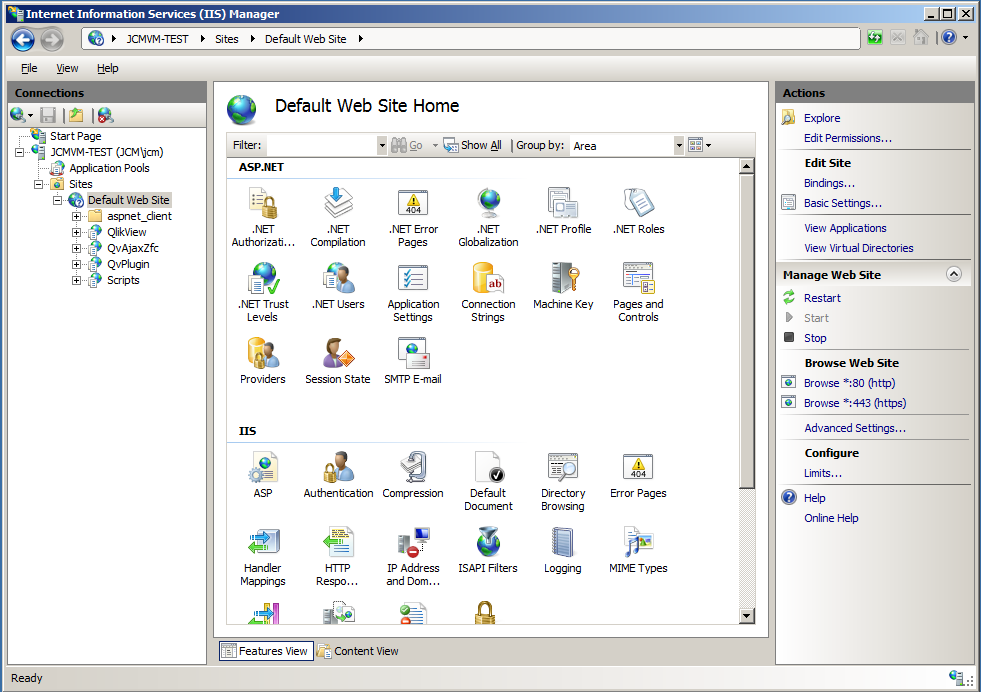
1. Click the Type drop down and select https, screen should appear as below.



1. Click the SSL Certificate drop down and select the certificate that was created.



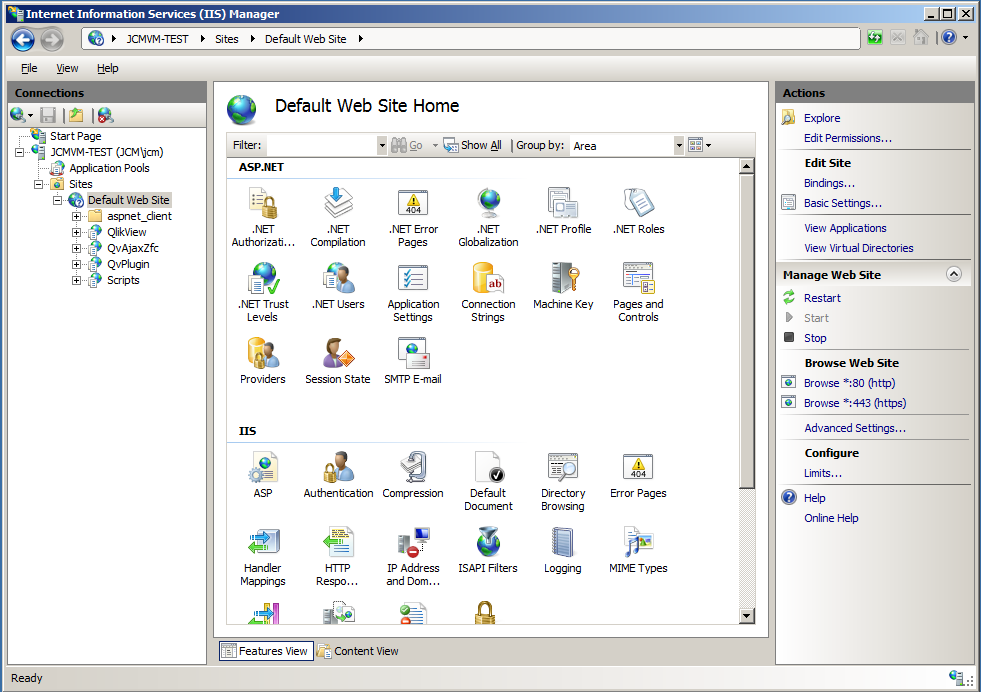
1. Click OK, Close
2. Now the site is configured to use SSL (port 443) HTTPS://



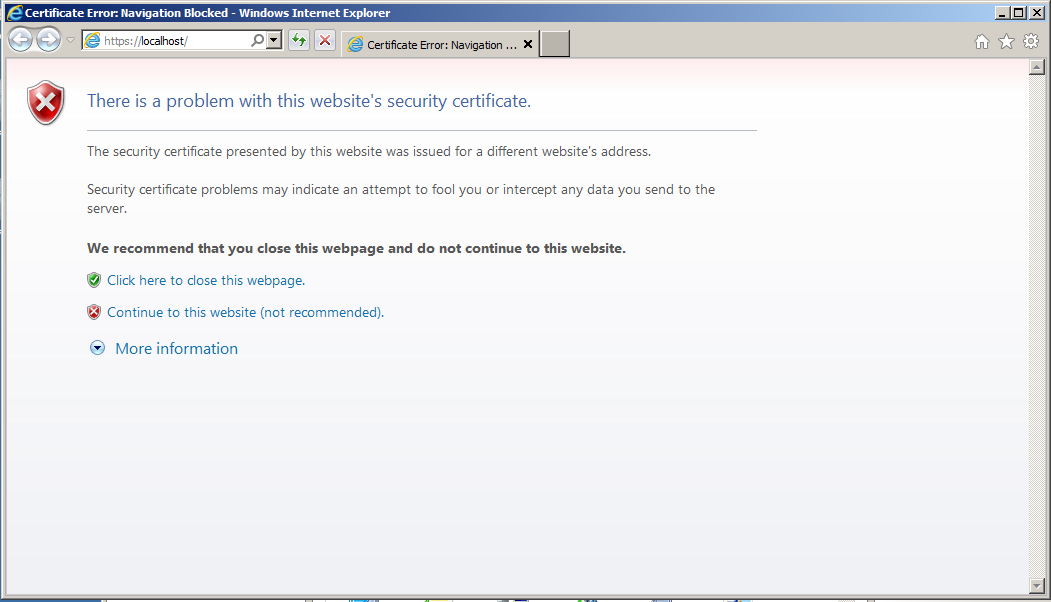
1. In this case it is also able to still use normal HTTP:// since port 80 is still bound. The binding for port 80 may be removed if only HTTPS:// is to be used on the site. The other option is to use the Require SSL check box on each virtual directory under the SSL Settings in the IIS section of the middle pane.

## Testing SSL (port 443) HTTPS://

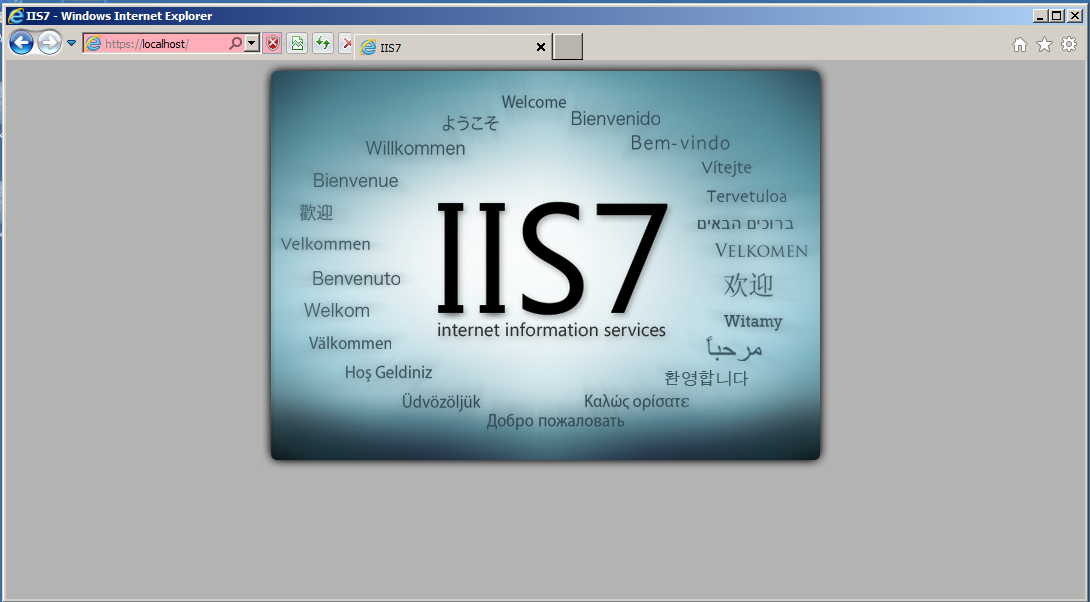
1. There are a couple of ways to test that SSL is working. The easiest is to browse to the site using HTTPS.
2. In IIS with the site highlighted click on the Browse \*.443(https) link in the right hand pane under the Browse Web Site



1. If things are working properly then the user will be presented with the following



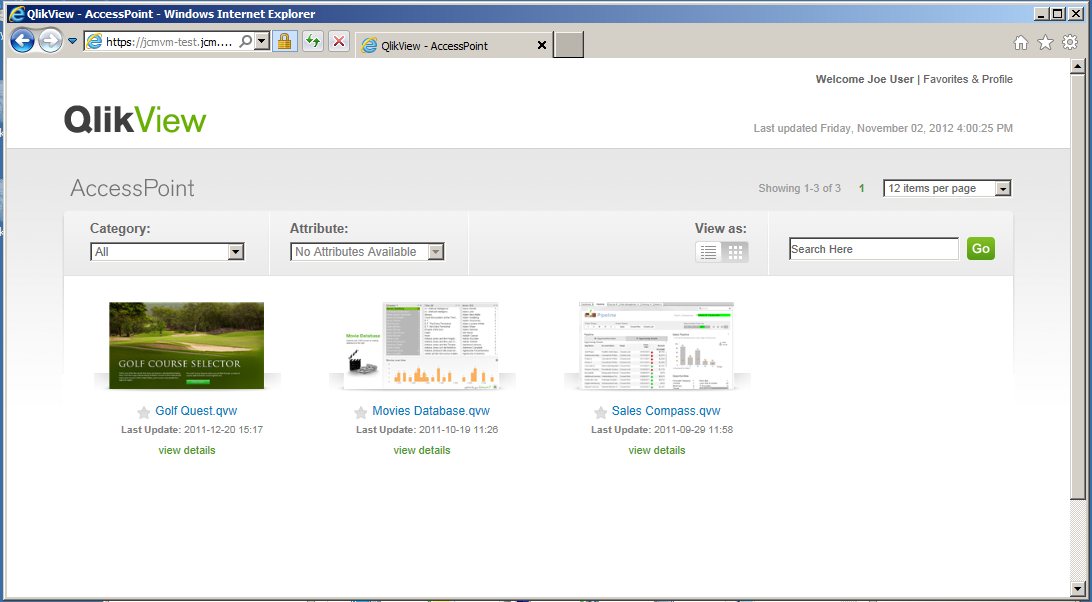
1. This is not actually an error. Looking at the URL in the address section, it is listed as <https://localhost>. Localhost is not registered to the certificate that was created in IIS. Clicking Continue to this website will present the following.



1. Notice in the figure above, the URL is highlighted red; this indicates there is a certificate error. What it really indicates, in this case, is that the correct name was not used in the URL.
2. For this to not show errors, the fully qualified domain name of the server must be used. In this case <https://jcmvmtest.jcm.local> (this is machine dependent, not all are the same). Notice that the address line is not red, and we have the lock icon.



1. At this point, the site is secure using SSL
2. What about the QlikView AccessPoint? In the URL above add qlikview after the last /. For example
   1. <https://jcmvm-test.jcm.local/qlikview>
   2. You will want to add the site to Local Intranet so that login credentials are passed, otherwise it may prompt for login credentials.
3. The AccessPoint should appear and the URL should be using HTTPS



1. Open a document using Ajax client and the page should still be using HTTPS

Congratulations, QlikView is using IIS as the web server with SSL

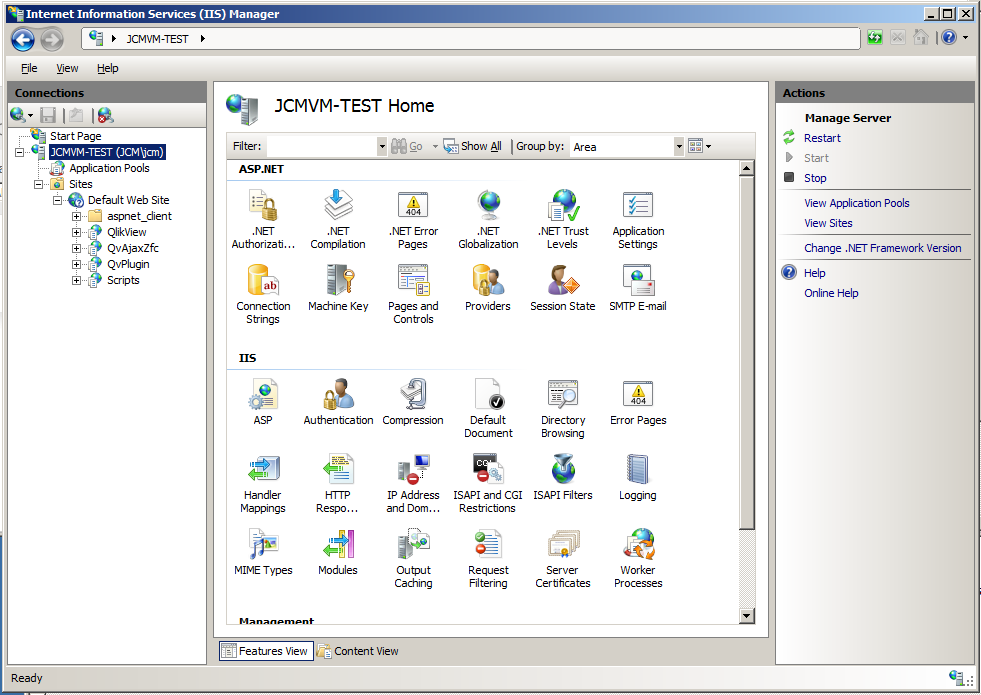
Tip: Set QlikView Security to Prohibit Anonymous and remove port 80 from the Bindings in IIS to be sure things are secure.

# Using QlikView Web Server and SSL

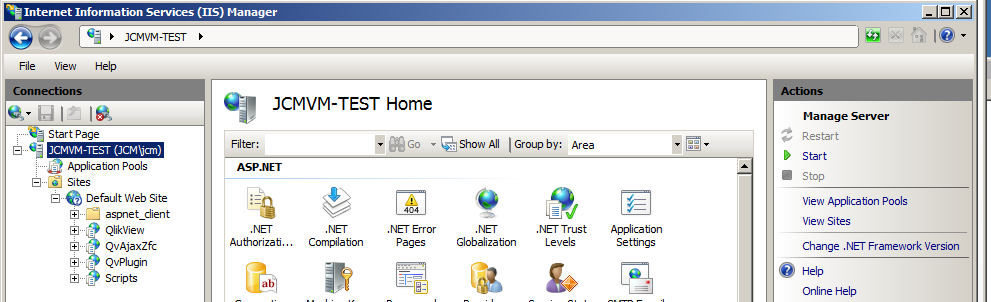
Since IIS has been configured to use SSL, most of the work has been completed to get SSL working with Qlikview Web Server.

## Configuration

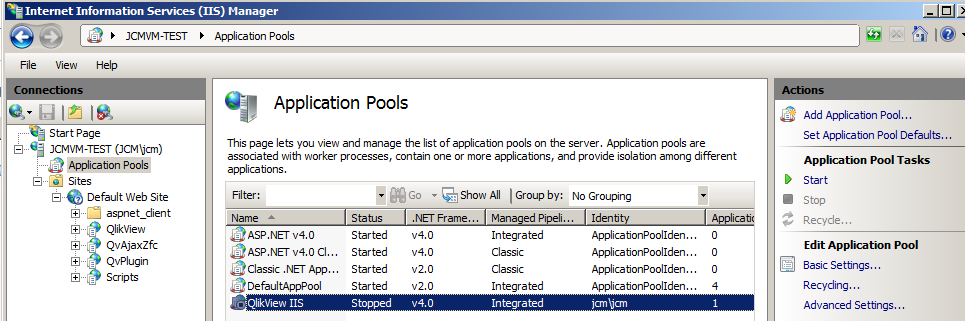
1. Start by stopping IIS, this is easily done by stopping the server in the IIS Manager.
2. Click on the server name in the IIS Manager (left hand panel), then click stop in the right hand panel (Actions – Manage Server)



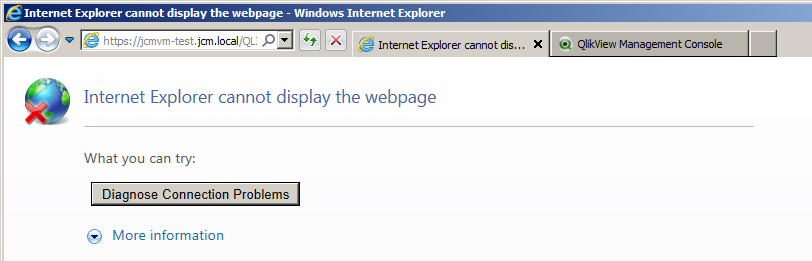
1. After clicking stop, it should appear as below



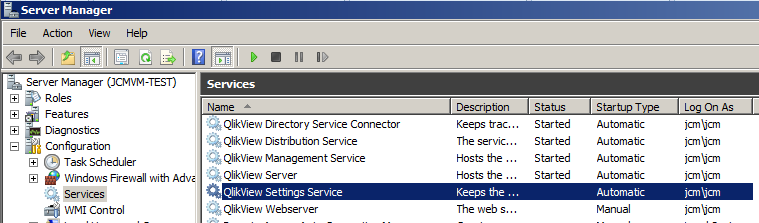
1. If it is desired, the Application Pool for QVIIS may be stopped as well.



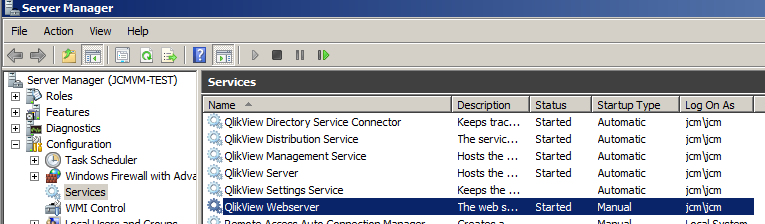
1. Test the AccessPoint or the default site to confirm IIS is down.



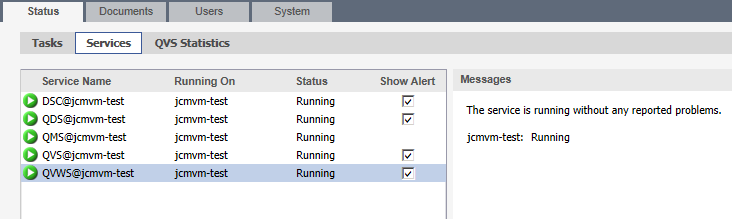
1. Stop the QlikView Settings service



1. Start the QlikView Web Server

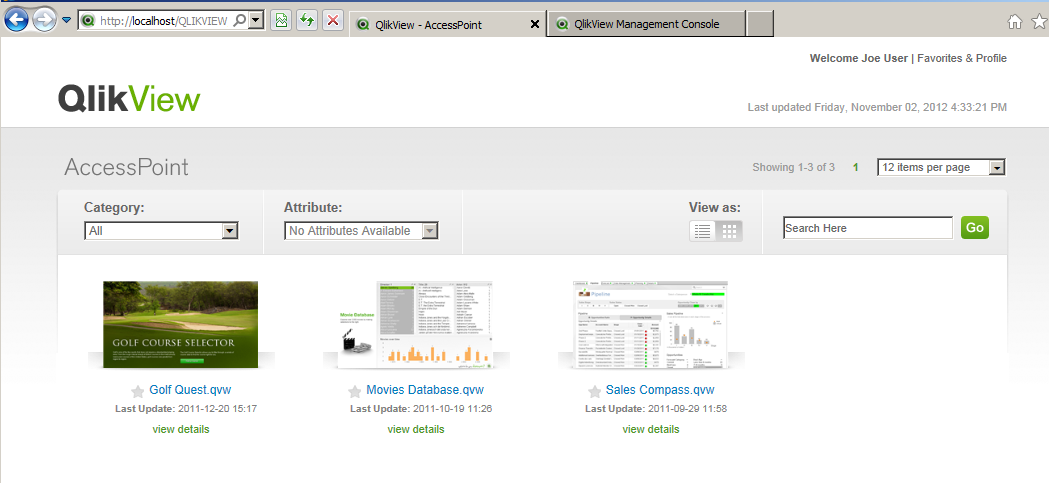


1. Check to see if things are connected in the QlikView Management console



**Note:** *Version 11 does not require a change to the URL as was the case in versions 9 and 10*

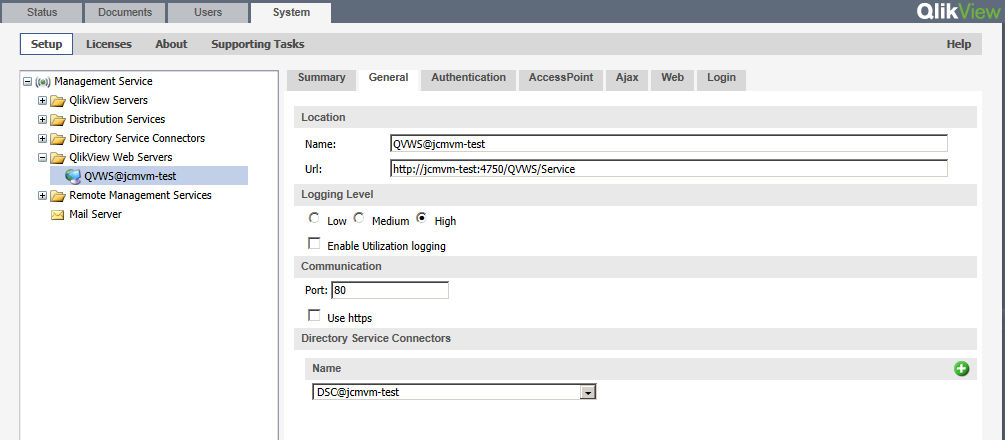
1. Check that the AccessPoint comes up by using the following URL: <http://localhost/QLIKVIEW/>



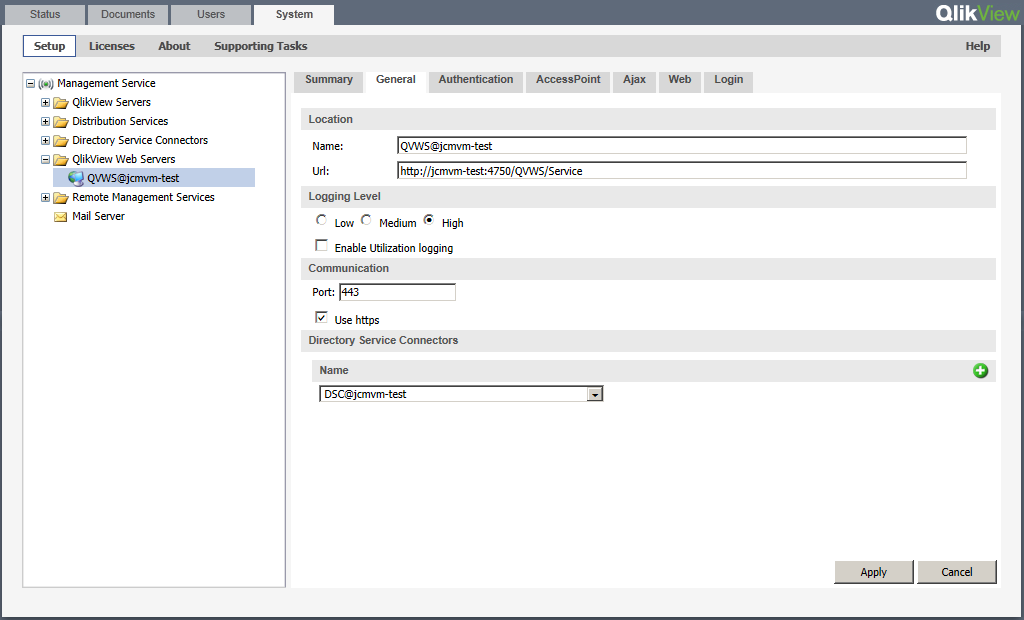
1. If the above are working correctly, then the QlikView Web Service is running properly
2. To get things running under SSL, there are a few additional steps to be completed.

## Configuring QlikView Web Server To Use SSL

1. Open the QlikView Management Console (QMC)
2. Navigate to System – Setup – QlikView Web Server(QVWS) – General Tab



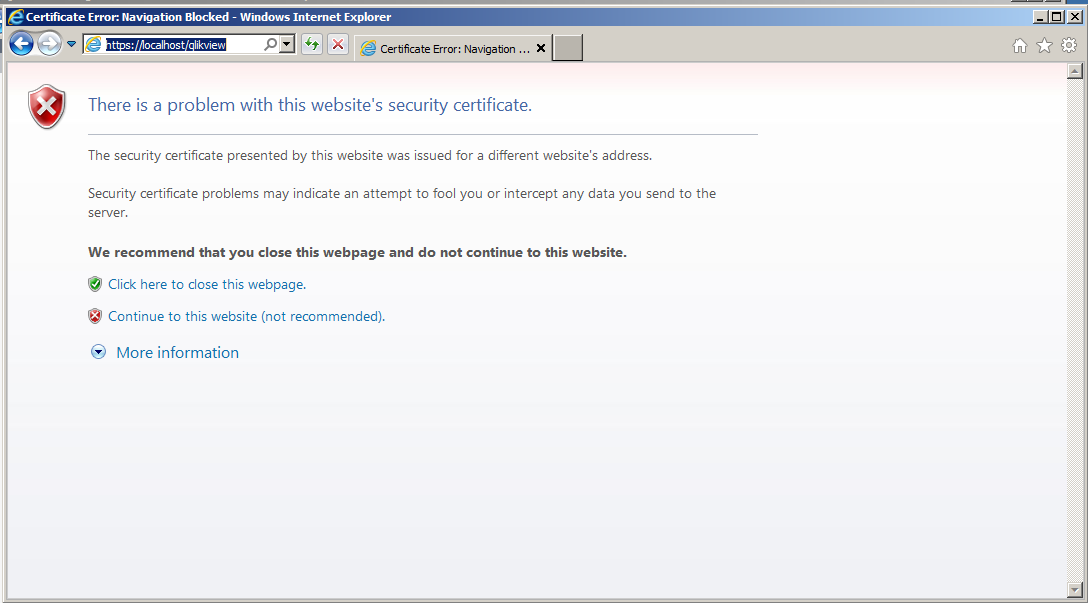
1. Under the Communication section, the Port needs to be changed to **443** and the check box for “Use” https needs to be **checked.**



1. Click Apply

## Testing SSL (port 443) HTTPS://

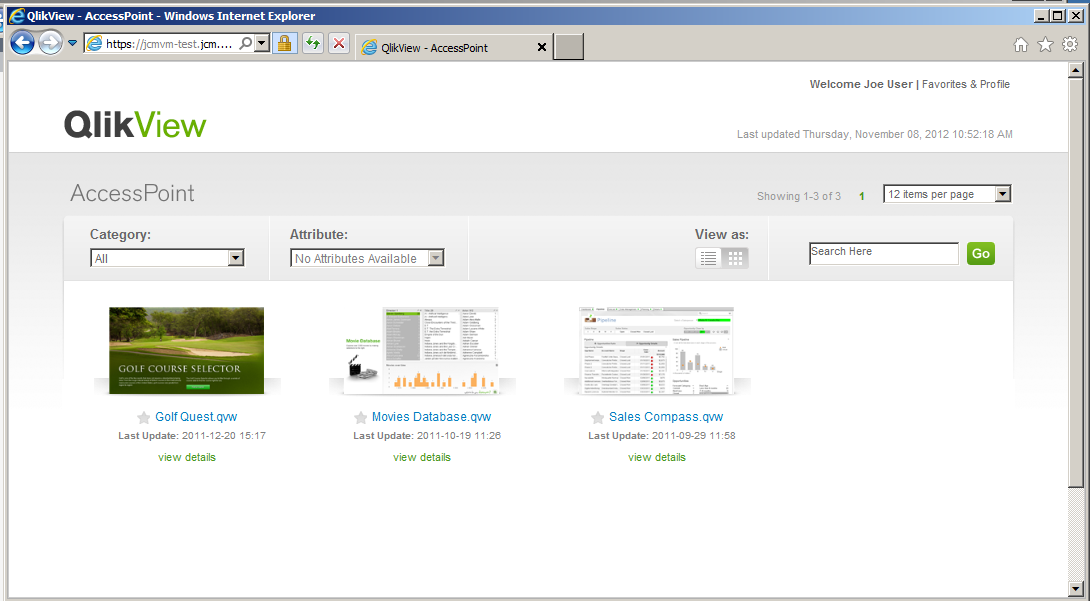
1. As with testing SSL above, if <https://localhost/qlikview> is entered in a browser the following should appear.



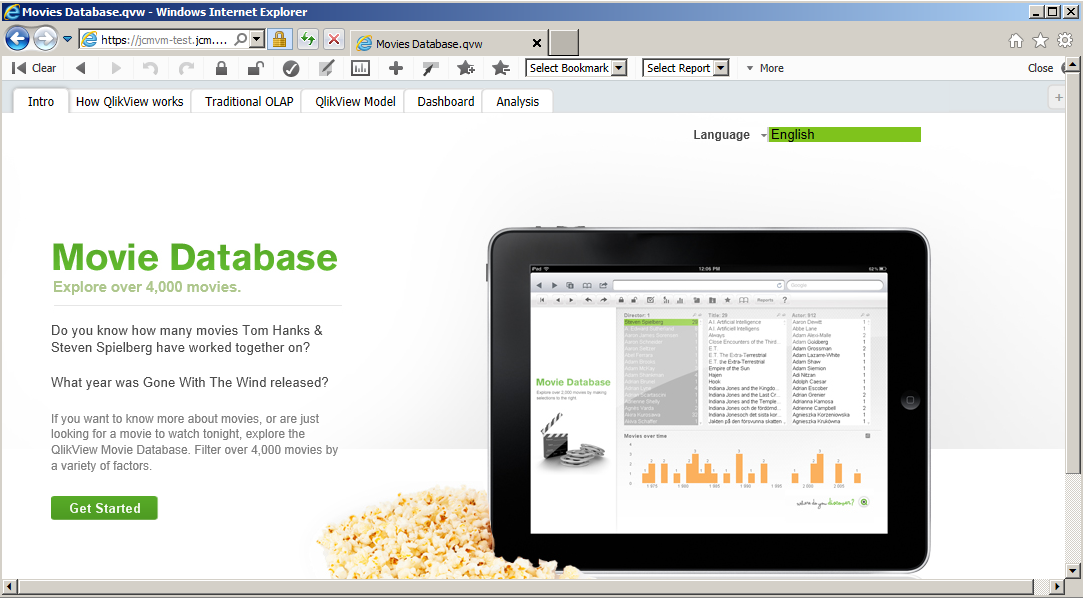
1. As before, the return is not correct since the certificate that was created, was created for the fully qualified domain name. Thus entering https://<FullyQualifiedDomainServerName>/qlikview should return the proper result. In the figure below using:

<https://jcmvm-test.jcm.local/QLIKVIEW/index.htm>

The proper response is given.



1. Opening a QVW, HTTPS should still be used.



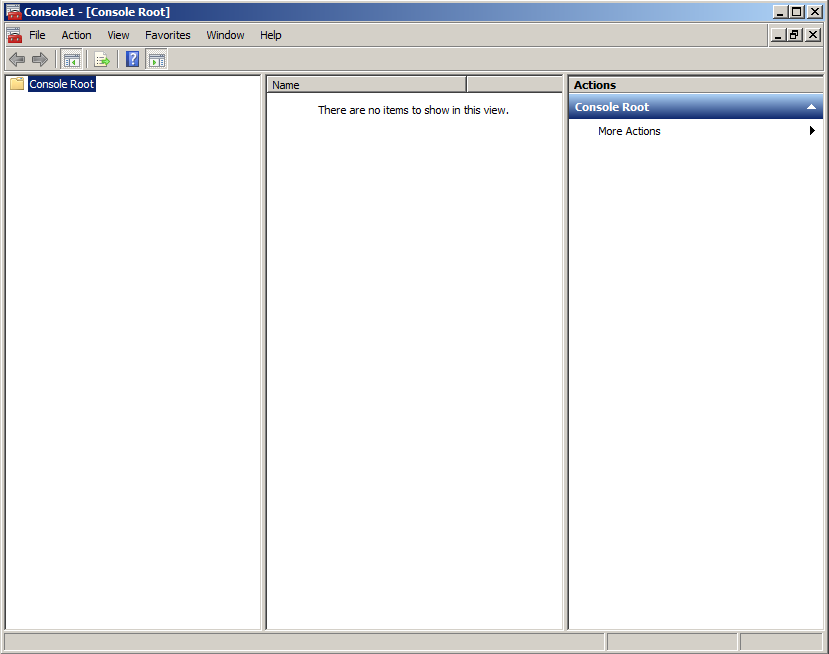
Congratulations, QlikView is using the QlikView Web Server configured as HTTPS://

# Configuring QlikView Web Services To Use SSL

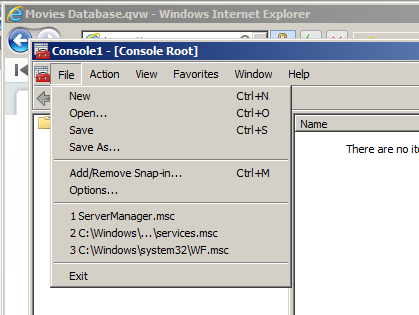
This section will describe how to configure SSL communication between the QlikView .Net web services, including Management console (QMS), Directory Service (DSC) Connector, QlikView Distribution Service (QDS), and the QlikView Web Server(QVWS).

It is assumed that the steps above have been followed and that either IIS or QlikView Web Server is being used and running SSL.

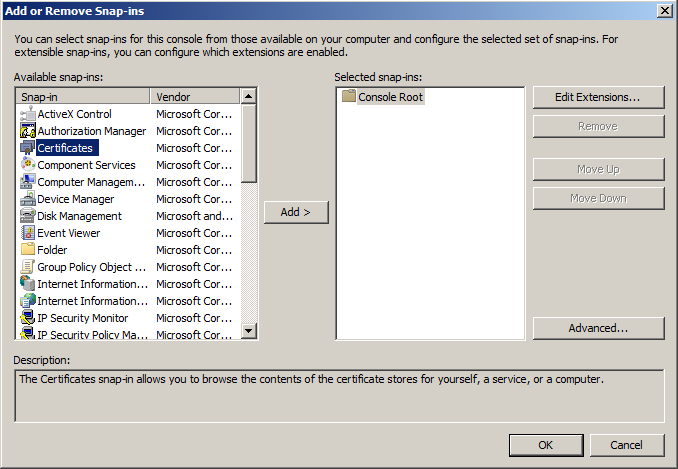
1. To start, the thumb print for the certificate is needed.
2. Open up an MMC window. Start - Run –MMC press Enter
3. The following dialog should open



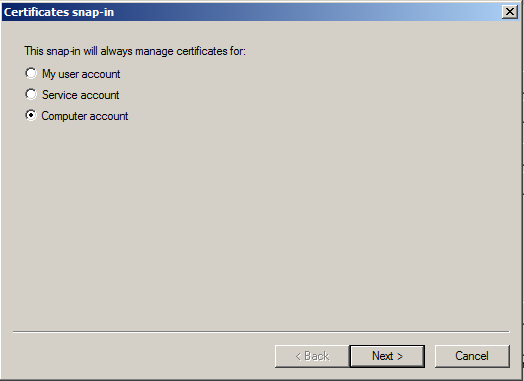
1. The Certificate snap-in needs to be added to the console
   1. Click File – Add/Remove Snap-in



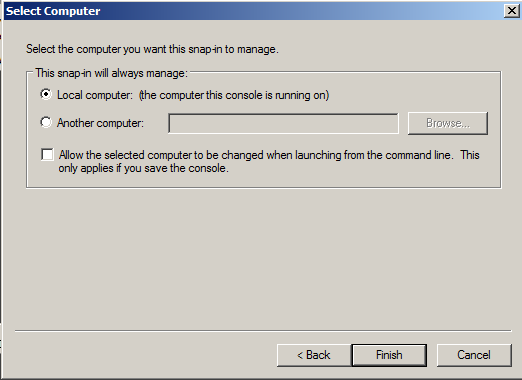
* 1. Scroll down to Certificates, select and add to the right hand pane.



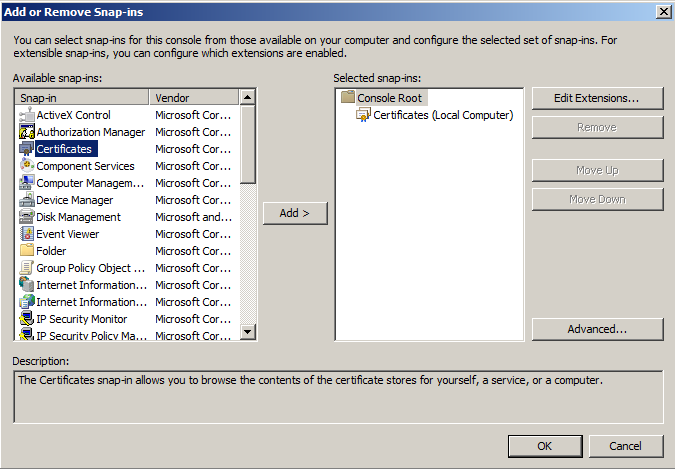
* 1. Select Computer Account on the next window, click next



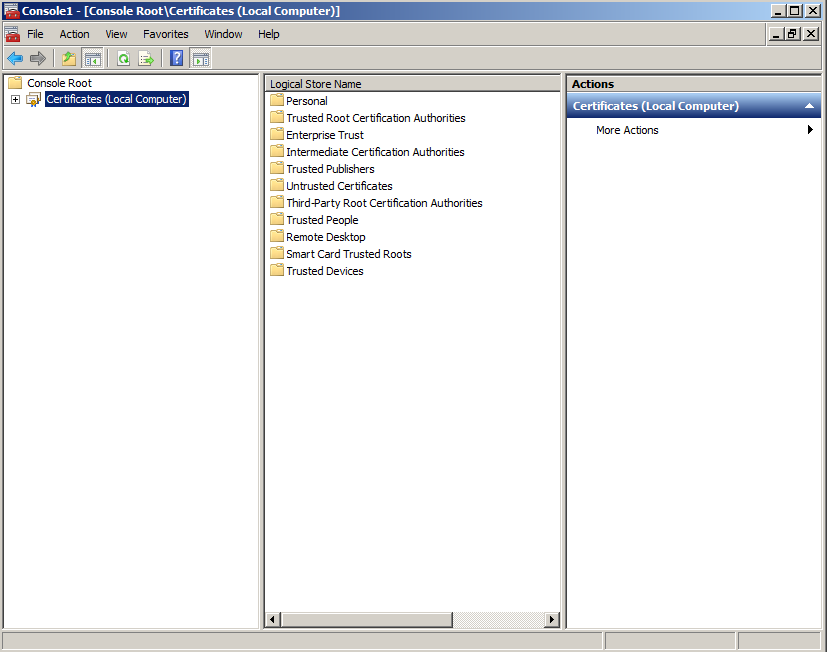
* 1. Select Local Computer on the next window, click Finish.



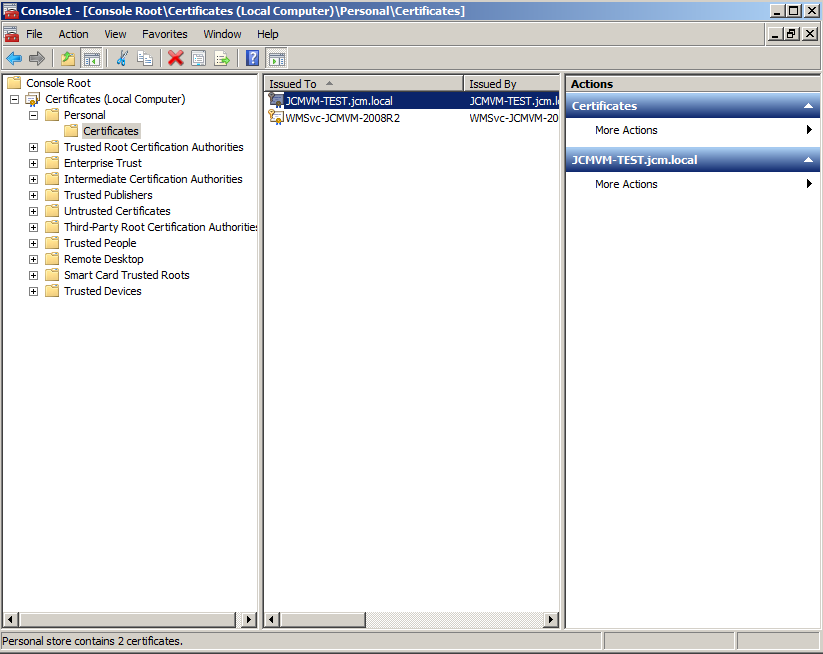
* 1. Click OK on the main Window



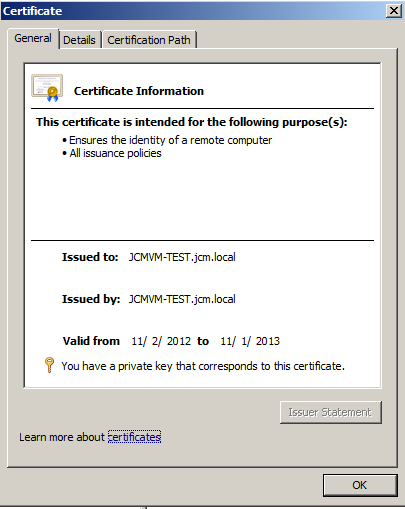
* 1. Once that is completed, the screen should resemble the figure below.



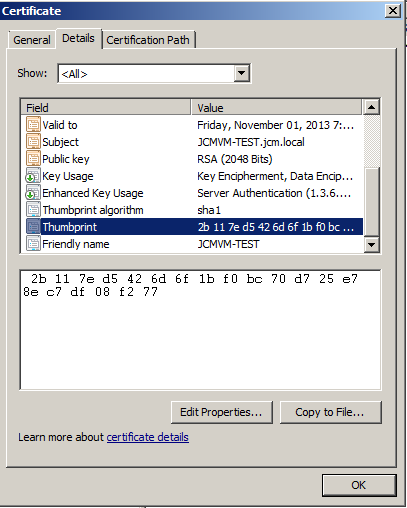
* 1. In the center panel, double click Personal, and then double click Certificates. The screen should resemble the figure below.



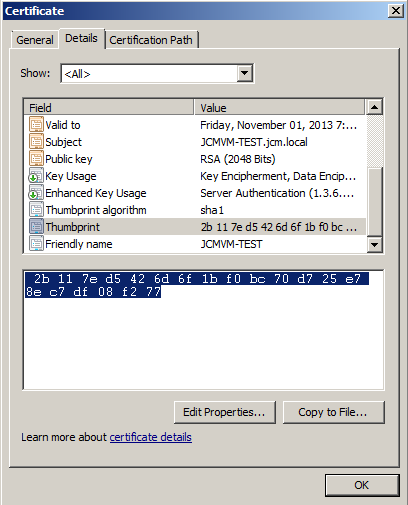
* 1. Based upon what was done when the certificate was created, the certificate should resemble the server name with which the user is working. In this example, JCMVM-TEST.JCM.LOCAL
  2. Double click the certificate to open and the screen should resemble the figure below.



* 1. Click the Details tab, scroll down and select thumbprint



* 1. In the lower pane, highlight and copy the alpha-numeric thumbprint

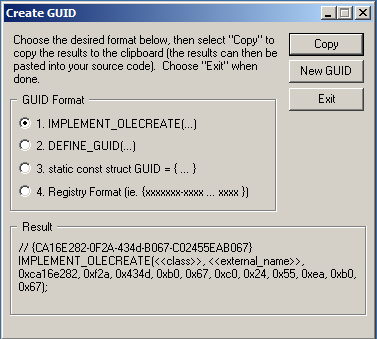


* 1. Open notepad and paste the thumbprint. Remove all the spaces between the pairs. It should look like this:

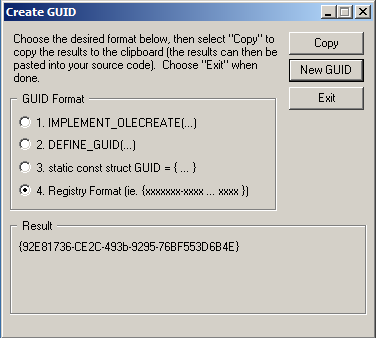
‎2b117ed5426d6f1bf0bc70d725e78ec7df08f277

* 1. Close the console, no need to save on close

1. The next step of the process is to generate a unique GUID to be used with the registration of the certificate
   1. Download Guidgen.exe from Microsoft
   2. <https://marketplace.visualstudio.com/items?itemName=AndrewLArnott.GuidGen20>
   3. Follow the instructions on the page to install
   4. Once the install is complete, run the Guidgen.exe
   5. The program will look like the following.



* 1. For this exercise a Registry Format GUID needs to be generated. Select option 4



* 1. Click New GUID and in the Result pane the new GUID will be generated.
  2. Click Copy
  3. Paste the GUID in the notepad that the thumbprint was copied to
  4. It should like the following

{92E81736-CE2C-493b-9295-76BF553D6B4E}

1. Now the certificate must be registered to each of the ports to be bound
2. The **netsh** command will be used to accomplish this.
3. The command line is as follows:

netsh http add sslcert ipport=0.0.0.0:***4799*** certhash=***thumbprint*** appid=***GUID***

Where:

**ipport** is the ipnumber of QlikView service (**always 0.0.0.0**)and the port used ( 4720, 4730, 4750, 4780, 4799).

**certhash** is the thumbprint hash of the certificate.

**appid** is the generated GUID in the form {xxxxxxxx-xxxx-….}”. The GUID must be enclosed by curly brackets.

1. Create five lines in notepad as follows:

netsh http add sslcert ipport=0.0.0.0:4799 certhash=hash appid=GUID

netsh http add sslcert ipport=0.0.0.0:4720 certhash=hash appid=GUID

netsh http add sslcert ipport=0.0.0.0:4730 certhash=hash appid=GUID

netsh http add sslcert ipport=0.0.0.0:4780 certhash=hash appid=GUID

netsh http add sslcert ipport=0.0.0.0:4750 certhash=hash appid=GUID

1. In each line where it says ***hash***, replace with the thumbprint. Where is says ***GUID*** replace with the GUID that was generated using Guidgen.exe, including the curly brackets.
2. The lines will look similar to the following (note the numbers used will vary from instance to instance).

netsh http add sslcert ipport=0.0.0.0:4799 certhash=**2b117ed5426d6f1bf0bc70d725e78ec7df08f277** appid=**{19E4B85D-380E-49d2-B46D-677F9F3FB0A9}**

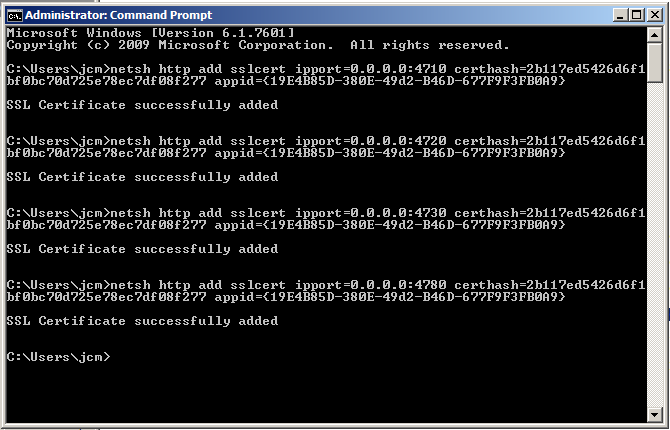
netsh http add sslcert ipport=0.0.0.0:4720 certhash=2b117ed5426d6f1bf0bc70d725e78ec7df08f277 appid={19E4B85D-380E-49d2-B46D-677F9F3FB0A9}

netsh http add sslcert ipport=0.0.0.0:4730 certhash=2b117ed5426d6f1bf0bc70d725e78ec7df08f277 appid={19E4B85D-380E-49d2-B46D-677F9F3FB0A9}

netsh http add sslcert ipport=0.0.0.0:4780 certhash=2b117ed5426d6f1bf0bc70d725e78ec7df08f277 appid={19E4B85D-380E-49d2-B46D-677F9F3FB0A9}

netsh http add sslcert ipport=0.0.0.0:4750 certhash=2b117ed5426d6f1bf0bc70d725e78ec7df08f277 appid={19E4B85D-380E-49d2-B46D-677F9F3FB0A9}

1. Open a command prompt and run each line in turn.
2. As each runs, the result should look like the following



1. To verify the registration of the certificate this command may be used:

netsh http show sslcert

1. The result in the command window should look similar to the following

SSL Certificate bindings:

-------------------------

IP:port : 0.0.0.0:443

Certificate Hash : 2b117ed5426d6f1bf0bc70d725e78ec7df08f277

Application ID : {4dc3e181-e14b-4a21-b022-59fc669b0914}

Certificate Store Name : MY

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

IP:port : 0.0.0.0:4799

Certificate Hash : 2b117ed5426d6f1bf0bc70d725e78ec7df08f277

Application ID : {19e4b85d-380e-49d2-b46d-677f9f3fb0a9}

Certificate Store Name : (null)

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

IP:port : 0.0.0.0:4720

Certificate Hash : 2b117ed5426d6f1bf0bc70d725e78ec7df08f277

Application ID : {19e4b85d-380e-49d2-b46d-677f9f3fb0a9}

Certificate Store Name : (null)

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

IP:port : 0.0.0.0:4730

Certificate Hash : 2b117ed5426d6f1bf0bc70d725e78ec7df08f277

Application ID : {19e4b85d-380e-49d2-b46d-677f9f3fb0a9}

Certificate Store Name : (null)

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

IP:port : 0.0.0.0:4750

Certificate Hash : 2b117ed5426d6f1bf0bc70d725e78ec7df08f277

Application ID : {19e4b85d-380e-49d2-b46d-677f9f3fb0a9}

Certificate Store Name : (null)

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Enabled

IP:port : 0.0.0.0:4780

Certificate Hash : 2b117ed5426d6f1bf0bc70d725e78ec7df08f277

Application ID : {19e4b85d-380e-49d2-b46d-677f9f3fb0a9}

Certificate Store Name : (null)

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

IP:port : 0.0.0.0:4799

Certificate Hash : 2b117ed5426d6f1bf0bc70d725e78ec7df08f277

Application ID : {19e4b85d-380e-49d2-b46d-677f9f3fb0a9}

Certificate Store Name : (null)

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Enabled

IP:port : 0.0.0.0:8172

Certificate Hash : 7658cfcd2fdbd7e94ecc76f0c752e3c007e85ee4

Application ID : {00000000-0000-0000-0000-000000000000}

Certificate Store Name : MY

Verify Client Certificate Revocation : Enabled

Verify Revocation Using Cached Client Certificate Only : Disabled

Usage Check : Enabled

Revocation Freshness Time : 0

URL Retrieval Timeout : 0

Ctl Identifier : (null)

Ctl Store Name : (null)

DS Mapper Usage : Disabled

Negotiate Client Certificate : Disabled

1. Each service needs some configuration changes so they work with SSL
2. Edit the Config.xml for the QlikView Web Server (Needs to be done if running IIS or QVWS)
3. The Config.xml can be found here in a default installation:

C:\ProgramData\QlikTech\WebServer

1. There are two items that need to be adjusted.
   1. The <configURL> for the web server needs to be changed from:

<ConfigUrl>[http://\_:4750/QVWS/Service</ConfigUrl](http://_:4750/QVWS/Service%3c/ConfigUrl)>

To

<ConfigUrl>[https://\_:4750/QVWS/Service</ConfigUrl](https://_:4750/QVWS/Service%3c/ConfigUrl)>

Note the https://

* 1. The <DirectoryServiceConnectorSettings> section has a URL than needs to be changed to the fully qualified domain name and to use HTTPS://

<Url>[http://jcmvm-test:4730/DSC/Service</Url](http://jcmvm-test:4730/DSC/Service%3c/Url)>

To

<Url>[https://jcmvm-test.jcm.local:4730/DSC/Service</Url](https://jcmvm-test.jcm.local:4730/DSC/Service%3c/Url)>

1. The configuration files for the following services must be changed to use SSL, QlikView Management Service, QlikView Directory Service Connector and the QlikView Distribution Service Connector. The configuration files can be found in the following locations:

C:\Program Files\QlikView\Management Service\**QVManagementService.exe.config**  
C:\Program Files\QlikView\Directory Service Connector\**DirectoryServiceConnector.exe.config**  
C:\Program Files\QlikView\Distribution Service\**QvDistributionService.exe.config**

1. Each file has the following lines:

<!-- Use HTTPS instead of HTTP for SSL-encrypted communication. You must configure a certificate for this to work -->

<add key="UseHTTPS" value="false"/>

1. Change the key from “false” to “true”

<!-- Use HTTPS instead of HTTP for SSL-encrypted communication. You must configure a certificate for this to work -->

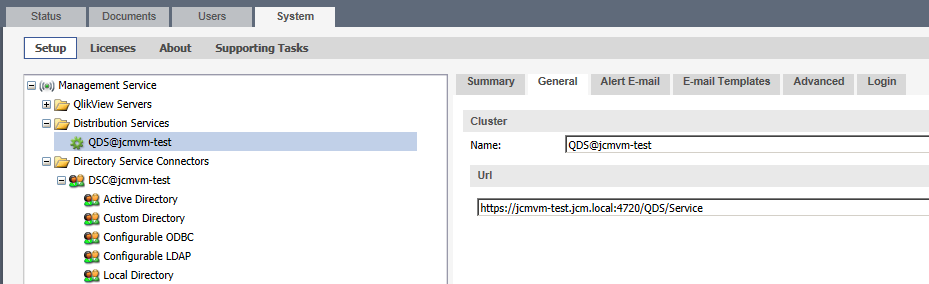
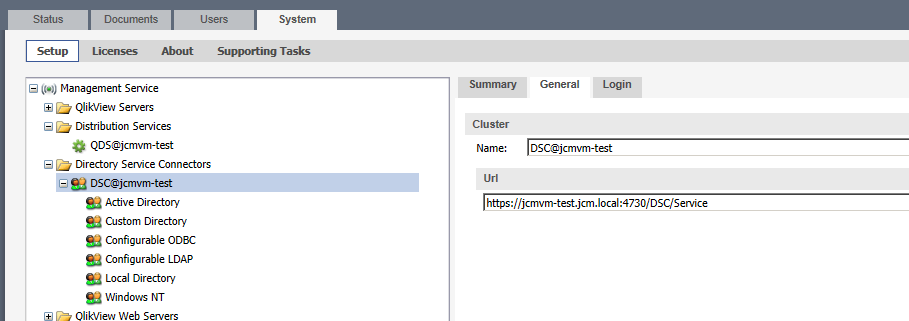
<add key="UseHTTPS" value="true"/>

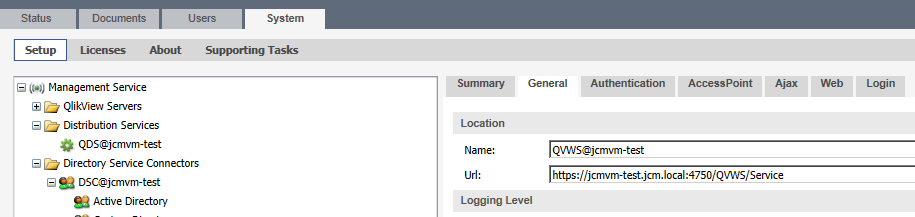
1. Save the files and restart the services.
2. For things to work properly, the URLs for the QlikView Distribution Service, Directory Service Connector and QlikView Web Service must be changed in the QlikView Management Console to use HTTPS and the fully qualified domain name.
3. Open the QlikView Management Console by using

https://<FullyQualifiedServerDomainName>:4780/qmc/default.htm

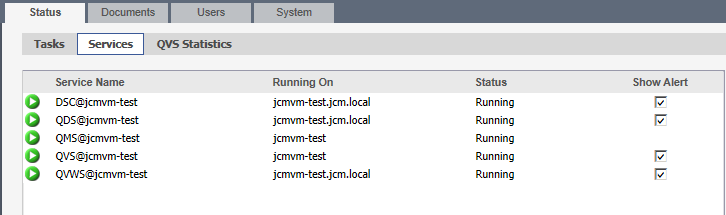
If https is not used, the Management Console will not open.

* 1. Navigate to each of the services General tab and adjust the URL, remember to click apply after each change.



1. If a service says it needs to be restarted after changing the URL, do so.
2. Check to be sure the services are all connected and display the green icon and show Running in the Status column.



Congratulations, Qlikview services are using SSL for communication.