

Bond V6 - Https configuration

- Over view
- Enable Https for ECC in Tomcat
 - Open cmd as Administrator
 - Move to the Tomcat config directory by using: `cd YOUR_TOMCAT_DIRECTORY/conf`
 - Generating Keystore
 - Uncomment Connector to port 8443 in `YOUR_TOMCAT_DIRECTORY/conf/server.xml`
 - Access your application
- Enable Https for BOND in IIS (Internet Information Services)
 - Open Internet Information Services (IIS) Manager
 - In the explorer, select YOUR_SERVER
 - In the IIS tab in the middle, double-clicked to select Server Certification
 - In Server Certificates, chose "Create Self-Signed Certificate...", uses localhost as your friend name for the certificate
 - Change the Binding of the Default Web Site:
 - Access your application
- Add Certification to Java TrustStore
 - Export IIS certification:
 - Add IIS certification to Java Trust Store
- Add IIS certificate to Browsers
 - Chrome, IE (Internet Exploer)
 - In IE 11
 - Firefox

Over view

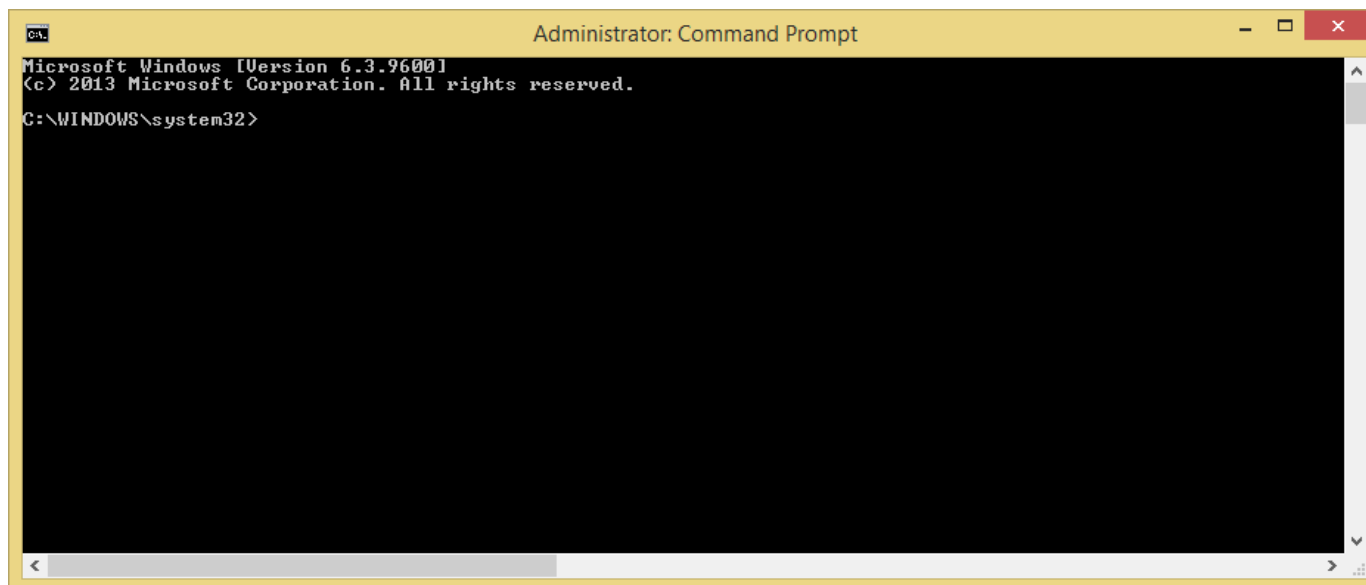
This documentation is about guide user to config system to run both ECC and BOND through Https.

To make ECC and BOND run through Httpss user needs:

- Enable Https for ECC in Tomcat.
- Enable Https for BOND in IIS (Internet Information Services).
- Add BOND's certificate to Trust Store of Tomcat's JVM (Tomcat which run ECC).
- Add BOND's certificate to Browsers (Chrome, Firefox, IE) run ECC.

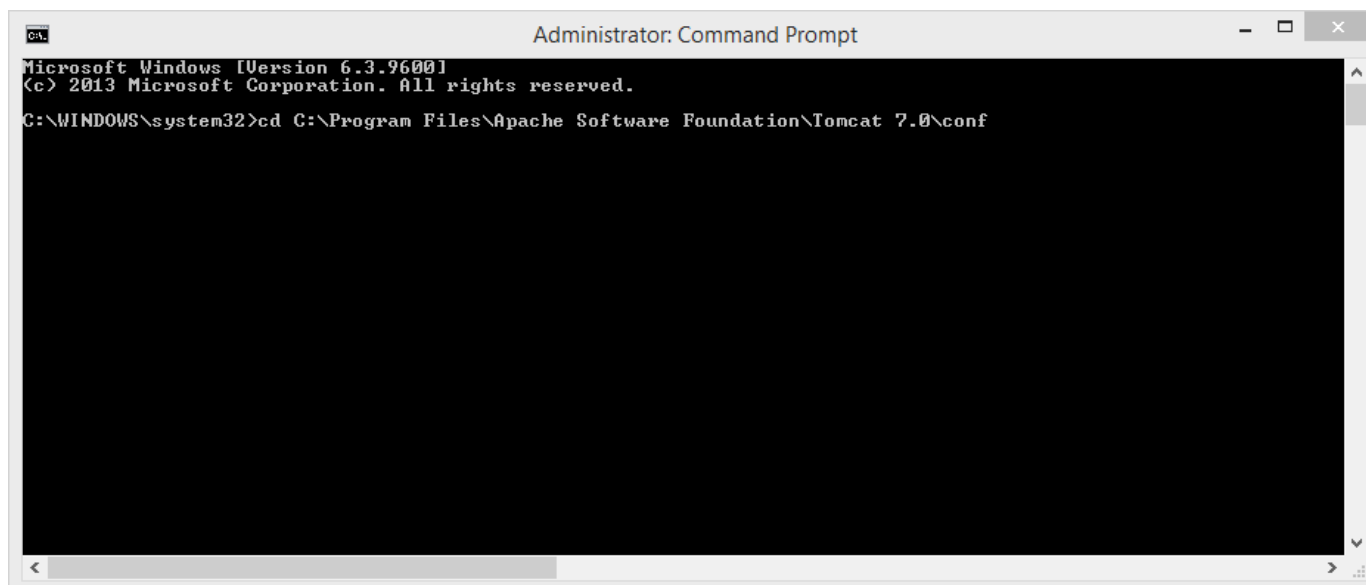
Enable Https for ECC in Tomcat

Open cmd as Administrator



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>
```

Move to the Tomcat config directory by using: `cd YOUR_TOMCAT_DIRECTORY/conf`



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\WINDOWS\system32>cd C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf
```

Generating Keystore

```

C:\Program Files\Apache Software Foundation\Tomcat
7.0\conf>"%JAVA_HOME%\bin\keytool" -genkey -alias nb080010 -keyalg RSA
-keystore myKeystore.jks -storepass administrator2011@
What is your first and last name?
[Unknown]: localhost
What is the name of your organizational unit?
[Unknown]: YOUR_UNIT
What is the name of your organization?
[Unknown]: YOUR_ORGANIZATION
What is the name of your City or Locality?
[Unknown]: YOUR_CITY
What is the name of your State or Province?
[Unknown]: YOUR_STATE
What is the two-letter country code for this unit?
[Unknown]: VN
Is CN=localhost, OU=YOUR_UNIT, O=YOUR_ORGANIZATION, L=YOUR_CITY,
ST=YOUR_STATE, C=VN correct?
[no]: YES
Enter key password for <nb080010>
(RETURN if same as keystore password):
Re-enter new password:

```

Note:

- In the question *"What is your first and last name?"*, uses *"localhost"*.

Uncomment Connector to port 8443 in YOUR_TOMCAT_DIRECTORY/conf/server.xml

```

79      redirectPort="8443" />
80      <!--
81      <!-- Define a SSL HTTP/1.1 Connector on port 8443
82      This connector uses the JSSE configuration, when using APR, the
83      connector should be using the OpenSSL style configuration
84      described in the APR documentation -->
85      <Connector port="8443" maxThreads="200"
86      scheme="https" secure="true" SSLEnabled="true"
87      keystoreFile='${catalina.home}/conf/tomcatKeyStore.jks' keystorePass="ventum2011@" truststoreFile='C:/Program Files/Java/jre7/lib/security/cacerts'
88      truststorePass='changeit'
89      clientAuth="false" sslProtocol="TLS"/>
90
91      <!--
92      <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"
93      maxThreads="150" scheme="https" secure="true"
94      clientAuth="false" sslProtocol="TLS" />
95      -->
96

```

Note: *keystorePass* is the password you've enter when Generating Keystore above

Please see [this](#) for example.

Reset tomcat to apply the changes

Access your application

By using: https://YOUR_DOMAIN:8443/YOUR_APPLICATION/

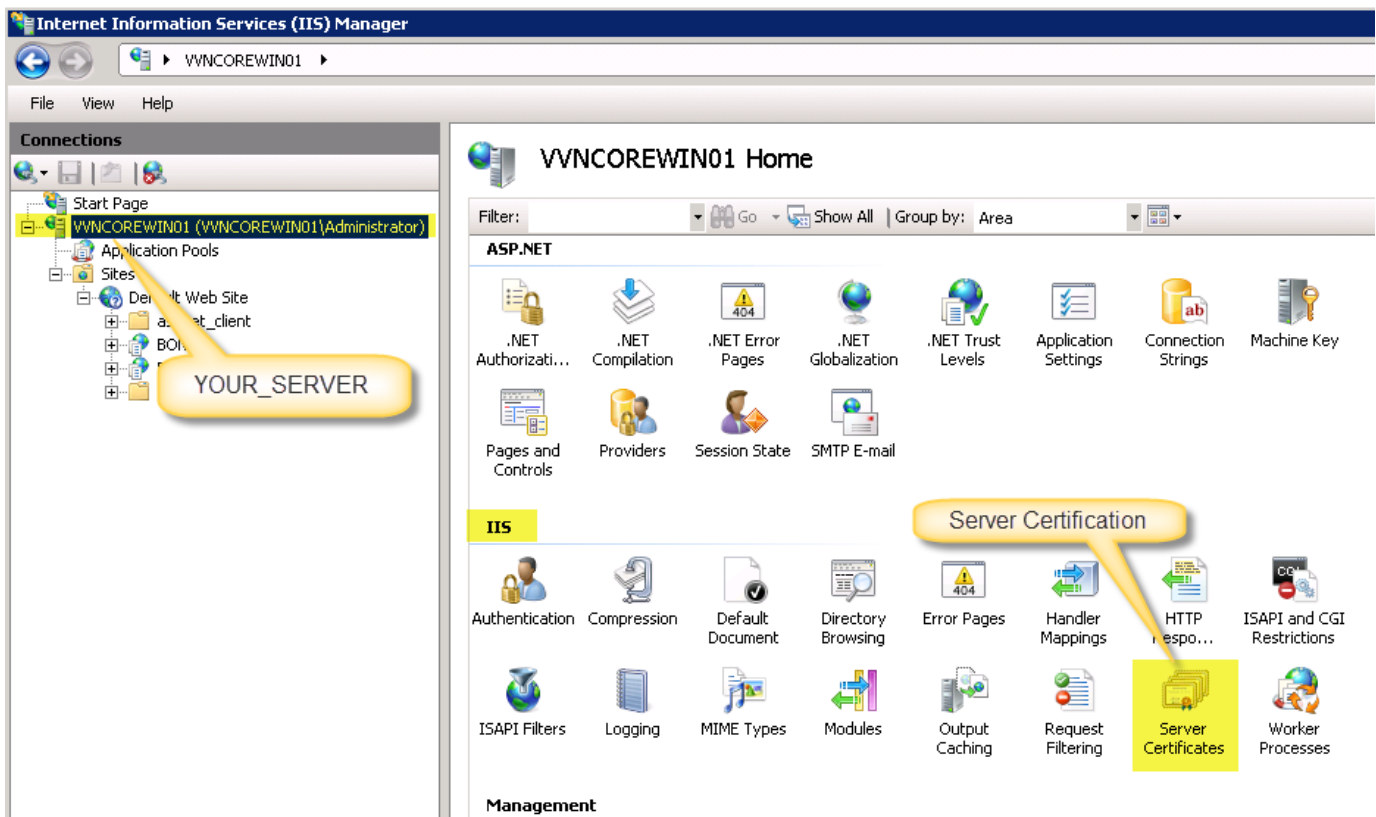
Example: <https://localhost:8443/ECC/>

Enable Https for BOND in IIS (Internet Information Services)


Open Internet Information Services (IIS) Manager

In the explorer, select **YOUR_SERVER**

In the IIS tab in the middle, double-clicked to select **Server Certification**



In Server Certificates, chose "Create Self-Signed Certificate...", uses *localhost* as your friend name for the certificate




Server Certificates

Use this feature to request and manage certificates that the Web server can use with Web sites configured for SSL.

Name	Issued To	Issued By	Expiration
localhost	VVNCOREWIN01.sbb01.spoc.global	AutomicSoftwareGmbHIssuingCA	6/18/201
automic.com	VVNCOREWIN01.sbb01.spoc.global	VVNCOREWIN01.sbb01.spoc.gl...	3/24/201
	VVNCOREWTN01.sbb01.spoc.global	AutomicSoftwareGmbHRootCA	4/4/2016
			4/6/2016
			5/6/2019

Create Self-Signed Certificate



Specify Friendly Name

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

Specify a friendly name for the certificate:

OK Cancel

Actions

- Import...
- Create Certificate Request...
- Complete Certificate Request...
- Create Domain Certificate...
- Create Self-Signed Certificate...
- Help
- Online Help

Change the Binding of the Default Web Site:

Step 1: Select "Default Web Site"

Step 2: Under Edit Site, select **Bindings ...**

Step 3: Select row **https**, then chose **Edit**

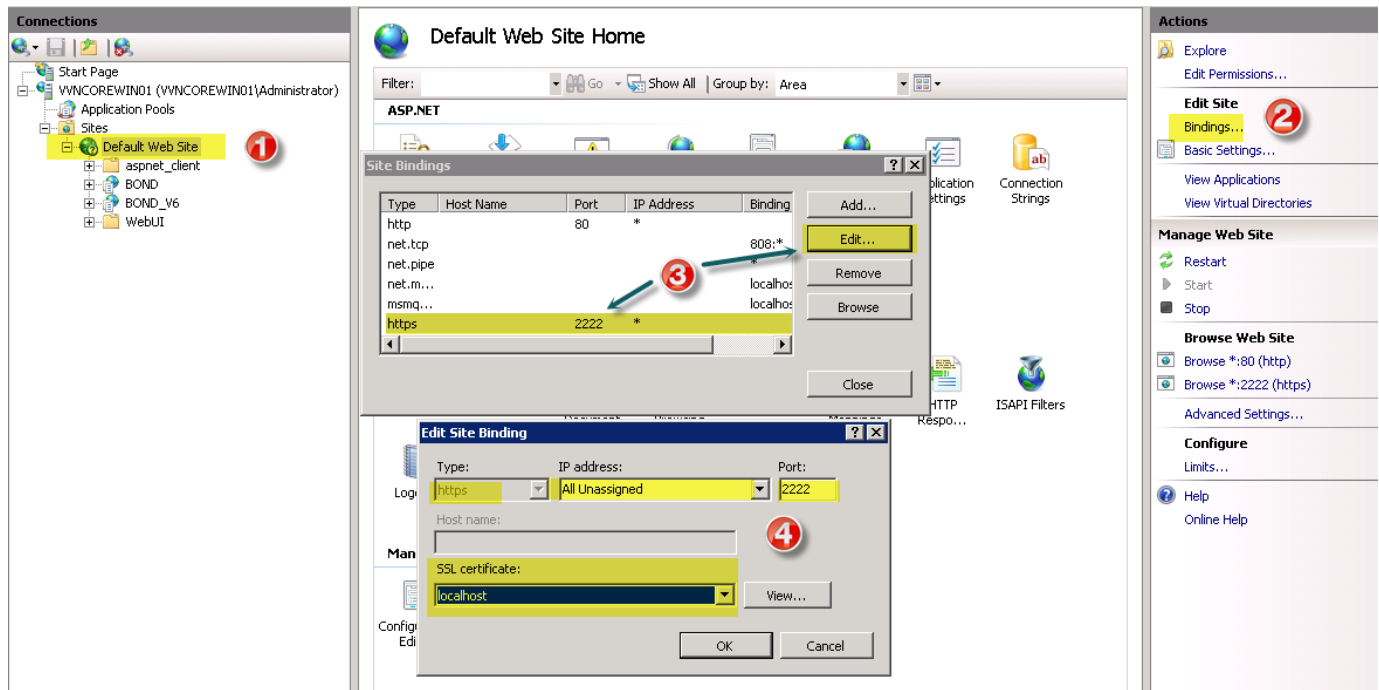
Step 4:

Type: https

IP address: All Unassigned

Port: the port, example: 2222

SSL certificate: Link to your "Self-Signed Certificate" created in above step.



Access your application

By using: https://YOUR_DOMAIN:2222/YOUR_APPLICATION/

Example: <https://localhost:2222/BOND/>

Add Certification to Java TrustStore

Export IIS certification:

Step 1: Select "Default Web Site"

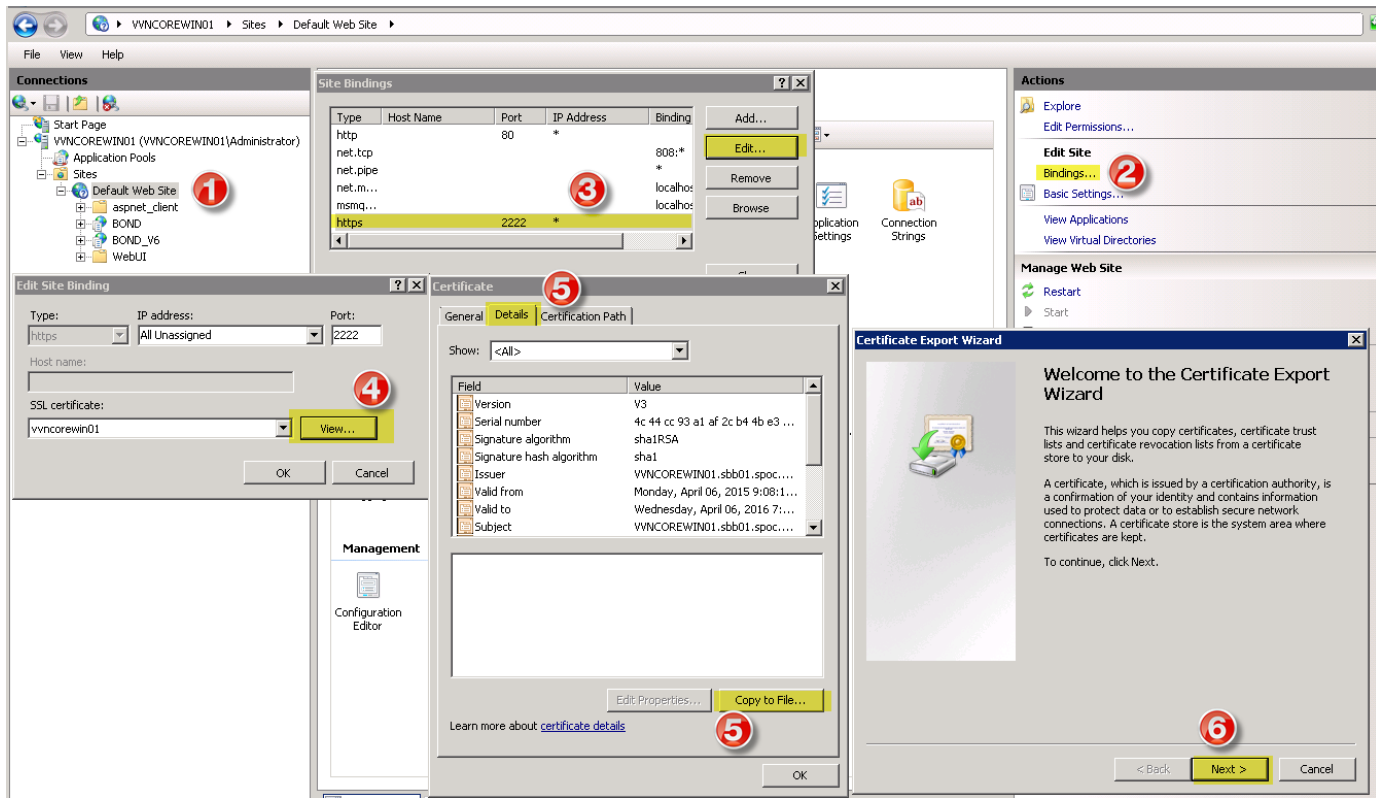
Step 2: Under Edit Site, select **Bindings ...**

Step 3: Select row **https**, then chose **Edit**

Step 4: Select **View**

Step 5: Select **Details** tab then click "**Copy to File...**"

Step 6: Click **Next**



Chose **No**, do not export the private key



Chose **DER encoded binary X.509**

Certificate Export Wizard ✕

Export File Format
Certificates can be exported in a variety of file formats.

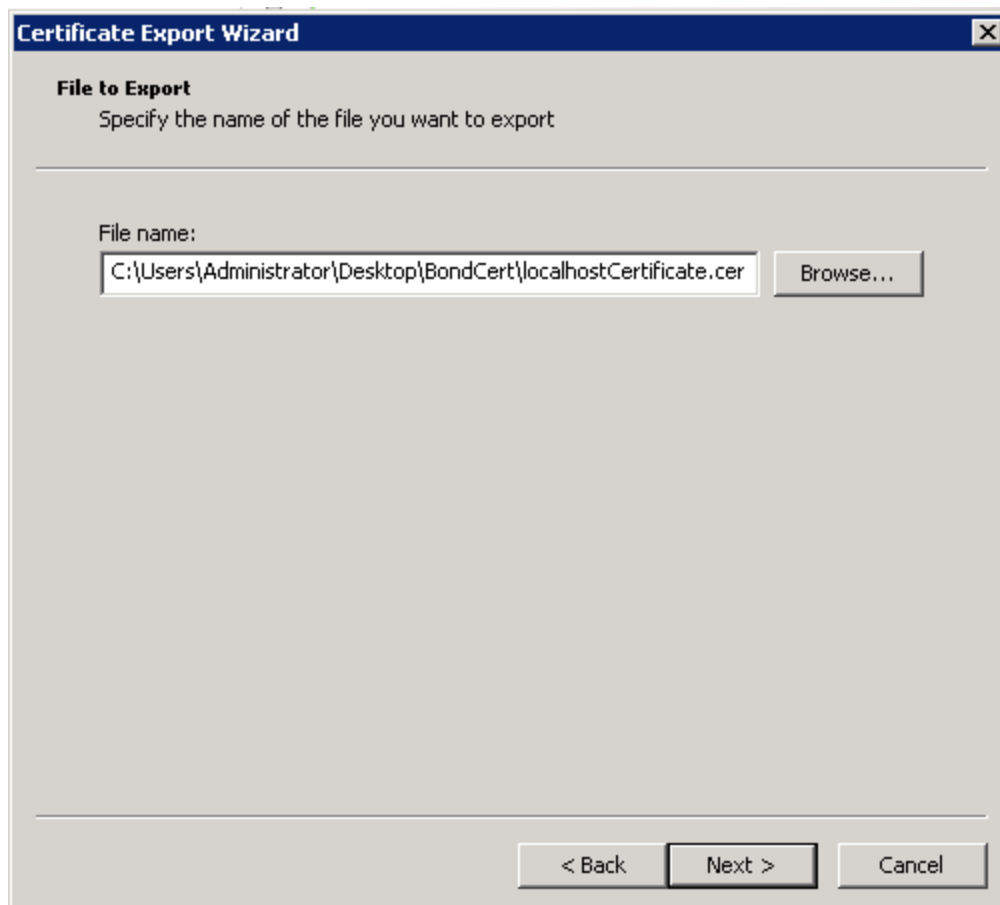
Select the format you want to use:

- ☒ DER encoded binary X.509 (.CER)
- ☐ Base-64 encoded X.509 (.CER)
- ☐ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
 - ☐ Include all certificates in the certification path if possible
- ☐ Personal Information Exchange - PKCS #12 (.PFX)
 - ☐ Include all certificates in the certification path if possible
 - ☐ Delete the private key if the export is successful
 - ☐ Export all extended properties
- ☐ Microsoft Serialized Certificate Store (.SST)

Learn more about [certificate file formats](#)

< Back Next > Cancel

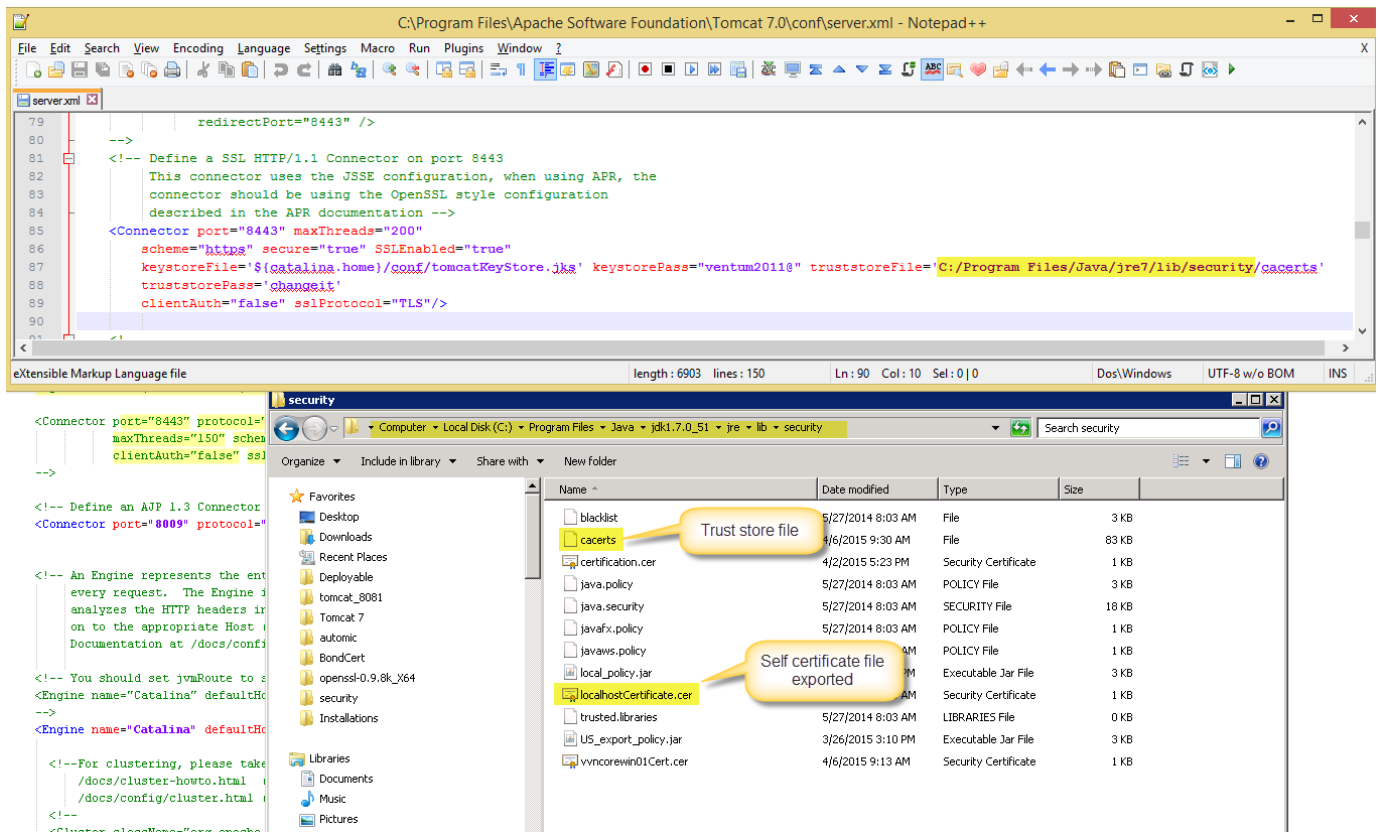
Select destination to export Certificate file



Click Next then Finish.

Add IIS certification to Java Trust Store

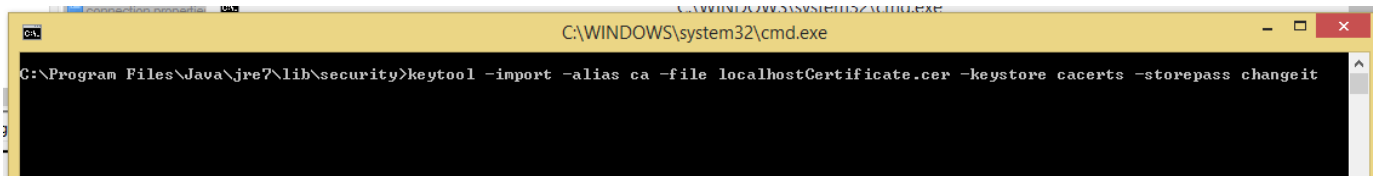
Copy certificate file generated above step to folder Security of Tomcat JVM (can be found in the Tomcat file config: server.xml, property: truststoreFile)



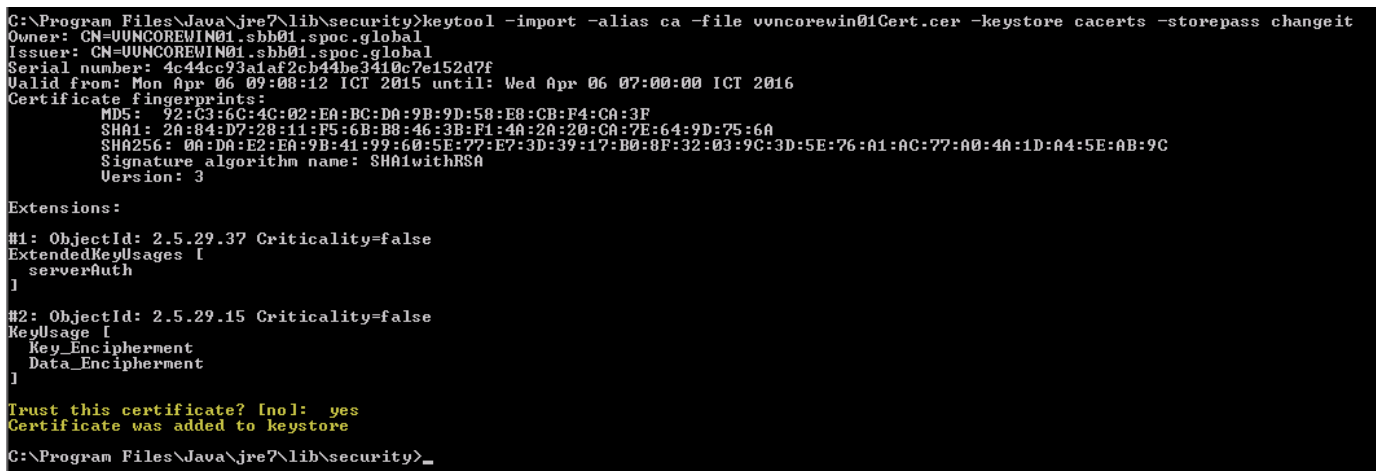
Open cmd and move it to folder Security of Tomcat JVM:

Add certificate to **cacerts** Trust Store by using: **keytool -import -alias ca -file <your_self_certificate.cer> -keystore cacerts -storepass changeit**

Example: **keytool -import -alias ca -file localhostCertificate.cer -keystore cacerts -storepass changeit**



Select Trust this certificate



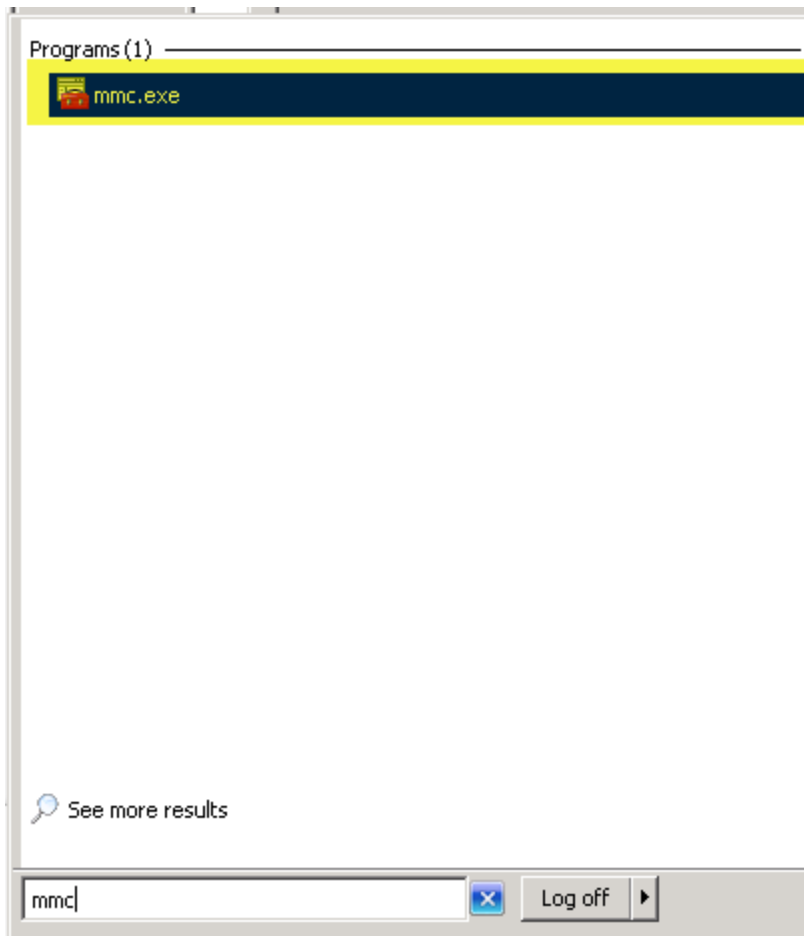
Add IIS certificate to Browsers

Chrome, IE (Internet Explorer)

Copy IIS certification (the same file IIS certification in step "*Add IIS certification to Java Trust Store*" above) to you local PC (**PC which run Browsers**). Assume IIS is copied to C:/Cerfitication

Start Mircrosoft Management Console by open run (Select **Start**, then **Run**).

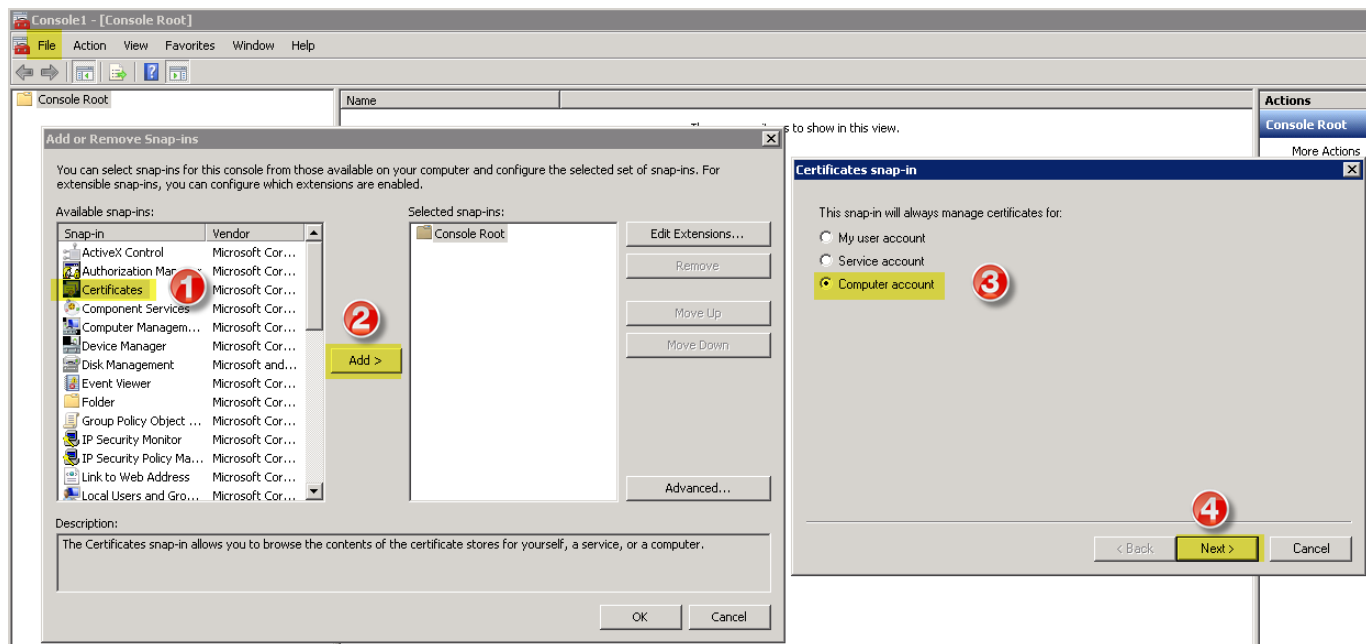
In the Run, type **mmc.exe** then press **Enter**



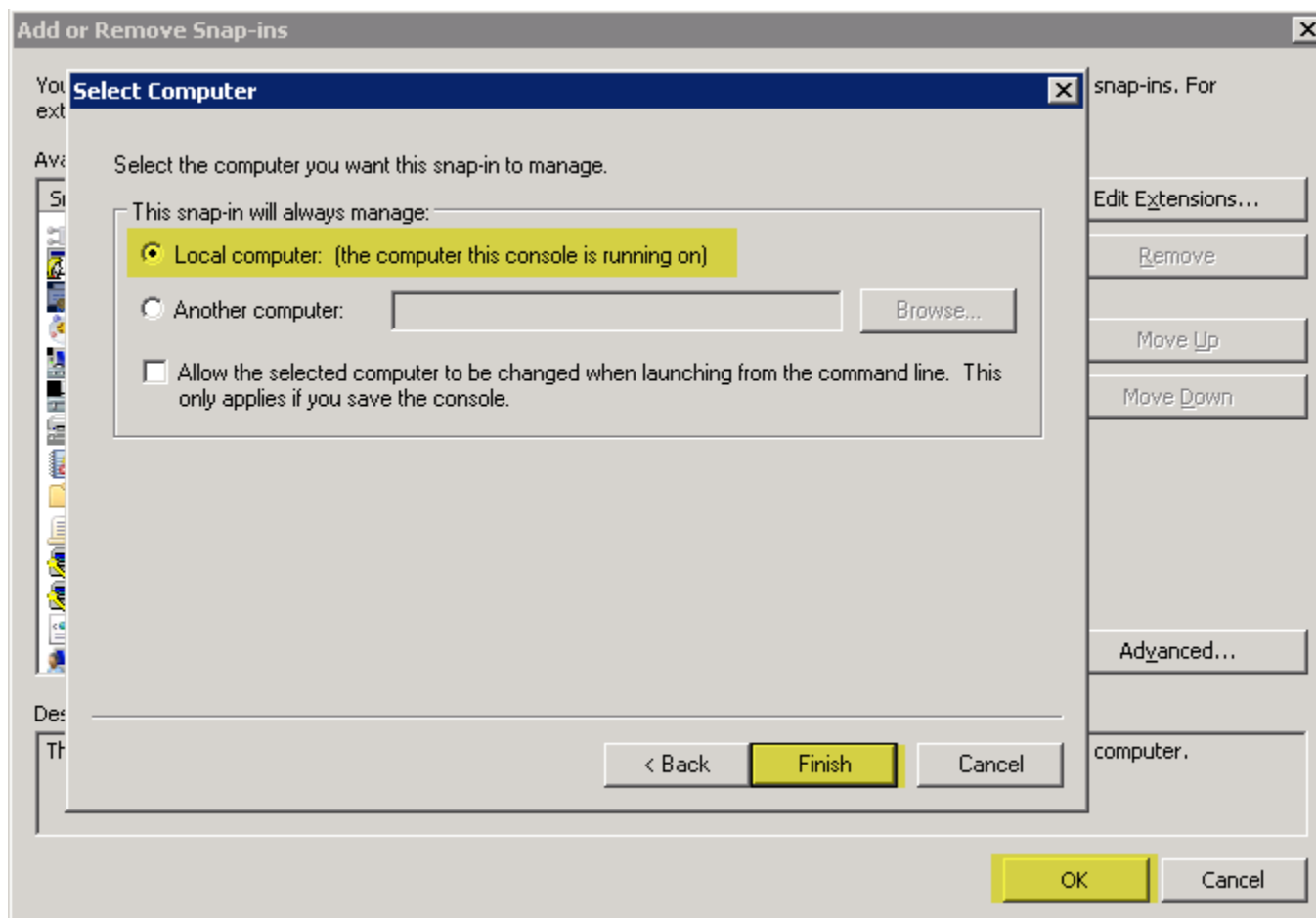
Select File -> Add/Remove Snap-in (Ctrl+M).

Under "**Available snap-ins**", select **Certificates** then click **Add**.

A **Certificates snap-in** window will show up, select **Computer account**, then **Next**

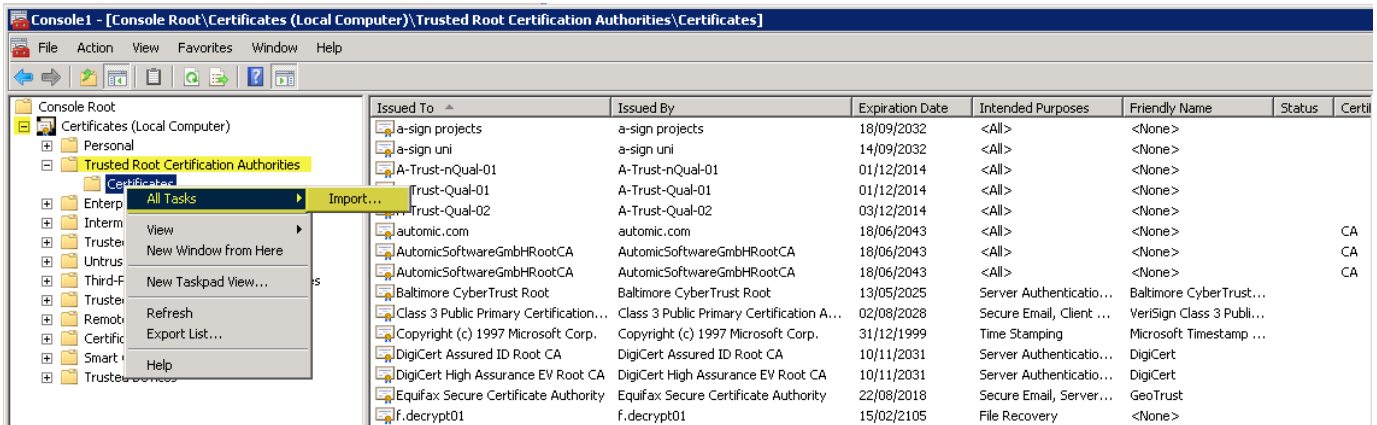


Select **Local Computer**, click **Finish** then **OK**

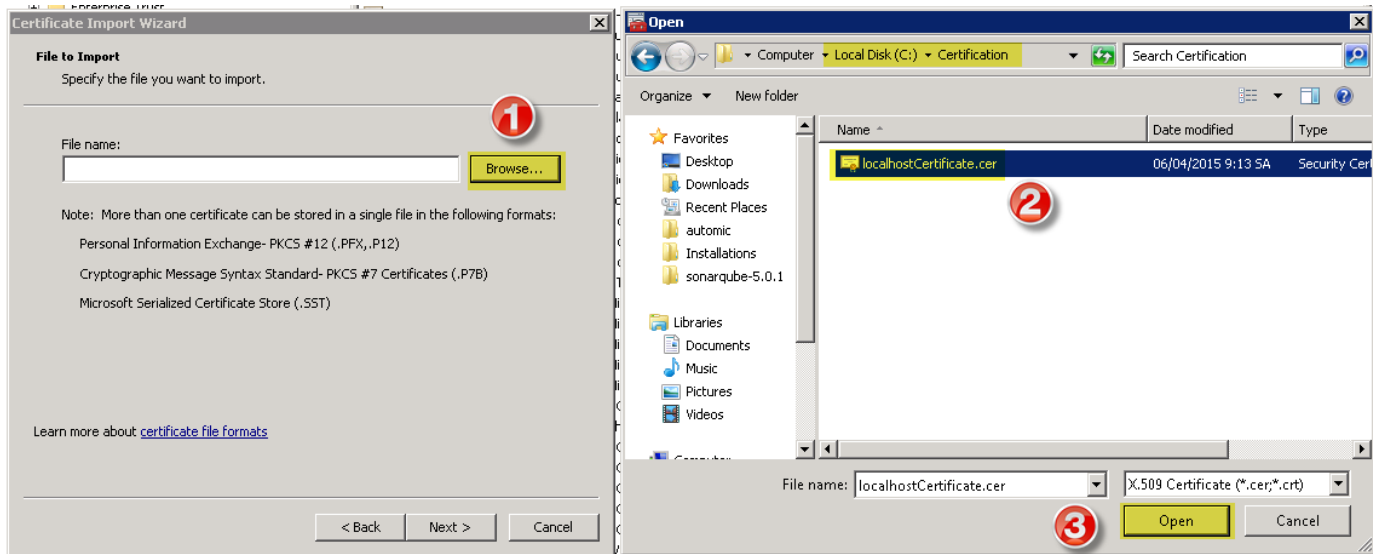


Expand **Certificates (Local Computer)**, expand **Trusted Root Certification Authorities**.

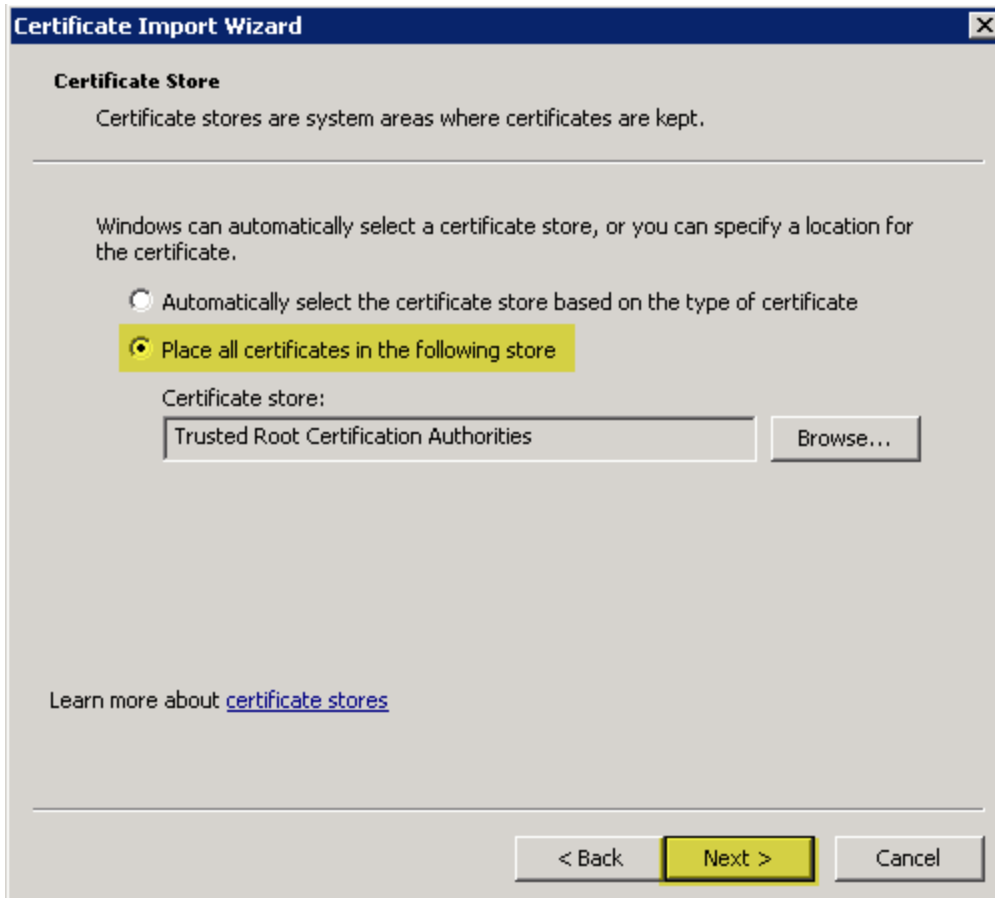
Under Trusted Root Certification Authorities, right click into **Certificates**, select **All Tasks**, **Import** then click **Next**



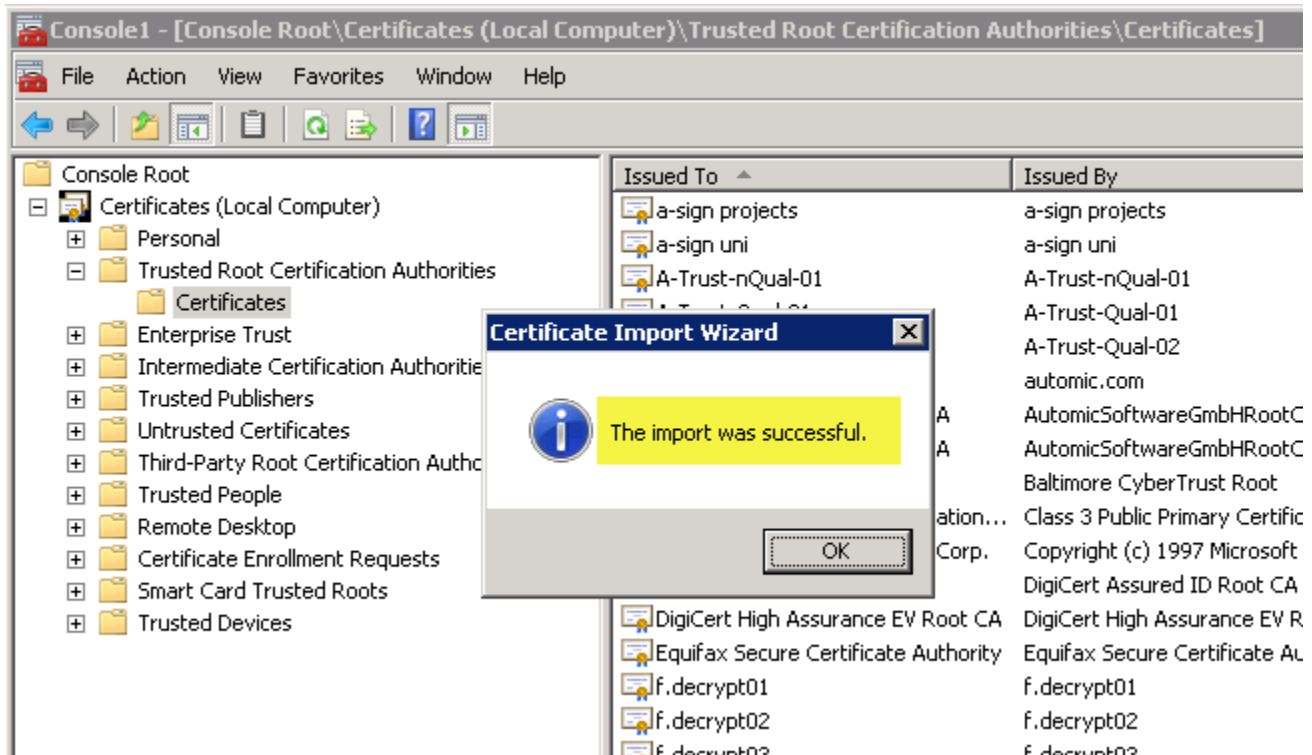
Browser to copied IIS certificate, then **Next**



Select **"Place all certificates in the following store"**, click **Next**, then **Finish**

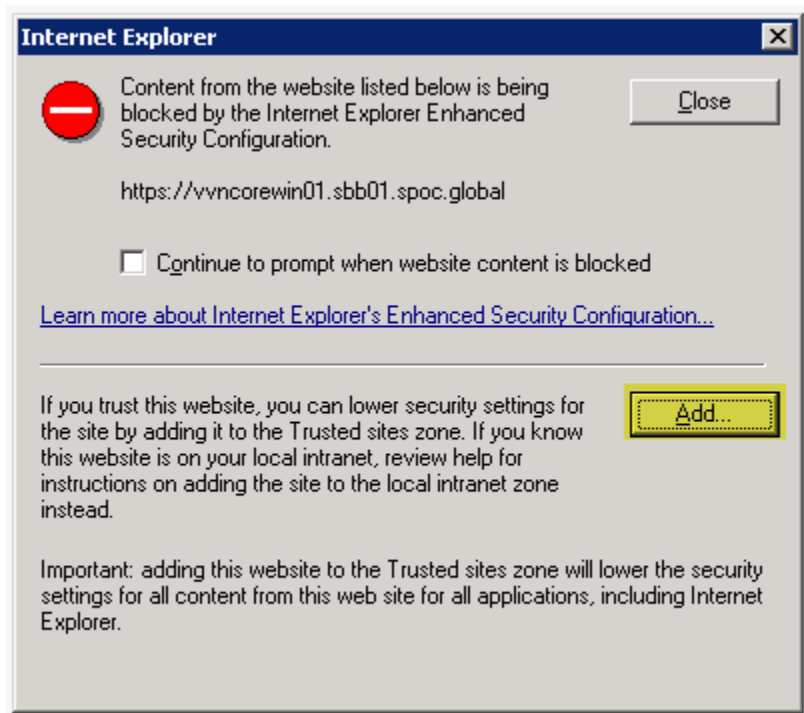


Success window will be shown

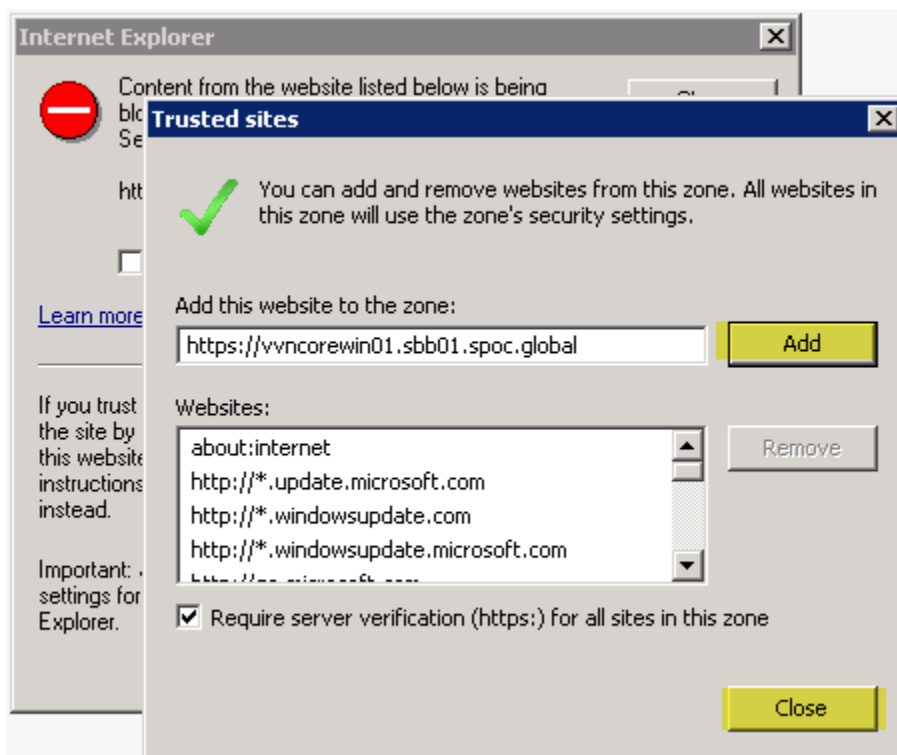


In IE 11

If got below warning

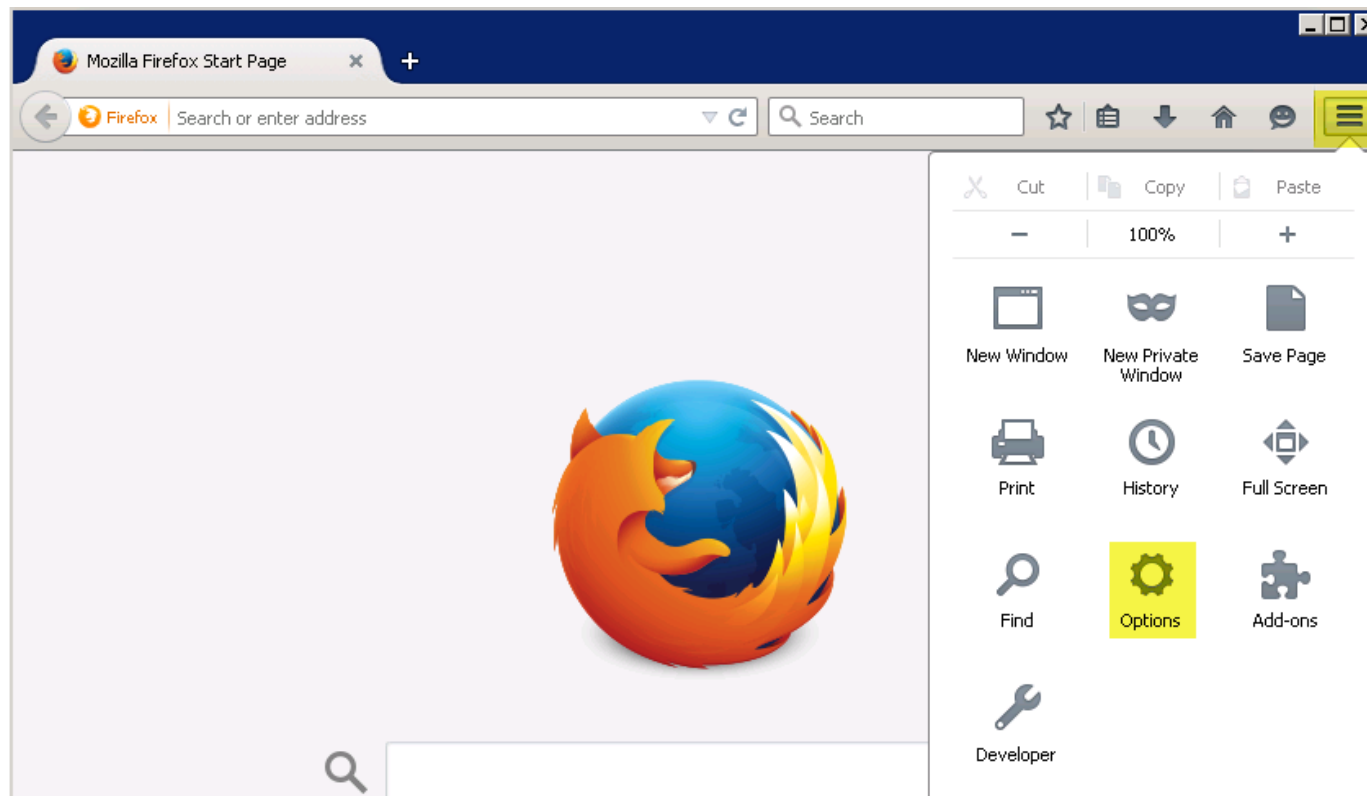


Click **Add**, a **Trusted sites** window will show up. Click **Add**, then **Close**



Firefox

Select **Open Menu**, chose **Option**



Select **Advanced**, tab **Certificates**, click **View Certificates**, **Certificate Manager** window will open.

Under **Certificate Manager**, select tab **Servers**, click **Add Exception**, an **Add Security Exception** window will open.

Under **Add Security Exception**, past BOND's full address to **Location**, then click Get Certificate. Keep check-box at **Permanently store this exception**, then click **Confirm Security Exception**.

