

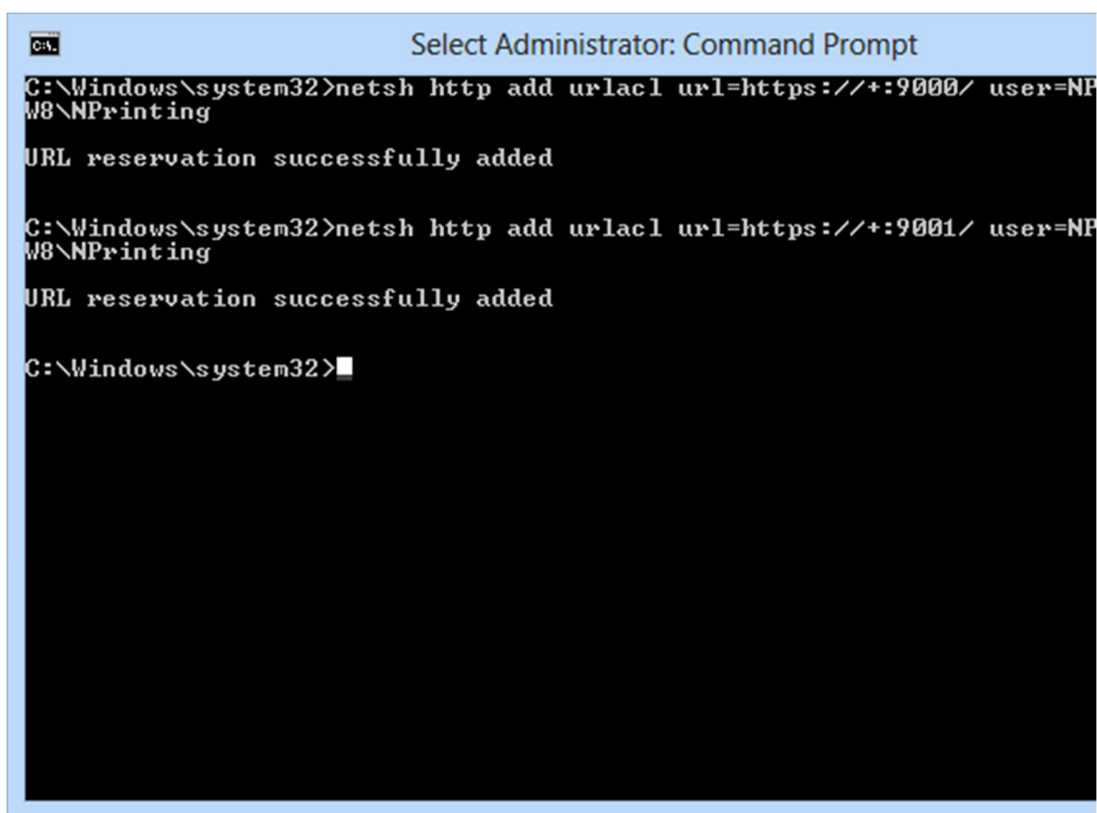
How to Enable SSL in On-Demand

SSL can be enabled selectively per-endpoint.

For example, you can enable SSL for HTTP endpoint and disable SSL for WS endpoint. Also see "[NPrinting On-Demand: Architecture and Configuration](#)".

A valid SSL certificate signed by a valid CA (public or domain) must be bound to the <https://yourhostdnsname:ajaxport/> address you plan to use for the endpoint.

Ports Reservation



```
C:\Windows\system32>netsh http add urlacl url=https://+:9000/ user=NPrinting
URL reservation successfully added

C:\Windows\system32>netsh http add urlacl url=https://+:9001/ user=NPrinting
URL reservation successfully added

C:\Windows\system32>
```

Ports reservation are done automatically at service startup in NPrinting 14.0.0.12 or higher releases. In some installations, you must reserve TCP ports listening for the On-Demand service process.

After opening a Command Prompt as Administrator, check if SSL is enabled:

1. Enter **netsh http add urlacl url=<https://+:9000/> user=DOMAIN\user** , replace DOMAIN\user with the domain and the name of your NPrinting Server account
2. Enter **netsh http add urlacl url=<https://+:9001/> user=DOMAIN\user**
If a port is reserved by another process and you are sure you can use it with On-Demand, remove the reservation before enabling it typing the following:
Enter **netsh http delete urlacl url=<https://+:9000/>** (replace 9000 with target TCP port and http with https if SSL is enabled)

Install Makecert Tool



Installation Options



Feature Description Detail

Tools

Installs tools that can help you use applications.

This feature requires 33,3 MB of hard disk space.

Disk Space Requirements

Volume	Available
C:	73,8 GB
S:	971,9 MB

Download Size

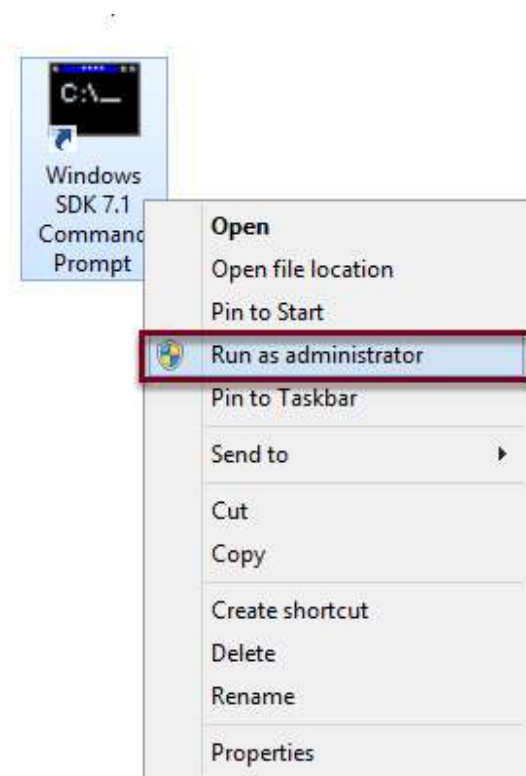
99,6 MB

If you already have a SSL certificate, go directly to "Get the Certificate Thumbprint" step further below in this tutorial.

After logging in with your NPrinting Server account, download and install "[Microsoft Windows SDK for Windows 7 and .NET Framework 4](#)" if your system does not have "makecert" installed.

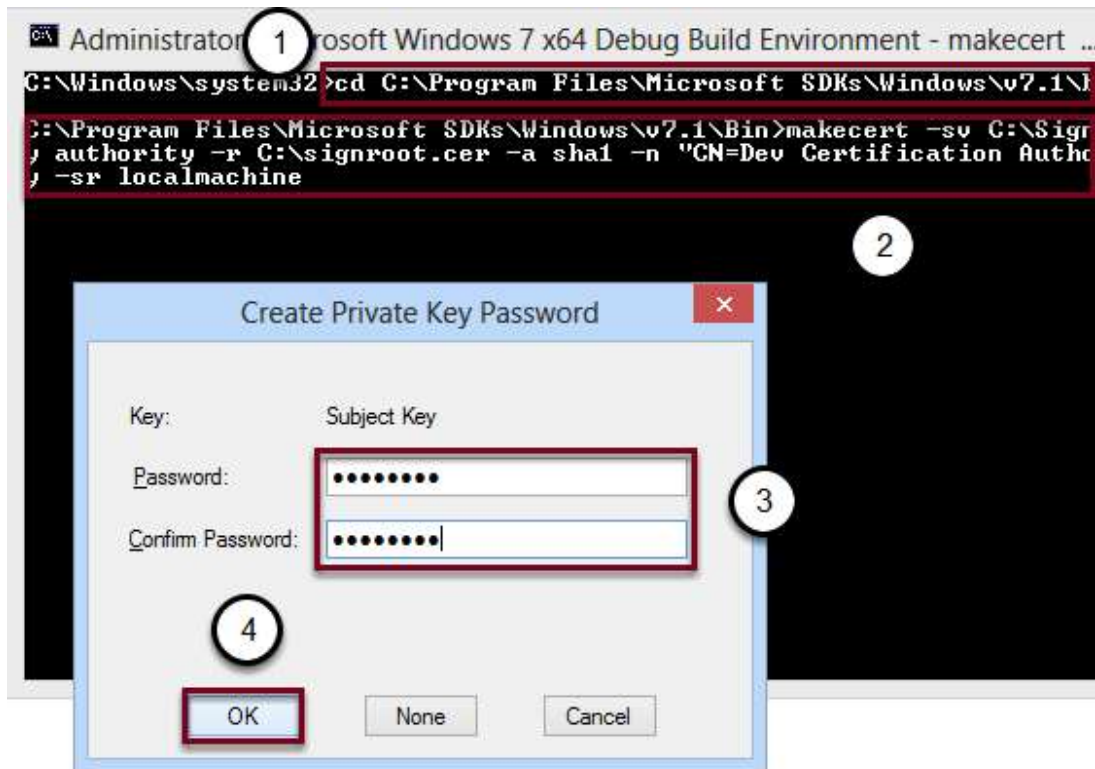
Select **Tools** during the installation and finish the installation

Create a Trusted Certificate only for Test



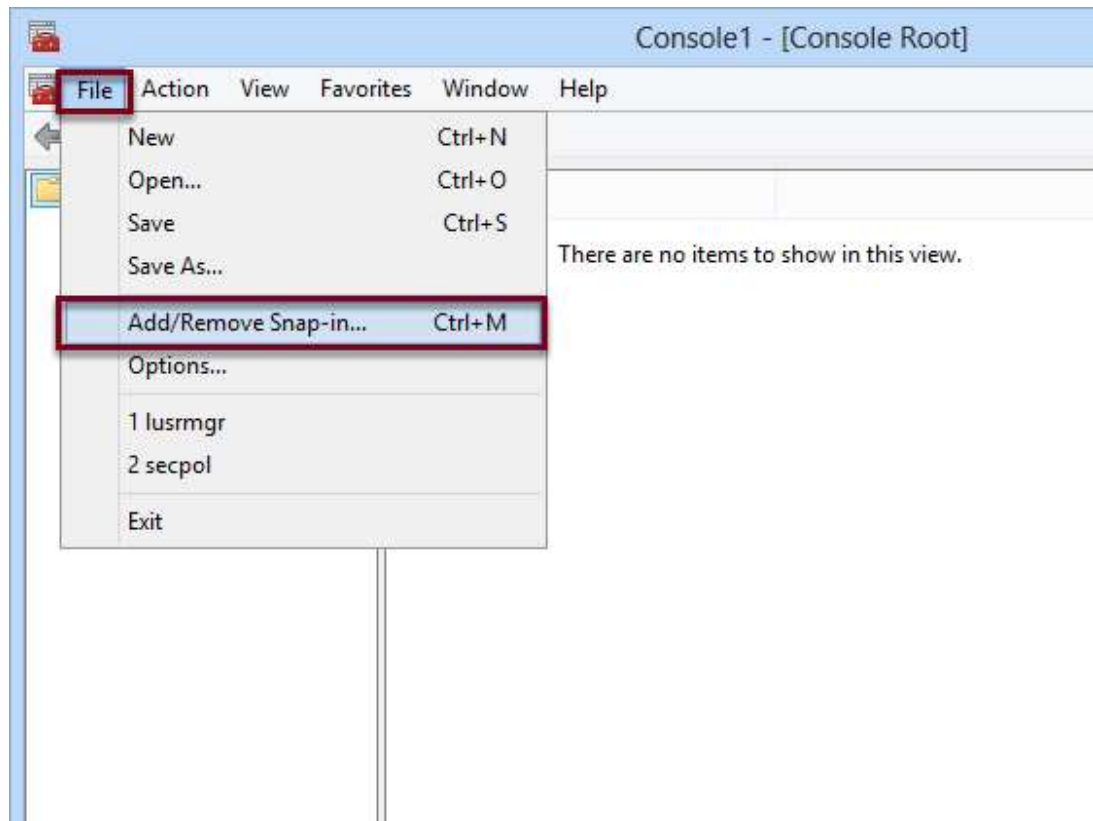
Right click on **Windows SDK 7.1 Command Prompt** and select **Run as administrator**

Generate the Trusted SSL Certificate



1. Enter `cd C:\Program Files\Microsoft SDKs\Windows\v7.1\bin`
 2. Enter `makecert -sv C:\SignRoot.pvk -cy authority -r C:\signroot.cer -a sha1 -n "CN=Dev Certification Authority" -ss my -sr localmachine` to create a trusted certificate only for tests. Refer to "[Makecert.exe \(Certificate Creation Tool\)](#)"
 3. Enter a password
 4. Click **OK**. If necessary retype the password
- This command create a certificate (.cer) and a Private Key (.pvk) in C:\ root folder.

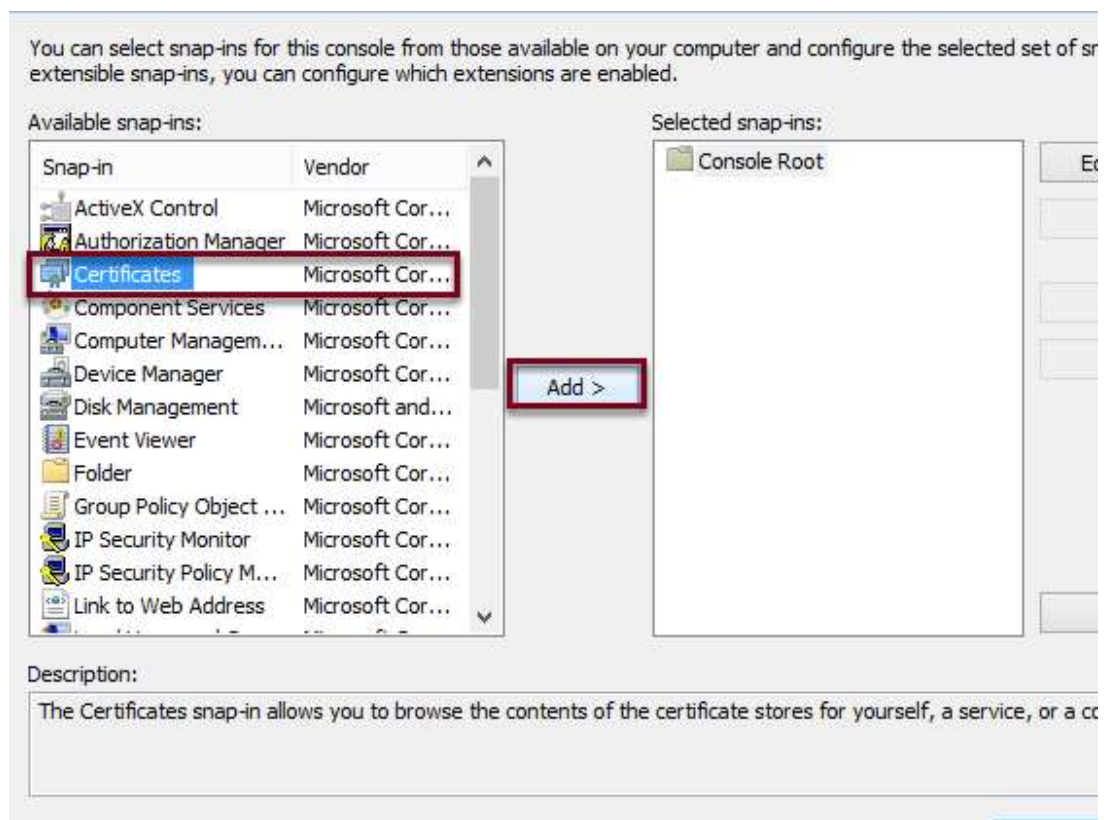
Open the Microsoft Management Console



Execute the command **mmc.exe** then:

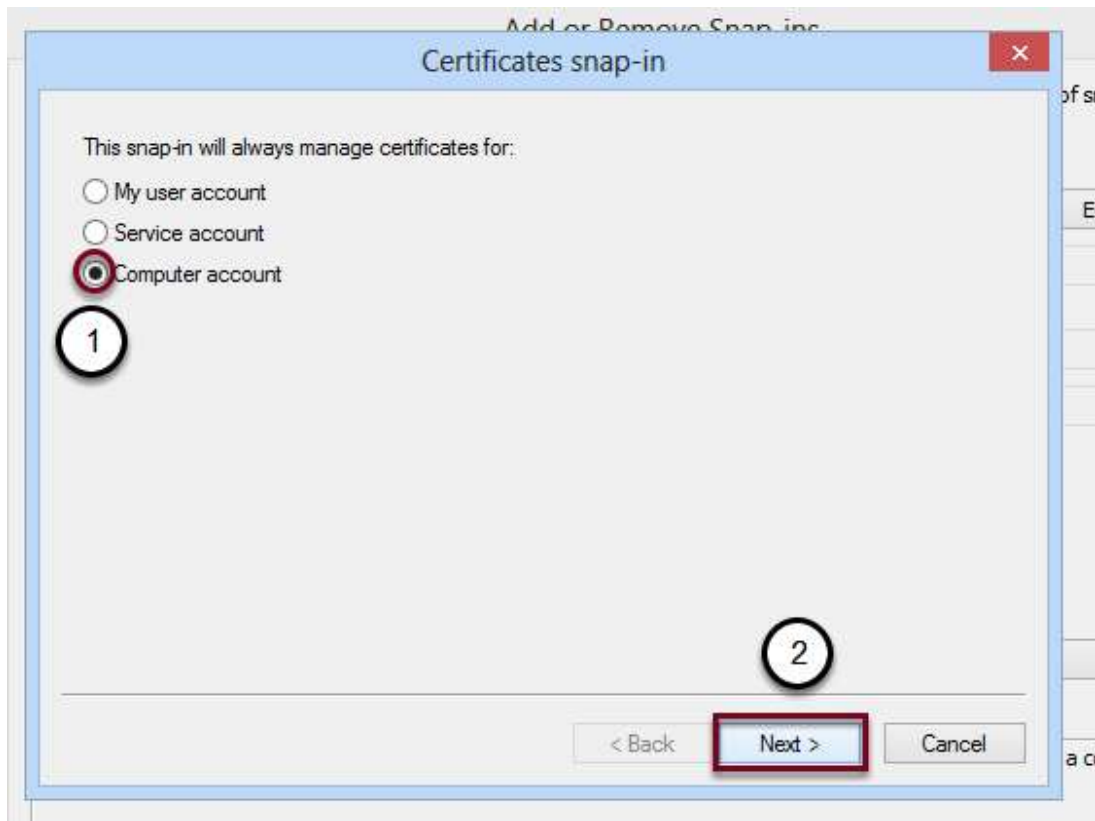
1. Click on **File**
2. Select **Add/Remove Snap-in...**

Add the Certificates to the Console



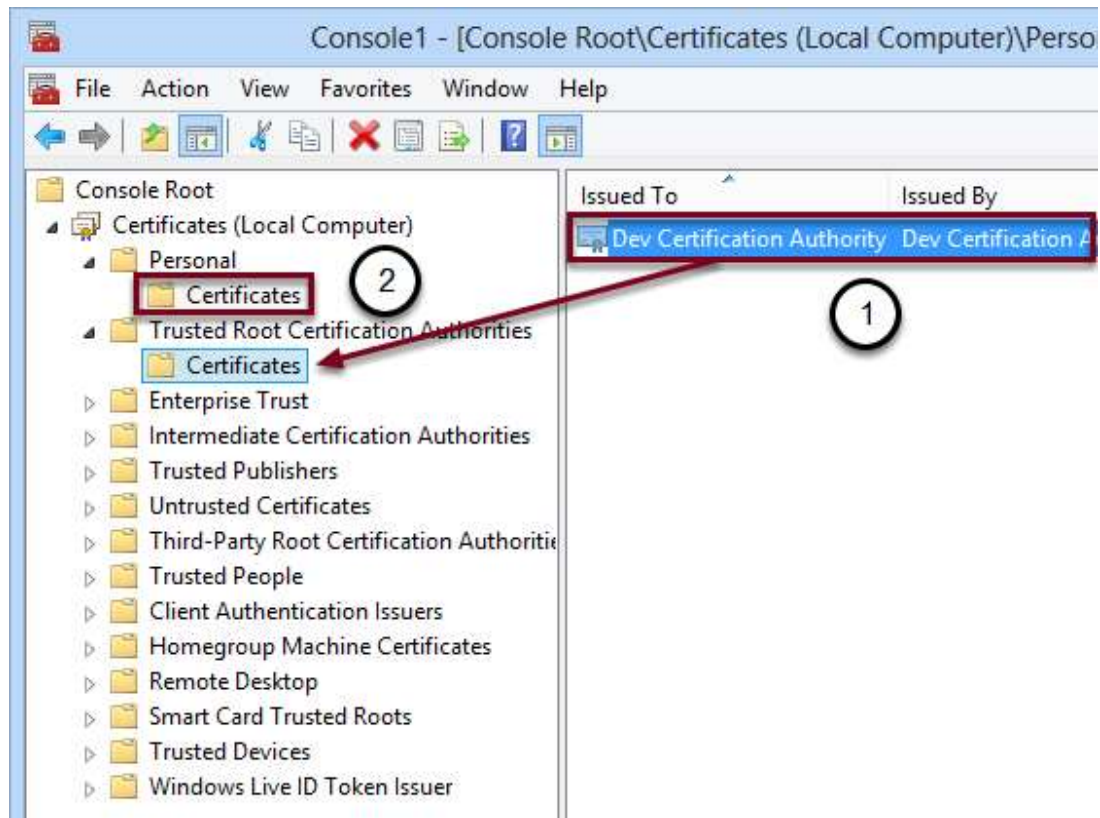
1. Select **Certificates** from the list
2. Click on **Add >** to import the selected element in the console and a new window will appears

Certificate snap-in



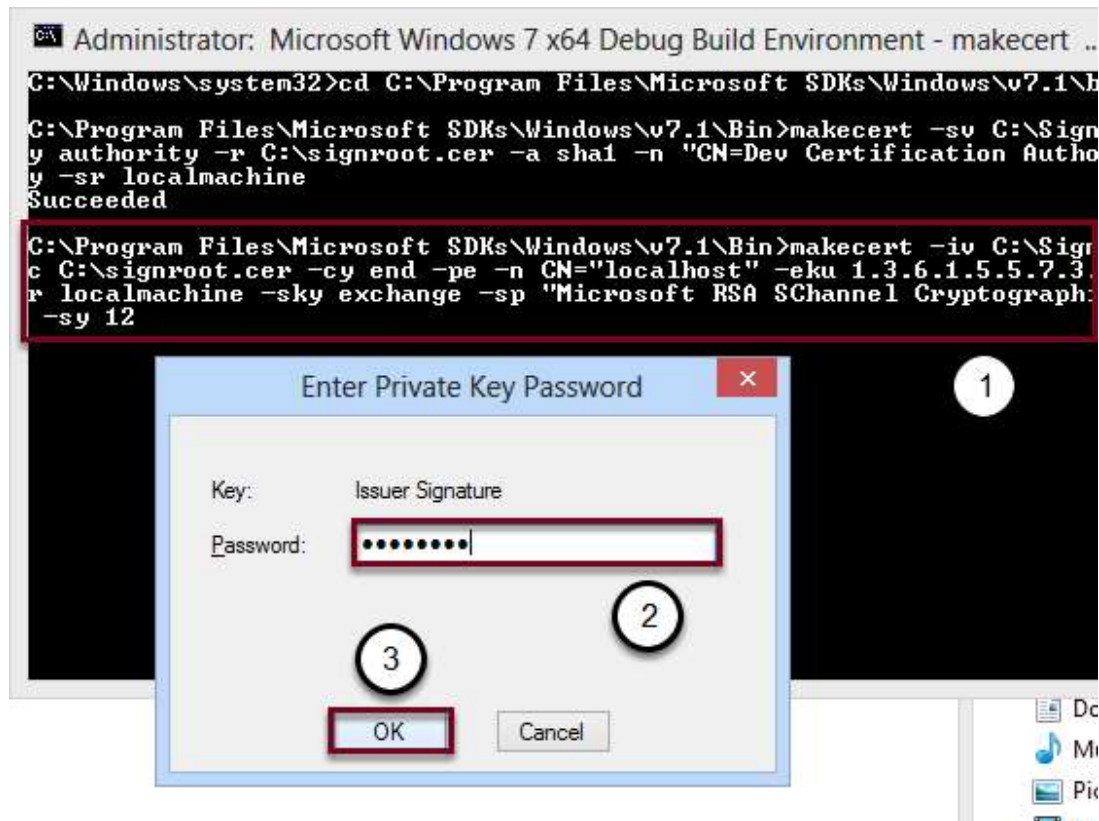
1. Select **Computer account**
2. Click on **Next**
After clicking on Finish, click on OK

Move the Certificate to Trusted Root Certification Authorities



1. Move into Certificates -> Personal -> Certificates
2. Select **Dev Certification Authority** and drag and drop it into **Trusted Root Certification Authorities**

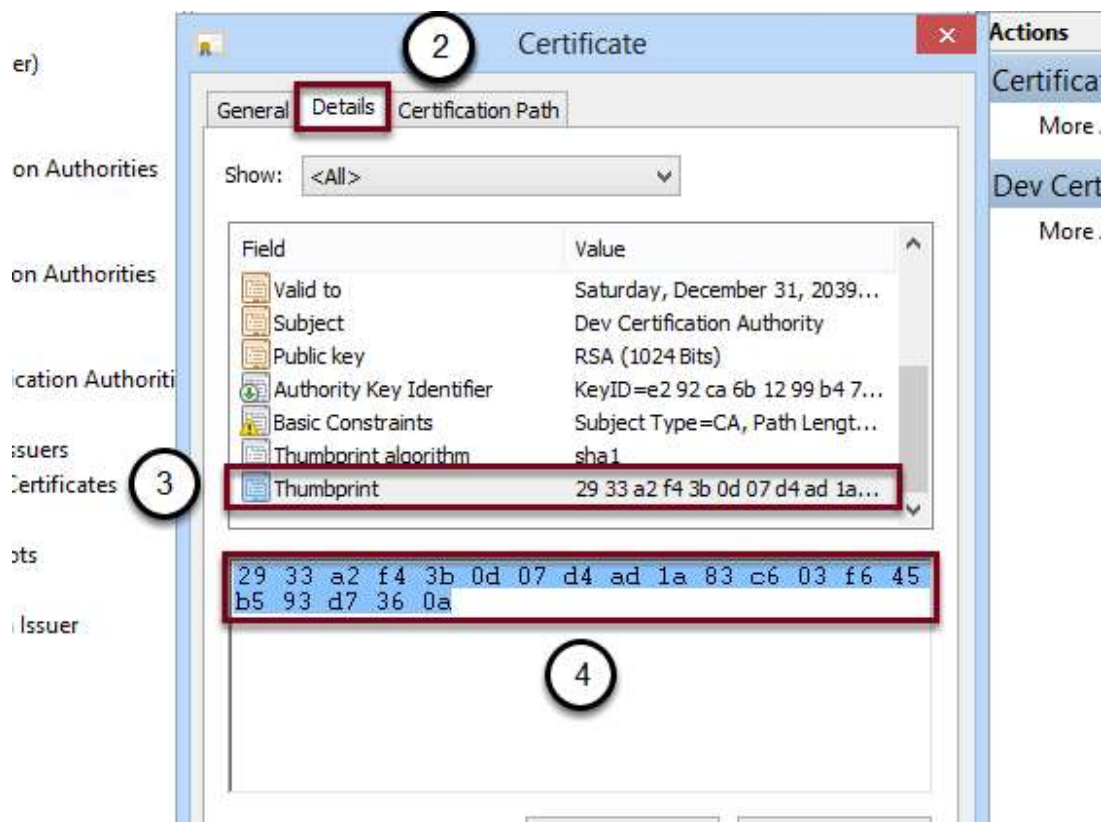
Create a localhost Certificate



After returning to the Command Prompt:

1. Enter **makecert -iv C:\SignRoot.pvk -ic C:\signroot.cer -cy end -pe -n CN="localhost" -eku 1.3.6.1.5.5.7.3.1 -ss my -sr localmachine -sky exchange -sp "Microsoft RSA SChannel Cryptographic Provider" -sy 12**
2. Enter the password created for the first certificate
3. Click **OK**

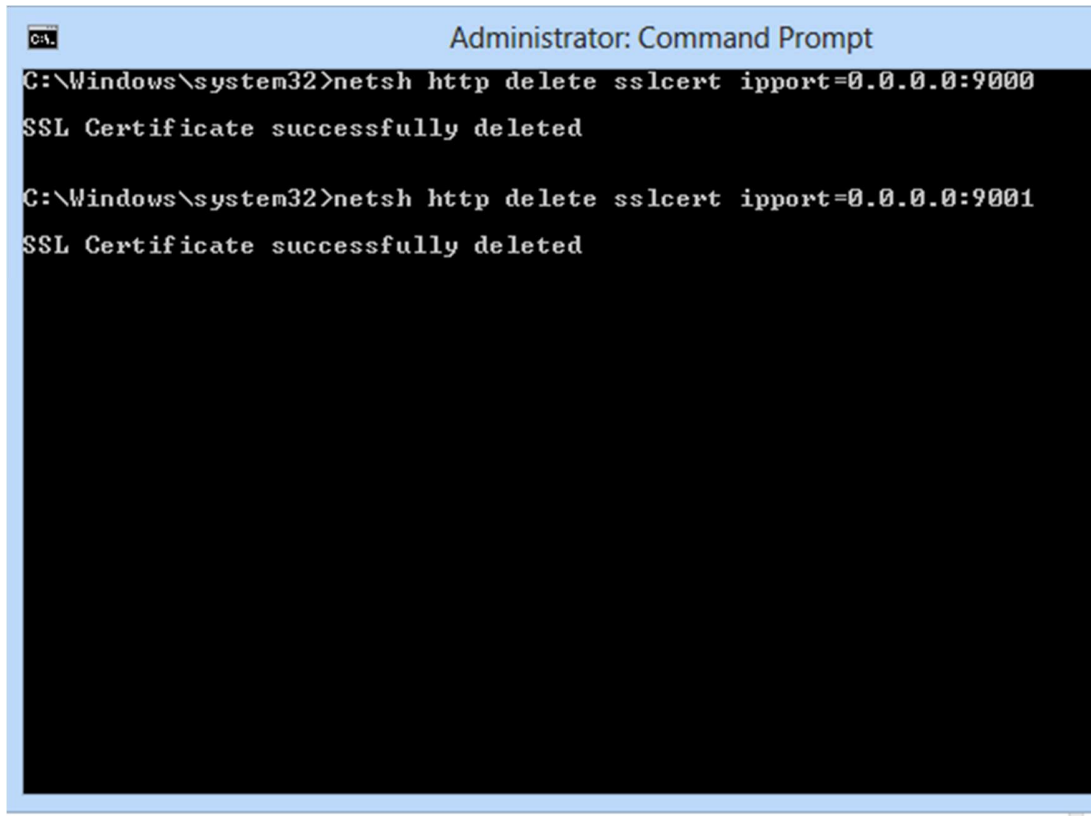
Get the Certificate Thumbprint



If you already have a certificate you can import it:

1. Go to **Certificates -> Personal -> Certificates**
2. Right-click on the empty list and select **All Tasks -> Import...**
After reopening the Microsoft Management Console and clicking F5:
1. Double click on **localhost** or on your certificate into **Certificates -> Personal -> Certificates**
2. Open the **Details** tab
3. Select from the list **Thumbprint**
4. Select the thumbprint and copy it into Notepad and remove the spaces, the number will be different from the screenshot

Remove old SSL Associations



```
Administrator: Command Prompt
C:\Windows\system32>netsh http delete sslcert ipport=0.0.0.0:9000
SSL Certificate successfully deleted

C:\Windows\system32>netsh http delete sslcert ipport=0.0.0.0:9001
SSL Certificate successfully deleted
```

After opening a **Command Prompt** as **Administrator**:

1. Enter **netsh http delete sslcert ipport=0.0.0.0:9000**
2. Enter **netsh http delete sslcert ipport=0.0.0.0:9001**

If you get the error "SSL Certificate deletion failed, Error: 2 The system cannot find the file specified." means that there weren't certificates bound to these ports.

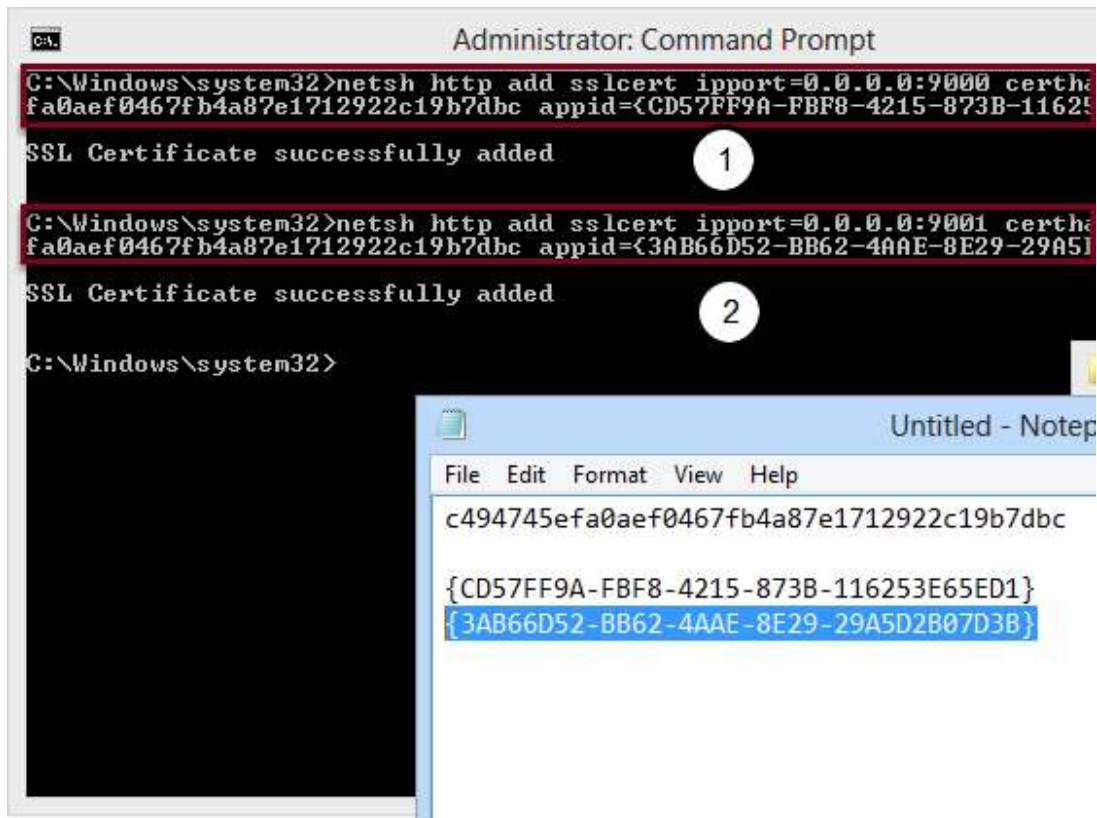
Netsh command works only starting from Windows Vista and Windows Server 2008, if you use an older version refer to "[How to: Configure a Port with an SSL Certificate](#)"

Generate GUIDs

The screenshot shows a web browser window with the address bar containing `www.guidgenerator.com/online-guid-generator.aspx`, marked with a circled '1'. The page title is "Online GUID Generator". Below the title, there is a form with the following elements: a text input field for "How many GUIDs do you want (1-2000):" containing the number '2', marked with a circled '2'; three checkboxes for "Uppcase:", "Braces:", and "Hyphens:", all of which are checked, marked with a circled '3'; and a button labeled "Generate some GUIDs!" marked with a circled '4'. Below the button, the "Results:" section shows two GUIDs: `{CD57FF9A-FBF8-4215-873B-116253E65ED1}` and `{3AB66D52-BB62-4AAE-8E29-29A5D2B07D3B}`, marked with a circled '5'. At the bottom of the results area, there is a disclaimer: "Use these GUIDs at your own risk! GUIDs generated by this site do not".

1. Go to "[Online GUID Generator](http://www.guidgenerator.com/online-guid-generator.aspx)"
2. Enter 2
3. Check all three boxes
4. Click on **Generate some GUIDs!**
5. Select and copy these two GUIDs into your Notepad, the GUIDs will be different from the screenshot.

Binding an SSL Certificate to a URL



After reopening the Command Prompt:

1. Enter **netsh http add sslcert ipport=0.0.0.0:9000 certhash="thumbprint" appid={GUID}** , replace "thumbprint" with your thumbprint and "GUID" with one of your GUIDs previously copied into the notepad without quotes (e.g. **netsh http add sslcert ipport=0.0.0.0:9000 certhash=c494745efa0aef0467fb4a87e1712922c19b7dbc appid={CD57FF9A-FBF8-4215-873B-116253E65ED1}**)
2. Enter **netsh http add sslcert ipport=0.0.0.0:9001 certhash="thumbprint" appid={GUID}** , replace "thumbprint" with your thumbprint and "GUID" with your second GUID (e.g. **netsh http add sslcert ipport=0.0.0.0:9001 certhash=c494745efa0aef0467fb4a87e1712922c19b7dbc appid={3AB66D52-BB62-4AAE-8E29-29A5D2B07D3B}**)

Check the Ports

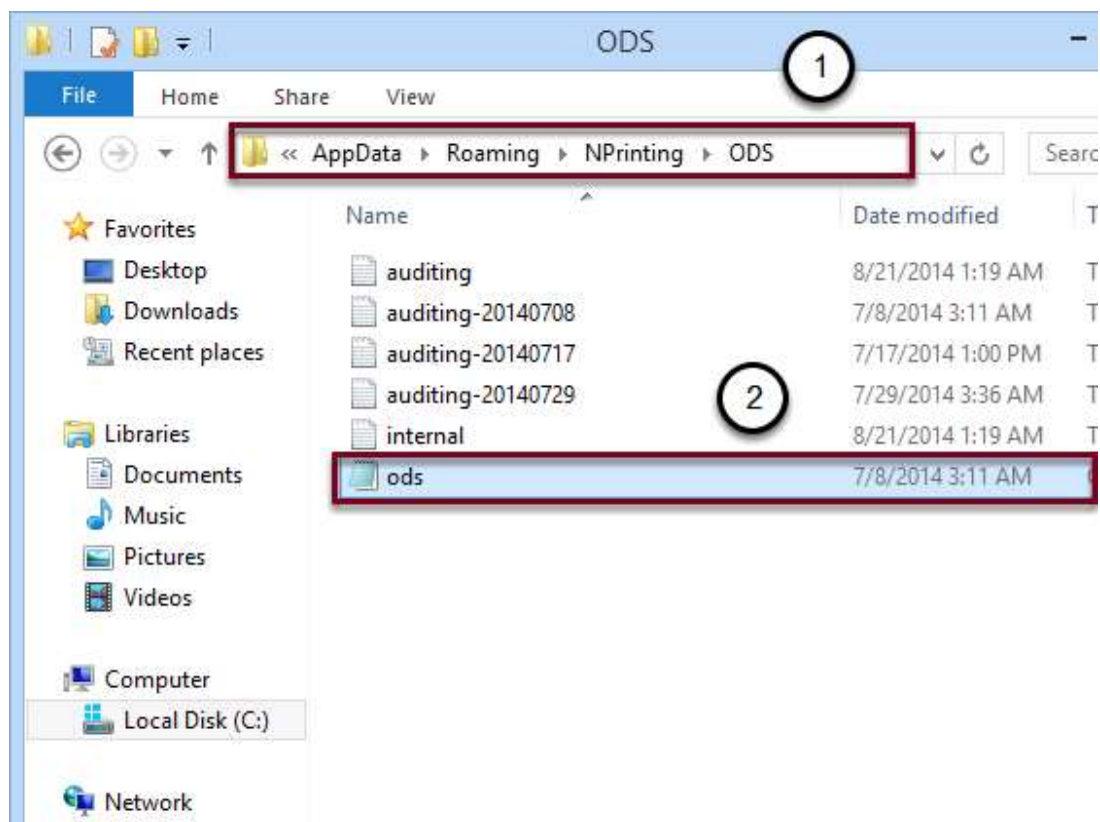
```
Administrator: Command Prompt
C:\Windows\system32>netsh http show sslcert
SSL Certificate bindings:
-----
IP:port                : 0.0.0.0:9000
Certificate Hash        : c494745efa0aef0467fb4a87e1712922c1
Application ID          : {cd57ff9a-fbf8-4215-873b-116253e65
Certificate Store Name  : <null>
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                : 0.0.0.0:9001
Certificate Hash        : c494745efa0aef0467fb4a87e1712922c1
Application ID          : {3ab66d52-bb62-4aae-8e29-29a5d2b07
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
```

Enter **netsh http show sslcert**

Using this command is possible to see all the SSL certificate added. If all step have been performed correctly, you will see the certificates which you added in previous steps.

Configure ods.config



1. Go to C:\Users\{UserName}\AppData\Roaming\NPrinting\ODS (e.g.C:\Users\NPrinting\AppData\Roaming\NPrinting\ODS)
2. Open ods.config with a text editor

Configure On-Demand Service Endpoints


```
ods - Notepad
File Edit Format View Help
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <appSettings>

    <!-- Web services endpoint settings -->

    <add key="WsEnabled" value="true" />
    <add key="WsHostname" value="localhost" />
    <add key="WsPort" value="9000" />
    <add key="WsEnableSSL" value="true" />

    <!-- HTTP endpoint settings -->

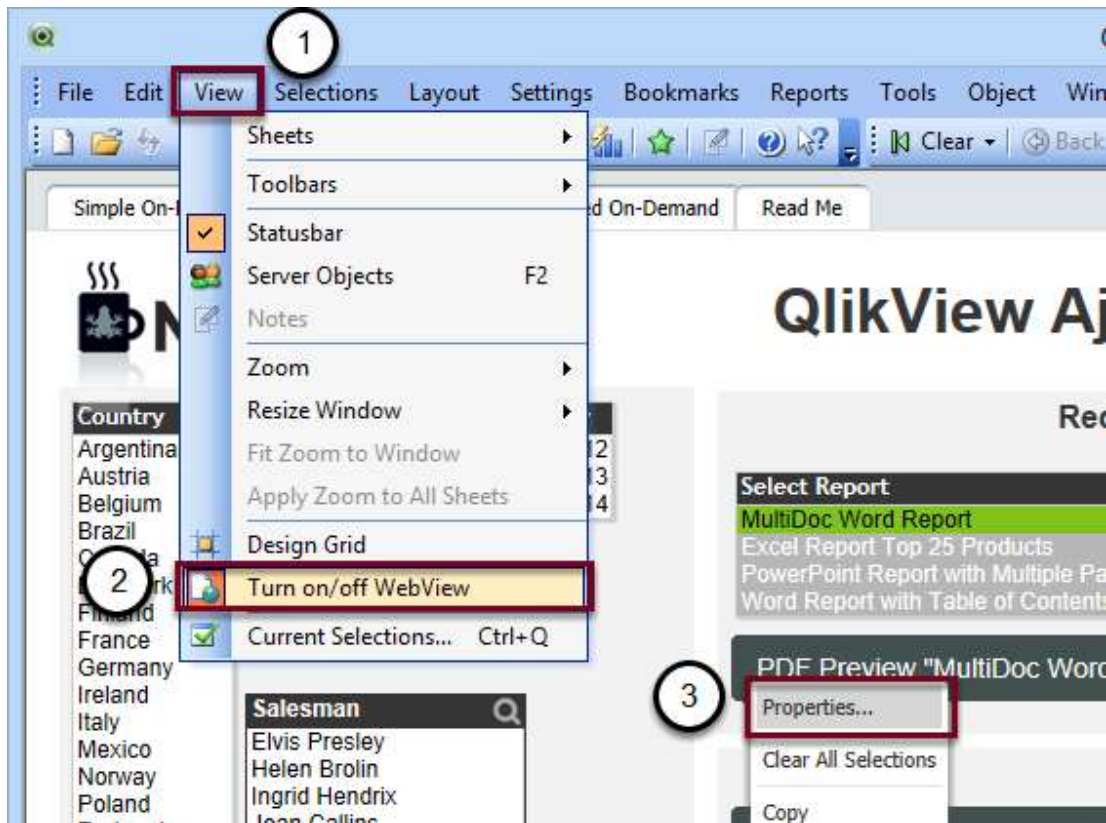
    <add key="HttpEnabled" value="true" />
    <add key="HttpHostname" value="localhost" />
    <add key="HttpPort" value="9001" />
    <add key="HttpEnableSSL" value="true" />

  </appSettings>
</configuration>
```

Diagram annotations: Red boxes highlight the values 'localhost' and 'true' in the configuration. Two numbered circles (1 and 2) with arrows indicate the steps: Circle 1 points to 'localhost' in 'WsHostname' and 'HttpHostname'; Circle 2 points to 'true' in 'WsEnableSSL' and 'HttpEnableSSL'.

- **WsEnabled** and **HttpEnabled** enable or disable the **WS** and **HTTP** endpoints respectively.
 - **WsHostname** and **HttpHostname** are the DNS hostnames of the WS and HTTP interfaces respectively as they appear to clients. If you enable SSL, these names must be the same as indicated in the SSL certificate. (e.g.**localhost**)
 - **WsPort** and **HttpPort** are the TCP ports used for the WS and HTTP interfaces respectively. If both endpoints are enabled these ports must be different.
 - **WsEnableSSL** and **HttpEnableSSL** enable or disable the SSL protocol in the respective interface.
1. Enter **localhost** in the WsHostname and HttpHostname value field
 2. Type **true** in the WsEnableSSL and HttpEnableSSL value field
 3. Save and Close

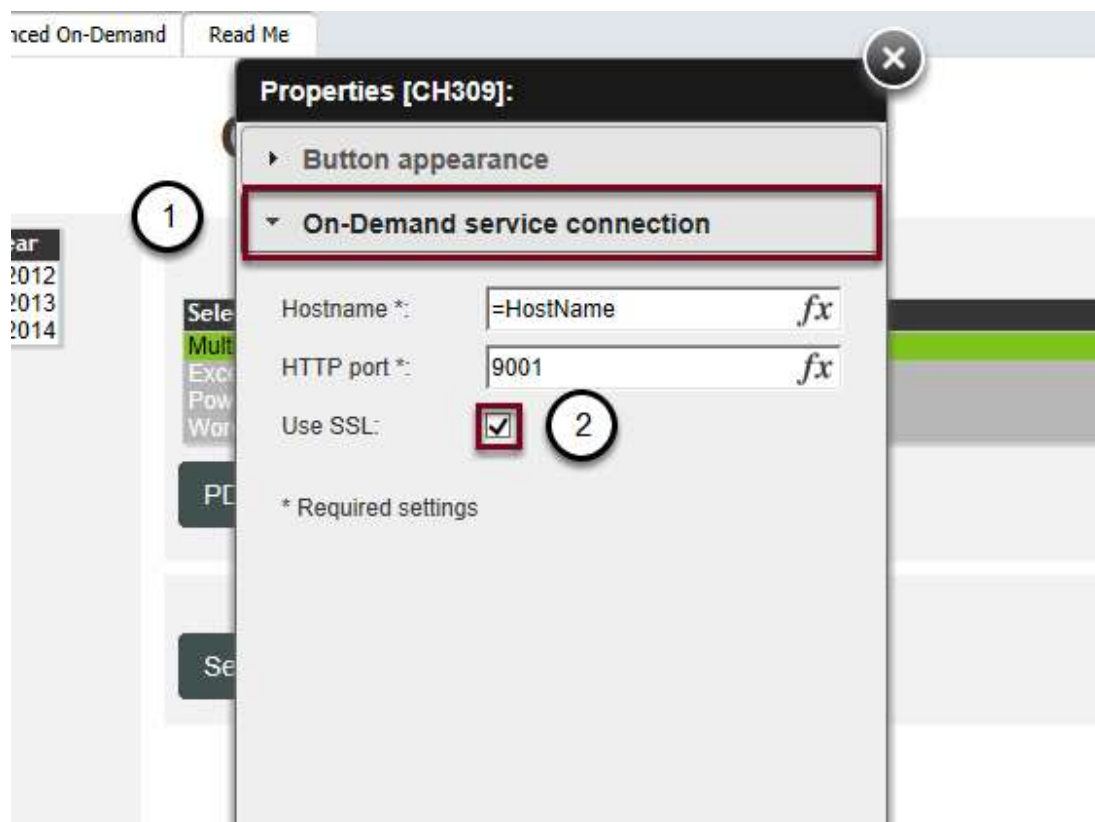
Edit the On-Demand Components



If you want to use SSL you must enable SSL on ON-Demand Components

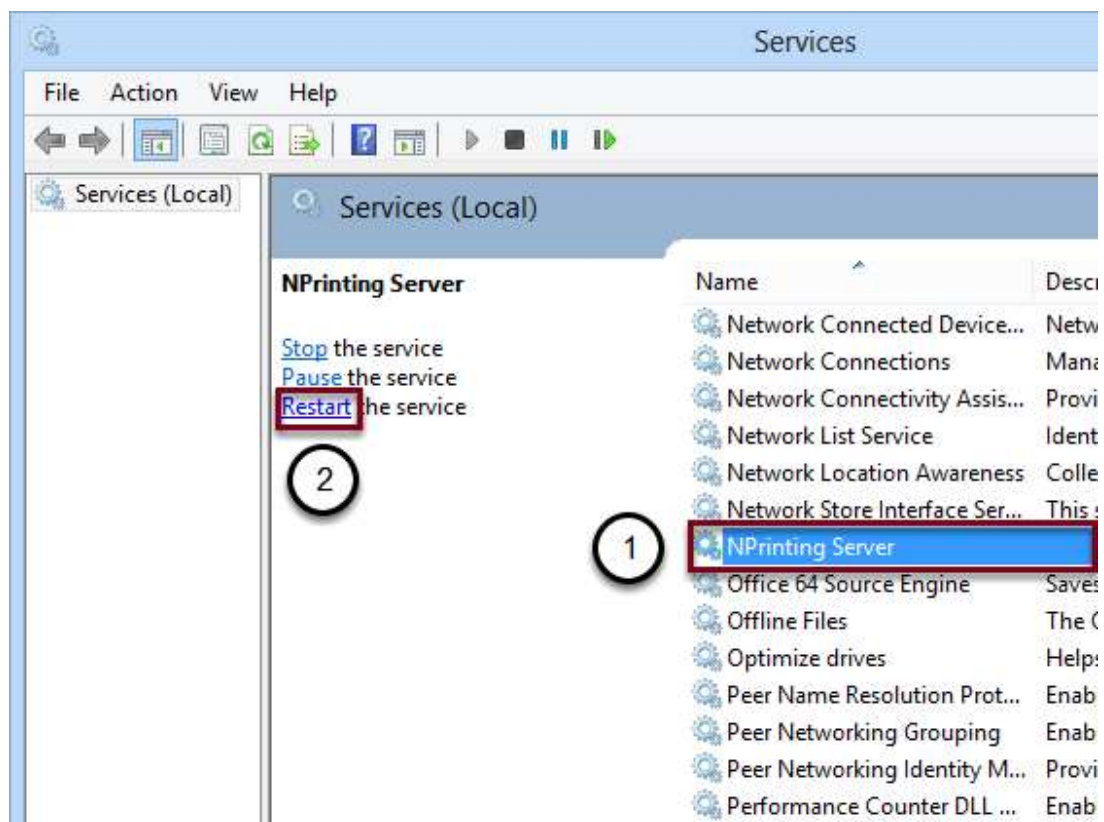
1. Click on **View**
2. Select **Turn on/off WebView**
3. Right-click on each button and click on **Properties**

Enable SSL on On-Demand Components



1. Select **On-Demand service connection**
2. Check **Use SSL**

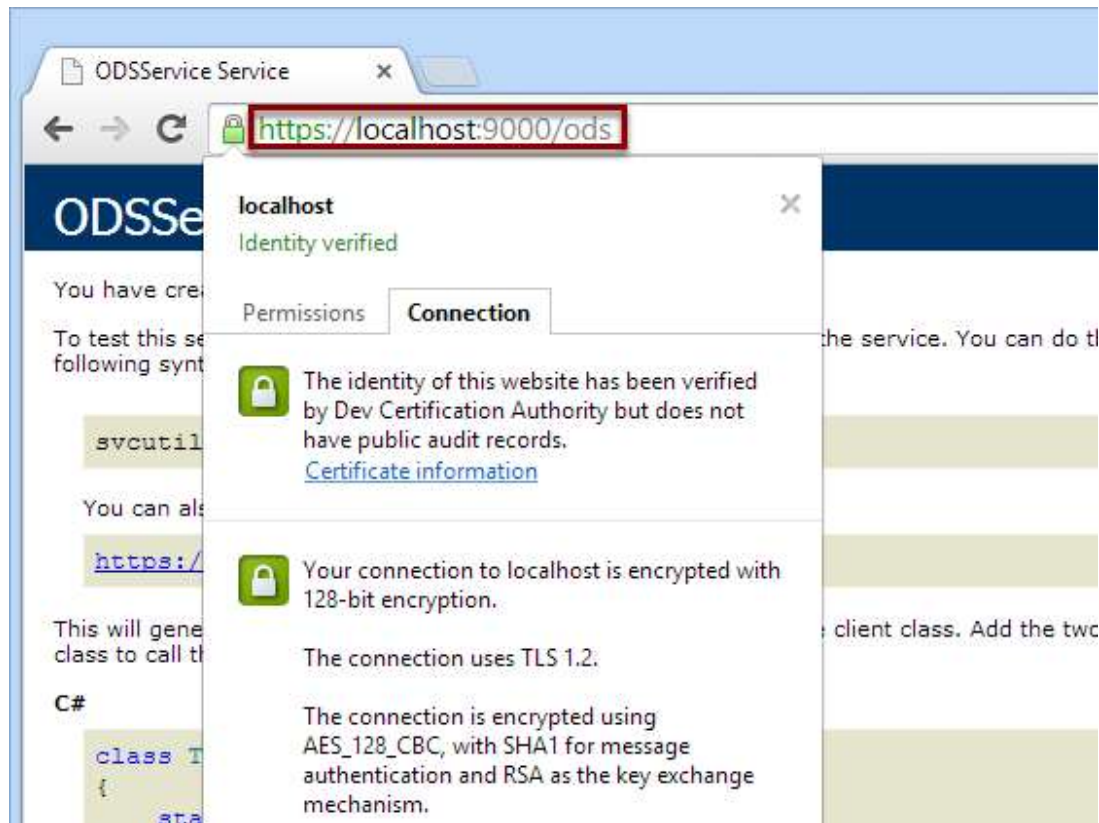
Restart the NPrinting Server Service



After opening the **Services** manager:

1. Select **NPrinting Server** service from the list
2. Click on **Restart**

Result



If you go to <https://localhost:9000/ods>, you can see the a green padlock and that the certificate has been accepted.