

## Steps to create a SHA 256 certificate

### Prerequisites:

This procedure assumes that you have a certificate authority configured on your domain server. This procedure uses a Windows certificate authority. Note that this information is provided as an aid to create a certificate request and sign the certificate using a local certificate authority. Avaya does not recommend to use a local certificate authority to sign the server certificates.

These steps have to be performed on the certificate authority server to enable SHA-2. If your Certificate authority is already SHA-2 enabled you can skip these steps.

1) Just check what hash algorithm is currently used, execute this below given command

```
certutil -getreg ca\csp\CNGHashAlgorithm
```

if this returns SHA256, skip to step 5.

2) By default the above should return SHA1. Run this below given command to configure the CA to use SHA256 for CNG hashes.

```
certutil -setreg ca\csp\CNGHashAlgorithm SHA256
```

3) Restart Certificate Services:

```
net stop CertSvc && net start CertSvc
```

If your root ca is not SHA-2 enabled you will need to migrate your server. See this blog

<http://arthurremy.com/index.php/107-tutorials/308-migrate-microsoft-certification-authority-to-sha-2-algorithm>

You should see following output

```

Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.SANCCMS1>certutil -getreg ca\csp\CNGHashAlgorithm
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ccms-SANCCMS1-CA\csp:
    CNGHashAlgorithm REG_SZ = SHA1
CertUtil: -getreg command completed successfully.

C:\Users\Administrator.SANCCMS1>certutil -setreg ca\csp\CNGHashAlgorithm SHA256
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ccms-SANCCMS1-CA\csp:
Old Value:
    CNGHashAlgorithm REG_SZ = SHA1
New Value:
    CNGHashAlgorithm REG_SZ = SHA256
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.

C:\Users\Administrator.SANCCMS1>certutil -getreg ca\csp\CNGHashAlgorithm
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\ccms-SANCCMS1-CA\csp:
    CNGHashAlgorithm REG_SZ = SHA256
CertUtil: -getreg command completed successfully.

C:\Users\Administrator.SANCCMS1>net stop CertSvc && net start CertSvc
The Active Directory Certificate Services service is stopping.
The Active Directory Certificate Services service was stopped successfully.
The Active Directory Certificate Services service is starting.
The Active Directory Certificate Services service was started successfully.

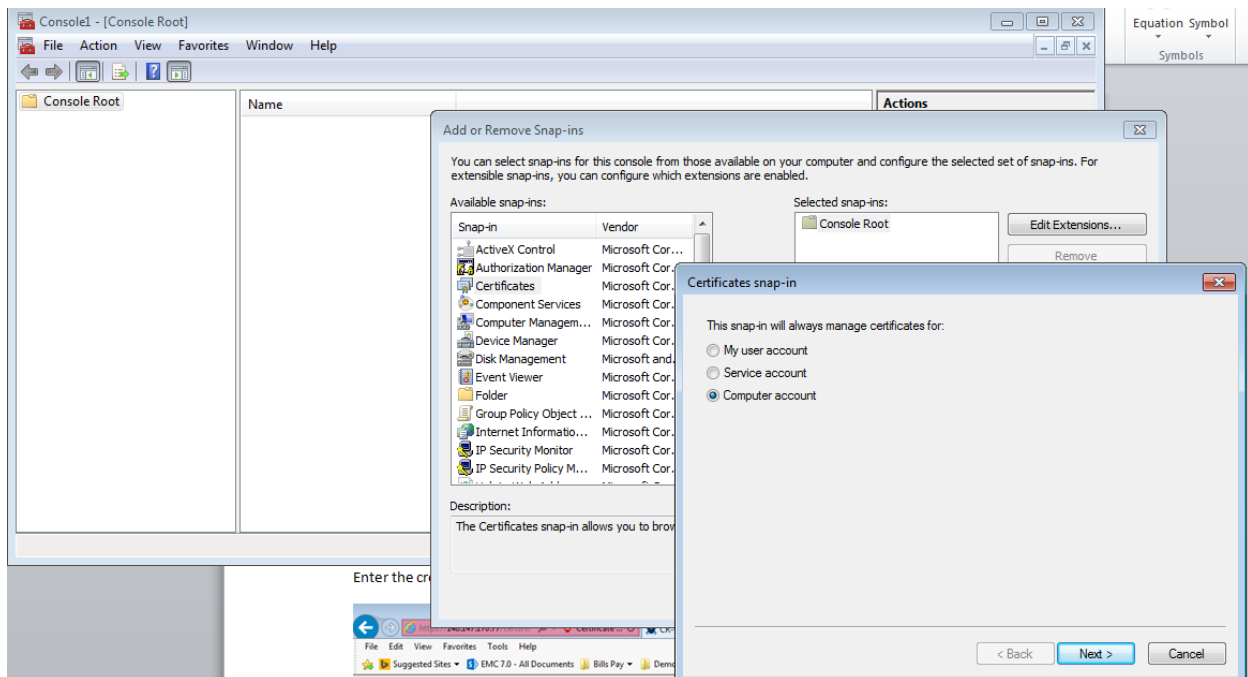
C:\Users\Administrator.SANCCMS1>_

```

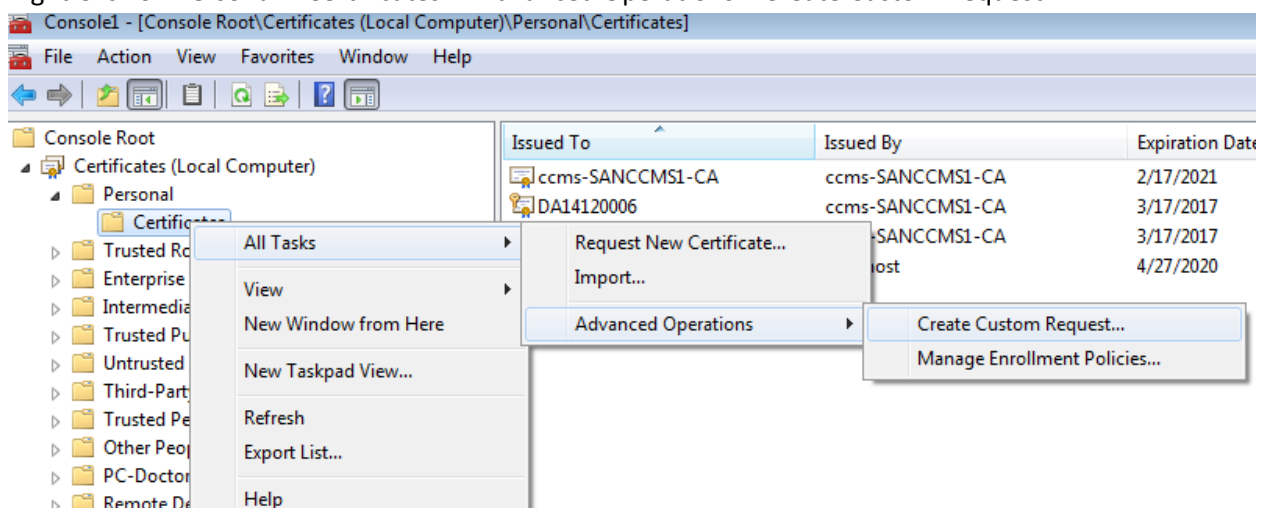
4. Execute step 1 and check SHA256 is set as the default hash algorithm

## Steps to create a Certificate Signing Request

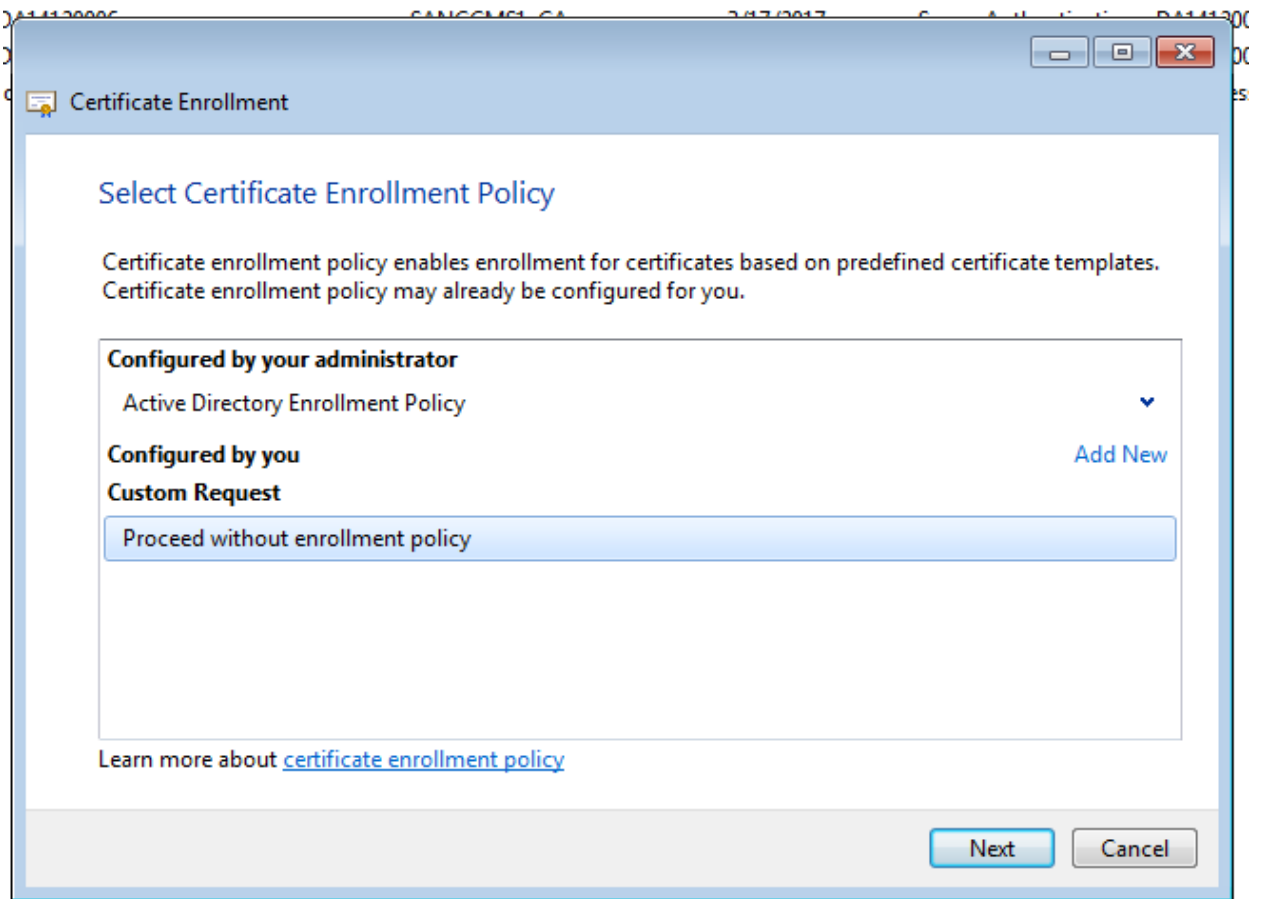
1. On the EMC SQL Server database machine Server certificate needs to be installed. Open MMC and add certificates snap-in. We need to create a certificate signing request for the same  
Note: The certificate request must be made from the same machine where the certificate needs to be installed.



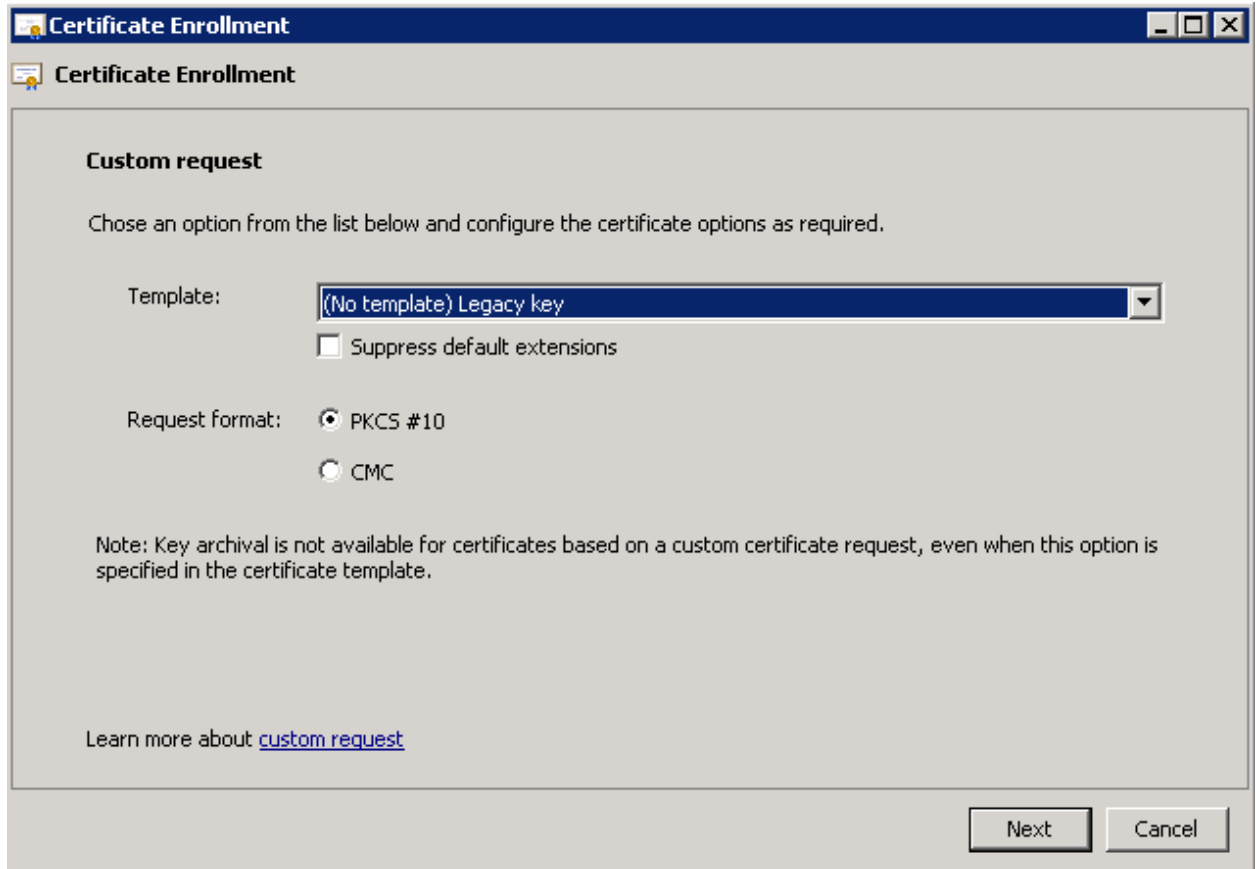
2. Right Click on Personal > Certificates -> Advanced Operations > Create Custom Request



3. Select proceed without enrollment policy



Select Legacy Key

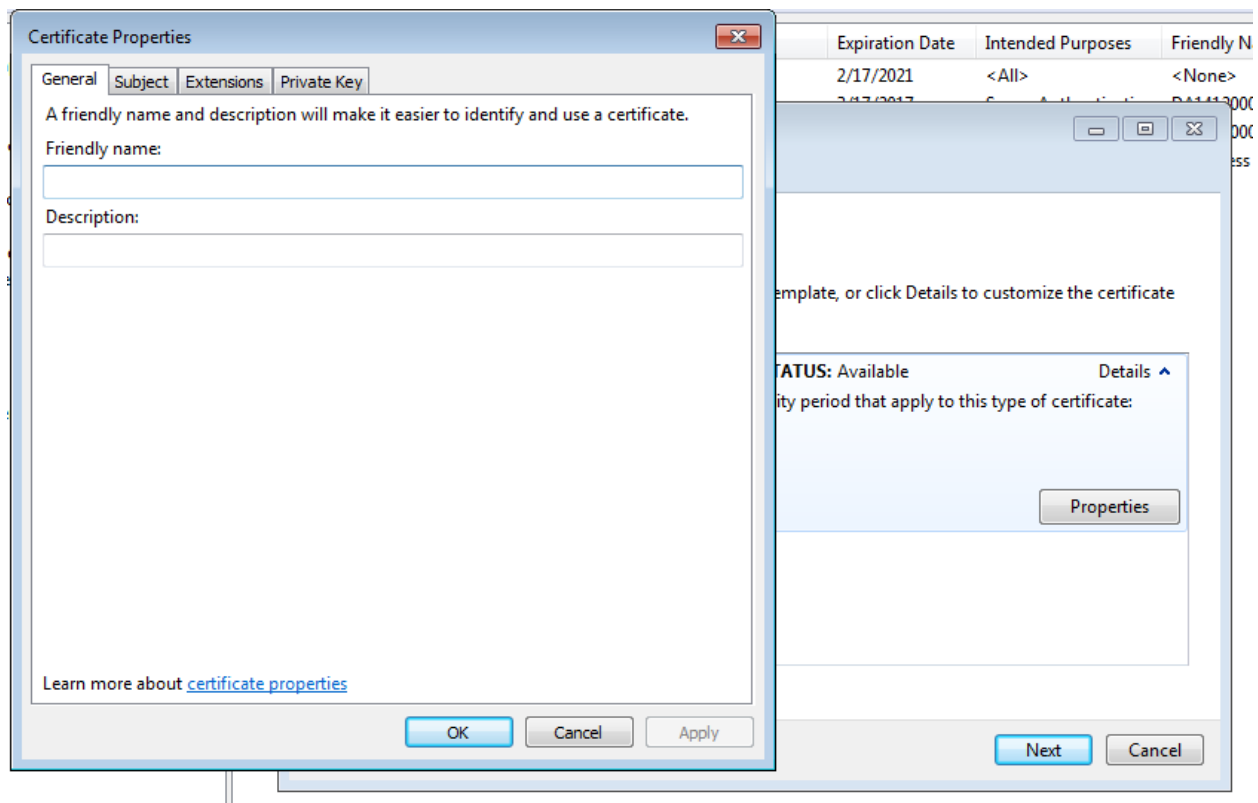


The image shows a Windows-style dialog box titled "Certificate Enrollment". It has a standard title bar with minimize, maximize, and close buttons. Below the title bar, there is a subtitle "Certificate Enrollment" with a small icon. The main content area is titled "Custom request" and contains the following elements:

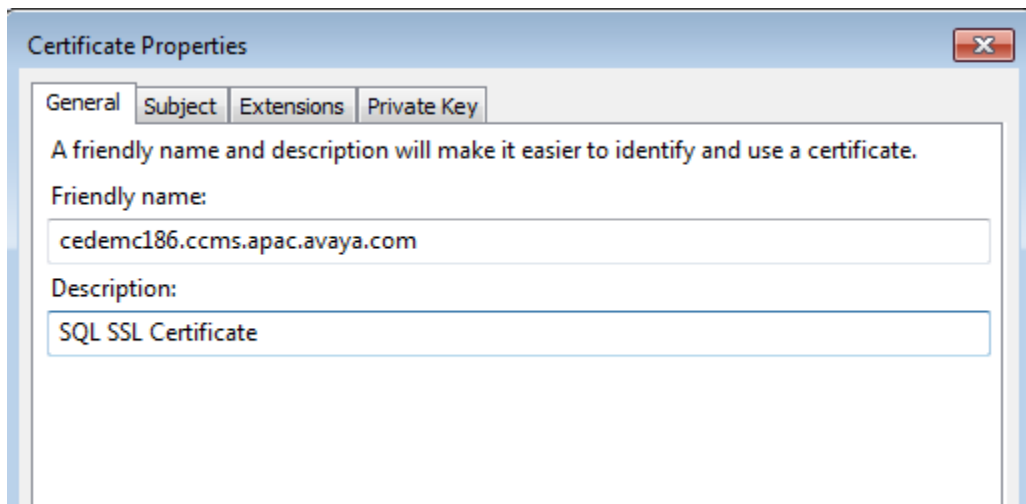
- A text label "Chose an option from the list below and configure the certificate options as required." (Note the typo "Chose").
- A "Template:" label followed by a dropdown menu showing "(No template) Legacy key".
- A checkbox labeled "Suppress default extensions" which is currently unchecked.
- A "Request format:" label followed by two radio buttons: "PKCS #10" (which is selected) and "CMC".
- A note: "Note: Key archival is not available for certificates based on a custom certificate request, even when this option is specified in the certificate template."
- A link: "Learn more about [custom request](#)".

At the bottom right of the dialog, there are two buttons: "Next" and "Cancel".

4. Go to Details -> Properties on Next Page



Type name of the certificate. This will be used to select the certificate



Enter the CN field and optionally the Alternate names, if using SQL aliases. All the aliases must be entered in Subject Alternate names

Certificate Properties

General Subject Extensions Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate  
The user or computer that is receiving the certificate

Subject name:

Type:  
Common name

Add >

< Remove

Value:  
CN=cedemc186.ccms.apac.ava

Alternative name:

Type:  
DNS

Add >

< Remove

Value:  
cedemc186

Learn more about [subject name](#)

OK Cancel Apply

Certificate Properties

General Subject Extensions Private Key

The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.

Subject of certificate  
The user or computer that is receiving the certificate

Subject name:

Type:  
Common name

Add >

Value:

< Remove

CN=cedemc186.ccms.apac.avaya.com

Alternative name:

Type:  
DNS

Add >

Value:

< Remove

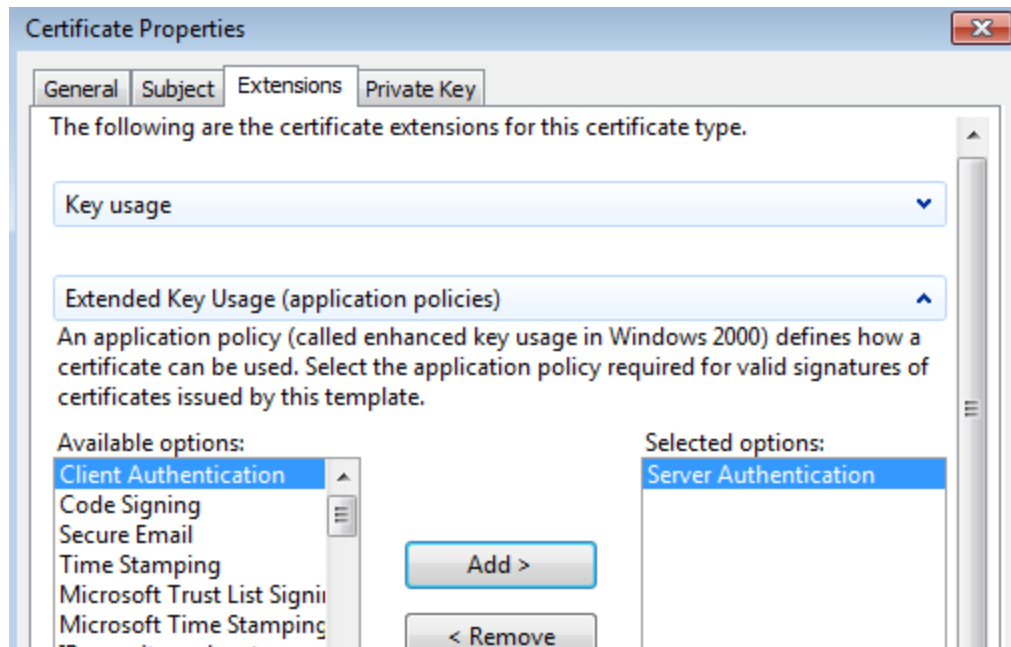
DNS  
cedemc186  
cedemc186.ccms.apac.avaya.com  
148.147.174.186

Learn more about [subject name](#)

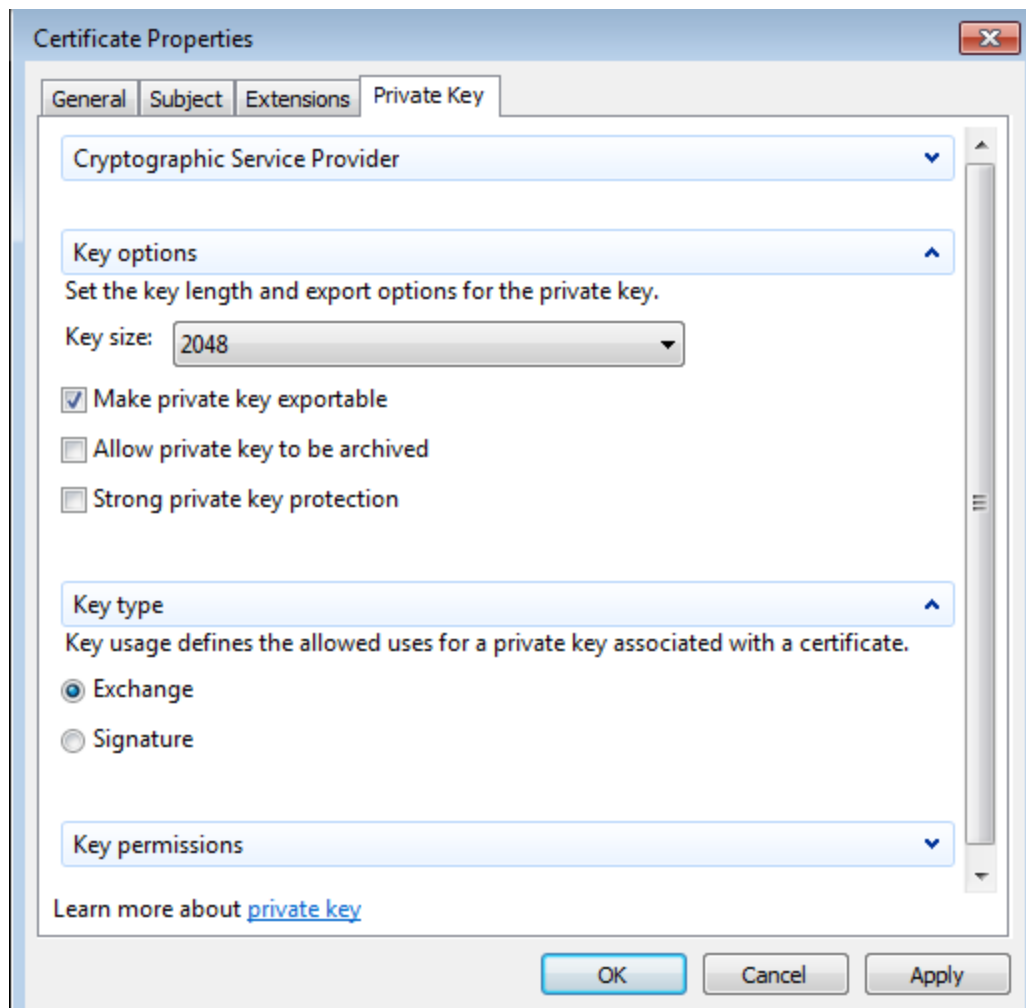
OK Cancel Apply

Select server authentication as Extended Key Usage





Select Key type Exchange and key length as 2048



Select a file location to create the certificate request

Certificate Enrollment

### Where do you want to save the offline request?

If you want to save a copy of your certificate request or want to process the request later, save the request to your hard disk or removable media. Enter the location and name of your certificate request, and then click Finish.

File Name:

File format:  
☒ Base 64  
☐ Binary

Learn more about [file format](#)

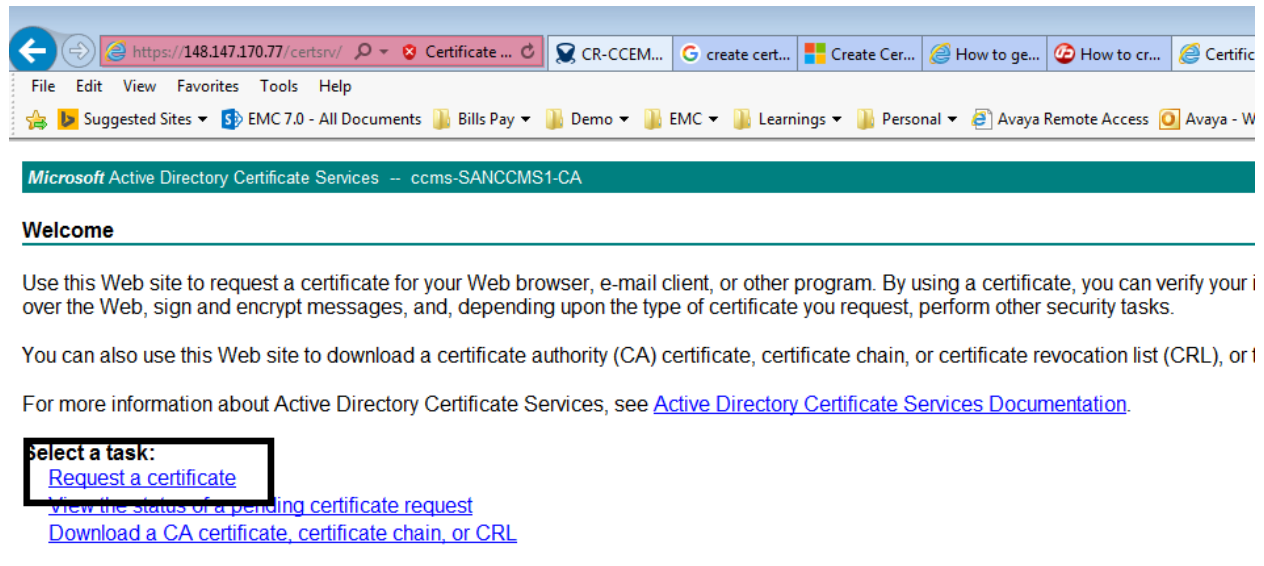
## Steps to sign the certificate

The certificate request needs to be signed by a certificate authority. Here Microsoft CA is used

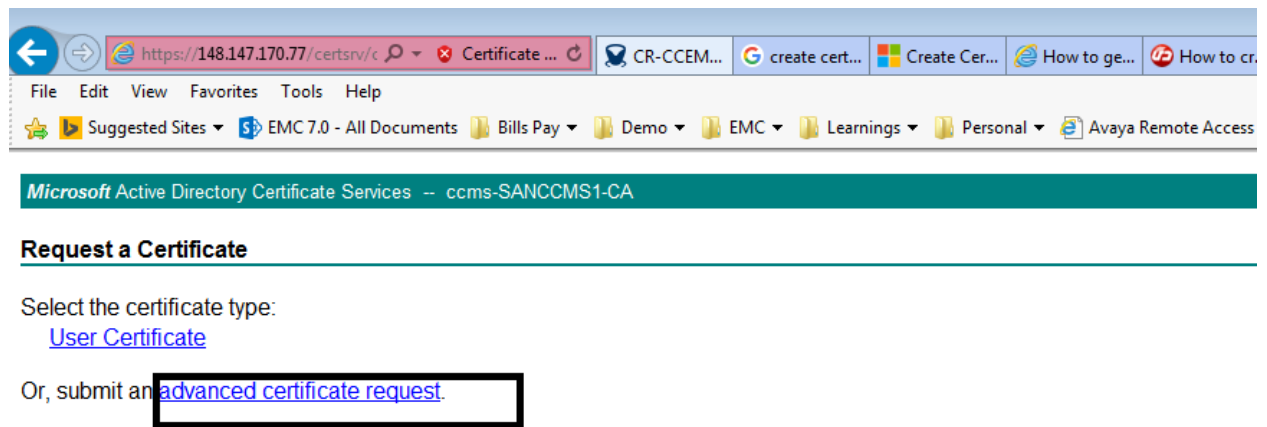
Go to the webbrowser and type the certificate server URL

<https://<certauthority>/certsrv/>.

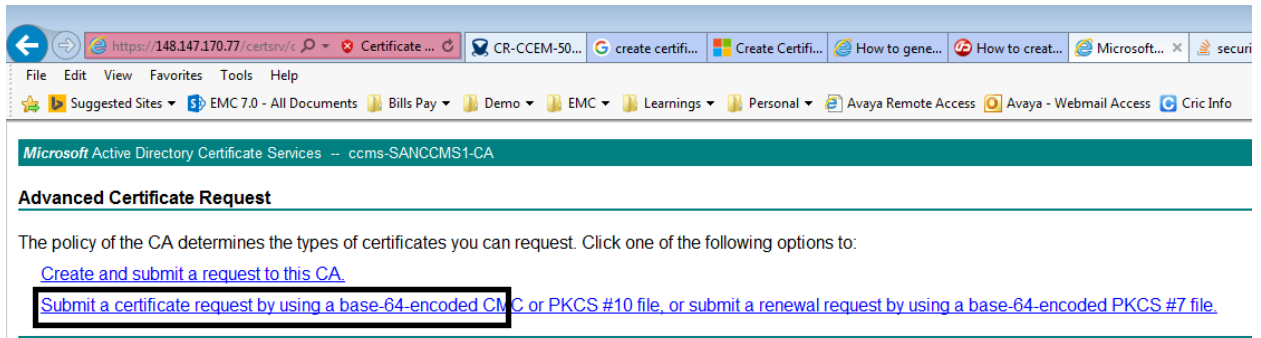
Enter the credentials as appropriate and select Request a certificate



6. Click on Advanced certificate request



7. Click on the second link as given below.



14) Go back to the browser, paste your copied encoded values in to the Base-64-encoded certificate request as given below. Open the certificate request file in notepad editor and copy all the contents into the Saved Request field shown below.

```

1 -----BEGIN CERTIFICATE REQUEST-----
2 MIIC0jCCAbOCAQAwDELMAkGA1UEBhMCSU4xDDAKBgNVBAgMA01BSDENMAzGA1UE
3 BwwEUHVuZTEUMBIGA1UECgwLQXZheWEgSW5kaWExDDAKBgNVBAsMA0dDUzEkMCIG
4 A1UEAwwbREExNDEyMDAwNi5nbG9iYWwvYXZheWEuY29tMIIIBIjANBgkqhkiG9w0B
5 AQEFAAOCAQ8AMIIBCgKCAQEAWnGIYazc8ojQVSpHjMvRbdwWdIUqMBgeitDWa9ym
6 6LC4kYix7ENDFp1d45EYybWfF3qY6dOiEWjs5oMqed6mqsz9eY6FoZgennar660Y
7 nAP1onXQIFBseMNq7MCS6wGTZwLwIX0Ly6fzzuc6yeNBAUgj12ZDGv/20tXm03f/
8 f4u7Kc6gXZNiaxajEkZeDwQgMc378apB3gQ6X83ndteDOJWc7mKK+bATcqPoeYwz
9 Ty10LaGc/sj57AX8N/a4LPYIQD9MVQICCH+PgBEiBB7ufCCQypN7GKCY1+utHfNm
10 FchRGPfyapjSdyo67ByElxW/0in/TxLrUaAfEma6rM9CwwIDAQABOikwFwYJKoZI
11 hvCNAQkHMqMCEf2YXlhMTIzMA0GCSqGSIb3DQEBCwUAA4IBAQCbydqFAGNdieRc
12 z+GY9RtyaZeCYi3S8//MjKhM9qtusdHbnRhGLCyZB2Lo8NSkqxPU/06IJL7E9Ns1
13 LYvQHfQQIo6roHxCculwZiTitZHNvUFOMw95ddXXIG4Sfs0Xh/rdxRD5/Lb9pq6Wr
14 MtCh9SSlt1/EA+QbwoB92fFtE4YpWFG001y1KkD4uNDP60ejhOSddSYzDtdBQXhh
15 yqZPx68xEIS0UC/68BoJQjPxxJAGPeQkX9e0ygIcP4lrqk6IaBCFJKzXXCYfwZAa
16 +2IeQeE+jnIn9dhmitWJJ6px9nhfALFrF/VHrtZiHZrs/HPw15S11HU+ifLsWmOI
17 CmcTYvRt
18 -----END CERTIFICATE REQUEST-----
19

```

15: Select the **proper Certificate template**. The certificate template should have “Server authentication” as extended key usage which is an important criteria to load the certificate

← → https://148.147.170.77/certsrv/c Certificate ... CR-CCEM-508 CCEM... How to generate a S... How to c

File Edit View Favorites Tools Help

★ Suggested Sites ▼ EMC 7.0 - All Documents Bills Pay ▼ Demo ▼ EMC ▼ Learnings ▼ Personal ▼ Avaya I

---

**Microsoft Active Directory Certificate Services -- ccms-SANCCMS1-CA**

---

**Submit a Certificate Request or Renewal Request**

---

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #10 Web server) in the Saved Request box.

**Saved Request:**

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
MtCh9SSLt1/EA+QbwoB92fFtE4YpWFG001y1KkD4
yqZPx68xEIS0UC/68BoJQjPxxJAGPeQkX9e0ygIc
+2IeQeE+jnTn9dhmitWJJ6px9nhfALFrF/VHrtZi
CmcTYvRt
-----END CERTIFICATE REQUEST-----
```

**Certificate Template:**

SM certs ▼

**Additional Attributes:**

Attributes: < >

Submit >

16. Click on submit button

### Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #10 Web server) in the Saved Request box.

#### Saved Request:

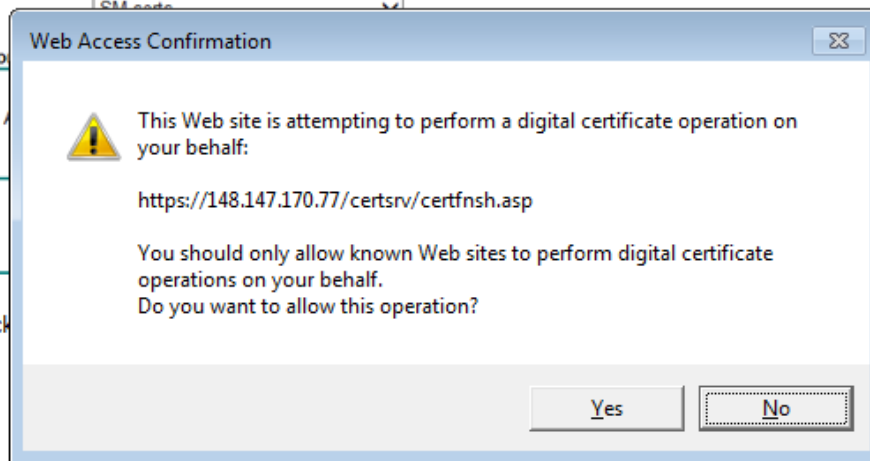
Base-64-encoded  
certificate request  
(CMC or  
PKCS #10 or  
PKCS #7):

```
MtCh9SSLt1/EA+QbwoB92fFtE4YpWFG001y1KkD4  
yqZPx68xEIS0UC/68BoJQjPxxJAGPeQkX9e0ygIc  
+2IeQeE+jnTn9dhmitWJJ6px9nhfALFrF/VHrtZi  
CmcTYvRt  
-----END CERTIFICATE REQUEST-----
```

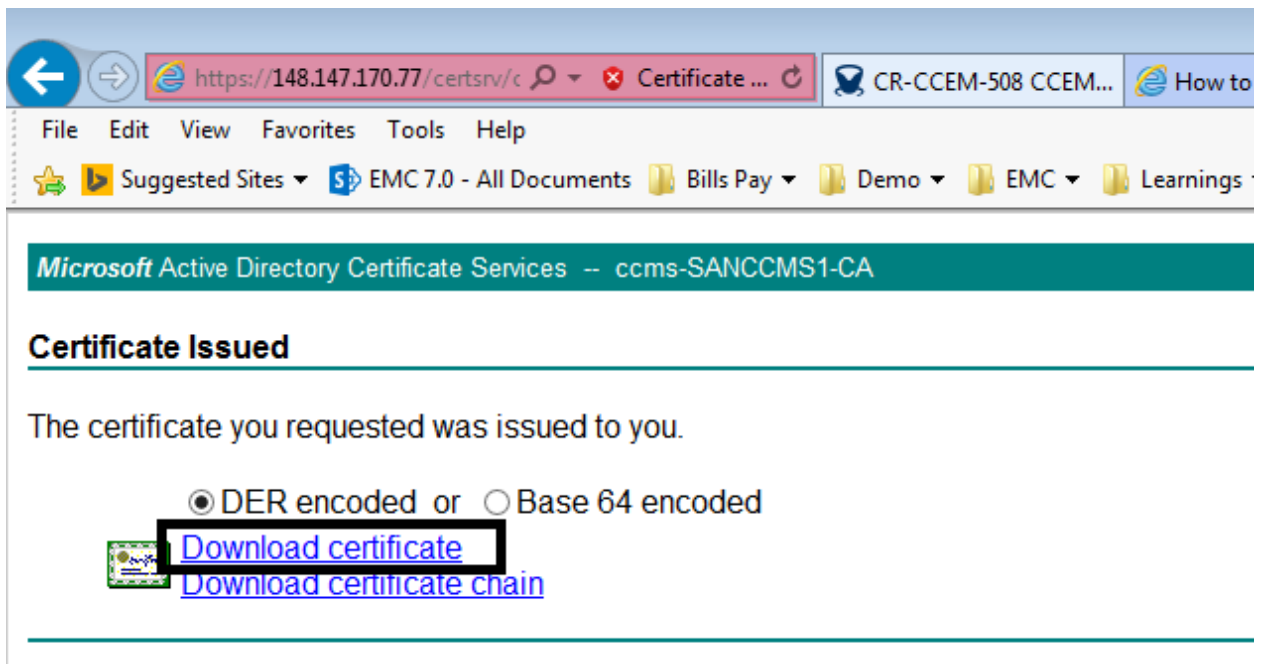
#### Certificate Template:

Additio

16. Click



17. Click on Yes and download the certificate


A screenshot of a web browser window. The address bar shows "https://148.147.170.77/certsrv/c". The browser has a menu bar (File, Edit, View, Favorites, Tools, Help) and a toolbar with "Suggested Sites" and several document icons. The page content has a teal header "Microsoft Active Directory Certificate Services -- ccms-SANCCMS1-CA". Below it is a section "Certificate Issued" with the text "The certificate you requested was issued to you." and two radio buttons: "DER encoded" (selected) and "Base 64 encoded". At the bottom are two links: "Download certificate" and "Download certificate chain".

Microsoft Active Directory Certificate Services -- ccms-SANCCMS1-CA

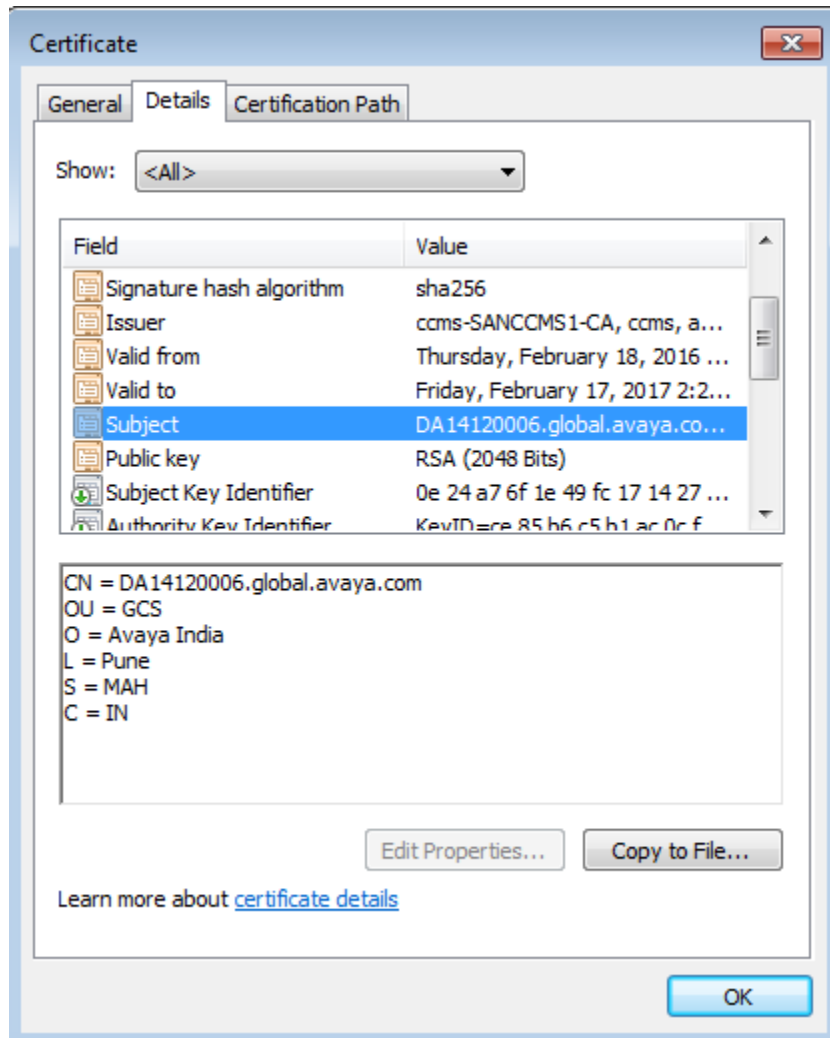
### Certificate Issued

The certificate you requested was issued to you.

☒ DER encoded or ☐ Base 64 encoded

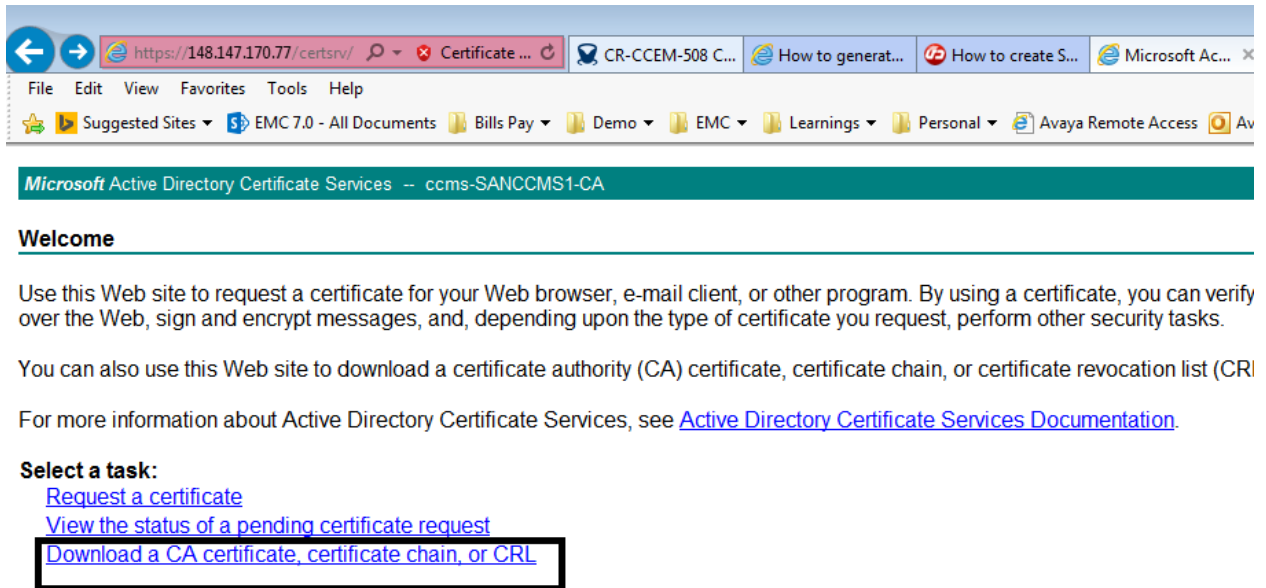
 [Download certificate](#)  
[Download certificate chain](#)

18. Save the certificate and ensure that the certificate is a SHA2-Certificate

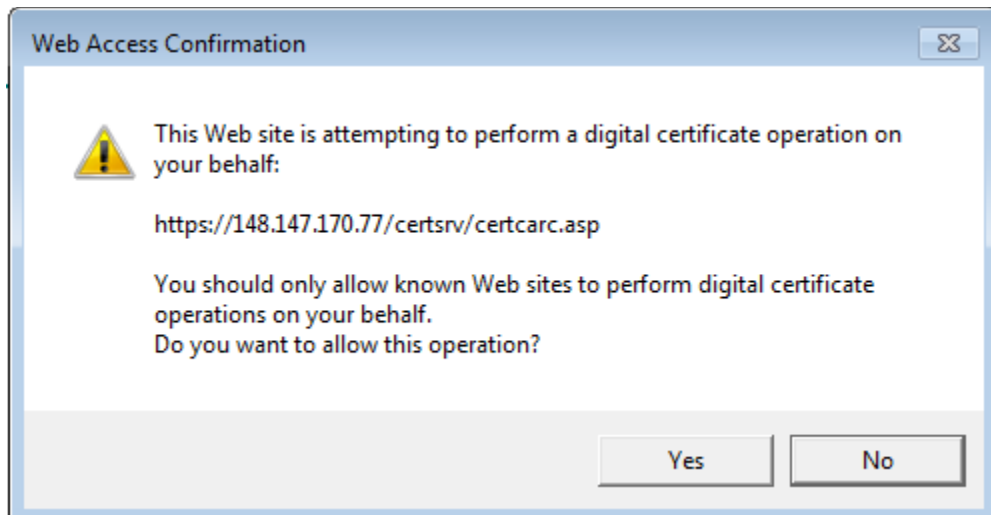


Also download the root –ca certificate from the certificate authority . This will be used later.





Select Yes



Download the CA certificate

← → https://148.147.170.77/certsrv/c Certificate ... CR-CCEM-508 C... How to generat... How to create S...

File Edit View Favorites Tools Help

Suggested Sites EMC 7.0 - All Documents Bills Pay Demo EMC Learnings Personal Avaya R

Microsoft Active Directory Certificate Services -- ccms-SANCCMS1-CA

### Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

**CA certificate:**

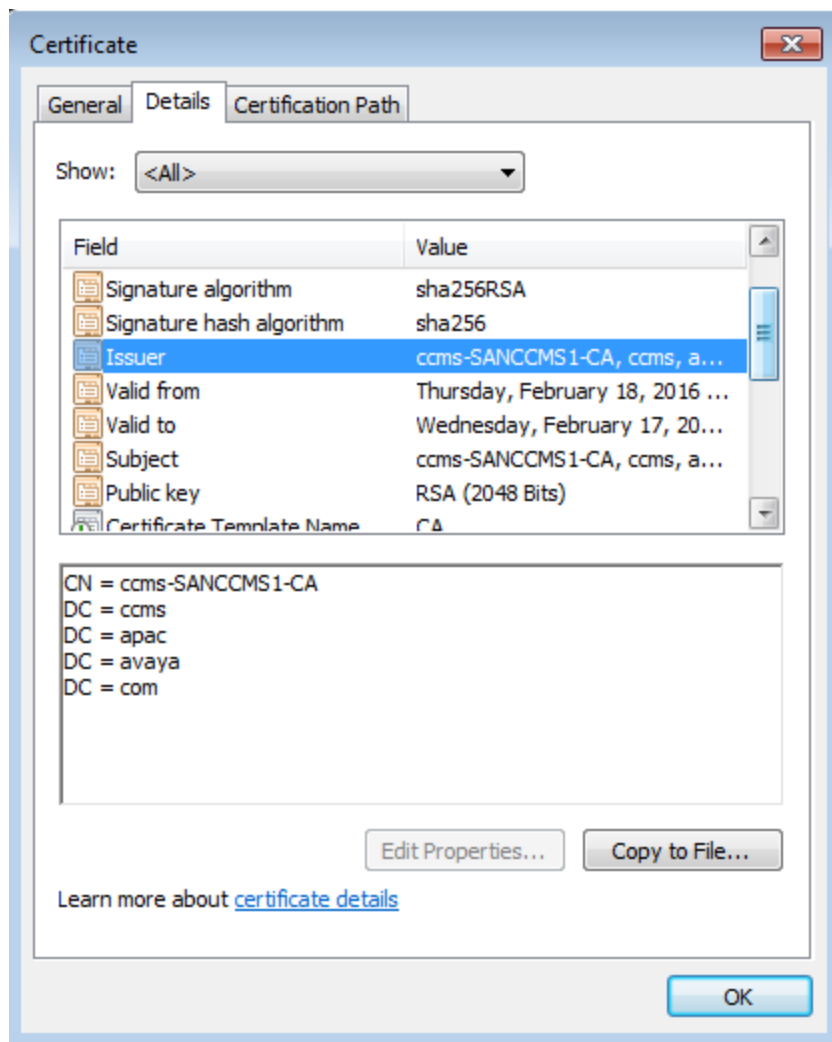
Current [ccms-SANCCMS1-CA]

**Encoding method:**

☒ DER  
☐ Base 64

[Download CA certificate](#)  
[Download CA certificate chain](#)  
[Download latest base CRL](#)  
[Download latest delta CRL](#)

Verify the CA certificate is SHA-256



# Installation of server certificate on SQL Server

Prerequisites for server certificate (Copied from [https://technet.microsoft.com/en-us/library/ms189067\(v=sql.105\).aspx](https://technet.microsoft.com/en-us/library/ms189067(v=sql.105).aspx))

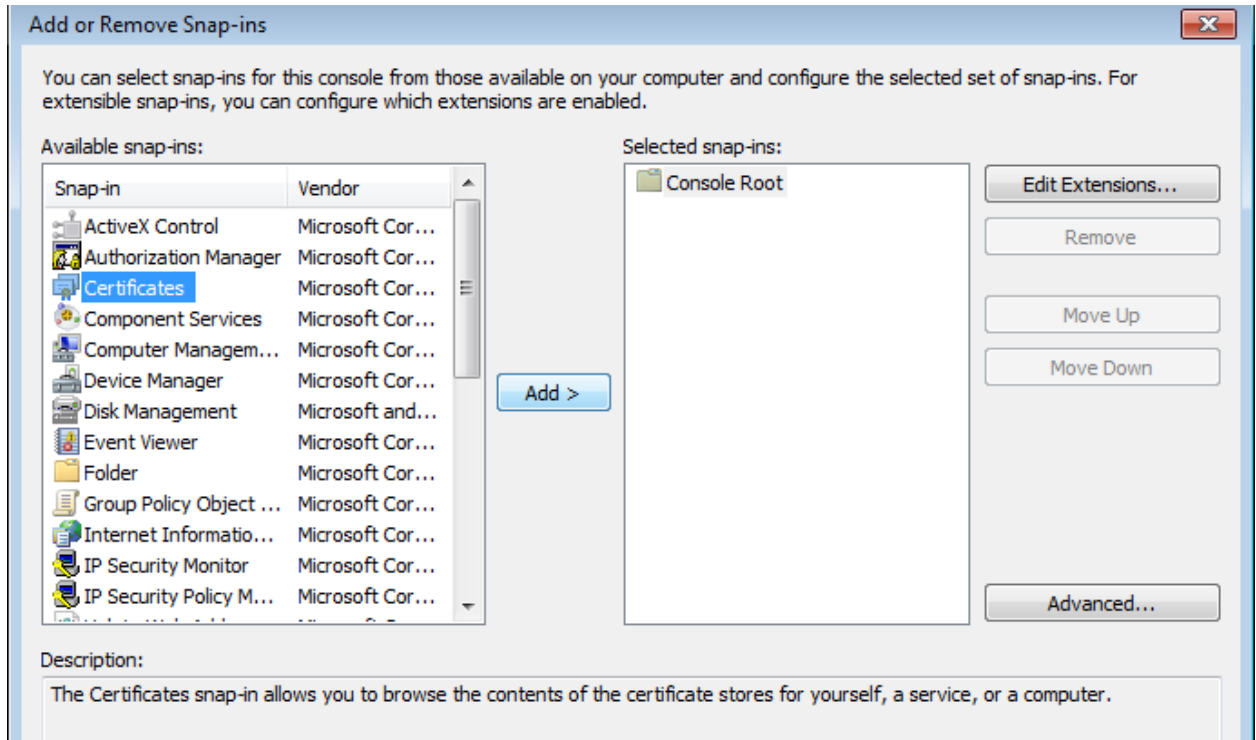
---

For SQL Server to load a SSL certificate, the certificate must meet the following conditions:

- The certificate must be in either the local computer certificate store or the current user certificate store.
- The current system time must be after the **Valid from** property of the certificate and before the **Valid to** property of the certificate.
- The certificate must be meant for server authentication. This requires the **Enhanced Key Usage** property of the certificate to specify **Server Authentication (1.3.6.1.5.5.7.3.1)**.
- The certificate must be created by using the **KeySpec** option of **AT\_KEYEXCHANGE**. Usually, the certificate's key usage property (**KEY\_USAGE**) will also include key encipherment (**CERT\_KEY\_ENCIIPHERMENT\_KEY\_USAGE**).
- The **Subject** property of the certificate must indicate that the common name (CN) is the same as the host name or fully qualified domain name (FQDN) of the server computer. If SQL Server is running on a failover cluster, the common name must match the host name or FQDN of the virtual server and the certificates must be provisioned on all nodes in the failover cluster.
- SQL Server 2008 R2 and the SQL Server 2008 R2 Native Client support wildcard certificates. Other clients might not support wildcard certificates. For more information, see the client documentation and [KB258858](#).

## To provision (install) a certificate on the server

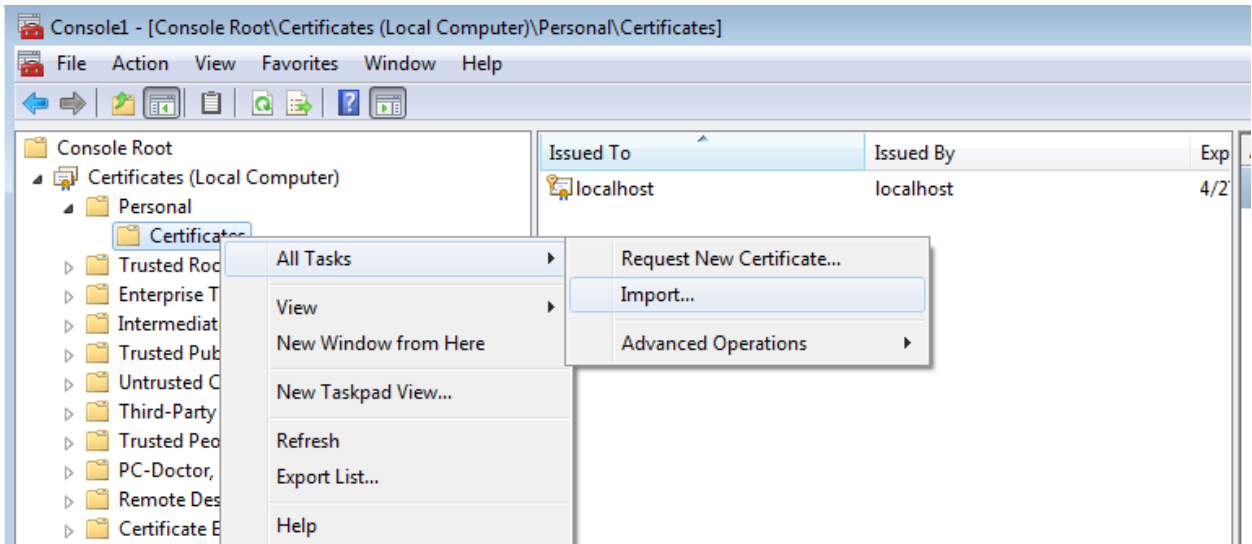
1. On the Start menu, click Run, and in the Open box, type MMC and click OK.
2. In the MMC console, on the File menu, click Add/Remove Snap-in.
3. In the Add/Remove Snap-in dialog box, click Add.
4. In the Add Standalone Snap-in dialog box, click Certificates, click Add.



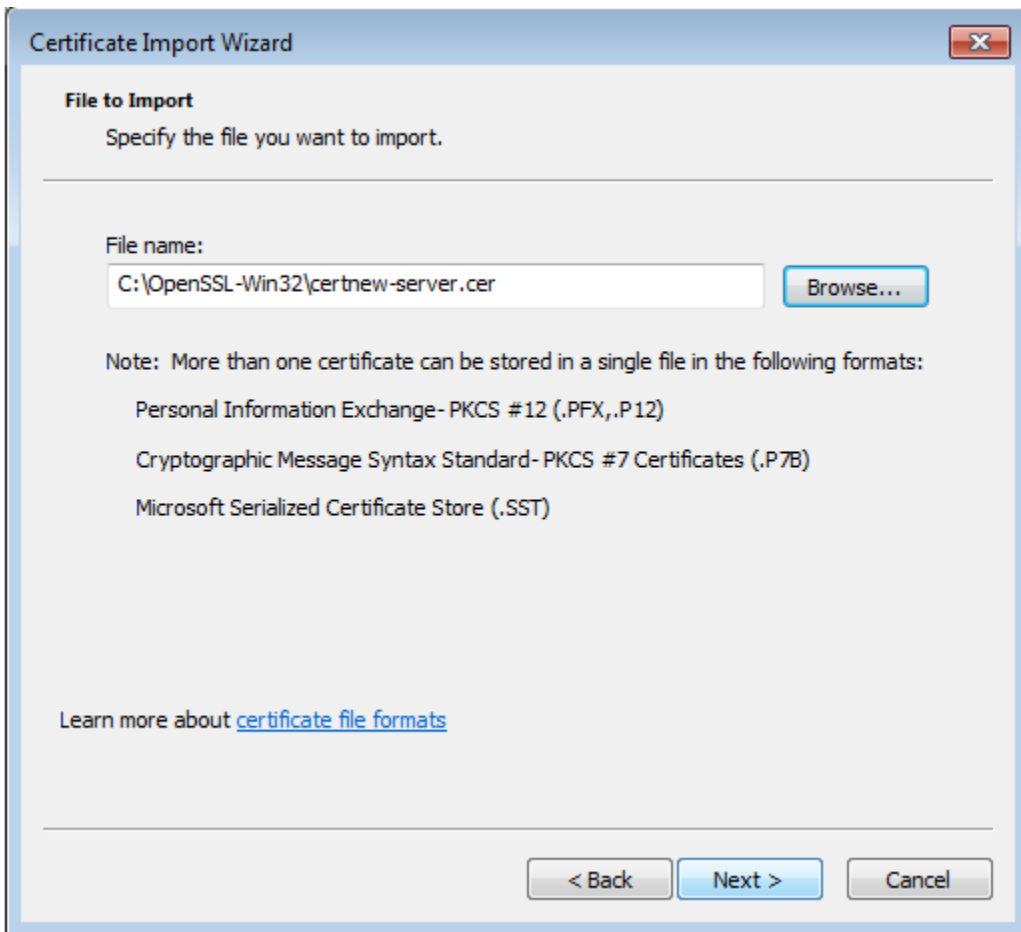
5. In the Certificates snap-in dialog box, click Computer account, and then click Finish.
6. In the Add Standalone Snap-in dialog box, click Close.
7. In the Add/Remove Snap-in dialog box, click OK.



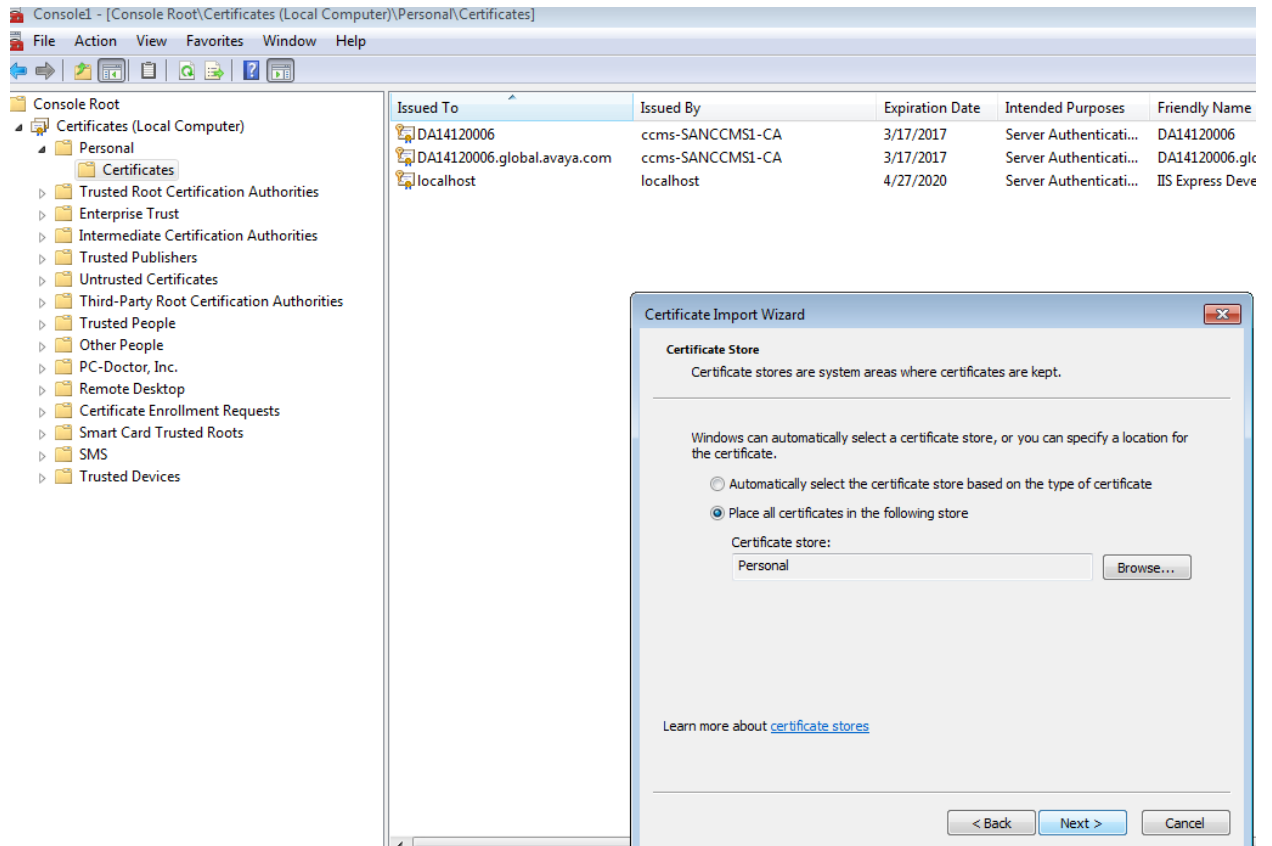
8. In the Certificates snap-in, expand Certificates, expand Personal, and then right-click Certificates, point to All Tasks, and then click Import.



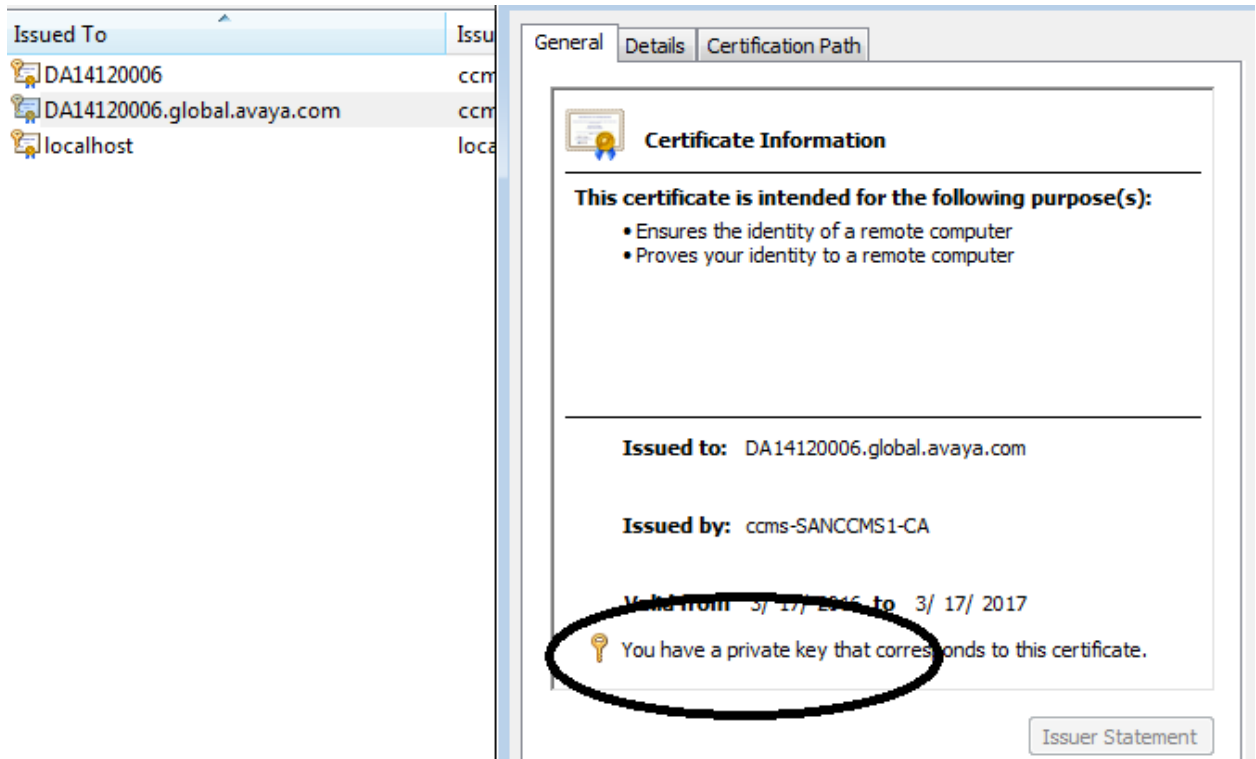
9. Complete the Certificate Import Wizard, to add a certificate to the computer, and close the MMC console. For more information about adding a certificate to a computer, see your Windows documentation. Select the server certificate created in step 18 in the previous section.



Select Next.

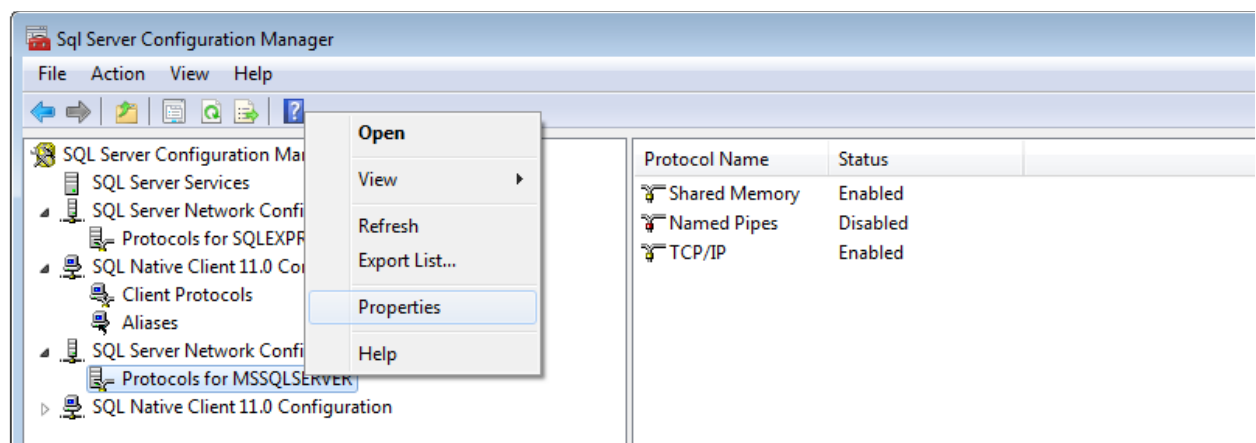


After importing ensure that the certificate has the private key symbol as shown below. It is important to import the certificate in the same store which was used to create the certificate signing request.



## To configure the server to accept encrypted connections

1. In SQL Server Configuration Manager, expand SQL Server Network Configuration, right-click Protocols for <server instance>, and then select Properties. Use < server instance > with the installed instance of SQL server



2. In the Protocols for <instance name> Properties dialog box, on the Certificate tab, select the desired certificate from the drop down for the Certificate box, and then click OK.



**Note that if the certificate is not shown in the dropdown** probably the SQL server is running under a different account than Local System/Network service. Either change the SQL service account or install the certificate under the corresponding user credentials.

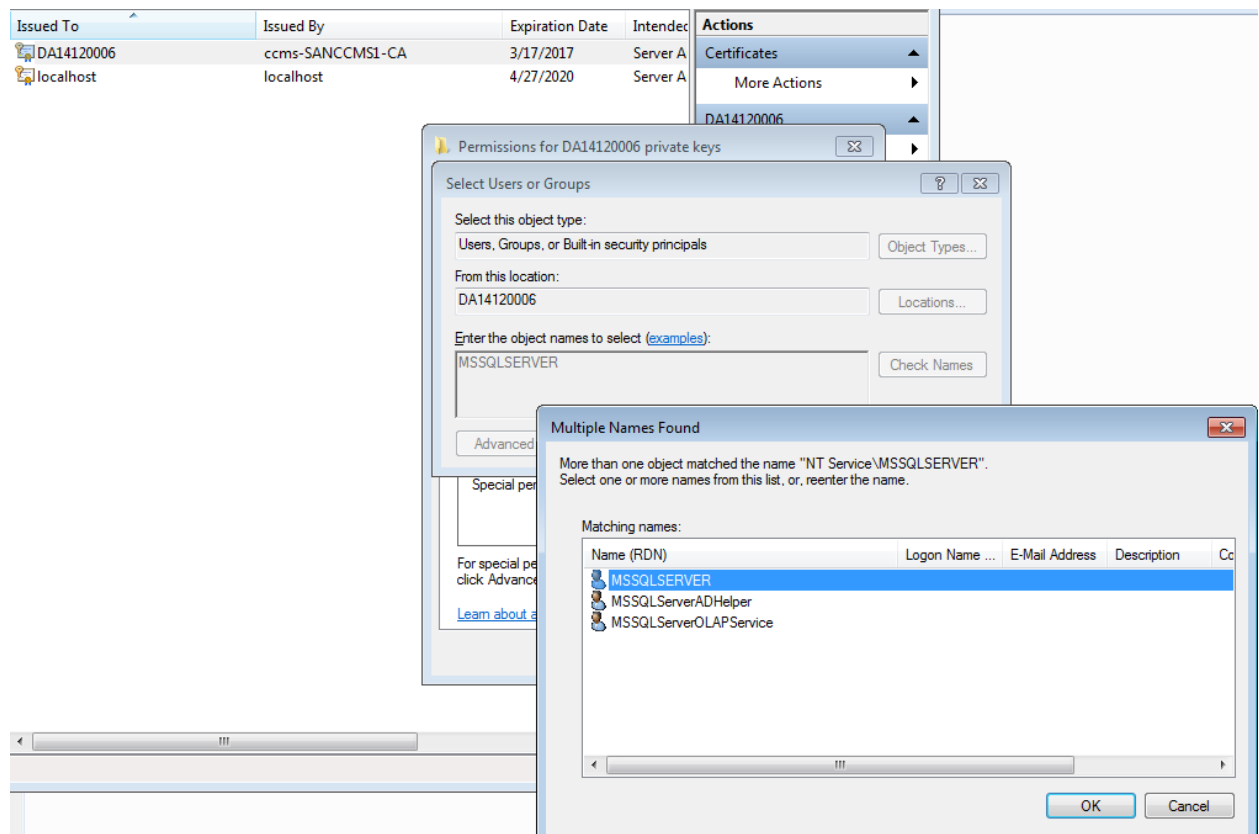
This procedure inserted here as an embedded document can also be used if the certificate authority is a local certificate authority.



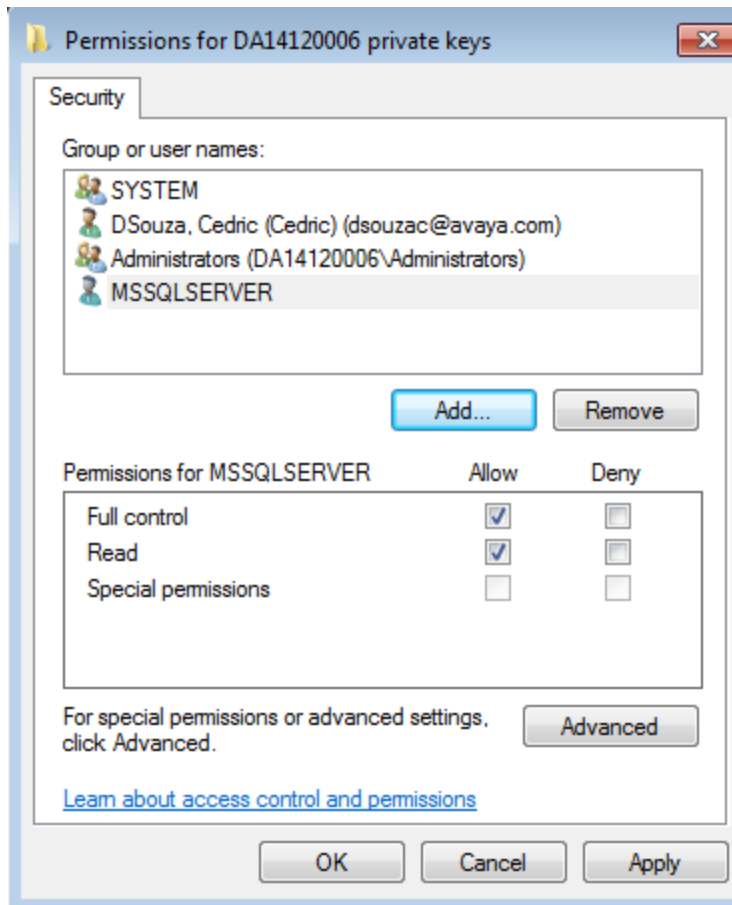
SSL\_Certificate.docx

3. If the SQL Service does not Start or gives certificate chain errors check to see which account the SQL Service is running. If the SQL Service is running in a different account as Local System, then the Server certificate needs to be given permissions to get access to the Private Key.

Select Manage Private key for the server certificate and select the account which is used to start SQL service. Normally it is NT Service\MSSQLSERVER



Provide full access to this User.



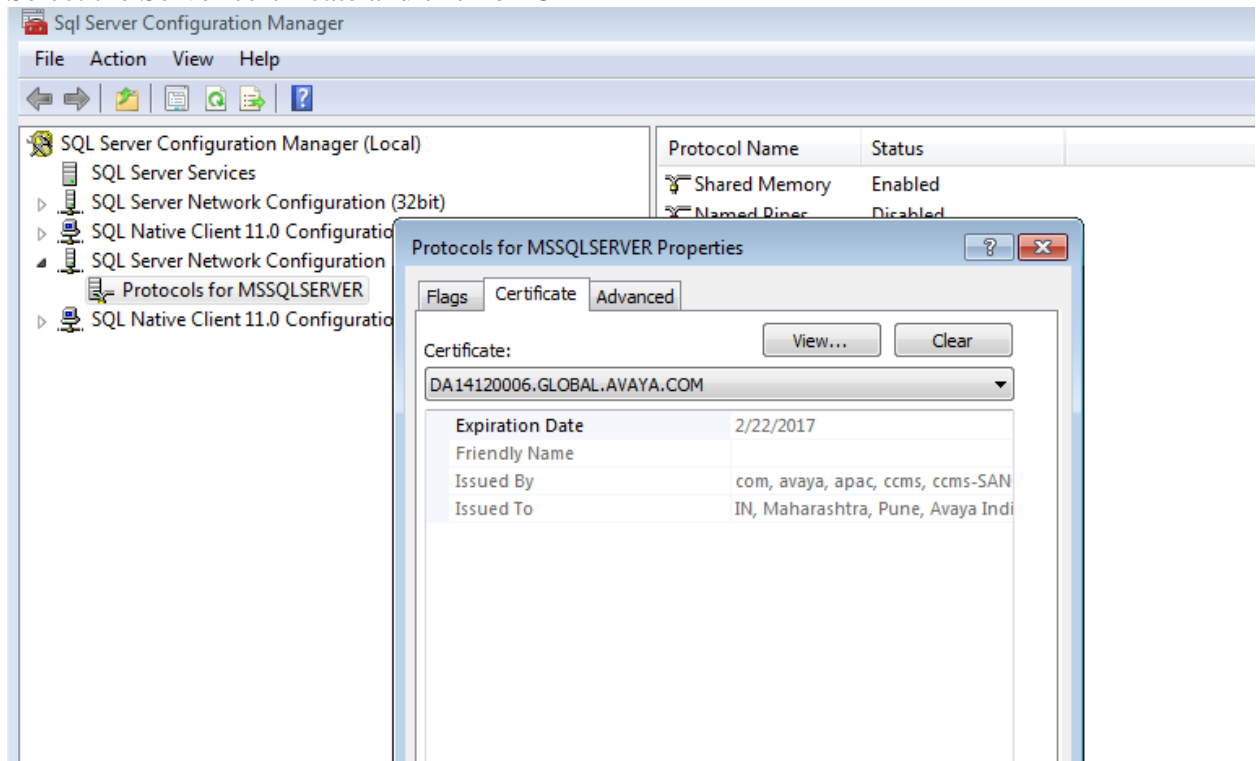
Restart the SQL server after this.

If the certificate is still not displayed maybe this might help

<http://thesqldude.com/2012/04/21/setting-up-ssl-encryption-for-sql-server-using-certificates-issues-tips-tricks/>

<https://www.mssqltips.com/sqlservertip/3299/how-to-configure-ssl-encryption-in-sql-server/>

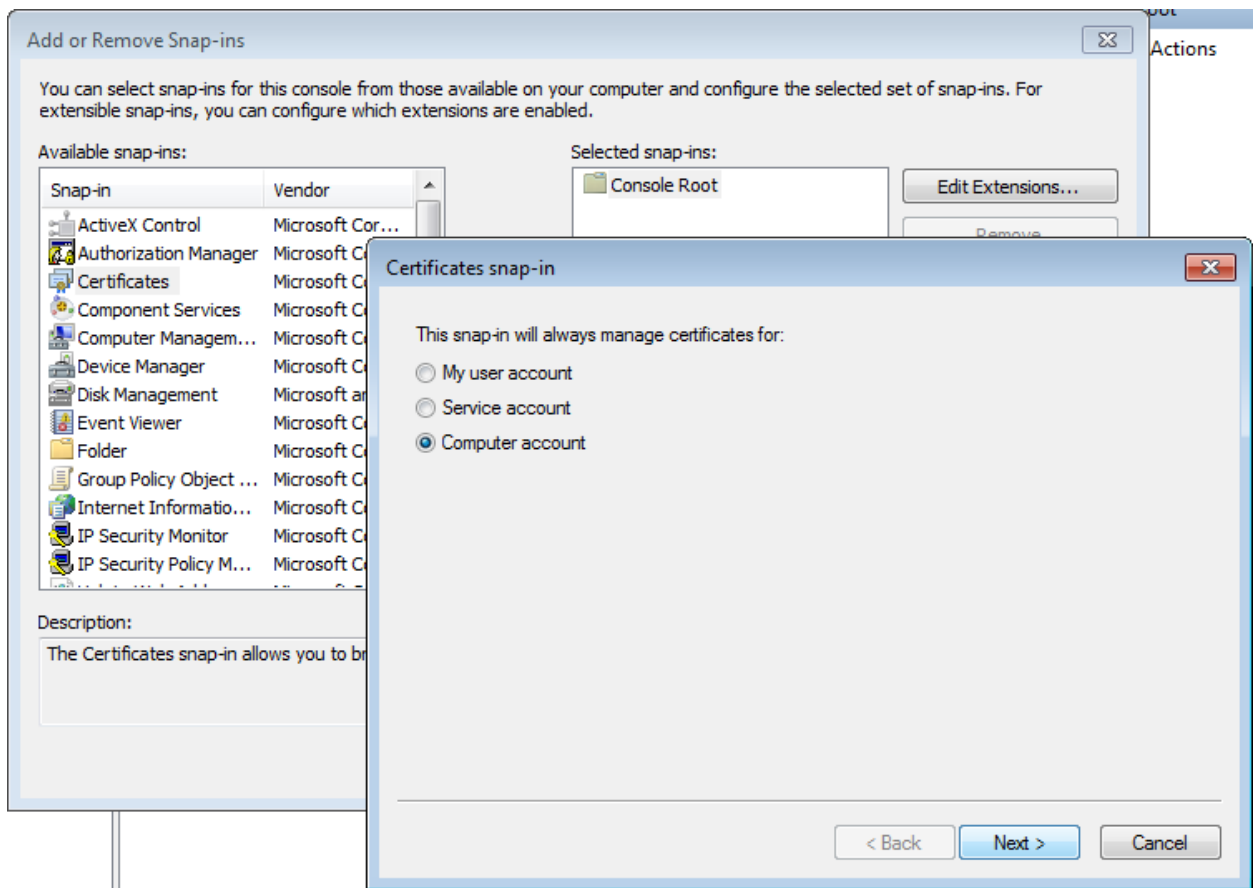
Select the Server certificate and click on OK



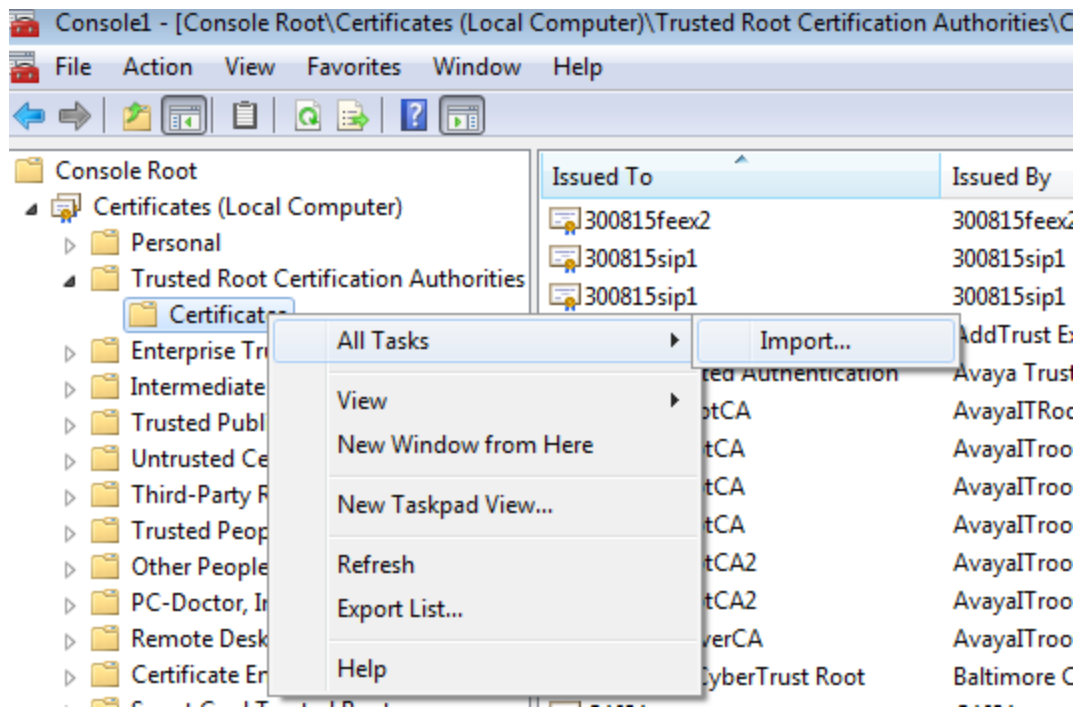
4. Restart the SQL Server service.

## Installation of root certificate on EMC machine(s)

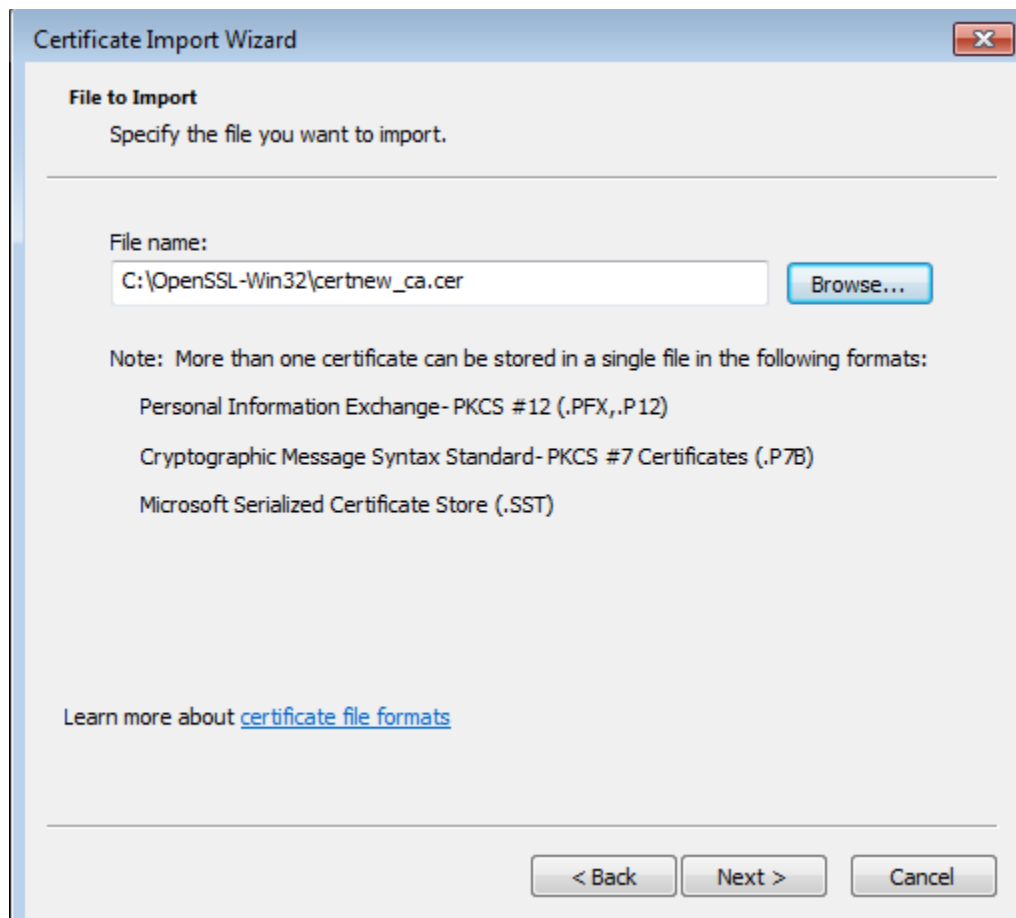
On each EMC desktop and EMC Server where database secure access is required the root certificate must be installed to



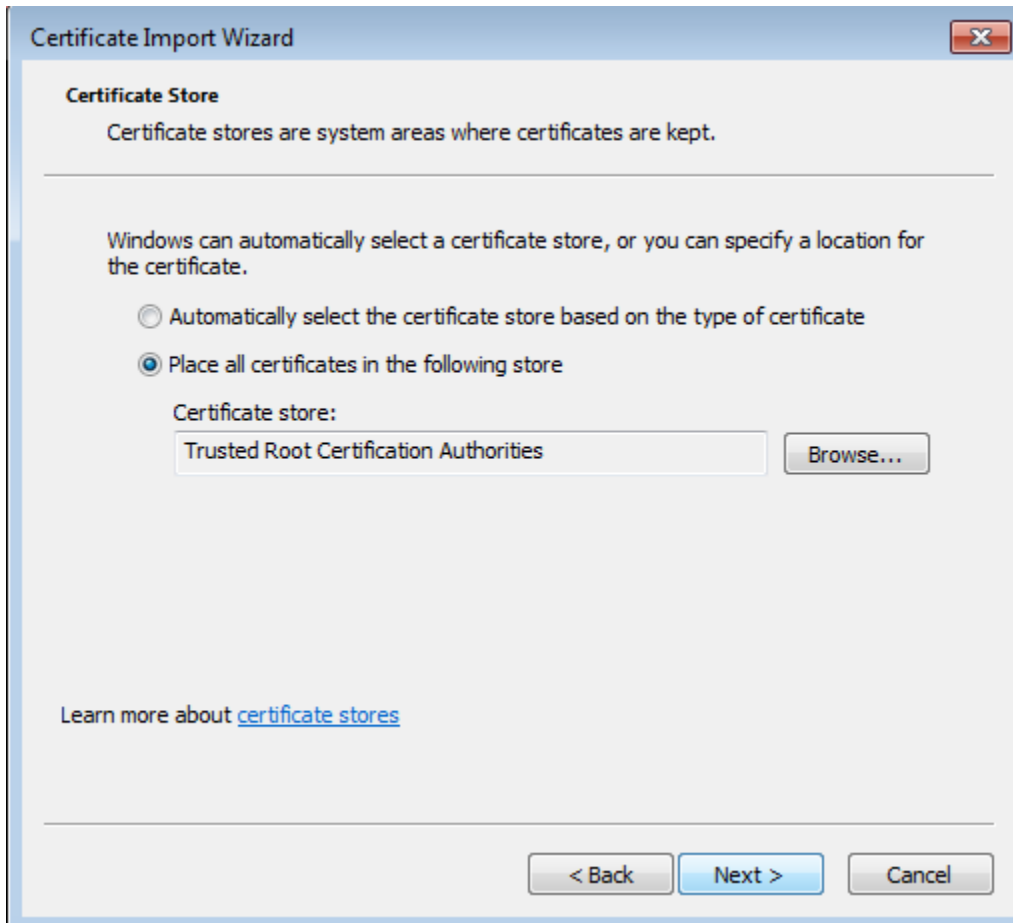
Select Import



Select the certificate



Select trusted root certificate authority



Select finish.

## Certificate Import Wizard

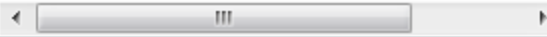


### Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certificate
Content	Certificate
File Name	C:\OpenSSL-Win32\ca



< Back

Finish

Cancel

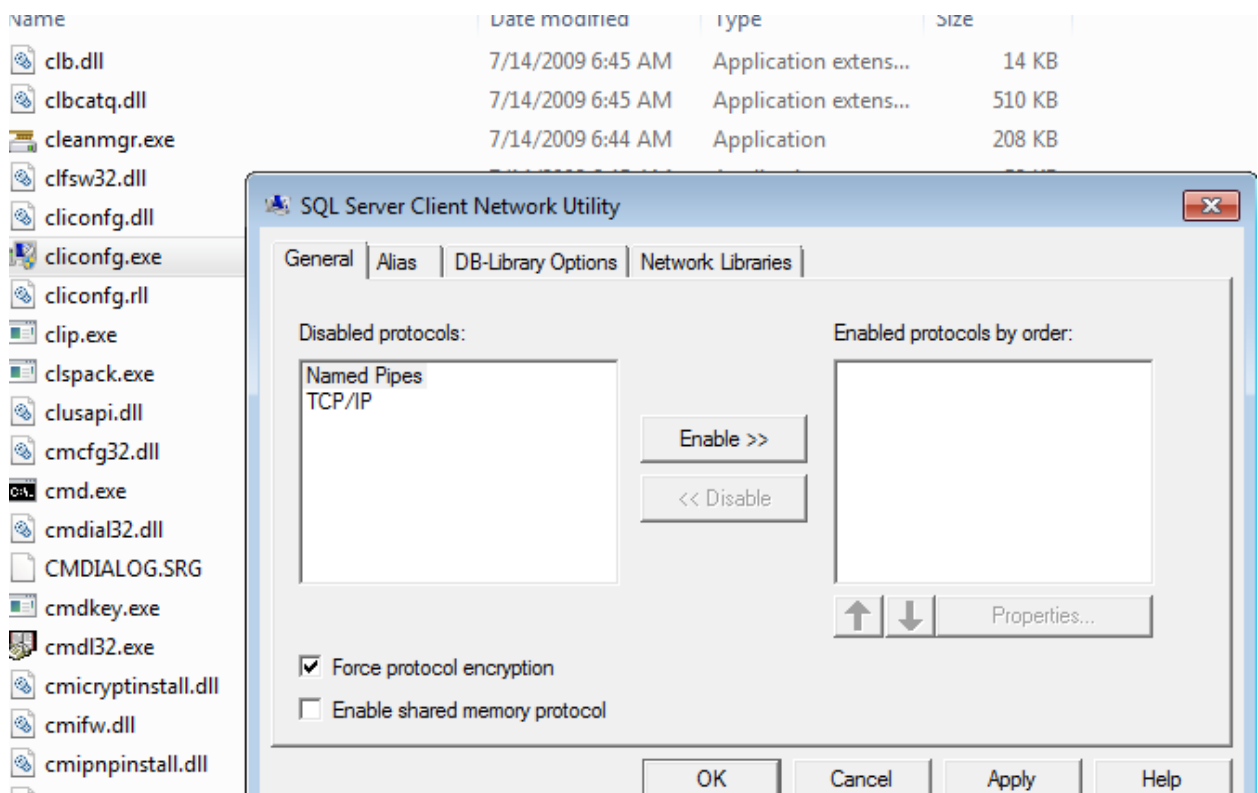
# Configurations on EMC Core and desktop

The following configuration changes will need to be performed on EMC Core servers, if secure connection is required from Servers. Note that **this is optional on Server**. All EMC servers can still connect through the unsecure channel.

## Server side changes required

Run Cliconfg.exe from c:\windows\syswow64 folder.

## Enable Force protocol encryption option



For Voice Media Store, Email Media Store, PCMS and SMMS change the Server name to the FQDN of the SQL server.



Media Store Database

Server name:  ...

User name:

Connection string:

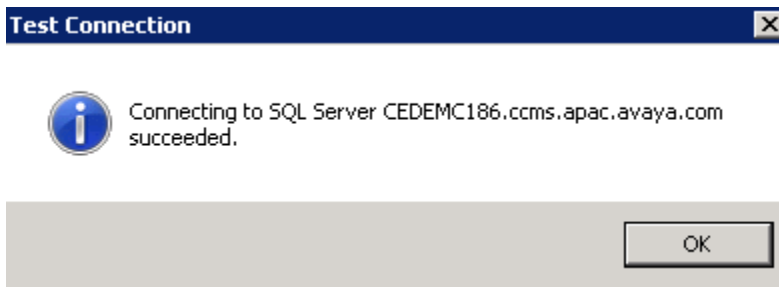
☒ Save empty UUI and collected digits

---

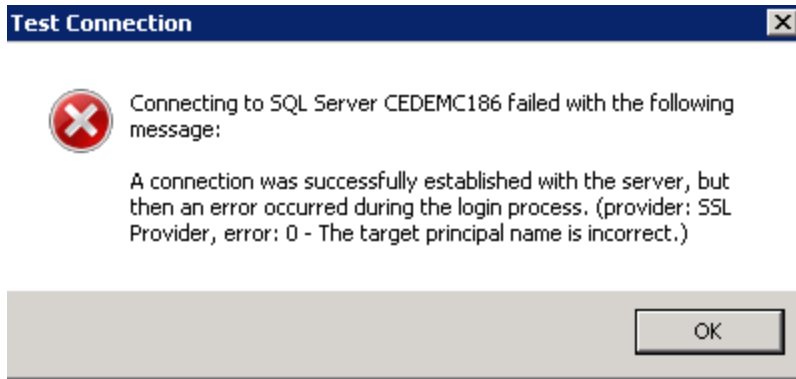
Contact Database

Server name:  ...

The connection can be tested with the Test connection button. If the connection succeeds and Server certificate Validation is passed then the following message will be displayed



If the connection fails due to certificate reasons the reason will be displayed as such



Stop the IDS View service and change the following ini parameter. Also if the Connection string is present ensure that it is emptied out before saving the file and restarting the IDS View service.

[IDS View Engine]

Database Connection String =

```
%%ENCRYPTED("814B1286E738AF50454519C08A4B456D2FC782C85543A3121F07A705DE6727DBC  
144C4D11CBAB0CAFEC33B6C647D596053090F8905637A5EE4573CCE0CFE51AAE5709C0EA07BA77  
8B483ED52D801E5C02F8B2AAEEE3635C0FE66665B26F0A93C3E8A4CDFD9D9F79139357A236942E5  
8A92AC36926509754B274B802F94FFE9B1BA0892455CC80F61FB1D4722CB3400F")
```

Database Server Name = **CEDEMC186.ccms.apac.avaya.com**

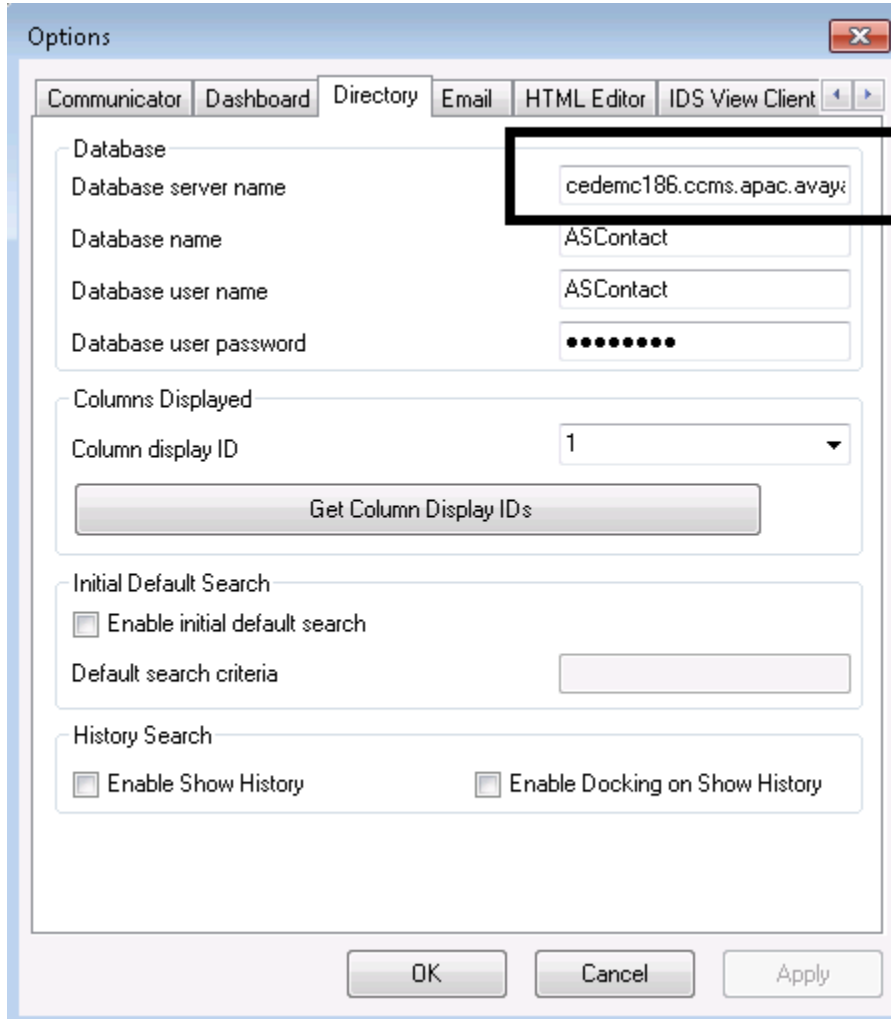
Change in **Task Director database** configuration as well

Changes are not required in Configuration server database settings

### Desktop side changes required

The database server name must match the FQDN of the database server / the subject alternate names of the DB server. / the alias if created.

For Alias creation to use a non- default SQL port refer to the “Changing the default SQL Server port number” section in “Chapter 8: Installing SQL Server” in the Installation guide.



The screenshot shows the 'Options' dialog box with the 'Directory' tab selected. The 'Database' section contains the following fields:

- Database server name: cedemc186.ccms.apac.avaya (highlighted with a black box)
- Database name: ASContact
- Database user name: ASContact
- Database user password: (masked with dots)

The 'Columns Displayed' section contains a dropdown menu for 'Column display ID' set to '1' and a 'Get Column Display IDs' button.

The 'Initial Default Search' section contains a checkbox for 'Enable initial default search' (unchecked) and a 'Default search criteria' text box.

The 'History Search' section contains two checkboxes: 'Enable Show History' (unchecked) and 'Enable Docking on Show History' (unchecked).

At the bottom of the dialog are 'OK', 'Cancel', and 'Apply' buttons.

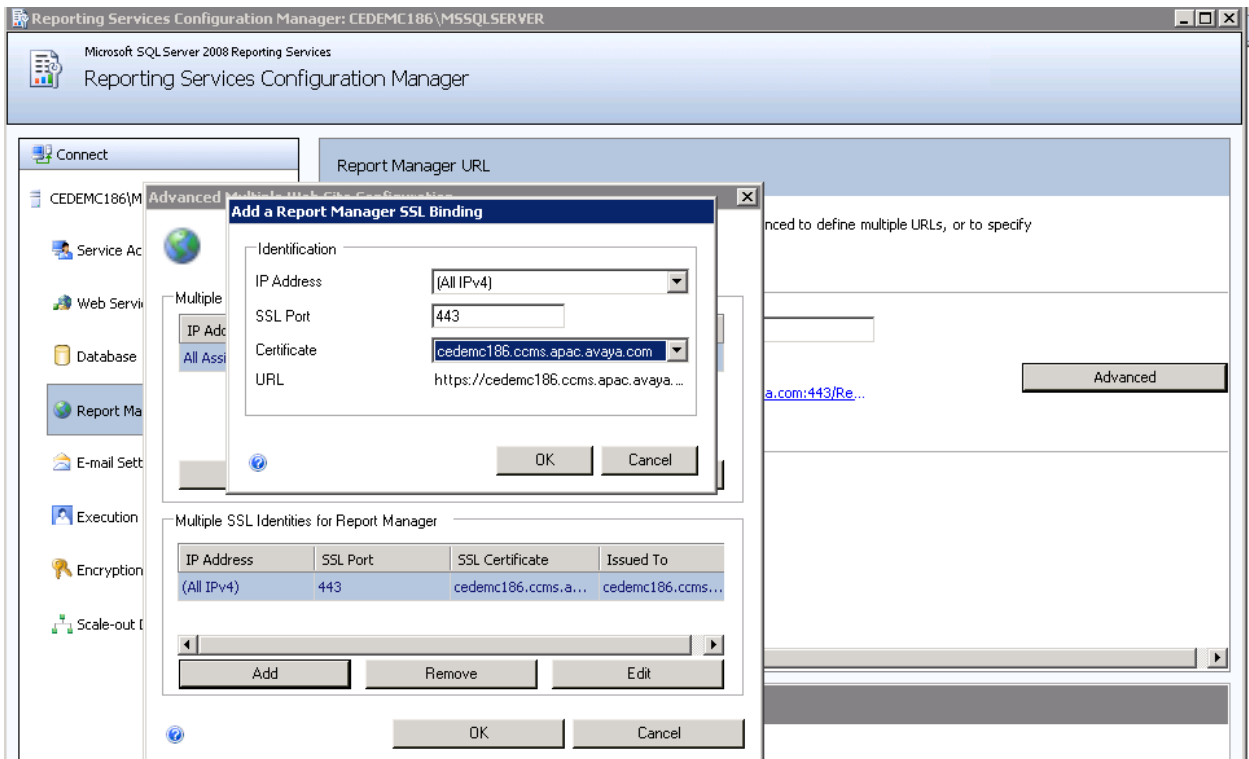
Ensure that the connection between EMC Desktop and the SQL Server is encrypted using a tool like Wireshark etc.

### To configure a report server URL for SSL

1. Start the Reporting Services Configuration tool and connect to the report server.
2. Click Web Service URL.
3. Expand the list of SSL Certificates. Reporting Services detects server authentication certificates in the local store. If you installed a certificate and you do not see it in the list, you might need to restart the service. You can use the Stop and Start buttons on the Report Server Status page in the Reporting Services Configuration tool to restart the service.
4. Select the certificate.
5. Click Apply.
6. Click the URL to verify it works.

URL reservations for Report Manager and the Report Server Web service are configured independently. If you want to also configure Report Manager access through an SSL-encrypted channel, continue with the following steps:

1. Click Report Manager URL.
2. Click Advanced.
3. In Multiple SSL Identities for Report Manager, click Add.
4. Select the certificate, click OK, and then click Apply.
5. Click the URL to verify it works.



Reporting Services Configuration Manager: CEDEMC186\MSSQLSERVER

Microsoft SQL Server 2008 Reporting Services

Reporting Services Configuration Manager

Connect

CEDEMC186\MSSQLSERVER

Service Account

Web Service URL

Database

Report Manager URL

E-mail Settings

Execution Account

Encryption Keys

Scale-out Deployment

Report Manager URL

Configure a URL to access Report Manager. Click Advanced to define multiple URLs, or to specify additional parameters on the URL.

Report Manager Site Identification

Virtual Directory: Reports

URLs:  
<http://CEDEMC186:80/Reports>  
<https://cedemc186.ccms.apac.avaya.com:443/Re...>

Advanced

Results

✓ Reserving url <https://cedemc186.ccms.apac.avaya.com:443>

✓ Create certificate binding.

The certificate binding was created successfully.

Apply

Exit

Options

World clock | Communicator | Dashboard | Directory | Email | Reporting | HTM

**Report Server**  
Task Director

Report Server Connection Details

Report Server Scheme:

Report Server Address:

Report Service Url:

Report Web Service Url:

Report Generation Timeout (Seconds):

Network Credentials

User name:

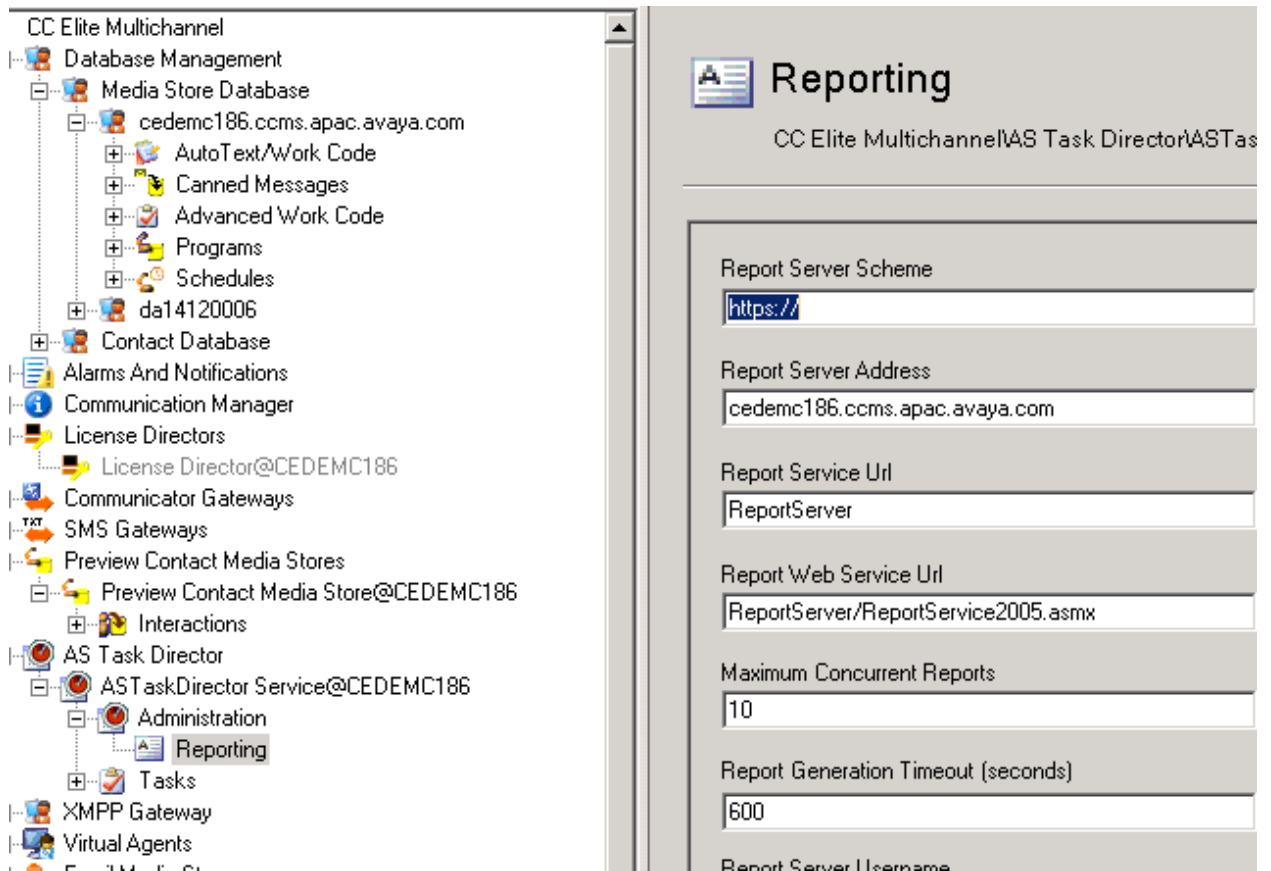
Password:

Domain:

OK Cancel Apply

Ensure that EMC Reporting Desktop is able to see all the reports and open the reports accordingly

The task director settings also need to change



Ensure that EMC Reporting desktop is able to schedule reports and the reports get created on EMC Server.