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-tosha-2-algorithm

You should see following output

Model Administrator: C:\Windows\system32\cmdexe Microsoft Windows [Uersion 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 Neu Value: CNGHashAlgorithm REG_SZ = SHA1 Neu 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: -setreg command completed successfully. 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 was stopped successfully. The Active Directory Certificate Services service was stopped successfully. 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

 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.

Console1 - [Console Root]	Window Help						Equation Symbol
Console Root	Name	Add or Remove Snap-ins You can select snap-ins for extensible snap-ins, you car Available snap-ins: Snap-in Active X Control Cartificates Component Services Computer Manager Dick Dick Dick Dick Dick Dick Dick Dick	this console from the configure which end of Microsoft Cor Microsoft Cor	iose available on yo xtensions are enabl Certificates snap-in This snap-in will a My user acco Service acco Service acco Service acco	Actions ur computer and configure the sel ed. Selected snap-ins: Console Root always manage certificates for: unt unt count	lected set of snap-ins. For Edit Extensions. Remove	
	← ⊕ ⊘ File Edit View ☆ № Suggested S	Favorites Tools Help Sites • 1 EMC 7.0 - All Documents	Bills Pay 👻 🀊 Demo			< Back Next >	Cancel

Right Click on Personal > Certificates -> Advanced Operations > Create Custom Request
 Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

🚡 File Action View	Favorites Window Help					
🗢 🔿 🚈 🗊 📋	Q 📑 🛛 🚺					
Console Root		Issue	ed To	Issue	ed By	Expiration Date
Certificates (Local	Computer)	i 🔄 co	cms-SANCCMS1-CA	ccm	s-SANCCMS1-CA	2/17/2021
Personal		🛛 🖾 D.	A14120006	ccm	s-SANCCMS1-CA	3/17/2017
	All Tasks	•	Request New Certificate		-SANCCMS1-CA	3/17/2017
Enterprise	View		Import		iost	4/27/2020
Intermedia	View		Advanced Occurticut		Create Creaters Berry	
D Trusted Pu	New Window from Here		Advanced Operations	•	Create Custom Reque	25t
D Untrusted	New Taskpad View				Manage Enrollment P	olicies
D Initial Part						
D Trusted Pe	Refresh					
D Other Peop	Export List					
PC-Doctor						
Remote De	Help					

3. Select proceed without enrollment policy



Select Legacy Key

🔄 Certificate Enrollment	
📮 Certificate Enrollment	
Custom request	
Chose an option from t	he list below and configure the certificate options as required.
Template:	(No template) Legacy key
Request format:	PKCS #10
	O CMC
Note: Key archival is r specified in the certific	not available for certificates based on a custom certificate request, even when this option is cate template.
Learn more about <u>cust</u>	om request
	Next Cancel

4. Go to Details -> Properties on Next Page

Certificate Properties	×	Expiration Date Intended Purposes Frien	dly N
General Subject Extensions Private Key		2/17/2021 <aii> <nor< th=""><th>1e></th></nor<></aii>	1e>
A friendly name and description will make it easier to identify and use a certificate.) pc
			25
Description:			
		mplate, or click Details to customize the certificate	
		ATUS: Available Details ^ ity period that apply to this type of certificate:	
		Properties	
Learn more about <u>certificate properties</u>			
OK Cancel App	y	Next Cancel	

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

Certificate Properties	—
General Subject Extensions Private Key	
A friendly name and description will make it easier to identify and use a certificate.	
Friendly name:	
cedemc186.ccms.apac.avaya.com	
Description:	
SQL SSL 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 Priv	ate Key	
The subject of a certificate is the t can enter information about the t can be used in a certificate.	user or computer to whi ypes of subject name a	ich the certificate is issued. You nd alternative name values that
Subject of certificate		
The user or computer that is recei	iving the certificate	
Subject name:		C11 1 105
Туре:		CN=cedemc186.ccms.apac.ava
Common name 🔹	Add >	
Value:	< Remove	
		< III >>
Alternative name:		
Туре:		
DNS 👻		
Value:	Add >	
cedemc186		
	< Remove	
Learn more about subject name		
	ОК	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: CN=cedemc186.ccms.apac.ava Common name Add >
Value: < Remove
Alternative name:
Type: DNS
DNS cedemc186
Value: Add > 148.147.174.186
< Remove
4
Learn more about <u>subject name</u>
OK Cancel Apply

Select server authentication as Extended Key Usage

Certificate Properties		×
General Subject Extensions Priva The following are the certificate extension Extensingradiance Extension <t< th=""><th>te Key tensions for this certificate type.</th><th>•</th></t<>	te Key tensions for this certificate type.	•
Key usage	~	
Extended Key Usage (application An application policy (called enha certificate can be used. Select the certificates issued by this template	policies) ^ Inced key usage in Windows 2000) defines how a application policy required for valid signatures of e.	E
Available options: Client Authentication Code Signing Secure Email Time Stamping Microsoft Trust List Signi Microsoft Time Stamping	Selected options: Server Authentication Add > < Remove	

Select Key type Exchange and key length as 2048

Certificate Properties	x
General Subject Extensions Private Key	
Cryptographic Service Provider	^
Key options	
Set the key length and export options for the private key.	
Key size: 2048	
✓ Make private key exportable	
Allow private key to be archived	
Strong private key protection	Ξ
Key type 🔺	
Key usage defines the allowed uses for a private key associated with a certificate.	
O Exchange	
Signature	
Key permissions	
Learn more about <u>private key</u>	Ŧ
OK Cancel Apply	

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 to your hard disk or removable media. Enter the location and name of your certificate request, and click Finish.	request I then
File Name: C:\OpenSSL-Win32\CertificateRequest.csr File format:	/se
Image is the main and the main	
Learn more about <u>file format</u>	
Finish	Cancel

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

A S Certificate C	CR-CCEM	G create cert	Freate Cer	<i>e</i> How to ge	How to cr	Certific
File Edit View Favorites Tools Help						
🚕 📴 Suggested Sites 👻 🚯 EMC 7.0 - All Documents 🌗 Bills Pay 🕶	🛯 🐌 Demo 🔻 🌗	EMC 👻 퉬 Learn	ings 👻 퉬 Perso	nal 🔻 🧃 Avaya I	Remote Access 🧯	🕽 Avaya - W
Microsoft Active Directory Certificate Services ccms-SANCCM	IS1-CA					
Welcome						

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your i over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or 1

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.



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.

📔 С:	\OpenSSL-Win32\CertificateRequest.csr - Notepad++
File	Edit Search View Encoding Language Settings Macro Run TextFX Plugins Window ?
	을 🗄 🖻 🔓 🕼 🖕 🖧 🗅 🛍 ⊋ ⊄ # 🍇 🤏 🤫 🖫 🖬 ≣ 🗊 11 ≣ ⊄ ● 🗉 🕨 🔤 조 △ ▼ Σ 😹
🗎 Ce	vtificateRequest.csr
1	BEGIN CERTIFICATE REQUEST
2	MIIC0jCCAboCAQAwdDELMAkGA1UEBhMCSU4xDDAKBgNVBAgMA01BSDENMAsGA1UE
3	BwwEUHVuZTEUMBIGA1UECgwLQXZheWEgSW5kaWExDDAKBgNVBAsMA0dDUzEkMCIG
4	A1UEAwwbREExNDEyMDAwNi5nbG9iYWwuYXZheWEuY29tMIIBIjANBgkqhkiG9w0B
5	AQEFAAOCAQ8AMIIBCgKCAQEAwnGIYazc8ojQVSpHjMvRbdwWdIUqMBgeitDWa9ym
6	6LC4kYix7ENdFp1d45EYybWfF3qY6dOiEWjs5oMqed6mqsz9eY6FoZgennar660Y
7	nAP1onXQIFBseMNq7MCS6wGTZwLwIX0Ly6fzzuc6yeNBAUgj122DGv/20tXm03f/
8	f4u7Kc6gXZNiaxajEkZeDwQgMc378apB3gQ6X83ndteD0JWc7mKK+bATcqPoeYwz
9	Ty10LaGc/sj57AX8N/a4LPYIQD9MVQiCCH+PgBEiBB7ufCCQypN7GKCYl+utHfNm
10	FchRGPfyapjSdyo67ByElxW/0in/TxLrUaAfEma6rM9CwwIDAQABoBkwFwYJKoZI
11	eq:hvcNAQkHMQoMCEF2YX1hMTIzMA0GCSqGSIb3DQEBCwUAA4IBAQCbydqFAGNdieRc
12	z+GY9RtyaZeCYi3S8//MjKhm9qtusdHbnRhGLCyZB2Lo8N5kqxPU/06IJL7E9Nsl
13	LYvQHFQQIo6roHxCculwZiTizHnVUFOmw95ddXXiG4Sfs0Xh/rdxRD5/Lb9pq6Wr
14	MtCh9SSLtl/EA+QbwoB92fFtE4YpWFG001y1KkD4uNDP60ejhOSddSYzDtdBQXhh
15	yqZPx68xEIS0UC/68BoJQjPxxJAGPeQkX9e0ygIcP4lrqk6IaBCFJKzXXCYfwZAa
16	+2IeQeE+jnTn9dhmitWJJ6px9nhfALFrf/VHrtZiHZrs/HPw15511HU+ifLsWm0I
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 퉳 Bills Pay 👻 鷆 Demo 👻 퉳 EMC 👻 퉱 Learnings 👻 퉳 Personal 👻 🧃 Avaya
Minnand Antina Directory Cartifacto Sanisan - come SANCOMS4 CA
MICROSON ACTIVE Directory Centificate Services CCMS-SANCCIVIS I-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 Web server) in the Saved Request box.
Saved Request:
Base-64-encoded MtCh9SSLtl/EA+QbwoB92fFtE4YpWFG001y1KkD4 certificate request yq2Px68xEIS0UC/68BoJQjPxxJAGPeQkX9e0ygIc (CMC or +21eQeE+jnTn9dhmitWJJ6px9nhfALFrf/VHrtZi PKCS #10 or END CERTIFICATE REQUEST PKCS #7):
Certificate Template:
SM certs V
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 ; Web server) in the Saved Request box.	
Saved Request: MtCh9SSLt1/EA+QbwoB92fFtE4YpWFG001y1KkD4	
Base-64-encoded yq22x63xE1SOUC/68BGJQj2xXJAGFeQxX9eOyg1C certificate request +21eQeE+jnTn9dhmitWJJ6px9nhfALFrf/VHrtZ1 (CMC or CmcTYVRt PKCS #10 orEND CERTIFICATE REQUEST	
Certificate Template:	
SM code	
Additio Additio This Web site is attempting to perform a digital certificate operation on your behalf: https://148.147.170.77/certsrv/certfnsh.asp You should only allow known Web sites to perform digital certificate operations on your behalf. Do you want to allow this operation?	
<u>Y</u> es <u>No</u>	

17. Click on Yes and download the certificate

A ttps://148.147.170.77/certsrv/c 🔎 🔹 S Certificate C S CR-CCEM-508 CCEM
File Edit View Favorites Tools Help
👍 🕨 Suggested Sites 🔻 🚯 EMC 7.0 - All Documents 🎚 Bills Pay 👻 🌗 Demo 👻 🌗 EMC 👻 🌗 Learnings ·
Microsoft Active Directory Certificate Services ccms-SANCCMS1-CA
Certificate Issued
The certificate you requested was issued to you.
DER encoded or OBase 64 encoded Download certificate Download certificate chain

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

Certificate	—
General Details Certification Path	
Show: <all></all>	•
Field	Value
Signature hash algorithm Signature hash algorithm Sugnature Valid from	sha256 ccms-SANCCMS1-CA, ccms, a Thursday, February 18, 2016 Friday, February 17, 2017 2:2
🗐 Subject	DA14120006.global.avaya.co
Public key	RSA (2048 Bits)
Subject Key Identifier	0e 24 a7 6f 1e 49 fc 17 14 27
Authority Key Identifier	KevID=ce 85 h6 c5 h1 ac 0c f
CN = DA14120006.global.avaya.co OU = GCS O = Avaya India L = Pune S = MAH C = IN	m
Ed Learn more about <u>certificate details</u>	it Properties Copy to File
	ОК

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

← → @ https://148.147.170.77/certsrv/	🔀 CR-CCEM-508 C	How to generat	🕝 How to create S	<i>e</i> Microsoft Ac ×
File Edit View Favorites Tools Help				
👍 🕨 Suggested Sites 🔻 🚯 EMC 7.0 - All Documents 🌗 Bills Pay 🔻	퉬 Demo 🔻 퉬 EMC ୟ	🔹 퉬 Learnings 👻 🌗	Personal 🔻 遵 Avaya	Remote Access 🧕 Av
Microsoft Active Directory Certificate Services ccms-SANCCMS	1-CA			

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CR)

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Select Yes

Web Acce	ss Confirmation	23
	This Web site is attempting to perform a digital certificate operation on your behalf: https://148.147.170.77/certsrv/certcarc.asp You should only allow known Web sites to perform digital certificate operations on your behalf. Do you want to allow this operation?	
	Yes No	

Download the CA certificate

🗲 🕀 🥭 htt	ps://148.147.170.77/certsrv/c 🔎 🔻 😵 Certificate 🖒 🕵 CR-CCEM-508 C 🧭 How to generat 🥝 How to create S
File Edit View	v Favorites Tools Help
👍 ▶ Suggested	d Sites 🔻 🚯 EMC 7.0 - All Documents 🌗 Bills Pay 👻 🌗 Demo 👻 🌗 EMC 👻 🌗 Learnings 👻 🌗 Personal 👻 🥭 Avaya
Microsoft Active	Directory Cartificate Services come SAN/CCMS1 CA
MICTOSON ACTIVE	Directory Certificate Services - Constanticol Vion-CA
Download a	CA Certificate, Certificate Chain, or CRL
To trust certific	cates issued from this certification authority, install this CA certificate chain.
l o download a	a CA certificate, certificate chain, or CRL, select the certificate and encoding method.
CA certificate:	
	Current [ccms-SANCCMS1-CA]
Encoding metho	od:
	• DER
	⊖ Base 64
Download CA	<u>certificate</u>
Download Late	certificate chain
Download late	est delta CRL

Verify the CA certificate is SHA-256

Certificate	×
General Details Certification Path]
Show: <ali></ali>	•
Field	Value 🔺
Signature algorithm	sha256RSA
Issuer	ccms-SANCCMS1-CA, ccms, a
Valid from Valid to Subject Public key Certificate Template Name CN = ccms-SANCCMS1-CA DC = ccms DC = apac DC = avaya DC = com	Thursday, February 18, 2016 Wednesday, February 17, 20 ccms-SANCCMS1-CA, ccms, a RSA (2048 Bits)
Ed	it Properties Copy to File
	ОК

Installation of server certificate on SQL Server

Prerequisites for server certificate (Copied from https://technet.microsoft.com/enus/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_ENCIPHERMENT_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 <u>KB258858</u>.

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.

vailable snap-ins:			Select	ed snap-ins:	
Snap-in	Vendor	*	C	onsole Root	Edit Extensions
ActiveX Control	Microsoft Cor				Remove
Authorization Manager	Microsoft Cor				
Certificates	Microsoft Cor	Ξ			
💩 Component Services	Microsoft Cor				Move Up
E Computer Managem	Microsoft Cor				
📇 Device Manager	Microsoft Cor	_			Move Down
🕋 Disk Management	Microsoft and		Add >		
🛃 Event Viewer	Microsoft Cor				
🚞 Folder	Microsoft Cor				
🗐 Group Policy Object	Microsoft Cor				
Internet Informatio	Microsoft Cor				
晃 IP Security Monitor	Microsoft Cor				
晃 IP Security Policy M	Microsoft Cor	-			Advanced

- 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.

Certificates snap-in	×
This snap-in will always manage certificates for:	
My user account	
Service account	
 Computer account 	

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

Console1 - [Console Root\Certificates (Local Computer)	Perso	nal\Certificates]		
🔚 File Action View Favorites Window Help				
Console Root	Issue	ed To	Issued By	Exp
a 🗊 Certificates (Local Computer)		ocalhost	localhost	4/2
a 📔 Personal	—		1000011030	.,-
Certificator				
Trusted Roc All Tasks	· _	Request New Certificate		
Enterprise T View	•	Import		
Intermediat		Advanced Operations		
Trusted Pub New Window from Here		Advanced Operations		
Image: Second				
Third-Party				
Trusted Peo Refresh				
PC-Doctor, Export List				
Remote Des				
Certificate E Help				

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.

Certificate Import Wizard
File to Import
Specify the file you want to import.
-1
File name:
C:\OpenSSL-Win32\certnew-server.cer Browse
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange-PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
< Back Next > Cancel

Select Next.

 Gonsole1 - [Console Root\Certificates (Local Compute) File Action View Favorites Window Help 	r)\Personal\Certificates]				
 Console Root Certificates (Local Computer) Personal Certificates Enterprise Trust Intermediate Certification Authorities Trusted Publishers Untrusted Certificates Trusted Poople Other People Other People Certificate Enrollment Requests Smart Card Trusted Roots SMS Trusted Devices 	Issued To	Issued By ccms-SANCCMS1-CA ccms-SANCCMS1-CA localhost	Expiration Date 3/17/2017 3/17/2017 4/27/2020	Intended Purposes Server Authenticati Server Authenticati Server Authenticati	Friendly Name DA14120006 DA14120006.glc IIS Express Deve
		Certificate Import Wizard Certificate Store Certificate stores are system. Windows can automatically se the certificate. Automatically select the Place all certificates in t Certificate store: Personal	areas where certificat lect a certificate store e certificate store base the following store	es are kept. e, or you can specify a loca ed on the type of certificate Brow	tion for
	<	Learn more about <u>certificate storer</u>	§	ack Next >	Cancel

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 selectProperties. Use < server instance > with the installed instance of SQL server

🚡 Sql Server Configuration Manager				
File Action View Help				
← → 2 ⊡ Q ⇒ 2	Open	Protocol Name	Status	
SQL Server Services	View 🕨	Shared Memory	Enabled	
▲ 및 SQL Server Network Confi 및 Protocols for SQLEXPF ▲ 및 SQL Native Client 11.0 Co	Refresh Export List	TCP/IP	Disabled Enabled	
Client Protocols	Properties			
SQL Server Network Confi	Help			
▷ ,費, SQL Native Client 11.0 Configu	uration			

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.



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

	1			1					
Issued To	Issued By	Expir	ration Date	Intendec	Actions				
🙀 DA14120006	ccms-SANCCMS1-CA	3/17	/2017	Server A	Certificates	A			
🛱 localhost	localhost	4/27	/2020	Server A	More Actions	•			
	ĺ	A Permissions	for DA14120	006 private	keys Σ	3 🕨	_		
		Select Users or	Groups			? 🛛			
		Select this obje	ect type:						
		Users, Groups	, or Built-in se	curity principa	als	Object Types			
		DA14120006	on.			Locations			
		Enter the object	t names to se	elect (example	ස):				
		MSSQLSERV	ER			Check Names			
			Multiple N	lames Found	ł				×
		Special per	More than Select one	one object m or more nam	natched the name "NT Servi nes from this list, or, reenter t	ice\MSSQLSERVER". he name.			
			Matchi	ing names:					
		For special pe click Advance	Nam	e (RDN) ISSQLSERV	ER	Logon Name .	E-Mail Address	Description	Co
		Leam about a	N S N	ISSQLServer ISSQLServer	ADHelper OLAPService				
	l								
٠ III									
			٠ .		III				•
							ОК	Canc	xel

Provide full access to this User.

🚶 Permissions for DA14120006 pri	vate keys	×			
Security					
Group or user names:					
SYSTEM DSouza, Cedric (Cedric) (dsouzac@avaya.com)					
Administrators (DA14120006)	Administrators)				
	Add	Remove			
Permissions for MSSQLSERVER	Allow	Deny			
Full control	V				
Read Special permissions					
For special permissions or advanced click Advanced.	d settings,	Advanced			
Learn about access control and per	missions				

Restart the SQL server after this.

If the certificate is still not displayed maybe this might help

 $\underline{http://thesqldude.com/2012/04/21/setting-up-ssl-encryption-for-sql-server-using-certificates-issues-tips-tricks/}$

https://www.mssqltips.com/sqlservertip/3299/how-to-configure-ssl-encryption-in-sqlserver/

Select the Server certificate and click on OK

a Sql Server Configuration Manager	<i>,</i> • • • • • • • • • • • • • • • • • • •				
File Action View Help					
🗢 🄿 🙎 🖺 🙆 🛃					
 SQL Server Configuration Manager (Loca SQL Server Services SQL Server Network Configuration (3 SQL Server Network Configuration (3) 	al) i2bit)	Protocol Name Shared Memory	Status Enabled Disabled		
SOL Server Network Configuration	Protocols for MSSQLSERVER	Properties	_?_	<u> </u>	
- Protocols for MSSQLSERVER	Flags Certificate Advan	ced			
▷ .豊. SQL Native Client 11.0 Configuratio	Certificate:	View	Clear		
	DA14120006.GLOBAL.AVAYA.COM				
	Expiration Date	2/22/2017			
	Friendly Name				
	Issued By	com, avaya, ap	ac, ccms, ccms-SAN		
	Issued To	IN, Maharasht	ra, Pune, Avaya Indi		

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

Add or Remove Snap-ins	tions
You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.	
Available snap-ins: Selected snap-ins:	
Snap-in Vendor Console Root Edit Extensions	
ActiveX Control Microsoft Cor	
Certificates snap-in	×
Component Services Microsoft C	
Computer Managem Microsoft C This snap-in will always manage certificates for:	
Bevice Manager Microsoft C My user account	
Disk Management Microsoft ar O Service account	
Folder Microsoft C Computer account	
🗐 Group Policy Object Microsoft C	
Participation Information Microsoft Co	
P Security Monitor Microsoft C	
B IP Security Policy M Microsoft C	
Description:	
The Certificates snap-in allows you to br	
< Back Next > Cance	
	······

Select Import

🛅 Console1 - [Console Root	Certificates (Local (Computer)\Tru	sted Root Certification	Authorities\C
🚠 File Action View Fa	vorites Window	Help		
🗢 🔿 🖄 📰 🗎 🗖	📑 📘			
🧮 Console Root		Issued To	*	Issued By
a 🙀 Certificates (Local Cor	nputer)	300815fee	0	300815feex
Personal		300815cip1	-	300815cip1
a 📔 Trusted Root Certi	fication Authorities	200815-in1	•	200815-5-1
Certificat				3008135101
Enterprise Tre	All Tasks	•	Import	Add I rust E
Intermediate	10		ted Authentication	- Avaya Trust
Trusted Public	View	•	ptCA	AvayaITRoc
Untrusted Ce	New Window from	Here	tCA	AvayaITroo
Third-Party R	New Taskpad View		tCA	AvayaITroo
Trusted Peop	New Taskpad View		tCA	AvayaITroo
Other People	Refresh		tCA2	AvayaITroo
PC-Doctor, Ir	Export List		tCA2	AvayaITroo
Remote Desk			verCA	AvayaITroo
Certificate Er	Help		LyberTrust Root	Baltimore C
. 🖴 o i o italia	10 1		a.	

Select the certificate

Certificate Import Wizard
File to Import Specify the file you want to import.
File name:
C:\OpenSSL-Win32\certnew_ca.cer Browse
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange-PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
< Back Next > Cancel

Select trusted root certificate authority

Certificate Import Wizard	x
Certificate Store Certificate stores are system areas where certificates are kept.	
Windows can automatically select a certificate store, or you can specify a location for the certificate.	
Automatically select the certificate store based on the type of certificate Place all certificates in the following store	
Certificate store:	
Irusted Root Certification Authorities Browse	
Learn more about <u>certificate stores</u>	
< Back Next > Cancel	

Select finish.

Certificate Import Wizard		×		
	Completing the Certificate Import Wizard			
	The certificate will be imported after	r you dick Finish.		
	Certificate Store Selected by Use	Trusted Poot Certifica		
	Content	Certificate		
	File Name	C:\OpenSSL-Win32\ce		
	•	4		
	< 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.

Name clb.dll clbcatq.dll clbcatq.dll cleanmgr.exe cleansgr.exe clfsw32.dll	Date modified Type Size 7/14/2009 6:45 AM Application extens 14 KB 7/14/2009 6:45 AM Application extens 510 KB 7/14/2009 6:44 AM Application 208 KB
 cliconfg.dll cliconfg.exe cliconfg.rll 	General Alias DB-Library Options Network Libraries
 clip.exe clspack.exe clusapi.dll cmcfg32.dll cmd.exe cmdial32.dll CMDIALOG.SRG 	Disabled protocols: Enabled protocols by order: Named Pipes TCP/IP
cmdkey.exe cmdl32.exe cmicryptinstall.dll cmifw.dll cmipnpinstall.dll	Force protocol encryption Enable shared memory protocol

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 Diatabase		
Server name:	CEDEMC186.ccms.apac.avaya.com	C
User name:	ASMSControl	F
Connection string:	Data Source=CEDEMC186.ccms.apac.avaya.com;Initial Catalog=A	3
🔽 Save empty UUI a	and collected digits	
Contact Database		
Server name:	CEDEMC186.ccms.apac.avaya.com	C

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 144C4D11CBAB0CAFEC33B6C647D596053090F8905637A5EE4573CCE0CEFE51AAE5709C0EA07BA77 8B483ED52D801E5C02F8B2AAEEE3635C0FE666665B26F0A93C3E8A4CDFD9D9F79139357A236942E5 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.

Options	— ×-			
Communicator Dashboard Directory Email	HTML Editor IDS View Client			
Database				
Database server name	cedemc186.ccms.apac.avaya			
Database name	ASContact			
Database user name	ASContact			
Database user password	•••••			
Columns Displayed				
Column display ID	1 •			
Get Column Display IDs				
⊂ Initial Default Search				
Enable initial default search				
Default search criteria				
History Search				
Enable Show History	Enable Docking on Show History			
OK	Cancel Apply			

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 Service	Reporting Services Configuration Manager: CEDEMC186\MSSQLSERVER			
Microsoft SQL Server 2008 Reporting Services Reporting Services Configuration Manager				
Sonnect	Report Manager URL			
CEDEMC186\M	Advanced Multiple Web City Configuration Add a Report Manager SSL Binding			
🛃 Service Ac	Identification			
🧀 Web Servi	Multiple SSL Port 443			
🗍 Database	IP Adc All Assi Certificate Cedemc186.ccms.apac.avaya.com	_		
🎯 Report Ma	UHL http://cedemc18b.ccms.apac.avaya a.com:443/Re			
🚖 E-mail Sett	OK Cancel			
Execution Multiple SSL Identities for Report Manager				
Encryption	IP Address SSL Port SSL Certificate Issued To (All IPv4) 443 cedemc186.ccms.a cedemc186.ccms.a			
📇 Scale-out (
	Add Remove Edit			
	OK Cancel			



Option	s	×
World	d clock Communicator Dashboard	Directory Email Reporting HTN
Report Server Task Director	Report Server Connection Details Report Server Scheme Report Server Address Report Service Url Report Web Service Url Report Generation Timeout (Second: User name Password Domain	https:// cedemc186.ccms.apac.avaya.com ReportServer ieportServer/ReportService2005.asmx s) 600
	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.