Avaya Solution & Interoperability Test Lab

Application Notes for configuring Transport Layer Security (TLS) with 3rd Party Certification Authority Certificates and Secure Real-Time Transport Protocol (SRTP) on Avaya Aura Contact Center 6.3 Service Pack 10 - Issue 1.0

Abstract

These Application Notes describe the steps to configure Avaya Aura® Contact Center 6.3 to use Transport Layer Security and 3rd party Certification Authority certificates in situations where default Avaya certificates must be replaced. The default product identification certificates and trusted root certificates are replaced with versions signed by customers own Certification Authority servers or by 3rd party Certificate Authority servers. In addition, Avaya Aura® Contact Center is configured to use Secure Real-time Transport Protocol to encrypt media transmissions between Avaya Aura® Contact Center elements and other telecommunications equipment. These application notes are intended for customers who intend to replace default Avaya supplied certificates in a high security networked environment, and who wish to secure signaling and encrypt voice.

Information in these Application Notes has been obtained through Solution Integration compliance testing and additional technical discussions. Testing was conducted at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the configuration of Avaya Aura® Contact Center with Transport Layer Security (TLS) using 3rd party Certificate Authority (CA) certificates and Secure Real-time Transport Protocol (SRTP). TLS certificates are used to validate a servers' identity prior to initiating secure network transactions, SRTP secures media streams from eavesdropping. Default TLS certificates certified by Avaya are initialized in Avaya Aura® Contact Center servers at software installation time, these Application Notes describe how to replace default certificates with new certificates signed by a 3rd party certification service.

There are two kinds of default certificate installed in Avaya Aura® Contact Center servers:

- Root certificates issued by Avaya which are from a trusted root CA.
- Product Identification Certificates signed by Avaya's trusted root CA.

Root Certificates are digital certificates issued by a trusted organization (e.g., VeriSign or Entrust) which initiate a "chain of trust" by signing intermediate CA certificates using a cryptographic digital key. Certificates lower down the chain inherit the trustworthiness of the root CA. Avaya Aura® Contact Center products contain a default Avaya root CA certificate (technically an intermediate root certificate) which can be verified by comparing the public key of the Avaya CA certificate against a locally held copy of the root CA certificate (i.e., VeriSign or Entrust certificate).

Product identification certificates are initialized at software install with values which uniquely identify the endpoint offering the certificate and are signed by the Avaya root CA service. TLS sessions use a client-server model. Clients (i.e., devices requiring a service) contact a server and are offered an identity certificate as proof of the server's integrity. Clients verify the offered certificate by testing authenticity with a common trusted root CA certificate. If successfully authenticated; the client and server commence negotiations on an encryption scheme, and if successful, transmission is secured from that point on. This is the standard model used by Internet browsers when contacting an unknown WWW server when security must be negotiated. TLS protocol allows for servers to request a certificate from a client and will authenticate it using a trusted root CA certificate. This is known as Mutual Authentication and is preferable to one-way authentication as it prevents unauthorized hosts obtaining services.

Mutual authentication requires the same root CA certificate be installed on both server and client and if default Avaya product certificates are replaced with 3rd party certificates, both the Avaya product identification certificate and the Avaya trusted root CA certificate must be replaced. Note, servers can have only offer one identity certificate, but may have several trusted root CA certificates. For enhanced security, only install a single trusted root CA certificate and ensure mutual authentication is activated.

SRTP is a variation of the standard RTP protocol with enhancements to provide message authentication and encryption, adding a layer of security to RTP. STRP requires endpoints to agree on a cryptographic algorithm and to exchange keys prior to commencing transmission.

Once secured, transmission is protected from replay attacks and alteration by unapproved sources. SRTP is independent of TLS; both are often used when Voice over Internet Protocol (VoIP) transmissions must be secured over an unknown network.

SRTP used the AES cipher to encrypt and decrypt messages and the HMAC-SHA1 algorithm to authenticate the message and protect its' integrity.

2. General Test Approach and Results

Avaya Aura® Contact Center is available in several configurations, interfaces with many telecommunications systems and works on both customer supplied hardware and virtualized platforms. These Application Notes can be used to install TLS certificates and enable SRTP in installations which use Session Initiation Protocol (SIP) for telecommunications signaling and Real-time Transport Protocol (RTP) for voice transmissions. .

Avaya Aura® Contact Center offers a suite of applications for voice and multimedia contact processing, agent handling, management and reporting, networking and third-party application interfaces. These high-level functions may be deployed on a single server (real or virtual) or on several servers. Each AACC server requires a unique identity certificate, but share a common root CA certificate. Where a server has multiple functions (e.g., provides Web Services, SIP telephony and auxiliary functions) it may present a unique identity certificate for each function.

These application notes focus primarily on securing SIP telephony communications with TLS and SRTP in an AACC environment. Securing server management functions (e.g., web management) are also presented where it is preferable to further enhance security.

Intended users of these Applications Notes should be familiar with AAAC installations procedures and necessary operating procedures. It is desirable to carry out these procedures during an maintenance window as some procedures require restarting services and functions which may impact service on live sites. When services may be affected, this will be highlighted in the text.

2.1. Test Description and Coverage

Test cases included calls between Communication Manager stations and AACC agents; using Secure SIP (SIPS) signaling and SRTP for media. CTI integration with AACC was tested with AES converting TR/87 messages into DMCC protocol and controlling SIP telephones used as AACC agent endpoints. A suite of traditional telephony operations and features such as extension dialing, hold/resume, transfer (supervised and unsupervised) and conferencing were tested

2.2. Test Results and Observations

All test cases were successful.

3. Reference Configuration

Figure 1 illustrates an example Avaya Aura® Contact Center installation. In this model, three AACC components Contact Center Manager Server (CCMS), Contact Center Manager Administration (CCMA) and Communication Control Toolkit (CCT) are installed co-resident on a single server (CCMS/CCMA & CCT #1). A fourth function, Contact Center Multimedia (CCMM #1) is installed in a separate server. AACC servers require Microsoft Windows Server 2008 R2 for the operating system.

A fifth AACC component, Avaya Media Server, is also present and installed on a server running the Linux operating system (Linux is required for High availability operation, otherwise AMS can be installed on a Windows 2008R2 server or as a co-resident installation with other AACC functions.

Servers enclosed in the solid box are mirrored in the dashed box, indicating this is a High Availability AACC installation. Each server has a hostname which uniquely identifies it on the network. Typically, the server identity certificate contains the hostname as the key element. Avaya Aura® Agent Desktop's (AAAD's) are configured to use TLS when communicating with AACC; AAAD TLS configuration is outside the scope of these Application Notes.

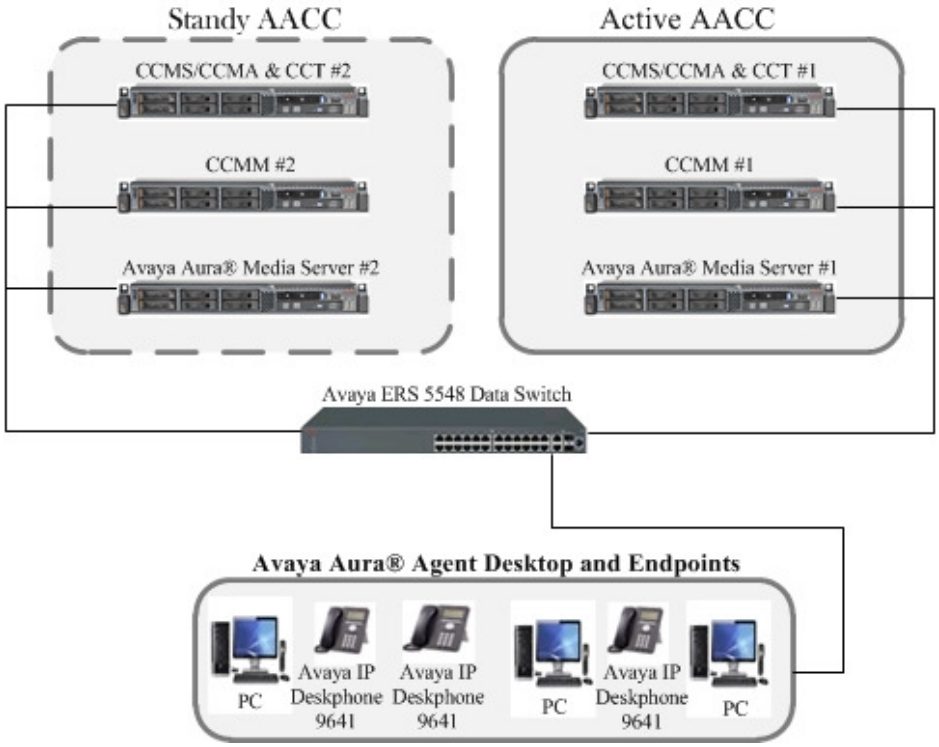


Figure 1: High Availability AACC installation

4. Equipment and Software Validated

The following equipment and software were used for the reference configuration

Equipment/Software	Release/Version
Avaya Aura® Contact Center Manager Server running on a Dell Poweredge R610	AvayaAura_CCMS_6.3.210.0-0677_ServicePack AvayaAura_CCMS_6.3.210.1-1084_Patch AvayaAura_CCMS_6.3.210.500-0156_Patch AvayaAura_CCMS_6.3.210.501-1098_Patch
Avaya Aura® Contact Center Manager Administration running on a Dell Poweredge R610	AvayaAura_CCMA_6.3.210.0-0716_ServicePack AvayaAura_CCMA_6.3.210.1-0689_Patch
Avaya Aura® Contact Center Communication Control Toolkit running on a Dell Poweredge R610	AvayaAura_CCT_6.3.210.0-0644_ServicePack AvayaAura_CCT_6.3.210.1-0300_Patch
Avaya Aura® Contact Center Manager Multi Media	AvayaAura_CCMM_6.3.210.0-0670_ServicePack AvayaAura_CCMM_6.3.210.1-0481_Patch
Avaya Media Server running on a Dell Poweredge R610	Avaya Media Server - v.7.5.0.1014 Contact Center Services for AMS - v.6.3.0.113 Linux version 2.6.18-194.el5PAE (mockbuild@x86-007.build.bos.redhat.com) (gcc version 4.1.2 20080704 (Red Hat 4.1.2-48)) #1 SMP Tue Mar 16 22:00:21 EDT 2010

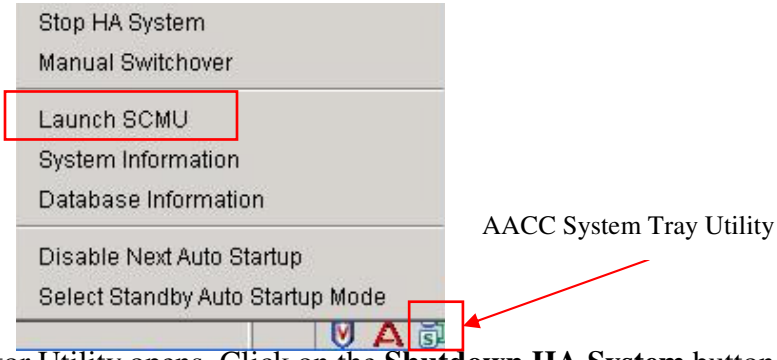
5. Configure SIP 3rd Party Certificates on CCMS

Replacement of default Avaya certificates with 3rd party certificates is a multi-step operation, involving the generation of a certificate signing request (CSR), exporting the CSR to a root CA server, signing the CSR and re-importing it back into the source together with the root CA certificate. Services need to be halted prior to certificates operations, in a HA installation, perform this procedure on the inactive CCMS, swap servers and repeat the procedure.

5.1. Logon to AACC and Stop Services

- Logon to the CCMS/CCMA/CCT server using Administrator credentials.
- Click on the **Start** button, and then click on **All Programs**.
- Click on **Avaya**, then **Contact Center**.
- Click on **Common Utilities**, then **System Control and Monitor Utility** (highlighted in the following screenshot).

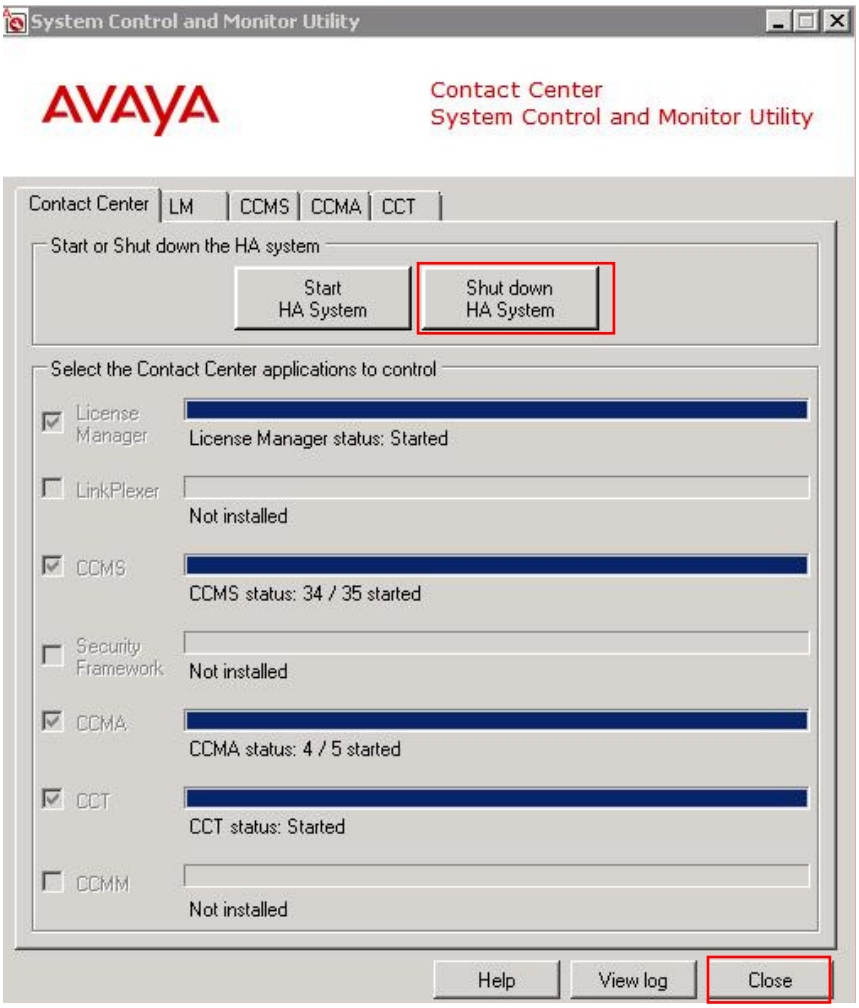
Alternatively, right click on the system tray icon & select **Launch SCMU**.



The System Control and Monitor Utility opens. Click on the **Shutdown HA System** button.

This action shuts down all services. This may take several minutes, progress indication is provided.

When all services are shutdown, click on the **Close** button.



Using Windows Explorer, navigate to the following folder:

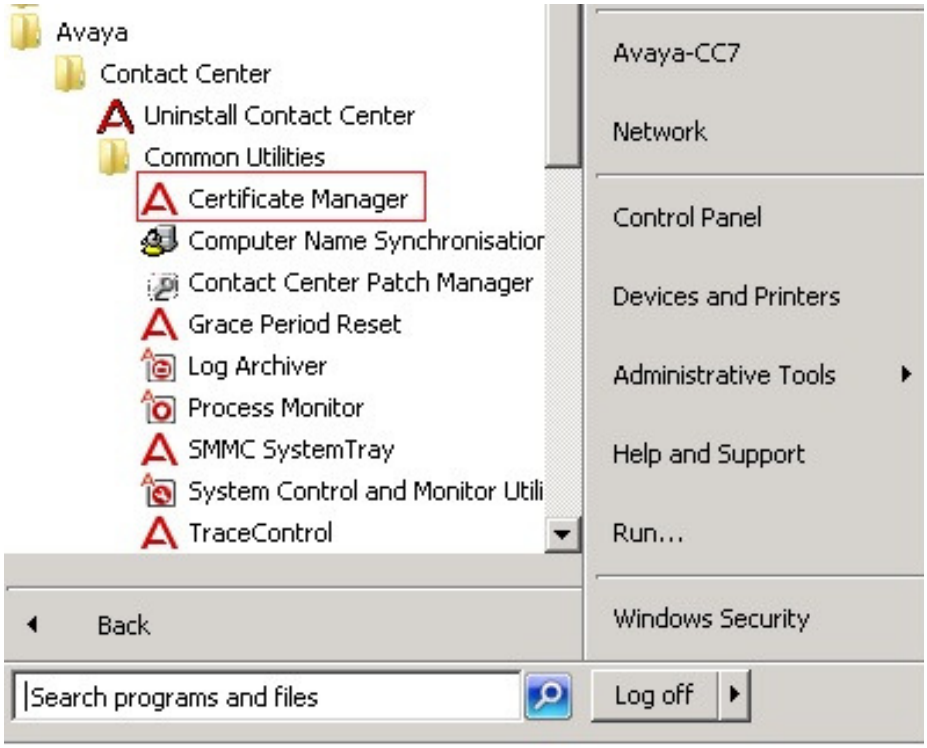
D:\Avaya\Contact Center\Manager Server\iccm\sgm\TLSCertificates

Delete or rename any files in this folder, or move them to another folder if preferred. When completed, proceed to the next section.

5.2. Generate a SIP-TLS Certificate Signing Request

This section describes the steps for configuring 3rd party certificates on a CCMS server. This procedure is only applicable to CCMS and certificates are for secure SIP telephony.

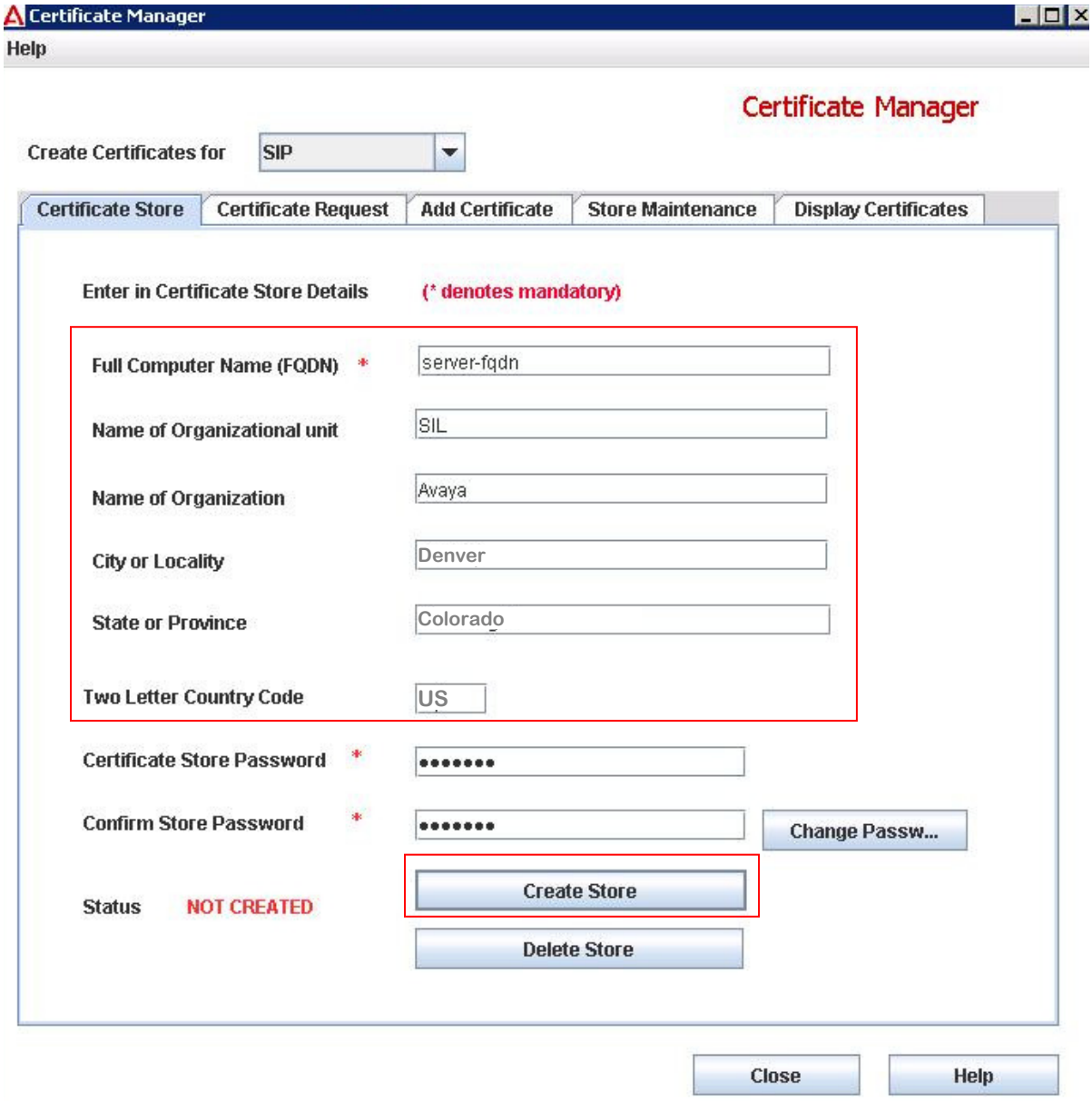
- Click on the **Start** button, and then click on **All Programs**.
- Click on **Avaya**, then **Contact Center**.
- Click on **Common Utilities**, then **Certificate Manager** (highlighted in the following screenshot).



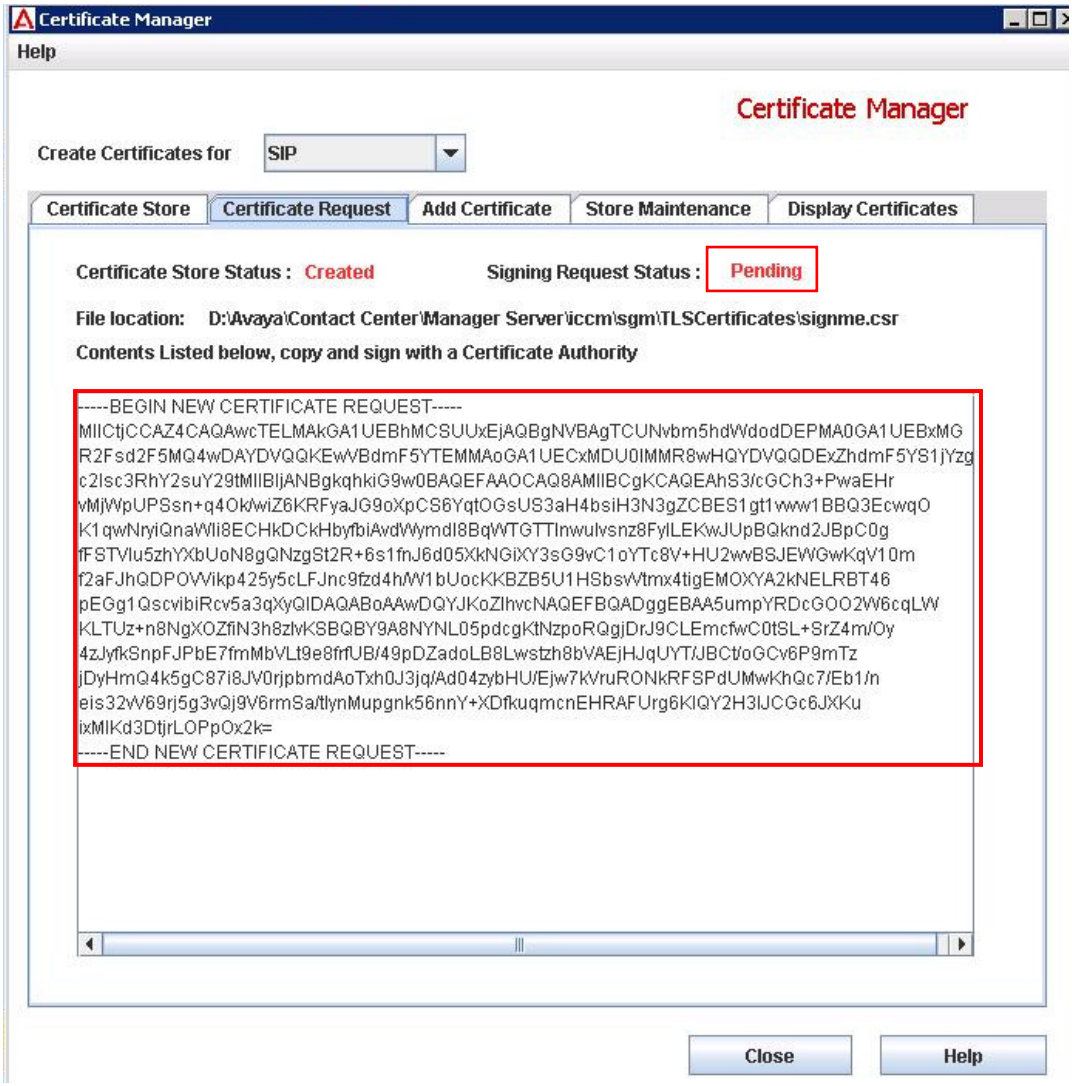
The Certificate Manager application launches and presents a logon screen, enter the Certificate Manager password (ask the systems administrator for this). A successful logon shows the following screen.

Enter the certificate details as show in the enclosed area. Only the server FQDN will be populated by default. Do not change the Certificate Store Password unless instructed to do so by the systems administrator.

Click on the **Create Store** button to setup a new certificate store.



When a new certificate store is created, a certificate signing request is generated. The signing request is the first step in creating an identity certificate for CCMS. Click on the **Certificate Request** tab, the following screen opens.



The **Signing Request Status** will be **Pending**. Copy the text from the **Certificate Request** window (inside the large red box) and paste this into a text editor, save the file as **ccms.csr**. Ensure you copy all of the text in the highlighted area.

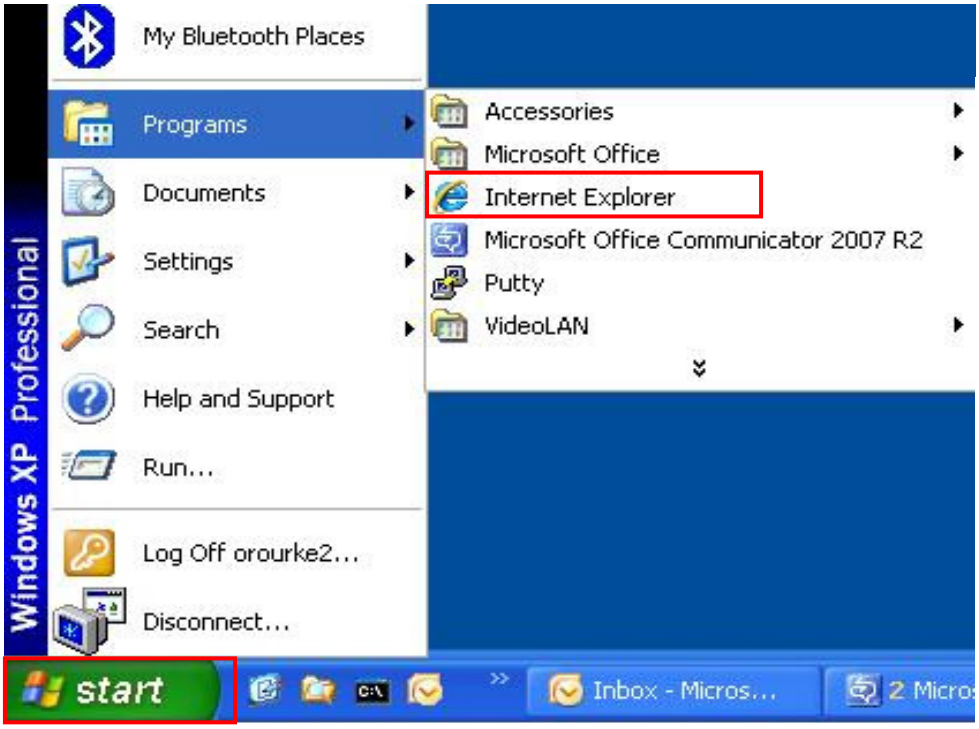
The certificate signing request will need to be imported into a Root Certificate Signing Authority server, signed and exported back as a signed certificate file, which will be installed in the CCMS server certificate store.

5.3. Login to the root Certificate Signing Authority, sign the CSR

This example will use a root Certificate Authority running on a Microsoft Windows 2008 server. It is assumed the Certificate Authority has been correctly configured with the required Certificate templates installed for Avaya Aura® Contact Center operation. For information on how to setup certificate templates, see **Section 12 item [5]**.

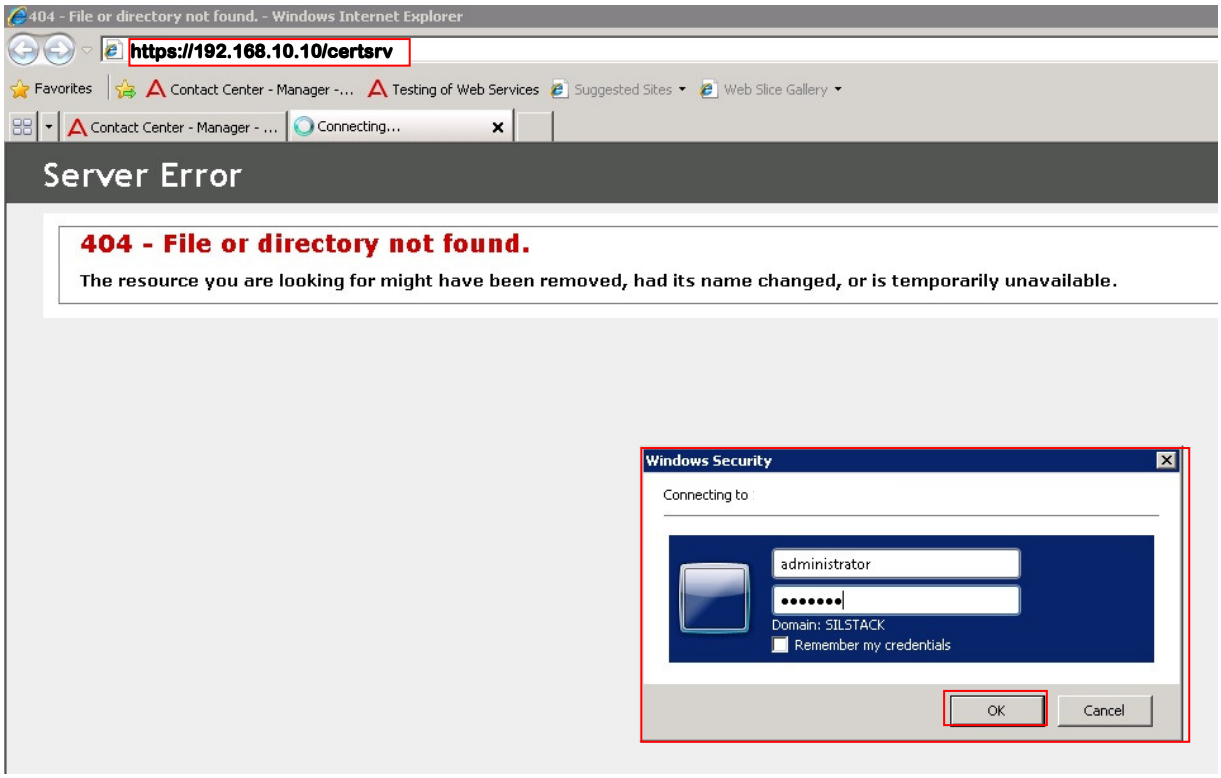
CSR's may be submitted to the Microsoft Certificate Authority server using a web browser (e.g., Microsoft Internet Explorer). The user must have valid domain username and password to access the Certificate Authority.

On the CCMS/CCMA/CCT server, click on the **Start** button, then **Programs**, then **Internet Explorer**.



A new web browser windows opens, type the address of the Microsoft Certificate Authority server in the browser address bar, typically **'https://192.168.10.10/certsrv'** and hit **Return.**.

If you have not logged in previously, an access error occurs and you are required to enter your login credentials in a Windows Security dialog box. Press the **OK** button when ready.



A new web page opens.

Click on **Request a certificate** (not shown).

Then click on **Advanced Certificate Reques**t (not shown).

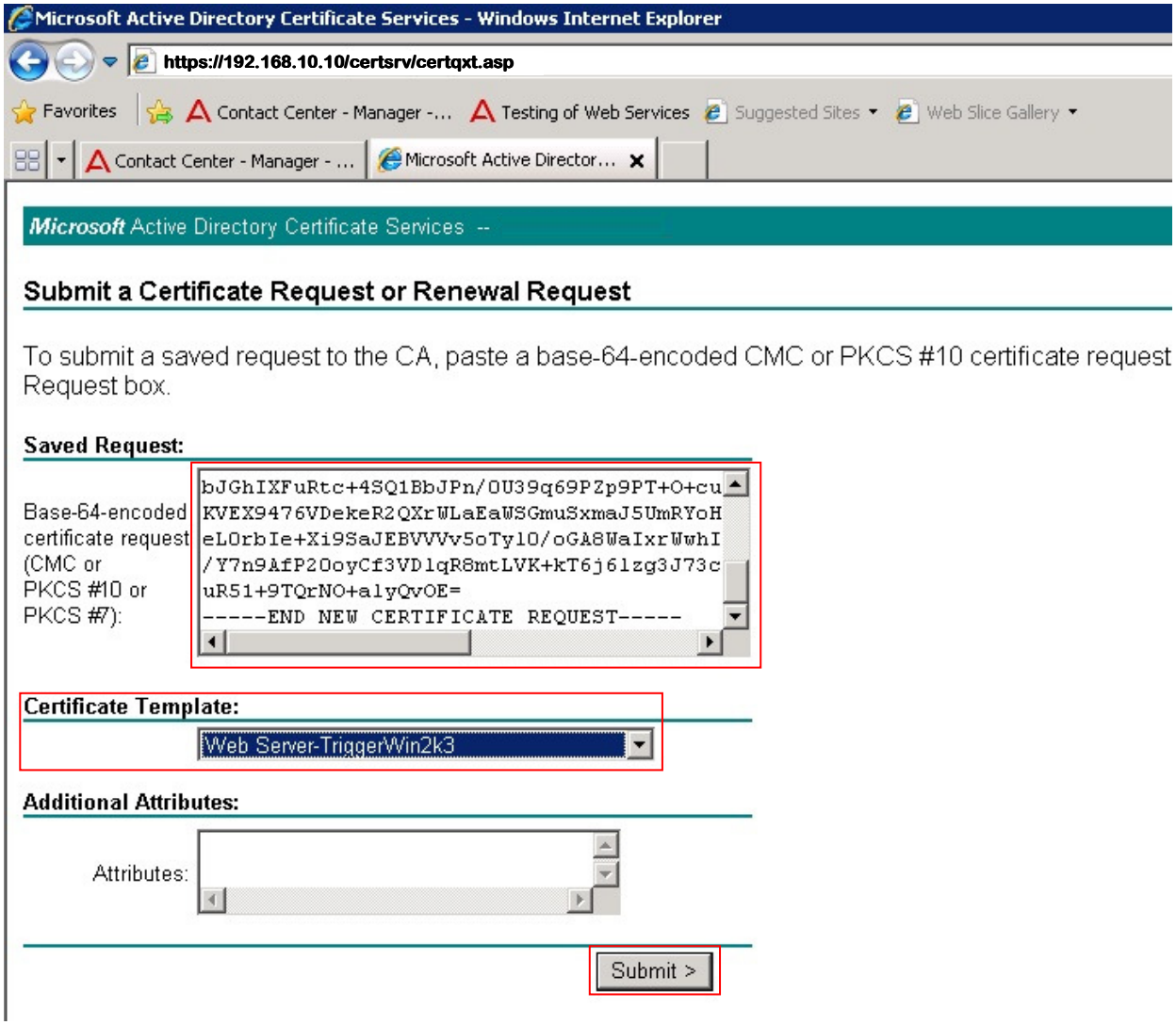
Finally, click on **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file**. (not shown).

A new web page opens.

Open the saved certificate signing request (file **ccms.csr** from **Section 5.2**) using a text editor (e.g., Microsoft Notepad or equivalent). Copy all of the text in the Notepad window and paste it into the **Saved Request** input area (highlighted in red in the following screenshot).

In the **Certificate Template** drop down menu (highlighted), ensure you select the correct Certificate Template for your server. If in doubt, contact your Systems Administrator.
For more information on generating certificate templates, see **Section 12 item [5]**.

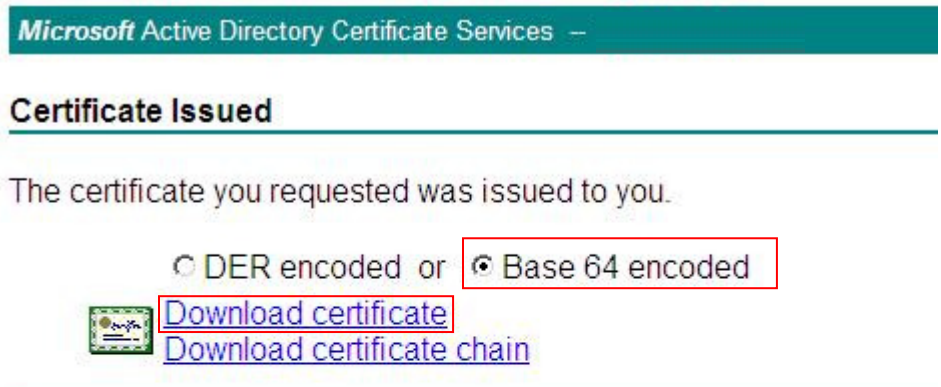
When ready, press the **Submit >** button.



The certificate signing request is validated and converted into a signed certificate which will be used to confirm the identity of the CCMS server when TLS is used. The signed certificate must be downloaded from the root Certificate Authority server. Multiple download options and formats are available.

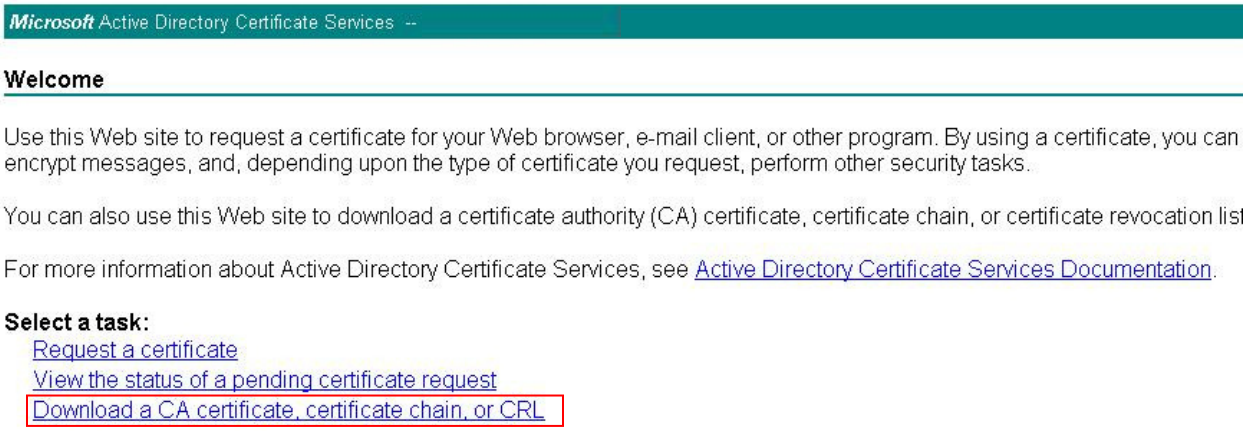
After successful validation and certificate signing by the Microsoft Certificate Authority server, a new web page will open (see below).

Select the **Base 64 encoded** radio button and click on the **Download certificate** hyperlink. Save the file with a new name, e.g., save as "**certCCMSsigned**".



While logged into the Certificate Signing authority server, download the root CA certificate which is required to validate certificates offered by other servers during TLS handshakes.

Click on the **Home** button in the page top right corner (not shown) to return to the main page. Click on the **Download a CA Certificate, certificate chain or CRL** hyperlink. In the new page (not shown), select the **Base 64** radio button and click on the **Download CA Certificate** link. Save the certificate with a new name, e.g., "**rootCAcert**".

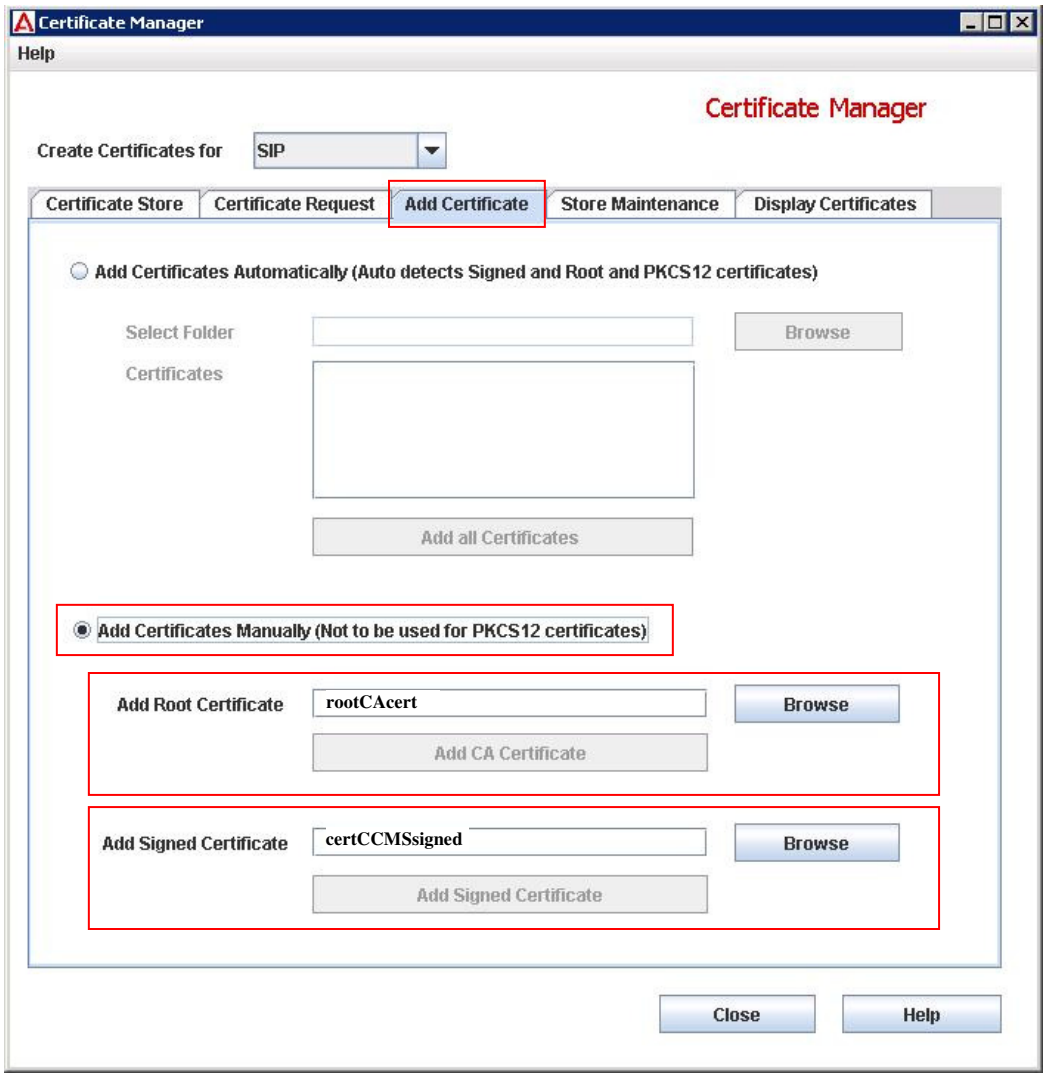


5.4. Install Certificates on CCMS server

Login to CCMS/CCMA/CCT Certificate Manager as in **Section 5.1**, click on the **Add Certificate** tab (third tab from left). The following screen is shown.

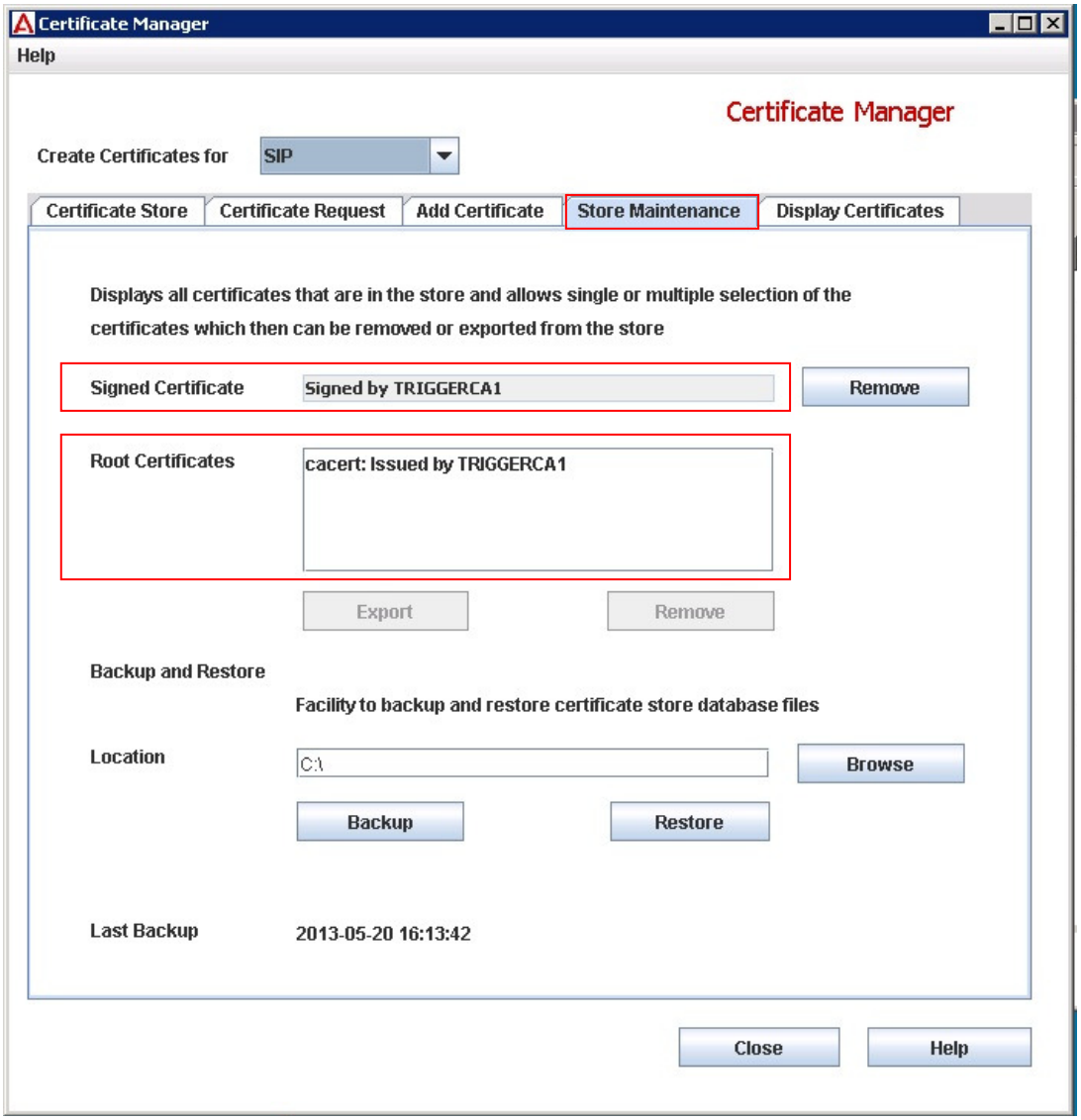
Click the **Add Certificates Manually (not to be used for PKCS12 certificates)** radio button. In the **Add Root Certificate** section, click the **Browse** button to navigate to the root CA certificate. Click the **Add CA Certificate** button to load it.

In the **Add Signed Certificate** section, click the **Browse** button to navigate to the Signed product identity certificate. Click the **Add Signed Certificate** button to load it.



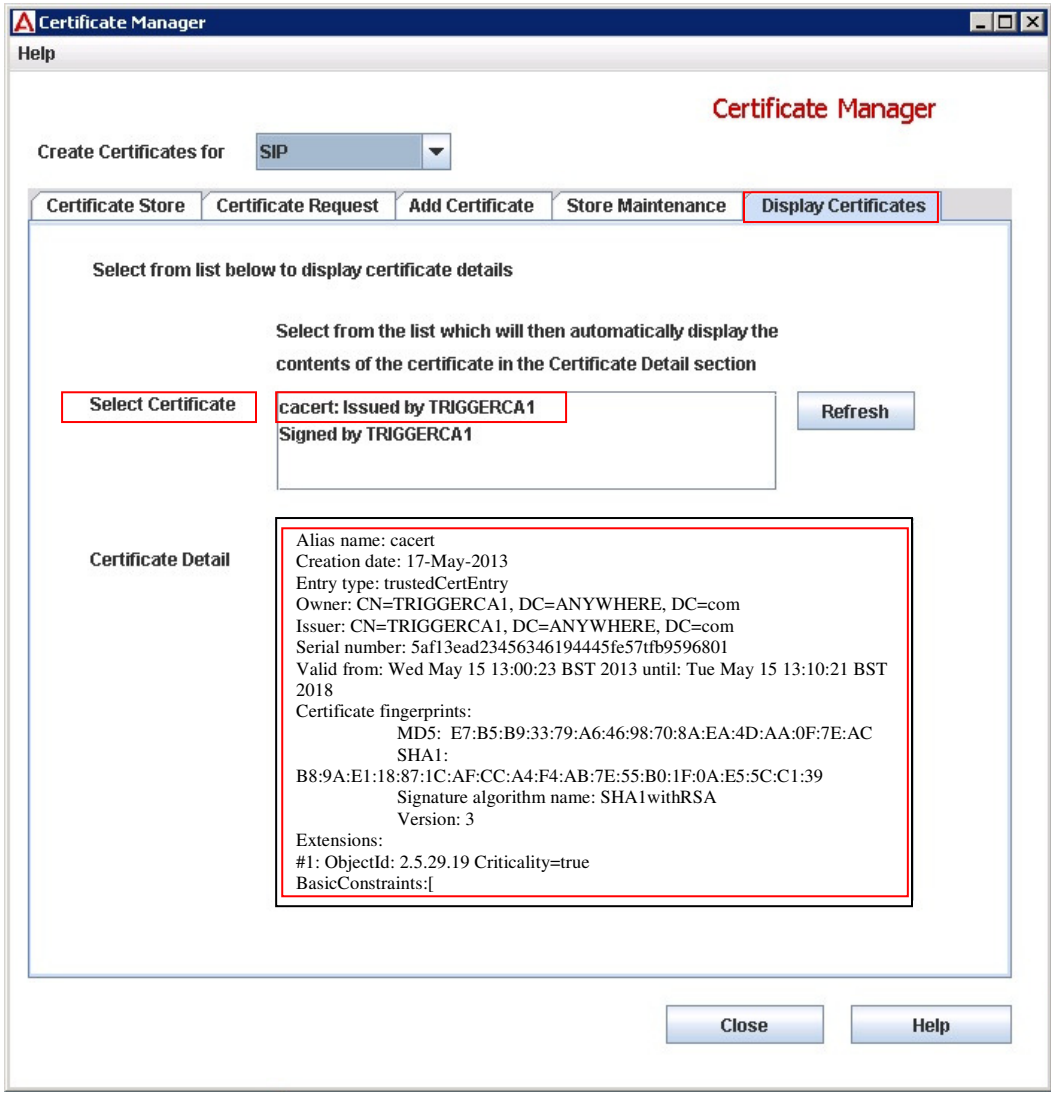
To confirm the certificate have been loaded correctly, click on the Certificate Manager **Store Maintenance** tab (4th from left). A screen similar to that below will display the recently loaded certificates.

Ensure the **Signed Certificate** entry is signed by your root CA authority and the root CA certificate in the **Root Certificates** area was issued by your root CA server.



To confirm certificate details, click on the Certificate Manager **Display Certificates** tab.
To display a certificate's information, click on the certificate name in the **Select Certificate** area, the certificate details will show up in the **Certificate Detail** area.

In the example below, the root CA certificate details are shown.



5.5. Logon to AACC and Start Services

Repeat the logon procedure in **Section 5.1**; press the **Start HA System** button on the SCMU. This action starts up all services. This may take several minutes, progress indication is provided.

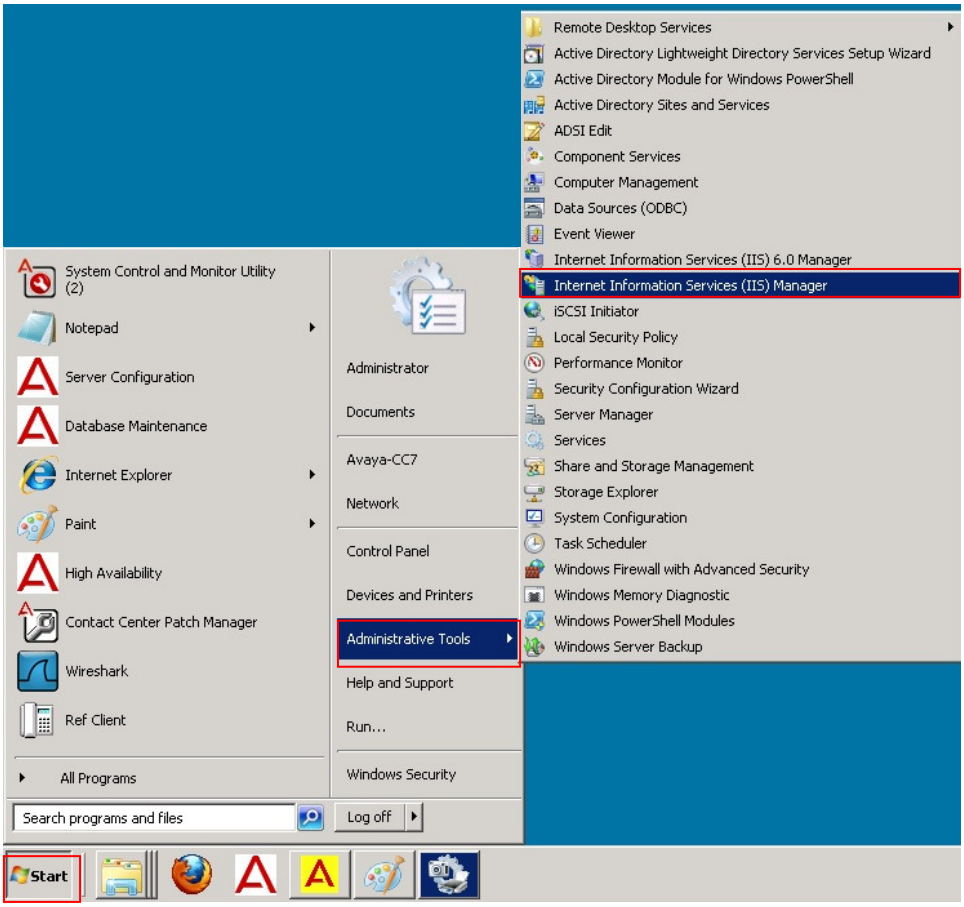
When all services are up, click on the **Close** button.
If using a HA installation, swap the active/standby servers and repeat **Section 5.1** through **Section 5.5**.

6. 3rd Party IIS Certificates on CCMS/CCMA/CCT/CCMM

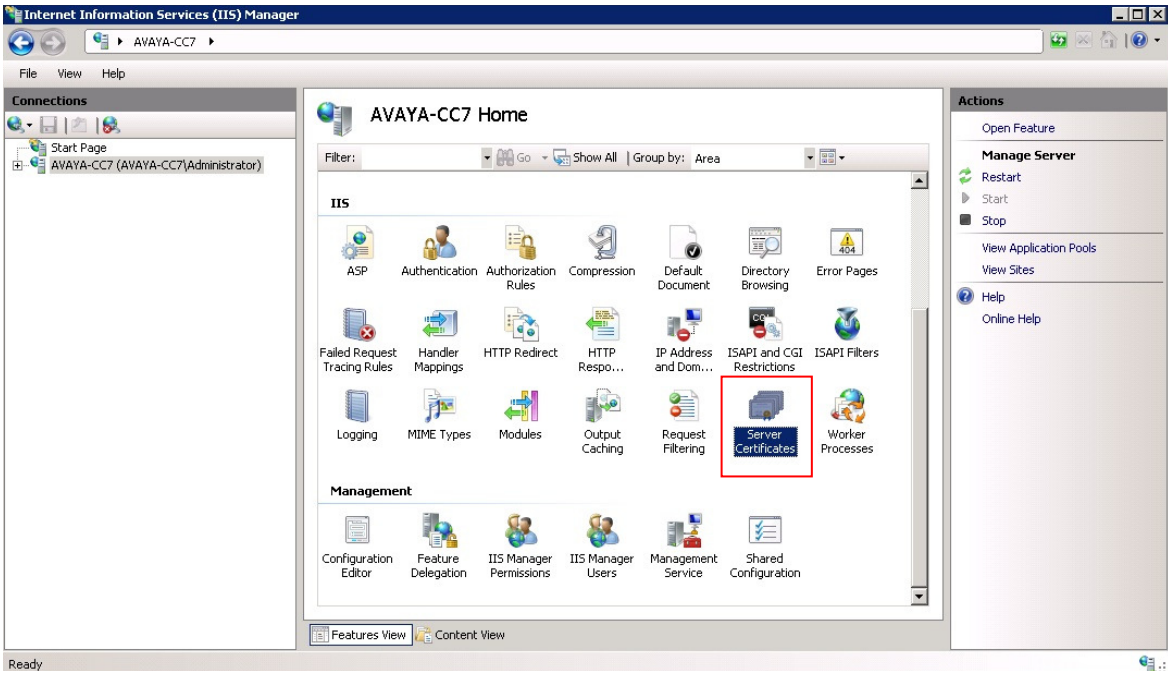
Procedures in **Section 5** detailed installation of 3rd party SIP certificates for CCMS telephony operations; 3rd party certificates are also required for Microsoft Internet Information Services (IIS) used by AACC (e.g., AACC web administration). The following procedures cover the installation of 3rd party certificates for IIS. Installation procedures are the same for CCMS/CCMA/CCT & CCMM servers and all servers should be configured with a unique identity certificate.

6.1. Generate a Certificate Signing Request for an Avaya Aura® Contact Center server

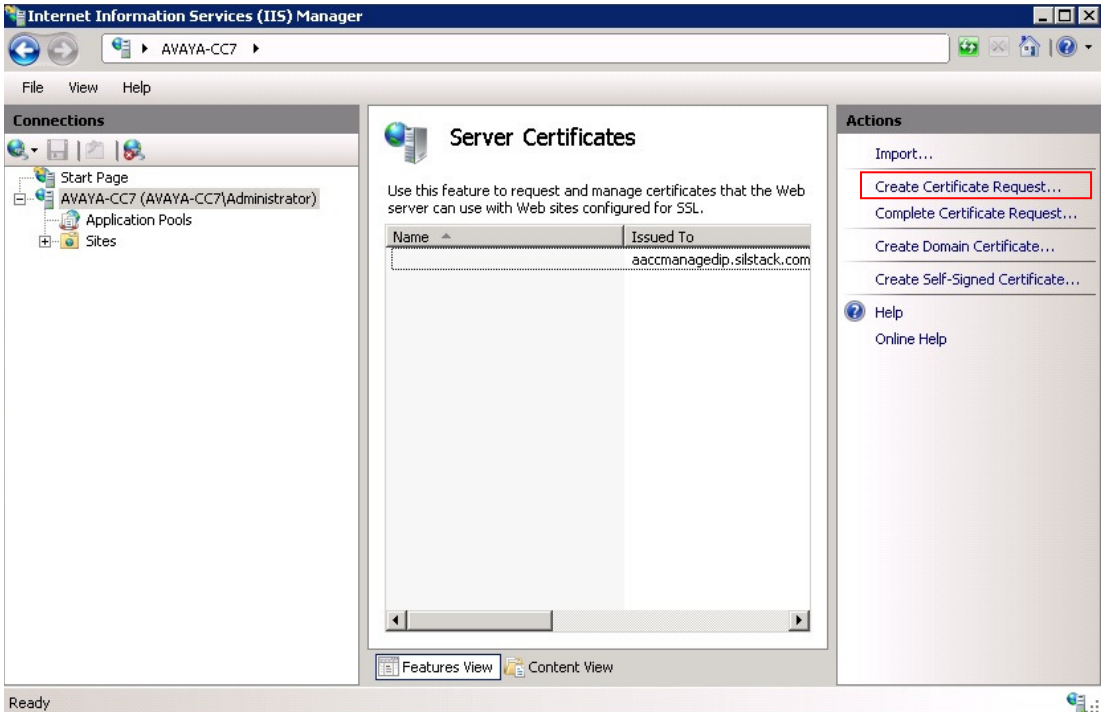
On the server, click on **Start → Administrative Tools → Internet Information Services (IIS) Manager**. The **Internet Information Services (IIS) Manager** window opens.



In the **Internet Information Services (IIS) Manager** window, search for the **Server Certificates** icon (highlighted). Double click the **Server Certificates** icon, a new window opens.



In the new window, click on **Create Certificate Request** (highlighted).

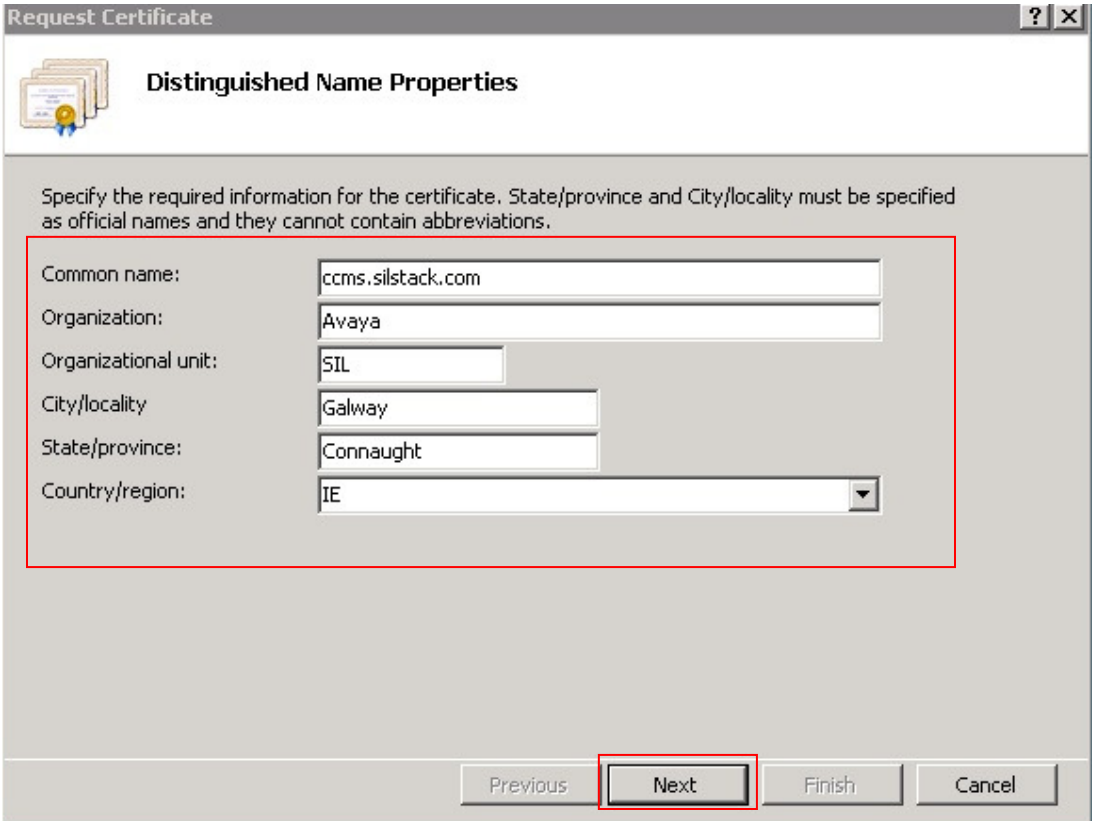


The **Request Certificate Distinguished Name Properties** dialog box opens (see below). Populate the highlighted areas with the server details:

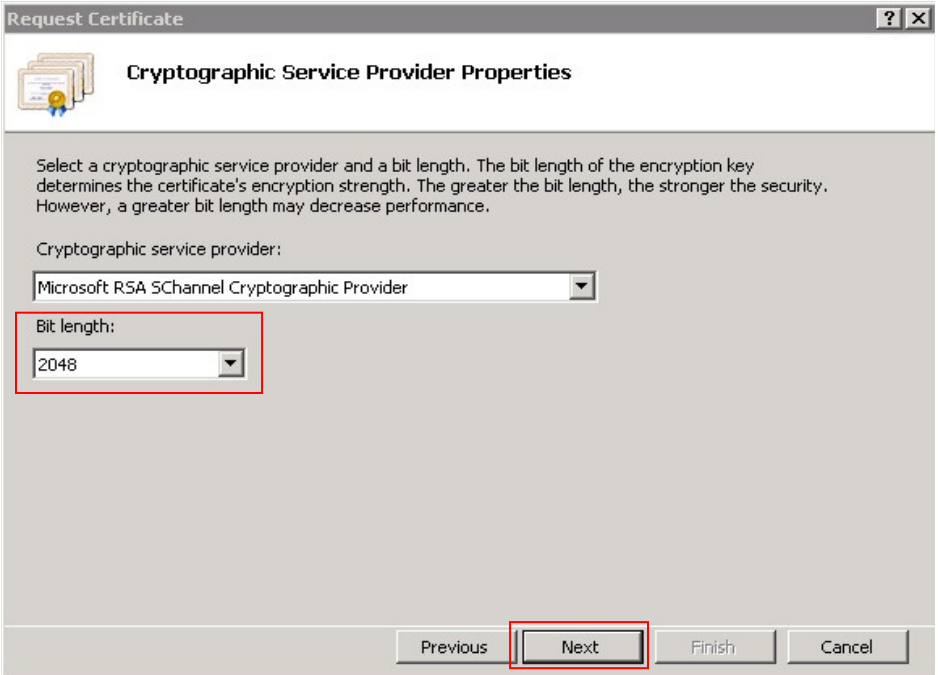
Common Name	(typically the server FQDN)
Organization	(usually company name)
Organization Unit	(department name)
City/locality	(municipal area where the server resides)
State/province	(sub region of country)

Select the correct **Country/region** from the drop down list.

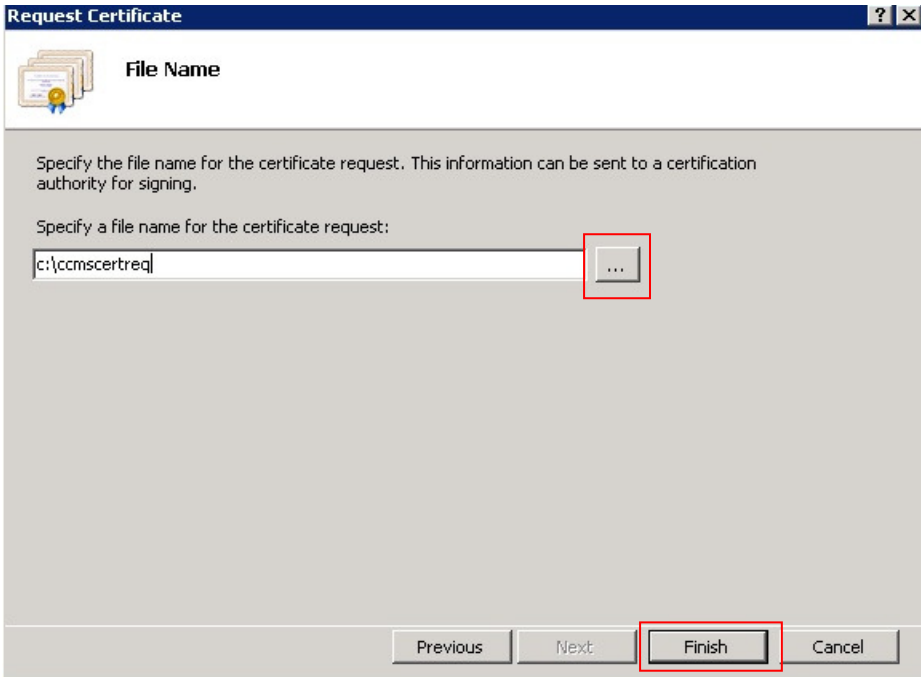
Ensure no property values are blank.
Click on the **Next** button when ready.



The **Request Certificate Cryptographic Service Provider Properties** dialog opens. Set the **Bit Length** value to **2048** and click the **Next** button.



The **Request Certificate File Name** dialog box opens. Click the highlighted **…** button, browse to a folder, select a filename or type a new one. Click on the **Finish** button when ready. This completes the certificate signing request operation.



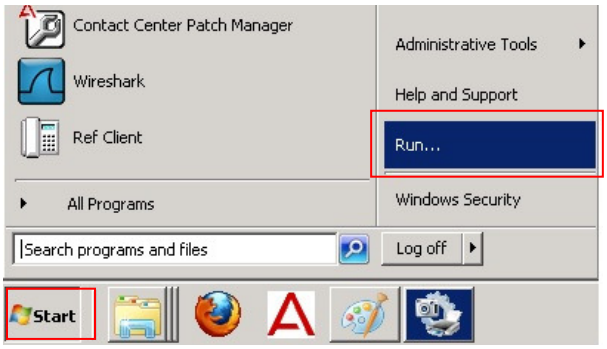
6.2. Sign an IIS Certificate Signing Request.

The IIS certificate signing request generated in **Section 6.1** must be signed by a root Certificate Authority before it can be imported. **Section 5.3** of this document shows how the SIP identity certificate may be signed using a web browser session to the root Certificate Authority server and the same procedure may be used to sign the IIS certificate signing request.

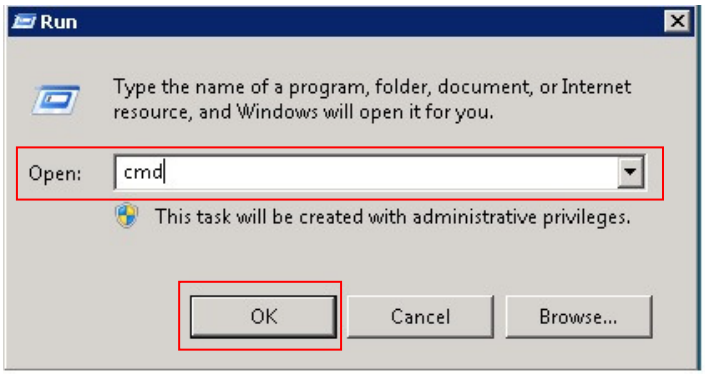
In the event a web session cannot be established with the root Certificate Authority server, an alternate certificate signing method is presented here. This gives the same results as the procedure in **Section 5.3**. This procedure requires the certificate signing request file to be copied from the Avaya Aura® Contact Center server to the root Certificate Authority server, either via file transfer protocols or USB keys.

Logon to the root Certificate Authority server and upload the IIS certificate signing request created in **Section 6.1**.

Click on the **Start** button, and then select **Run**.



A **Run** dialog box opens. In the **Open:** input field, type **cmd** and click the **OK** button.



A DOS window will open. Navigate to the folder which contains the IIS server certificate signing request file.

The command **certreq** will be used to complete the certificate signing procedure. Before commencing the certificate signing procedure, the following values must be known in advance:

CAHostName\CAName	This is the host and hostname of the root Certificate Authority server which will sign the request. A typical example would be **someserver.somwhere.com\rootCA**.
CertificateTemplate:	This is a unique template which will be used to apply the correct format and content to signed certificate requests. A typical name might be **ServerTemplate**.
Certifcate Request File	This is the certificate request copied/uploaded from the Avaya Aura® Contact Center server.

Obtain the first two values from your system administrator. When ready, type the following:

```
C:\>certreq -submit -config "someserver.somewhere.com\rootCA" -attrib "Certifica
teTemplate:ServerTemplate" yourCSR.csr_
```

The system will respond with the following if the request is processed successfully:

```
RequestId: 206
RequestId: "206"
Certificate retrieved(Issued) Issued
```

A standard file selector dialog box will open to permit saving the newly signed IIS server certificate. Save the certificate for later importation into CCMS/CCMA/CCT and CCMM.

This procedure can also be used to sign CCMS TLS certificate signing requests.

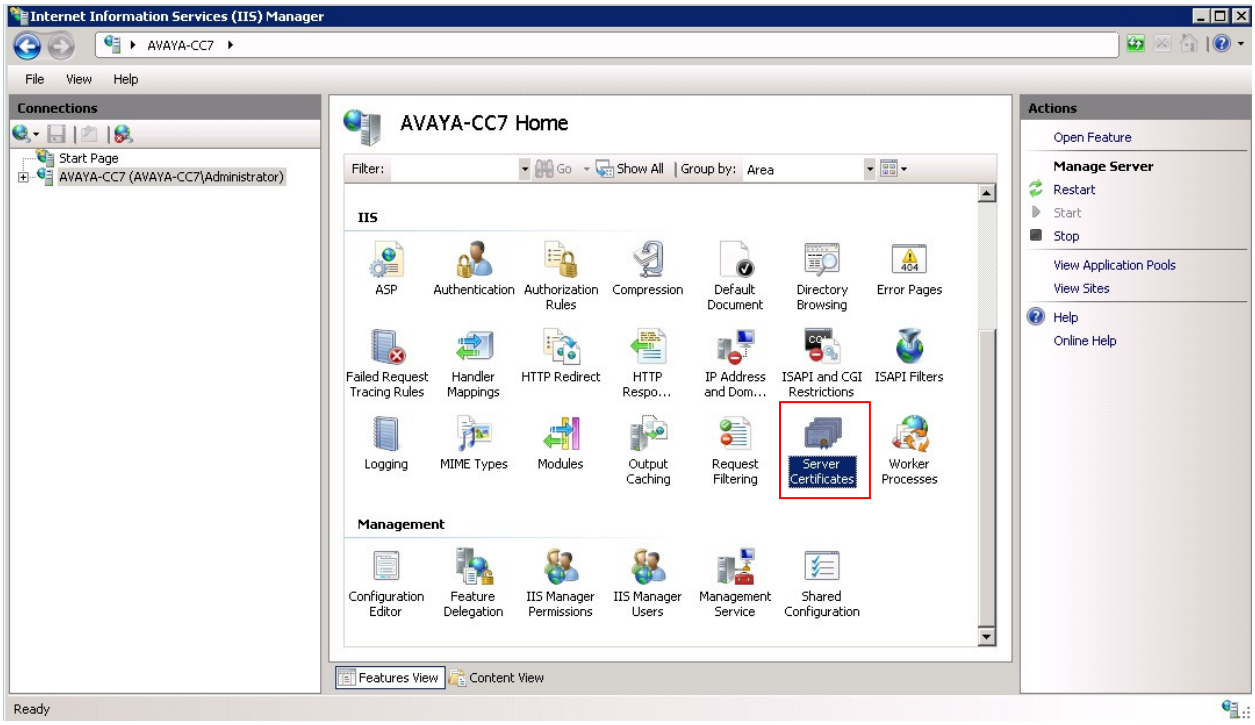
6.3. Import the signed certificate into Avaya Aura® Contact Center

TLS protocol requires an identity certificate exchange prior to encrypted communications commencing. Identity certificates must be signed by a common root Certificate Authority. Both the server identity certificate and the root Certificate Authority certificate must be installed on all Avaya Aura® Contact Center servers if mutual authentication is required.

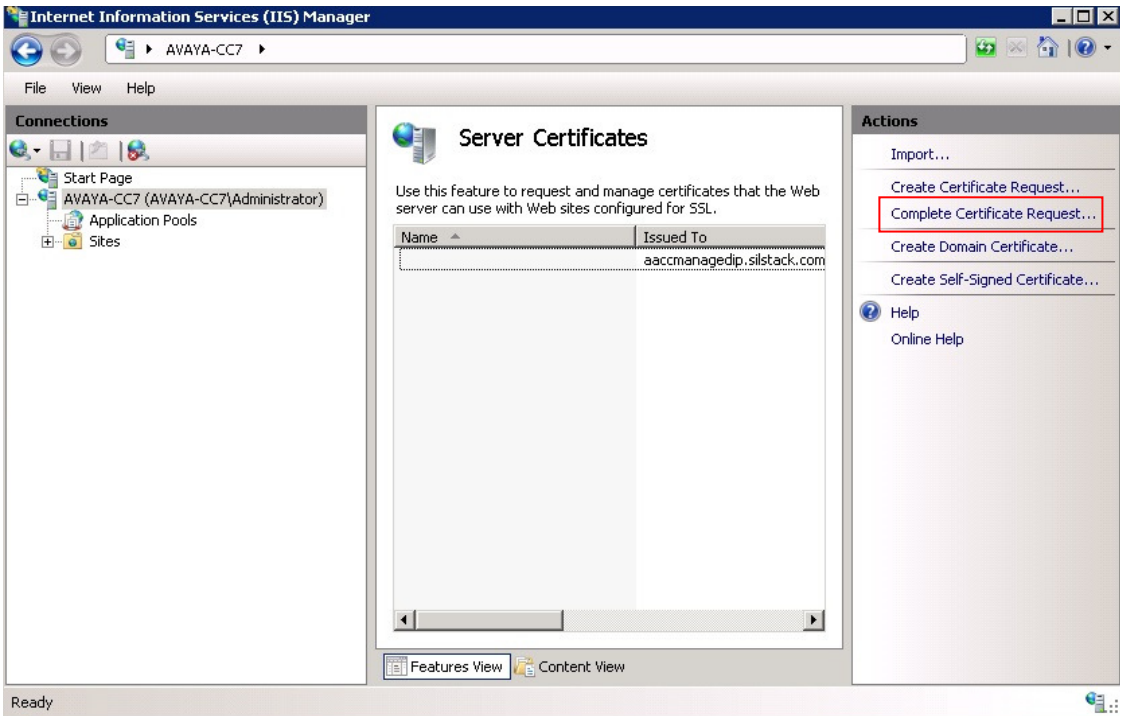
Obtain a copy of the server identity certificate generated in **Section 6.2** as well as a copy of the root Certificate Authority server certificate (see **Section 5.3**).

On the Windows 2008 R2 server, click on **Start → Administrative Tools → Internet Information Services (IIS) Manager** application (not shown – see **Section 6.1**). The **Internet Information Services (IIS) Manager** window opens.

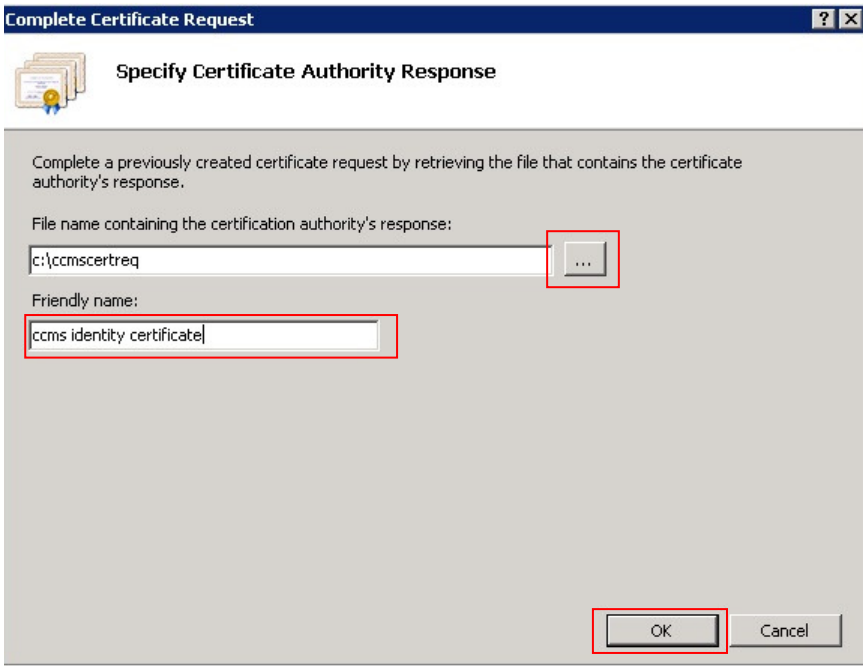
In the **Internet Information Services (IIS) Manager** window, search for the **Server Certificates** icon (highlighted). Double click the **Server Certificates** icon, a new window opens.



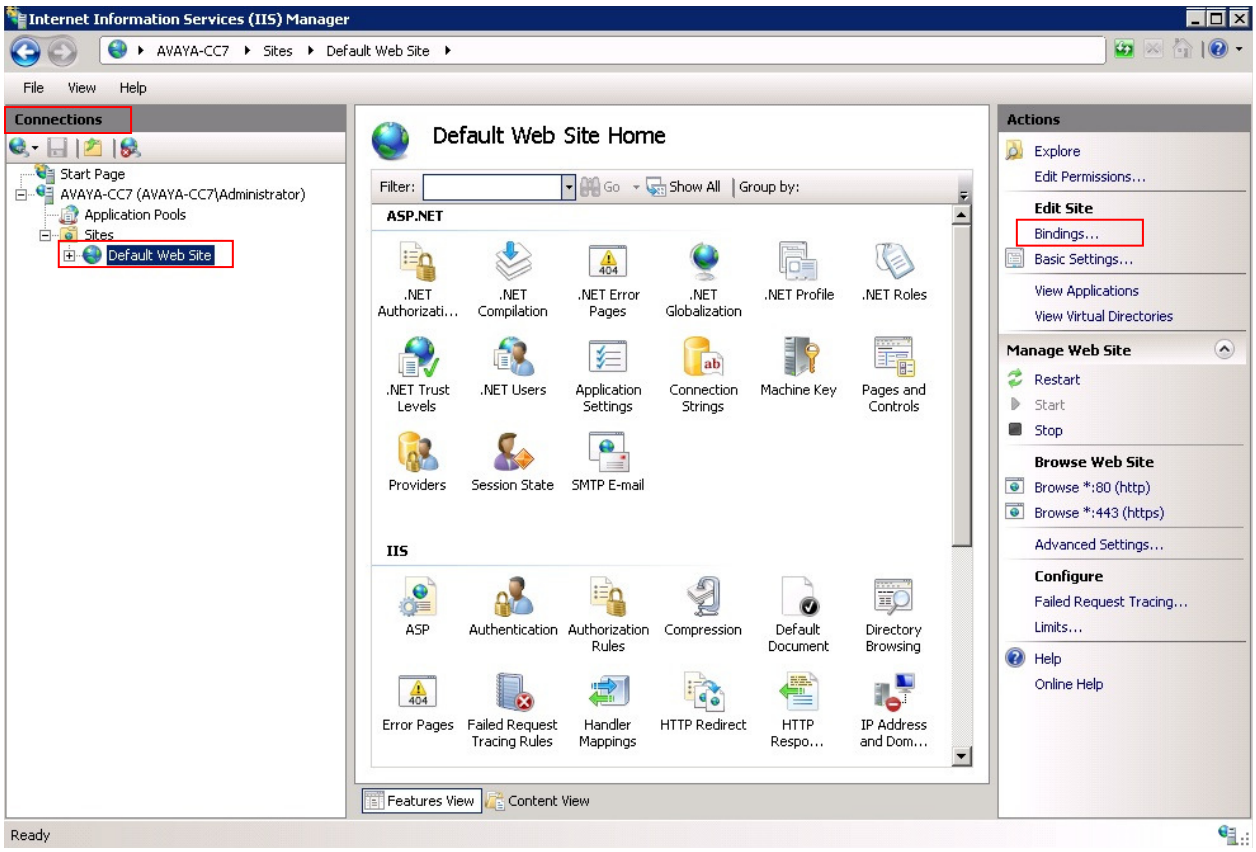
In the new window, click on **Complete Certificate Request** (highlighted).



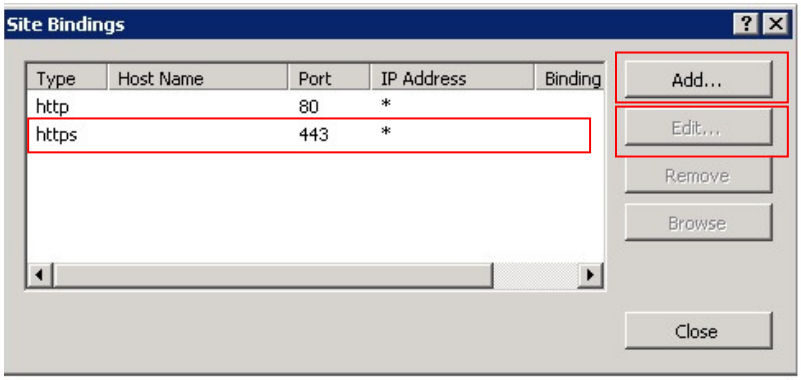
The **Complete Certificate Request** dialog box opens. Click on the "**…**" button (highlighted) to select the certificate generated in **Section 5.2**. In the **Friendly name:** section, type some text to describe the certificate. Click on the **OK** button when ready.



The newly installed identity certificate must be selected as the default identity certificate for all port 443 TLS transactions. Go to the **Internet Information Services (IIS) Manager** window (see start of **Section 6.3**). In the **Connections** pane, right click on the "**+**" symbol to the left of the server name. The tree expands to show the **Sites** folder. Click on the **Sites** "**+**" symbol, the **Default Web Site** property appears. Now go to the **Actions** area on the right side and click on **Bindings…** (highlighted).

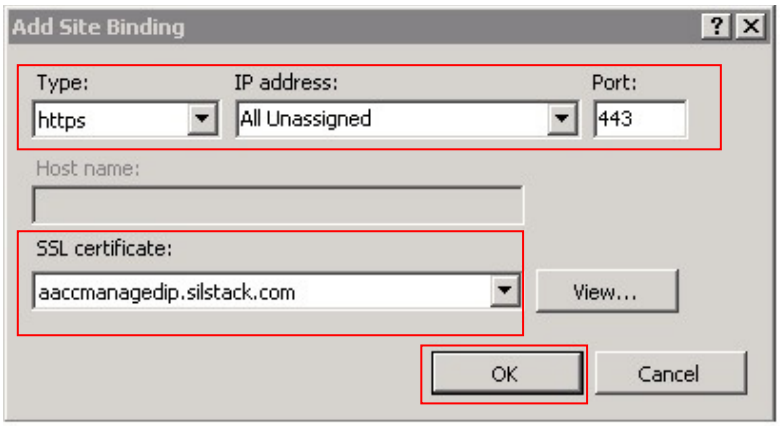


The **Site Bindings** window opens. If no certificates have been installed, the white area will be blank. Click the **Add** button. If there are certificates installed, the bindings will be shown. Select **https** (highlighted) and press the **Edit** button.



The **Add (Edit) Site Binding** window opens.
Under **Type**, select **https**
Under **IP Address**, ensure **All Unassigned** is selected
Type **443** for the **Port** value
For **SSL Certificate:** select the certificate created in **Section 6.2**.

Click the **OK** button when ready, this returns you to the **Site Bindings** window (not shown).
Click the **Close** button to complete identity certificate installation and binding activities.



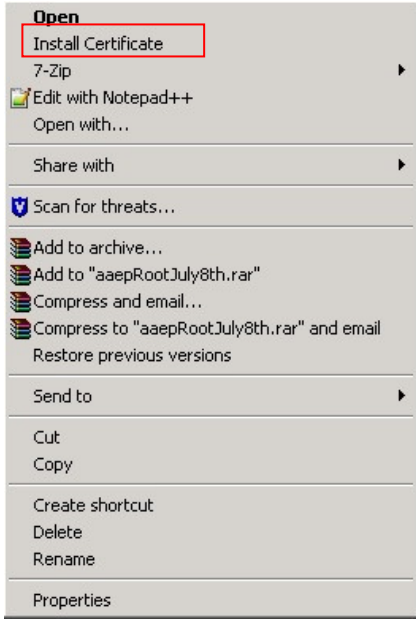
6.4. Import the Root CA Certificate into Avaya Aura® Contact Center

The IIS certificate installed in the previous section provides a unique verifiable identity for the contact center server during TLS handshakes. If this server is used to manage other contact center servers it will require a trusted root CA certificate to prevent TLS handshake failures.

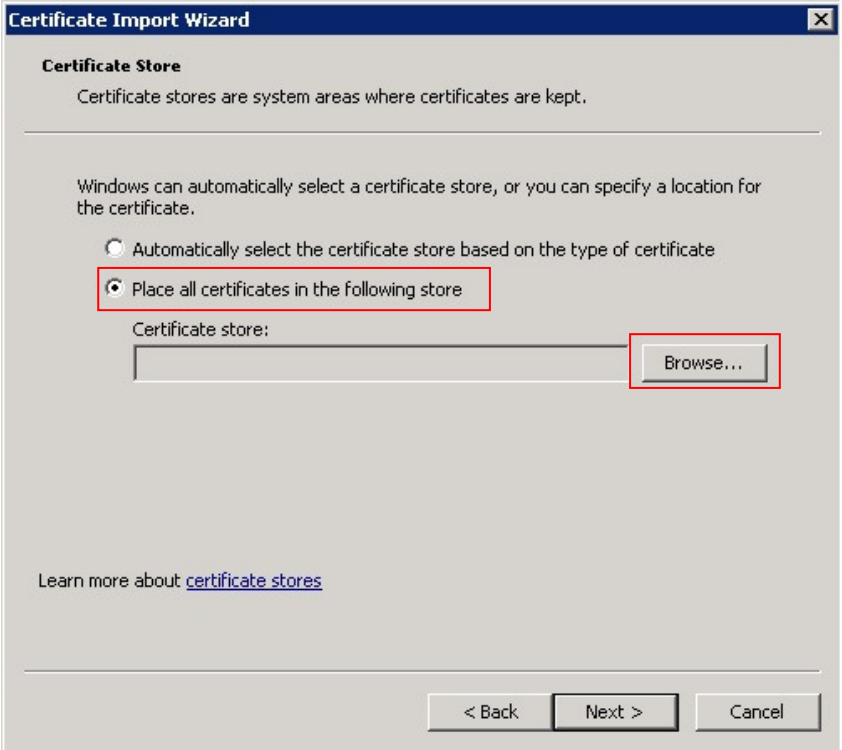
The trusted root CA certificate is the same one installed in CCMS (see **Section 5.3**).
This will be placed in the server's trusted root store and will eliminate web browser security warnings when connecting to other AACC servers.

Upload a copy of the root CA certificate (obtained in **Section 5.3**) to the CCMS/CCMM/CCT or CCMM server. Navigate to the folder where the certificate resides, highlight the just uploaded root CA certificate and right click.

A menu appears (see below), select the **Install Certificate** entry.

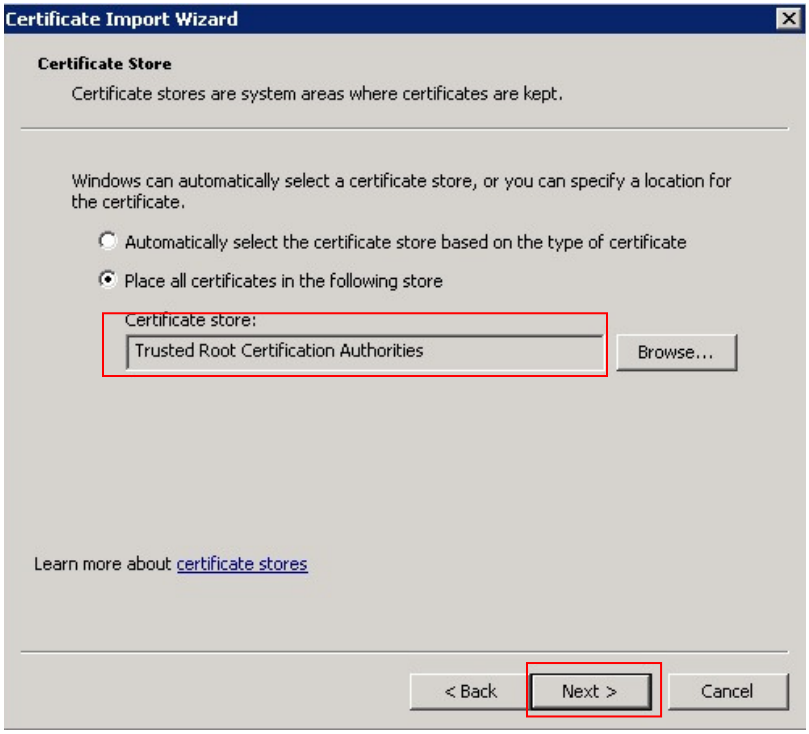


The **Certificate Import Wizard** opens. Ensure the **Place all certificates in the following store** radio button is checked. Click on the **Browse…** button when ready.

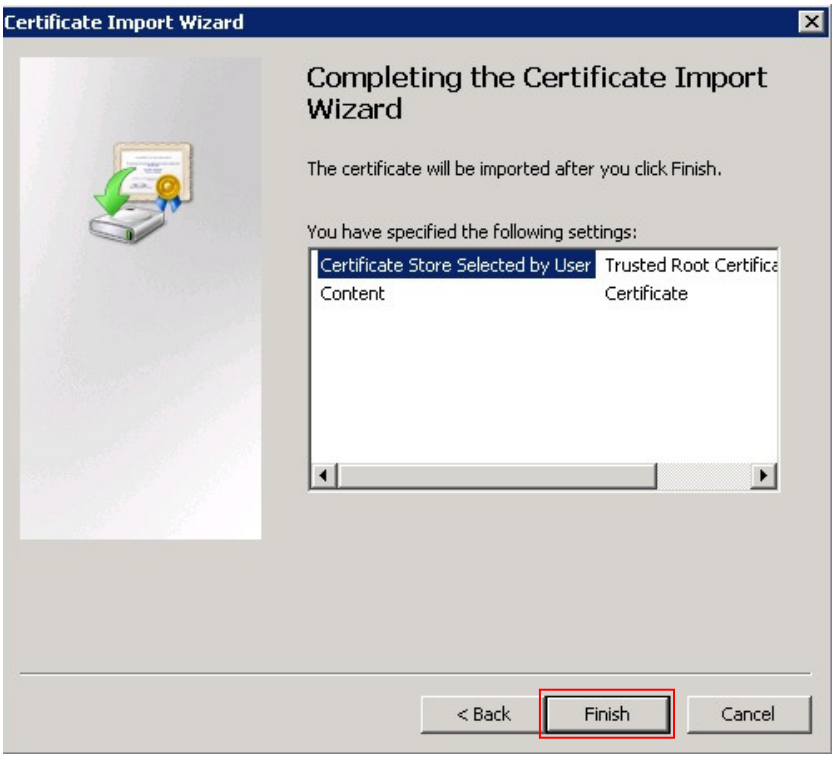


The **Select Certificate Store** opens, select **Trusted Root Certification Authorities** from the list and click the **OK** button.

The **Certificate Import Wizard** re-opens. Click on the **Next** button when ready.



The last Certificate Import Wizard window opens. Click on the **Finish** button.



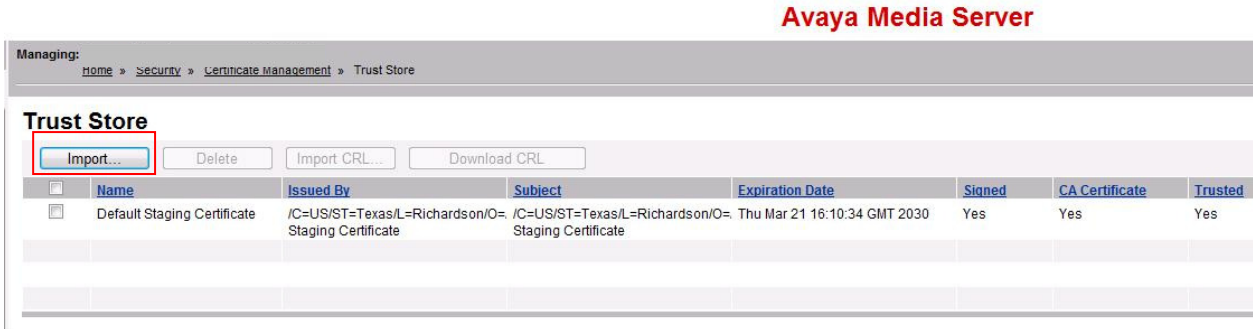
7. Install 3rd Party Certificates in Avaya Aura® Media Server

Avaya Aura® Media Server (AMS - a component of Avaya Aura® Contact Center) provides media management services for all contact center calls. Incoming calls to the contact center are anchored on AMS while an available agent is located. The agent and caller are "bridged" on AMS for the duration of the call, facilitating call recording and conferencing. AMS resources are not used when agents make or receive non-contact center related calls.

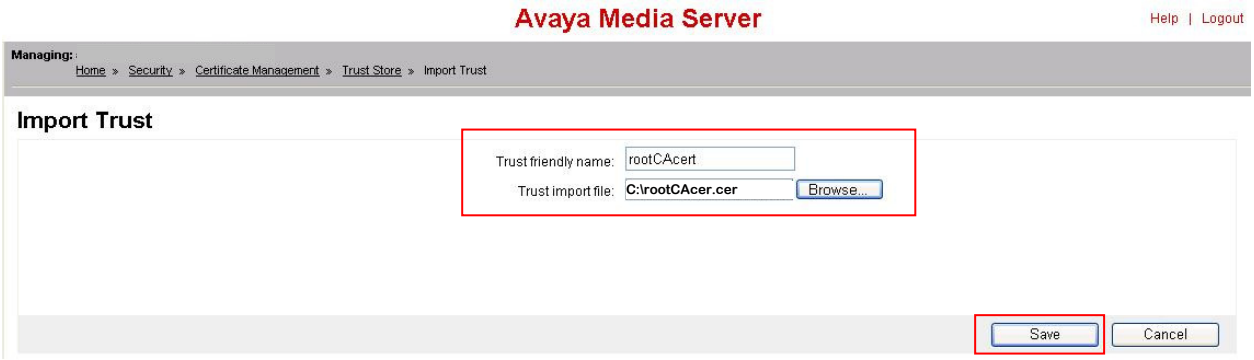
AMS may be installed co-resident with other AACC components if High Availability is not required. For High Availability operation, AMS must be installed on a pair of Linux servers.

7.1. Install 3rd Party Root Certificates in Avaya Aura® Media Server

AMS come pre-installed with default Avaya root CA certificates, to replace these obtain a copy of your root CA certificate (see **Section 5.3**). Login to the primary AMS server (not shown) and on the side menu, navigate to **Security → Certificate Management → Trust Store**. The **Trust Store** page opens. Click on the **Import…** button (highlighted).



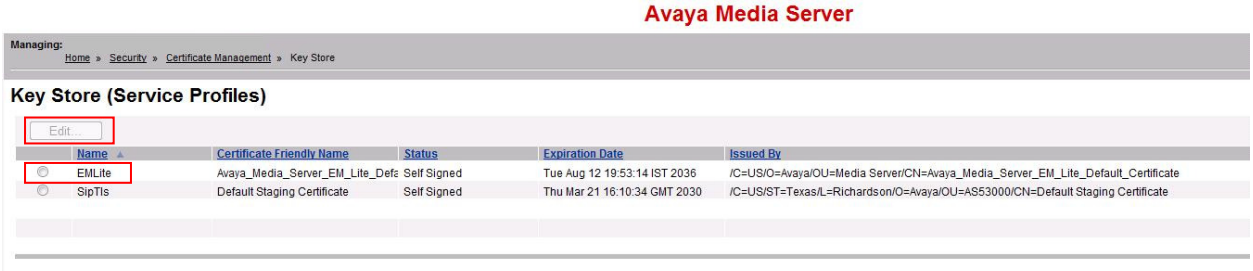
The **Import Trust** page opens. **Trust friendly name** can be any text to identify the certificate. Click on the **Browse…** button, use the file selector dialog box (not shown) to load the root CA certificate. Click on the **Save** button when ready. Repeat this procedure for the Backup AMS server.



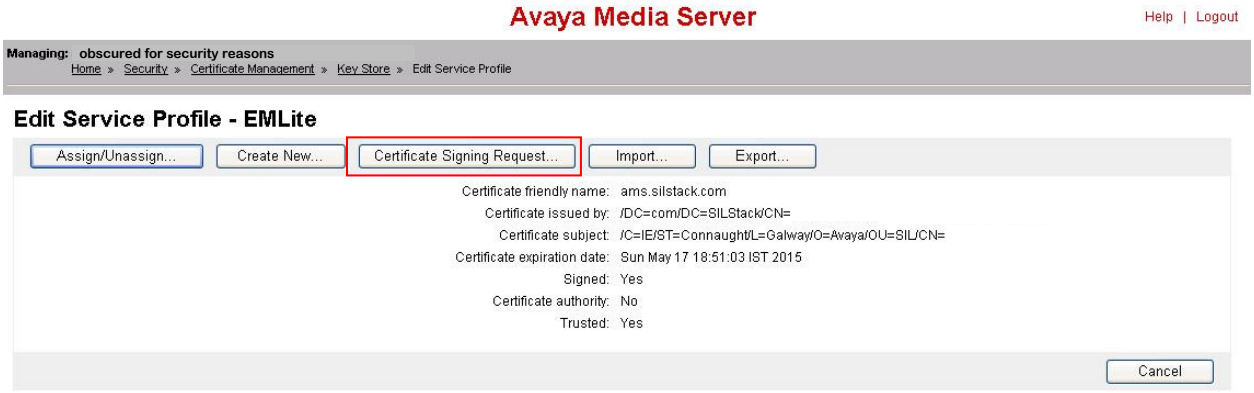
7.2. Install 3rd Party Server Identity Certificates in Avaya Aura ®Media Server

If 3rd party certificates are installed in Avaya Aura® Contact Center servers, Avaya Media Server certificates must be altered to ensure communications are not interrupted. The following procedure shows how to change AMS certificates.

AMS comes with a default product identity certificate. To examine current certificates, logon to the primary AMS server (using a web browser) and navigate to **Security → Certificate Management → Key Store**. **The Key Store (Service Profiles)** page opens. There are two AMS service profiles, **EMlite** is the profile for AMS management and this certificate is presented when users logon to AMS using a web browser. The **SipTls** service profile is required for secure SIP calls; this certificate is presented to SIP servers which connect to AMS.



Click on the radio button beside **EMLite** (highlighted) and then click on the **Edit** button to see certificate details. The **Edit Service Profile – EMLite** page opens. Essential certificate properties are displayed.



To examine the **SipTls** certificate properties, navigate to the **Security → Certificate Management → Key Store** page, click on the radio button beside **SipTls** and repeat this procedure,

7.2.1. Replacing Product Identity Certificates with 3rd Party Certificates

Replacement of existing Product Identity certificates requires use of the AMS command line to generate a Certificate Signing Request (CSR). Openssl will be used to generate the CSR and to package the signed CSR together with the AMS private keys into a PKCS#12 file which can be imported using AMS GUI functions.

Logon to the primary AMS using a SSH client (e.g., Putty).
If not already root, issue the "**su –** " command and enter the root password.

At the shell prompt, enter the following command:-

openssl req -out EMSlite.csr -new -newkey rsa:2048 -nodes -keyout Emslite.key

This command generates a CSR called EMSlite.csr signed with a 2048 bit key and also exports the private key used to sign the CSR. Two files, EMSlite.csr and EMSlite.key will be placed in root's home folder.

You are prompted for necessary information during file generation; ensure you have the correct information to hand before commencing this step. Example responses are in **bold**.

```
Generating a 2048 bit RSA private key
..............+++
...............................................+++
writing new private key to 'EMSlite.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:                          US
State or Province Name (full name) [Berkshire]:             Colorado
Locality Name (eg, city) [Newbury]:                         Denver
Organization Name (eg, company) [My Company Ltd]:          Avaya
Organizational Unit Name (eg, section) []:                  SIL
Common Name (eg, your name or your server's hostname) []:   ams1
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:                                    Avayaams1
An optional company name []:
```

Take note of the **challenge password** value, this will be required when importing the signed certificate into AMS.

7.2.2. Submitting the CSR for Signing

At the shell prompt, enter the following command **cat EMSlite.csr**

The result will be similar to the following.


```
-----BEGIN CERTIFICATE REQUEST-----
MIICyzCCAbMCAQAwbDELMAkGA1UEBhMCSUUxEjAQBgNVBAgTCUNvbm5hdWdodDEP
MA0GA1UEBxMGR2Fsd2F5MQ4wDAYDVQQKEwVBdmF5YTEMMAoGA1UECxMDU0lMMRow
GAYDVQQDExFhbXMyLnNpbHN0YWNrLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAMhFpnf3OZxaJxamCXRFPebuf2nJG/qVSfVllVfPpvxhgUAsc9zq
2ZnJGK60KOsROBYjRN5JJCSQKtvhPpReH74bV2o0ogKwgMhtCBs5sf7wO2DaV2MC
zSIXjp4iRMlTBzoEsuqM7UQCevESuJOLCLXYga7Ixxfg+AKdv0Gy/adIBFKVyvVl
DHqCCDJnEfzOcJbBMDum6TTsiDXy+2Tj6UkpZocrBBCb1g/bz2lxsGlnEYaCZeEF
uI3GvXeyX9riySLY4uCEVQeSGxCqPniA+b56jY6ciqioQHanPYt8jwKEXSa+O4JD
DURbNsf5Abkbyr1C/KaUjUoa9xhgMrKZlT0CAwEAAaAaMBgGCSqGSIb3DQEJBzEL
DAlBdmF5YTEyMyQwDQYJKoZIhvcNAQEFBQADggEBAMeSHoCYxCiAAyitNaRmP16K
TrRap1p5cBS8vTlrF7IBFobMGfCzccukkHWOux8clE+SQDEFLkAtNSmQfPDRmRHU
MpnvMWsHOgCpSIpaWanxvwyva+Aej4wuBkX/9KM9us72ZB6N6kvGbO0UrbnO+4Qz
rLCSJGkfLvCC0b8pKUp0pe0A0NexeiQrEQUNCTBnaOIdvvJSwRRji1EsIqGlNNb3
/j6MvN50HFqdRqX/mS9CmWBt1sMKEGSpoVu1Vw4BbZT/uWZ6i3EsSYNJEjqZqrC5
s8XrUCEiX1ATIeXvxNKKDGI2966nA2y7Fko4wkSM0Hq2EYvpfbRbW+SgF7MTg+A=
-----END CERTIFICATE REQUEST-----
```


Copy all the text from **----BEGIN** up to and including **REQUEST----**

Follow the procedure in **Section 5.2** to submit the CSR to the Certificate Authority.

If this is not possible, use the procedure in **Section 6.2** to sign the CSR. Copy the file **EMSlite.csr** to the Certificate Authority using file transfer protocols or USB disks.

7.2.3. Import the signed CSR into AMS

When the CSR has been signed, copy the file back to AMS (using file transfer protocols or a USB disk) to root's home folder. Rename the file **EMSlitesigned.cer**.

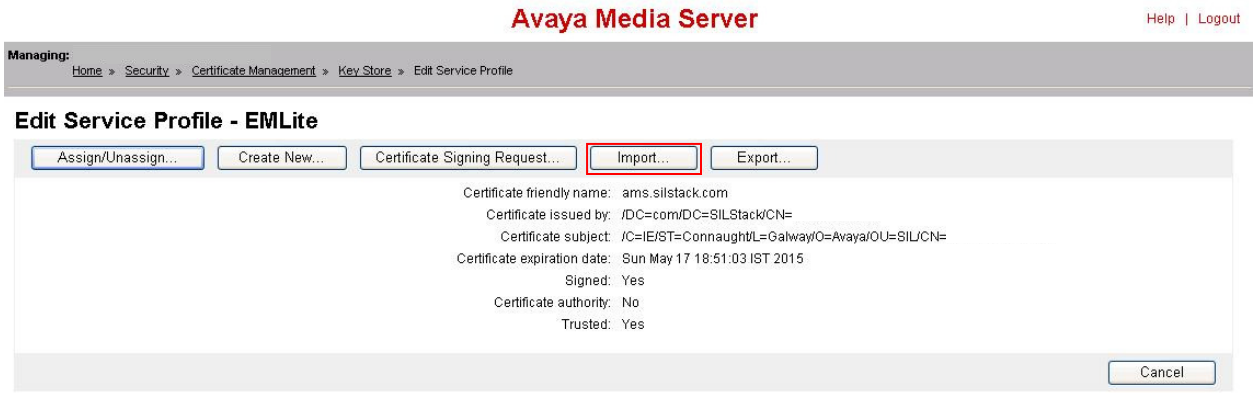
At the shell prompt, enter the following command:-

openssl pkcs12 -export -out EMSlite.pk12 -inkey EMSlite.key -in EMSlitesigned.cer

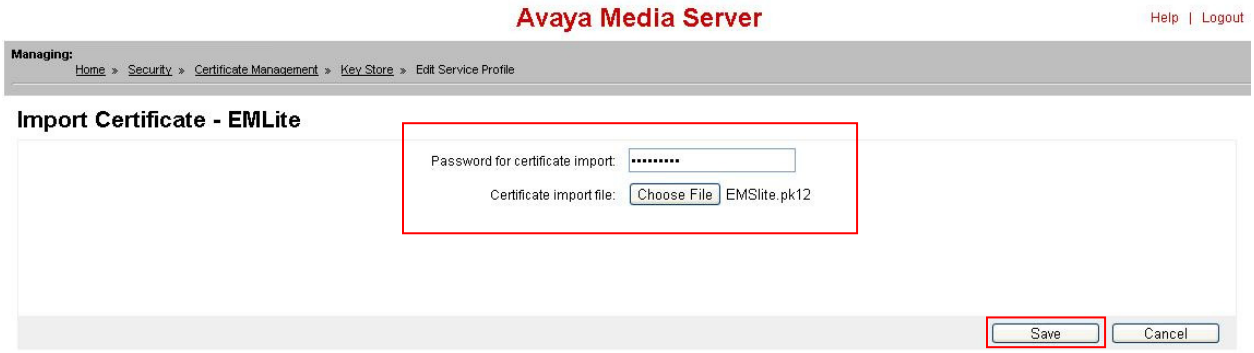
This command generates a PKCS#12 package called **EMSlite.pk12** containing the signed **EMSlite.cer** file and the original private key used to sign the CSR (**EMSlite.key**).

The file **EMSlite.pk12** must be imported into AMS using the GUI. Copy file **EMSlite.pk12** to wherever the browser is running from or use a networked drive or USB drive to make the file available to the browser.

Logon to AMS and navigate to **Security → Certificate Management → Key Store** (as per the start of **Section 7.2**), click on the radio button beside **EMLite** and then click on the **Edit** button to see certificate details. The **Edit Service Profile – EMLite** page opens. Click on the **Import…** button (highlighted).



A new page opens. Type the **challenge password** value in the **Password for certificate import** area (typed characters are replaced by dots). Click on the **Choose File** button and navigate to the folder or disk where the **EMSlite.pk12** file is stored. Choose this file and click return. Click on the **Save** button when ready.

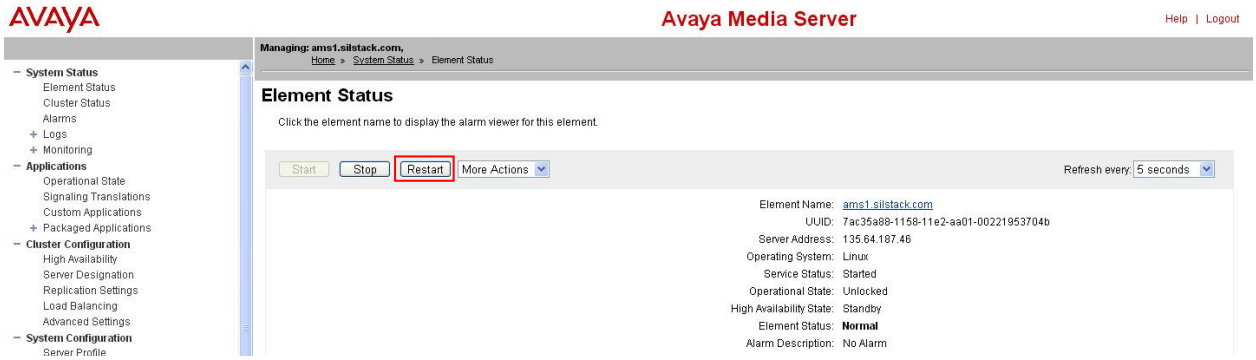


Repeat **Sections 7.2.1** to **7.2.3** inclusive to replace the default SIP product identity certificate, substituting **SIPtls** for **EMSlite** in filenames when required.

7.2.4. Restart AMS services to begin using the new certificates.

To load and activate the new AMS certificates, logon to the primary AMS using a web browser. Navigate to the **System Status→Element Status** page.

Click on the **Restart** button (highlighted). Wait 2 minutes for the AMS server to restart.



Logon to the backup AMS and Repeat **Sections 7.1** to **7.2.4** inclusive to replace the default trusted root CA certificate and default SIP product identity certificates.

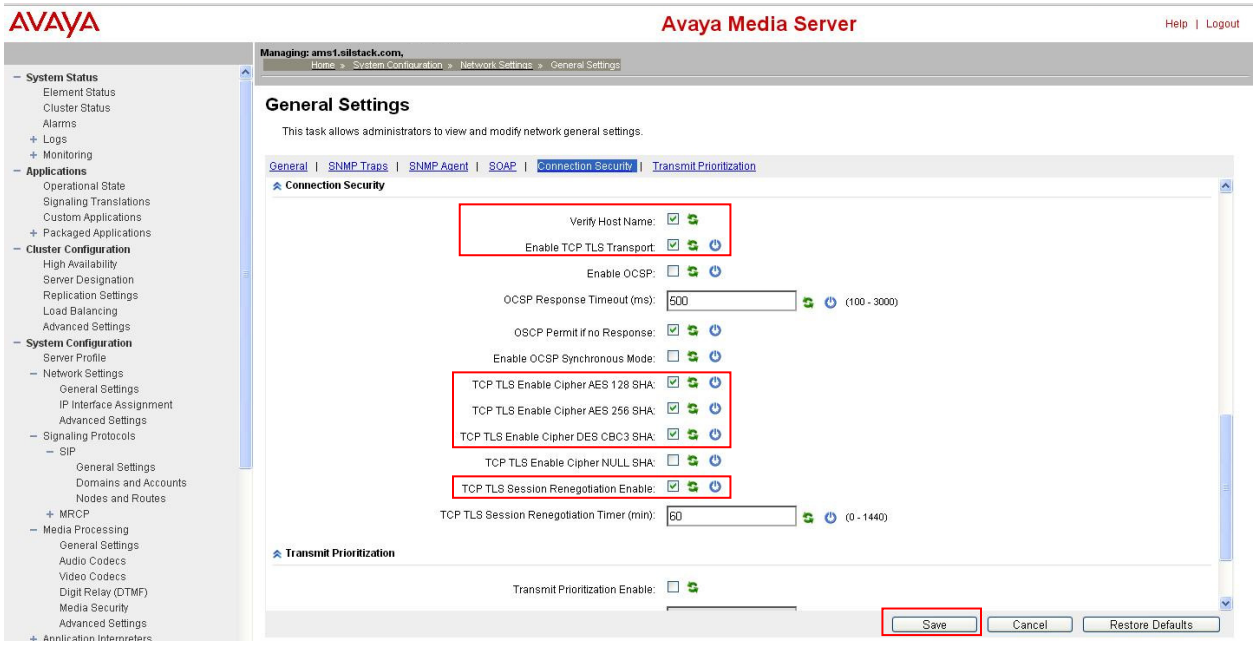
8. Configure Avaya Aura® Media Server for Transport Layer Security and Secure Real-time Transport Protocol

Avaya Media server can be configured to use Secure Real-time Transport Protocol (SRTP) when media security is required. Typically, SRTP is also used when signaling is secured using Transport Layer Security (TLS) as part of a secure Session Initiation Protocol (SIPS) call. SRTP is secured between media endpoints or between intervening media gateways using cryptographic algorithms.

8.1. Configure Avaya Aura® Media Server to use TLS

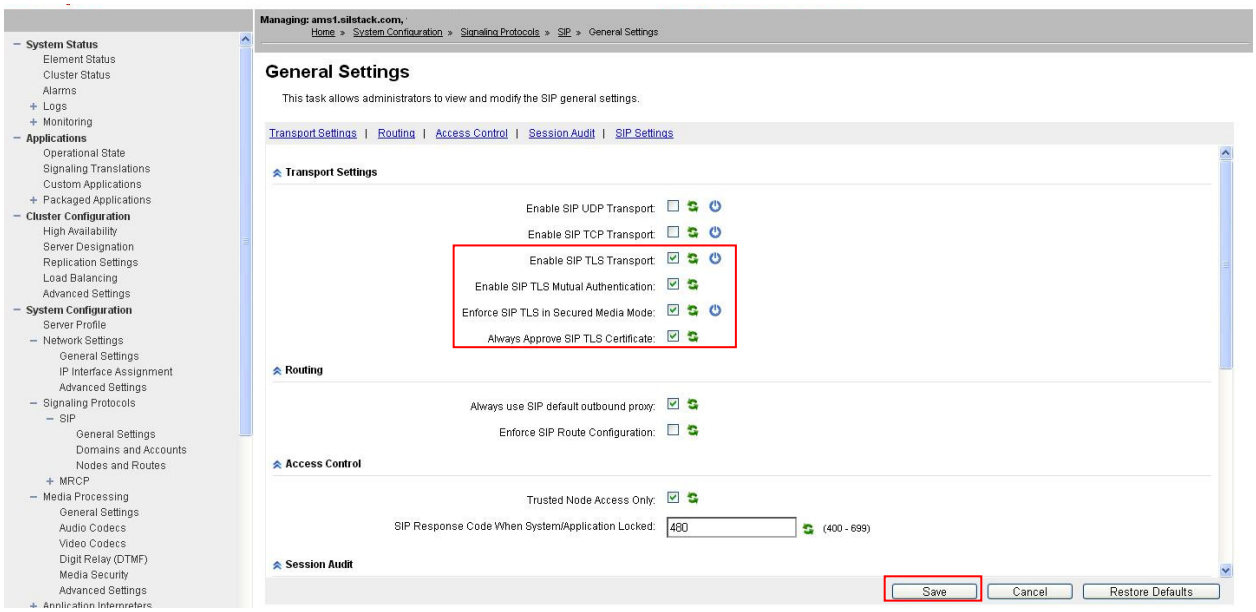
Logon to the primary AMS and navigate to **Home → System Configuration → Network Settings → General Settings → Connection Security.**

Configure **Connection Security** as in the following screenshot.
Click on the **Save** button when ready.



Navigate to **Home → System Configuration → Signaling Protocols →SIP →General Settings → Transport Settings**.

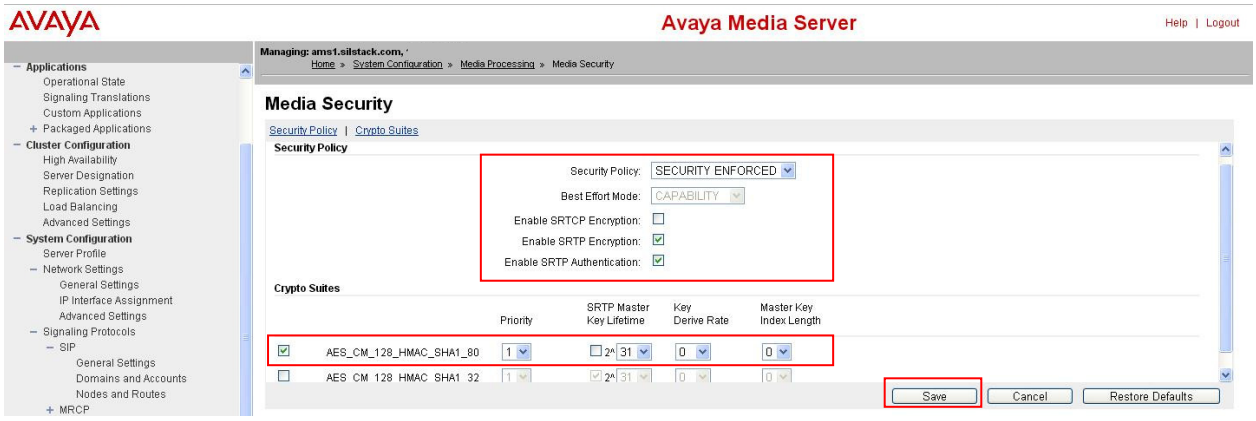
Configure **Transport Settings** as in the following screenshot.
Click on the **Save** button when ready.



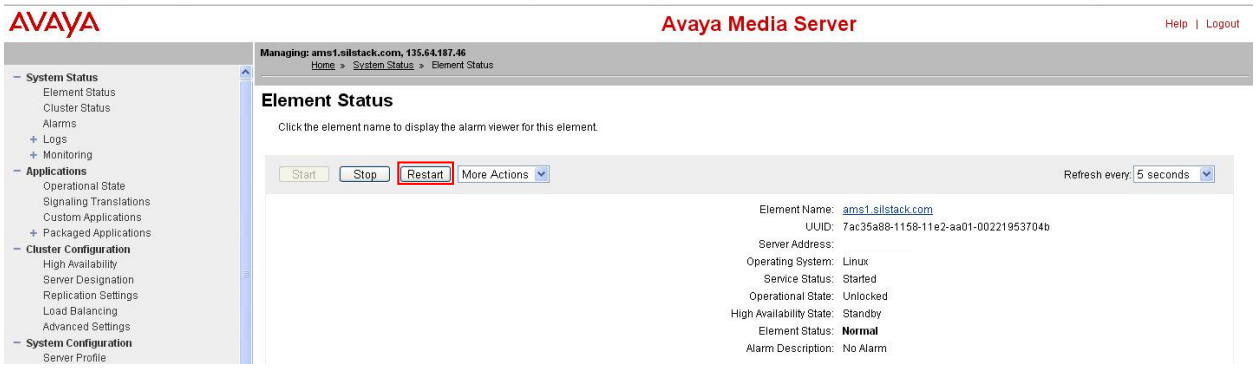
8.2. Configure Avaya Aura® Media Server to use Secure Real-time Transport Protocol

Navigate to **Home → System Configuration →Media Processing → Media Security.**

Configure **Security Policy** and **Crypto Suites** as in the following screenshot.
Ensure the chosen cryptographic algorithm matches what is configured in other communication elements. Click on the **Save** button when ready.



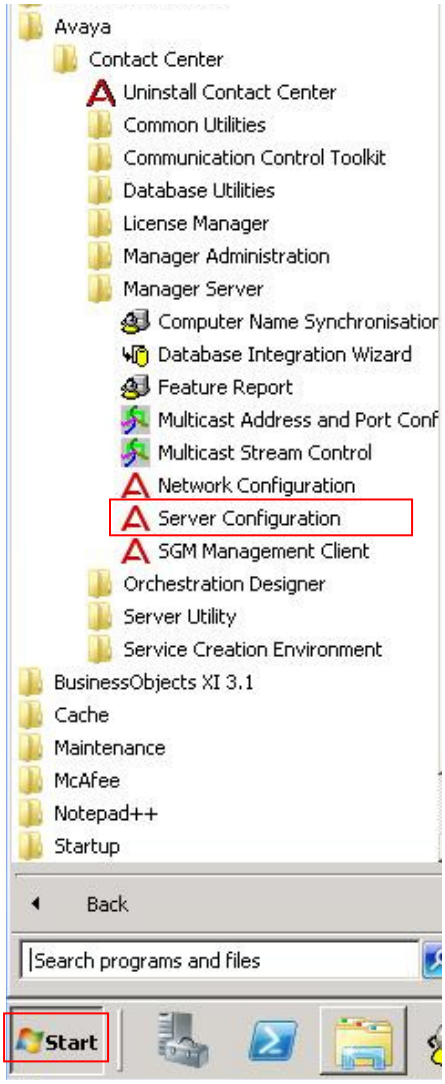
Navigate back to the **Home → System Status → Element Status** page.
Click on the Restart button to make the changes active.



These changes are automatically copied to the backup AMS but require a restart to activate. Login to the backup AMS, navigate back to the **Home → System Status → Element Status** page and click the **Restart** button.

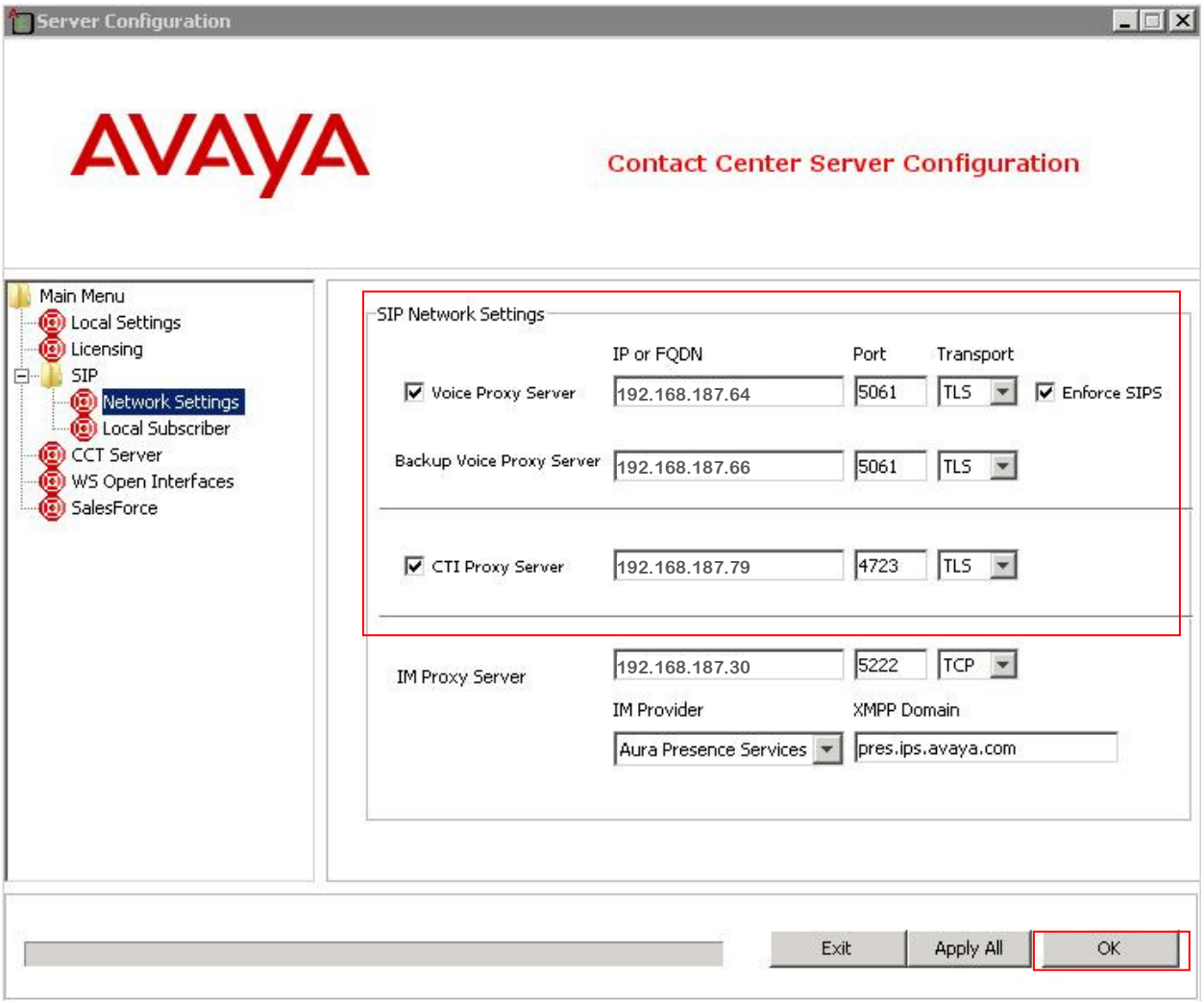
9. Configure Avaya Aura® Contact Center to use Transport Layer Protocol

AACC can only utilize one SIP transport protocol at a time. To change the configuration to TLS, launch the server configuration application by clicking on **Start → All Programs → Avaya → Contact Center → Manager Server → Server Configuration** (highlighted).



The application launches and displays the current configuration. Click on **Network Settings** (see below, highlighted); the SIP Network Settings property page opens. Ensure the SIP Network settings enclosed in the red box are as shown. When ready, click on the **OK** button.

The changes are applied.
When ready, click on the **Exit** button; a dialog box appears (not shown) asking for confirmation, click **OK**. A further warning dialog box appears to remind users to make the same configuration changes on the other server (in a High Availability environment only).



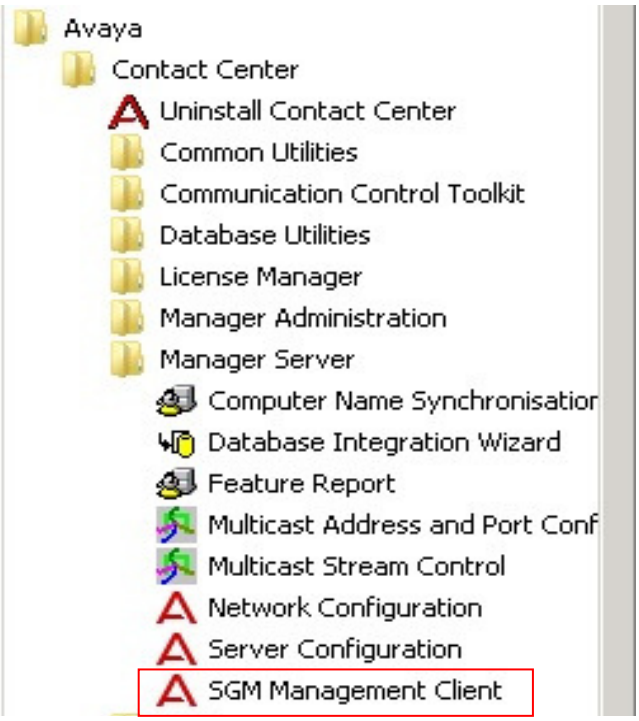
Follow the steps in **Section 5.1** to stop services. Follow the steps in **Section 5.5** to restart services. Repeat **Section 9** for the other CCMS server in the HA-pair.

10. Verification Steps

To verify the configuration steps have been successfully completed, perform the following operational tests.

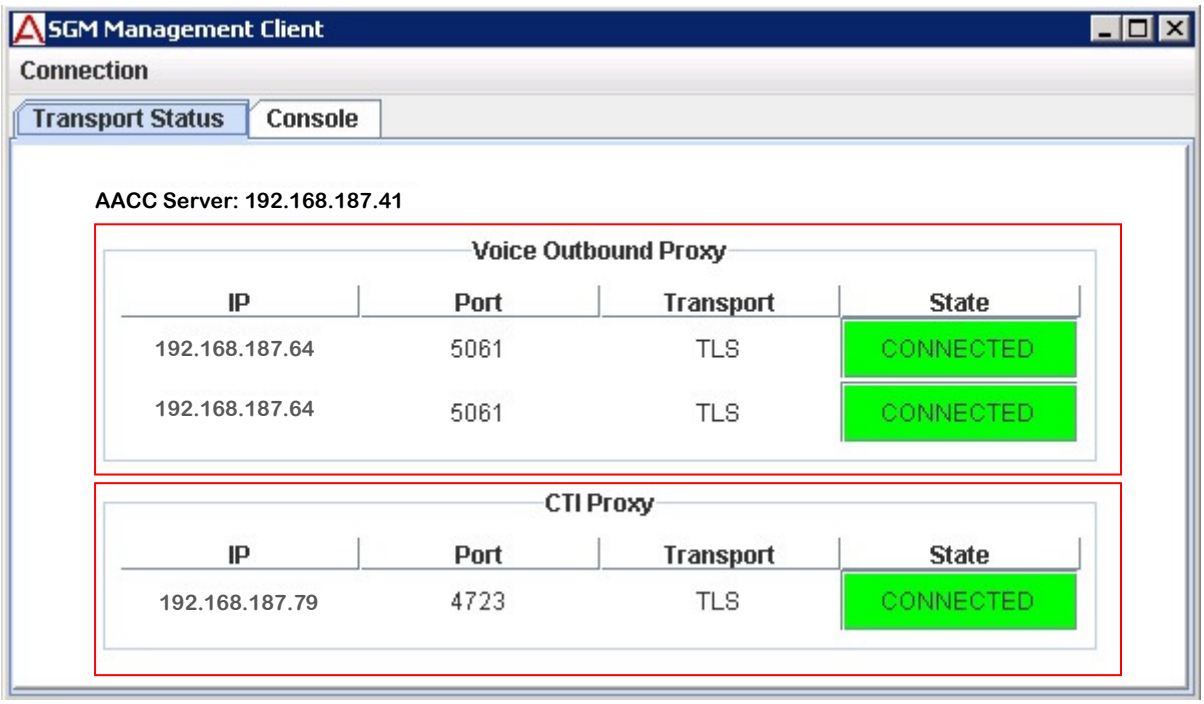
10.1. Logon to Avaya Aura® Contact Center to check TLS connections

Using Microsoft Remote Desktop (or direct via the system console), logon to the AACC managed IP address. Click on the **Start→All Programs→Avaya→Contact Center→ Manager Server→SGM Management Client.** The **SGM Management Client** application starts up and presents a **New Connection** dialog box with server connection details (not shown).



Click the **New Connection** button (not shown). The SGM Management Client opens and displays the Transport Status tab as default. Confirm the **Voice Outbound Proxy Transport** is **TLS** (on both proxies if the installation is HA) and **State** is **CONNECTED** (green).

Also, confirm the **CTI Proxy** is also using **TLS** for the **Transport** protocol and **State** is **CONNECTED** (green). This confirms TLS handshakes were successful between AACC and Session Manager.



10.2. Place a Telephone Call from the PSTN to a Avaya Aura® Communication Manager Station

Logon to Avaya Aura® Session Manager using a SSH client and the craft account. At the command line, enter the following command:

traceSM –uni –dt (hit the enter key)

Using a PSTN phone, place a call from a Communication Manager station to an AACC agent telephone. Observe the incoming call on the SIP trace. Confirm the call is using SIPS and the SDP contains information on cryptographic options.

Answer the call, confirm there is two-way speech.

Logon to Communication Manager using the SAT interface (craft account) and enter the following command:

status trunk x (where x is the SIP trunk between Communication Manager and Session Manager). Page through the screens until the active trunk member is located. In the example below, member **0002/032** is active.

```
status trunk 2                                                          Page   3

                              TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0002/029 T00035   in-service/idle    no
0002/030 T00036   in-service/idle    no
0002/031 T00037   in-service/idle    no
0002/032 T00038   in-service/active  no   T00050
```

Issue the command status trunk 0002/032 and scroll to **Page 3**. Observe the SRTP encryption scheme in use, it should be as configured in **Section 8.2**.

```
status trunk 0002/032                                          Page   3 of   3
                       SRC PORT TO DEST PORT TALKPATH
src port: T00038
T00038:TX:192.168.187.37:35010/g711u/20ms/1-srtp-aescm128-hmac80
T00050:RX: 192.168.187.120:37118/g711u/20ms/1-srtp-aescm128-hmac80
```

11. Conclusion

These Application Notes describe the configuration of Aura Contact Center 6.3 Service Pack 10 to use TLS and SRTP with third-party certificates when communicating with SIP telephone systems, such as Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

The use of TLS significantly increases the signaling security and SRTP confirms the integrity of the voice channel. Using third-party TLS certificates with mutual authentication enabled diminishes the possibility of unauthorized clients or servers establishing communications with Aura Contact Center 6.3 Service Pack 10.

12. Additional References

Avaya Product documentation relevant to these Application Notes is available at http://support.avaya.com.

[1] Implementing and Administering Avaya Media Server 7.5 (Release 7.5 June 2013)

[2] Avaya Aura® Contact Center Server Administration Release 6.3
NN44400-610 Issue 04.02 May 2013

[3] Avaya Aura® Contact Center Installation Release 6.3
NN44400-311 Issue 04.02 May 2013

[4] Avaya Aura® Contact Center Fundamentals Release 6.3
NN44400-110 Issue 04.02 May 2013

[5] Configuring Avaya Aura® System Manager 6.2 FP2 and Avaya Aura® Session Manager 6.2 FP2 to use Third-Party Security Certificates for Transport Layer Security

[6] RFC 3711 - The Secure Real-time Transport Protocol (SRTP)
- available from http://www.ietf.org/

[7] RFC 5246 - The Transport Layer Security (TLS) Protocol
- available from http://www.ietf.org/

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com