Avaya Solution & Interoperability Test Lab

Configuring Secure SIP Connectivity using Transport Layer Security (TLS) between Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Communication Server 1000E R7.6 – Issue 1.0

Abstract

These Application Notes describe a sample configuration of a network that provides a secure SIP connection using Transport Layer Security (TLS) between Avaya Aura® Communication Manager R6.2, Avaya Aura® Session Manager R6.2 and Avaya Communication Server 1000E R7.6. Avaya Aura® Session Manager R6.2 provides SIP proxy/routing functionality, routing SIP sessions across a TCP/IP network with centralized routing policies and adaptations to resolve SIP protocol differences across different telephony systems. Avaya Aura® System Manager R6.2 provides centralized administration and acts as a certification authority (CA). Non-default customer defined Identity certificates are used for Avaya Aura® Session Manager.

Information in these Application Notes has been obtained through Collaboration Pack for Communication Server 1000 testing in the Solution and Interoperability Test Lab and additional technical discussions.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration of a network that provides a secure SIP signaling connection using Transport Layer Security (TLS) between Avaya Aura® Session Manager Release R6.2 Service Pack 3, Avaya Aura® Communication Manager R6.2 Service Pack 3 and Avaya Communication Server 1000E R7.6. Avaya Aura® System Manager R6.2 is a central management system that delivers a set of shared management services and a common console for System Management and its components. It is used to manage a number of shared management services, including user management and security management. Avaya Aura® System Manager R6.2 Trust Management supports two Certificate Authorities. One for Avaya Aura® System Manager and its managed elements (Avaya Aura® Communication Manager and Avaya Aura® Session Manager), and the other for Unified Communications Management (UCM) and its managed elements (Avaya Communication Server 1000E). Thus Avaya Aura® System Manager R6.2 supports two independent user interfaces for Certificate Authority.

These Application Notes will focus on TLS certificate management, the configuration of the secure SIP trunks, and call routing. TLS certificates are created using private certificates signed internally by the System Manager Certificate Authority. Third party certificates are not detailed in this application note. Detailed administration of other aspects of Avaya Communication Server 1000E or Avaya Aura® Session Manager will not be described. For more information on these other administration actions, see the appropriate documentation listed in **Section 11**.

2. Stack Compliance Testing

Avaya Aura® Communication Manager, Avaya Aura® Session Manager and Avaya Communication Server 1000E using TLS were tested as part of the Collaboration Pack for Communication Server 1000 solution testing in the Solution and Interoperability Test Lab. The network configuration shown in **Section 3** is a subset of the overall test environment and focuses on the SIP TLS Trunk setup, TLS management and relevant test cases.

2.1. Test Description and Coverage

This section provides an overview of the test cases performed after the installation and configuration of SIP TLS trunking between Communication Server 1000E to Session Manager and between Session Manager and Communication Manager. A number of UNIStim and TDM endpoints have been configured on CS1000 and SIP endpoints have been configured off Session Manager and Communication Manager. The areas tested as part of Collaboration Pack for CS1000 solution testing and relevant to this application note are:

- Server installation and software upgrades
- Basic calls between CS1000 and Avaya Aura® Communication Manager
- Call hold/resume
- Music on hold (Both CS1000 and Communication Manager)
- Transfers (Both blind and attended)
- Ad-hoc Conference
- Call Forward
- Long Call duration
- Presence provided by Avaya Aura® Presence Services
- Negative testing including Communication Server 1000 Call Server and Signaling Server failover
- Wireless infrastructure provided by Avaya Wireless LAN 8100
- Wireless Authentication and authorization managed by Avaya Identity Engines

Basic Calls:

- Verify displays and talk path for calls between different types of stations on CS1000E and SIP endpoints registered to Session Manager.
- Verify a second call can be made between different types of stations on CS1000E and SIP endpoints registered to Session Manager after the first call is abandoned.

Supplemental Call Features:

- Verify calls from different types of stations on CS1000E to a SIP endpoint registered to Session Manager can be placed on hold and taken off-hold.
- Verify calls from different types of stations on CS1000E to a SIP endpoint registered to Session Manager can be transferred to another SIP endpoint.
- Verify calls from different types of stations on CS1000E can create a conference with two SIP endpoints registered to Session Manager.
- Repeat the hold, transfer, and conference scenarios with calls originating from a SIP endpoint registered to Session Manager.

Long Duration Calls

- Place a call from different types of stations on CS1000E to a SIP endpoint registered to Session Manager. Answer the call, leave the call active for at least 30 minutes, and verify displays and talk path.
- Place a call from different types of stations on CS1000E to a SIP endpoint registered to Session Manager. Answer the call, put the call on hold for at least 20 minutes, and verify displays and talk path after returning to the call.
- Repeat the long duration scenarios with calls originating from a station on SIP endpoint registered to Session Manager.

CS1000E Signaling Server Failover

- Disconnect CS1000E Leader Signaling Server from network. Verify virtual trunks are established on Follower Signaling Server. Verify SIP TLS trunk is established to Session Manager. Verify all IP phones register to follower Signaling Server. Verify all IP phones can make and receive calls to phones on Session Manager.

CS1000E Call Server Failover

- Disconnect CS1000E active call Server from network. Verify the inactive call server core in the High-Availability pair becomes active. Verify all IP phones can make and receive calls to phones on Session Manager and check call features are working.

2.2. Test Results and Observations

Majority of test cases passed for calls between Avaya Communication Server 1000E R7.6 endpoints and Avaya Aura® Communication Manager over SIP-TLS trunk via Avaya Aura® Session Manager. There were no issues in relation to TLS management. Some issues were noted in relation to update of Calling Party Name Display (CPND) and Caller Line Identification (CLID) on the CS1000 phone display during transfer scenarios. After investigation with design teams, this scenario is noted as a current interoperability design limitation and will be addressed in a future release of CS1000. The problem call scenario is as follows:

- Set A is a CS1000 phone or Avaya Aura® phone (SIP or H.323)
- Set B is a CS1000 UNIStim phone
- Set C is Avaya Aura® phone (SIP or H.323)
- Set A calls Set B and call is established
- Set B performs a blind (unattended transfer) to Set C.
- When Set C answers the call, the CPND and CLID shown is that of Set B, rather than Set A

Another issue found is where music-on-hold is not played when CS1000 UNIStim phone is on a call with Avaya Aura® SIP endpoint and the CS1000 phone uses the hold feature more than once. The first time the hold feature is activated, music is heard on the Avaya Aura® SIP endpoint. The second or subsequent times the hold feature is activated, music is not heard on the Avaya Aura® SIP endpoint, however when the call is resumed two-way speech is successful. These call related issues were not specific to TLS on the network and also occur on TCP Trunks.

3. Reference Configuration

In our sample configuration and as shown in **Figure 1**,(shown on the next page) Avaya Communication Server 1000E R7.6 runs on the Common Processor Pentium Mobile (CP PM) server in a high availability configuration and supports a number of endpoints, including; Avaya 1100 series IP Deskphones (UNIStim), Avaya 1200 series IP Deskphones (UNIStim) and Avaya 3900 series Digital Deskphones.

Avaya Aura® System Manager, Avaya Aura® Session Manager and Avaya Aura® Communication Manager are delivered in a virtualized environment as part of a pre-packaged single server unified communications solution called Avaya Aura® Solution for Midsize Enterprise with a G450 Media Gateway. However, the application note applies to any Avaya Aura® Configuration. Avaya Communication Server 1000E is connected over a secure SIP trunk to Avaya Aura® Session Manager Release R6.2, using the SIP Signaling network interface on Avaya Aura® Session Manager. An adaptation module designed for Avaya Communication Server 1000E is configured on Avaya Aura® Session Manager to support protocol conversion between Avaya Communication Server 1000E and other Avaya products, including Avaya Aura® Communication Manager.

Avaya Aura® Communication Manager supports various client including; Avaya one-X Deskphone SIP, Avaya one-X® Communicator, Avaya Flare Experience for Microsoft Windows, and Avaya Flare Experience for Apple iOS. Avaya Aura® Communication Manager connects to Avaya Aura® Session Manager over a secure SIP trunk. The default Avaya Aura® Session Manager Identity Certificate uses a hard-coded Common Name (sm100). Avaya recommends replacing the default Session Manager Identity certificate with a unique certificate based on the Fully Qualified Domain Name (FQDN) of the Avaya Aura® Session Manager Security Module.

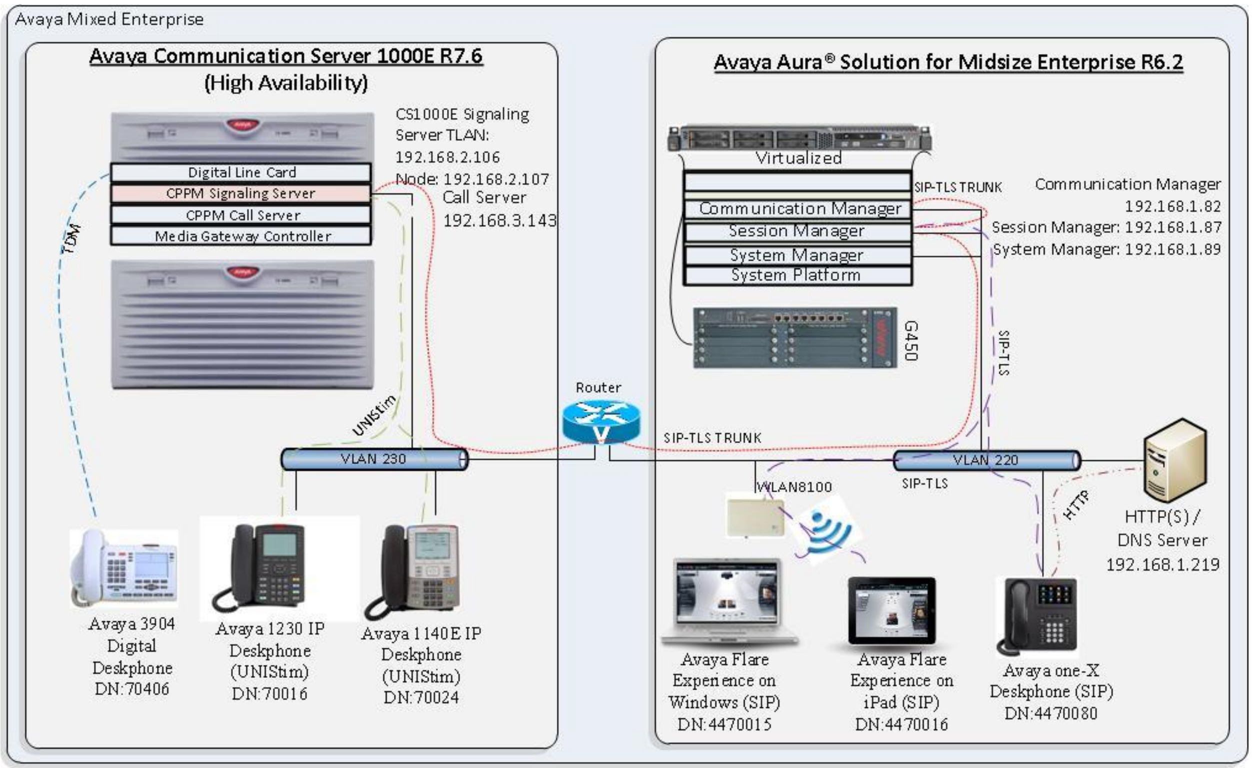


Figure 1 – Network Topology: SIP TLS Trunk between Avaya Communication Server 1000E R7.6 and Avaya Aura® Communication Manager R6.2

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration.

Component	Software Version
HP Proliant DL360 G7 Server	Avaya Aura® System Platform 6.2.1.0.9 Avaya Aura® Solution for Midsize Enterprise R6.2 - Midsize Enterprise Template 6.2.0.0.3105 - Avaya Aura® Communication Manager 6.2 SP3 (6.2.0.823.0-20199) - Avaya Aura® System Manager 6.2 SP3 (6.2.12) - Avaya Aura® Session Manager 6.2 SP3 (6.2.3.0.623006) - Avaya Aura® Presence Services 6.1 SP5 (6.1.5.0.1204)
Avaya G450 Media Gateway	30.18.1
Avaya Communication Server 1000E running on CP+PM server in High-Availability configuration	Release 7.6 Version 7.65.16/7.65P
Avaya 1140 IP Deskphone	UNIStim R5.5
Avaya 1230 IP Deskphone	UNIStim R5.5
Avaya one-X© Deskphone 9641	SIP Release 6.2 (Build 6.2.2r7.v4r70b)
Apple iPad2	Avaya Flare Experience Release 1.1 (Build 95) Apple iOS 6.0.1
Hewlett Packard Compaq 6000 Microtower	Avaya Flare Experience Release 1.1 (Build 1.1.0.5) Microsoft Windows 7 SP1 and Microsoft Windows XP SP3
Avaya 8180 Wireless LAN Controller	Version 1.2.0.75
Avaya 8120 Wireless Access Point	Version 1.2
Dell Poweredge 1950	Avaya Identity Engines Ignition Server version 8.0 (build 022931) running as a virtual image on VMWare EXSi 4.0
Avaya Ethernet Routing Switch 2550T-PWR	Version 4.4.0.010
Avaya Ethernet Routing Switch 4548GT-PWR	Version 5.4.2.032 Firmware: 5.3.0.3

5. Security Certificate Configuration and Management

This section describes the security certificate configuration and management. The following administration steps are described:

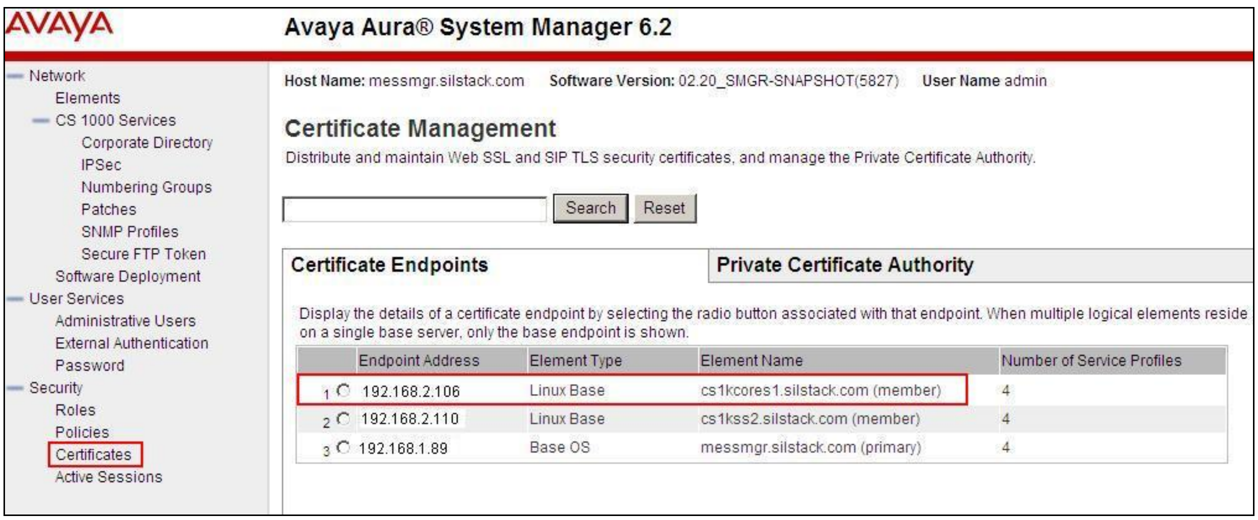
1) Create a TLS Certificate for Avaya Communication Server 1000E SIP Signaling Gateway
2) Install Avaya Communication Server 1000E Security Certificate on Session Manager
3) Replace the default Avaya Aura® Session Manager Identity Certificate
4) Update the Installed Certificates on Avaya Aura® Session Manager
5) Distribute Avaya Aura® System Manager Certificate Authority file to Avaya Aura® Communication Manager
6) Install Root Certificate Authority Certificate onto Avaya one-X SIP Deskphones

5.1. Create a TLS Certificate for Avaya Communication Server 1000E SIP Gateway

Configure trust management between Communication Server 1000E SIP Signaling Gateway on the Signaling Server and System Manager Unified Communications Management (UCM) Certificate Authority. View the UCM Services web interface by accessing the System Manager URL **https://<SMGR-FQDN>/SMGR**, where **< SMGR-FQDN >** is the Fully Qualified Domain Name(FQDN) of the System Manager. The Personal Computer where the web browser is accessed has Domain Name Server (DNS) configured to resolve the System Manager FQDN to an IP address. Enter the appropriate **Used ID** and **Password** and click **Log On** to access System Manager.

Click on **UCM Services**

From the **Avaya Unified Communication Management** home page, click on **Security → Certificates** as shown below.



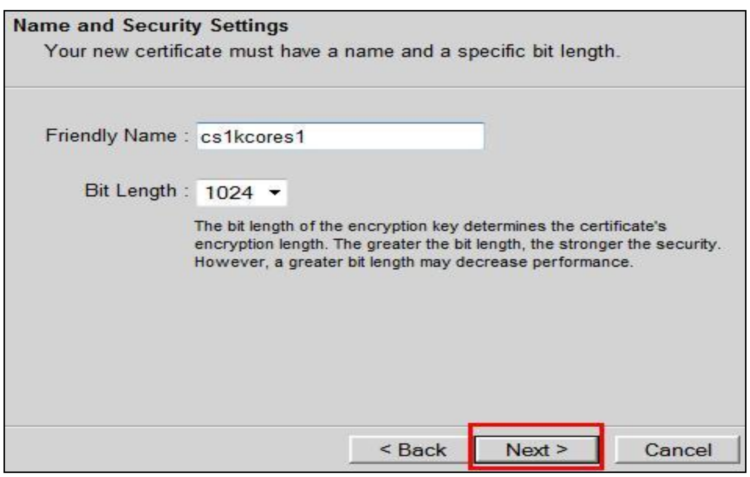
Under the **Certificate Endpoints** tab on the **Certificate Management** page, enter associated with the Signaling Server where the CS1000E SIP Gateway application resides. This will open the **Endpoint Details** page shown below. Select **SIP_TLS** link to open the **Server Certificate** window.

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	cs1kcores1.silstack.com	Aug 13, 2022
2	DTLS	signed	cs1kcores1	Mar 7, 2022
3	Web SSL	none		
4	SIP TLS	signed	cs1kcores1	Aug 13, 2022

Enter to select **the Create a new certificate, signed by local private Certificate Authority** option and click **Next**.

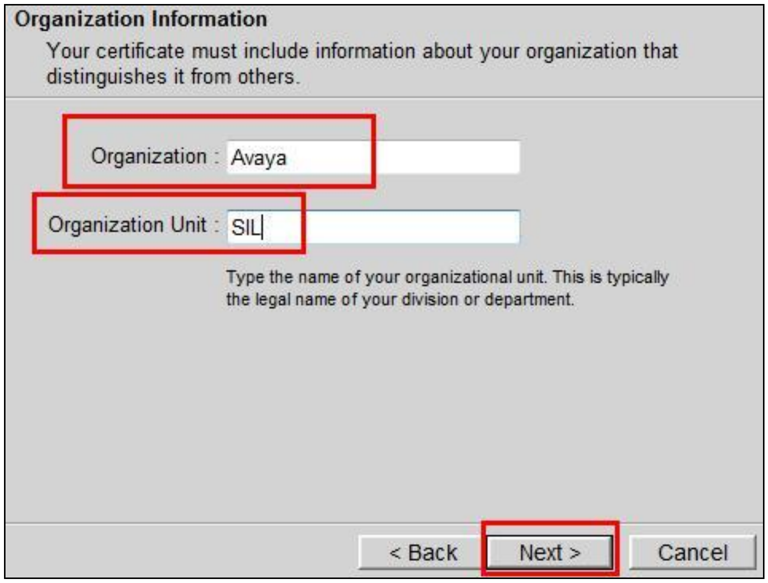
On the **Name and Security Settings** window, enter the following values and click **Next.**

- **Friendly Name:** Enter descriptive name for the system. In sample configuration, **cs1kcores1** is used
- **Bit Length:** Retain default value of **1024**



On the **Organization Information** window, enter the following values and click **Next**.

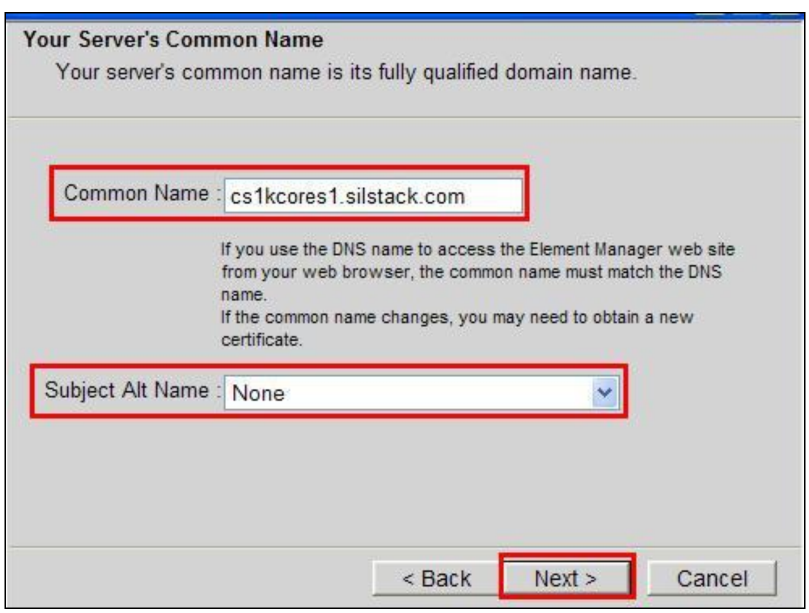
- **Organization:** Enter brief descriptive name of Organization. In sample configuration, **Avaya** is used
- **Organization Unit:** Enter name of the Organization Unit. In sample configuration, **SIL** is used



On the **Your Server's Common Name** window, enter the following values and click **Next**.

- **Common Name:** Verify the correct FQDN of the CS1000E SIP Signaling Gateway (SSG) is used. In the sample configuration, **cs1kcores1.silstack.com** is used.
- **Subject Alt Name**: Select **None** from the drop down menu

Click **Next** to continue to the geographic information.

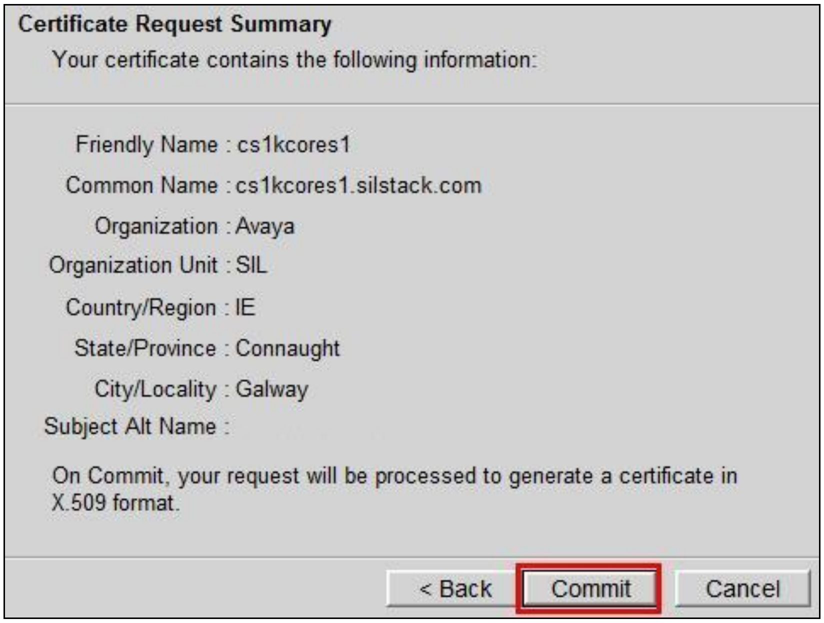


On the **Geographic Information** window, enter the following values and click **Next**.

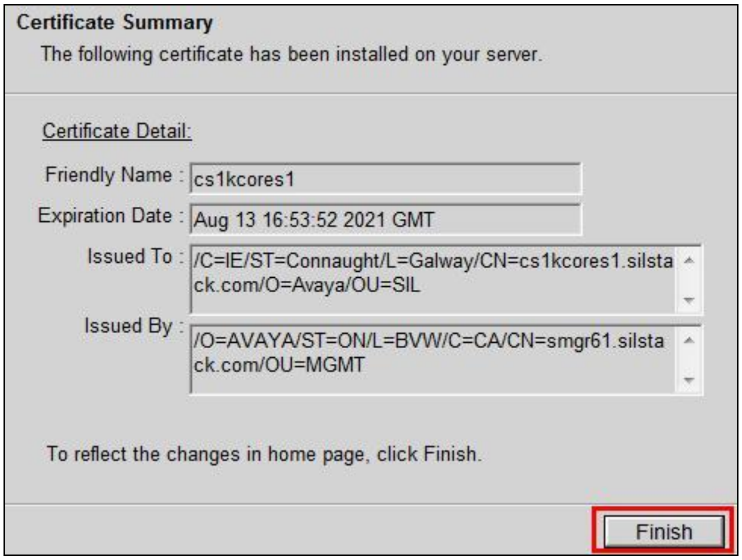
- **Country/Region:** Select appropriate **Country/Region** from drop-down menu
- **State/Province**: Enter full name of the **State/Province**
- **City/Locality:** Enter full name of **City/Locality**

The values used for sample configuration are shown below.

Verify the settings on the **Certificate Request Summary** window and click **Commit.**



Click **Finish** to finish the process of defining a new certificate. It is necessary to restart the virtual trunk application on the signaling server to enable use of the new TLS certificate. From the Communication Server 1000 Signaling Server Command Line Interface (CLI) use the command **appstart vtrk restart** to perform this action.



Once system restart completes, return to the System Manager Unified Communication Management home page and expand **Security → Certificates**. Under the **Certificate Endpoints** tab on the **Certificate Management** page, enter associated with the Signaling Server to open the **Endpoint Details** page and verify **Status** of **SIP_TLS** certificate is **signed** as shown below.

For Communication Server 1000E High Availability, there will be two Signaling Servers in each Node. One Signaling Server acts as a Leader and contains the active SIP Signaling Gateway. If this Leader server fails or loses network connection, the Follower Signaling Server will take over the SIP Signaling Gateway process. For this reason, a TLS certificate should be created for this server also using the Follower Signaling Server FQDN. See **Section 11**, Reference **[7]**

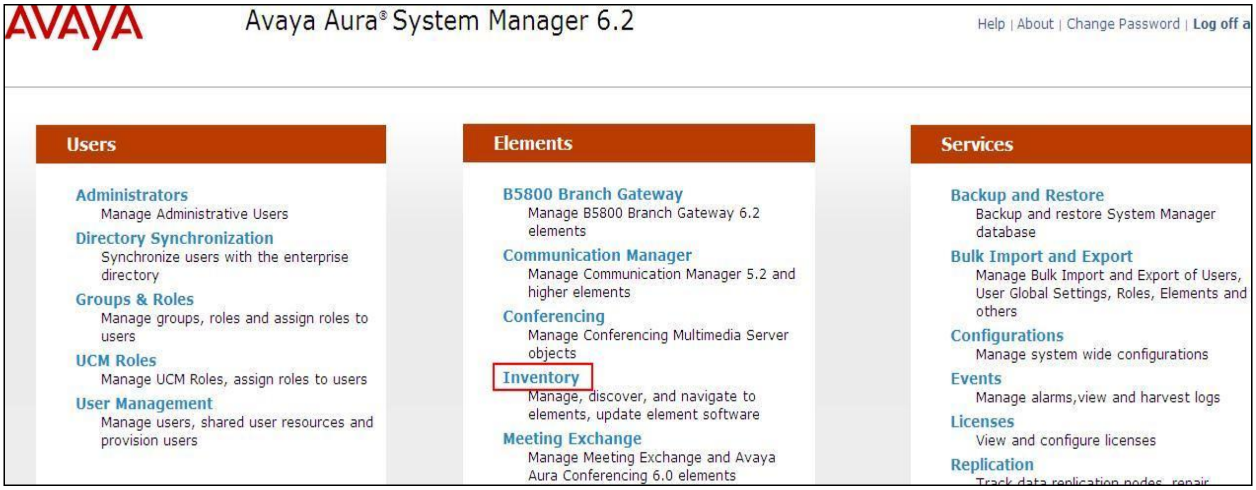
5.2. Install Avaya Communication Server 1000E Security Certificate on Avaya Aura® Session Manager

During the installation of Session Manager the user enters an enrollment password to set up a trust relationship with System Manager as a managed element. As mentioned in **Section 5.1** the CS1000E SIP Signaling Gateway (SSG) has a trust relationship with System Manager UCM. To enable System Manager UCM managed elements, such as CS1000E SSG to be in the same trust domain as the System Manager managed elements, such as Session Manager, the System Manager UCM Certificate Authority (CA) certificate should be imported into the System Manager managed elements trusted certificate list. As System Manager acts as the primary security server for CS1000E there is no need to install a System Manager certificate on the Avaya Communication Server 1000E.

Step 1: Export the System Manager UCM CA security certificate to a file. To export the certificate, expand **Security → Certificates** and select **Private Certificate Authority** tab. Under the **Private Certificate Authority Details** section**,** click **Download** to save contents of the certificate signed by the Primary Security Server to a file as shown below.

On the web browser file download security warning dialog (not shown), click **Save** (not shown) and save the **ca.cer** file to the local desktop.

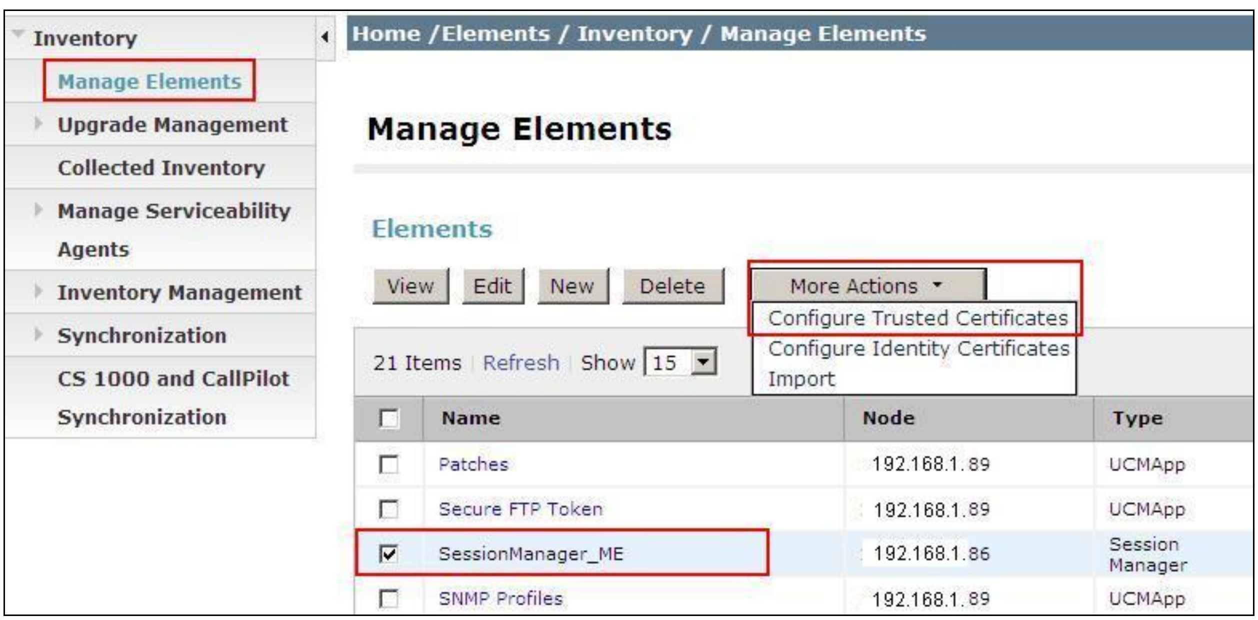
Step 2: Add the CS1000E System Manager UCM CA to the managed elements of System Manager's trusted certificate list. On the System Manager dashboard click on the **Inventory** link.



To install the CS1000E security certificate on System Manager, navigate to **Inventory → Manage Elements** and verify Session Manager has already been defined as an Managed Element as shown below.

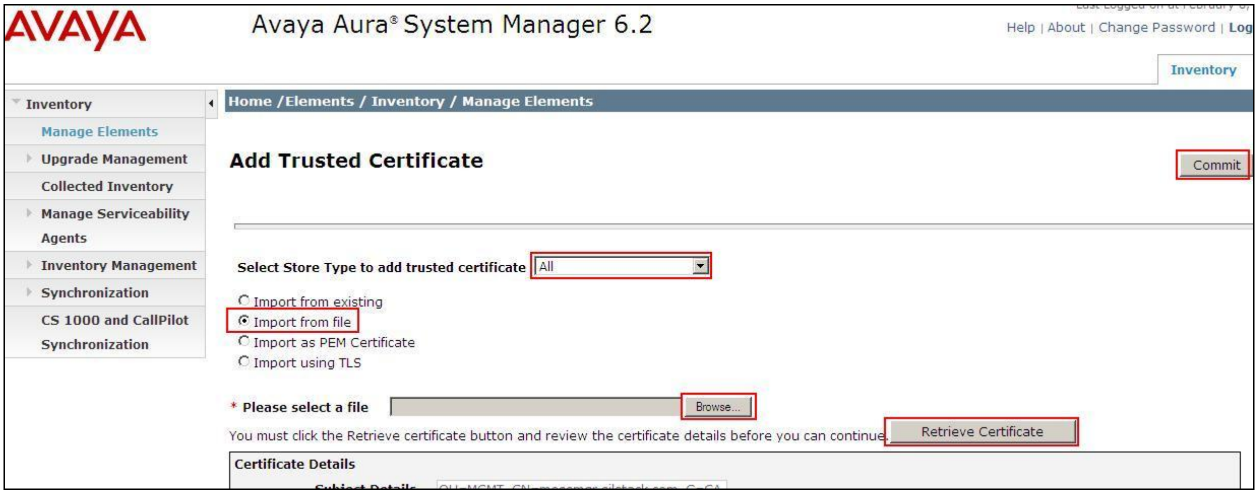
Note: To add Session Manager as a Managed Element, see **Section 11**, **Reference [2]**.

Enter for the Session Manager entry and select **Configure Trusted Certificates** from **More Actions** menu as shown below.



The certificates that are currently installed for Session Manager appear. Click **Add** to add the CS1000E UCM security certificate (not shown). Choose **All** for the select store type to add the trusted certificate. Import the certificate using **Import from file**. Browse to the desktop location where the file was saved from Step 1. Click **Retrieve Certificate** and review the certificate details before you continue.

Click **Commit** to add the trusted certificate.



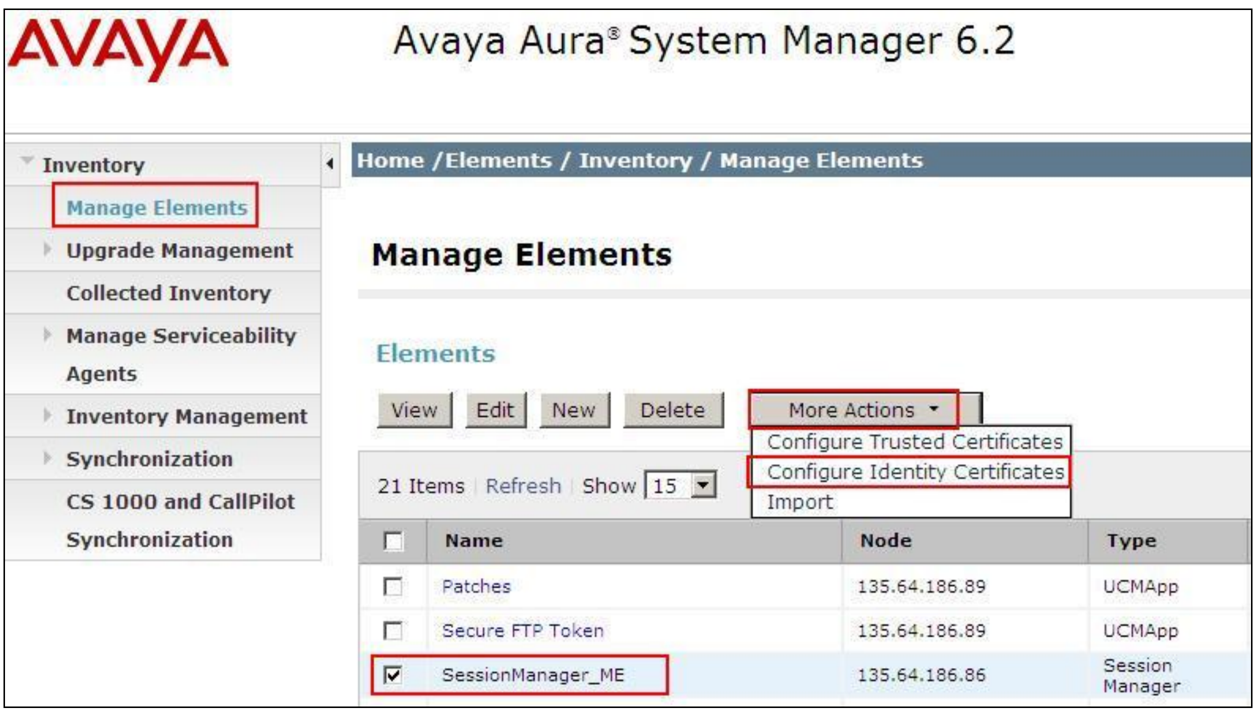
Confirm the Avaya Communication Server 1000E certificate was successfully added as shown below. Click **Done** to return to the Manage Elements page

5.3. Replace the default Avaya Aura® Session Manager Identity Certificate

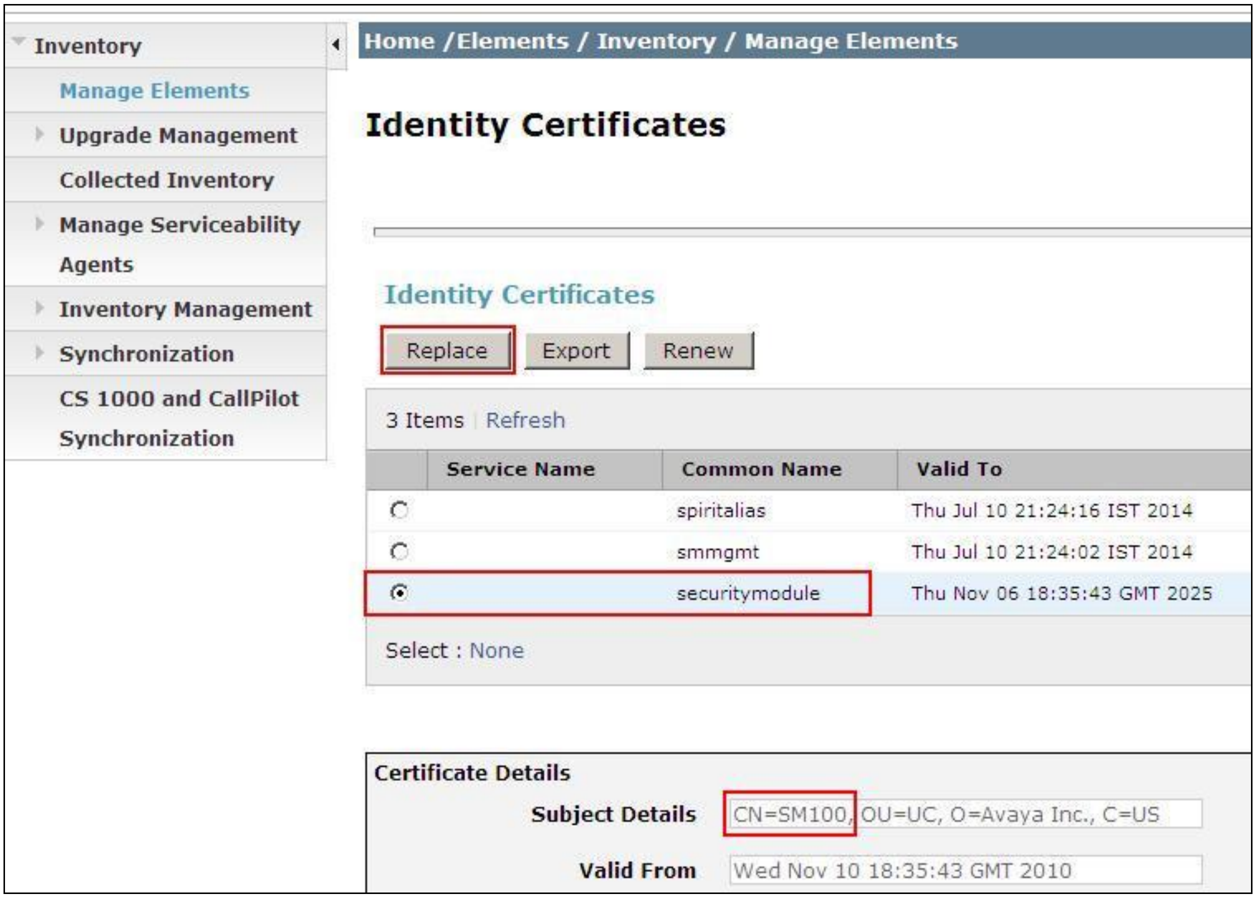
Session Manager contains a default Identity certificate with a hardcoded Common Name (CN) **sm100**. During TLS exchange between Session Manager and CS1000E, the CS1000E SSG performs a check to match the CN against the remote IP address of the Session Manager security module. During this check a Domain Name Server (DNS) lookup is performed for the CN as a Fully Qualified Domain Name (FQDN). As **sm100** is not a valid FQDN on the DNS, this check will not return a response and hence TLS handshake will fail. It is therefore necessary to create a new Internal CA Signed Identity Certificate for the Session Manager using the correct FQDN of the security module. This will allow for a successful DNS lookup during the TLS handshake process when CS1000E is connecting to Session Manager using TLS. For more details on replacing SIP Identity Certificate, refer to **Section 11**, **Reference [3]**

Note: A workaround is to add **sm100** and the IP address of the Session Manager Security Module to the host file on the CS1000E Signaling Server SSG (etc/hosts). This is only recommended for lab use and will not work when CS1000E is connecting to multiple Session Managers as each Session Manager uses the same default Identity Name "sm100".

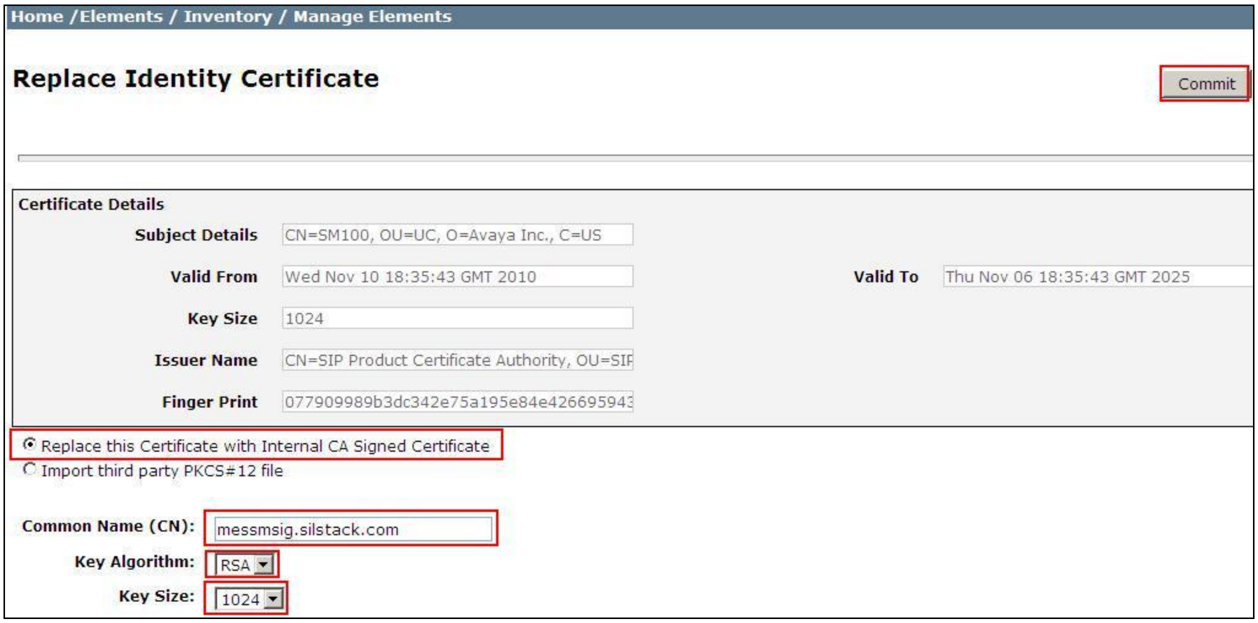
Navigate to **Inventory → Manage Elements**. Enter ☑ for the Session Manager entry and select **Configure Identity Certificates** from **More Actions** menu as shown below.



Select the radio button beside **securitymodule** as shown below. The details of the default Session Manager Security certificate are shown. Note SM100 as the CN. Click on the **Replace** button in order to replace this default identity certificate with a customer defined certificate.



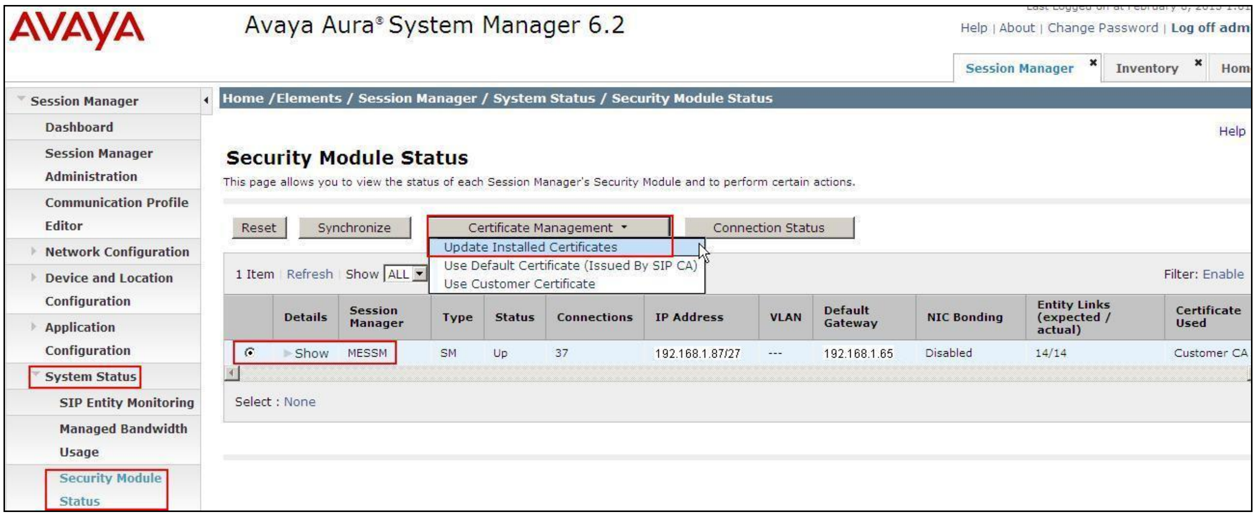
Ensure the radio button beside **Replace this Certificate with Internal CA Signed Certificate** is selected. Refer to **Section 11**, **Reference [11]** if you wish to use a third party signed certificate. Enter the **Common Name (CN)**. This is the FQDN of the Session Manager security module and should be added to the DNS to ensure it resolves to the correct IP Address entered when installing Session Manager. Example used here is "messmsig.silstack.com" and this resolves to IP address 192.168.1.87. SIP Endpoints and servers will connect to this IP address. Select **RSA** from the drop-down menu for **Key Algorithm** and **1024** for **Key Size**. Select **Commit** to save the changes. Click **Done** on the following screen (Not shown).



5.4. Update the Installed Certificates on Avaya Aura® Session Manager

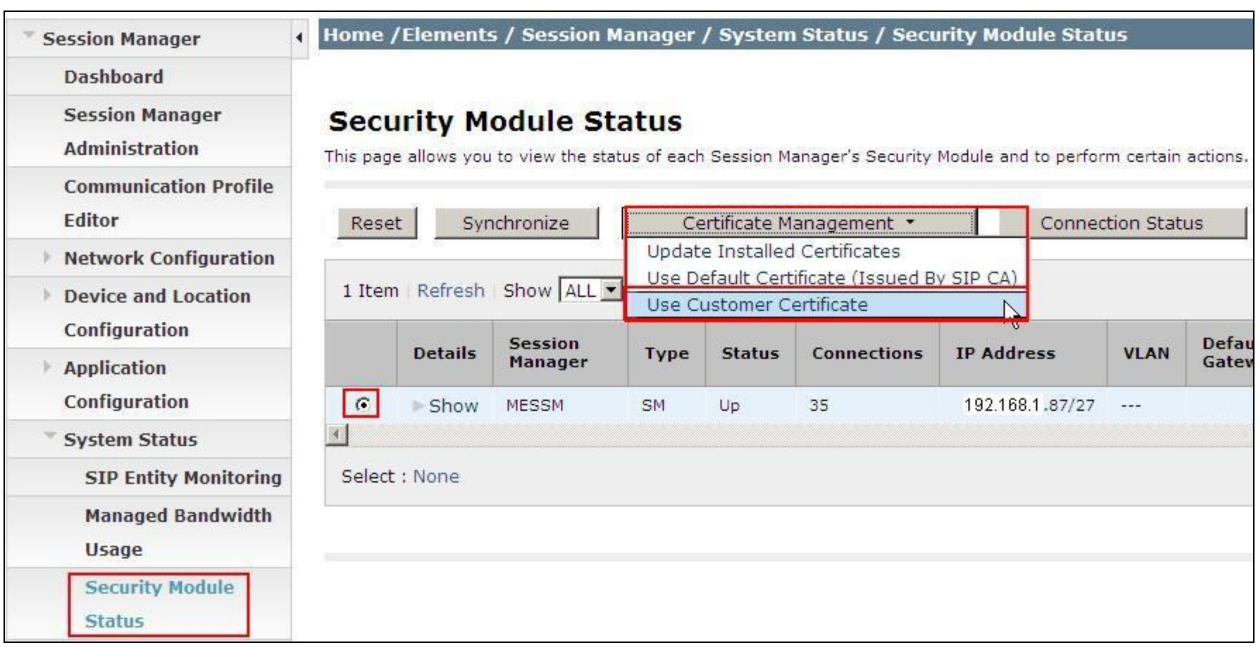
After making the changes in the previous two sections, it is required to update the security certificates to the Session Manager Security Module. Expand **Elements → Session Manager → System Status → Security Module Status**.

Enter to select appropriate Session Manager and select **Update Installed Certificates** under the **Certificate Management** drop-down menu.



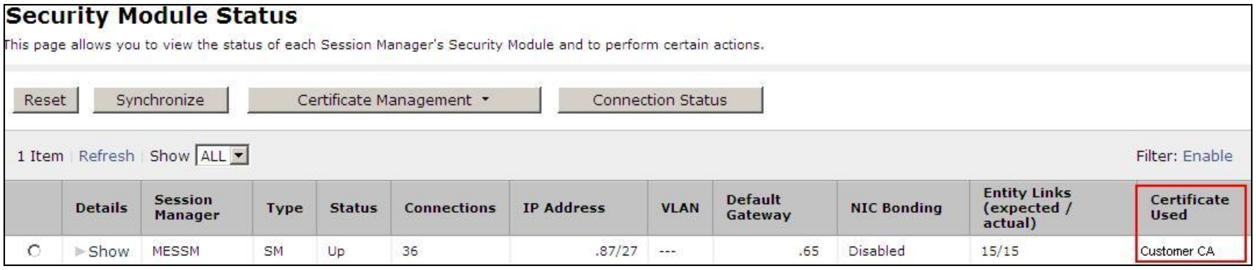
Click **Confirm** on **Confirm Security Module Update Installed Certificates** window (not shown).

From the **Certificate Management** drop-down menu select **Use Customer Certificate**.



From the resulting window click **Confirm** (Not Shown)

Ensure **Customer CA** is now shown under the heading **Certificate Used**.



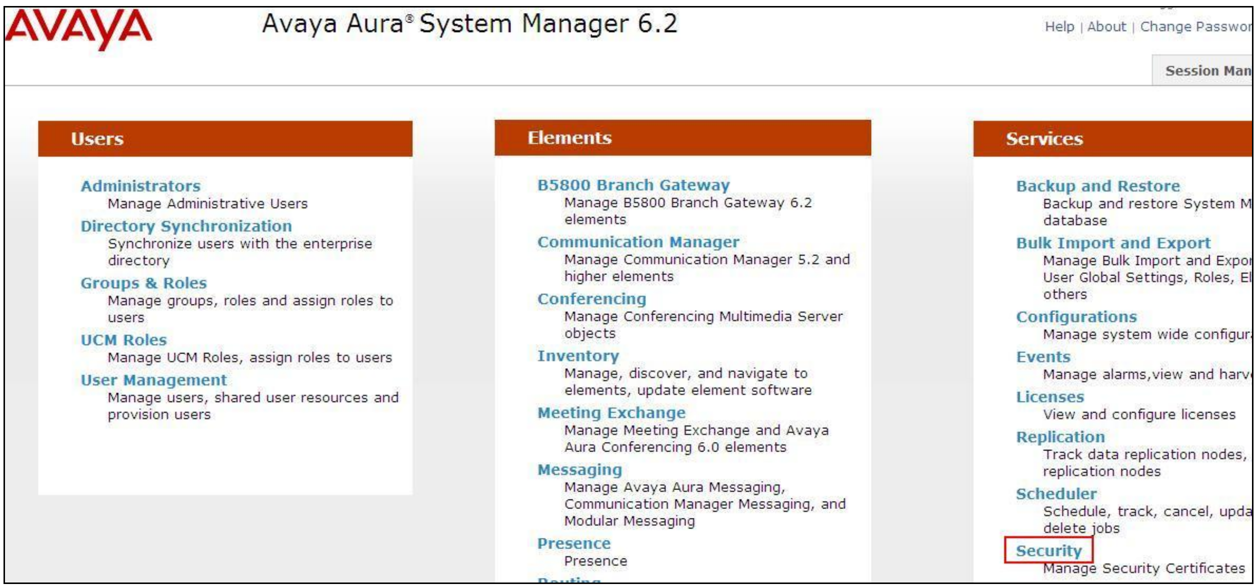
Note: If a second Session Manager is required for failover, a SIP entity link will be required from Session Manager Two to the CS1000E Signaling Server SIP Gateway (Node IP Address). For the second Session Manager, it is necessary to:

1. Install Avaya Communication Server 1000E Security Certificate on Avaya Aura® Session Manager Two, **Section 5.2**
2. Replace the default Avaya Aura® Session Manager Two Identity Certificate, **Section 5.3**
3. Update the Installed Certificates on Avaya Aura® Session Manager Two, **Section 5.4**
4. Configure CS1000 SIP Gateway Proxy Server Route 1, Secondary TLAN IP address as the Session Manager Two SIP Signaling Interface IP address, **Section 6.4**
5. Configure Session Manager Two SIP Entity to CS1000, **Section 7.4 – Section 7.7**

5.5. Distribute Avaya Aura® System Manager Certificate Authority file to Avaya Aura® Communication Manager

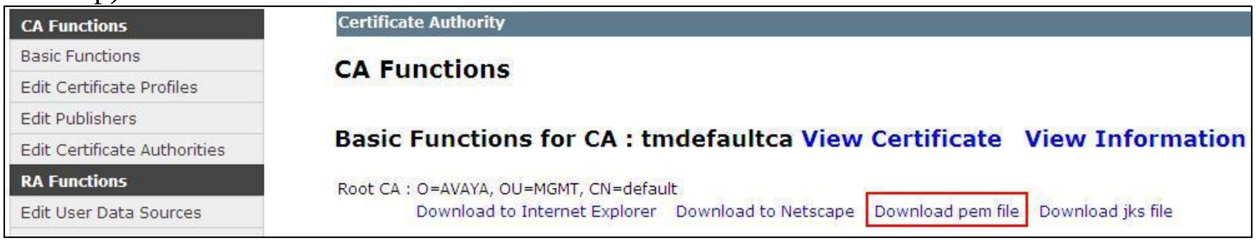
The new Identity Certificate created for Session Manager is signed internally by the System Manager as a Certificate Authority (CA) and uses the FQDN of the System Manager as the issuer. The issuer would be a third party name in the case of an external third party CA. The trusted certificate for the System Manager CA must be distributed to all endpoints connecting to Session Manager, including Communication Manager, in order for mutually authenticated TLS Connections to be made. It is essential that either end is able to establish the identity of the other party during the initial TLS handshake and establish the relationship back to a known trusted authority. CS1000E already has System Manager listed in its list of Certificate Authorities since it joins the System Manager UCM Security Domain. **Section 11**, **Reference [6]**.

Download the System Manager CA file. On System Manager, navigate to **Services → Security**

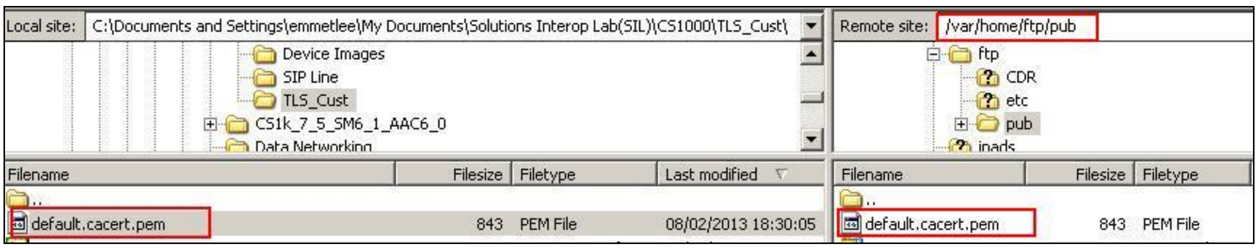


Click on **Certificates** and **Authority**

Click on the link **Download pem file** to save a copy of the System Manager CA, in a Privacy Enhanced Email (PEM) container format, to a directory on your Personal Computer. (Example Desktop)



Use a Secure File Transfer Protocol (SFTP) client, such as Filezila or WinSCP, to connect to the Communication Manager IP address (192.168.1.82 in the example). Copy the .pem file from the local computer to the directory **/var/home/ftp/pub** on Communication Manager.



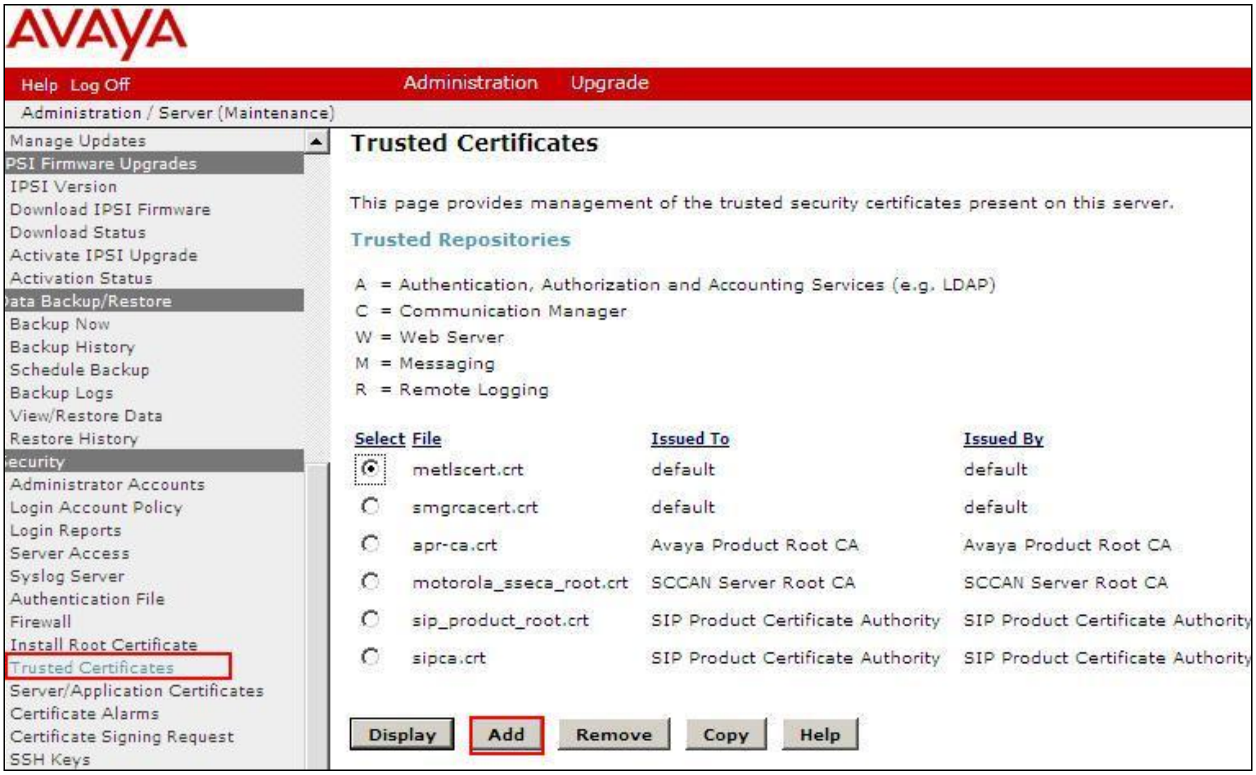
Use a terminal emulator application, such as PuTTY to connect to Communication Manager over a Secure Socket Shell (SSH) connection. Log into Communication Manager using the appropriate username and password. Enter the following command
tlscertmanage –I <*System_Manager_CA.crt*> </var/home/ftp/pub/*default.cacert.pem*>

where <*System_Manager_CA.crt*> is a descriptive name for the resulting crt file and </var/home/ftp/pub/*default.cacert.pem*> is the file path and name of the pem file copied from the local computer to Communication Manager.

```
init@mescm> tlscertmanage -i SMGR_CA.crt /var/home/ftp/pub/default.cacert.pem
certificate is ok
Certificate Authority SMGR_CA.crt is now installed!

init@mescm>
```

On a web browser enter the IP address or FQDN of Communication Manager. Log into Communication Manager using the system username and password (Not shown). From the menu select **Administration→Server (Maintenance)** (Not Shown). On the side menu select **Security → Trusted Certificates**. Select the **Add** button.



Enter the name of the pem file copied over from the local computer to Communication Manager. Example **default.cacert.pem**. Click **Open**

Enter the pem file name again and select the check box beside **Communication Manager** and any other service requiring this certificate. Click **Add**

The digital certificate .cer file for System Manager is now shown in the list of trusted repositories on Communication Manager.

Select	File	Issued To	Issued By	Expiration Date	Trusted By
◯	default.cacert.crt	default	default	Fri Jul 8 2022	A C W M

Communication Manager must be restarted to load this certificate for use. Before restarting Communication Manager, issue a **Save Translation** to save the current configuration. Open a System Access terminal (SAT) session into Communication Manager. Refer to **Section 11, Reference [9]** for details on starting a SAT session. Issue the command **save translation**. The resulting screen should show **Success** as shown below.

```
save translation
                           SAVE TRANSLATION

      Command Completion Status                          Error Code

      Success                                            0
```

On Communication Manager Web interface, select **Server → Shutdown Server** from the menu on the sidebar. Select **Delayed Shutdown**, check the box beside **Restart Server after Shutdown** and select **Shutdown.**

Select **OK** on the resulting warning screen to confirm Communication Manager restart (Not shown).

5.6. Install Root CA Certificate onto Avaya one-X® SIP Deskphones connecting to Avaya Aura® Session Manager

Endpoints connecting to Session Manager using TLS need to trust the certificate authority (CA). As the default CA has changed in this configuration, the trusted certificate for the System Manager CA must be distributed to all endpoints connecting to Session Manager, including the Avaya one-X SIP Deskphones. Use the procedure described in **Section 5.5** to download the System Manager CA root certificate (default.cacert.pem). Copy this certificate to the root directory on the HTTP(S) server used by the phones to download their configuration and software files. Refer to **Section 11, Reference [12]** for more information on downloading a 46xxsettings file to a SIP Deskphone from a HTTP server. The 46xxsettings file for the 96XX or 96X1 SIP deskphones requires some editing.

1) Configure the TLSSRVID = 0 as follows;

```
## TLS Server Identification
##  TLSSRVRID parameter is used for TLS servers identification.
##  If it is set to 1 then TLS/SSL connection will only be established
##  if the server’s identity matches the server’s certificate.
##  If it is set to 0 then connection will be established anyway.
SET TLSSRVRID 0
```

2) Configure the phone to download the CA root certificate from the HTTP(S) Server. In this example the System Manager CA file is named “default.cacert.pem”. Edit this change on the 46xxsetting file under the

```
############### Authentication section ######################
##
##  CERTIFICATE SETTINGS
##
## Authentication Certificates
##   List of trusted certificates to download to phone. This
##   parameter may contain one or more certificate filenames,
##   separated by commas without any intervening spaces.
##   Files may contain only PEM-formatted certificates.
## SET TRUSTCERTS avayaprca.crt,sip_product_root.crt,avayacallserver.crt
SET TRUSTCERTS default.cacert.pem
##
```

<u>Flare Experience</u>
There was no requirement to load a CA root certificate onto Flare Experience on Windows or Flare Experience on Apple iPad to allow TLS to work.

6. Configure Communication Server 1000 SIP Trunks and Call Routing

This section describes the details for configuring CS1000E to route calls to Session Manager over a secure SIP trunk using TLS protocol. In the sample configuration, CS1000E R7.6 was deployed as a High Availability configuration with an active-standby call server running on a VxWorks operating systems on CP PM hardware. The active-active SIP Signaling Server application runs on a Linux operating system on a CP PM server platform.

These instructions assume the CP PM server platform was configured as a member of the security domain managed by the Unified Communications Management (UCM) application on System Manager R6.2. For more information on how to configure System Manager to integrate with the Unified Communications Management application, see **Section 9**, **Reference [6]**. In addition, these instructions also assume the configuration of the Call Server and SIP Signaling Server applications has been completed and CS 1000E is configured to support the 1140 IP Deskphone (UNIStim)and 1230 IP Deskphone. For information on how to administer these functions of Avaya Communication Server 1000E, see **References [5]** through **[8]** in **Section 11.**

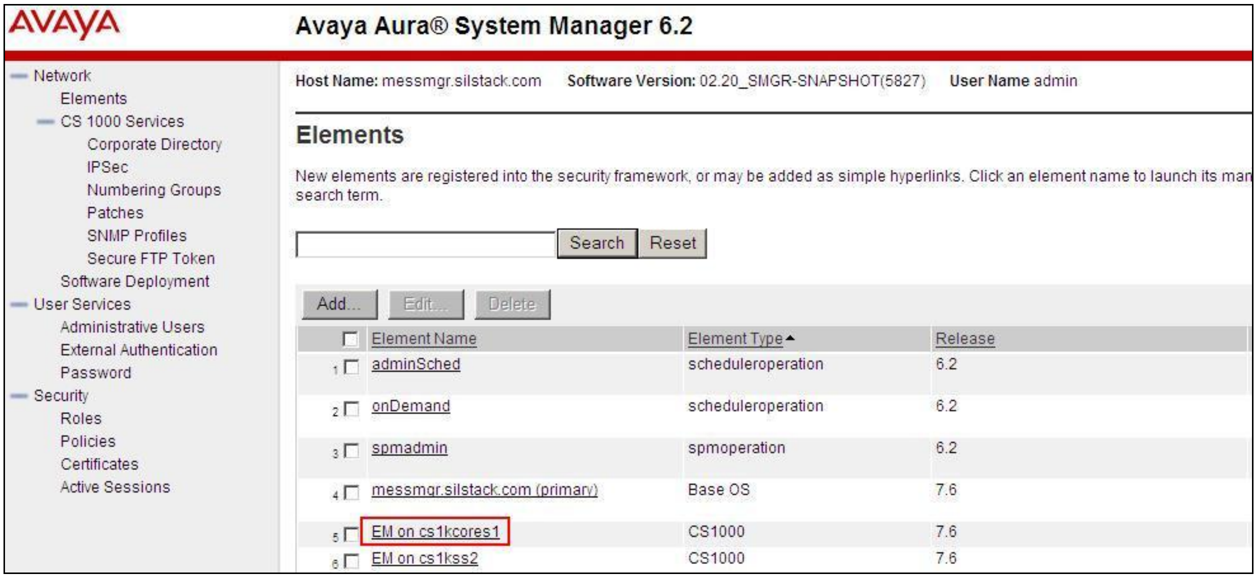
Using the Avaya Unified Communications Management web interface on System Manager, the following administration steps will be described:

- Confirm Node and IP addresses
- Confirm Virtual D-Channel, Routes and Trunks
- Configure Route List Block and Distant Steering Code
- Configure secure SIP Trunk to Avaya Aura® Session Manager
- Save Configuration

Note: Some administration screens have been abbreviated for clarity.

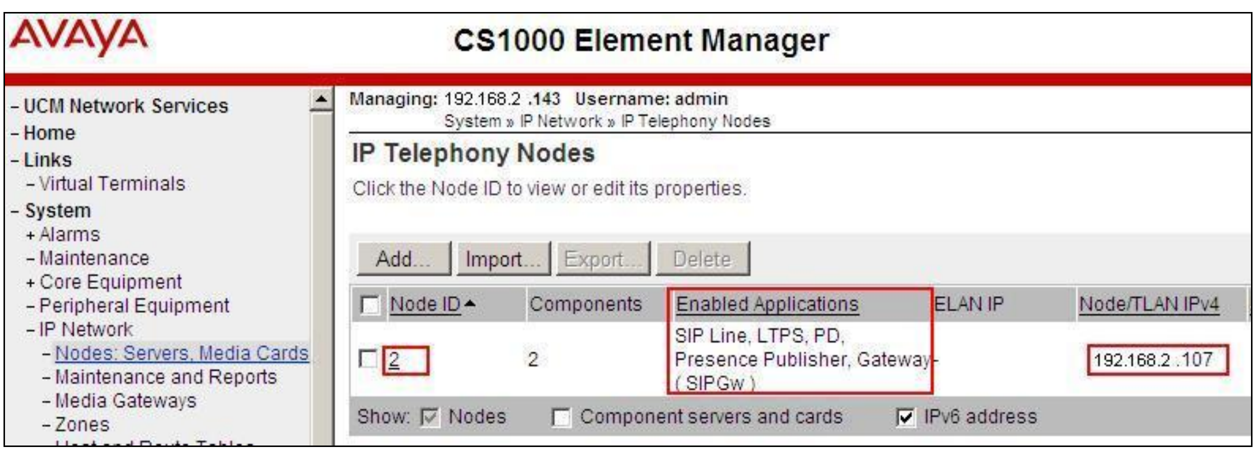
6.1. Confirm Node ID and IP Addresses

Access the Avaya Unified Communications Management (UCM) Services web interface through System Manager as described in **Section 5.1**. The Avaya Unified Communications Management **Elements** page will be displayed. Click on the **Element Name** corresponding to the element manager (EM) for the **CS1000** in the **Element Type** column.



In the newly opened CS1000 Element manager screen expand **System → IP Network** on the left panel and select **Nodes: Servers, Media Cards**.

The **IP Telephony Nodes** page is displayed as shown below. Make a note of the Node/TLAN IP address as this will be used for the SIP trunk configuration. Confirm **SIPGw** is included in the list of enabled applications on this Signaling Server. Click **<Node Id>** in the **Node ID** column to view details of the node. In the sample configuration, Node ID **2** is used.

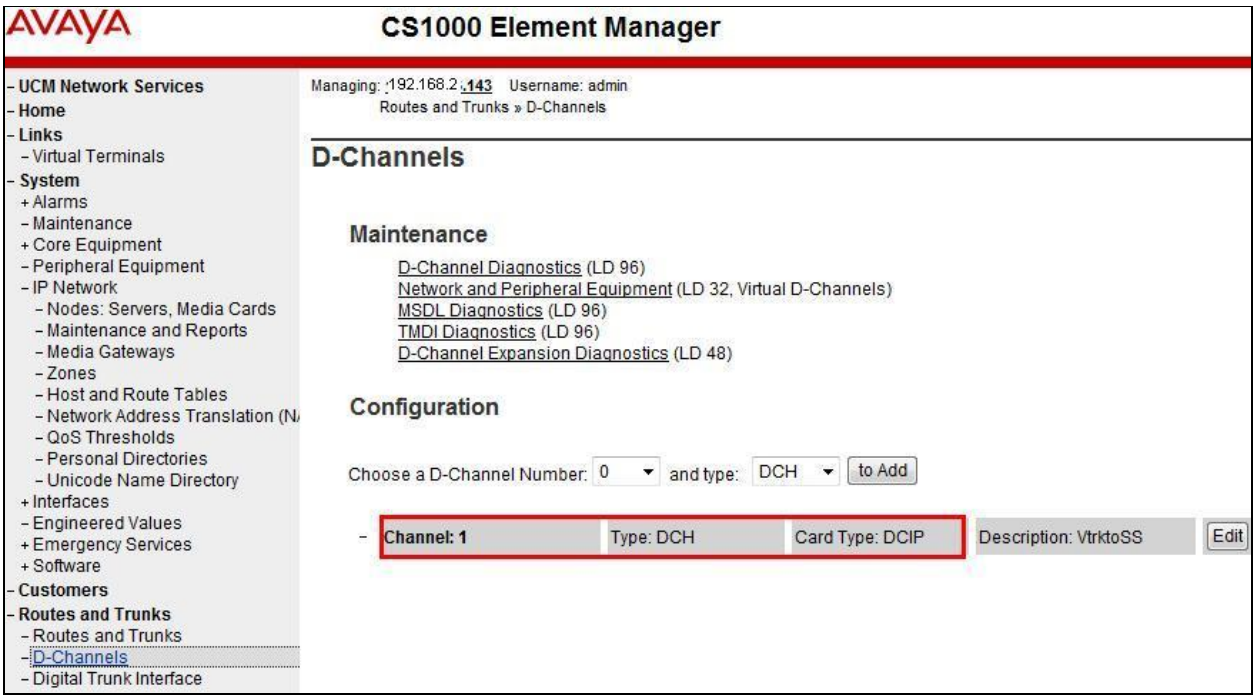


6.2. Confirm Virtual D-Channel, Routes and Trunks

CS 1000E Call Server utilizes a virtual D-channel and associated Route and Trunks to communicate with the Signaling Server. This section describes the steps to verify that this administration has already been completed.

Step 1: Confirm virtual D-Channel Configuration

Expand **Routes and Trunks** on the left navigation panel and select **D-Channels**. The screen below shows all the D-channels administered on the sample configuration. In the sample configuration, there is a single D-channel assigned to **Channel: 1** with **Card Type: DCIP.** Specifying **DCIP** as the type indicates the D-channel is a virtual D-channel.

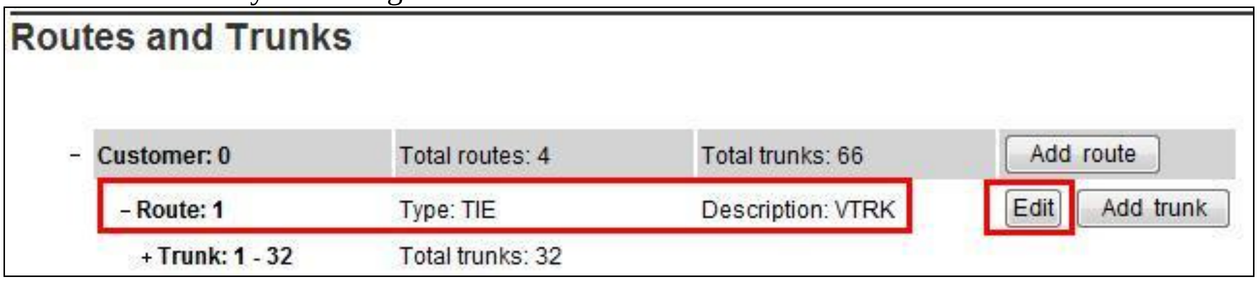


Step 2: Confirm Routes and Trunks Configuration

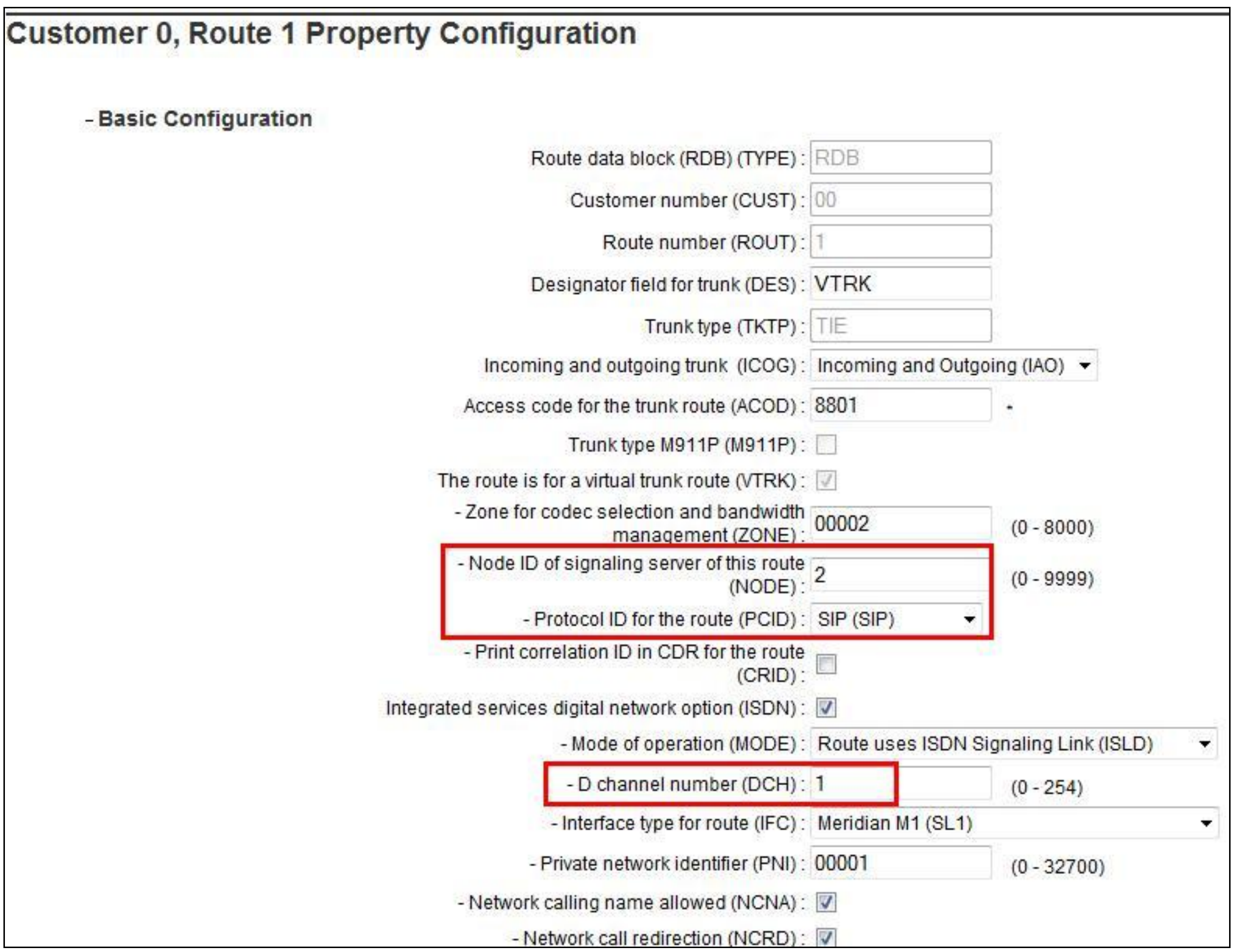
Expand **Routes and Trunks** on the left navigation panel and select **Routes and Trunks** (not shown) to verify a route with enough trunks to handle the expected number of simultaneous calls has been configured.

As shown in the screen below, **Route 1** has been configured with 32 trunks which indicate the system can handle 32 simultaneous calls.

Select **Edit** to verify the configuration.



The details of the virtual Route defined for sample configuration is shown below. Verify **SIP (SIP)** has been selected for **Protocol ID for the route (PCID)** field and the **Node ID of signaling server of this route (NODE)** and **D channel number (DCH)** fields match the values identified in the previous section.



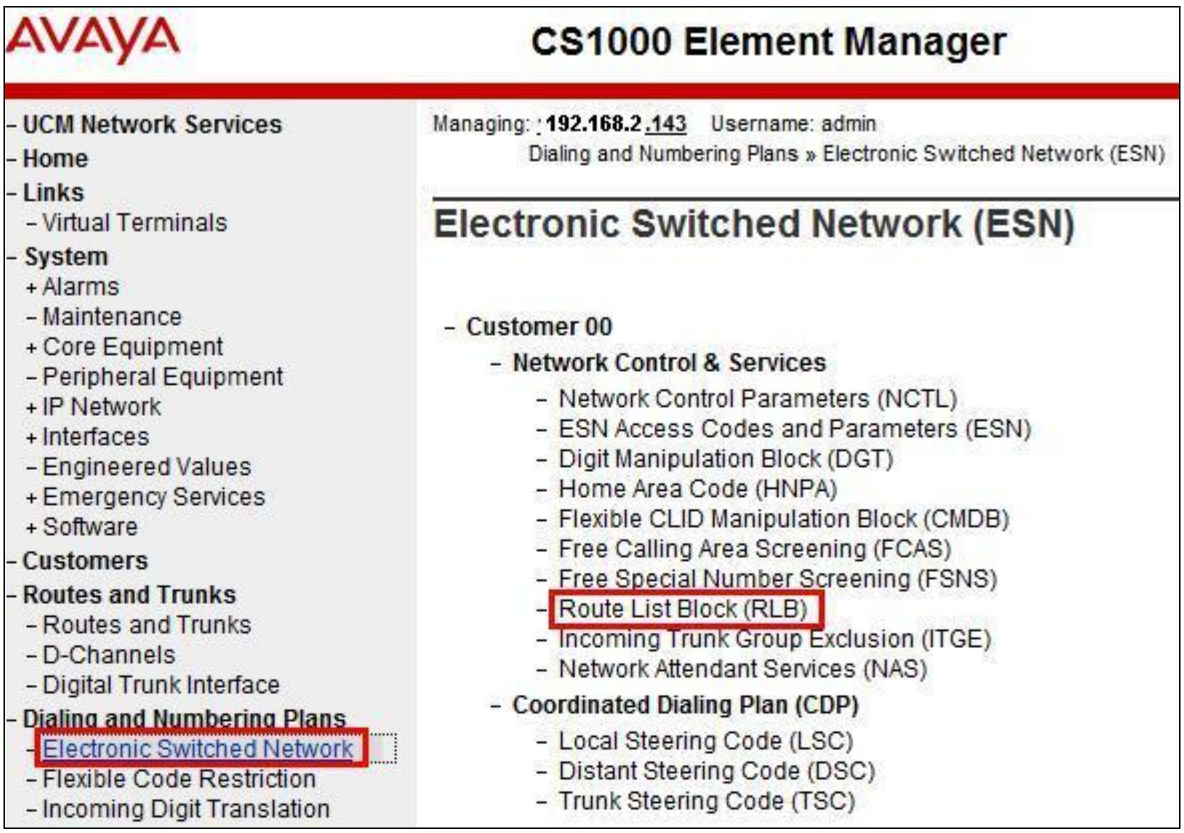
6.3. Configure Route List Block and Distant Steering Code

This section provides the configuration of the routing used for sending calls over the SIP Trunk between CS1000E and Session Manager.

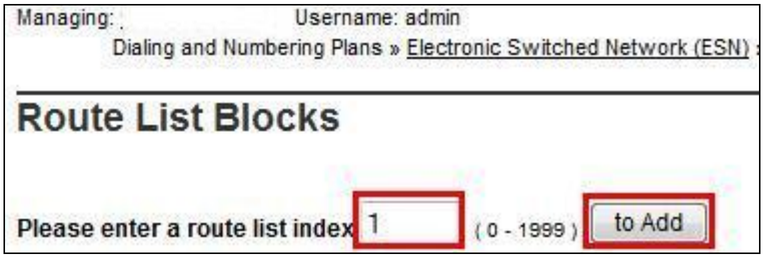
Note: The routing rule defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

Step 1: Create Route List Index

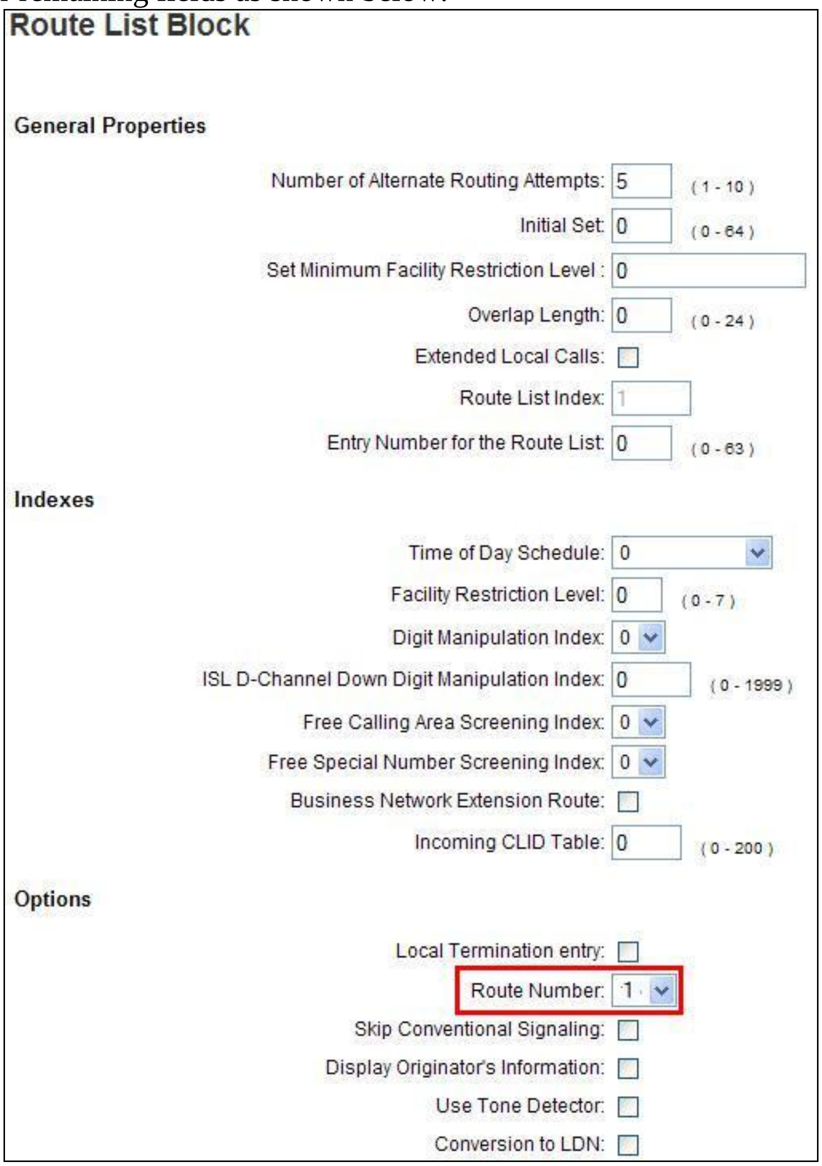
Expand **Dialing and Numbering Plans** on the left navigational panel and select **Electronic Switched Network.** Select **Route List Block (RLB)** on the **Electronic Switched Network (ESN)** page as shown below.



The **Route List Blocks** screen is displayed. Enter an available route list index number in the **Please enter a route list index** field and click **to Add** as shown below.



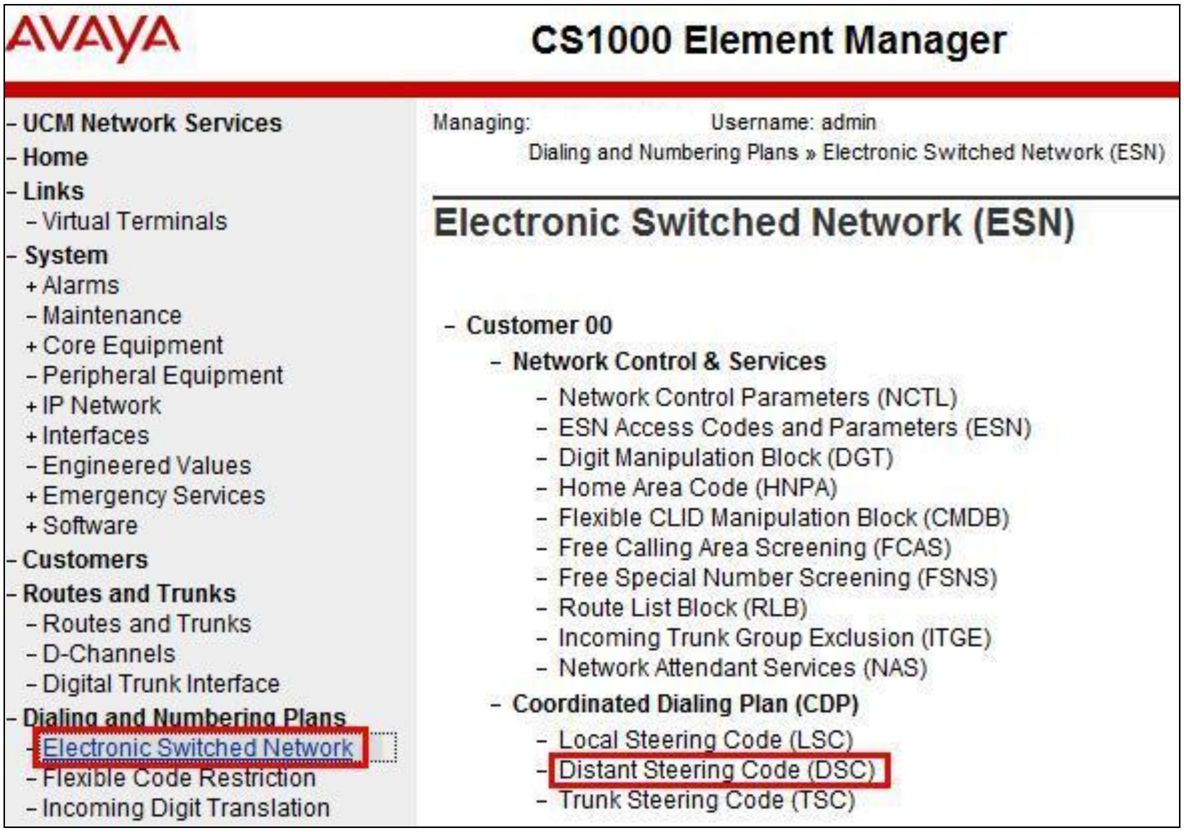
Under the **Options** section, select **Route Number** of the route identified in **Section 6.2** and use default values for remaining fields as shown below.



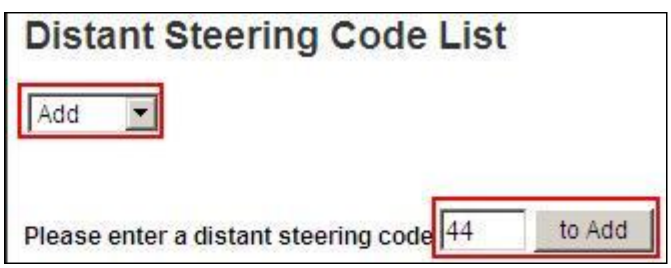
Click **Save** (not shown) to save new Route List Block definition.

Step 2: Create Distant Steering Code

Expand **Dialing and Numbering Plans** on the left and select **Electronic Switched Network.** Select **Distant Steering Code (DSC)** under the **Coordinated Dialing Plan (CDP)** section on the **Electronic Switched Network (ESN)** page as shown below.



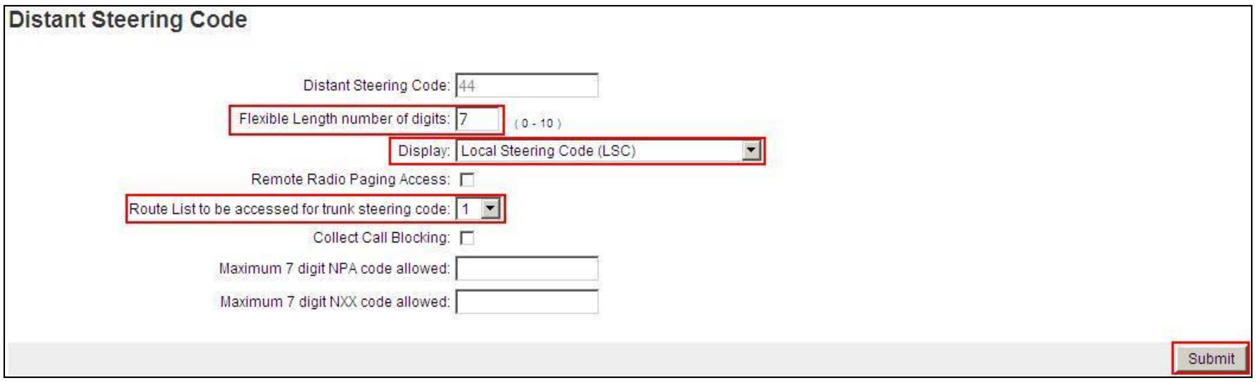
Select **Add** from the drop-down menu and enter the dialed prefix for CS1000E calls to be routed over SIP trunk to Session Manager in the **Please enter a distant steering code** field. For the sample configuration, **44** will be used since SIP endpoints registered to Session Manager were assigned extensions starting with **44**. Click **to Add** as shown below.



Enter the following values and use default values for remaining fields.

- **Flexible Length number of digits:** Enter number of digits in dialed numbers In the sample configuration 7-digit dialplan is used on Avaya Aura®
- **Route List to be accessed for trunk steering code:** Select **number** of the Route List Index created in **Step 1**.

Click **Submit** to save new Distant Steering Code definition.



When a user dials a seven-digit number beginning with 44, this call will be directed out over route 1 which is the SIP trunk to Session Manager.

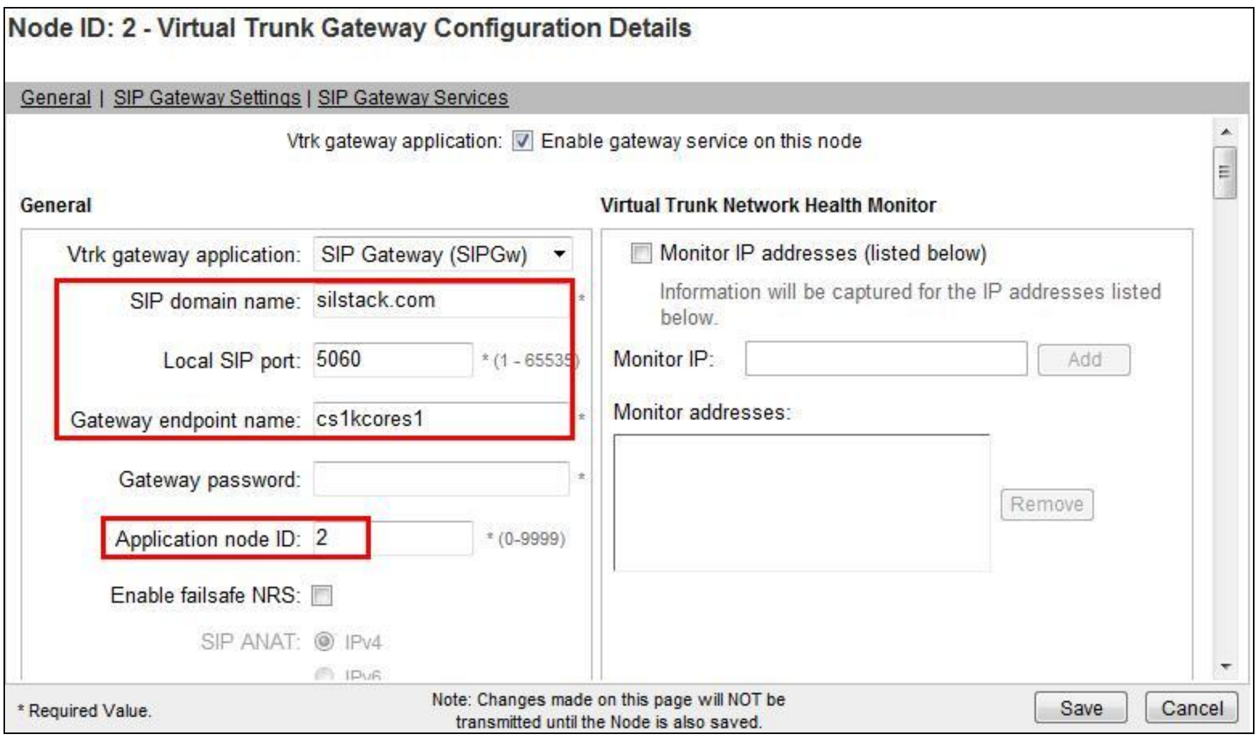
6.4. Configure Secure SIP Trunk from Communication Server 1000E to Avaya Aura® Session Manager

On System Manager UCM Element Manager webpage: Expand **System → IP Network → Nodes: Servers, Media Cards** and click **2** in the **Node ID** column (not shown) to return to the Node Details page. Using the scroll bar on the right side of the screen, navigate to the **Applications** and select the **Gateway (SIPGw)** link (not shown).

Step 1: On the **Node ID: 2 - Virtual Trunk Gateway Configuration Details** page, enter the following values and use default values for remaining fields**.**

- **SIP domain name:** Enter name of domain. In the sample configuration, **silstack.com** is used.
- **Local SIP port:** Enter **5060**
- **Gateway endpoint name:** Enter descriptive name.
- **Application node ID:** Enter the node ID. In the sample configuration, **2** is used.

The values defined for the sample configuration are shown below.

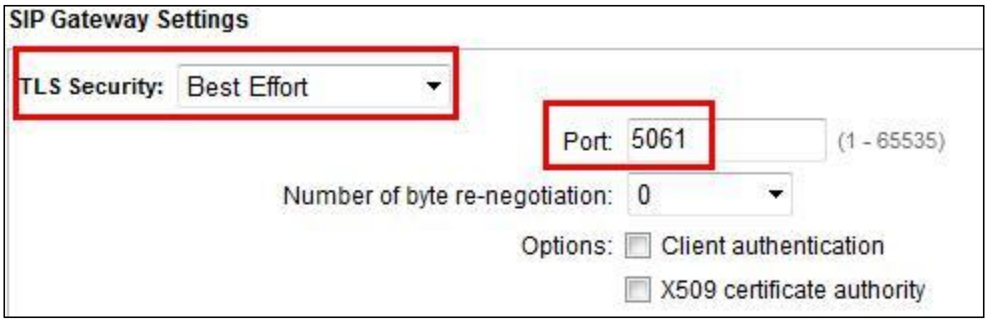


Step 2: Scroll to the **SIP Gateway Settings** section, enter the following values and use default values for remaining fields**.**

- **TLS Security:** Select **Best Effort**
- **Port:** Enter **5061**

Note: the TLS port number specified in **SIP Gateway Settings** section should not use the same port number specified above for the **Local SIP port** field.

The values defined for the sample configuration are shown below.

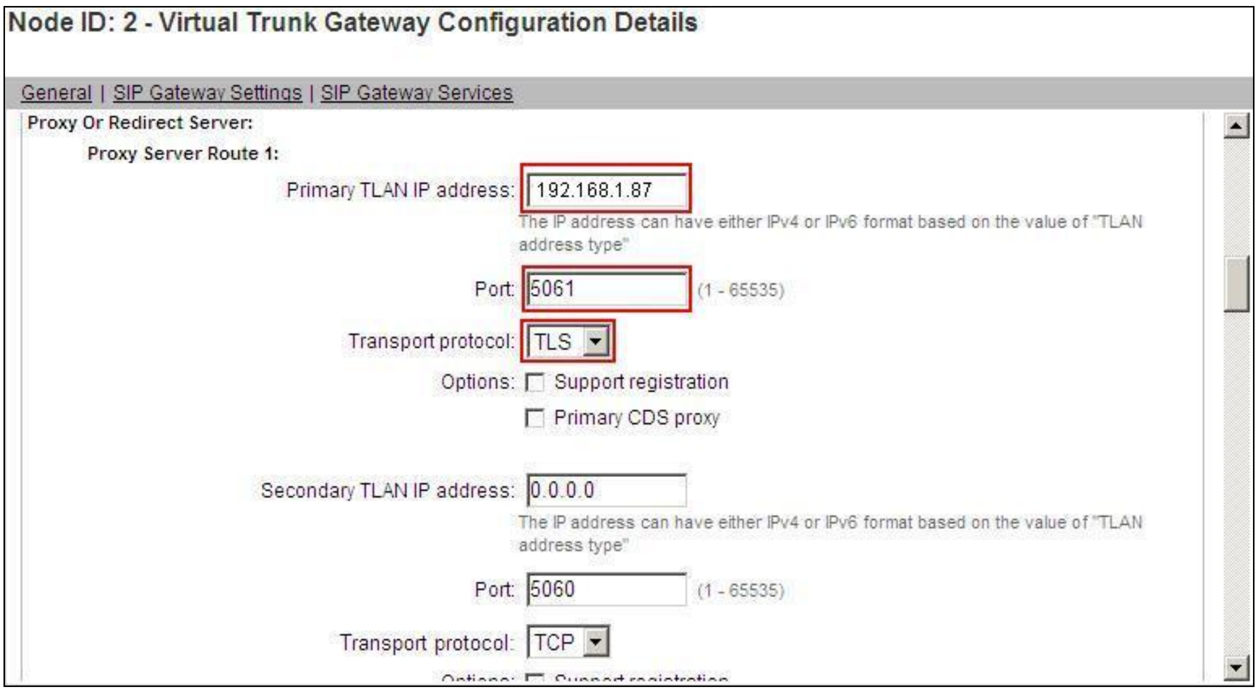


Step 3: Scroll down to **Proxy or Redirect Server**: section of the page. Under **Proxy Server Route 1:** section, enter the following values and use default values for remaining fields.

- **Primary TLAN IP address:** Enter IP address of the Session Manager SIP signaling interface. In sample configuration, **192.168.1.87** is used.
- **Port:** Enter **5061**
- **Transport protocol:** Select **TLS**

Note: the port number configured as the TLS port for the SIP Proxy Server should match the port number defined on Session Manager for the SIP Entity Link between CS1000E and Session Manager. See **Section 6.4** for more information.

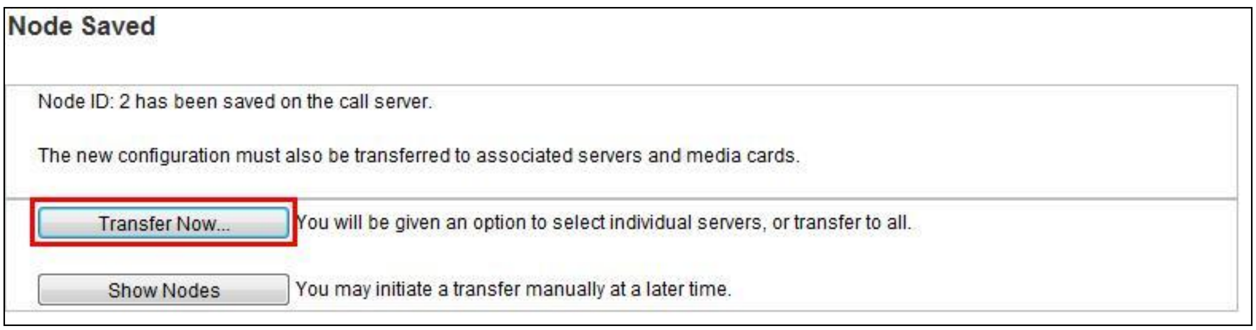
The values defined for the sample configuration are shown below. If you have a secondary Session Manager, this IP address can be added in the **Secondary TLAN IP Address** field. Otherwise this field can be set as 0.0.0.0.



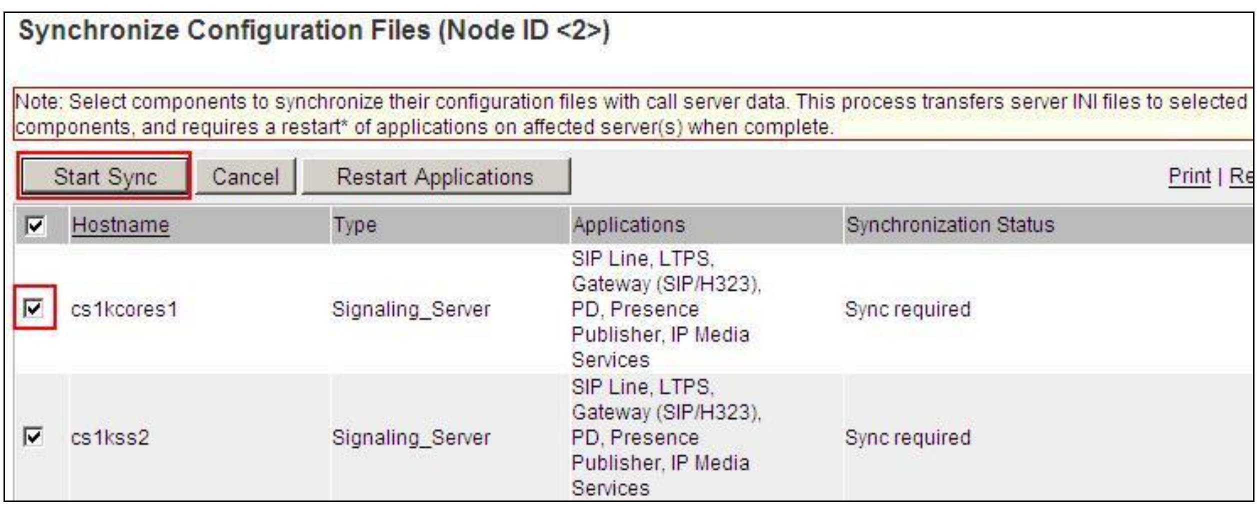
Repeat these steps for the **Proxy Server Route 2.**

Step 4: Scroll down to the **SIP URI Map** section of the page and enter the appropriate names for the **UDP** and **CDP Private domain names** fields. The values defined for the sample configuration are shown below.

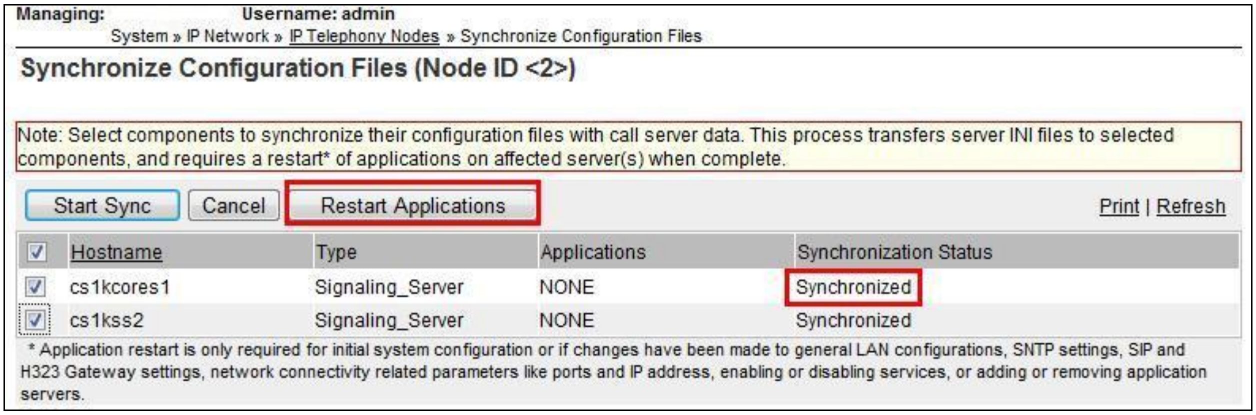
Step 5: Scroll to the bottom of the page and click **Save** (not shown) to save SIP Gateway configuration settings. Click **Save** on the **Node Details** screen (not shown). Select **Transfer Now** on the **Node Saved** page as shown below.



The **Synchronize Configuration Files (Node ID <id>)** page is displayed. Enter associated with the appropriate Signaling Server and click **Start Sync.** The screen will automatically refresh until the synchronization is finished.

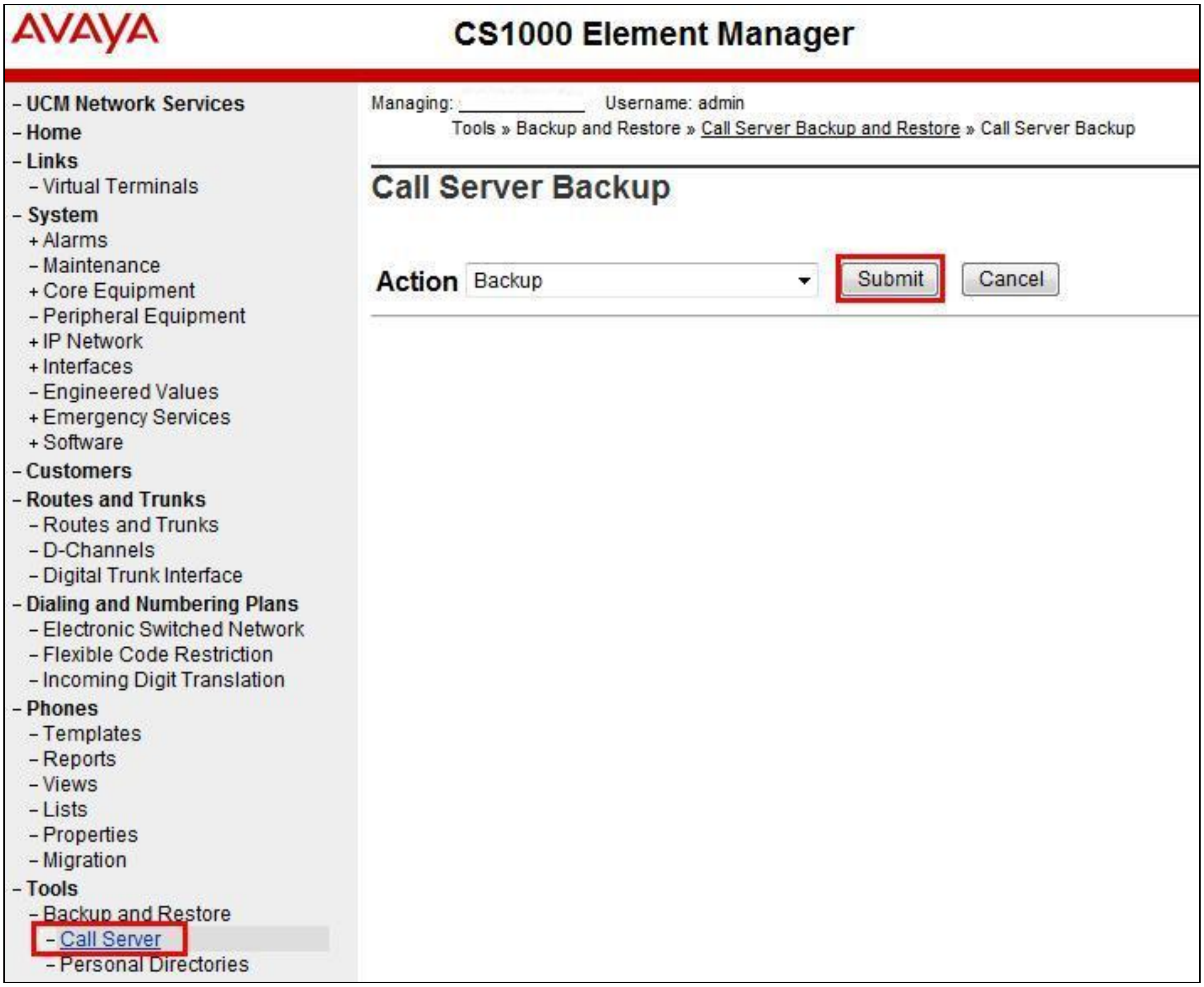


The **Synchronization Status** field will update from **Sync required** to **Synchronized**. After synchronization completes, enter associated with the appropriate Signaling Server and click **Restart Applications** to use the new SIP gateway settings.



6.5. Save Configuration

Expand **Tools → Backup and Restore** on the left navigation panel and select **Call Server.** Select **Backup** (not shown) and click **Submit** to save configuration changes to the call server database as shown below.



Backup process will take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

Configuration of Avaya Communication Server 1000E is complete.

7. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Avaya Aura® Session Manager to receive and route calls over the secure SIP trunk between Avaya Communication Server 1000E and Avaya Aura® Communication Manager. These instructions assume other administration activities have already been completed such as defining the SIP entity for Session Manager, defining the network connection between System Manager and Session Manager, and adding SIP endpoints. For more information on these additional actions, see **Section 11, References [1]** through **[4].**

The following administration activities will be described:

- Define SIP Domain
- Define Location for SIP Entities
- Configure the Adaptation Module designed for Avaya Communication Server 1000E R7.6
- Define SIP Entity corresponding to Avaya Communication Server 1000E
- Define SIP Entity corresponding to Avaya Aura® Communication Manager
- Define an Entity Link describing the secure SIP trunk between Avaya Communication Server 1000E and Session Manager
- Define an Entity Link describing the secure SIP trunk between Avaya Aura® Communication Manager and Session Manager
- Define Routing Policies, which control call routing between the SIP Entities
- Define Dial Patterns, which govern to which SIP Entity a call is routed

Note: Some administration screens have been abbreviated for clarity.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of Avaya Aura® System Manager. Login with the appropriate credentials.

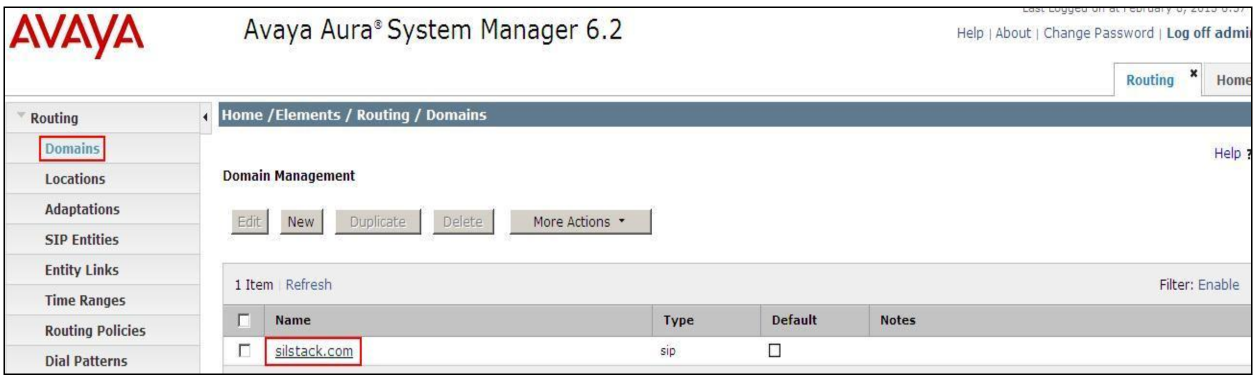
7.1. Define SIP Domain

Expand **Elements → Routing** and select **Domains** from the left navigation menu.

Click **New** (not shown)**.** Enter the following values and use default values for remaining fields.

- **Name** Enter the Domain Name specified for the SIP Gateway in **Section 6.4.** In the sample configuration, **silstack.com** is used.
- **Type** Verify **SIP** is selected.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



7.2. Define Location

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing. Expand **Elements → Routing** and select **Locations** from the left navigational menu.

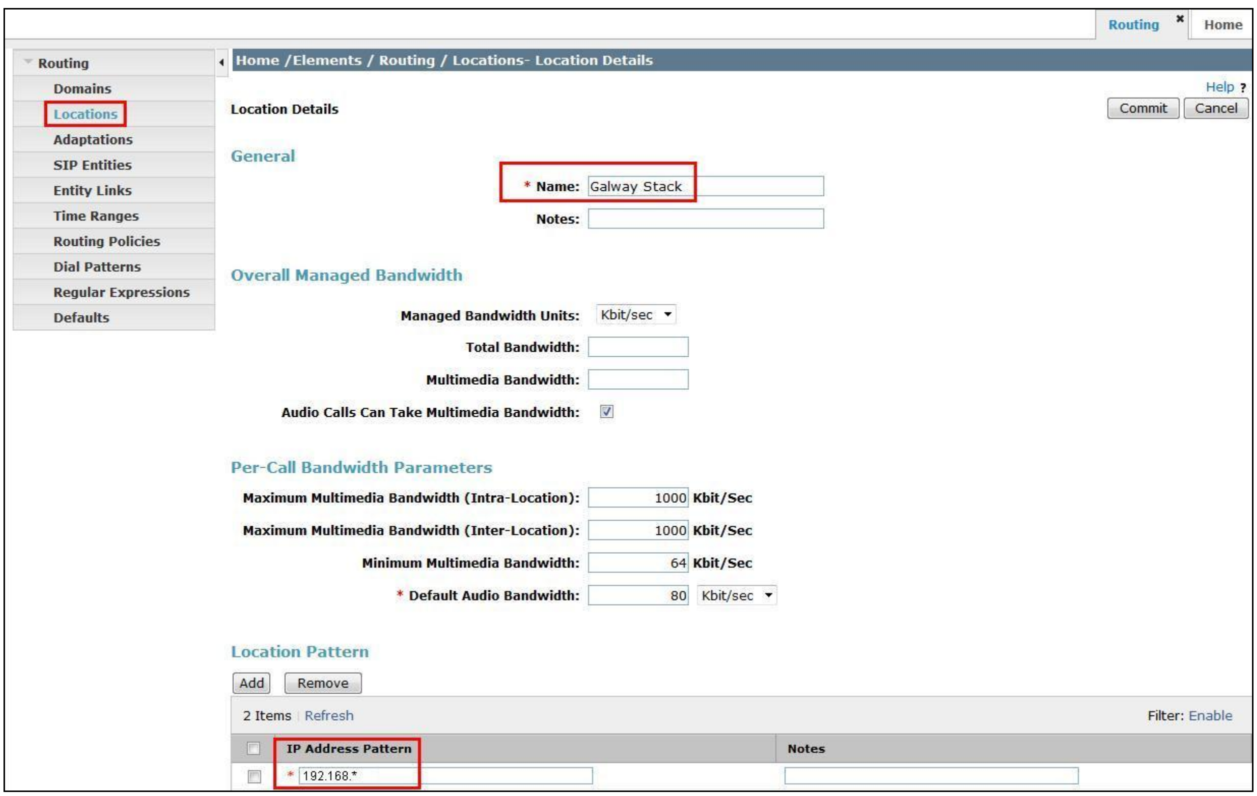
Click **New** (not shown)**.** In the **General** section**,** enter the following values and use default values for remaining fields**.**

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location. For the sample configuration, **192.168.*** is used.
- **Notes** Add a brief description. [Optional]

Click **Commit** to save.
The screen below shows the Location defined for servers in the sample configuration.



7.3. Configure Adaptation Module

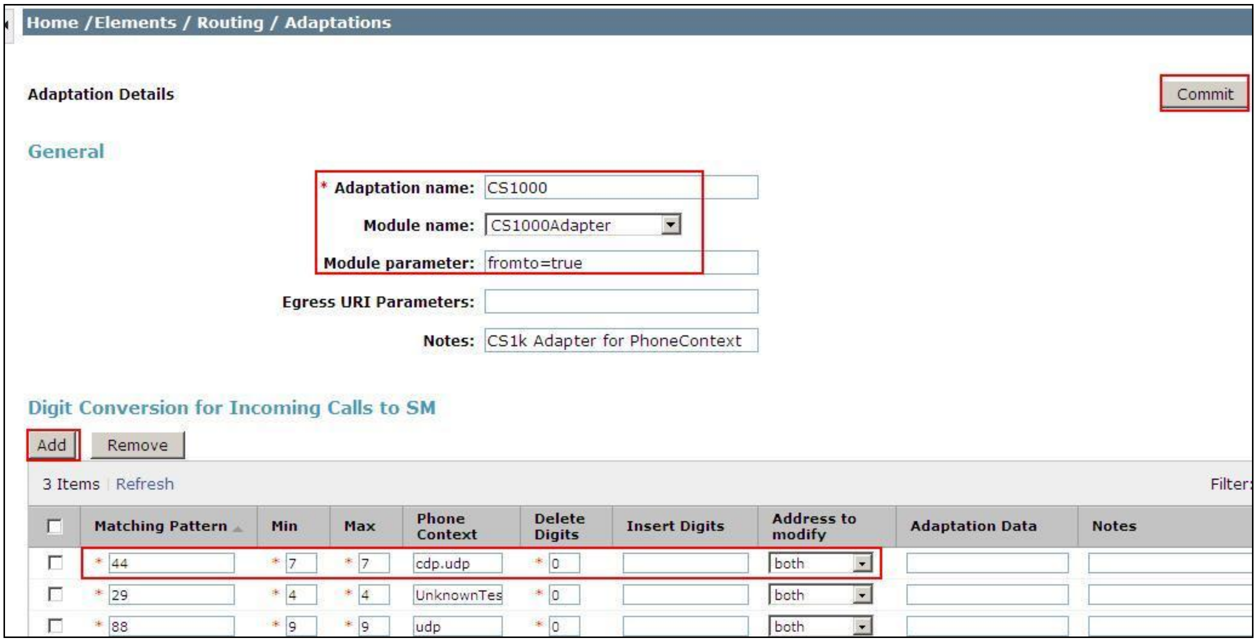
To enable calls between stations on Avaya Communication Server 1000E and SIP endpoints registered to Session Manager, Session Manager should be configured to use an Adaptation Module designed for Avaya Communication Server 1000E to convert SIP headers in messages sent by Avaya Communication Server to the format used by other Avaya products and endpoints. Expand **Elements → Routing** and select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select CS1000Adapter from drop-down menu. If CS1000 is not shown, select <**click to add module**> from the **Module Name** drop-down menu and then configure a module name called CS1000Adapter

In the **Digit Conversion for Incoming Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls incoming from CS1000E to Session Manager. In sample configuration **44** is used.
- **Min** Enter minimum number of digits that must be dialed.
- **Max** Enter maximum number of digits that may be dialed. In the sample configuration, **7** is used as extensions on Communication Manager are 7-digits in length.
- **Phone Context** Enter value of **Private CDP domain name** defined in **Section 6.4.**
- **Delete Digits** Enter **0**, unless digits should be removed from dialed number before call is routed by Session Manager
- **Address to modify** Select **both**

Click Commit. The Adaptation Module defined for sample configuration is shown below.



7.4. Define SIP Entities

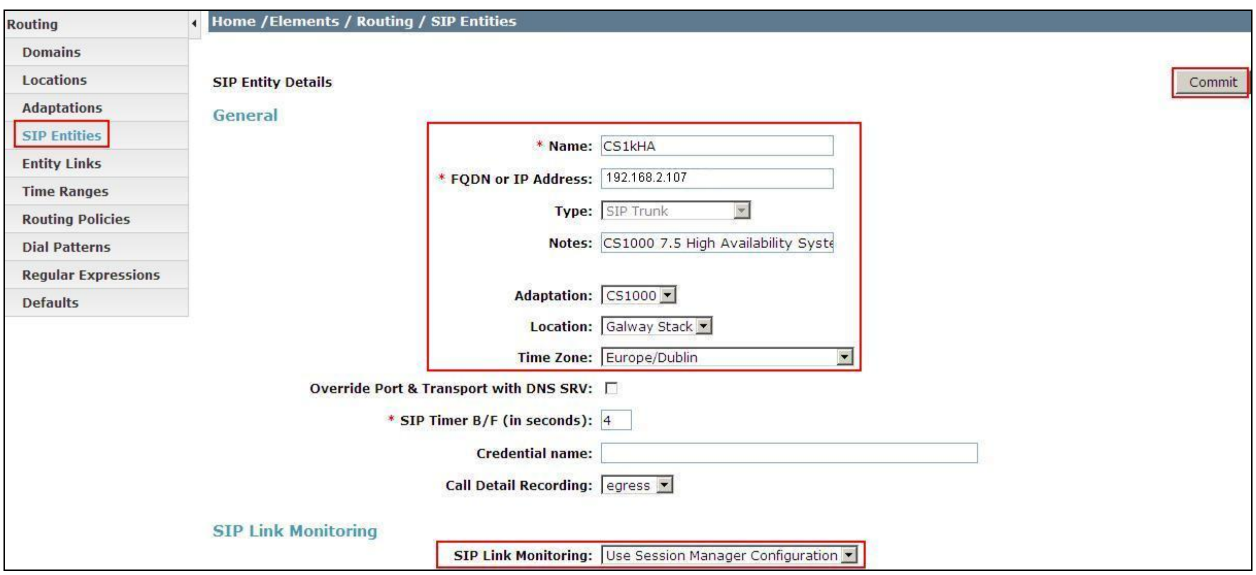
A SIP Entity must be added for CS1000E and another SIP Entity for Communication Manager. Expand **Elements → Routing** and select **SIP Entities** from the left navigation menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields.

- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter TLAN IP address of CS1000E Node identified in **Section 6.4**
- **Type:** Select **SIP Trunk**
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** Select the Adaptation Module defined in **Section 7.3**
- **Location:** Select the Location defined for CS1000E in **Section 7.2**

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select **Use Session Manager Configuration**

Click **Commit** to save the definition of the new SIP Entity. The following screen shows the SIP Entity defined for Avaya Communication Server 1000E in the sample configuration.

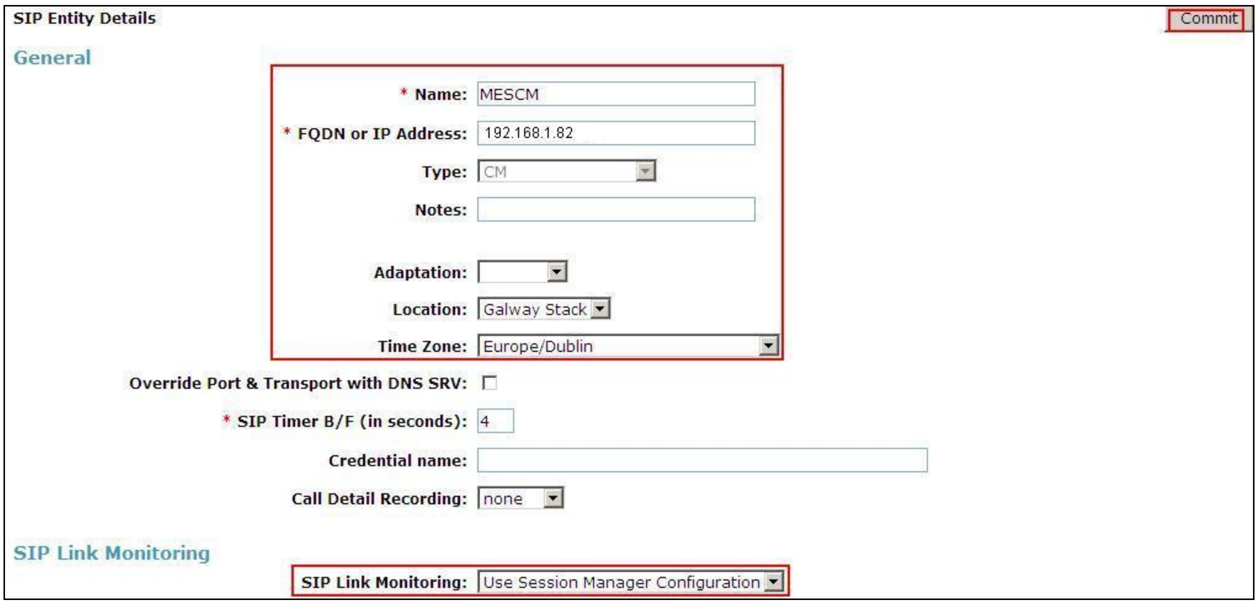


Repeat this procedure to add the Sip Entity for Communication Manager.

- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter IP address or FQDN for Communication Manager
- **Type:** Select **CM**
- **Notes:** Enter a brief description. [Optional]
- **Adaptation:** No Adaptation is required for CM
- **Location:** Select the Location defined in **Section 7.2**

In the **SIP Link Monitoring** section:

- **SIP Link Monitoring:** Select **Use Session Manager Configuration**

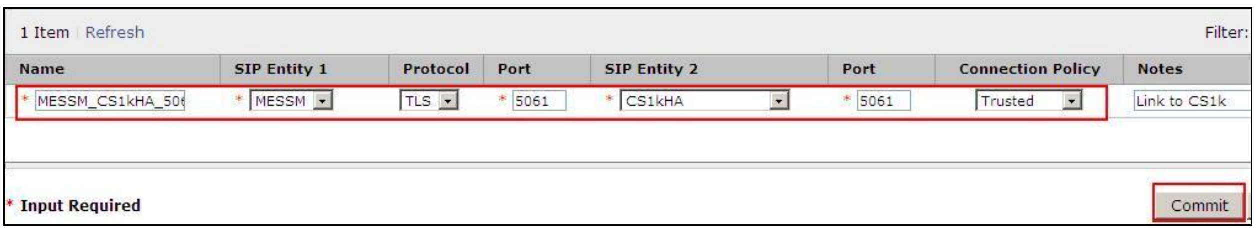


7.5. Define Entity Links

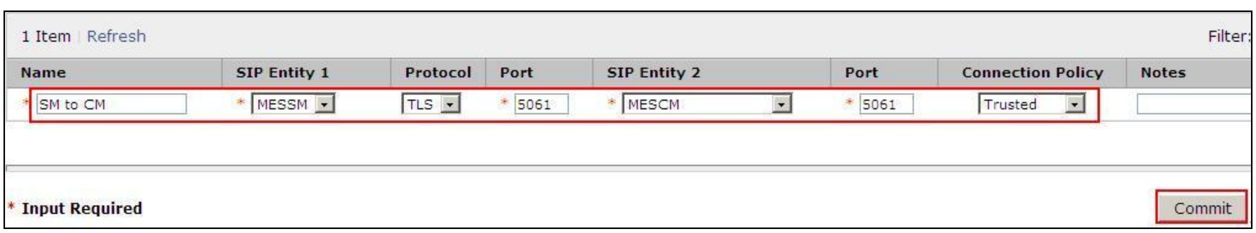
The SIP trunk between Session Manager and Avaya Communication Server 1000E and between Session Manager and Communication Manager is described by an Entity link. Expand **Elements → Routing** and select **Entity Links** from the left navigation menu. Click **New** (not shown).Enter the following values.

- **Name** Enter an identifier for the link to each telephony system.
- **SIP Entity 1** Select SIP Entity defined for Session Manager.
- **SIP Entity 2** Select the SIP Entity defined for CS1000E in **Section 7.4**.
- **Protocol** After selecting both SIP Entities, select **TLS** as the required protocol.
- **Port** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is **5061**.
- **Trusted** Enter **Trusted.**
- **Notes** Enter a brief description. [Optional]

Click **Commit** to save **Entity Link** definition. The following screen shows the entity link defined for the SIP trunk between **Session Manager** and **CS1000E**.



Repeat this process for the entity link from **Session Manager** to **Communication Manager**.



7.6. Define Routing Policy

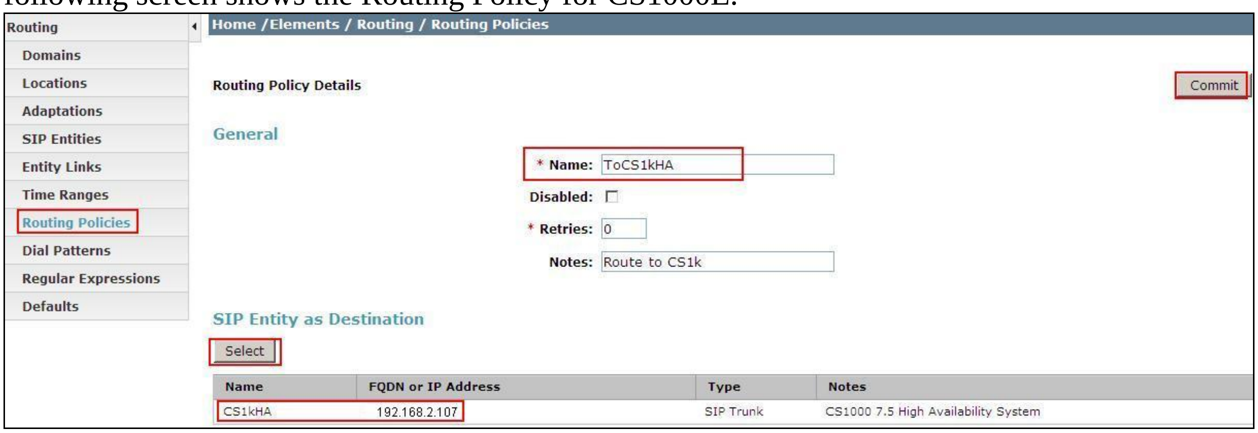
Routing policies describe the conditions under which calls will be routed to CS1000E or to Communication Manager from Session Manager. To add a routing policy, expand **Elements → Routing** and select **Routing Policies.**

Click **New** (not shown). In the **General** section, enter the following values

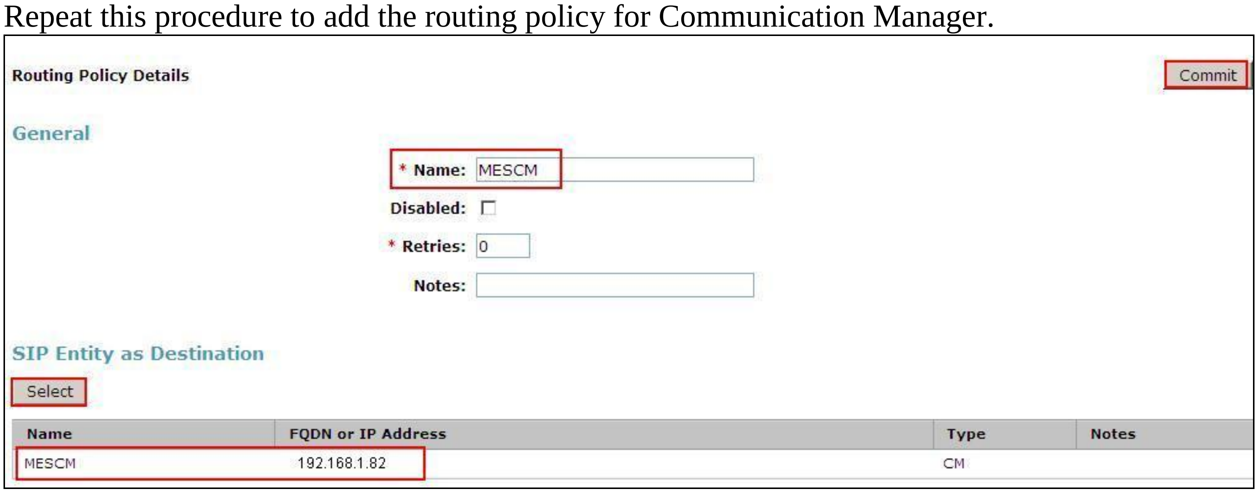
- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked
- **Notes:** Enter a brief description. [Optional]

In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select the SIP Entity associated with CS1000E defined in **Section 7.4** and click **Select.** The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks. The following screen shows the Routing Policy for CS1000E.



Repeat this procedure to add the routing policy for Communication Manager.



7.7. Define Dial Pattern

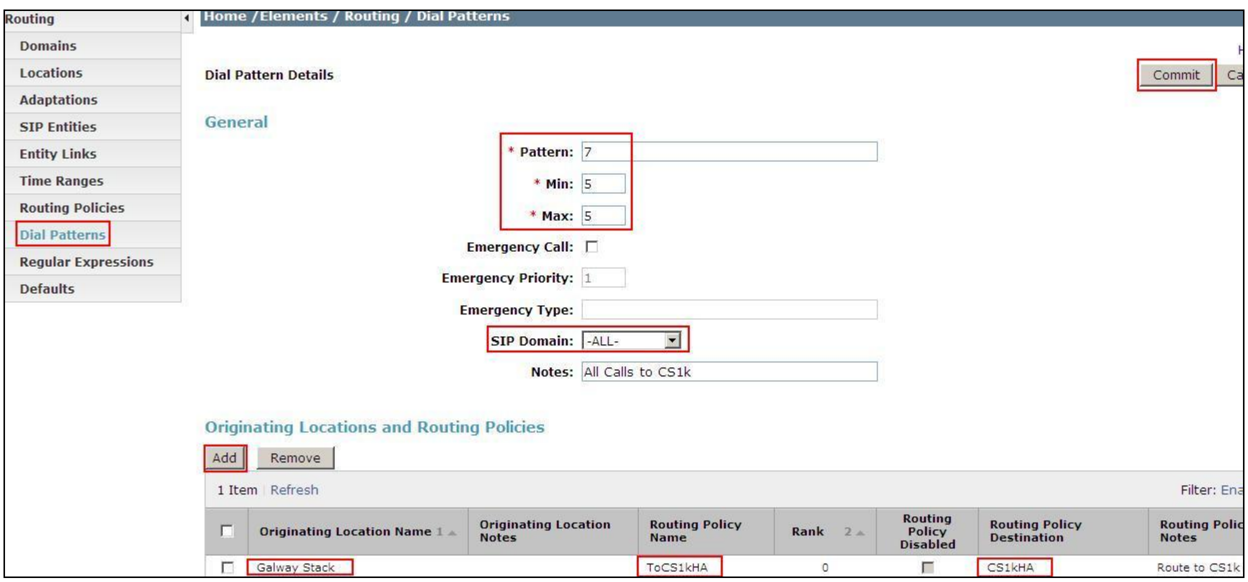
Dial patterns are used to route calls to appropriate SIP Entities. In the sample configuration, stations on CS1000E were assigned extensions starting with **"7"**, so calls starting with digits "**7**" will be routed to CS1000E. To define a dial pattern, expand **Elements → Routing** and select **Dial Patterns** (not shown). Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Avaya Communication Server 1000E
- **Min:** Enter the minimum number digits that must to be dialed.
- **Max:** Enter the maximum number digits that may be dialed.
- **SIP Domain:** Select the SIP Domain from drop-down menu or select **All** if Session Manager should accept incoming calls from all SIP domains.
- **Notes:** Enter a brief description. [Optional]

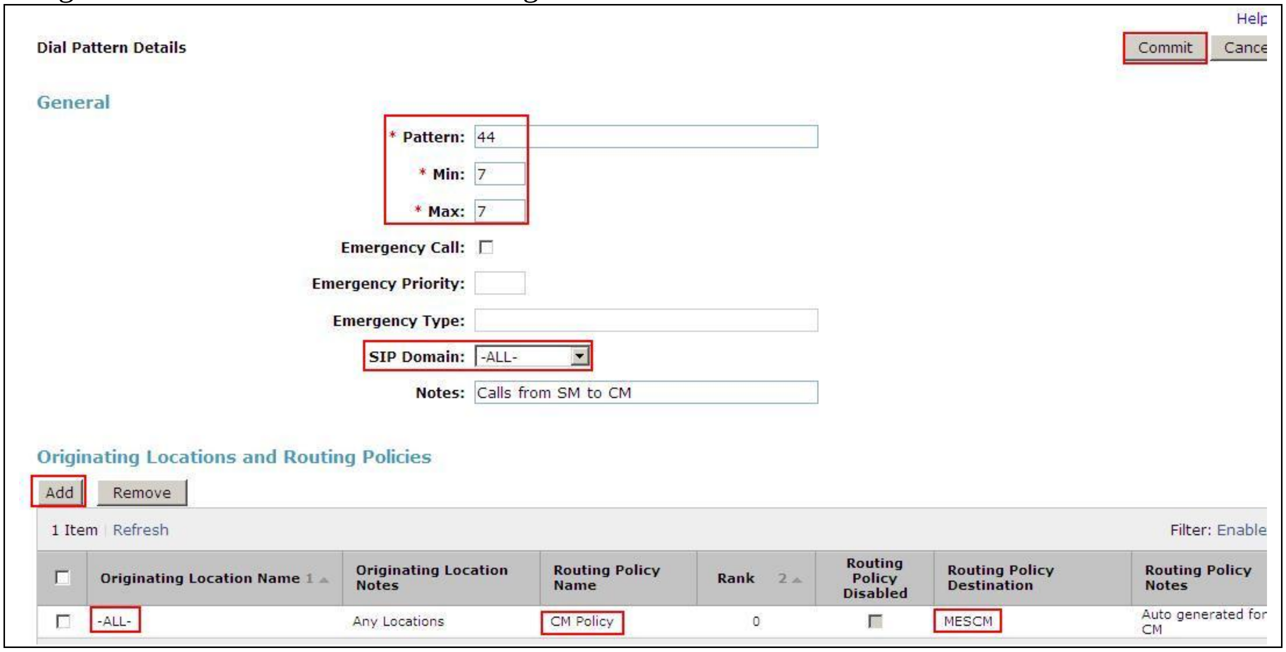
In the **Originating Locations and Routing Policies** section, click **Add.** The **Originating Locations and Routing Policy List** page opens (not shown).

- In **Originating Locations** table, select **ALL** (or select the Location defined in **Section 7.2**)
- In **Routing Policies** table, select the Routing Policy defined for CS 1000E in **Section 7.6.**
- Click **Select** to save these changes and return to **Dial Pattern Details** page.

Click **Commit** to save. The following screen shows the Dial Pattern defined for sample configuration.



Repeat the same procedure to add a dial pattern for Communication Manager. In the sample configuration, extensions on Communication Manager begin with digits **44** and are 7 digits in length. Click **Commit** to save the configuration.



Session Manager configuration is now complete.

8. Configure Avaya Aura® Communication Manager

This section provides details on the configuration of Avaya Aura® Communication Manager. All configurations in this section are administered using the System Access Terminal (SAT). This section provides the procedures for configuring Communication Manager on the following areas:

- Verify Avaya Aura® Communication Manager License
- Administer System Parameters Features
- Administer IP Node Names
- Administer IP Network Region and Codec Set
- Administer Signaling Group and Trunk Groups
- Administer Route Pattern
- Administer Private Numbering
- Administer Locations
- Administer Dial Plan and AAR Analysis
- Create Stations
- Save Changes

The following assumptions have been made as part of this document:

- It is assumed that Communication Manager, System Manager and Session Manager have been installed, configured, licensed. Refer to **Section 11** for documentation regarding these procedures.
- Throughout this section, the administration of Communication Manager is performed using a System Access Terminal (SAT). The commands are entered on the system with the appropriate administrative permissions. Some administration screens have been abbreviated for clarity.

The user has experience of administering the Avaya system via both SAT and Web Based Management systems.

8.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameter customer options** command to compare the **Maximum Administered SIP Trunks** field value with the corresponding value in the **USED** column. The difference between the two values needs to be greater than or equal to the desired number of simultaneous SIP trunk connections.

Note: The license file installed on the system controls the maximum features permitted. If there is insufficient capacity or a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                               USED
                     Maximum Administered H.323 Trunks: 12000 0
           Maximum Concurrently Registered IP Stations: 18000 1
             Maximum Administered Remote Office Trunks: 12000 0
Maximum Concurrently Registered Remote Office Stations: 18000 0
              Maximum Concurrently Registered IP eCons: 414   0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 18000 2
                   Maximum Video Capable IP Softphones: 18000 4
                       Maximum Administered SIP Trunks: 24000 22
  Maximum Administered Ad-hoc Video Conferencing Ports: 24000 0
   Maximum Number of DS1 Boards with Echo Cancellation: 522   0
                             Maximum TN2501 VAL Boards: 128   0
                     Maximum Media Gateway VAL Sources: 250   0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   1
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

8.2. Administer System Parameter Features

Use the **change system-parameters features** command to allow for trunk-to-trunk transfers. This feature is needed to allow for transferring an incoming/outgoing call from /to a remote switch back out to the same or different switch. For simplicity, the **Trunk-to-Trunk Transfer** field was set to **all** to enable trunk-to-trunk transfer on a system wide basis.

```
display system-parameters features                                 Page   1 of
19
                            FEATURE-RELATED SYSTEM PARAMETERS
                               Self Station Display Enabled? y
                                    Trunk-to-Trunk Transfer: all
               Automatic Callback with Called Party Queuing? n
    Automatic Callback - No Answer Timeout Interval (rings): 3
                       Call Park Timeout Interval (minutes): 1
        Off-Premises Tone Detect Timeout Interval (seconds): 20
                                 AAR/ARS Dial Tone Required? y
```

8.3. Administer IP Node Names

Use the **change node-names-ip** command to add entries for Communication Manager and Session Manager that will be used for connectivity. In the sample network, **clan** and **192.168.1.104** are entered as **Name** and **IP Address** for the CLAN card in Communication Manager running on the Avaya S8800 Server. In addition, **SM** and **192.168.1.87** is entered for Session Manager.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
clan                    192.168.1.104
default                 0.0.0.0
gateway                 192.168.1.1
medpro                  192.168.1.4
procr                   192.168.1.82
procr6                  ::
SM                           192.168.1.87
```

8.4. Administer IP Network Region and Codec Set

Use the **change ip-network-region n** command, where **n** is the network region number, to configure the network region being used. In the sample network, ip-network-region 1 is used. For the **Authoritative Domain** field, enter the SIP domain name configured for this enterprise and a descriptive **Name** for this ip-network-region. Set the **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes** to allow for direct media between endpoints. Set the **Codec Set** to **1** to use ip-codec-set 1.

```
IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: silstack.com
    Name: To Session Manager
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                      IP Audio Hairpinning? n
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS
 Call Control PHB Value: 0
        Audio PHB Value: 0
        Video PHB Value: 0
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 0
        Audio 802.1p Priority: 0
        Video 802.1p Priority: 0      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

Use the **change ip-codec-set n** command to configure IP Codec Set paramenters where **n** is the IP Codec Set number. In these Application Notes, **IP Codec Set 1** was used as the main default codec set. The standard G.711 codecs and G729 codec were selected.

- **Audio Codec** Set for **G.711MU, G.711A, G729** and **G.729A**
- **Silence Suppression:** Retain the default value **n**
- **Frames Per Pkt:** Enter **2**
- **Packet Size (ms):** Enter **20**

Retain the default values for the remaining fields, and submit these changes.

```
add ip-codec-set 1                                          Page   1 of
2

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711A            n          2        20
 2: G.711MU           n          2        20
 3: G.729             n          2        20
 4: G.729A            n          2        20
```

8.5. Create SIP Signaling Group and Trunk Group

8.5.1. SIP Signaling Group

In the test configuration, Communications Manager acts as an Evolution Server. An IMS enabled SIP trunk is not required. The example uses signal group **3** in conjunction with Trunk Group **3** to reach the Session Manager. Use the **add signaling-group n** command where **n** is the signaling group number being added to the system. Use the values defined in **Sections 8.3** and **8.4** for the **Near-end Node name**, **Far-end Node name** and **Far-end Network Region**. The **Far-end Domain** is configured as **silstack.com** which is a domain used on Session Manager. Set **IMS enabled** to **n**. Set **Direct IP-IP Audio Connections** to **y** so trunk "shuffling" is on. Set **IP Video** to **y**.

```
add signaling-group 3                                           Page   1 of   1
                             SIGNALING GROUP

 Group Number: 3            Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y         Priority Video? y             Enforce SIPS URI for SRTP? n
  Peer Detection Enabled? n  Peer Server: SM



   Near-end Node Name: procr                    Far-end Node Name: SM
 Near-end Listen Port: 5061                  Far-end Listen Port: 5061
                                          Far-end Network Region: 1

Far-end Domain: silstack.com
                                             Bypass If IP Threshold Exceeded? n
Incoming Dialog Loopbacks: eliminate                  RFC 3389 Comfort Noise? n
         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? y
Session Establishment Timer(min): 3                     IP Audio Hairpinning? n
         Enable Layer 3 Test? n                  Initial IP-IP Direct Media? y
H.323 Station Outgoing Direct Media? n           Alternate Route Timer(sec): 6
```

8.5.2. SIP Trunk Group

Use the command **add trunk-group n** to add a corresponding trunk group, where **n** is the trunk group number.

- **Group Number** Set from the **add-trunk-group n** command
- **Group Type** Set as **sip**
- **COR** Set Class of Restriction (default 1)
- **TN** Set Tenant Number (default 1)
- **TAC** Choose integer value, usually set the same as the Trunk Group number
- **Group Name** Choose an appropriate name
- **Service Type** Set to **tie**
- **Signaling Group** Enter the corresponding Signaling group number
- **Number of Members** Enter the number of members

```
add trunk-group 3                                                  Page   1 of  21
                                TRUNK GROUP

Group Number: 3                  Group Type: sip          CDR Reports: y
  Group Name: SIP Trunk to SM    COR: 1        TN: 1        TAC: *03
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                              Member Assignment Method: auto
                                                       Signaling Group: 3
                                                     Number of Members: 255
```

Navigate to **Page 3** and set **Numbering Format** to **private**.

```
add trunk-group 3                                                  Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                        Maintenance Tests? y



                     Numbering Format: private
                                              UUI Treatment: service-provider
                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n

                                Modify Tandem Calling Number: no
 Show ANSWERED BY on Display? y
```

8.6. Administer Route Pattern

Configure a route pattern to correspond to the newly added SIP trunk group. Use the **change route-pattern n** command, where **n** is the route pattern number**.** Configure this route pattern to route calls to **trunk group 3**, as configured in **Section 8.5.** Assign the lowest **FRL** (facility restriction level) to allow all callers to use this route pattern, Assign **0** to **No. Del Digits**.

```
change route-pattern 3                                                Page   1 of   3
                    Pattern Number: 3 Pattern Name: SIP Trunk
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                            DCS/ IXC
    No          Mrk Lmt List Del  Digits                              QSIG
                             Dgts                                     Intw
 1: 3    0                    0                                        n   user
 2:                                                                    n   user
 3:                                                                    n   user
 4:                                                                    n   user
 5:                                                                    n   user
 6:                                                                    n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
                                                        Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

8.7. Administer Private Numbering

Use the **change private-numbering** command to define the calling part number to be sent out through the SIP trunk. In the sample network configuration, all calls originating from a **7** digit extension beginning with **44** will result in a **7**-digit calling number. The calling party number will be in the SIP "From" header.

```
NUMBERING - PRIVATE FORMAT

Ext Ext             Trk         Private          Total
Len Code            Grp(s)      Prefix           Len
 7  44              3                            7      Total Administered: 9
 5  24              150                          5        Maximum Entries: 540
```

8.8. Administer Locations

Use the **change locations** command to define the proxy route to use for outgoing calls. In the sample network, the proxy route will be the trunk group defined in **Section 8.5.**

```
change locations                                                  Page   1 of   1
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y
 Loc  Name            Timezone DST  CITY/                               Proxy Sel
 No                    Offset        AREA                                 Rte Pat
 1:  Main            + 00:00   0                                          3
```

8.9. Administer Dial Plan and AAR Analysis

Configure the dial plan for dialing 5-digit extensions beginning with **7** to stations registered with the CS1000E. Use the **change dialplan analysis** command to define Dialed String **7** as an **aar Call Type.**

```
change dialplan analysis                                    Page   1 of  12
                             DIAL PLAN ANALYSIS TABLE
                                   Location: all          Percent Full: 5

    Dialed    Total  Call      Dialed    Total  Call      Dialed    Total  Call
    String    Length Type      String    Length Type      String    Length Type
   1            3   dac      9             5   aar
   44           7   ext
   7            5   aar
   80955        5   aar
```

Use the **change aar analysis 0** command to configure an **aar** entry for **Dialed String 7** to use **Route Pattern 3**. Use **unku** for **call type**. Use dialed string **44** with **7** digit length and call type **aar** for Communication Manager SIP extensions registered via Session manager.

```
change aar analysis 0                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 1

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    44                    7    7     3        aar           n
    7                     5    5     3        unku          n
    9                     5    7     3        unku          n
```

8.10. Create H.323 and SIP Stations

Refer to **Section 11** references **[9]** and **[13]** on how to add H.323 and SIP stations on Communication Manager. SIP Stations should be added through System Manager User Management.

8.11. Save Changes

Use the **save translation** command to save all changes.

```
save translation

                              SAVE TRANSLATION

           Command Completion Status                        Error Code

           Success                                              0
```

9. Verification Steps

A number of steps can be taken to verify if the completed configuration is operating correctly.

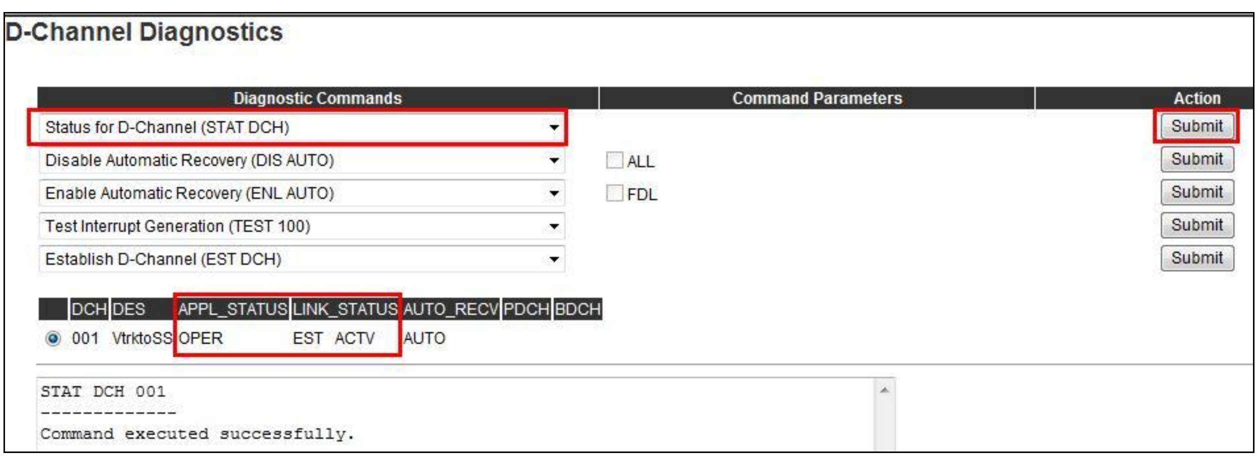
9.1. Verify Avaya Communication Server 1000E Operational Status

Step 1: Verify status of virtual D-Channel.

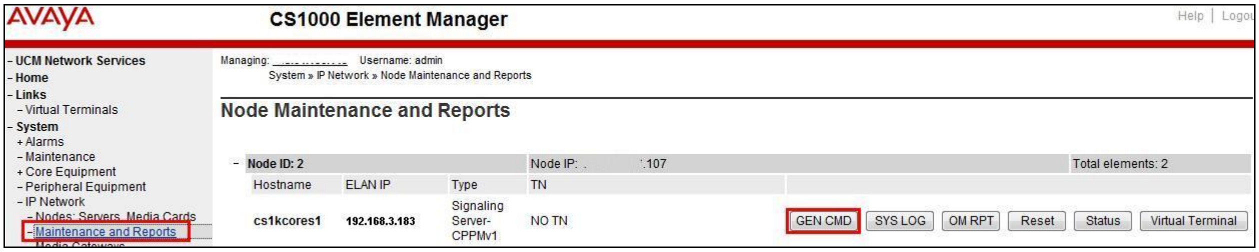
Log into System Manager UCM Services. Click on the Element Manager link to access CS1000E management interface (Not Shown). Expand **System** on the left navigation panel and select **Maintenance.** Select **LD 96 - D-Channel** from the **Select by Overlay** table and the **D-Channel Diagnostics** function from the **Select Group** table as shown below.

Select **Status for D-Channel (STAT DCH)** command and click **Submit** to verify status of virtual D-Channel as shown below. Verify the status of the following fields:

- **Appl_Status** Verify status is **OPER**
- **Link_Status** Verify status is **EST ACTV**



Step 2: Verify status of SIP trunk to Session Manager. Expand **System → IP Network** on the left navigation panel and select **Maintenance and Reports.** Click **GEN CMD**.

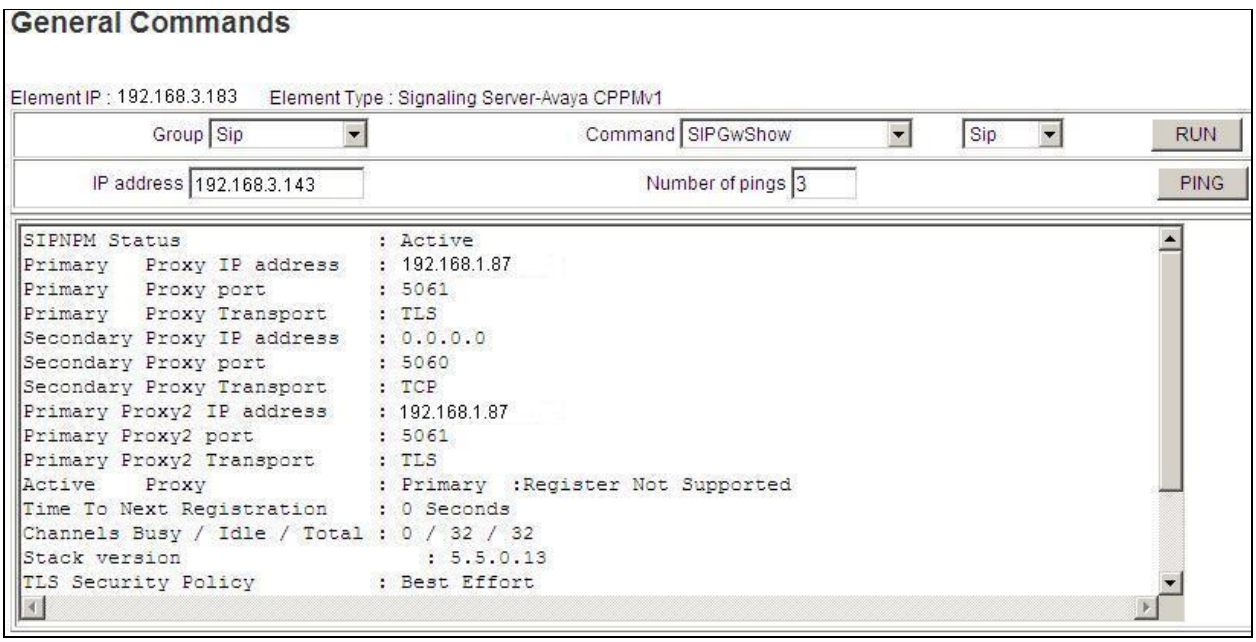


Enter following values and click **RUN.**

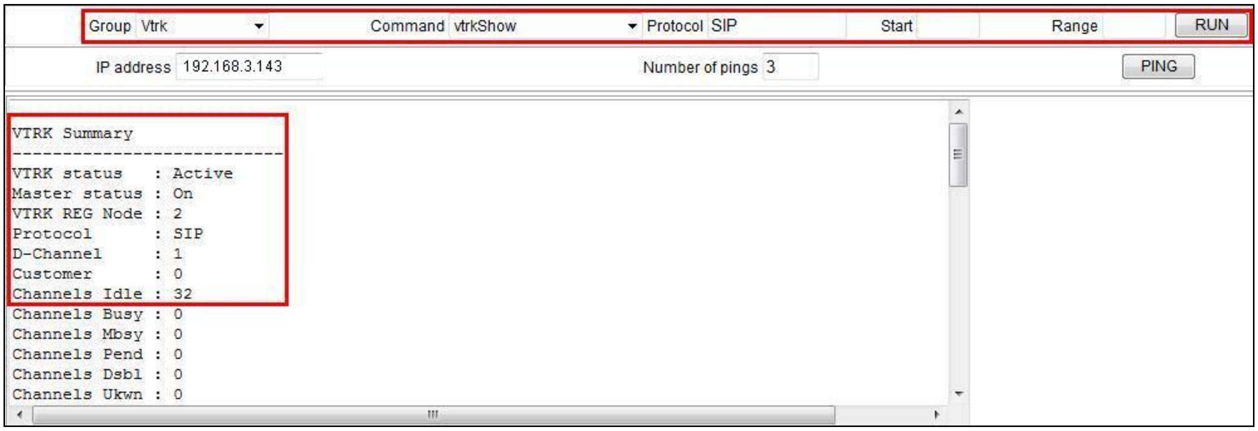
- **Group** Select **Sip**
- **Command** Select **SIPGwShow**
  Select **SIP**

Verify the status of the following fields as shown below.

- **SIPNPM_Status** Verify status is **Active**
- **Primary Proxy IP Address** Verify IP address matches address of Session Manager SIP signaling interface
- **Primary Proxy Port** Verify port is **5061**
- **Primary Proxy Transport** Verify transport value is **TLS**



The following screenshot is another debug command for the virtual SIP trunk. Ensure the **VTRK Status** is **Active.**



Step 3: Monitor the debug log output on CS1000E Signaling Server SIP Signaling Gateway. Open an SSH terminal emulator session into CS1000E Signaling server Node IP address. Refer to **Section 6.1** to confirm the TLAN Node IP address. Log in using the CS1000E Signaling Server **admin2** username and password, as configured during the Signaling Server installation. Enter the command **syslogLevelSet vtrk tSSG debug** to turn on logging Debug level for the SIP Signaling Gateway (SSG) task on the virtual trunk.

WARNING: Take care when enabling Debug level commands on a busy CS1000E Signaling Server as it may degrade the processing capacity during heavy traffic.

The output is then piped to the **ss_common.log** file located in the directory **/var/log/nortel**
To see the output of the ss_common.log printed to the screen in real-time use the command: **tail –f /var/log/Nortel/ss_common.log** when the SIP TLS trunk is expecting to be established between the CS100E Signaling Server and Session manager. A successful log output is shown as follows (make a note of the items shown in bold letters:

[admin2@cs1kcores1 ~]$ syslogLevelSet vtrk tSSG debug
[admin2@cs1kcores1 ~]$ tail -f /var/log/nortel/ss_common.log

Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: hConnection=0x4505260 hAppConnection=0x0 tlsState=**TLS Handshake Ready** eReason=1
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: **Remote IP:Port 192.168.1.87:5061**
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: **Starting Client side handshake**, rv=0
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: hConnection=0x4505260 hAppConnection=0x0 tlsState=TLS Handshake started eReason=-1
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: Remote IP:Port 192.168.1.87:5061
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmGetCrl_cb: Requesting CRL for certificate **/CN=messmsig.silstack.com**/O=Avaya/C=US which was issued by /CN=default/OU=MGMT/O=AVAYA

Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmGetClrByIssuer:: strCaIssuer = /CN=default/OU=MGMT/O=AVAYA doesn't match crlS /O=AVAYA/ST=ON/L=BVW/C=CA/CN=messmgr.silstack.com/OU=MGMT
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmGetCrl_cb: CRL not found for issuer /CN=default/OU=MGMT/O=AVAYA
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: prevError=0 certificate=0x27ee348
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=messmsig.silstack.com/O=Avaya/C=US
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: Unable to get CRL Cert Analysis - issued to:/CN=messmsig.silstack.com/O=Avaya/C=US
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=messmsig.silstack.com/O=Avaya/C=US#012 OK
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmGetCrl_cb: Requesting CRL for certificate /CN=default/OU=MGMT/O=AVAYA which was issued by /CN=default/OU=MGMT/O=AVAYA
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmGetClrByIssuer:: strCaIssuer = /CN=default/OU=MGMT/O=AVAYA doesn't match crlS /O=AVAYA/ST=ON/L=BVW/C=CA/CN=messmgr.silstack.com/OU=MGMT
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmGetCrl_cb: CRL not found for issuer /CN=default/OU=MGMT/O=AVAYA
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: prevError=0 certificate=0x27ee348
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=default/OU=MGMT/O=AVAYA
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: Unable to get CRL Cert Analysis - issued to:/CN=default/OU=MGMT/O=AVAYA
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=default/OU=MGMT/O=AVAYA#012 OK
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: prevError=1 certificate=0x27ee348
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=default/OU=MGMT/O=AVAYA
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=default/OU=MGMT/O=AVAYA#012 OK
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: prevError=1 certificate=0x27ee348
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=messmsig.silstack.com/O=Avaya/C=US
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportVerifyCertificateEv: szLogData=Cert Analysis - issued to:/CN=messmsig.silstack.com/O=Avaya/C=US#012 OK
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: hConnection=0x4505260 hAppConnection=0x0 tlsState=**TLS Handshake Completed** eReason=-1
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: Remote IP:Port 192.168.1.87:5061
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTlsPostConnectionAssertionEv hConnection=0x4505260 hAppConnection=0x0 strHostName=192.168.1.87 hMsg=(nil)
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTlsPostConnectionAssertionEv Remote IP:Port 192.168.1.87:5061
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTlsCheckSANandCN: entering, **remoteIP = 192.168.1.87**
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTlsCheckSANandCN: **CN = "messmsig.silstack.com"**
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpm**DNSLookup**: **Entering, fqdn = messmsig.silstack.com**, ip_buffer =
Feb 11 18:45:13 cs1kcores1 vtrk: (DEBUG) tSSG: taskSpawn: thread 0xA95BCB90, tid 0x9EC9BB8, name tSIPDNSlookup.

Feb 11 18:45:14 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTlsCheckSANandCN: [CN check] **DNS lookup for messmsig.silstack.com resulted in 192.168.1.87**
Feb 11 18:45:14 cs1kcores1 vtrk: (DEBUG) tSSG: piEnabled: PI 30526 bitByteIndex 1315
Feb 11 18:45:14 cs1kcores1 vtrk: (DEBUG) tSSG: piEnabled: PI 30526 bitTrue 0
Feb 11 18:45:14 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTlsCheckSANandCN: **Remote IP=192.168.1.87 matches strIpCert=192.168.1.87**
Feb 11 18:45:14 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTlsCheckSANandCN: retVal = 1
Feb 11 18:45:14 cs1kcores1 vtrk: (DEBUG) tSSG: sipNpmTransportConnectionTlsStateChanged: hConnection=0x4505260 hAppConnection=0x0 tlsState=**TLS Connected** eReason=-1

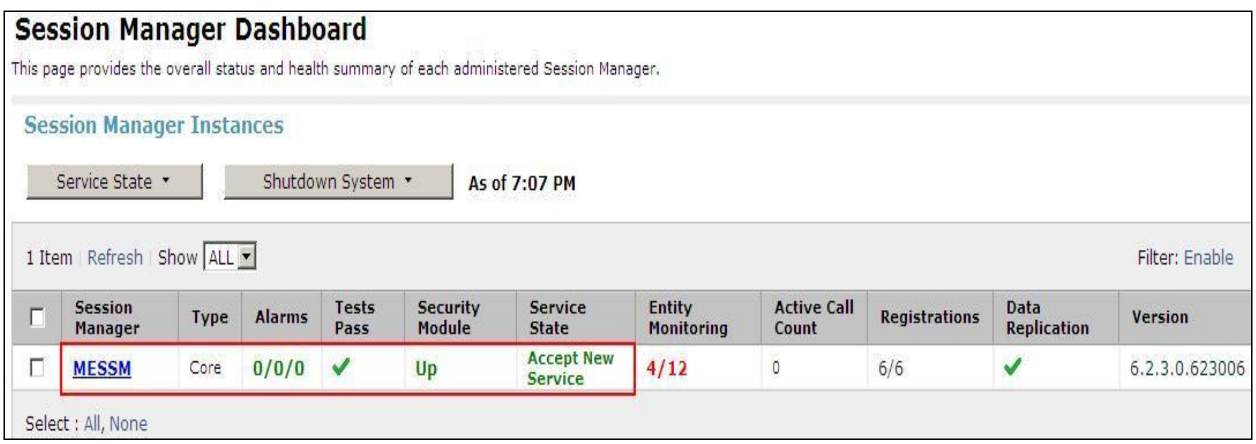
To cancel out of the real-time log printout, use **Ctrl** and **c** keys on the keyboard.

WARNING: Ensure to turn off Debug level logging when finished. Use the command: **syslogLevelSet vtrk tSSG info**

9.2. Verify Avaya Aura® Session Manager Operational Status

Step 1: Verify overall system status of Session Manager.
Navigate to **Elements → Session Manager → Dashboard** (not shown) and verify the status of the following fields as shown below:

- **Tests Pass**
- **Security Module**
- **Service State**



Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

Reset | Synchronize | Certificate Management ▾ | Connection Status

1 Item | Refresh | Show ALL — Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
○	▶ Show	MESSM	SM	Up	29	192.168.1 /27	---	192.168.1.1	Disabled	14/14	Customer CA

Step 2: Verify status of the SIP Trunk between CS 1000E and Session Manager and Session manager and Communication Manager.

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Trunk. Select the SIP Entity for CS1000E from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

In the **All Entity Links to SIP Entity: CS1kHA** table, verify the **Conn. Status** for the TLS link is **Up** as shown below.

All Entity Links to SIP Entity: CS1kHA

Summary View

1 Item | Refresh — Filter: Enable

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	MESSM	192.168.2.107	5061	TLS	Up	200 OK	Up

Click **Summary View** to return to the SIP Entity Summary View. Click on the link for Communication Manager, example **MESCM** to view the status of the entity link to Communication Manager.

All Entity Links to SIP Entity: MESCM

Summary View

1 Item | Refresh — Filter: Ena

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
▶ Show	MESSM	192.168.1.82	5061	TLS	Up	200 OK	Up

9.3. Verify Communication Manager Operational Status

Confirm that the SIP Signaling Group and Trunk Group are in service. Open a SAT connection to Communication Manager. Issue the command **status signaling-group 3** and the output should show a **Group State: in-service**
Issue the command **status trunk 3** and the resulting output should list the trunk members with a **Service State** showing **in-service/idle**

10. Conclusion

These Application Notes describe how to configure a sample network that provides a secure SIP connection using Transport Layer Security (TLS) between Avaya Aura® Communication Manager Release R6.2 and Avaya Communication Server 1000E Release 7.6 via Avaya Aura® Session Manager R6.2. Non-default customer defined Identity certificates are created for Avaya Aura® Session Manager to ensure they are uniquely identified for TLS security purposes. Along with configuring and securing SIP Trunks between Communication Server 1000E, Avaya Aura® Session Manager and Avaya Aura® Communication Manager, SIP TLS is also enabled between Avaya one-X® SIP Deskphones and Session Manager.

Interoperability tests included making bi-directional calls between TDM and UNIStim stations on Avaya Communication Server 1000E and both SIP and H.323 stations on Avaya Aura® Communication Manager with various features including hold, transfer, and conference. SIP trunk failover testing with two Communication Server 1000 Signaling Servers and one session manager was also completed. All test cases passed apart from the items mentioned in **Section 2.2.**

11. Additional References

This section provides references to the product documentation relevant to these Application Notes which can be found at; http://support.avaya.com

Avaya Aura® Session Manager

1) Avaya Aura® Session Manager Overview, Doc ID 03-603323
2) Installing and Configuring Avaya Aura® Session Manager
3) Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325
4) Administering Avaya Aura® Session Manager, Doc ID 03-603324

Avaya Communication Server 1000E

5) IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313
6) Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116
7) Communication Server 1000E Planning and Engineering Avaya Communication Server 1000, Document Number NN43041-220
8) Security Management Fundamentals – Avaya Communication Server 1000E Release 7.5, Document Number NN43001-604

Avaya Aura® Communication Manager

9) Administering Avaya Aura® Communication Manager, Document Number 03-300509

Avaya Application Notes

10) Configuring a SIP Trunk between Avaya Aura® Session Manager Release 6.1 and Avaya Communication Server 1000E Release 7.5
11) Application notes for supporting third-party certificate in Avaya Aura® System Manager 6.1, Document Number 100144833

Avaya Aura® one-X® Deskphones

12) Avaya one-X® Deskphone9608, 9611G, 9621G, and 9641G Administrator Guide SIP release 6.2, Document Number 16-601944

Avaya Aura® System Manager

13) Administering Avaya Aura® System Manager, Release 6.2, Issue 2.0

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