



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for configuring SIP TLS between Vocera Communication System Release 4.3 SP1 and Avaya Communication Server 1000E Release 7.5 and Avaya Aura® Session Manager 6.1 – Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring SIP TLS between Avaya Communication Server 1000E and Avaya Aura® Session Manager and between Vocera Communication System and Avaya Aura® Session Manager, the solution uses Avaya Aura® Session Manager to route calls between Avaya Communication Server 1000E and Vocera Communication System. The overall objective of the interoperability compliance testing is to verify basic functions of Vocera system is able to work with Avaya Communication Server 1000E over SIP Trunk that is secured by TLS.

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

# 1. Introduction

These Application Notes describe the procedures to integrate Vocera Communication system with Avaya Communication Sever 1000E via SIP TLS that was configured on Avaya Aura® Session Manager. The Avaya Communication Server 1000E that was used for the testing is co-resident system which has Call Server, Signaling Server and Element Manager applications residing on the same CPPM card. The solution has Avaya Aura® Session Manager to provide SIP TLS and networking routing service to route calls between Avaya Communication Server 1000E and Vocera Communication system.

## 2. General Test Approach and Test Results

The general test approach was to have different telephone types of the Avaya Communication Server 1000E (hereafter referred as Avaya CS1000) to place a call to and from the Vocera Server and follow its voice instructions to verify other features of the Vocera Communication System such as: Basic call, transfer, conference and call forward.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute a full product performance or feature testing performed by third party vendors, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a third party solution.

### 2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- SIP TLS is established successfully between the Vocera Server and Avaya CS1000 via the Session Manager
- Basic calls between the Vocera Server and different telephone types of Avaya CS1000 (SIP, non-SIP and emulated PSTN telephones).
- DTMF RFC2833 transmission.
- Conference and Transfer calls from different telephone types of Avaya CS1000 (SIP, non-SIP and emulated PSTN telephones) to the Vocera Server clients (wireless badge B3000) and vice versa.
- Call Forward (All Call, No Answer, and Busy) and Call Forward to voicemail with Message Waiting Indication (MWI) notification.
- Other telephony features: Busy, Hold and Retrieve calls.

### 2.2. Test Results

All test cases were passed with the following one observation.

- Conference button on the Avaya CS1000 IP Unistim phone is not available if Ring Again feature is enabled on the phone that hosts the conference. The scenario happens when the second Vocera badge user is being invited to join the conference hosted by Avaya CS1000 IP Unistim phone that already has the first call with the first Vocera badge. The

work around is not to provision the Ring Again feature on the IP phone. Work Item has been raised to track the issue to resolution.

- SIP OPTIONS message to keep alive sent from Vocera server to Session Manager is not recognized by Session Manager. The recommendation is disable SIP OPTIONS message on Vocera server and let Session Manager send OPTIONS to keep the SIP Trunk up.

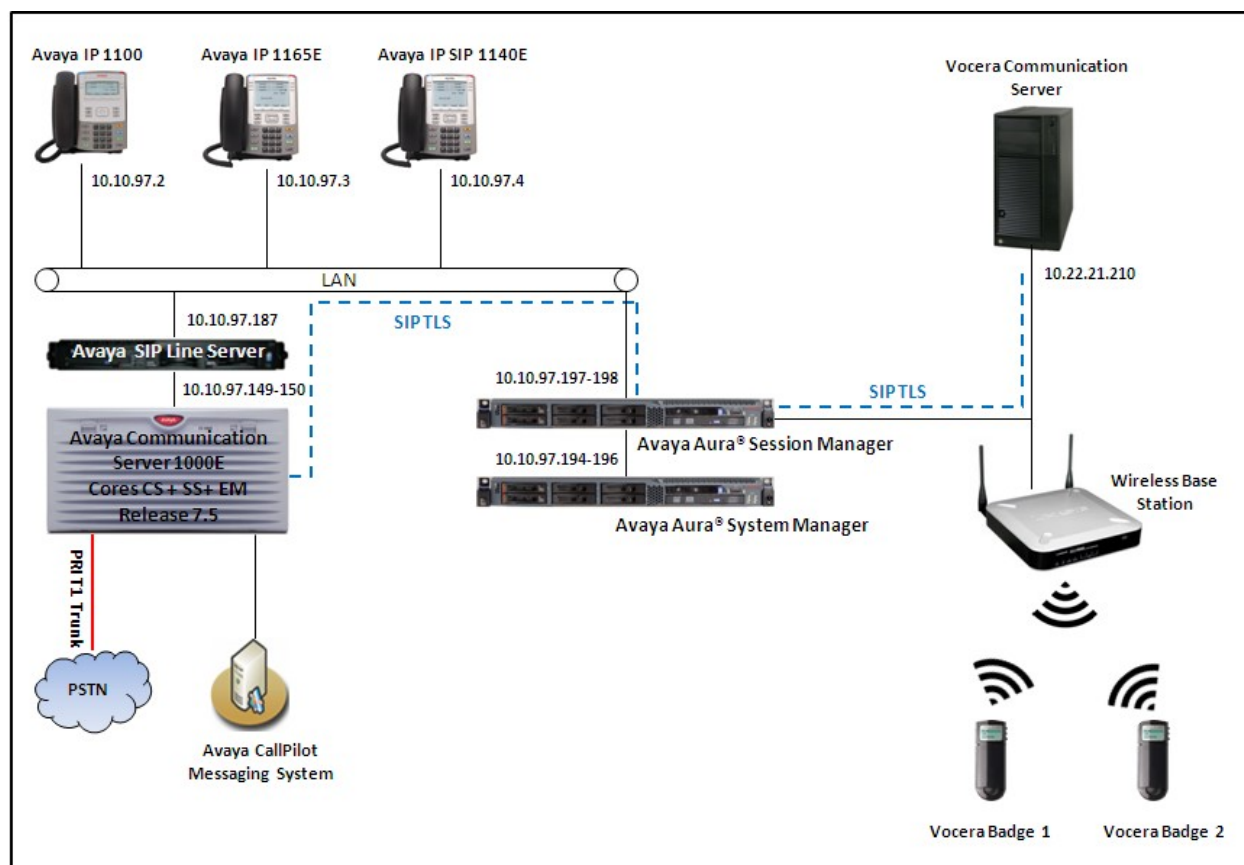
## 2.3. Support

For technical support on the Vocera product, contact Vocera Support via phone, email or website.

- **Phone:** +1 408-882-5700
- **Email:** [support@vocera.com](mailto:support@vocera.com)
- **Web:** <http://www.vocera.com>

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration with an Avaya Communication Server 1000E SIP trunk network that includes the following Avaya products: Avaya Communication Server 1000E connected to the Avaya Aura® Session Manager via SIP TLS. Avaya Communication Server 1000E SIP Line server provides SIP registration for SIP Phone. Vocera Communication System connected to Avaya Aura® Session Manager via SIP TLS. Avaya 1140E SIP phone registers to Avaya Communication Server 1000E SIP Line server, IP Unistim 1110 and 1165E Unistim phones register to Avaya Communication Server 1000E TPS application that resides on the same server with SIP Virtual trunk application and Emulated PSTN over PRI trunk.



**Figure 1: Test Configuration Diagram**

## 4. Equipment and Software Validated

The following equipment and software were used for the compliance test:

Equipment	Software
Avaya S8800 server running Avaya Aura® Session Manager Server	Avaya Aura® Session Manager 6.1 SP6 (Build No 6.1.6.0.616008)
Avaya S8800 server running Avaya Aura® System Manager Server	Avaya Aura® System Manager 6.1 SP6 (Build No: 6.1.0.0.7345-6.1.5.606 Software Update Revision No: 6.1.10.1.1774)
Avaya Communication Server 1000E/CPPM	Avaya Communication Server Release 7.5 Q+ Plus Deplist 1 (created: 2012-03-14) and Service Pack Linux (created 20120314)
Avaya CallPilot® 600i	Version 05.00.41.143
Avaya IP Unistim Phone 1110	Version 0623C8L
Avaya IP Unistim Phone 1165E	Version 0625C8L
Avaya IP SIP Phone 1140E	Version 4.03
Vocera Server	Version 4.3 SP1 Build 2349

## 5. Configure Avaya Communication Server 1000E

This document assumes that the Avaya Communication Server 1000E system that was used for the testing was already installed and configured for:

- Telephony Node ID ( Node 511)
- Customer ID ( customer 0)
- Zone
- D-channel for VoIP.
- SIP Route and Trunks
- Co-ordinate Dialing Plan (CDP) for local prefix of directory number in Avaya CS1000 starts from **54xxx** and prefix of CDP dialing plan for Vocera system is assigned to **732x** on the Avaya CS1000 system, this will be described in **Section 6.7**.

This section describes procedures of how to configure SIP Trunk secured by TLS between Avaya CS1000 SIP gateway and Session Manager.

## 5.1. Create certificate For SIP TLS

Log in to Unified Communication Management (UCM) server that is managing the Avaya CS1000 system used to establish SIP TLS with Session Manager. The homepage of UCM is displayed as the screen below.

**AVAYA** Avaya Unified Communications Management [Help](#) | [Logout](#)

Host Name: car2-sipl-ucm.bvwdev.com Software Version: 02.20.0023.00(5197) User Name admin

### Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

<input type="checkbox"/>	Element Name	Element Type	Release	Address	Description
<input type="checkbox"/>	<a href="#">EM on car2-cores</a>	CS1000	7.5	135.10.97.90	New element.
<input type="checkbox"/>	<a href="#">EM on car2-ssq-carrier</a>	CS1000	7.5	135.10.97.90	New element.
<input type="checkbox"/>	<a href="#">EM on cpppm3</a>	CS1000	7.5	135.10.97.78	New element.
<input type="checkbox"/>	<a href="#">sip175.bvwdev.com (member)</a>	Linux Base	7.5	135.10.97.136	Base OS element.
<input type="checkbox"/>	<a href="#">car2-ssq2.bvwdev.com (member)</a>	Linux Base	7.5	135.10.97.157	Base OS element.
<input type="checkbox"/>	<a href="#">car2-ssq-carrier.bvwdev.com (member)</a>	Linux Base	7.5	135.10.97.167	Base OS element.

Copyright 2002-2010 Avaya Inc. All rights reserved.

In the left navigation pane, select **Security** → **Certificates**, the **Certification Management** page is displayed in the right of UCM page.

Under **Certificate Endpoints** section, select an associated SIP gateway member that needs to be configured for the TLS certificate, in this document the SIP gateway member **10.10.97.150** is used to configure SIP TLS.

**AVAYA** Avaya Unified Communications Management [Help](#) | [Logout](#)

Host Name: car2-sipl-ucm.bvwdev.com Software Version: 02.20.0023.00(5197) User Name admin

### Certificate Management

Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

**Certificate Endpoints** **Private Certificate Authority**

Display the details of a certificate endpoint by selecting the radio button associated with that endpoint. When multiple logical endpoints exist on a single base server, only the base endpoint is shown.

<input type="radio"/>	Endpoint Address	Element Type	Element Name	Number of Service
<input type="radio"/>	10.10.97.172	Linux Base	car2-sps.bvwdev.com (member)	4
<input type="radio"/>	10.10.97.163	Linux Base	car2-sipl-ucm.bvwdev.com (primary)	4
<input type="radio"/>	10.10.97.171	Linux Base	car2-mas.bvwdev.com (member)	4
<input checked="" type="radio"/>	10.10.97.150	Linux Base	cpppm3.bvwdev.com (member)	4

The **Endpoint Details** section of the SIP gateway **10.10.97.150** shows the current certificates installed in the **Certificates** window.

The screenshot shows the 'Endpoint Details' window for a selected endpoint. The left sidebar contains a navigation menu with categories like 'Secure FTP Token', 'Software Deployment', 'User Services', 'Security', and 'Tools'. The 'Certificates' link under 'Security' is highlighted. The main content area is titled 'Endpoint Details' and 'Details for the selected endpoint'. It features a 'Certificates' table with the following data:

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	cpppm3	Jan 17, 2021
2	DTLS	none		
3	Web SSL	none		
4	SIP TLS	none		

Below the table is a 'Certificate Authorities' section with buttons for 'Add...', 'Enable Trust', 'Disable Trust', 'Delete', and 'Update CRL'. It contains a table with one entry:

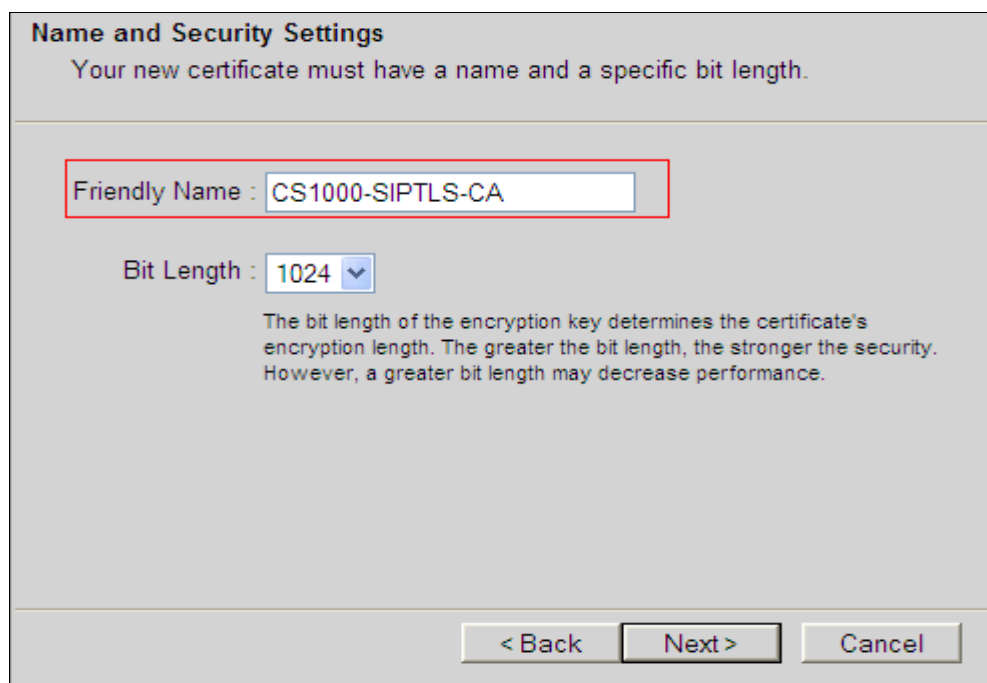
	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1	car2-sipl-ucm.bwvd...	Feb 1, 2035	yes	/O=avaya/ST=ONL=Belleville/...	Nov 17, 2011

If in the **Status** column of **SIP TLS** service presents as **none**, this means the certificate for SIP TLS has not been configured for that SIP gateway. Click on the **SIP TLS** link to configure certificate for SIP TLS. Note: The certificate for SIP TLS will be created and signed by local UCM Certificate Authority (CA).

The **Server Certificate** window is displayed, select option “**Create a new certificate, signed by local private Certificate Authority**” and click on **Next** button to continue.

The screenshot shows the 'Server Certificate' window with the subtitle 'These are the methods for assigning a certificate to your server.' It contains five radio button options. The first option, 'Create a new certificate, signed by local private Certificate Authority', is selected and highlighted with a red box. The other options are 'Import a certificate and its private key from a file', 'Assign an existing certificate', 'Create a new self-signed certificate', and 'Create a new certificate request to be signed by third party Certificate Authority'. At the bottom right, there are 'Next >' and 'Cancel' buttons.

The **Name and Security Settings** page is displayed, enter a name in the **Friendly Name** field, e.g. “CS1000-SIPTLS-CA” and leave **Bit Length** field at default. Click on **Next** button to continue.



**Name and Security Settings**  
Your new certificate must have a name and a specific bit length.

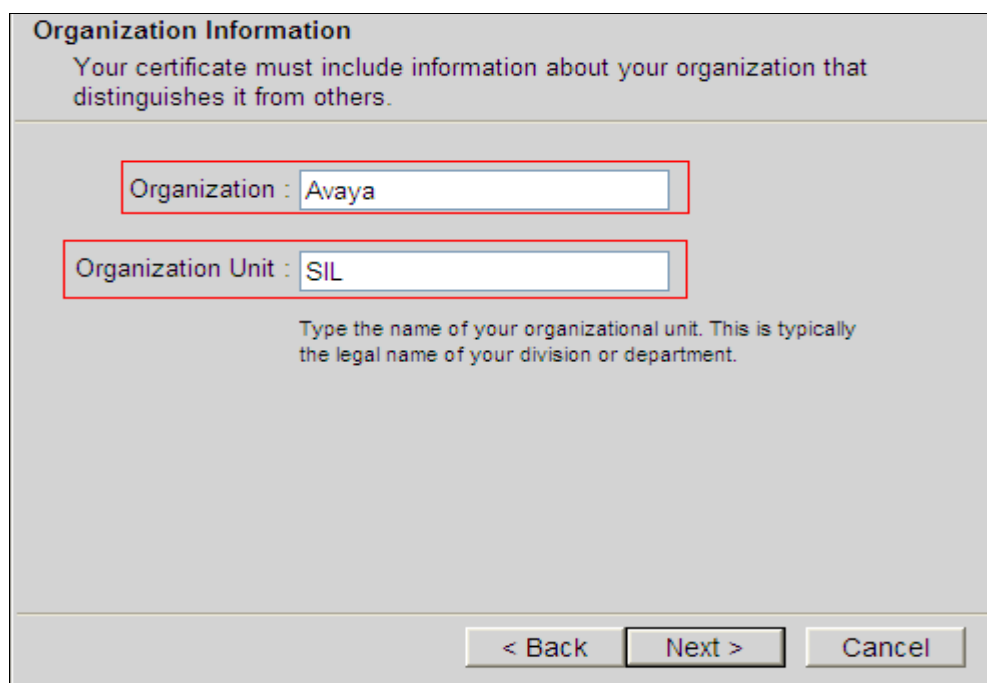
Friendly Name :

Bit Length :

The bit length of the encryption key determines the certificate's encryption length. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance.

< Back   Next >   Cancel

The **Organization Information** page is displayed, enter organization and organization unit names in the **Organization** and **Organization Unit** fields, e.g. “Avaya” and “SIL”. Click **Next** button to continue.



**Organization Information**  
Your certificate must include information about your organization that distinguishes it from others.

Organization :

Organization Unit :

Type the name of your organizational unit. This is typically the legal name of your division or department.

< Back   Next >   Cancel



The **Your Server's Common Name** page is displayed, enter the FQDN of the SIP gateway in the **Common Name** field and leave the **Subject Alt Name** field at default. Note: The name in the **Common Name** field must be the FQDN or host name of the SIP gateway. Click **Next**.

**Your Server's Common Name**  
Your server's common name is its fully qualified domain name.

Common Name :

If you use the DNS name to access the Element Manager web site from your web browser, the common name must match the DNS name.  
If the common name changes, you may need to obtain a new certificate.

Subject Alt Name :

< Back   Next >   Cancel

The **Geographical Information** page is displayed, enter country “**CANADA**”, state “**ON**”, and city “**Belleville**” where the server locates in the **Country/Region**, **State/Province**, and **City/Locality** fields. Click **Next**.

**Geographical Information**  
The certificate requires the following geographical information.

Country/Region :

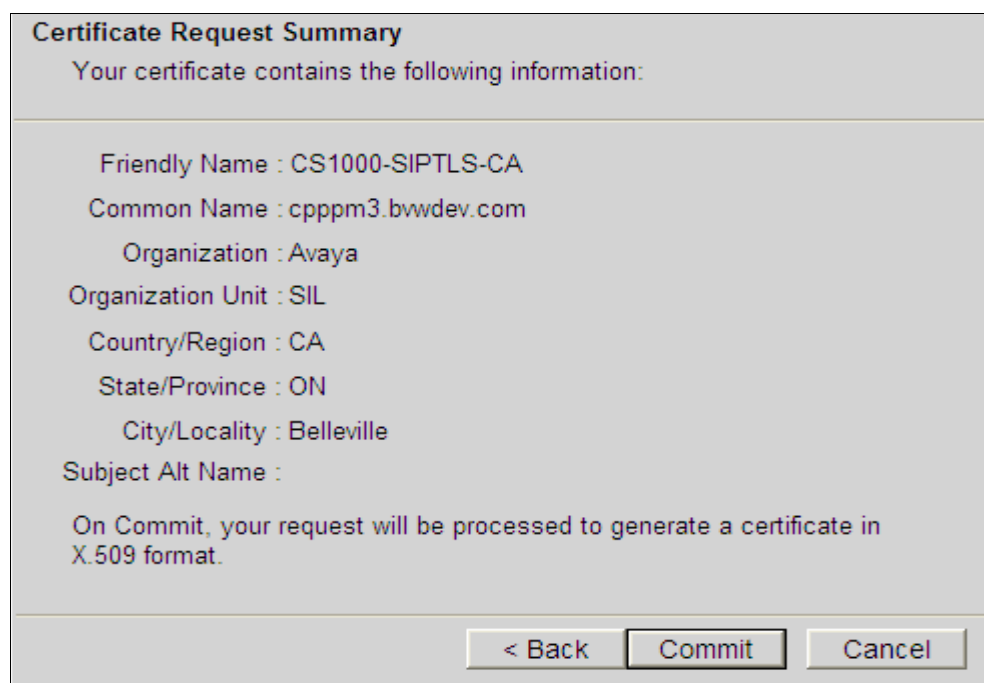
State/Province :

City/Locality :

State/Province and City/Locality must be complete, official names and must not contain abbreviations.

< Back   Next >   Cancel

The **Certificate Request Summary** page is displayed, this display the summary of the certificate information that has been entered by the user in previous steps. Click **Commit** button to create the certificate.



**Certificate Request Summary**

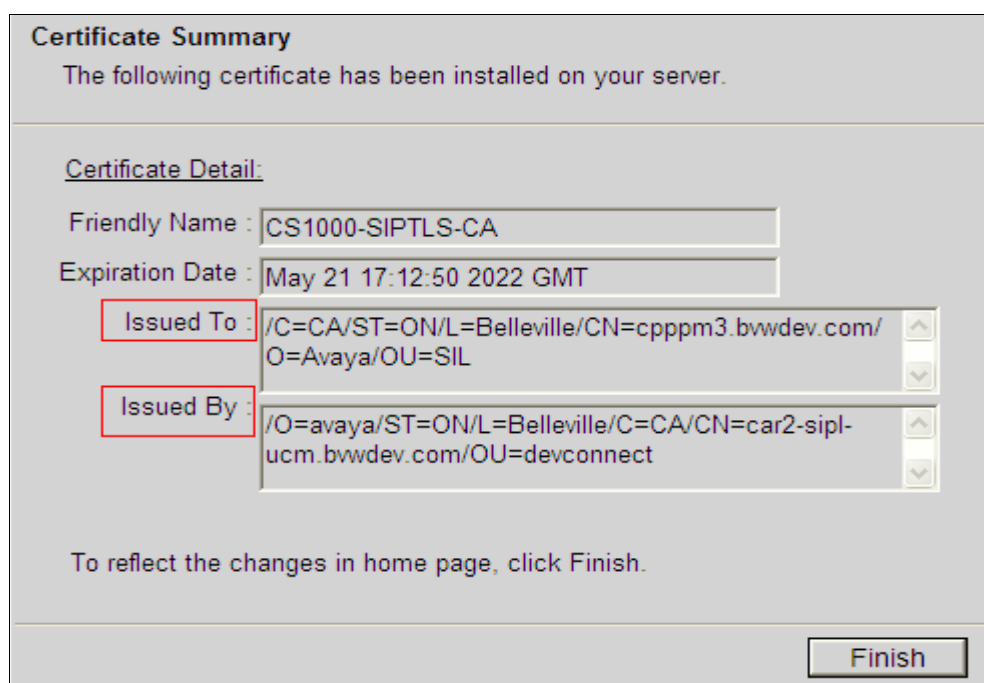
Your certificate contains the following information:

Friendly Name : CS1000-SIPTLS-CA  
Common Name : cpppm3.bwwdev.com  
Organization : Avaya  
Organization Unit : SIL  
Country/Region : CA  
State/Province : ON  
City/Locality : Belleville  
Subject Alt Name :

On Commit, your request will be processed to generate a certificate in X.509 format.

< Back   Commit   Cancel

The **Certificate Summary** page is displayed to indicate that the certificate is successfully created and signed by local private Certificate Authority, UCM. Click **Finish** button to complete and close the window.



**Certificate Summary**

The following certificate has been installed on your server.

Certificate Detail:

Friendly Name : CS1000-SIPTLS-CA  
Expiration Date : May 21 17:12:50 2022 GMT  
Issued To : /C=CA/ST=ON/L=Belleville/CN=cpppm3.bwwdev.com/O=Avaya/OU=SIL  
Issued By : /O=avaya/ST=ON/L=Belleville/C=CA/CN=car2-sipl-ucm.bwwdev.com/OU=devconnect

To reflect the changes in home page, click Finish.

Finish

The screen below shows the new certificate for SIP TLS has been created and signed in the **Certificates** window of SIP gateway member **10.10.97.150**.

**Endpoint Details**  
Details for the selected endpoint.

**Certificates**

	Service Profile	Status	Friendly name	Expiration date
1	Default Certificate	signed	car2-sps.bvwdev.com	Jan 8, 2021
2	<a href="#">DTLS</a>	none		
3	<a href="#">Web SSL</a>	none		
4	<a href="#">SIP TLS</a>	signed	CS1000-SIPTLS-CA	May 21, 2022

**Certificate Authorities**

[Add...](#) [Enable Trust](#) [Disable Trust](#) [Delete](#) [Update CRL](#)

	Friendly name	Expiration date	Trusted	Issued by	Last CRL Update
1	<input type="radio"/> car2-sipl-ucm.bvwdev.com	Feb 1, 2035	yes	/O=avaya/ST=ON/L=Belleville/...	May 23, 2012

## 5.2. Download Local Private Certificate Authority of Avaya Communication Server 1000E

The certificate of local private Certificate Authority on UCM server which is used to sign for the SIP TLS certificate configured in **Section 5.1** needs to be added to certificate store in Session Manager. This procedure shows how to obtain the CA. In the **Certificate Management** page, click on **Private Certificate Authority** tab and in the **Private Certificate Authority Details** window, click on **Download** button to download the CA certificate.

Host Name: car2-sipl-ucm.bvwdev.com    Software Version: 02.20.0023.00(5197)    User Name admin

**Certificate Management**  
Distribute and maintain Web SSL and SIP TLS security certificates, and manage the Private Certificate Authority.

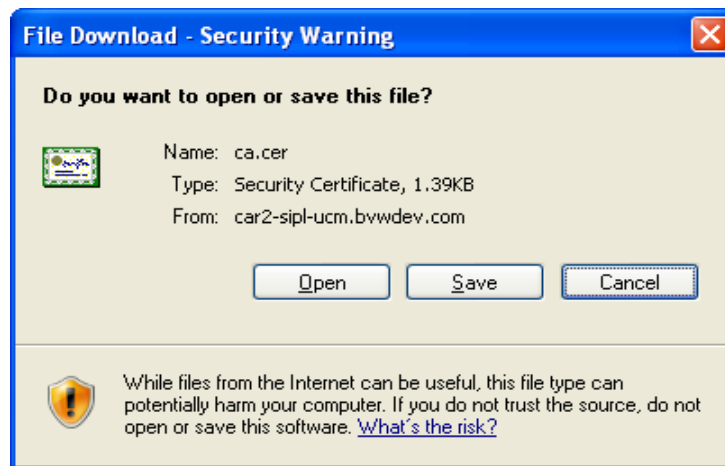
[Search](#) [Reset](#)

**Certificate Endpoints**    **Private Certificate Authority**

**Private Certificate Authority Details**  
Click the download button to save the certificate contents. It can be later imported into the Trusted Root Certificate Authorities of your client.

Subject: OU=devconnect,CN=car2-sipl-ucm.bvwdev.com,C=CA,L=Belleville,ST=ON,O=avaya  
Expiration date: Feb 1, 2035  
Fingerprint: 0a:d4:7f:06:d7:a0:64:36:50:60:31:ec:f8:67:37:82  
Contents: [Download](#)

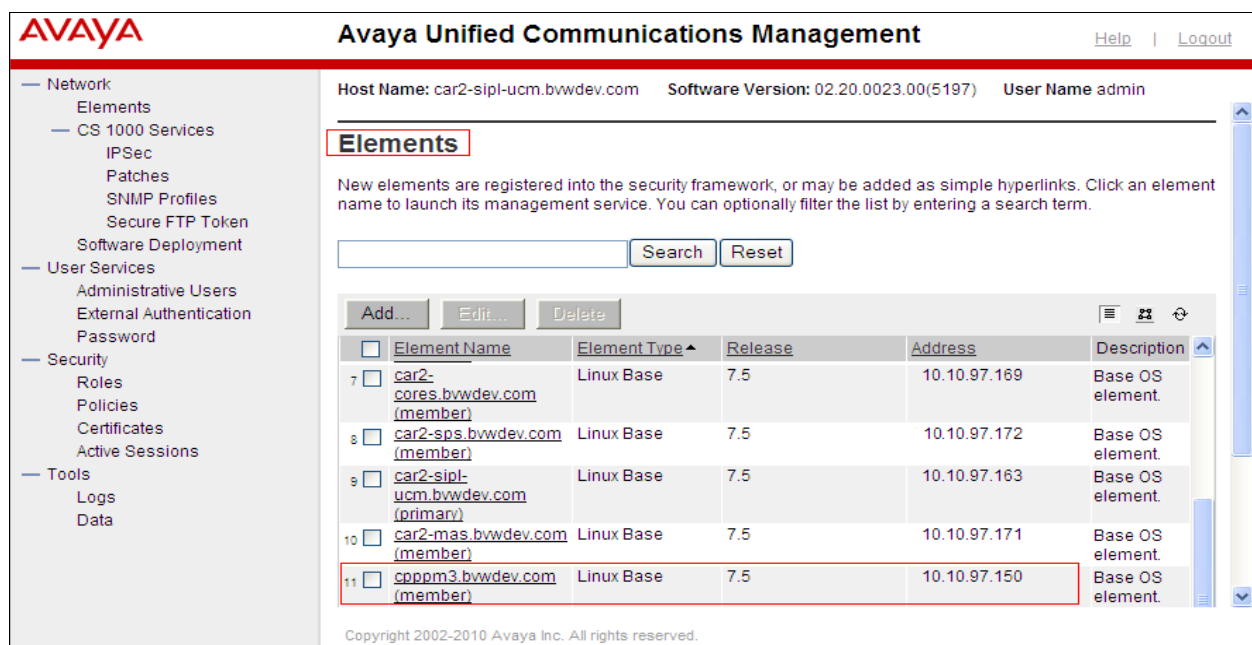
The popup window below is displayed; click **Save** button to save the CA certificate to local computer, this CA will be used to add to Session Manager in **Section 6.9**.



### 5.3. Add Common Name of Session Manager Certificate to Host File of SIP Gateway

When exchanging certificates between Avaya CS1000 SIP gateway and Session Manager to establish SIP TLS, Session Manager uses the default certificate that is shipped with the server and in the certificate of Session Manager, the **Common Name** is named as “SM100” and this name needs to be resolved to Session Manager signaling IP address in the host file of Avaya CS1000 SIP gateway.

In order to add an entry in the host file for SIP gateway server, log in to the UCM server, in the left navigation pane select **Elements**. The **Elements** page is displayed in the right, select Avaya CS1000 member server, in this case **cpppm3.bvwdev.com** with IP **10.10.97.150**.



**AVAYA** Avaya Unified Communications Management Help | Logout

Host Name: car2-sipl-ucm.bvwdev.com Software Version: 02.20.0023.00(5197) User Name admin

**Elements**

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	Element Name	Element Type	Release	Address	Description
7	<a href="#">car2-cores.bvwdev.com (member)</a>	Linux Base	7.5	10.10.97.169	Base OS element.
8	<a href="#">car2-sps.bvwdev.com (member)</a>	Linux Base	7.5	10.10.97.172	Base OS element.
9	<a href="#">car2-sipl-ucm.bvwdev.com (primary)</a>	Linux Base	7.5	10.10.97.163	Base OS element.
10	<a href="#">car2-mas.bvwdev.com (member)</a>	Linux Base	7.5	10.10.97.171	Base OS element.
11	<a href="#">cpppm3.bvwdev.com (member)</a>	Linux Base	7.5	10.10.97.150	Base OS element.

Copyright 2002-2010 Avaya Inc. All rights reserved.

The **Base Manager** page of **cpppm.bvwdev.com** server is displayed.

**AVAYA** **Base Manager** [Help](#) | [Logout](#)

Managing: 10.10.97.150 ( Member UCM server )  
Base System

**Base Overview**

Product Release:	7.50.17.00
Base Applications	
base 7.50.17	[patched]
NTAFS	7.50.17
sm	7.50.17
cs1000-Auth	7.50.17
Jboss-Quantum 7.50.17	[patched]
cnd	7.50.17
lhmonitor	7.50.17
baseAppUtils 7.50.17	[patched]
dfoTools	7.50.17
nnnm	7.50.17
cppmUtil	7.50.17
oam-logging 7.50.17	[patched]
dmWeb n/a	[patched]
baseWeb n/a	[patched]

Click on **DNS and Hosts** tab in the left navigation pane in the screen above, **Domain Name Server (DNS)** page is displayed in the right (screen not shown), click on **Add** button under **Hosts** window in this page to add a new host (screen not shown).

The **New Host** page is displayed, enter Session Manager signaling IP **10.10.97.198** in the **IP Address** field, “**SM100**” in the **Host name** field and “**bvwdev.com**” in the **Domain** field. Click **Save** button to save changes.

**AVAYA** **Base Manager** [Help](#) | [Logout](#)

Managing: 10.10.97.150 ( Member UCM server )  
[Base System](#) » [Networking](#) » [DNS and Hosts](#) » New Host

**New Host**

IP address:	<input type="text" value="10.10.97.198"/>	*
Host name:	<input type="text" value="SM100"/>	*
Domain:	<input type="text" value="bvwdev.com"/>	*

\*Required value.

## 5.4. Configure Avaya Communication Server 1000E SIP Gateway using TLS

Access to Avaya CS1000 SIP Gateway Element Manager via UCM, from the homepage of UCM, navigate to **Network** → **Elements**, the Element page is displayed in the right, click **EM\_on\_cpppm3** which is the Element Manager of the Avaya CS1000 system that is to be administered.

**AVAYA** Avaya Unified Communications Management Help | Logout

Host Name: car2-sipl-ucm.bvwdev.com Software Version: 02.20.0023.00(5197) User Name admin

**Elements**

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

<input type="checkbox"/>	Element Name	Element Type	Release	Address	Description
<input type="checkbox"/>	EM on car2-cores	CS1000	7.5	10.10.97.90	New element.
<input type="checkbox"/>	EM on car2-ssq-carrier	CS1000	7.5	10.10.97.90	New element.
<input type="checkbox"/>	EM on cpppm3	CS1000	7.5	10.10.97.78	New element.

Copyright 2002-2010 Avaya Inc. All rights reserved.

The CS1000 Element Manager page is displayed; in the left navigation pane select **System** → **IP Network** → **Nodes: Servers and Media Cards**, **IP Telephony Nodes** page is displayed in the right.

**AVAYA** CS1000 Element Manager Help | Logout

Managing: 10.10.97.78 Username: admin  
System » IP Network » IP Telephony Nodes

**IP Telephony Nodes**

Click the Node ID to view or edit its properties.

<input type="checkbox"/>	Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6
<input type="checkbox"/>	511	1	LTPS, Gateway ( SIPGw )	-	10.10.97.149	
<input type="checkbox"/>	512	1	SIP Line	-	10.10.97.187	

Show: ☒ Nodes ☐ Component servers and cards ☒ IPv6 address

Select **Node 511** which has SIPGw and LTPS applications installed on this node in the **IP Telephony Nodes** page above. The **Node Details (ID: 511 - LTPS, Gateway ( SIPGw ))** section is displayed. Click on **Gateway (SIPGw)** application in the **Applications (click to edit configuration)** section to edit.

CS1000 Element Manager

Managing: 10.10.97.78 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

**Node Details (ID: 511 - LTPS, Gateway ( SIPGw ))**

Subnet mask: 255.255.255.192 \*

Subnet mask: 255.255.255.192 \*

Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)**
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

\* Required Value.

Save

The **Node ID: 511 - Virtual Trunk Gateway Configuration Details** page is displayed, in the **General** section, select **SIP Gateway (SIPGw)** in **Vtrk gateway application** field, enter SIP domain “**bwvdev.com**” in **SIP domain name** field, this SIP domain will be defined in **Section 6.1, 5060** in **Local SIP port** field, “**cpppm3**” in **Gateway endpoint name**, and **511** in **Application ID** field.

CS1000 Element Manager

Managing: 10.10.97.78 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

**Node ID: 511 - Virtual Trunk Gateway Configuration Details**

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw)

SIP domain name: bwvdev.com \*

Local SIP port: 5060 \* (1 - 65535)

Gateway endpoint name: cpppm3 \*

Gateway password: \*

Application node ID: 511 \* (0-9999)

Enable failsafe NRS: ☐

SIP ANAT: IPv4

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses list below.

Monitor IP: Add

Monitor addresses: Remove



Continue to scroll down to **SIP Gateway Settings** section, select **Best Effort** in **TLS security** dropdown menu and enter port **5061** in **Port** field.

CS1000 Element Manager Help | Logout

Managing: 10.10.97.78 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

### Node ID: 511 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

**SIP Gateway Settings**

TLS Security: **Best Effort** (v)

Port: **5061** (1 - 65535)

Number of byte re-negotiation: **0** (v)

Options: ☐ Client authentication  
☐ X509 certificate authority

Direct SIP Route

☐ Enforce Direct SIP Route to Microsoft Mediation Server

FQDN of Microsoft Mediation Server:

Port: **5060** (1 - 65535)

Transport protocol: **TLS** (v)

Proxy Or Redirect Server:

Proxy Server Route 1:

Scroll down to **Proxy Or Redirect Server** subsection of **SIP Gateway Settings** section, in the **Proxy Server Route 1**, enter signaling IP address of Session Manager **10.10.97.198** in **Primary TLAN IP address** field, **5061** in **Port** field, and select **TLS** from **Transport protocol** menu. Keep other values in the **Proxy Or Redirect Server** at default.

CS1000 Element Manager Help | Logout

Managing: 10.10.97.78 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

### Node ID: 511 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

**Proxy Or Redirect Server:**

**Proxy Server Route 1:**

Primary TLAN IP address: **10.10.97.198**  
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: **5061** (1 - 65535)

Transport protocol: **TLS** (v)

Options: ☐ Support registration  
☐ Primary CDS proxy

Scroll down to **SIP URI Map** subsection of the **SIP Gateway Settings** section, default values in **Private domain names** is displayed in the screen. If it is not same as displayed values, change it to default values.

**CS1000 Element Manager** Help | Logout

---

Managing: 10.10.97.78 Username: admin  
 System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

**Node ID: 511 - Virtual Trunk Gateway Configuration Details**

General | SIP Gateway Settings | SIP Gateway Services

**SIP URI Map:**

Public E.164 domain names		Private domain names	
National:	<input type="text"/>	UDP:	<input type="text" value="udp"/>
Subscriber:	<input type="text"/>	CDP:	<input type="text" value="cdp.udp"/>
Special number:	<input type="text" value="PublicSpecial"/>	Special number:	<input type="text" value="PrivateSpecial"/>
Unknown:	<input type="text" value="PublicUnknown"/>	Vacant number:	<input type="text" value="PrivateUnknown"/>
		Unknown:	<input type="text" value="UnknownUnknown"/>

Scroll down to end of the **Node ID: 511 - Virtual Trunk Gateway Configuration Details** page, and select **Save** button to save changes in this page (screen not shown) and then click **Save** button in the **Node Details (ID: 511 - LTPS, Gateway ( SIPGw ))** page to save change in the **Node 511**.

The **Node Saved** page is displayed, click on **Transfer Now** button to transfer changes to associated server, SIP Gateway **10.10.97.150**.

**CS1000 Element Manager** Help | Logout

---

Managing: 10.10.97.78 Username: admin  
 System » IP Network » IP Telephony Nodes » Node Saved

**Node Saved**

Node ID: 511 has been saved on the call server.

The new configuration must also be transferred to associated servers and media cards.

You will be given an option to select individual servers, or transfer to all.

You may initiate a transfer manually at a later time.

The changes also need to be synchronized with call server, **Synchronize Configuration Files (Node ID <511>)** page is displayed, select signaling **cpppm3** in **Hostname** column and then select **Start Sync** button to start synchronizing data between SIP Gateway and call server.

**CS1000 Element Manager** Help | Logout

Managing: 10.10.97.78 Username: admin  
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

**Synchronize Configuration Files (Node ID <511>)**

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart\* of applications on affected server(s) when complete.

[Print](#) | [Refresh](#)

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cpppm3	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

\* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNTP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

The SIP gateway needs to be restarted for configuration changes in the SIP gateway and for creating of new certificate of SIP TLS to take effect. In order to restart the SIP Gateway signaling, log in to Linux command line of your SIP gateway with administrator privileges and issue the command **appstart vtrk restart** as shown below:

```
[admin@cpppm3 ~] $
[admin@cpppm3 ~] $ appstart vtrk restart

[ OK ]
[ OK ]
Synchronizing the system host database file [ OK ]
Stopping VTRK: [ OK ]
Starting VTRK: [ OK ]
```

## 6. Configure Avaya Aura® Session Manager

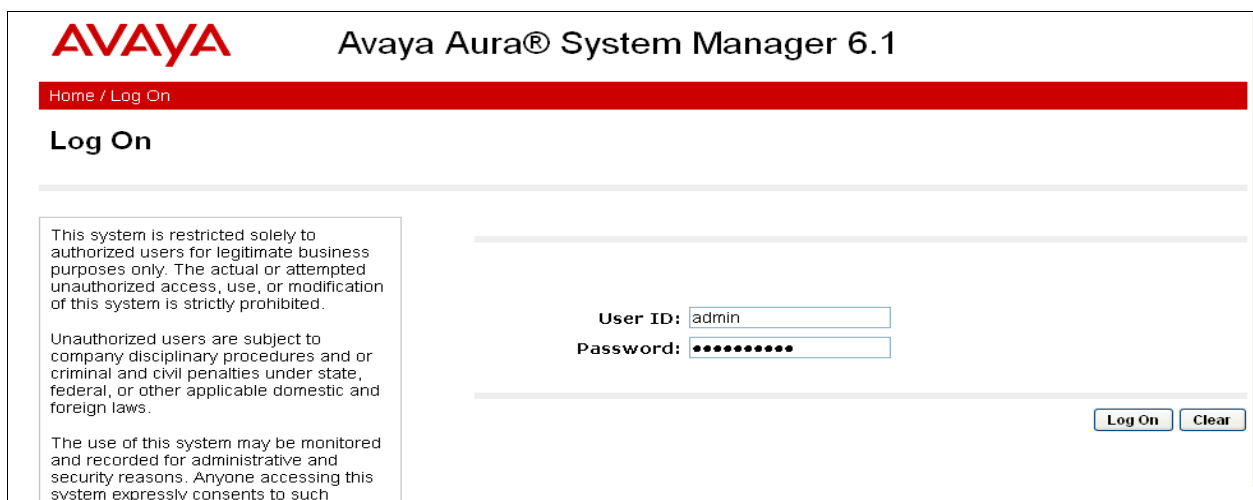
This section provides the procedures for configuring Session Manager. Session Manager is comprised of two functional components: The Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

This section assumes that Session Manager and System Manager have been installed, and network connectivity exists between the two platforms. The following steps describe the configuration needed for Session Manager.

- SIP Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Configure SIP TLS certificate For CS1000 SIP Gateway and Vocera Server

### 6.1. Configure SIP Domain

Launch a web browser, enter <https://<IP address of System Manager>> in the URL, and log in with the appropriate credentials.



**AVAYA** Avaya Aura® System Manager 6.1

Home / Log On

### Log On

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such

User ID:

Password:

Navigate to **Elements→Routing→Domains** and click on the **New** button to create a new SIP Domain (screen not shown). Enter the following values and use defaults for the remaining fields:

- **Name** –Enter the Authoritative Domain name specified in CS1000 SIP Gateway in **Section 5.4**, which is **bwvdev.com**.
- **Type** – Select **SIP**

Click **Commit** to save. The following screen shows the Domains page, listed is the newly created domain that was used during the compliance test.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar has a 'Routing' menu with 'Domains' highlighted. The main content area is titled 'Domain Management' and shows a table of 18 items. The table has columns for Name, Type, Default, and Notes. The domain 'bvwdev.com' is highlighted in red in the original image.

	Name	Type	Default	Notes
<input type="checkbox"/>	acebvw.com	sip	<input type="checkbox"/>	ACE SIP domain
<input type="checkbox"/>	avaya.com	sip	<input type="checkbox"/>	
<input type="checkbox"/>	broadconnect.ca	sip	<input type="checkbox"/>	Broadconnect testing
<input type="checkbox"/>	bvwdev7.com	sip	<input type="checkbox"/>	For VPath
<input type="checkbox"/>	bvwdev.com	sip	<input type="checkbox"/>	For testing SIP TLS with CS1K and Vocera
<input type="checkbox"/>	cm521.mtsallstream.com	sip	<input type="checkbox"/>	
<input type="checkbox"/>	cm601.avaya.com	sip	<input type="checkbox"/>	Enterprise domain for CM601

## 6.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. This is used for bandwidth management or location-based routing.

Navigate to **Routing→Locations**, and click on the **New** button to create a new SIP Entity location (screen not shown).

### General section

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

- Enter a descriptive Location in the **Name** field (e.g. **Belleville**).
- Enter a description in the **Notes** field if desired.

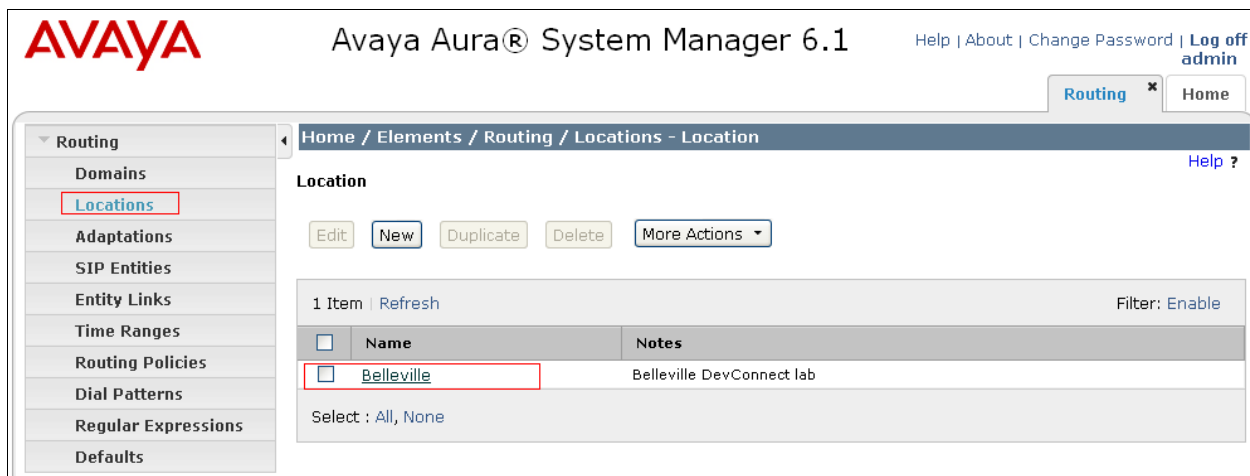
### Location Pattern section

Click **Add** and enter the following values:

- The IP address information for the **IP address Pattern** (e.g. **10.10.97.\***).
- A description in the **Notes** field if desired.

Repeat these steps in the Location Pattern section if the Location has multiple IP segments. Modify the remaining values on the form, if necessary; otherwise, use all the default values. Click on the **Commit** button.

Repeat all the steps for each new Location. The following screen shows the **Location** used during the compliance test.



### 6.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk. During the compliance test the following SIP Entities were configured:

- Session Manager
- Avaya CS1000 SIP Gateway
- Vocera Server

Navigate to **Routing → SIP Entities** and click on the **New** button to create a new SIP entity (screen not shown). Provide the following information:

#### General section

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the IP address of the signaling interface on each:
  - Avaya CS1000 SIP Gateway: 10.10.97.149
  - Signaling Session Manager: 10.10.97.198
  - Vocera server: 10.20.21.210
- From the **Type** drop down menu, select a type that best matches the SIP Entity:
  - For Avaya CS1000 SIP Gateway: select **SIP Trunk**
  - For Session Manager, select **Session Manager**
  - For Vocera Server, select **Other**
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

Click on the **Commit** button to save each SIP entity. Repeat all the steps for each new entity.

The screen below shows the detail of **Session Manger SIP Entity**.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities - SIP Entity Details

Help ?

Commit

Cancel

SIP Entity Details

General

Name: DevASM

\* FQDN or IP Address: 10.10.97.198

Type: Session Manager

Notes: For Session Manager

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The screen below shows the details of Avaya CS1000 SIP Entity.

AVAYA

Avaya Aura® System Manager 6.1

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / SIP Entities - SIP Entity Details

Help ?

Commit

Cancel

SIP Entity Details

General

Name: CS1000SIPGw

\* FQDN or IP Address: 10.10.97.149

Type: SIP Trunk

Notes: SIP Entity For CS1K Bottom

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: egress

The screen below shows the detail of **Vocera SIP Entity**.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. Below this, a breadcrumb trail reads 'Home / Elements / Routing / SIP Entities - SIP Entity Details'. The left sidebar contains a menu with 'Routing' expanded, showing sub-items like 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. A red box highlights the 'Name' field (containing 'Vocera') and the 'FQDN or IP Address' field (containing '10.22.21.210'). Other fields include 'Type' (set to 'Other'), 'Notes' (containing 'SIP Entity for Vocera'), 'Adaptation' (a dropdown menu), 'Location' (set to 'Belleville'), and 'Time Zone' (set to 'America/Toronto'). There is an unchecked checkbox for 'Override Port & Transport with DNS SRV'. The 'SIP Timer B/F (in seconds)' is set to '4'. The 'Credential name' field is empty. The 'Call Detail Recording' is set to 'none'. At the top right of the form area are 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

## 6.4. Configure Entity Links

Entity Links define the connections between the SIP Entities (in this case, Avaya CS1000 SIP gateway and Vocera server) and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Avaya CS1000 SIP Gateway
- Session Manager ⇔ Vocera Server

Navigate to **Routing → Entity Links** and click on the **New** button to create a new entity link (screen not shown). Provide the following information:

- **Name:** Enter a descriptive name.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section Error! Reference source not found.** (e.g. **DevASM**).
- In the **Protocol** drop down menu, select the TLS protocol.
- In the **Port** field, enter the port to be used (e.g. **5061**).
- In the **SIP Entity 2** drop down menu, select **CS1000SIPGw** for the entity link between Session Manager and Avaya CS1000 SIP gateway and select **Vocera** for the Vocera entity.
- In the **Port** field, enter the port to be used (e.g. **5061**).
- Check the **Trusted** box.
- Enter a description in the **Notes** field if desired.



Click on the **Commit** button to save each Entity Link definition. Repeat all the steps for each new SIP Entity Link.

The newly created entity link between Session Manager and Avaya CS1000 SIP Gateway is shown below in the screen shot.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM_CS1K_5061_TLS	* DevASM	TLS	* 5061	* CS1000SIPGw	* 5061	Trusted

The newly created entity link between Session Manager and Vocera server is shown below in the screen shot.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Entity Links - Entity Links

Entity Links

Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
* SM_Vocera_5061_TL	* DevASM	TLS	* 5061	* Vocera	* 5061	Trusted

## 6.5. Time Ranges

Time Ranges define admission control criteria to be specified for Routing Policies (**Section** Error! Reference source not found.). In the reference configuration, no restrictions were used.

To add a Time Range, navigate to **Routing**→**Time Ranges**, and click on the **New** button (screen not shown). Provide the following information:

- Enter a descriptive name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

Click the **Commit** button. The following screen shows the Time Range page used during the compliance test.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing × Home

Home / Elements / Routing / Time Ranges - Time Ranges

Time Ranges

Edit New Duplicate Delete More Actions ▾

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

## 6.6. Configure Routing Policy

Routing Policies associate destination SIP Entities (**Section** Error! Reference source not found.) with Time of Day admission control parameters (**Section** Error! Reference source not found.) and Dial Patterns (**Section** Error! Reference source not found.). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Avaya CS1000 SIP gateway.
- Inbound calls to Vocera server.

To add a Routing Policy, navigate to **Routing**→**Routing Policies** and click on the **New** button on the right (screen not shown). Provide the following information:

### General section

- Enter a descriptive name in the **Name** field (e.g. **To\_CS1K75\_Bottom**, **To\_Vocera**).
- Enter a description in the **Notes** field if desired.

### SIP Entity as Destination section

- Click the **Select** button.
- Select a SIP Entity that will be the destination for this call.
- Click the **Select** button and return to the Routing Policy Details form.

### Time of Day section

- Leave default values.

Click **Commit** to save Routing Policy definition. Repeat the steps for each new Routing Policy.

The following screen shows the Routing Policy used for Avaya CS1000 during the compliance test.

Routing Policy Details

General

\* Name: To\_CS1K75\_Bottom

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1000SIPGw	10.10.97.149	SIP Trunk	SIP Entity For CS1K Bottom

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

The following screen shows the Routing Policy used for Vocera during the compliance test

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

General

\* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Vocera	10.22.21.210	Other	SIP Entity for Vocera

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh Filter: Enable

	Ranking 1 ▲	Name 2 ▲	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

## 6.7. Configure Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In the compliance test, the following dial patterns are defined from Session Manager.

- 54xxx – dial pattern used to route calls to Avaya CS1000.
- 732x – dial pattern used to route to Vocera.

To add a Dial Pattern, select **Routing → Dial Patterns** and click on the **New** button (screen not shown) on the right pane. Provide the following information:

### General section

- Enter a unique pattern in the **Pattern** field (e.g. **54**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** drop down menu select the domain **bvwdev.com** defined in **Section 6.1**.

### Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (screen not shown).
- Click on the box for the appropriate Originating Locations, and Routing Policies (see **Section 6.6**) that pertain to this Dial Pattern.
  - Select the Originating Location to apply the selected routing policies to **All**.
  - Select appropriate Routing Policies.
  - Click on the **Select** button and return to the **Dial Pattern** page.

Click the **Commit** button to save the new definition. Repeat steps for the remaining Dial Patterns. The following screen shows the dial pattern **54xxx** used to route calls to Avaya CS1000 system during the compliance test.

**Avaya Aura® System Manager 6.1**

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Commit Cancel

General

\* Pattern: 54

\* Min: 5

\* Max: 5

Emergency Call: ☐

SIP Domain: bvwddev.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To_CS1K75_Bottom	0	<input type="checkbox"/>	CS1000SIPGw	

The following screen shows the dial pattern **732x** used to route calls to Vocera server during the compliance test.

**Avaya Aura® System Manager 6.1**

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

Commit Cancel

General

\* Pattern: 732

\* Min: 4

\* Max: 4

Emergency Call: ☐

SIP Domain: bvwddev.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	To_Vocera	0	<input type="checkbox"/>	Vocera	Route to Vocera

## 6.8. Configure Manage Elements

To define a new Manage Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (screen not shown) to open the **New Entities Instance** page.

In the **New Entities Instance** Page

- In the **Type** field, select **Session Manager** using the drop-down menu and the **New Session Manager Instance** page opens (screen not shown).

In the **New Session Manager Instance** page, provide the following information:

- Application section
  - **Name** – Enter name for Session Manager Instance, e.g. “SM\_INS”.
  - **Description** - Enter description if desired.
  - **Node** – Enter IP address of the administration interface, **10.10.97.197**.

The screenshot displays the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows 'Home / Elements / Inventory / Manage Elements - New Session Manager Instance'. The left sidebar contains a tree view with 'Inventory' expanded, showing 'Manage Elements' (highlighted with a red box), 'Discovered Inventory', 'Discovery Management', and 'Synchronization'. The main content area is titled 'New Session Manager Instance' and includes 'Commit' and 'Cancel' buttons. The 'Application' section is expanded, showing a dropdown menu for 'Application'. Below this, there are four input fields, each with a red asterisk indicating a required field: 'Name' (containing 'SM\_INS'), 'Type' (a dropdown menu set to 'Session Manager' with a 'Reset' button), 'Description' (a text area), and 'Node' (containing '10.10.97.197'). At the bottom, there is an 'Access Point' section with a dropdown arrow.

- Access Point section: Check on **Session Manager** radio button and then click **Edit** button to edit, in the **Access Point Details** section, enter host name of Session Manager server in the **Host** field, e.g. “DevASM” and keep other values at default. Click **Save** button to save changes.

Click **Commit** button in the **New Session Manager Instance** page to complete creation of new element of Session Manager.

**Access Point**

View

Edit

New

Delete

1 Item

	Name	Access Point Type	Protocol	Host	Port	Order
	Session Manager	TrustManagement	jnp		1299	0

Select : None

Access Point Details

\* Name

Session Manager

Access Point Type

TrustManagement

\* Container Type

JBOSS

\* Protocol

jnp

\* Host

DevASM

\* Port

1299

\* URI

None

\* Order

0

Description

Save

Cancel

## 6.9. Configure TLS for Avaya Communication Server 1000E SIP Gw and Vocera Server

In System Manager, navigate to **Elements** → **Inventory** → **Manage Elements**. Click the Session Manager SM\_INS created in Section 6.8 and select **More Actions** → **Configure Trusted Certificates** (not shown), the **Trusted Certificates** page is displayed as the screen below.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left sidebar shows the 'Inventory' menu with 'Manage Elements' highlighted. The main content area is titled 'Trusted Certificates' and includes a 'Home / Elements / Inventory / Manage Elements - Trusted Certificates' breadcrumb. Below the title are buttons for 'View', 'Add', 'Export', and 'Remove'. A table lists 26 items with columns for 'Store Description', 'Store Type', and 'Subject Name'. The 'Add' button is highlighted with a red box.

<input type="checkbox"/>	Store Description	Store Type	Subject Name
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=avaya development team, OU=UK Engineering, O=avaya, L=Cardiff, ST=Wales, C=UK
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	EMAILADDRESS=igonzaes@avaya.com, OU=EMMC, O=AVAYA, L=Andover, ST=MA, C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	EMAILADDRESS=support@vocera.com, CN=157.22.21.210, L=CUPERTINO, ST=CALIFORNIA, C=US



Click **Add** button as shown above to add the local CA certificate of Avaya CS1000 UCM that is already saved in **Section 5.2**. In the **Add Trusted Certificate** page, select “**All**” in the **Select Store Type to add trusted certificate** field, check on radio button to **Import from file**, the **Please Select a file** box is displayed, select **Browse** button to upload the local CA certificate of UCM and then click **Retrieve Certificate** button to retrieve. Click **Commit** button to save.

Home / Elements / Inventory / Manage Elements - Add Trusted Certificate

**Add Trusted Certificate**

Select Store Type to add trusted certificate: All

☐ Import from existing  
☒ Import from file  
☐ Import as PEM Certificate  
☐ Import using TLS

\* Please select a file

You must click the Retrieve certificate button and review the certificate details before you can continue.

**Certificate Details**

Subject: OU=devconnect, CN=car2-sipl-ucm.bvwdev.c  
 Valid From: Thu Jan 06 10:06:30 EST 2011 Valid To: Wed Jan 31 19:00:00 EST 2035  
 Key Size: X.509  
 Issuer Name: OU=devconnect, CN=car2-sipl-ucm.bvwdev.c  
 Finger Print: bb0fe47c8f236ff39494f459c84d2b01c4a6617

Repeat the same procedure above to add the self-signed certificate of Vocera server into the certificate store of **Session Manager**, the screen below shows the **Add Trusted Certificate** page while adding Vocera’s certificate.

Home / Elements / Inventory / Manage Elements - Add Trusted Certificate

**Add Trusted Certificate**

Select Store Type to add trusted certificate: All

☐ Import from existing  
☒ Import from file  
☐ Import as PEM Certificate  
☐ Import using TLS

\* Please select a file

You must click the Retrieve certificate button and review the certificate details before you can continue.

**Certificate Details**

Subject: EMAILADDRESS=support@vocera.com, CN=15  
 Valid From: Tue May 15 17:23:15 EDT 2012 Valid To: Sun May 14 17:23:15 EDT 2017  
 Key Size: X.509  
 Issuer Name: EMAILADDRESS=support@vocera.com, CN=15  
 Finger Print: 37c9e763c9ed3fcbfa9f3991bfd57d1a6497e0

Return to **Manage Elements** page. Select **Session Manager** element and then select **Configure Trusted Certificates** from **More Actions** menu (not shown) to confirm the local Avaya CS1000 UCM and Vocera certificates were successfully added as shown below.

**Trusted Certificates**

26 Items | Refresh | Filter: Enable

<input type="checkbox"/>	Store Description	Store Type	Subject Name
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=SIP Product Certificate Authority, OU=SIP Product Certificate Authority, O=Avaya Inc., C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=avaya development team, OU=UK Engineering, O=avaya, L=Cardiff, ST=S Wales, C=UK
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	EMAILADDRESS=igonzaes@avaya.com, OU=EMMC, O=AVAYA, L=Andover, ST=MA, C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	EMAILADDRESS=support@vocera.com, CN= 10.22.21.210, L=CUPERTINO, ST=CALIFORNIA, C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=SCCAN Server Root CA, OU=Seamless Converged Communication Across Networks, O="Motorola, Inc.", C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=Avaya Call Server, OU=Media Server, O=Avaya Inc., C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	OU=devconnect, CN=car2-sipl-ucm.bvwddev.com, C=CA, L=Belleville, ST=ON, O=avaya
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=Avaya Product Root CA, OU=Avaya Product PKI, O=Avaya Inc., C=US
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	O=AVAYA, OU=MGMT, CN=default
<input type="checkbox"/>	Used for validating TLS client identity certificates	SM_SECURITY_MODULE	CN=Avaya Manufacturing Subordinate CA, OU=Avaya Product PKI, O=Avaya Inc., C=US

It is required to update the security certificates to the Session manager Security Module. Navigate to **Elements** → **Session Manager** → **System Status** → **Security Module Status**, select name of the Session Manager that needs to be updated, in this case **DevASM**, and select **Update Installed Certificates** from **Certificate Management** menu.

**Avaya Aura® System Manager 6.1**

Home / Elements / Session Manager / System Status / Security Module Status - Security Module Status

**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 | Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding
<input type="checkbox"/>	Show	DevASM	SM	Up	47	10.10.97.198/26	---	10.10.97.193	Disabled

Select : None

## 7. Configure Vocera System

This section assumes that Vocera system is already installed and configured by Vocera Engineer, the section describes procedure of how to configure the Vocera Communication System to inter-work with the Avaya CS1000 system and Session Manager.

### 7.1. Configure TLS Certificate

When installing Vocera server VSTG, it uses OpenSSL to generate a private key and a self-signed certificate in the `\vocera\telephony\vgw` folder. The certificate (**server.crt**) is set to expire 5 years after the date it was created and this certificate is used to upload to the store certificate in Session Manager as mentioned in **Section 6.9** for configuring TLS between Session Manager and Vocera server.

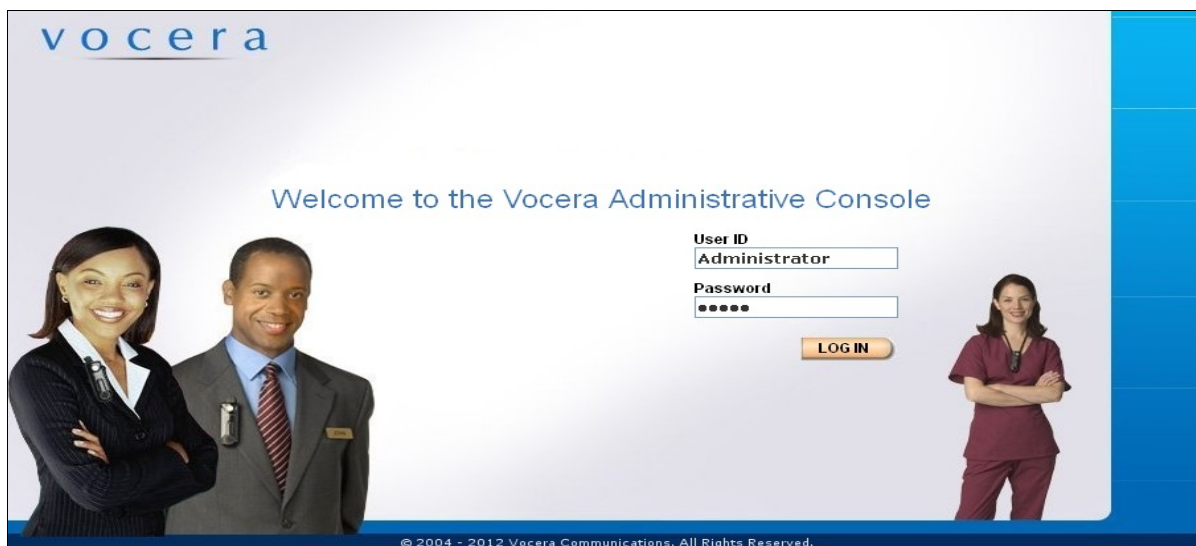
Note: If the 5-year VSTG certificate expires, a new certificate can be generated by running the `\vocera\telephony\certificate\cert.bat` batch file. However, if an upgrade VSTG is required at regular intervals, it should never need to generate a new certificate other than by running the VSTG installer.

To enable TLS transport between VSTG and Session Manager, complete the following tasks:

- Upload the TLS certificate from the following location on each Vocera SIP Telephony Gateway to Session Manager: `\vocera\telephony\vgw\server.crt`
- Set the following property in `c:\vocera\telephony\vgw\vgwproperties.txt` on each Vocera SIP Telephony Gateway: **VTGSIPTransport = tls**
- Restart each Vocera SIP Telephony Gateway.

### 7.2. Configure Vocera SIP Connectivity

Open the Vocera Communication Systems web page by addressing the IP address of the Vocera Server in the Microsoft Internet browser, <http://10.22.21.210/>. The **Welcome to the Vocera** page will appear (screen not shown), then click on the **Vocera Administration Console** link to get to the console web page as shown below.



Input proper credentials to log on to the **Console** page, click on the **Log In** button to log in. The screen below shows the **Console** page with the **Status Monitor** menu page as default.



For all the details on the configuration of Vocera Communication System, user can click on the **Documentation** option on the left navigation pane. In the **Administration and Configuration** column, select on the **Telephony Configuration Guide** to view the details description of all the available attribute settings.

To configure the Vocera Server to work with the Avaya CS1000, click on the **Telephony** option on the left navigation pane. The **Telephony** page is displayed with the **Basic Info** menu tab being selected as default, as shown in the screen below. Fill in the details of the highlighted attributes in the red-boxes. Others fields leave at default. Then Click **Save Changes** button.

- **Enable Telephony Integration:** check the check box.
- **Vocera Hunt Group Numbers** section:
  - **Guess Access:** enter the DN “7320”.
  - **Direct Access:** enter the DN “7329”.
- **Number of Lines:** the default number is “24”.
- **Integration Type:** select the “IP” radio button.
- **IP SIP Settings** section: select “SIP Version 2.0” in the drop down list.
- **SIP Settings section:**
  - **Call Signaling Address:** enter the signaling IP of Session Manager “10.10.97.198”.
  - **Call Party Number:** enter the DN “7320”. This DN will be displayed on the called party.

The screenshot displays the Vocera Administrator web interface for configuring the Telephony section. The left navigation pane includes links for Status Monitor, Sites, Users, Groups, Departments, System, Defaults, Locations, Email, Telephony (selected), Reports, Maintenance, Address Book, Devices, and Documentation. The main content area is titled 'Telephony' and features several tabs: Basic Info, Access Codes, Toll Info, DID Info, PIN, Dynamic Extensions, Sharing, and Cisco. The 'Basic Info' tab is active, showing a 'Select Site' dropdown set to 'Global'. Below this, the 'Enable Telephony Integration' checkbox is checked. The 'Vocera Hunt Group Numbers' section contains two input fields: 'Guest Access' with the value '7320' and 'Direct Access' with the value '7329'. To the right, the 'Number of Lines\*' is set to '24'. The 'Integration Type' section has two radio buttons: 'Analog' and 'IP', with 'IP' selected. A note states: 'Note: Saving any changes to digital parameters will cause the telephony server to restart.' The 'IP Settings' section includes a 'Signaling Protocol' dropdown menu set to 'SIP Version 2.0'. The 'SIP Settings' section contains two input fields: 'Call Signaling Address' with the value '135.10.97.198' and 'Calling Party Number' with the value '7320'. An 'Enable Call Trace' button is located below these fields. At the bottom of the page, there are 'Save Changes' and 'Reset' buttons, and a footer indicating 'Vocera Server 4.3SP1 [Build 2349] Console [Build 2349]'.

To configure the dialing rule on the Vocera Server, navigate to the **Access Codes** tab, fill in the red highlighted text box of the attributes as shown in the screen below. Then click **Save Changes** button.

**Vocera** ADMINISTRATOR Log Out

**Telephony**

Basic Info **Access Codes** Toll Info DID Info PIN Dynamic Extensions Sharing Cisco

Select Site: Global

Local Area Code\* **613**

☐ Omit Area Code when Dialing Locally

Default Local Access Code

Default Long-Distance Access Code

Company Voicemail Access Code

**Access Code Exceptions**

By default, numbers in the local area code use the Default Local Access Code and all others use the Default Long-Distance Access Code. Enter exceptions in the table below:

Area Code	Range of Numbers	Access Code

Add Edit Delete

Save Changes Reset

Vocera Server 4.3SP1 [Build 2349] Console [Build 2349]

### 7.3. Configure Users

To configure the users on the Vocera Server to be able to send and receive calls from the Avaya CS1000, click on the **Users** menu option. The **Users** page is displayed as shown in the screen below.

**Vocera** ADMINISTRATOR Log Out

**Users**

**Users**

**Add, Edit, and Delete Users**

Search

Type	Full Name	Site	User ID
	1, user	Global	u1
	2, user	Global	u2

1 to 2 of 2

Site Filter: All Sites

Add New User Edit User Delete User

Vocera Server 4.3SP1 [Build 2349] Console [Build 2349]

To add a user, click **Add New User** button, the user **Info** detail configuration page is displayed. Fill in the required fields, which are indicated with the red stars. The **Badge ID** field will be populated when the badge is registered to Vocera Server. Others are left at default. Click **Save**.

**Add New User**

Info Phone Speech Rec Groups Depts

First Name \* John

Last Name \* Smith

User ID \* Johns

Employee ID

Password

Re-enter Password

Email Address

Site Global Select C

Cost Center

Badge ID 0009ef07ca56

☐ Temporary User

Expiration Date (mm/dd/yyyy)

**Note:** Temporary users are removed from the system by the first message sweep after midnight on the expiration date.

Save Save & Continue Cancel

From the **Add New User** page, continue to click on the **Phone** tab to configure user specific phone number information such as **Desk phone or Extension**, **Home phone**. Others fields are optional. Click **Save**.

The screenshot shows the 'Add New User' interface with the 'Phone' tab selected. The 'Desk Phone or Extension' field contains '7321' and the 'Home Phone' field contains '6139654001'. Other fields like 'Cell Phone', 'Pager', 'Vocera Extension', 'Dynamic Extension', 'PIN for Long Distance Calls', 'Cisco EM Extension', and 'Cisco EM Auto-Answer' are empty. The 'Vocera Access Anywhere' section has an unchecked checkbox for 'Enable Vocera Access Anywhere' and two empty password fields. A note at the bottom states: 'Note: Phone password not required if caller ID permission is used.' The bottom of the form has three buttons: 'Save', 'Save & Continue', and 'Cancel'.

Click on the **Group** tab to assign the newly created user to a group with specific permission to use other call features on the Vocera Server. By default, in this example, every new user is assigned to the **Group Everyone** and belong to the **Site Global** (screen not shown).

For detailed configuration on how these **Groups** and **Sites** are configured, please refer to the **Administration Guide** by clicking on the **Documentation** option menu, under the **Administration and Configuration**.



## 8. Verification Steps

The following typical steps are used to verify SIP TLS between Session Manager and Avaya CS1000 and between Session Manager and the Vocera server.

- Verify SIP TLS entity link status is up between Session Manager and Avaya CS1000 SIP gateway by navigating to **Elements** → **Session Manager** → **System Status** → **SIP Entity Monitoring** and select the Avaya CS1000 entity link.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The breadcrumb trail is: Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring. The page title is "SIP Entity, Entity Link Connection Status". Below the title, it says "This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity." There is a search bar with the text "All Entity Links to SIP Entity: CS1000SIPGw". Below the search bar is a "Summary View" button. The table shows 1 item with a "Refresh" button and a "Filter: Enable" dropdown. The table has columns: Details, Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The row shows "► Show", "DevASM", "10.10.97.149", "5061", "TLS", "Up", "200 OK", and "Up".

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	DevASM	10.10.97.149	5061	TLS	Up	200 OK	Up

- Repeat the same procedure to verify SIP TLS entity link between Session Manager and Vocera server.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The breadcrumb trail is: Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring. The page title is "SIP Entity, Entity Link Connection Status". Below the title, it says "This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity." There is a search bar with the text "All Entity Links to SIP Entity: Vocera". Below the search bar is a "Summary View" button. The table shows 1 item with a "Refresh" button and a "Filter: Enable" dropdown. The table has columns: Details, Session Manager Name, SIP Entity Resolved IP, Port, Proto., Conn. Status, Reason Code, and Link Status. The row shows "► Show", "DevASM", "10.22.21.210", "5061", "TLS", "Up", "200 OK", and "Up".

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	DevASM	10.22.21.210	5061	TLS	Up	200 OK	Up

- Place calls from Avaya CS1000 phone to Vocera wireless badge user and vice versa to make sure SIP TLS trunks between Avaya CS1000 SIP gateway and Session Manager and between Vocera server and Session Manager are established without any failures.

- Verify audio quality for calls established between Avaya CS1000 phones (Unistim and SIP phones) with Vocera wireless badge user.

## 9. Conclusion

These Application Notes have described the administration steps required to integrate the Vocera Communication System with the Avaya Communication Server 1000E via SIP TLS trunk configured on the Avaya Aura® Session Manager. All test cases passed with observations noted in **Section Error! Reference source not found.**

## 10. Additional References

The following Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Session Manager*, Release 6.1, November 2010, Issue 1.1, Document Number 03-603324
- [2] *Administering Avaya Aura® System Manager*, Release 6.1, November 2010
- [3] *Avaya Communication Installation and Commissioning*, Doc# NN43041-310, Issue 05.04, Date May 2011.
- [4] *Avaya Communication Server 1000 Unified Communications Management Common Services Fundamentals*, Doc # NN43001-116, Issue 05.11, Date June 2011.
- [5] *Avaya Communication Server 1000 Co-resident Call Server and Signaling Server Fundamentals*, Doc # NN43001-509, Issue 03.02, Date June 2011.
- [6] *Avaya Communication Server 1000 Element Manager System Reference - Administration*, Doc# NN43001-632, Issue 05.09, Date July 2011.

Product information for Vocera Communication System can be found at <http://www.vocera.com/products/resources/documentation.aspx>

---

**©2012 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).