



# **Application Notes for Configuring Vocera Communications using TLS as the transport protocol with Avaya Aura® Session Manager and Avaya Aura® Communication Manager – Issue 1.0**

## **Abstract**

These Application Notes describe the procedure for configuring Vocera Communications to interoperate with Avaya Aura® Session Manager using TLS as the transport protocol.

The overall objective of the interoperability compliance testing is to verify Vocera Communication functionalities in an environment comprised of Avaya Aura® Communication Manager, Avaya Aura® Session Manager, and various Avaya phones including SIP, H.323 and Digital.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 procedure for configuring Vocera Communications, to interoperate with Avaya Aura® Session Manager using TLS as the transport protocol. The tested configuration comprised of the wireless communication features of Vocera Communications System with Avaya Aura® Communication Manager and Avaya Aura® Session Manager.

Vocera Communications Solution is comprised of three main components:

- Vocera Badges
- Vocera Server
- Vocera SIP Telephony Gateway

The Vocera Badges are wireless 802.11a/b/g/n devices that serve as communicators in a wireless environment. By pressing the call button on a badge, a user can interface with the Vocera Server to start the call process. Vocera B3000 and B3000N badges have a speech zone, the region in which audio can be detected. To get the best possible speech recognition, the top of the badge should be between 6 to 8 inches (15 to 20 centimeters) directly below the mouth. Any sound coming from another direction or beyond that distance is reduced or eliminated by the noise canceling microphones

The Vocera Server acts as a communication server to service calls between the badges. The Vocera Server stores the user and Badge information, and has the speech access interface that allows users to place and receive calls.

The Vocera SIP Telephony Gateway was utilized for the test, to setup a SIP trunk between the Vocera SIP Telephony Gateway and Avaya Aura® Session Manager. The Vocera SIP Telephony Gateway allows the Vocera Server to connect Badges to Avaya Aura® Communication Manager endpoints, as well as route calls to the public network through Avaya Aura® Communication Manager.

The two server applications, Vocera Server and Vocera SIP Telephony Gateway, can reside on the same physical server platform. Vocera recommends using multiple Vocera SIP Telephony Gateway servers, and array for redundancy, especially if the Vocera SIP Telephony Gateway will be hosted on a Virtual Machine.

For additional information on Vocera Communication System, please refer to Vocera documentation (3-5).

## 2. General Test Approach and Test Results

The focus of the interoperability compliance testing was to verify the ability of the Vocera Communications System to interoperate with an Avaya SIP-enabled IP Telephony environment comprised of Session Manager, Communication Manager and various Avaya phones including SIP, H.323.

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

### 2.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The feature testing focused on the following areas:

- Verify basic network connectivity
  - Badges to Access Point
  - SIP Trunk using TLS between Vocera and Avaya
- Basic calls
  - Badge to Badge
  - Badge to Phone
  - Phone to Badge
- Audio codec negotiation using G.711MU and G.711A
- Call and Voice Features
  - Proper set up and tear down of the calls
  - Proper display of Caller ID information
  - Call Transfer
  - Call Conference
  - Call Hold/Resume
  - Badge Emergency Broadcast all Badges
- DTMF transmission using RFC 2833

Feature testing was primarily done using TLS for SIP. However, interoperability for SIP was tested using UDP and TCP as well, by performing basic test calls.

Serviceability testing focused on verifying the ability of Vocera SIP Telephony Gateway (VSTG), Vocera Server and Vocera Badges to recover from adverse conditions such as network and server (e.g., Vocera, Session Manager, and Communication Manager) outages.

## 2.2. Test Results

All test cases were executed and passed with following observations:

- For TLS VSTG only supports one-way authentication. VSTG provided a certificate and it was imported into Session Manager as a trusted certificate. See **Section 6.7** for details.
- Vocera performs SIP Options to SIP user agent (end-point) and not the SIP proxy server. When the UA wouldn't respond, or was incapable of responding, Vocera would mark the SIP Trunk out-of-service. SIP Options can be disabled. A workaround/fix is included in **Section 7.3**.

## 2.3. Support

Technical support on the Vocera Communications solution can be obtained by contacting Vocera Communications:

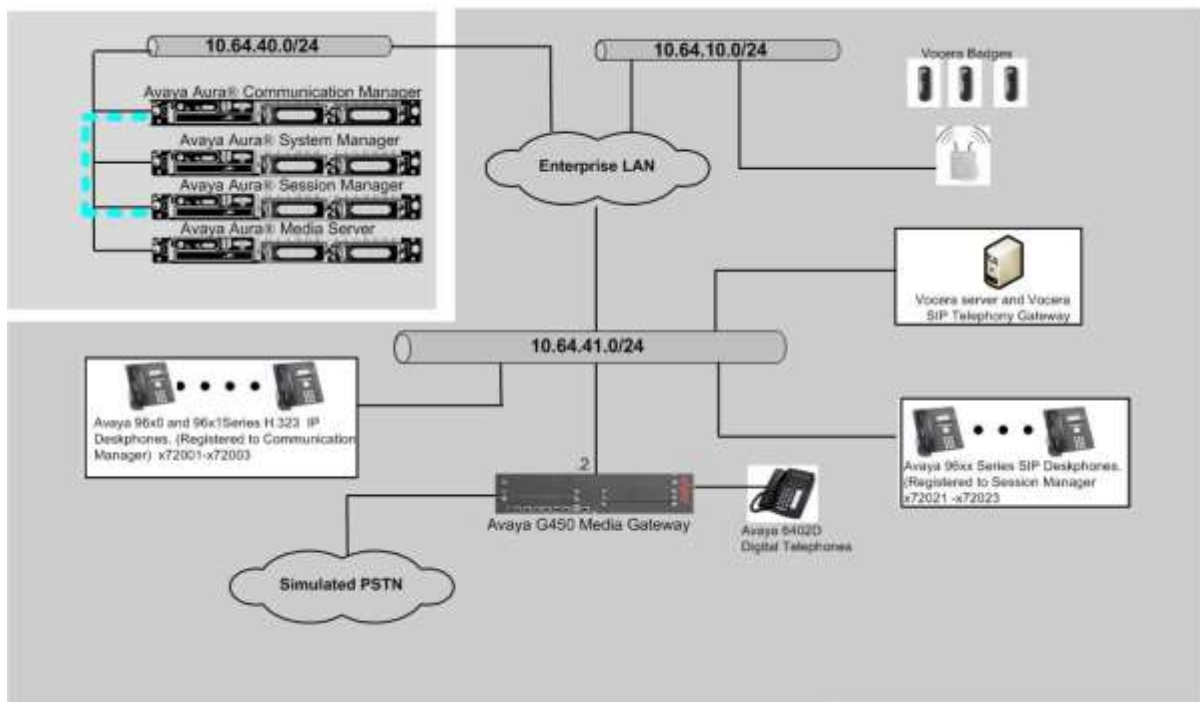
- URL – [www.vocera.com/index.php/support](http://www.vocera.com/index.php/support)
- Phone – (800) 473-3971

### 3. Reference Configuration

**Figure 1** illustrates a sample configuration consisting of the following.

- Avaya Aura® Communication Manager in a Virtual Environment
- Avaya G450 Media Gateway
- Avaya Aura® Media Server in a Virtual Environment
- Avaya Aura® System Manager in a Virtual Environment
- Avaya Aura® Session Manager in a Virtual Environment
- Avaya SIP and H.323 phones, and PSTN
- Vocera Server
- Vocera SIP Telephony Gateway
- Vocera Badges

The enterprise also had connectivity to a simulated PSTN via Communication Manager.



**Figure 1: Vocera Communications Test Configuration**

## 4. Equipment and Software Validated

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

Equipment/Software		Release/Version
Avaya Aura® Communication Manager in a		7.0.1(R017x.00.0.441.0 – 23012) –FP1
Avaya G450 Media Gateway		37.19
Avaya Aura® Media Server		7.7.0.226
Avaya Aura® System Manager		7.0.1.0.64859
Avaya Aura® Session Manager		7.0
Avaya 96x1 Series SIP Deskphones		
	9641 (SIP)	7.0.0.39
	9611(SIP)	7.0.0.39
Avaya 96xx Series Deskphones		
	9621G (H.323)	6.6.115
	9650C (H.323)	3.25
Vocera Communications		
• Vocera Server & Telephony Server OS		Windows 2012 R2
• Vocera Server		5.2.0.266
• Vocera SIP Telephony Gateway		5.2.0.266
• Vocera Badges		B3000N 4.1.0.55

## 5. Configure Avaya Aura® Communication Manager

Since the solution is a SIP trunk between Session Manager and Vocera SIP Telephony Gateway, these Application Notes are only focused on configuring Session Manager and Vocera SIP Telephony Gateway.

An assumption is made that configuration of Communication Manager and the trunk between Communication Manager and Session Manager are already in place.

For configuring the following in Communication Manager, please refer [3].

- Verify Communication Manager License
- IP Codec Set
- IP Network Region
- IP Node Names
- SIP Signaling Group
- SIP Trunk Group
- Route Pattern
- Private Numbering
- AAR Analysis
- ARS Analysis

## 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface.

The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

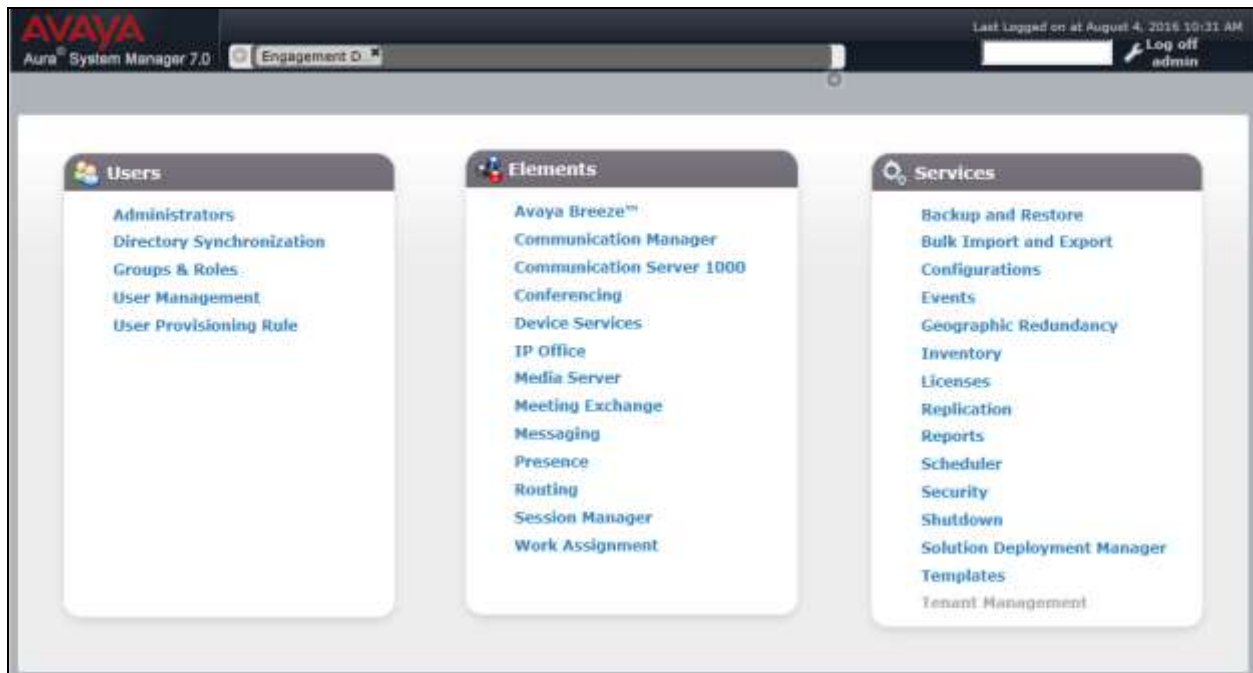
The procedures described in this section include configurations for the following:

- **SIP Domains** - SIP Domains are the domains for which Session Manager is authoritative in routing SIP calls. In other words, for calls to such domains, Session Manager applies Network Routing Policies to route those calls to SIP Entities. For calls to other domains, Session Manager routes those calls to another SIP proxy (either a pre-defined default SIP proxy or one discovered through DNS)
- **Locations** – Logical/physical areas that may be occupied by SIP Entities
- **SIP Entities** – Typically SIP Entities represent SIP network elements such as Session Manager instances, Communication Manager Systems, Session Border Controllers, SIP gateways, SIP trunks, and other SIP network devices
- **Entity Links** – Connection information which define the SIP trunk parameters used by Session Manager when routing calls to/from other SIP Entities, (e.g., ports, protocol (UDP/TCP), and trust relationship))
- **Routing Policies** - Policies that determine which control call routing between the SIP Entities based on applicable Dial Patterns
- **Dial Patterns** – Matching digit patterns which govern to which SIP Entity a call is routed



Session Manager is managed via System Manager. Using a web browser, access <https://ip-address of System Manager/SMGR>

Log in using appropriate credentials. The main page for the administrative interface is shown below.

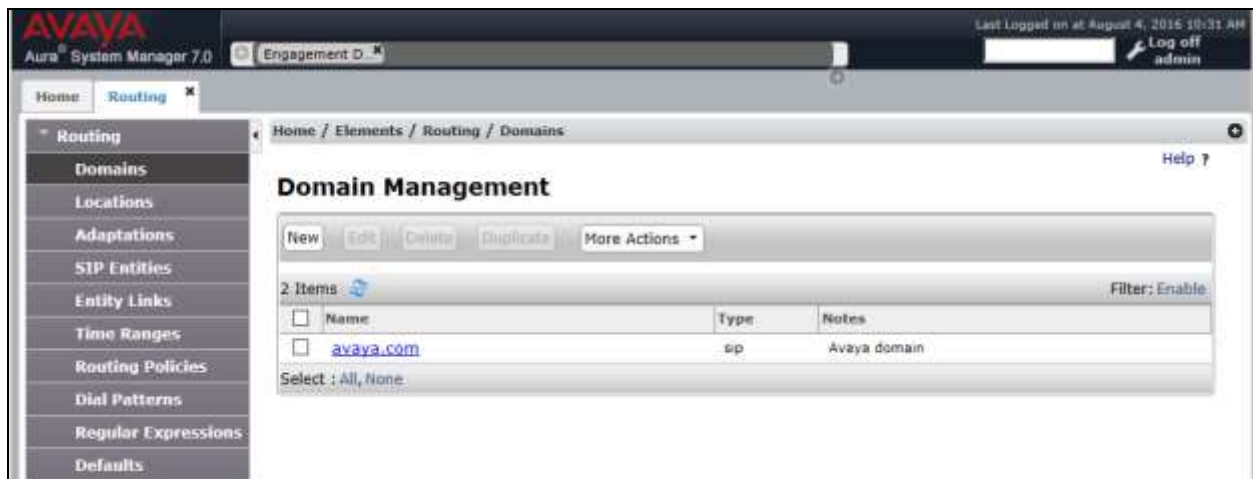


## 6.1. SIP Domains

In the reference configuration, one SIP domain was used; **avaya.com**.

Navigate to **Elements → Routing → Domains** and click the **New** (not shown) to add a new SIP domain with the following:

- Enter the SIP Domain (**avaya.com**) in the **Name** field
- **Type : sip**
- Enter a description in the **Notes** field if desired
- Click on the **Commit** button



## 6.2. Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, by specifying the IP addressing for the locations as well as for purposes of bandwidth management if required.

Navigate to **Routing → Locations** and click the **New** button (not shown) to add the Location. Enter the following information:

### Section **General**

- Enter a descriptive Location name in the **Name** field (e.g., **41-subnets**)
- Enter a description in the **Notes** field if desired

### Section **Location Pattern** (not shown)

- Click on **Add**.
- Enter the IP address information for the Location (e.g., **10.64.41.\***)
- Enter a description in the **Notes** field if desired
- Repeat 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

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The top navigation bar includes the Avaya logo, the product name 'Aura System Manager 7.0', and a user session bar showing 'Engagement D...', the last login time 'Last Logged on at August 6, 2016 11:09 AM', and a 'Log off admin' button. The left sidebar contains a list of navigation links: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Location Details' and features a 'General' section with a 'Name' field containing '41-subnet' and an empty 'Notes' field. Below this is the 'Dial Plan Transparency in Survivable Mode' section, which includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field. The interface also includes 'Commit' and 'Cancel' buttons in the top right corner of the form area.

## 6.3. SIP Entities

A SIP Entity must be added for Session Manager and for each SIP-based telephony system supported by it using SIP trunks. In the sample configuration, a SIP Entity is added for Vocera SIP Telephony Gateway (VSTG).

Note, the Session Manager and Communication Manager SIP Entities are assumed to have already been configured. This section only discusses configuring Vocera SIP Entity.

To add a SIP Entity, navigate to **Routing → SIP Entities** and click the **New** button (not shown). The configuration details for the SIP Entity defined for the Communication Manager are below:

### Section General

- **Name:** Enter an descriptive name
- **FQDN or IP Address:** Enter the IP address of the SIP Entity (e.g., **10.64.41.189**)
- **Type:** Select best match for the SIP entity (e.g., **Gateway**)
- **Location:** Select the appropriate location (Configured in **Section 6.2**) from the drop down menu (e.g., **41- subnets**)

### Section SIP Link Monitoring

- Select a desired option

The screenshot displays the Avaya Aura System Manager 7.0 interface. The top navigation bar includes the Avaya logo, the text 'Aura System Manager 7.0', and a user profile section showing 'Engagement D.' and 'Last Logged on at August 4, 2016 10:31 AM'. The main content area is titled 'SIP Entity Details' and features a 'General' tab. The configuration fields are as follows:

- Name:** Vocera
- FQDN or IP Address:** 10.64.41.189
- Type:** Gateway
- Notes:** Vocera Gateway
- Adaptation:** (empty dropdown)
- Location:** 41-subnet
- Time Zone:** America/Denver
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Securable:** ☐
- Call Detail Recording:** none
- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200
- SIP Link Monitoring:** Use Session Manager Configuration

The left sidebar contains a tree view with the following items: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The top right corner of the main area has 'Commit' and 'Cancel' buttons, and a 'Help ?' link.

## 6.4. Add Entity Link

A SIP trunk between Session Manager and Vocera system is described by an Entity link.

Navigate to **Routing → Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager with Vocera with UDP as the transport protocol.

- **Name:** a descriptive name
- **SIP Entity 1:** select the Session Manager SIP Entity
- **Protocol:** select TLS as the transport protocol
- **Port: 5061.** This is the port number to which the other system sends SIP requests
- **SIP Entity 2:** select the Vocera SIP Entity
- **Port: 5061.** This is the port number on which the other system receives SIP requests
- **Connection Policy:** select *Trusted*
- **Notes:** optional descriptive text

Click **Commit** to save the configuration.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left sidebar contains a navigation menu with options: Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (selected), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and shows a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The item in the table is 'SM70Vocera\_TLS', 'SM7.x-1', 'TLS', '5061', 'vocera', '5061', and 'trusted'. There are 'Commit' and 'Cancel' buttons at the top right and bottom right of the table.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
SM70Vocera_TLS	SM7.x-1	TLS	5061	vocera		5061	trusted

## 6.5. Routing Policies

Routing Policies associate destination SIP Entities (**Section 6.3**) and Dial Patterns (**Section 6.6**). In the reference configuration, Routing Policies are defined for outbound calls to Vocera

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

### Section General

- **Name:** Enter an descriptive name
- **Notes:** Add a brief description (optional)

### Section SIP Entity as Destination

- Click **Select**, and then select the appropriate SIP Entity to which this routing policy applies. In this case, Vocera SIP Entity was selected.

**AVAYA**  
Aura® System Manager 7.0

Home / Elements / Routing / Routing Policies

### Routing Policy Details

Commit Cancel

**General**

\* Name: Route2Vocera

Disabled: ☐

\* Retries: 0

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
vocera	10.84.41.108	Gateway	Vocera Gateway

**Time of Day**

Add Remove View Gaps/Overlaps

1 Item

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
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	

Select: All, None

**Dial Patterns**

Add Remove

1 Item

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
7778	4	4	<input type="checkbox"/>	-ALL-	-ALL-	

Select: All, None

## 6.6. Dial Patterns

Session Manager uses dial patterns to route calls to the appropriate SIP Entity. A dial pattern specifies which routing policy or routing policies are used to route a call based on the digits dialed by a user which match that pattern.

Navigate to **Routing → Dial Patterns**, and click the **New** button (not shown) to add a new Dial Pattern.

### Section General.

- **Pattern:** dialed number or prefix
- **Min:** minimum length of dialed number
- **Max:** maximum length of dialed number
- **SIP Domain:** select the SIP Domain created in **Section 6.1** (or select – ALL – to be less restrictive)
- **Notes:** optional descriptive text

### Section Originating Locations and Routing Policies.

Click **Add** to select the appropriate originating Location and Routing Policy from the list (not shown). Default settings can be used for the remaining fields. Click **Commit** to save the configuration.

The following is the dial pattern used to route calls that match the pattern x7778 to Vocera.

**Avaya Aura System Manager 7.0** Environment: D

Home / Elements / Routing / Dial Patterns

### Dial Pattern Details

Commit Cancel

General

\* Pattern: 7778

\* Min: 4

\* Max: 4

Emergency Call: ☐

Emergency Priority: 3

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/> -ALL-	Route2Vocera	0	<input type="checkbox"/>	vocera		

Select: All, None

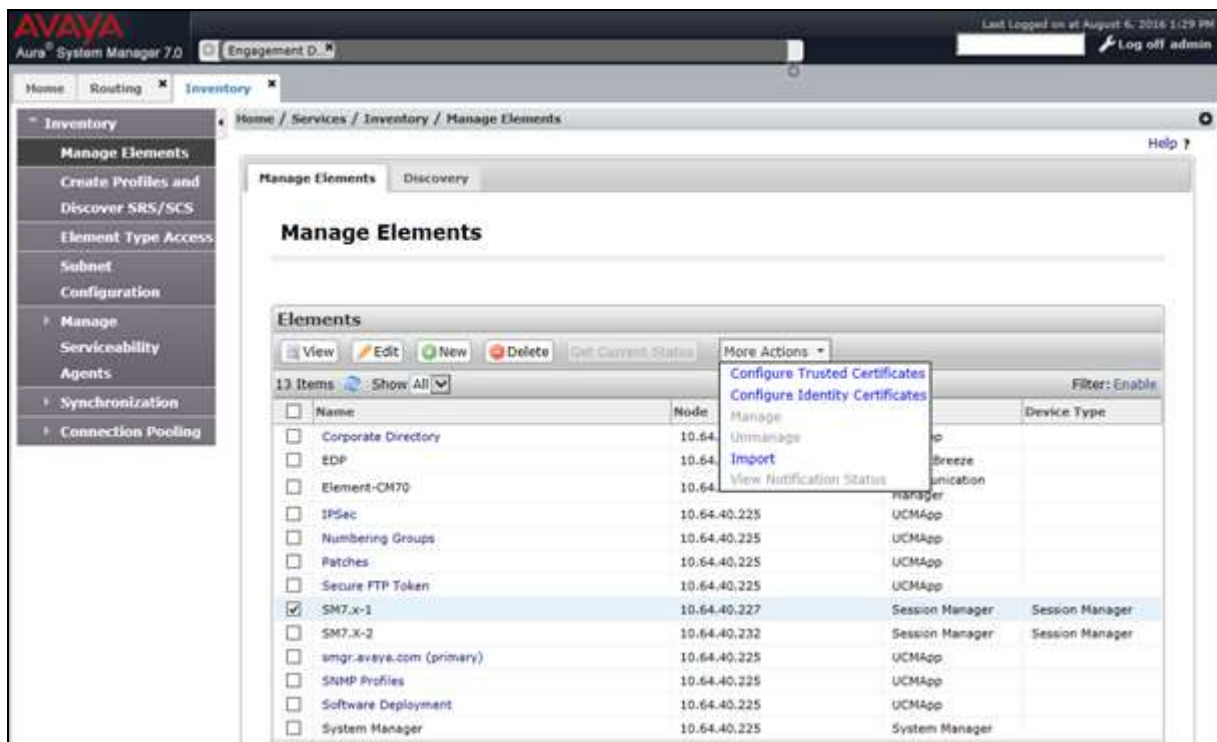
## 6.7. Manage Certificate

In order for Session Manager and the Vocera SIP Telephony Gateway (VSTG) to successfully negotiate a TLS connection, certificates are exchanged and authenticated during the TLS handshake. For two-way authentication both the Session Manager and VSTG would need to import each other's certificate. During this compliance test, only one-way authentication was performed with Session Manager importing VSTG's certificate. If it were two-way authentication steps for exporting Avaya's certificate and importing it into the VSTG would have been displayed below.

Trusted certificated file provided by VSTG imported to Session Manager.

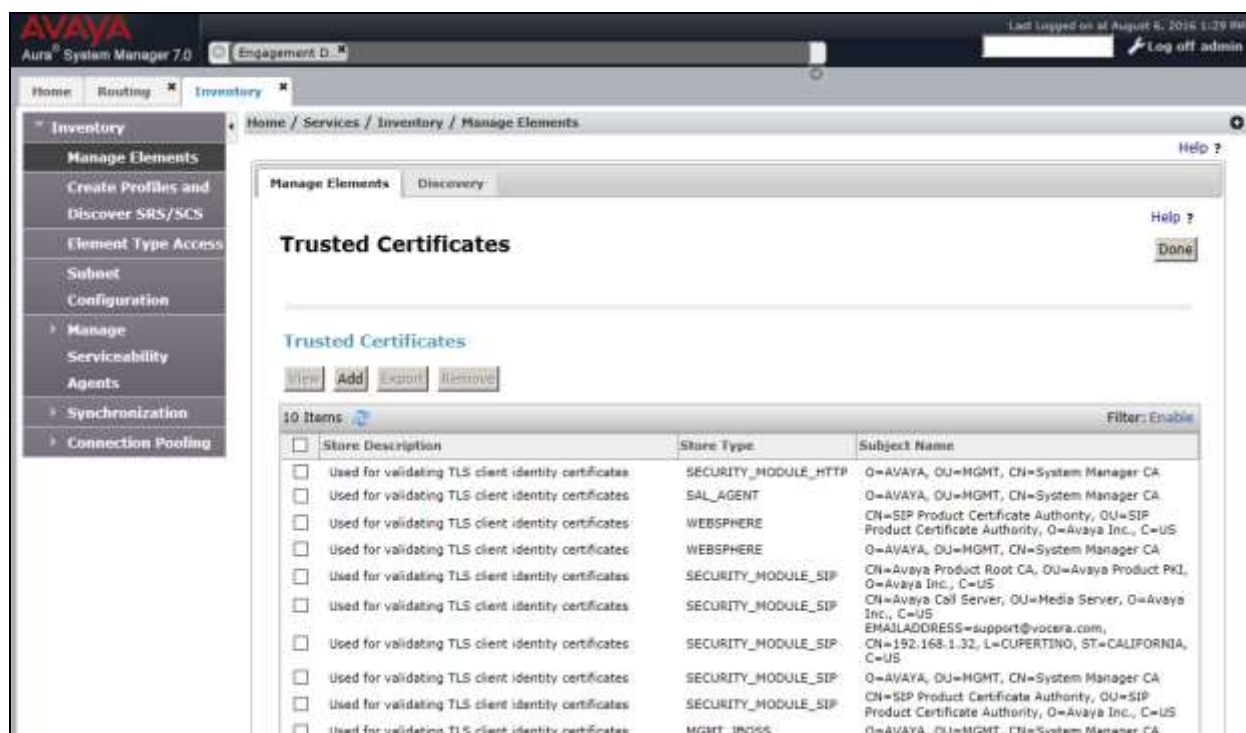
Navigate to **Home → Services → Inventory → Managed Elements**.

Select **Session Manager** (e.g., SM7.x-1), and select the **Configure Trusted Certificate** button under the **More Actions** drop-down menu.

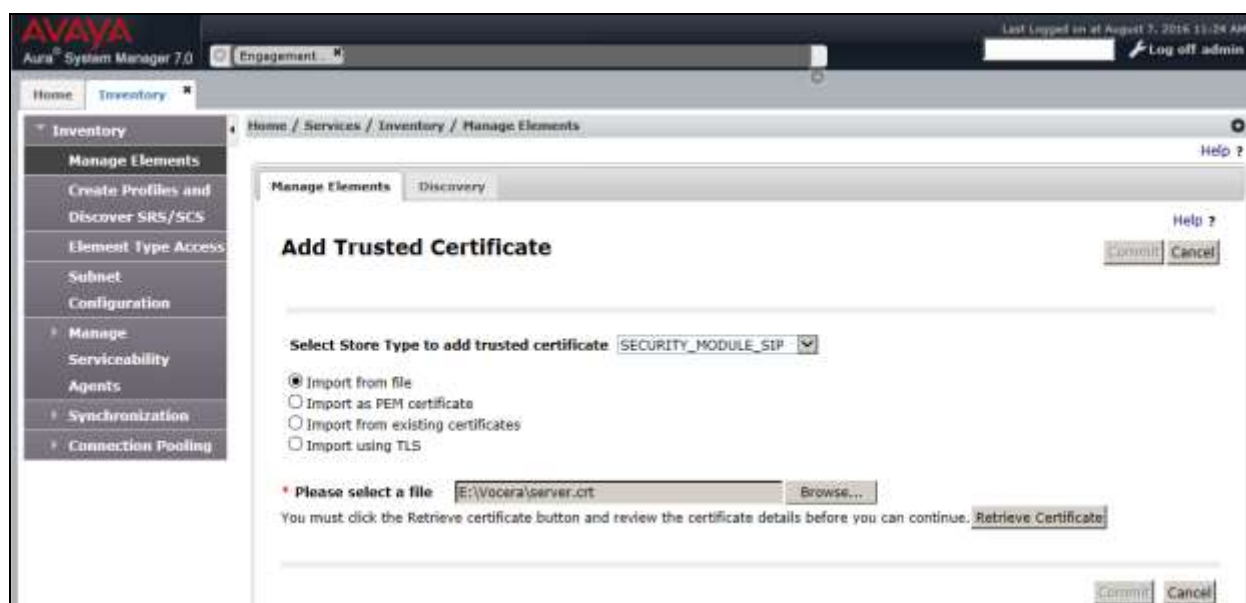




The **Trusted Certificates** screen will appear, as shown below. Click the **Add** button.



The **Add Trusted Certificate** screen will appear, as shown below. Select **SECURITY\_MODULE\_SIP** from the **Select Store Type to add trusted certificate** drop-down menu, and select the **Import from file** radio button. Use the **Browse** button to locate the file provided by Vocera. Click the **Retrieve Certificate** button. Verify certificate information and then click the **Commit** button to store the certificate.



The following screen shows details of the Trusted Certificate.

AVAYA  
Aura System Manager 7.0

Engagement

Last Logged on: 11 August 7, 2016 11:24 AM  
Log off admin

Home Inventory

Home / Services / Inventory / Manage Elements

Help ?

Manage Elements Discovery

Help ?

**Add Trusted Certificate**

Commit Cancel

Select Store Type to add trusted certificate: SECURITY\_MODULE\_SIP

☒ Import from file  
☐ Import as PEM certificate  
☐ Import from existing certificates  
☐ Import using TLS

\* Please select a file:  Browse...

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

**Certificate Details**

Subject Details	EMAILADDRESS=support@vocera.com, CN=192	
Valid From	Wed Jun 22 10:32:11 MDT 2016	Valid To
Key Size	1024	Mon Jun 21 10:32:11 MDT 2021
Issuer Name	EMAILADDRESS=support@vocera.com, CN=192	
Certificate Fingerprint	cd429cae40dd9d0d9fbd6020e6c404a50963a685	
CA Certificate	No	

Commit Cancel

## 7. Configure Vocera Communications

This section will only describe the basic configuration to interface with Avaya Aura® Session Manager. For configuration steps for Vocera Communications System, refer to (4 - 6) documentation.

The Vocera Communications System is configured using a web based console interface. Launch a web browser, enter <http://<IP address of Vocera Server>/console/AdminController> in the URL, and log in with the appropriate credentials.



## 7.1. Configure Telephony

This section shows the basic configuration needed to place calls to and from the badges. Once at the Administrator page, navigate to the **Telephony** → **Basic Info** tab and provide the following information:

- Check the Enable Telephony Integration check box
- Enter the Guest Access and Direct Access numbers. During the preparation phase of the compliance test, the following extensions were provided:
  - **Guest Access Number** –7778
  - **Direct Access Number** – 7779
  - **Number of Lines** – 6
- Select **Integration Type** to **IP**
- Using the drop-down menu, select **SIP Version 2.0** for the **Signaling Protocol** field under the **IP Settings** section
- Enter Avaya Aura® Session Manager IP address, **10.64.40.226**, for the **Call Signaling Address** field under the **SIP Settings** section.
- Enter the Call Party extension Number. During the compliance test, Calling Party Number, **408-555-1212**, was utilized
- Click on the **Save Changes** button

The screenshot shows the Vocera Administrator web interface for configuring telephony. The browser address bar shows the URL <http://10.64.41.188/cnoolce/AdminControllerFormAction?telephone>. The page title is "Vocera Administrator | Tele...". The left sidebar contains a navigation menu with items: Status Monitor, Sites, Users, Groups, Departments, System, Defaults, Active Directory, Locations, Email, **Telephony**, Reports, Maintenance, Address Book, Devices, and Documentation. The main content area is titled "Telephony" and has several tabs: Basic Info, Access Codes, Toll Info, DID Info, PIN, Dynamic Extensions, and Sharing. The "Basic Info" tab is selected. At the top right of the main area is a "Log Out" button. Below the tabs, there is a "Select Site" dropdown menu set to "Global". The "Enable Telephony Integration" checkbox is checked. Under "Vocera Hunt Group Numbers", the "Guest Access" field contains "7778" and the "Direct Access" field contains "7779". To the right, the "Number of Lines" field contains "6". The "Integration Type" section has two radio buttons: "Analog" and "IP", with "IP" selected. A note below states: "Note: Saving any changes to digital parameters will cause the telephony server to restart." The "IP Settings" section has a "Signaling Protocol" dropdown menu set to "SIP Version 2.0". The "SIP Settings" section has a "Call Signaling Address" field containing "10.64.40.226" and a "Calling Party Number" field containing "408-555-1212". There is an "Enable Call Trace" button. At the bottom of the page are "Save Changes" and "Reset" buttons. The footer text reads "Vocera Server 5.2 GA (Build 266) Console (Build 369)".

## 7.2. User Configuration

To configure a user navigate to **Users** → **User** tab. Click the **Add New User** button. Configure the following under **Info** tab:

- First Name
- Last Name
- User ID

Click the **Save** button.

Once the user is added, the user is able to login to any badge via voice command. Click the call button on the badge and the Genie will ask “Please say or spell your first and last name”. Speaking “User One” will log the user in.

**Add New User**

Info Phone Speech Rec Groups Depts ?

First Name \*  Last Name \*

User ID \*  Employee ID

Password  Re-enter Password

Email Address  Site

Cost Center  Badge ID

☐ 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.

To configure the extension associated with the user, select the **Phone** tab and enter in extension number. (e.g., 2527) Then click the **Save** button.

The screenshot shows the 'Add New User' form with the 'Phone' tab selected. The form contains several input fields for phone-related information. The 'Desk Phone or Extension' field is populated with '2527'. Other fields like 'Cell Phone', 'Home Phone', 'Vocera Extension', 'PIN for Long Distance Calls', 'Cisco EM Extension', 'Cell Phone', 'Pager', 'Dynamic Extension', and 'Cisco EM Auto-Answer' are empty. There is a 'Vocera Access Anywhere' section with a checkbox 'Enable Vocera Access Anywhere' which is unchecked, and two password fields 'Phone Password (minimum 5 chars.)' and 'Re-enter Phone Password' which are also empty. A note at the bottom of this section states: 'Note: Phone password not required if caller ID permission is used.' At the bottom of the form are three buttons: 'Save', 'Save & Continue', and 'Cancel'.

Add New User	
Info	Phone
Speech Rec	Groups
Depts	
Desk Phone or Extension	Cell Phone
2527	
Home Phone	Pager
Vocera Extension	Dynamic Extension
PIN for Long Distance Calls	
Cisco EM Extension	Cisco EM Auto-Answer
<b>Vocera Access Anywhere</b>	
<input type="checkbox"/> Enable Vocera Access Anywhere	
Phone Password (minimum 5 chars.)	Re-enter Phone Password
<b>Note:</b> Phone password not required if caller ID permission is used.	
Save	Save & Continue
Cancel	

### 7.3. Configure SIP OPTIONS

On the server running Vocera SIP Telephony Gateway, modify the *C:\vocera\telephony\vgw\vgwproperties.txt* file with the following for Option Keep Alive.

- VTGUseOPTIONSForKeepAlive = true
- VTGOPTIONSKeepAliveInterval = 30
- VTGOPTIONSKeepAliveToUser =
- VTGUseOPTIONSKeepAliveText = false

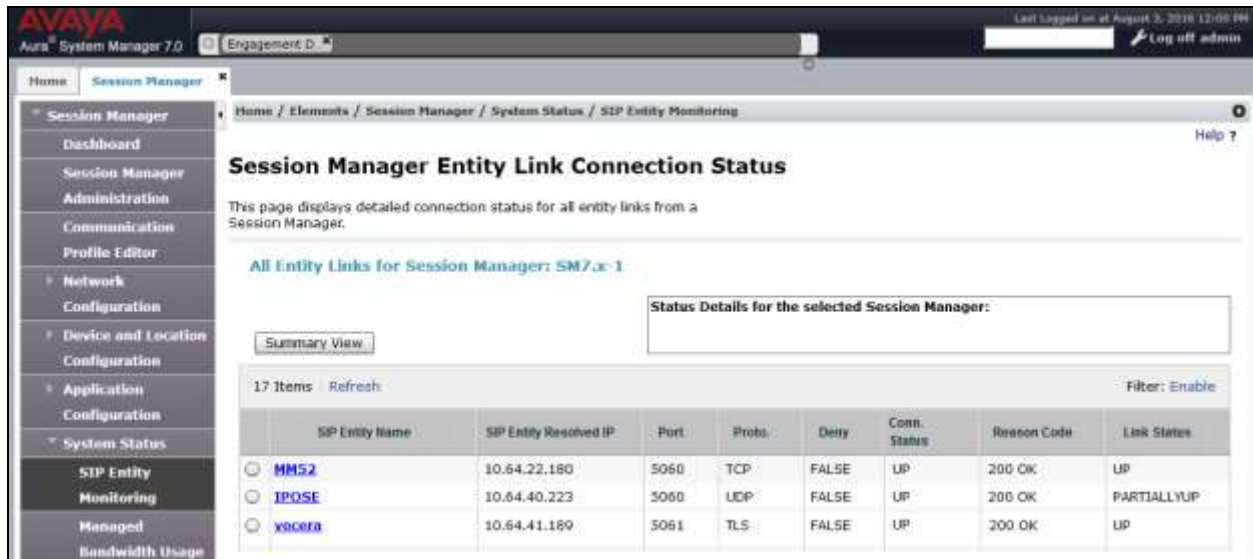


## 8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Session Manager and Vocera.

### 8.1. Verify Avaya Aura® Session Manager

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring**, and select the Vocera SIP Entity. Verify the **Conn. Status** and **Link Status** are **UP**.



**Session Manager Entity Link Connection Status**

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: SM7.x-1

Summary View

Status Details for the selected Session Manager:

17 Items Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	MM52	10.64.22.180	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	IPOSE	10.64.40.223	5060	UDP	FALSE	UP	200 OK	PARTIALLYUP
<input type="radio"/>	vocera	10.64.41.189	5061	TLS	FALSE	UP	200 OK	UP



## 8.2. Verify Vocera Communications

Make the following calls and verify the calls are set up properly, there is two-way audio with good audio quality, and the calls are torn down properly after completing the calls.

- Place a call from a Vocera Badge to another Vocera Badge
- Place a call from a Vocera Badge to an enterprise Avaya phone
- Place a call from an enterprise Avaya phone to a Vocera Badge.
- Place a call from a Vocera Badge to the PSTN

On the Vocera SIP Telephony Gateway, locate the most recent log file in **x:\vocera\logs** and look for following:

- **“listening on Address [x.x.x.x:x] – TLS;”**- This indicates a successful TLS connection between Session Manager and VSTG.
- **“SIP Trunk [x.x.x.x:x] is alive;”**- This indicates successful SIP connectivity between Session Manager and VSTG.

## 9. Conclusion

These Application Notes describe a sample configuration of how to configure Vocera Communications to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager via a SIP trunk using TLS as the transport protocol. All feature and serviceability test cases were completed and passed with the exceptions/observations noted in **Section 2.2**.

## 10. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>

- (1) *Administering Avaya Aura® Communication Manager Release 7.0.1, Issue 2, May 2016, Document Number 03-300509.*
- (2) *Administering Avaya Aura® System Manager for Release 7.0.1, Issue 2, Release 7.0.1, June 2016.*

The following document was provided by Vocera.

- (3) *Vocera Telephony Configuration Guide, Version 5.2*
- (4) *Vocera B3000 Badge Guide, Version 5.2*
- (5) *Vocera Administration Guide Version 5.2*

---

**©2016 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).