



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Vocera Communications System 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 and Avaya Aura® Communication Manager.

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.

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 steps to configure Avaya SIP trunk solution with Vocera Communications System. 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 802.11b/g 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 B2000 and B3000 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 and Digital.

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:

- Avaya Certificate for TLS was not imported into the VSTG. Resulting in one-way authentication.
- Vocera is using RFC 5373 for Answer-Mode. When the supported feature is sent in the invite with answer-mode type Manual, Avaya 96x0 and 96x1 IP Phones configured as SIP, would auto-answer. The issue had been identified with Avaya endpoints and an enhancement request had been submitted during previous test cycle; there is no update.
- There is an empty TCP PUSH packet is sent to Session Manager by VSTG. This does not have any impact on functionality. However, the packet is reported as **ERROR** on traceSM tool that is run on Session Manager. Vocera is aware of this and is investigating the cause.

2.3. Support

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

- URL – 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 with Avaya G450 Media Gateway
- Avaya Aura® Session Manager (configured using Avaya Aura® System Manager)
- Avaya SIP and non-SIP phones
- Vocera Server
- Vocera SIP Telephony Gateway
- Vocera Badges

Communication Manager also had connectivity to the PSTN via Communication Manager

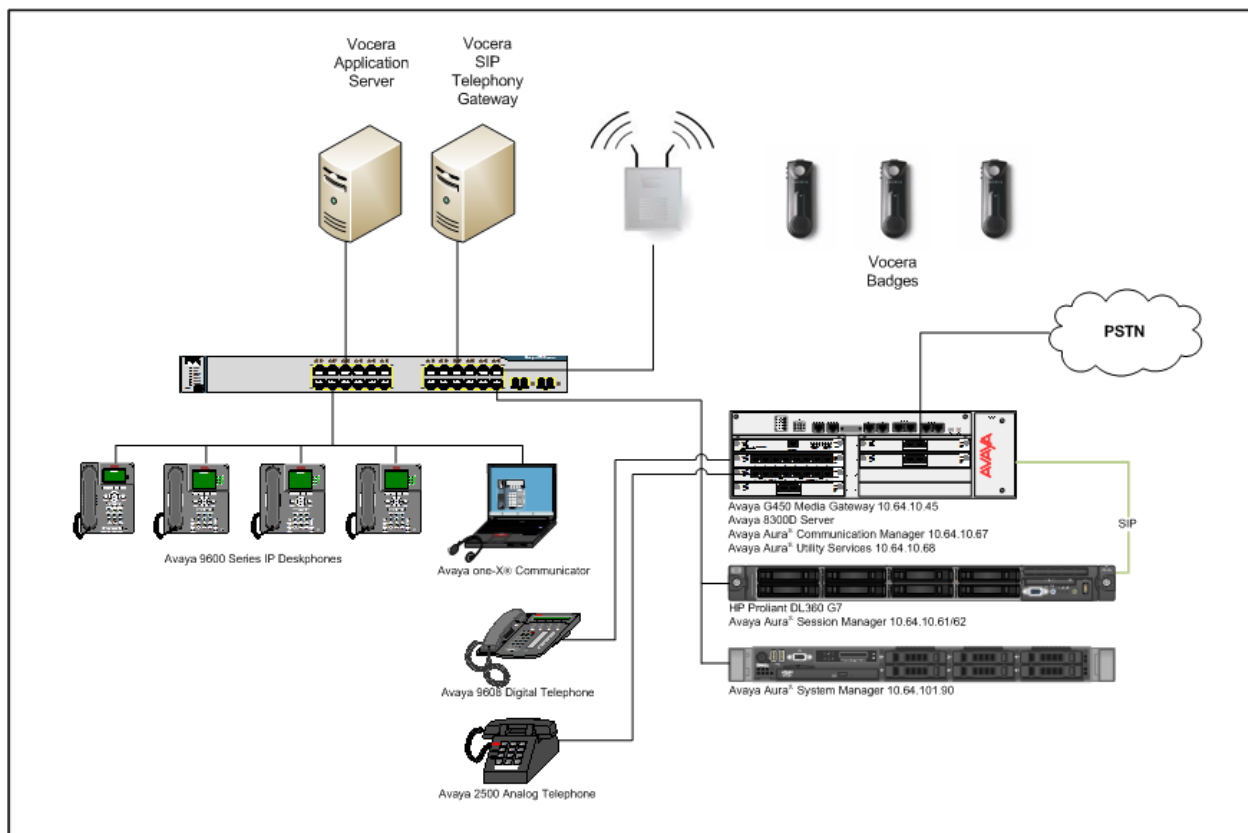


Figure 1: Vocera Communications Test Configuration

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 Running on Avaya S8300D Server	6.3 SP5
Avaya G450 Media Gateway	32.20.1
Avaya Aura® Session Manager running on HP GL360 G7	6.3 SP3
Avaya Aura® System Manager running on VMWare Virtual Appliance	6.3.5
Avaya 9600 Series IP Deskphones <ul style="list-style-type: none">• 96x0 SIP• 96x0 H.323• 96x1 SIP• 96x1 H.323	3.2.1 2.6.11 6.3.0 6.3.0
Avaya 9400 Series Digital Telephone	2.0 SP2
Avaya one-X Communicator	6.2
Avaya 2500 Analog Telephone	-
Vocera Communications <ul style="list-style-type: none">• Vocera Server• Vocera SIP Telephony Gateway• Vocera Badges<ul style="list-style-type: none">○ B2000○ B3000	4.4 build 171 4.4 build 171 536 172

5. Configure Avaya Aura® Communication Manager

This section provides the procedures for configuring Communication Manager. The procedures include the following areas:

- 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

5.1. Verify Avaya Aura® Communication Manager License

Use the **display system-parameters customer-options** command and on **Page 2**, verify that the **Maximum Administered SIP Trunks** value is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that **4000** licenses are available and **30** are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES	USED	
Maximum Administered H.323 Trunks:	4000	36
Maximum Concurrently Registered IP Stations:	2400	2
Maximum Administered Remote Office Trunks:	4000	0
Maximum Concurrently Registered Remote Office Stations:	2400	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	100	0
Maximum Video Capable Stations:	2400	0
Maximum Video Capable IP Softphones:	2400	0
Maximum Administered SIP Trunks:	4000	30
Maximum Administered Ad-hoc Video Conferencing Ports:	4000	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0
Maximum TN2501 VAL Boards:	10	0
Maximum Media Gateway VAL Sources:	50	0
Maximum TN2602 Boards with 80 VoIP Channels:	128	0
Maximum TN2602 Boards with 320 VoIP Channels:	128	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. IP Codec Set

This section describes the steps for administering an IP codec set in Communication Manager. This IP codec set is used in the IP network region for communications between Communication Manager and Session Manager. Use the **change ip-codec-set *n* command**, where *n* is a number between **1** and **7**, inclusive. IP codec sets are used in [Section 5.3](#) for configuring IP network regions to specify which codec sets may be used within and between network regions. During compliance testing ip-codec-set 1 was used.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size (ms)			
1: G.711MU	n	2	20			
2: G.711A	n	2	20			
3:						
4:						
5:						
6:						
7:						

5.3. IP Network Region

This section describes the steps for administering an IP network region in Communication Manager for communication between Communication Manager and Session Manager. Use the **change ip-network-region *n*** command, where *n* is a number between **1** and **250** inclusive, and configure the following:

- **Authoritative Domain** - Enter the appropriate name for the Authoritative Domain.
- During the compliance test, the authoritative domain is set to **avaya.com**.
- **Intra-region** and **Inter-region IP-IP Direct Audio** (media shuffling) – By default are set to **yes** if supported. This allows audio traffic to be sent directly between IP endpoints to reduce the use of media resources.
- **Codec Set** – Enter the IP codec set number as provisioned in [Section 5.2](#).

change ip-network-region 1		Page 1 of 20
IP NETWORK REGION		
Region: 1		
Location:	Authoritative Domain: avaya.com	
Name: Compliance Testing		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

5.4. IP Node Names

This section describes the steps for setting the IP node name for Session Manager in Communication Manager. Use the **change node-names ip** command, and add a node name for Session Manager signaling. The node name for Session Manager is **SM_10_62** with IP Address **10.64.10.62**.

change node-names ip		Page 1 of 2
IP NODE NAMES		
Name	IP Address	
SM_10_62	10.64.10.62	

5.5. SIP Signaling Group

This section describes the steps for administering a SIP signaling group for a new trunk that will be created for the connection between Communication Manager and Session Manager. Use the **add signaling-group <s>** command, where **s** is an available signaling group number. Enter the following values for the specified fields and the default values may be used for the remaining fields.

- **Group Type:** sip
- **IMS Enabled:** n
- **Transport Method:** tls
- **Peer Detection Enabled:** y
- **Peer Server:** SM (this field will be automatically populated)
- **Near-end Node Name:** Processor node, in this case **procr**
- **Near-end Listen Port:** 5061
- **Far-end Node Name:** Session Manager node name from [Section 5.4](#)
- **Far-end Listen Port:** 5061
- **Far-end Network Region:** The IP network region number from [Section 5.4](#)
- **DTMF over IP:** rtp-payload
- **Direct IP-IP Audio Connections:** y

```
add signaling-group 10                                     Page 1 of 1
                                     SIGNALING GROUP

Group Number: 1                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
    Q-SIP? n                               SIP Enabled LSP? n
    IP Video? n                          Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y  Peer Server: SM

Near-end Node Name: procr                Far-end Node Name: SM_10_62
Near-end Listen Port: 5061              Far-end Listen Port: 5061
                                     Far-end Network Region: 1

Far-end Domain: avaya.com

                                     Bypass If IP Threshold Exceeded? N

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

5.6. SIP Trunk Group

This section describes the steps for administering a trunk group for connectivity between Communication Manager and Session Manager. Use the **add trunk-group <t>** command, where **t** is an available trunk group number.

- **Group Type:** **sip**
- **Group Name:** Enter a descriptive name (e.g., **SM_10_62**)
- **TAC:** Set to any available trunk access code that is valid in the provisioned dial plan. (e.g., ***010**)
- **Service Type:** **tie**
- **Signaling Group:** **1** (Signaling group added in [Section 5.5](#))
- **Number of Members:** **10** (Enter a desired value for trunk group members)
- **Numbering Format:** **private**

Note: The number of members determines how many simultaneous calls can be processed by the trunk through Session Manager.

add trunk-group 10		Page 1 of 21	
TRUNK GROUP			
Group Number: 1	Group Type: sip	CDR Reports: y	
Group Name: SM_10_62	COR: 1	TN: 1	TAC: *010
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: tie	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 10	
		Number of Members: 10	

add trunk-group 10		Page 3 of 21	
TRUNK FEATURES			
ACA Assignment? n	Measured: none	Maintenance Tests? y	
Numbering Format: private		UII Treatment: service-provider	
		Replace Restricted Numbers? n	
		Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no			
Show ANSWERED BY on Display? y			

5.7. Route Pattern

Create a route pattern to use for the newly created SIP trunk group. Use the **change route-pattern <r>** command, where **r** is an available route pattern.

- **Pattern Name:** A descriptive name (e.g., **SM_10_62**)
- **Grp No:** The trunk group number from [Section 5.6](#) (e.g., **1**)
- **Set the FRL:** Enter a level that allows access to this trunk, with 0 being least restrictive.
- **Numbering Format:** **lev0-pvt**, this forces the use of Private Number format

change route-pattern 10													Page		1 of 3		
Pattern Number: 10													Pattern Name: SM_10_62				
SCCAN? n													Secure SIP? n				
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted						DCS/	IXC			
No			Mrk	Lmt	List	Del	Digits						QSIG				
													Dgts		Intw		
1:	10	0											n	user			
2:											n	user					
3:											n	user					
4:											n	user					
5:											n	user					
6:											n	user					
		BCC	VALUE	TSC	CA-TSC			ITC	BCIE	Service/Feature	PARM	No.	Numbering	LAR			
		0	1	2	M	4	W	Request				Dgts	Format				
													Subaddress				
1:	y	y	y	y	y	n	n	rest				lev0-pvt	none				
2:	y	y	y	y	y	n	n	rest					none				
3:	y	y	y	y	y	n	n	rest					none				
4:	y	y	y	y	y	n	n	rest					none				
5:	y	y	y	y	y	n	n	rest					none				
6:	v	v	v	v	v	n	n	rest					none				

5.8. Private Numbering

Use the **change private-numbering 0** command, to define the calling party number to send to Session Manager. Add an entry for the trunk group defined in [Section 5.6](#). In the example shown below, all calls originating from a 5-digit extension beginning with 2 will be routed over any trunk group, since the Trk Grp(s) field is blank, will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

change private-numbering 0										Page 1 of 2	
NUMBERING - PRIVATE FORMAT											
Ext	Ext	Trk		Private		Total					
Len	Code	Grp(s)		Prefix		Len					
5	2					5		Total Administered: 2			
5	5					5		Maximum Entries: 540			

5.9. Automatic Alternate Routing Analysis

This section provides a sample Automatic Alternate Routing (AAR) routing used for routing calls with dialed digits 500xx to Session Manager. (See [Section 6.7](#) for corresponding Session Manager configuration) Note that other methods of routing may be used. Use the **change aar analysis 5** command, and add an entry to specify how to route calls to 500xx. In the example shown below, calls with digits 500xx will be routed as an AAR call using route pattern 1 from [Section 5.7](#). These calls will be routed to Session Manager and then to the VSTG.

change aar analysis 2							Page 1 of 2	
AAR DIGIT ANALYSIS TABLE								
Location: all					Percent Full: 2			
Dialed		Total		Route	Call	Node	ANI	
String		Min	Max	Pattern	Type	Num	Reqd	
500		5	5	10	aar		n	

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. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya Aura® network, including the central administration of routing policies, and a common format for logs and alarms.

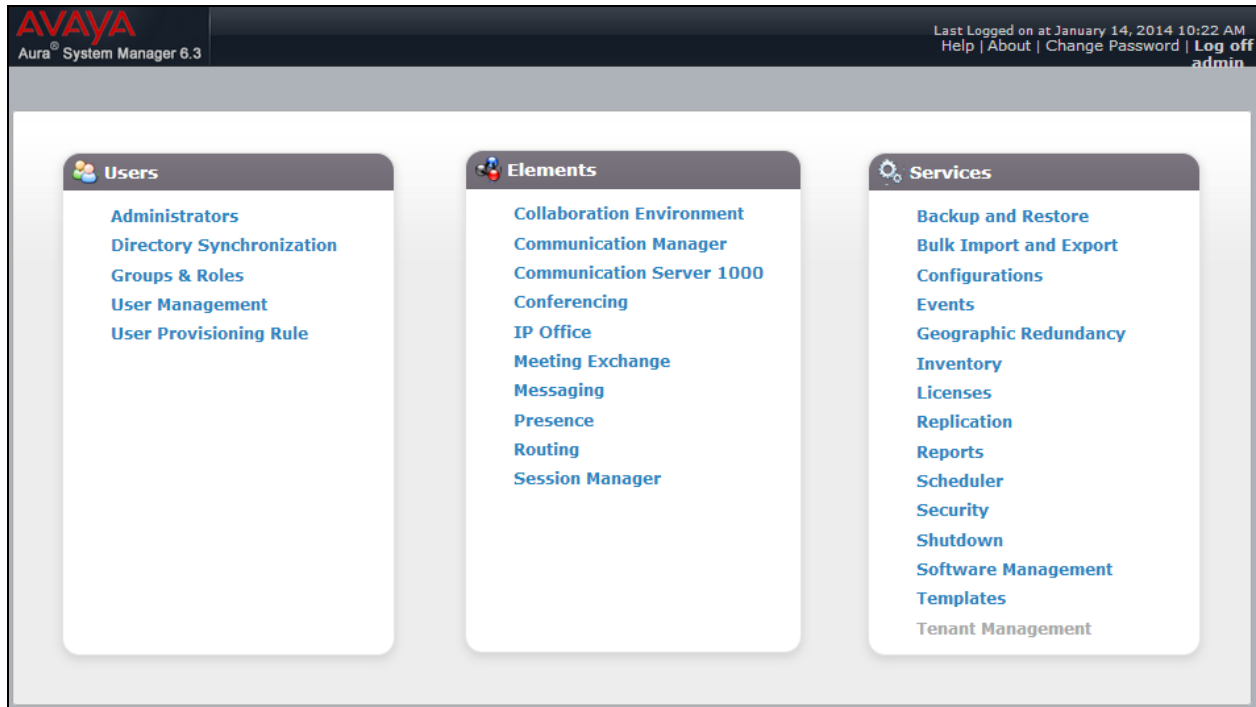
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

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/TLS), and trust relationship)
- **Time Ranges** – Specified windows during which SIP call processing is permitted for a particular Routing Policies
- **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.
- **Manage Certificate** - In order for 3rd party equipment and Session Manager to use TLS to secure communications, a certificate must be installed on the Avaya equipment, and an Avaya certificate should be installed on the 3rd party equipment.

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

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

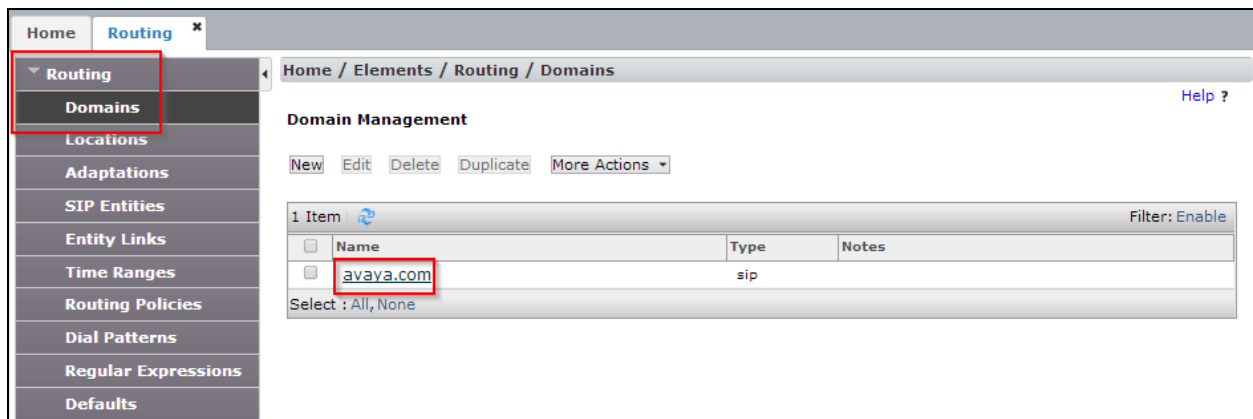


6.1. SIP Domains

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

Navigate to **Element** → **Routing** → **Domains** and click the **New** 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., **.60 & .101 subnets**).
- Enter a description in the **Notes** field if desired.

Section **Location Pattern** heading, click on **Add**

- Enter the IP address information for the Location (e.g., **10.64.60.* & 10.64.101***).
- 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.

Home / Elements / Routing / Locations

Location Details Commit Cancel

General

* Name: Test Room 1

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Alarm Threshold

Overall Alarm Threshold: 80 %

Multimedia Alarm Threshold: 80 %

* Latency before Overall Alarm Trigger: 5 Minutes

* Latency before Multimedia Alarm Trigger: 5 Minutes

Location Pattern

Add Remove

2 Items Filter: Enable

IP Address Pattern	Notes
* 10.64.10.*	
* 10.64.101.*	

Select: All, None

Commit Cancel

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 Session Manager, Communication Manager and Vocera SIP Telephony Gateway (VSTG).


Note, the Session Manager SIP Entity is assumed to have already been configured. Navigate to **Routing** → **SIP Entities**; check the checkbox for the Session Manager SIP Entity, and click the Edit button (not shown). Under the **Ports** section, verify the required Session Manager listening port for communication with VSTG is configured (e.g., **Port 5061** and **Protocol TLS**). If necessary, click the **Add** button to add the listening port and then click the **Commit** button when done to save the changes.







Port

TCP Failover port:

TLS Failover port:

Add **Remove**

3 Items  Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP 	avaya.com 	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP 	avaya.com 	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS 	avaya.com 	<input type="text"/>

Select: All, None

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., **10.64.10.242**)
- **Type**: Select best match for the SIP entity (e.g., **SIP Trunk**)
- **Location** : Select the appropriate location (Configured in [Section 6.2](#)) from the drop down menu (e.g., **.60 & .101 subnets**)

Section **SIP Link Monitoring**:

- Select desired option

Click **Commit** when done.

The following screen shows addition of the VSTG SIP Entity. Note the selection of **SIP Trunk** for **Type**.

The screenshot displays the 'SIP Entity Details' configuration page for 'Vocera SIP Trunk - TLS'. The left sidebar shows the navigation menu with 'Routing' and 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes a 'Commit' button. The 'General' section contains the following fields:

- Name**: vocera-tr1
- FQDN or IP Address**: 10.64.10.242
- Type**: SIP Trunk (selected from a dropdown)
- Notes**: Vocera SIP Trunk - TLS
- Adaptation**: (empty dropdown)
- Location**: Test Room 1 (selected from a dropdown)
- Time Zone**: America/Denver (selected from a dropdown)
- SIP Timer B/F (in seconds)**: 4
- Credential name**: (empty text field)
- Call Detail Recording**: egress (selected from a dropdown)

The 'Loop Detection' section shows 'Loop Detection Mode' set to 'Off'. The 'SIP Link Monitoring' section shows 'SIP Link Monitoring' set to 'Use Session Manager Configuration'.

6.4. Add Entity Link

A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created:

- Session Manager ↔ Communication Manger
- Session Manager ↔ VSTG

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 SIP Telephony Gateway.

- **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 VSTG SIP Entity
- **Port: 5061.** This is the port number on which the other system receives SIP requests
- **Connection Policy:** default *Trusted*
- **Notes:** optional descriptive text

Click **Commit** to save the configuration

Entity Links

Override Port & Transport with DNS ☐ SRV:

Add **Remove**

1 Item Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	asm-tr1	TLS	*5061	vocera-tr1	*5061	trusted	<input type="checkbox"/>

Select: All, None

SIP Responses to an OPTIONS Request

Add **Remove**

0 Items Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit **Cancel**

The Entity Link for connecting Session Manager with VSTG was similarly defined as shown in the screen below. Note the use of **TLS** and port **5061**. (See [Section 6.8](#) for corresponding TLS configuration)

6.5. Time Ranges

The **Time Ranges** form allows admission control criteria to be specified for **Routing Policies** ([Section 6.6](#)). In the reference configuration, no restrictions were used.

To add a **Time Range**, navigate to **Elements** → **Routing** → **Time Ranges** and click the **New** button to add a new Time Range. Enter the following information:

- **Name:** Enter an descriptive name
- **Mo** through **Su:** check the box under each of these headings
- **Start Time:** enter **00:00**.
- **End Time:** enter **23:59**.
- **Notes:** Enter a description if desired.

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

Home / Elements / Routing / Time Ranges

Time Ranges

New Edit Delete Duplicate More Actions

1 Item Filter: Enable

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
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

6.6. Routing Policies

Routing Policies associate destination SIP Entities ([Section 6.3](#)) with Time of Day admission control parameters ([Section 6.5](#)) and Dial Patterns ([Section 6.7](#)). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.
- 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

Section **Time of Day**:

- Click **Add**, and select the time range configured from [Section 6.5](#).

Defaults can be used for the remaining fields. Click **Commit** to save each **Routing Policy** definition.

The following screens show the Routing Policy for Communication Manager.

The screenshot shows the 'Routing Policy Details' page for a policy named 'cm-tr1'. The left sidebar has 'Routing' and 'Routing Policies' highlighted. The main area is divided into sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' is 'cm-tr1', 'Disabled' is unchecked, 'Retries' is 0, and 'Notes' is empty. In the 'SIP Entity as Destination' section, a table lists the destination entity 'cm-tr1' with FQDN '10.64.10.67', Type 'CM', and Notes 'Avaya Aura® Communication Manager - Test Room 1'. In the 'Time of Day' section, a table shows a single time range '24/7' with a ranking of 0, active from 00:00 to 23:59, and enabled.

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name: cm-tr1

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm-tr1	10.64.10.67	CM	Avaya Aura® Communication Manager - Test Room 1

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

The following screen shows the Routing Policy for routing calls to Vocera.

The screenshot shows the 'Routing Policy Details' page for a policy named 'vocera-tr1'. The left sidebar has 'Routing' and 'Routing Policies' highlighted. The main area is divided into sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' is 'vocera-tr1', 'Disabled' is unchecked, 'Retries' is 0, and 'Notes' is empty. In the 'SIP Entity as Destination' section, a table lists the destination entity 'vocera-tr1' with FQDN '10.64.10.242', Type 'SIP Trunk', and Notes 'Vocera SIP Trunk - TLS'. In the 'Time of Day' section, a table shows a single time range '24/7' with a ranking of 0, active from 00:00 to 23:59, and enabled.

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel Help ?

General

* Name: vocera-tr1

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
vocera-tr1	10.64.10.242	SIP Trunk	Vocera SIP Trunk - TLS

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

6.7. Dial Patterns

Session Manager uses dial pattern to route calls to appropriate SIP Entity for processing. 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**: default
- **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 an example of routing to route calls that match the pattern 2xxxx to Communication Manager.

AVAYA
Aura® System Manager 6.3

Last Logged on at March 10, 2014 11:18 AM
Help | About | Change Password | Log off admin

HomeSession Manager *Routing *

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

CommitCancel

Help ?

General

* Pattern: 25

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

AddRemove

1 Item

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		cm-tr1		<input type="checkbox"/>	cm-tr1	

Select : All, None

The following is an example of routing to route calls that match the pattern 5xxxx to Vocera.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details [Commit](#) [Cancel](#) [Help ?](#)

General

* Pattern: 500

* Min: 5

* Max: 5

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Filter: Enable](#)

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Test Room 1		vocera-tr1	0	<input type="checkbox"/>	vocera-tr1	

Select : All, None

The following is an example of routing to route calls that match the pattern 3035xxxxxx to Vocera.

AVAYA

Aura® System Manager 6.3

Last Logged on at March 10, 2014 11:18 AM

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

Home

Session Manager

Routing

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Home / Elements / Routing / Dial Patterns

Commit

Cancel

Help ?

Dial Pattern Details

General

* Pattern: 3035xxxxxx

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add

Remove

1 Item

Filter: Enable

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Test Room 1		vocera-tr1	0	<input type="checkbox"/>	vocera-tr1	

Select : All, None

6.8. 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**.

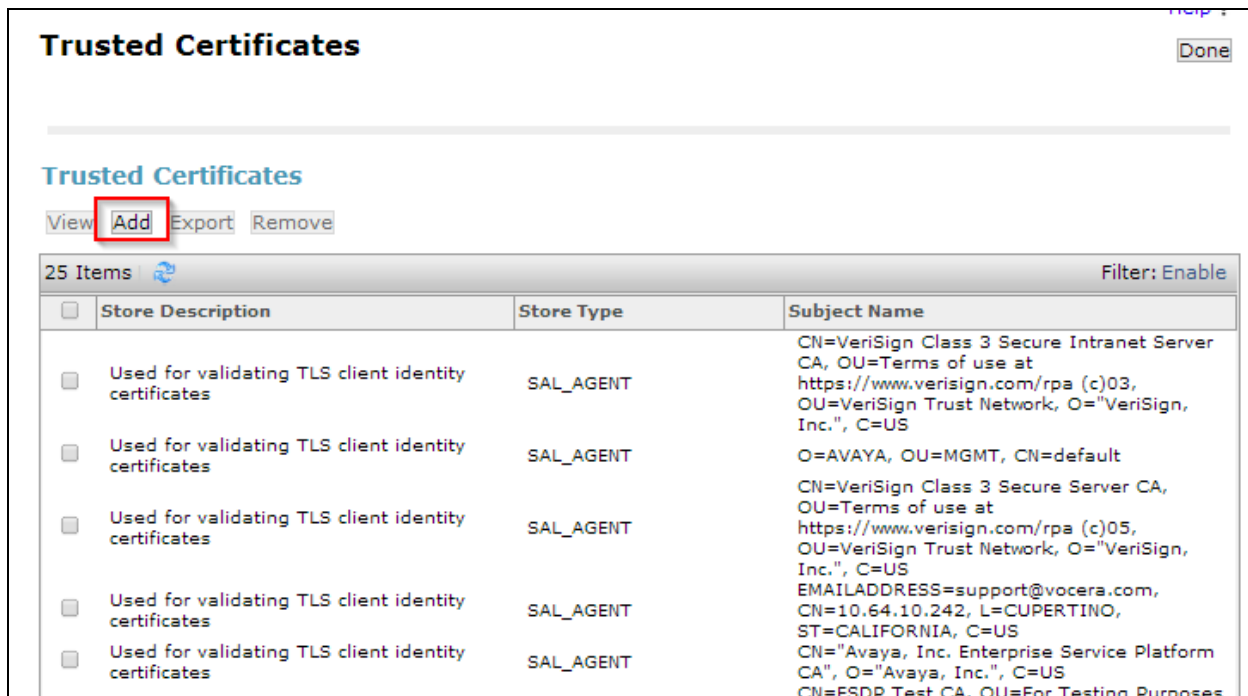
Section Entities

Select **Session Manager** (e.g., asm-tr1) → **More Actions** drop-down menu, select **Configure Trusted Certificate** button.

The screenshot displays the 'Manage Elements' interface. On the left, the 'Inventory' menu is expanded, and 'Manage Elements' is highlighted. The main content area shows a table of elements. The element 'asm-tr1' is selected, and the 'More Actions' dropdown menu is open, showing 'Configure Trusted Certificates' as the first option. Other options include 'Configure Identity Certificates', 'Manage', 'Unmanage', 'Import', and 'View Notification Status'.

Name	IP Address	Application
asm-tr1	10.64.101.90	Session Manager
cm-tr1	10.64.101.90	Communication Manager
Corporate Directory	10.64.101.90	UCMAApp
IPSec	10.64.101.90	UCMAApp
Numbering Groups	10.64.101.90	UCMAApp
Patches	10.64.101.90	UCMAApp
Secure FTP Token	10.64.101.90	UCMAApp
smgr-tr1.avaya.com (primary)	10.64.101.90	UCMAApp
SNMP Profiles	10.64.101.90	UCMAApp
Software Deployment	10.64.101.90	UCMAApp
System Manager	10.64.101.90	System Manager

The **Trusted Certificate** 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 **Choose File** 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.

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

Choose File

server.crt

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=10.64

Valid From

Tue Jan 07 16:05:51 MST 2014

Valid To

Sun Jan 06 16:05:51 MST 2019

Key Size

1024

Issuer Name

EMAILADDRESS=support@vocera.com, CN=10.64

Certificate Fingerprint

f1b126d1302349cb7df07e95166d6611a7342d85

CA Certificate

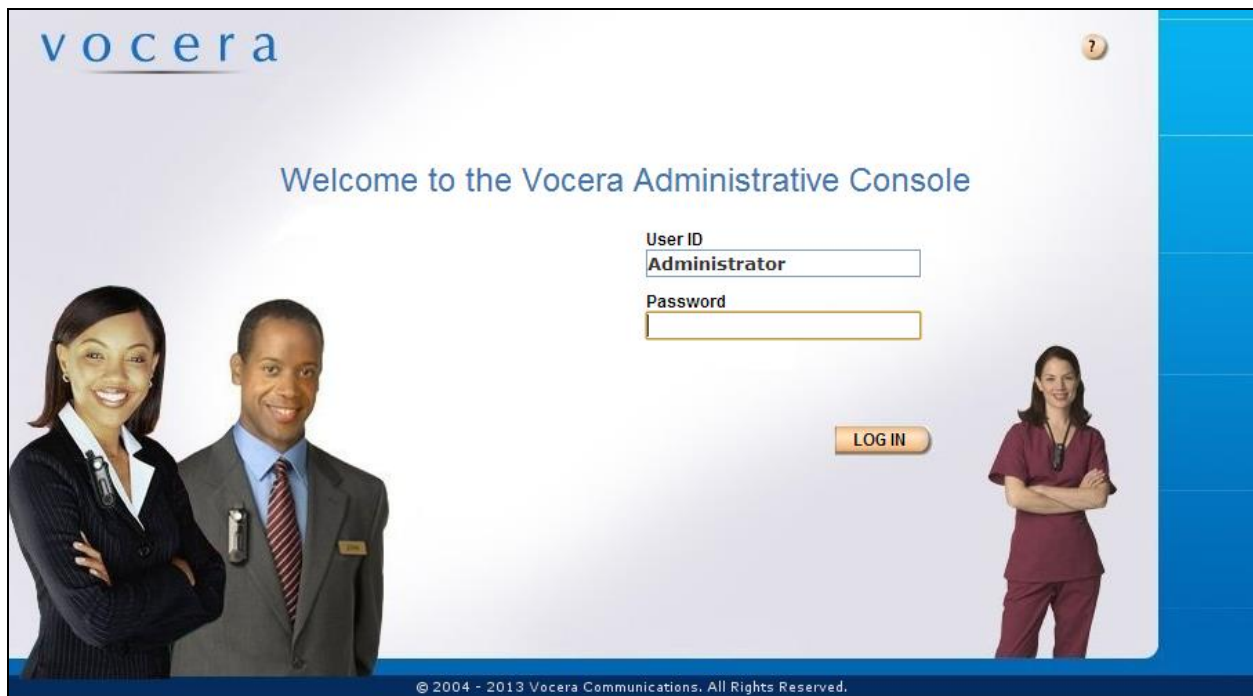
No

7. Configure Vocera Communications

This section will only describe the basic configuration to interface with Session Manager. For configuration steps for Vocera Communications System, refer to [\(3 -5\)](#) 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 will show basic configuration needed to place calls to and from the badges.

Once at the Administrator page, navigate to **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 – 5-0000
 - Direct Access Number – 5-0001
 - Number of Lines – 6
 - User extensions: 5-0003 to 5-0009
- Set the Integration Type to **IP**.
- Using the drop-down menu, select **SIP Version 2.0** for Signaling Protocol field under the IP Settings section.
- Enter Session Manager IP address for the Call Signaling Address field under the SIP Settings section. During the compliance test, IP address, **10.64.10.62**, was utilized.
- Enter the Call Party extension Number. During the compliance test, Calling Party Number, **800-555-1212**, was utilized.
- Click on the **Save Changes** button.

The screenshot shows the Vocera Administrator interface for configuring telephony. The 'Basic Info' tab is active, and the 'Enable Telephony Integration' checkbox is checked. The 'Vocera Hunt Group Numbers' section shows 'Guest Access' as 5-0000 and 'Direct Access' as 5-0001. The 'Integration Type' is set to 'IP'. The 'IP Settings' section shows 'Signaling Protocol' as 'SIP Version 2.0'. The 'SIP Settings' section shows 'Call Signaling Address' as 10.64.10.62 and 'Calling Party Number' as 800-555-1212. The 'Number of Lines*' field is set to 6. A 'Save Changes' button is located at the bottom of the form.

Select **DID Info** tab to configure Direct Inward Dialing numbers for the badges.

Select the **Add** button and enter in the DID range, and then click **Save Changes**.

The screenshot shows the Vocera Administrator interface. The top navigation bar includes the Vocera logo, 'ADMINISTRATOR' role, and a 'Log Out' button. The main header is 'Telephony'. Below it, there are tabs: 'Basic Info', 'Access Codes', 'Toll Info', 'DID Info' (highlighted with a red box), 'PIN', 'Dynamic Extensions', 'Sharing', and 'Cisco'. A 'Select Site' dropdown is set to 'Global'. The 'Direct Inward Dialing (DID)' section contains a description: 'Allocate ranges of phone numbers for use as DID numbers. When an outside caller dials a number within a specified DID range, the call goes directly to the associated badge. Otherwise, the Genie prompts the caller to say the full name of the person or group, or enter an extension.' Below this is a table with two columns: 'Prefix' and 'Range of Numbers'. The table has one row with '5' in the 'Prefix' column and '0003 To 0009' in the 'Range of Numbers' column. To the right of the table are three buttons: 'Add' (highlighted with a red box), 'Edit', and 'Delete'. At the bottom of the page, there are 'Save Changes' (highlighted with a red box) and 'Reset' buttons. The footer text reads 'Vocera Server 4.4 [Build 171] Console [Build 171]'.

Prefix	Range of Numbers
5	0003 To 0009

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 “Keyur Amin” will log the user in.

Vocera Administrator | Add/Edit/View User -- Webpage Dialog

http://10.64.10.240/console/admin/adduserdialogframe.jsp

Edit User
(keyur amin)

Info Phone Speech Rec Groups Depts

First Name *
keyur

Last Name *
amin

User ID *
ka

Password
[Empty]

Re-enter Password
[Empty]

Email Address
[Empty]

Site
Global Select

Cost Center
[Empty]

Badge ID
0009ef115d4e

☐ Temporary User

Expiration Date (mm/dd/yyyy) [Empty]

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

Save Cancel

To configure the extension associated with the user, select the **Phone** tab and enter in extension number. (e.g., 0005) Then click the **Save** button.

Info Phone Speech Rec Groups Depts

Desk Phone or Extension
0005

Cell Phone
[Empty]

Home Phone
[Empty]

Pager
[Empty]

Vocera Extension
[Empty]

Dynamic Extension
[Empty]

PIN for Long Distance Calls
[Empty]

Cisco EM Extension
[Empty]

Cisco EM Auto-Answer
[Empty]

Vocera Access Anywhere

☐ Enable Vocera Access Anywhere

Phone Password (minimum 5 chars.)
[Empty]

Re-enter Phone Password
[Empty]

Note: Phone password not required if caller ID permission is used.

Save Cancel

7.3. Configure SIP OPTIONS

On the server running Vocera SIP Telephony Gateway edit the file vgwproperties.txt. The file may be found in x:\vocera\telephony\vgw\. Configure as follows:

- Set VTGUseOPTIONSForKeepAlive to true
- Set VTGOPTIONSKeepAliveToUser to blank (no value)
- Set VTGUseOPTIONSKeepAliveText to true
- Set VTGSipTransport to udp or tcp or tls

```
VTGUseOPTIONSForKeepAlive = true
VTGOPTIONSKeepAliveInterval = 30
VTGOPTIONSKeepAliveToUser =
VTGUseOPTIONSKeepAliveText = true
VTGSipTransport = tls
```

8. Verification Steps

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

8.1. Verify Avaya Aura® Communication Manager

On Communication Manager, verify the status of the SIP signaling group by using the **status signaling-group <s>** command, where **s** is the signaling group number administered in [Section 5.5](#). Verify that the signaling group is *in-service* as indicated in the Group State field shown below.

```
status signaling-group 10
                        STATUS SIGNALING GROUP

      Group ID: 10
      Group Type: sip

      Group State: in-service
```

Verify the status of the local SIP trunk group by using the **status trunk <t>** command, where **t** is the trunk group number administered in [Section 5.6](#). Verify that all trunks are in the *in-service/idle* state as shown below.

```
status trunk 10

                        TRUNK GROUP STATUS

Member   Port      Service State      Mtce Connected Ports
                               Busy

0010/001 T00001    in-service/idle    no
0010/002 T00002    in-service/idle    no
0010/003 T00003    in-service/idle    no
0010/004 T00004    in-service/idle    no
0010/005 T00005    in-service/idle    no
0010/006 T00006    in-service/idle    no
0010/007 T00007    in-service/idle    no
0010/008 T00008    in-service/idle    no
0010/009 T00009    in-service/idle    no
0010/010 T00010    in-service/idle    no
```

While calls are established, **Enter status trunk <t/r>** command, where **t** is the SIP trunk group configured in [Section 5.6](#), and **r** is the trunk group member used for a call. Verify **Service State** is *in-service/active*.

```
status trunk 0010/001                                     Page 1 of 3

                                TRUNK STATUS

Trunk Group/Member: 0010/001                               Service State: in-service/active
Port: T00001                                                Maintenance Busy? no
Signaling Group ID: 1

IGAR Connection? no

Connected Ports: T00003
```

8.2. Verify Avaya Aura® Session Manager

Navigate to **Home → Elements → Session Manager → System Status → SIP Entity Monitoring** and select the Communication Manager SIP Entity (not shown). Verify the **Conn. Status** and **Link Status** are *Up*.

The screenshot shows the Avaya Aura® System Manager 6.1 interface. The left sidebar contains a navigation menu with 'Session Manager' and 'System Status' highlighted. The main content area is titled 'SIP Entity, Entity Link Connection Status' and shows a table of entity links. The table has columns for 'Session Manager Name', 'SIP Entity Resolved IP', 'Port', 'Proto.', 'Conn. Status', 'Reason Code', and 'Link Status'. The 'Conn. Status' and 'Link Status' columns are highlighted in red boxes, both showing 'Up'.

Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
Show	sm_60_19	10.64.60.13	5061	TLS	Up	200 OK	Up

Repeat the procedure above selecting the VSTG SIP Entity, and verify the **Conn. Status** and **Link Status** are *Up*.

8.3. 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 open it. Look for “listening on Address [x.x.x.x:x] – TLS;” This indicates a successful TLS connection between Session Manager and VSTG. Look for “SIP Trunk [x.x.x.x:x] is alive;” this indicates successful SIP connectivity between Session Manager and VSTG.

```
2014:01:14 10:44:55.191 [02268,INFO_] [-----] VTGSipTransport  tls
...
2014:01:14 10:44:55.222 [02268,INFO_] [-----] [VTSIPStack] TLS From
URI is [<sip:vtg@10.64.10.242:5061;transport=tls>]
2014:01:14 10:44:55.222 [02268,INFO_] [-----] [VTSIPStack] TLS Contact
URI is [<sip:vtg@10.64.10.242:5061;transport=tls>]
...
2014:01:14 10:44:55.269 [02288,INFO_] [-----] [VTSIPStack] Start TLS
Transport
2014:01:14 10:44:55.269 [02288,PJSIP] [pjsiplogging] [VTSIPStack] PJSIP[4] -
SIP TLS listener is ready for incoming connections at 10.64.10.242:5061
2014:01:14 10:44:55.269 [02288,INFO_] [-----] [VTSIPStack] listening
on address [10.64.10.242:5061] - TLS

2014:01:14 10:46:17.633 [02288,PJSIP] [pjsiplogging] [VTSIPStack] PJSIP[4] -
TLS listener 10.64.10.242:5061: got incoming TLS connection from
10.64.10.62:41121, sock=115173892
2014:01:14 10:46:17.633 [02288,PJSIP] [pjsiplogging] [VTSIPStack] PJSIP[4] -
TLS server transport created
2014:01:14 10:46:17.633 [02288,DEBUG] [-----] [VTSIPStack]
*****PJSIP_TP_STATE_CONNECTED***** [10.64.10.62]
2014:01:14 10:46:17.634 [02288,INFO_] [-----] [SIPTrunkMgr] SIP Trunk
[10.64.10.62] is alive
```

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. 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, December 2013, Release 6.3, Document Number 03-300509.*
- (2) *Administering Avaya® Session Manager, October 2013, Release 6.3, Issue 3*

The following document was provided by Vocera.

- (3) *Vocera Telephony Configuration Guide, Version 4.4*
- (4) *Vocera B3000 Badge Guide, Version 4.4*
- (5) *Vocera Administration Guide Version 4.4*

©2014 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.