



Avaya Solution & Interoperability Test Lab

Application Notes for Vocera Platform with Avaya Aura® Communication Manager and Avaya Aura® Session Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate the Vocera SIP Telephony Gateway component within the Vocera Platform with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Vocera Platform is a mobile communication solution for hospital staff and mobile workers across diverse enterprise organizations. The Vocera Platform allows wireless voice communication between small, wearable Vocera Badges and an Avaya IP telephony network using a SIP trunk to Avaya Aura® Session Manager. For this compliance test, the Vocera V5000 Smartbadge and Vocera B3000n Badge were used.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in Section **2.1** as well as the 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 configuration steps required to integrate the Vocera SIP Telephony Gateway (VSTG) component within the Vocera Platform with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The Vocera Platform allows wireless voice communication between small, wearable Vocera Badges and an Avaya IP telephony network using a SIP trunk to Avaya Aura® Session Manager. The Vocera Platform allows wireless voice communication between small, wearable Vocera Badges and an Avaya IP telephony network using a SIP trunk. The SIP trunk is established between the Vocera SIP Telephony Gateway service within the Vocera Platform and Avaya Aura® Session Manager. For this compliance test, the Vocera V5000 Smartbadge and Vocera B3000n Badge were used. The Vocera Badges are wireless devices that gain network access through a wireless access point.

2 General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on establishing calls between Vocera Badges, Avaya SIP and H.323 IP Deskphones, and the PSTN, and exercising basic telephony features, such as hold, mute, and transfer.

The serviceability testing focused on verifying that the Vocera Platform came back into service after re-connecting the Ethernet cable and rebooting the system. The following sub-section covers the features and functionality that were covered in more detail.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Vocera SIP Telephony Gateway did not include use of any specific encryption features as requested by Vocera.

2.1 Interoperability Compliance Testing

Interoperability compliance testing covered the following features and functionality:

- Establishing a SIP trunk between Session Manager and VSTG. This included verifying that VSTG and Session Manager can both respond successfully to SIP OPTIONS messages.
- Calls between Vocera Badges and Avaya SIP/H.323 IP Deskphones with Direct IP Media (Shuffling) enabled and disabled.
- Calls between Vocera Badges and the PSTN.
- Calls to Vocera Genie (i.e., auto attendant).
- Emergency broadcasts from one badge to all badges within a group.
- G.711 codec support.
- UDP/TCP transport protocol support.
- Proper recognition of DTMF tones from VSTG.
- Basic telephony features, including mute, hold, redial, multiple calls, blind transfers, and attended conferences.
- Proper system recovery after a reboot of the Vocera Platform server and loss of IP network connectivity.

2.2 Test Results

All test cases passed with the following observation(s).

- The Vocera V5000 Smartbadge currently cannot initiate a conference with an Avaya phone. However, other Vocera Badges can be conferenced. The Vocera B3000n Badge does allow Avaya phones to be conferenced.
- The Vocera Platform supports blind transfers and attended conferences only.

2.3 Support

Vocera Technical Support for the Vocera Platform and Vocera Badges can be obtained via phone, email, or website.

- **Phone:** 1 (800) 9-VOCERA
- **Email:** support@vocera.com
- **Web:** <https://www.vocera.com/services-support/vocera-portal-access>

3 Reference Configuration

Figure 1 illustrates a sample configuration with an Avaya SIP-based network that includes the following products:

- Communication Manager running with a G450 Media Gateway and Avaya Aura® Media Server providing media resources.
- Session Manager connected to Communication Manager and VSTG via SIP trunks.
- Session Manager connected to the PSTN via Avaya Session Border Controller for Enterprise (SBCE).
- Avaya Aura® System Manager to configure Session Manager.
- Avaya H.323 and SIP Deskphones.
- Vocera Badges gaining network access via a wireless access point (not shown).

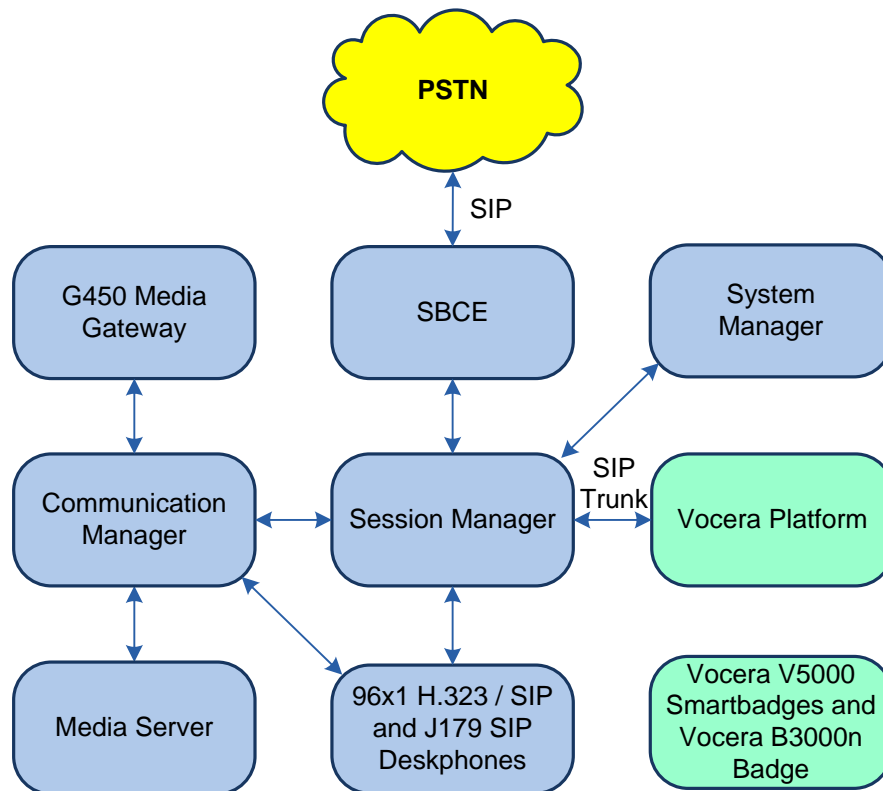


Figure 1: Avaya SIP Telephony Network with Vocera Platform and Vocera Badges

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	8.1.1.0.0-FP1
Avaya G450 Media Gateway	FW 40.25.0
Avaya Aura® Media Server	v.8.0.1.121
Avaya Aura® System Manager	8.1.0.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.0.0.079814
Avaya Aura® Session Manager	8.1.0.0.810007
Avaya 96x1 Series IP Deskphones	6.8304 (H.323) 7.1.7.0.11 (SIP)
Avaya J179 SIP Deskphone	4.0.3.1.4
Avaya Session Border Controller for Enterprise	
Vocera Platform with Vocera SIP Telephony Gateway	6.2.0.3
Vocera V5000 Smartbadge	5.1.1 [41]
Vocera B3000n Badge	4.3.1.17

5 Configure Avaya Aura® Communication Manager

This section describes the steps for configuring a SIP trunk to Session Manager and routing calls to Vocera Platform. Administration of Communication Manager was performed using the System Access Terminal (SAT).

This section covers the following configuration:

- **IP Node Names** to associate names with IP addresses.
- **IP Codec Set** to specify the codec type used for calls to VSTG.
- **IP Network Region** to specify the domain name and the IP codec set, to enable IP-IP direct audio (i.e., Shuffling), and to specify the UDP port range.
- **SIP trunk** for calls towards Session Manager and VSTG.
- **Private Numbering** to allow the caller's extension to be sent to VSTG.
- **Call Routing** to route calls to VSTG using AAR.

5.1 Administer IP Node Names

In the **IP Node Names** form, assign an IP address and host name for Communication Manager (*procr*) and Session Manager (*devcon-sm*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip                                     Page 1 of 2
                                                    IP NODE NAMES
  Name                IP Address
  default              0.0.0.0
  devcon-aes           10.64.102.119
  devcon-ams           10.64.102.118
  devcon-sm           10.64.102.117
  procr              10.64.102.115
  procr6              ::
( 6 of 6 administered node-names were displayed )
Use 'list node-names' command to see all the administered node-names
Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

5.2 Administer IP Codec Set

In the **IP Codec Set** form, select the audio codec type supported for calls routed over the SIP trunk to Vocera Platform. The form is accessed via the **change ip-codec-set 1** command. Note the codec set number since it will be used in the IP Network Region covered in the next section. For the compliance test, G.711MU codec was used.

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

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio          Silence      Frames      Packet
Codec          Suppression  Per Pkt    Size (ms)
1: G.711MU      n              2          20
2:
3:
4:
5:
6:
7:

Media Encryption          Encrypted SRTP: best-effort
1: 1-srtp-aescm128-hmac80
2: none
3:
4:
5:
```

5.3 Administer IP Network Region

In the **IP Network Region** form, the **Authoritative Domain** field is configured to match the domain name configured on Session Manager. In this configuration, the domain name is *avaya.com*. By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between the Vocera Platform and IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. The **IP Network Region** form also specifies the **IP Codec Set** to be used for calls routed over the SIP trunk to Session Manager. This codec set is used when its corresponding network region (i.e., IP Network Region 1) is specified in the SIP signaling group.

```
change ip-network-region 1                                     Page 1 of 20
                                                           IP NETWORK REGION
  Region: 1
Location: 1          Authoritative Domain: avaya.com
  Name:              Stub Network Region: n
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: 50999
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
H.323 IP ENDPOINTS
  H.323 Link Bounce Recovery? y
  Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
  Keep-Alive Count: 5
                                AUDIO RESOURCE RESERVATION PARAMETERS
                                RSVP Enabled? n
```


5.4 Administer SIP Trunk to Session Manager

Prior to configuring a SIP trunk group for communication with Session Manager, a SIP signaling group must be configured. Configure the **Signaling Group** form as follows:

- Set the **Group Type** field to *sip*.
- Set the **IMS Enabled** field to *n*.
- The **Transport Method** field was set to *tls*.
- Specify the Ethernet processor (*procr*) of Communication Manager and Session Manager as the two ends of the signaling group in the **Near-end Node Name** field and the **Far-end Node Name** field, respectively. These field values are taken from the **IP Node Names** form in **Section 5.1**.
- Ensure that the TLS port value of *5061* is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields.
- The preferred codec for the call will be selected from the IP codec set assigned to the IP network region specified in the **Far-end Network Region** field.
- Enter the domain name of Session Manager in the **Far-end Domain** field. In this configuration, the domain name is *avaya.com*.
- The **Direct IP-IP Audio Connections** field was enabled on this form.
- The **DTMF over IP** field should be set to the default value of *rtp-payload*.

Communication Manager supports DTMF transmission using RFC 2833. The default values for the other fields may be used.

```
add signaling-group 10                                     Page 1 of 2
                                     SIGNALING GROUP
Group Number: 10                Group Type: sip
IMS Enabled? n                  Transport Method: tls
  Q-SIP? n
  IP Video? n                    Enforce SIPS URI for SRTP? n
Peer Detection Enabled? y Peer Server: SM                Clustered? n
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n
Alert Incoming SIP Crisis Calls? n
Near-end Node Name: procr                Far-end Node Name: devcon-sm
Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                     Far-end Network Region: 1
Far-end Domain: avaya.com
Incoming Dialog Loopbacks: eliminate                Bypass If IP Threshold Exceeded? n
                                     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
```

Configure the **Trunk Group** form as shown below. This trunk group is used for SIP calls to the Vocera Platform. Set the **Group Type** field to *sip*, set the **Service Type** field to *tie*, specify the signaling group associated with this trunk group in the **Signaling Group** field, and specify the

Number of Members supported by this SIP trunk group. Accept the default values for the remaining fields.

```
add trunk-group 10                                     Page 1 of 5
                                     TRUNK GROUP
Group Number: 10                                     Group Type: sip          CDR Reports: y
  Group Name: To devcon-sm                          COR: 1                  TN: 1            TAC: 1010
  Direction: two-way                                Outgoing Display? n
  Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                                Auth Code? n
                                                Member Assignment Method: auto
                                                Signaling Group: 10
                                                Number of Members: 10
```

On **Page 3** of the trunk group form, set the **Numbering Format** field to *private*. This field specifies the format of the calling party number sent to the far-end.

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

On **Page 4** of the trunk group form, the default settings were used as shown below.

```
add trunk-group 10                                     Page 4 of 21
                                     PROTOCOL VARIATIONS
                                     Mark Users as Phone? n
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n
  Send Transferring Party Information? n
  Network Call Redirection? n
  Send Diversion Header? n
  Support Request History? y
  Telephone Event Payload Type:
  Convert 180 to 183 for Early Media? n
  Always Use re-INVITE for Display Updates? n
  Identity for Calling Party Display: P-Asserted-Identity
  Block Sending Calling Party Location in INVITE? n
  Accept Redirect to Blank User Destination? n
  Enable Q-SIP? n
  Interworking of ISDN Clearing with In-Band Tones: keep-channel-active
  Request URI Contents: may-have-extra-digits
```

5.5 Configure Private Numbering

Configure the **Numbering – Private Format** form to send the calling party number to the far-end. Add an entry so that local stations with a 5-digit extension beginning with ‘7’ whose calls are routed over any trunk group, including SIP trunk group 10, have the extension sent to the Vocera Platform.

```
change private-numbering 0
```

Page 1 of 2

NUMBERING - PRIVATE FORMAT

Ext Len	Ext Code	Trk Grp(s)	Private Prefix	Total Len	
5	7			5	Total Administered: 1 Maximum Entries: 540

5.6 AAR Call Routing

Configure the uniform dial plan table to route calls using AAR for dialed digits that are 5-digits long and begin with ‘78’. This would cover call routing to the Vocera Platform extensions (i.e., 78800 – 78809).

```
change uniform-dialplan 7
```

Page 1 of 2

UNIFORM DIAL PLAN TABLE

Percent Full: 0

Matching Pattern	Len	Del	Insert Digits	Net Conv	Node Num
78	5	0		aar	n

SIP calls to Session Manager are routed over a SIP trunk via AAR call routing. Configure the AAR analysis form and add an entry that routes digits beginning with “78” to route pattern 10 as shown below. Note that the **Call Type** was set to *lev0*. This routes calls to SIP stations and to the Vocera Platform, including the Vocera Badges.

```
change aar analysis 7
```

Page 1 of 2

AAR DIGIT ANALYSIS TABLE

Location: all

Percent Full: 2

Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Reqd
7	7	7	254	aar		n
78	5	5	10	lev0		n
8	7	7	254	aar		n
9	7	7	254	aar		n
						n
						n

Configure a preference in **Route Pattern 10** to route calls over SIP trunk group 10 as shown below.

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

6 Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP Entity for VSTG
- Entity Link, which defines the SIP trunk parameters used by Session Manager when routing calls to/from the Vocera Platform
- Routing Policies and Dial Patterns
- Session Manager, corresponding to the Avaya Aura® Session Manager Server to be managed by Avaya Aura® System Manager

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

Note: It is assumed that basic configuration of Session Manager has already been performed. This section will focus on the configuration of the SIP entity, entity link, and call routing for the Vocera Platform.

6.1 Add SIP Entity for VSTG

In the sample configuration, one SIP trunk was configured for VSTG.

A SIP Entity must be added for VSTG. To add a SIP Entity, select **SIP Entities** on the left and click on the **New** button on the right (not shown). The following screen is displayed. Fill in the following:

Under *General*:

- **Name:** A descriptive name.
- **FQDN or IP Address:** IP address of VSTG.
- **Type:** Select *SIP trunk*.
- **Location:** Select the location defined previously (not shown).
- **Time Zone:** Time zone for this location.

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

AVAYA Aura® System Manager 8.1 | Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home | Routing

Routing
 Domains
 Locations
 Conditions
 Adaptations
SIP Entities
 Entity Links
 Time Ranges
 Routing Policies
 Dial Patterns
 Regular Expressions
 Defaults

SIP Entity Details Commit Cancel [Help ?](#)

General

* Name: Vocera
 * FQDN or IP Address: 192.168.100.220
 Type: SIP Trunk
 Notes: Vocera VSTG Server

Adaptation:
 Location: Thornton
 Time Zone: America/New_York

* SIP Timer B/F (in seconds): 4
 Minimum TLS Version: Use Global Setting
 Credential name:
 Securable:
 Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On
 Loop Count Threshold: 5
 Loop Detection Interval (in msec): 200

Monitoring

SIP Link Monitoring: Use Session Manager Configuration
 CRLF Keep Alive Monitoring: Use Session Manager Configuration

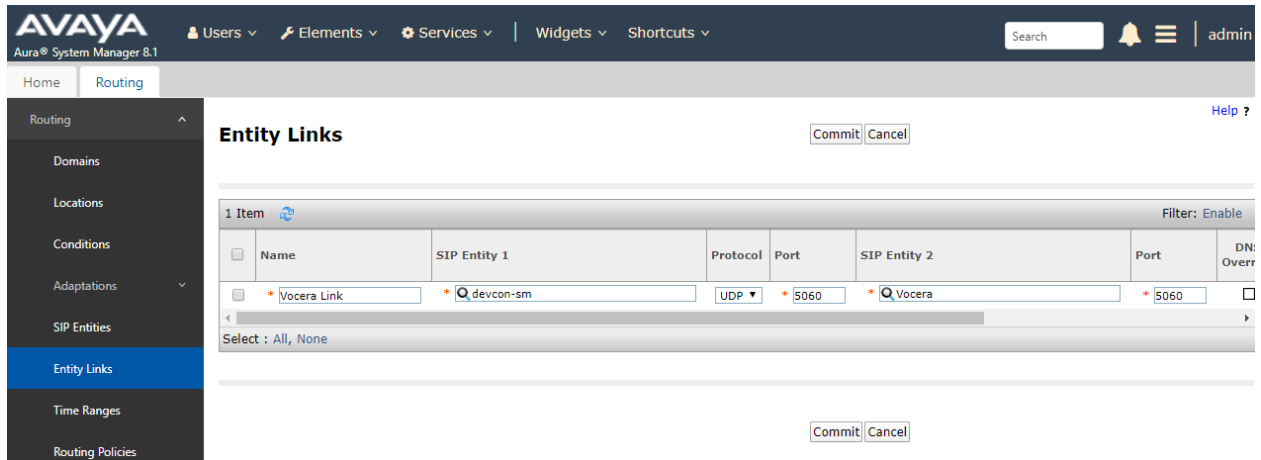
6.2 Add Entity Link for VSTG

This section covers the configuration of an Entity Link for VSTG. This entity link will specify that SIP entity configured in **Section 6.1**.

The SIP trunk from Session Manager to VSTG is described by an Entity link. To add an Entity Link, select **Entity Links** on the left and click on the **New** button (not shown) on the right. Fill in the following fields in the new row that is displayed:

- **Name:** A descriptive name (e.g., *Vocera Link*).
- **SIP Entity 1:** Select Session Manager.
- **Protocol:** Select the appropriate protocol (e.g., *UDP* or *TCP*).
- **Port:** Port number to which the other system sends SIP requests.
- **SIP Entity 2:** Select the VSTG entity configured in **Section 6.1**.
- **Port:** Port number on which the other system receives SIP requests.
- **Connection Policy:** Select *Trusted*. *Note: If Trusted is not selected, calls from the associated SIP Entity specified in Section 6.2 will be denied.*

Click **Commit** to save the Entity Link definition.



The screenshot shows the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, user information, and various menu items. The main content area is titled "Entity Links" and features a table with one row of configuration data. The table columns are: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, and DN: Overr. The row contains the following values: Name: * Vocera Link, SIP Entity 1: * devcon-sm, Protocol: UDP, Port: * 5060, SIP Entity 2: * Vocera, Port: * 5060, and DN: Overr: [checkbox]. The interface also includes "Commit" and "Cancel" buttons at the top and bottom of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DN: Overr
* Vocera Link	* devcon-sm	UDP	* 5060	* Vocera	* 5060	<input type="checkbox"/>

6.3 Add Routing Policies

Routing policies describe the conditions under which calls will be routed to the VSTG SIP Entity specified in **Section 6.1**. To add a routing policy, select **Routing Policies** on the left and click on the **New** button (not shown) on the right. The following screen is displayed. Fill in the following:

Under *General*:

Enter a descriptive name in **Name**.

Under *SIP Entity as Destination*:

Click **Select** and then select the appropriate SIP entity to which this routing policy applies. In this case, the VSTG SIP entity is selected.

Defaults can be used for the remaining fields. Click **Commit** to save the Routing Policy definition. The following screen shows the Routing Policy for VSTG.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 8.1', and various menu items: Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a navigation tree with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains the following sections:

- General**:
 - * Name: Vocera Policy
 - Disabled:
 - * Retries: 0
 - Notes: (empty text box)
- SIP Entity as Destination**:
 - Select button
 - Table with columns: Name, FQDN or IP Address, Type, Notes
 - Row: Vocera, 192.168.100.220, SIP Trunk, Vocera VSTG Server
- Time of Day**:
 - Buttons: Add, Remove, View Gaps/Overlaps
 - 1 Item (Filter: Enable)
 - Table with columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, Notes
 - Row: 0, 24/7, [checked], [checked], [checked], [checked], [checked], [checked], [checked], 00:00, 23:59, Time Range 24/7
 - Select: All, None

6.4 Add Dial Patterns

Dial patterns must be defined to direct calls to the appropriate SIP Entity. In the sample configuration, a 5-digit number beginning with '7880' will be routed to VSTG.

To add a dial pattern, select **Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

Under *General*:

- **Pattern:** Dialed number or prefix.
- **Min** Minimum length of dialed number.
- **Max** Maximum length of dialed number.
- **SIP Domain** SIP domain of dial pattern.
- **Notes** Comment on purpose of dial pattern (optional).

Under *Originating Locations and Routing Policies*:

Click **Add** and then select the appropriate location and routing policy from the list. In this case, the VSTG routing policy is selected.

Default values can be used for the remaining fields. Click **Commit** to save this dial pattern. The following screen shows the dial pattern definitions for VSTG extensions.

AVAYA Aura® System Manager 8.1

Users | Elements | Services | Widgets | Shortcuts | Search | admin

Home | Routing

Dial Pattern Details

Commit | Cancel | Help ?

General

* Pattern: 7880
* Min: 5
* Max: 5
Emergency Call:
SIP Domain: -ALL-
Notes: Vocera VSTG

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"/>	Thornton		Vocera Policy	0	<input type="checkbox"/>	Vocera	

Select : All, None

Denied Originating Locations

Add | Remove

0 Items

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

Commit | Cancel

6.5 Add Session Manager

Adding the Session Manager will provide the linkage between System Manager and Session Manager. Expand the **Session Manager** menu on the left and select **Session Manager Administration**. Then click **Add** (not shown), and fill in the fields as described below and shown in the following screen:

Under *General*:

- **SIP Entity Name:** Select the name of the SIP Entity added for Session Manager
- **Description:** Descriptive comment (optional)
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

Under *Security Module*:

- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager

Use default values for the remaining fields. Click **Commit** to add this Session Manager.

The screenshot shows the 'Edit Session Manager' configuration page in the Avaya Aura System Manager 8.1 interface. The page is divided into two main sections: 'General' and 'Security Module'. The 'General' section includes fields for 'SIP Entity Name' (devcon-sm), 'Description', '*Management Access Point Host Name/IP' (10.64.102.116), '*Direct Routing to Endpoints' (Enable), 'Data Center' (None), 'Avaya Aura Device Services Server Pairing' (None), and 'Maintenance Mode' (checkbox). The 'Security Module' section includes fields for 'SIP Entity IP Address' (10.64.102.117), '*Network Mask' (255.255.255.0), '*Default Gateway' (10.64.102.1), '*Call Control PHB' (46), and '*SIP Firewall Configuration' (SM 6.3.8.0). The page has a top navigation bar with 'AVAYA' logo, user 'admin', and search bar. A left sidebar shows the navigation menu with 'Session Manager Administration' selected. Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area.

The following screen shows the **Monitoring** section, which determines how frequently Session Manager sends SIP Options messages to VSTG. Use default values for the remaining fields. Click **Commit** to add this Session Manager. In the following configuration, Session Manager sends a SIP Options message every 900 secs. If there is no response, Session Manager will send a SIP Options message every 120 secs.

Monitoring ▾

Enable SIP Monitoring

*Proactive cycle time (secs)

*Reactive cycle time (secs)

*Number of Tries

*Number of Successes

Enable CRLF Keep Alive Monitoring

*CRLF Ping Interval (secs)

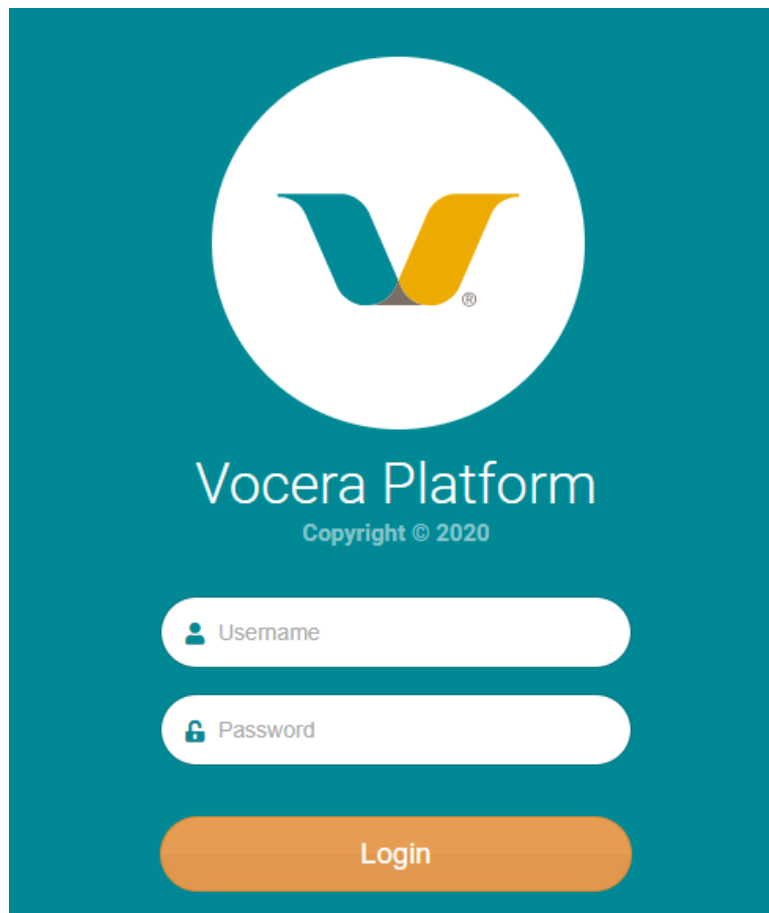
7 Configure Vocera Platform

This section covers the configuration of the Vocera SIP Telephony Gateway component within the Vocera Platform via the **Vocera Platform Web Console**. Launch a web browser and enter <https://<ip-address>> as the URL, where <ip-address> is the IP address of the Vocera Platform server. Log in with the appropriate credentials in the following webpage.

In the **Vocera Platform Web Console**, the following procedures are performed:

- Configure SIP Telephony
- Configure Users
- Enable SIP OPTIONS and Configure SIP transport protocol

Refer to [3] for more details on configuring the Vocera Platform.



7.1 Configure SIP Telephony

In the **Web Console**, navigate to **Manage** → **Facilities** to the **Hospital Locations** webpage shown below. Click the settings gearbox and select **Edit Facility** as shown below.

The screenshot displays the Vocera Web Console interface for managing hospital locations. The left sidebar contains navigation options, with 'Manage' highlighted. The main content area shows a table of facilities. The table has columns for Name, Description, and Department Count. One facility is listed: 'Global' with description 'Default Global facility' and a count of '0'. A settings gear icon is visible next to this row, with a dropdown menu open showing 'View Departments' and 'Edit Facility' options.

Name	Description	Department Count	
Global	Default Global facility	0	

The **Edit Facility** webpage is displayed as shown below.

vocera W < **Edit Facility** [Help](#)

Cancel Save

General

Name * Global Description Default Global facility

Time Zone * Pacific Emergency Broadcast Group Avaya (unde) Find Group

Enable Code Lavender Initiate Emergency Broadcast Silently

Enable Easter Eggs

Voice

Telephony - Basic Information

Telephony - Access Code Exceptions

Telephony - Toll Exceptions

Telephony - DID Information

Telephony - PINs

Telephony - Dynamic Extensions

Telephony - Sharing

Expand the **Telephony – Basic Information** section and configure the following parameters.

- **Number of Lines:** Specify the number of lines for the SIP trunk (e.g., 23).
- **Call Signaling Address:** Set to the Signaling IP address of Session Manager.
- **Calling Party Number:** Specify the extension to access Genie (i.e., auto attendant) for guest access.
- **Guest Access:** Specify the extension to access Genie (i.e., auto attendant) for guest access.
- **Direct Access:** Specify the extension to access Genie (i.e., auto attendant) for users with badges.

The screenshot displays the Vocera Edit Facility interface. The left sidebar contains navigation options: Messaging, Staff Assignment, My Profile, Status, Manage (highlighted), Users, Groups, Facilities, Contacts, AP Locations, Device Inventory, Templates, Bulk Actions, Settings, and Security. The main content area is titled 'Edit Facility' and features a 'Telephony - Basic Information' section. This section includes the following configuration options:

- Enable Telephony Integration
- Number of Lines * (input field: 23)
- Local Area Code * (input field: 408)
- Omit Area Code when Dialing Locally
- Default Local Access Code (input field: 7)
- Company Voicemail Access Code (input field: empty)
- SIP Settings**
 - Call Signaling Address (input field: 10.64.102.117)
 - Calling Party Number (input field: 78800)
- Vocera Hunt Group Numbers**
 - Guest Access (input field: 78800)
 - Direct Access (input field: 78801)
- Default Long-Distance Access Code (input field: empty)

Expand the **Telephony – DID Information** to configure the range of numbers to be assigned to users with badges. For the compliance test, 5-digit extensions starting with “7880” were used to route calls directly to badges. The leading two digits (i.e., 78) was assigned as the **Prefix** and the last three digits were assigned to badges as extensions (e.g., 802 to 809).

The screenshot shows the Vocera Edit Facility interface. On the left is a navigation sidebar with options: Messaging, Staff Assignment, My Profile, Status, Manage (Users, Groups, Facilities, Contacts, AP Locations, Device Inventory, Templates, Bulk Actions), Settings, and Security. The main content area is titled 'Edit Facility' and includes a 'Time Zone' dropdown set to 'Pacific', an 'Emergency Broadcast Group' dropdown set to 'Avaya (undefined)', and checkboxes for 'Enable Code Lavender', 'Enable Easter Eggs', and 'Initiate Emergency Broadcast Silently'. Below these are expandable sections for 'Voice', 'Telephony - Basic Information', 'Telephony - Access Code Exceptions', 'Telephony - Toll Exceptions', and 'Telephony - DID Information'. The 'Telephony - DID Information' section is expanded, showing a table with columns 'Prefix' and 'Range of Numbers'. A row shows a prefix of '78' and a range of '802 to 809'. Below the table is an 'Add DID' button.

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 user. Otherwise, the Genie prompts the caller to say the full name of the person or group, or enter an extension.

Prefix	Range of Numbers
78	802 to 809

+ Add DID

7.2 Configure Users

This section covers the assignment of a badge extension to an existing user. Navigate to **Manage** → **Users** to display the **Users** webpage shown below. Click on the setting gearbox associated with the user to be assigned a badge extension and select **Edit User**.

The screenshot displays the Vocera Users management interface. The main content area shows a table of users with the following data:

Last Name	First Name	Username	Facility	
Brown	Dan	dbrown	Global	
Ford	Tom	tford		
Grey	Meredith	mgrey		
Support	Customer	administrator	Global	
Support	Vocera	eisupport	Global	
user1	gen5	g5u1	Global	
user2	gen5	g5u2	Global	
user3	gen5	g5u3	Global	
user4	gen5	g5u4	Global	
	Vocera	extension	Global	

The context menu for the 'Support' user is open, showing the following options:

- Edit User
- Delete User

The page also includes a search bar, a filter dropdown for 'All Facilities', and a pagination indicator '1 - 10 of 10'.

In the **Edit User** webpage, expand the **Contact Information** section and assign an extension in the **Desk Phone or Extension** field. In this example, extension 802 was assigned. The range of valid extensions was configured in **Section 7.1**.

The screenshot shows the 'Edit User' interface in the Vocera system. The left sidebar contains navigation options: Messaging, Staff Assignment, My Profile, Status, Manage (Users, Groups, Facilities, Contacts, AP Locations, Device Inventory, Templates, Bulk Actions), Settings, and Security. The main content area is titled 'Edit User' and includes a 'Delete User' button, 'Cancel', and 'Save' buttons. The 'General' section is expanded, showing fields for Facility (Global), Profile Photo (DB), First Name (Dan), Middle Name, Last Name (Brown), Job Title (Dr.), Personal Title (Mr.), Home Department, and Notes. The 'Login Information' section is collapsed. The 'Contact Information' section is expanded, showing fields for Email Address, Cell Phone, and Desk Phone or Extension (802).

7.3 Configure SIP OPTIONS and Transport Protocol

The parameters to enable VSTG to send SIP OPTIONS to Session Manager and to specify the transport protocol for the SIP trunk are specified in the `/opt/vocera/bin/vstgproperties.txt` file on the Vocera Platform server. The parameters to enable SIP OPTIONS are shown below. Ensure that the `VTGOPTIONSKeepAliveToUser` parameter is blank.

```
#####
# The VSTG does not have a direct physical connection to the IP PBX (or VoIP
# gateway). However, some IP PBXs support using the OPTIONS message to ping
# the PBX to determine if the SIP trunk is up. The following properties are
# for sending an OPTIONS message to the IP PBX to determine if the SIP trunk
# is still alive or not. If the connection goes down (perhaps due to a network
# problem), an email notification is sent to the Vocera administrator.
#
# Note: If you have set up a VSTG server array and one of the servers stops
# responding, the Vocera Server automatically redirects outbound calls to another
# available VSTG server for uninterrupted service.
#
# VTGUseOPTIONSForKeepAlive = Whether to use the OPTIONS message to ping
# the IP PBX to determine if the SIP trunk is up.
# The default is TRUE.
#
# Note: You should only set this property to
# TRUE if your PBX supports using an OPTIONS
# message as a keep-alive mechanism.
#
# VTGOPTIONSKeepAliveInterval = Specifies the time interval between pings of
# the IP PBX in seconds. The default is 30, but
# you can set it as low as 5.
#
# VTGOPTIONSKeepAliveToUser = Specifies the number for the user part of
# the To header and for the Request URI. The
# default is "trunk_status". In most cases, you
# should not change this value. Do NOT change
# the default value to a real user number.
#
# VTGUseOPTIONSKeepAliveText = Whether to include the text "keepalive" in
# the OPTIONS message payload. The default is
# TRUE, which is appropriate for most IP PBXs.
# Note: If you are connecting to a PBX using
# Dialogic Media Gateway, set this property to
# FALSE.
#
###
VTGUseOPTIONSForKeepAlive = true
VTGOPTIONSKeepAliveInterval = 30
VTGOPTIONSKeepAliveToUser =
VTGUseOPTIONSKeepAliveText = false
```

The **VTGSipTransport** parameter is used to specify the transport protocol used by VSTG. This parameter should match the transport protocol used by the Session Manager Entity Link described in **Section 6.2**. In the example, UDP transport protocol is used, but TCP is also supported.

```
#####
# VSTG uses UDP to send SIP packets to the IP PBX, but you can also configure
# the server to use TCP.
#
# VTGSipTransport = Specifies the transport protocol used to send
# SIP packets to the IP PBX. Specify "udp" (the
# default), or "tcp".
#
# You can enter a comma-delimited list of values to support
# multiple transport types. The first value in the list denotes
# the transport protocol for outgoing calls. All values in the
# list denote supported protocols for incoming calls. Also,
# the calls can originate from different PBX trunks. If you
# specify TCP or UDP, both TCP and UDP are supported.
#
# Here's an example:
#
# VTGSipTransport = tcp, tcp
#
# This means that all outgoing calls use TCP transport,
# but incoming calls can use TCP, or UDP transport.
###
VTGSipTransport = udp
```

8 Verification Steps

This section provides the tests that can be performed to verify proper configuration of the Vocera Platform with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. The following steps can be used to verify installations in the field.

1. Verify that the SIP trunk between Session Manager and the Vocera Platform is up by navigating to **Home→Elements→Session Manager→System Status→SIP Entity Monitoring** on System Manager. Below is the status of the SIP trunk to the Vocera Platform.

The screenshot displays the Avaya Aura System Manager 8.1 interface. The top navigation bar includes the Avaya logo, user information, and various menu options like Users, Elements, Services, Widgets, and Shortcuts. The main content area is titled "SIP Entity, Entity Link Connection Status" and provides a summary of connection details for a selected Session Manager. A table lists the "All Entity Links to SIP Entity: Vocera" with columns for Session Manager Name, IP Address Family, SIP Entity Resolved IP, Port, Proto., Deny, Conn. Status, Reason Code, and Link Status. The table shows one item with a status of "UP".

Session Manager Name	IP Address Family	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
devcon-sm	IPv4	192.168.100.220	5060	UDP	FALSE	UP	200 OK	UP

2. Verify that the SIP trunk between Communication Manager and Session Manager is in-service using the **status trunk** command on Communication Manager.
3. Place an incoming call to a Vocera Badge and answer the call. Verify two-way audio is provided.
4. Place an outgoing call from a Vocera Badge to an Avaya local station or PSTN and answer the call. Verify two-way audio is provided.

9 Conclusion

These Application Notes describe the configuration steps required to integrate the Vocera SIP Telephony Gateway component within the Vocera Platform with Avaya Aura® Communication Manager and Avaya Aura® Session Manager. A SIP trunk was established between Vocera SIP Telephony Gateway and Avaya Aura® Session Manager and basic telephony features were verified with Vocera Badges. All feature and serviceability test cases were completed successfully with observations noted in **Section 2.2**.

10 References

This section references the product documentation relevant to these Application Notes.

- [1] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 2, July 2019, available at <http://support.avaya.com>.
- [2] *Administering Avaya Aura® Session Manager*, Release 8.1, Issue 1, June 2019, available at <http://support.avaya.com>.
- [3] *Vocera Platform Telephony Guide*, Version 6.2.0, available on Vocera Documentation Portal at <http://pubs.vocera.com/portal/index.html>.

©2020 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.