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 10.1. 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. During compliance testing, the Vocera V5000 Smartbadge was 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 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 was used. The Vocera Badges are wireless devices that gain network access through a wireless access point. The Vocera platform tested is hosted on a Red Hat Enterprise Linux Server release 7.9 virtual environment.

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 these DevConnect Application Notes 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 these Application Notes, 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 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 Platform supports blind transfers and attended conferences only as blind conferences and attended transfers are not supported.
- All calls initiated from badges employed dialing extensions as opposed to specifying the Vocera name. Calls between badges remain internal to the Vocera Platform.
- The Vocera Platform was configured for audio mode only.

2.3 Support

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

- **Phone:** +1 (888) 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. The Vocera V5000 Smartbadge connects to the network via wireless access point (not shown).

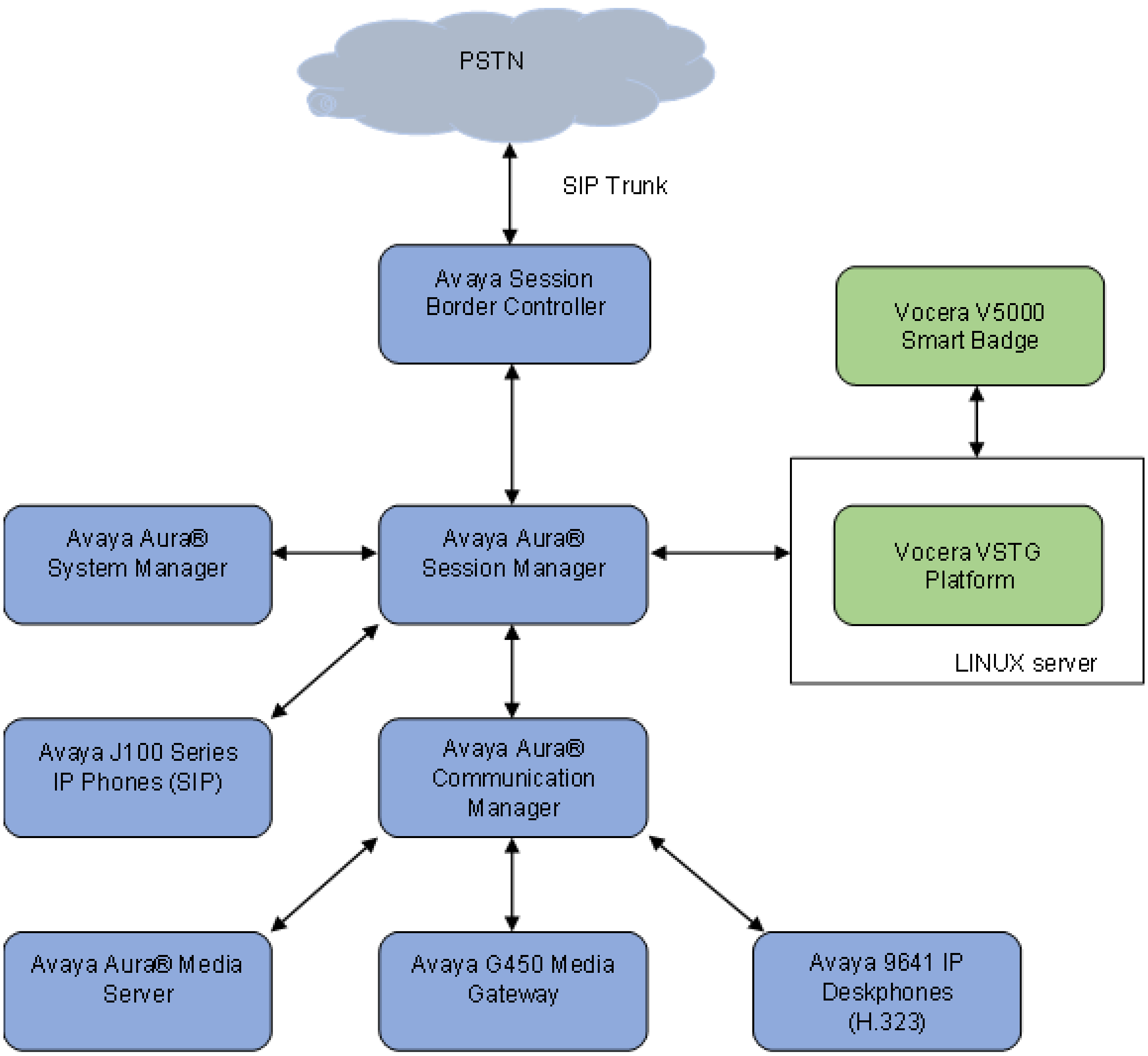


Figure 1: Avaya SIP Telephony Network with Vocera Platform and Vocera Badges

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 running on Virtual Machine	10.1.0.1 R020x.01.0.974.0
Avaya G450 Media Gateway	FW 42.7.0
Avaya Aura® Media Server running on Virtual Machine	10.1.0.77
Avaya Aura® System Manager running on Virtual Machine	10.1.0.1.0614394 (SP1)
Avaya Session Border Controller for Enterprise running on Virtual Machine	10.1.1.0-35-21872
Avaya Aura® Session Manager running on Virtual Machine	10.1.0.0.1010105
Avaya 96x1 Series IP Deskphones	6.8.5.2.3 (H.323)
Avaya J139 SIP Deskphone	4.0.12.0.6 (SIP)
Vocera Platform with Vocera SIP Telephony Gateway on LINUX running on Virtual Machine	6.5.0.20 Telephony service on LINUX 6.5.0.304 Voice service Red Hat Enterprise Linux Server release 7.9
Vocera V5000 Smartbadge	5.1.6.23

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 (*sm10*). The host names will be used in other configuration screens of Communication Manager.

```
change node-names ip
                                  IP NODE NAMES
    Name              IP Address
ams10               10.64.110.214
aura_cms18          10.64.110.20
cms19               10.64.110.225
default             0.0.0.0
procr               10.64.110.213
procr6              ::
remotecms191        10.64.110.226
sm10                10.64.110.212

( 8  of 8    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 SRTCP: best-effort
 1: none
 2:
 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. Set **IP-IP Direct** Audio to *no* to disable shuffling when needed for testing. 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       NR Group: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Main                    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: 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 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 (*sm10*) 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 1                                    Page   1 of   3
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority 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: sm10
 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): 65                    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 1                                          Page   1 of  5
                               TRUNK GROUP

Group Number: 1                  Group Type: sip          CDR Reports: y
  Group Name: SM Trunk 1               COR: 1        TN: 1        TAC: 101
   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: 1
                                                    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 1                                          Page   3 of   5
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                      Maintenance Tests? y

   Suppress # Outpulsing? n  Numbering Format: private
                                               UUI Treatment: shared
                                             Maximum Size of UUI Contents: 128
                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? N


                                Modify Tandem Calling Number: tandem-cpn-form
               Send UCID? y


 Show ANSWERED BY on Display? Y

DSN Term? n
```

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 1, have the extension sent to the Vocera Platform.

```
change private-numbering 0                                    Page   1 of   2
                          NUMBERING - PRIVATE FORMAT

Ext Ext             Trk        Private          Total
Len Code            Grp(s)     Prefix           Len
5   5                                          5     Total Administered: 3
5   7                                          5        Maximum Entries: 540
5   5999                                       5
```

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 '7204'. This would cover call routing to the Vocera Platform extensions (i.e., 72041 – 72049).

```
change uniform-dialplan 7                                          Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                                 Percent Full: 0

  Matching                    Insert              Node
  Pattern       Len Del       Digits      Net Conv Num
 7204           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 "7204" to route pattern 1 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: 0

          Dialed          Total     Route    Call   Node  ANI
          String         Min  Max  Pattern   Type   Num   Reqd
    70                   7    7     1        lev0         n
    71                   7    7     1        aar          n
    7204                 5    5     1        lev0         n
    73999                5    5     1        aar          n
                                                          n
                                                          n
```

Configure a preference in **Route Pattern** 1 to route calls over SIP trunk group 1 as shown below.

```
change route-pattern 1                                          Page   1 of   4
                    Pattern Number: 1      Pattern Name: main
    SCCAN? n    Secure SIP? y     Used for SIP stations? n

    Grp FRL NPA Pfx Hop Toll No.  Inserted                              DCS/ IXC
    No          Mrk Lmt List Del  Digits                                QSIG
                             Dgts                                       Intw
 1: 1    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 Sub  Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
 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
- Dial Patterns
- Session Manager, corresponding to the Session Manager server to be managed by Avaya System Manager

Configuration is accomplished by accessing the browser-based GUI of System Manager using the URL "https://<*ip-address*>/SMGR", where <*ip-address*> is the IP address of 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

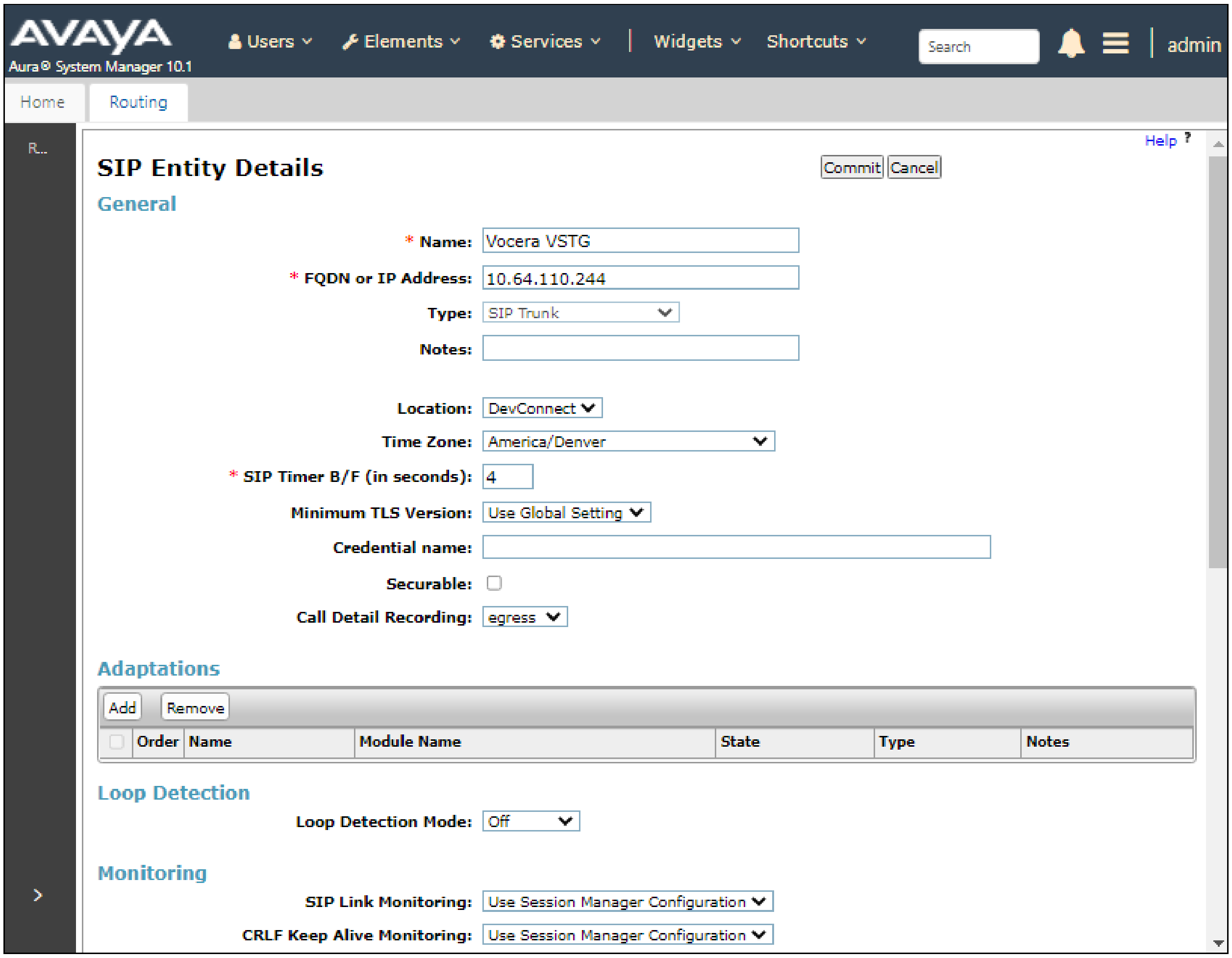
In the sample configuration, one SIP trunk was configured for VSTG.

A SIP Entity must be added for VSTG. To add a SIP Entity, select **Elements → Routing → SIP Entities** 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 10.1
Users
Elements
Services
Widgets
Shortcuts
Search
admin
Home
Routing
R...
Help ?
SIP Entity Details
Commit
Cancel
General
* Name: Vocera VSTG
* FQDN or IP Address: 10.64.110.244
Type: SIP Trunk
Notes:
Location: DevConnect
Time Zone: America/Denver
* SIP Timer B/F (in seconds): 4
Minimum TLS Version: Use Global Setting
Credential name:
Securable:
Call Detail Recording: egress
Adaptations
Add
Remove
Order
Name
Module Name
State
Type
Notes
Loop Detection
Loop Detection Mode: Off
Monitoring
SIP Link Monitoring: Use Session Manager Configuration
CRLF Keep Alive Monitoring: Use Session Manager Configuration

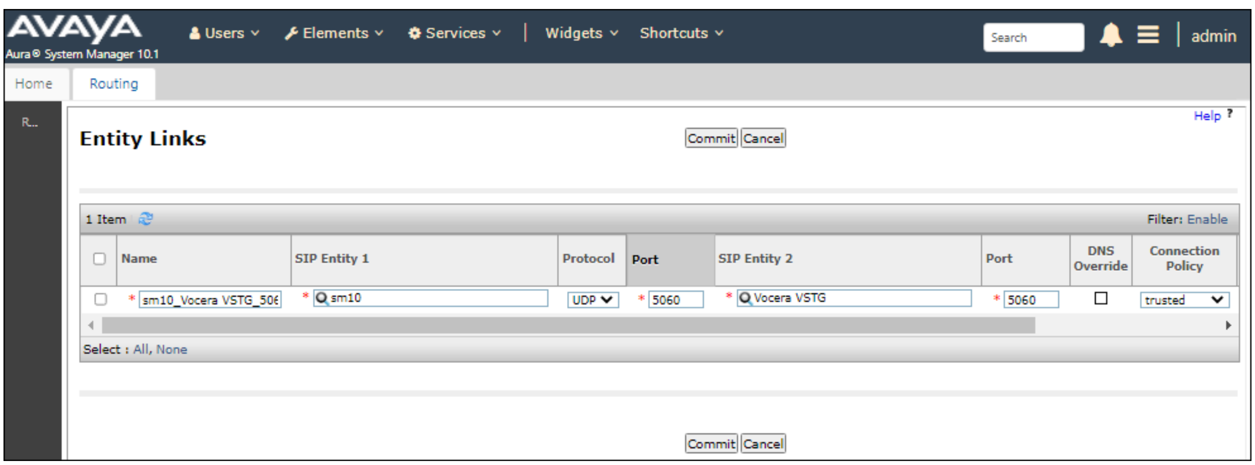
6.2 Add Entity Link for VSTG

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 **Elements → Routing → 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., *sm10_Vocera VSTG_5060_UDP_IPv4*).
- **SIP Entity 1:** Select Session Manager (e.g., *sm10*).
- **Protocol:** Select the appropriate protocol (e.g., *UDP*).
- **Port:** Port number to which the other system sends SIP Requests (e.g., *5060*).
- **SIP Entity 2:** Select the VSTG entity configured in **Section 6.1**.
- **Port:** Port number on which the other system receives SIP requests (e.g., *5060*).
- **Connection Policy:** Select *Trusted*. *Note: If Trusted is not selected, calls with the Session Manager SIP Entity defined in **Section 6.5** will be denied.*

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



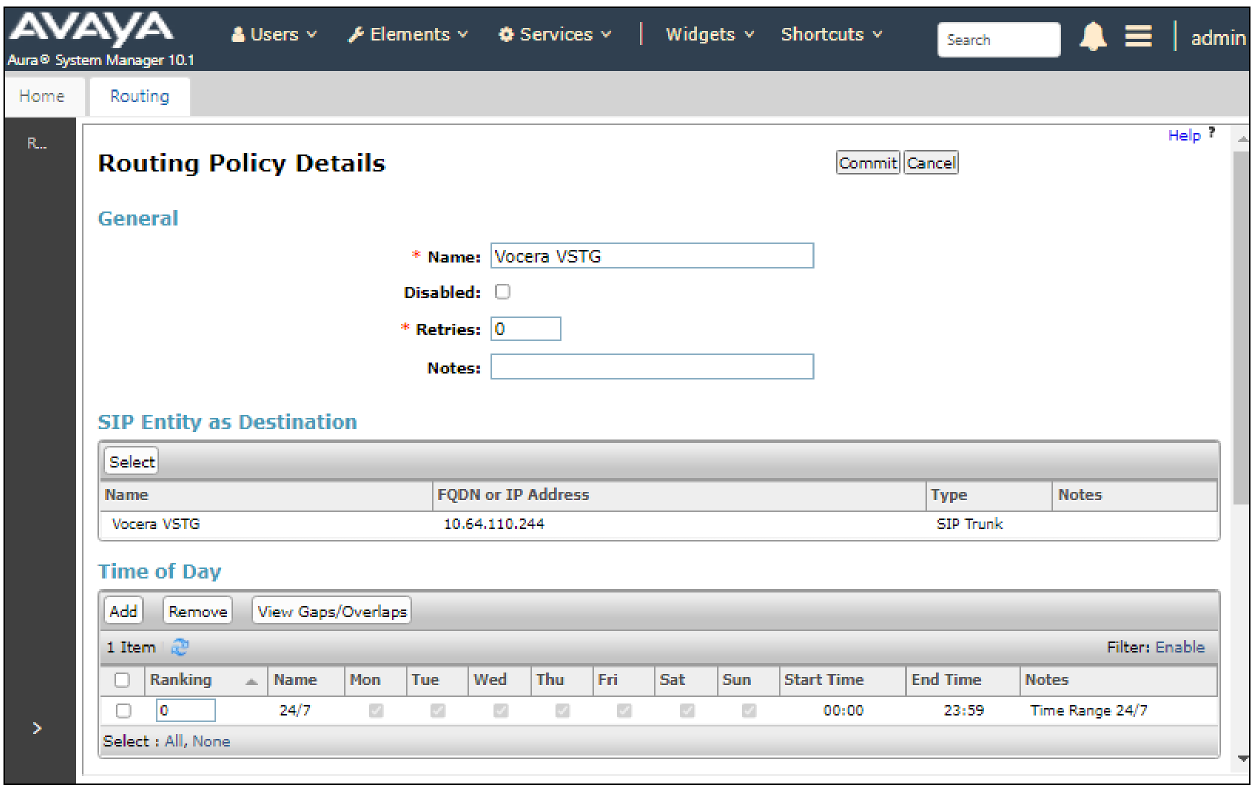
6.3 Add Routing Policies

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 **Elements → Routing → 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** (e.g., *Vocera VSTG*).

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 (e.g., *Vocera VSTG*) 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.



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 '7204' will be routed to VSTG.

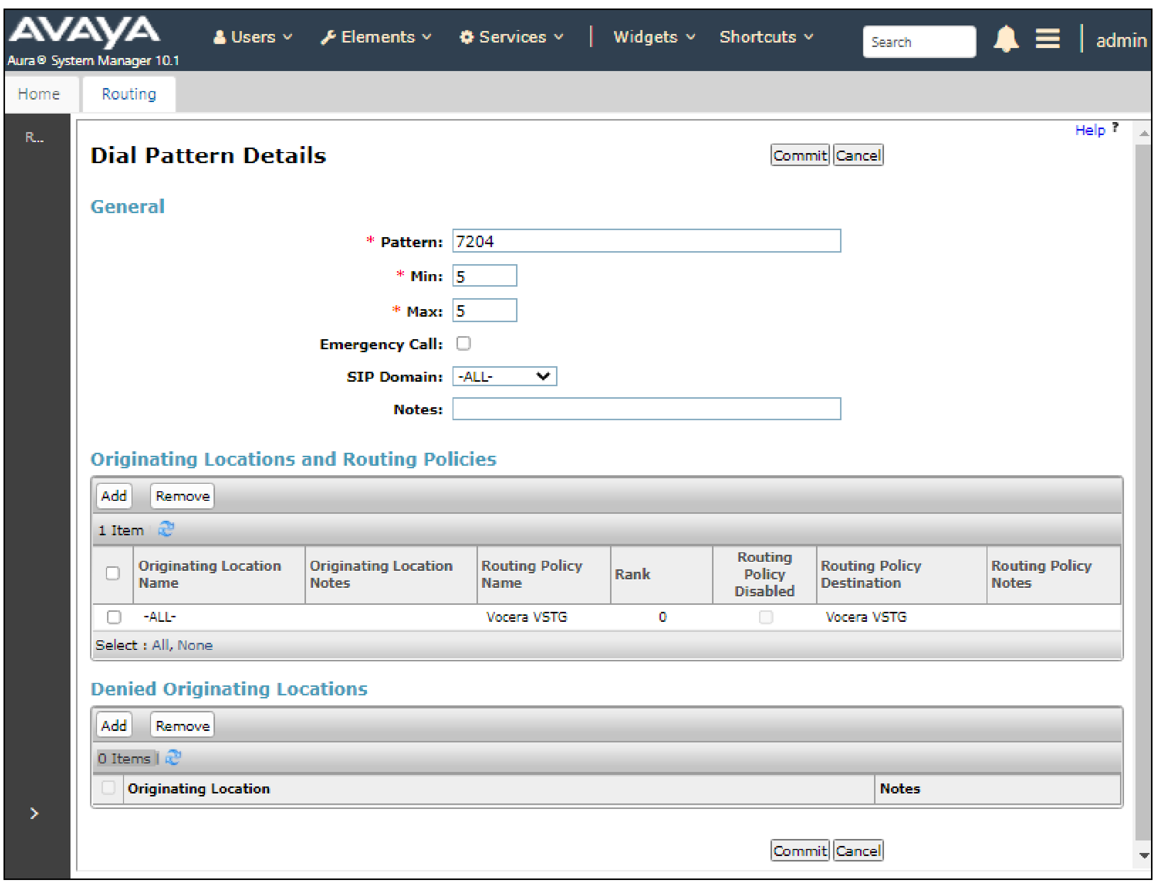
To add a dial pattern, select **Elements → Routing → Dial Patterns** on the left and click on the **New** button (not shown) on the right. Fill in the following:

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.



6.5 Add Session Manager

Adding the Session Manager will provide the linkage between System Manager and Session Manager. Select **Elements → Session Manager → Session Manager Administration**. Then click **New** (not shown), and fill in the fields as described below and shown in the following screen:

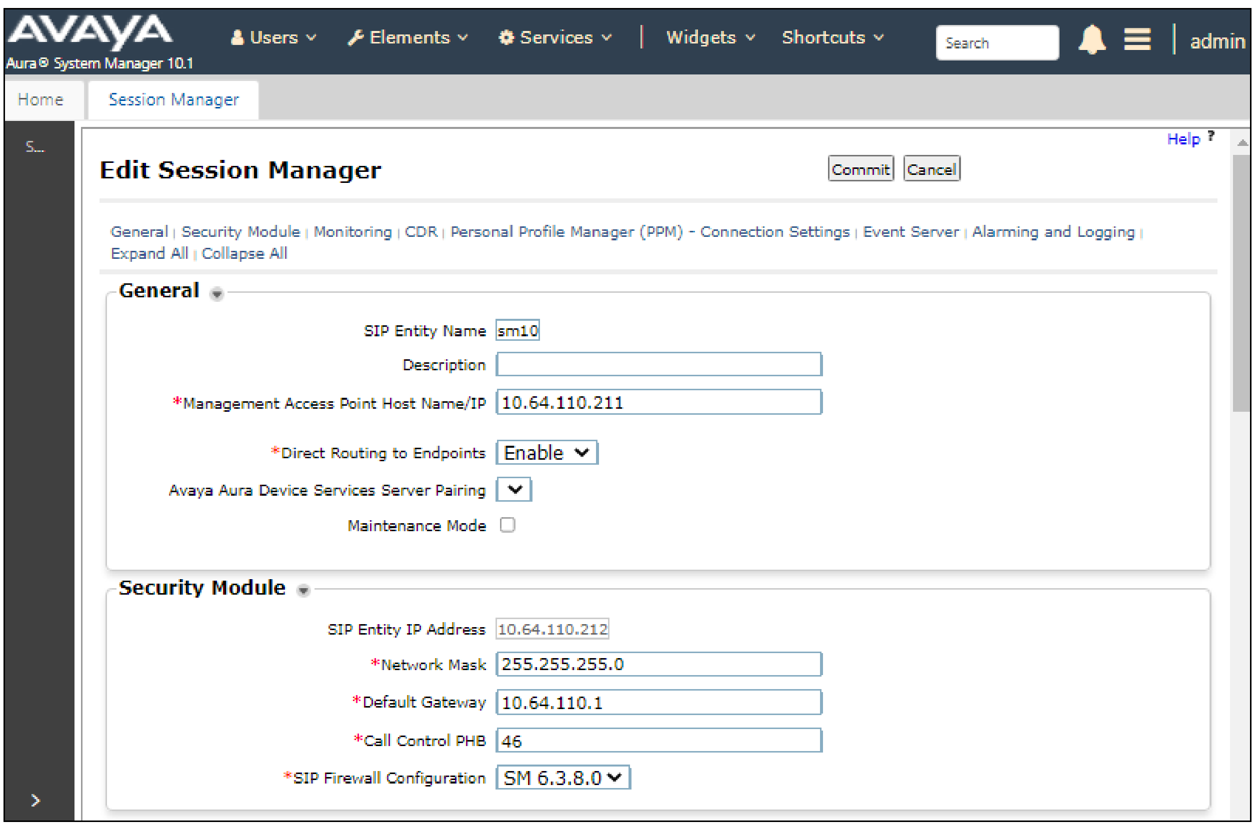
Under *General*:

- **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.

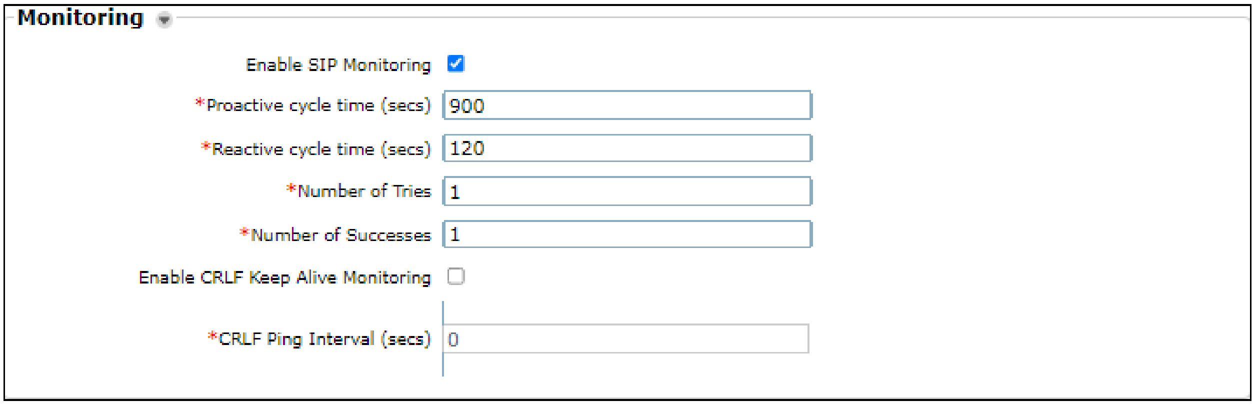
Under *Security Module*:

- **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 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.



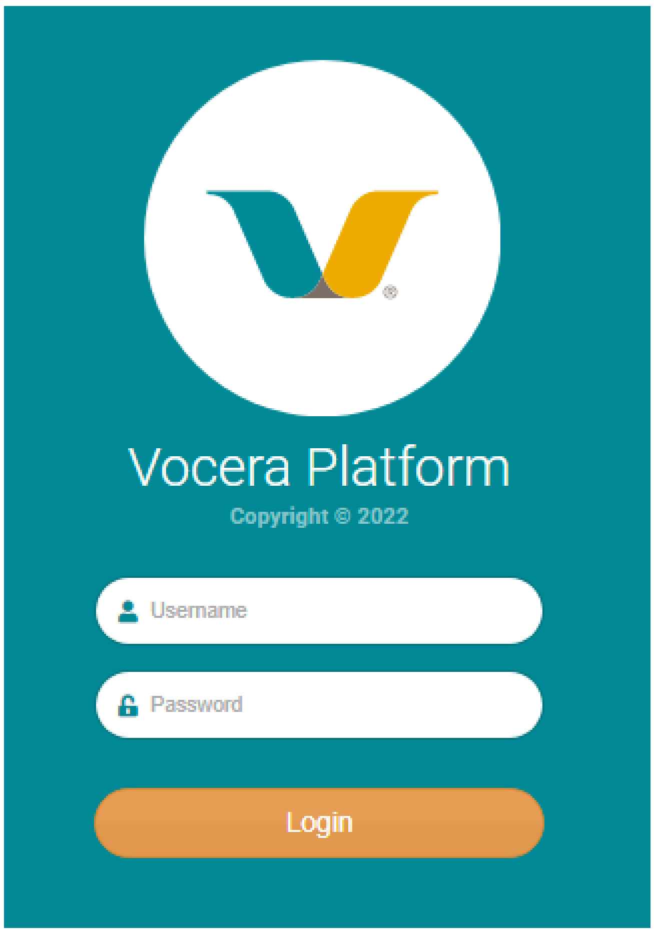
7 Configure Vocera Platform

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:

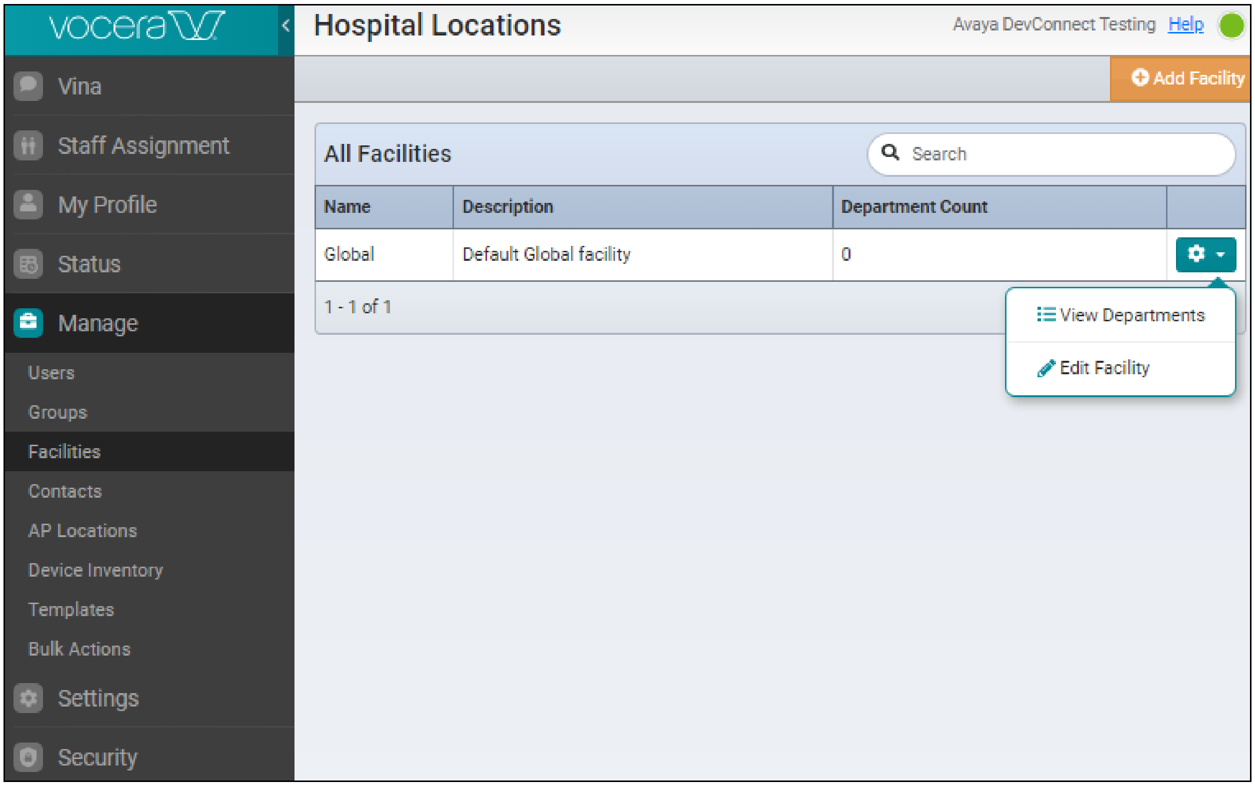
- Configure SIP Telephony
- Configure Users

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

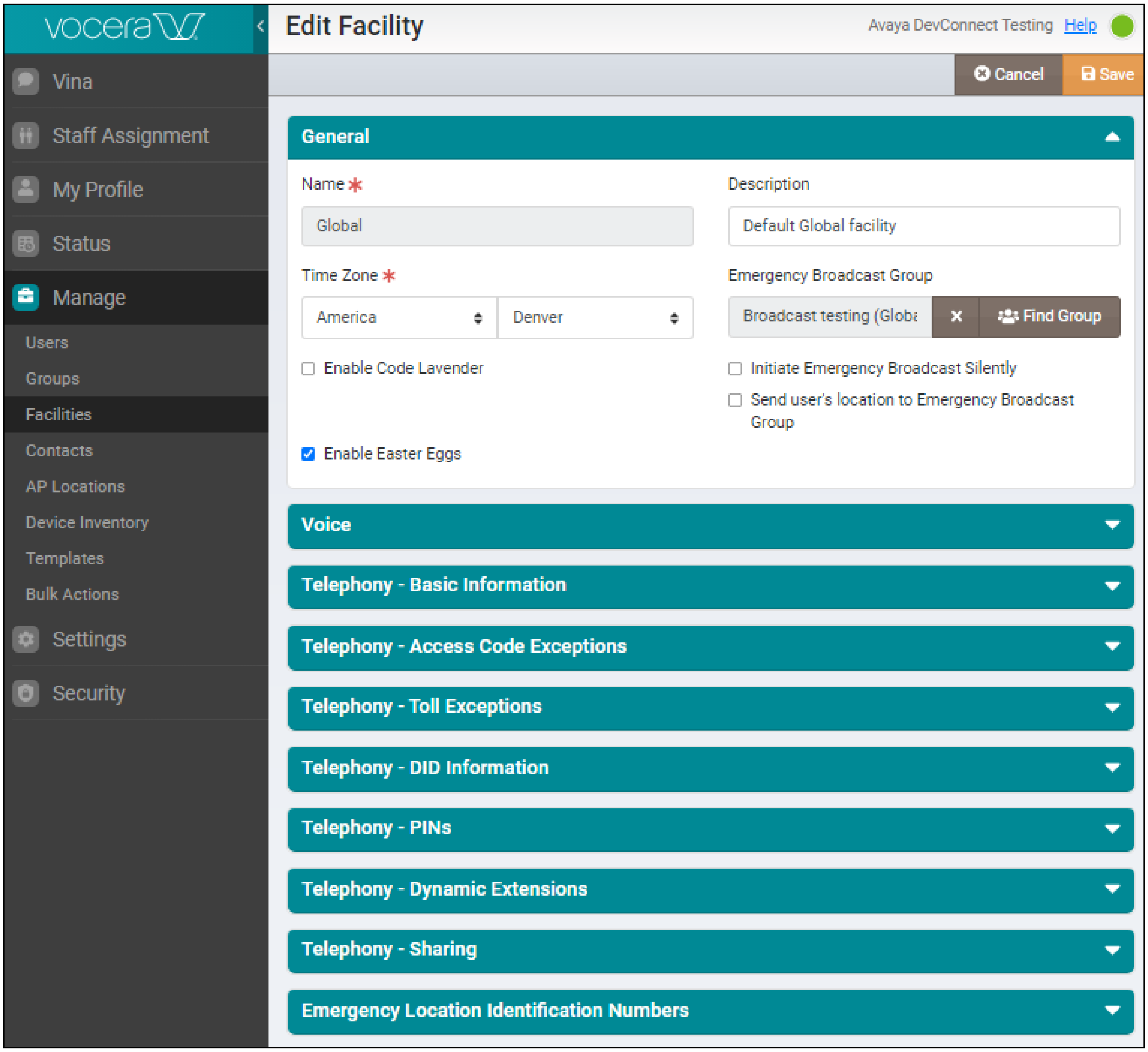


7.1 Configure SIP Telephony

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.

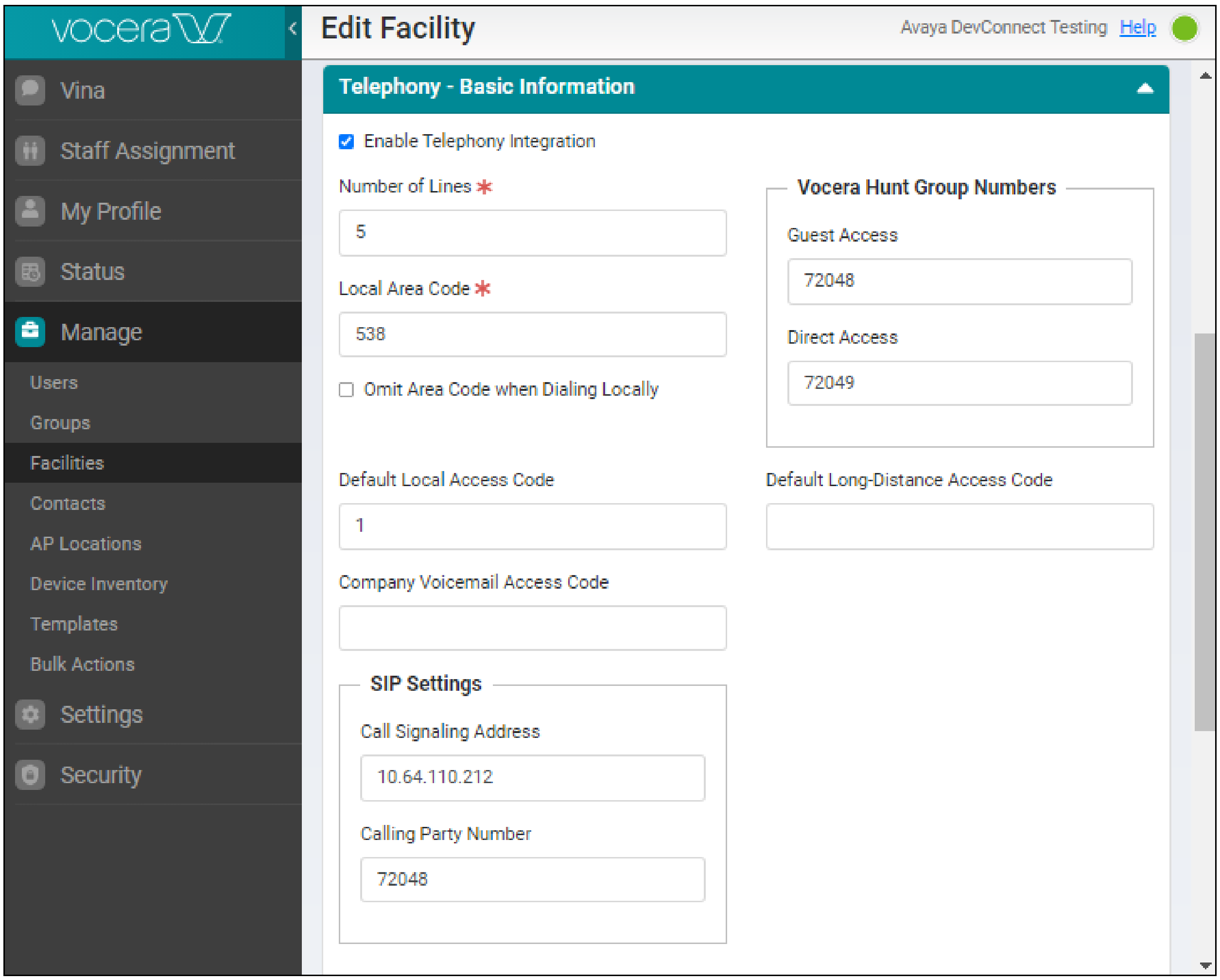


The **Edit Facility** webpage is displayed as shown below.

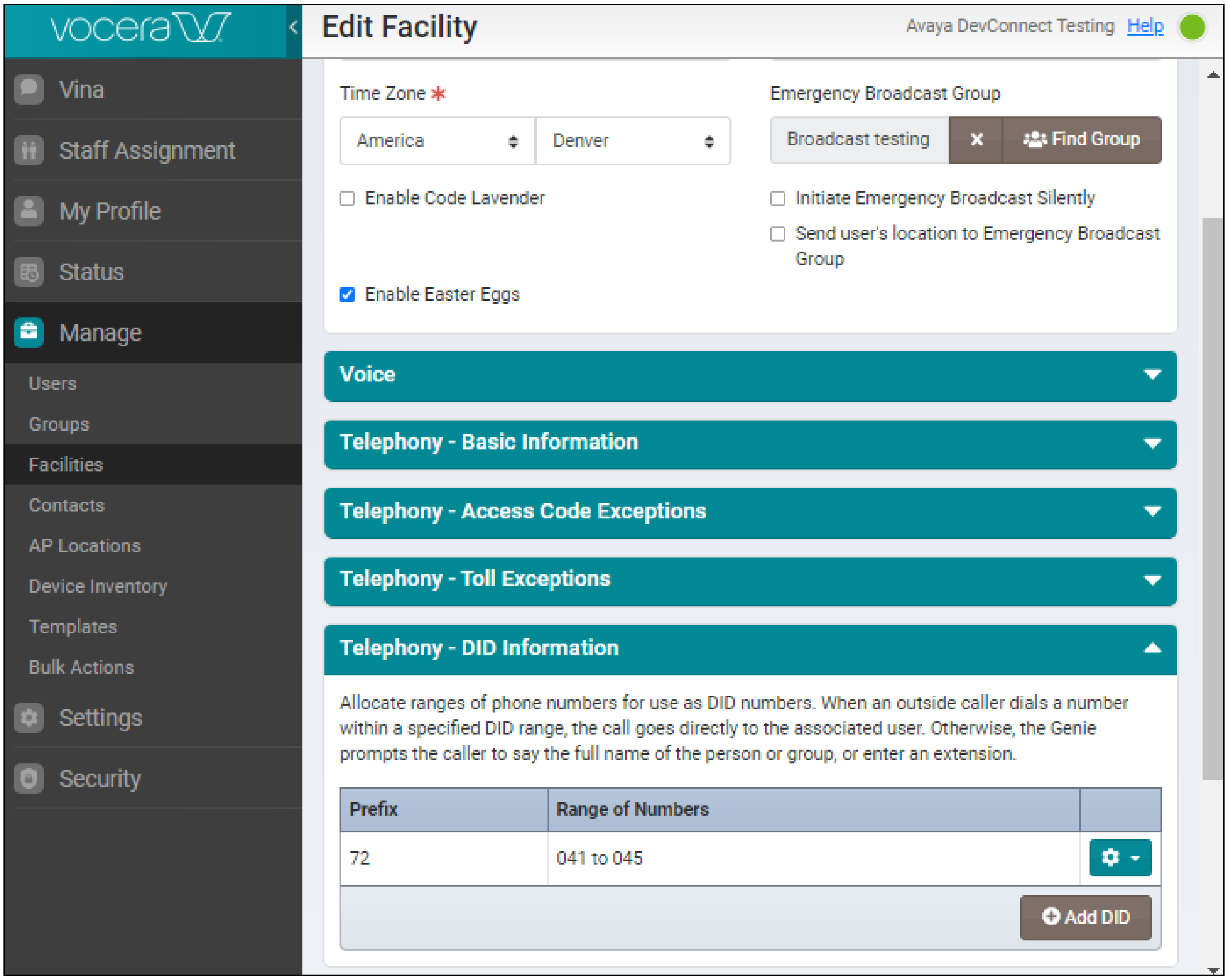


Expand the **Telephony – Basic Information** section and configure the following paramters.

- **Number of Lines:** Specify the number of lines for the SIP trunk (e.g., *5*).
- **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.

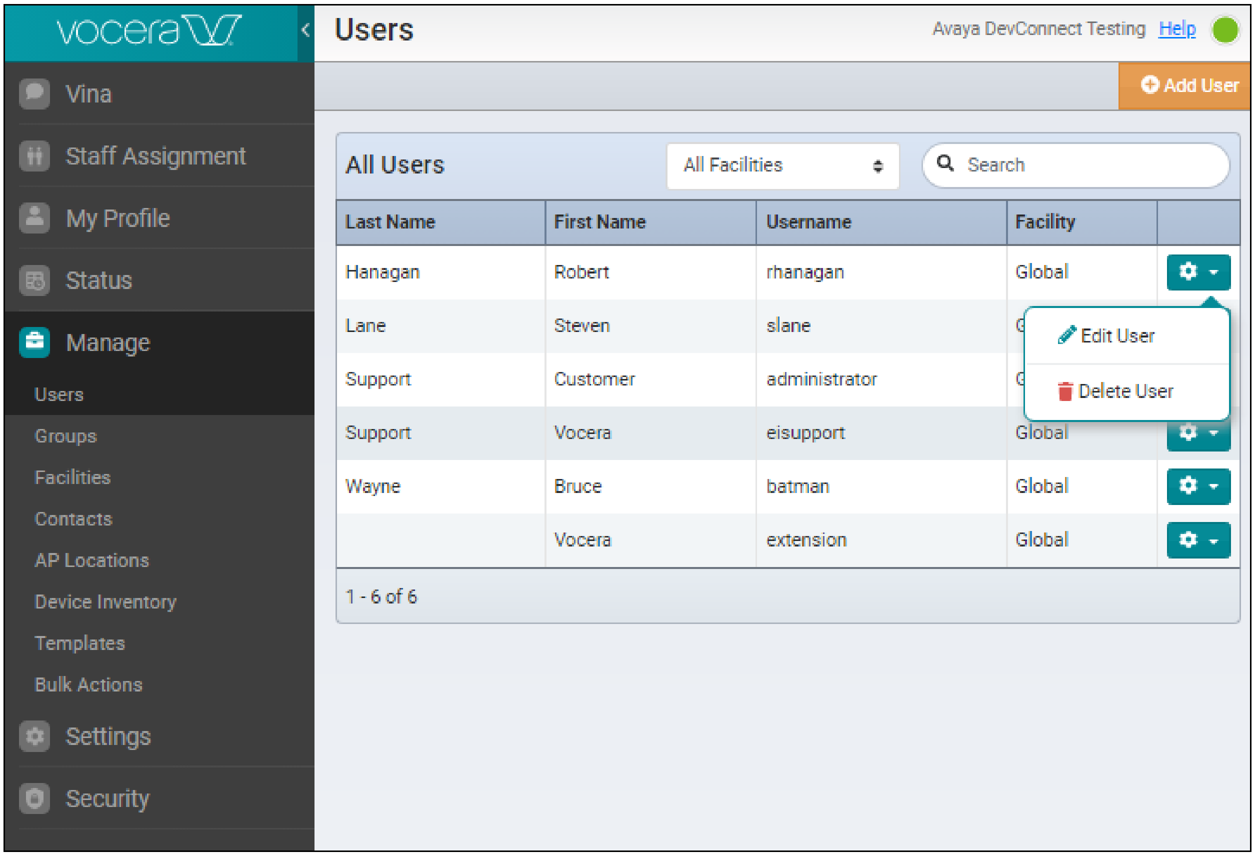


Expand the **Telephony – DID Information** to configure the range of numbers to be assigned to users with badges. For the compliance test, 5-digit extensions starting with “72” were used to route calls directly to badges. The leading two digits (i.e., *72*) was assigned as the **Prefix** and the last three digits were assigned to badges as extensions (e.g., *041* to *045*).

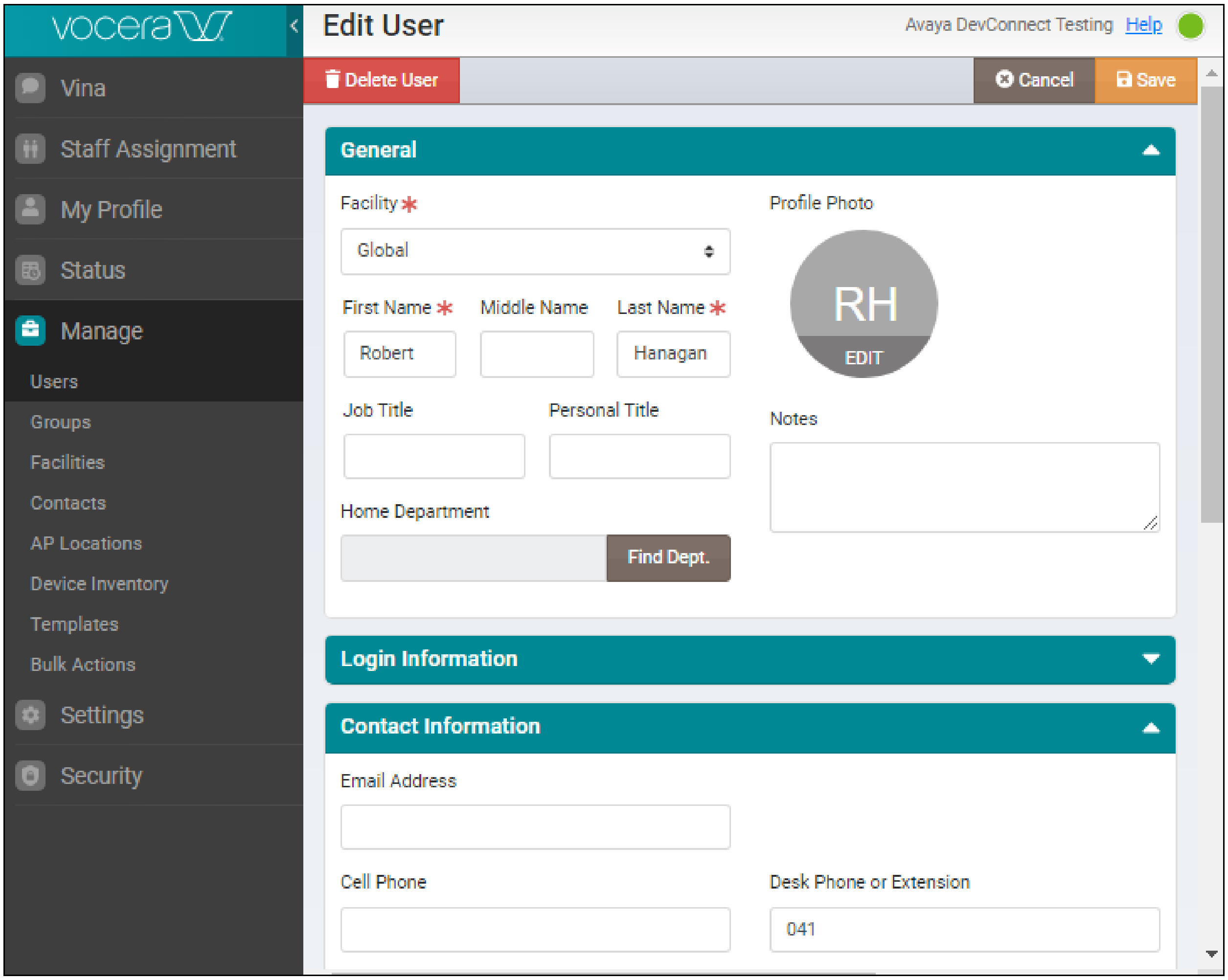


7.2 Configure Users

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**.



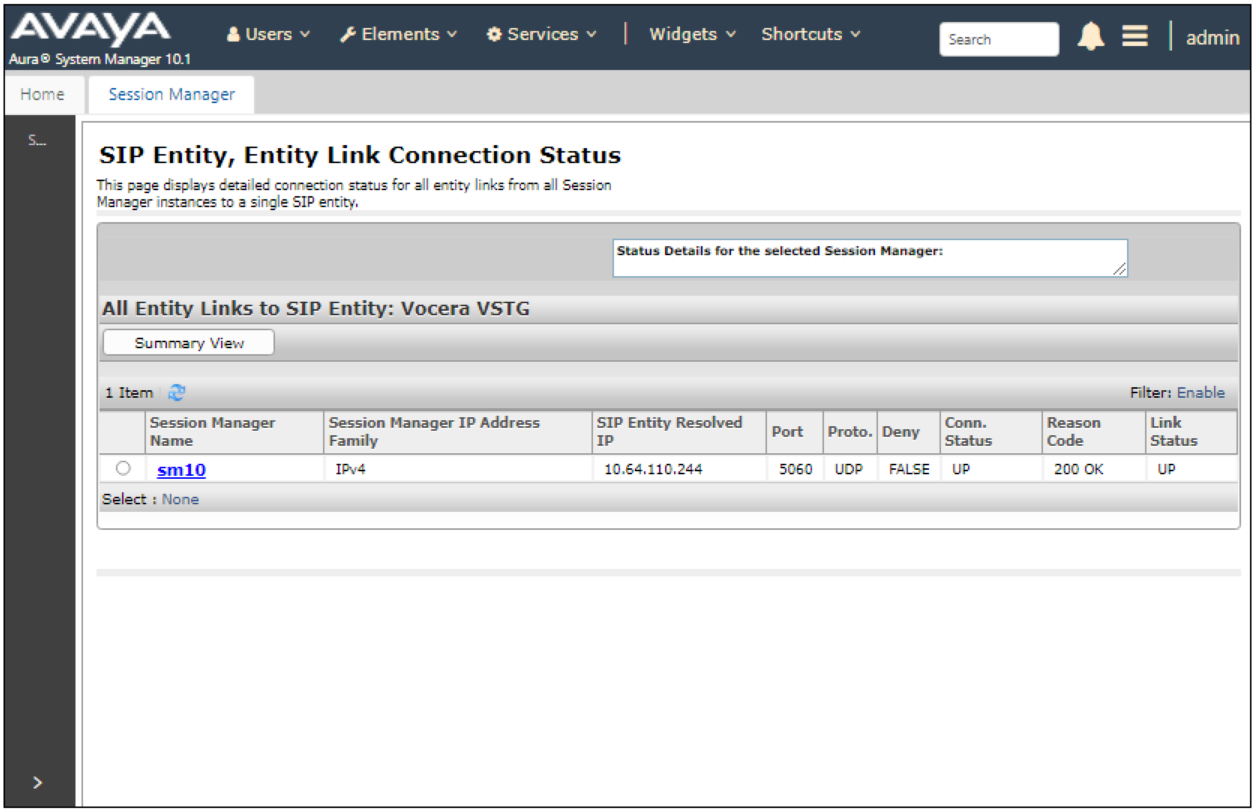
In the **Edit User** webpage, expand the **Contact Information** section and assign an extension in the **Desk Phone or Extension** field. In this example, extension *041* was assigned. The range of valid extensions was configured in **Section 7.1**.



7.3 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 **Elements→Session Manager→System Status→SIP Entity Monitoring** on System Manager. Below is the status of the SIP trunk to the Vocera Platform.



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.

8 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**.

9 References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 1, December 2021, available at http://support.avaya.com.

[2] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022, available at http://support.avaya.com.

[3] *Vocera Platform Telephony Guide*, Version 6.5.0, available on Vocera Documentation Portal at http://pubs.vocera.com/portal/index.html.

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.