Avaya Solution & Interoperability Test Lab

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

## Abstract

These Application Notes describe the procedure for configuring Vocera Communications to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager.

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

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

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

# 1. Introduction

These Application notes describe the steps to configure Session Initiation Protocol (SIP) trunking utilizing TCP / UDP between Vocera Communications and an Avaya Aura® Session Manager. The Avaya enterprise solution consists of Avaya Aura® Communication, Avaya Aura® Session Manager, and various Avaya endpoints.

Vocera Communications Solution is comprised of three main components:

- Vocera Badges
- Vocera Server
- Vocera SIP Telephony Gateway

The Vocera Badges are wireless 802.11a/b/g/n devices that serve as communicators in a wireless environment. By pressing the call button on a badge, a user can interface with the Vocera Server to start the call process. The Vocera badge model, B3000N, has 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 (VSTG) 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 the Avaya enterprise solution, as well as route calls to the PSTN 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 VSTG will be hosted on a Virtual Machine.

For additional information on Vocera Communication System, please refer to **[3-5]**.

# 2. General Test Approach and Test Results

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

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

## 2.1. Interoperability Compliance Testing

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

- Verify basic network connectivity
  - Badges to Access Point
  - SIP Trunk using TCP between Vocera and Avaya
  - SIP Trunk using UDP between Vocera and Avaya
- Basic calls (verifying proper set up and tear down of the calls), the phones and badges displayed Caller ID information, and voice paths/quality
  - Badge to Badge
  - Badge to Phone (H.323/SIP/PSTN)
  - Phone to Badge (H.323/SIP/PSTN)
- Audio codec negotiation using G.711MU and G.711A
- Voice Features
  - Call Transfer
  - Call Conference
  - Call Hold/Resume
- DTMF transmission using RFC 2833

Serviceability testing focused on verifying the ability of Vocera SIP Telephony Gateway, 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.

## 2.3. Support

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

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

# 3. Reference Configuration

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

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

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

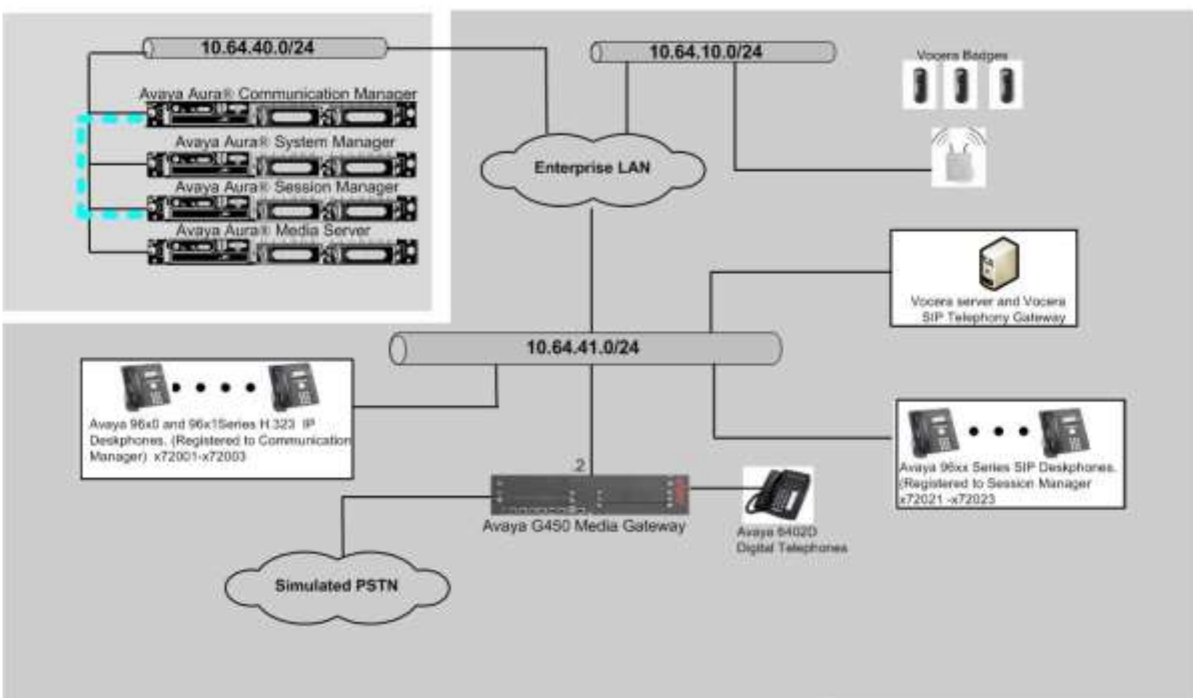



**Figure 1: Vocera Communications Test Configuration**

# 4. Equipment and Software Validated

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

| Equipment/Software | | Release/Version |
|---|---|---|
| Avaya Aura® Communication Manager in a<br>Avaya G450 Media Gateway<br>Avaya Aura® Media Server | | 7.0.1(R017x.00.0.441.0 – 23012) –FP1<br>37.19.0<br>7.7.0.226 |
| Avaya Aura® System Manager | | 7.0.1.0.64859 |
| Avaya Aura® Session Manager | | 7.0 |
| Avaya 96x1 Series Deskphones | | |
| | 9641 (SIP)<br>9611(SIP) | 7.0.0.39<br>7.0.0.39 |
| Avaya 96xx Series Deskphones | | |
| | 9621G (H.323)<br>9650C (H.323) | 6.6.115<br>3.25 |
| Vocera Communications<br>• Vocera Server & Telephony Server OS<br>• Vocera Server<br>• Vocera SIP Telephony Gateway<br>• Vocera Badges | | <br>Windows 2012 R2<br>5.2.0.266<br>5.2.0.266<br>B3000N 4.1.0.55 |

# 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

## 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 **20** 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  12
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  17
           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  1
                       Maximum Administered SIP Trunks: 4000  20
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    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. During the compliance test, G.711MU and G.711A were tested.

```
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:
 3:
 4:
 5:
 6:
 7:

     Media Encryption                  Encrypted SRTCP: enforce-unenc-srtcp
 1: none
 2:
 3:
 4:
 5:
```

## 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: 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: 16390                       IP Audio Hairpinning? n
   UDP Port Max: 16999
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 **SM70** with IP Address **10.64.40.226**.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
SM70                10.64.40.226
```

## 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 5.3**
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connections:** **y**

```
add signaling-group 92                                          Page   1 of   2
                                SIGNALING GROUP

 Group Number: 92             Group Type: sip
  IMS Enabled? n        Transport Method: tls
        Q-SIP? n
     IP Video? y          Priority Video? y        Enforce SIPS URI for SRTP? y
  Peer Detection Enabled? y  Peer Server: SM
 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: SM70
 Near-end Listen Port: 5061                 Far-end Listen Port: 5061
                                         Far-end Network Region: 1

Far-end Domain:
                                            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., **SM70** )
- **TAC**: Set to any available trunk access code that is valid in the provisioned dial plan. (e.g., **1092)**
- **Service Type**: **tie**
- **Signaling Group**: **92** (Signaling group added in **Section 5.5**)
- **Number of Members**: **10** (Enter a desired value for trunk group members)

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

```
add trunk-group 92                                                Page   1 of  21
                                TRUNK GROUP

Group Number: 92                   Group Type: sip          CDR Reports: y
  Group Name: SM70                        COR: 1        TN: 1        TAC: 1092
   Direction: two-way        Outgoing Display? y
 Dial Access? n                                   Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n
                                            Member Assignment Method: auto
                                                     Signaling Group: 92
                                                   Number of Members: 10
```

On **Page3**, the **Numbering Format** field is set to ***private***.

```
add trunk-group 92                                                Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                         Maintenance Tests? y



   Suppress # Outpulsing? n  Numbering Format: private
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? y
                                               Replace Unavailable Numbers? y

                                                 Hold/Unhold Notifications? y
                                Modify Tandem Calling Number: tandem-cpn-form




 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., **2SM70**)
- **Grp No:** The trunk group number from **Section 5.6 (**e.g., **92)**
- 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 92                                         Page   1 of   3
                    Pattern Number: 92     Pattern Name: 2SM70
    SCCAN? n    Secure SIP? n     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: 92   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                               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: y y y y y 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 4-digit extension beginning with 777 will be routed over any trunk group.

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

Ext Ext              Trk        Private           Total
Len Code             Grp(s)     Prefix            Len
 5  332                                           5     Total Administered: 3
 5  720                                           5        Maximum Entries: 540
 4  777                                           4
```

## 5.9. AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to the VSTG via the route pattern created in **Section 5.7**. Enter the **change aar analysis <x>** command, where **x** is a starting partial digit (or full digit). The dialed string created in the AAR Digit Analysis table should contain a map to the Vocera system extension, which is configured as 777xx. During the configuration of aar table, the Call Type field was set to **unku**.

```
change aar analysis 720                                        Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                   Location: all          Percent Full: 3

          Dialed           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    777                     5    5     92       unku           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.

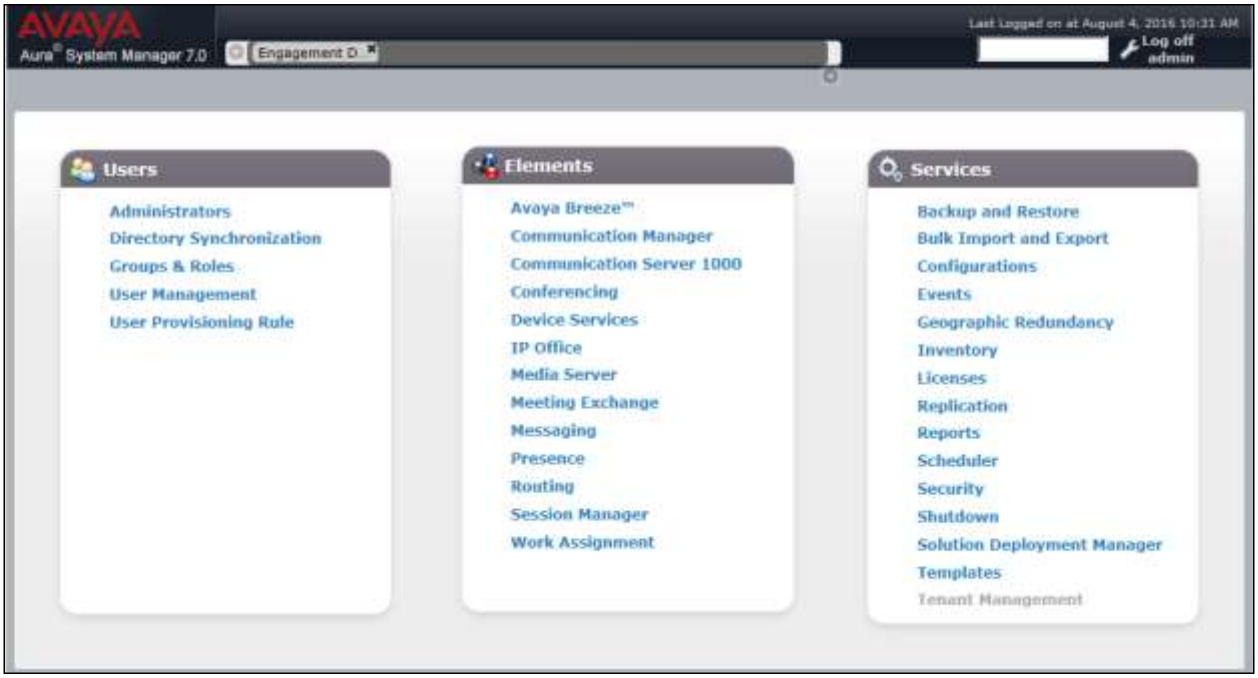
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

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

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

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

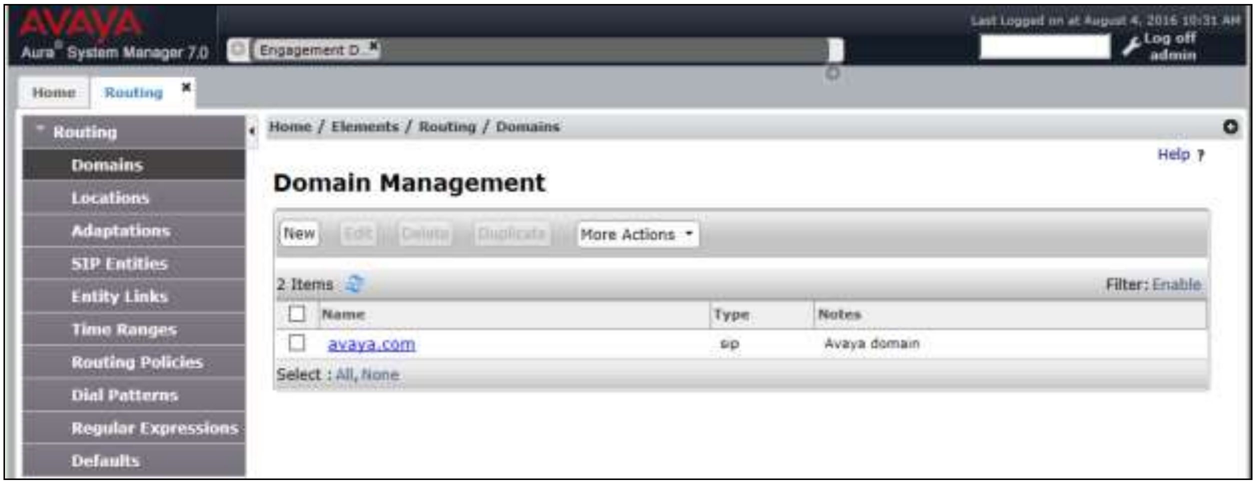
Log in using appropriate credentials. The main page for the administrative interface is shown below.



## 6.1. SIP Domains

In the reference configuration, one SIP domain was used; **avaya.com**.
Navigate to **Elements → Routing → Domains** and click the **New** (not shown) to add a new SIP domain with the following:

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



## 6.2. Locations

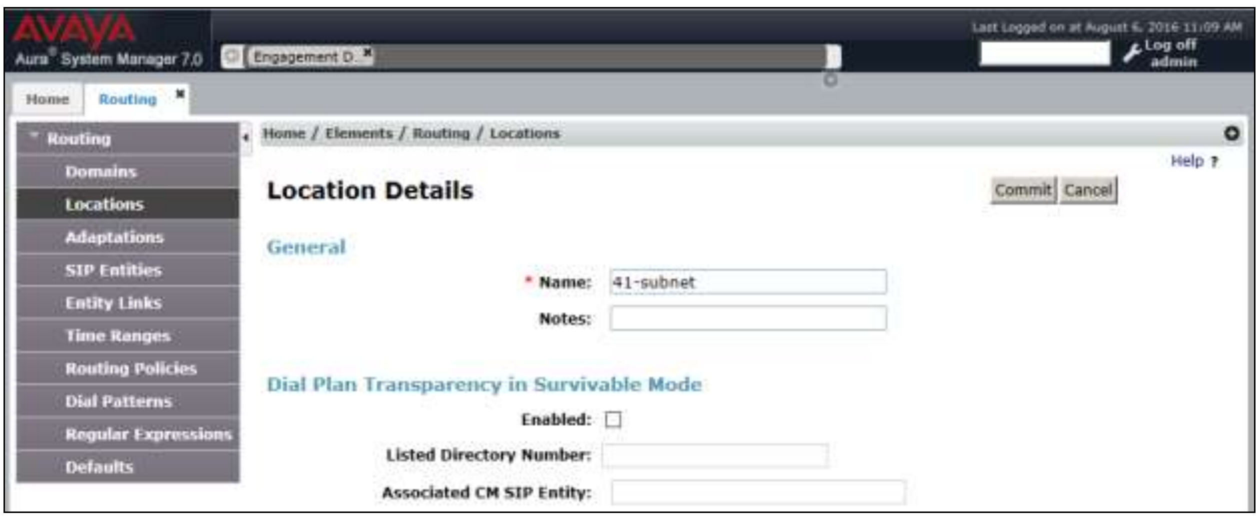
Locations are used to identify logical and/or physical locations where SIP Entities reside, by specifying the IP addressing for the locations as well as for purposes of bandwidth management if required.

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

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

Section **Location Pattern** (not shown)

- Click on **Add**.
- Enter the IP address information for the Location (e.g., **10.64.41.*)**
- Enter a description in the **Notes** field if desired
- Repeat steps in the Location Pattern section if the Location has multiple IP segments.
- Modify the remaining values on the form, if necessary; otherwise, use all the default values
- Click on the **Commit** button



## 6.3. SIP Entities

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

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

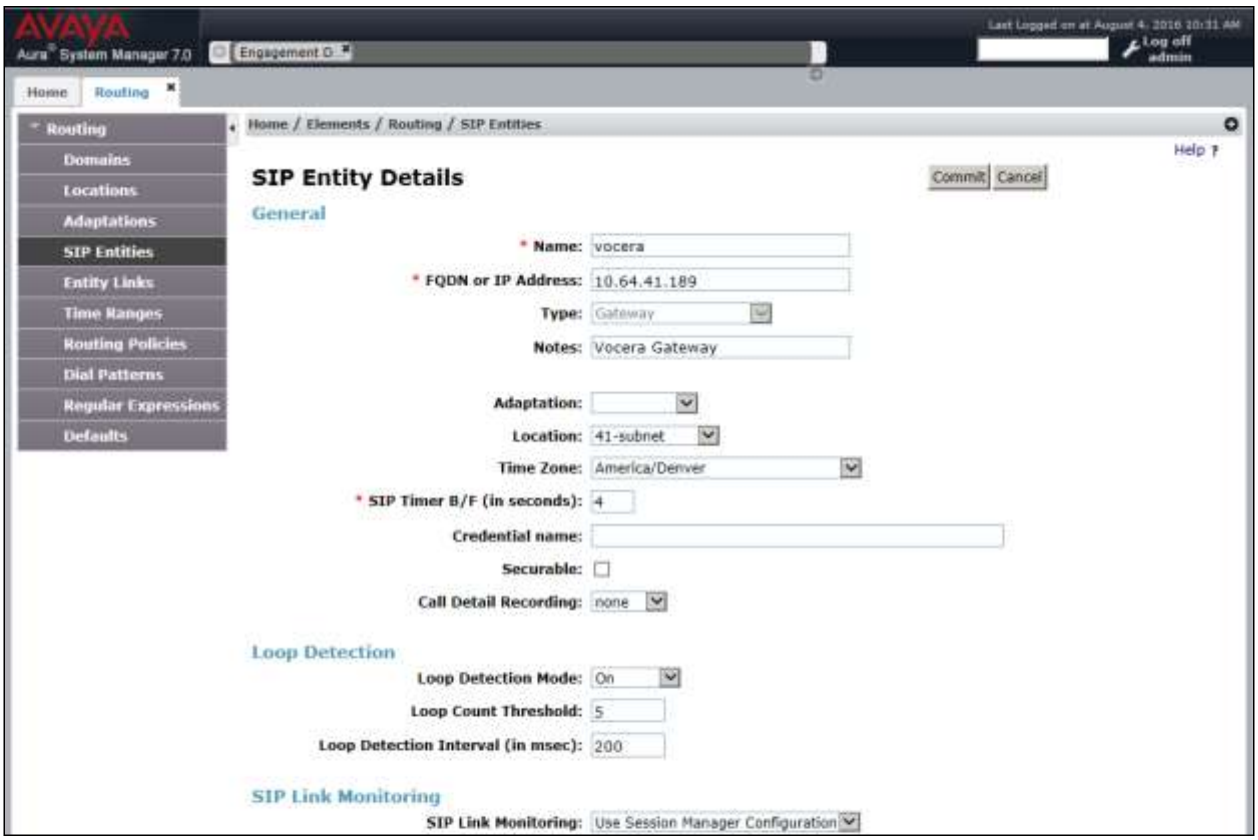
To add a SIP Entity, navigate to **Routing → SIP Entities** and click the **New** button (not shown). The configuration details for the SIP Entity defined for the Communication Manager are below:

<u>Section **General**</u>

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

<u>Section **SIP Link Monitoring**</u>

- Select a desired option



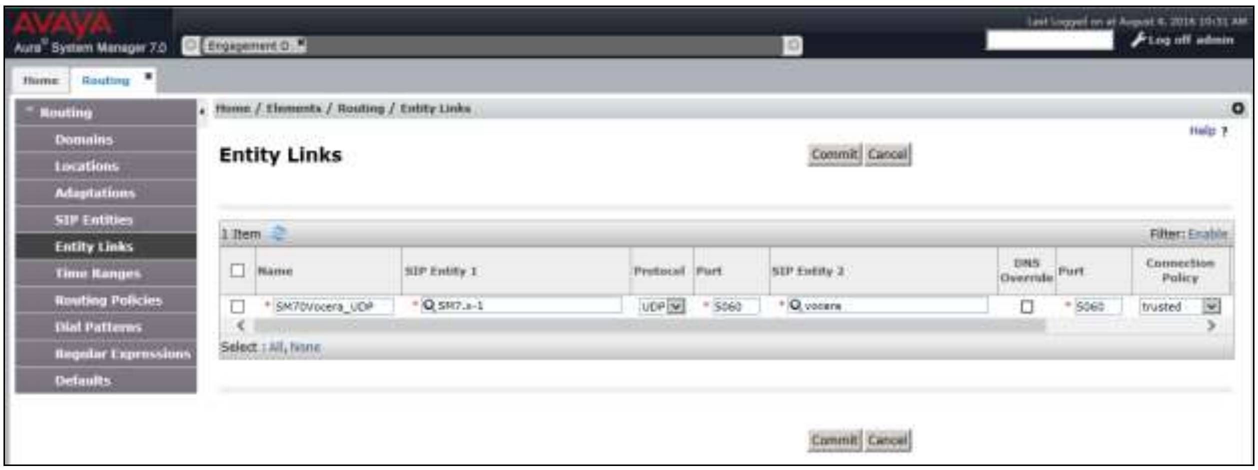

## 6.4. Add Entity Link

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

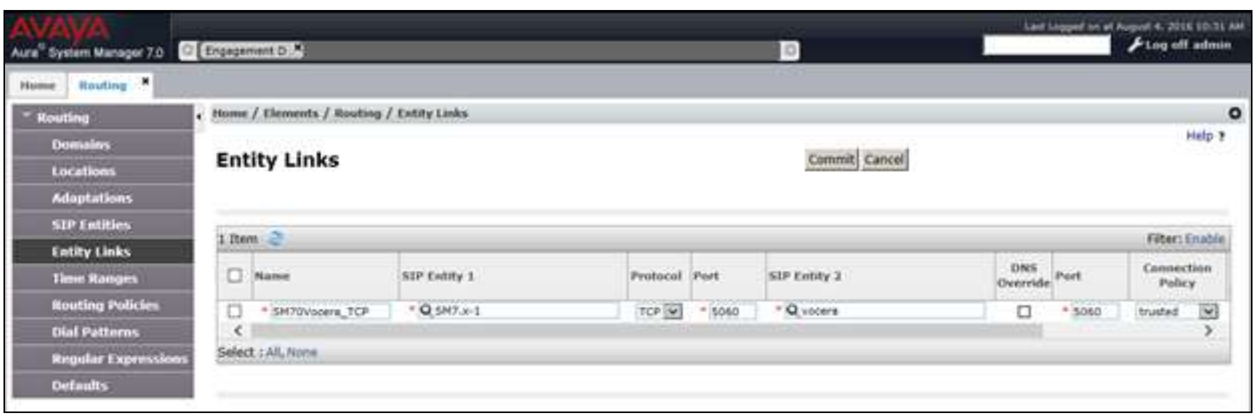
Navigate to **Routing → Entity Links**, and click the **New** button (not shown) to add a new Entity Link. The screen below shows the configuration details for the Entity Link connecting Session Manager with Vocera with UDP as the transport protocol.

- **Name**: a descriptive name
- **SIP Entity 1**: select the Session Manager SIP Entity
- **Protocol**: select UDP as the transport protocol
- **Port: 5060**. This is the port number to which the other system sends SIP requests
- **SIP Entity 2**: select the Vocera SIP Entity
- **Port: 5060**. This is the port number on which the other system receives SIP requests
- **Connection Policy**: select ***Trusted***
- **Notes**: optional descriptive text

Click **Commit** to save the configuration.




The following shows TCP protocol between Session Manager and Vocera SIP Telephony Gateway.




## 6.5. Routing Policies

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

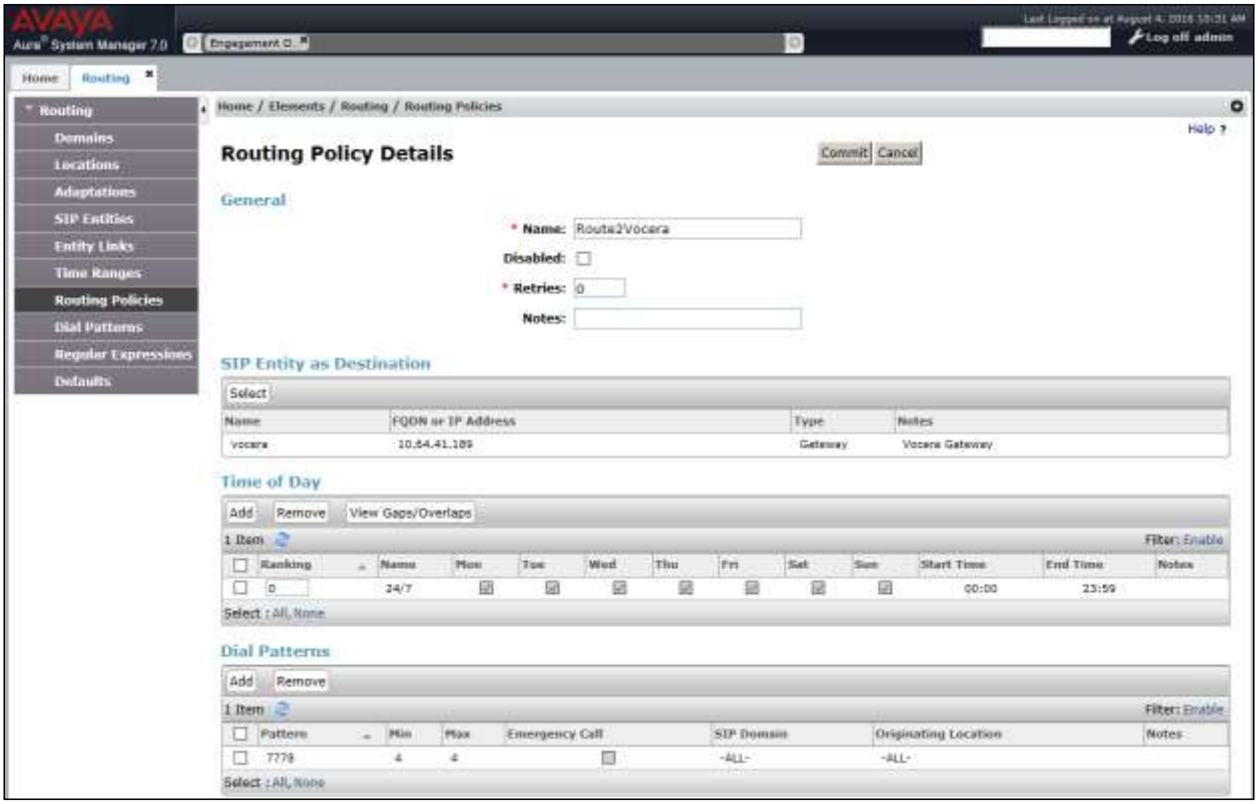
To add a Routing Policy, navigate to **Routing → Routing Policies**, and click on the **New** button (not shown) on the right. Provide the following information:

Section **General**

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

Section **SIP Entity as Destination**

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



## 6.6. Dial Patterns

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

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

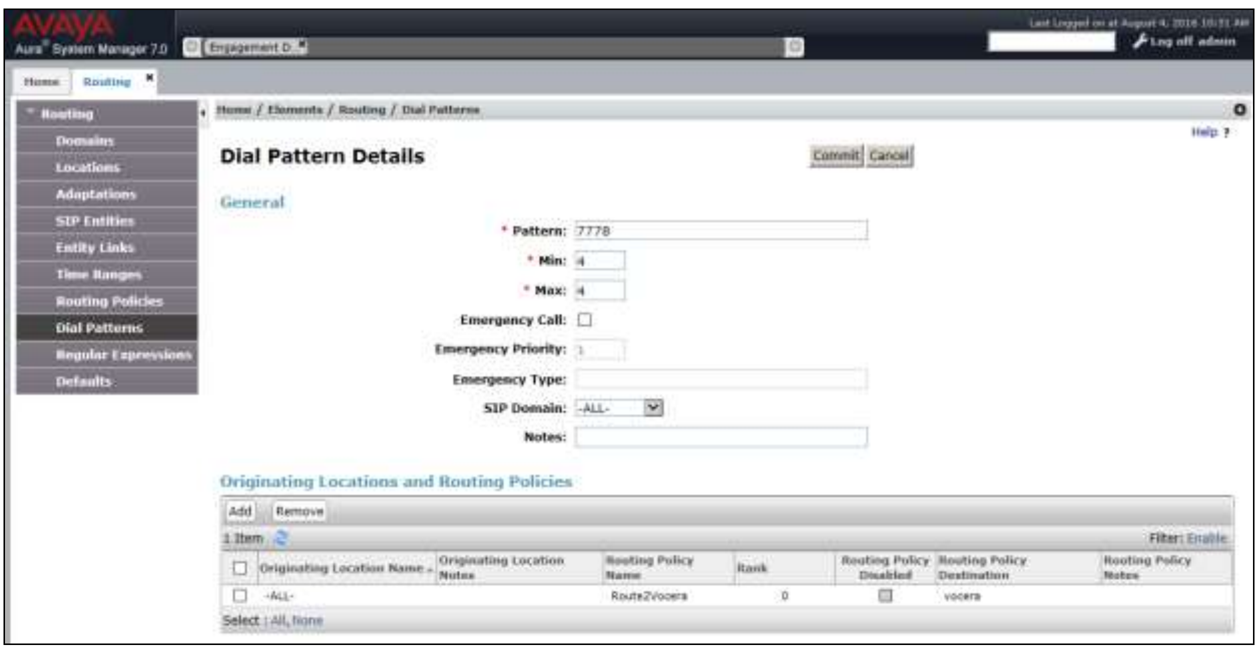
Section **General**.

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

Section **Originating Locations and Routing Policies**.

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

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



# 7. Configure Vocera Communications

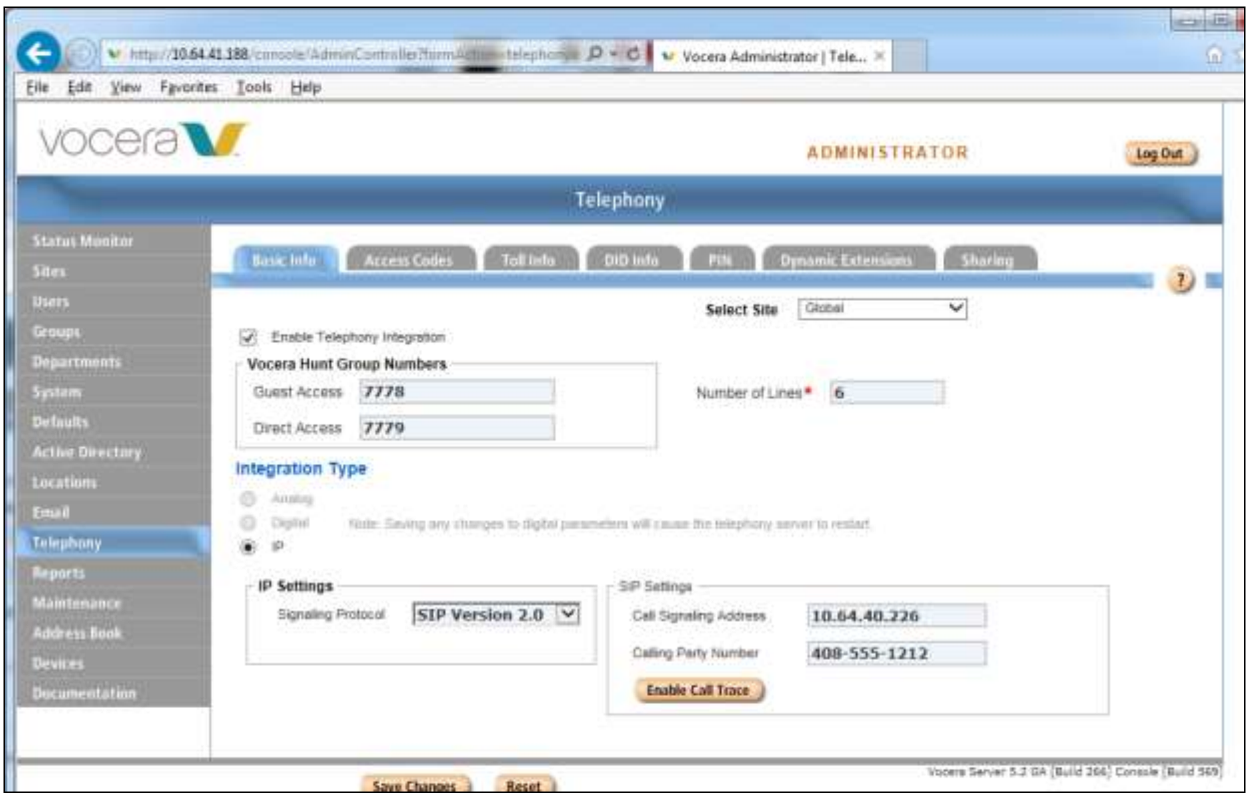
This section will only describe the basic configuration to interface with Avaya Aura® Session Manager. For configuration steps for Vocera Communications System, refer to **(3-5)** documentation.

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

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



## 7.2. User Configuration

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

- First Name
- Last Name
- User ID

Click the **Save** button.

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

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

## 7.3. Configure SIP OPTIONS

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

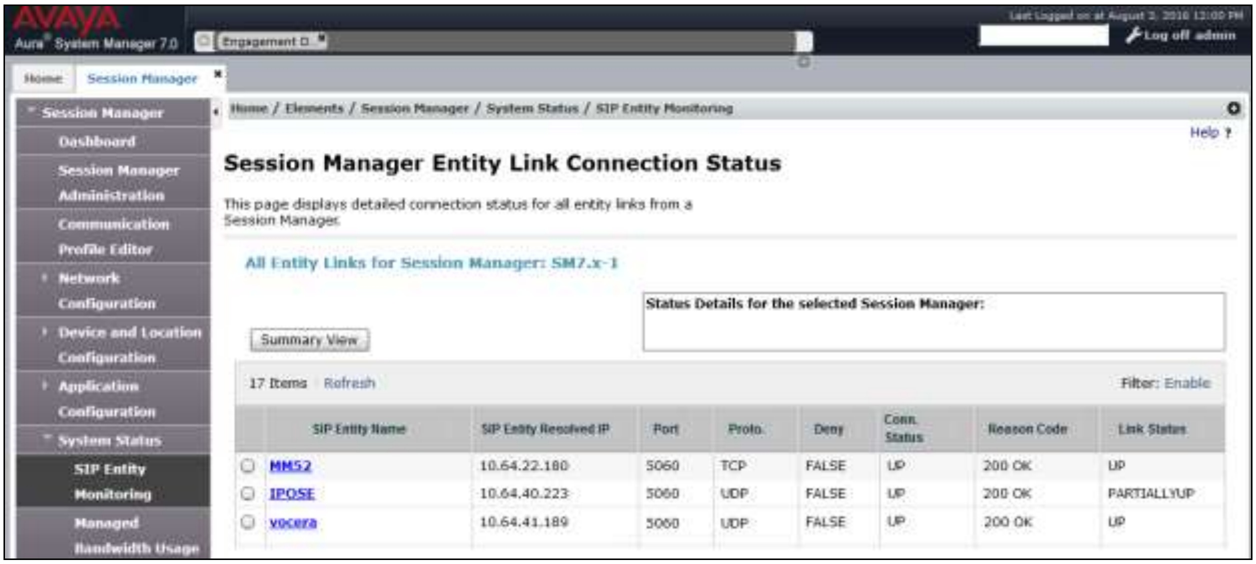
- VTGUseOPTIONSForKeepAlive = true
- VTGOPTIONSKeepAliveInterval = 30
- VTGOPTIONSKeepAliveToUser =
- VTGUseOPTIONSKeepAliveText = false

# 8. Verification Steps

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

## 8.1. Verify Avaya Aura® Session Manager

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




## 8.2. Verify Vocera Communications

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

- Place a call between Vocera Badges
- Place a call between a Vocera Badge and Avaya phone
- Place a call between a Vocera Badge and the PSTN

## 9. Conclusion

These Application Notes describe a sample configuration of how to configure Vocera Communications to interoperate with Avaya Aura® Session Manager via a SIP trunk using UDP/TCP as the transport. All feature and serviceability test cases were completed and passed.

## 10. Additional References

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


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

(2) *Administering Avaya Aura® System Manager for Release 7.0.1, Issue 2, Release 7.0.1, June 2016.*


The following document was provided by Vocera.


(3) *Vocera Telephony Configuration Guide, Version 5.2*

(4) *Vocera B3000 Badge Guide, Version 5.2*

(5) *Vocera Administration Guide Version 5.2*

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.