Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Vocera Communications using TCP and UDP as the Transport Protocol with Avaya Aura® Session Manager 6.1 and Avaya Aura® Communication Manager 6.0.1 – 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 Digital.

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

1. Introduction

These Application notes describe the steps to configure Session Initiation Protocol (SIP) Trunking utilizing TCP and UDP, between Vocera Communications and an Avaya SIP-enabled enterprise solution. The Avaya enterprise solution consists of Avaya Aura® Communication 6.0.1 and Avaya Aura® Session Manager 6.1.

Vocera Communications Solution is comprised of three main components:

- Vocera Badges
- Vocera Server
- Vocera SIP Telephony Gateway

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

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

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

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

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

2. General Test Approach and Test Results

The focus of the interoperability compliance testing was to verify the ability of the Vocera 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, H.323 and Digital.

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

2.1. Interoperability Compliance Testing

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

- Verify basic network connectivity
    - Badges to Access Point
    - SIP Trunk using 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
    - Phone to Badge
- Audio codec negotiation using G.711MU and G.711A
- Voice Features
    - Call Transfer
    - Call Conference
    - Call Hold/Resume
    - Badge Emergency Broadcast all Badges
- 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 with the following exceptions/observations noted.

- Vocera performs SIP Options to SIP user agent (end-point) and not the SIP proxy server. When the UA wouldn't respond, or was incapable of responding, Vocera would mark the SIP Trunk out-of-service. SIP Options can be disabled. Vocera does have a fix available.
- Vocera is using RFC 5373 for Answer-Mode. When the supported feature is sent in the invite with answer-mode type Manual, Avaya 96x0 and 96x1 IP Phones configured as SIP, would auto-answer. The issue has been identified with the Avaya endpoints and an enhancement request has been submitted.

2.3. Support

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

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

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of the following.

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

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

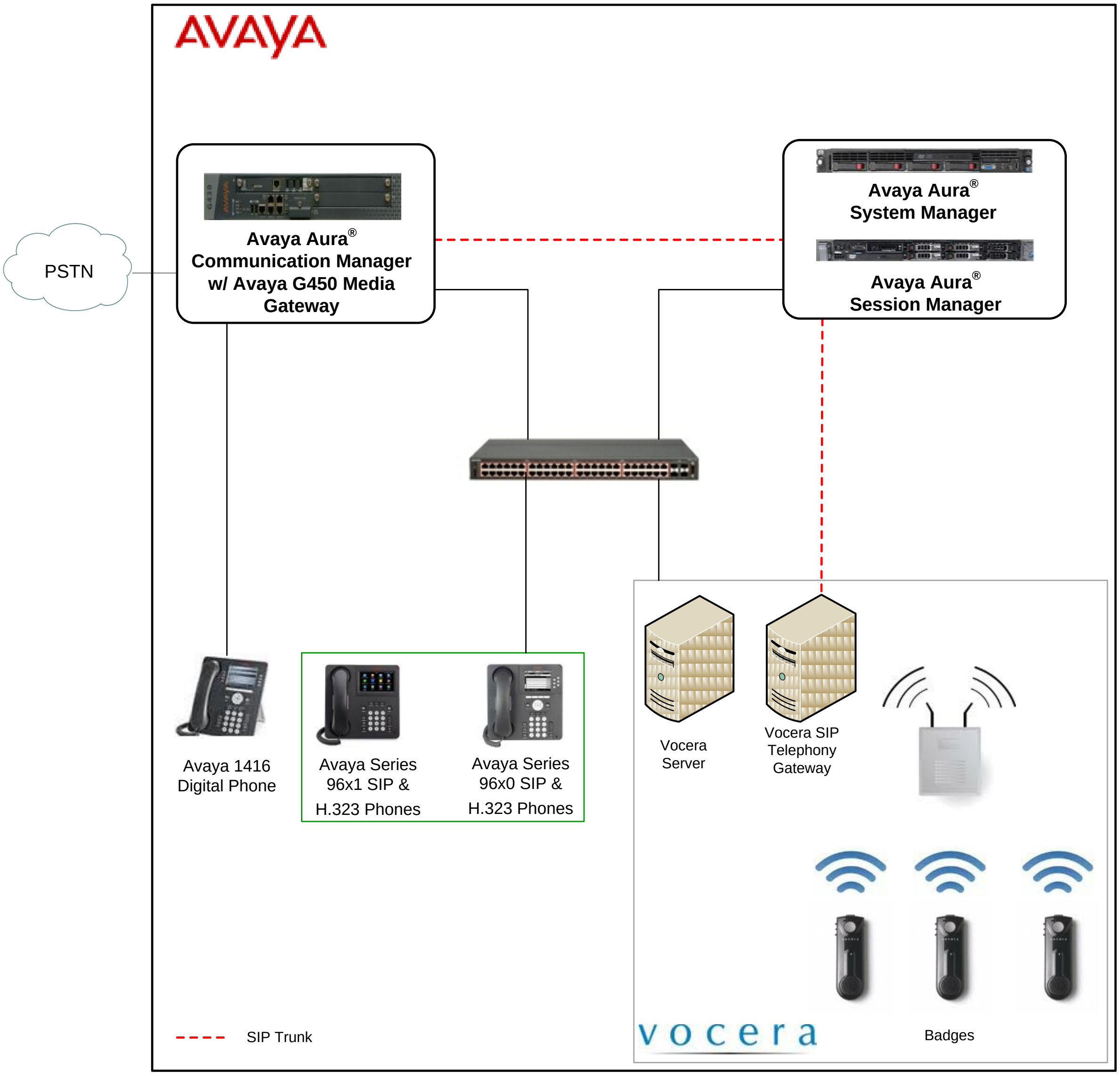

AVAYA
PSTN
Avaya Aura® Communication Manager w/ Avaya G450 Media Gateway
Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya 1416 Digital Phone
Avaya Series 96x1 SIP & H.323 Phones
Avaya Series 96x0 SIP & H.323 Phones
Vocera Server
Vocera SIP Telephony Gateway
vocera
Badges
SIP Trunk

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 with Avaya Communication Manager Messaging running on Avaya S8300 Server with an Avaya G450 Media Gateway	6.0.1 SP7 (R016x.00.1.510.1-19528)
Avaya Aura® Session Manager running on HP ProLiant DL360 G7 Server	6.1 SP7 (6.1.7.0.617012)
Avaya Aura® System Manager running on HP ProLiant DL360 G7 Server	6.1 SP8 (Build No. - 6.1.0.0.7345-6.1.5.803 Software Update Revision No: (6.1.12.1.1906)
Avaya 96x0 Series IP Telephones (SIP) • 9650 Avaya 96x0 Series IP Telephones (H.323) • 9630	2.6 SP7 3.1 SP4
Avaya 96x0 Series IP Telephones (SIP) • 9650 Avaya 96x0 Series IP Telephones (H.323) • 9630	2.6 SP7 3.1 SP4
Avaya 96x1 Series IP Telephones (SIP) • 9611 • 9621 • 9641 Avaya 96x1 Series IP Telephones (H.323) • 9608 • 9641	6.0 SP4 6.2 SP1
Avaya1416 Digital Telephone	-
Vocera Communications • Vocera Server & Telephony Server OS • Vocera Server • Vocera SIP Telephony Gateway • Vocera Badges	Windows Server 2008 R2 – 6.1 4.3 SP1 build 2349 4.3 SP1 build 2349 B3000-fw 129

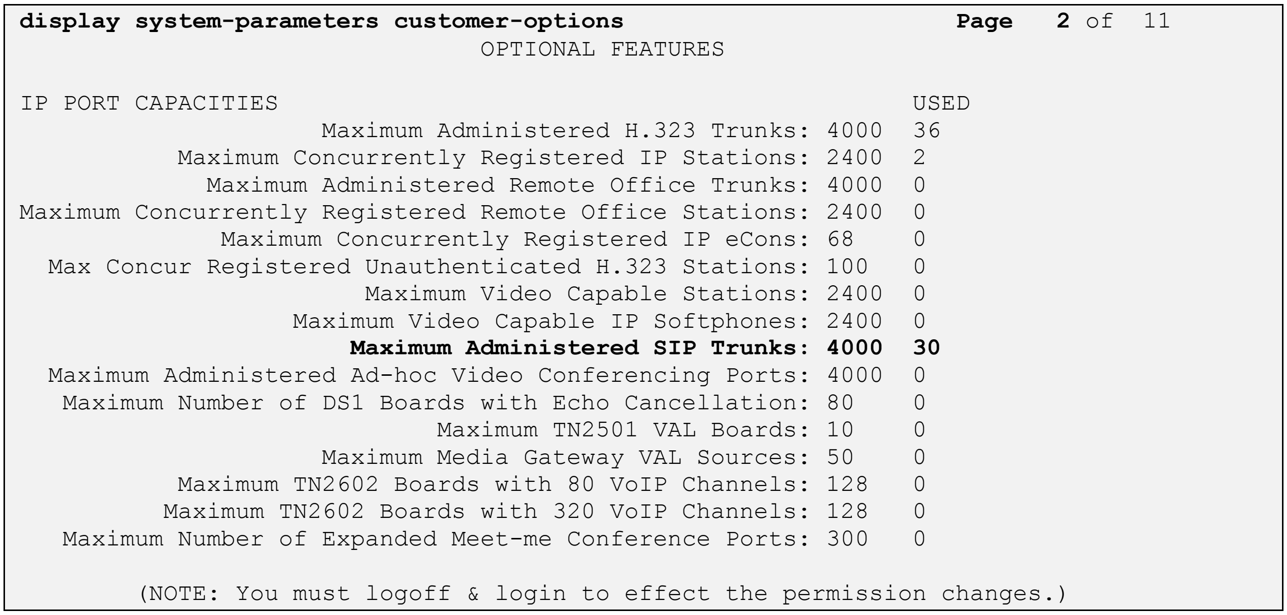
5. Configure Avaya Aura® Communication Manager

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

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

5.1. Verify Avaya Aura® Communication Manager License

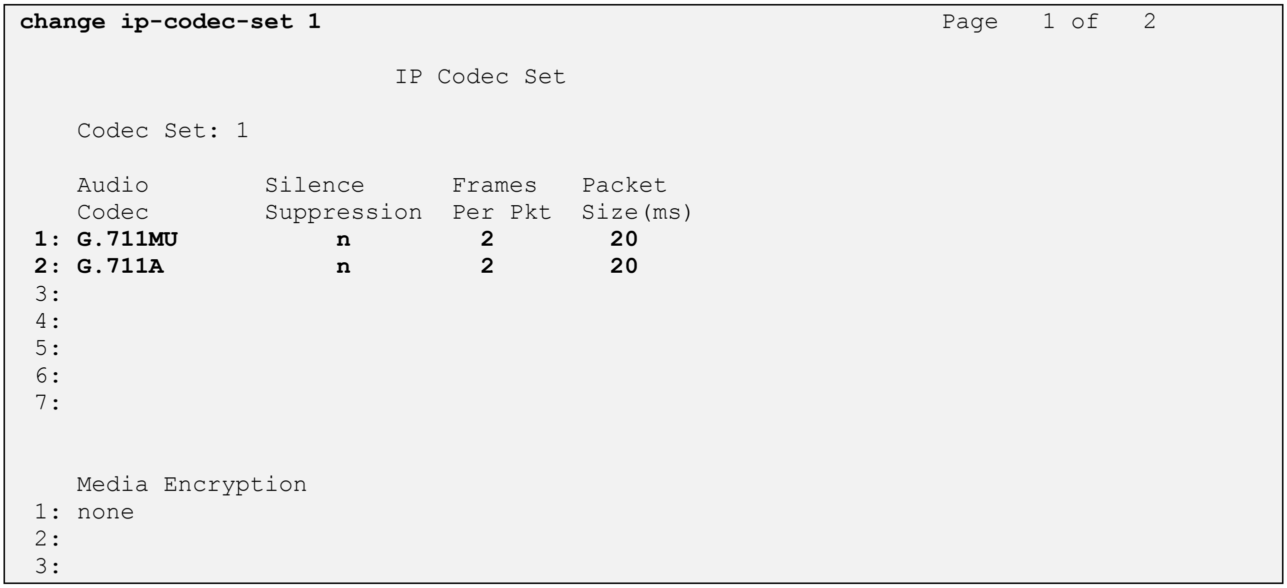
Use the **display system-parameters customer-options** command and on **Page 2,** verify that the **Maximum Administered SIP Trunks** value is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example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



```
display system-parameters customer-options                      Page   2 of  11
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                            USED
                     Maximum Administered H.323 Trunks: 4000  36
           Maximum Concurrently Registered IP Stations: 2400  2
             Maximum Administered Remote Office Trunks: 4000  0
Maximum Concurrently Registered Remote Office Stations: 2400  0
              Maximum Concurrently Registered IP eCons: 68    0
  Max Concur Registered Unauthenticated H.323 Stations: 100   0
                        Maximum Video Capable Stations: 2400  0
                   Maximum Video Capable IP Softphones: 2400  0
                       Maximum Administered SIP Trunks: 4000  30
  Maximum Administered Ad-hoc Video Conferencing Ports: 4000  0
   Maximum Number of DS1 Boards with Echo Cancellation: 80    0
                             Maximum TN2501 VAL Boards: 10    0
                     Maximum Media Gateway VAL Sources: 50    0
           Maximum TN2602 Boards with 80 VoIP Channels: 128   0
          Maximum TN2602 Boards with 320 VoIP Channels: 128   0
   Maximum Number of Expanded Meet-me Conference Ports: 300   0

        (NOTE: You must logoff & login to effect the permission changes.)
```

5.2. IP Codec Set

This section describes the steps for administering an IP codec set in Communication Manager. This IP codec set is used in the IP network region for communications between Communication Manager and Session Manager. Use the **change ip-codec-set <c> command**, where **c** 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.



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

                          IP Codec Set

    Codec Set: 1

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


    Media Encryption
 1: none
 2:
 3:
```

5.3. IP Network Region

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

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

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

5.4. IP Node Names

This section describes the steps for setting the IP node name for Session Manager in Communication Manager. Use the **change node-names ip** command, and add a node name for Session Manager signaling. The node name for Session Manager is **sm_60_19** with IP Address **10.64.60.19**. Note: The **procr / 10.64.60.13** entries, which are the node name / IP address for the processor board. It will be used later to configure the SIP Trunk in Session Manager.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
default             0.0.0.0
msgserver           10.64.60.13
procr               10.64.60.13
procr6              ::
sm_60_19            10.64.60.19
```

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 name from **Section 5.4**
- **Near-end Listen Port:** **5061**
- **Far-end Node Name:** Session Manager node name from **Section 5.4**
- **Far-end Listen Port:** **5061**
- **Far-end Network Region**: The IP network region number from **Section 5.4**
- **DTMF over IP:** **rtp-payload**
- **Direct IP-IP Audio Connections:** **y**

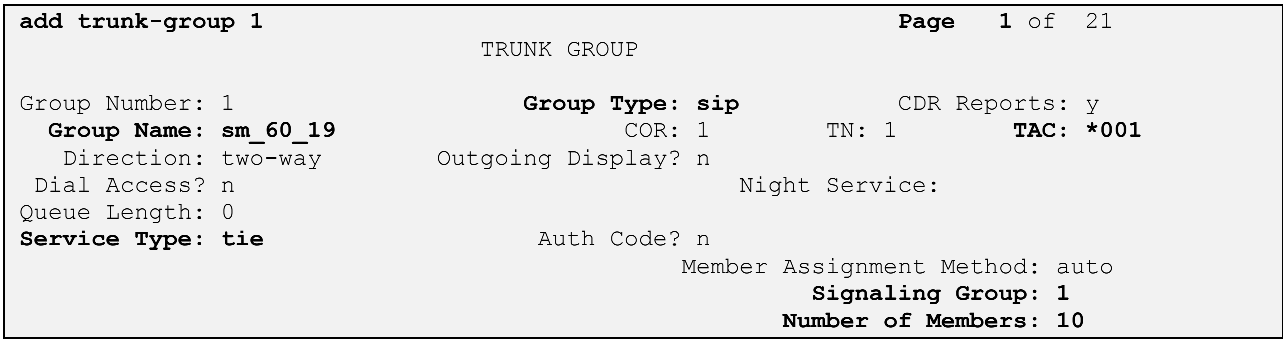
```
add signaling-group 1                                        Page   1 of   1
                                SIGNALING GROUP

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



   Near-end Node Name: procr                 Far-end Node Name: sm_60_19
 Near-end Listen Port: 5061                Far-end Listen Port: 5061
                                        Far-end Network Region: 1

Far-end Domain: avaya.com
                                             Bypass If IP Threshold Exceeded? N



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

5.6. SIP Trunk Group

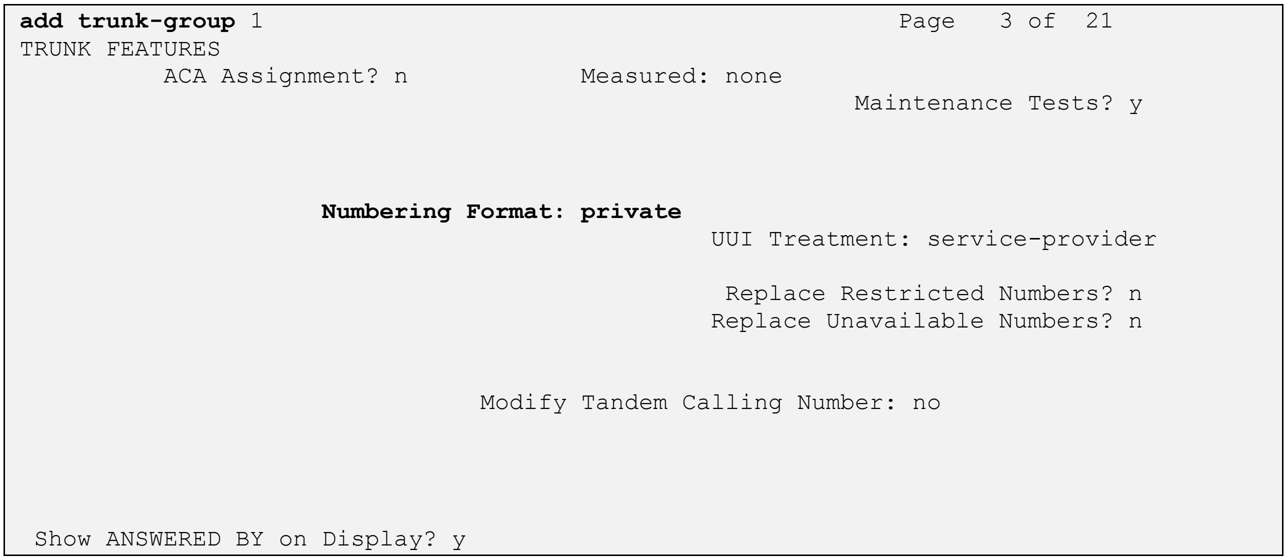
This section describes the steps for administering a trunk group in Communication Manager for communication between Communication Manager and Session Manager. Use the **add trunk-group <t>** command, where **t** is an available trunk group number.

- **Group Type**: **sip**
- **Group Name**: Enter a descriptive name (e.g., **sm_60_19**)
- **TAC**: Set to any available trunk access code that is valid in the provisioned dial plan (e.g., ***001)**
- **Service Type**: **tie**
- **Signaling Group**: **1** (Signaling group added in **Section 5.5**)
- **Number of Members**: **10** (Enter a desired value for trunk group members)
- **Numbering Format:** **private**

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



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

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: sm_60_19                    COR: 1        TN: 1        TAC: *001
   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
```



```
add trunk-group 1                                            Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: private
                                                UUI Treatment: service-provider

                                                 Replace Restricted Numbers? n
                                                Replace Unavailable Numbers? n


                                Modify Tandem Calling Number: no




 Show ANSWERED BY on Display? y
```

5.7. Route Pattern

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

- **Pattern Name:** A descriptive name (e.g., **sm_60_19**)
- **Grp No:** The trunk group number from **Section 5.6 (**e.g., **1)**
- Set the **FRL:** Enter a level that allows access to this trunk, with **0** being least restrictive

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 1   Pattern Name: sm_60_19
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                                DCS/ IXC
    No          Mrk Lmt List Del  Digits                                  QSIG
                             Dgts                                         Intw
 1: 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  No. Numbering LAR
    0 1 2 M 4 W     Request                                Dgts Format
                                                        Subaddress
 1: y y y y y n  n            rest                             lev0-pvt  none
 2: y y y y y n  n            rest                                       none
 3: y y y y y n  n            rest                                       none
 4: y y y y y n  n            rest                                       none
 5: y y y y y n  n            rest                                       none
 6: 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 5-digit extension beginning with 4 or a 5 will be routed over any trunk group, since the Trk Grp(s) field is blank this will result in a 5-digit calling number. The calling party number will be in the SIP "From" header.

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

Ext Ext              Trk        Private           Total
Len Code             Grp(s)     Prefix            Len
 5  4                                             5     Total Administered: 2
 5  5                                             5        Maximum Entries: 540
```

Note: There are two ways that an inbound call can reach an individual badge.

- A caller calls the Guest Access or Direct Access Number. In this case, the user is greeted by the 'Genie' voice interface, and prompted for a badge user to contact. (e.g., 28020)
- A user calls a Direct Inward Dialing (DID) number for a badge user. In this case, the call will be directly connected to the badge user without a greeting. (e.g., 303-252-8010)

During the compliance test, 5 digit and 10 digit dialing plans were utilized. Automatic Alternate Routing was utilized for 5 digits. Automatic Route Selection was utilized for 10 digits.

5.9. Automatic Alternate Routing Analysis

This section provides a sample Automatic Alternate Routing (AAR) routing used for routing calls with dialed digits 2*xxxx* to Session Manager. (See **Section 6.7** for corresponding Session Manager configuration). Note that other methods of routing may be used. Use the **change aar analysis 2** command and add an entry to specify how to route calls to 2*xxxx*. In the example shown below, calls with digits 2*xxxx* will be routed as an AAR call using route pattern 1 from **Section 5.7**. These calls will be routed to Session Manager and then to the Vocera SIP Telephony Gateway.

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

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    2                     5    5     1         aar          n
```

5.10. Automatic Route Selection

This section provides a sample Automatic Route Selection (ARS) routing used for routing calls with dialed digits 30325*xxxxx* to Session Manager (See **Section 6.7** for corresponding Session Manger configuration). Note that other methods of routing maybe used. Use the **change ars analysis 3** command and add an entry to specify how to route calls to 30325*xxxxx*. In the example shown below, calls with digits 303252*xxxx* will be routed as an ARS call using route pattern 1 from **Section 5.7**. These calls will be routed to Session Manager and then to Vocera SIP Telephony Gateway.

- **Dialed String** field to **30325**
- **Total Min** field to **10**
- **Total Max** field to **10**
- **Route Pattern** field to **1**
- **Call Type** field to **fnpa**

```
change ars analysis 3                                           Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location: all           Percent Full: 2

          Dialed           Total     Route     Call   Node  ANI
          String          Min  Max  Pattern    Type   Num   Reqd
    30325                 10   10    1         fnpa         n
```

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as shown in the reference configuration. All provisioning for Session Manager is performed via the System Manager web interface. System Manager delivers a set of shared, secure management services and a common console across multiple products in the Avaya network, including the central administration of routing policies, and a common format for logs and alarms.

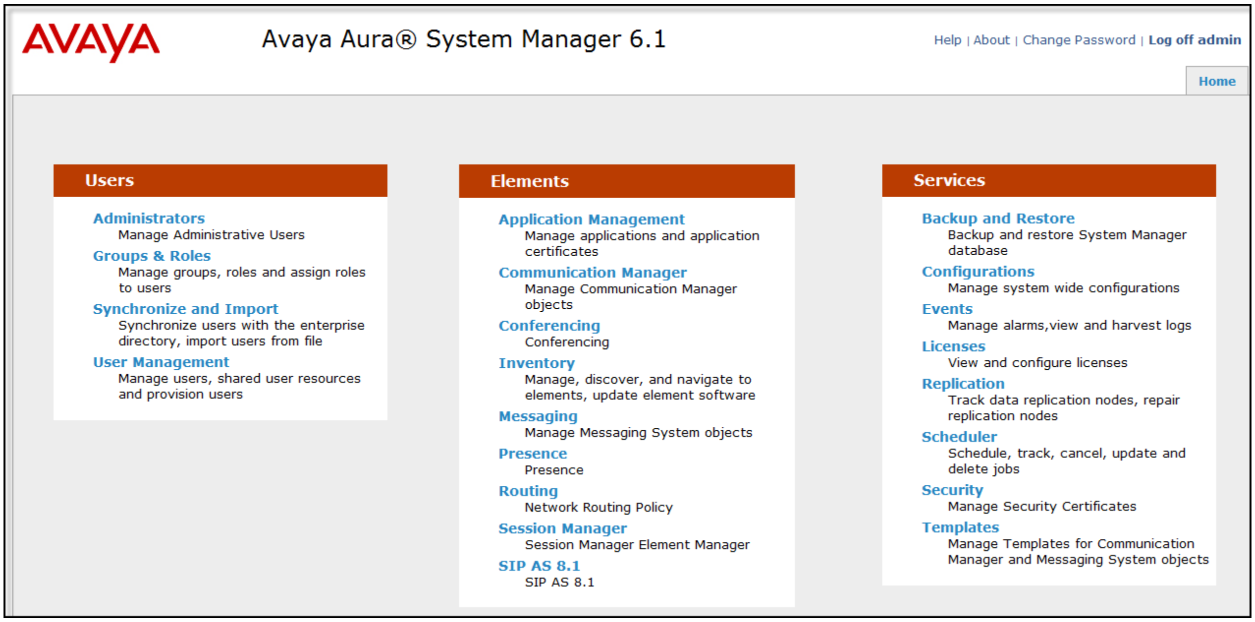
The following sections assume that Session Manager and System Manager have been installed and that network connectivity exists between the two platforms.

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

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

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

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



Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Home

Users

Administrators
Manage Administrative Users

Groups & Roles
Manage groups, roles and assign roles to users

Synchronize and Import
Synchronize users with the enterprise directory, import users from file

User Management
Manage users, shared user resources and provision users

Elements

Application Management
Manage applications and application certificates

Communication Manager
Manage Communication Manager objects

Conferencing
Conferencing

Inventory
Manage, discover, and navigate to elements, update element software

Messaging
Manage Messaging System objects

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Configurations
Manage system wide configurations

Events
Manage alarms,view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

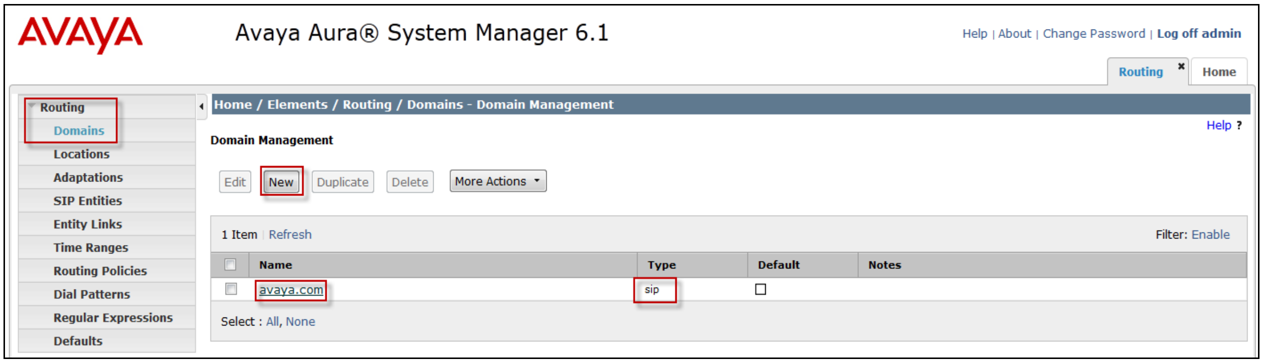
Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager and Messaging System objects

6.1. SIP Domains

In the reference configuration, one SIP domain was used; **avaya.com**.
Navigate to **Element** → **Routing** → **Domains** and click the **New** to add a new SIP domain with the following:

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



□	Name	Type	Default	Notes
□	avaya.com	sip	□	

6.2. Locations

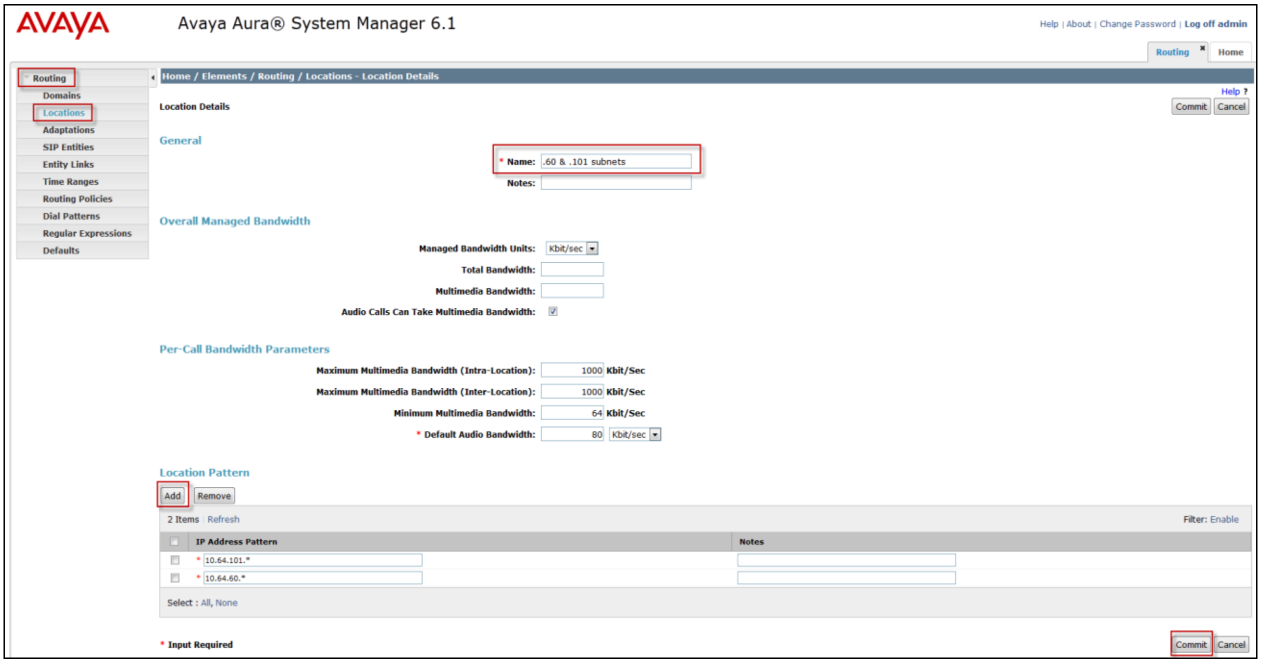
Locations are used to identify logical and/or physical locations where SIP Entities reside, by specifying the IP addressing for the locations as well as for purposes of bandwidth management if required.

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

- Enter a descriptive Location name in the **Name** field (e.g., **.60 & .101 subnets**)
- Enter a description in the **Notes** field if desired

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

- Enter the IP address information for the Location (e.g., **10.64.60.* & 10.64.101***)
- Enter a description in the **Notes** field if desired
- Repeat steps in the Location Pattern section if the Location has multiple IP segments.
- Modify the remaining values on the form, if necessary; otherwise, use all the default values
- Click on the **Commit** button



Location Details

General

* Name: .60 & .101 subnets

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☑

Per-Call Bandwidth Parameters

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

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

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

2 Items | Refresh Filter: Enable

□	IP Address Pattern	Notes
□	* 10.64.101.*	
□	* 10.64.60.*	

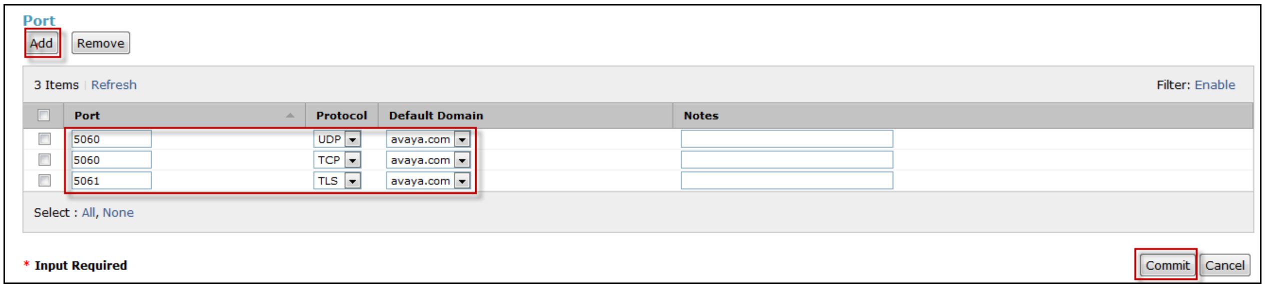
Select : All, None

* Input Required

6.3. SIP Entities

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

Note, the Session Manager SIP Entity is assumed to have already been configured. Navigate to **Routing→ SIP Entities**; check the checkbox for the Session Manager SIP Entity, and click the Edit button (not shown). Under the **Ports** section, verify the required Session Manager listening port for communication with VSTG is configured (e.g., **Port 5060** and **Protocol TCP and UDP)**. If necessary, click the **Add** button to add the listening port and then click the **Commit** button when done to save the changes.


Port

3 Items | Refresh Filter: Enable

□	Port	Protocol	Default Domain	Notes
□	5060	UDP	avaya.com	
□	5060	TCP	avaya.com	
□	5061	TLS	avaya.com	

Select : All, None

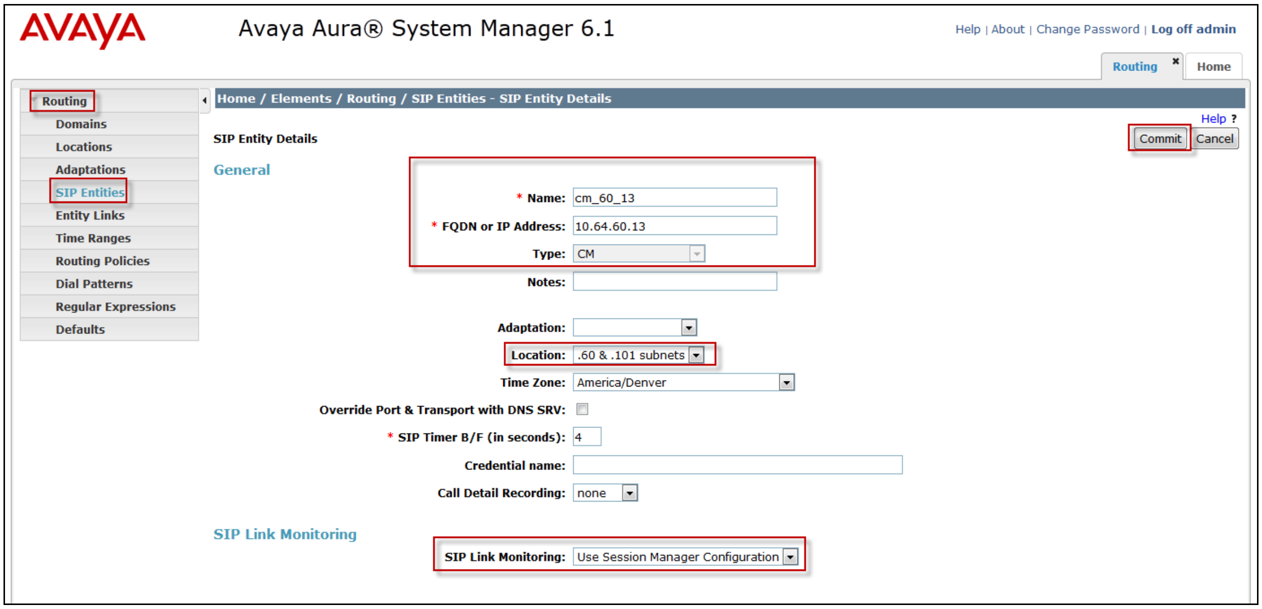
* Input Required

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

- **Name**: Enter an descriptive name
- **FQDN or IP Address**: Enter the IP address of the SIP Entity (e.g., **10.64.60.13**)
- **Type:** Select best match for the SIP entity (e.g.,**CM**)
- **Location :** Select the appropriate location (Configured in **Section 6.2**) from the drop down menu (e.g., **.60 & .101 subnets)**

Section **SIP Link Monitoring**.

- Select desired option



Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

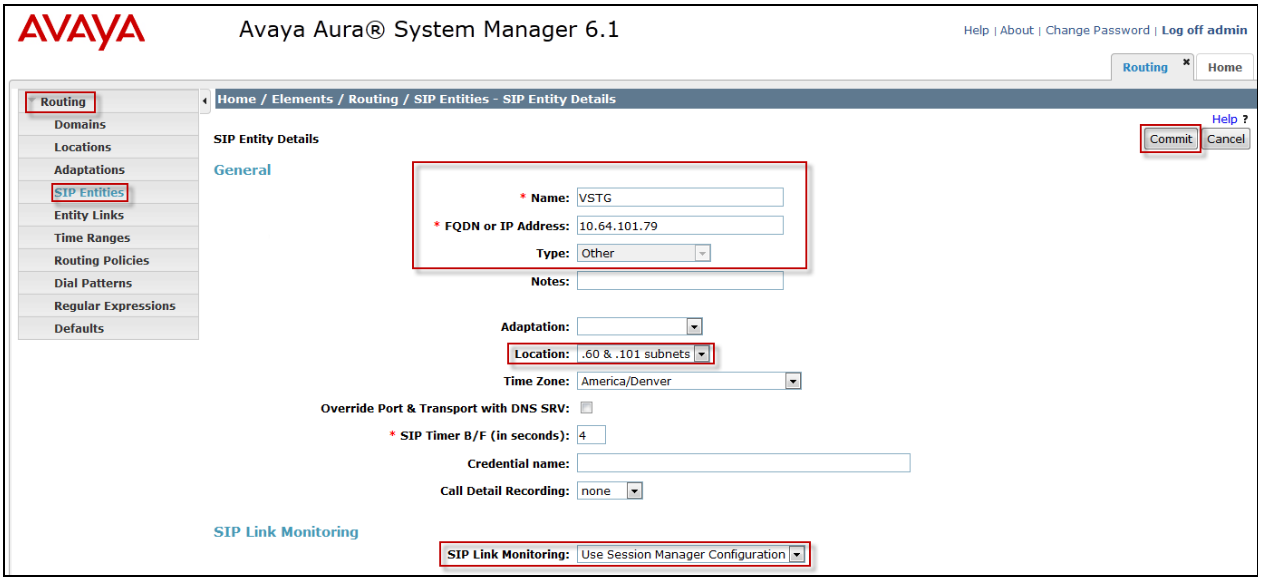
General

* Name: cm_60_13
* FQDN or IP Address: 10.64.60.13
Type: CM
Notes:
Adaptation:
Location: .60 & .101 subnets
Time Zone: America/Denver
Override Port & Transport with DNS SRV: □
* SIP Timer B/F (in seconds): 4
Credential name:
Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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



SIP Entity Details

General

* Name:	VSTG
* FQDN or IP Address:	10.64.101.79
Type:	Other
Notes:	
Adaptation:	
Location:	.60 & .101 subnets
Time Zone:	America/Denver
Override Port & Transport with DNS SRV:	☐
* SIP Timer B/F (in seconds):	4
Credential name:	
Call Detail Recording:	none

SIP Link Monitoring

SIP Link Monitoring:	Use Session Manager Configuration

6.4. Add Entity Link

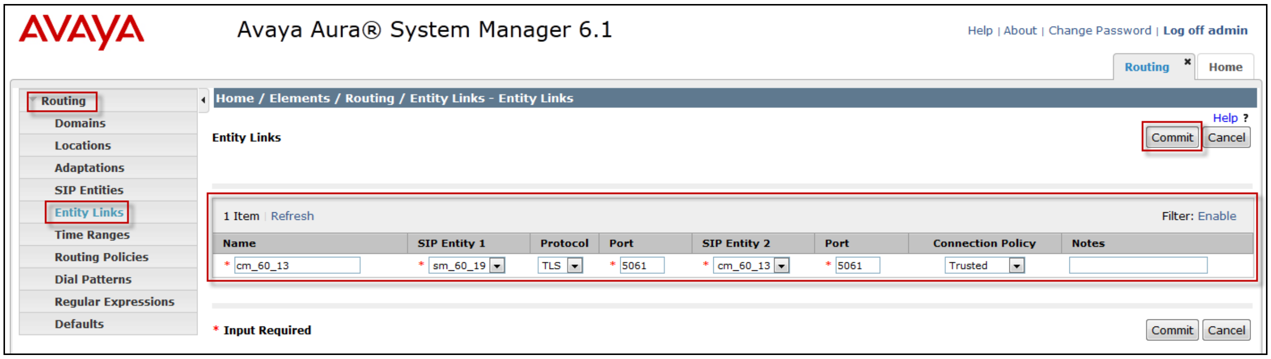
A SIP trunk between Session Manager and a telephony system is described by an Entity link. Two Entity Links were created:

- Session Manager <-> Communication Manger
- Session Manager <-> VSTG

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

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

Click **Commit** to save the configuration.

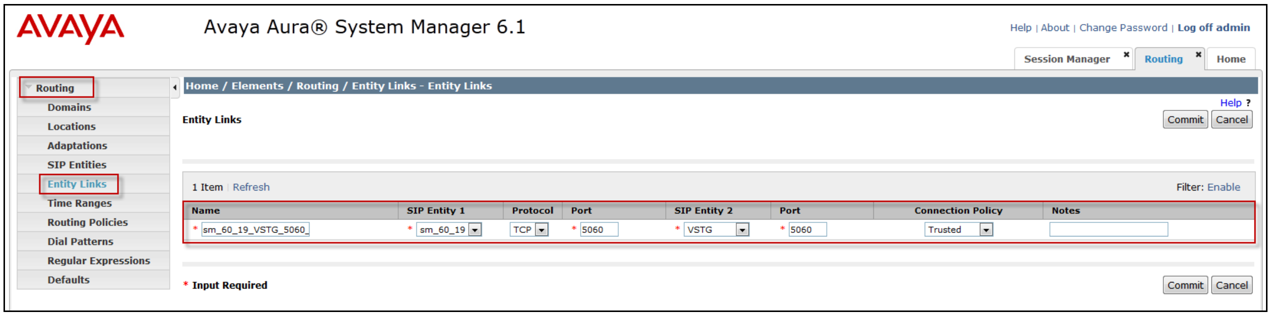


Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* cm_60_13	* sm_60_19	TLS	* 5061	* cm_60_13	* 5061	Trusted	

Note: Acceptance testing was performed first using TCP as the transport protocol and the second test was performed with UDP as the transport protocol.

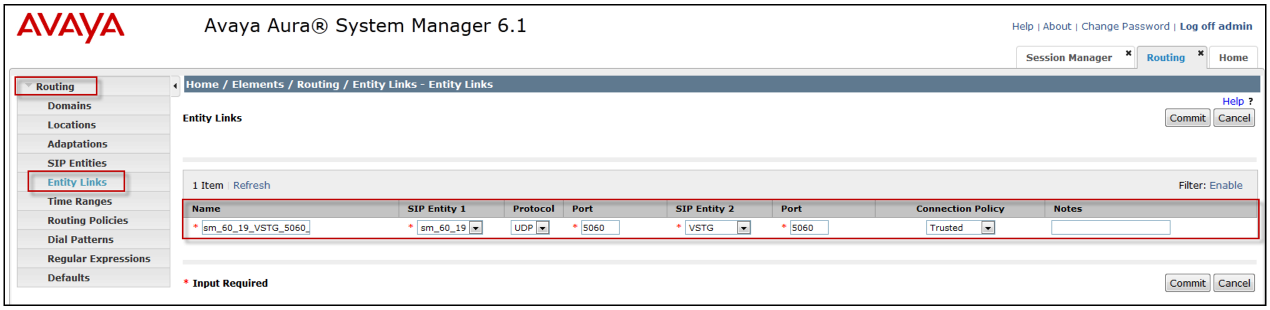
The Entity Link for connecting Session Manager with VSTG was similarly defined as shown in the screen below. Note the use of **TCP** and port **5060**.



Entity Links

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* sm_60_19_VSTG_5060_	* sm_60_19	TCP	* 5060	* VSTG	* 5060	Trusted	

The Entity Link for connecting Session Manager with VSTG was similarly defined as shown in the screen below. Note the use of **UDP** and port **5060**.



Entity Links

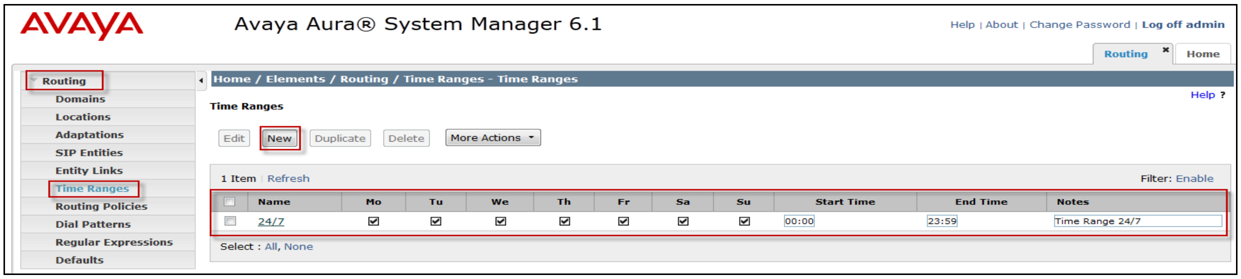
Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* sm_60_19_VSTG_5060_	* sm_60_19	UDP	* 5060	* VSTG	* 5060	Trusted	

6.5. Time Ranges

The **Time Ranges** form allows admission control criteria to be specified for **Routing Policies** (**Section 6.6**). In the reference configuration, no restrictions were used. To add a **Time Range**, navigate to **Elements** → **Routing** → **Time Ranges** and click the **New** button to add a new Time Range. Enter the following information.

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

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



Time Ranges

1 Item

□	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
□	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

6.6. Routing Policies

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

- Inbound calls to Communication Manager
- Outbound calls to Vocera

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

Section **General**.

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

Section **SIP Entity as Destination**.

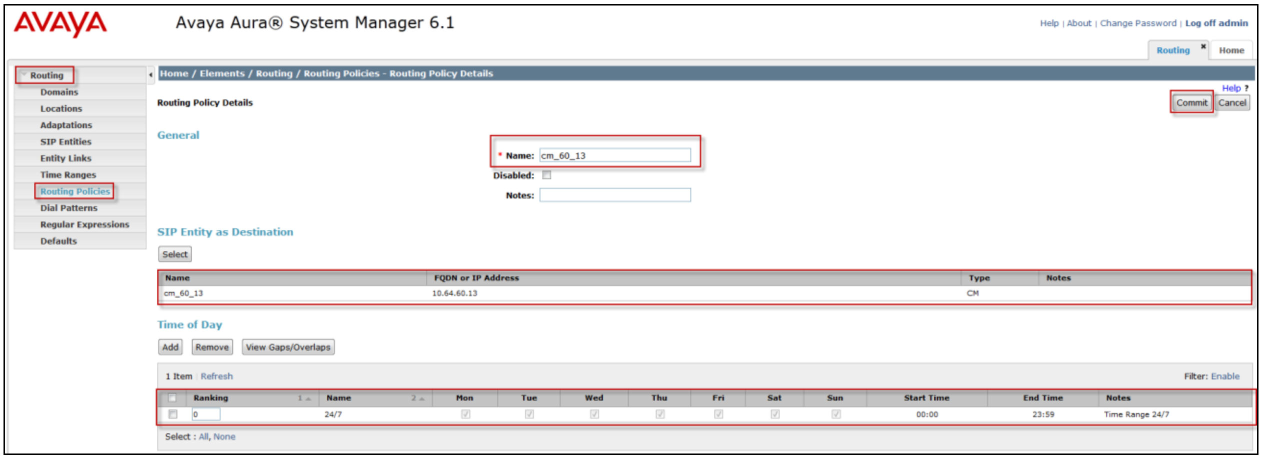
- Click **Select**, and then select the appropriate SIP Entity to which this routing policy applies

Section **Time of Day**.

- Click **Add**, and select the time range configured from **Section 6.2.6**

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

The following screens show the Routing Policy for Communication Manager.



Routing Policy Details

General

* Name: cm_60_13
Disabled: □
Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
cm_60_13	10.64.60.13	CM	

Time of Day

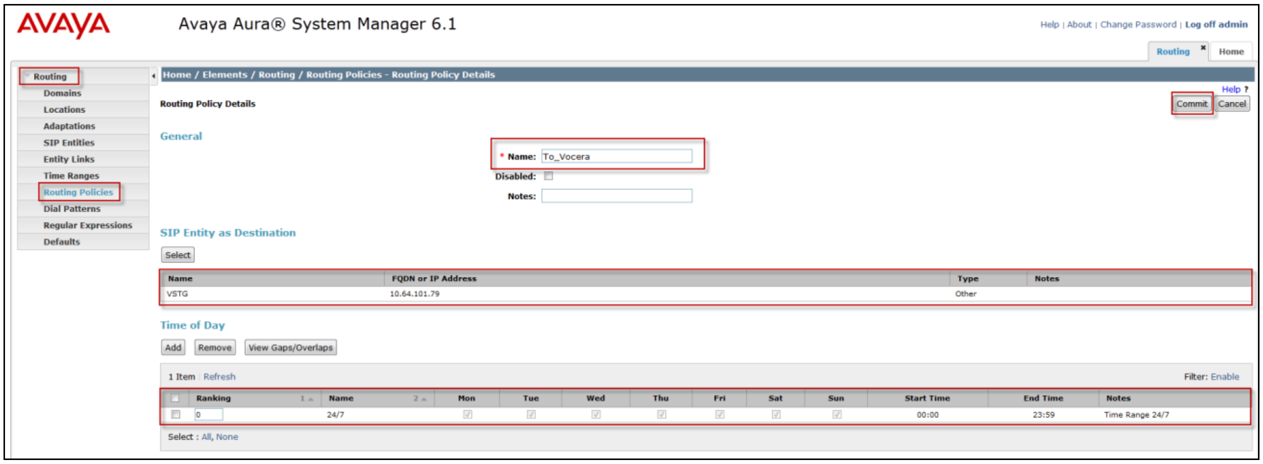
Add Remove View Gaps/Overlaps

1 Item | Refresh   Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

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



Routing Policy Details

General

* Name: To_Vocera
Disabled: □
Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
VSTG	10.64.101.79	Other	

Time of Day

Add Remove View Gaps/Overlaps

1 Item | Refresh   Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

6.7. Dial Patterns

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

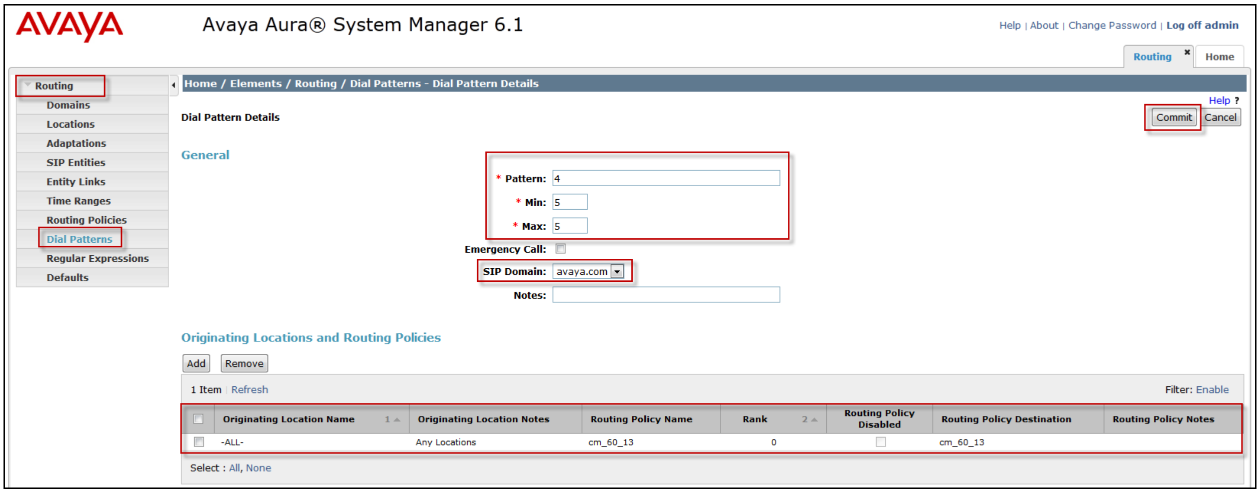
Navigate to **Routing →Dial Patterns**, and click the **New** button (not shown) to add a new Dial Pattern.

Section **General**.

- **Pattern**: dialed number or prefix
- **Min**: minimum length of dialed number
- **Max**: maximum length of dialed number
- **SIP Domain**: 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 an example of routing to route calls that match the pattern 4*xxxx* to Communication Manager.



Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

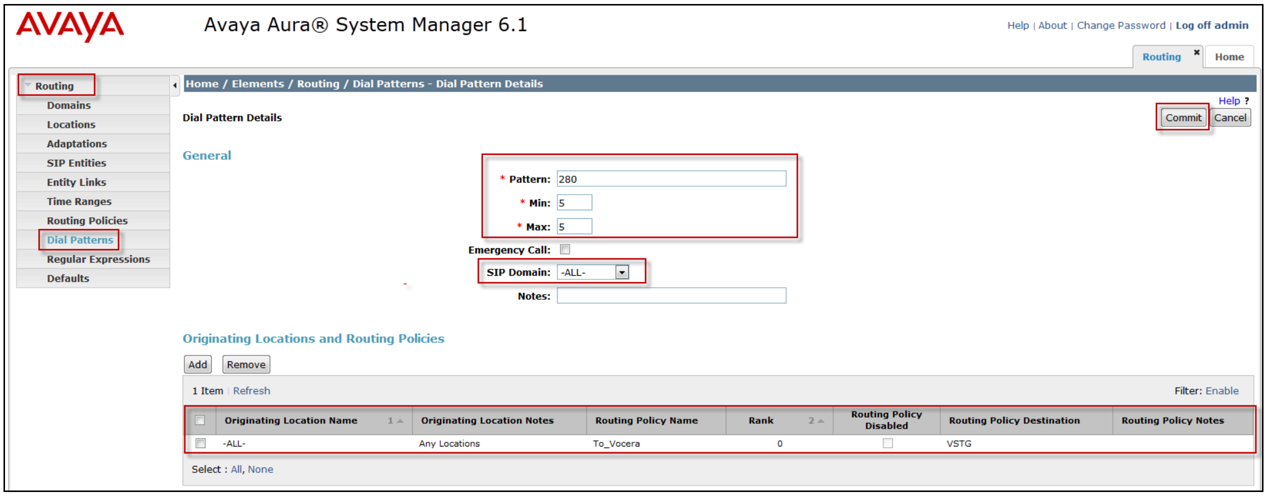
* Pattern: 4
* Min: 5
* Max: 5
Emergency Call: □
SIP Domain: avaya.com
Notes:

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	cm_60_13	0	□	cm_60_13	

The following is an example of routing to route calls that match the pattern 2*xxxx* to Vocera.



Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

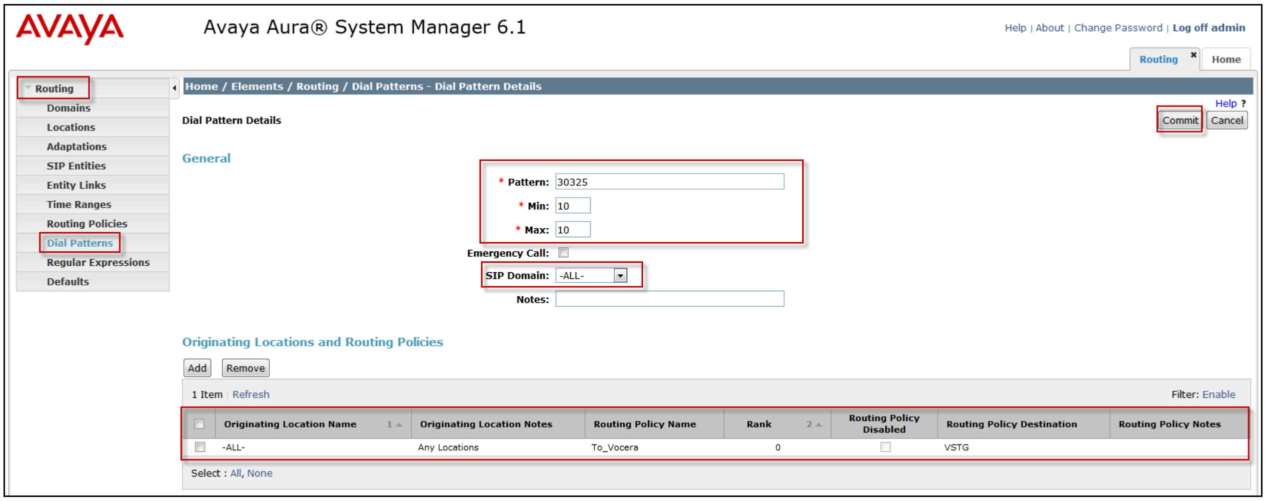
General

* Pattern:	280
* Min:	5
* Max:	5
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	To_Vocera	0	□	VSTG	

The following is an example of routing to route calls that match the pattern 30325*xxxxx* to Vocera.



Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern:	30325
* Min:	10
* Max:	10
Emergency Call:	□
SIP Domain:	-ALL-
Notes:	

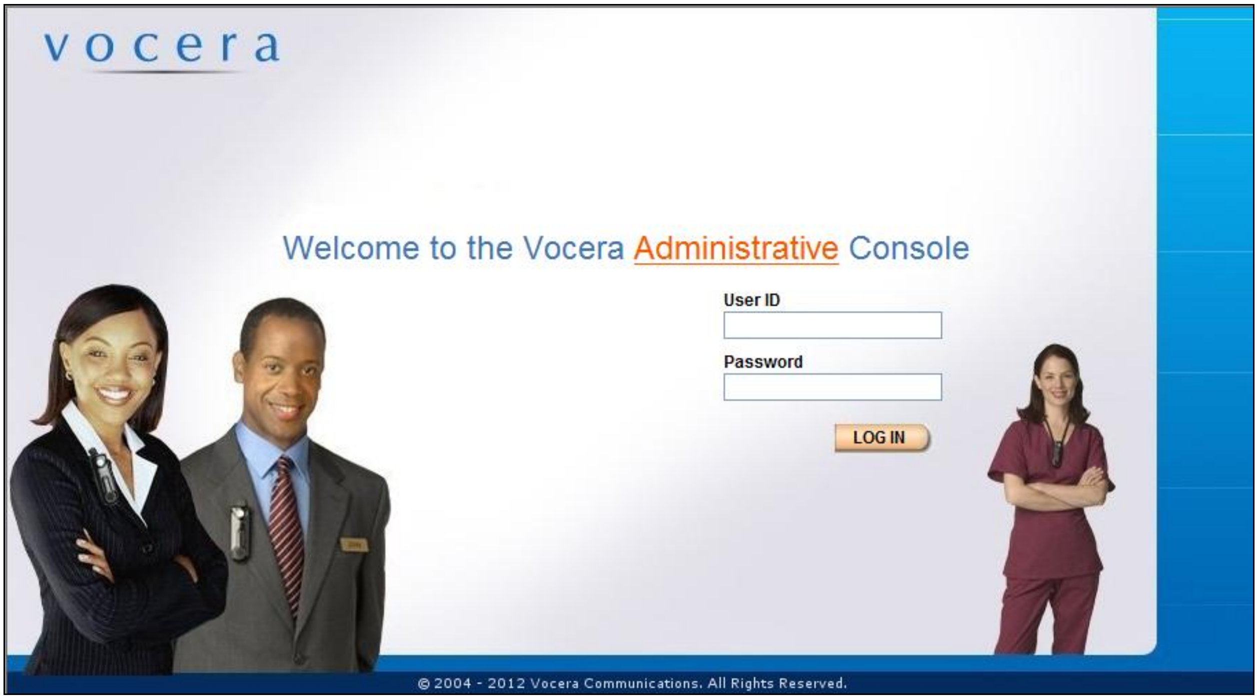
Originating Locations and Routing Policies

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	-ALL-	Any Locations	To_Vocera	0	□	VSTG	

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.

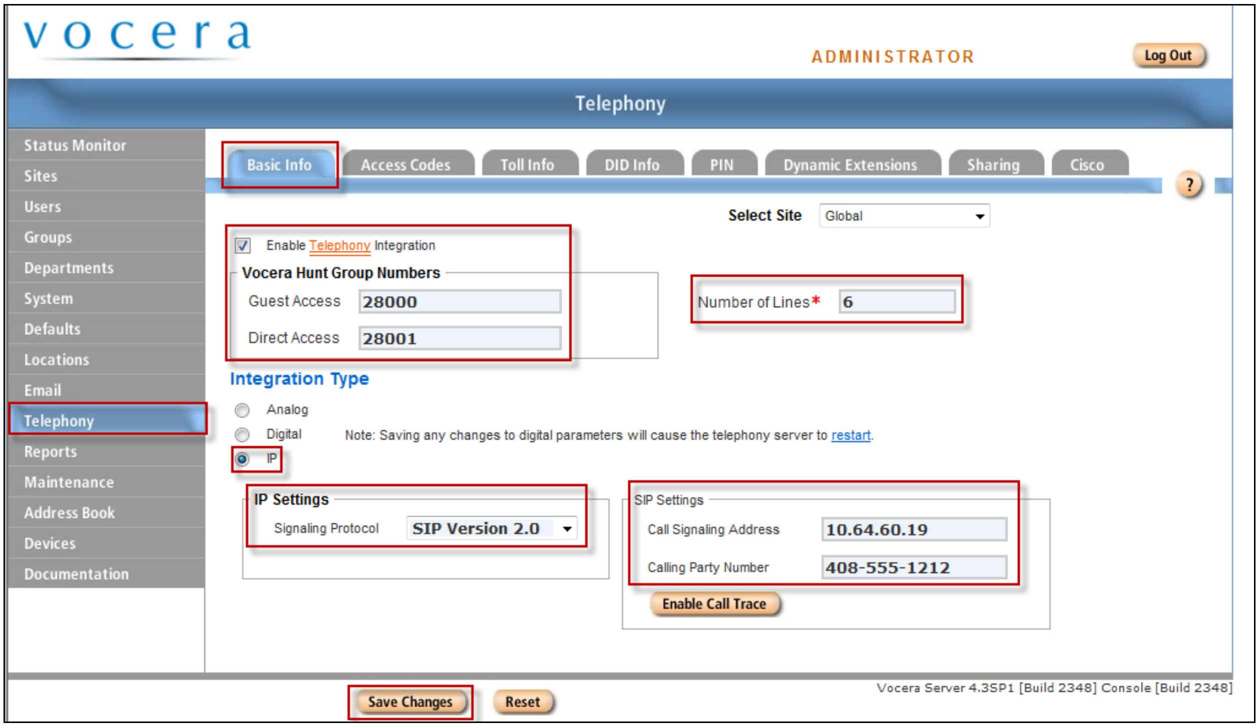
The Vocera Communications System is configured using a web based console interface. Launch a web browser, enter **http://<IP address of Vocera Server>/console/AdminController** in the URL, and log in with the appropriate credentials.


vocera
Welcome to the Vocera Administrative Console
User ID
Password
LOG IN
© 2004 - 2012 Vocera Communications. All Rights Reserved.

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 **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 – x28000
  - Direct Access Number – x28001
  - Number of Lines – 6
  - Three user extensions: x28010, x28011, x28012
- Set the Integration Type to **IP**
- Using the drop-down menu, select **SIP Version 2.0** for Signaling Protocol field under the IP Settings section
- Enter Avaya Aura® Session Manager IP address for the Call Signaling Address field under the SIP Settings section. During the compliance test, IP address, **10.64.60.19**, was utilized
- Enter the Call Party extension Number. During the compliance test, Calling Party Number, **408-555-1212**, was utilized
- Click on the **Save Changes** button



Select Site: Global

☑ Enable Telephony Integration

Vocera Hunt Group Numbers

Guest Access: 28000

Direct Access: 28001

Number of Lines*: 6

Integration Type

○ Analog

○ Digital

● IP

Note: Saving any changes to digital parameters will cause the telephony server to restart.

IP Settings

Signaling Protocol: SIP Version 2.0

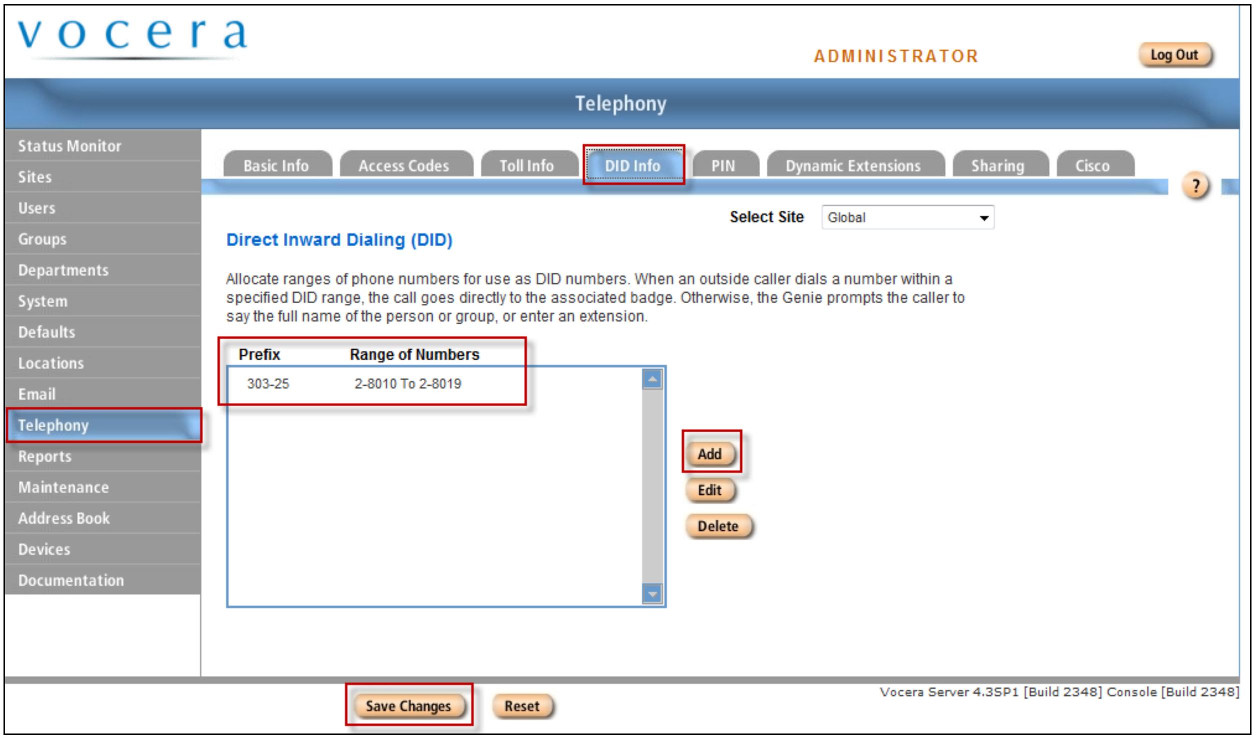
SIP Settings

Call Signaling Address: 10.64.60.19

Calling Party Number: 408-555-1212

Vocera Server 4.3SP1 [Build 2348] Console [Build 2348]

Select **DID Info** tab to configure Direct Inward Dialing numbers for the badges. Select the **Add** button and enter in the DID range, and then click **Save Changes**.



Select Site: Global

Direct Inward Dialing (DID)

Allocate ranges of phone numbers for use as DID numbers. When an outside caller dials a number within a specified DID range, the call goes directly to the associated badge. Otherwise, the Genie prompts the caller to say the full name of the person or group, or enter an extension.

Prefix	Range of Numbers
303-25	2-8010 To 2-8019

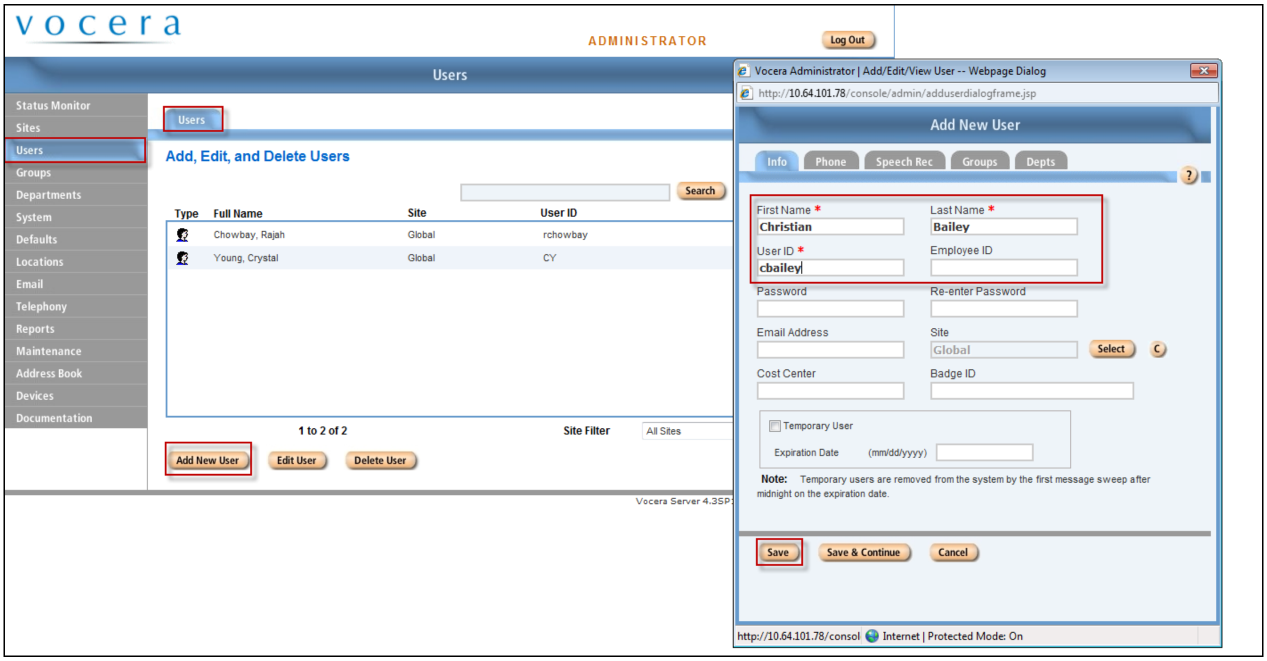
7.2. User Configuration

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 “Christian Bailey” will log the user in.

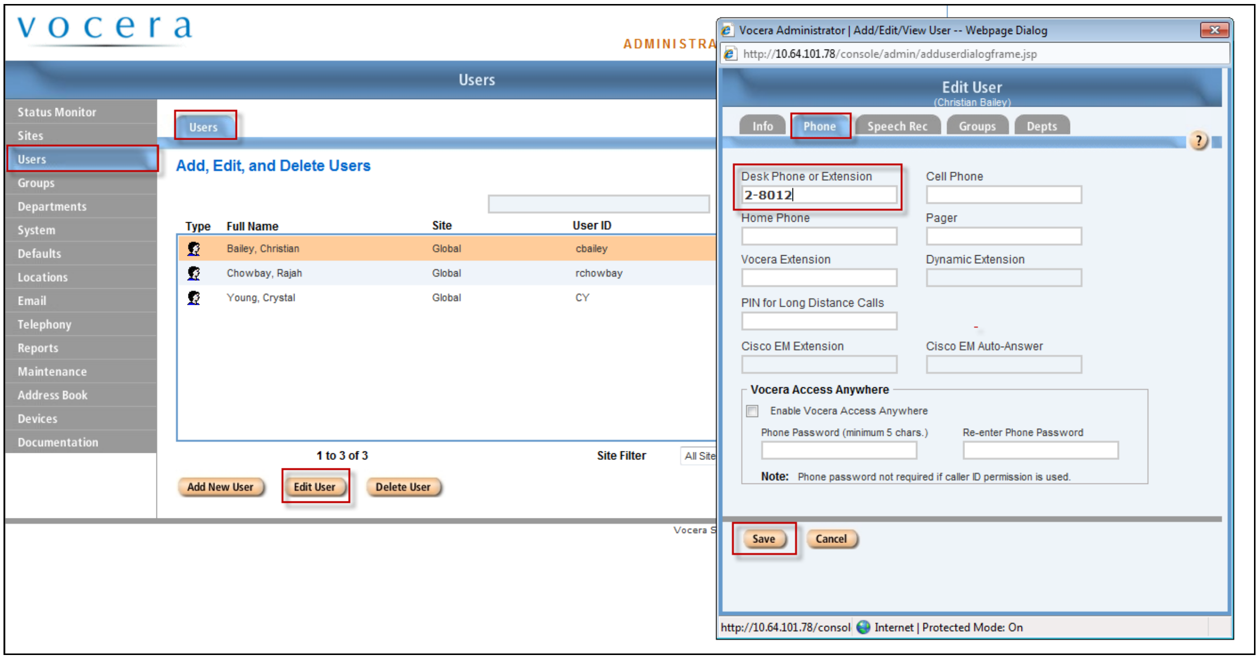


Type	Full Name	Site	User ID
	Chowbay, Rajah	Global	rchowbay
	Young, Crystal	Global	CY

First Name * Christian
Last Name * Bailey
User ID * cbailey
Employee ID
Password
Re-enter Password
Email Address
Site Global
Cost Center
Badge ID
□ Temporary User
Expiration Date (mm/dd/yyyy)

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

To configure the extension associated with the user, select the **Phone** tab and enter in extension number. (e.g., 2-8012) Then click the **Save** button.



Type	Full Name	Site	User ID
	Bailey, Christian	Global	cbailey
	Chowbay, Rajah	Global	rchowbay
	Young, Crystal	Global	CY

Desk Phone or Extension: 2-8012

□ Enable Vocera Access Anywhere

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

8. Verification Steps

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

8.1. Verify Avaya Aura ® Communication Manager

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

```
status signaling-group 1
                         STATUS SIGNALING GROUP

        Group ID: 1
      Group Type: sip

     Group State: in-service
```

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

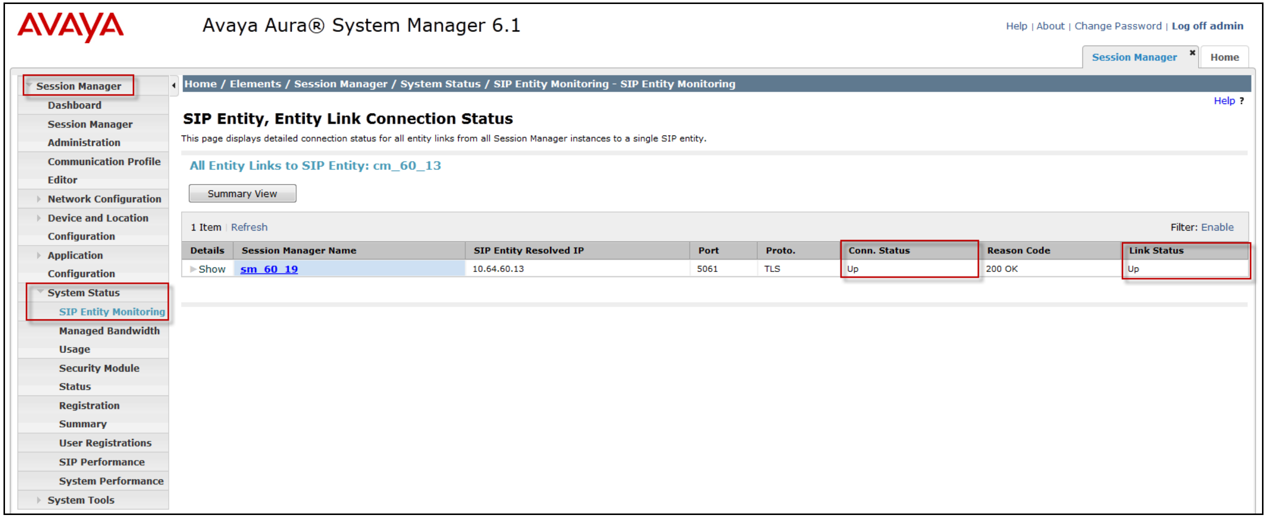
```
status trunk 1

                             TRUNK GROUP STATUS

Member   Port     Service State      Mtce Connected Ports
                                     Busy

0001/001 T00001   in-service/idle    no
0001/002 T00002   in-service/idle    no
0001/003 T00003   in-service/idle    no
0001/004 T00004   in-service/idle    no
0001/005 T00005   in-service/idle    no
0001/006 T00006   in-service/idle    no
0001/007 T00007   in-service/idle    no
0001/008 T00008   in-service/idle    no
0001/009 T00009   in-service/idle    no
0001/010 T00010   in-service/idle    no
```

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

```
status trunk 0001/001                                          Page   1 of   3
                              TRUNK STATUS

 Trunk Group/Member: 0001/001            Service State: in-service/active
               Port: T00001           Maintenance Busy? no
 Signaling Group ID: 1

   IGAR Connection? no

    Connected Ports: T00003
```

8.2. Verify Avaya Aura® Session Manager

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


AVAYA
Avaya Aura® System Manager 6.1
Help | About | Change Password | Log off admin
Session Manager
Home
Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
SIP Entity Monitoring
Managed Bandwidth Usage
Security Module Status
Registration Summary
User Registrations
SIP Performance
System Performance
System Tools
Home / Elements / Session Manager / System Status / SIP Entity Monitoring - SIP Entity Monitoring
Help ?
Summary View
1 Item | Refresh
Filter: Enable

SIP Entity, Entity Link Connection Status

This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.

All Entity Links to SIP Entity: cm_60_13

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

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

8.3. Verify Vocera Communications

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

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

9. Conclusion

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

10. Additional References

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

(1) *Administering Avaya Aura® Communication Manager Release 6.0, Issue 6.0, June 2010, Document Number 03-300509.*

(2) *Administering Avaya Aura® Session Manager, Document 03-603324, Issue 1.1, Release 6.1, November 2010.*

The following document was provided by Vocera.

(3) *Vocera Telephony Configuration Guide, Version 4.3, Part No:: 930-01825 Rev B, 09-Mar-2012 Build 2786.*

(4) *Vocera B3000 Badge Guide, Version 4.3, Part No :: 930-01814 Rev B, 28-May-2012 Build 2349.*

(5) *Vocera Administration Guide Version 4.3, Part No :: 930-01811 Rev B, 09-Mar-2012 Build 2786.*

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.