Avaya Solution & Interoperability Test Lab

Application Notes for Configuring the Vocera Communications System with Avaya Aura^{TM} Session Manager and Avaya Aura^{TM} Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedure for configuring the Vocera Communications System to interoperate with Avaya Aura^{TM} Session Manager and Avaya Aura^{TM} Communication Manager.

The overall objective of the interoperability compliance testing is to verify Vocera Communications System functionalities in an environment comprised of Avaya Aura^{TM} Communication Manager, Avaya Aura^{TM} Session Manager, and various SIP IP Telephones.

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 a compliance-tested configuration comprised of the wireless communication features of Vocera Communications System with Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager.

Vocera Communications System 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 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 provides connectivity to Avaya Aura™ Communication Manager. 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].

1.1. Interoperability Compliance Testing

The interoperability compliance test included features and serviceability. The focus of the interoperability compliance testing was primarily on verifying call establishment on the Vocera Communications System. Vocera Communications System operations such as inbound calls, outbound calls, call transfer, DTMF, and Vocera Communications System interactions with Session Manager, Communication Manager, and Avaya SIP and H.323 IP telephones were verified. The serviceability testing introduced failure scenarios to see if Vocera Communications System can recover from failures.

1.2. Support

For technical support on the Vocera Communications System solution can be obtained by contacting Vocera Commuications System:

- URL – support@Vocera.com
- Phone – (800) 473-3971

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Avaya Aura^{TM} Communications Manager on an Avaya S8300D Server, an Avaya G450 Media Gateway, an Avaya Aura^{TM} Session Manager, an Avaya Aura^{TM} System Manager, and the Vocera Communications System. The solution described herein is also extensible to other Avaya Servers and Media Gateways. Avaya S8720 Servers with an Avaya G650 Media Gateway were included in the test to provide an inter-switch scenario. For completeness, Avaya 4600 Series H.323 IP Telephones, Avaya 9600 Series SIP IP Telephones, and Avaya 9600 Series H.323 IP Telephones are included in **Figure 1** to verify calls between the SIP-based Vocera Communications System and Avaya SIP, H.323, and digital telephones.

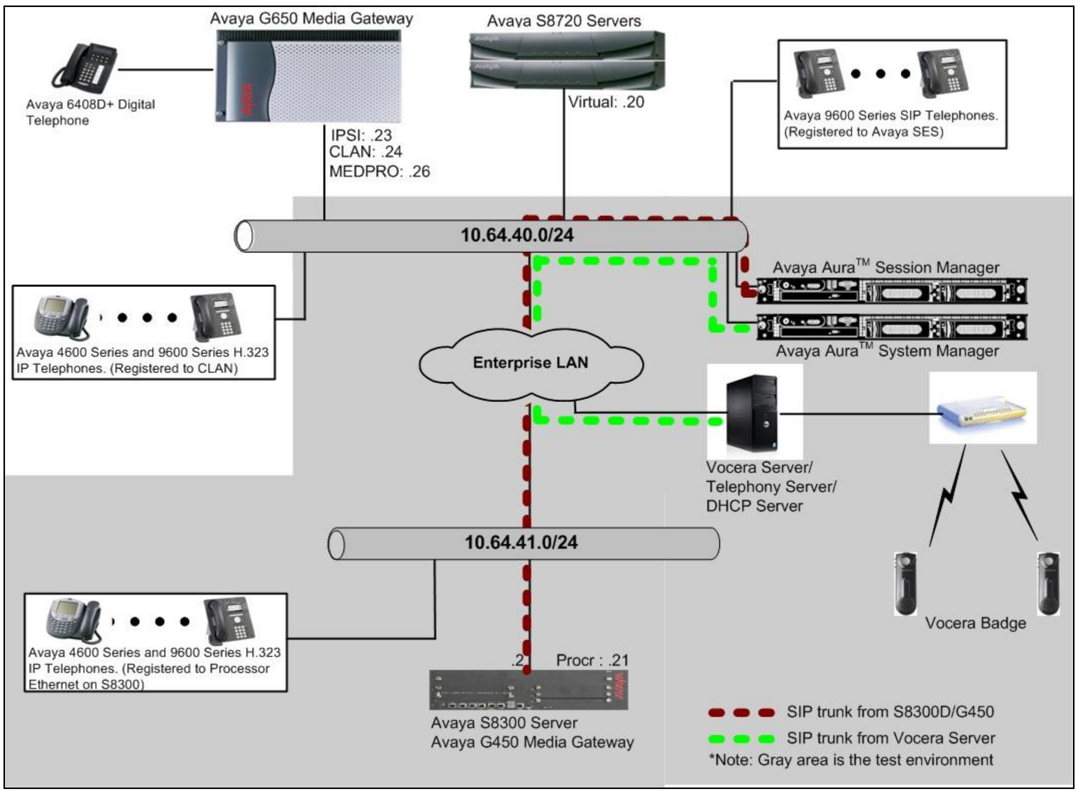


Figure 1: Test Configuration of Vocera Communications System

3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Equipment	Software/Firmware
Avaya S8300 Media Server with Avaya G450 Media Gateway	Avaya Aura™ Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0345.0-18246
Avaya Aura™ System Manager	Avaya Aura™ System Manager 6.0 (6.0.0.0-556)
Avaya Aura™ Session Manager	Avaya Aura™ System Manager 6.0 (6.0.0.0.600020)
Avaya S8720 Servers with Avaya G650 Media Gateway	Avaya Aura™ Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series SIP Telephones	
9620 (SIP)	2.5
9630 (SIP)	2.5
9650 (SIP)	2.5
Avaya 4600 and 9600 Series IP Telephones	
4625 (H.323)	2.9
9620 (H.323)	3.1
9630 (H.323)	3.1
9650 (H.323)	3.1
Avaya 6408D+ Digital Telephone	-
Vocera Communications System	
Vocera Server and Vocera SIP Telephony Gateway	4.1 SP5 build 1977
Vocera Badge	B1000 -1977
Vocera Badge	B2000-345

4. Configure Avaya Aura™ Communication Manager

In the compliance test, Avaya Aura™ Communication Manager was set up as an Evolution Server (Full Call Model). This section describes the procedure for setting up a SIP trunk between Avaya Aura™ Communication Manager and Avaya Aura™ Session Manager. The steps include setting up an IP codec set, an IP network region, IP node name, a signaling group, a trunk group, route pattern, and aar anaysis. Before a trunk can be configured, it is necessary to verify if there is enough capacity to setup an additional trunk. The highlights in the following screens indicate the values used during the compliance test. Default values may be used for all other fields.

These steps are performed from the Avaya Aura™ Communication Manager System Access Terminal (SAT) interface.

4.1. Capacity Verification

Enter the **display system-parameters customer-options** command. Verify that there are sufficient Maximum Off-PBX Telephones – OPS licenses for Avaya SIP endpoints. If not, contact an authorized Avaya account representative to obtain additional licenses. During the compliance test, the Vocera Communications System was not utilized as a SIP endpoint, but did utilize the SIP trunk.

```
display system-parameters customer-options                      Page   1 of  11
                                OPTIONAL FEATURES

     G3 Version: V16                                Software Package: Standard
       Location: 2                                   System ID (SID): 1
       Platform: 28                                  Module ID (MID): 1

                                                                USED
                                Platform Maximum Ports: 6400   185
                                      Maximum Stations: 500    19
                              Maximum XMOBILE Stations: 2400   0
                    Maximum Off-PBX Telephones - EC500: 10     0
                    Maximum Off-PBX Telephones -   OPS: 500    9
                    Maximum Off-PBX Telephones - PBFMC: 10     0
                    Maximum Off-PBX Telephones - PVFMC: 10     0
                    Maximum Off-PBX Telephones - SCCAN: 0      0
                         Maximum Survivable Processors: 0      0
```

On **Page 2** of the form, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. If not, contact an authorized Avaya account representative to obtain additional licenses.

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

IP PORT CAPACITIES                                              USED
                     Maximum Administered H.323 Trunks: 4000   20
           Maximum Concurrently Registered IP Stations: 2400   3
             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: 10     0
                       Maximum Administered SIP Trunks: 4000   110
  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: 8      0
```

4.2. IP Codec Set

This section describes the steps for administering a codec set in Communication Manager. This codec set is used in the IP network region for communications between Communication Manager and Session Manager. Enter the **change ip-codec-set <c>** command, where **c** is a number between **1** and **7**, inclusive. IP codec sets are used in **Section 4.3** 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
```

4.3. Configure 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. Enter 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**. This should match the SIP Domain value on Session Manager, in **Section 5.1**.
- Codec Set – Set the codec set number as provisioned in **Section 4.2**.

```
change ip-network-region 1                                      Page   1 of  20
                               IP NETWORK REGION
  Region: 1
Location:          Authoritative Domain: avaya.com
    Name:
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
```

4.4. Configure IP Node Name

This section describes the steps for setting the IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for Session Manager along with its IP address.

```
change node-names ip                                                Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
CLAN                    10.64.40.24
SM-1                    10.64.40.42
default                 0.0.0.0
procr                   10.64.41.21
procr6                  ::
```

4.5. Configure SIP Signaling

Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- Group Type – Set to **sip**.
- IMS Enabled – Verify that the field is set to **n**. Setting this filed to **y** will cause Communication Manager to act as a Feature Server.
- Transport Method – Set to **tls** (Transport Layer Security).
- Near-end Node Name – Set to **procr** as displayed in **Section 4.4**.
- Far-end Node Name – Set to the Session Manager name configured in **Section 4.4**.
- Far-end Network Region – Set to the region configured in **Section 4.3**.
- Far-end Domain – Set to **avaya.com**. This should match the SIP Domain value in **Section 4.3**.

```
add signaling-group 92
                                SIGNALING GROUP

 Group Number: 92             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-1
 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? n                     Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

4.6. Configure Trunk Group

To configure the associated trunk group, enter the **add tunk-group <t>** command, where **t** is an available trunk group and configure the following:

- Group Type – Set the Group Type field to **sip**.
- Group Name – Enter a descriptive name.
- TAC (Trunk Access Code) – Set to any available trunk access code.

- Service Type – Set the Service Type field to **tie**.
- Signaling Group – Set to the Group Number field value configured in **Section 4.5**.
- Number of Members – Allowed value is between 0 and 255. Set to a value large enough to accommodate the number of SIP telephone extensions being used.

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

Group Number: 92                   Group Type: sip          CDR Reports: y
Group Name: SIP trk                       COR: 1        TN: 1        TAC: 1092
   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: 92
                                                    Number of Members: 20
```

On Page 3, set the Numbering Format field to **unk-pvt.**

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




                     Numbering Format: unk-pvt
                                               UUI Treatment: service-provider

                                                Replace Restricted Numbers? n
                                               Replace Unavailable Numbers? n



                                Modify Tandem Calling Number: no





 Show ANSWERED BY on Display? y
```

4.7. Configure Route Pattern

For the trunk group created in **Section 4.6**, define the route pattern by entering the **change route-pattern <r>** command, where **r** is an unused route pattern number. The route pattern consists of a list of trunk groups that can be used to route a call. The following screen shows route-pattern 92 will utilize trunk group 92 to route calls. The default values for the other fields may be used.

```
change route-pattern 92                                        Page   1 of   3
```

```
                    Pattern Number: 92  Pattern Name: IMS SIP trunk
                             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: 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  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                          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
```

4.8. Configure AAR Analysis

For the AAR Analysis Table, create the dial string that will map calls to the Vocera Communications System via the route pattern created in **Section 4.7**. Enter the **change aar analysis <x>** command, where **x** is a starting digit. The dialed string created in the AAR Digit Analysis table should contain a map to the Vocera Communications System extensions, which are configured as x28021 – x28025. During the configuration of the 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
    2802                    5    5      92       unku            n
```

5. Configure Avaya Aura™ Session Manager

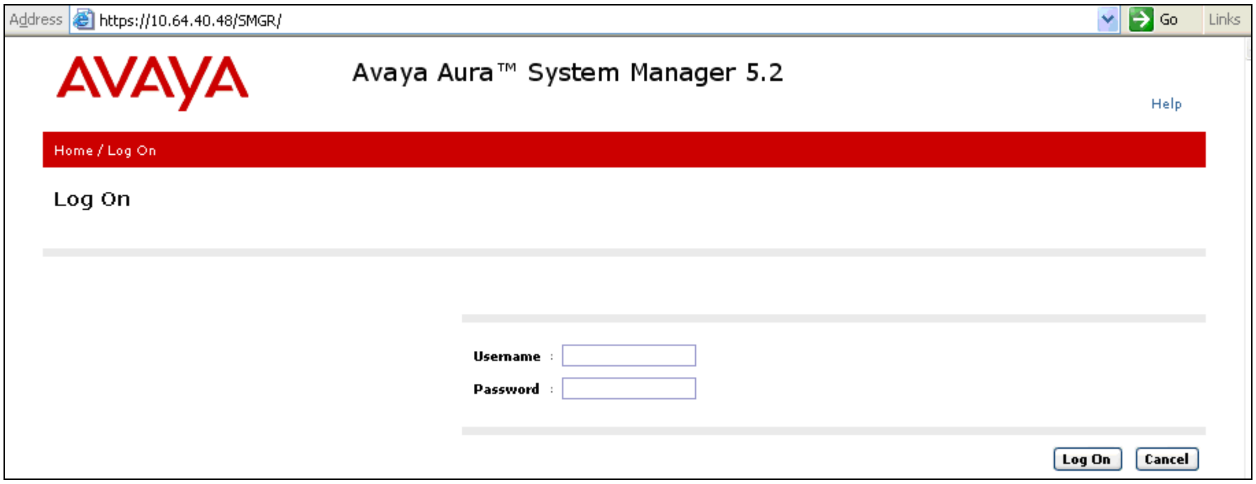
This section provides the procedures for configuring Avaya Aura™ Session Manager as provisioned in the reference configuration. Avaya Aura™ Session Manager is comprised of two functional components: the Avaya Aura™ Session Manager server and the Avaya Aura™ System Manager server. All SIP call provisioning for Avaya Aura™ Session Manager is performed through the Avaya Aura™ System Manager Web interface and is then downloaded into Avaya Aura™ Session Manager.

This section assumes that Avaya Aura™ Session Manager and Avaya Aura™ System Manager have been installed, network connectivity exists between the two platforms, and that basic configuration has been performed.
The following steps describe the sequence for configuring Avaya Aura™ Session Manager

- Domains
- Locations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policy
- Dial Patterns
- Manage Element
- Applications
- Application Sequence
- User Management
- Synchronization

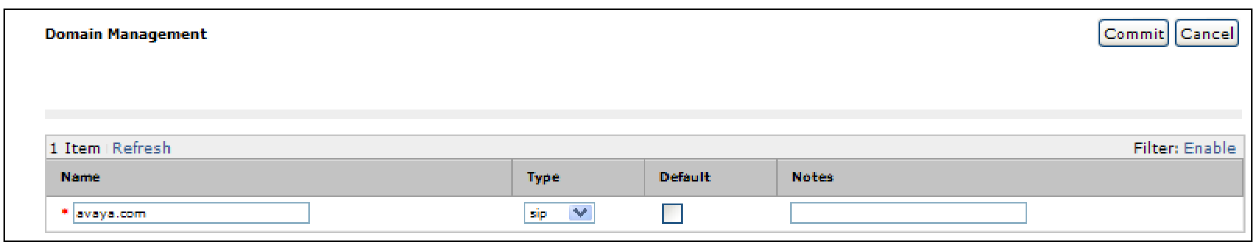
5.1. Configure Domains

Launch a web browser, enter **http://<IP address of System Manager>/SMGR** in the URL, and log in with the appropriate credentials.

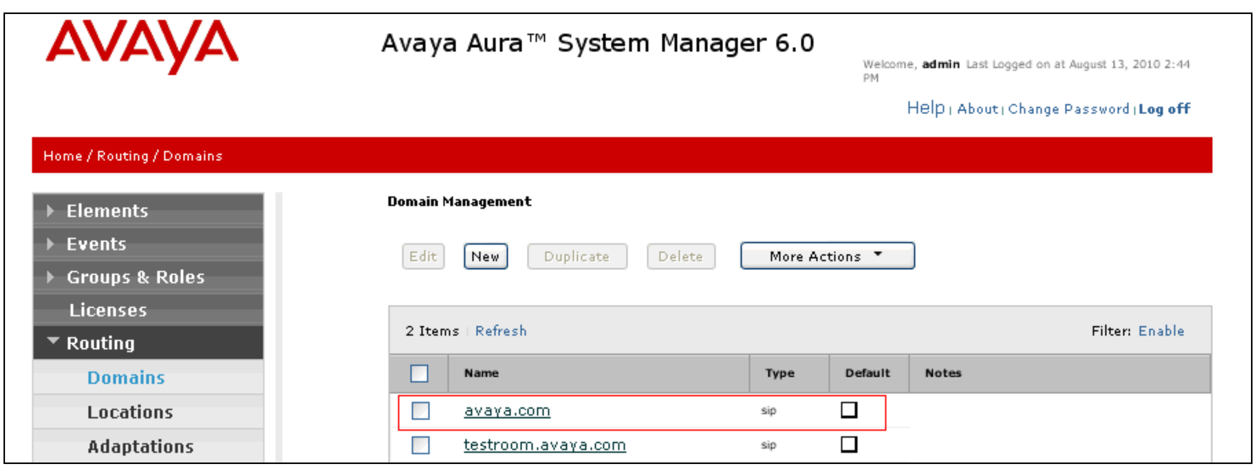


Navigate to **Routing → Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for remaining fields:

- **Name** – Enter the Authoritative Domain Name specified in **Section 4.3**, which is **Avaya.com**.
- **Type** – Select **SIP**



Click **Commit** to save. The following screen shows the Domain used during the compliance test.



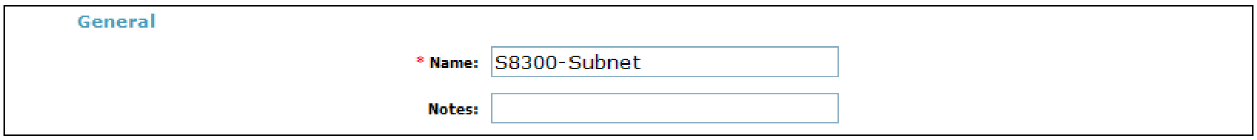
5.2. Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing.

Navigate to **Routing → Locations**, and click on the **New** button (not shown) to create a new SIP endpoint location.

In the **General** section**,** enter the following values and use default values for remaining fields.

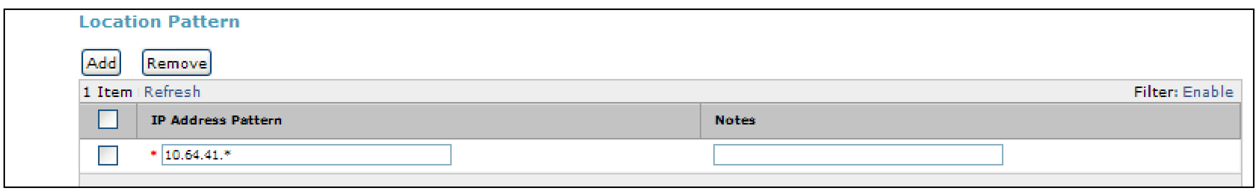
- Enter a descriptive Location name in the Name field (e.g. **S8300-Subnet**).
- Enter a description in the **Notes** field if desired.



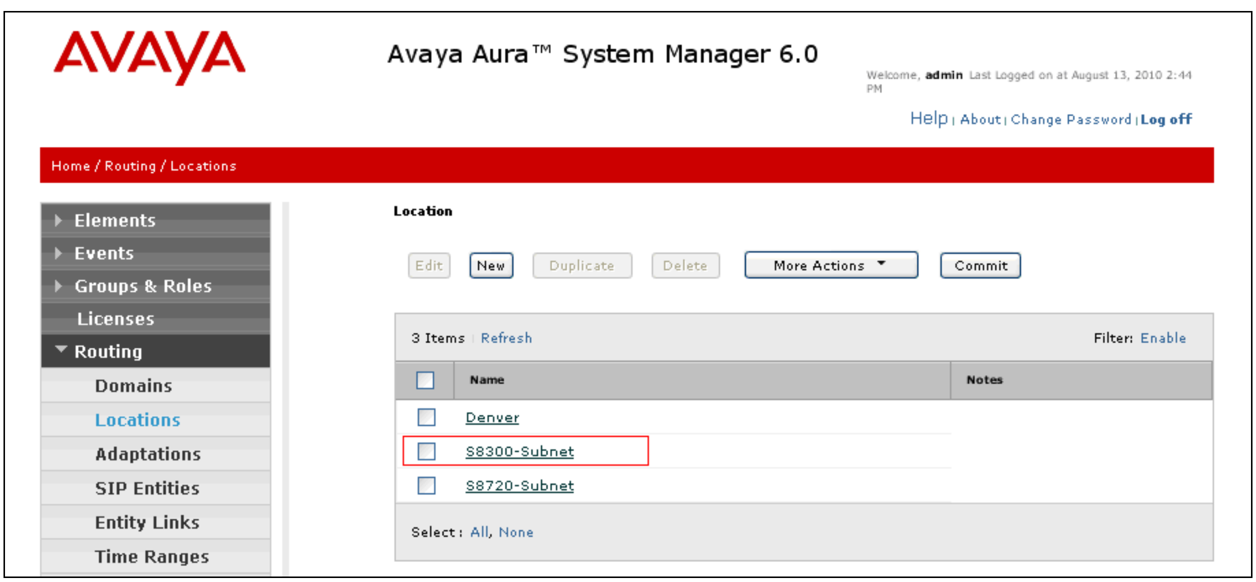
In the **Location Pattern** section, click **Add** and enter the following values:

- Enter the IP address information for the IP address Pattern (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. The following screen shows the Locations page used during the compliance test.



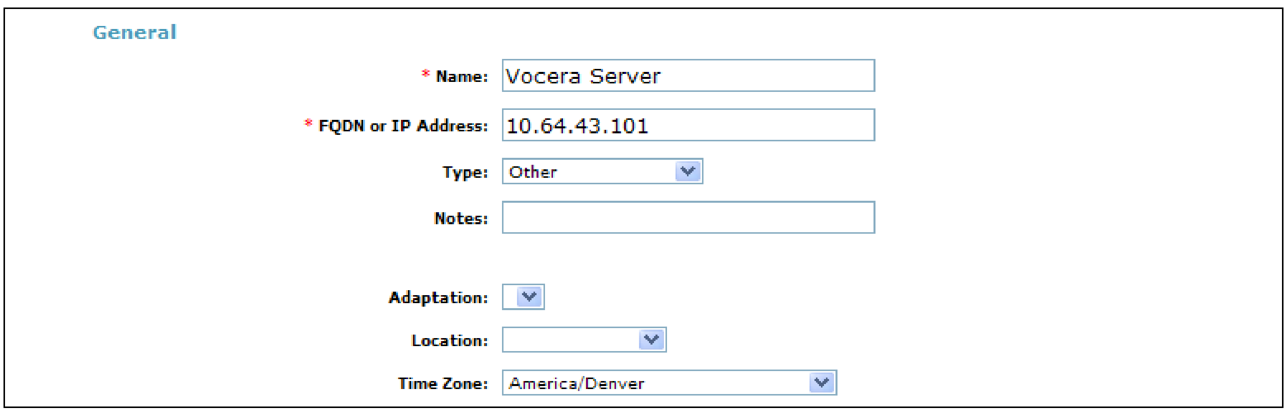
5.3. Configure SIP Entities

A SIP Entity must be added for Session Manager and for each network component that has a SIP trunk provisioned to Session Manager. During the compliance test, the following SIP Entities were configured:

- Session Manager itself.
- Communication Manager
- Vocera

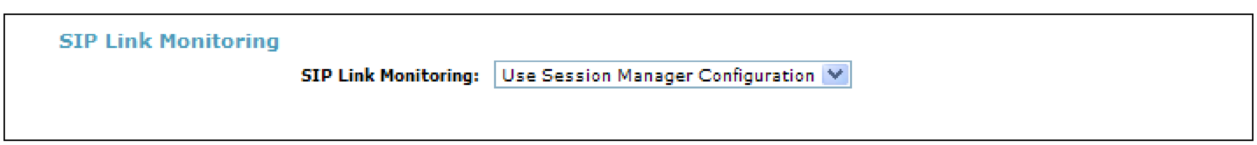
Navigate to **Routing → SIP Entities**, and click on the **New** button (not shown) to create a new SIP entity. Provide the following information:
In the **General** section**,** enter the following values and use default values for remaining fields.

- Enter a descriptive Location name in the **Name** field.
- Enter IP address for signaling interface on each Communication Manager, virtual SM-100 interface on Session Manager, or 3rd party device on the FQDN or IP Address field
- From the **Type** drop down menu select a type that best matches the SIP Entity.
  - For Communication Manager, select CM
  - For Session Manager, select Session Manager
  - For Vocera Server, select other
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.



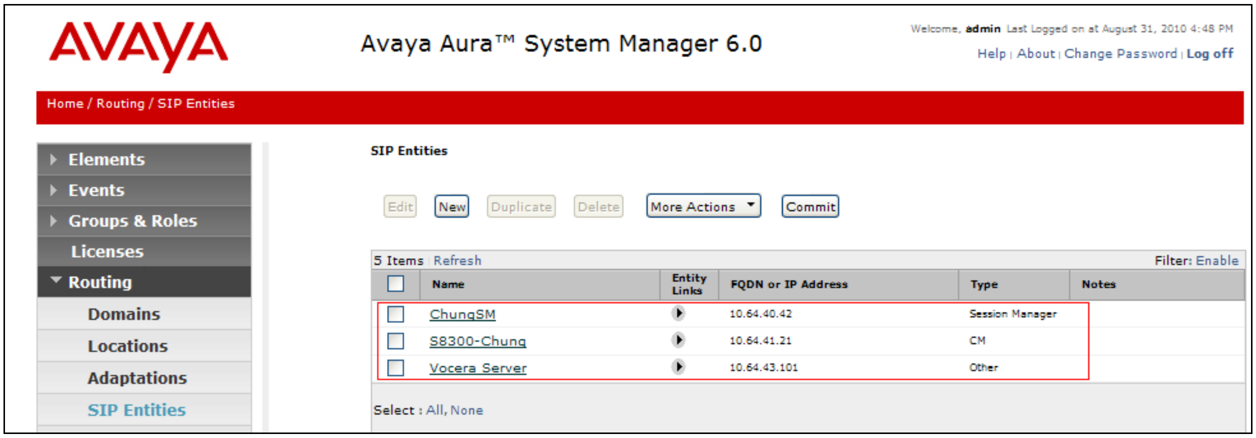
In the **Sip Link Monitoring** section:

- Select a desired option. During the compliance test, **Use Session Manager Configuration** option was utilized.



Click on the **Commit** button to save each SIP entity.

The following screen shows the SIP Entities page used during the compliance test.



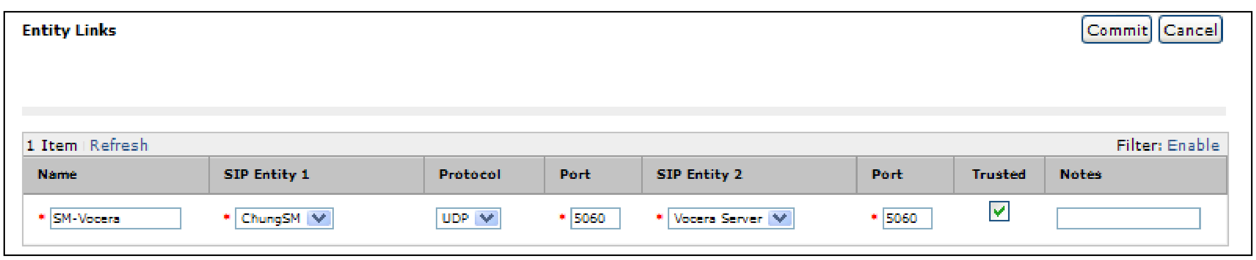
5.4. Configure Entity Links

Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Communication Manager
- Session Manager ⇔ Vocera

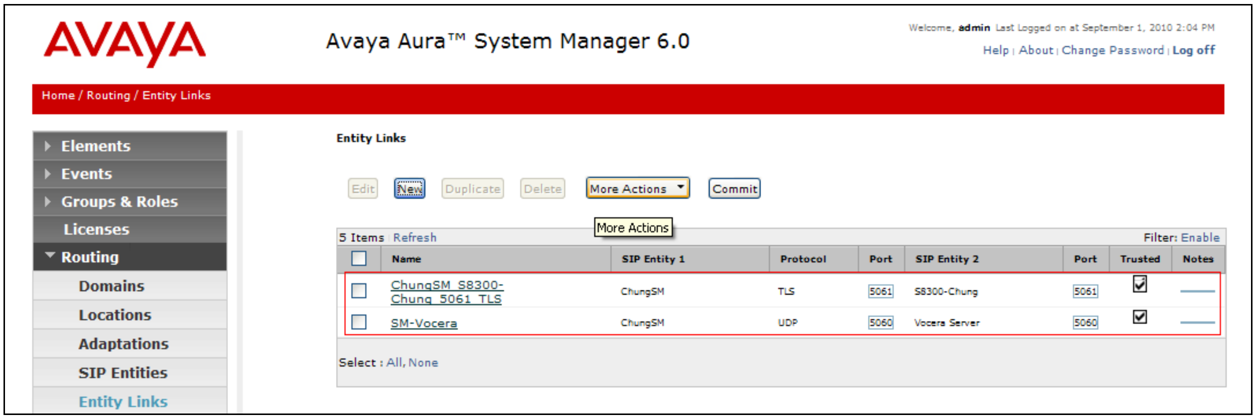
Navigate to **Routing → Entity Links**, and click on the **New** button (not shown) to create a new entity link. Provide the following information:

- Enter a descriptive name in the **Name** field.
- In the **SIP Entity 1** drop down menu, select the Session Manager SIP Entity created in **Section 5.3** (e.g. **ChungSM**).
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- In the **SIP Entity 2** drop down menu, select one of the two entities in the bullet list above (which were created in **Section 5.3**). In the compliance test **Vocera Server** was selected.
- In the **Port** field, enter the port to be used (e.g. **5060** or **5061**).
- Check the **Trusted** box.
- In the **Protocol** drop down menu, select the protocol to be used.
- Enter a description in the **Notes** field if desired.



Click on the **Commit** button to save each Entity Link definition.

The following screen shows an Entity Links used during the compliance test.



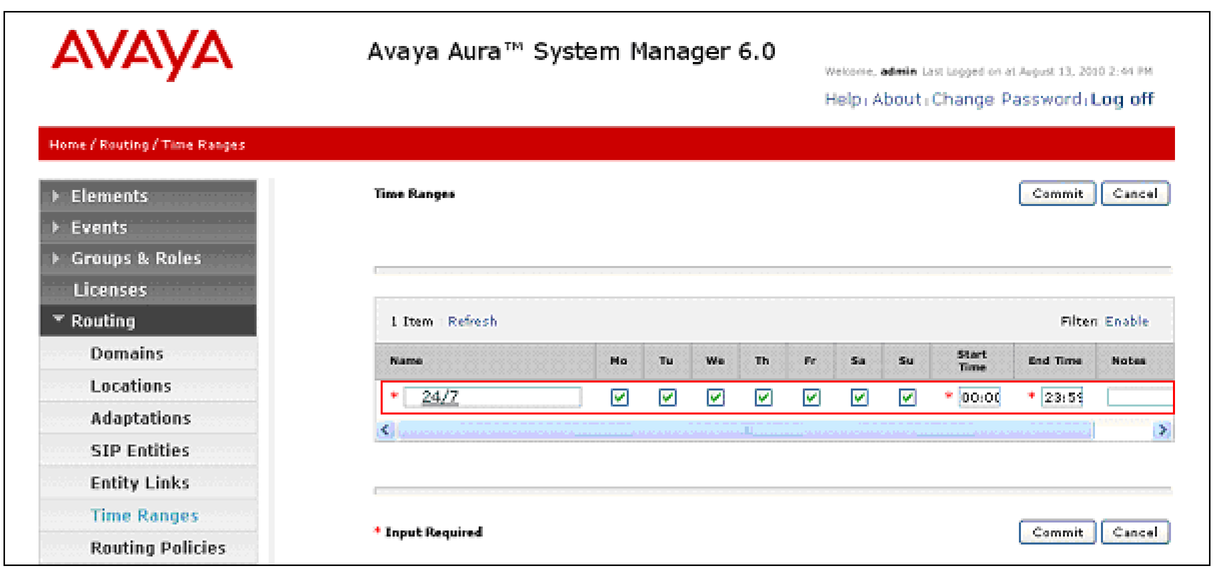
5.5. Time Ranges

The Time Ranges form allows admission control criteria to be specified for Routing Policies (**Section 5.6**). In the reference configuration, no restrictions were used.

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

- Enter a descriptive Location name in the **Name** field (e.g. **24/7**).
- Check each day of the week.
- In the **Start Time** field, enter **00:00**.
- In the **End Time** field, enter **23:59**.
- Enter a description in the **Notes** field if desired.

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



5.6. Configure Routing Policy

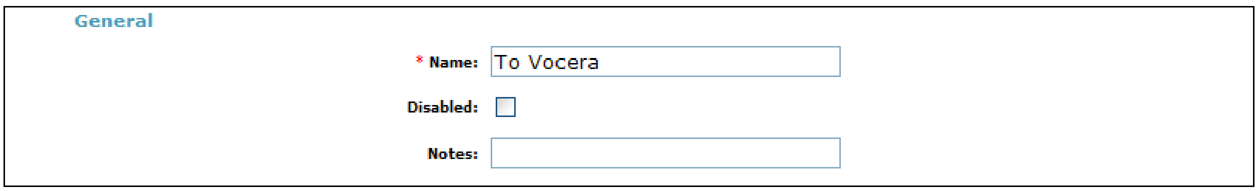
Routing Policies associate destination SIP Entities (**Section 5.3**) with Time of Day admission control parameters (**Section 5.5**) and Dial Patterns (**Section 5.7**). In the reference configuration, Routing Policies are defined for:

- Inbound calls to Communication Manager.
- Outbound calls to Vocera

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

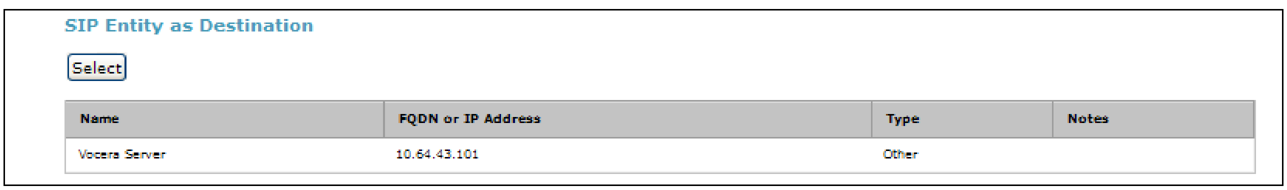
General section

- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.



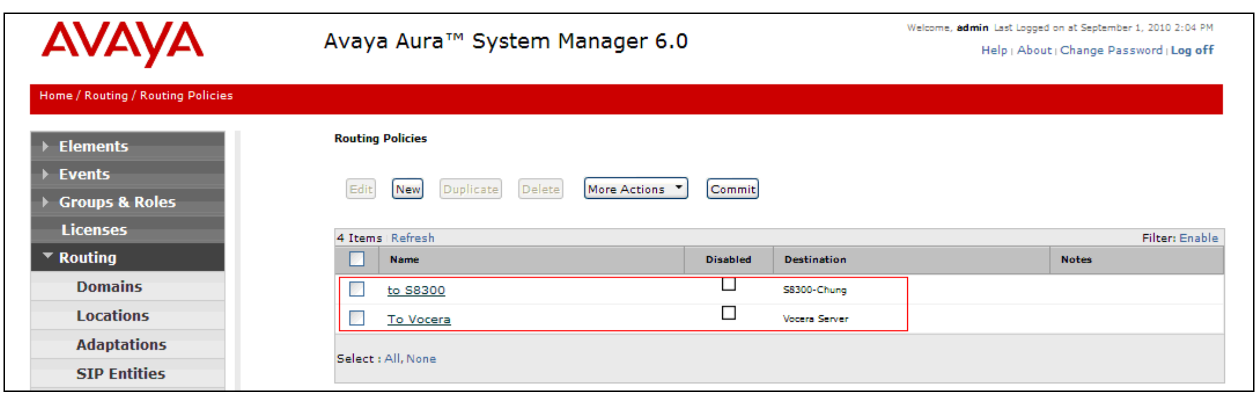
SIP Entity as Destination section

- Click the **Select** button.
- Select the SIP Entity that will be the destination for this call (not shown).
- Click the **Select** button and return to the Routing Policy Details form.



Leave default values for the Time of Day section.

Click **Commit** to save the Routing Policy definition. The following screen shows the Routing Policies used during the compliance test.



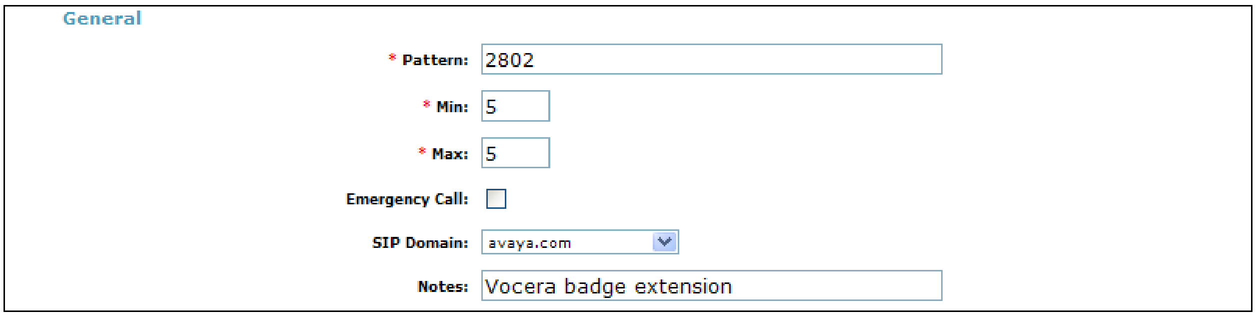
5.7. Dial Patterns

Dial Patterns define digit strings to be matched for inbound and outbound calls. In addition, the domain in the request URI is also examined.

To add a Dial Pattern, select **Routing → Dial Patterns,** and click on the **New** button (not shown) on the right. During the compliance test a 5 digit dial plan was utilized. Provide the following information:

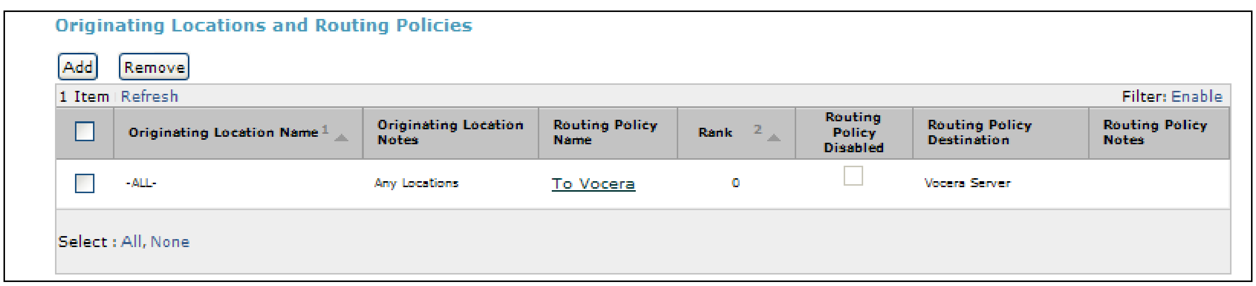
General section

- Enter a unique pattern in the **Pattern** field (e.g. **2802**).
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* by Session Manager from Communication Manager.
- Enter a description in the **Notes** field if desired.



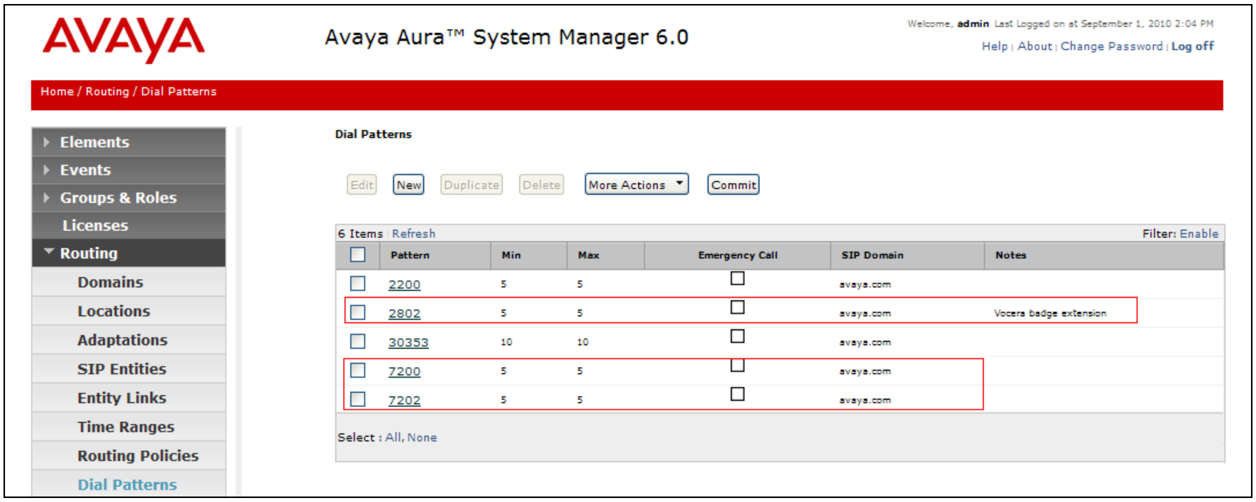
Originating Locations and Routing Policies section

- Click on the **Add** button and a window will open (not shown).
- Click on the boxes for the appropriate Originating Locations (see **Section 5.2**), and Routing Policies (see **Section 5.6**) that pertain to this Dial Pattern.
    - Location **10.64.41.0**.
    - Routing Policies **To Vocera**
    - Click on the **Select** button and return to the Dial Pattern window.



	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		Vocera Server	

Click the **Commit** button to save the new definition. The following screen shows the dial patterns used during the compliance test.

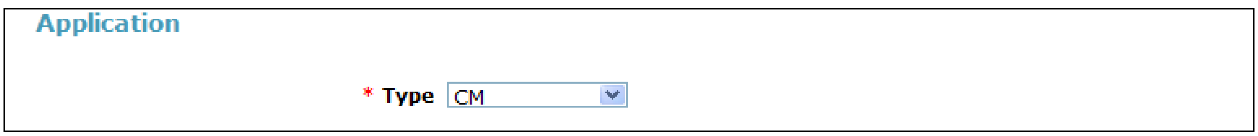


5.8. Configure Managed Elements

To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

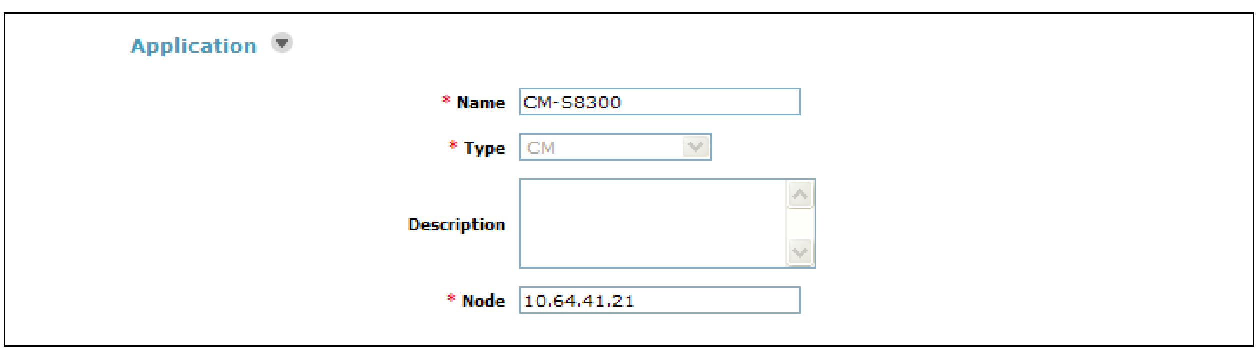
In the **New Entities Instance** Page

- In the Type field, select **CM** using the drop-down menu, and the New CM Instance page opens.



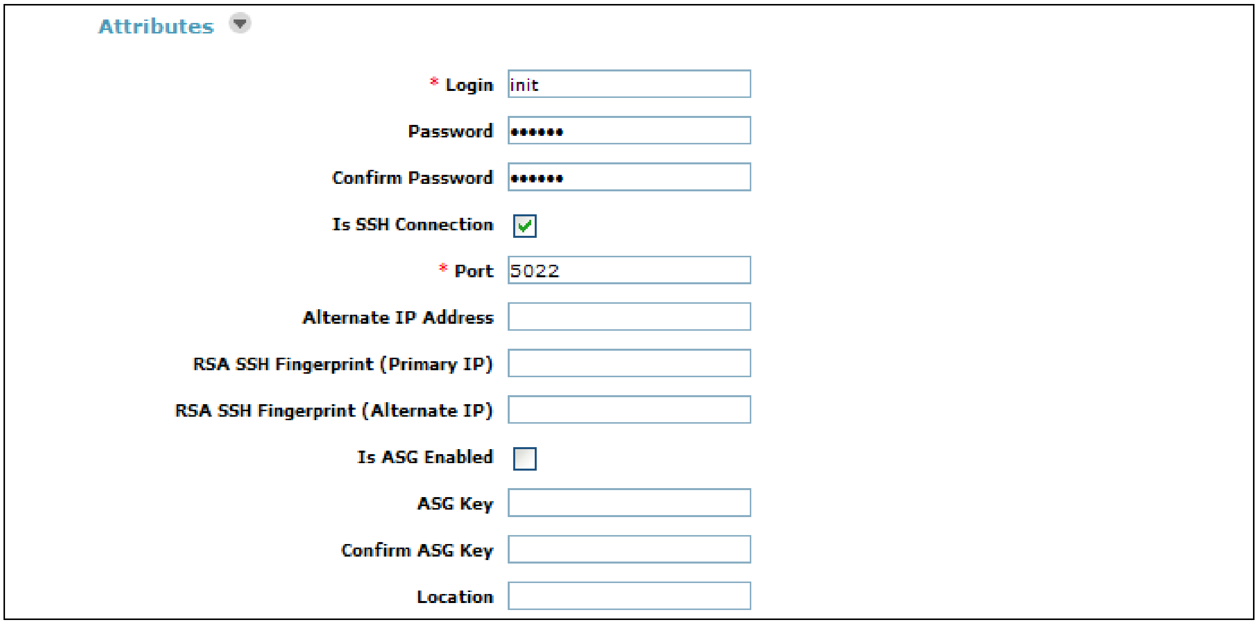
In the New CM Instance Page, provide the following information:

- Application section
  - **Name –** Enter the name for Communication Manager Feature Server.
  - **Description -** Enter description if desired.
  - **Node –** Enter IP address of the Communicatio Manager administration interface. During the compliance test, the procr IP address (10.64.41.21) was utilized.



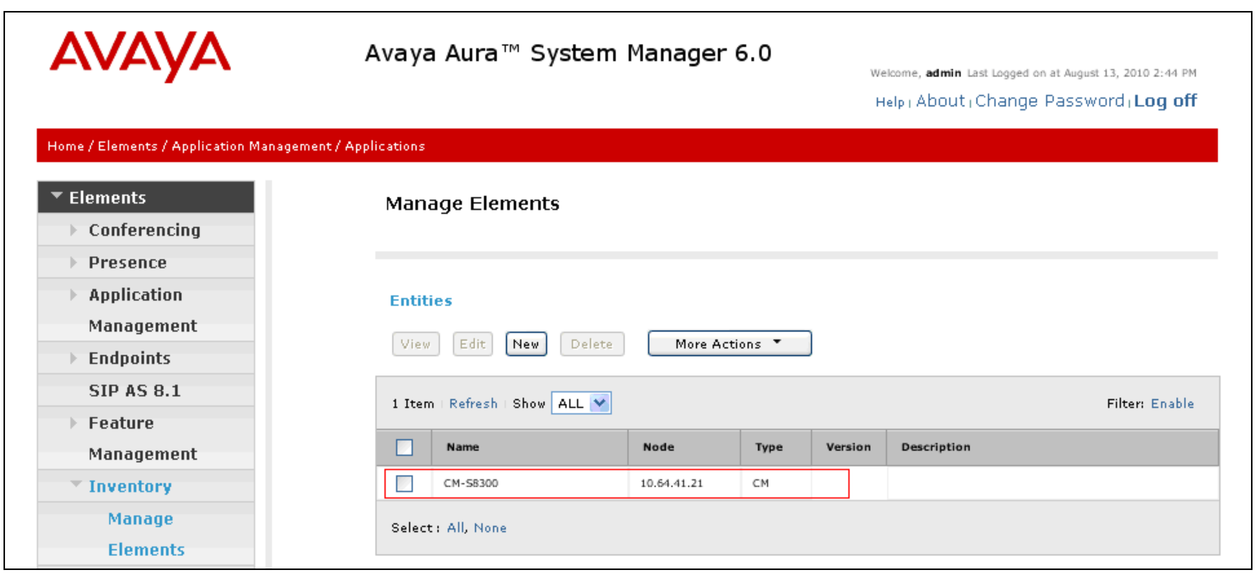
- Leave the fields in the Port and Access Point sections blank. In the SNMP Attributes section, verify the default value of **None** is selected for the Version field.

- Attributes section.
System Manager uses the information entered in this section to log into Communication Manager Feature Server using its administration interface. Enter the following values and use default values for remaining fields.
    - **Login –** Enter login used for administration access to Communciation Manager
    - **Password –** Enter password used for administration access to Communication Manger
    - **Confirm Password –** Repeat value entered in above field.
    - **Is SSH Connection –** Check the check box**.**
    - **Port –** Verify **5022** has been entered as default value



Click **Commit** to save the element.

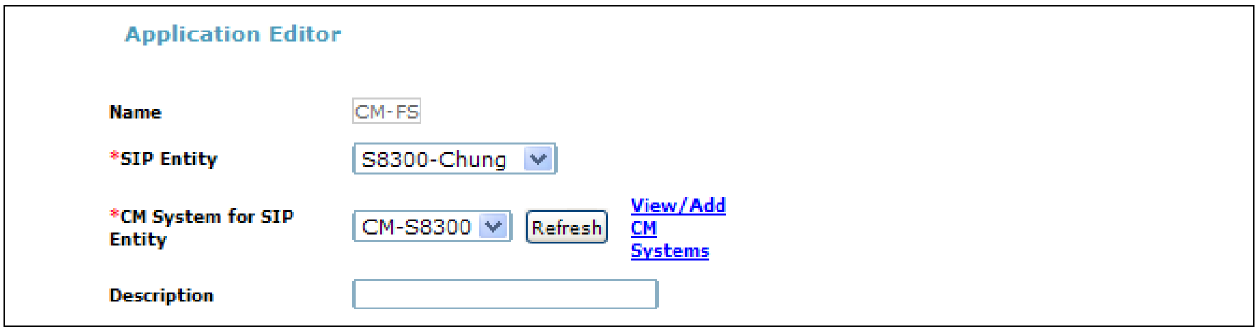
The following screen shows the element created, CM-S8300, during the compliance test.



5.9. Configure Applications

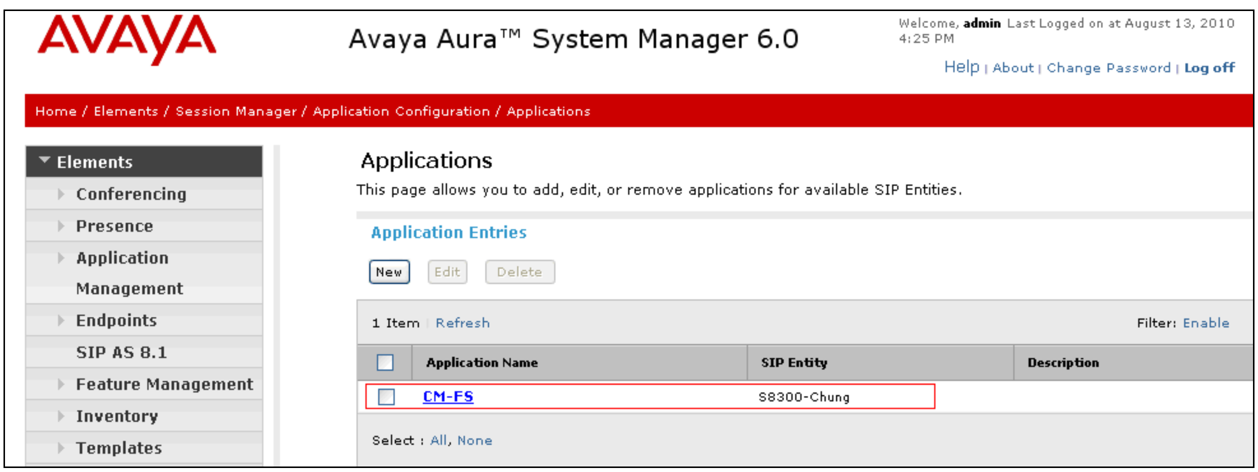
To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page, and provide the following information:

- Application Editor section
    - **Name** – Enter a name for the application.
    - **SIP Entity** - Select the SIP Entity for Communication Manager Feature Server defined in **Section 5.3**
    - **CM System for SIP Entity** – Select the name of the Managed Element defined for Communication Manager in **Section 5.8**
    - **Description** – Enter a description if desired.



- Leave fields in the Application Attributes (optional) section blank.

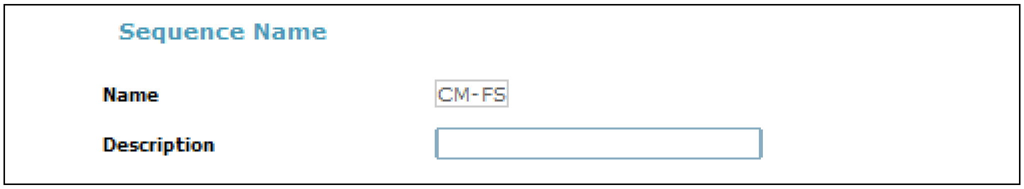
Click the **Commit** button (not shown) to save the Application. The screen below shows the Application, CM-FS, defined for Communication Manager.



5.10. Define Application Sequence

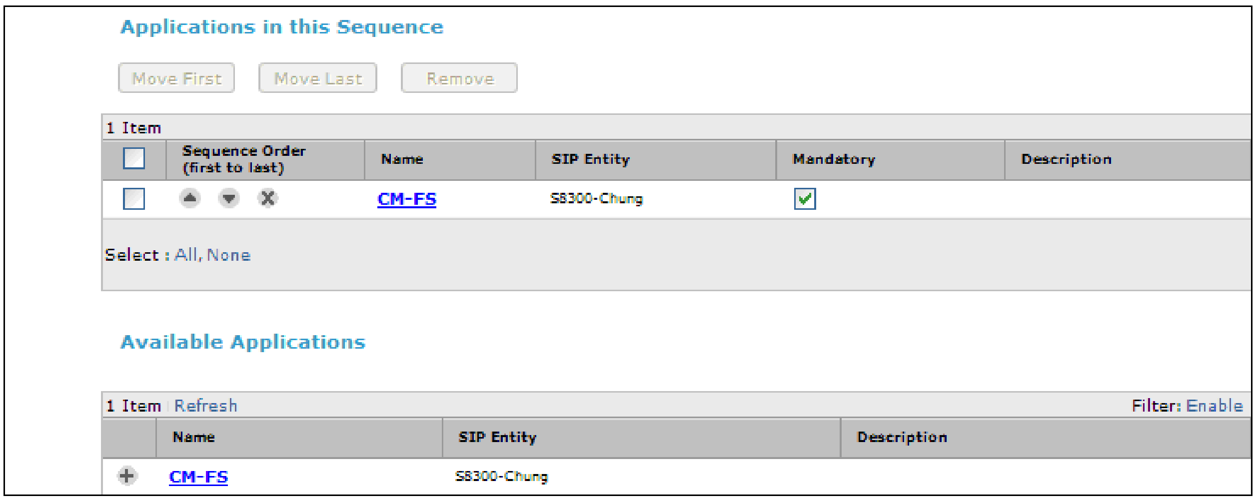
Navigate to **Elements → Session Manager → Application Configuration → Application Sequences**. Click **New** (not shown) and provide the following information:

- Sequence Name section
    - **Name** – Enter a name for the application
    - **Description** – Enter a description, if desired.

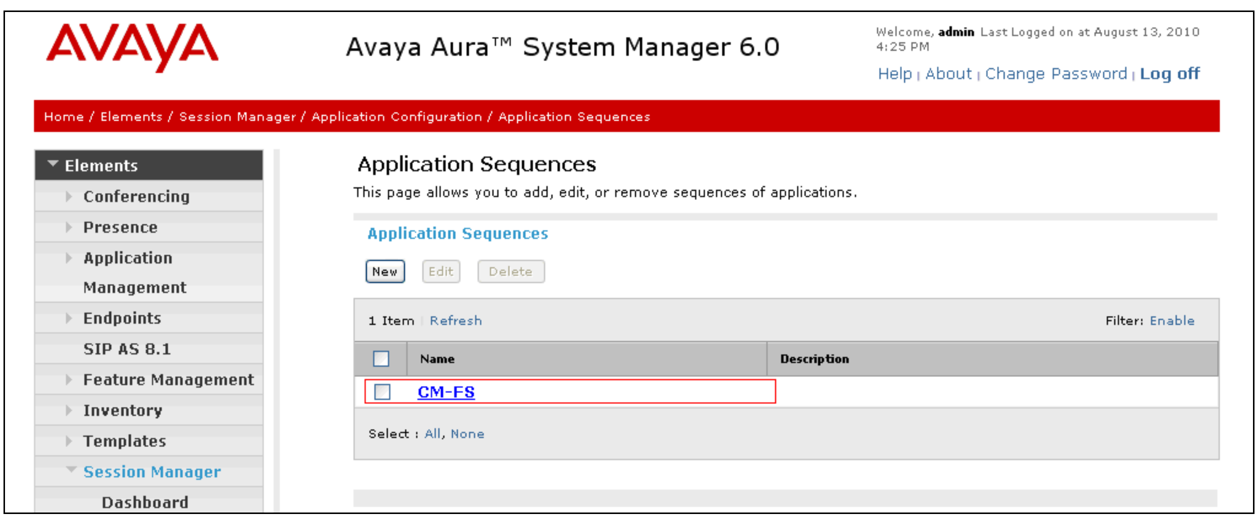


- Available Applications section
  - Click icon associated with the Application for Communication Manager defined in **Section 5.9** to select this application.
  - Verify a new entry is added to the Applications in this Sequence table as shown below.

Click the **Commit** button (not shown) to save the new Application Sequence.



The screen below shows the Application Sequence, CM-FS, defined during the compliance test.



6. Configure Vocera Communications System

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]. The Vocera Communications System is configured using a web based console interface using appropriate credentials.

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 voice interface, and prompted for a badge user to contact.
- 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.

During the compliance test, 5 digit and 10 digit dialing plans were utilized. The first test was executed utilizing 5 digits. The second test utilized 10 digits. For 10 digit calling, the following modifications have to be implemented.

- Modification in Avaya Aura™ Communication Manager (uniform-dialplan and aar analysis forms):

```
display uniform-dialplan 303                                        Page   1 of   2
                       UNIFORM DIAL PLAN TABLE
                                                              Percent Full: 0

  Matching                    Insert                Node
  Pattern        Len  Del     Digits       Net  Conv  Num
30353             10   0                   aar   n
```

```
display aar analysis 303                                            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
   30353                       10    10    92        aar             n
```

- Modification in Avaya Aura™ Session Manager (Dial Pattern in Routing Policies):

Dial Patterns

Add Remove

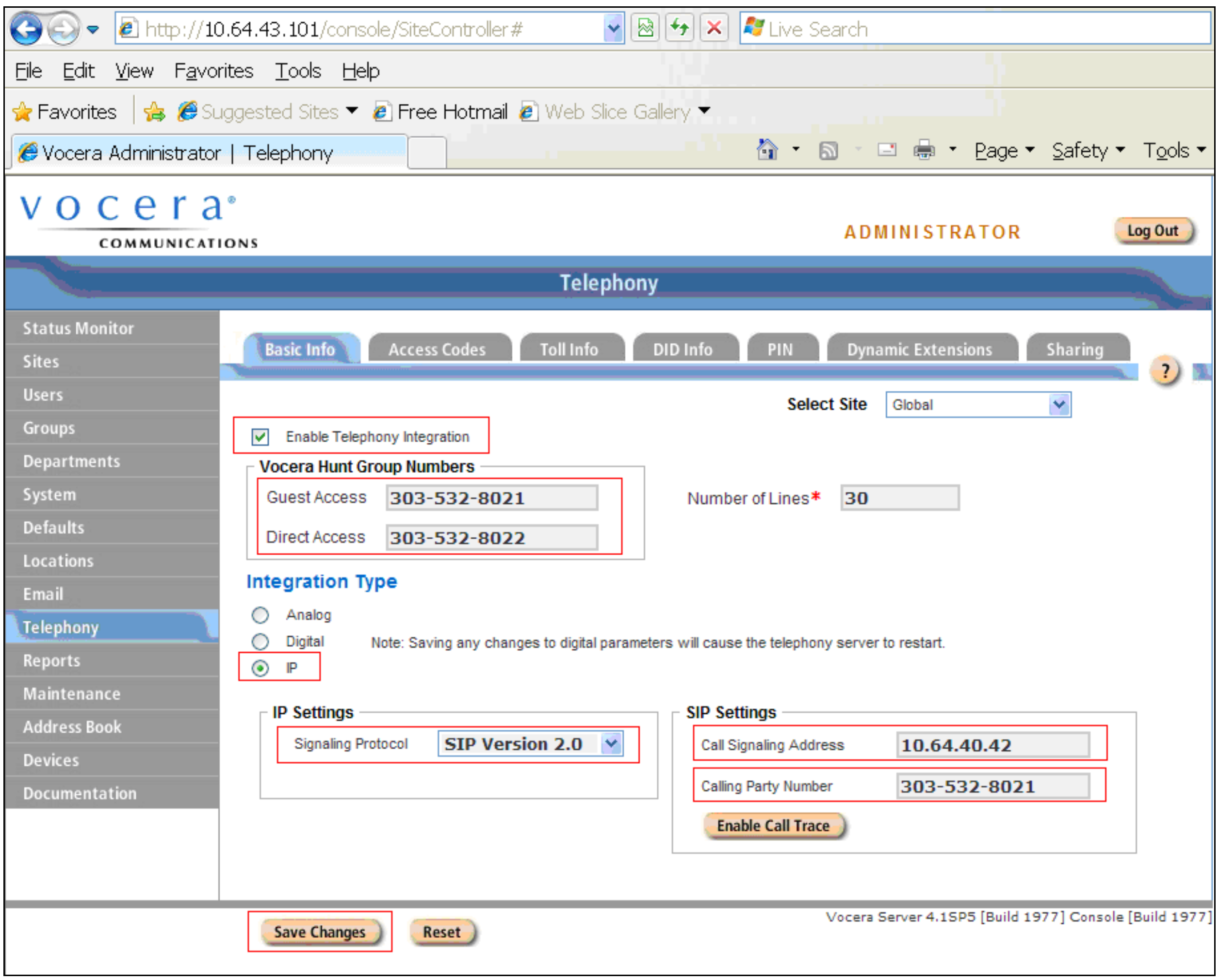
2 Items Refresh — Filter: Enable

	Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
☐	2802	5	5	☐	avaya.com	-ALL-	Vocera Domain Numbers
☐	30353	10	10	☐	avaya.com	-ALL-	

Select : All, None

Launch a web browser, enter **http://<IP address of Vocera Server>/console/AdminController** in the URL, and log in with the appropriate credentials. Once at the Administrator page, select the 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 – x28021
    - Direct Access Number – x28022
    - Three user extensions: x28023, x28024, x28025
- 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 the Avaya Aura™ Session Manager IP address for the Call Signaling Address field under the SIP Settings section. During the compliance test, IP address, **10.64.40.42**, was utilized.
- Enter the Call Party extension Number. During the compliance test, Calling Party Number, **x28021**, was utilized.
- Click on the **Save Changes** button.



7. General Test Approach and Test Results

The general test approach was to place calls to and from the Vocera Communications System and exercise basic telephone operations. The main objectives were to verify that:

- Calls can be successfully established between Vocera Communications System and Avaya SIP and H.323 telephones.
- Calls were able to Hold /unHold.
- Vocera Communications System successfully negotiates the right codec (G.711MU, G.711A).
- Vocera Communications System successfully blind transfers a call.
- Vocera Communications System successfully consult transfers a call.
- Vocera Communications System successfully conferences three party calls.
- Successfully tested DTMF using the vector steps.

For serviceability testing, failures such as cable pulls and hardware resets were applied.

The test objectives were verified. For serviceability testing, the Vocera Communications System operated properly after recovering from failures such as cable disconnects, and resets of the Vocera Communications System and the Avaya Aura™ Session Manager.

8. Verification Steps

The following steps may be used to verify the configuration:

- Verify the SIP trace, using traceSM from Avaya Aura™ Session Manager.
- Place calls to and from the Vocera Communications System and verify that calls are successfully established with two-way talk path. Select the Vocera SIP Entity. Verify the Conn. Status and Link Status are **Up**.
- While calls are established, Enter **status trunk <t/r>** command, where **t** is the SIP trunk group configured in **Section 4.6**, and **r** is the trunk group member used for a call.

9. Conclusion

Vocera Communications System was compliance tested with Avaya Aura™ Communication Manager (Version 6.0) and Avaya Aura™ Session Manager (Version 6.0). Vocera Communications System (Vocera Server and SIP Telephony Gateway Version 4.1 SP5 – build 1977) functioned properly for features and serviceability. During compliance testing, Vocera Communications System successfully placed and received calls to and from SIP and non-SIP telephones, and executed other telephony features like transfer, conference and DTMF.

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™ System Manager*, Release 6.0, June 2010.

The following document was provided by Vocera.

[3] *Vocera Communications System Quick Start Guide*, Document Version 1.2, October 2009.

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.