Avaya Solution & Interoperability Test Lab

Application Notes for Veramark VeraSMART with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Veramark VeraSMART call accounting software to successfully interoperate with Avaya Aura® Communication Manager.

Veramark VeraSMART eCAS is a call accounting software that interoperates with Avaya Aura® Communication Manager over the Avaya Reliable Session Protocol (RSP). Call records can be generated for various types of calls. Veramark VeraSMART collects, and processes the call records.

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

The overall objective of this interoperability compliance testing is to verify that the Veramark VeraSMART eCAS call accounting software can interoperate with Avaya Aura® Communication Manager 6.2. Veramark VeraSMART eCAS connects to Communication Manager over the local or wide area network using a CDR link running on RSP. Avaya Aura® Communication Manager is configured to send CDR records to Veramark VeraSMART eCAS using a specific port.

VeraSMART eCAS Call Accounting provides traditional call collection, rating, and reporting for any size businesses. VeraSMART eCAS Call Accounting can interface with most telephone systems - in particular, with the Avaya Aura® Communication Manager - to collect and interpret the detailed records of inbound, outbound, tandem, and internal telephone calls. VeraSMART eCAS Call Accounting then calculates the appropriate charge for local, long distance, international & special calls and allocates them to responsible parties.

During the test, SIP endpoints were included. SIP endpoints registered with Avaya Aura® Session Manager. An assumption is made that Avaya Aura® Session Manager and Avaya Aura® System Manager are already installed and basic configuration have been performed.

Only steps relevant to this compliance test will be described in this document. In these Application Notes, the following topics will be described:

- Avaya Aura® Communication Manager – A SIP trunk configuration between Avaya Aura® Communication Manager and Avaya Aura® Session Manager. A CDR link configuration on Avaya Aura® Communication Manager.
- Avaya Aura® Session Manager – SIP trunk configuration between Avaya Aura® Communication Manager and Avaya Aura® Session Manager.
- Veramark VeraSMART eCAS – A CDR link configuration on VeraSMART eCAS.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inbound trunk and outbound trunk calls, transfer, conference, and verify that Veramark VeraSMART eCAS collects the CDR records, and properly classifies and reports the attributes of the call.

For serviceability testing, physical and logical links were disabled/re-enabled, Avaya Servers were reset and Veramark VeraSMART eCAS was restarted.

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 testing included features and serviceability tests. The focus of the compliance testing was primarily on verifying the interoperability between Veramark VeraSMART eCAS and Communication Manager.

2.2. Test Results

All executed test cases passed, except noted below. Veramark VeraSMART eCAS successfully collected the CDR records from Communication Manager via a RSP connection for all types of calls generated including intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, and conference calls.

For serviceability testing, Veramark VeraSMART eCAS was able to resume collecting CDR records after failure recovery including buffered CDR records for calls that were placed during the outages.

The following issues were observed:
Avaya side – These issues will be investigated or escalated. All are related to SIP endpoints

- During an Internal call, the call shows Incoming with the condition code “9”.
- During an outbound call from a SIP endpoint (either a PSTN or a trunk call), the call record shows two records; an inbound call to CM1 from SM, and an outbound call to other CM (CM2) from CM1 via a PRI trunk.
- When a call is coming from a trunk or from the PSTN and the call is transferred, the call record only shows a call (called to transferred-to). The call record does not show the initial call leg (calling to called party).
- Two condition code “I” records were observed from PSTN to CM1 phone.
- Difference between Pri and SIP trunk.
    - Using H323 phones on inbound inter-switch (PRI trunk) call scenario: Record shows Phone1→Phone2, and Phone1→Phone3.
    - Using SIP phones on inbound inter-switch (SIP trunk) call scenario: Record shows Phone1→Phone2, and Phone2→Phone3
- Outbound inter-switch call from SIP endpoint, the call record shows a call (called to conferenced-to) only. It does not show the initial call leg.
- Outbound Inter-switch call from SIP endpoint, Two problems noticed:
    - The initial leg shows outbound call instead of conference.
    - An extra record was recorded,
    - The third leg, which is a call between phone3 and phone2 are not recorded.
- During a blind Trunk to Trunk transfer (inbound) utilizing SIP endpoints, two call records received. However, both showed Inbound.
- When used H323 as a calling party, instead of PSTN (This make all internal call) for the transfer scenario, the call record only shows the first leg. The transferred-to leg does not show. For this call scenario, the call flow is following: 72001(H323) calls 72021 (SIP), then transfer to 72022(SIP).
- During a call scenario (SIP endpoint1 calls SIP endpoint2, and SIP endpoint 2 transfers the call to PSTN), four call records were observed:

- A call record that supposed to be an internal call shows inbound call.
    - Call records include an extra record.

The other two outbound records have the same originator (in this case, Phone2). However, the duration of the calls are different

- During a call scenario (Place an outbound PSTN call from a SIP endpoint1. From the SIP endpoint1 conferences in another SIP endpoint2. Leave the conference active for at least 15 sec. Drop the SIP endpoint2 first and then hang up all other phones.), four call records were observed:
    - Call records include an extra record
    - There were two outbound call records (condition code '7') from the originator (SIP endpoint1), instead of the condition code "C". These two outbound records have the same originator (in this case, SIP endpoint1). However, the duration of the calls are different
- During a call scenario (Place an intra-switch call from SIP endpoint1 to SIP endpoint2. From SIP endpoint2, conference SIP endpoint3 via SIP trunk. Leave the conference active for at least 15 sec. Drop the SIP endpoint2 first and then hang up other phones.), four call records were observed:
    - Call records include an extra record
    - There were two outbound call records (condition code '7') from the SIP endpoint2, instead of the condition code "C". These two outbound records have the phone2. However, the duration of the calls are different

Veramark side

- For tandem calls VeraSMART reports the ANI number in the "Special Code" field.

2.3. Support

Technical support for VeraSMART eCAS can be obtained through the following:

- Phone: (585) 381-0115
- Email: tech_support@veramark.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of an Avaya S8300D Server running Communication Manager, an Avaya G450 Media Gateway, a Session Manager, and Veramark VeraSMART eCAS on one side, and Avaya S8720 Servers running Communication Manager with an Avaya G650 Media Gateway on the other side. Session Manager terminates SIP trunks from both sides. For completeness, Avaya 9600 Series SIP IP Telephones on the Avaya S8300D Server side have been registered to Session Manager. Avaya 9600 Series SIP IP Telephones on the Avaya S8720 Server side have been registered to SIP Enablement Services, and are included in Figure 1 to demonstrate calls between the SIP IP telephones that are going through Session Manager.

Since Avaya SIP Enablement Services (SES) is not a part of this compliance test (only the SIP endpoints were utilized), there will not be any discussion on configuring Avaya SES.

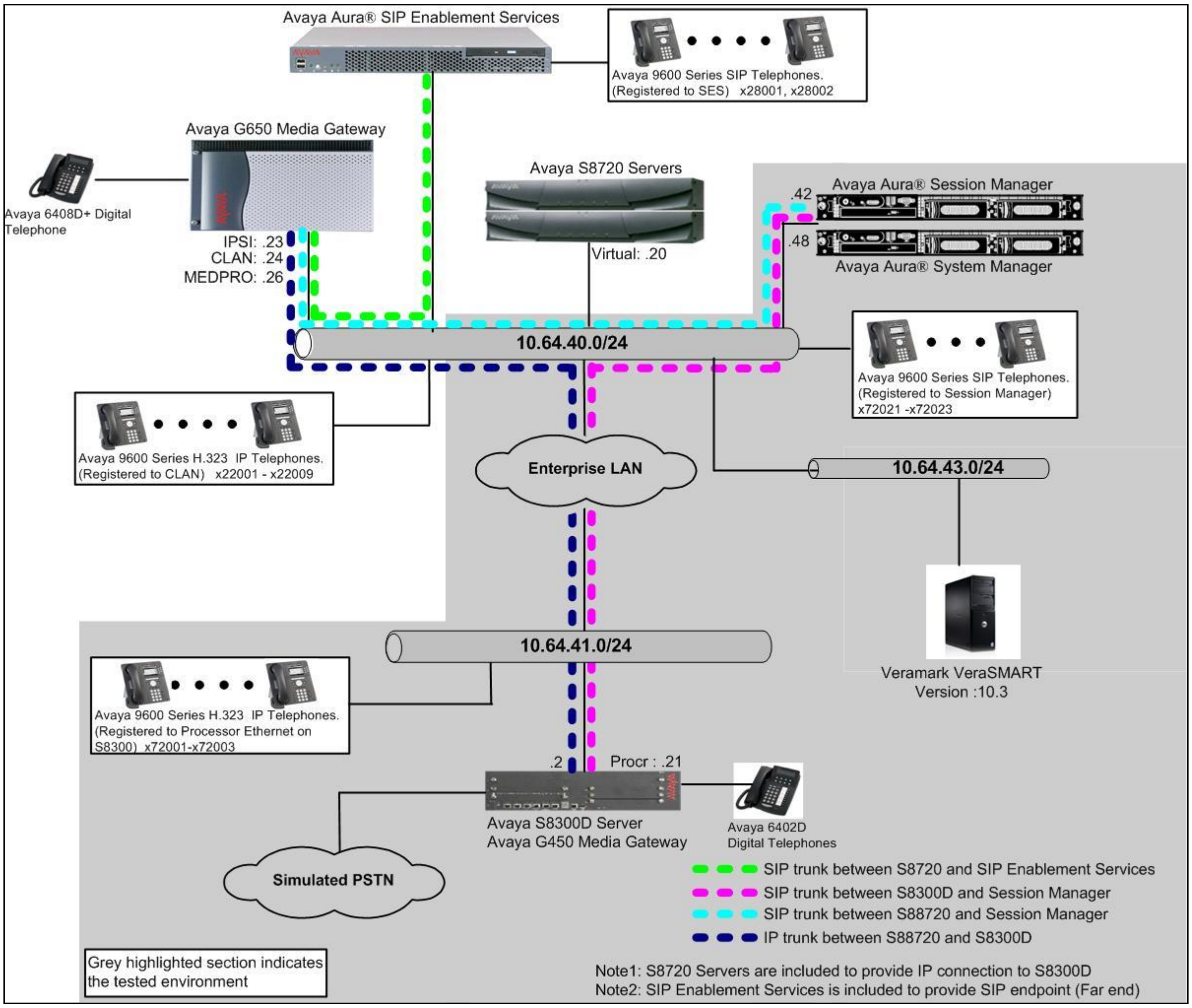


Figure 1. Test configuration of Veramark VeraSMART eCAS with Avaya Aura® Communication Manager

4. Equipment and Software Validated

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

Equipment		Software
Avaya S8300D Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.2 (R016x.02.0.823.0) with Patch 02.0.823.0-20001
Avaya Aura® System Manager		6.0.6.0
Avaya Aura® Session Manager		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 Aura® SIP Enablement Services		5.2.1 (SES-5.2.1.0-016.4) with Service Pack SES-5.2.1.0-016.4-SP3b
Avaya 9600 Series SIP IP Telephone		
	9620 9630 9650	2.6.8 2.6.8 2.6.8
Avaya 9600 Series H.323 IP Telephone		
	9620 9630 9650	3.1 3.1 3.1
Veramark VeraSMART eCAS on Windows 2003 Server with Service Pack 2		10.3 SP5 (Build 186.35.5.1)

5. Configure Aura® Avaya Communication Manager

This section describes the procedure for configuring call detail recording (CDR) in Communication Manager. These steps are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8300D Server. All steps are the same for the other Avaya Servers. Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the PC running Veramark VeraSMART eCAS. For the Avaya S8300D Media Server, the RSP link originates at the IP address of the local processor (with node-name - “procr”

5.1. Configure CDR

Use the **change node-names ip** command to create a new node name, for example, **verasmart**. This node name is associated with the IP Address of the PC running the Veramark VeraSMART eCAS application. Also, take note of the node name – "procr". It will be used in the next step. The "procr" entry on this form was previously administered.

```
change node-names ip                                                Page   1 of   2
                                  IP NODE NAMES
    Name              IP Address
verasmart           10.64.43.249
default             0.0.0.0
procr               10.64.41.21
procr6              ::
rdtt-1              10.64.40.14
SM-1                10.64.41.42
```

Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, provide the following information:

- **Service Type**: **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node**: **procr** [For the Avaya S8720 Server, set the Local Node to the node name of the CLAN board.]
- **Local Port**: **0** [The Local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.]
- **Remote Node**: **veramark** [The Remote Node is set to the node name previously defined.]
- **Remote Port**: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in Veramark VeraSMART.]

```
change ip-services                                                  Page   1 of   4

                                   IP SERVICES
 Service      Enabled     Local        Local        Remote       Remote
  Type                    Node         Port         Node         Port
AESVCS          y       procr         8765
CDR1                    procr         0        verasmart          9000
CDR2                    procr         0        rdtt-1             9001
```

On **Page 3** of the ip-services form, enable the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to "y".

```
change ip-services                                                  Page   3 of   4

                              SESSION LAYER TIMERS
  Service      Reliable   Packet Resp   Session Connect  SPDU  Connectivity
   Type        Protocol     Timer        Message Cntr    Cntr     Timer

 CDR1             y          30                3           3        60
 CDR2             y          30                3           3        60
```

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- **CDR Date Format**: "month/day"
- **Primary Output Format**: "unformatted"
- **Primary Output Endpoint**: "CDR1"

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats?**: "n" [Allows CDR formats to use 4.x CDR formats. If the field is set to "y", then CDR formats utilize the 3.x CDR formats.]
- **Intra-switch CDR**: "y" [Allows call records for internal calls involving specific stations. Those stations must be specified in the INTRA-SWITCH CDR form.]
- **Record Outgoing Calls Only?**: "n" [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting?**: "y" [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting?**: "y" [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]
- **Call Account Code Length:** "6" [The length may be set to a value between 1 and 15. However, during the compliance test, "6" was used.]

```
change system-parameters cdr                                   Page   1 of   2
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                           CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format: unformatted Secondary Output Endpoint: CDR2
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? y
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? n                 Remove # From Called Number? n
Modified Circuit ID Display? n                              Intra-switch CDR? y
                  Record Outgoing Calls Only? n      Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? n       Outg Attd Call Record? n
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                   Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? y       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                  Inc Attd Call Record? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 6
```

If the **Intra-switch CDR** field is set to "y" on **Page 1** of the **system-parameters cdr** form, then use the **change intra-switch-cdr** command to define the extensions that will be subject to call detail records. In the Assigned Members field, enter the specific extensions whose usage will be tracked.

Note: To simplify the process of adding multiple extensions in the Assigned Members field, the **Intra-switch CDR by COS (SA8202)** feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

```
change intra-switch-cdr                                         Page   1 of   3
                           INTRA-SWITCH CDR

                                Assigned Members:   9    of 1000   administered
   Extension              Extension              Extension              Extension
   72001
   72002
   72003
```

5.2. 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. Set to the appropriate domain. During the compliance test, the authoritative domain is set to "avaya.com".
- **Codec Set** – Set the codec set number as provisioned in the **IP Codec Set** form.

```
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
```

5.3. Configure IP Node Name

This section describes the steps for setting IP node name for Session Manager in Communication Manager. Enter the **change node-names ip** command, and add a node name for **SM-1** (Session Manager) along with its IP address.

```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                IP Address
verasmart              10.64.43.249
default                0.0.0.0
procr                  10.64.41.21
procr6                 ::
rdtt                   10.64.40.14
SM-1                   10.64.41.42
```

5.4. Configure SIP Signaling

This section describes the steps for administering a signaling group in Communication Manager for signaling between Communication Manager and Session Manager. Enter the **add signaling-group <s>** command, where **s** is an available signaling group and configure the following:

- **Group Type** – Set to "sip".
- **Transport Method** – Set to "tls".
- **Near-end Node Name** - Set to "procr" as displayed in **Section 5.3**.
- **Far-end Node Name** - Set to the "SM-1" configured in **Section 5.3**.
- **Far-end Network Region** - Set to the region configured in **Section 5.2**.
- **Far-end Domain** - Set to "avaya.com". This should match the SIP Domain value in **Section 5.2**.
- **Direct IP-IP-Audio Connections:** Set to "y"

```
add signaling-group 92                                          Page   1 of   1
                                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? y                    Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n             Alternate Route Timer(sec): 3
```

5.5. Configure SIP Trunk

This section describes the steps for administering a trunk group in Communication Manager for trunking between Communication Manager and Session Manager. Enter the **add trunk-group <t>** command, where **t** is an unallocated 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.
- **Signaling Group** – Set to the Group Number field value configured in **Section 5.4**.
- **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: r
  Group Name: No IMS 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: 10
```

5.6. Configure Uniform Dial Plan

This section describes the steps for administering a uniform dial plan in Communication Manager. Enter **change uniform-dialplan <u>**, where **u** is the uniform-dialplan number. The following screen shows the Uniform Dial Plan configuration. The 5-digit extension range starting with 2xxxx was used for the Avaya S8720 Servers side SIP telephones, and utilized Automatic Alternate Routing (AAR).

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

  Matching                    Insert              Node
  Pattern         Len Del     Digits     Net Conv Num
 2                  5   0                aar   n
```

5.7. Configure Automatic Alternate Routing

Enter **change aar analysis <a>**, where **a** is the AAR number. Automatic Alternate Routing (AAR) was used to route calls to the appropriate route pattern. The 5-digit extension range starting with 22 was used the route pattern 11. 22xxx extensions are H.323 IP phones in S8720. To call these H.323 IP phones from S8300D Server, utilizes the route pattern 11 which is an ISDN/PRI trunk. On the other hand, to call the 5-digit extension range starting with 28 used the route pattern 92. 28xxx extensions are SIP IP phones in S8720/SIP Enablement Services. To call these SIP IP phones from S8300D Server, utilizes the route pattern 92 which is a SIP trunk.

```
change aar analysis 2                                              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
    20004                   5    5       91        unku           n
    22                      5    5       11        aar            n
    28                      5    5       92        aar            n
    33                      5    5       91        unku           n
    415                     10   10      92        aar            n
    50000                   5    5       92        unku           n
    53005                   5    5       91        unku           n
```

5.8. Configure Route Pattern

Enter **change route-pattern <r>**, where **r** is the route-pattern number. The route pattern 92 routes calls to the trunk group 92, which is the SIP trunk to Session Manager.

```
change route-pattern 92                                            Page   1 of   3
                   Pattern Number: 210 Pattern Name: SIP-to-SM
                            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

     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
```

5.9. Configure Off-PBX-Telephone Configuration-Set

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when users (SIP endpoints) were created in Session Manager.

However, the off-pbx-telephone configuration-set form needs to be modified. Enter **change off-pbx-telephone configuration-set** and disable the **CDR for Calls to EC500 Destination?** field by setting it to "n".

```
change off-pbx-telephone configuration-set 2                    Page   1 of   1



                                     CONFIGURATION SET: 2

                         Configuration Set Description:
                                  Calling Number Style: network
                                   CDR for Origination: phone-number
                    CDR for Calls to EC500 Destination? n
                           Fast Connect on Origination? n
                          Post Connect Dialing Options: dtmf
                         Cellular Voice Mail Detection: timed  (seconds): 4
                                         Barge-in Tone? n
                           Calling Number Verification? y
             Call Appearance Selection for Origination: primary-first
                                      Confirmed Answer? n

 Use Shared Voice Connections for Second Call Answered? n
Use Shared Voice Connections for Second Call Initiated? n
```

6. Configure Avaya Aura® Session Manager

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

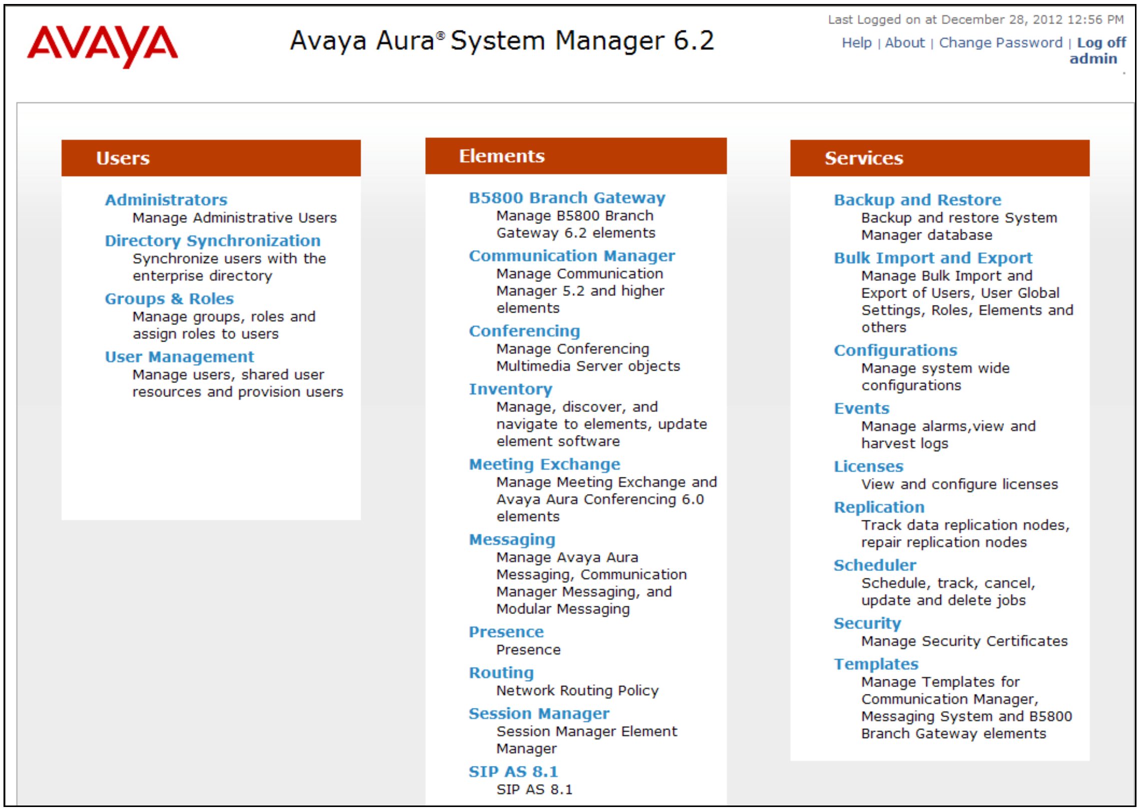
The following sections assume that Session Manager, and System Manager have been installed and that network connectivity exists between the two platforms.

In this section, the following topics are discussed:

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

6.1. Configure SIP Domain

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

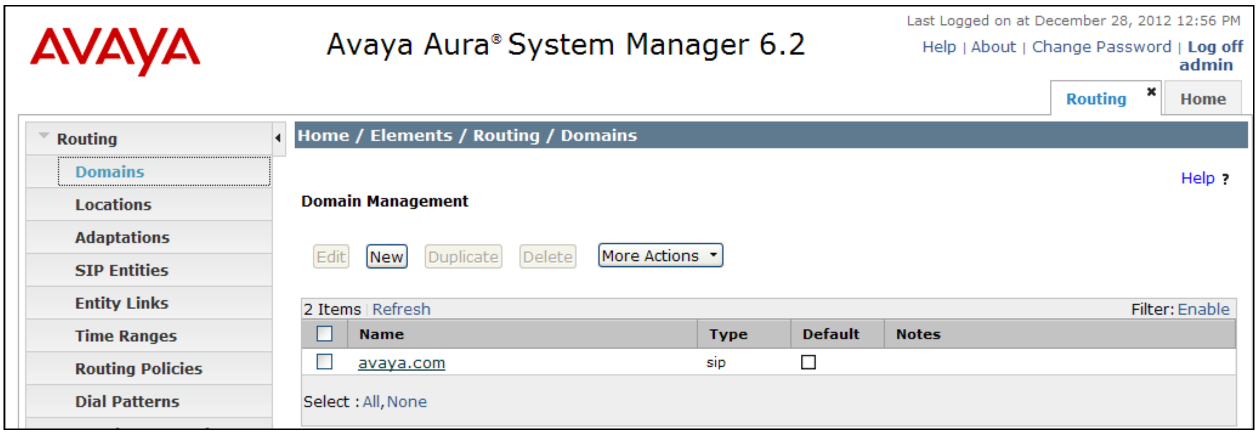


Navigate to **Elements→Routing → Domains**, and click on the **New** button (not shown) to create a new SIP Domain. Enter the following values and use default values for remaining fields:

- **Name –** Enter the Authoritative Domain Name specified in **Section 5.2**, which is **avaya.com**.
- **Type** – Select **SIP**

Click **Commit** to save.

The following screen shows the Domains page used during the compliance test.



6.2. 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.

<u>General section</u>
Enter the following values and use default values for remaining fields.

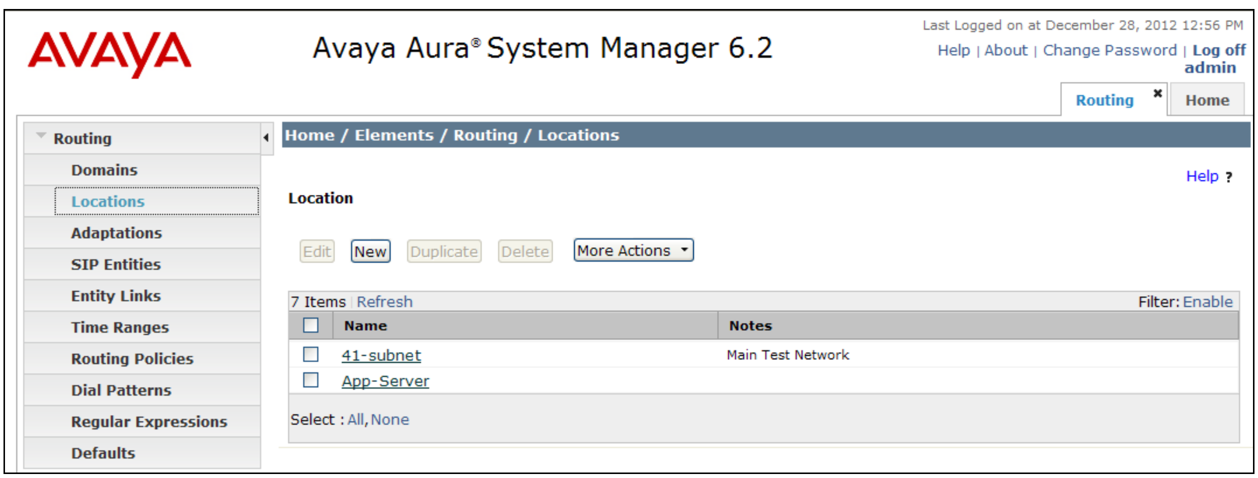
- Enter a descriptive Location name in the **Name** field (e.g. **41-subnet**).
- Enter a description in the **Notes** field if desired.

<u>Location Pattern section</u>
Click **Add** and enter the following values:

- Enter the IP address information for the **IP address Pattern** field (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.



6.3. 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. This entity was created prior to the compliance test.
- Communication Manager. This entity was created prior to the compliance test.

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

General section

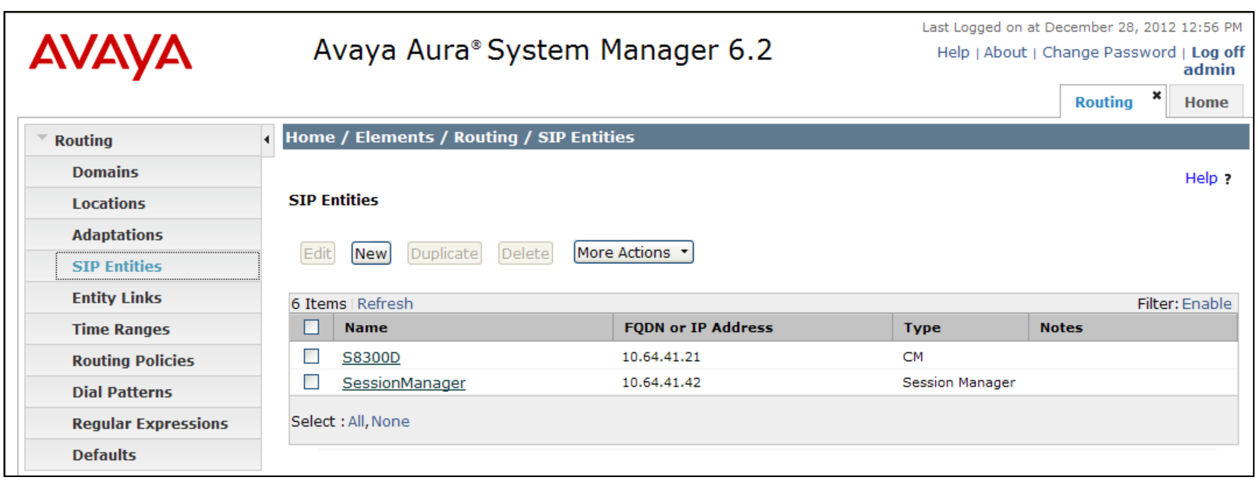
Enter the following values and use default values for remaining fields.

- Enter a descriptive Entity 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"
  - Others, select "Other"
- Enter a description in the **Notes** field if desired.
- Select the appropriate time zone.
- Accept the other default values.

SIP Link Monitoring section

Select the **Use Session Manager Configuration** using the drop-down list. Accept all other default values.

Click on the **Commit** button to save each SIP entity. The following screen shows the SIP Entities page used during the compliance test. Repeat all the steps for each new entity.



6.4. Configure Entity Links

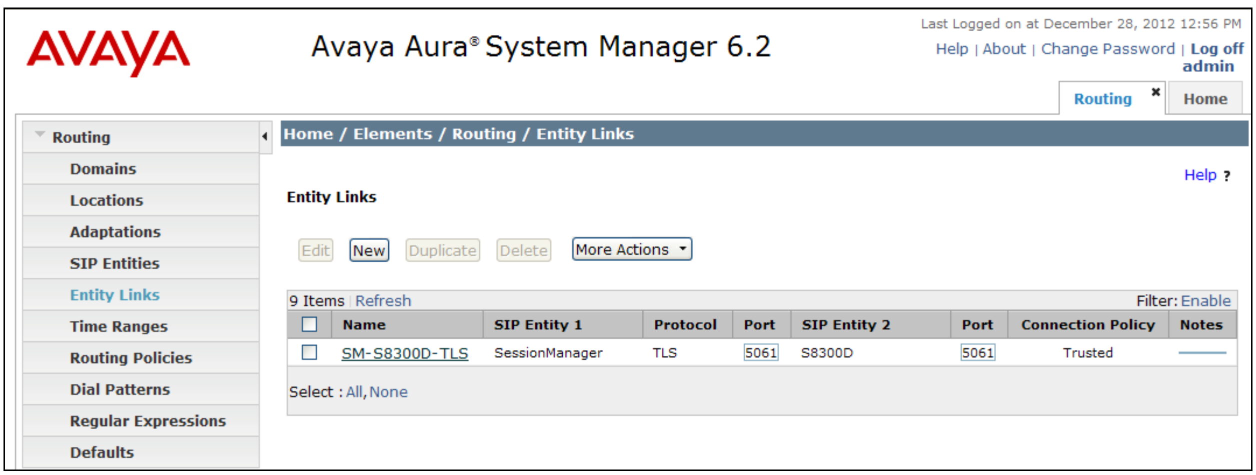
Entity Links define the connections between the SIP Entities and Session Manager. In the compliance test, the following entity links are defined from Session Manager.

- Session Manager ⇔ Communication Manager (Avaya S8300D Server). This entity link was created prior to the compliance test.

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 6.3** (e.g. "SessionManager").
- In the **Protocol** drop down menu, select the protocol to be used.
- In the **Port** field, enter the port to be used (e.g. "5060" or "5061").
  - TLS – "5061"
  - UDP or TCP – "5060"
- In the **SIP Entity 2** drop down menu, select one of the two entities in the bullet list above (which were created in **Section 6.3**).
- In the **Port** field, enter the port to be used (e.g. "5060" or "5061").
- Enter a description in the **Notes** field if desired.
- Accept the other default values.

Click on the **Commit** button to save each Entity Link definition. The following screen shows an Entity Links page used during the compliance test.



Repeat the steps to define Entity Link using a different protocol.

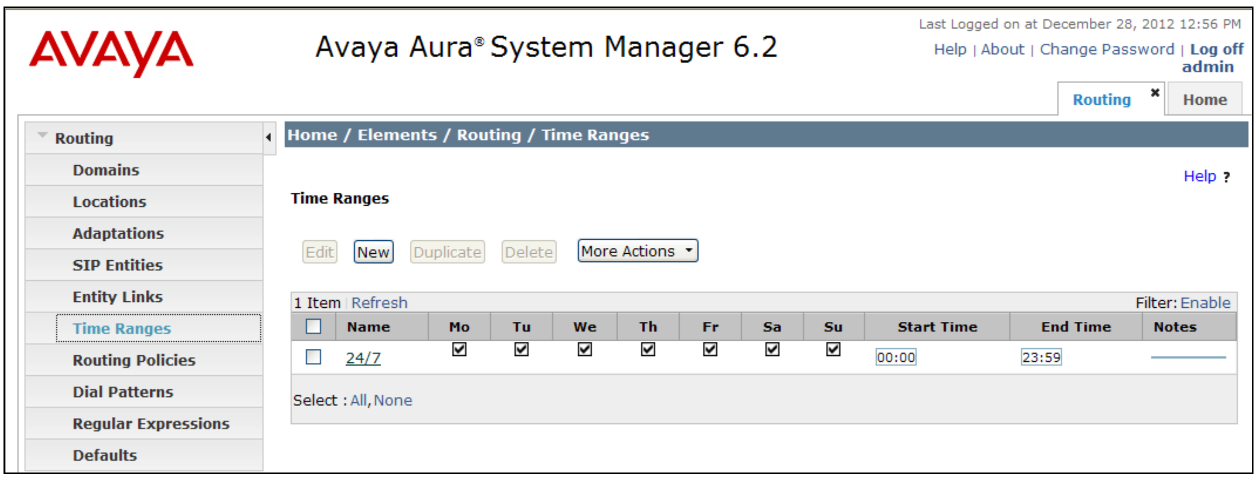
6.5. Time Ranges

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 **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.



6.6. Configure Routing Policy

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:

- H.323 calls to Communication Manager (S8300D) – 7200x
- SIP calls to Communication Manager (S8720)/ SIP Enablement Services – 2800x

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:

General section

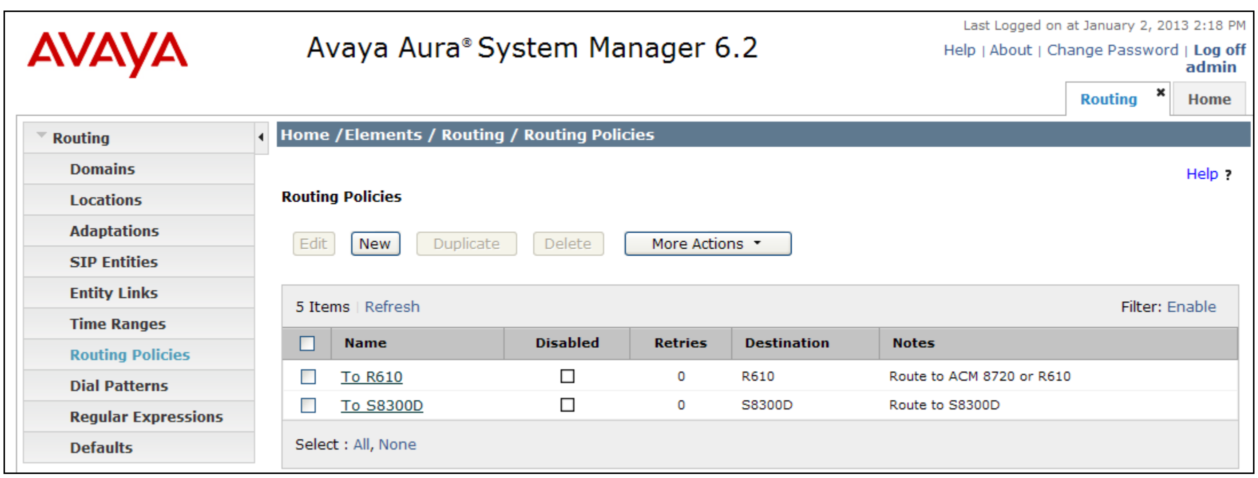
- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

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.

Time of Day section – Leave default values.

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



6.7. 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. In the compliance test, the following dial patterns are defined from Session Manager.

- 2800x – SIP endpoints in Avaya S8720 Servers/SIP Enablement Services
- 7200x – H.323 endpoints in Avaya S8300D Server

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

General section

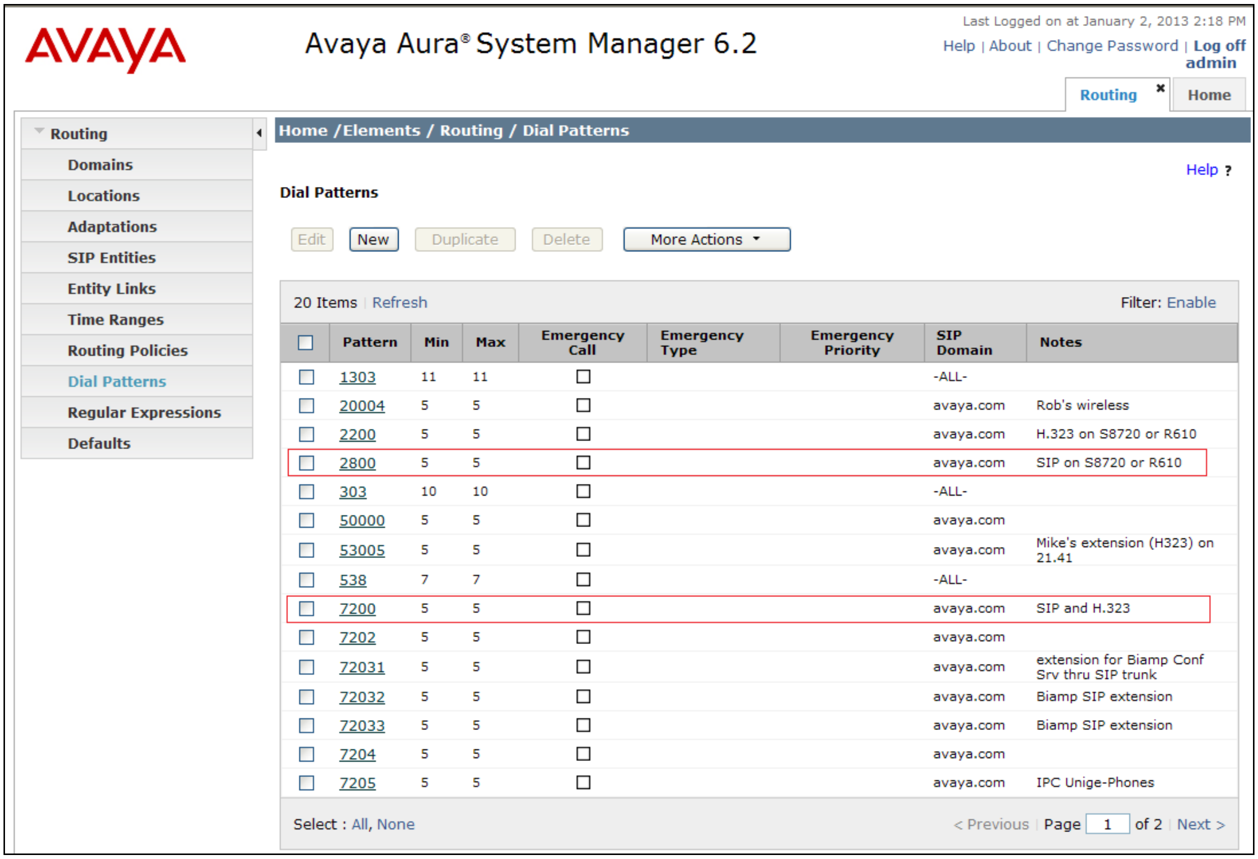
- Enter a unique pattern in the **Pattern** field.
- In the **Min** field enter the minimum number of digits (e.g. **5**).
- In the **Max** field enter the maximum number of digits (e.g. **5**).
- In the **SIP Domain** field drop down menu select the domain that will be contained in the Request URI *received* 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, and Routing Policies (see **Section 6.6**) that pertain to this Dial Pattern.
    - Originating Location –Check the **Apply The Selected Routing Policies to All Originating Locations** box.
    - Routing Policies **To S8300**.
    - Click on the **Select** button and return to the Dial Pattern window.

Click the **Commit** button to save the new definition.

The following screen shows the dial pattern used for S8300 during the compliance test.

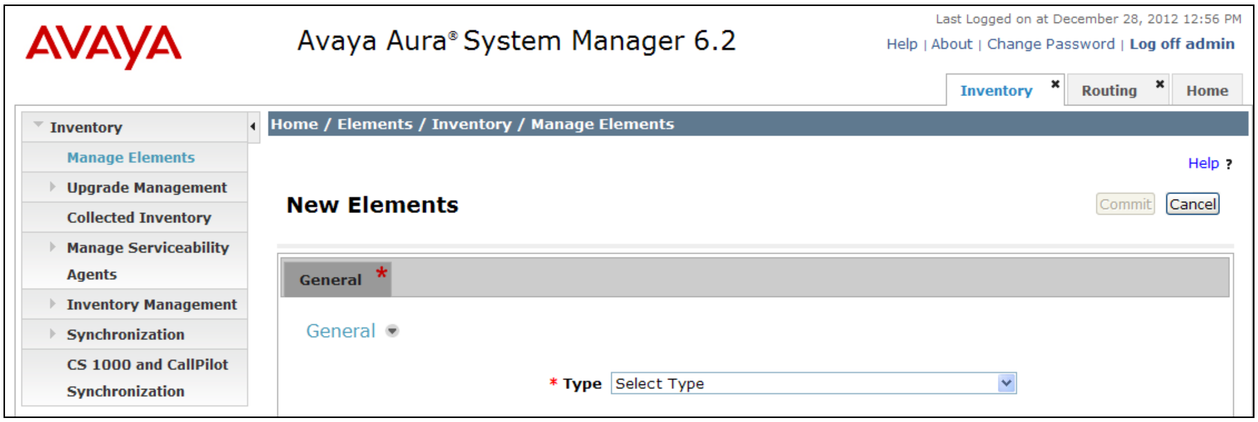


6.8. Configure Managed Elements

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

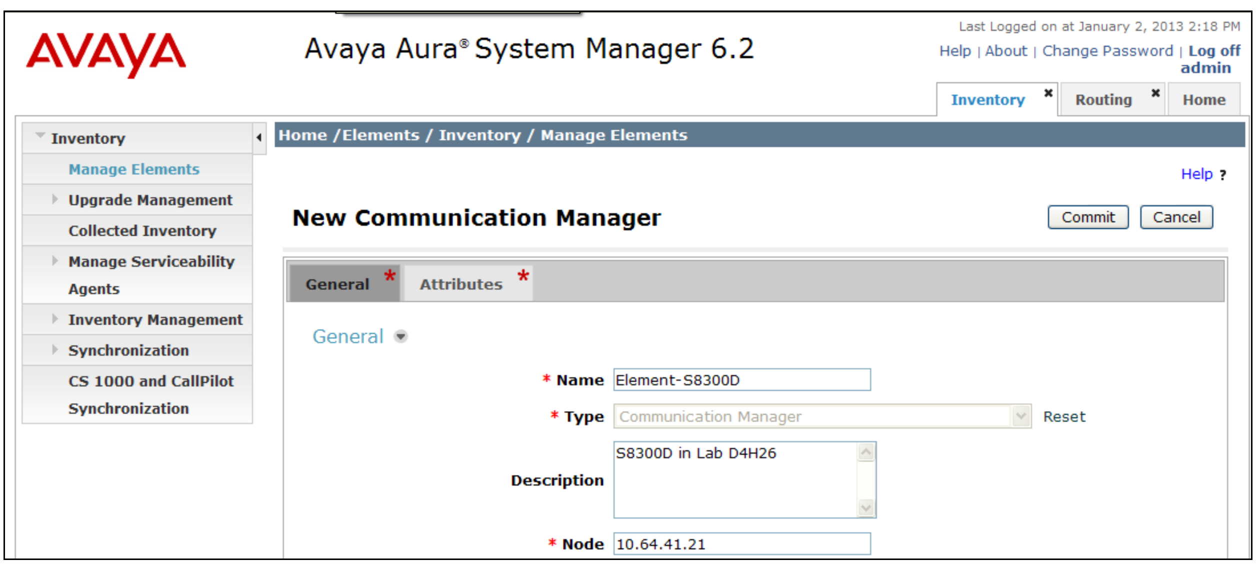
In the **New Elements** Page provide the following information:

- In the **Type** field, select "Communication Manager" using the drop-down menu, and the **New Communication Manager** page opens (not shown).



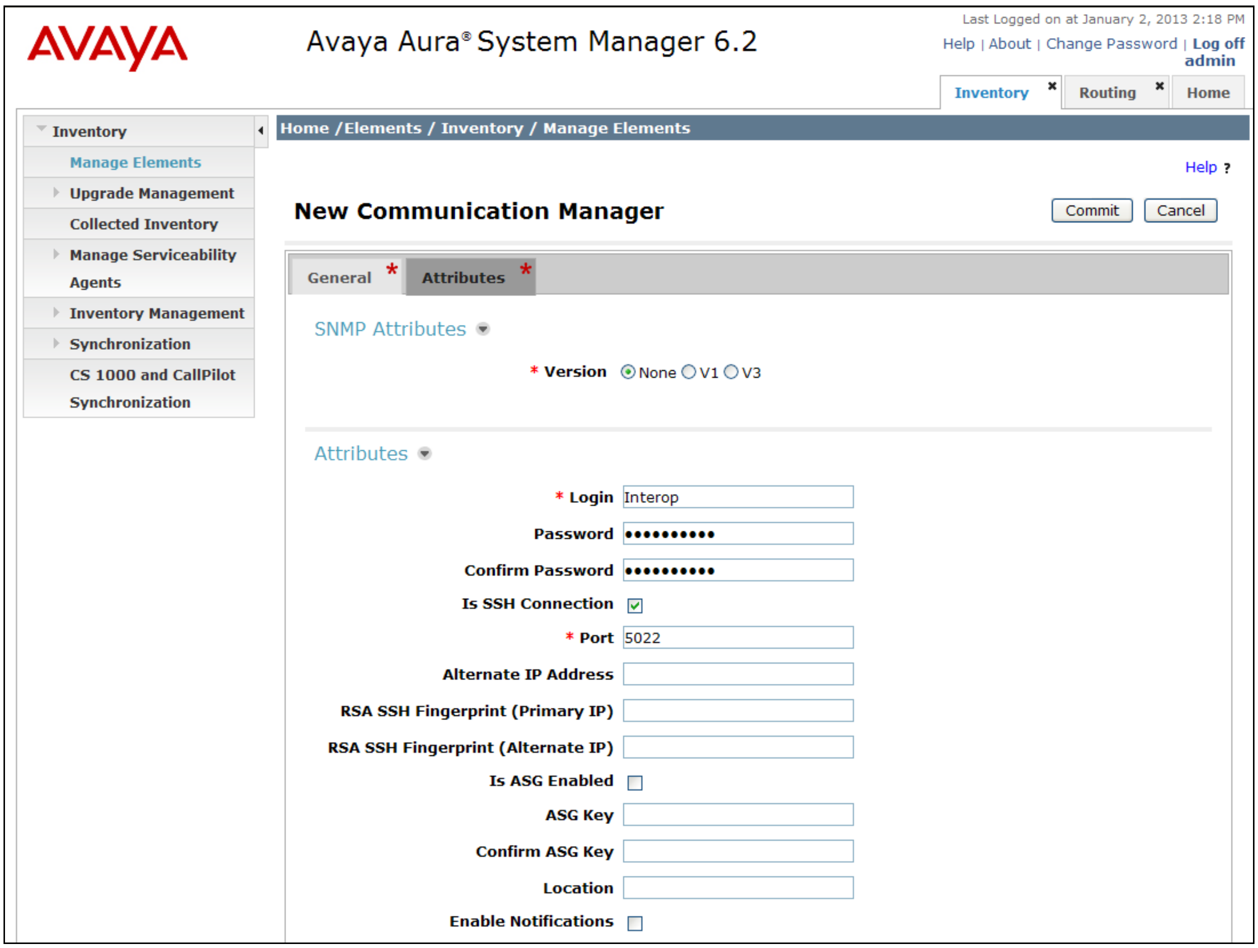
In the **New Communication Manager** Page, provide the following information:

- General section
  - **Name** – Enter name for Communication Manager Feature Server.
  - **Description -** Enter description if desired.
  - **Node –** Enter IP address of the 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.

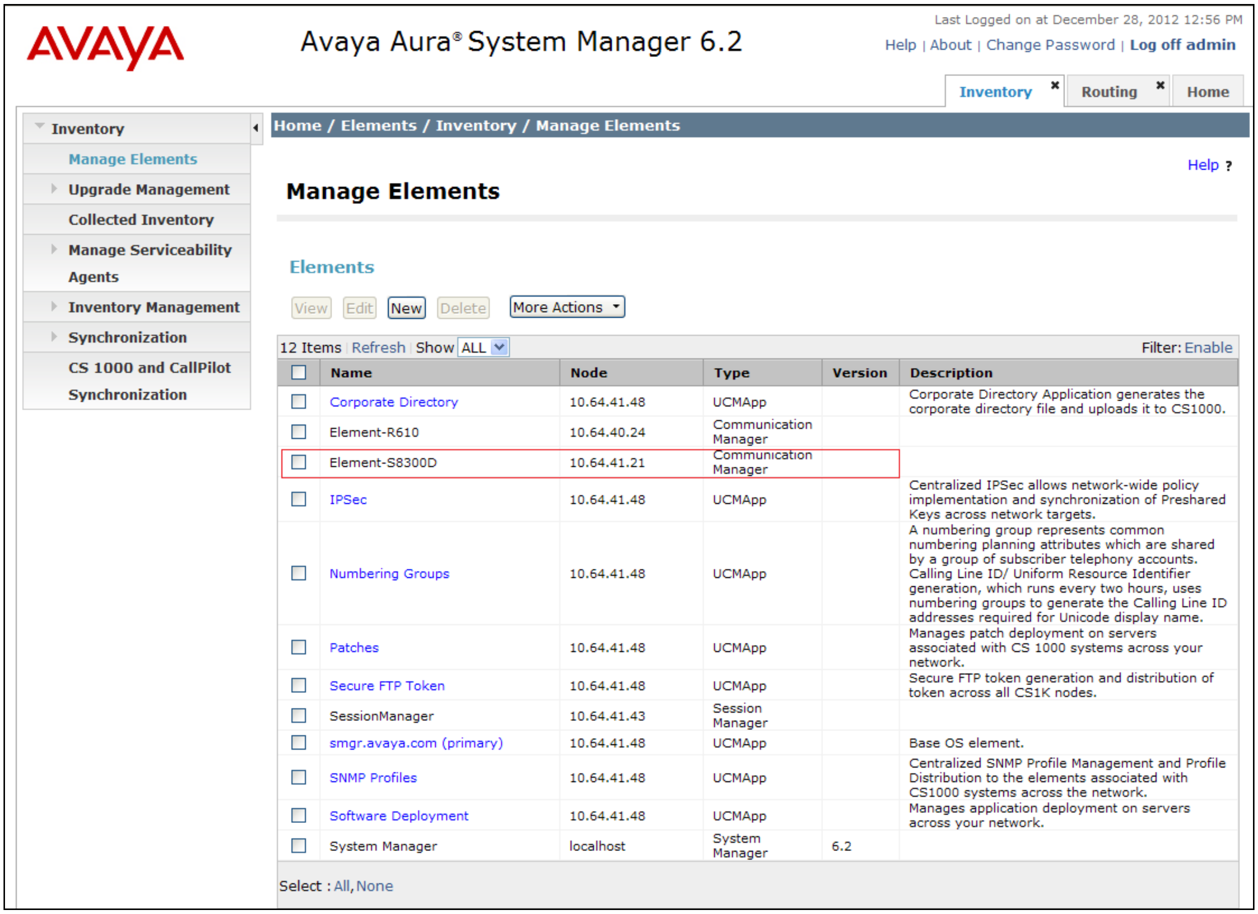


- Attributes section.
  System Manager uses the information entered in this section to log into Communication Manager using its administration interface. Enter the following values and use default values for remaining fields.
  - **Login –** Enter login used for administration access
  - **Password –** Enter password used for administration access
  - **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.

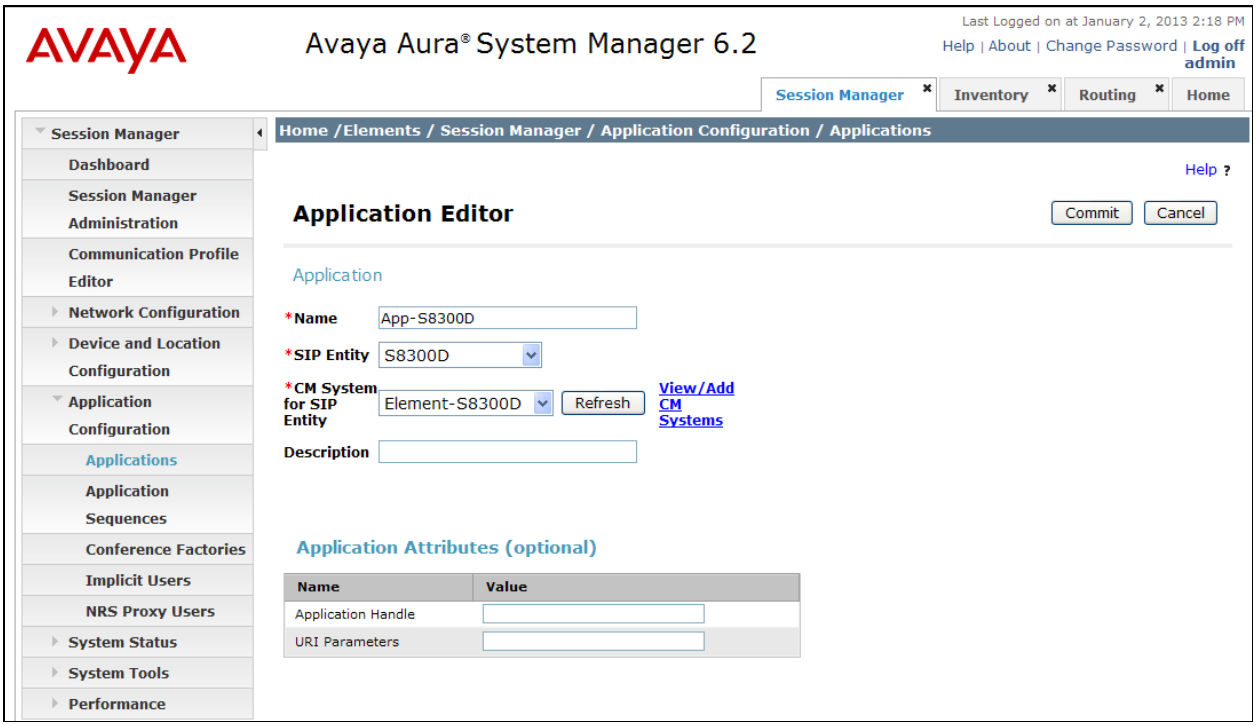


6.9. Configure Applications

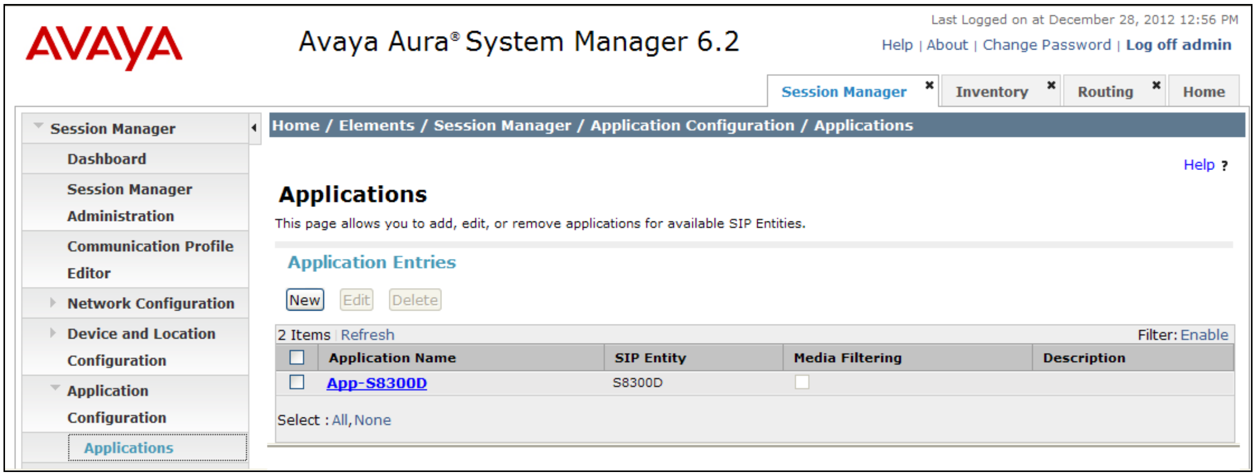
To define a new Application, navigate to **Elements → Session Manager → Application Configuration → Applications**. Click **New** (not shown) to open the Applications Editor page, and provide the following information:

- Application section
  - **Name** – Enter name for the application.
  - **SIP Entity** - Select SIP Entity for Communication Manager defined in **Section 6.3**
  - **CM System for SIP Entity** – Select name of Managed Element defined for Communication Manager in **Section 6.8**
  - **Description** – Enter description if desired.
- Leave fields in the Application Attributes (optional) section blank.

Click the **Commit** button to save the Application.



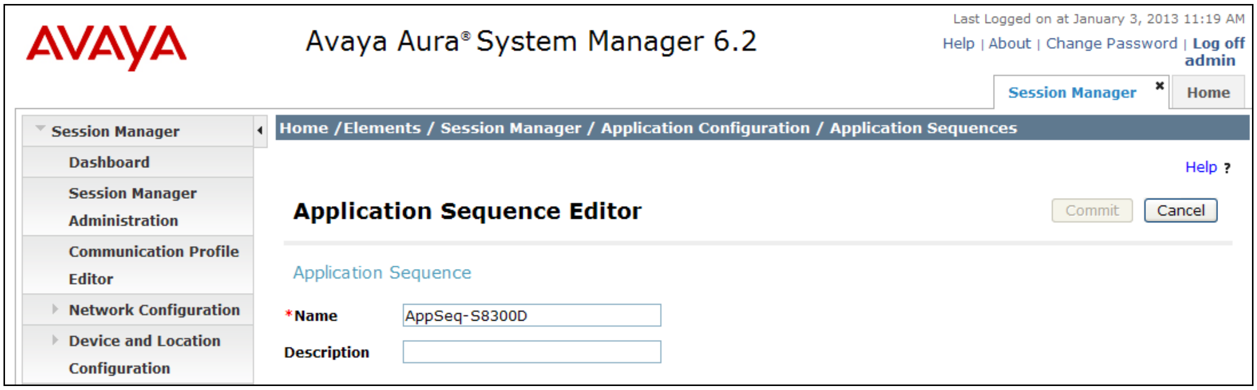
The screen below shows the Application, App-S8300D, defined for Communication Manager.



6.10. Define Application Sequence

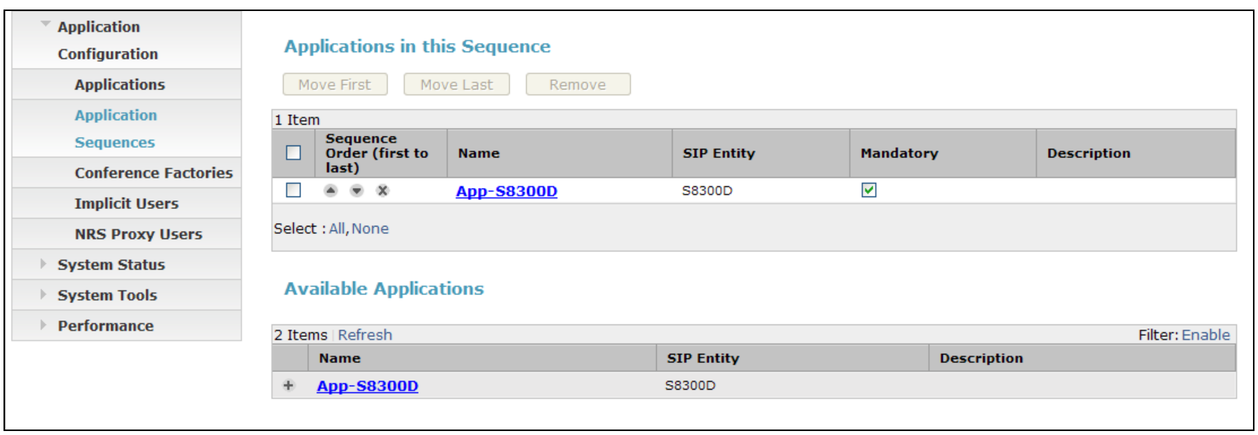
Navigate to **Elements → Session Manager → Application Configuration → Application Sequences**. Click **New** (not shown) and provide the following information:

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

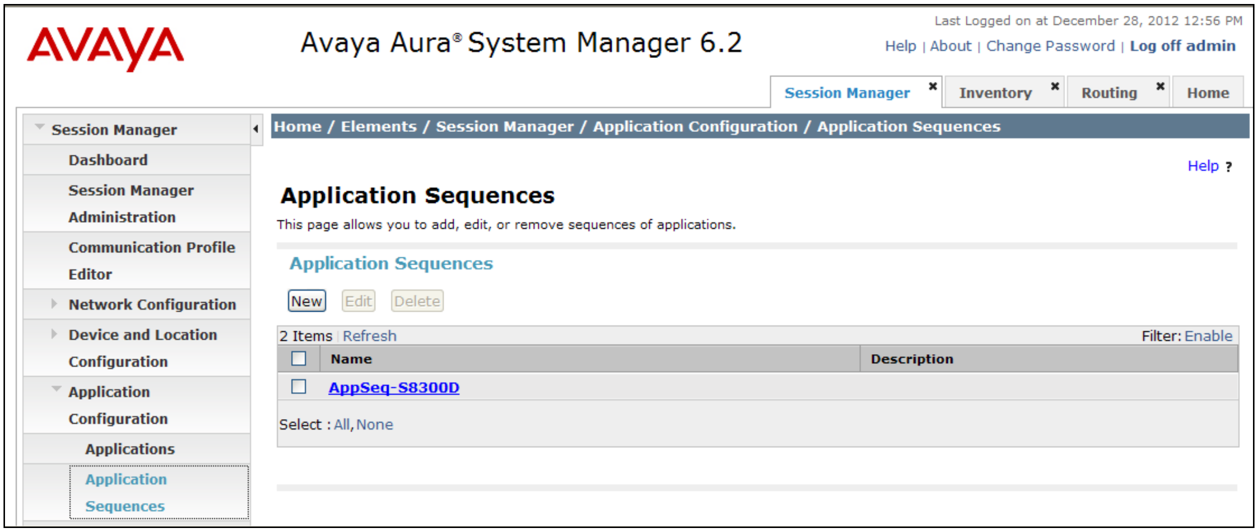


- Available Applications section
  - Click icon associated with the Application for Communication Manager defined in **Section 6.9** to select this application.
  - Verify a new entry is added to the Applications in this Sequence table as shown below.

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



The screen below shows the Application Sequence, **AppSeq-S8300D**, defined during the compliance test.



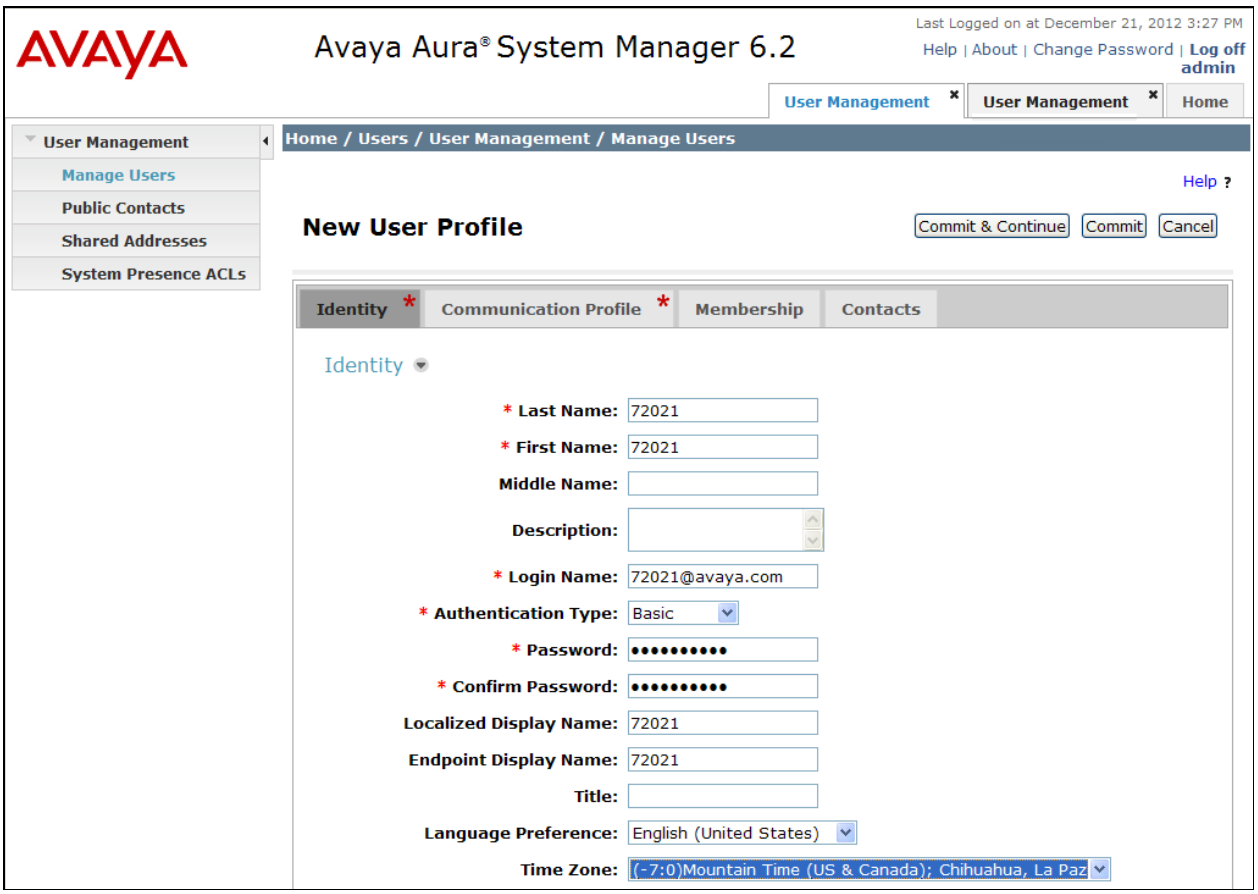
Repeat steps if multiple applications are needed as part of the Application Sequence.

6.11. Configure SIP Users

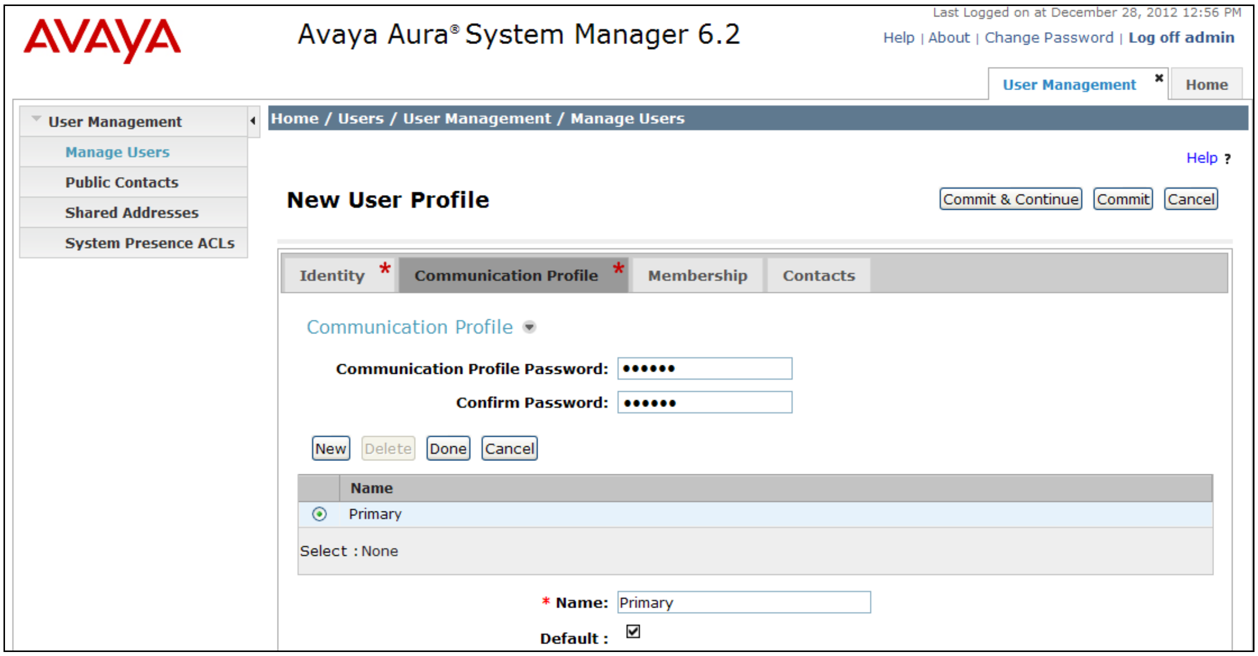
During the compliance test, no special users were created for this solution. All users were created prior to the compliance test. However, steps to configure a user are included. When adding new SIP user, use the option to automatically generate the SIP station in Communication Manager, after adding a new SIP user.

To add new SIP users, Navigate to **Users → User management → Manage Users**. Click **New** (not shown) and provide the following information:

- <u>Identity section</u>
    - **Last Name** – Enter last name of user.
    - **First Name** – Enter first name of user.
    - **Login Name** – Enter extension number@sip domain. The sip domain is defined as Authoritative Domain in **Section 5.2**.
    - **Authentication Type** – Verify **Basic** is selected.
    - **SMGR Login Password** – Enter password to be used to log into System Manager.
    - **Confirm Password** – Repeat value entered above.

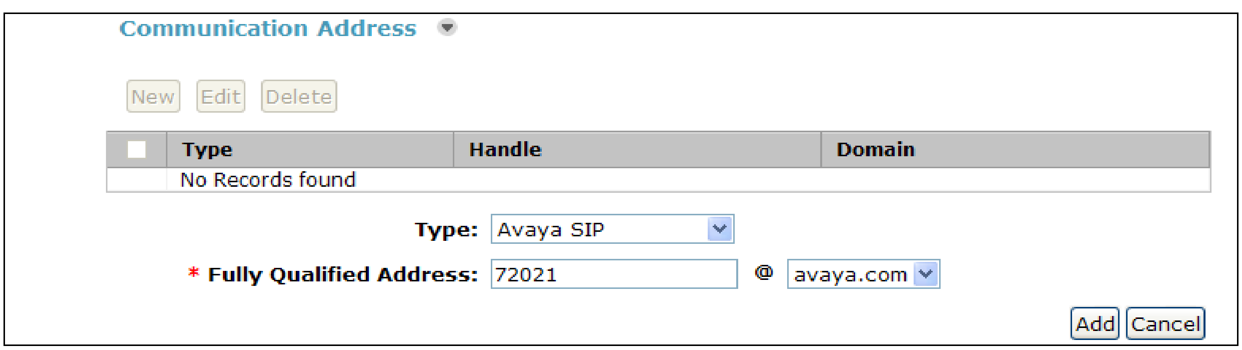


- Communication Profile section
    - **Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
    - **Confirm Password** – Repeat numeric password
    - Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:
        - **Name** – Enter **Primary**
        - **Default** – Enter ☑

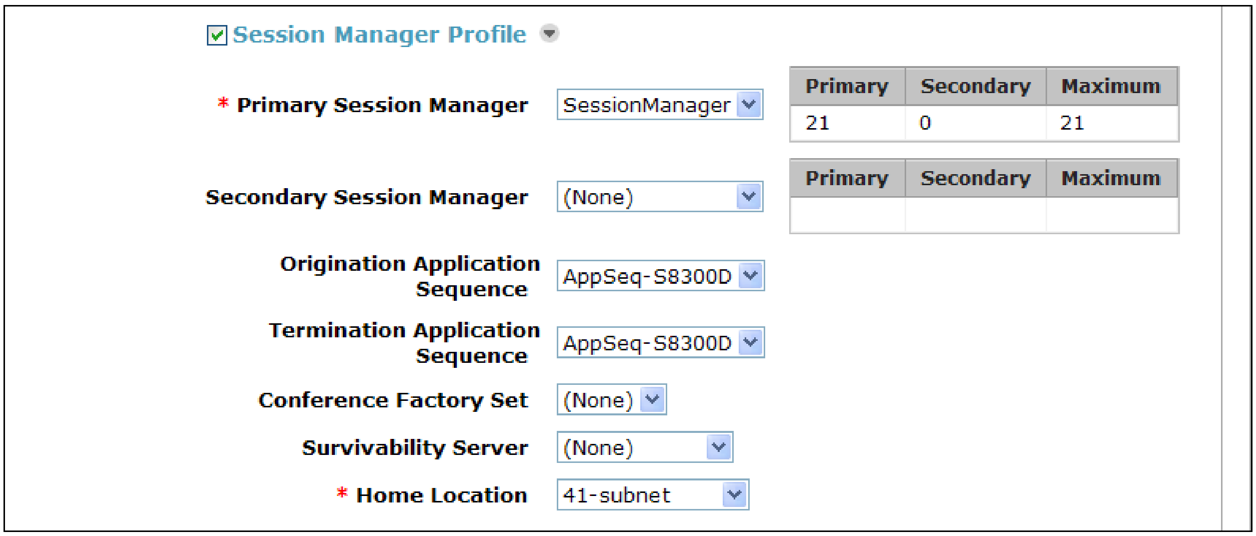


- Communication Address sub-section
  Select **New** to define a **Communication Address** for the new SIP user, and provide the following information.
    - **Type** – Select **Avaya SIP** using drop-down menu.
    - **Fully Qualified Address** – Enter same extension number and domain used for Login Name, created previously.

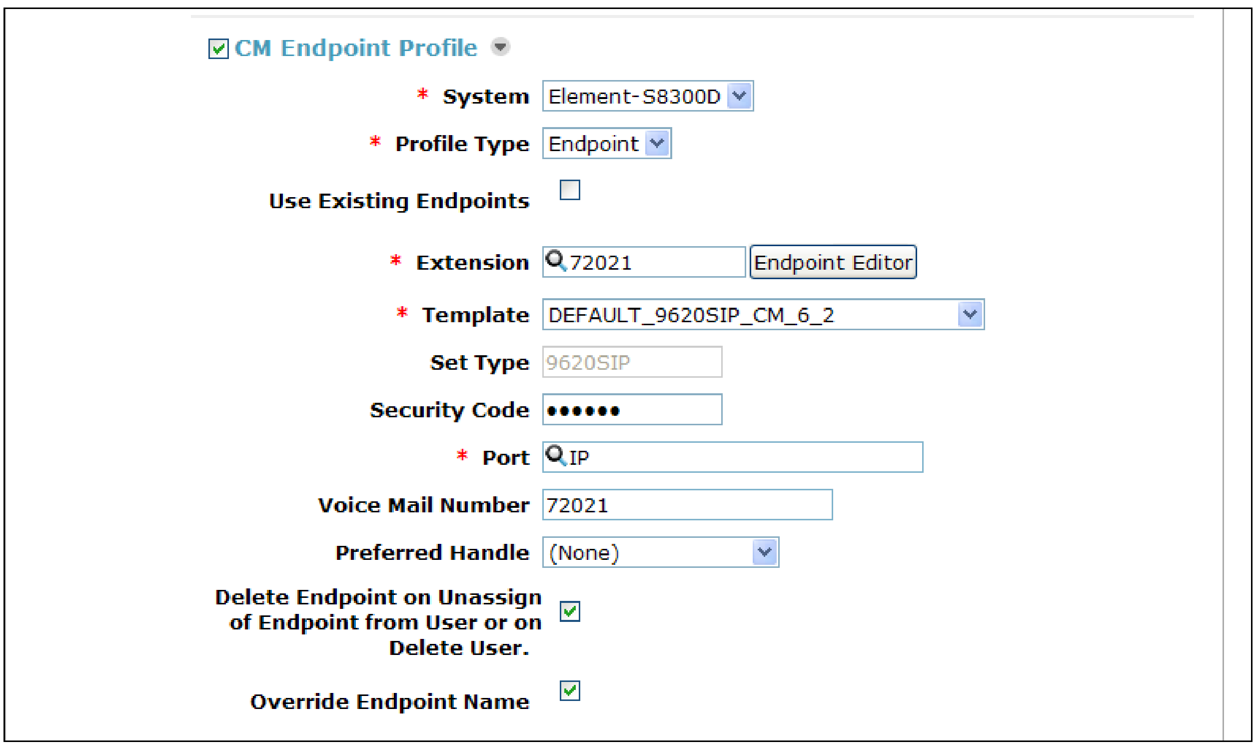
  Click the **Add** button to save the Communication Address for the new SIP user.



- <u>Session Manager Profile section</u>
  - **Primary Session Manager** – Select one of the Session Managers.
  - **Secondary Session Manager** – Select **(None)** from drop-down menu.
  - **Origination Application Sequence –** Select Application Sequence defined in **Section 6.10** for Communication Manager.
  - **Termination Application Sequence** – Select Application Sequence defined in **Section 6.10** for Communication Manager.
  - **Survivability Server** – Select **(None)** from drop-down menu.
  - **Home Location** – Select Location defined in **Section 6.2**.

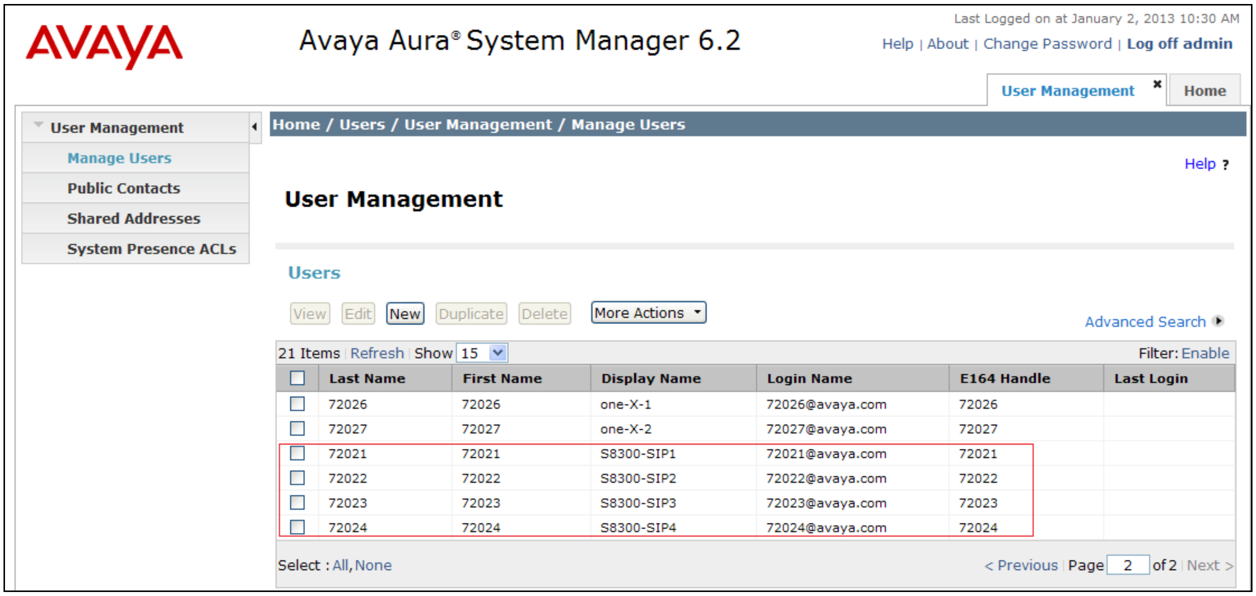


- Endpoint Profile section
  - **System** – Select Managed Element defined in **Section 6.8**.
  - **Use Existing Endpoints -** Leave unchecked to automatically create new endpoint when new user is created. Or else, check the box if endpoint is already defined in Communication Manager.
  - **Extension** - Enter same extension number used in this section.
  - **Template** – Select template for type of SIP phone
  - **Security Code** – Enter numeric value used to logon to SIP telephone. (**Note:** this field must match the value entered for the Shared Communication Profile Password field.
  - **Port** – Select **IP** from drop down menu
  - **Voice Mail Number –** Enter **Pilot Number** for Avaya Modular Messaging if installed. Or else, leave field blank. This feature is not used during the compliance test.
  - **Delete Station on Unassign of Endpoint from User or on Delete User**– Check the box to automatically delete station when Endpoint Profile is un-assigned from user.



Click **Commit** (not shown) to save definition of new user.

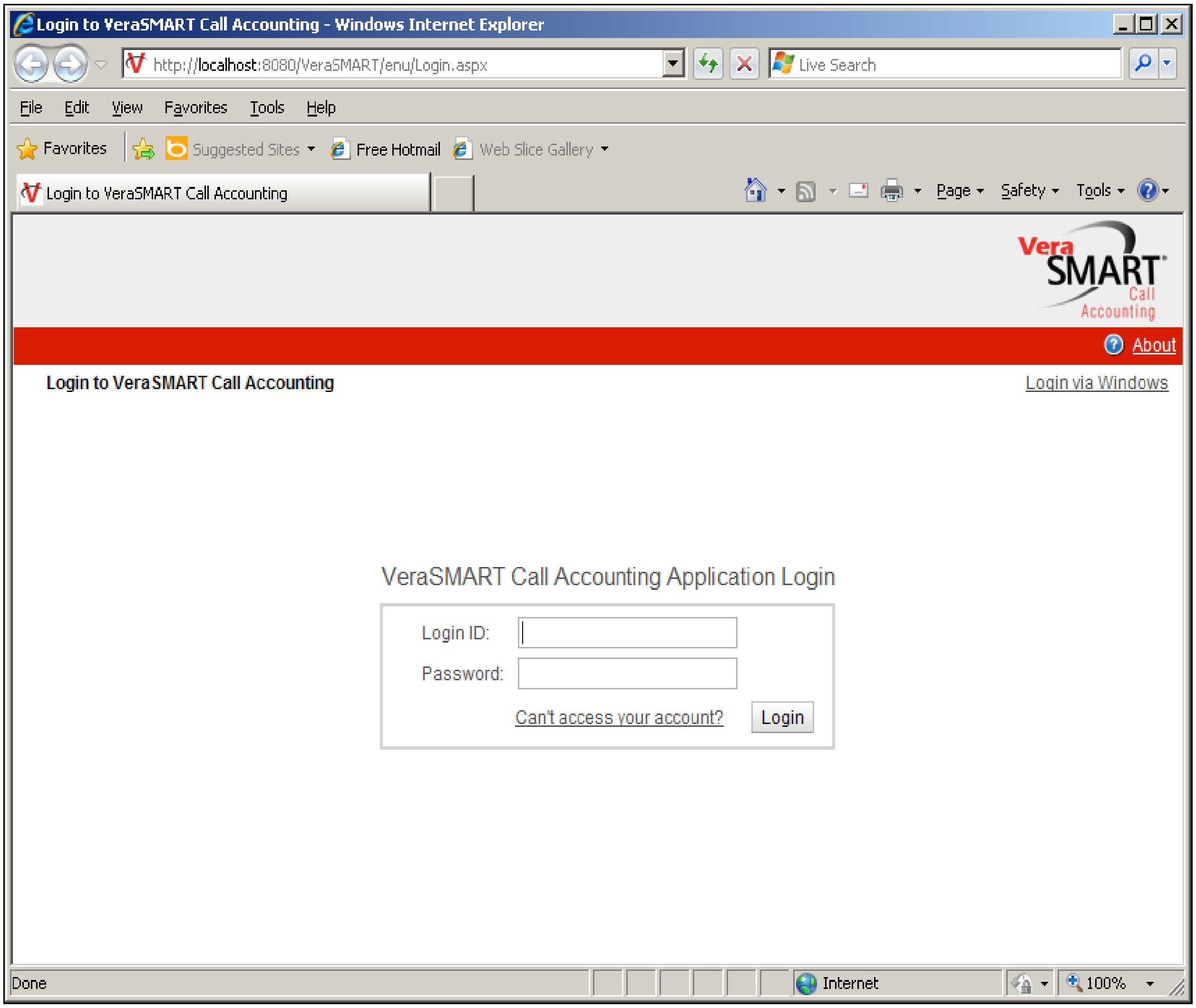
The following screen shows the created users during the compliance test.



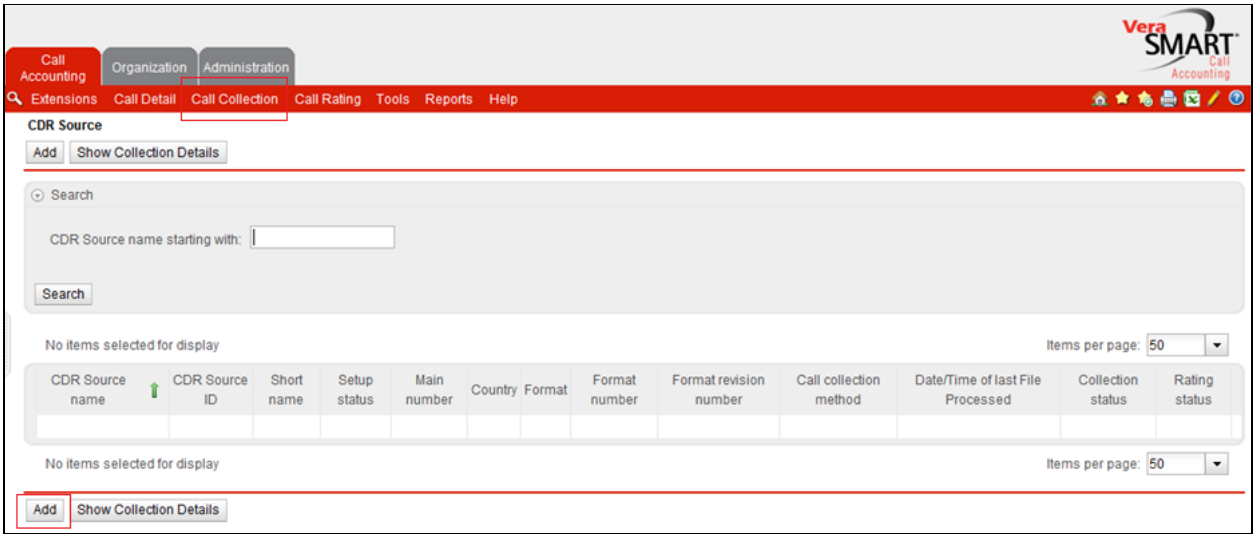
7. Configure Veramark VeraSMART

This section describes the operation of Veramark VeraSMART eCAS to receive CDR data from Communication Manager.

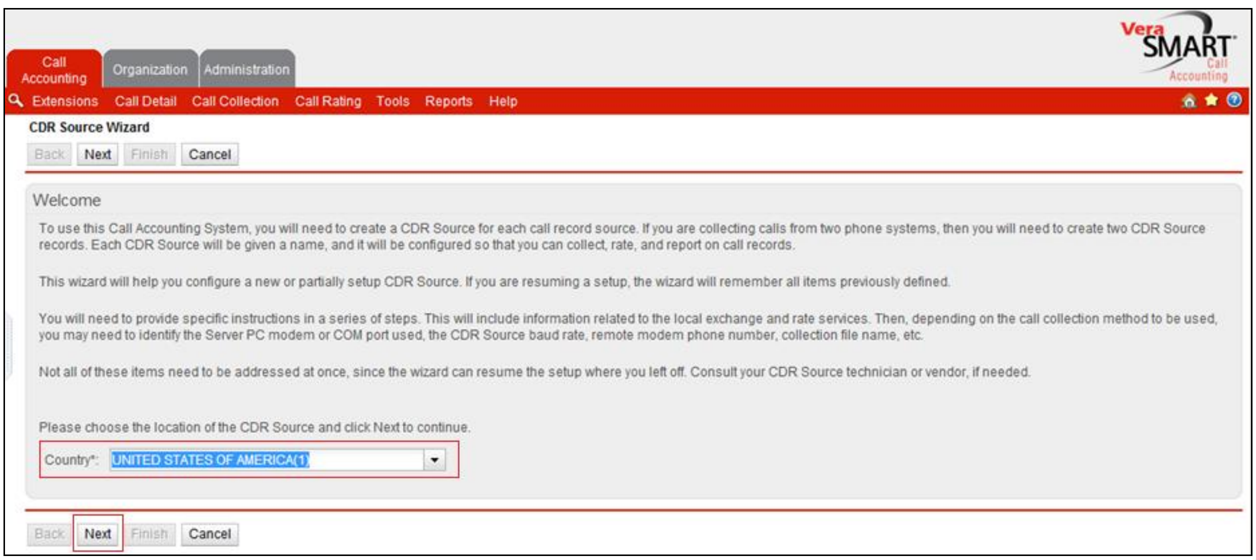
To configure Veramark VeraSMART eCAS, launch a web browser, enter **http://<IP address of Veramark VeraSMART eCAS server>:8080/VeraSMART/enu/Login.aspx>** as URL, and log in with the appropriate credentials.



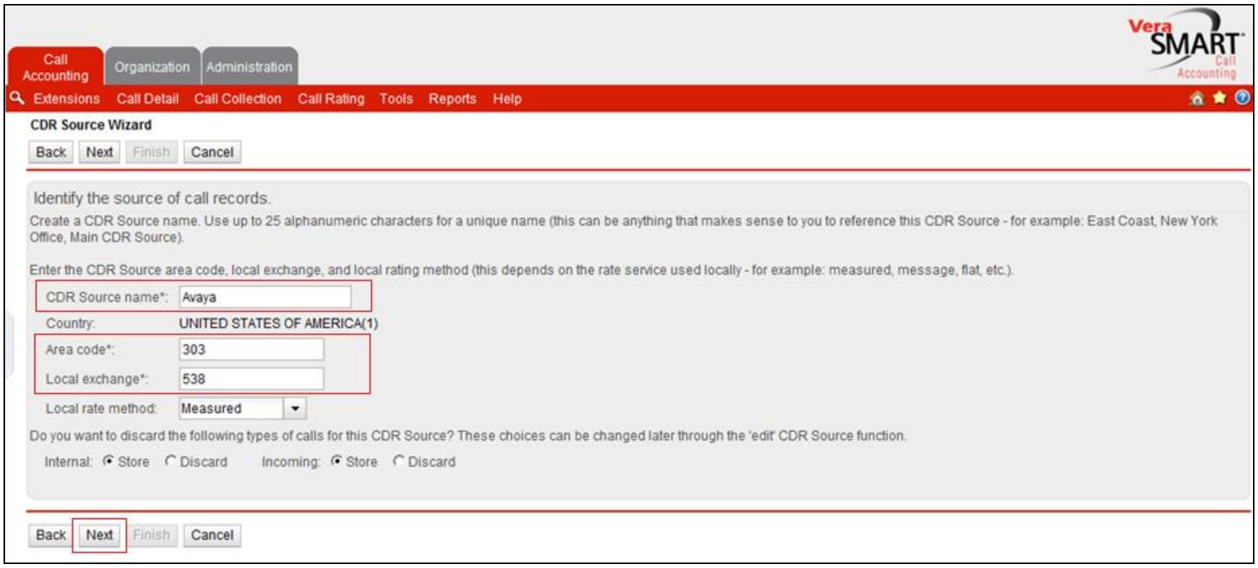
From the Main window, click on the **Call Accounting → Call Collection → CDR Source** link. Click **Add**.



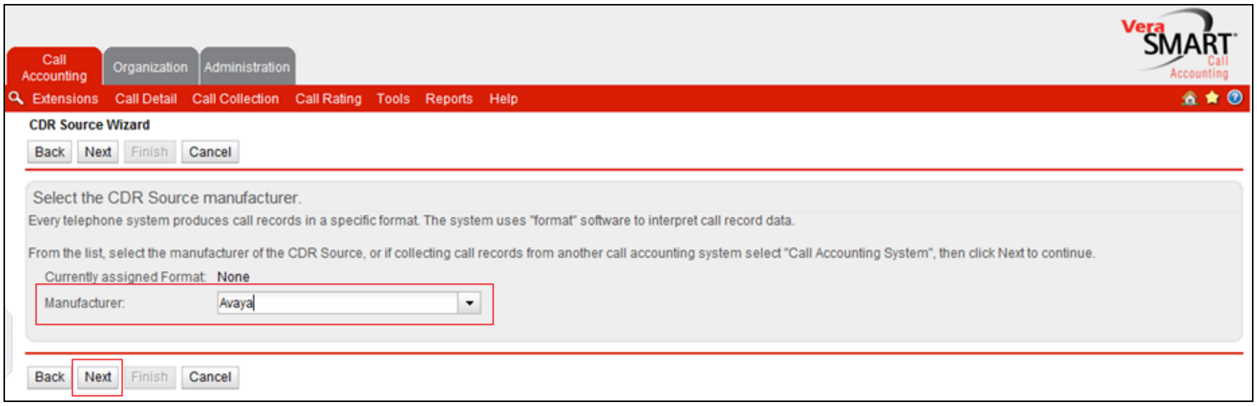
In the CDR Source Wizard window, provide the location of the CDR source and click on the **Next** tab.



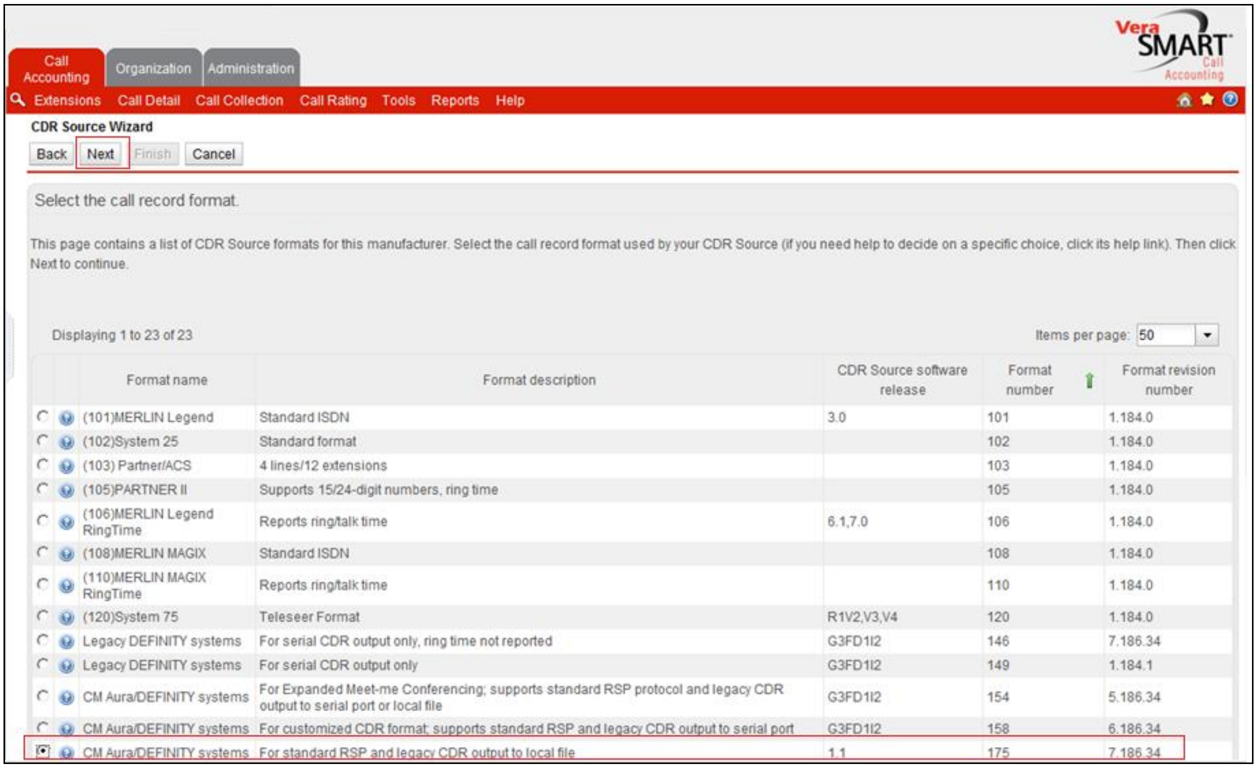
In the CDR Source Wizard window, provide needed information and click **Next.**



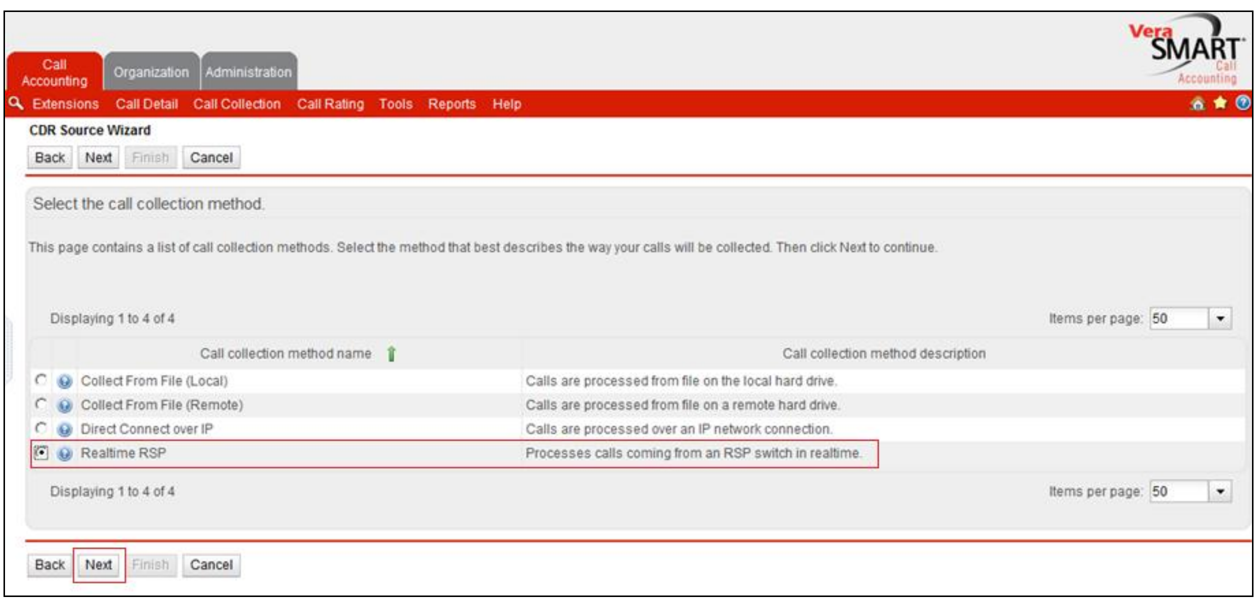
In the CDR Source Wizard window, select Manufacturer using the drop down menu and click **Next**.



In the Select the call record format page, select the format number **175** and click **Next**.



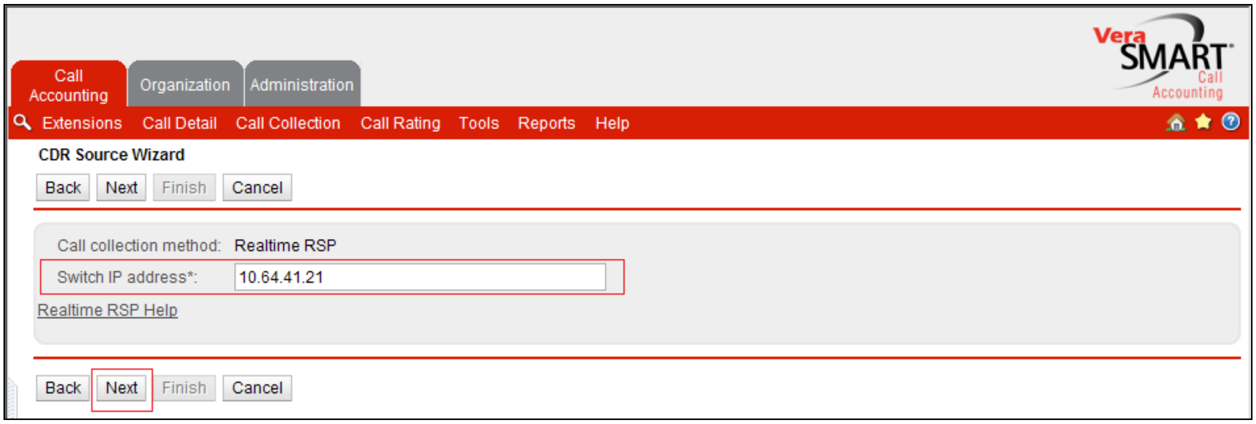
In the **Select the call collection method** page, select the **Realtime RSP** method.
Click on the **next** link.



Provide the following information:

- Switch IP address – Enter the IP address of Communication Manager’s **Procr** IP address.

Click on the **Next** link.



8. Verification Steps

The following steps may be used to verify the configuration:

- Check the CDR status, by running the **status cdr** command in Communication Manager.
- Make several SIP calls between two Communication Managers, and verify that call records were collected from Veramark VeraSMART eCAS.

9. Conclusion

These Application Notes describe the procedures for configuring Veramark VeraSMART eCAS to collect call detail records from Session Manager. Testing was successful except for the issues noted in **section 2.2**.

10. References

This section references the Avaya and Veramark documentation that are relevant to these Application Notes.

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 7.0, Release 6.2, July 2012, available at http://support.avaya.com.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 9.0, Release 6.2, July 2012

The VeraSMART Solution and Product information is available from Veramark. Visit http://www.veramark.com/Call-Accounting/eCAS/

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.