Avaya Solution & Interoperability Test Lab

Application Notes for Veramark VeraSMART with Avaya Aura™ Session 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™ Session Manager.

Veramark VeraSMART is a call accounting software that utilizes Secure File Transfer Protocol to log into Avaya Aura™ Session Manager, and retrieve, transfer raw SIP CDR data to Veramark VeraSMART where the raw data is transformed into call records and available for their end customers.

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 call accounting software can collect raw CDR data from Avaya Aura™ Session Manager using the Secure File Transfer Protocol (SFTP). The serviceability test was conducted to assess the reliability of the solution. Avaya Aura™ System Manager is utilized to configure Avaya Aura™ Session Manager.

These Application Notes assume that Avaya Aura™ Communication Manager and Avaya Aura™ SIP Enablement Services are already installed and configuration steps have been performed. Since the compliance test solution is with Session Manager, an assumption is made that Session Manager and System Manager are already installed and basic configuration have been performed. In these Application Notes, configuration steps on SIP Enablement Services are not included.

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

- Communication Manager – SIP trunk configuration between Communication Manager and Session Manager
- Session Manager – SIP trunk configuration between Communication Manager and Session Manager, and routing information.

1.1. Interoperability Compliance Testing

The focus of the interoperability compliance testing was primarily on verifying whether the Veramark VeraSMART call accounting software can establish the SFTP session with Session Manager, and collect raw data and automatically populate the collect data into their reporting system.
The serviceability testing introduced failure scenarios to see if the Veramark VeraSMART call accounting software can recover from failures.

1.2. Support

Technical support for VeraSMART can be obtained by contacting Veramark via email at tech_support@veramark.com or by calling 585 381-0115.

2. Reference Configuration

Figure 1 illustrates a sample configuration consisting of a redundant pair of Avaya S8720 Servers running Communication Manager, an Avaya G650 Media Gateway, an SIP Enablement Services server, and Veramark VeraSMART on one side, and Avaya S8300 Server running Communication Manager with an Avaya G450 Media Gateway on the other side. Session Manager terminates SIP trunks from both sides. For completeness, Avaya 9600 Series SIP IP Telephones on both sides 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.

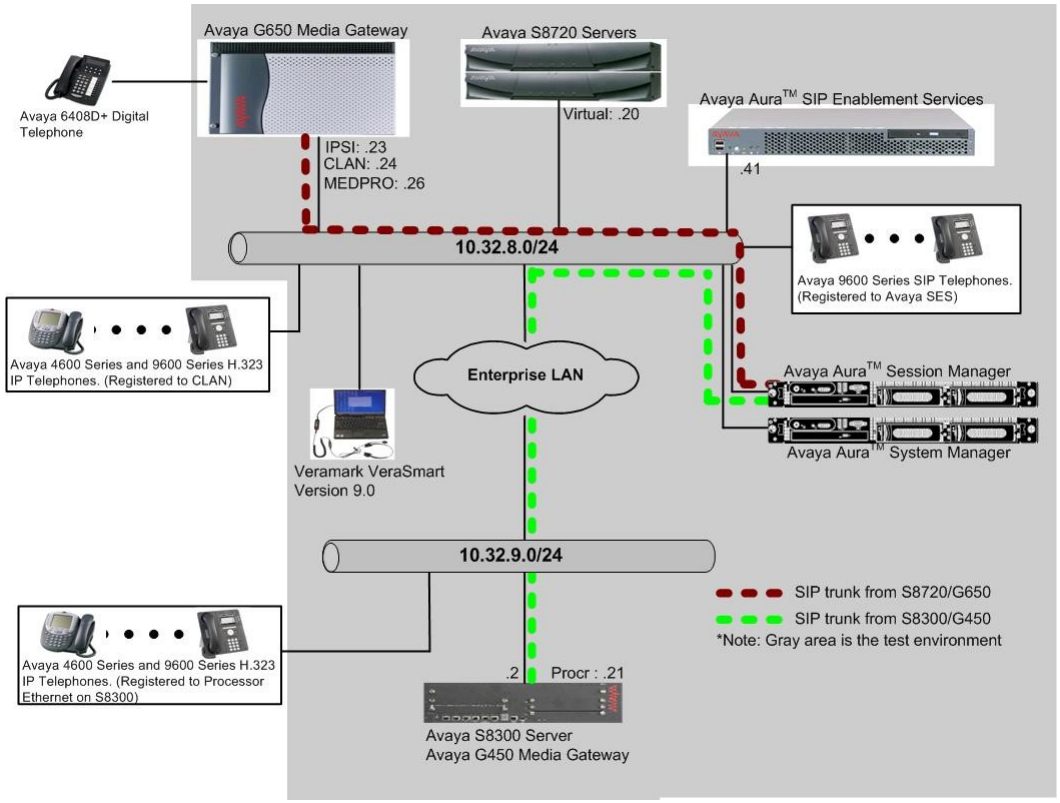


Figure 1. Test configuration of the VeraSMART with Avaya Aura™ Session Manager

3. Equipment and Software Validated

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

Equipment		Software
Avaya S8720 Servers		Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G650 Media Gateway		
	TN2312BP IPSI TN799DP CLAN TN2302AP MEDPRO	HW11 FW044 HW01 FW028 HW20 FW118
Avaya S8300 Server		Avaya Aura™ Communication Manager 5.2 (R015x.02.0.947.3)
Avaya G450 Media Gateway		28.17
Avaya Aura™ Session Manager		1.1.6 Build 113009
Avaya Aura™ System Manager		1.1.6 Build 113009
Avaya Aura™ SIP Enablement Services		5.2 (R015x.02.0.947.3) with Service Pack SES-02.0.947.3-SP2a
Avaya 9600 Series SIP Telephone		
	9620 9630 9650	2.0.5 2.0.5 2.0.5
Veramark VeraSMART on Windows 2003 Server with Service Pack 2		9.0

4. Configure Aura™ Avaya Communication Manager

This section provides procedures for configuring a SIP trunk between Communication Manager and Session Manager. All configuration changes in Communication Manager are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8720 Server. All steps are the same for the other Avaya Servers unless otherwise noted. The highlights in the following screens indicate the parameter values used during the compliance test.

4.1. 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 **testroom.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 the **IP Codec Set** form.

```
change ip-network-region 1                                    Page   1 of  19
                              IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: testroom.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: 65531
DIFFSERV/TOS PARAMETERS                RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        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
```

4.2. 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** (Session Manager) along with its IP address.

```
change node-names ip                                          Page   1 of   2
                                   IP NODE NAMES
    Name                  IP Address
CLAN                   10.32.8.24
CLAN-AES               10.32.8.25
MEDPRO                 10.32.8.26
SES                    10.32.8.41
SM                     10.32.8.10
```

4.3. 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 **CLAN** as displayed in **Section 4.2**.
- Far-end Node Name - Set to the **SM** configured in **Section 4.2**.
- Far-end Network Region - Set to the region configured in **Section 4.1**.
- Far-end Domain - Set to **testroom.avaya.com**. This should match the SIP Domain value in **Section 5.1**.

```
add signaling-group 210                                        Page   1 of   1
                              SIGNALING GROUP

 Group Number: 210            Group Type: sip
                         Transport Method: tls
  IMS Enabled? n




   Near-end Node Name: CLAN                 Far-end Node Name: SM
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1
Far-end Domain: testroom.avaya.com

                                                Bypass If IP Threshold Exceeded? 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                      Direct IP-IP Early Media? n
H.323 Station Outgoing Direct Media? n              Alternate Route Timer(sec): 6
```

4.4. 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 4.3**.
- 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 210                                            Page   1 of  21
                              TRUNK GROUP

Group Number: 210                 Group Type: sip           CDR Reports: y
  Group Name: To SM                        COR: 1        TN: 1        TAC: 1021
   Direction: two-way       Outgoing Display? y
 Dial Access? n                                  Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                      Signaling Group: 210
                                                    Number of Members: 10
```

4.5. 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 27 was used for the Avaya S8300 Server 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
27               5   0                   aar  n
```

4.6. 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 27 was used the route pattern 10.

```
change aar analysis 7                                          Page   1 of   2
                            AAR DIGIT ANALYSIS TABLE
                                  Location:  all           Percent Full:    2

          Dialed           Total     Route    Call   Node  ANI
          String          Min  Max  Pattern   Type   Num   Reqd
    27                    5    5     210       aar          n
```

4.7. Configure Route Pattern

Enter **change route-pattern <r>**, where **r** is the route-pattern number. The route pattern 10 routes calls to the trunk group 210, which is the SIP trunk to Session Manager.

```
change route-pattern 210                                       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: 210  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. Configure Avaya Aura™ Session Manager

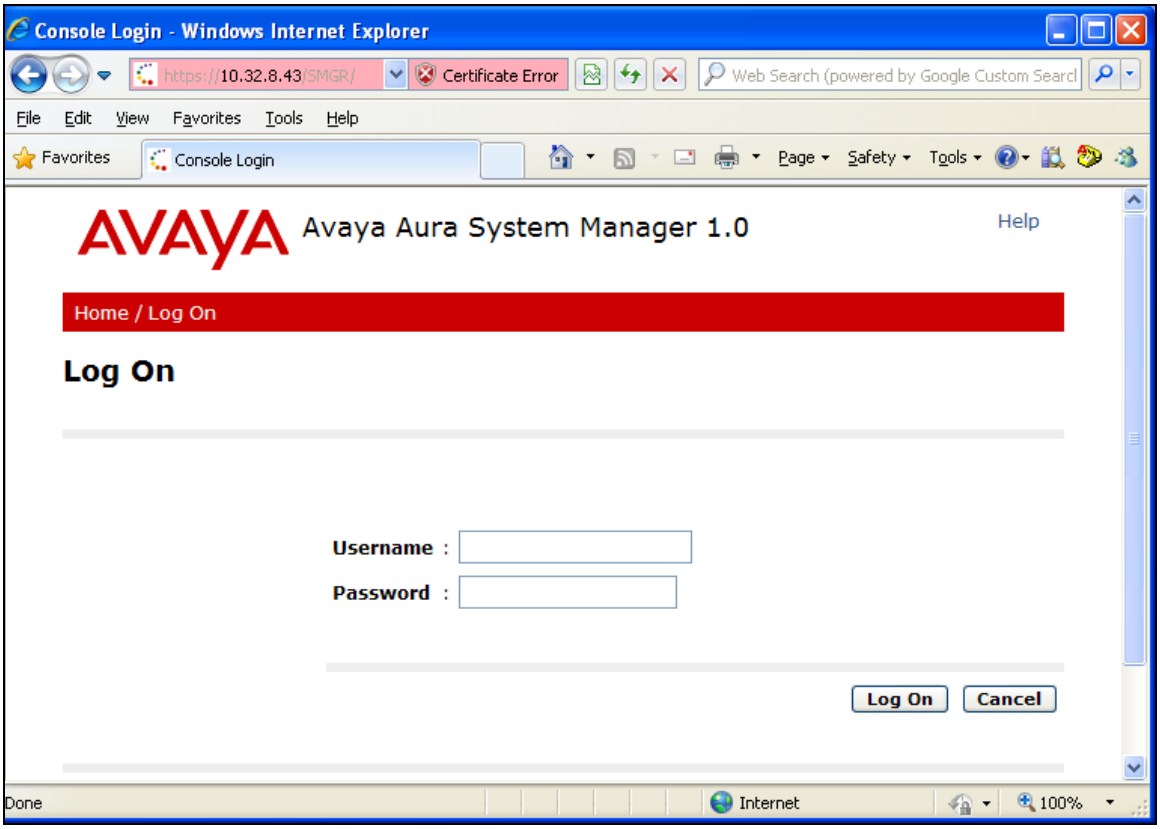
This section provides procedures for configuring the Session Manger side of a SIP trunk between Communication Manager and Session Manager. The highlights in the following screens indicate the parameter values used during the compliance test.

Note 1: *Session Manager associates with two IP addresses. One is for the Session Manager management IP address, and the other is the Session Manager SIP entity IP address. In this section, unless specified as the Session Manager management IP address (10.32.8.42), the Session Manager IP address refers to the Session Manager entity IP address (10.32.8.10).*

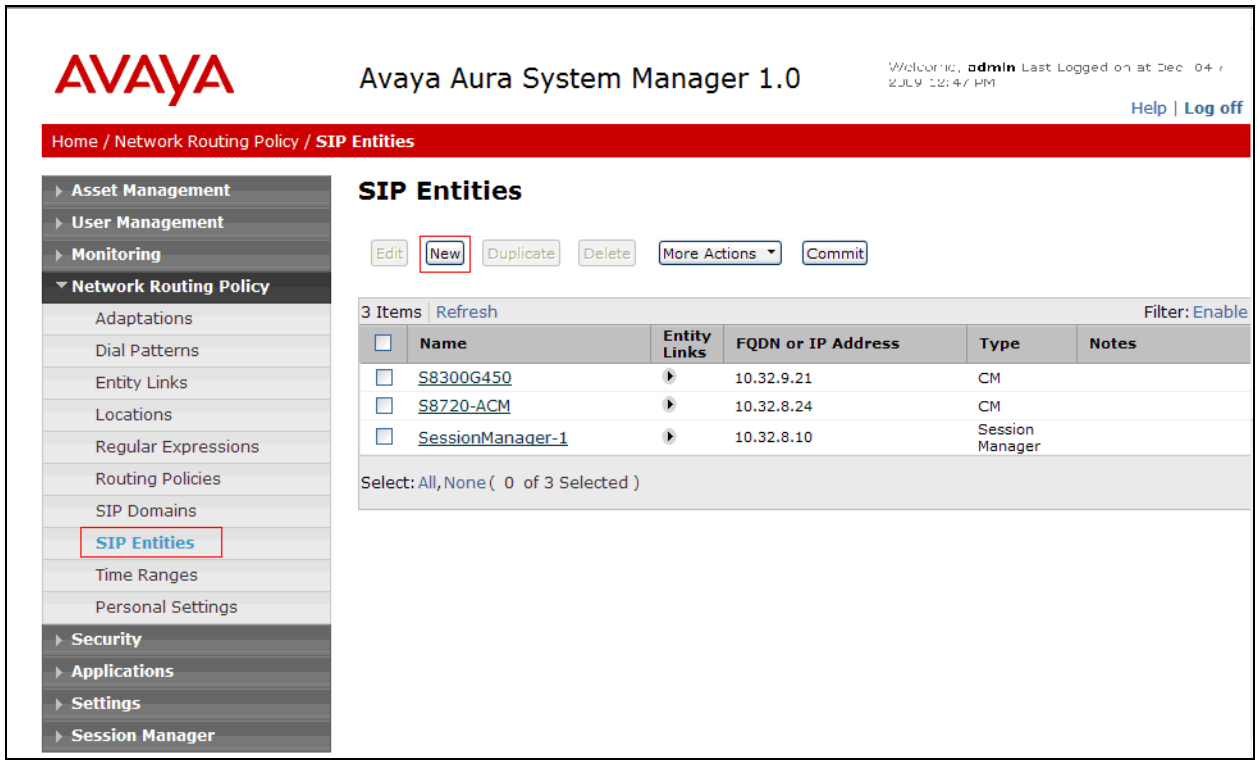
Note 2: *The Session Manager configuration should be performed through System Manager. A user needs to use a web browser to access the web administrative interface on System Manager.*

5.1. Configure SIP Entities

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



Navigate to **Network Routing Policy → SIP Entities**, and click on the **New** button to create a new SIP entity.



The following is a sample configuration of a SIP Entity for SessionManager-1.

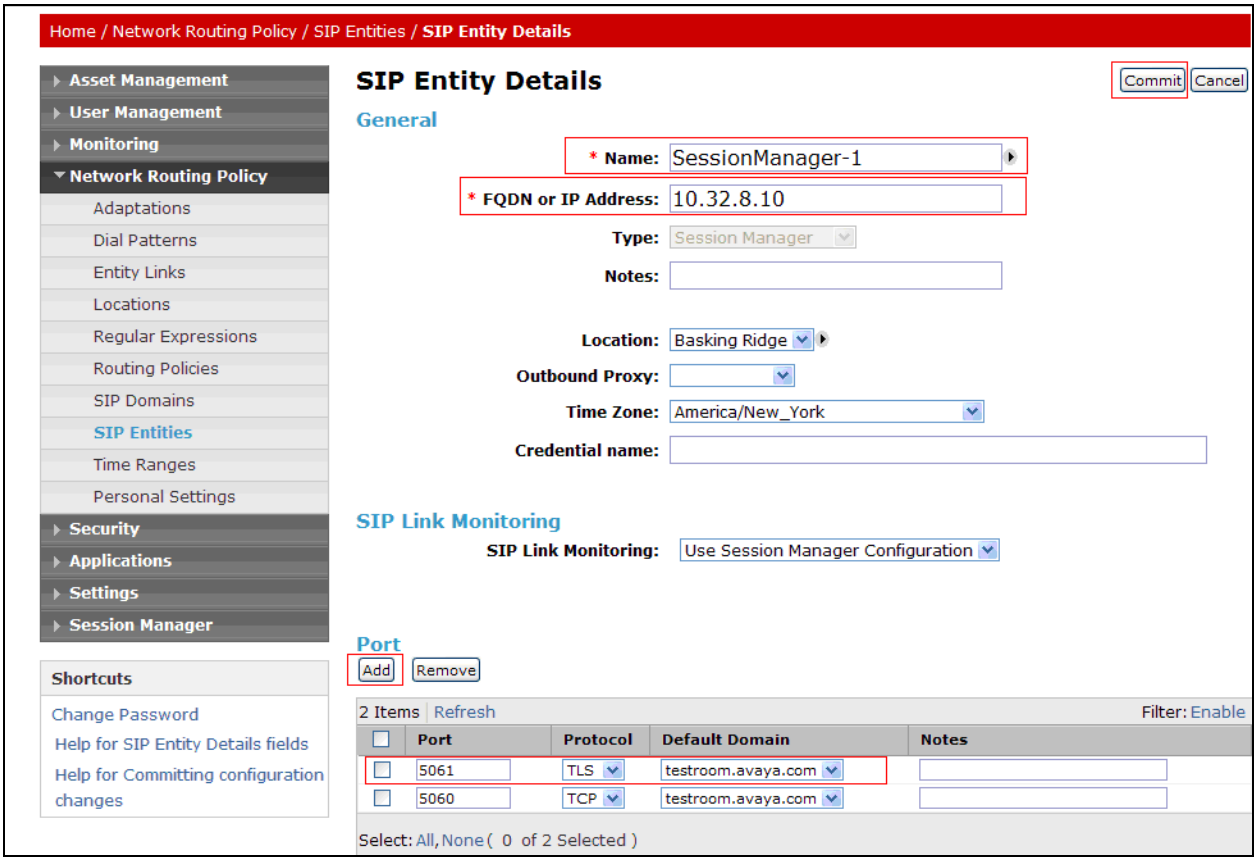
- Name – Enter a descriptive name.
- FQDN – Enter the IP address of Session Manager.

Default values may be used for all other fields. After completing the above fields, click on the **Add** button under the Port section, and provide the Default Domain. During the compliance test, the domain is set to **testroom.avaya.com**. Click on the **Commit** button at the top right of the window.

Repeat this process for adding SIP Entities for two Communication Managers (Avaya S8720 Servers w/ G650 Media Gateway and Avaya S8300 Server w/ G450 Media Gateway).

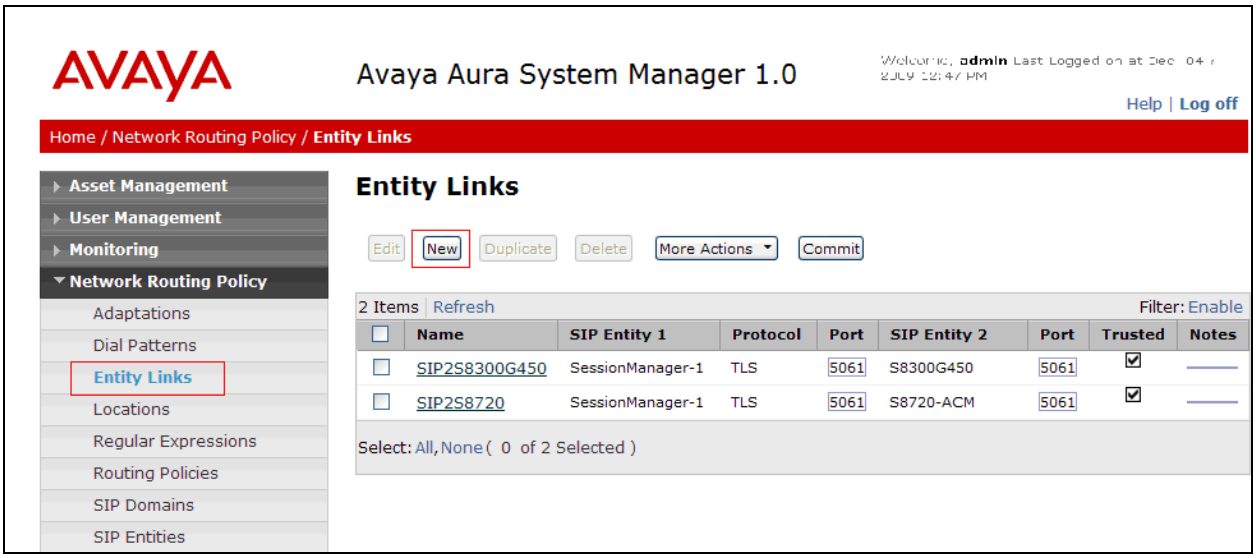
Note: *During the SIP Entities configuration for Communication Manager, the SIP trunk termination points (the **FQDN or IP Address** filed) are followed:*

- *Avaya S8720 Servers w/ G650 Media Gateway – CLAN*
- *Avaya S8300 Server w/ G450 Media Gateway – Processor Ethernet (Procr)*



5.2. Configure Entity Links

Navigate to **Network Routing Policy → Entity Links**, and click on the **New** button to create a new entity link.



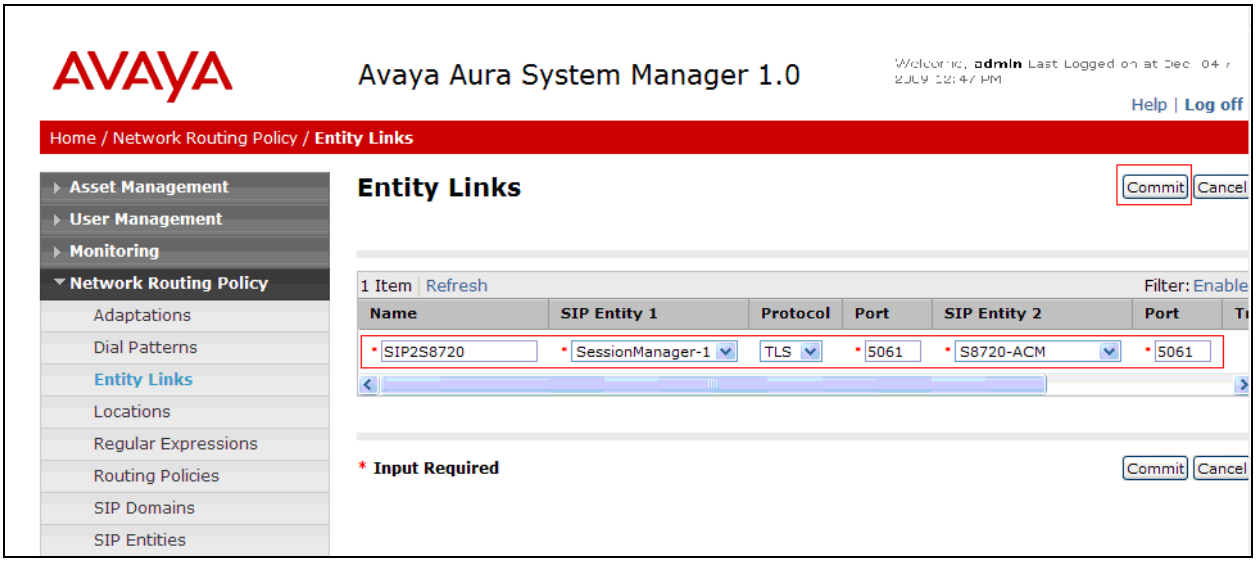
On the Entity Link page, provide the following information:

- Name – Enter a descriptive name for an entity link.
- SIP Entity 1 – Select the Session Manager SIP entity created in **Section 5.1**.
- SIP Entity 2 – Select the Communication Manager SIP entity created in **Section 5.1**.

During the compliance test, the following two entity links are utilized:

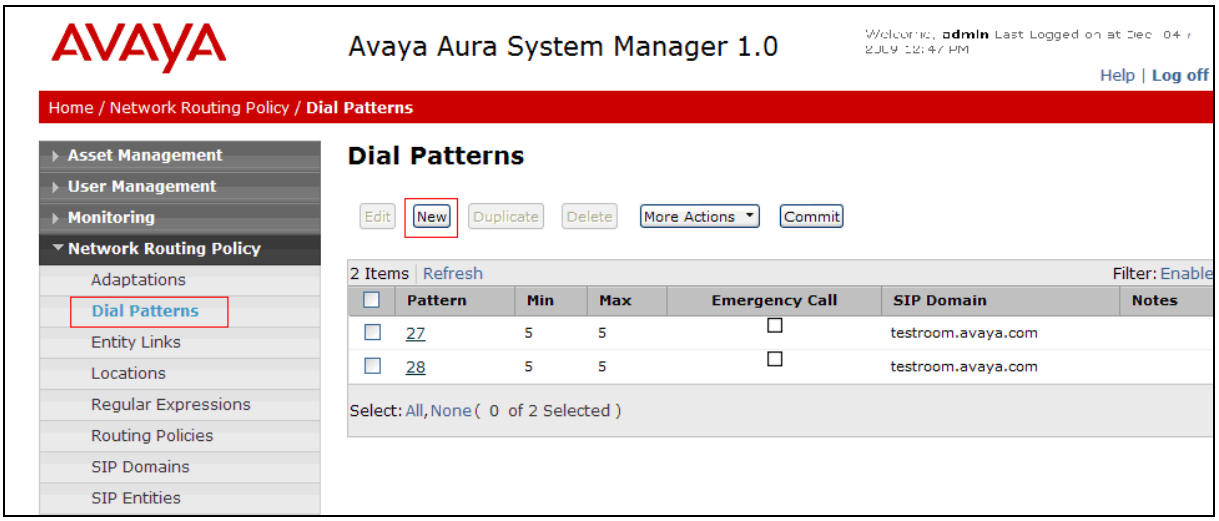
- Link between Session Manager and Avaya S8720 Servers w/ G650 Media Gateway.
- Link between Session Manager and Avaya S8300 Server w/ G450 Media Gateway.

Click on the **Commit** button at the top right of the window.



5.3. Configure Dial Patterns

Navigate to **Network Routing Policy → Dial Patterns** and click on the **New** button to create a new dial pattern.

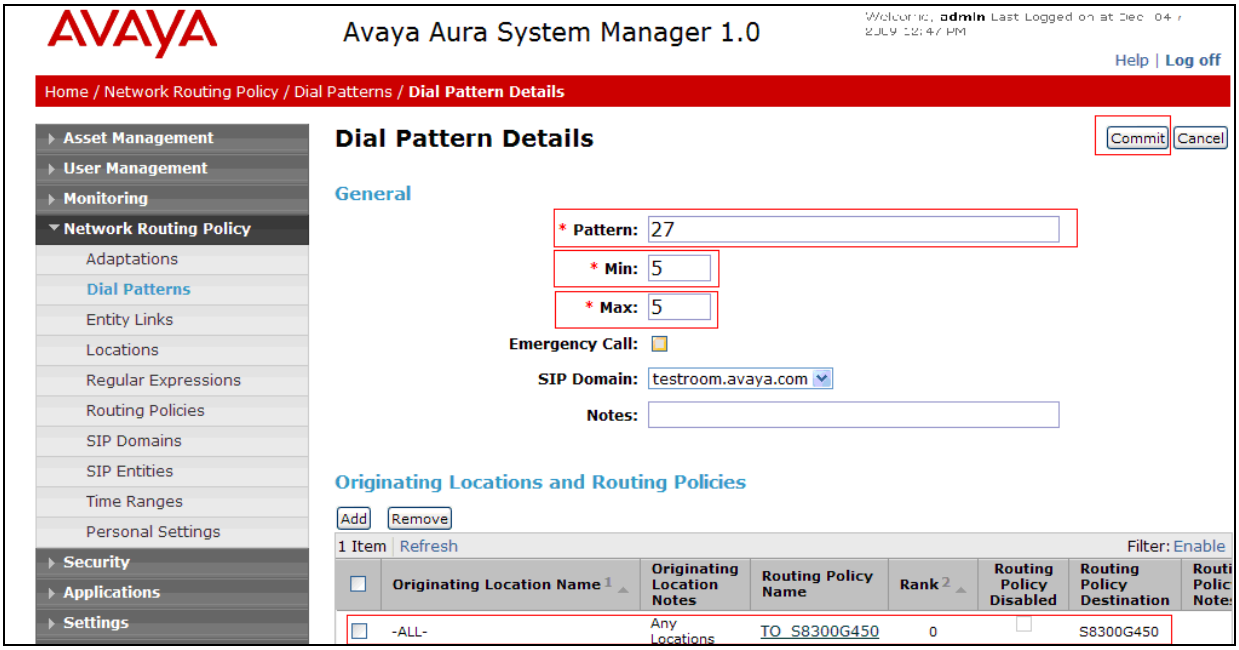


On the Dial Details page, provide the following information:

- Pattern – Enter a leading portion of extensions.
- Min / Max – Enter the minimum and maximum extension digits.

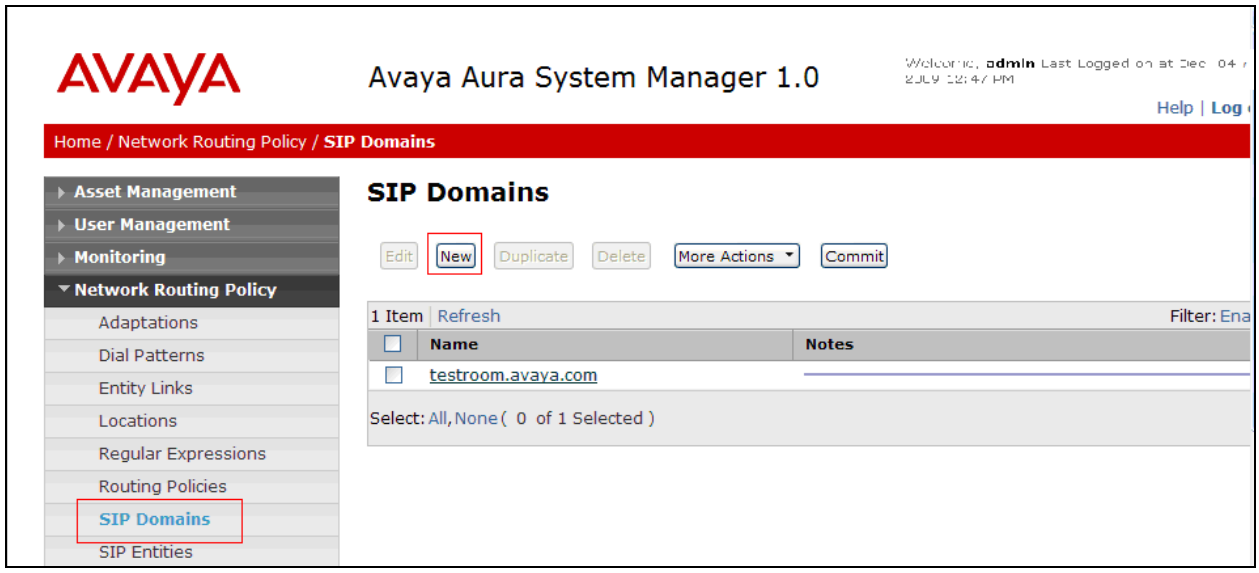
Default values may be used for all other fields. After completing the above fields, click on the **Add** button under the Originating Locations and Routing Policies section, and select an appropriate routing policy name. Click on the **Commit** button at the top right of the window.

Repeat this process for routing pattern on the other side.

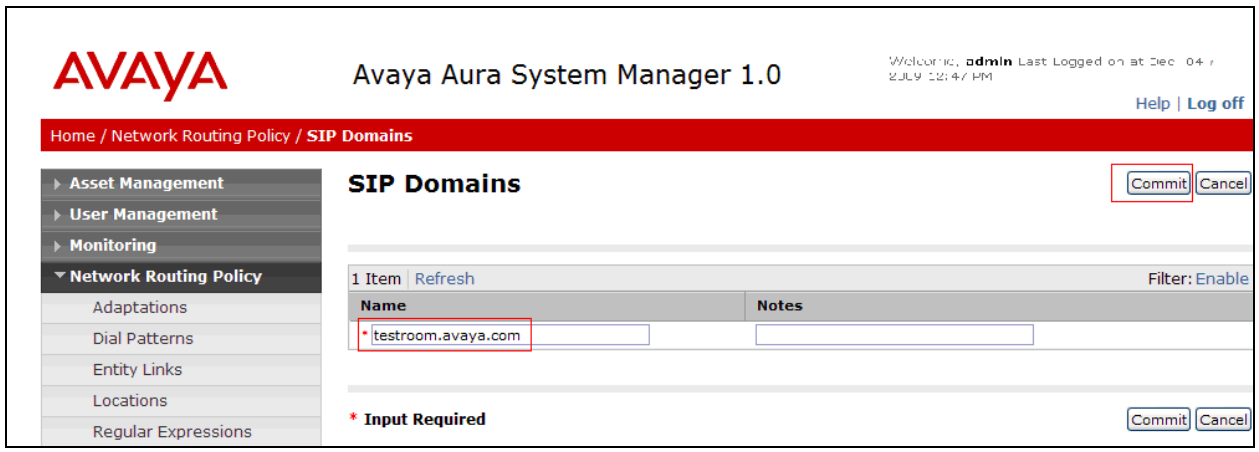


5.4. Configure SIP Domains

Navigate to **Network Routing Policy → SIP Domains,** and click on the **New** button to create a new SIP domain.



On the SIP Domain page, enter the SIP domain name, and click on the **Commit** button.



5.5. Configure Session manager instances

Navigate to **Session Manager → Session Manager Administration,** and click on the **New** button.

On the Add Session Manager window, provide the following information:

Under General Section

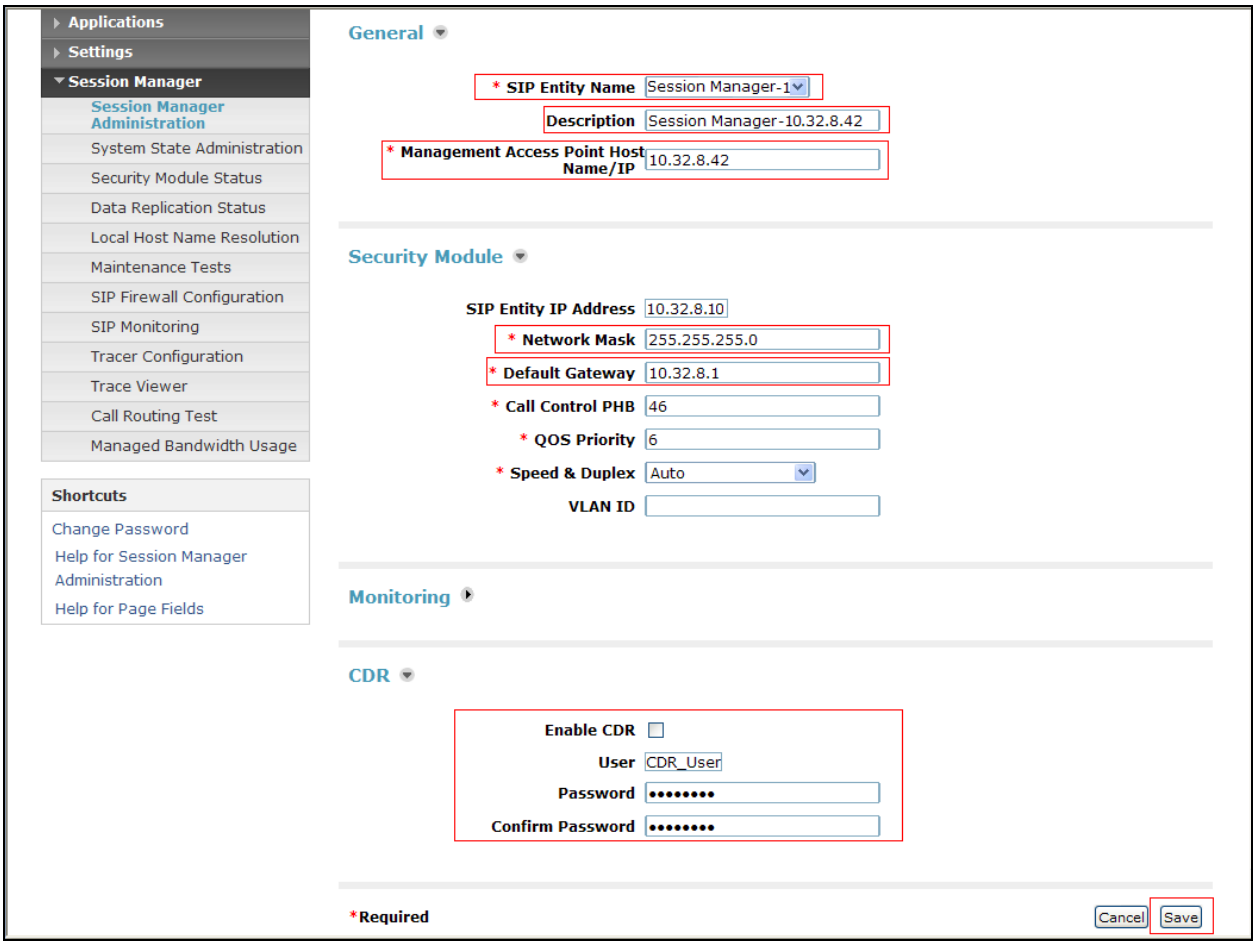
- SIP Entity Name – Enter name of the SIP entity created in **Section 5.1**.
- Description – Enter a description for the SIP entity.
- Management Access Point Host Name/IP – Enter the management IP address of Session Manager.

Under Security Module

- Network Mask – Enter the subnet mask of the SIP entity IP address.
- Default Gateway – Enter the default gateway for the SIP entity IP address.

Under CDR Section

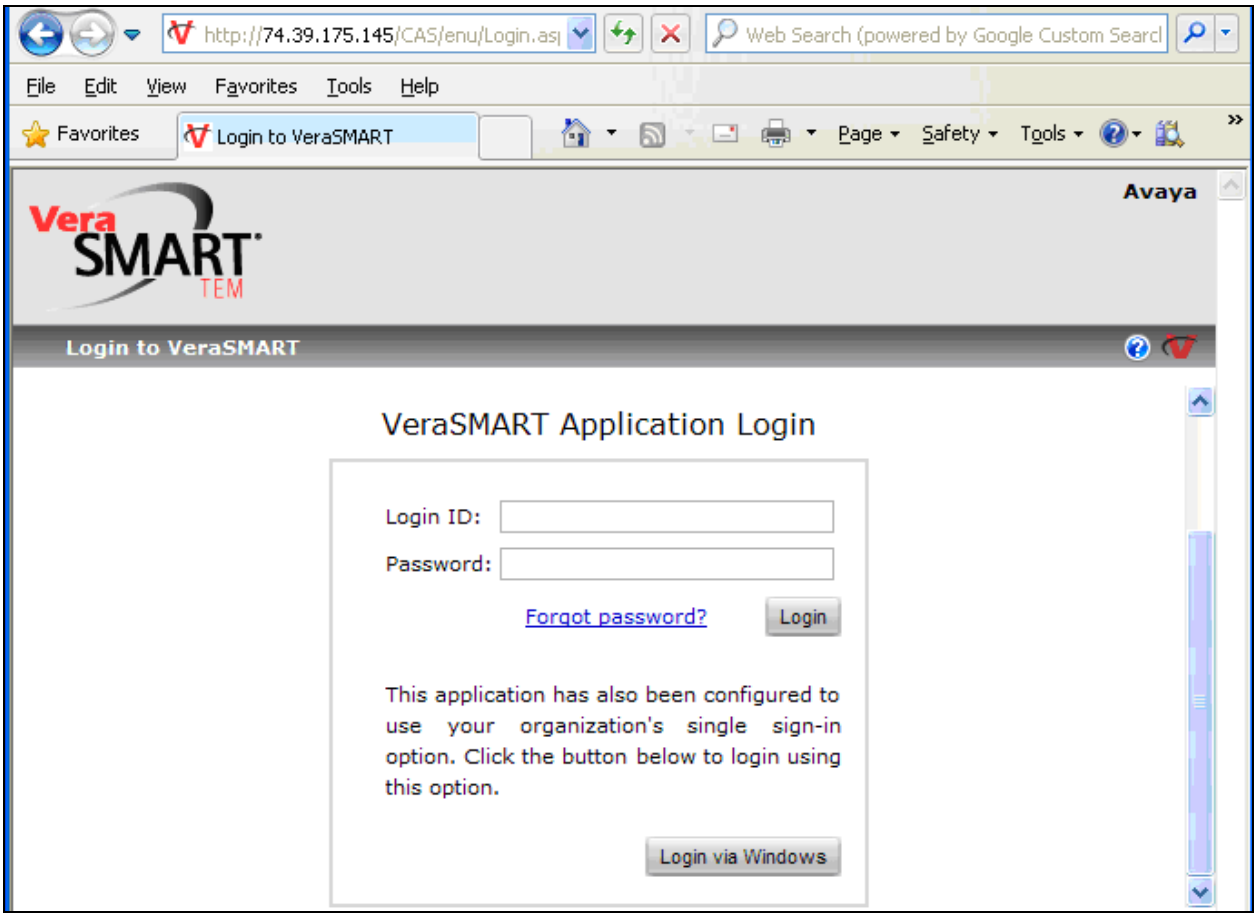
- Check on the Enable CDR check box.
- User – Enter the CDR user to be used in **Section 6**.
- Password – Enter the CDR user password to be used in **Section 6**.
- Confirm Password – Re-enter the CDR user password.



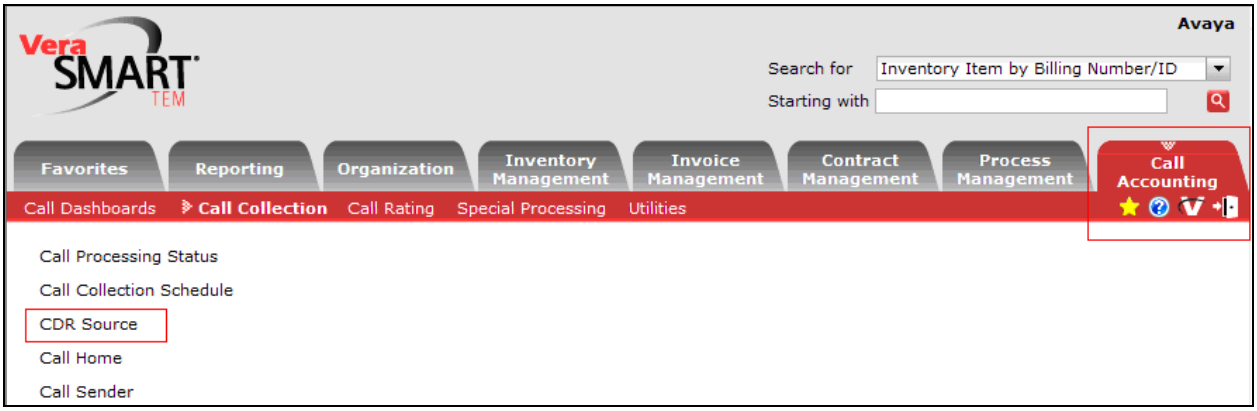
6. Configure Veramark VeraSMART

This section describes the operation of Veramark VeraSMART. During the compliance test, Veramark VeraSMART does not receive CDR records automatically. Instead, Veramark VeraSMART needs to access Session Manager, and pulls the CDR data, as in the local survivable processor (LSP) operation.

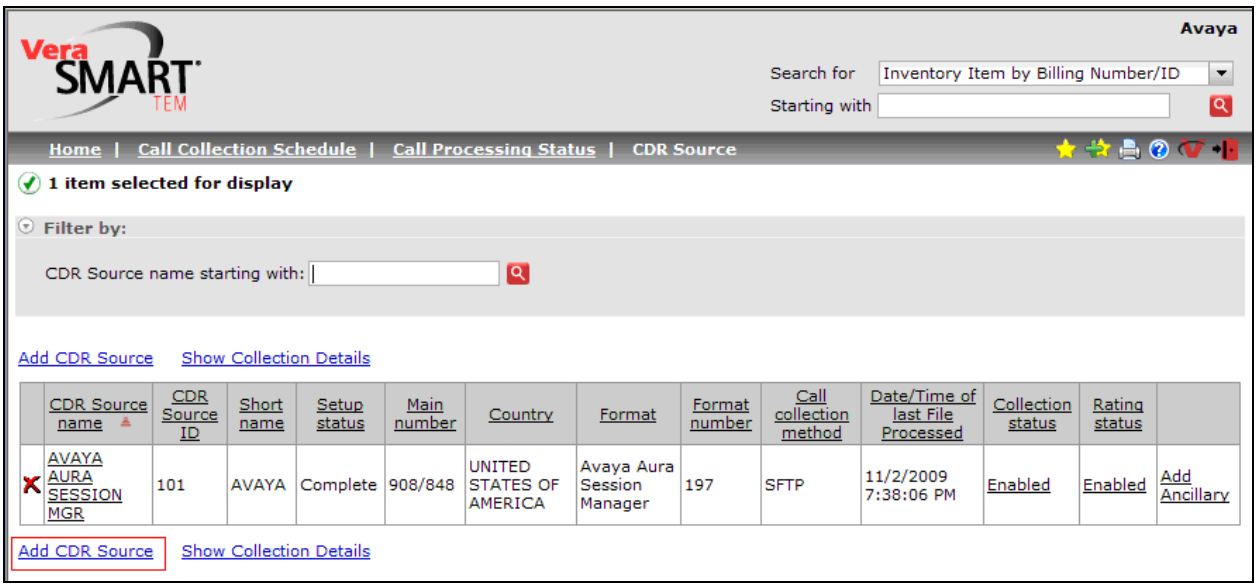
To configure SFTP on Veramark VeraSMART, launch a web browser, enter **http://<IP address of Veramark VeraSMART server>** as URL, and log in with the appropriate credentials.



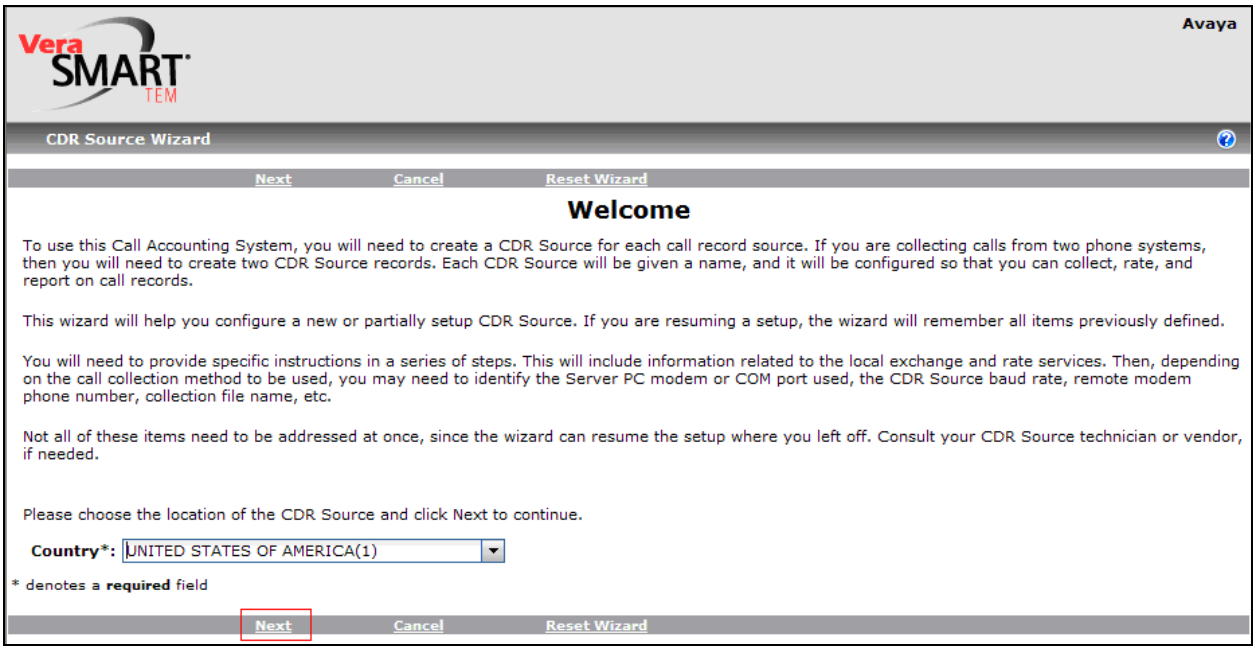
From the Main window, click on the **Call Accounting → Call Collection → CDR Source** link.



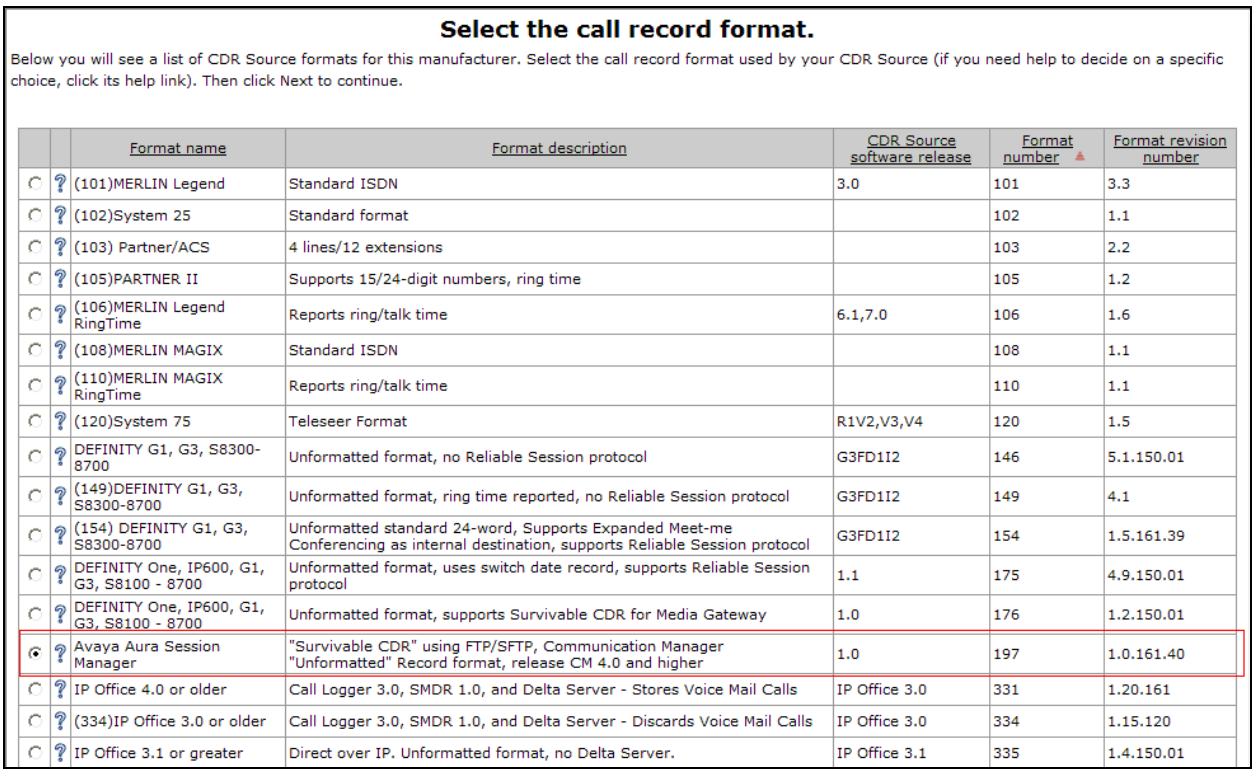
In the CDR Source window, click on the **Add CDR Source** link.



In the CDR Source Wizard, keep click **next** until the **Select the call record format** page is displayed.



In the **Select call record format** page, select **Avaya Aura Session Manager** format.

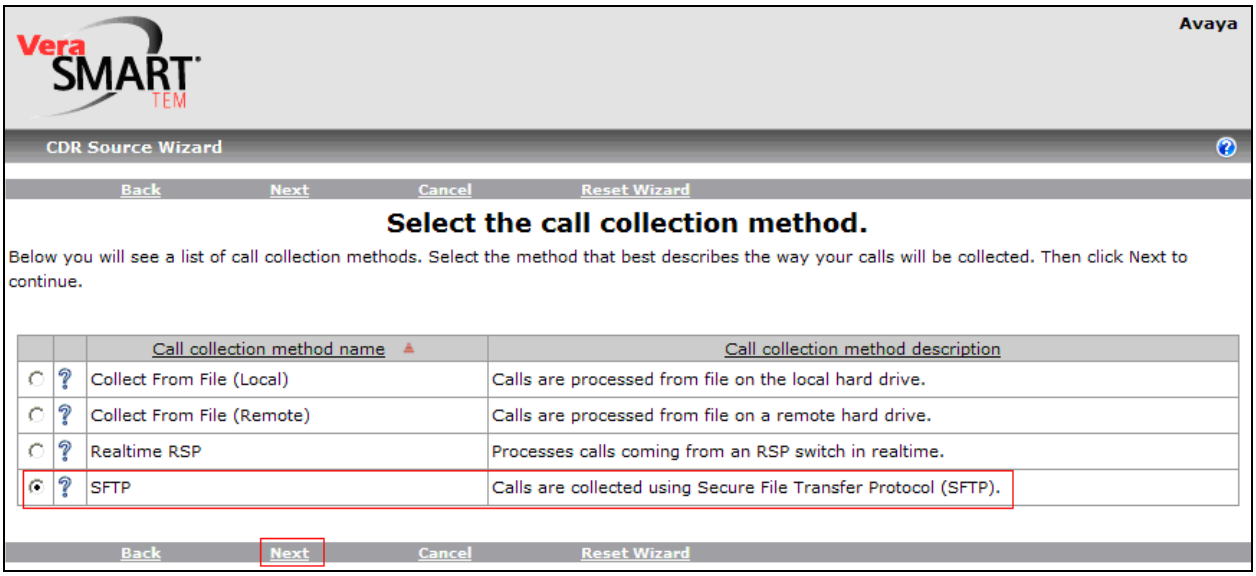


Select the call record format.

Below you will see a list of CDR Source formats for this manufacturer. Select the call record format used by your CDR Source (if you need help to decide on a specific choice, click its help link). Then click Next to continue.

	Format name	Format description	CDR Source software release	Format number	Format revision number
○	(101)MERLIN Legend	Standard ISDN	3.0	101	3.3
○	(102)System 25	Standard format		102	1.1
○	(103) Partner/ACS	4 lines/12 extensions		103	2.2
○	(105)PARTNER II	Supports 15/24-digit numbers, ring time		105	1.2
○	(106)MERLIN Legend RingTime	Reports ring/talk time	6.1,7.0	106	1.6
○	(108)MERLIN MAGIX	Standard ISDN		108	1.1
○	(110)MERLIN MAGIX RingTime	Reports ring/talk time		110	1.1
○	(120)System 75	Teleseer Format	R1V2,V3,V4	120	1.5
○	DEFINITY G1, G3, S8300-8700	Unformatted format, no Reliable Session protocol	G3FD1I2	146	5.1.150.01
○	(149)DEFINITY G1, G3, S8300-8700	Unformatted format, ring time reported, no Reliable Session protocol	G3FD1I2	149	4.1
○	(154) DEFINITY G1, G3, S8300-8700	Unformatted standard 24-word, Supports Expanded Meet-me Conferencing as internal destination, supports Reliable Session protocol	G3FD1I2	154	1.5.161.39
○	DEFINITY One, IP600, G1, G3, S8100 - 8700	Unformatted format, uses switch date record, supports Reliable Session protocol	1.1	175	4.9.150.01
○	DEFINITY One, IP600, G1, G3, S8100 - 8700	Unformatted format, supports Survivable CDR for Media Gateway	1.0	176	1.2.150.01
◉	Avaya Aura Session Manager	"Survivable CDR" using FTP/SFTP, Communication Manager "Unformatted" Record format, release CM 4.0 and higher	1.0	197	1.0.161.40
○	IP Office 4.0 or older	Call Logger 3.0, SMDR 1.0, and Delta Server - Stores Voice Mail Calls	IP Office 3.0	331	1.20.161
○	(334)IP Office 3.0 or older	Call Logger 3.0, SMDR 1.0, and Delta Server - Discards Voice Mail Calls	IP Office 3.0	334	1.15.120
○	IP Office 3.1 or greater	Direct over IP. Unformatted format, no Delta Server.	IP Office 3.1	335	1.4.150.01

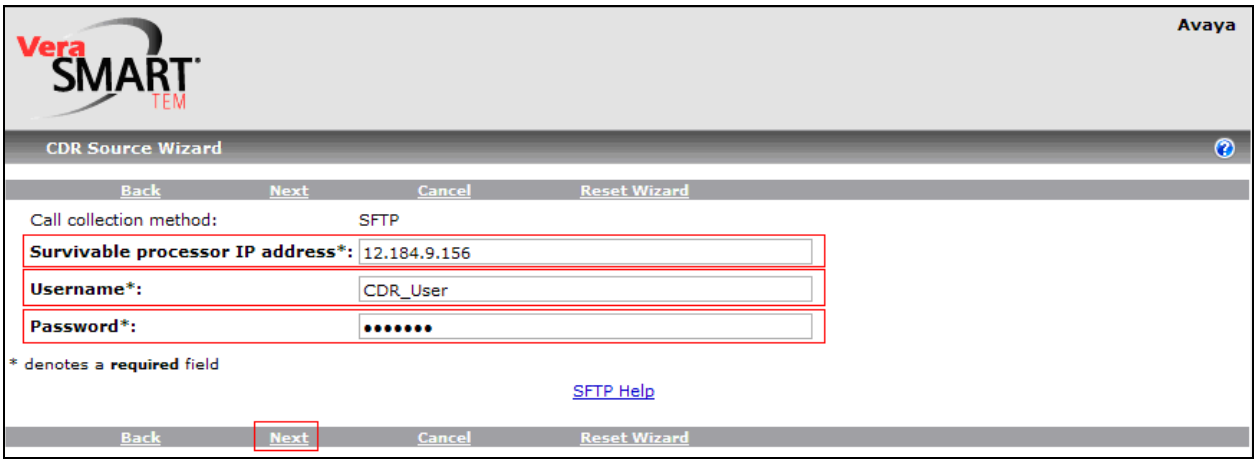
In the **Select the call collection method** page, select the **SFTP** method.
Click on the **next** link.



Provide the following information:

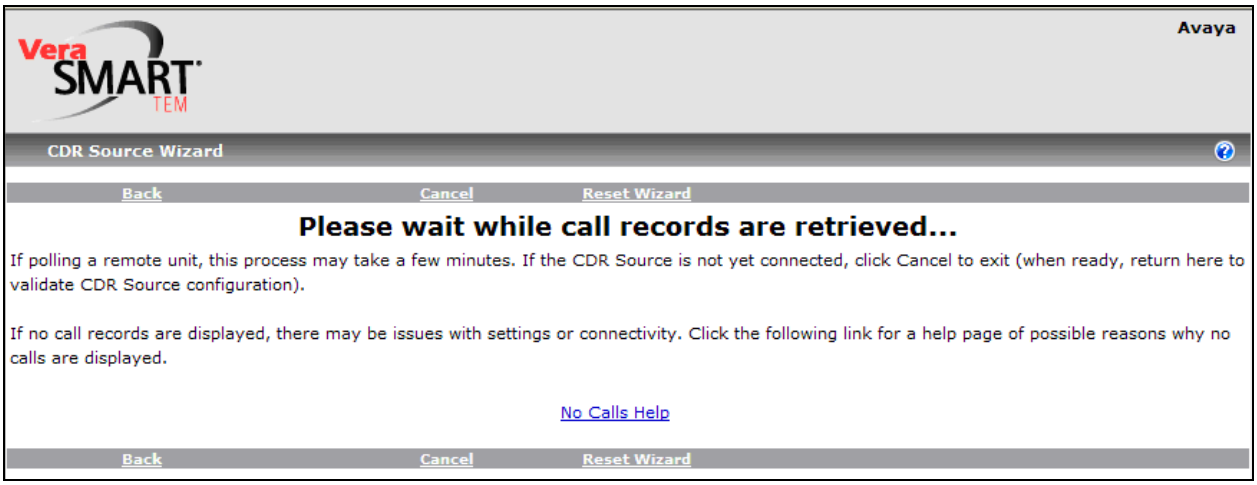
- Survivable processor IP address – Enter the IP address of Session Manager. The following screen shows the public IP address of Session Manager. This IP address has been NATed to private IP address during the compliance test.
- Username – Enter the username created in Session Manager in **Section 5.5**.
- Password – Enter the password created in Session Manager in **Section 5.5**

Click on the **Next** link.

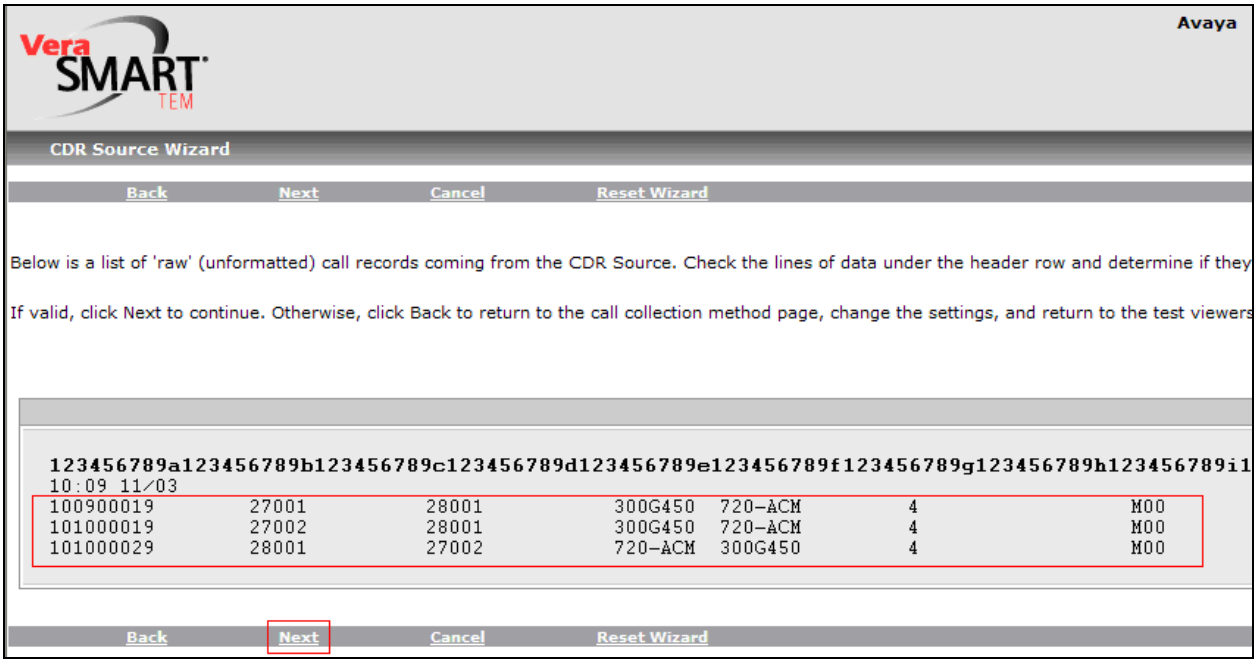


Before the next step, make sure there is a record stored in the CDR directory in Session Manager. The CDR directory is located in /var/home/ftp/CDR.

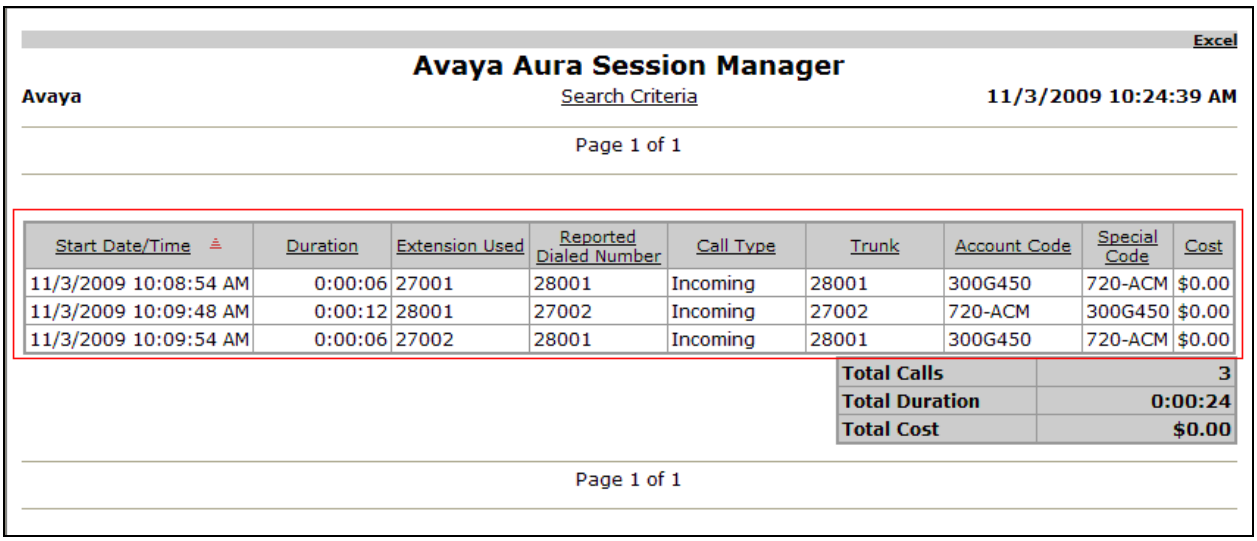
The following two windows show collecting raw CDR data from Session Manager using SFTP.



Click on the **Next** link.



The following window shows the final CDR report from Veramark VeraSMART.



Excel

Avaya Aura Session Manager

Avaya | Search Criteria | 11/3/2009 10:24:39 AM

Page 1 of 1

Start Date/Time	Duration	Extension Used	Reported Dialed Number	Call Type	Trunk	Account Code	Special Code	Cost
11/3/2009 10:08:54 AM	0:00:06	27001	28001	Incoming	28001	300G450	720-ACM	$0.00
11/3/2009 10:09:48 AM	0:00:12	28001	27002	Incoming	27002	720-ACM	300G450	$0.00
11/3/2009 10:09:54 AM	0:00:06	27002	28001	Incoming	28001	300G450	720-ACM	$0.00

Total Calls	**3**
Total Duration	**0:00:24**
Total Cost	**$0.00**

Page 1 of 1

7. Interoperability Compliance Testing

The compliance test included SFTP operation to allow Veramark VeraSMART to collect raw CDR data in Session Manager. The serviceability test introduced failure scenarios to see if the VeraSMART can resume CDR collection after recovery.

7.1. General Test Approach and Test Results

The general test approach was to let Veramark VeraSMART manually SFTP into the Session Manager using the credentials that were provided to Veramark VeraSMART during the Session Manager configuration. Once the VeraSMART collects raw data, the Vera SMART transforms raw data into call records available for end customers.

For serviceability testing, physical and logical links were disabled/re-enabled, Session Manager was reset and the VeraSMART was restarted.

7.2. Test Results

All executed test cases passed. Veramark VeraSMART successfully collected the CDR records from Session Manager via a SFTP connection for all types of SIP calls between two Communication Managers. For serviceability testing, Veramark VeraSMART was able to resume collection of CDR records after failure recovery including buffered CDR records for calls that were placed during the outages.

8. Verification Steps

The following steps may be used to verify the configuration:

- Make several SIP calls between two Communication Managers, and verify that call records were stored in CDR directory of Session Manager (/var/home/ftp/CDR).
- Run the SFTP script from Veramark VeraSMART. Veramark VeraSMART was able to SFTP into Session Manager, pulled raw data, transferred raw data to Veramark VeraSMART, and transformed them into report.

9. Conclusion

These Application Notes describe the procedures for configuring Veramark VeraSMART to collect call detail records from Session Manager, and Veramark VeraSMART successfully passed all compliance testing.

10. References

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

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

[1] *Avaya Aura™ Session Manager Call Detail Recording Interface*, Issue 1.0, 20 Apr 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.