



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.

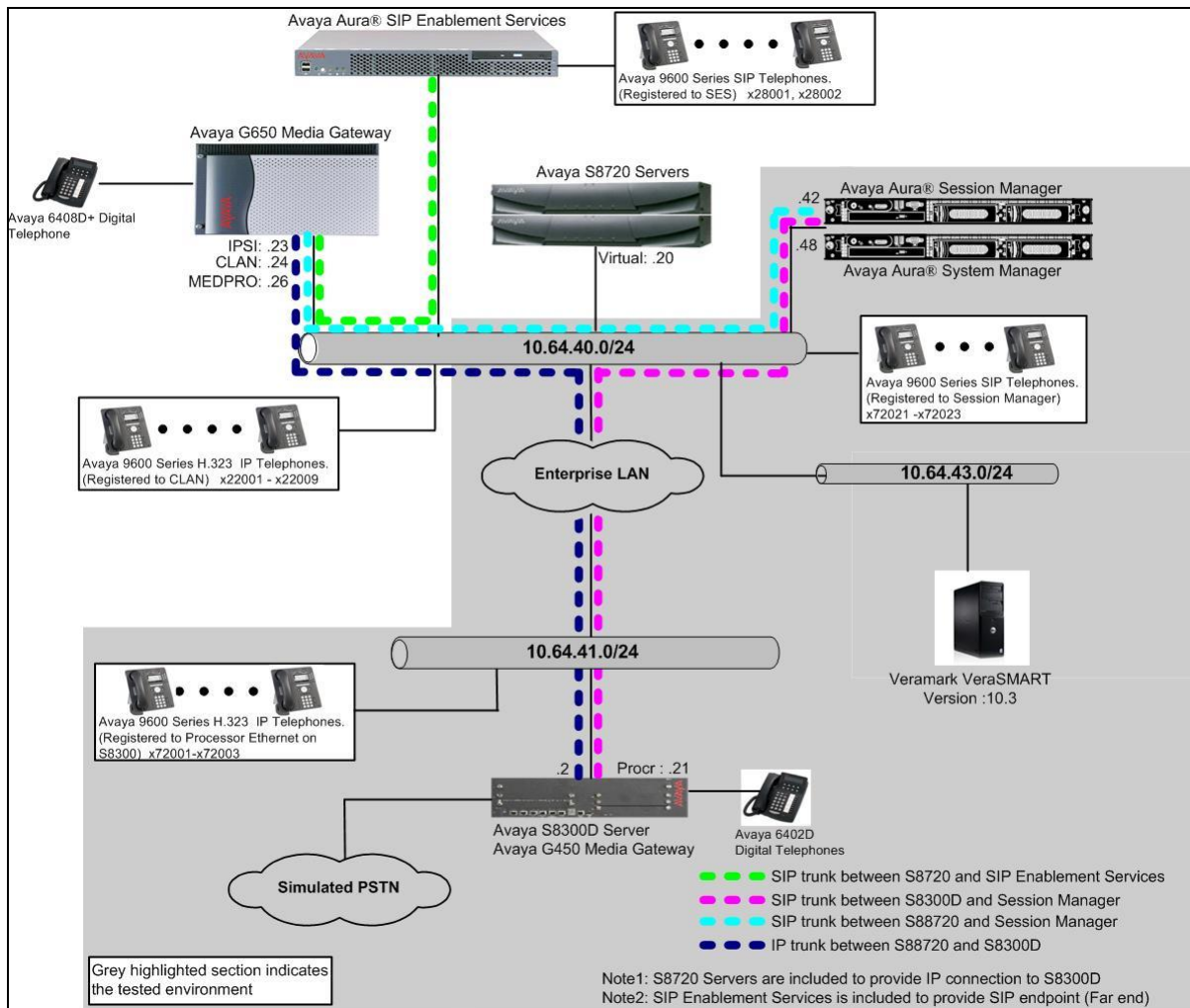


Figure 1. Test configuration of Veramark VeraSMART eCAS with Avaya Aura® Communication Manager

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	2.6.8
	9630	2.6.8
	9650	2.6.8
Avaya 9600 Series H.323 IP Telephone		
	9620	3.1
	9630	3.1
	9650	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: verasmart** [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 Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer		
CDR1	y	30	3	3	60		
CDR2	v	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			
Extension	Assigned Members:	9	of 1000 administered
72001	Extension	Extension	Extension
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			
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 Link Bounce Recovery? y		RSVP Enabled? n	
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		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Initial IP-IP 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      Len Del      Insert      Net Conv      Node
Pattern                               Digits
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 String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
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:	v	v	v	v	v	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
<p>CONFIGURATION SET: 2</p> <p>Configuration Set Description:</p> <p>Calling Number Style: network</p> <p>CDR for Origination: phone-number</p> <p>CDR for Calls to EC500 Destination? n</p> <p>Fast Connect on Origination? n</p> <p>Post Connect Dialing Options: dtmf</p> <p>Cellular Voice Mail Detection: timed (seconds): 4</p> <p>Barge-in Tone? n</p> <p>Calling Number Verification? y</p> <p>Call Appearance Selection for Origination: primary-first</p> <p>Confirmed Answer? n</p> <p>Use Shared Voice Connections for Second Call Answered? n</p> <p>Use Shared Voice Connections for Second Call Initiated? n</p>	

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.

Avaya Aura® System Manager 6.2

Last Logged on at December 28, 2012 12:56 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Users

Administrators
Manage Administrative Users

Directory Synchronization
Synchronize users with the enterprise directory

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

User Management
Manage users, shared user resources and provision users

Elements

B5800 Branch Gateway
Manage B5800 Branch Gateway 6.2 elements

Communication Manager
Manage Communication Manager 5.2 and higher elements

Conferencing
Manage Conferencing Multimedia Server objects

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

Meeting Exchange
Manage Meeting Exchange and Avaya Aura Conferencing 6.0 elements

Messaging
Manage Avaya Aura Messaging, Communication Manager Messaging, and Modular Messaging

Presence
Presence

Routing
Network Routing Policy

Session Manager
Session Manager Element Manager

SIP AS 8.1
SIP AS 8.1

Services

Backup and Restore
Backup and restore System Manager database

Bulk Import and Export
Manage Bulk Import and Export of Users, User Global Settings, Roles, Elements and others

Configurations
Manage system wide configurations

Events
Manage alarms, view and harvest logs

Licenses
View and configure licenses

Replication
Track data replication nodes, repair replication nodes

Scheduler
Schedule, track, cancel, update and delete jobs

Security
Manage Security Certificates

Templates
Manage Templates for Communication Manager, Messaging System and B5800 Branch Gateway elements

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.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and user information: 'Last Logged on at December 28, 2012 12:56 PM', 'Help | About | Change Password | Log off admin'. The breadcrumb trail is 'Home / Elements / Routing / Domains'. The left sidebar shows a tree view with 'Routing' expanded, containing 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', and 'Dial Patterns'. The main content area is titled 'Domain Management' and includes buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these is a table with 2 items. The table has columns: Name, Type, Default, and Notes. The first row shows 'avaya.com' with Type 'sip' and an unchecked 'Default' checkbox. At the bottom, there is a 'Select : All, None' option.

Name	Type	Default	Notes
avaya.com	sip	<input type="checkbox"/>	

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.

General section

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.

Location Pattern section

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.

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.2', and a 'Last Logged on' timestamp of 'December 28, 2012 12:56 PM'. Navigation links for 'Help', 'About', 'Change Password', and 'Log off admin' are present. A breadcrumb trail shows 'Home / Elements / Routing / Locations'. On the left, a sidebar menu lists various configuration areas, with 'Locations' highlighted under the 'Routing' section. The main content area, titled 'Location', contains action buttons ('Edit', 'New', 'Duplicate', 'Delete', 'More Actions') and a table of existing locations. The table has columns for 'Name' and 'Notes' and shows two entries: '41-subnet' with the note 'Main Test Network' and 'App-Server'. A 'Filter: Enable' option is visible at the top right of the table. Below the table, a 'Select : All, None' option is provided.

Name	Notes
41-subnet	Main Test Network
App-Server	

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.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and a 'Last Logged on at December 28, 2012 12:56 PM' status. Below the navigation bar, there are links for 'Help', 'About', 'Change Password', and 'Log off admin'. The main content area is titled 'SIP Entities' and includes a 'Home / Elements / Routing / SIP Entities' breadcrumb. A sidebar on the left lists various configuration options: Routing, Domains, Locations, Adaptations, SIP Entities (selected), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main area contains a table with 6 items, showing a list of SIP entities. The table has columns for Name, FQDN or IP Address, Type, and Notes. The entities listed are S8300D and SessionManager. The table also includes a 'Filter: Enable' option and a 'Select : All, None' dropdown.

Name	FQDN or IP Address	Type	Notes
S8300D	10.64.41.21	CM	
SessionManager	10.64.41.42	Session Manager	

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.

Avaya Aura® System Manager 6.2

Last Logged on at December 28, 2012 12:56 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Entity Links

Entity Links

Edit New Duplicate Delete More Actions

9 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
<input type="checkbox"/>	SM-S8300D-TLS	SessionManager	TLS	5061	S8300D	5061	Trusted	

Select : All, None

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.

The screenshot displays the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and user information: 'Last Logged on at December 28, 2012 12:56 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing / Time Ranges'. On the left, a sidebar menu lists various configuration options, with 'Time Ranges' selected under the 'Routing' section. The main content area, titled 'Time Ranges', contains action buttons: 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these is a table with one item, '24/7'. The table has columns for Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. The '24/7' entry has checkboxes for all days of the week checked, a start time of '00:00', and an end time of '23:59'. A 'Filter: Enable' link is present at the top right of the table. At the bottom of the table, it says 'Select : All, None'.

	Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
<input type="checkbox"/>	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	

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

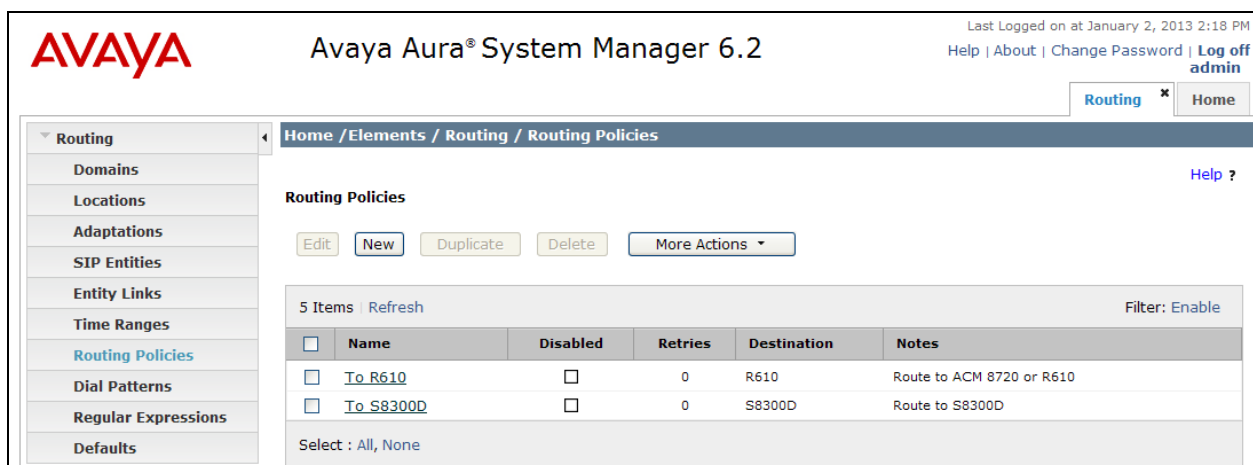
- Enter a descriptive name in the **Name** field.
- Enter a description in the **Notes** field if desired.

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.



The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.2", and user information: "Last Logged on at January 2, 2013 2:18 PM", "Help | About | Change Password | Log off admin". The main navigation menu on the left lists: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The breadcrumb trail is "Home / Elements / Routing / Routing Policies". The "Routing Policies" section has buttons for "Edit", "New", "Duplicate", "Delete", and "More Actions". Below this is a table with 5 items, showing a list of routing policies. The table has columns: Name, Disabled, Retries, Destination, and Notes. The first two rows are visible: "To R610" and "To S8300D".

	Name	Disabled	Retries	Destination	Notes
<input type="checkbox"/>	To R610	<input type="checkbox"/>	0	R610	Route to ACM 8720 or R610
<input type="checkbox"/>	To S8300D	<input type="checkbox"/>	0	S8300D	Route to S8300D

Filter: Enable

Select : All, None

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.

Avaya Aura® System Manager 6.2

Last Logged on at January 2, 2013 2:18 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Dial Patterns

Routing
Home

Dial Patterns

Edit
New
Duplicate
Delete
More Actions

20 Items | Refresh
Filter: Enable

	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	1303	11	11	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	20004	5	5	<input type="checkbox"/>			avaya.com	Rob's wireless
<input type="checkbox"/>	2200	5	5	<input type="checkbox"/>			avaya.com	H.323 on S8720 or R610
<input type="checkbox"/>	2800	5	5	<input type="checkbox"/>			avaya.com	SIP on S8720 or R610
<input type="checkbox"/>	303	10	10	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	50000	5	5	<input type="checkbox"/>			avaya.com	
<input type="checkbox"/>	53005	5	5	<input type="checkbox"/>			avaya.com	Mike's extension (H323) on 21.41
<input type="checkbox"/>	538	7	7	<input type="checkbox"/>			-ALL-	
<input type="checkbox"/>	7200	5	5	<input type="checkbox"/>			avaya.com	SIP and H.323
<input type="checkbox"/>	7202	5	5	<input type="checkbox"/>			avaya.com	
<input type="checkbox"/>	72031	5	5	<input type="checkbox"/>			avaya.com	extension for Biamp Conf Srv thru SIP trunk
<input type="checkbox"/>	72032	5	5	<input type="checkbox"/>			avaya.com	Biamp SIP extension
<input type="checkbox"/>	72033	5	5	<input type="checkbox"/>			avaya.com	Biamp SIP extension
<input type="checkbox"/>	7204	5	5	<input type="checkbox"/>			avaya.com	
<input type="checkbox"/>	7205	5	5	<input type="checkbox"/>			avaya.com	IPC Unige-Phones

Select : All, None

Previous
Page 1 of 2
Next

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).

The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and a user status 'Last Logged on at December 28, 2012 12:56 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail reads 'Home / Elements / Inventory / Manage Elements'. On the left, a sidebar menu lists 'Inventory' (expanded) with sub-items: 'Manage Elements' (selected), 'Upgrade Management', 'Collected Inventory', 'Manage Serviceability Agents', 'Inventory Management', 'Synchronization', and 'CS 1000 and CallPilot Synchronization'. The main content area is titled 'New Elements' and contains a 'General' tab with a red asterisk. Below the tab is a 'General' dropdown menu and a required field '* Type' with a dropdown menu currently showing 'Select Type'. 'Commit' and 'Cancel' buttons are located at the top right of the form area.

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.

The screenshot shows the Avaya Aura System Manager 6.2 interface for the 'New Communication Manager' page. The top navigation bar is identical to the previous screenshot. The breadcrumb trail is 'Home / Elements / Inventory / Manage Elements'. The left sidebar menu is the same. The main content area is titled 'New Communication Manager' and contains two tabs: 'General' (selected, with a red asterisk) and 'Attributes' (with a red asterisk). Below the tabs is a 'General' dropdown menu. The form contains several required fields: '* Name' (text box with 'Element-S8300D'), '* Type' (dropdown menu with 'Communication Manager' and a 'Reset' button), 'Description' (text box with 'S8300D in Lab D4H26'), and '* Node' (text box with '10.64.41.21'). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

- 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 screenshot shows the Avaya Aura System Manager 6.2 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.2', and a 'Last Logged on' timestamp. Navigation links for 'Help', 'About', 'Change Password', and 'Log off admin' are present. A breadcrumb trail indicates the current path: 'Home / Elements / Inventory / Manage Elements'. The left sidebar contains a tree view with categories like 'Inventory', 'Upgrade Management', and 'Manage Serviceability Agents'. The main content area is titled 'New Communication Manager' and features two tabs: 'General' and 'Attributes'. The 'Attributes' tab is active, showing 'SNMP Attributes' and 'Attributes' sections. The 'Attributes' section contains several form fields: 'Login' (Interop), 'Password' (masked), 'Confirm Password' (masked), 'Is SSH Connection' (checked), 'Port' (5022), 'Alternate IP Address', 'RSA SSH Fingerprint (Primary IP)', 'RSA SSH Fingerprint (Alternate IP)', 'Is ASG Enabled' (unchecked), 'ASG Key', 'Confirm ASG Key', 'Location', and 'Enable Notifications' (unchecked). 'Commit' and 'Cancel' buttons are located at the top right of the form area.

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

Avaya Aura® System Manager 6.2

Last Logged on at December 28, 2012 12:56 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Inventory

Manage Elements

Upgrade Management

Collected Inventory

Manage Serviceability Agents

Inventory Management

Synchronization

CS 1000 and CallPilot Synchronization

Home / Elements / Inventory / Manage Elements

Manage Elements

Elements

View

Edit

New

Delete

More Actions

12 Items

Refresh

Show ALL

Filter: Enable

<input type="checkbox"/>	Name	Node	Type	Version	Description
<input type="checkbox"/>	Corporate Directory	10.64.41.48	UCMAApp		Corporate Directory Application generates the corporate directory file and uploads it to CS1000.
<input type="checkbox"/>	Element-R610	10.64.40.24	Communication Manager		
<input type="checkbox"/>	Element-S8300D	10.64.41.21	Communication Manager		
<input type="checkbox"/>	IPSec	10.64.41.48	UCMAApp		Centralized IPSec allows network-wide policy implementation and synchronization of Preshared Keys across network targets.
<input type="checkbox"/>	Numbering Groups	10.64.41.48	UCMAApp		A numbering group represents common numbering planning attributes which are shared by a group of subscriber telephony accounts. Calling Line ID/ Uniform Resource Identifier generation, which runs every two hours, uses numbering groups to generate the Calling Line ID addresses required for Unicode display name.
<input type="checkbox"/>	Patches	10.64.41.48	UCMAApp		Manages patch deployment on servers associated with CS 1000 systems across your network.
<input type="checkbox"/>	Secure FTP Token	10.64.41.48	UCMAApp		Secure FTP token generation and distribution of token across all CS1K nodes.
<input type="checkbox"/>	SessionManager	10.64.41.43	Session Manager		
<input type="checkbox"/>	smgr.avaya.com (primary)	10.64.41.48	UCMAApp		Base OS element.
<input type="checkbox"/>	SNMP Profiles	10.64.41.48	UCMAApp		Centralized SNMP Profile Management and Profile Distribution to the elements associated with CS1000 systems across the network.
<input type="checkbox"/>	Software Deployment	10.64.41.48	UCMAApp		Manages application deployment on servers across your network.
<input type="checkbox"/>	System Manager	localhost	System Manager	6.2	

Select : All, None

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 screenshot shows the Avaya Aura System Manager 6.2 web interface. The top header includes the Avaya logo, the product name "Avaya Aura® System Manager 6.2", and user information: "Last Logged on at January 2, 2013 2:18 PM" and "Help | About | Change Password | Log off admin". Below the header is a breadcrumb trail: "Home / Elements / Session Manager / Application Configuration / Applications". The left sidebar contains a navigation menu with categories like Session Manager, Network Configuration, Device and Location Configuration, Application Configuration (selected), and System Status. Under Application Configuration, "Applications" is highlighted. The main content area is titled "Application Editor" and contains the following fields:

- Application** section:
 - *Name: Text input field containing "App-S8300D".
 - *SIP Entity: Dropdown menu showing "S8300D".
 - *CM System for SIP Entity: Dropdown menu showing "Element-S8300D" with a "Refresh" button and a link "View/Add CM Systems".
 - Description: Text input field.
- Application Attributes (optional)** section:
 - A table with two columns: "Name" and "Value".
 - Row 1: "Application Handle" with an empty text input field.
 - Row 2: "URI Parameters" with an empty text input field.

At the top right of the main content area are "Commit" and "Cancel" buttons.

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

Avaya Aura® System Manager 6.2

Last Logged on at December 28, 2012 12:56 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Session Manager *Inventory *Routing *Home

Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
Applications

Home / Elements / Session Manager / Application Configuration / Applications

Help ?

Applications

This page allows you to add, edit, or remove applications for available SIP Entities.

Application Entries

New Edit Delete

2 Items RefreshFilter: Enable

<input type="checkbox"/>	Application Name	SIP Entity	Media Filtering	Description
<input type="checkbox"/>	App-S8300D	S8300D	<input type="checkbox"/>	


Select : All, None

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.

The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title "Avaya Aura® System Manager 6.2", and user information: "Last Logged on at January 3, 2013 11:19 AM", "Help | About | Change Password | Log off admin". The left sidebar shows a tree view with "Session Manager" expanded, containing "Dashboard", "Session Manager Administration", "Communication Profile Editor", "Network Configuration", "Device and Location Configuration", and "Performance". The main content area is titled "Application Sequence Editor" and shows the "Application Sequence" section. It has input fields for "Name" (containing "AppSeq-S8300D") and "Description". There are "Commit" and "Cancel" buttons.

- 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 screenshot shows the "Applications in this Sequence" section of the Avaya Aura System Manager 6.2 interface. It includes a table with 1 item and a section for "Available Applications" with 2 items.

Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>	App-S8300D	S8300D	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

Name	SIP Entity	Description
App-S8300D	S8300D	

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

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The top header includes the Avaya logo, the product name, and the user's login status. A navigation menu on the left lists various system management functions. The main content area is titled 'Application Sequences' and contains a table listing the defined sequences. One sequence, 'AppSeq-S8300D', is visible in the table.

Avaya Aura® System Manager 6.2

Last Logged on at December 28, 2012 12:56 PM
Help | About | Change Password | Log off admin

Session Manager * Inventory * Routing * Home

Home / Elements / Session Manager / Application Configuration / Application Sequences

Application Sequences

This page allows you to add, edit, or remove sequences of applications.

[Application Sequences](#)

[New](#) [Edit](#) [Delete](#)

2 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	AppSeq-S8300D	

Select : All, None

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:

- Identity section
 - **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.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at December 21, 2012 3:27 PM Help | About | Change Password | Log off admin

User Management * User Management * Home

Home / Users / User Management / Manage Users

Manage Users Public Contacts Shared Addresses System Presence ACLs

New User Profile Commit & Continue Commit Cancel Help ?

Identity * Communication Profile * Membership Contacts

Identity

* Last Name: 72021

* First Name: 72021

Middle Name:

Description:

* Login Name: 72021@avaya.com

* Authentication Type: Basic

* Password:

* Confirm Password:

Localized Display Name: 72021

Endpoint Display Name: 72021

Title:

Language Preference: English (United States)

Time Zone: (-7:0)Mountain Time (US & Canada); Chihuahua, La Paz

- 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 ☒

The screenshot shows the Avaya Aura System Manager 6.2 interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. The user is logged in as 'admin'. The left sidebar shows 'User Management' with sub-links: 'Manage Users', 'Public Contacts', 'Shared Addresses', and 'System Presence ACLs'. The main content area is titled 'New User Profile' and has tabs for 'Identity', 'Communication Profile', 'Membership', and 'Contacts'. The 'Communication Profile' tab is active, showing fields for 'Communication Profile Password' and 'Confirm Password', both masked with dots. Below these are buttons for 'New', 'Delete', 'Done', and 'Cancel'. A table lists communication profiles, with 'Primary' selected and marked as the default. Below the table, the 'Name' field is set to 'Primary' and the 'Default' checkbox is checked.

- 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.

The screenshot shows the 'Communication Address' form. At the top, there are buttons for 'New', 'Edit', and 'Delete'. Below these is a table with columns 'Type', 'Handle', and 'Domain'. The table is empty, with a message 'No Records found'. Below the table, the 'Type' dropdown menu is set to 'Avaya SIP'. The 'Fully Qualified Address' field is set to '72021' and the domain dropdown is set to 'avaya.com'. At the bottom right, there are 'Add' and 'Cancel' buttons.

- Session Manager Profile section
 - **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**.

☒ **Session Manager Profile**

* **Primary Session Manager**

SessionManager

Primary	Secondary	Maximum
21	0	21

Secondary Session Manager

(None)

Primary	Secondary	Maximum

Origination Application Sequence

AppSeq-S8300D

Termination Application Sequence

AppSeq-S8300D

Conference Factory Set

(None)

Survivability Server

(None)

* **Home Location**

41-subnet

- 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.

The screenshot shows a web-based configuration form titled "CM Endpoint Profile" with a dropdown arrow. The form contains the following fields and options:

- * System:** A dropdown menu showing "Element-S8300D".
- * Profile Type:** A dropdown menu showing "Endpoint".
- Use Existing Endpoints:** An unchecked checkbox.
- * Extension:** A text input field containing "72021" and a magnifying glass icon. To its right is a button labeled "Endpoint Editor".
- * Template:** A dropdown menu showing "DEFAULT_9620SIP_CM_6_2".
- Set Type:** A text input field containing "9620SIP".
- Security Code:** A text input field containing six dots "••••••".
- * Port:** A dropdown menu showing "IP" with a magnifying glass icon.
- Voice Mail Number:** A text input field containing "72021".
- Preferred Handle:** A dropdown menu showing "(None)".
- Delete Endpoint on Unassign of Endpoint from User or on Delete User:** A checked checkbox.
- Override Endpoint Name:** A checked checkbox.

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

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

AVAYA

Avaya Aura® System Manager 6.2

Last Logged on at January 2, 2013 10:30 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

User Management xHome

User ManagementManage UsersPublic ContactsShared AddressesSystem Presence ACLs

Home / Users / User Management / Manage Users

User ManagementHelp ?

UsersViewEditNewDuplicateDeleteMore ActionsAdvanced Search ▶

21 Items Refresh Show 15 Filter: Enable

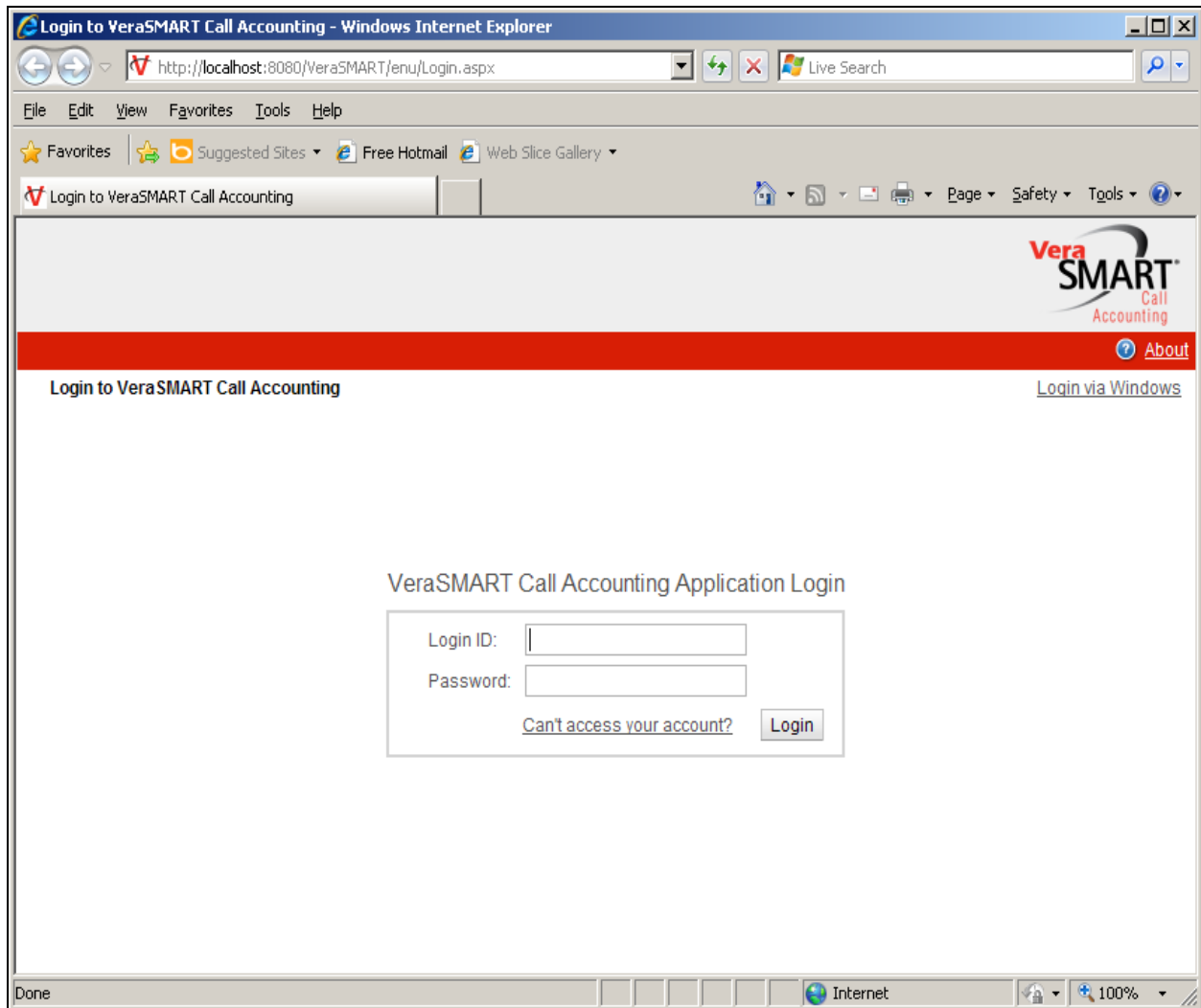
<input type="checkbox"/>	Last Name	First Name	Display Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>	72026	72026	one-X-1	72026@avaya.com	72026	
<input type="checkbox"/>	72027	72027	one-X-2	72027@avaya.com	72027	
<input type="checkbox"/>	72021	72021	S8300-SIP1	72021@avaya.com	72021	
<input type="checkbox"/>	72022	72022	S8300-SIP2	72022@avaya.com	72022	
<input type="checkbox"/>	72023	72023	S8300-SIP3	72023@avaya.com	72023	
<input type="checkbox"/>	72024	72024	S8300-SIP4	72024@avaya.com	72024	

Select : All, None< PreviousPage 2 of 2Next >

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**.

CDR Source

Add Show Collection Details

Search

CDR Source name starting with:

Search

No items selected for display Items per page: 50

CDR Source name	CDR Source ID	Short name	Setup status	Main number	Country	Format	Format number	Format revision number	Call collection method	Date/Time of last File Processed	Collection status	Rating status
No items selected for display												

No items selected for display Items per page: 50

Add Show Collection Details

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

CDR Source Wizard

Back Next Finish Cancel

Welcome

To use this Call Accounting System, you will need to create a CDR Source for each call record source. If you are collecting calls from two phone systems, then you will need to create two CDR Source records. Each CDR Source will be given a name, and it will be configured so that you can collect, rate, and report on call records.

This wizard will help you configure a new or partially setup CDR Source. If you are resuming a setup, the wizard will remember all items previously defined.

You will need to provide specific instructions in a series of steps. This will include information related to the local exchange and rate services. Then, depending on the call collection method to be used, you may need to identify the Server PC modem or COM port used, the CDR Source baud rate, remote modem phone number, collection file name, etc.

Not all of these items need to be addressed at once, since the wizard can resume the setup where you left off. Consult your CDR Source technician or vendor, if needed.

Please choose the location of the CDR Source and click Next to continue.

Country: UNITED STATES OF AMERICA(1)

Back Next Finish Cancel

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

Call Accounting Organization Administration

Extensions Call Detail Call Collection Call Rating Tools Reports Help

CDR Source Wizard

Back Next Finish Cancel

Identify the source of call records.
Create a CDR Source name. Use up to 25 alphanumeric characters for a unique name (this can be anything that makes sense to you to reference this CDR Source - for example: East Coast, New York Office, Main CDR Source).

Enter the CDR Source area code, local exchange, and local rating method (this depends on the rate service used locally - for example: measured, message, flat, etc.).

CDR Source name*: Avaya

Country: UNITED STATES OF AMERICA(1)

Area code*: 303

Local exchange*: 538

Local rate method: Measured

Do you want to discard the following types of calls for this CDR Source? These choices can be changed later through the 'edit' CDR Source function.

Internal: ☒ Store ☐ Discard Incoming: ☒ Store ☐ Discard

Back Next Finish Cancel

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

Call Accounting Organization Administration

Extensions Call Detail Call Collection Call Rating Tools Reports Help

CDR Source Wizard

Back Next Finish Cancel

Select the CDR Source manufacturer.
Every telephone system produces call records in a specific format. The system uses "format" software to interpret call record data.

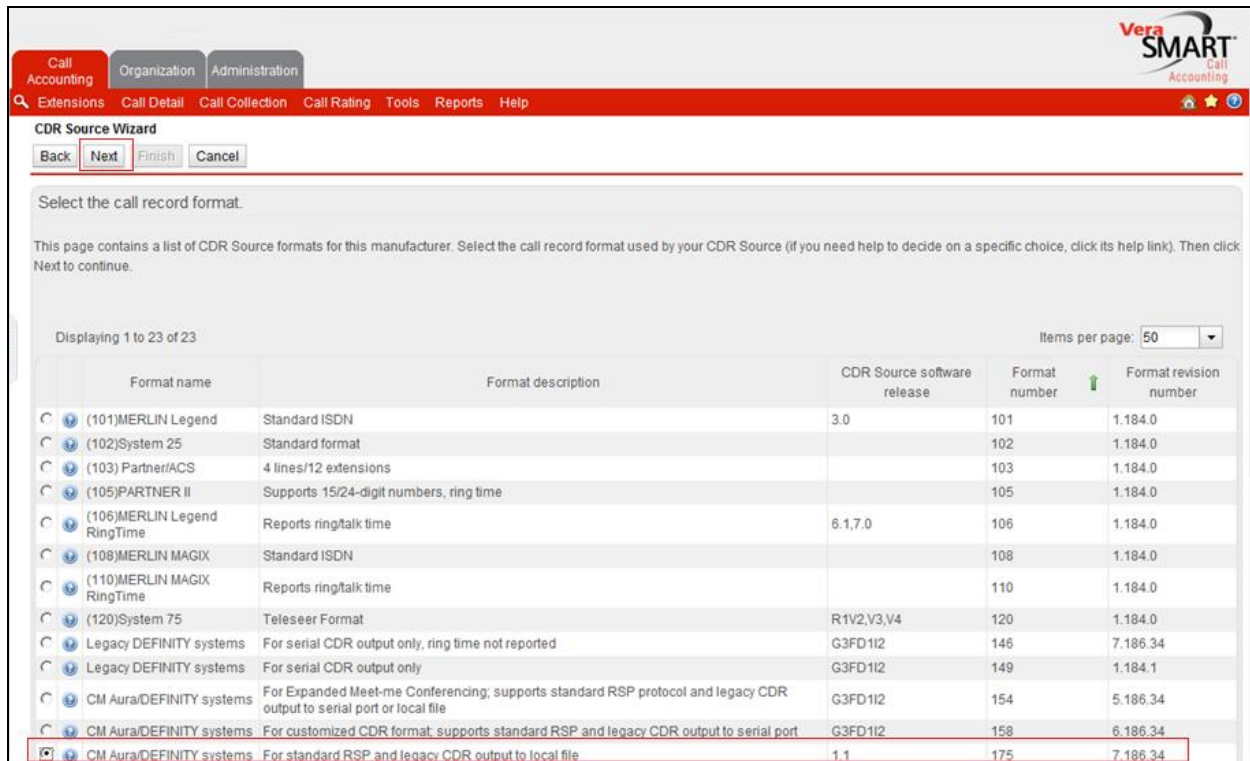
From the list, select the manufacturer of the CDR Source, or if collecting call records from another call accounting system select "Call Accounting System", then click Next to continue.

Currently assigned Format: None

Manufacturer: Avaya

Back Next Finish Cancel

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



CDR Source Wizard

Back Next Finish Cancel

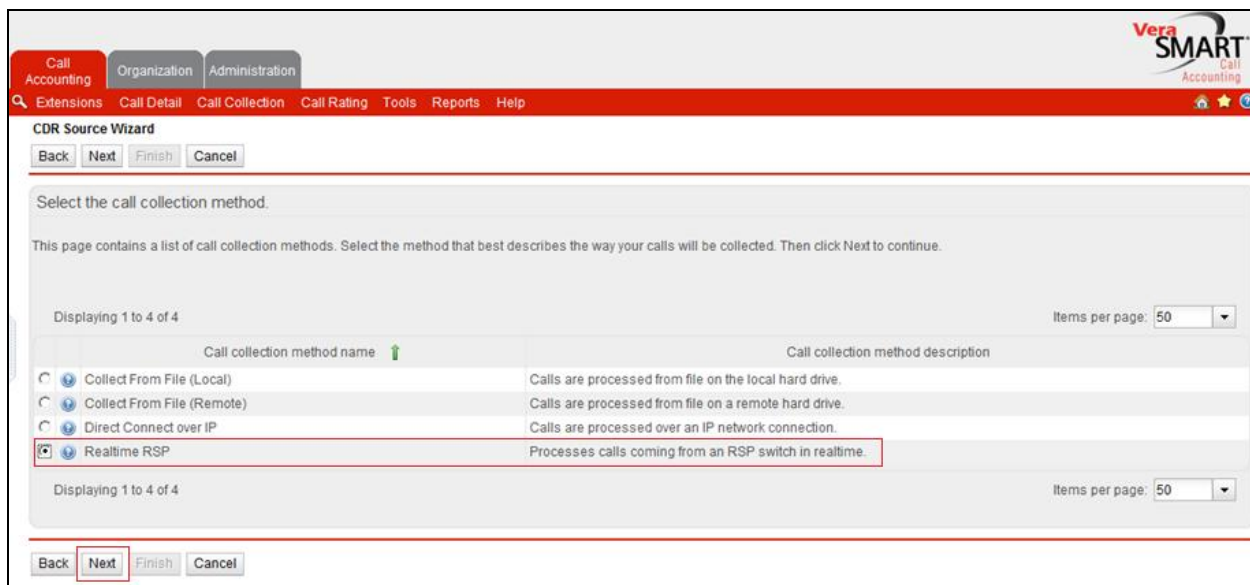
Select the call record format.

This page contains 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.

Displaying 1 to 23 of 23 Items per page: 50

Format name	Format description	CDR Source software release	Format number	Format revision number
(101)MERLIN Legend	Standard ISDN	3.0	101	1.184.0
(102)System 25	Standard format		102	1.184.0
(103) Partner/ACS	4 lines/12 extensions		103	1.184.0
(105)PARTNER II	Supports 15/24-digit numbers, ring time		105	1.184.0
(106)MERLIN Legend RingTime	Reports ringtalk time	6.1.7.0	106	1.184.0
(108)MERLIN MAGIX	Standard ISDN		108	1.184.0
(110)MERLIN MAGIX RingTime	Reports ringtalk time		110	1.184.0
(120)System 75	Teleseer Format	R1V2,V3,V4	120	1.184.0
Legacy DEFINITY systems	For serial CDR output only, ring time not reported	G3FD112	146	7.186.34
Legacy DEFINITY systems	For serial CDR output only	G3FD112	149	1.184.1
CM Aura/DEFINITY systems	For Expanded Meet-me Conferencing; supports standard RSP protocol and legacy CDR output to serial port or local file	G3FD112	154	5.186.34
CM Aura/DEFINITY systems	For customized CDR format; supports standard RSP and legacy CDR output to serial port	G3FD112	158	6.186.34
CM Aura/DEFINITY systems	For standard RSP and legacy CDR output to local file	1.1	175	7.186.34

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



CDR Source Wizard

Back Next Finish Cancel

Select the call collection method.

This page contains a list of call collection methods. Select the method that best describes the way your calls will be collected. Then click Next to continue.

Displaying 1 to 4 of 4 Items per page: 50

Call collection method name	Call collection method description
Collect From File (Local)	Calls are processed from file on the local hard drive.
Collect From File (Remote)	Calls are processed from file on a remote hard drive.
Direct Connect over IP	Calls are processed over an IP network connection.
Realtime RSP	Processes calls coming from an RSP switch in realtime.

Displaying 1 to 4 of 4 Items per page: 50

Back Next Finish Cancel

Provide the following information:

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

Click on the **Next** link.

The screenshot shows the VeraSMART Call Accounting web interface. At the top, there is a navigation bar with tabs for 'Call Accounting' (selected), 'Organization', and 'Administration'. Below this is a red menu bar with links: 'Extensions', 'Call Detail', 'Call Collection' (selected), 'Call Rating', 'Tools', 'Reports', and 'Help'. The main content area is titled 'CDR Source Wizard' and contains a form. The form has a 'Call collection method' dropdown set to 'Realtime RSP'. Below this is a text input field labeled 'Switch IP address*' with the value '10.64.41.21'. A link for 'Realtime RSP Help' is visible. At the bottom of the form, there are four buttons: 'Back', 'Next' (highlighted with a red box), 'Finish', and 'Cancel'.

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/>

©2013 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.