



Avaya Solution & Interoperability Test Lab

Application Notes for Veramark VeraSMART with Avaya Aura® Communication Manager - Issue 1.1

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 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 call accounting software can interoperate with Avaya Aura® Communication Manager 6.0. Veramark VeraSMART connects to Communication Manager over the local or wide area network using a CDR link running on RSP. Communication Manager is configured to send CDR records to Veramark VeraSMART using a specific TCP/IP port.

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

The serviceability test was conducted to assess the reliability of the solution.

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. CDR link configuration on Communication Manager.
- Session Manager – SIP trunk configuration between Communication Manager and Session Manager
- VeraSMART – CDR link configuration on VeraSMART.

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 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 was restarted.

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 and Communication Manager.

2.2. *Test Results*

All executed test cases passed, except noted below. Veramark VeraSMART 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 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:

- An incorrect CDR condition code with SIP endpoints was being generated. This was escalated to the Avaya development team. A patch was created which corrected the problem.
- A trunk to trunk transfer test case with blind transfer did not provide CDR records. This is under investigation by the Avaya development team.

2.3. Support

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

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 on one side, and Avaya S8720 Server 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.

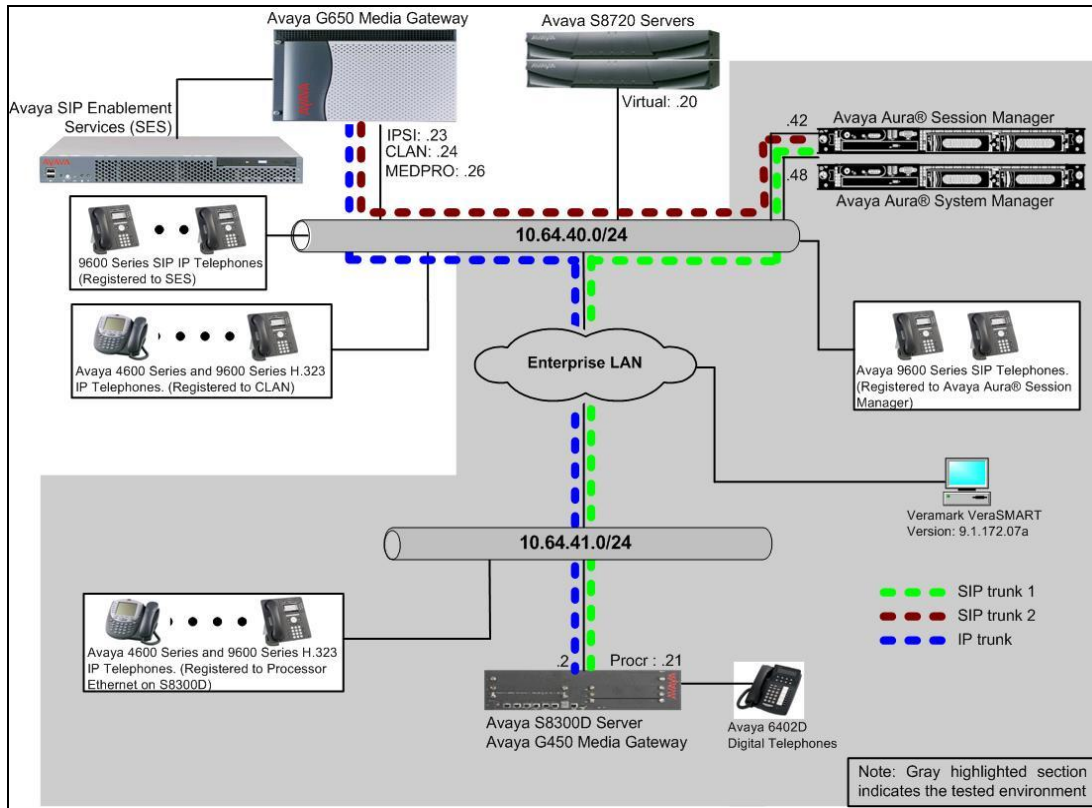


Figure 1: Test configuration of the VeraSMART with Avaya Aura® Session Manager

4. Equipment and Software Validated

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

Equipment		Software
Avaya S8300D Media Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0) with Patch 00.0.345.0-18824
Avaya S8720 Servers with Avaya G650 Media Gateway		Avaya Aura® Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya Aura® System Manager		6.0.6.0
Avaya Aura® Session Manager		6.0.0.0.600020
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	2.6.4
	9630	2.6.4
	9650	2.6.4
Avaya 9600 Series H.323 IP Telephone		
	9620	3.1
	9630	3.1
	9650	3.1
Veramark VeraSMART on Windows 2003 Server with Service Pack 2		9.1.172.07a

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 unless otherwise noted. Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the PC running Veramark VeraSMART. 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, **veramark**. This node name is associated with the IP Address of the PC running the Veramark VeraSMART 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	
veramark	10.64.43.111	
default	0.0.0.0	
procr	10.64.41.21	
procr6	::	
rdtt	10.64.43.10	
SM-1	10.64.40.42	

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

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

change ip-services

Page1 of 4

IP SERVICES

Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		
CDR1		procr	0	veramark	9000

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	

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: expanded**
- **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.]

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: customized	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? y	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: 15	

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

change intra-switch-cdr				Page 1 of 3
INTRA-SWITCH CDR				
		Assigned Members:	9	of 1000 administered
Extension	Extension	Extension	Extension	
72001				
72002				
72003				
72004				
72005				
72007				

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.

display 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	
veramark	10.64.43.111	
default	0.0.0.0	
procr	10.64.41.21	
procr6	::	
rdtt	10.64.43.10	
SM-1	10.64.40.42	

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**.

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 7202 was used for the Avaya S8300D Server side SIP telephones, and utilized Automatic Alternate Routing (AAR).

```
change uniform-dialplan 7202                           Page 1 of 2
                                     UNIFORM DIAL PLAN TABLE
                                     Percent Full: 0

Matching      Len Del      Insert      Net Conv      Node
Pattern                               Digits                               Num
7202          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 7202 was used the route pattern 92.

change aar analysis 72									
AAR DIGIT ANALYSIS TABLE									
Location: all					Percent Full: 3				
Dialed		Total		Route	Call	Node	ANI		
String		Min	Max	Pattern	Type	Num	Reqd		
7202		5	5	92	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			
												Intw			
1:	92	0											n	user	
2:											n	user			
3:											n	user			
BCC VALUE		TSC	CA-TSC		ITC		BCIE		Service/Feature		PARM	No.	Numbering	LAR	
0 1 2 M 4 W			Request									Dgts	Format		
														Subaddress	
1:	y	y	y	y	y	n	n	rest						none	
2:	y	y	y	y	y	n	n	rest						none	
3:	y	y	y	y	y	n	n	rest						none	

5.9. Configure Off-PBX-Telephone Configuration-Set

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

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

change off-pbx-telephone configuration-set 2	Page 1 of 1
<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 Domains**
- **Locations**
- **SIP Entities**
- **Entity Links**
- **Time Ranges**
- **Routing Policy**
- **Dial Patterns**
- **Manage Element**
- **Applications**
- **Application Sequence**
- **User Management**

6.1. Configure SIP Domain

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

Navigate to **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.

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 13, 2010 2:44 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Domains

Domain Management

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#)

2 Items | [Refresh](#) Filter: [Enable](#)

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

Select: [All](#), [None](#)

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. **S8300-Subnet- 10.64.41**).
- 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 SIP Domain page used during the compliance test.

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at February 24, 2011 1:18 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Routing / Locations

Location

[Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) [Commit](#)

8 Items [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	Name	Notes
<input type="checkbox"/>	S8300-Subnet- 10.64.41	10.64.41.0 Net
<input type="checkbox"/>	S8720-Subnet-10.64.40	10.64.40.0 Net

Select : All, None

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.

	Name	Entity Links	FQDN or IP Address	Type	Notes
<input type="checkbox"/>	S8300D-D4H26	▶	10.64.41.21	CM	
<input type="checkbox"/>	S8720-D4H26	▶	10.64.40.24	CM	
<input type="checkbox"/>	SM-D4H26	▶	10.64.40.42	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. **SM-D4H26**).
- 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.

	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	SM-D4H26_S8300-D4H26	SM-D4H26	TLS	5061	S8300D-D4H26	5061	<input checked="" type="checkbox"/>
<input type="checkbox"/>	SM-D4H26_S8720-D4H26	SM-D4H26	TLS	5061	S8720-D4H26	5061	<input checked="" type="checkbox"/>

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 6.0 interface. The top header shows the Avaya logo and the title 'Avaya Aura™ System Manager 6.0'. A welcome message for 'admin' is visible. The left sidebar contains a navigation menu with options like Elements, Events, Groups & Roles, Licenses, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges (highlighted), and Routing Policies. The main content area is titled 'Time Ranges' and features a table with the following columns: Name, Mo, Tu, We, Th, Fr, Sa, Su, Start Time, End Time, and Notes. A single row is shown with the name '24/7', all days of the week checked, and start/end times of 00:00 and 23:59 respectively. The page includes 'Commit' and 'Cancel' buttons at the top right and bottom right. A red box highlights the '24/7' name and the day selection checkboxes.

Name	Mo	Tu	We	Th	Fr	Sa	Su	Start Time	End Time	Notes
* 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:

- Calls to/from Communication Manager.

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

General section

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

SIP Entity as Destination section

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

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.

Home / Routing / Routing Policies / Routing Policy Details

Routing Policy Details [Commit](#) [Cancel](#)

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

[Select](#)

Name	FQDN or IP Address	Type	Notes
S8300D-D4H26	10.64.41.21	CM	

Time of Day

[Add](#) [Remove](#) [View Gaps/Overlaps](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Ranking ¹	Name ²	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	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	

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.

- 7202x – SIP endpoints in Avaya S8300D Server
- 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.

Dial Pattern Details [Commit] [Cancel]

General

* Pattern: 7200

* Min: 5

* Max: 5

Emergency Call: ☐

SIP Domain: avaya.com

Notes: H323 station on S8300D

Originating Locations and Routing Policies

[Add] [Remove]

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name ¹	Originating Location Notes	Routing Policy Name	Rank ²	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	to S8300	0	<input type="checkbox"/>	S8300-Chung	

6.8. Configure Managed Elements

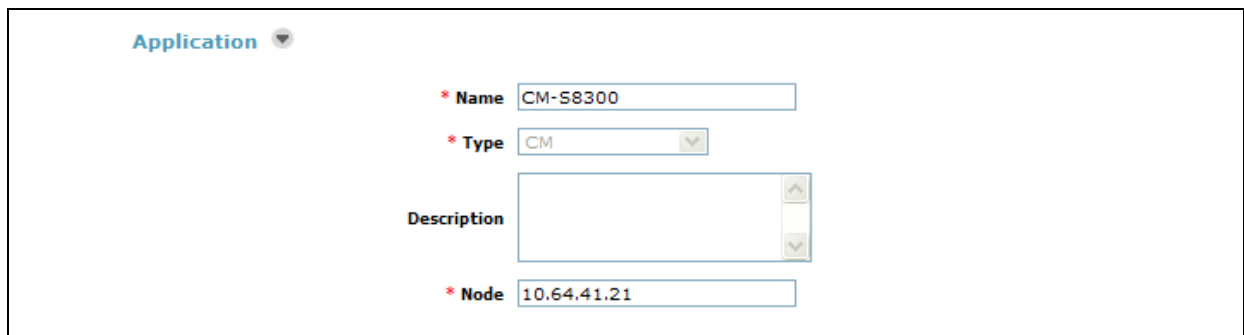
To define a new Managed Element, navigate to **Elements → Inventory → Manage Elements**. Click on the **New** button (not shown) to open the **New Entities Instance** page.

In the **New Entities Instance** Page

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

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

- Application 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.



The screenshot shows the 'Application' section of a web form. It contains four fields: 'Name' with the value 'CM-58300', 'Type' with a dropdown menu showing 'CM', 'Description' which is an empty text area, and 'Node' with the value '10.64.41.21'. Each field is preceded by a red asterisk indicating it is required.

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

System Manager uses the information entered in this section to log into Communication Manager 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.

Attributes ▼

* **Login**

Password

Confirm Password

Is SSH Connection ☒

* **Port**

Alternate IP Address

RSA SSH Fingerprint (Primary IP)

RSA SSH Fingerprint (Alternate IP)

Is ASG Enabled ☐

ASG Key

Confirm ASG Key

Location

* **Required**

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

AVAYA Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 13, 2010 2:44 PM
[Help](#) [About](#) [Change Password](#) [Log off](#)

Home / Elements / Application Management / Applications

Elements

- Conferencing
- Presence
- Application Management
- Endpoints
- SIP AS 8.1
- Feature Management
- Inventory**
 - Manage Elements**
 - Elements

Manage Elements

Entities

1 Item | Refresh | Show **ALL** ▼ Filter: Enable

<input type="checkbox"/>	Name	Node	Type	Version	Description
<input type="checkbox"/>	CM-S8300	10.64.41.21	CM		

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 Editor 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.

The screenshot shows the 'Application Editor' form. On the left is a sidebar with a tree view under 'Elements', including 'Conferencing', 'Presence', 'Application Management', 'Endpoints', 'SIP AS 8.1', 'Feature Management', 'Inventory', 'Templates', 'Session Manager' (highlighted), 'Dashboard', and 'Session Manager'. The main area is titled 'Application Editor' and contains the following fields: 'Name' (text box with 'CM-APP'), '*SIP Entity' (dropdown menu with 'S8300D-D4H26'), '*CM System for SIP Entity' (dropdown menu with 'CM-S8300' and a 'Refresh' button), and 'Description' (text box). There are 'Commit' and 'Cancel' buttons in the top right corner. A link 'View/Add CM Systems' is also present.

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

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

The screenshot shows the 'Applications' page. On the left is the same sidebar as in the previous screenshot. The main area is titled 'Applications' and contains the text 'This page allows you to add, edit, or remove applications for available SIP Entities.' Below this is a section 'Application Entries' with 'New', 'Edit', and 'Delete' buttons. A table shows 3 items with columns 'Application Name', 'SIP Entity', and 'Description'. The first item is 'CM-APP' with SIP Entity 'S8300D-D4H26'. There are 'Refresh' and 'Filter: Enable' buttons. At the bottom, it says 'Select : All, None'.

	Application Name	SIP Entity	Description
<input type="checkbox"/>	CM-APP	S8300D-D4H26	

6.10. Define Application Sequence


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

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

Sequence Name

***Name**

Description

- 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.

Applications in this Sequence

1 Item

<input type="checkbox"/>	Sequence Order (first to last)	Name	SIP Entity	Mandatory	Description
<input type="checkbox"/>		CM-APP	S8300D-D4H26	<input checked="" type="checkbox"/>	

Select : All, None

Available Applications

3 Items [Refresh](#) Filter: E

	Name	SIP Entity	Description
	CM-APP	S8300D-D4H26	

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

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

▼ Elements

► Conferencing

► Presence

► Application Management

► Endpoints

SIP AS 8.1

► Feature Management

► Inventory

► Templates

▼ Session Manager

Application Sequences

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

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

4 Items [Refresh](#) Filter: [Enable](#)

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

Select : All, None

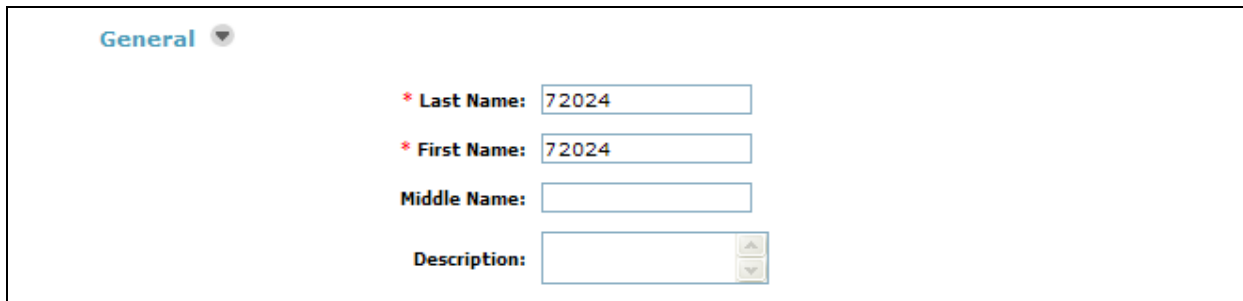
Repeat steps if multiple applications are needed as part of the Application Sequence.

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 users, 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 → Manage Users**. Click **New (not shown)** and provide the following information:

- General section
 - **Last Name** – Enter last name of user.
 - **First Name** – Enter first name of user.



The screenshot shows the 'General' section of a user configuration form. It includes the following fields:

- * Last Name:** 72024
- * First Name:** 72024
- Middle Name:** (empty)
- Description:** (empty)

- Identity section
 - **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.
 - **Shared Communication Profile Password** – Enter a numeric value used to logon to SIP telephone.
 - **Confirm Password** – Repeat numeric password



The screenshot shows the 'Identity' section of a user configuration form. It includes the following fields:

- * Login Name:** 72024@avaya.com
- * Authentication Type:** Basic
- SMGR Login Password:**
 - * Password:** (masked with dots)
 - * Confirm Password:** (masked with dots)
- Shared Communication Profile Password:**
 - Confirm Password:** (masked with dots)

- Communication Profile section

Verify there is a default entry identified as the **Primary** profile for the new SIP user. If an entry does not exist, select **New** and enter values for the following required attributes:

- **Name** – Enter **Primary**.
- **Default** – Enter ☒

Communication Profile

New Delete Done Cancel

Name
Primary

Select: None

* Name: Primary

Default: ☒

- 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.

Communication Address

New Edit Delete

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 72024 @ avaya.com

Add Cancel

- 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 SM-D4H26

Primary	Secondary	Maximum
22	0	22

Secondary Session Manager (None)

Primary	Secondary	Maximum

Origination Application Sequence CM-AppSeq

Termination Application Sequence CM-AppSeq

Survivability Server (None)

* Home Location Denver

- 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** – Check the box to automatically delete station when Endpoint Profile is un-assigned from user.

☐ Endpoint Profile

* System CM-S8300

Use Existing Endpoints ☒

* Extension 72024 [Endpoint Editor](#)

Template DEFAULT_9630SIP_CM_6_0

Set Type 9630SIP

Security Code

* Port IP

Voice Mail Number 72024

Delete Endpoint on Unassign of Endpoint from User ☒

Click **Commit** to save definition of new user. The following screen shows the created users during the compliance test.

AVAYA

Avaya Aura™ System Manager 6.0

Welcome, **admin** Last Logged on at August 13, 2010 2:44 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)

Home / Users / Manage Users

▸ Elements

▸ Events

▸ Groups & Roles

Licenses

▸ Routing

▸ Security

▸ System Manager

Data

▼ Users

Manage Users

Public Contact

Lists

Shared Addresses

System Presence

ACLs

Help

User Management

Users

View

Edit

New

Duplicate

Delete

More Actions ▾

Advanced Search ▶

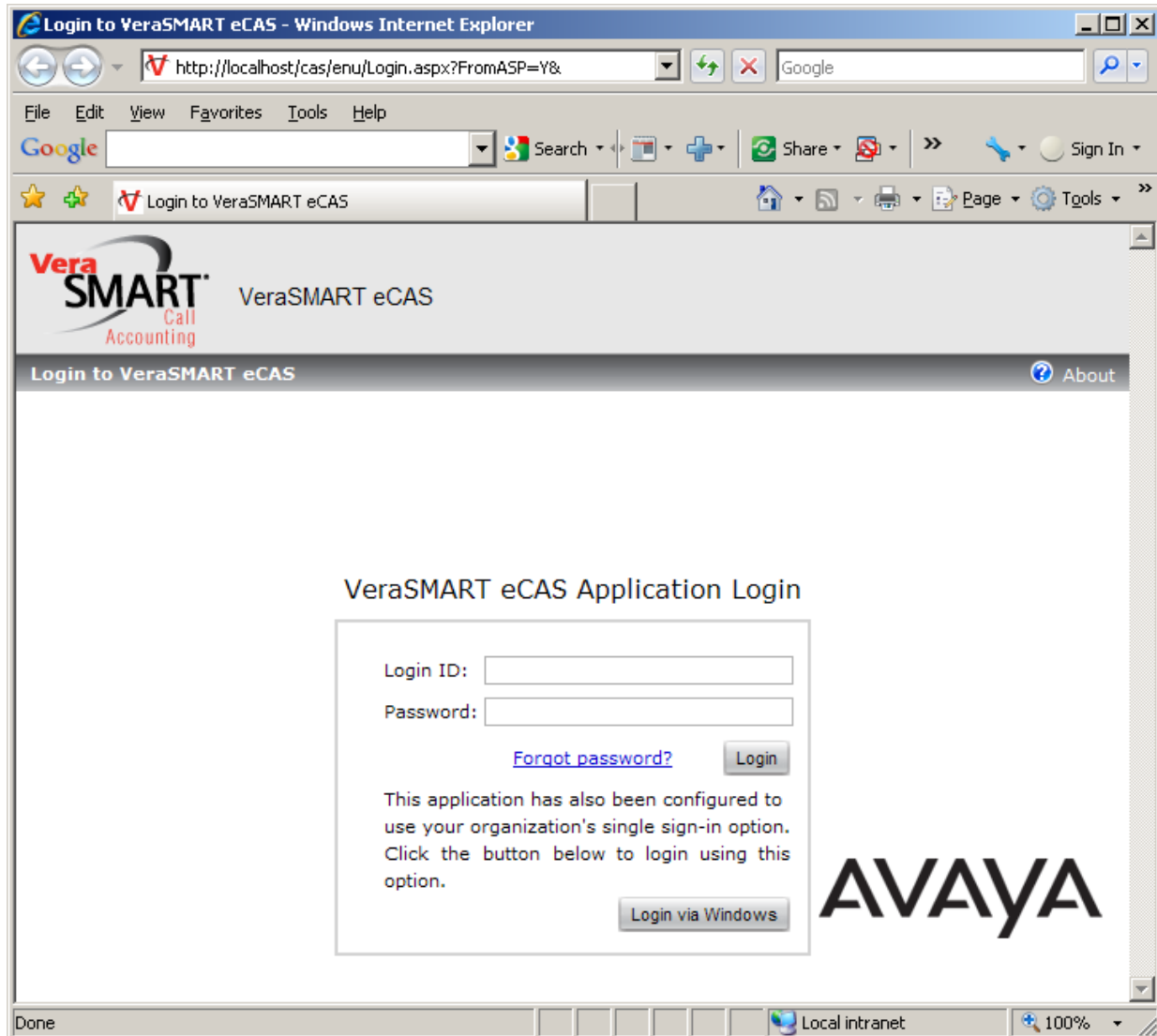
8 Items [Refresh](#) Show **ALL** ▾ Filter: [Enable](#)

<input type="checkbox"/>	Status	Name	Login Name	E164 Handle	Last Login
<input type="checkbox"/>		72024, 72024	72024@avaya.com	72024	
<input type="checkbox"/>		72025, 72025	72025@avaya.com	72025	
<input type="checkbox"/>		72026, 72026	72026@avaya.com	72026	
<input type="checkbox"/>		72027, 72027	72027@avaya.com	72027	
<input type="checkbox"/>		72028, 72028	72028@avaya.com	72028	
<input type="checkbox"/>		72029, 72029	72029@avaya.com	72029	
<input type="checkbox"/>		Default Administrator	admin		August 13, 2010 2:46:57 PM -06:00
<input type="checkbox"/>		System User	system		

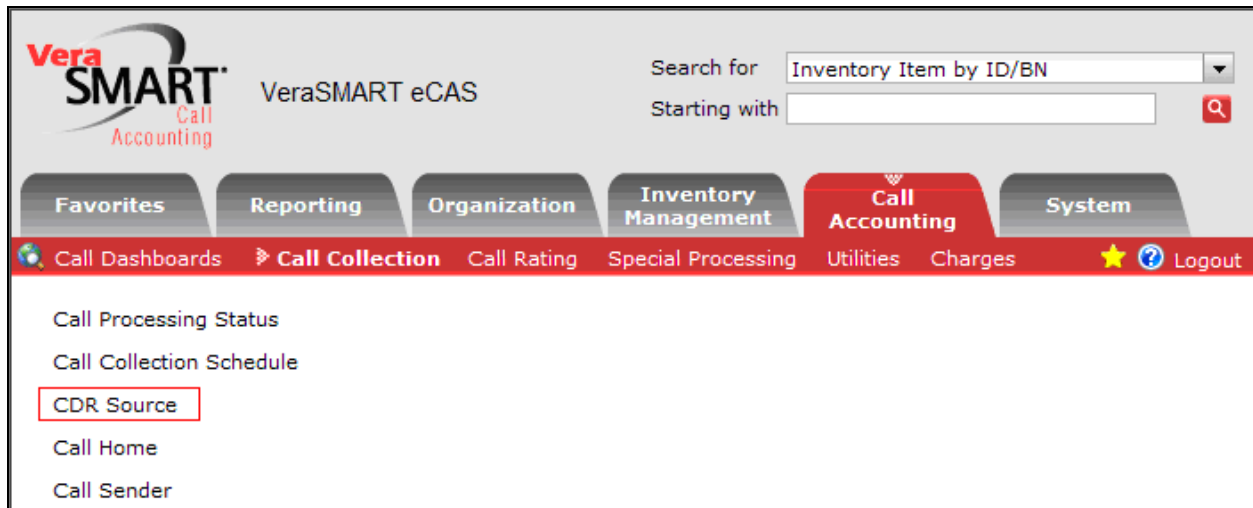
7. Configure Veramark VeraSMART

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

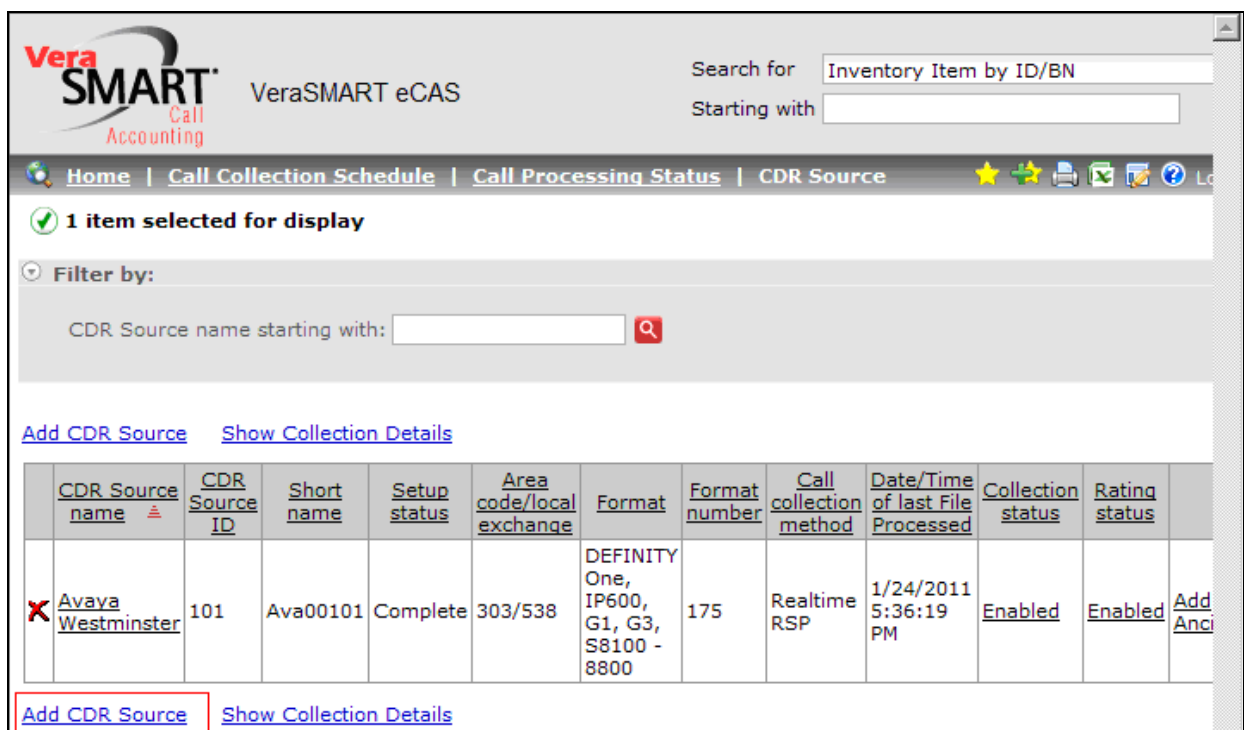
To configure Veramark VeraSMART, launch a web browser, enter <http://<IP address of Veramark VeraSMART server>> as URL, and log in with the appropriate credentials.



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, provide needed information and click **next** until the **Select the call record format** page is displayed.

CDR Source Wizard ?

[Next](#) [Cancel](#) [Reset Wizard](#)

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 click Next to continue.

[Next](#) [Cancel](#) [Reset Wizard](#)

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

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
<input type="radio"/>	(101)MERLIN Legend	Standard ISDN	3.0	101	3.3
<input type="radio"/>	(102)System 25	Standard format		102	1.1
<input type="radio"/>	(103) Partner/ACS	4 lines/12 extensions		103	2.2
<input type="radio"/>	(105)PARTNER II	Supports 15/24-digit numbers, ring time		105	1.2
<input type="radio"/>	(106)MERLIN Legend RingTime	Reports ring/talk time	6.1,7.0	106	1.6
<input type="radio"/>	(108)MERLIN MAGIX	Standard ISDN		108	1.1
<input type="radio"/>	(110)MERLIN MAGIX RingTime	Reports ring/talk time		110	1.1
<input type="radio"/>	(120)System 75	Teleseer Format	R1V2,V3,V4	120	1.5
<input type="radio"/>	DEFINITY G1, G3, S8300-8800	Unformatted format, no Reliable Session protocol	G3FD112	146	5.1.150.01
<input type="radio"/>	(149)DEFINITY G1, G3, S8300-8800	Unformatted format, ring time reported, no Reliable Session protocol	G3FD112	149	4.1
<input type="radio"/>	(154) DEFINITY G1, G3, S8300-8800	Unformatted standard 24-word, Supports Expanded Meet-me Conferencing as internal destination, supports Reliable Session protocol	G3FD112	154	1.5.161.39
<input type="radio"/>	DEFINITY G1, G3, S8300-8800	Avaya Customized CDR Format, supports Reliable Session Protocol	G3FD112	158	1.0.171.02
<input checked="" type="radio"/>	DEFINITY One, IP600, G1, G3, S8100 - 8800	Unformatted format, uses switch date record, supports Reliable Session protocol	1.1	175	4.9.150.01
<input type="radio"/>	DEFINITY One, IP600, G1, G3, S8100 - 8800	Unformatted format, supports Survivable CDR for Media Gateway	1.0	176	1.2.150.01
<input type="radio"/>	Avaya Aura Session Manager	SIP data collection from Avaya Aura Session Manager. Does not provide complete call accounting data.	1.0	197	1.1.171.01
<input type="radio"/>	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

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

Select the call collection method.

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

	<u>Call collection method name</u> ▲	<u>Call collection method description</u>
<input type="radio"/> ?	Collect From File (Local)	Calls are processed from file on the local hard drive.
<input type="radio"/> ?	Collect From File (Remote)	Calls are processed from file on a remote hard drive.
<input type="radio"/> ?	Direct Connect over IP	Calls are processed over an IP network connection.
<input checked="" type="radio"/> ?	Realtime RSP	Processes calls coming from an RSP switch in realtime.

[Back](#) [Next](#) [Cancel](#) [Reset Wizard](#)

Provide the following information:

- Survivable processor IP address – Enter the IP address of Communication Manager's **Procr** IP address.

Click on the **Next** link.

VeraSMART
Call Accounting

VeraSMART eCAS

CDR Source Wizard ?

[Back](#) [Next](#) [Cancel](#) [Reset Wizard](#)

Call collection method: Realtime RSP

Switch IP address*:

* denotes a **required** field

[Realtime RSP Help](#)

[Back](#) [Next](#) [Cancel](#) [Reset Wizard](#)

8. Verification Steps

The following steps may be used to verify the configuration:

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

9. Conclusion

These Application Notes describe the procedures for configuring Veramark VeraSMART 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.

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

[1] *Administering Avaya Aura™ Communication Manager*, ID 03-300509, Release 6.0, Issue 6.0, June 2010.

[2] *Avaya Aura™ Communication Manager Feature Description and Implementation*, ID 555-245-205, Release 6.0, Issue 8.0, 20 June 2010

©2011 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.