



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Micro-Tel MicroCall with Avaya Aura® Communication Manager - Issue 1.0**

### **Abstract**

These Application Notes describe the configuration steps required for the Micro-Tel MicroCall to successfully interoperate with Avaya Aura® Communication Manager.

Micro-Tel MicroCall 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. Micro-Tel MicroCall 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 Micro-Tel MicroCall call accounting software can interoperate with Avaya Aura® Communication Manager 6.2. Micro-Tel MicroCall (herein referred to as MicroCall) connects to Avaya Aura® 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 MicroCall using a specific port.

MicroCall provides traditional call collection, rating, and reporting for any size businesses. MicroCall can interface with most telephone systems - in particular, with Avaya Aura® Communication Manager - to collect and interpret the detailed records of inbound, outbound, tandem, and internal telephone calls. MicroCall 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.
- MicroCall – A CDR link configuration on MicroCall.

# 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 MicroCall 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 MicroCall 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 MicroCall and Communication Manager.

## 2.2. Test Results

All executed test cases passed. MicroCall 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 inter-switch calls over an H.323 trunk, transferred calls, and conference calls.

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

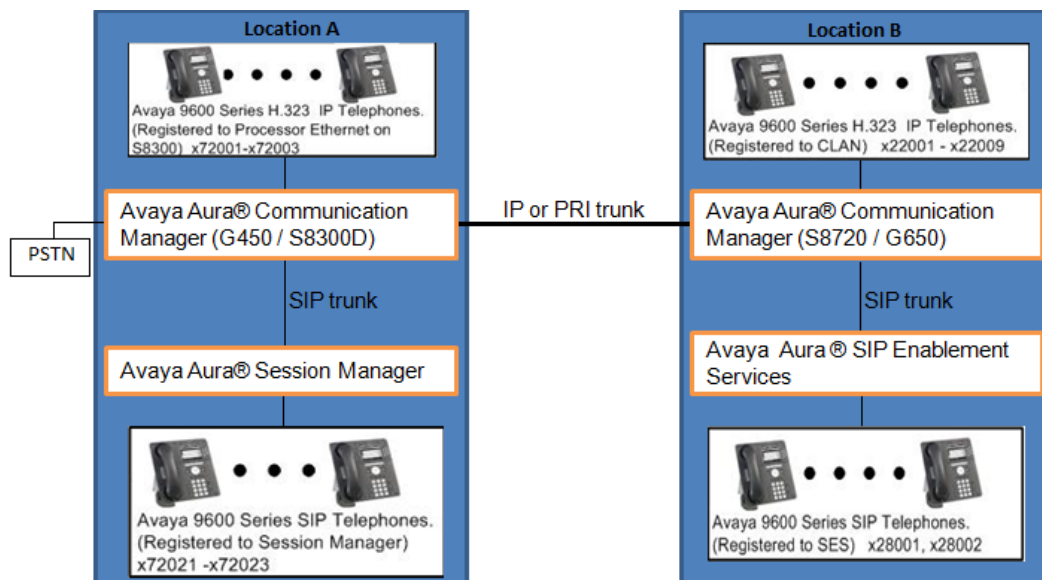
## 2.3. Support

Technical support for MicroCall can be obtained through the following:

- <http://www.microcall.com>
- (770) 447-5408

## 3. Reference Configuration

**Figure 1** illustrates a call path consisting of an Avaya S8300D Server, an Avaya G450 Media Gateway and a Session Manager on one side, and Avaya S8720 Servers with an Avaya G650 Media Gateway and Avaya Aura® SIP Enablement Services on the other side. Here, SIP Enablement Services was utilized only to register SIP endpoints in Location B.

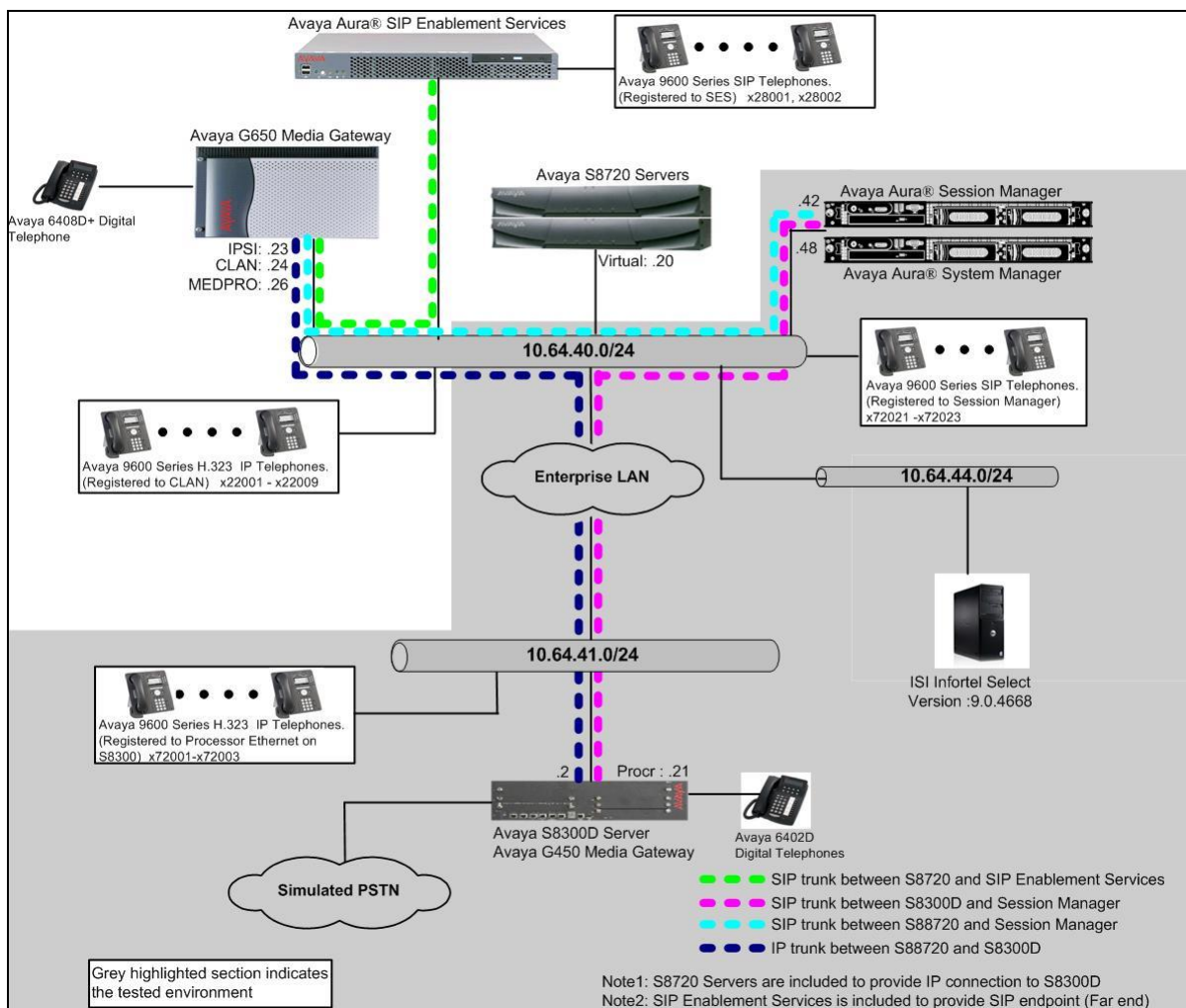


**Figure 1. Call Path Configuration between two Locations**

**Figure 2** illustrates a configuration used during the compliance test. 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 Avaya Aura® SIP Enablement Services, and are included in Figure 1 to demonstrate calls between the SIP IP telephones that are going through the IP/PRI trunk between two Avaya Communication managers. The solution described herein is also extensible to other Avaya Servers and Media Gateways.

**Note1:** SIP Enablement Services is not a part of this compliance test (only the SIP endpoints were utilized). Thus, there will not be any discussion on configuring SIP Enablement Services.

**Note2:** Avaya S8720 Servers with an Avaya G650 Media Gateway was included in the test only to provide an inter-switch scenario. Thus, there will not be any discussion on configuring Avaya S8720 Servers with an Avaya G650 Media Gateway.



**Figure 2. Test configuration of MicroCall 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 6.3 (R016x.03.0.124.0) with Patch 03.0.124.0-21291
Avaya Aura® System Manager		6.3.5.5.2017
Avaya Aura® Session Manager		6.3.5.0.635005
Avaya 9600 Series SIP IP Telephone		
	9620	2.6.3
	9630	2.6.2
Avaya 9600 and 96X1 Series H.323 IP Telephone		
	9620	3.1
	9621G	6.22
	9650	3.22
MicroCall on Windows 2003 Server		5.40

## 5. Configure Avaya Aura® 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 MicroCall. For the Avaya S8300D Media Server, the RSP link originates at the IP address of the local processor (with node-name - "procr"). For the Avaya S8720 Server, the SIP trunk terminates at the IP address of the CLAN board.

## 5.1. Configure CDR

Use the **change node-names ip** command to create a new node name, for example, **microcall**. This node name is associated with the IP Address of the PC running the MicroCall 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	
microcall	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 Servers set the Local Node to the node name of the CLAN board.]
- **Local Port:** “0” [The Local Port is fixed to 0 because Communication Manager initiates the CDR link.]
- **Remote Node:** “microcall” [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 MicroCall.]

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	microcall	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:** “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.]
- **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 1
                        CDR SYSTEM PARAMETERS

Node Number (Local PBX ID): 1                                CDR Date Format: month/day
Primary Output Format: expanded                               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.

***Note3:** 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	Extension	Assigned Members: 9	of 1000 administered
72001		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	
MicroCall	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”.
- **Direct IP-IP-Audio Connections**: Set to “y”

add signaling-group 92		Page 1 of 2
SIGNALING GROUP		
Group Number: 92	Group Type: sip	
IMS Enabled? n	Transport Method: tls	
Q-SIP? n		
IP Video? n	Priority Video? y	Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y	Peer Server: SM	
Prepend '+' to Outgoing Calling/Alerting/Diverting/Connected Public Numbers? y		
Remove '+' from Incoming Called/Calling/Alerting/Diverting/Connected Numbers? n		
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): 6	

## 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: y
Group Name: SM 41 42                                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 IP/SIP telephones, and utilized Automatic Alternate Routing (AAR).

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

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

## 5.7. Configure Automatic Alternate Routing

Enter **change aar analysis <a>**, where **a** is the AAR number. Automatic Alternate Routing (AAR) was used to route calls to the appropriate route pattern. The 5-digit extension range starting with 2 was used the route pattern 10. 2xxxx extensions are H.323 IP and SIP phones in S8720, and 28xxx extensions are SIP IP phones in S8720/SIP Enablement Services. To call these H.323 IP and SIP phones from S8300D Server, utilizes the route pattern 10 which is an ISDN/PRI or IP 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 Reqd	
20004	5	5	91	unku		n	
2	5	5	10	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 10 routes calls to the trunk group 10, which is either the IP or PRI trunk to S8720.

change route-pattern 10													Page 1 of 3	
Pattern Number: 10													Pattern Name: To8720	
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:	10	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 1**. Set the **CDR for Origination** field to “none”, and disable the **CDR for Calls to EC500 Destination?** field by setting it to “n”.

change off-pbx-telephone configuration-set 1	Page 1 of 1
CONFIGURATION SET: 1	
Configuration Set Description:	
Calling Number Style: network	
CDR for Origination: none	
CDR for Calls to EC500 Destination? n	
Fast Connect on Origination? n	
Post Connect Dialing Options: dtmf	
Cellular Voice Mail Detection: timed (seconds): 4	
Barge-in Tone? n	
Calling Number Verification? y	
Call Appearance Selection for Origination: primary-first	
Confirmed Answer? n	
Use Shared Voice Connections for Second Call Answered? n	
Use Shared Voice Connections for Second Call Initiated? n	
Provide Forced Local Ringback for EC500? n	
Apply Ringback upon Receipt of: Call-Proceeding	

## 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.

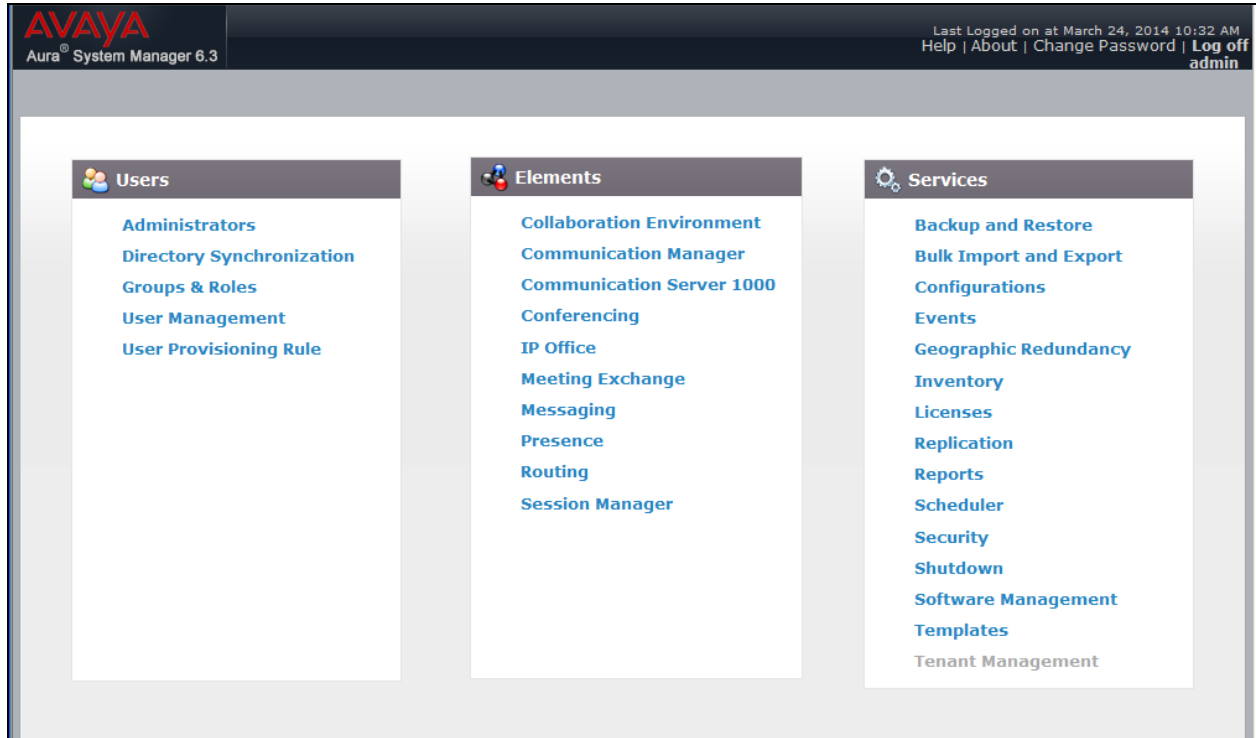
It is assumed that Session Manager and System Manager have been installed, network connectivity exists between the two platforms, and following topics are already configured:

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

This section only discusses the User Management process to add SIP users that will be used during the compliance test.

## 6.1. Configure SIP Users

Launch a web browser, enter <http://<IP address of System Manager>> in the URL, and log in with the appropriate credentials (not shown).



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 **Home → 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.

**Manage Users**

- Public Contacts
- Shared Addresses
- System Presence ACLs
- Communication Profile
- Password Policy

**New User Profile** Commit & Continue Commit Cancel Help ?

**Identity** \* **Communication Profile** **Membership** **Contacts**

**User Provisioning Rule**

User Provisioning Rule:

**Identity** \*

**\* Last Name:**

Last Name (Latin Translation):

**\* First Name:**

First Name (Latin Translation):

Middle Name:

Description:

**\* Login Name:**

**\* Authentication Type:**

Password:

Confirm Password:

Localized Display Name:

Endpoint Display Name:

- 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 displays the 'New User Profile' configuration page. On the left is a sidebar menu with options: Manage Users, Public Contacts, Shared Addresses, System Presence ACLs, Communication Profile, and Password Policy. 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. It contains two password fields (masked with dots) and buttons for New, Delete, Done, and Cancel. Below these is a list of profiles with 'Primary' selected. At the bottom, the 'Name' field is set to 'Primary' and the 'Default' checkbox is checked. Buttons for 'Commit & Continue', 'Commit', and 'Cancel' are in the top right corner.



- 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 a web interface titled "Communication Address" with a dropdown arrow. Below the title is a toolbar with three buttons: "New" (with a green plus icon), "Edit" (with a pencil icon), and "Delete" (with a red minus icon). The "New" button is highlighted with a red box. Below the toolbar is a table with three columns: "Type", "Handle", and "Domain". The table is empty, and the text "No Records found" is displayed. Below the table are two input fields. The first is a dropdown menu labeled "Type:" with "Avaya SIP" selected. The second is a text input field labeled "\* Fully Qualified Address:" containing "72021", followed by an "@" symbol and a dropdown menu containing "avaya.com". The "Add" button is highlighted with a red box.

- Session Manager Profile section
  - **Primary Session Manager** – Select one of the Session Managers from the drop down list.
  - **Origination Application Sequence** – Select Application Sequence for Communication Manager from the drop down list.
  - **Termination Application Sequence** – Select Application Sequence for Communication Manager from the drop down list.
  - **Home Location** – Select a location already defined in the **Location** form.

☒ **Session Manager Profile** ▼

**SIP Registration**

\* Primary Session Manager  ▼

Secondary Session Manager  ▼

Survivability Server  ▼

Max. Simultaneous Devices  ▼

Block New Registration When Maximum Registrations Active? ☐

Primary	Secondary	Maximum
14	0	14

**Application Sequences**

Origination Sequence  ▼

Termination Sequence  ▼

**Call Routing Settings**

\* Home Location  ▼

Conference Factory Set  ▼

- CM Endpoint Profile section
  - **System** – Select “Managed Element”, using the drop down menu.
  - **Profile Type** – Select “Endpoint”, using the drop down menu.
  - **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, using the drop down menu
  - **Security Code** – Enter numeric value used to logon to SIP telephone.
  - **Port** – Verify “IP” is shown for this field.
  - **Delete Endpoint on Unassign of Endpoint from User or on Delete User** – Check the box to automatically delete station when Endpoint Profile is unassigned from user.

☒ **CM Endpoint Profile**

\* System: Element-S8300D

\* Profile Type: Endpoint

Use Existing Endpoints: ☐

\* Extension: 72021 [Endpoint Editor]

\* Template: 9620SIP\_DEFAULT\_CM\_6\_3

Set Type: 9620SIP

Security Code: ●●●●●●

Port: IP

Voice Mail Number:

Preferred Handle: (None)

Enhanced Callr-Info display for 1-line phones: ☐

Delete Endpoint on Unassign of Endpoint from User or on Delete User: ☒

Override Endpoint Name and Localized Name: ☒

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

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

**AVAYA**  
Aura® System Manager 6.3

Last Logged on at March 24, 2014 12:31 PM  
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Home / **User Management**

Home / Users / User Management / Manage Users

**User Management**

**Users**

[View](#) [Edit](#) [New](#) [Duplicate](#) [Delete](#) [More Actions](#) [Advanced Search](#)

14 Items [Show](#) ALL [Filter: Enable](#)

	Last Name	First Name	Display Name	Login Name	SIP Handle	Last Login
<input type="checkbox"/>	72031	72031	Biamp-1	72031@avaya.com	72031	
<input type="checkbox"/>	72032	72032	Biamp-2	72032@avaya.com	72032	
<input type="checkbox"/>	72033	72033	Biamp-3	72033@avaya.com	72033	
<input type="checkbox"/>	72034	72034	Biamp-4	72034@avaya.com	72034	
<input type="checkbox"/>	72035	72035	Biamp-5	72035@avaya.com	72035	
<input type="checkbox"/>	admin	admin	Default Administrator	admin		March 24, 2014 1:01:44 PM -06:00
<input type="checkbox"/>	72041	72041	Flare-1	72041@avaya.com	72041	
<input type="checkbox"/>	72042	72042	Flare-2	72042@avaya.com	72042	
<input type="checkbox"/>	72021	72021	SIP-1	72021@avaya.com	72021	
<input type="checkbox"/>	72023	72023	SIP-3	72023@avaya.com	72023	

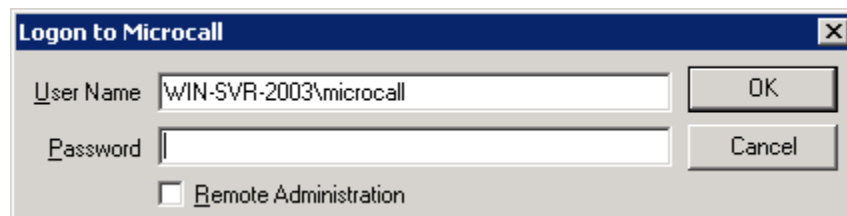
## 7. Configure MicroCall

This section describes the operation of MicroCall to receive CDR data from Communication Manager. Installation of the MicroCall software was performed by a Micro-Tel engineer prior to the actual compliance test. In this section, the following topics are discussed:

- Configure MicroCall
- View MicroCall CDR report

### 7.1. Configure MicroCall

To configure MicroCall to communicate with Communication Manager, navigate to **Start → All Programs → Microcall → Microcall**, and provide credentials to log into the Control Center page.



From the Main page, navigate to **File → Data Collection Options → Data Sources** (not shown).



From the **Data Collection Options** page, select **IP Addresses** submenu.

The screenshot shows the 'Data Collection Options' window. The 'IP Addresses' tab is selected and highlighted with a red box. The left pane shows a 'Data Source List' with 'Avaya RSP Collection' selected. Below this, fields for 'Data Source Name', 'Data Source Type' (set to 'Avaya RSP TCP/IP'), and 'Telephone Equipment Vendor' (set to 'AVAYA') are visible. The right pane contains various configuration options, including checkboxes for 'Enable Data Collection Alarms' and 'Enable Instant Alarms', numeric fields for 'Dialing Digits To Subtract', 'Minimum Call Duration', and 'Duration To Subtract', and dropdown menus for 'Area Code', 'Authorization Code Source', and 'Account Code Source'.

Enter the IP address of Communication Manager, and port that is utilizing for CDR data.

This screenshot shows the same 'Data Collection Options' window, but now the 'IP Address List' table is visible. The 'IP Address' and 'IP Port' columns are highlighted with a red box. The table contains one entry: IP Address '10. 64. 41. 21' and IP Port '9000'. The left pane remains the same as in the previous screenshot.

IP Address	IP Port
10. 64. 41. 21	9000

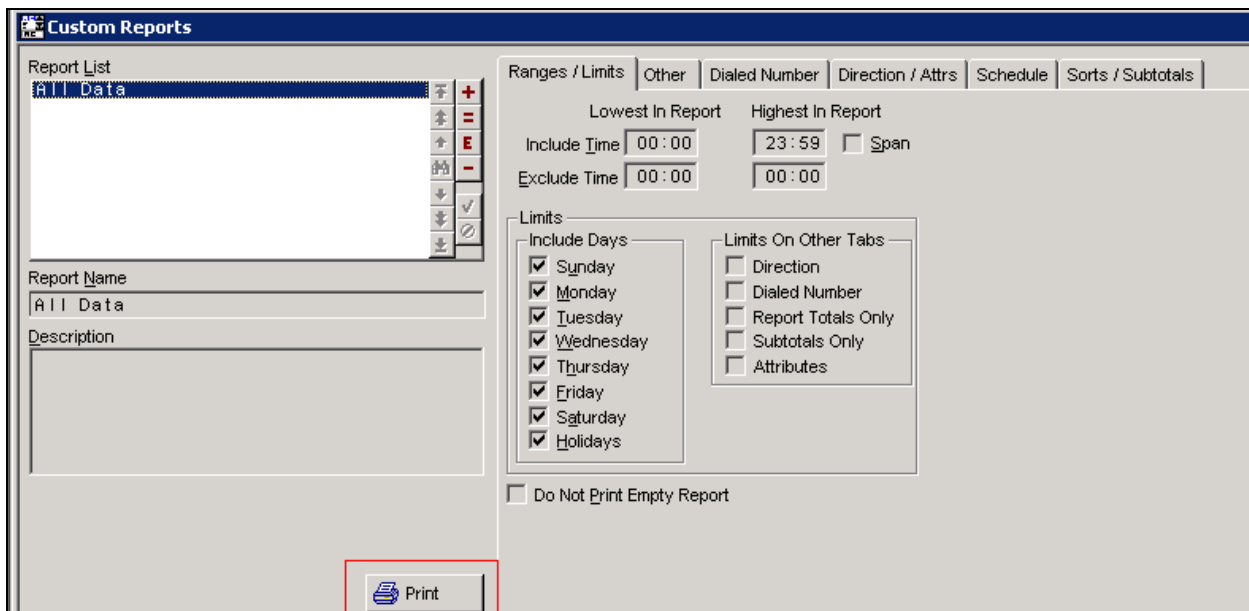
**Note4:** A Micro-Tel engineer configured setting up a **format type** and **RSP configuration** prior to the actual test. Please contact Micro-Tel for above configuration issues.

## 7.2. View MicroCall Report

To view the CDR report, launch the **Custom Report** from the Main menu.



From the Custom Reports page, select the **Print** button at the bottom.



From the Print - All Data page, select **From** and **To** dates to collect CDR data. Click the **Print** button. The following screen shows From date (03/19/14) and To date (03/19/14).

The following shows the sample report collected during the compliance test.

NOTE: This report was generated for printing in landscape orientation (Print/Preferences).									
AVAYA DEVCONNECT TESTING SYSTEM					Printed: 03/24/2014 12:00				
All Data					Report Range: 03/19/2014 – 03/19/2014				
Date/Time	Duration	Extension	Trunk	From Ext.	Dialed Number	Dir	Auth Code	Account Code	Condition Co
03/19/2014 09:59:54	0:00:06	72027	99999999		7-2001	EXT	88888		0
03/19/2014 09:59:55	0:00:06	72001	99999998	72027		EXTI	88888		0
03/19/2014 10:01:54	0:00:06	72001	99999999		7-2021	EXT			0
03/19/2014 10:01:55	0:00:06	72021	99999998	72001		EXTI			0
03/19/2014 10:10:48	0:00:12	72001	10		303-538-2324	IN			9
03/19/2014 10:10:54	0:00:06	72021	10		303-538-2324	IN			0
03/19/2014 10:19:36	0:00:24	72001	10		303-538-2324	IN			0
03/19/2014 10:20:54	0:01:06	72001	10		303-538-2324	IN			9
03/19/2014 10:21:24	0:00:36	72001	10		303-538-2324	IN			0
03/19/2014 10:22:18	0:05:42	72001	10		303-538-2324	IN			9
03/19/2014 10:26:42	0:00:18	72001	10		303-538-2324	IN			9
03/19/2014 10:27:06	0:00:54	72002	10		303-538-2324	IN			9
03/19/2014 10:29:30	0:00:30	72002	10		303-538-2324	IN			9
03/19/2014 10:38:00	0:01:00	72027	10		303-538-2324	IN			9
03/19/2014 10:41:48	0:00:12	72002	1080		1-303-538-2324	OUT			7



## 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, and verify the **Link State** is “up” and **Reason Code** is “OK”.

status cdr-link	
CDR LINK STATUS	
Primary	Secondary
Link State: up	down
Number of Retries: 999	
Date & Time: 2014/03/19 14:16:45	2014/03/19 16:17:47
Forward Seq. No: 11	0
Backward Seq. No: 0	0
CDR Buffer % Full: 0.00	0.07
Reason Code: OK	CDR connection is closed

- Make several SIP calls between two Communication Managers, and verify that call records were collected from MicroCall.

## 9. Conclusion

These Application Notes describe the procedures for configuring MicroCall to collect call detail records from Communication Manager. Testing was successful.

## 10. References

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

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 9 Release 6.3, October 2013, available at <http://support.avaya.com>.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Release 6.3, October 2013, available at <http://support.avaya.com>.

The MicroCall Solution and Product information is available from MicroCall. Visit [https://www.microcall.com/literature\\_request.html](https://www.microcall.com/literature_request.html)

---

**©2014 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](mailto:devconnect@avaya.com).