



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Resource Software International Shadow CMS with Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Resource Software International Shadow CMS to interoperate with Avaya Aura® Communication Manager.

Resource Software International Shadow CMS is a reporting solution that uses Avaya Reliable Session Protocol (RSP) to collect and process call detail recording from Avaya endpoints and produce detailed reports.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 Resource Software International Shadow CMS (hereafter referred as Shadow CMS) software can interoperate with Avaya Aura® Communication Manager. Shadow CMS connects to Communication Manager over the local or wide area network using a Call Detail Recording (hereafter referred as CDR) link Avaya Aura® Communication Manager is configured to send CDR records to Shadow CMS using a specific port.

Shadow CMS provides traditional call collection, rating, and reporting for any size businesses. Shadow CMS 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. Shadow CMS then calculates the appropriate charge for local, long distance, international & special calls and allocates them to responsible parties.

During the compliance 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.

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 Shadow CMS 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 Shadow CMS connection and its server 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the SFR TELEPHONIE SIP did not include use of any specific encryption features as requested by SFR.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included features and serviceability tests. The feature testing focused on verifying the proper parsing and displaying of CDR data by Shadow CMS for call scenarios including internal, inbound PSTN, outbound PSTN, hold, reconnect, transfer, conference, authorization code, account codes and CDR data on survivable remote server in event of main Communication Manager disconnected. The verification included raw CDR data that sent to Avaya Reliable Data Transport Tool (RTTD) application used to compare with Shadow CMS reports that were processed and generated from the received CDR data.

The serviceability testing focused on verifying the ability of Shadow CMS to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection to Shadow CMS.

2.2. Test Results

All executed test cases were verified and passed.

2.3. Support

Technical support on Shadow CMS can be obtained through the following:

- Phone: (800) 891-6014
- Email: support@telecost.com
- Web: www.telecost.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Site 1 that includes Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Local Survivable Processor and Avaya Aura® Media Server running on Virtualized Environment, Avaya G450 Media Gateway that has PRI/T1 trunk to PSTN, and Resource Software International Shadow CMS server. Avaya IP Office Server Edition running on Virtualized Environment on the Site 2, Session Manager terminates SIP trunks from both sides.

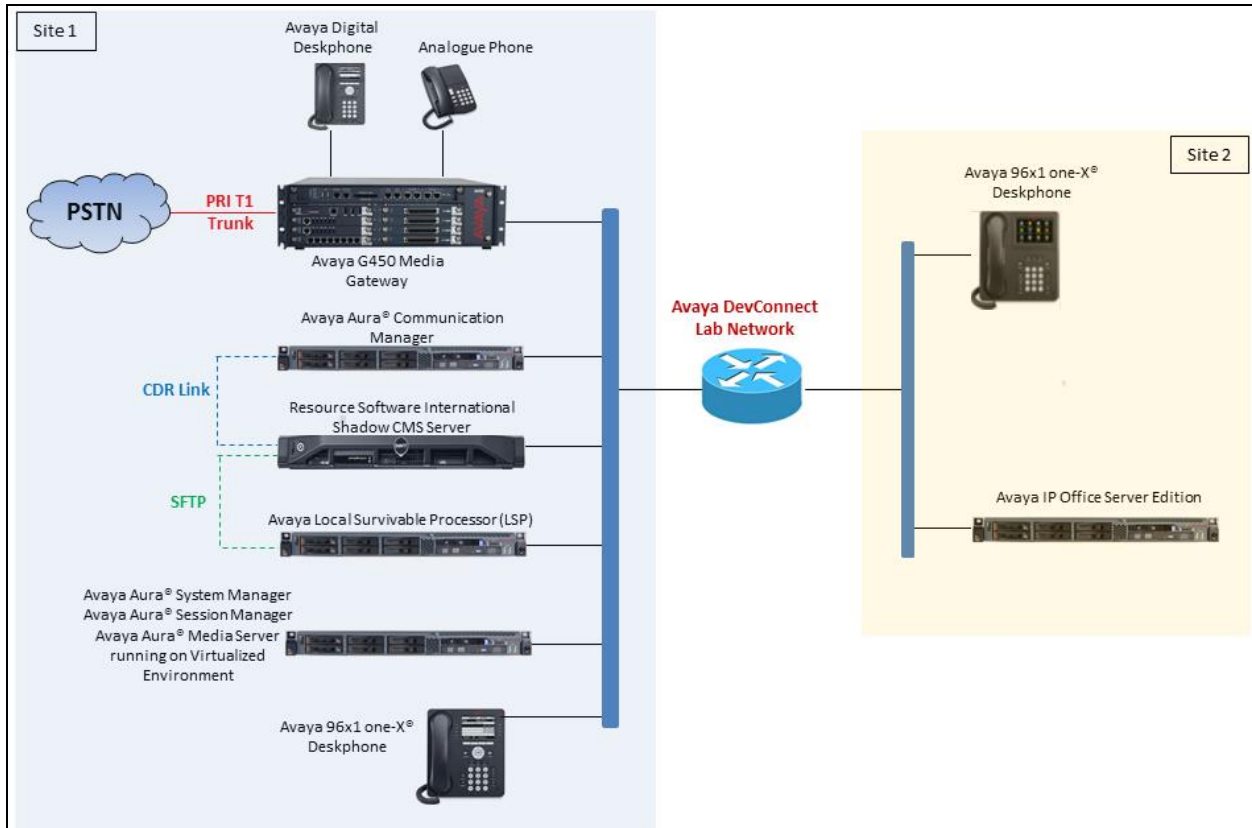


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtualized Environment	8.0 R018x.00.0.822.0 Patch 24826
Avaya Aura® System Manager running on Virtualized Environment	8.0 Build 8.0.0.0.931077
Avaya Aura® Session Manager running on Virtualized Environment	8.0 Build 8.0.0.0.800035
Avaya Aura® Media Server running on Virtualized Environment	8.0.0.150
Avaya G450 Media Gateway <ul style="list-style-type: none">• MGP	40.10.0
Avaya 96x1 IP Deskphones	H.323 6.6604 SIP 7.1.3
Avaya 1416 Digital Deskphone	FW1
Resource Software International Shadow CMS running on Windows Server 2012	5.2.0
WinLink Application	2.0.9

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). Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the server running Shadow CMS.

5.1. Configure Node-Names IP

Use the **change node-names ip** command to create a new node name, for example, **RSI-Shadow**. This node name is associated with the IP Address of the server running the Shadow CMS 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	
AMS1	10.33.1.30	
CMS18	10.33.1.20	
RDTT	10.10.98.86	
RSI-Shadow	10.10.97.233	
default	0.0.0.0	
lsp	10.33.1.17	
procr	10.33.1.6	
procr6	::	

5.2. Configure IP Services

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**
- **Local Port: 0** - The local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.
- **Remote Node: RSI-Shadow** - 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 the Shadow CMS.

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	RSI-Shadow	9000	
CDR2		procr	0	RDTT	9001	

On Page 3 of the ip-services form, disable the Reliable Session Protocol for the primary CDR link that is configured for Shadow CMS by setting the **Reliable Protocol field** to “n”

change ip-services						Page 3 of 4
Service Type	Reliable Protocol	SESSION LAYER TIMERS				Connectivity Timer
		Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr		
CDR1	n	30	3	3	60	
CDR2	y	30	3	3	60	

5.3. Configure System Parameters CDR

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.

- **Enable CDR Storage on Disk?** Set to “y”, this field must be enabled so that CDR data can be saved into a file in the local survivable processor when the main Communication Manager becomes inactive
- **Use Legacy CDR Formats?** Set to “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** set to “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?** Set to “n” - Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls
- **Inc Trk Call Splitting?** Set to “y” - Allows a separate call record for any portion of an incoming call that is transferred or conferenced
- **Call Account Code Length** Set to “5” - The length may be set to a value between 1 and 15. However, during the compliance test, “5” was used

```
change system-parameters cdr
                                CDR SYSTEM PARAMETERS

Node Number (Local PBX ID):                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? y  Outg Attd Call Record? y
Disconnect Information in Place of FRL? y     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? y
Record Agent ID on Incoming? n              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: 5
Remove '+' from SIP Numbers? y
```


5.4. Configure Intra-Switch CDR

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.

```
change intra-switch-cdr                                     Page 1 of 3
                                     INTRA-SWITCH CDR
                                     Assigned Members: 15 of 5000 administered
Extension      Extension      Extension      Extension
3301
3302
3303
3401
3402
Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add
new members and 'change intra-switch-cdr <ext>' to change/remove other members
```

5.5. Configure Off-PBX-Telephone Configuration Set

SIP endpoints and off-pbx-telephone stations will be automatically created in Communication manager when SIP endpoints were created in Session Manager. However, the off-pbx-telephone configuration-set form needs to be modified in order to call records of SIP endpoint are generated correctly. Enter **change off-pbx-telephone configuration-set 1** and set **CDR for Origination** to “none” and disable the **CDR for Calls to EC500 Destination?** 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
Location to Route Incoming Overlap Calls: station-location-if-set
```

5.6. Enable CDR in Trunk Group

Enter the command **change trunk-group <id>** which the <id> is the trunk number that needs to be modified. Set **CDR Report** field to “y” to enable call record for calls going in and out from this trunk group. Note that this field is set to “y” by default.

```
change trunk-group 1                                     Page 1 of 21
                                     TRUNK GROUP
Group Number: 1                                         Group Type: sip           CDR Reports: y
  Group Name: For-Private                               COR: 1                   TN: 1               TAC: #01
  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: 1
                                                Number of Members: 14
```

6. Configure Resource Software International Shadow CMS

This section provides the procedures for configuring Shadow CMS. The procedures include the following areas:

- Administer Winlink Configuration
- Administer CDR Driver
- Verify CDR Data

The configuration of Shadow CMS is typically performed by RSI Support Services. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Administer Winlink Configuration

Launch **Winlink** application from the list of application from Shadow CMS server. The **Winlink Configuration** window is displayed as below. The **Main Location**, **Connection 1** source, **Data File** and **Backup File** were previously configured during the testing they are displayed in the picture for showing purposes. From the **Connection 1** source displayed in the right-hand side of the window, select “Generic – Socket Listener” in **Connection Type**.


- **Connection Settings:**
 - **IP:** leave IP address at default which is 0.0.0.0 the CMS Winlink will listen and establish a connection on a specific port configured in Avaya CM
 - **Port:** enter the port “9000” as configured in **Section 5.2**
 - **Protocol:** select “TCP” from the dropdown menu.
 - **Inactivity:** enter 1000 ms. Note that the default value is 3000 ms that is not good for a special case when the CDR link connection between CMS and Communication Manager is lost and resumed the Winlink application was not able to receive the CDR record therefore the 1000 ms was configured during the compliance test.

WinLink Configuration

Add Location Add Destination Delete Source Restart Connection Add Application Monitor Service

Overview
 Main Location
 Connection 1
 Data File
 Backup File
 Shadow CMS Service

Connection 1 Main Location


 Name:
 Connection Type:

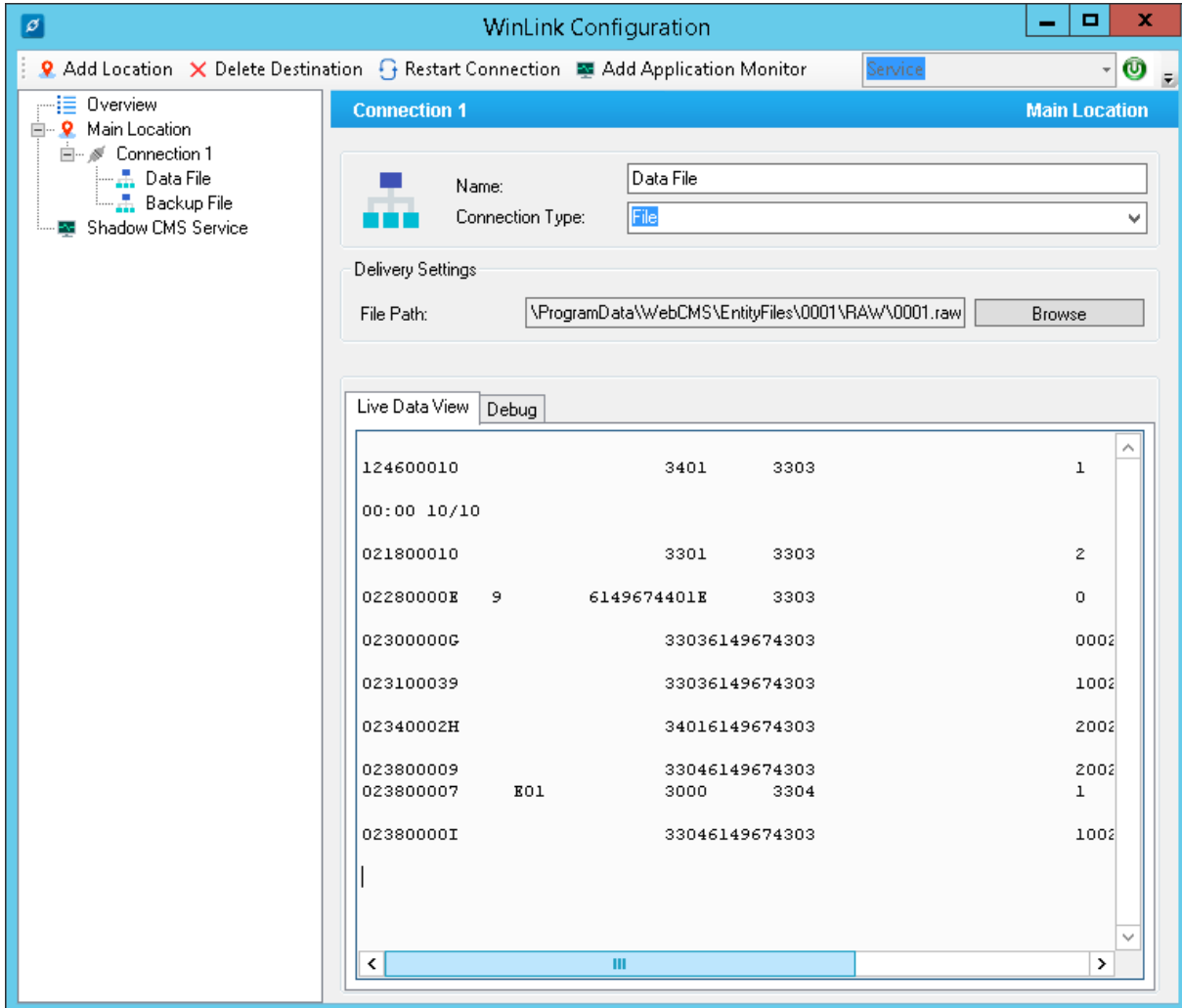
Connection Settings

IP: Port:
 Inactivity (ms): Protocol:

Live Data View Debug

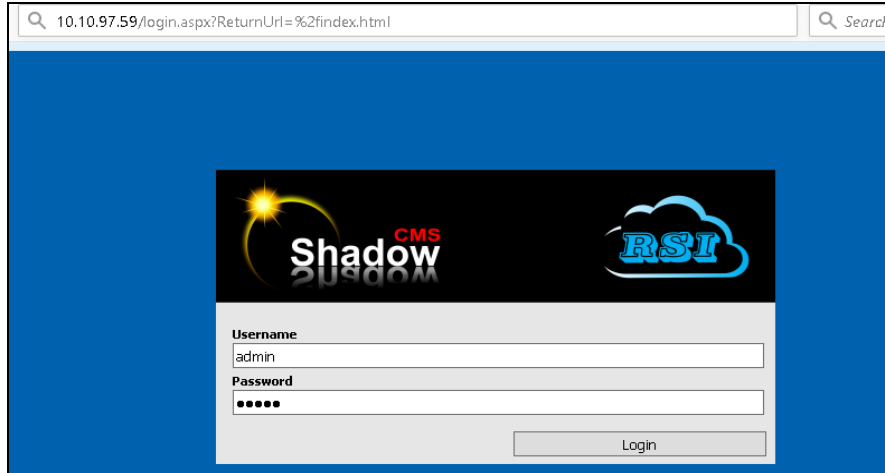
123300097	9 E04	6149674303E	3401	88888	1
134000007	E01	4800	3303		1
13430000E	9	614C145C74E	3303		0
13440000E	9	614C145C74E	3303		0
13450000E	9	423C12C123	3303		0
13490000E	9	61496743C0E	3303		0
135300007	9 E04	61496C430CE	3303		2
00:00 10/11					
213500027	E01	3000	3303		1
00:00 10/12					

Select **Data File** under **Avaya CM Source** from the left navigation pane. The Data File is displayed in the right hand of the window. Select “File” in the **Connection Type** and in the **Delivery Settings** section, creates a raw CDR file in the local server by selecting **Browse** button and specifying a full path where the raw CDR data can be saved.



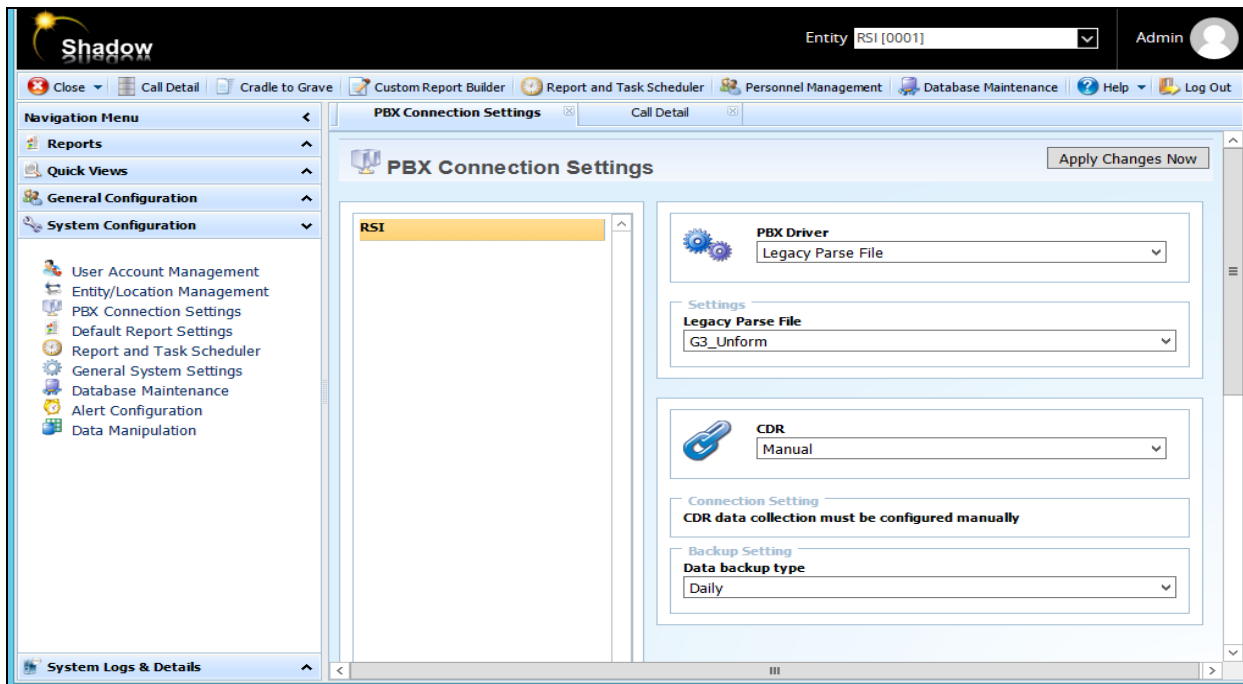
6.2. Administer CDR Driver

Log in the Shadow CMS web management by entering its IP address into an internet browser as shown in the picture below. Enter username “admin” and appropriate password to log in.



From the Navigation Menu, navigate to **System Configuration** → **PBX Connection Settings**, the PBX Connection Settings is displayed in the right-hand side of the window.

- **PBX Driver:** select “Legacy Parse File” from the dropdown menu
- **Settings – Legacy Parse File:** select “G3_Unform” from the dropdown menu
- **CDR:** select “Manual” from the dropdown menu



6.3. Verify CDR Data

The raw CDR data can be verified by selecting **Call Detail** button in the horizontal menu, Call Detail displays all CDR records that Shadow CMS processes from the processed CDR file saved by the Winlink application.

The screenshot shows the Shadow CMS interface. The top menu bar includes 'Call Detail' (highlighted with a red box), 'Cradle to Grave', 'Custom Report Builder', 'Report and Task Scheduler', 'Personnel Management', 'Database Maintenance', 'Help', and 'Log Out'. The left navigation menu has 'System Configuration' expanded, showing options like 'User Account Management', 'Entity/Location Management', 'PBX Connection Settings', 'Default Report Settings', 'Report and Task Scheduler', 'General System Settings', 'Database Maintenance', 'Alert Configuration', and 'Data Manipulation'. The main content area displays the 'Call Detail' report with a table of call records. The table has columns: DATE, TIME, TIMEEXTENDED, DURATION, CALLTYPE, EXTENSION, and TRUNK. The data is as follows:

DATE	TIME	TIMEEXTENDED	DURATION	CALLTYPE	EXTENSION	TRUNK
20171110	1708	170800	3095	TE	3401	3300
20171110	1709	170900	42	TE	60011	3300
20171111	0210	021000	35994	TE	4234684603	16479673303
20171111	0211	021100	35994	ET	3403	4301
20171111	0607	060700	35994	TE	60011	3301
20171111	0809	080900	7321	TE	60011	3301
20171111	1210	121000	35994	TE	4234684603	16479673303
20171111	1211	121100	35994	ET	3403	4301
20171111	1826	182600	22505	ET	3403	4301
20171111	1826	182600	22557	TE	4234684603	16479673303
20171113	0938	093800	14	TE	60011	4603
20171113	1119	111900	4	TE	4306	4603
20171113	1119	111900	18	TE	3303	4089674306
20171113	1135	113500	3	TE	4306	4603
20171113	1136	113600	44	TE	3303	4089674306
20171113	1356	135600	26	TE	3303	5100
20171113	1403	140300	37	TE	3303	5100
20171113	1406	140600	41	ET	3403	5100

7. 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. The status should be **UP** for the primary CDR.

```

status cdr-link
                                CDR LINK STATUS
                                Primary                Secondary
Link State: up                    up
Date & Time: 2018/10/10 12:10:56    2018/10/12 02:23:11
Forward Seq. No: 0                    62
Backward Seq. No: 0                    0
CDR Buffer % Full: 0.00                0.08
Reason Code: OK                       OK
  
```

- Make several different types of calls such as between local stations, outgoing call via SIP trunk, and incoming call via PSTN and verify that call records were collected from Shadow CMS and shown up in the report.

Page 4 of 6



Chronological Detail
All Calls
 Avaya Testing
 40 King St. W Suite 300 Oshawa Ontario

Report Date: All
Print Date: 2018-10-12

Date	Time	Dir	From	To	Location	Digits	Duration	Cost	Route	Comment
2018/10/09	09:44	Int	E3401	E4300		4300	00:00:12	0.00		
2018/10/09	09:45	Out	E3303	T1	other NPA	96149674300	00:00:12	0.00		
2018/10/09	09:45	Inc	T	E3303		4303	00:00:36	0.00		
2018/10/09	11:47	Int	E3303	E3301		3301	00:00:18	0.00		
2018/10/09	11:47	Out	E3401	T1		4300	00:00:30	0.00		
2018/10/09	11:48	Inc	T2	E3403	OHIO	6149674303	00:00:18	0.00		
2018/10/09	11:49	Out	E3303	T1		4303	00:00:12	0.00		
2018/10/09	11:49	Out	E3403	T1		4306	00:00:30	0.00		
2018/10/09	12:46	Int	E3303	E3401		3401	00:00:06	0.00		
2018/10/10	02:18	Int	E3303	E3301		3301	00:00:06	0.00		
2018/10/10	02:28	Int	E3303	E674401		674401	00:00:00	0.00		
2018/10/10	02:30	Inc	T2	E3303	OHIO	6149674303	00:00:00	0.00		
2018/10/10	02:31	Inc	T2	E3303	OHIO	6149674303	00:00:18	0.00		
2018/10/10	02:34	Inc	T2	E3401	OHIO	6149674303	00:00:12	0.00		

8. Conclusion

These Application Notes describe the procedures for configuring Resource Software International Shadow CMS with Avaya Aura® Communication Manager. Testing was successful with some observations noted in Test Result section; refer to **Section 2.2** for details.

9. Additional References

This section references the Avaya and Resource Software International documentation that are relevant to these Application Notes. Product documentation for Avaya Aura® Communication Manager, including the following, is available at: <http://support.avaya.com/>.

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 8.0, August 2018

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 9.0, Release 8.0, August 2018

The Resource Software International Shadow CMS Product information is available from RSI. Visit <http://www.telecost.com/#!/url=shadow.php>.

©2018 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.