Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Resource Software International Shadow Enterprise CMS Version 5.3.7 with Avaya Aura® Communication Manager Release 10.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the Resource Software International Shadow Enterprise 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 running on Reliable Session Protocol. 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 the 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.

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 these DevConnect Application Notes 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 these Application Notes, the interface between Avaya systems and the RSI did not include use of any specific encryption features as requested by RSI. 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 also 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: +1 (800) 891-6014
- Email: support@telecost.com
- Web: www.telecost.com

.

3. Reference Configuration

Figure 1 illustrates a sample configuration of enterprise that consists of Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Avaya G450 Media Gateway and Avaya Aura® Media Server running on Virtualized Environment. Resource Software International Shadow Enterprise CMS server receives Call Detail Recording via Reliable Session Protocol.

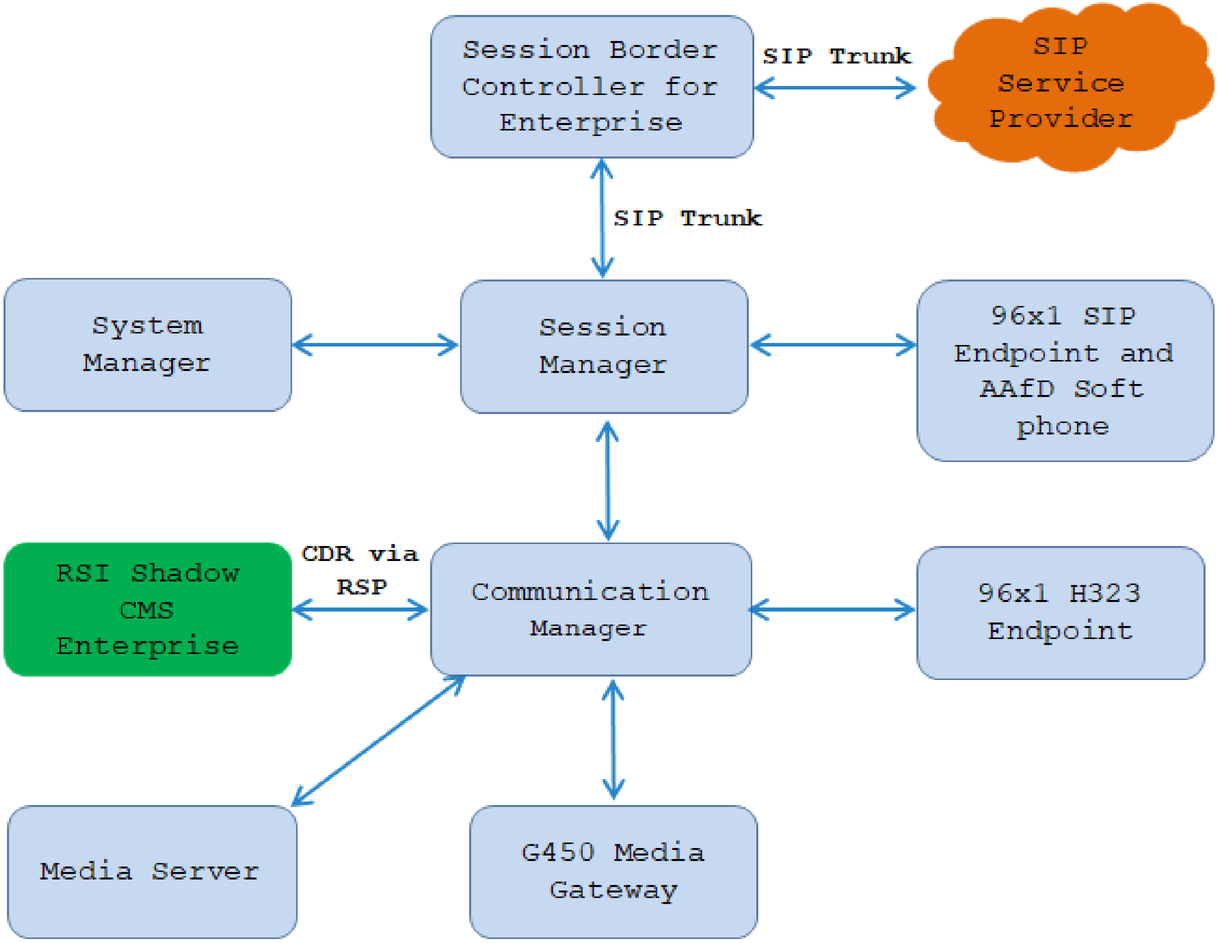


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

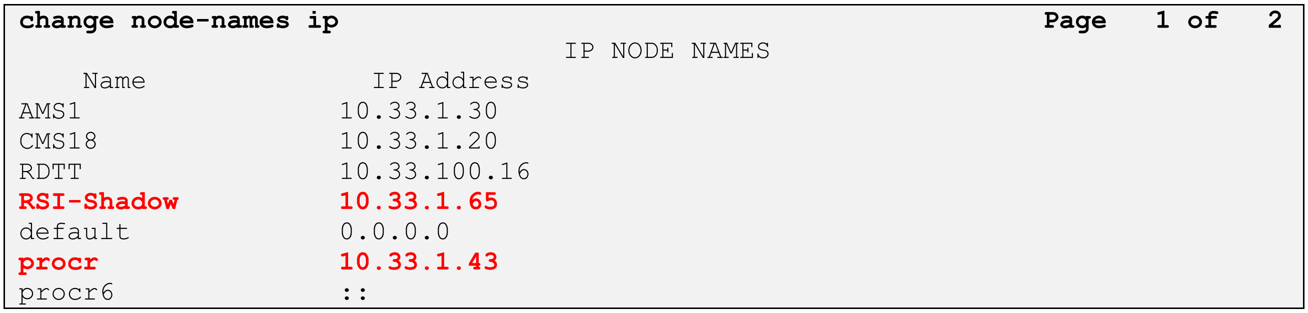
Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on virtualized environment	10.1 10.1.0.1.0.974.27372
Avaya Aura® Session Manager running on virtualized environment	10.1 10.1.0.0.1010019
Avaya Aura® System Manager running on virtualized environment	10.1 10.1.0.0.0614119
Avaya Aura® Media Server running on virtualized environment	8.0 8.0.2.163
Avaya Session Border Controller for Enterprise	8.1.3
Avaya G450 Media Gateway	42.07.0
Avaya IP Deskphones • 9608 (H.323) • 9621 (H.323) • 9641GS (SIP) • J189 (SIP)	 6.8.304 6.8.304 7.1.9.0.8 4.0.7.1.5
Avaya Digital 9408 Deskphone	2.0 Service Pack 9 (R20)
Resource Software International Shadow Enterprise CMS running on Windows 2012 VM	5.3.7

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.

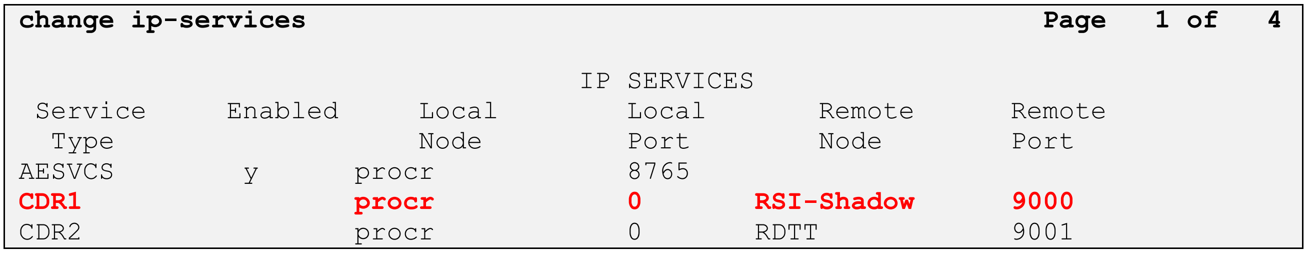


```
change node-names ip                                            Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
AMS1                    10.33.1.30
CMS18                   10.33.1.20
RDTT                    10.33.100.16
RSI-Shadow              10.33.1.65
default                 0.0.0.0
procr                   10.33.1.43
procr6                  ::
```

5.2. Configure IP Services

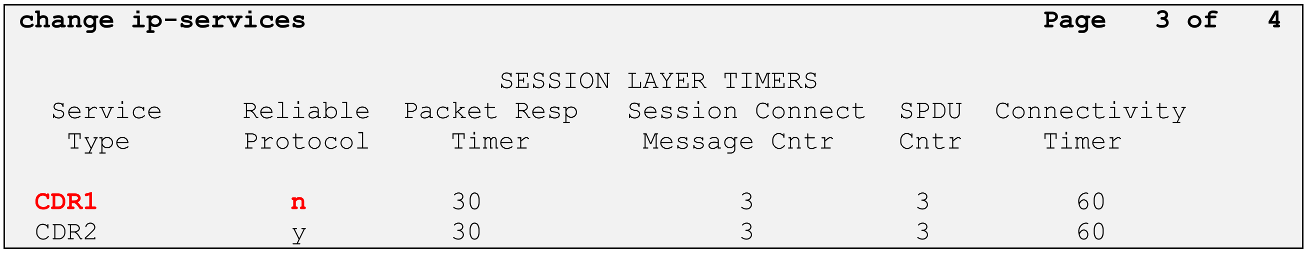
Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, provide the following information:

- **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 theVeraSMART eCAS



```
change ip-services                                              Page   1 of   4

                                   IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         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

                              SESSION LAYER TIMERS
  Service      Reliable   Packet Resp   Session Connect   SPDU   Connectivity
   Type        Protocol      Timer       Message Cntr     Cntr      Timer

 CDR1             n          30                3            3         60
 CDR2             y          30                3            3         60
```

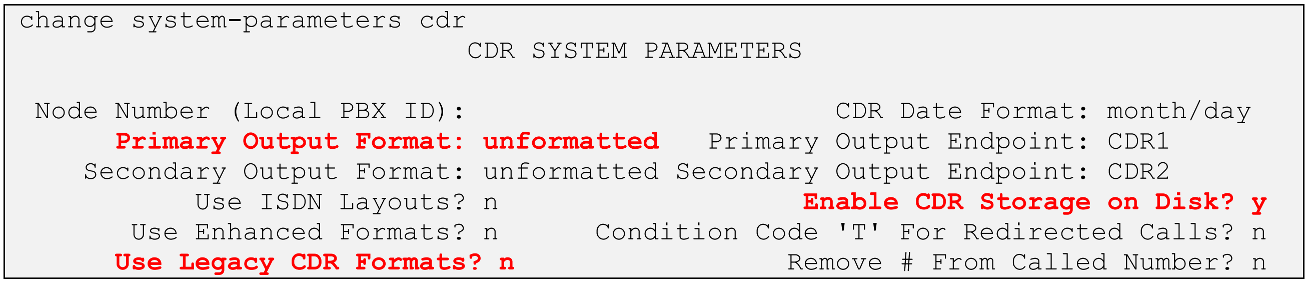
5.3. Configure System Parameters CDR

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:

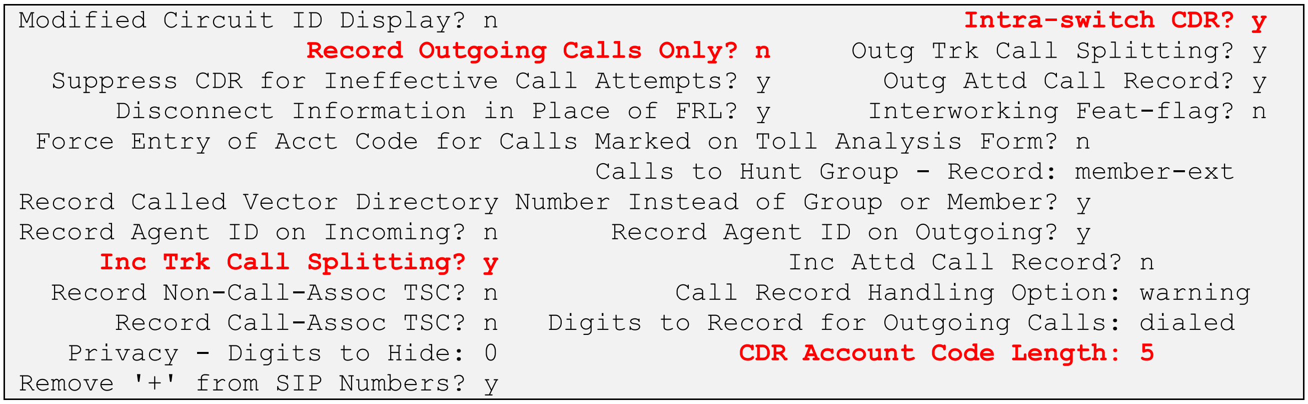
- **CDR Date Format**: “month/day”
- **Primary Output Format**: “unformatted”
- **Primary Output Endpoint**: “CDR1”

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



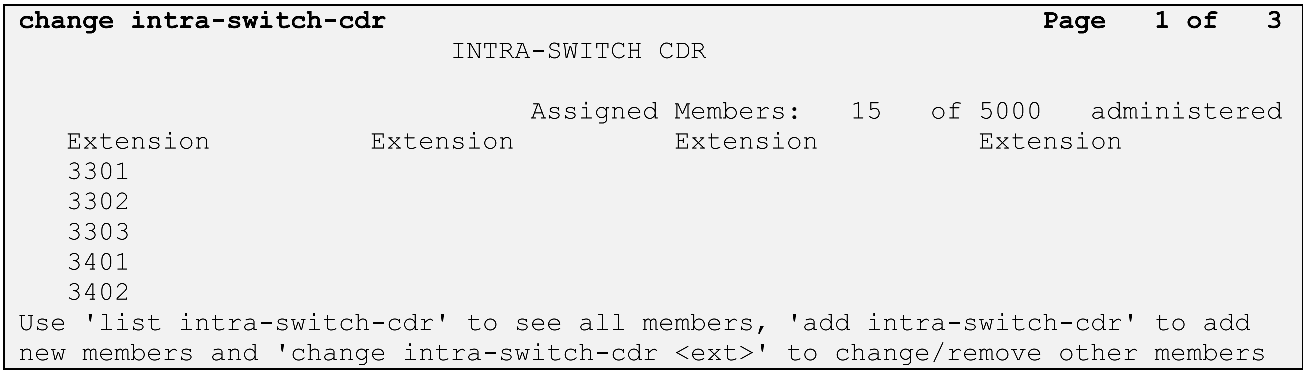
```
change system-parameters cdr
                            CDR SYSTEM PARAMETERS

 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 are 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** and set **CDR or 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 RSI Shadow CMS

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

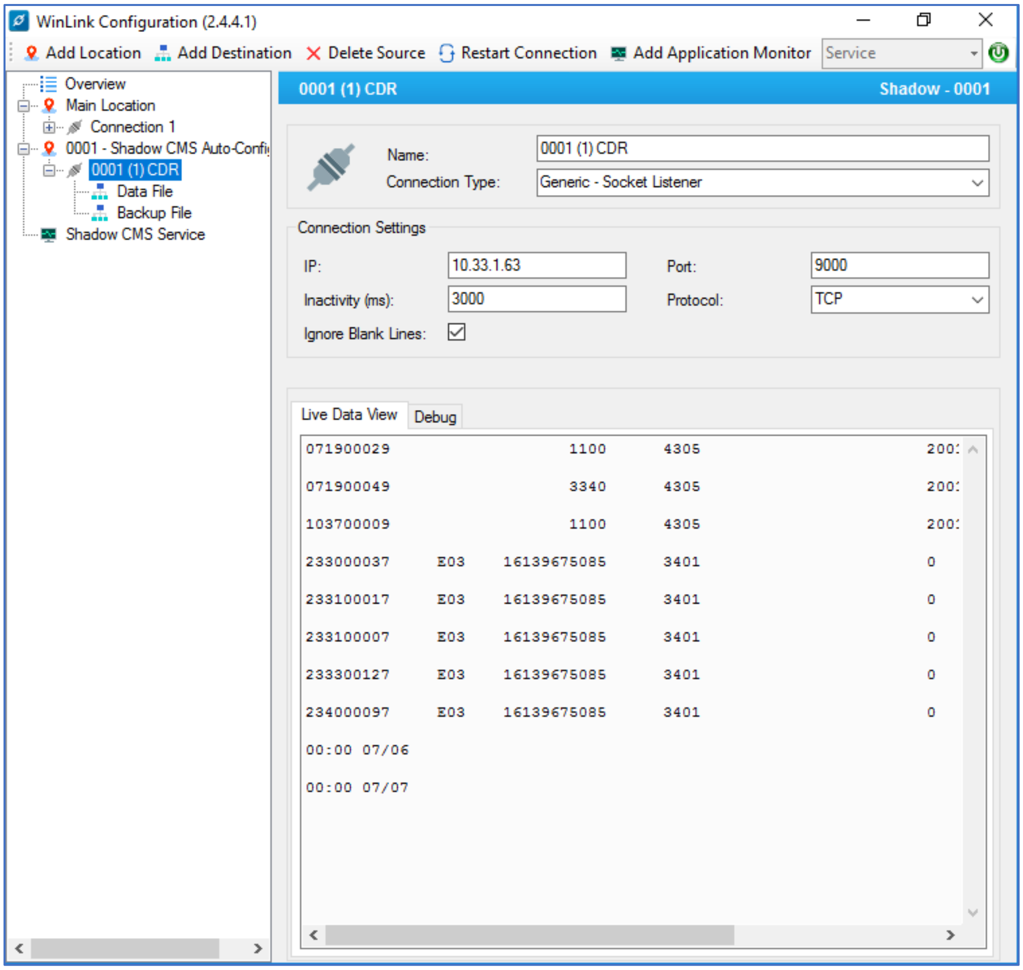
- Administer Winlink Configuration
- Administer CDR Driver
- Verify CDR Data

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**, **Avaya CM** source, **Data File** and **Backup File** were previously configured during the testing they are displayed in the picture for showing purposes. From the **Avaya CM** 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 (ms)**: enter a desired value, e.g. 3000



Name: 0001 (1) CDR

Connection Type: Generic - Socket Listener

Connection Settings

IP: 10.33.1.63

Port: 9000

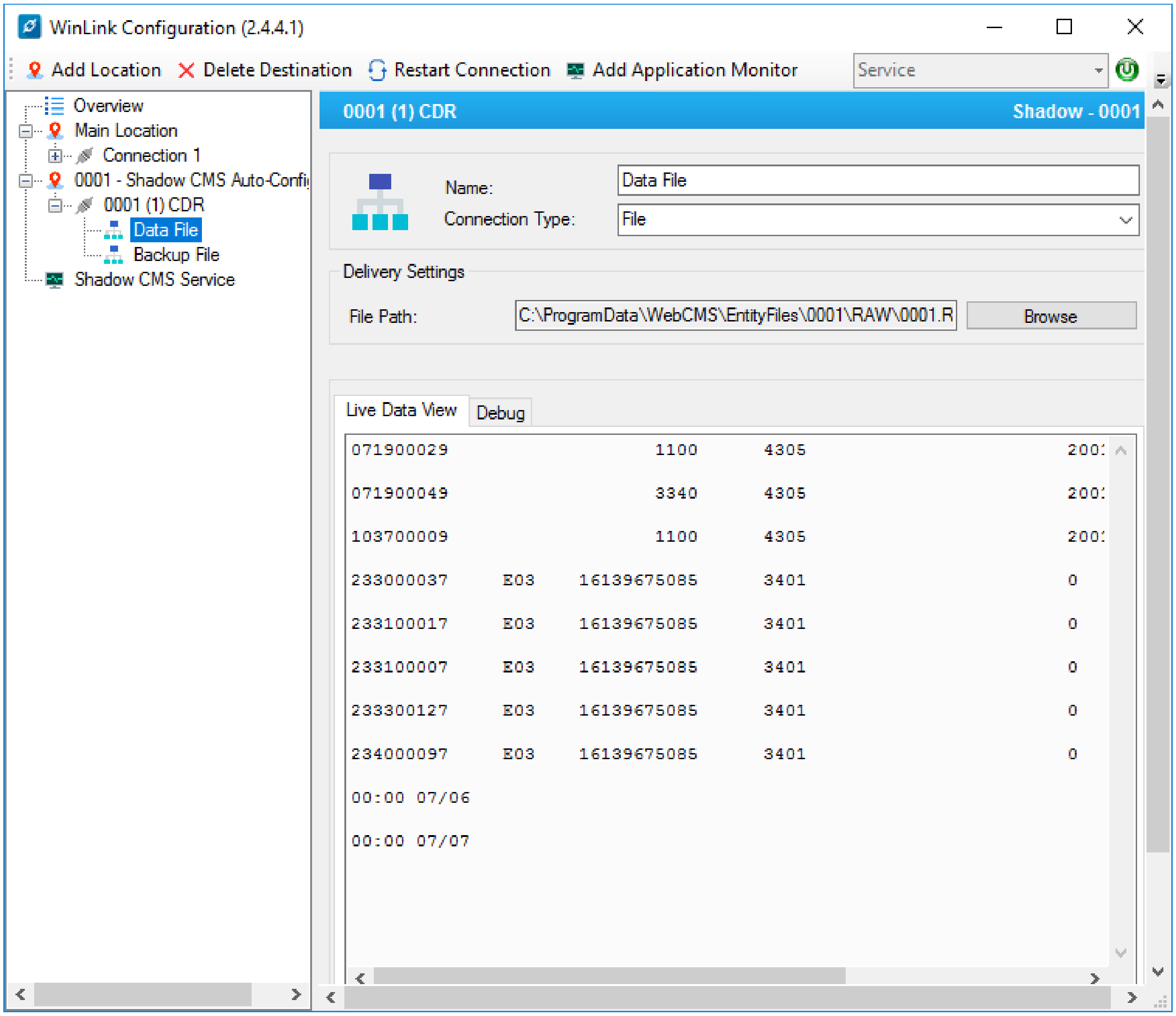
Inactivity (ms): 3000

Protocol: TCP

Ignore Blank Lines: ☑

```
071900029                  1100      4305                        200:

071900049                  3340      4305                        200:

103700009                  1100      4305                        200:

233000037     E03    16139675085     3401                        0

233100017     E03    16139675085     3401                        0

233100007     E03    16139675085     3401                        0

233300127     E03    16139675085     3401                        0

234000097     E03    16139675085     3401                        0

00:00 07/06

00:00 07/07
```

Select **Data File** under **CDR** 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.



Name: Data File

Connection Type: File

File Path: C:\ProgramData\WebCMS\EntityFiles\0001\RAW\0001.R

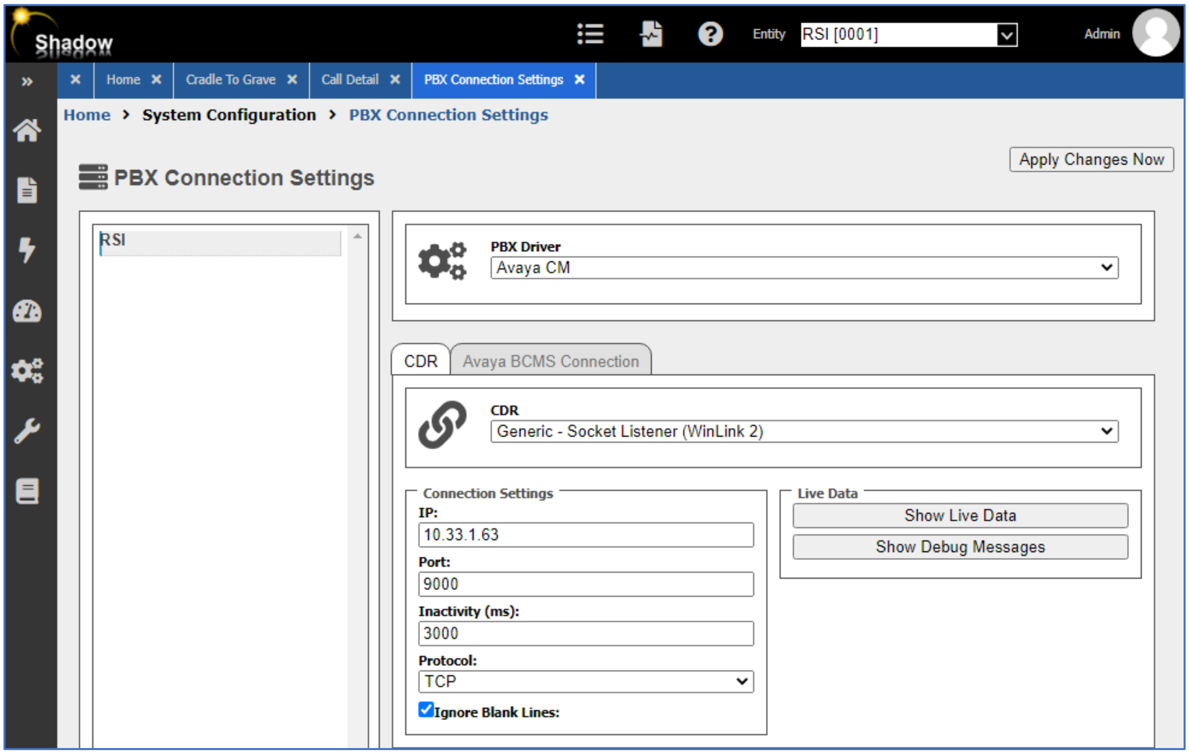
```
071900029                   1100      4305                       200:
071900049                   3340      4305                       200:
103700009                   1100      4305                       200:
233000037     E03    16139675085      3401                       0
233100017     E03    16139675085      3401                       0
233100007     E03    16139675085      3401                       0
233300127     E03    16139675085      3401                       0
234000097     E03    16139675085      3401                       0
00:00 07/06
00:00 07/07
```

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 its password to log in (not shown).

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

- In the **PBX Driver** section: select “Avaya CM” from the dropdown menu
- In the **CDR** tab, select **Generic – Socket Listener (WinLink 2)**
- In the Connection Settings, enter the IP address of Shadow CMS server, Port 9000, Inactivity (ms) 3000 and select the **TCP** protocol



Entity: RSI [0001]

Home › System Configuration › PBX Connection Settings

PBX Connection Settings

RSI

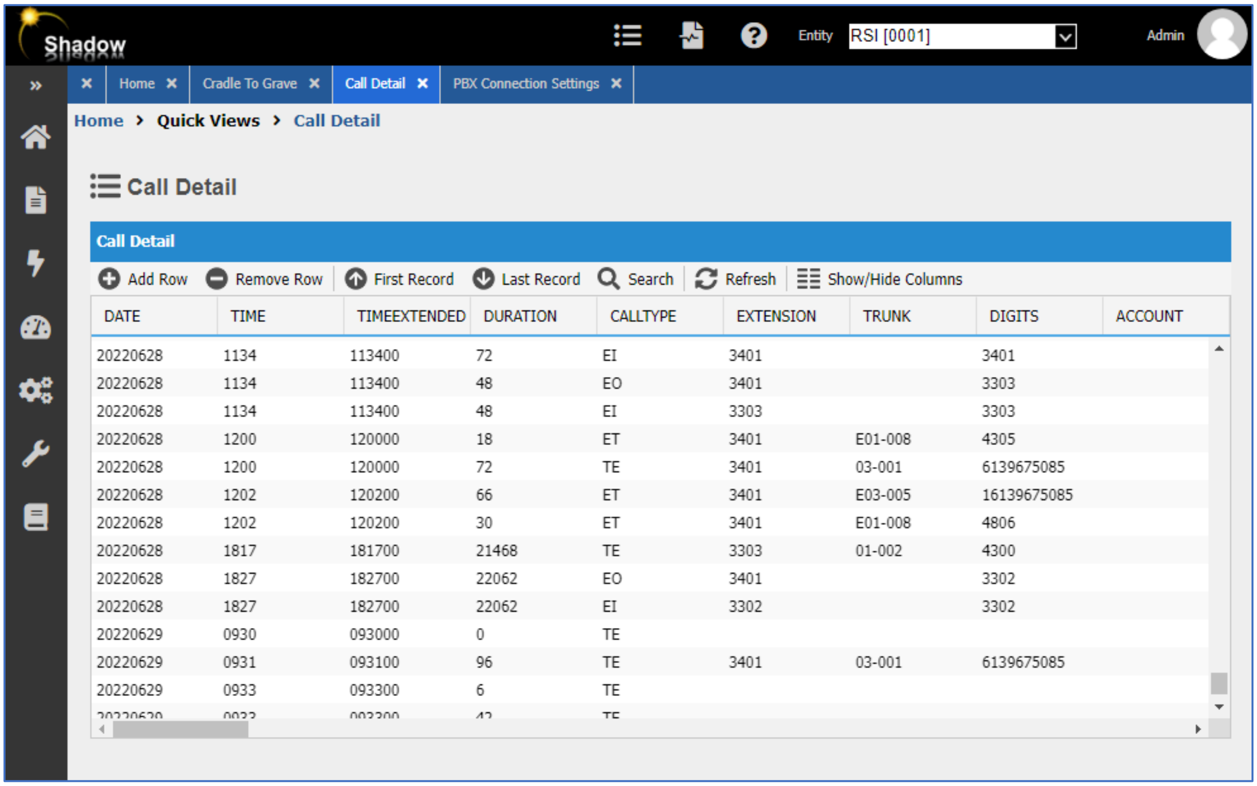
PBX Driver: Avaya CM

CDR: Generic - Socket Listener (WinLink 2)

Connection Settings
IP: 10.33.1.63
Port: 9000
Inactivity (ms): 3000
Protocol: TCP
☑ Ignore Blank Lines:

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.



DATE	TIME	TIMEEXTENDED	DURATION	CALLTYPE	EXTENSION	TRUNK	DIGITS	ACCOUNT
20220628	1134	113400	72	EI	3401		3401	
20220628	1134	113400	48	EO	3401		3303	
20220628	1134	113400	48	EI	3303		3303	
20220628	1200	120000	18	ET	3401	E01-008	4305	
20220628	1200	120000	72	TE	3401	03-001	6139675085	
20220628	1202	120200	66	ET	3401	E03-005	16139675085	
20220628	1202	120200	30	ET	3401	E01-008	4806	
20220628	1817	181700	21468	TE	3303	01-002	4300	
20220628	1827	182700	22062	EO	3401		3302	
20220628	1827	182700	22062	EI	3302		3302	
20220629	0930	093000	0	TE				
20220629	0931	093100	96	TE	3401	03-001	6139675085	
20220629	0933	093300	6	TE				
20220629	0933	093300	42	TE				

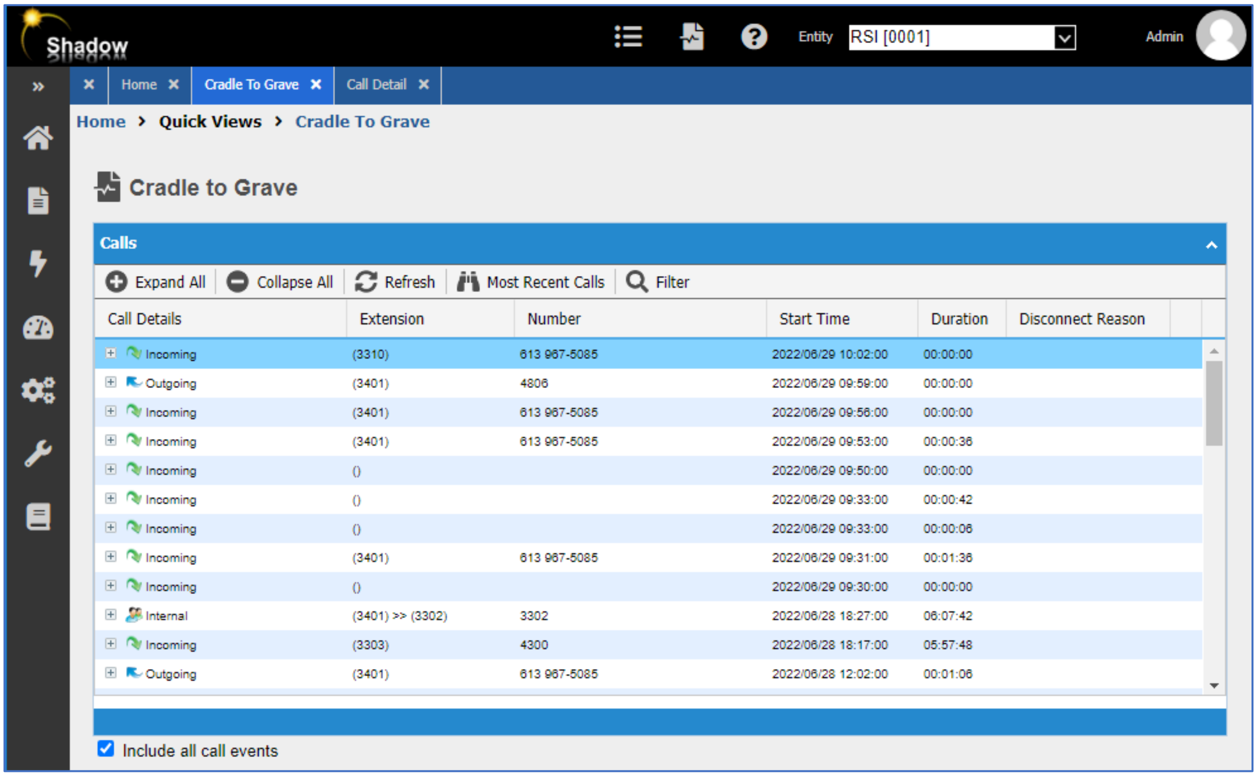
7. Verification Steps

The following steps may be used to verify the configuration:

- Check the CDR status, by running the “**status cdr-link**” 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: 2022/06/08 11:10:31         2022/07/07 07:50:54
  Forward Seq. No: 0                           81
 Backward Seq. No: 0                           0
CDR Buffer % Full:   0.00                        0.00
      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.



Cradle to Grave

Calls

Call Details	Extension	Number	Start Time	Duration	Disconnect Reason
Incoming	(3310)	613 967-5085	2022/06/29 10:02:00	00:00:00	
Outgoing	(3401)	4806	2022/06/29 09:59:00	00:00:00	
Incoming	(3401)	613 967-5085	2022/06/29 09:56:00	00:00:00	
Incoming	(3401)	613 967-5085	2022/06/29 09:53:00	00:00:36	
Incoming	()		2022/06/29 09:50:00	00:00:00	
Incoming	()		2022/06/29 09:33:00	00:00:42	
Incoming	()		2022/06/29 09:33:00	00:00:06	
Incoming	(3401)	613 967-5085	2022/06/29 09:31:00	00:01:36	
Incoming	()		2022/06/29 09:30:00	00:00:00	
Internal	(3401) >> (3302)	3302	2022/06/28 18:27:00	06:07:42	
Incoming	(3303)	4300	2022/06/28 18:17:00	05:57:48	
Outgoing	(3401)	613 967-5085	2022/06/28 12:02:00	00:01:06	

☑ Include all call events

.

8. Conclusion

These Application Notes describe the procedures for configuring Resource Software International Shadow CMS with Avaya Aura® Communication Manager. Testing was successful.

9. Additional References

This section references the product documentation relevant to these Application Notes.

[1] Administering Avaya Aura® Communication Manager, Release 10.1, Issue 1, December 2021.

[2] Administering Avaya Aura® Session Manager, Release 10.1, Issue 1, April 2021.

[3] Administering Avaya Aura® Application Enablement Services, Release 10.1, Issue 4, April 2022.

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.