Avaya Solution & Interoperability Test Lab

Application Notes for Resource Software International Shadow Call Management System Version 4.3.0 with Avaya Aura® Communication Manager 6.2 – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring steps required for the Resource Software International Shadow Call Management Software call accounting software to successfully interoperate with Avaya Aura® Communication Manager.

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 Resource Software International (RSI) Shadow Call Management Software (CMS) call accounting software can interoperate with Avaya Aura® Communication Manager. RSI CMS connects to Communication Manager over the local or wide area network using a Call Detail Recording (CDR) link running Reliable Session Protocol (RSP). Communication Manager is configured to send CDR records to RSI CMS using a specific TCP/IP port. The serviceability and load tests were conducted to assess the reliability of the solution.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch and inter-switch calls, inbound trunk and outbound trunk calls to and from telephones attached to the Communication Manager Servers, and verified that the CMS collected the CDR records and properly classified and reported the attributes of the call. For serviceability testing, physical and logical links were disabled/re-enabled, the Communication Manager was restarted and the CMS was restarted.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute a full product performance or feature testing performed by third party vendors, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a third party solution.

2.1. Interoperability Compliance Testing

The compliance test included feature, serviceability, and load testing. The feature testing evaluated the ability of the CMS to collect and process CDR records for various types of calls. The unformatted format was utilized during the compliance test. The serviceability test introduced failure scenarios to see if the CMS can resume CDR collection after recovery. The load test was manually executed by placing more than 100 test calls to generate a substantial amount of CDR records

2.2. Test Results

All test cases were executed and there were some unexpected behaviors that related to SIP endpoints. The following statement was made for SIP endpoint.

There are some differences in Communication Manager in the call records generated by SIP endpoints compared to Analog, Digital, and H.323 endpoints. As a result in certain scenarios involving SIP endpoints (e.g., two-party call, transfer, or conference), a CDR application may see more or less records, or records with condition codes/calling party other than expected. Avaya is investigating the differences and fixes will be made available in a future release.

2.3. Support

Technical support for Resource Software International Shadow Call Management can be obtained by contacting Resource Software International via http://www.telecost.com/services.htm or by calling (905)576-4575.

3. Reference Configuration

Figure 1 illustrates a sample configuration that was used for the compliance test. The configuration consists of two Avaya S8800 and S8300 Servers running Communication Manager. Site 1 is comprised of Communication Manager running on Avaya S8800 Server with an Avaya G650 Media Gateway. Site 2 is comprised of Communication Manager running on an Avaya S8300 Server residing in an Avaya G450 Media Gateway. Each Communication Manager is connected to an IP network comprised of a layer 2 switch. Resource Software International CMS is running on a Windows 2008 Server connected to the layer 2 switch in Site 1, and has a TCP Winlink session established to the Communication Manager to collect CDR records. Each site has trunks and phones to generate calls. Site 1 has a PRI trunk to route calls to a real PSTN for test calls.

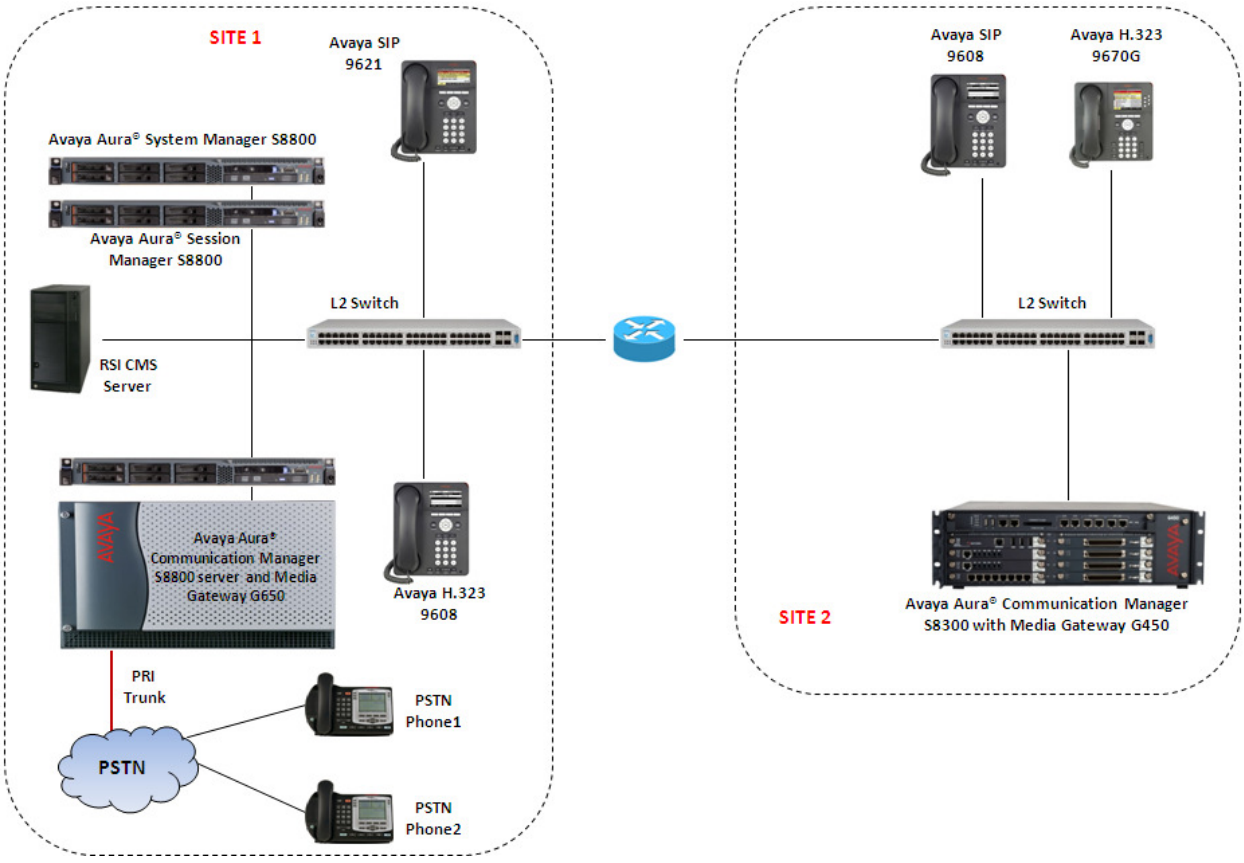


Figure 1: Test Configuration Diagram

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Communication Manager Server	6.2 SP3
Avaya Media Gateway G650 • IP Service TN2312BP • C-LAN TN799DP • MEDPRO TN2302AP	 • HW06 FW043 • HW01 FW026 • HW20 FW117
Avaya S8800 System Manager Server	6.3 SP1
Avaya S8800 Session Manager Server	6.3 SP1
Avaya S8300 Communication Manager	6.2 SP3
Avaya G450 Media Gateway	32 .24 .0 /1
Avaya H.323 IP Phone 9670G	S3.1.5
Avaya H.323 IP Phone 9608	S6.02
Avaya SIP IP Phone 9621G	6.2.0.72
Avaya SIP IP Phone 9608G	6.2.0.72
RSI CMS Operating System	Windows 2008 64-Bit Standard R2
RSI Shadow CMS	4.3.0

5. Configure Avaya Aura ® Communication Manager

This section provides procedures for configuring the CDR feature in Communication Manager. All configuration changes in Communication Manager are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Communication Manager. All steps are the same for the other Communication Manager unless otherwise noted. Communication Manager will be configured to generate CDR records and send CDR records to the IP address of RSI CMS. For the Communication Manager, the CDR link originates at the IP address of the Processor interface, and terminates at the CMS. The highlights in the following screens indicate the parameter values used during the compliance test.

Enter the **change node-names ip** command to create a new node name, for example, RSI CMS server is named **Server-1**. This node name is associated with the IP address of the CMS server. During the test, Avaya CDR RDTT tool was also used to receive CDR records from Communication Manager to compare with the CDR records received from the CMS. The RDTT tool installed was also administered.

```
change node-names ip                                          Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
AVAYARDTT              10.10.98.68
CLAN1                  10.10.97.217
DevCM3                 10.33.4.9
GW                     10.10.97.193
MedPro1                10.10.97.218
SM63                   10.10.97.198
Server-1               10.10.97.19
procr                  10.10.97.201
procr6                 ::
```

Enter the **change ip-services** command to define the CDR link to use RSP over TCP/IP. The following information should be provided:

- Service Type: **CDR1** → This CDR service is for RSI CMS
- Local Node: **Procr** → The default IP Address of Communication Manager
- Local Port: **0** → Leave it as default
- Remote Node: **Server-1** → The Remote Node is set to the node name Server-1 as defined previously
- 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 CMS.

```
change ip-services                                            Page   1 of   4

                                  IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
CDR1                      procr        0         Server-1        9000
CDR2                      procr        0         AVAYARDTT       9001
```

On Page 3, disable the Reliable Protocol for the CDR link connected to RSI CMS server by setting the Reliable Protocol field to **N**. However, set to **Y** for the CDR2 connection to Avaya RDTT server if the Avaya RDTT tool is used.

```
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
```

Enter the **change system-parameters cdr** command 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**
- Enable CDR Storage on Disk?: **n** →Enable the Survivable CDR feature. Default is n.
- Use Legacy CDR Formats?: **n** → Allows CDR formats to use 5.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   1
                            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? n
       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? 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? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? y                  Inc Attd Call Record? y
  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: 3
```

If the Intra-switch CDR field is set to y on Page 1 of the system-parameters cdr form, then enter 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:   10   of 5000   administered
   Extension          Extension          Extension          Extension
   53010
   53012
   53013
   53014
   53100
   53101
   53102
   53104
```

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group n** command, where n is the trunk group number, to verify that the CDR Reports field is set to y. This applies to all types of trunk groups.

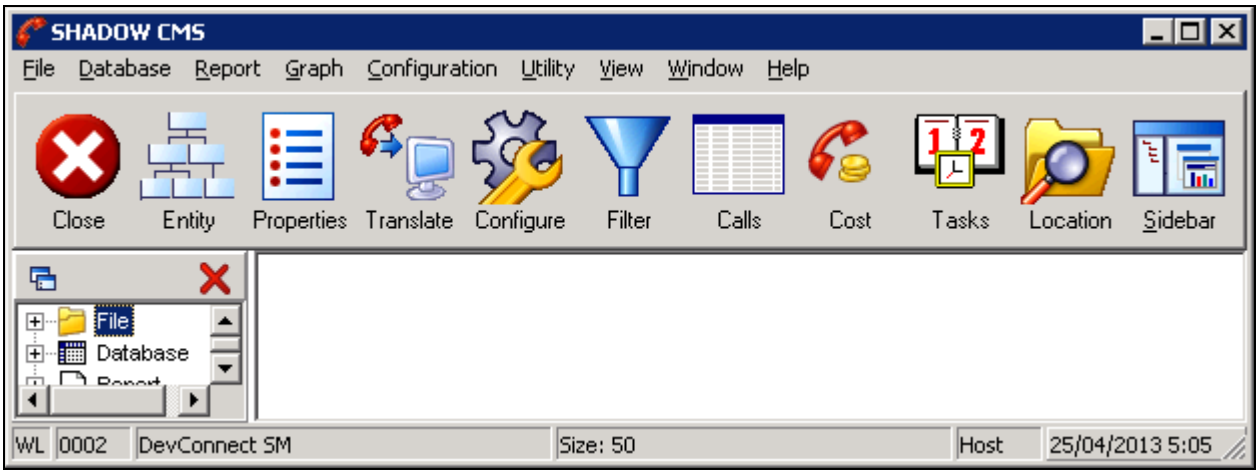
```
change trunk-group 6                                            Page   1 of  21
                                  TRUNK GROUP

Group Number: 6                      Group Type: isdn           CDR Reports: y
  Group Name: T1-To-Jeff(PSTN)             COR: 2        TN: 1        TAC: #006
   Direction: two-way        Outgoing Display? y         Carrier Medium:
PRI/BRI
 Dial Access? y              Busy Threshold: 255  Night Service:
Queue Length: 0
Service Type: tie                    Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
```

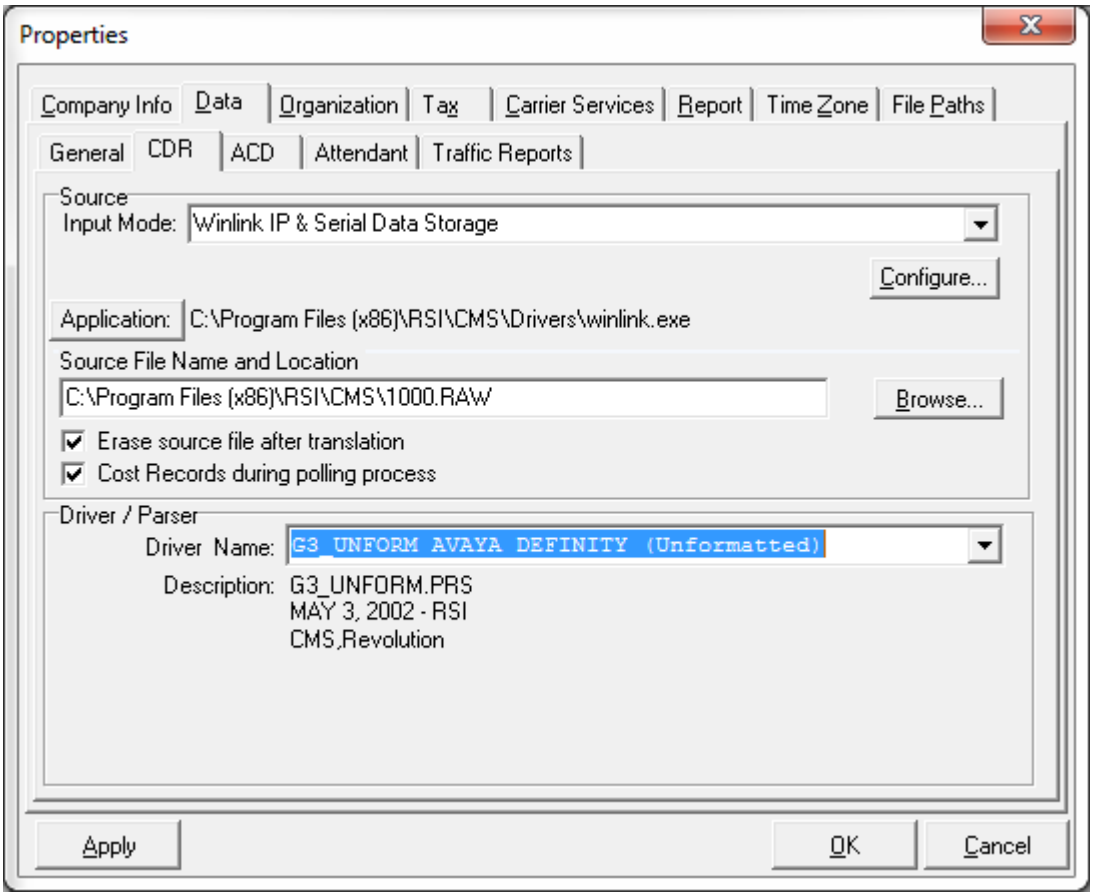
6. Configure Resource International Software Shadow CMS

This section describes the operation of RSI Shadow CMS. The Shadow CMS connects to Communication Manager via RSP over the TCP/IP port. CDR records are sent from Communication Manager (Processor port) into the Shadow CMS where the raw data is transformed into call records, which are then immediately available for reporting. RSI installs, configures, and customizes the Shadow CMS application for their end customers.

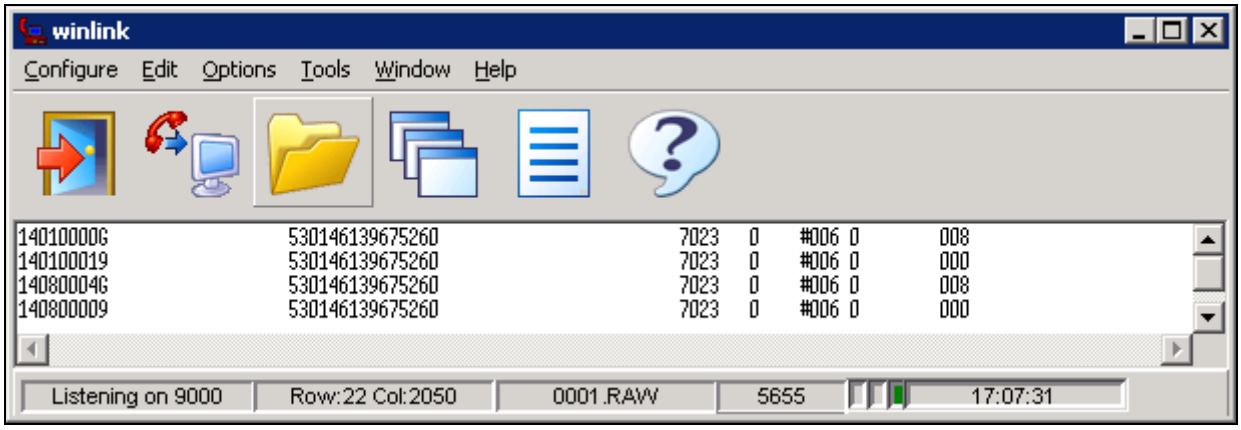
To launch the RSI Shadow CSM application, from the server which the CMS application is installed, navigate to menu **Start → All Program → RSI → CMS** (not shown). The Shadow CMS window is displayed as shown below.



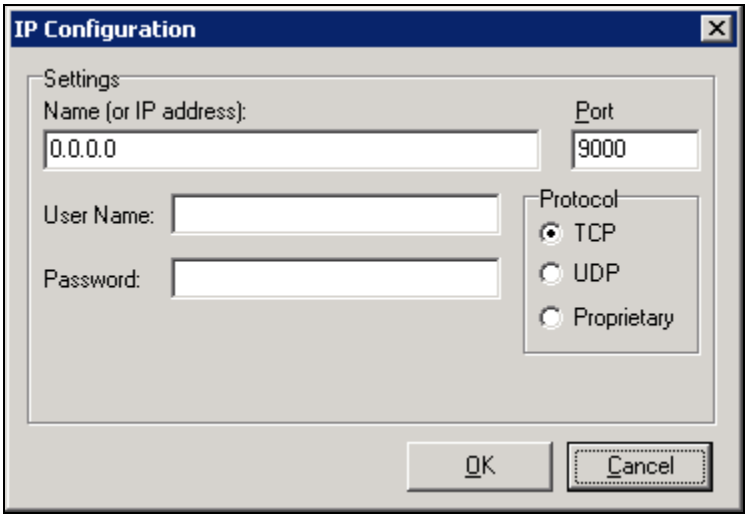
To configure the CDR format for the Shadow CMS, navigate to **File → Properties** (not shown). The **Properties** window is displayed, click on the **Data** tab on the **Properties** window and select **CDR** sub-tab. Select **Winlink IP & Serial Data Storage** from the **Source Input Mode** dropdown box. Select **G3_UNFORM AVAYA DEFINITY (Unformatted)** from the **Driver Name** dropdown box. Click **OK** to complete.



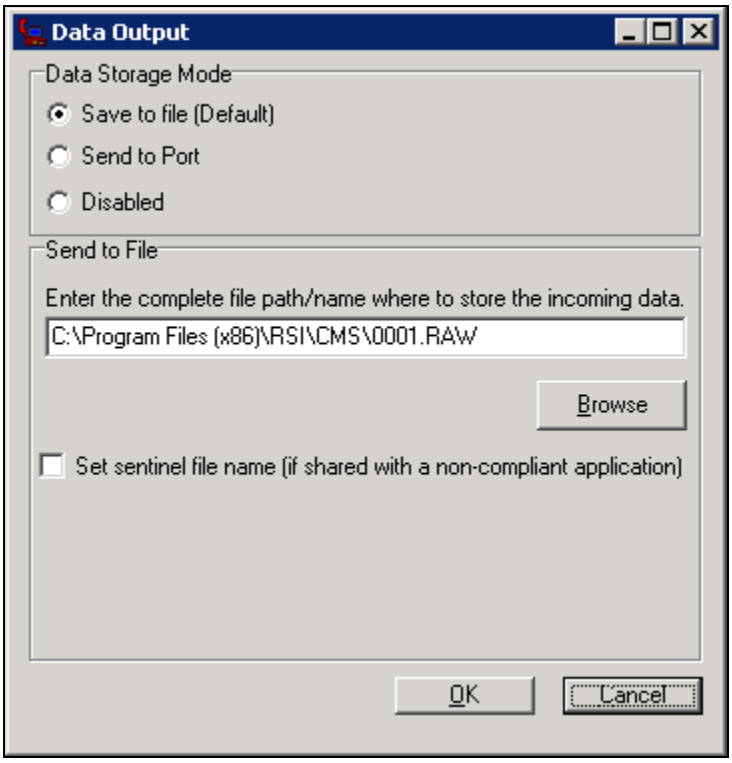
The Shadow CMS application uses Winlink application to listen and receive CDR from Communication Manager. To configure the Winlink application, click the Winlink icon on the desktop, the Winlink application is displayed as below.



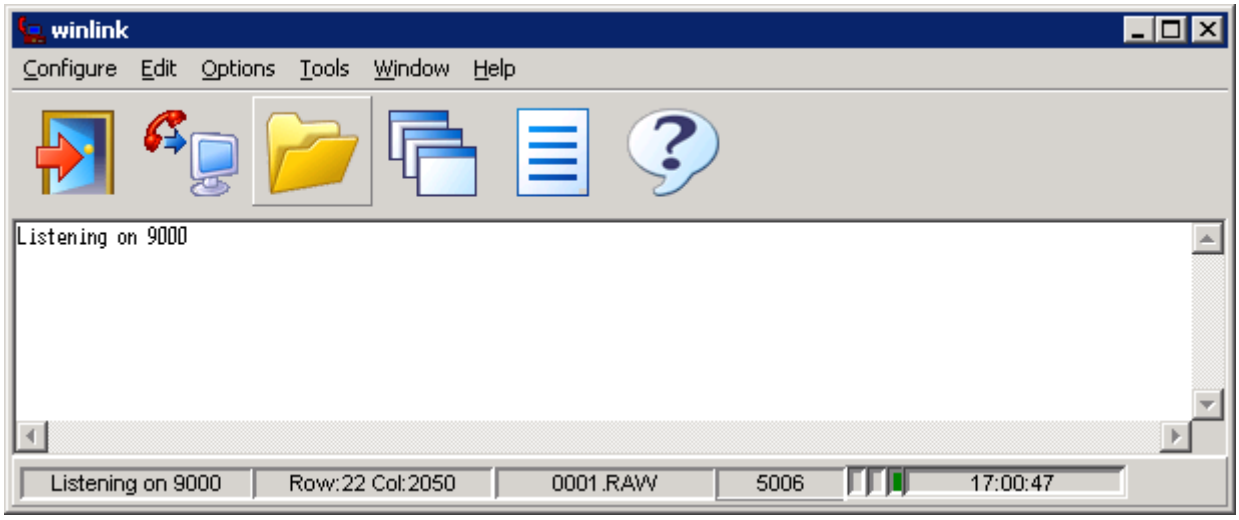
Navigate to **Configure → Telnet and Socket Settings** (not shown). The **IP Configuration** is displayed. Enter port **9000** in the **Port** field as configured in the **ip-services** command in **Section 5** and select **TCP** option button as the screen shown below. Click **OK** button to complete.



To configure Data Output, navigate to **Options → File Path/Data Storage Mode** (not shown). The **Data Output** window is displayed. Select the option **Save to file (Default)**. Enter the path to save the RAW CDR file in the "**Enter the complete file path/name where to store the incoming data**" field. Click **OK** to complete.



Navigate to **Configure→ Listen** (not shown), to start listening on port 9000 and receive CDR from Communication Manager.



7. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of the Communication Manager enter the **status cdr-link** command and verify that the primary CDR link state is **up**.

```
status cdr-link
                                CDR LINK STATUS
                    Primary                       Secondary

       Link State: up                            up

      Date & Time: 2013/04/24 15:39:18           2013/04/24 17:14:38
  Forward Seq. No: 0                            91
 Backward Seq. No: 0                            0
CDR Buffer % Full: 0.00                         0.00
      Reason Code: OK                           OK
```

- Place a call and verify that RSI Shadow CMS received CDR records for the call. Compare the values of the data fields in the CDR record with the expected values, and verify that they match.
- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in RSI Shadow CMS, and verify the report's accuracy.

8. Conclusion

These Application Notes describe the procedures for configuring Resource Software International Shadow Call Management System to collect call detail records from Avaya Aura® Communication Manager. There are some unexpected CDR for SIP endpoints, refer to **Section 2.2** for details.

9. Additional References

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

[1] *Administering Avaya Aura® Communication Manager*, Release 6.2, June 2012, Issue 6.2,Document Number 03-300509
[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.2 , Feb 2012, Issue 0.9, Doc# 555-245-205
[3] *Administering Avaya Aura® Session Manager*, Release 6.3, November 2012, Issue 1.1, Document Number03-603324
[4] *Administering Avaya Aura® System Manager*, Release 6.3, November 2012

The following Resource Software International CMS product documentation can be found at http://www.telecost.com or by contacting their support department.

[1] CMS User Guide
[2] Avaya Communication Manager RSI CMS Integration Guide

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.