Avaya Solution & Interoperability Test Lab

Application Notes for Resource Software International Shadow Call Management System Version 4.3.0 with Avaya Aura® Session Manager 6.3 – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring steps required for the Resource Software International Shadow Call Management System call accounting software to successfully interoperate with Avaya Aura® Session 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 the Resource Software International (RSI) Shadow Call Management Software (CMS) call accounting software can interoperate with Avaya Aura® Session Manager. RSI CMS connects to Session Manager over the local or wide area network using Secure File Transfer Protocol (SFTP). Session Manager is configured to generate Call Detail Records (CDR) into files and save them to a specific folder on the Session Manager server. RSI CMS using SFTP connects to the server, to access these folders and download them to the local CMS server for reports. 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 Sessiong Manager Server, and verified that the CMS collected the CDR records and properly classified and reported the attributes of the call. For serviceability testing, Session Manager Server 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 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 passed. There is an observation captured on the SIP endpoint during the test.

- By default, SIP Trunk: Auto Alternative Route (AAR) is assigned to SIP endpoint when it is newly created and the CDR will not be logged in the case of SIP endpoint placed calls to H.323 endpoints in the same local Communication Manager. There is a workaround for this issue which is to assign a specific SIP trunk group number to the SIP endpoints instead of using the default AAR. The issue is already reported and is investigated by Avaya.

2.3. Support

Technical support for RSI Shadow Call Management System 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 Servers 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 Winlink FTP session established to Session Manager S8800 to collect CDR records. Each site has trunks and phones to generate calls. The real PSTN is connected to the Communication Manager via a PRI/ISDN trunk.

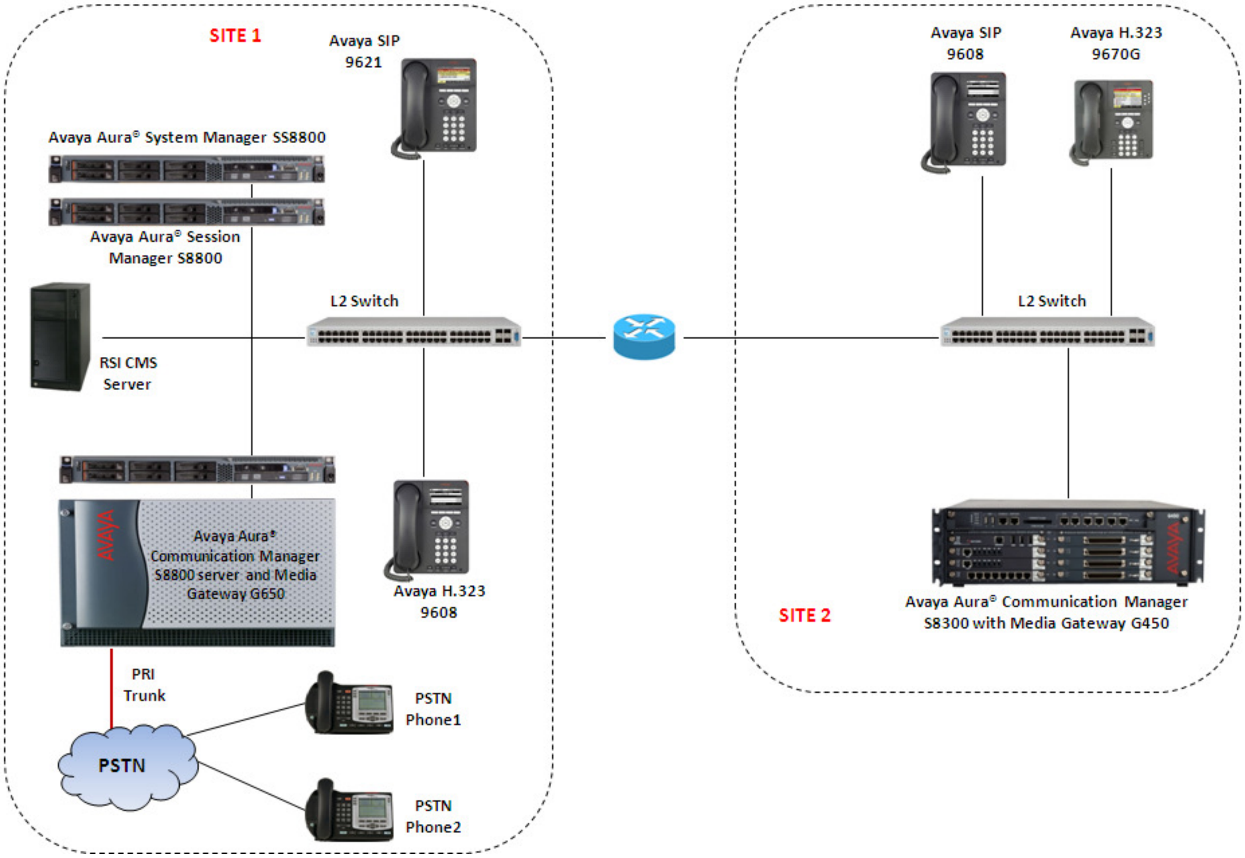

SITE 1
Avaya SIP 9621
Avaya Aura® System Manager SS8800
Avaya Aura® Session Manager S8800
L2 Switch
RSI CMS Server
Avaya Aura® Communication Manager S8800 server and Media Gateway G650
Avaya H.323 9608
PRI Trunk
PSTN
PSTN Phone1
PSTN Phone2
Avaya SIP 9608
Avaya H.323 9670G
L2 Switch
SITE 2
Avaya Aura® Communication Manager S8300 with Media Gateway G450

Figure 1: Test Configuration Diagram

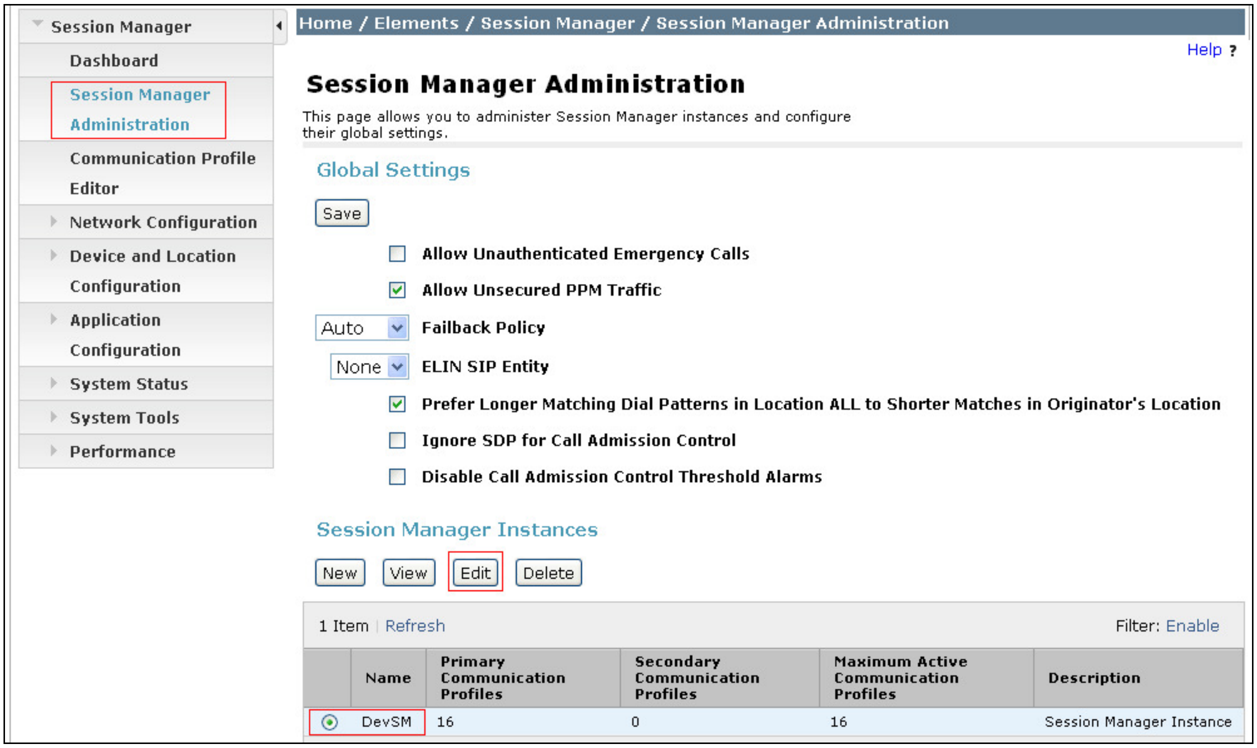
4. Equipment and Software Validated

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 ® Session Manager

To enable CDR on Session Manager, log in System Manager to which the Session Manager is managed. From the homepage of System Manager, navigate to **Elements → Session Manager** (not shown). The **Session Manager** tab is displayed, in the left navigation pane, select **Session Manager Administration**. When the **Session Manager Administration** page is displayed select the Session Manager instance e.g. **DevSM** in the **Session Manager Instance** section and click on **Edit** button to edit.


Session Manager
Dashboard
Session Manager Administration
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Session Manager Administration
Help ?
Save
New
View
Edit
Delete
Refresh
Filter: Enable

Session Manager Administration

This page allows you to administer Session Manager instances and configure their global settings.

Global Settings

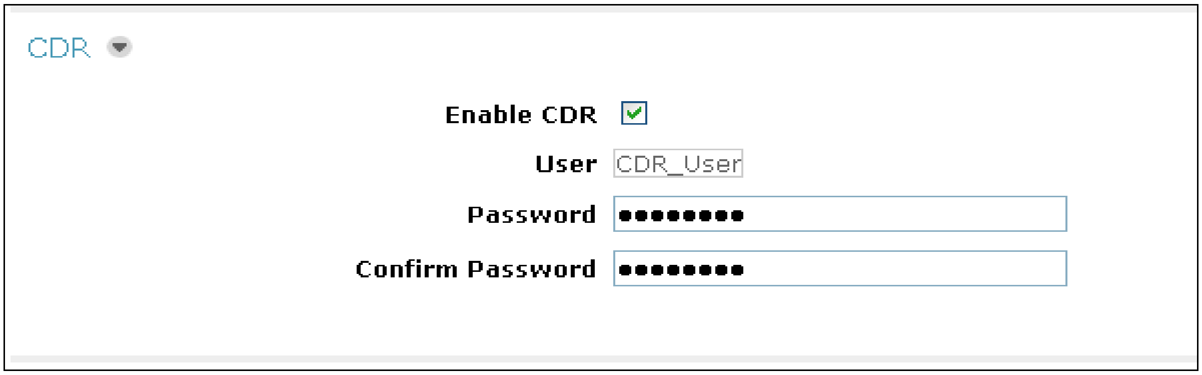
☐ Allow Unauthenticated Emergency Calls
☑ Allow Unsecured PPM Traffic
Auto Failback Policy
None ELIN SIP Entity
☑ Prefer Longer Matching Dial Patterns in Location ALL to Shorter Matches in Originator's Location
☐ Ignore SDP for Call Admission Control
☐ Disable Call Admission Control Threshold Alarms

Session Manager Instances

1 Item

	Name	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
●	DevSM	16	0	16	Session Manager Instance

The **Edit Session Manager** page is displayed. Scroll down to the CDR section, check on the check box **Enable CDR** to enable the CDR feature and enter a password in the **Password** and **Confirm Password** box for the **CDR_User**. Click the **Commit** button at the end of the page to commit the changes (not shown).

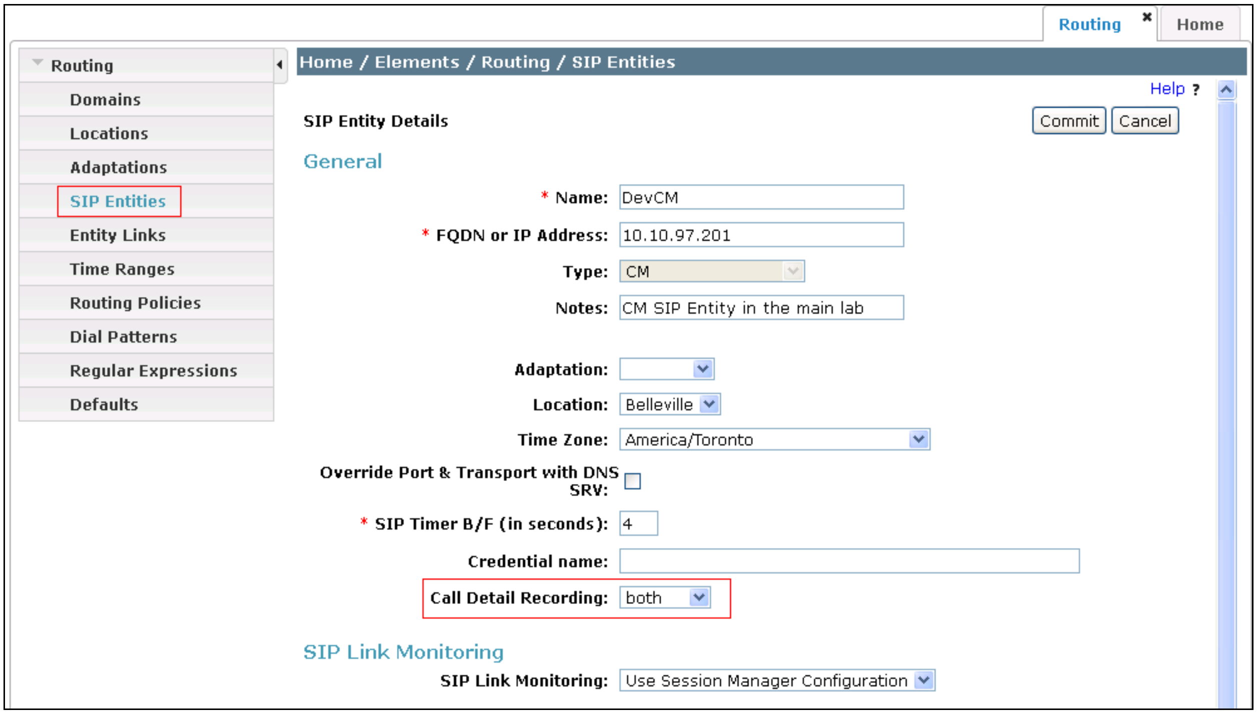


CDR

Enable CDR ☑
User CDR_User
Password ●●●●●●●●●
Confirm Password ●●●●●●●●●

From the homepage of System Manager, navigate to **Elements** → **Routing** → **SIP Entities**. The **SIP Entities** page is displayed (not shown). Select the desired SIP entity which the Call Detail Recording feature needs to be enabled for, in this case the CM SIP Entity is **DevCM**. Click the **Edit** button, the **SIP Entity Details** page is displayed, in the **Call Detail Recording** dropdown menu select "**both**" as in the screen shown below. Click the **Commit** button to commit the change.

Note: Repeat the same procedure for other SIP Entities if needed.



SIP Entity Details

General

* Name: DevCM

* FQDN or IP Address: 10.10.97.201

Type: CM

Notes: CM SIP Entity in the main lab

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: both

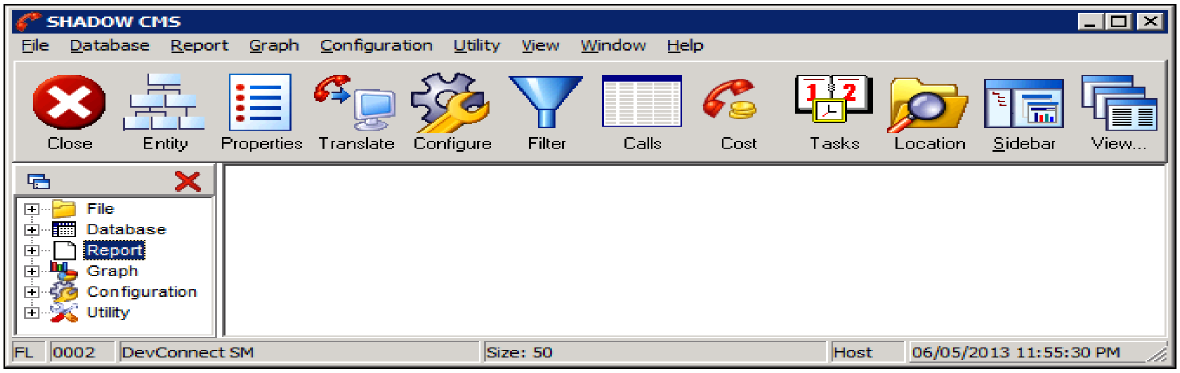
SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6. Configure Resource International Software Shadow CMS

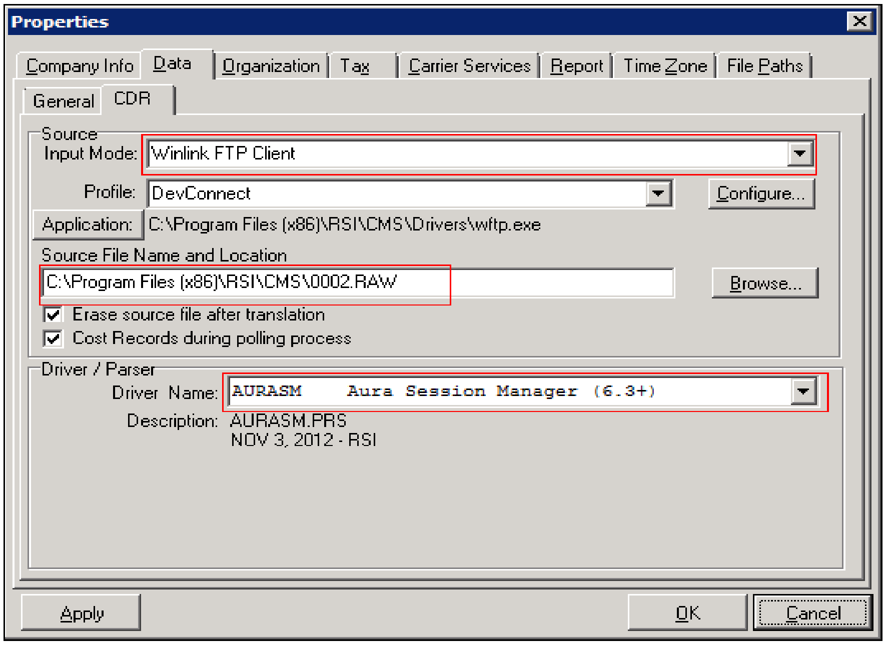
This section describes the operation of RSI Shadow CMS. The Shadow CMS connects to Session Manager via SFTP, CDR files are downloaded from Session Manager into the Shadow CMS where the raw data is transformed into call records, which are then immediately available for reporting. RSI installs, configures, and customizes the Shadow CMS application for their end customers.

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



FL | 0002 | DevConnect SM | Size: 50 | Host | 06/05/2013 11:55:30 PM

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 FTP client** in the **Source Input Mode** filed. Select **AURASM Aura Session Manager (6.3+)** in the field **Driver Name** field.



Input Mode: Winlink FTP Client

Profile: DevConnect

Application: C:\Program Files (x86)\RSI\CMS\Drivers\wftp.exe

Source File Name and Location: C:\Program Files (x86)\RSI\CMS\0002.RAW

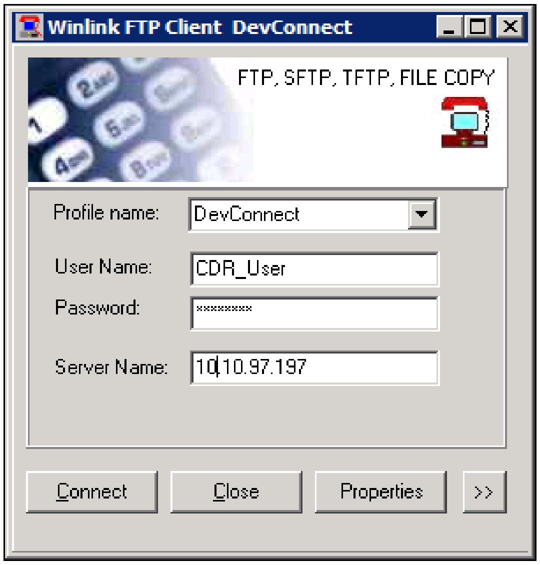
☑ Erase source file after translation

☑ Cost Records during polling process

Driver Name: AURASM Aura Session Manager (6.3+)

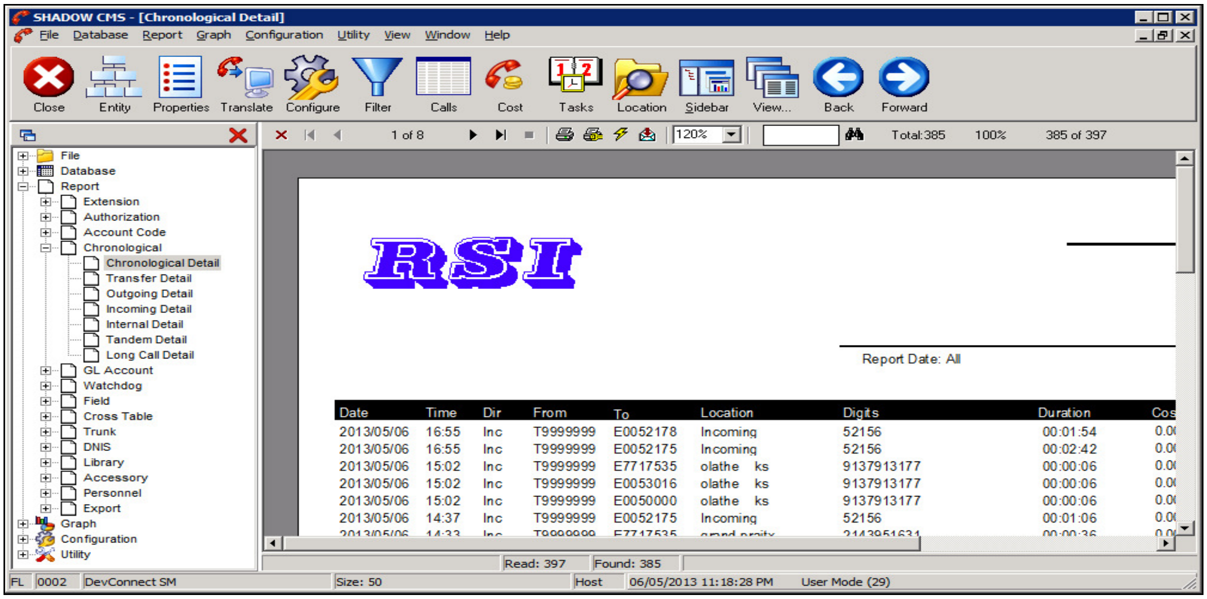
Description: AURASM.PRS
NOV 3, 2012 - RSI

Click the **Configure** button in the **Source Input Mode** section (not shown) to configure the FTP Client. The **Winlink FTP Client** window is displayed. Enter a profile name in the **Profile Name field** e.g. **DevConnect**, **CDR_User** name in the **User Name** field. Enter the password as configured in **Section 5** in the **Password** field and the IP address of Session Manager **10.10.97.197** in the **Server Name** field. Click the **Connect** button to start secure FTP to the Session Manager. Click the **Properties** button followed by the **OK** button (not shown) to complete.



Profile name: DevConnect
User Name: CDR_User
Password: ********
Server Name: 10.10.97.197

To run reports on the Shadow CMS, from the left navigation pane, expand the **Report** tab and select the type of report required, in this example it is **Chronological Detail**. The Chronological Detail query window is displayed, click the **OK** button (not shown) on this window to launch the report. The Chronological Detail report is shown as on the screen below.



Report Date: All

Date	Time	Dir	From	To	Location	Digits	Duration	Cos
2013/05/06	16:55	Inc	T9999999	E0052178	Incoming	52156	00:01:54	0.0
2013/05/06	16:55	Inc	T9999999	E0052175	Incoming	52156	00:02:42	0.0
2013/05/06	15:02	Inc	T9999999	E7717535	olathe ks	9137913177	00:00:06	0.0
2013/05/06	15:02	Inc	T9999999	E0053016	olathe ks	9137913177	00:00:06	0.0
2013/05/06	15:02	Inc	T9999999	E0050000	olathe ks	9137913177	00:00:06	0.0
2013/05/06	14:37	Inc	T9999999	E0052175	Incoming	52156	00:01:06	0.0

7. Verification Steps

The following steps may be used to verify the configuration:

- Use a secure FTP application, e.g. WinSCP to connect to Session Manager by using the CDR_User and password to access the special folder that store the CDR files.
- Place some different kinds of call, wait some minutes for Session Manager to generate the CDR files.
- Use the WinSCP to copy the CDR files and compare with the call records in the report from RSI Shadow CMS. Make sure the number of the calls and other values are correct and match.

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® Session Manager. Refer to **Section 2.2** for a note relating to SIP endpoints.

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/

[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.