Avaya Solution & Interoperability Test Lab

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

Abstract

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

Resource Software International Shadow CMS is a reporting solution that uses Secure File Transfer Protocol to collect CDR data from Avaya Aura® Session Manager.

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® Session Manager (hereafter referred as Session Manager). Shadow CMS collects CDR data from Session Manager over a local or wide area network using a Secure File Transfer Protocol (SFTP). Session Manager is configured to produce CDR records.

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 Session Manager - to collect and interpret the detailed records of inbound, outbound, 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 Session Manager. An assumption is made that Avaya Aura® Session Manager and Avaya Aura® System Manager (hereafter referred as 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 Shadow CMS did not include use of any specific encryption features as requested by Resource Software International (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, and outbound trunk calls.

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 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.

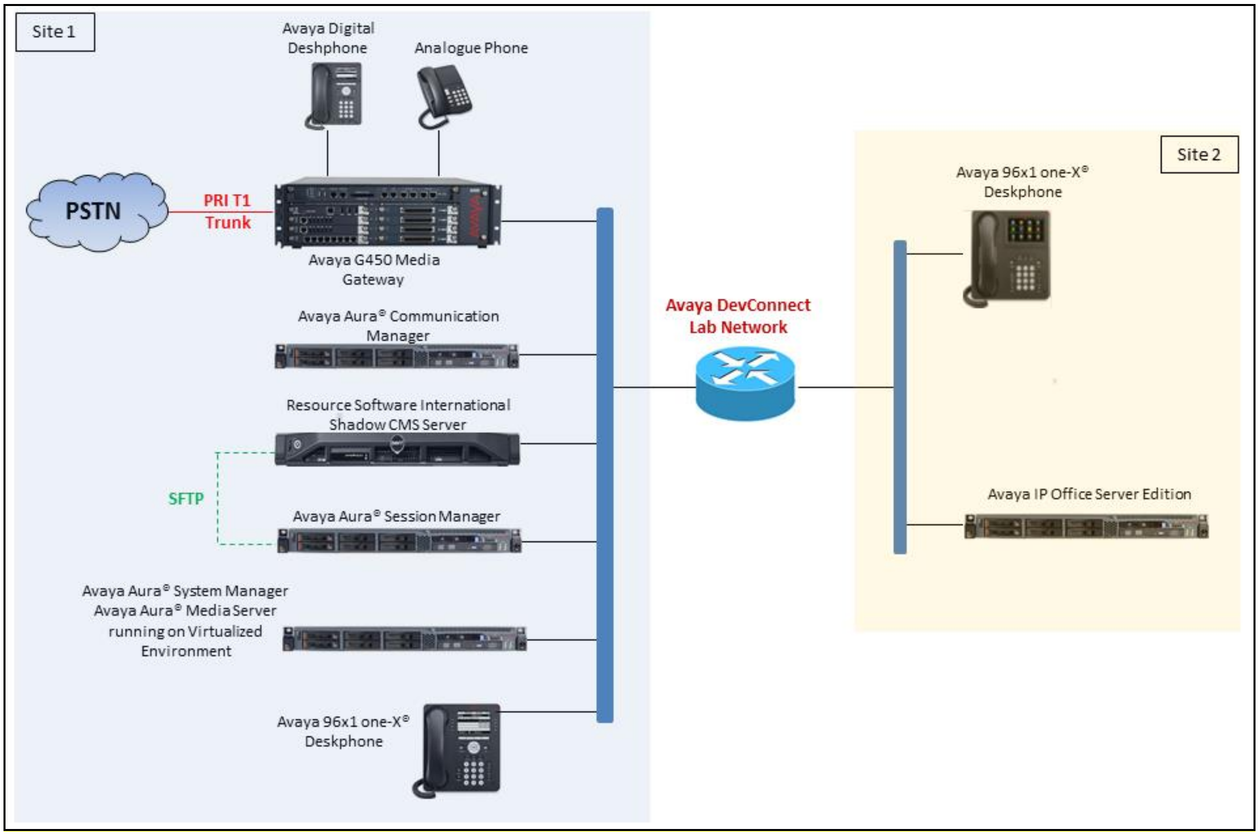

Site 1
Avaya Digital Deshphone
Analogue Phone
PSTN
PRI T1 Trunk
Avaya G450 Media Gateway
Avaya Aura® Communication Manager
Resource Software International Shadow CMS Server
SFTP
Avaya Aura® Session Manager
Avaya Aura® System Manager
Avaya Aura® Media Server
running on Virtualized Environment
Avaya 96x1 one-X® Deskphone
Avaya DevConnect Lab Network
Site 2
Avaya 96x1 one-X® Deskphone
Avaya IP Office Server Edition

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	7.1.1.0.0-FP1 R017x.01.0.532.0
Avaya Aura® System Manager running on Virtualized Environment	7.1.1.0.046931
Avaya Aura® Session Manager running on Virtualized Environment	7.1.1.0.711008
Avaya Aura® Media Server running on Virtualized Environment	7.8.0.395
Avaya G450 Media Gateway	38 .20 .1
Avaya 96x1 IP Telephones	H323 6.6506 SIP 7.1.1.0.9
Avaya 1416 Digital Telephone	FW1
Resource Software International Shadow CMS running on Windows Server 2012	5.1

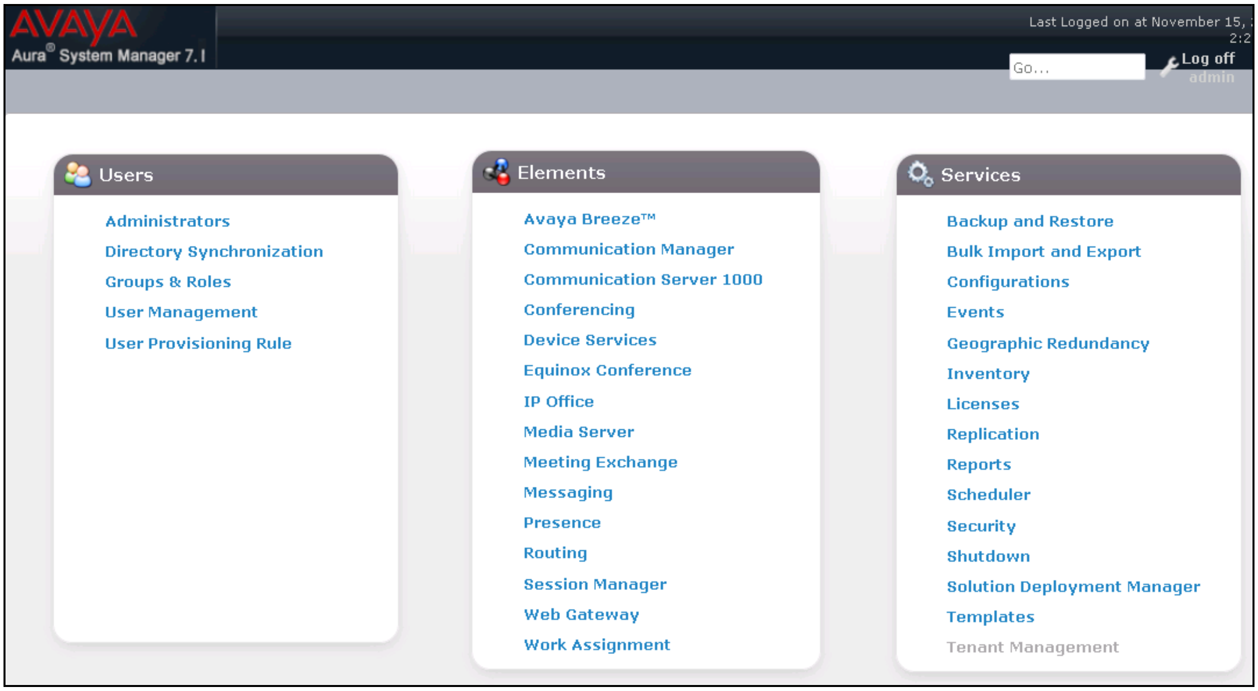
5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. Session Manager is configured by opening a web browser to System Manager. The procedures include the following areas:

- Log onto System Manager
- Administer Call Detail Recording on Session Manager
- Administer Call Detail Recording on SIP Entity

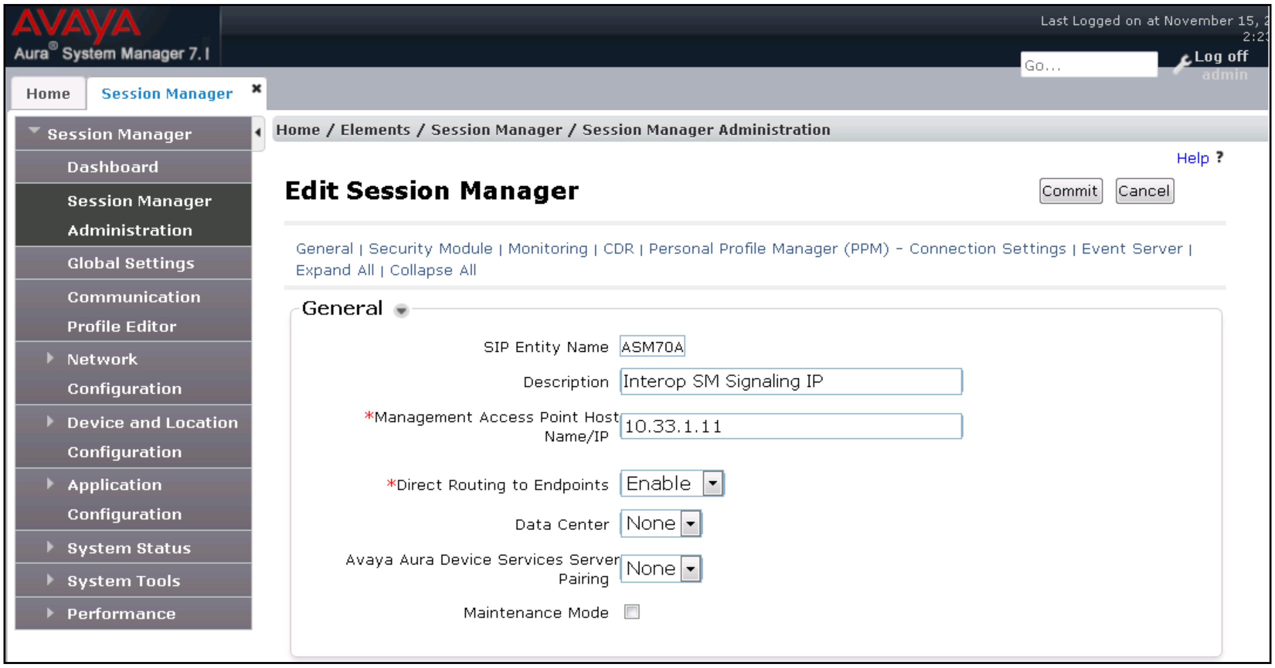
5.1. Log in to Avaya Aura® System Manager

Access the System Manager using a web browser and entering **http://<FQDN >/SMGR**, where <**FQDN**> is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the home page will be presented with menu options shown below.



5.2. Administer Call Detail Recording on Session Manager

From the home page of System Manager, navigate to **Elements → Session Manager**; the **Session Manager** tab is displayed. Select **Session Manager Administration** from the left pane and select a preconfigured Session Manager, for example "ASM70A" from list of Session Managers in the right hand side and then select **Edit** button (not shown) to edit. The **Edit Session Manager** is displayed as below.


AVAYA
Aura® System Manager 7.1
Last Logged on at November 15, 2
Go...
Log off
admin
Home
Session Manager
Session Manager
Dashboard
Session Manager Administration
Global Settings
Communication Profile Editor
Network Configuration
Device and Location Configuration
Application Configuration
System Status
System Tools
Performance
Home / Elements / Session Manager / Session Manager Administration
Help ?
Commit
Cancel
General | Security Module | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

Edit Session Manager

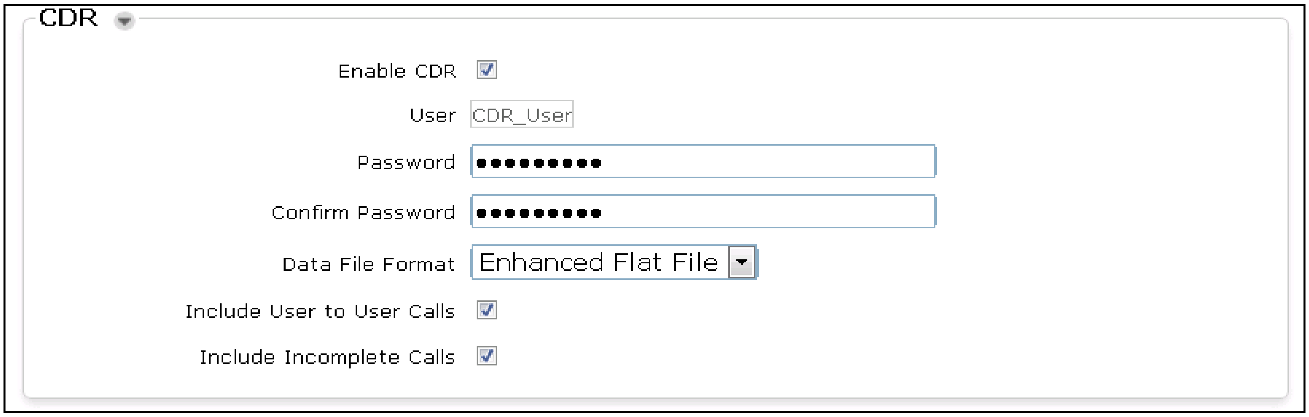
General

SIP Entity Name	ASM70A
Description	Interop SM Signaling IP
*Management Access Point Host Name/IP	10.33.1.11
*Direct Routing to Endpoints	Enable
Data Center	None
Avaya Aura Device Services Server Pairing	None
Maintenance Mode	□

Scroll down to the CDR section, and do the following:

- **Enable CDR**: select the check box to enable CDR feature on Session Manager
- **Password** and **Confirm Password**: enter a password for user "CDR_User"
- Keep other fields at default

On the completion, click **Commit** button to save the changes.

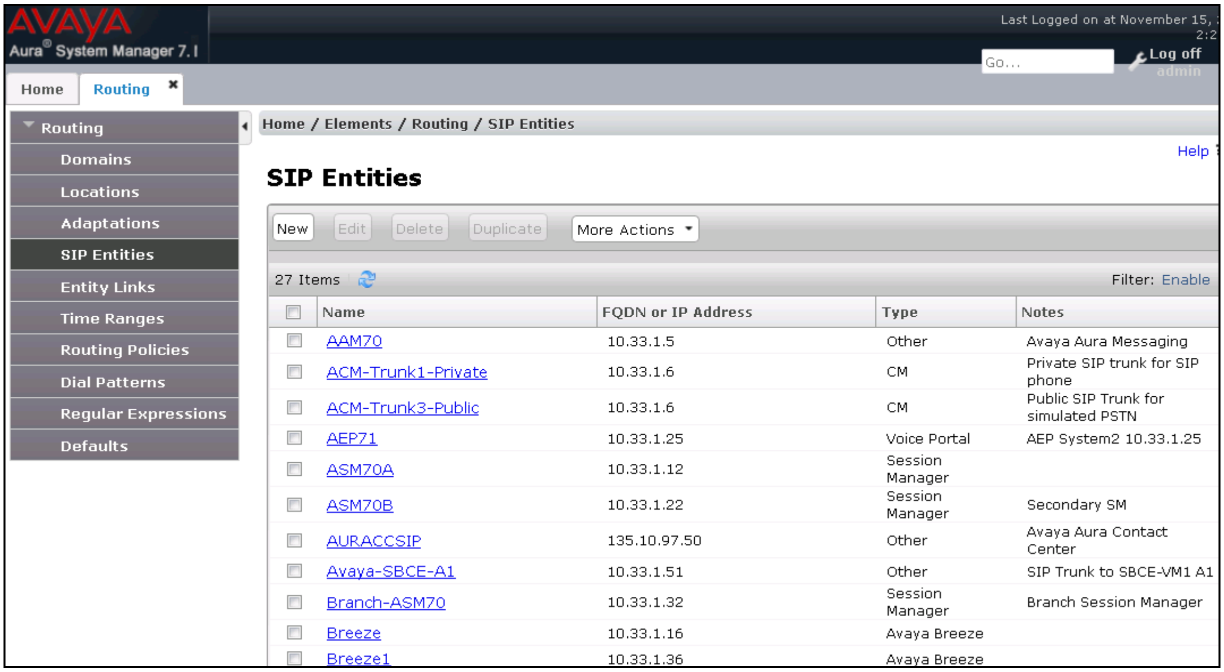


CDR

Enable CDR	☑
User	CDR_User
Password	●●●●●●●●●●
Confirm Password	●●●●●●●●●●
Data File Format	Enhanced Flat File
Include User to User Calls	☑
Include Incomplete Calls	☑

5.3. Administer Call Detail Recording on SIP Entity

From the home page of System Manager, navigate to **Elements → Routing**. The **Routing** tab is displayed with SIP Entities shown up in the right hand side of window.



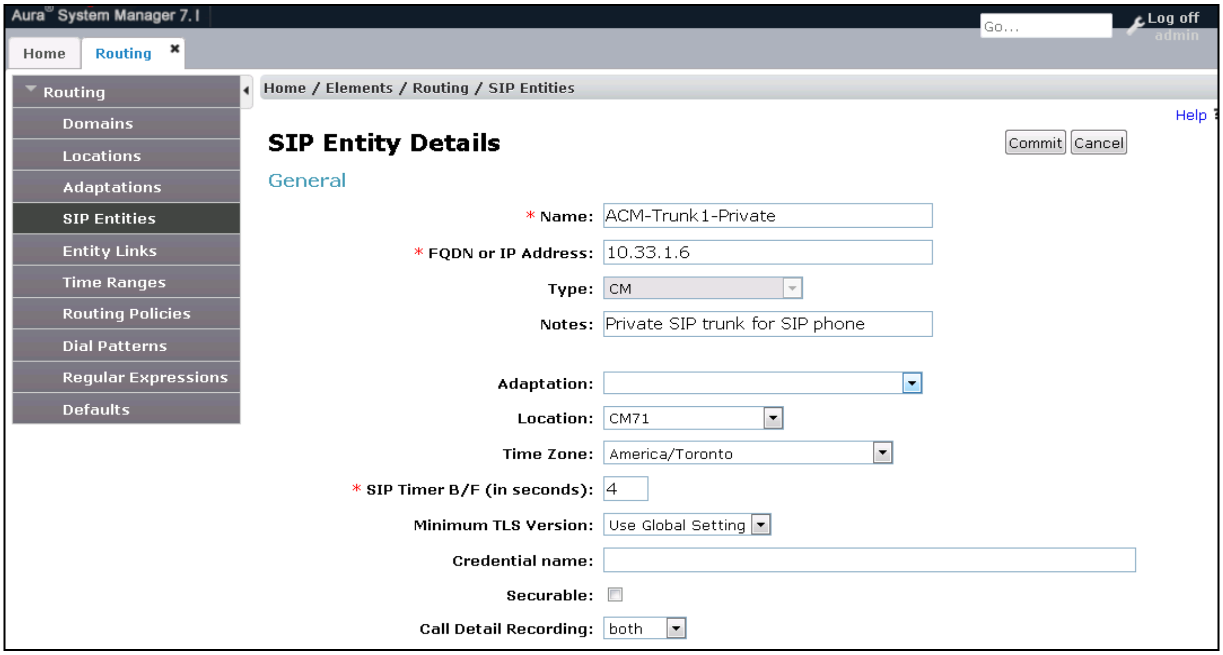
Home / Elements / Routing / SIP Entities

SIP Entities

27 Items

□	Name	FQDN or IP Address	Type	Notes
□	AAM70	10.33.1.5	Other	Avaya Aura Messaging
□	ACM-Trunk1-Private	10.33.1.6	CM	Private SIP trunk for SIP phone
□	ACM-Trunk3-Public	10.33.1.6	CM	Public SIP Trunk for simulated PSTN
□	AEP71	10.33.1.25	Voice Portal	AEP System2 10.33.1.25
□	ASM70A	10.33.1.12	Session Manager	
□	ASM70B	10.33.1.22	Session Manager	Secondary SM
□	AURACCSIP	135.10.97.50	Other	Avaya Aura Contact Center
□	Avaya-SBCE-A1	10.33.1.51	Other	SIP Trunk to SBCE-VM1 A1
□	Branch-ASM70	10.33.1.32	Session Manager	Branch Session Manager
□	Breeze	10.33.1.16	Avaya Breeze	
□	Breeze1	10.33.1.36	Avaya Breeze	

Select the "ACM-Trunk1-Private" SIP entity which is Communication Manager SIP entity and select "both" on the **Call Detail Recording** field. On the completion, click **Commit** button to save the change.



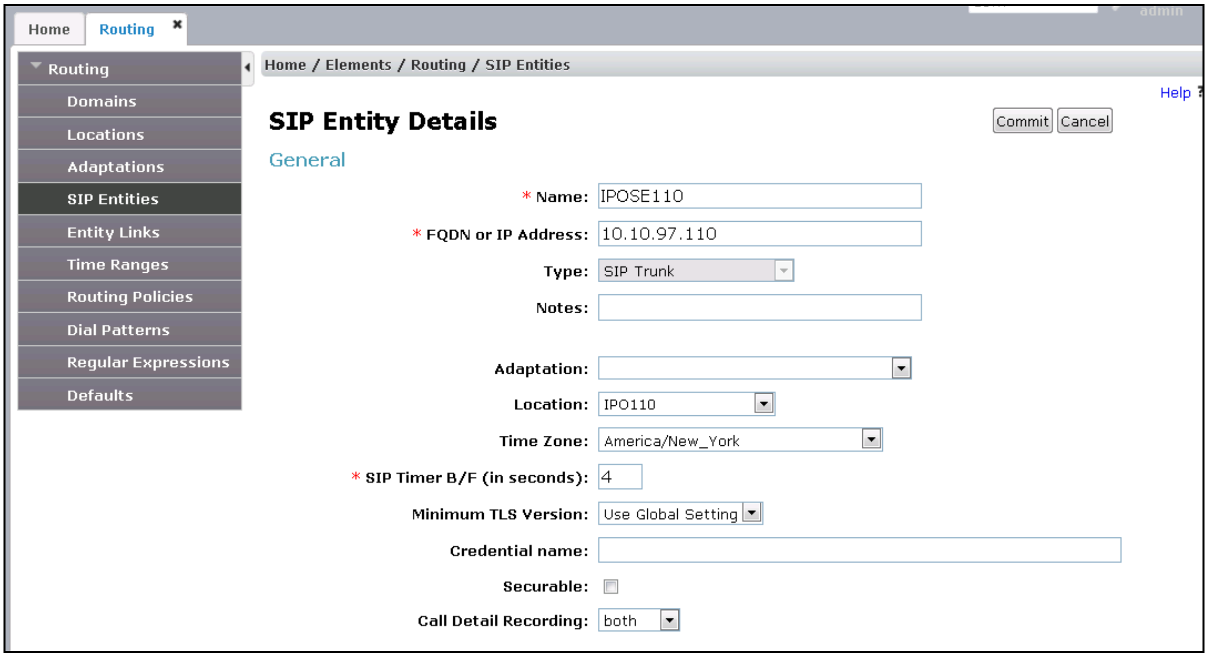
Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name:	ACM-Trunk1-Private
* FQDN or IP Address:	10.33.1.6
Type:	CM
Notes:	Private SIP trunk for SIP phone
Adaptation:	
Location:	CM71
Time Zone:	America/Toronto
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	both

Repeat the procedure above for another SIP entity that wishes Session Manager to log CDR. The example below is for Avaya IP Office performing as Site 2 as shown up in **Figure 1**.



SIP Entity Details

General

* Name:	IPOSE110
* FQDN or IP Address:	10.10.97.110
Type:	SIP Trunk
Notes:	
Adaptation:	
Location:	IPO110
Time Zone:	America/New_York
* SIP Timer B/F (in seconds):	4
Minimum TLS Version:	Use Global Setting
Credential name:	
Securable:	□
Call Detail Recording:	both

6. Configure Resource Software International Shadow CMS

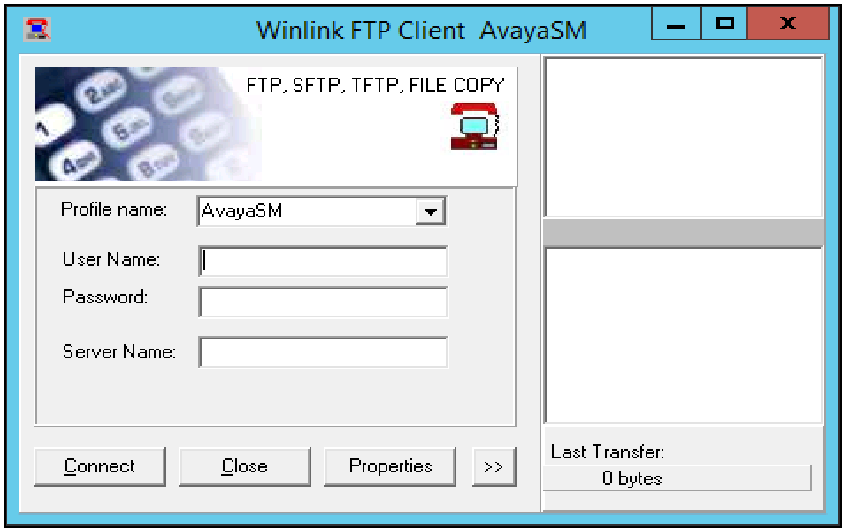
This section provides the procedures for configuring Shadow CMS. The procedures include the following areas:

- Administer Winlink FTP Client
- 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.

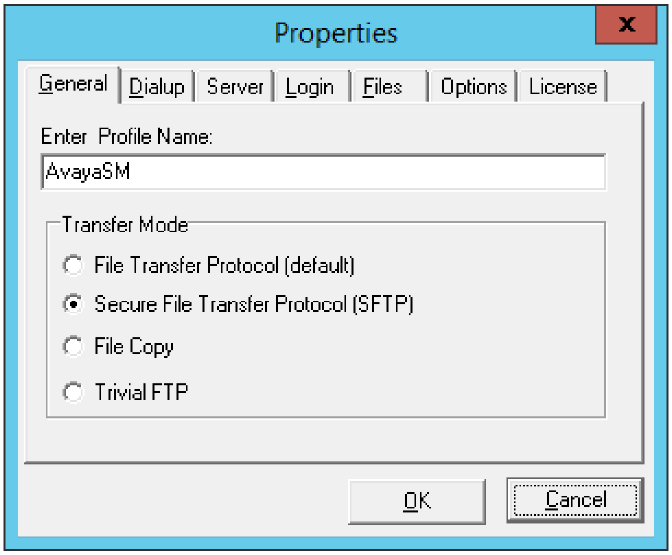
6.1. Administer Winlink FTP Client Utility

From the Shadow CMS server, launch **Winlink FTP Client** from the path C:\Program Files (x86)\RSI\Web CMS\winlink\WFTP. The **Winlink FTP Client** window is displayed as below. Select the **Properties** button to configure the Winlink FTP application.



Profile name: AvayaSM
User Name:
Password:
Server Name:
Last Transfer:
0 bytes

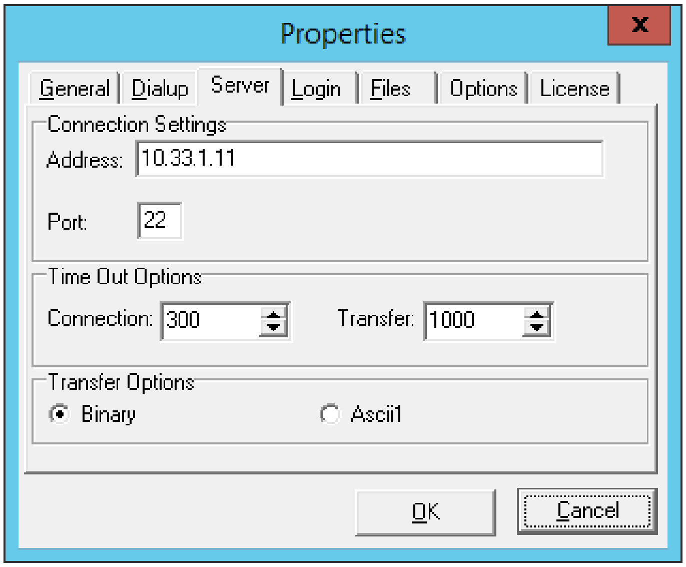
The **Properties** window is displayed, in the **General** tab, enter a name in the **Enter Profile Name** box, e.g. "AvayaSM", and select radio button "Secure File Transfer Protocol (SFTP)" in the **Transfer Mode** section.



Enter Profile Name:
AvayaSM

Transfer Mode
○ File Transfer Protocol (default)
● Secure File Transfer Protocol (SFTP)
○ File Copy
○ Trivial FTP

In the **Server** tab, enter the management IP address “10.33.1.11” of Session Manager in the **Address** box of **Connection Settings** section and keep other fields at default.



Connection Settings

Address: 10.33.1.11

Port: 22

Time Out Options

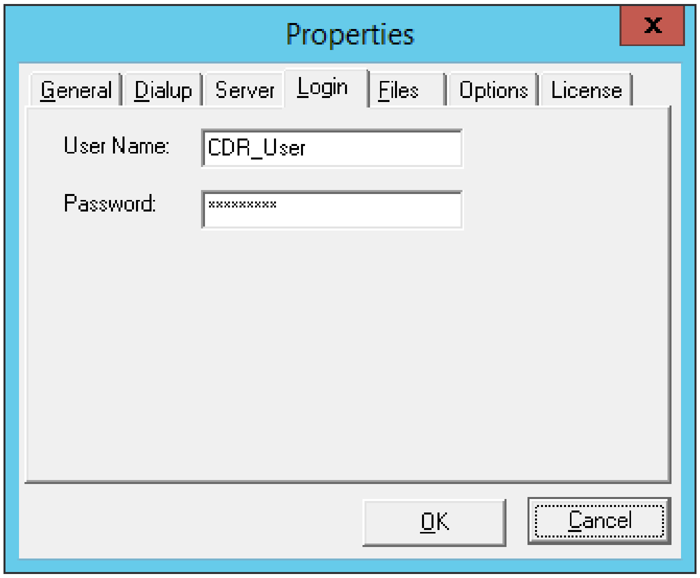
Connection: 300

Transfer: 1000

Transfer Options

● Binary ○ Ascii1

In the **Login** tab, enter the user name “CDR_User” and its password that is enabled in Session Manager as configured in **Section 5.2**.



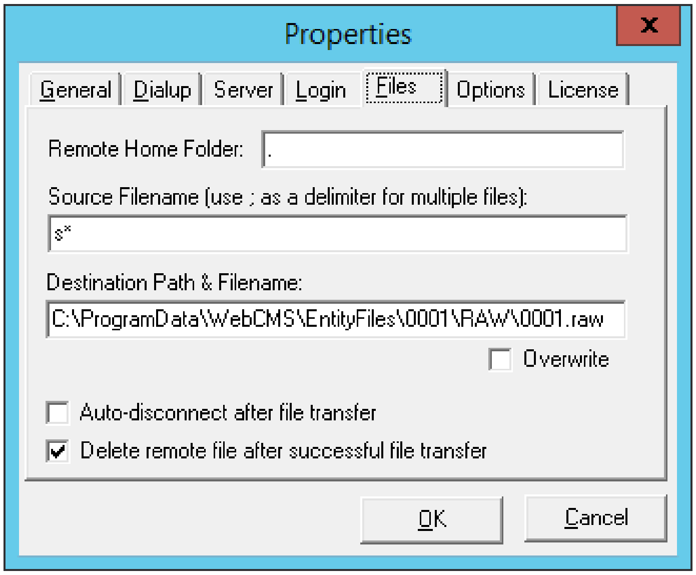
User Name: CDR_User

Password: **********

In the **Files** tab, do the following:

- **Remote Home Folder**: enter ".", the FTP client switches to home folder of CDR_User where the CDR file stored in Session Manager
- **Source Filename**: enter "s*" the FTP client get all CDR files starting with "s" letter
- **Destination Path and Filename**: enter a full path where the CDR files can be saved in the Shadow CMS server
- Check on the **Delete remote file after successful file transfer** check box, in order to delete the CDR file after it is copied to the Shadow CMS server. This will prevent the same CDR file from being retrieved by a subsequent FTP request (i.e. prevents call duplication in Shadow CMS)

On the completion, click OK button to save the changes.



Remote Home Folder: .

Source Filename (use ; as a delimiter for multiple files): s*

Destination Path & Filename: C:\ProgramData\WebCMS\EntityFiles\0001\RAW\0001.raw

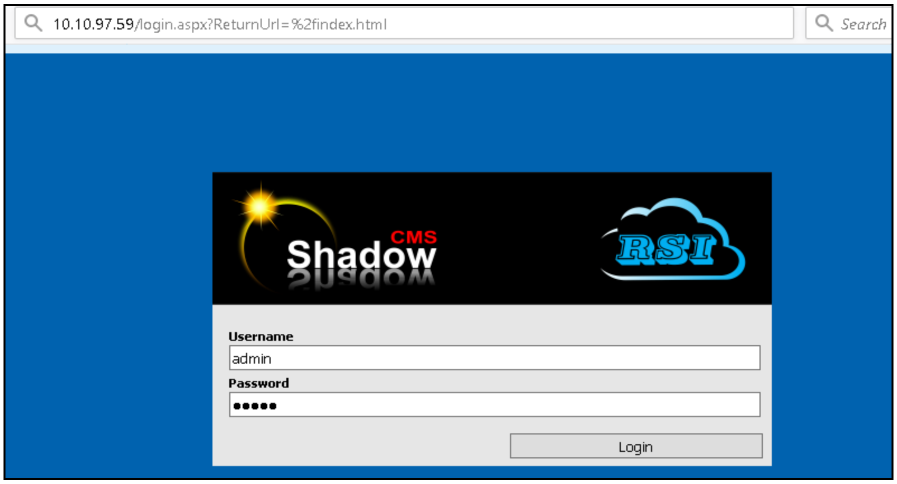
□ Overwrite

□ Auto-disconnect after file transfer

☑ Delete remote file after successful file transfer

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 on.



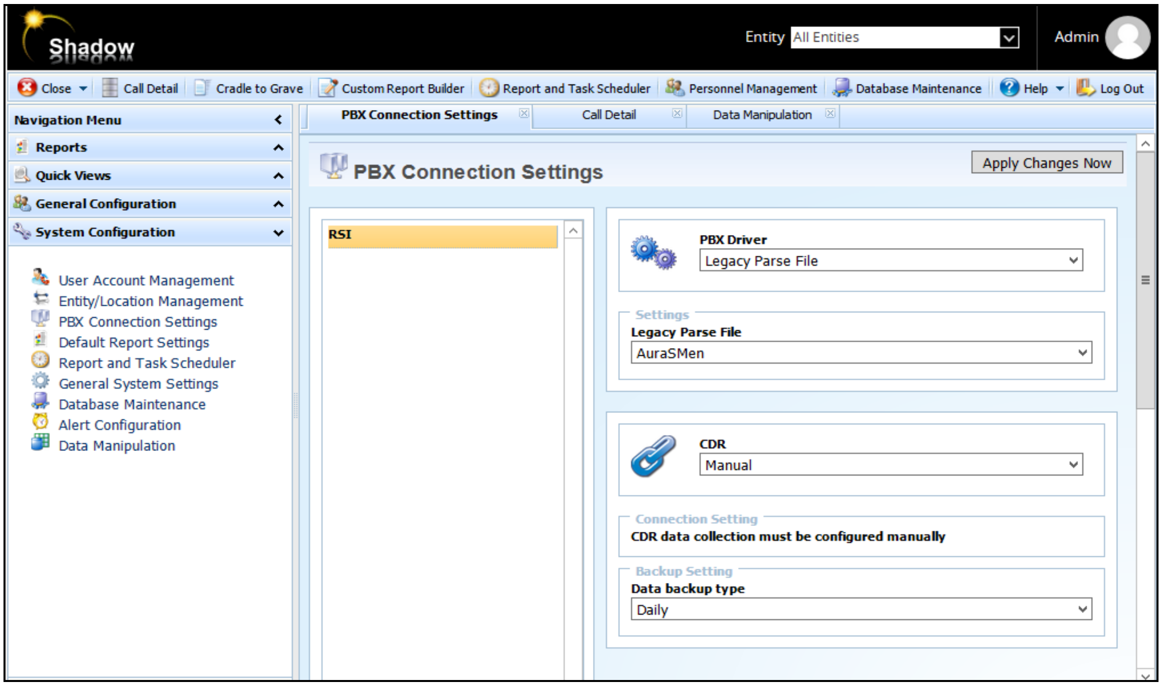
10.10.97.59/login.aspx?ReturnUrl=%2findex.html

Username: admin

Password: ●●●●●

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

- **PBX Driver**: select "Legacy Parse File" from the dropdown menu
- **Settings – Legacy Parse File**: select "AuraSMen" from the dropdown menu
- **CDR**: select "Manual" from the dropdown menu



PBX Connection Settings

RSI

PBX Driver: Legacy Parse File

Settings

Legacy Parse File: AuraSMen

CDR: Manual

Connection Setting

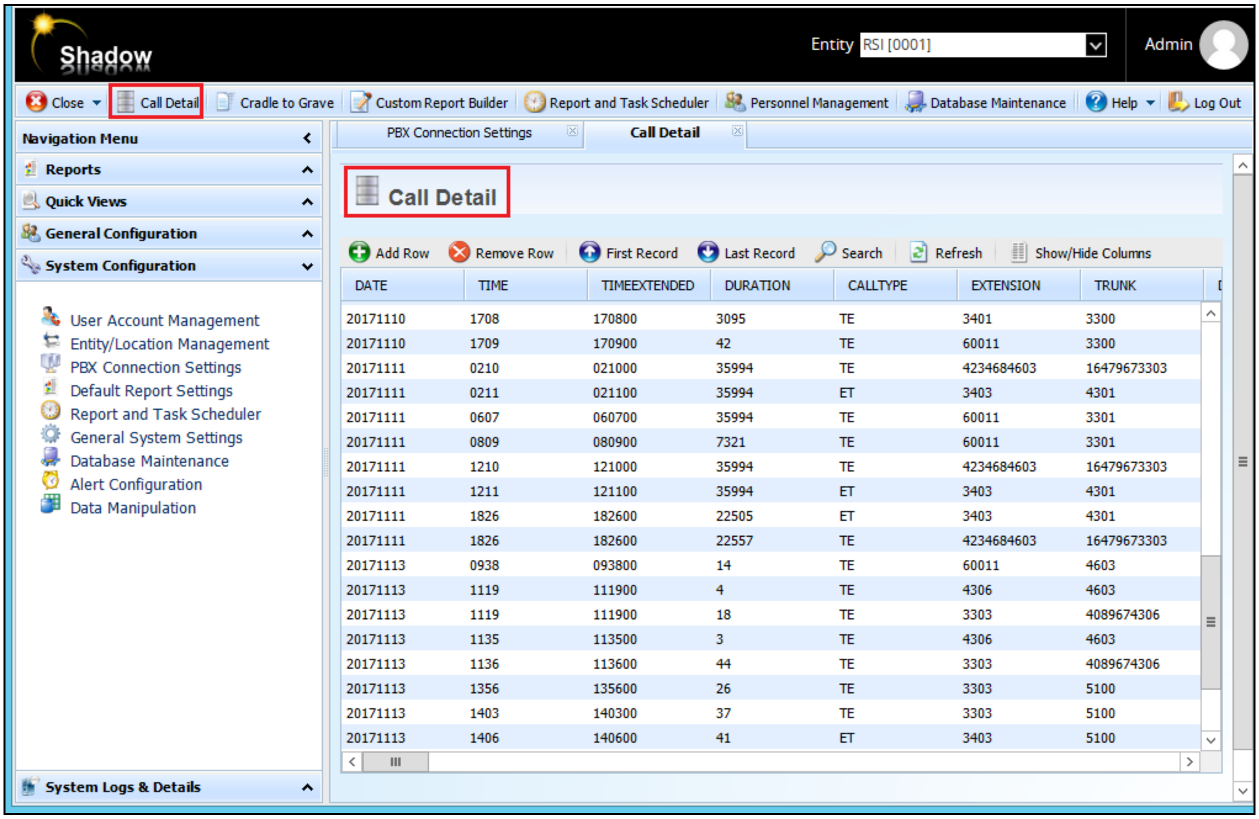
CDR data collection must be configured manually

Backup Setting

Data backup type: Daily

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 FTP Client application.

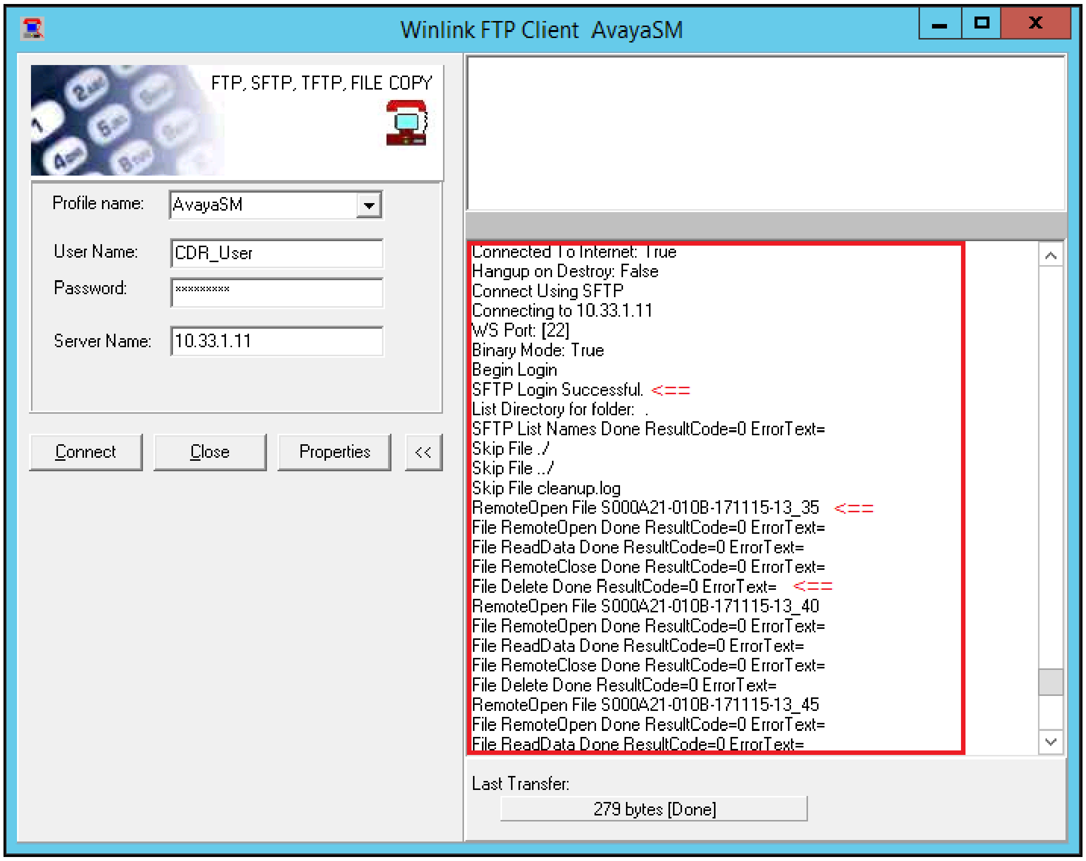


DATE	TIME	TIMEEXTENDED	DURATION	CALLTYPE	EXTENSION	TRUNK
20171110	1708	170800	3095	TE	3401	3300
20171110	1709	170900	42	TE	60011	3300
20171111	0210	021000	35994	TE	4234684603	16479673303
20171111	0211	021100	35994	ET	3403	4301
20171111	0607	060700	35994	TE	60011	3301
20171111	0809	080900	7321	TE	60011	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:

- From the **Winlink FTP Client**, select **Connect** button to perform SFTP connection to Session Manager. The right hand side of window shows the status, it should show no Error during the session.



Profile name: AvayaSM

User Name: CDR_User

Password: **********

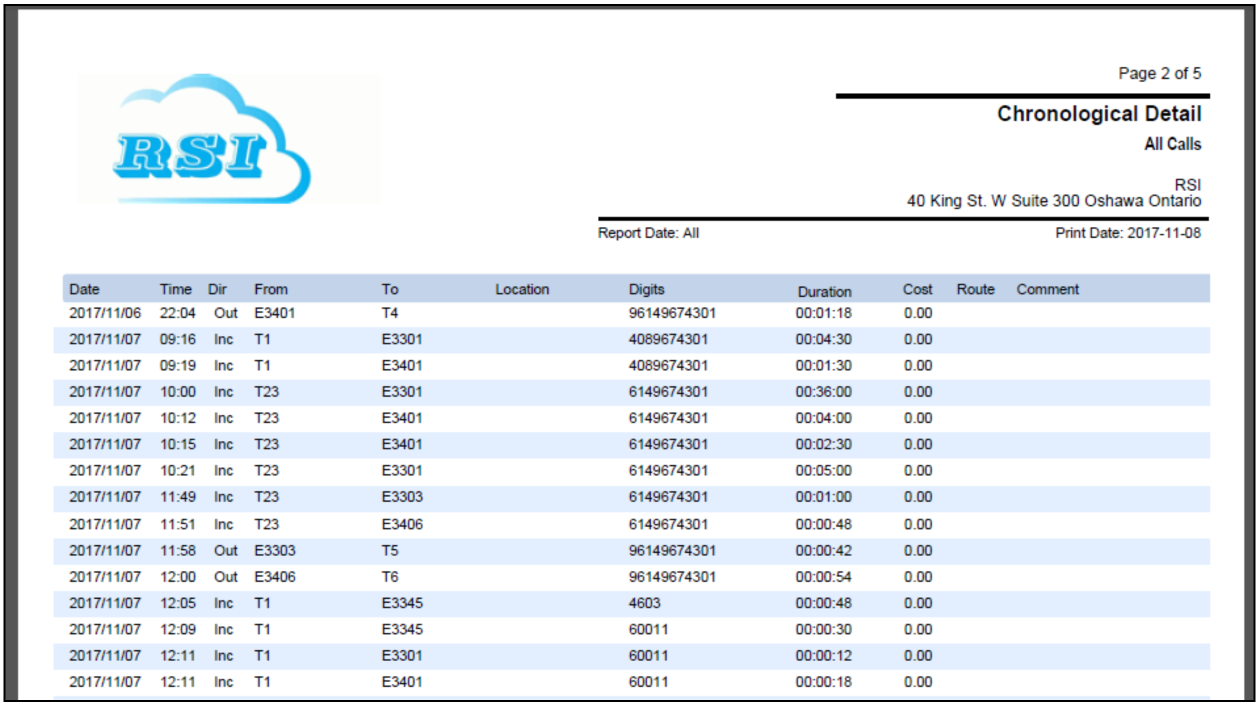
Server Name: 10.33.1.11

```
Connected To Internet: True
Hangup on Destroy: False
Connect Using SFTP
Connecting to 10.33.1.11
WS Port: [22]
Binary Mode: True
Begin Login
SFTP Login Successful.  <==
List Directory for folder:  .
SFTP List Names Done ResultCode=0 ErrorText=
Skip File ./
Skip File ../
Skip File cleanup.log
RemoteOpen File S000A21-010B-171115-13_35   <==
File RemoteOpen Done ResultCode=0 ErrorText=
File ReadData Done ResultCode=0 ErrorText=
File RemoteClose Done ResultCode=0 ErrorText=
File Delete Done ResultCode=0 ErrorText=   <==
RemoteOpen File S000A21-010B-171115-13_40
File RemoteOpen Done ResultCode=0 ErrorText=
File ReadData Done ResultCode=0 ErrorText=
File RemoteClose Done ResultCode=0 ErrorText=
File Delete Done ResultCode=0 ErrorText=
RemoteOpen File S000A21-010B-171115-13_45
File RemoteOpen Done ResultCode=0 ErrorText=
File ReadData Done ResultCode=0 ErrorText=
```

Last Transfer:

279 bytes [Done]

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



Page 2 of 5

Chronological Detail

All Calls

RSI
40 King St. W Suite 300 Oshawa Ontario

Report Date: All

Print Date: 2017-11-08

Date	Time	Dir	From	To	Location	Digits	Duration	Cost	Route	Comment
2017/11/06	22:04	Out	E3401	T4		96149674301	00:01:18	0.00		
2017/11/07	09:16	Inc	T1	E3301		4089674301	00:04:30	0.00		
2017/11/07	09:19	Inc	T1	E3401		4089674301	00:01:30	0.00		
2017/11/07	10:00	Inc	T23	E3301		6149674301	00:36:00	0.00		
2017/11/07	10:12	Inc	T23	E3401		6149674301	00:04:00	0.00		
2017/11/07	10:15	Inc	T23	E3401		6149674301	00:02:30	0.00		
2017/11/07	10:21	Inc	T23	E3301		6149674301	00:05:00	0.00		
2017/11/07	11:49	Inc	T23	E3303		6149674301	00:01:00	0.00		
2017/11/07	11:51	Inc	T23	E3406		6149674301	00:00:48	0.00		
2017/11/07	11:58	Out	E3303	T5		96149674301	00:00:42	0.00		
2017/11/07	12:00	Out	E3406	T6		96149674301	00:00:54	0.00		
2017/11/07	12:05	Inc	T1	E3345		4603	00:00:48	0.00		
2017/11/07	12:09	Inc	T1	E3345		60011	00:00:30	0.00		
2017/11/07	12:11	Inc	T1	E3301		60011	00:00:12	0.00		
2017/11/07	12:11	Inc	T1	E3401		60011	00:00:18	0.00		

8. Conclusion

These Application Notes describe the procedures for configuring Resource Software International Shadow CMS with Avaya Aura® Session 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.

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10, Release 7.1, August 2017

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Issue 9.0, Release 7.1, August 2017

[3] *Administering Avaya Aura® Session Manager*, Release 7.1, Issue 4 August 2017

[4] *Administering Avaya Aura® System Manager*, Release 7.1, Issue 4, August, 2017

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

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.