



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 the 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 files 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 8.0. Shadow CMS collects CDR files from Session Manager over the local or wide area network using a secure file transfer protocol (SFTP). Avaya Aura® 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 Avaya Aura® 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 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 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 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 Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, 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 has SIP Trunk to Session Manager, Session Manager terminates SIP trunk from both Communication Manager and IP Office.

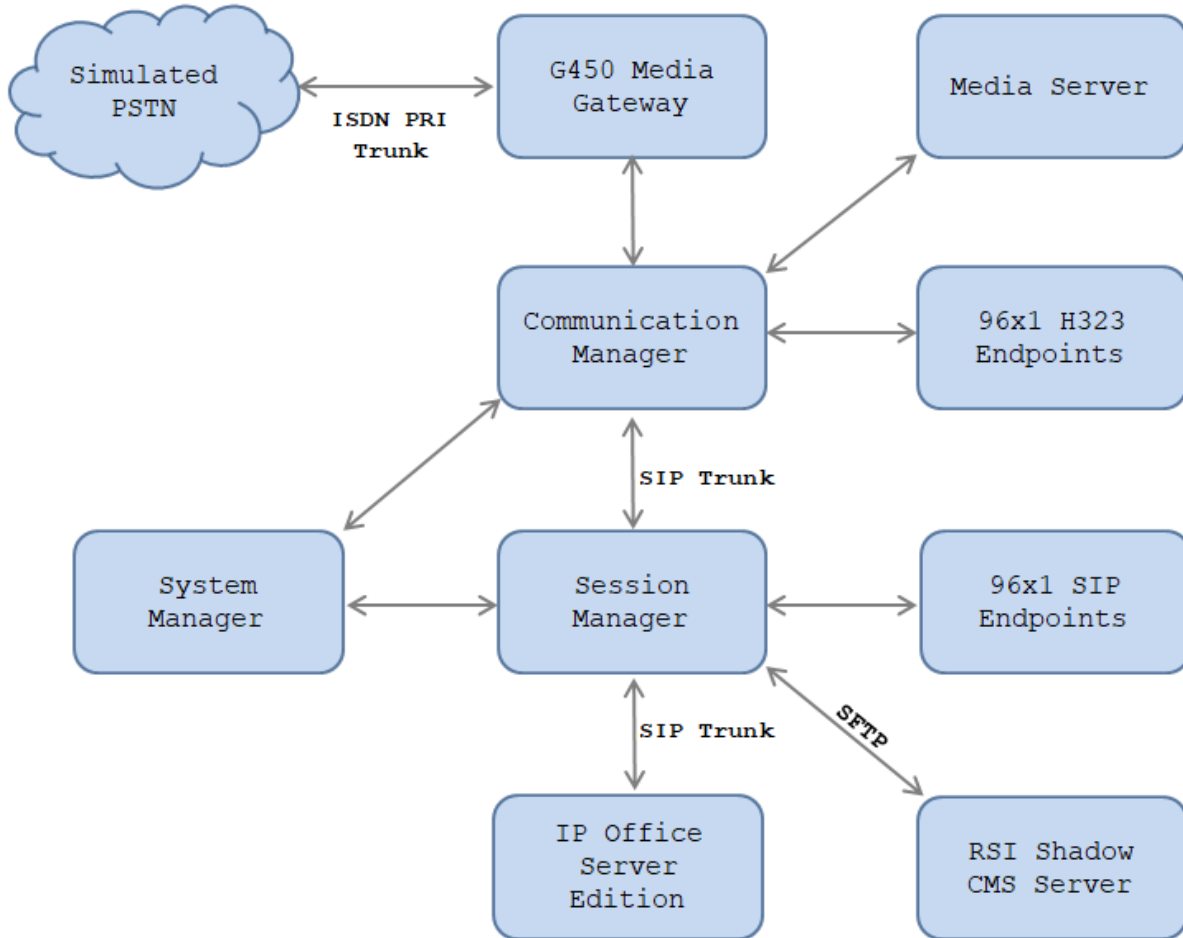


Figure 1: Test Configuration Diagram

The following table indicates the IP addresses that were assigned to the systems in the test configuration diagram:

| Description | IP Address |
|---------------------------|-------------------------|
| System Manager | 10.33.1.10 |
| Session Manager Signaling | 10.33.1.12 |
| IP Office Server Edition | 10.10.97.110 |
| Communication Manager | 10.33.1.6 |
| Media Server | 10.33.1.30 |
| G450 Media Gateway | 10.33.1.40 |
| Avaya 96x1 Endpoints | 10.33.5.45 – 10.33.5.50 |
| RSI Shadow CMS Server | 10.10.97.59 |

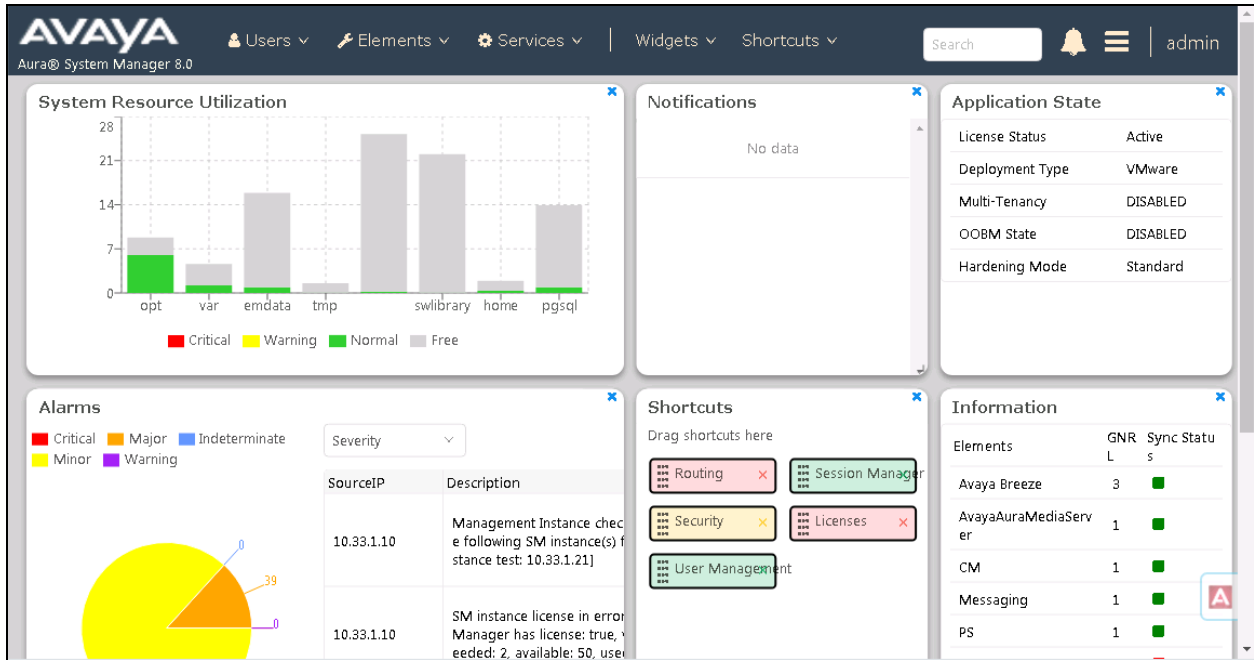
4. Equipment and Software Validated

The following equipment and software/firmware were used for the test configuration.

| Equipment/Software | Release/Version |
|--|---------------------------|
| Avaya Aura® System Manager running on virtualized environment | 8.0.1.0 8.0.1.0.038826 |
| Avaya Aura® Session Manager running on virtualized environment | 8.0.1.0 8.0.1.0.801007 |
| Avaya Aura® Communication Manager running on virtualized environment | 8.0.1.0 |
| Avaya IP Office Server Edition | 11.0.2 |
| Avaya 96x1 H.323 | 6.714 |
| Avaya 96x1 SIP Deskphones | 7.1.4.0.11 |
| RSI Shadow CMS running on Virtualized Environment | 5.2.3 |

5. 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** tab will be presented with menu options shown below.



5.1. Administer Call Detail Recording on Session Manager

From the homepage 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 desired Session Manager entity, for example “ASM70A” from list of Session Manager entity in the right hand side and then select **Edit** button (not shown) to edit. The Edit Session Manager screen is displayed as below.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows 'Session Manager Administration' selected. The main content area is titled 'Edit Session Manager' and contains the following configuration fields:

- General**
 - SIP Entity Name:
 - Description:
 - *Management Access Point Host Name/IP:
 - *Direct Routing to Endpoints:
 - Data Center:
 - Avaya Aura Device Services Server Pairing:
 - Maintenance Mode:
- Security Module**
- CDR** (highlighted in the image below)

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

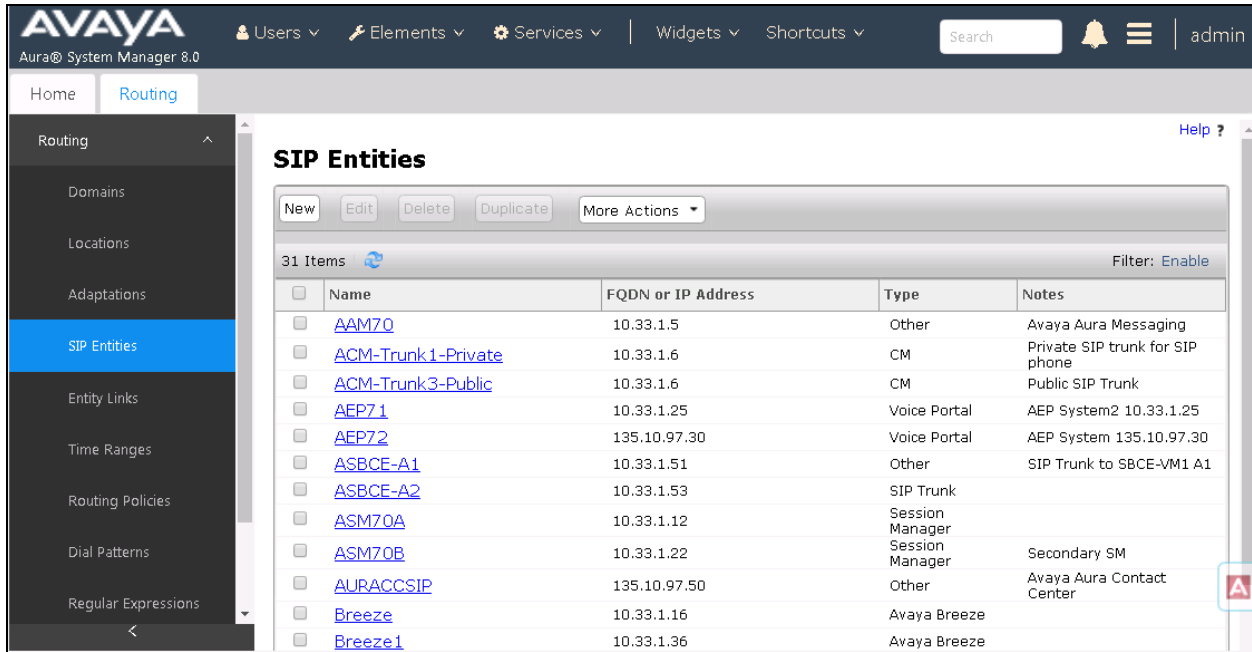
On the completion, click **Commit** button (not shown) to save the changes.

The CDR configuration section is shown with the following settings:

- Enable CDR:
- User:
- Password:
- Confirm Password:
- Data File Format:
- Include User to User Calls:
- Include Incomplete Calls:

5.2. Administer Call Detail Recording on SIP Entity

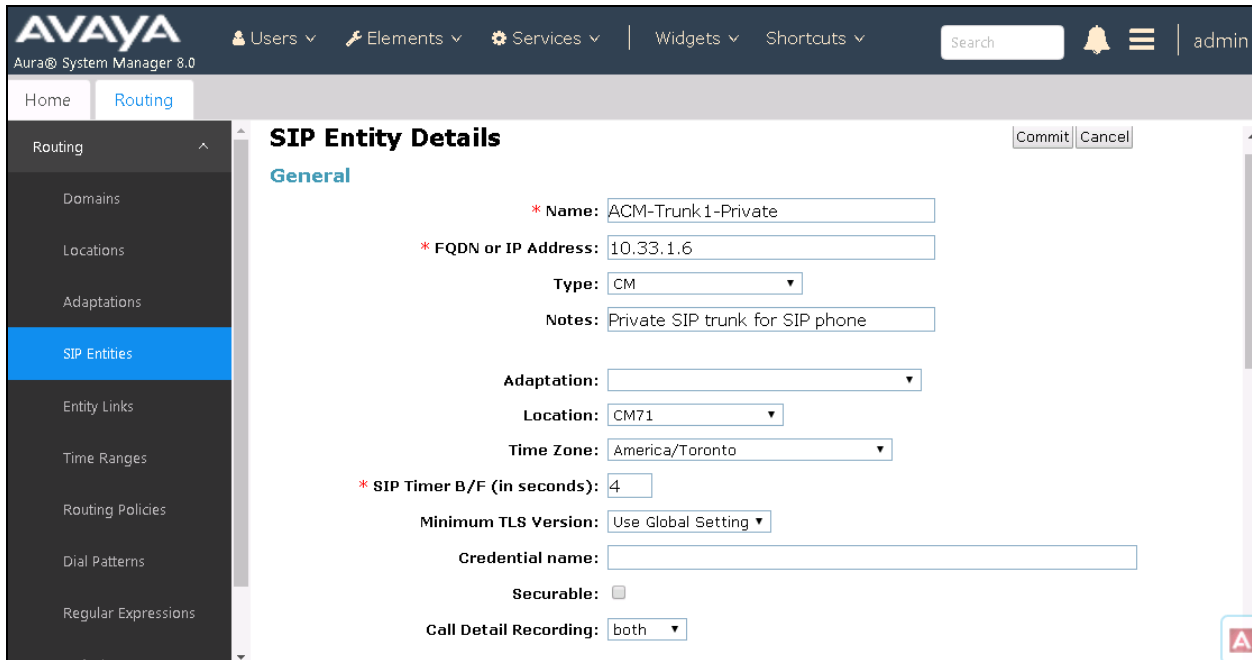
From the home page of System Manager, navigate to **Elements** → **Routing**. The **Routing** tab is displayed with SIP Entities shown in the right hand side of window.



The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar is expanded to the 'Routing' section, with 'SIP Entities' selected. The main content area displays a table of 31 SIP entities. The table has columns for Name, FQDN or IP Address, Type, and Notes. The 'ACM-Trunk1-Private' entity is highlighted in blue.

| 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 |
| AEP71 | 10.33.1.25 | Voice Portal | AEP System2 10.33.1.25 |
| AEP72 | 135.10.97.30 | Voice Portal | AEP System 135.10.97.30 |
| ASBCE-A1 | 10.33.1.51 | Other | SIP Trunk to SBCE-VM1 A1 |
| ASBCE-A2 | 10.33.1.53 | SIP Trunk | |
| 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 |
| 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.



The screenshot shows the Avaya Aura System Manager 8.0 interface with the 'SIP Entity Details' form open for the 'ACM-Trunk1-Private' entity. The 'General' tab is active, and the 'Call Detail Recording' field is set to 'both'. The 'Commit' button is visible at the top right of the form.

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: [Dropdown]

Location: CM71

Time Zone: America/Toronto

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

Minimum TLS Version: Use Global Setting

Credential name: [Text Field]

Securable: [Checkbox]

Call Detail Recording: both

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

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes the Avaya logo, user information (Users), and various menu options (Elements, Services, Widgets, Shortcuts). A search bar and a notification bell are also present. The main content area is titled "SIP Entity Details" and is currently on the "General" tab. The configuration fields are as follows:

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

Buttons for "Commit" and "Cancel" are visible at the top right of the form. A "Help ?" link is also present. The left sidebar shows a navigation menu with "SIP Entities" selected.

6. Configure Resource Software International Shadow CMS

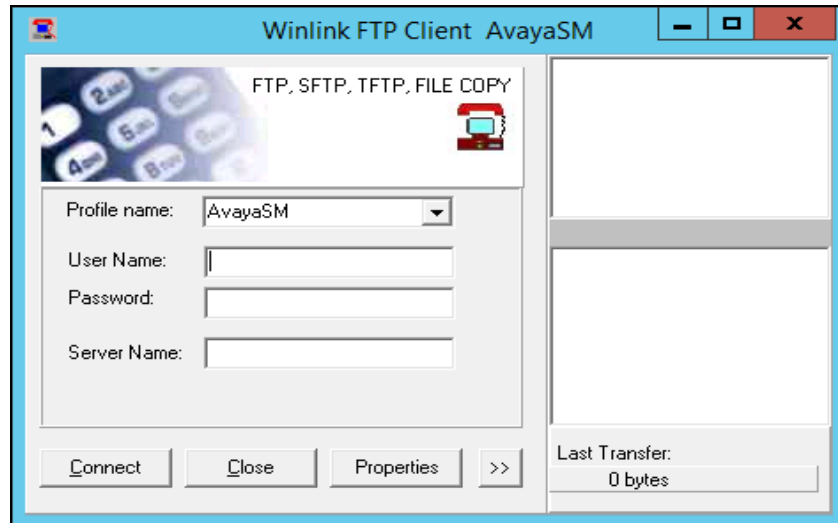
This section provides the procedures for configuring Shadow CMS. The procedures include the following areas:

- Administer Winlink FTP Client
- Administer CDR Driver
- Verify CDR Data

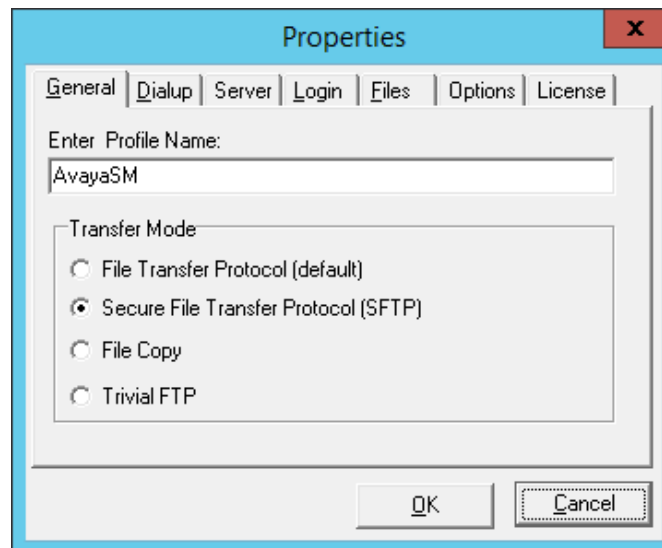
The configuration of Shadow CMS is typically performed by RSI Support Services. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Administer Winlink FTP Client Utility

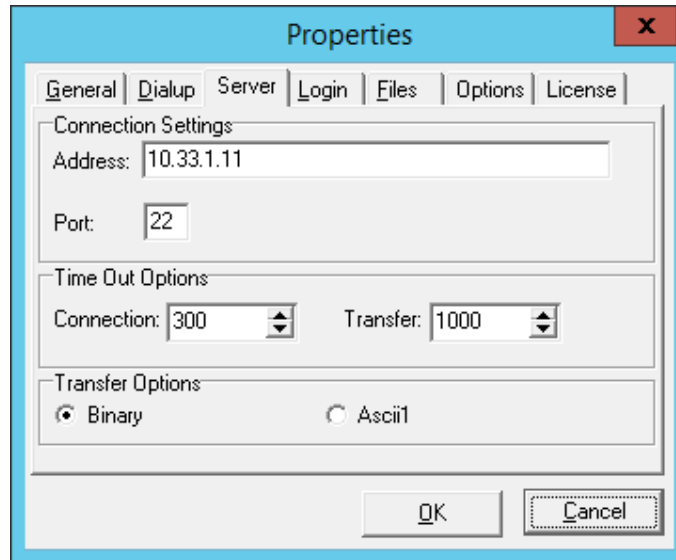
From the Shadow CMS server, launch **Winlink** FTP Client from the path C:\Program Files (x86)\RSI\Web CMS\winlink\WFTP. The **Winlink FTP Client** window is displayed as below. Select the **Properties** button to configure the Winlink FTP application.



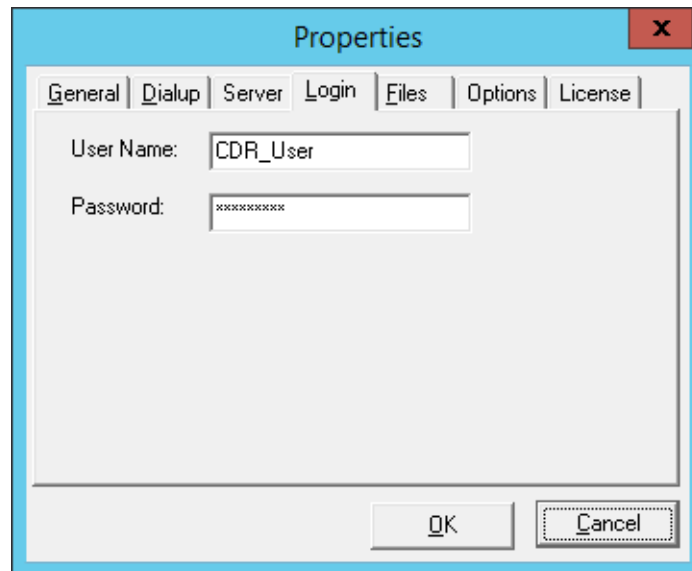
The Properties window is displayed, in the General tab, enter a name in the **Enter Profile Name** box, e.g. "AvayaSM", and select radio button "Secure File Transfer Protocol (SFTP)" in the **Transfer Mode** section.



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.



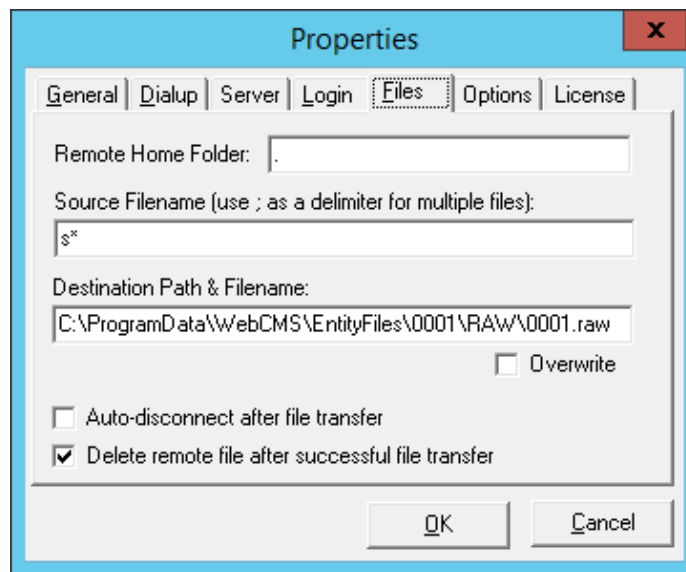
In the Login tab, enter the user name “CDR_User” and its password that is enabled in Session Manager as configured in **Section 5.2**.



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

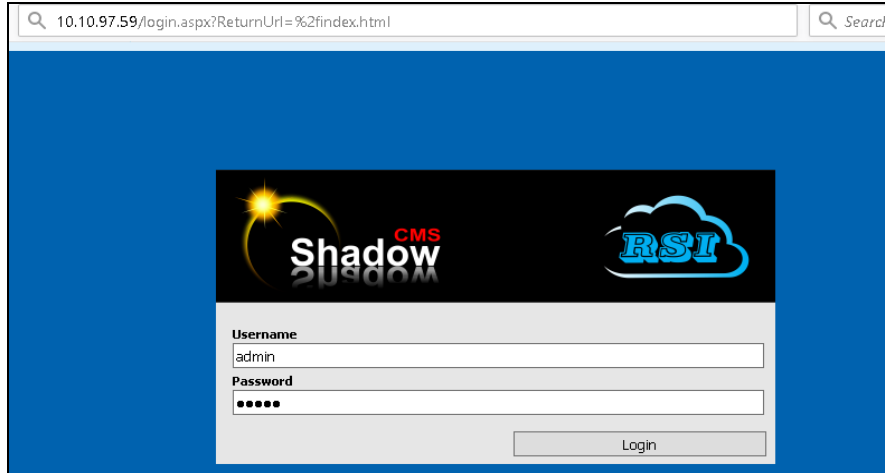
- **Remote Home Folder:** enter “.”, the FTP client switches to home folder of CDR_User where the CDR file stored in Session Manager
- **Source Filename:** enter “s*”, the FTP client get all CDR files starting with “s” letter
- **Destination Path and Filename:** enter a full path where the CDR files 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.



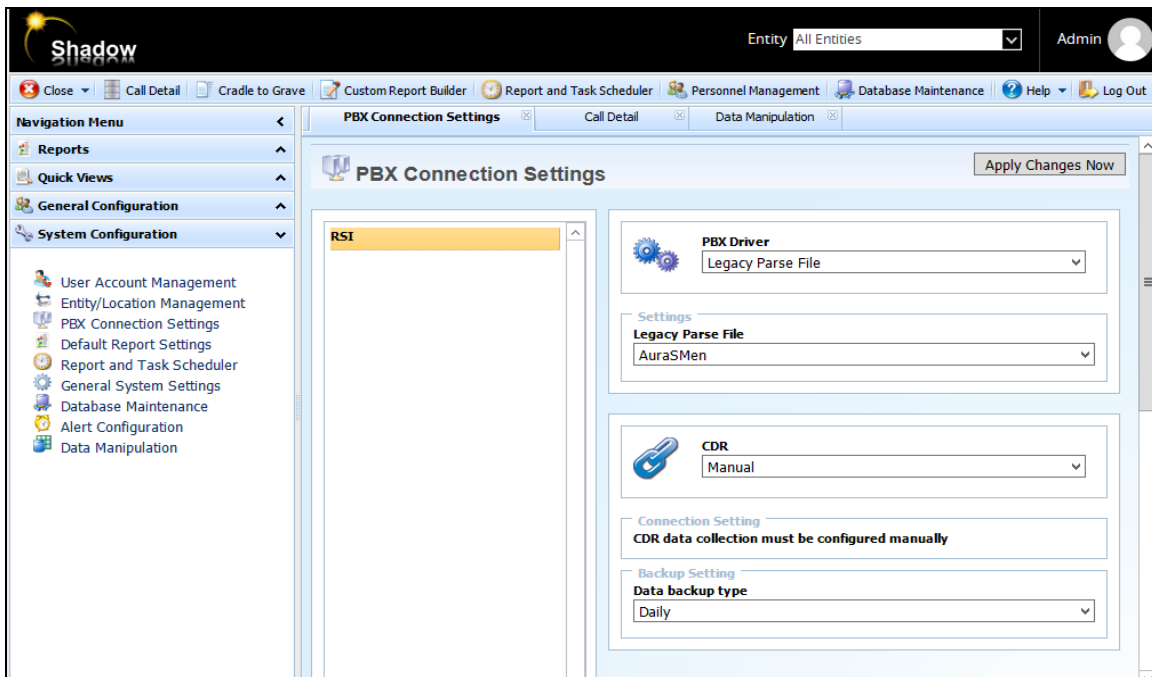
6.2. Administer CDR Driver

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.



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 “AuraSMen” 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 FTP Client application.

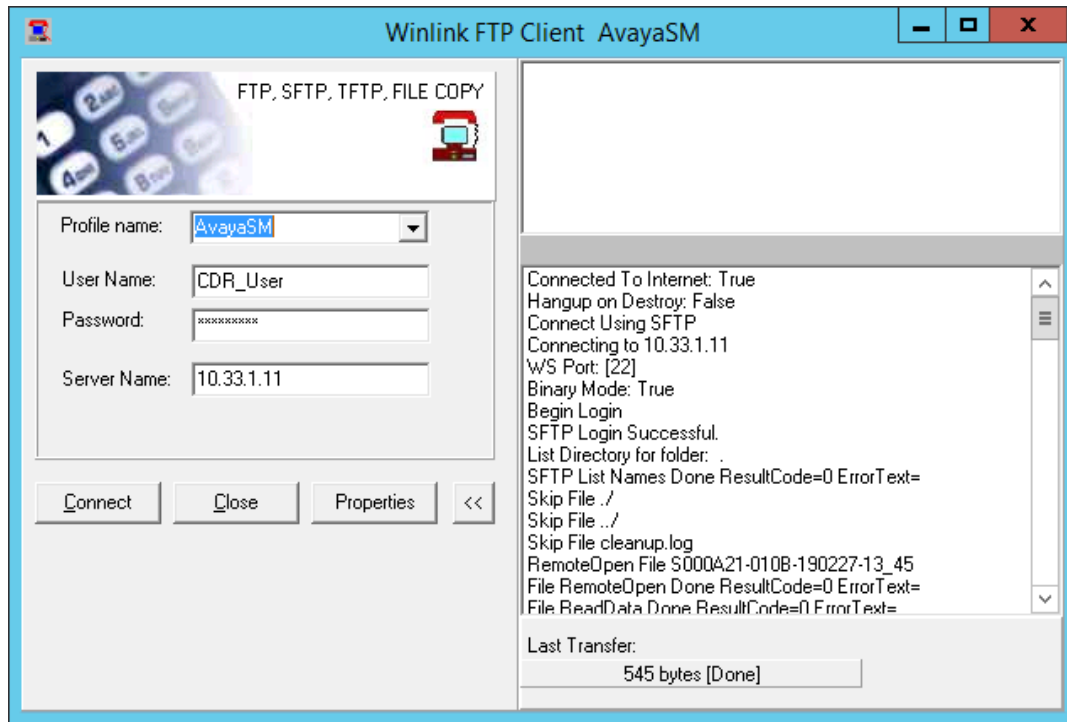
The screenshot shows the Shadow CMS application interface. The top right corner displays the user 'Admin' and the entity 'Avaya Devconnect [0001]'. The main window is titled 'Call Detail' and contains a table of CDR records. The table has the following columns: DATE, TIME, TIMEEXTENDED, DURATION, CALLTYPE, EXTENSION, TRUNK, and DIGITS. The data rows show various call records with their respective timestamps and durations.

| DATE | TIME | TIMEEXTENDED | DURATION | CALLTYPE | EXTENSION | TRUNK | DIGITS |
|----------|------|--------------|----------|----------|-------------|------------|------------|
| 20190227 | 1325 | 132500 | 20 | ET | 3401 | 4801 | 4801 |
| 20190227 | 1326 | 132600 | 38 | TE | 3303 | 4303 | 4303 |
| 20190227 | 1341 | 134100 | 70 | ET | 3403 | 3301 | 3301 |
| 20190227 | 1342 | 134200 | 23 | TE | 3403 | 3301 | 3301 |
| 20190227 | 1347 | 134700 | 5 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190227 | 1858 | 185800 | 5940 | ET | 3406 | 3402 | 3402 |
| 20190228 | 0120 | 012000 | 222 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0125 | 012500 | 40 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0131 | 013100 | 160 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0146 | 014600 | 40 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0150 | 015000 | 40 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0159 | 015900 | 391 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0213 | 021300 | 40 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0219 | 021900 | 40 | TE | 16137717498 | 5872330370 | 5872330370 |
| 20190228 | 0226 | 022600 | 40 | TE | 16137717498 | 5872330370 | 5872330370 |


7. Verification Steps

The following steps may be used to verify the configuration:

- From the Winlink FTP Client application, select **Connect** button to do SFTP to Session Manager. The right hand side of window shows the status of how SFTP session is going, it should show no Error text during the session.



- 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 5 of 6

Chronological Detail
All Calls
Avaya Devconnect

Report Date: All
Print Date: 2019-02-28

| Date | Time | Dir | From | To | Location | Digits | Duration | Cost | Route | Comment |
|------------|-------|-----|-------------|--------------|----------|--------------|----------|------|-------|---------|
| 2019/02/26 | 01:21 | Inc | T3301 | E4300 | | 3301 | 00:00:48 | 0.00 | INC | |
| 2019/02/26 | 01:21 | Inc | T3303 | E4402 | | 3303 | 00:00:44 | 0.00 | INC | |
| 2019/02/26 | 01:22 | Out | E3401 | T3301 | | 3301 | 00:00:46 | 0.00 | INV | |
| 2019/02/26 | 01:24 | Out | E3403 | T4303 | | 4303 | 00:00:49 | 0.00 | INV | |
| 2019/02/26 | 01:25 | Inc | T3303 | E3403 | | 3303 | 00:00:50 | 0.00 | INC | |
| 2019/02/26 | 06:23 | Inc | T4303 | E3403 | | 4303 | 04:55:23 | 0.00 | INC | |
| 2019/02/26 | 07:57 | Inc | T3301 | E4300 | | 3301 | 06:29:47 | 0.00 | INC | |
| 2019/02/26 | 11:03 | Inc | T6137717498 | E5872330370 | | 613 771-7498 | 00:00:56 | 0.00 | INC | |
| 2019/02/26 | 11:49 | Inc | T6137717498 | E5872330370 | | 613 771-7498 | 00:00:54 | 0.00 | INC | |
| 2019/02/26 | 12:16 | Inc | T6137717498 | E5872330370 | | 613 771-7498 | 00:22:26 | 0.00 | INC | |
| 2019/02/26 | 12:54 | Out | E3401 | T16139092719 | | 613 909-2719 | 00:00:22 | 0.00 | LD01 | |
| 2019/02/26 | 12:55 | Inc | T6139092719 | E5872330371 | | 613 909-2719 | 00:00:12 | 0.00 | INC | |
| 2019/02/26 | 12:56 | Inc | T6139092719 | E5872330371 | | 613 909-2719 | 00:00:21 | 0.00 | INC | |
| 2019/02/26 | 22:59 | Out | E3406 | T3402 | | 3402 | 09:59:54 | 0.00 | INV | |
| 2019/02/27 | 02:07 | Inc | T6139092719 | E5872330371 | | 613 909-2719 | 00:00:41 | 0.00 | INC | |
| 2019/02/27 | 02:15 | Inc | T6139092719 | E5872330371 | | 613 909-2719 | 00:00:28 | 0.00 | INC | |

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. Product documentation for Avaya Aura® Communication Manager, including the following, is available at: <http://support.avaya.com/>

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

[2] *Administering Avaya Aura® System Manager*, 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>

©2019 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.