Avaya Solution & Interoperability Test Lab

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

Abstract

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

Resource Software International Shadow Enterprise 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 Resource Software International Shadow Enterprise CMS (hereafter referred as Shadow CMS) software can interoperate with Avaya Aura® Session Manager 10.1. Shadow CMS collects CDR files from Session Manager over the local or wide area network using 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 business. 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 and 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 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 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, 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 were verified and 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 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 (CDR) files from Session Manager via SFTP.

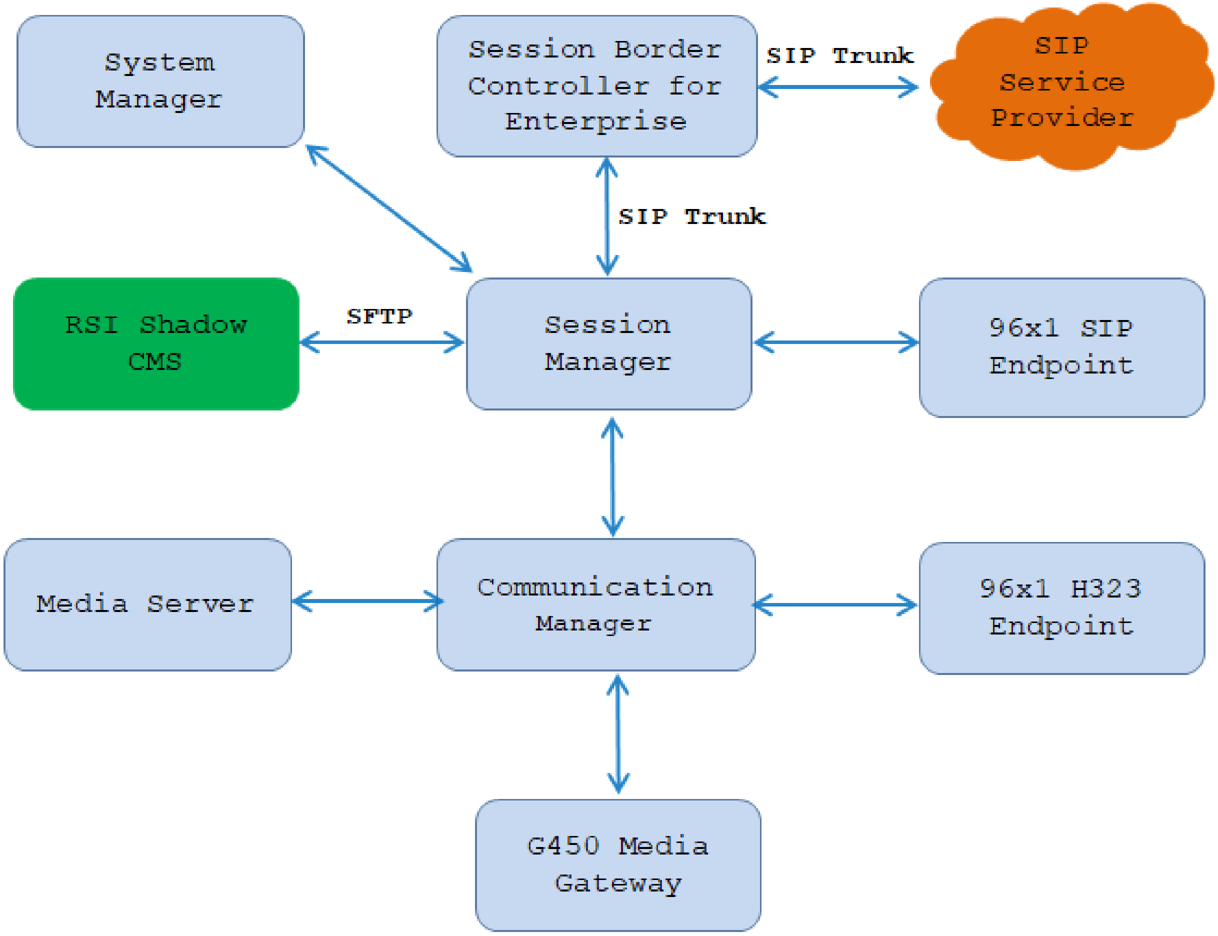


Figure 1: Test Configuration Diagram

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® Application Enablement Services running on virtualized environment	10.1 10.1.0.0.0.11
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
Resource Software International Shadow Enterprise CMS running on Windows 2016	5.4.0

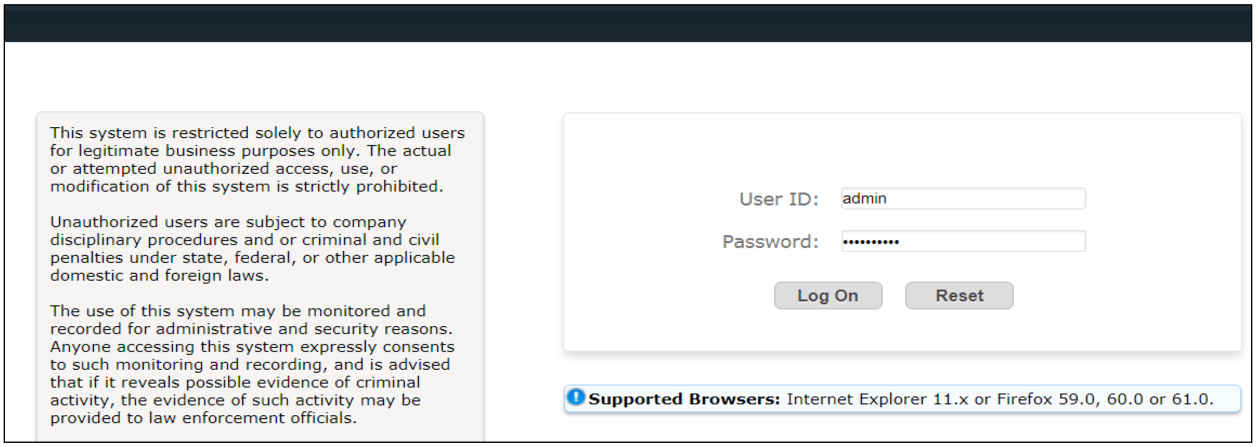
5. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include the following areas:

- Launch System Manager
- Administer locations
- Administer SIP entities
- Administer routing policies
- Administer dial patterns

5.1. Launch System Manager

Access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.



This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

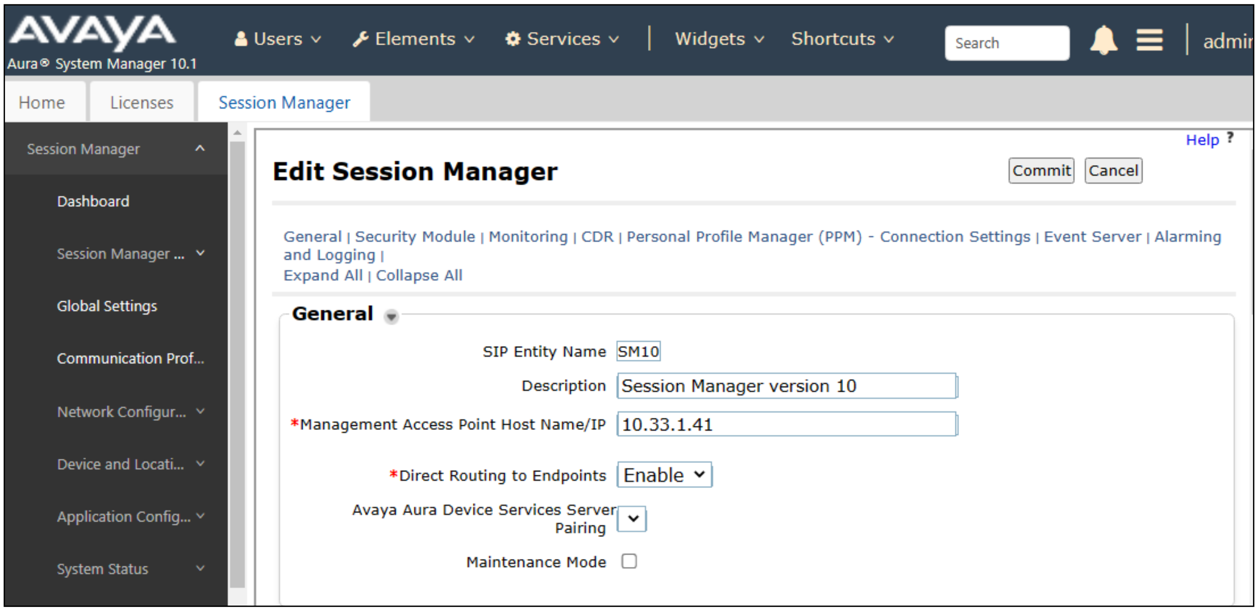
User ID: admin

Password: ••••••••••

Supported Browsers: Internet Explorer 11.x or Firefox 59.0, 60.0 or 61.0.

5.2. 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 "SM10" from list of Session Manager entities in the right-hand side and then select **Edit** button (not shown) to edit. The **Edit Session Manager** is displayed as below.



Edit Session Manager

General

SIP Entity Name: SM10

Description: Session Manager version 10

*Management Access Point Host Name/IP: 10.33.1.41

*Direct Routing to Endpoints: Enable

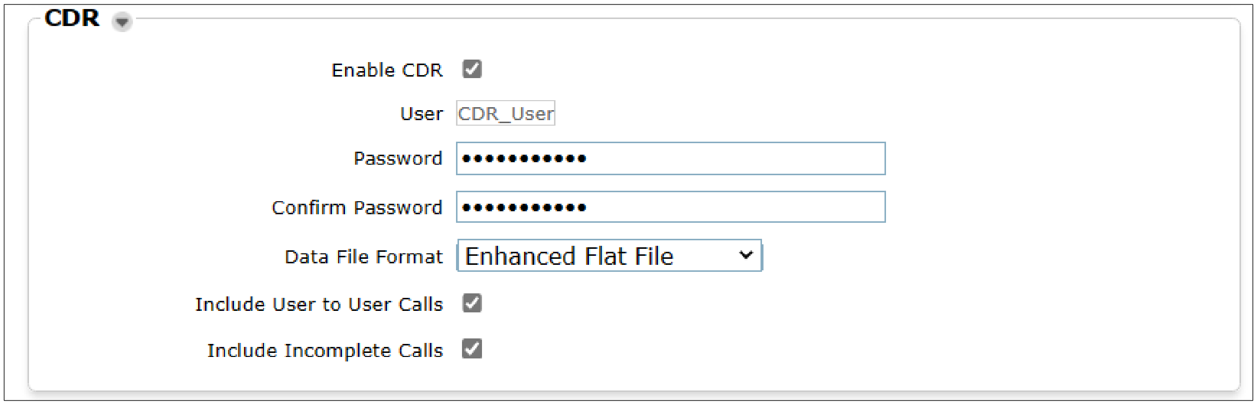
Avaya Aura Device Services Server Pairing:

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 and confirm password for user “CDR_User”
- **Data file Format**: select **Enhanced Flat File** from the drop down menu
- **Include User to user Calls**: selected
- **Include Incomplete Calls**: selected

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



CDR

Enable CDR: ☑

User: CDR_User

Password: •••••••••••

Confirm Password: •••••••••••

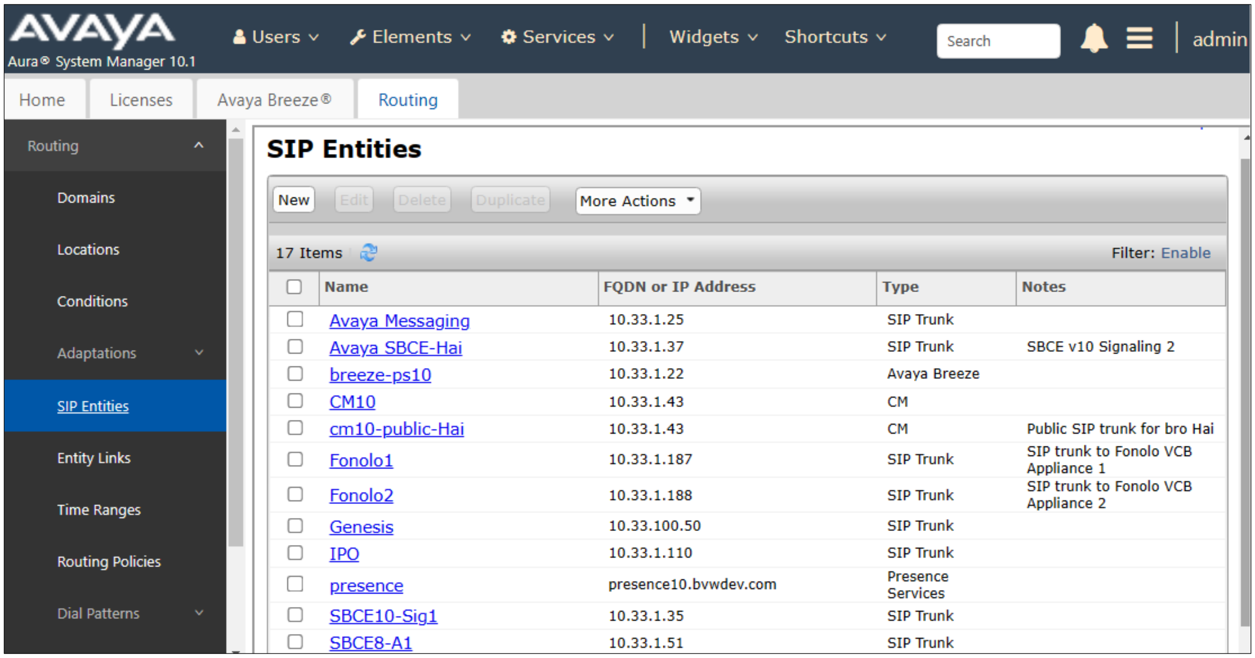
Data File Format: Enhanced Flat File

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 in the right-hand side of window.

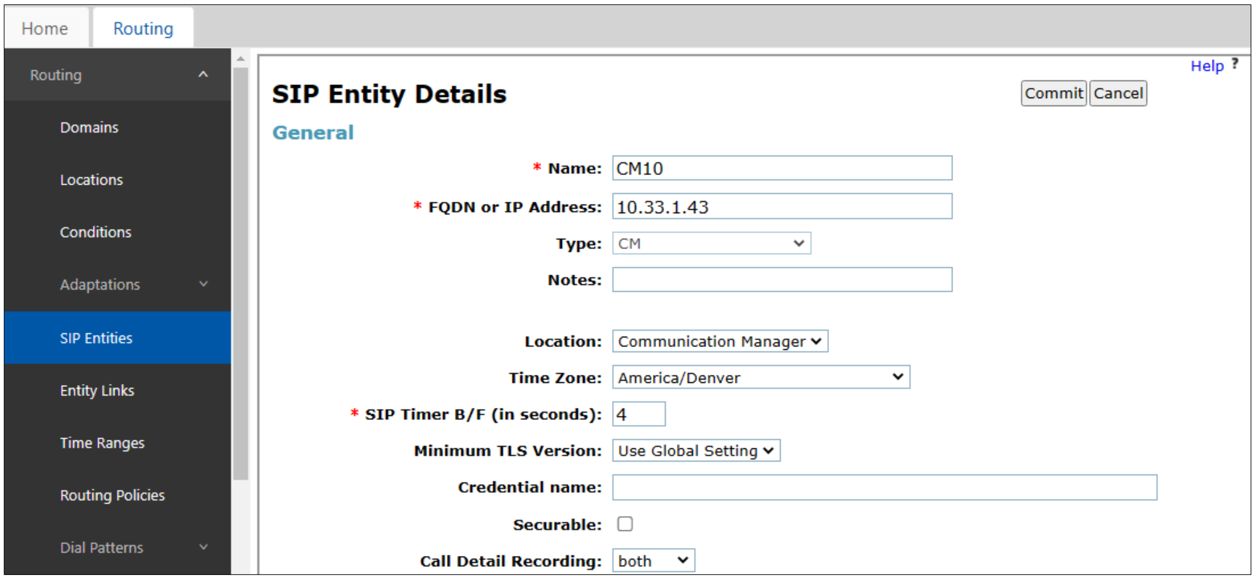


SIP Entities

17 Items — Filter: Enable

□	Name	FQDN or IP Address	Type	Notes
□	Avaya Messaging	10.33.1.25	SIP Trunk	
□	Avaya SBCE-Hai	10.33.1.37	SIP Trunk	SBCE v10 Signaling 2
□	breeze-ps10	10.33.1.22	Avaya Breeze	
□	CM10	10.33.1.43	CM	
□	cm10-public-Hai	10.33.1.43	CM	Public SIP trunk for bro Hai
□	Fonolo1	10.33.1.187	SIP Trunk	SIP trunk to Fonolo VCB Appliance 1
□	Fonolo2	10.33.1.188	SIP Trunk	SIP trunk to Fonolo VCB Appliance 2
□	Genesis	10.33.100.50	SIP Trunk	
□	IPO	10.33.1.110	SIP Trunk	
□	presence	presence10.bvwdev.com	Presence Services	
□	SBCE10-Sig1	10.33.1.35	SIP Trunk	
□	SBCE8-A1	10.33.1.51	SIP Trunk	

Select the "CM10" SIP entity, which is Communication Manager SIP entity, and select "both" on the **Call Detail Recording** field. On completion, click **Commit** button to save the change.



SIP Entity Details

General

* Name: CM10

* FQDN or IP Address: 10.33.1.43

Type: CM

Notes:

Location: Communication Manager

Time Zone: America/Denver

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

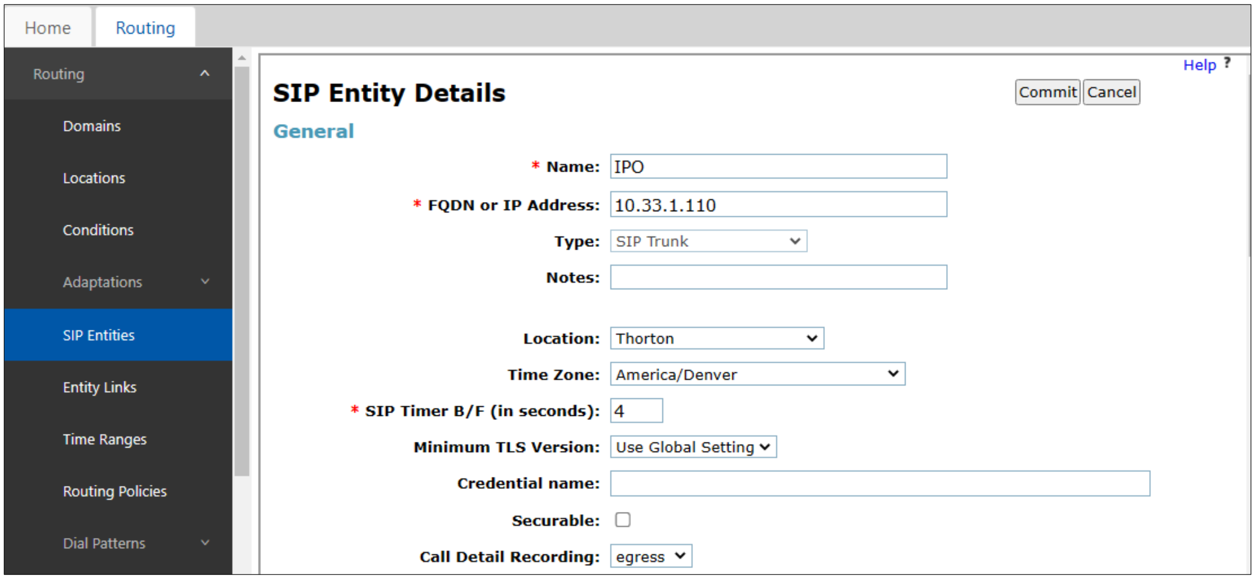
Minimum TLS Version: Use Global Setting

Credential name:

Securable: □

Call Detail Recording: both

Repeat the procedure above for another SIP entity that wants Session Manager to log CDR on their SIP entity, the example below is for Avaya IP Office.



SIP Entity Details

General

* Name: IPO

* FQDN or IP Address: 10.33.1.110

Type: SIP Trunk

Notes:

Location: Thorton

Time Zone: America/Denver

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

Minimum TLS Version: Use Global Setting

Credential name:

Securable: □

Call Detail Recording: egress

6. Configure RSI Shadow CMS

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

- Administer Secure 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.

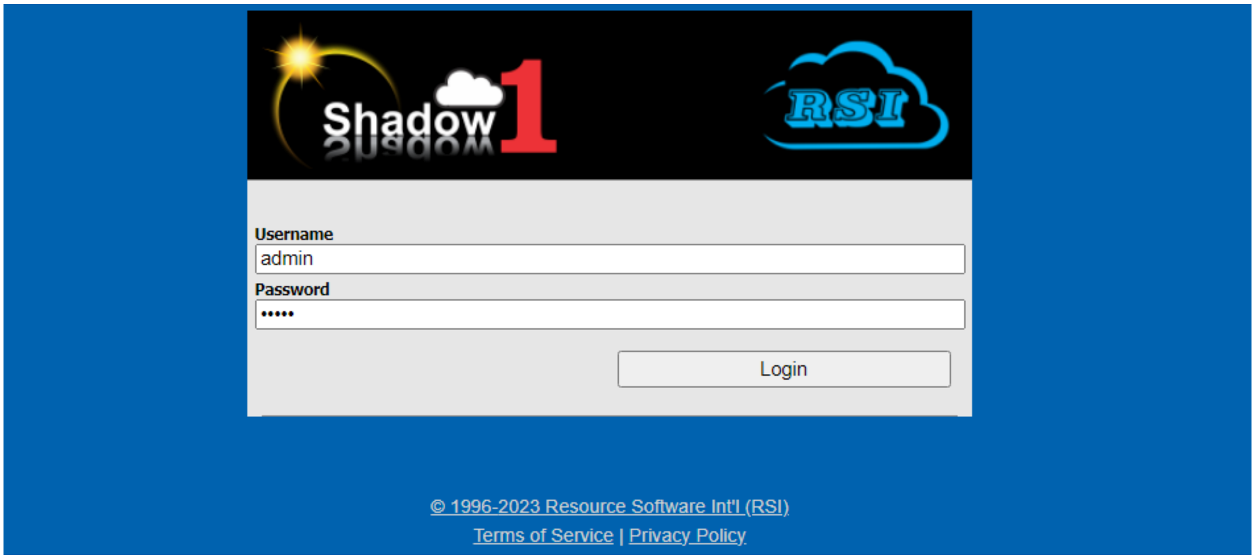
6.1. Administer Winlink FTP Client Utility

From the Shadow CMS server, create a script in Windows command line to use the WinSCP application to establish a secure connection to Session Manager to download the CDR files. The detail of script is displayed below.

```
@echo off

"C:\Program Files (x86)\WinSCP\WinSCP.com" ^

  /log="C:\ProgramData\WebCMS\Logs\WinSCP.log" /ini=nul ^

  /command ^
    "open sftp://CDR_User:<CDR_User password as configured in Section
5.2>@10.33.1.41/ -hostkey=""{ENTER YOUR AVAYA SM SSH HOST Key HERE}""" ^
    "get -append S* C:\ProgramData\WebCMS\EntityFiles\0001\RAW\0001.RAW" ^
    "rm S*" ^
    "exit"
set WINSCP_RESULT=%ERRORLEVEL%

if %WINSCP_RESULT% equ 0 (
  echo Success
) else (
  echo Error
)
 exit /b %WINSCP_RESULT%
```

6.2. Administer CDR Driver

Log into 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.



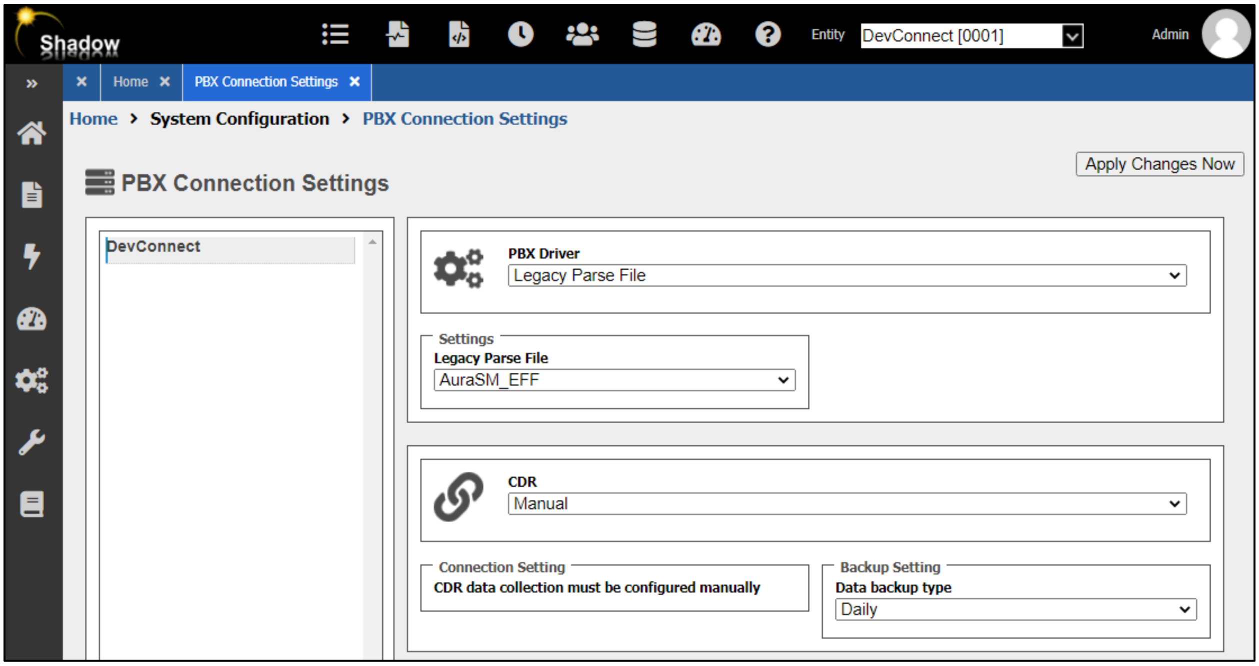
Username
admin

Password
•••••

© 1996-2023 Resource Software Int'l (RSI)
Terms of Service | Privacy Policy

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 "AuraSM_EFF" from the dropdown menu
- **CDR**: select "Manual" from the dropdown menu



Home > System Configuration > PBX Connection Settings

PBX Connection Settings

PBX Driver: Legacy Parse File

Settings
Legacy Parse File: AuraSM_EFF

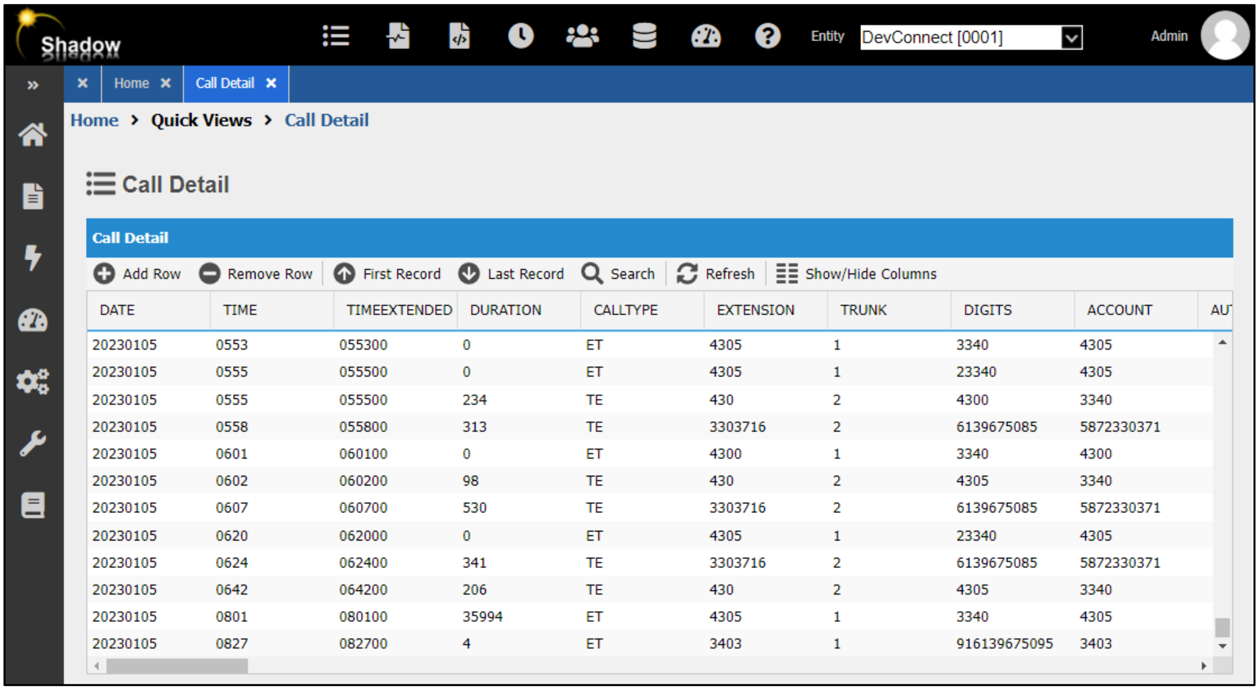
CDR: Manual

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 secure FTP application.

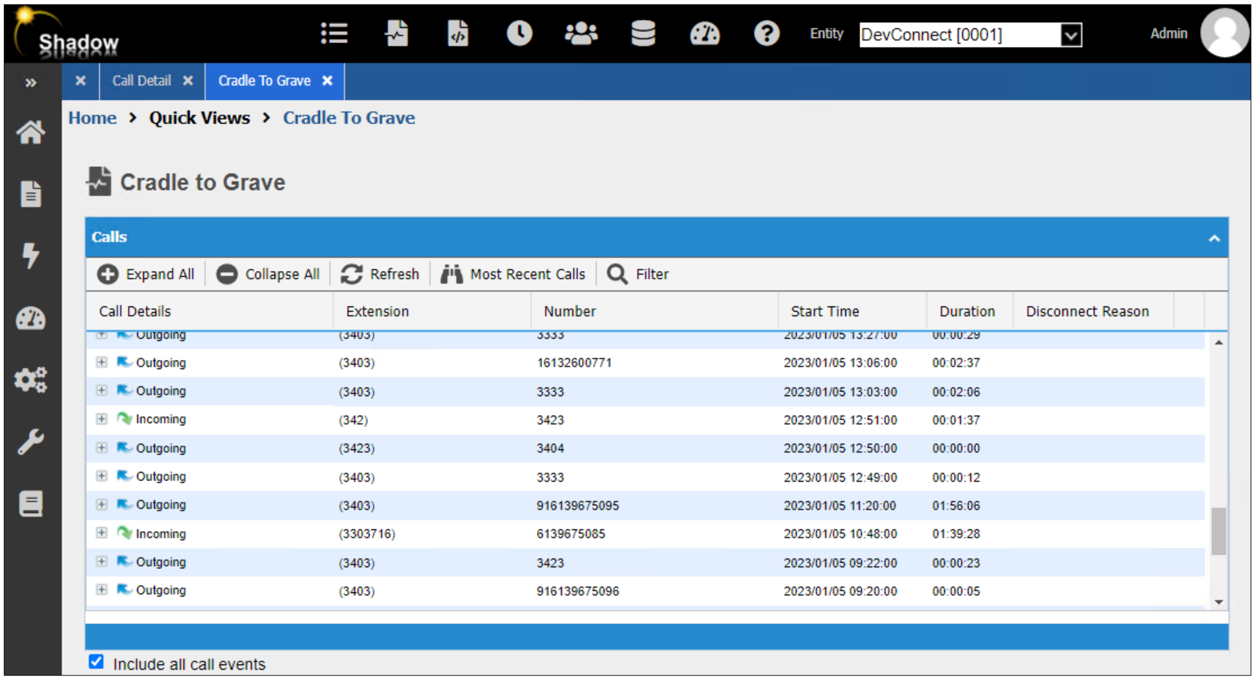


DATE	TIME	TIMEEXTENDED	DURATION	CALLTYPE	EXTENSION	TRUNK	DIGITS	ACCOUNT	AU
20230105	0553	055300	0	ET	4305	1	3340	4305	
20230105	0555	055500	0	ET	4305	1	23340	4305	
20230105	0555	055500	234	TE	430	2	4300	3340	
20230105	0558	055800	313	TE	3303716	2	6139675085	5872330371	
20230105	0601	060100	0	ET	4300	1	3340	4300	
20230105	0602	060200	98	TE	430	2	4305	3340	
20230105	0607	060700	530	TE	3303716	2	6139675085	5872330371	
20230105	0620	062000	0	ET	4305	1	23340	4305	
20230105	0624	062400	341	TE	3303716	2	6139675085	5872330371	
20230105	0642	064200	206	TE	430	2	4305	3340	
20230105	0801	080100	35994	ET	4305	1	3340	4305	
20230105	0827	082700	4	ET	3403	1	916139675095	3403	

7. Verification Steps

The following steps may be used to verify the configuration:

- Make several different types of calls such as between local stations, outgoing call via SIP trunk, and incoming call via PSTN and run the script to manually copy all CDR files from Session Manager.
- Verify that call records were collected from Shadow CMS and show up in the report.



Call Details	Extension	Number	Start Time	Duration	Disconnect Reason
⊞ Outgoing	(3403)	3333	2023/01/05 13:27:00	00:00:29	
⊞ Outgoing	(3403)	16132600771	2023/01/05 13:06:00	00:02:37	
⊞ Outgoing	(3403)	3333	2023/01/05 13:03:00	00:02:06	
⊞ Incoming	(342)	3423	2023/01/05 12:51:00	00:01:37	
⊞ Outgoing	(3423)	3404	2023/01/05 12:50:00	00:00:00	
⊞ Outgoing	(3403)	3333	2023/01/05 12:49:00	00:00:12	
⊞ Outgoing	(3403)	916139675095	2023/01/05 11:20:00	01:56:06	
⊞ Incoming	(3303716)	6139675085	2023/01/05 10:48:00	01:39:28	
⊞ Outgoing	(3403)	3423	2023/01/05 09:22:00	00:00:23	
⊞ Outgoing	(3403)	916139675096	2023/01/05 09:20:00	00:00:05	

☑ Include all call events

8. Conclusion

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

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.