Application Notes for @Comm CommView with Avaya Aura® Session Manager - Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the @Comm CommView call accounting software to successfully interoperate with Avaya Aura® Session Manager.

@Comm CommView is a call accounting software that interoperates with Avaya Aura® Session Manager. Call records can be generated for various types of calls. @Comm CommView collects, and processes the call records, using SFTP credentials.

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 @Comm CommView call accounting software can interoperate with Avaya Aura® Session Manager 7.0. @Comm CommView (herein referred to as CommView) connects to Avaya Aura® Session Manager over a local or wide area network using a SFTP.

CommView uses SFTP to log into Avaya Aura® Session Manager and access CDR files. CDR files are stored in the **/var/home/ftp/CDR** directory on Avaya Aura® Session Manager. Anytime CommView logs into the Avaya Aura® Session Manager server, CommView will be provided direct access to this directory. The CDR files stored in the special directory are those CDR data files that Avaya Aura® Session Manager has completed and closed and that are ready for CommView to collect. Once the CDR files have been retrieved, CommView should delete the files from Avaya Aura® Session Manager's directory. Typically multiple CDR files will be created each day. The file naming convention that is used for the CDR data files is shown below:

tssssss-ssss-YYMMDD-hh_mm

Where:

- The file name is fixed at 25 alphanumeric characters, including dashes "-" and underscore "_".
- "t" is populated with the character "S" in the first SM release.
- "ssssss-ssss" is an alphanumeric string of six characters, followed by a dash "-", and followed by an alphanumeric string of four characters, for a total of eleven characters. This string uniquely identifies the Session Manager server through its IPv4 IP address, in hexadecimal.
- "YY" is a two digit number representing the year when the file was created.
- "MM" is a two digit number representing the month when the file was created.
- "DD" is a two digit number representing the day of the month when the file was created.
- "hh" is a two digit number representing the hour of the day when the file was created. (24 hour clock server time)
- "mm" is a two digit number representing the number of minutes after the hour when the file was created.

CommView provides traditional call collection, rating, and reporting for any size businesses. CommView can interface with most telephone systems - in particular, with Avaya Aura® Communication Manager and Avaya Aura® Session Manager - to collect and interpret the detailed records of inbound, outbound, tandem, and internal telephone calls. CommView then calculates the appropriate charge for local, long distance, international & special calls and allocates them to responsible parties.

CommView is comprised of three components that reside on a Windows Server or workstation at the customer's premises: the CommView IP Software Buffer application, the CommView application and the WebReporter module. The CommView IP Software Buffer application runs as a background service process that utilizes the SFTP protocol to collect the call records from Avaya Aura® Session Manager, and stores the records in a text file. The CommView main application periodically pulls the data from the text file, parses the data and processes the data based on customer specific variables. The WebReporter module is then used to provide the reporting capabilities, both on demand and scheduled, for authorized users to access desired data.

During the test, both Avaya H.323 and 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. In these Application Notes, the following topics will be described:

- Avaya Aura® Session Manager – creating SFTP credentials for CommView
- CommView – SFTP configuration

2. General Test Approach and Test Results

The general test approach was to manually place several SIP trunk calls through Session Manager (inbound/outbound). Session Manager will store CDR data in a specific directory in Session Manager.
CommView logs in to Session Manager (Management IP address), using the SFTP credentials. Then, CommView collects CDR records, and properly classifies and reports the attributes of the call, and deletes CDR data from Session Manager, which CommView collected.

For serviceability testing, Session Manager was rebooted, and, after Session Manager came back up, CommView was able to login using SFTP account and collect CDR data.

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.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included features and serviceability tests. The focus of the compliance testing was primarily on verifying the interoperability between CommView and Session Manager.

2.2. Test Results

All executed test cases passed, with the observations noted below. CommView was able to successfully collect the CDR records from Session Manager, using the SFTP credentials. Observation: In Session Manger Release 7.x, an application is no longer able to delete the data in the CDR directory in Session Manager. In previous versions, Release 6.x and earlier, the application was able to delete the data once it had been collected. As a result the collecting application needs to be able to handle duplicate records as it collects the data at multiple intervals. It was verified that CommView was able to filter out the duplicate records during call processing and not include the duplicates in the reports produced.

2.3. Support

Technical support for CommView can be obtained through the following:

- http://www.atcomm.com/support/
- (603) 628-3000
- support@atcomm.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Communication Manager, an Avaya G450 Media Gateway, a Session Manager, and CommView. Avaya 96xx Series SIP IP Deskphones have been registered to Session Manager. The solution described herein is also extensible to other Avaya Servers and Media Gateways.

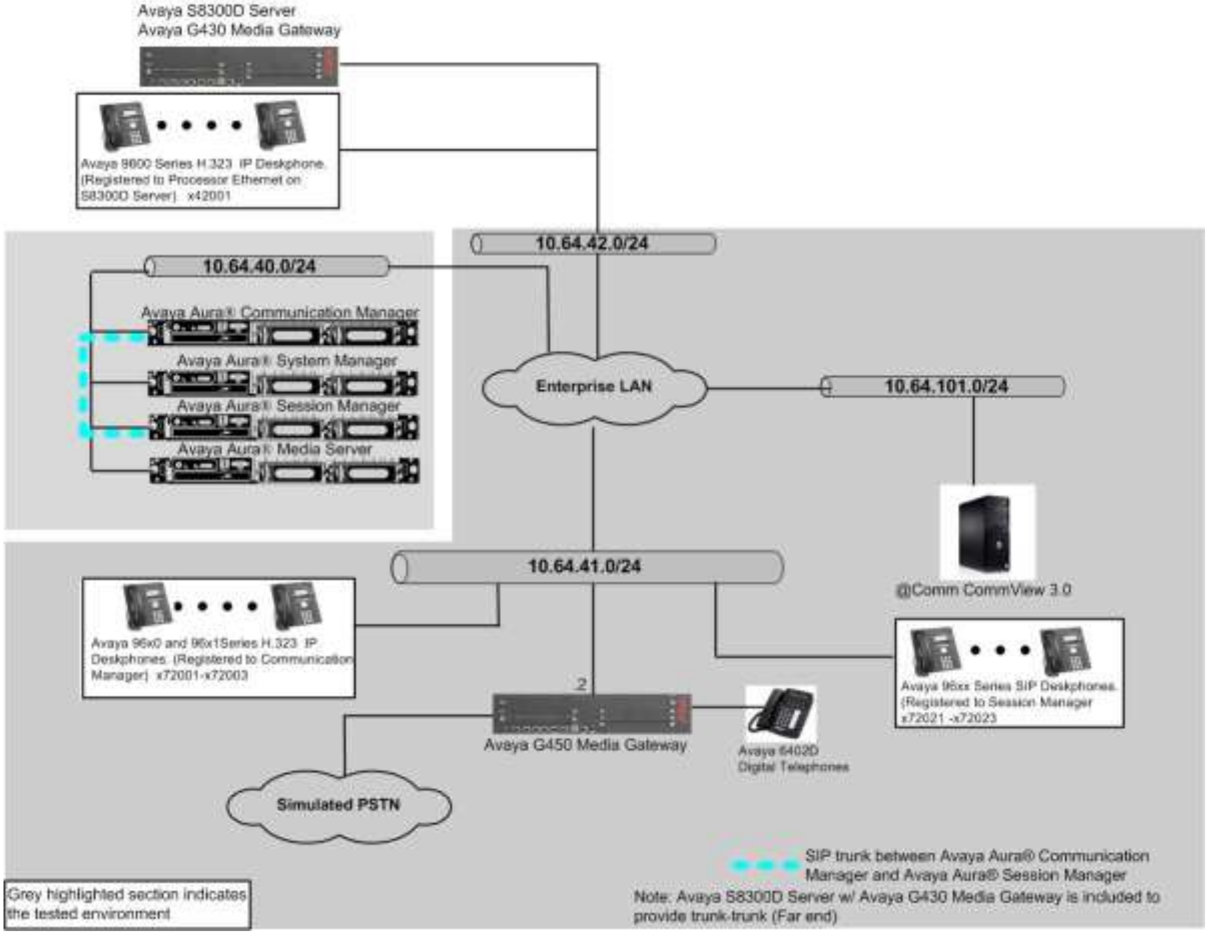

Avaya S8300D Server
Avaya G430 Media Gateway
Avaya 9600 Series H.323 IP Deskphone. (Registered to Processor Ethernet on S8300D Server) x42001
10.64.42.0/24
10.64.40.0/24
Avaya Aura® Communication Manager
Avaya Aura® System Manager
Avaya Aura® Session Manager
Avaya Aura® Media Server
Enterprise LAN
10.64.101.0/24
@Comm CommView 3.0
10.64.41.0/24
Avaya 96x0 and 96x1Series H.323 IP Deskphones. (Registered to Communication Manager) x72001-x72003
2
Avaya G450 Media Gateway
Avaya 6402D Digital Telephones
Avaya 96xx Series SIP Deskphones. (Registered to Session Manager x72021 -x72023
Simulated PSTN
SIP trunk between Avaya Aura® Communication Manager and Avaya Aura® Session Manager
Note: Avaya S8300D Server w/ Avaya G430 Media Gateway is included to provide trunk-trunk (Far end)
Grey highlighted section indicates the tested environment

Figure 1. Test configuration of @Comm CommView with Avaya Aura® Session Manager

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 on Virtual Environment Avaya G450 Media Gateway Avaya Aura® Media Server on Virtual Environment		7.0 (R017x.00.0.441.0) 37.19.0 7.7.0.226
Avaya Aura® System Manager on Virtual Environment		7.0.0.0.3929
Avaya Aura® Session Manager on Virtual Environment		7.0.0.0.700007
Avaya 96x1/96x0 Series SIP IP Deskphone		
	9611G 9630	7.0.0.39 2.6.14
Avaya 96x0 and 96x1 Series H.323 IP Deskphone		
	9620 9621G 9650	3.25 6.6 3.25
CommView on Windows 2008 Server R2 Standard, 64 bit • @Comm CommView • @Comm WebReporter • @Comm CommView IP Software Buffer		3.0 3.0 1.0.0.27

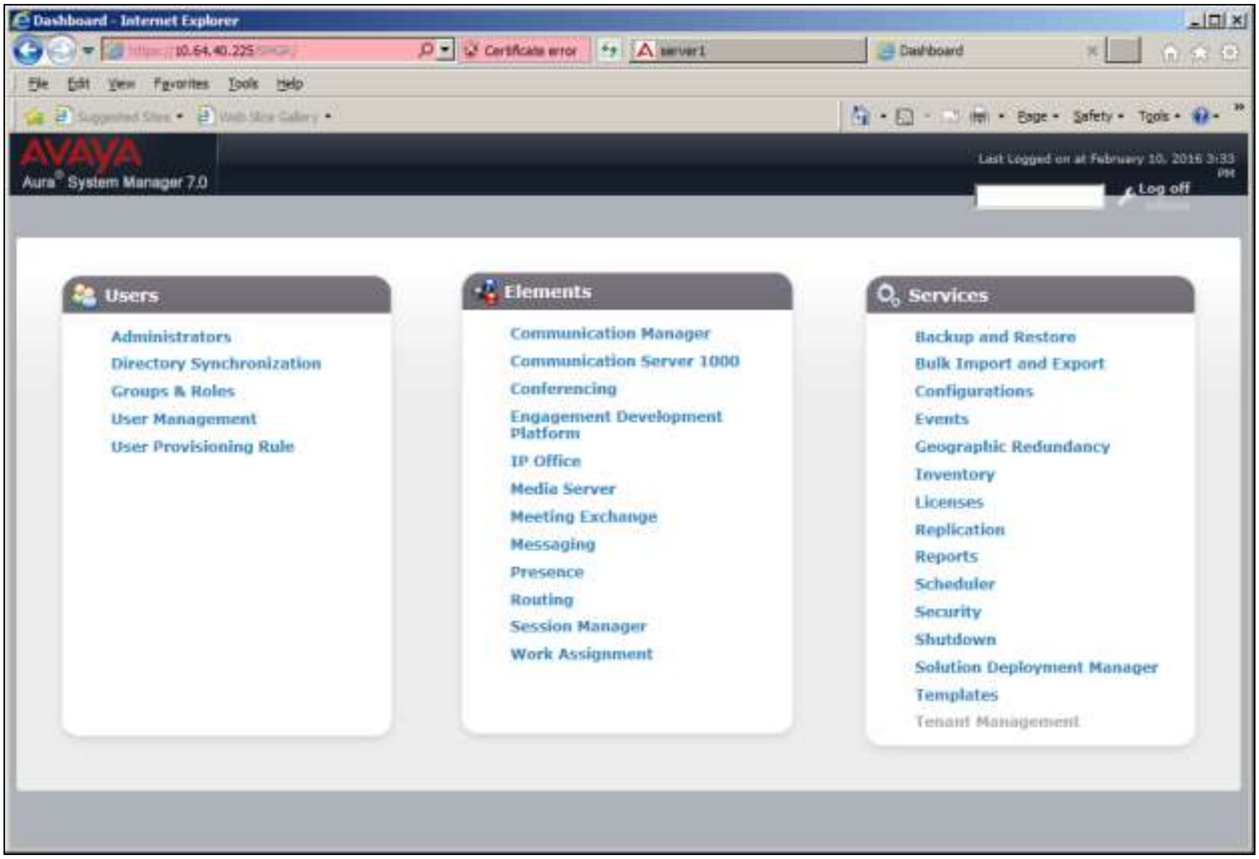
5. Configure Avaya Aura® Session Manager

This section describes how to create a CDR user account. This CDR user account will be utilized for CommView to SFTP to Session Manager for collecting and removing CDR data.

This section assumes that initial configuration on Session Manager has been performed, and Routing and Session Manager Instance are administered properly. This section will only discuss enabling the CDR configuration. During the compliance test, the CDR data will be stored on the hard disk drive of Session Manager. All calls that pass through this trunk (or entity link) will have their associated call data stored. To enable CDR in Session Manager, the following has to be modified:

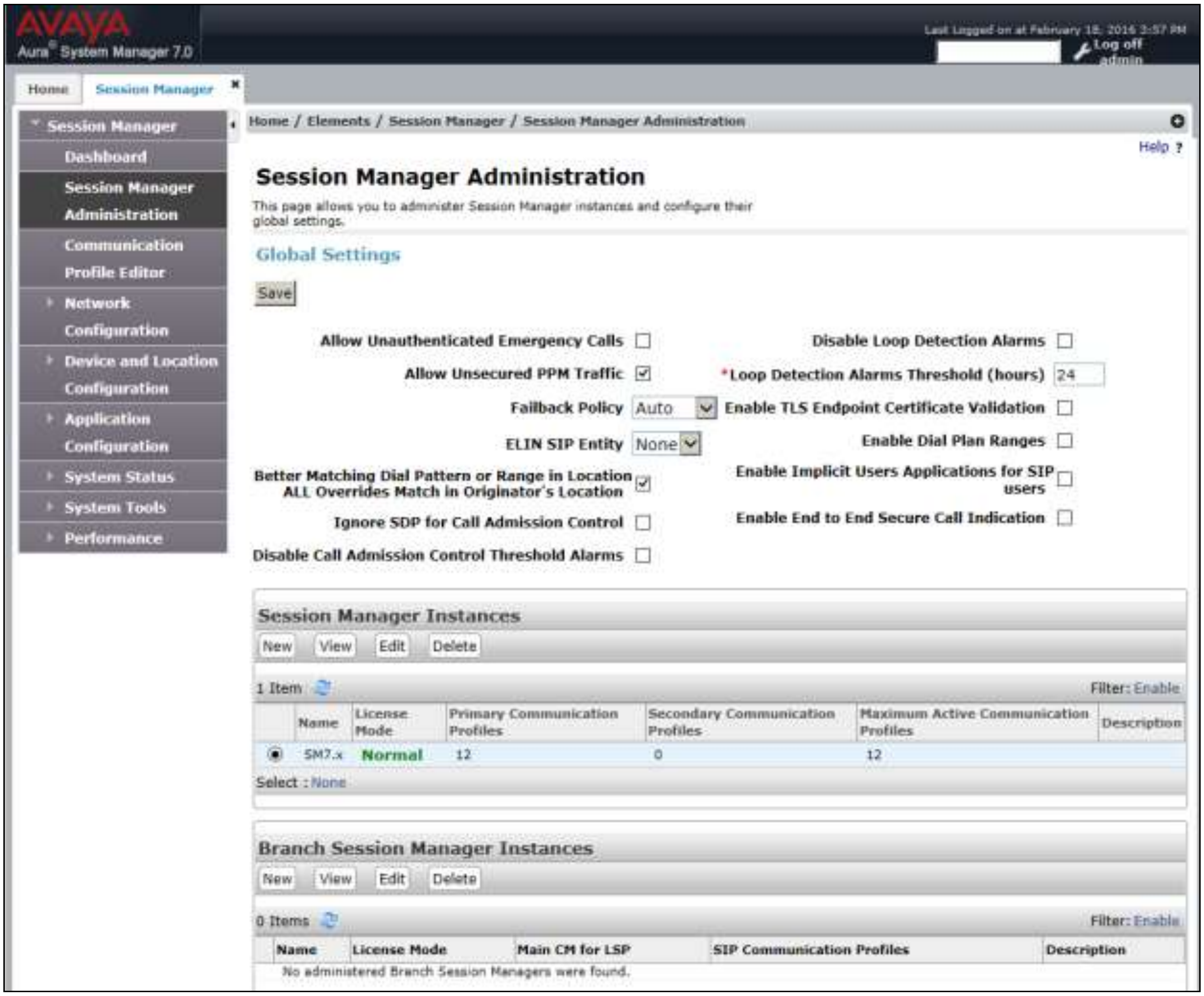
- Session Manager instances (**Elements → Session Manager → Session Manager Administration**)
- SIP Entities (**Routing → SIP Entities**)

Launch a web browser, enter http://<IP address of System manager> in the URL, and log in with the appropriate credentials. Navigate to **Elements→ Session Manager → Session Manager Administration**.



The **Session Manager Administration** screen is displayed.

Under the **Session Manager Instances** section, select the applicable instance and click **Edit**.


AVAYA
Aura® System Manager 7.0
Last Logged on at February 18, 2016 3:57 PM
Log off admin
Home
Session Manager
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

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 ☑
- Failback Policy: Auto
- ELIN SIP Entity: None
- Better Matching Dial Pattern or Range in Location ALL Overrides Match in Originator's Location ☑
- Ignore SDP for Call Admission Control ☐
- Disable Call Admission Control Threshold Alarms ☐
- Disable Loop Detection Alarms ☐
- *Loop Detection Alarms Threshold (hours): 24
- Enable TLS Endpoint Certificate Validation ☐
- Enable Dial Plan Ranges ☐
- Enable Implicit Users Applications for SIP users ☐
- Enable End to End Secure Call Indication ☐

Session Manager Instances

1 Item — Filter: Enable

	Name	License Mode	Primary Communication Profiles	Secondary Communication Profiles	Maximum Active Communication Profiles	Description
●	SM7.x	Normal	12	0	12	

Select : None

Branch Session Manager Instances

0 Items — Filter: Enable

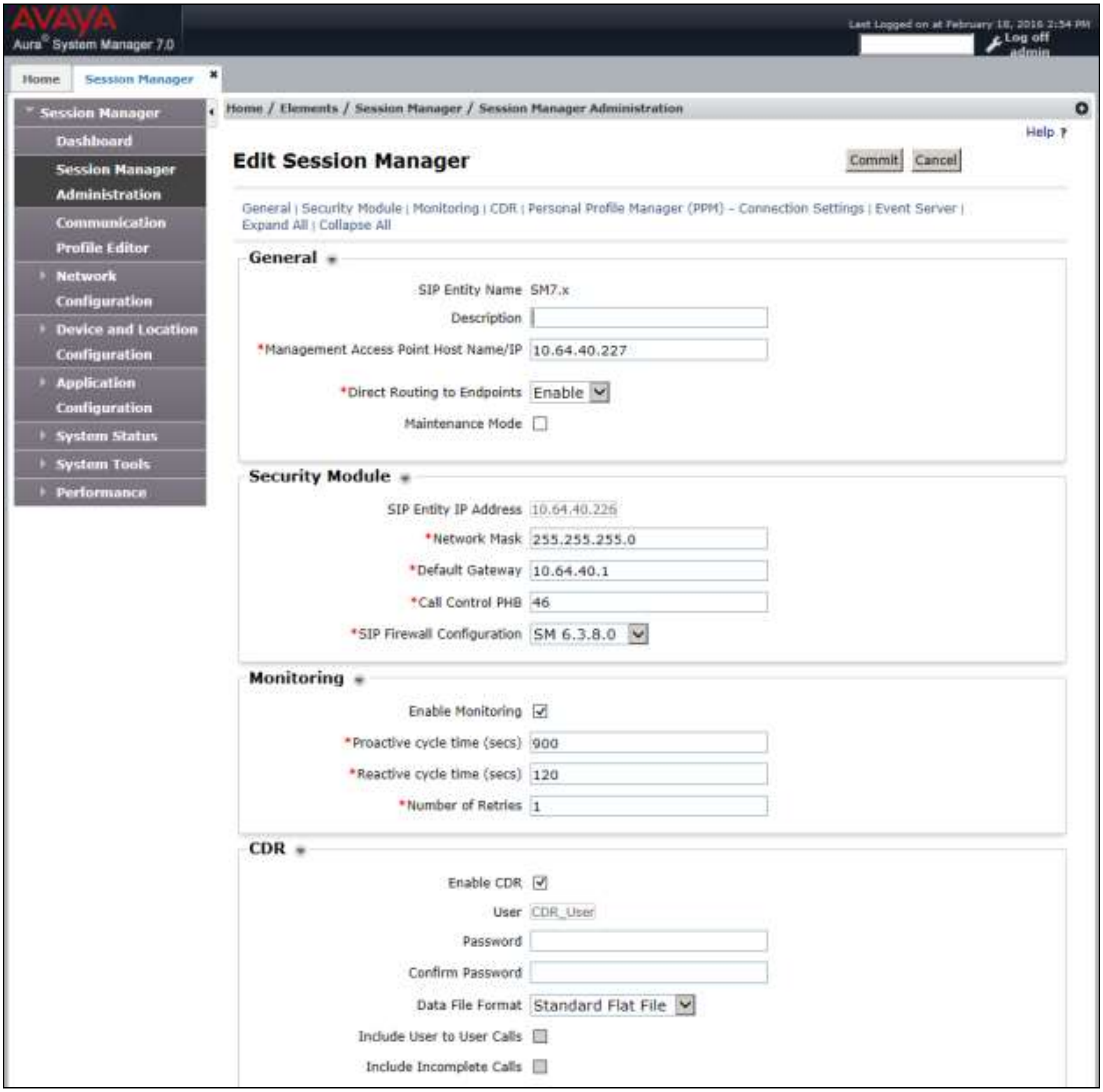
	Name	License Mode	Main CM for LSP	SIP Communication Profiles	Description
	No administered Branch Session Managers were found.				

The **Edit Session Manager** screen is displayed.

Under the **CDR** section, provide the following information:

- Check the checkbox on the **Enable CDR** field to enable the CDR process.
- Provide a password for **CDR_User**. This password will be utilized by CommView for SFTP access to Session Manager.
- Enter the same password for the **Confirm Password** field.

Click **Commit**.


AVAYA
Aura® System Manager 7.0
Last Logged on at February 18, 2016 2:54 PM
Log off admin
Home
Session Manager
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 ?
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	SM7.x
Description	
*Management Access Point Host Name/IP	10.64.40.227
*Direct Routing to Endpoints	Enable
Maintenance Mode	□

Security Module

SIP Entity IP Address	10.64.40.226
*Network Mask	255.255.255.0
*Default Gateway	10.64.40.1
*Call Control PHB	46
*SIP Firewall Configuration	SM 6.3.8.0

Monitoring

Enable Monitoring	☑
*Proactive cycle time (secs)	900
*Reactive cycle time (secs)	120
*Number of Retries	1

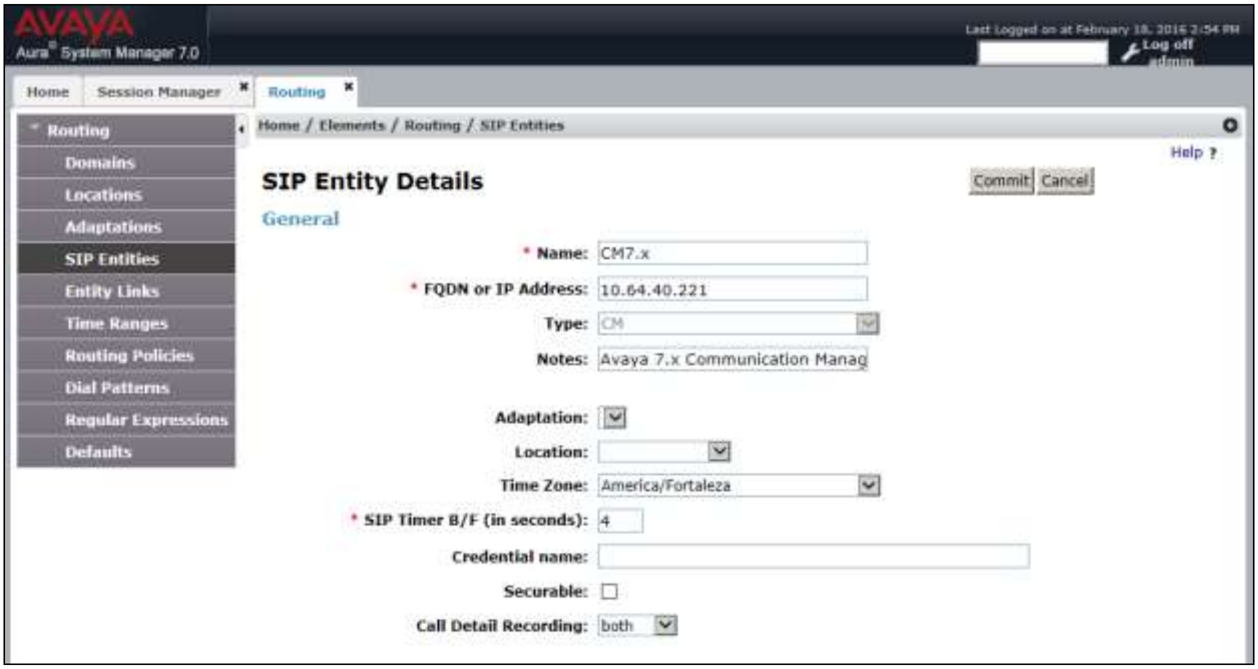
CDR

Enable CDR	☑
User	CDR_User
Password	
Confirm Password	
Data File Format	Standard Flat File
Include User to User Calls	□
Include Incomplete Calls	□

During the SIP entity configuration every SIP entity that collects CDR data has to be enabled and specified the direction of calls (ingress/egress/both/none) to be stored.

Navigate to **Elements → Routing → SIP Entities**. The following screen describes **CM7.x** entity details, which was already configured prior to the compliance test. On the **Call Detail Recording** field, select the direction of calls to be stored in Session Manager. During the compliance test, "both" was selected.

Click **Commit**.



SIP Entity Details

General

* Name: CM7.x

* FQDN or IP Address: 10.64.40.221

Type: CM

Notes: Avaya 7.x Communication Manag

Adaptation:

Location:

Time Zone: America/Fortaleza

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

Credential name:

Securable: □

Call Detail Recording: both

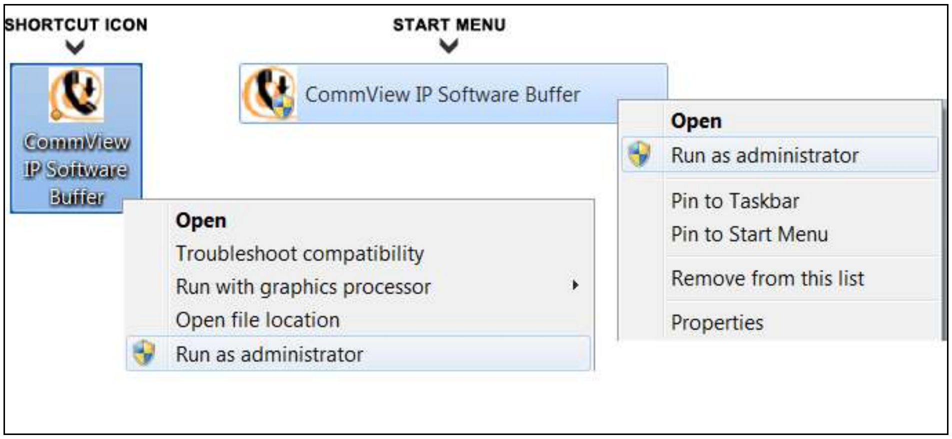
6. Configure @Comm CommView

This section describes the operation of CommView to collect CDR data from Session Manager. Installation of the CommView software was performed by a @Comm engineer prior to the actual compliance test. In this section, the following topics are discussed:

- Configure CommView for SFTP
- View CommView CDR Report

6.1. Configure CommView for SFTP

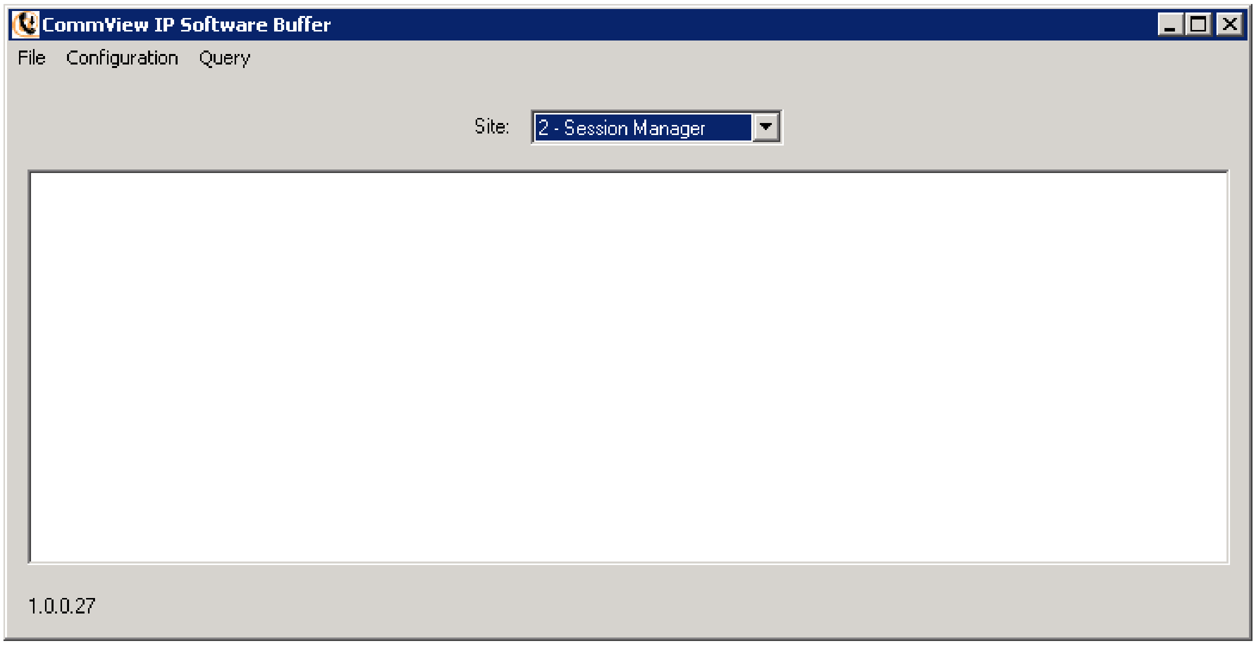
To configure CommView IP Software Buffer to communicate with Communication Manager, navigate to **SHORTCUT ICON** or **START MENU → CommView IP Software Buffer**. Right mouse click the icon and choose “Run as administrator”.



The **CommView IP Software Buffer** screen is displayed. Select “2 – Session Manager” in the **Site** field. During the CommView installation, @Comm engineer configured two sites.

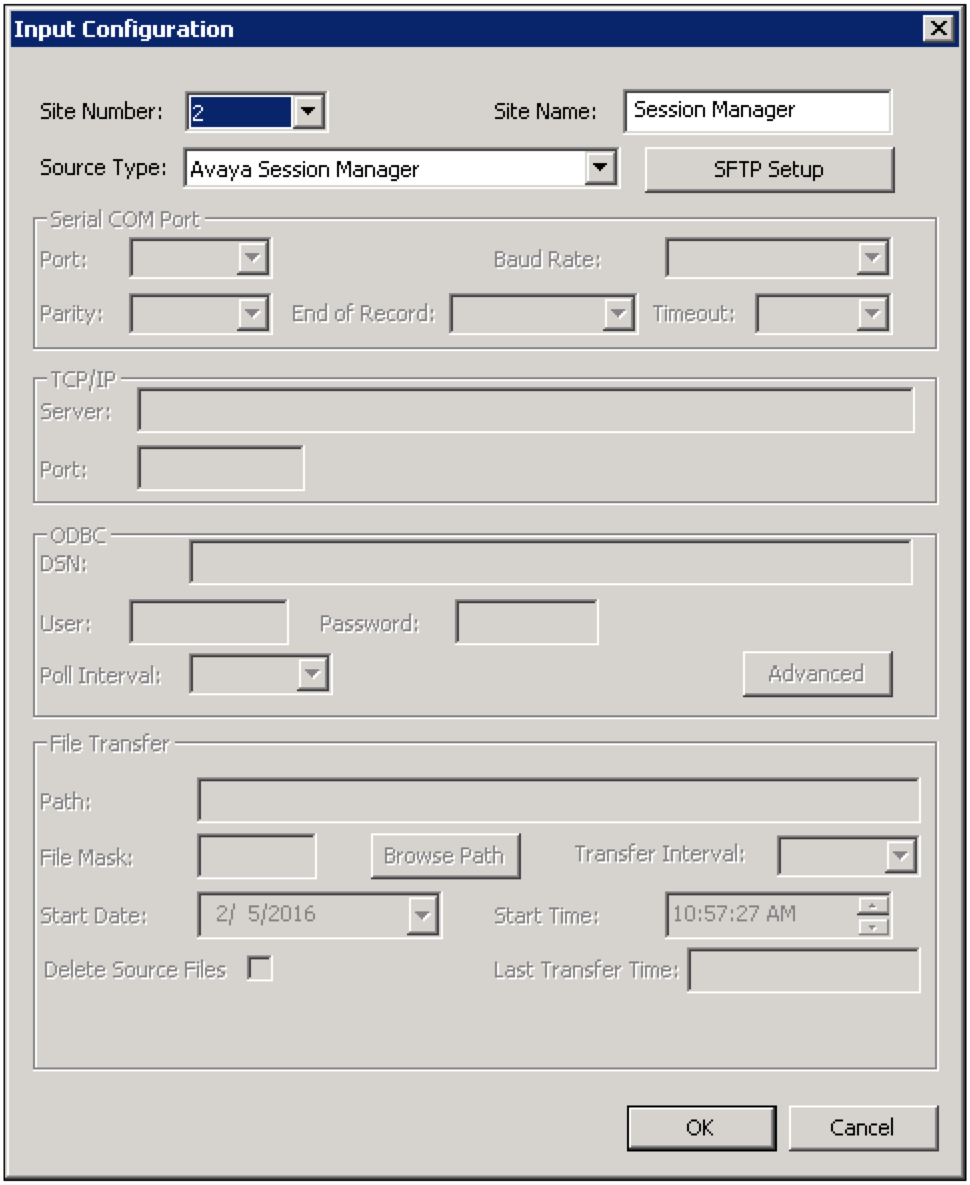
- 1 – Communication Manager
- 2 – Session Manager

Navigate to **Configuration → Input** (not shown) to display the **Input Configuration** screen.



Site: 2 - Session Manager

As a default, **Site Number** displays “2”, and **Site Name** displays “Session Manager”. Select “Avaya Session Manager” on the **Source Type** field. Click the **SFTP Setup** button.



Input Configuration

Site Number: 2

Site Name: Session Manager

Source Type: Avaya Session Manager

Start Date: 2/ 5/2016

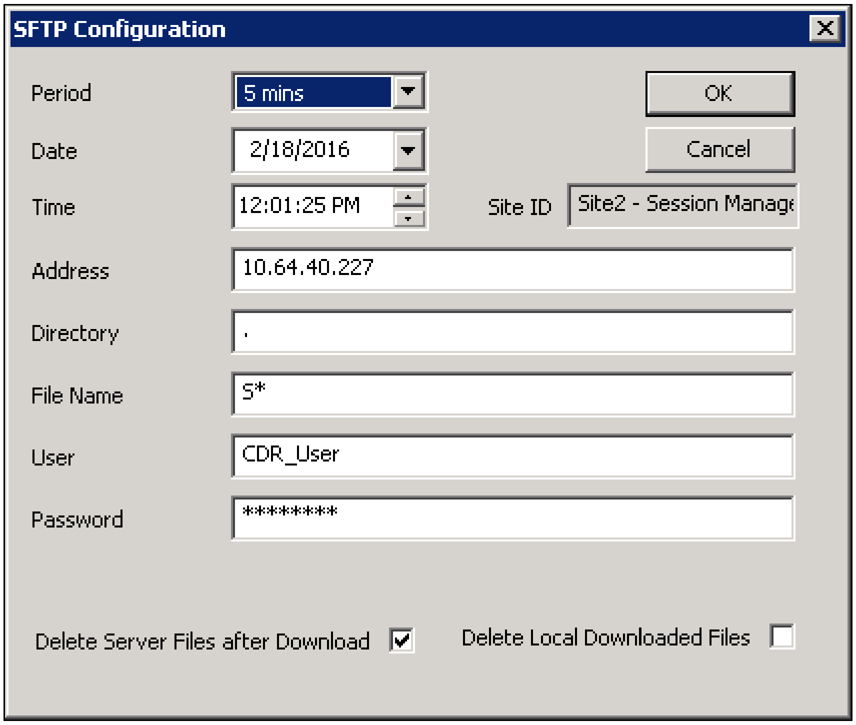
Start Time: 10:57:27 AM

Delete Source Files ☐

The **SFTP Configuration** screen is displayed. Provide the following information:

- **Period**: Select the incremental time that CommView collects CDR data from Session manager, using drop-down list.
- **Date**: Enter the correct date.
- **Time**: Enter the correct time.
- **Address**: Enter the IP address of Session Manager (Management IP address).
- **Directory**: Enter ”.” meaning CommView uses the default directory.
- **File Name**: CommView will collect all files that start “S”.
- **User**: Utilizes **CDR_User** as the user name, which was created in System Manager in **Section 5**.
- **Password**: Utilizes the password which was created in System Manager in **Section 5**.
- Check the checkbox on **Delete Server Files after Download**.

Click on the **OK** button at the top right of the screen.



SFTP Configuration

Period: 5 mins

Date: 2/18/2016

Time: 12:01:25 PM

Site ID: Site2 - Session Manage

Address: 10.64.40.227

Directory: .

File Name: S*

User: CDR_User

Password: *********

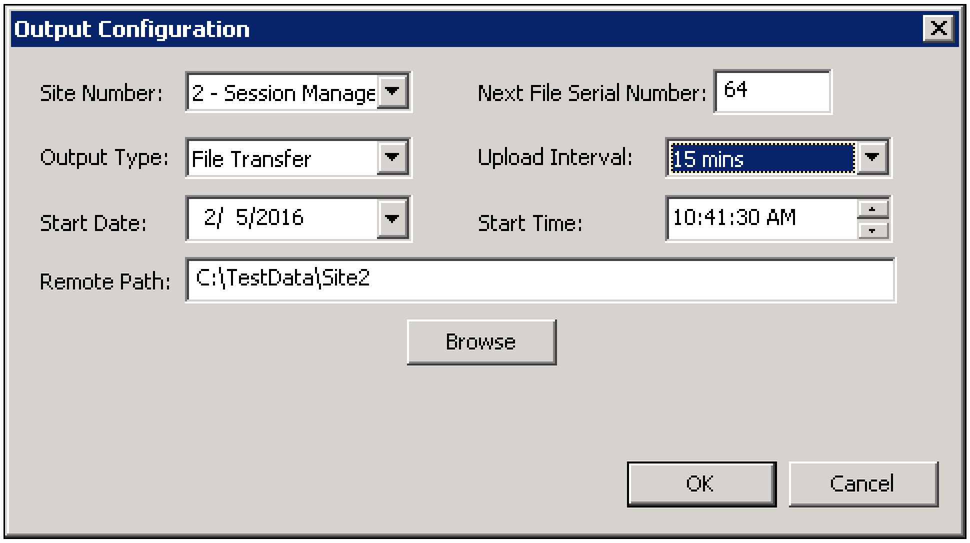
Delete Server Files after Download ☑

Delete Local Downloaded Files □

From the **CommView IP Software Buffer** screen, navigate to **Configuration → Output**, and the **Output Configuration** screen is displayed. Provide the following parameters:

- **Output Type**: Select "File Transfer" using drop-down list.
- **Upload Interval**: Enter the appropriate uploading interval time. During the compliance test, "15 mins" was used.
- **Start Date**: Set the correct date.
- **Start Time**: Set the correct time.
- **Remote Path**: Specify the directory where the raw data is stored.

Click **OK**.



Output Configuration

Site Number: 2 - Session Manage

Next File Serial Number: 64

Output Type: File Transfer

Upload Interval: 15 mins

Start Date: 2/ 5/2016

Start Time: 10:41:30 AM

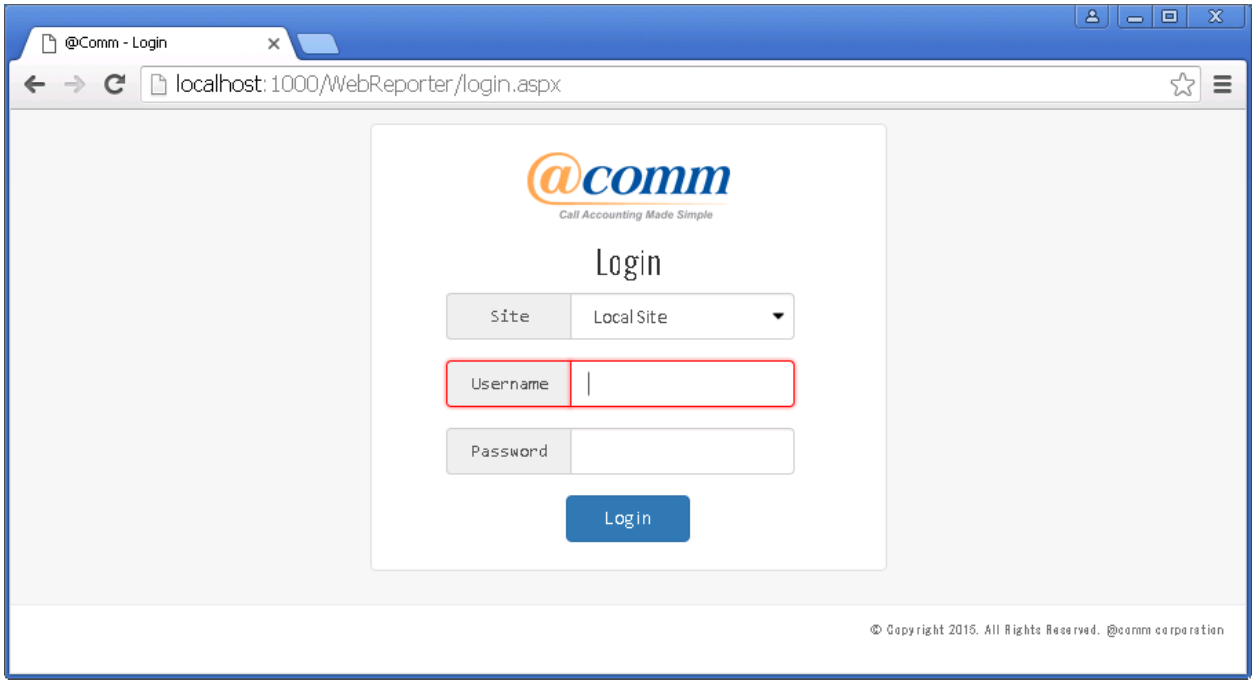
Remote Path: C:\TestData\Site2

6.2. View CommView CDR Report

There are two ways to view CDR report:

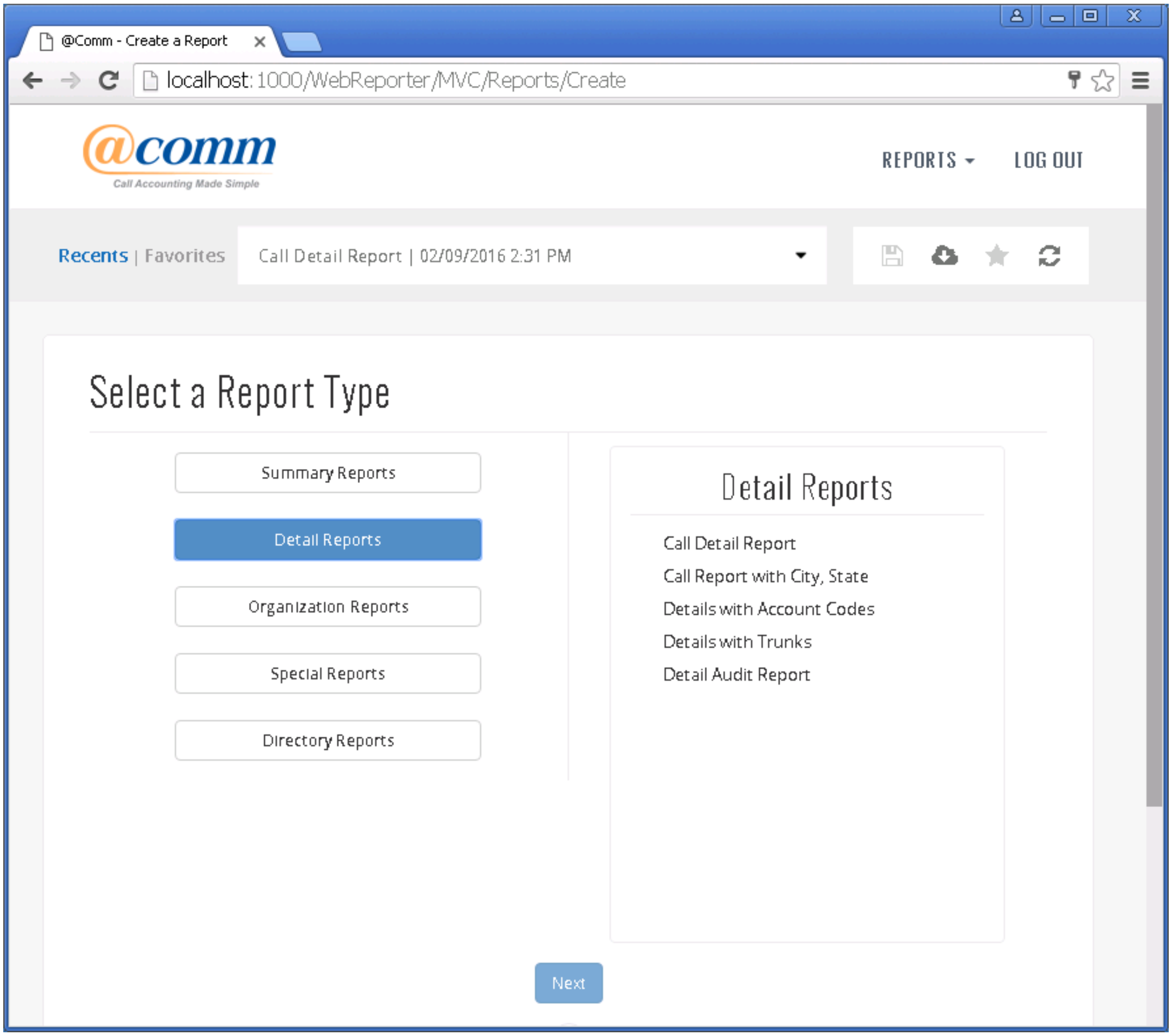
- CommView CDR Report
- WebReporter CDR Report

During the compliance test, WebReporter CDR Report was utilized. To view the CDR report, launch a web browser. Enter **http://<IP address of CommView>:1000/WebReporter** in the URL, and log in with appropriate credentials.


@Comm - Login
localhost:1000/WebReporter/login.aspx
@comm
Call Accounting Made Simple
Login
Site
Local Site
Username
Password
Login
© Copyright 2015. All Rights Reserved. @comm corporation

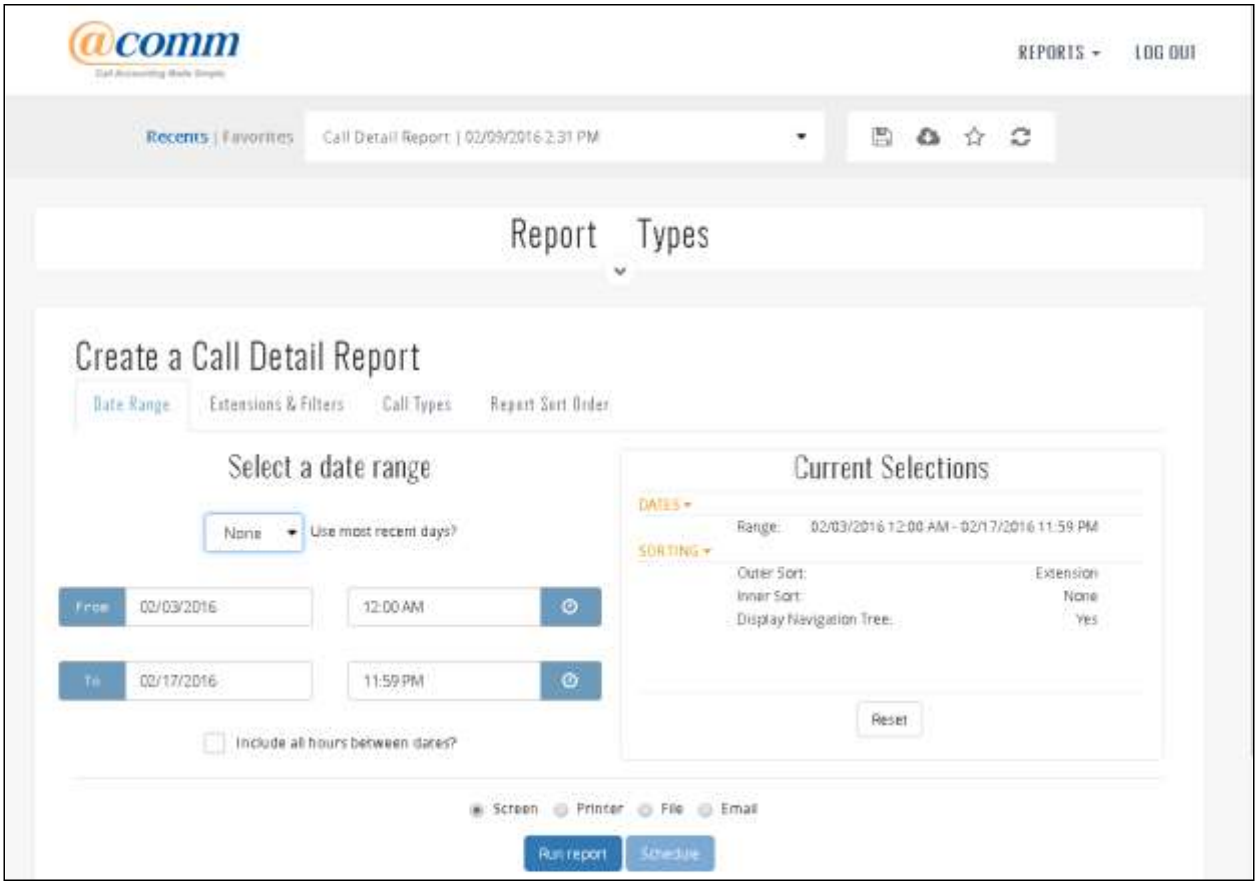
On the @Comm CommView main screen, select the following parameters:

- Under **Select a Report Type** section, select “Detail Reports”.
- Under **Detail Reports** section, select “Call Detail Report”
- Click **Next**.



On the following screen, provide information:

- Click the **Date Range** tab,and provide which days (or how many days) the CDR data will be displayed.
- Click the **Report Sort Order** tab, and provide **Outer Sort** and **Inner Sort** sorting option (not shown).
- Click the **Run report** button at the bottom.



Call Detail Report | 02/09/2016 2:31 PM

Create a Call Detail Report

Select a date range

None ▾ Use most recent days?

From 02/03/2016 12:00 AM

To 02/17/2016 11:59 PM

□ Include all hours between dates?

Current Selections

DATES ▾

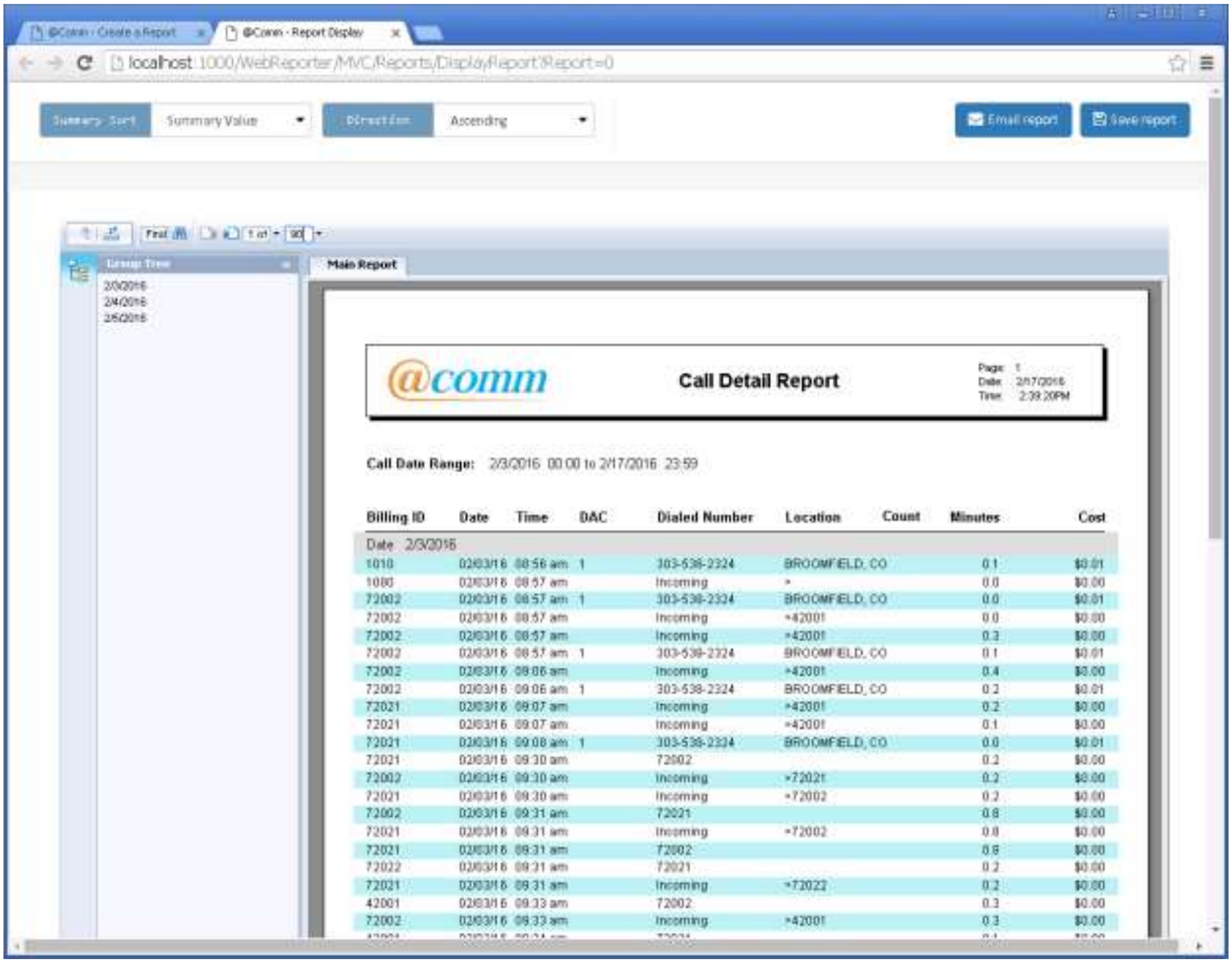
Range: 02/03/2016 12:00 AM - 02/17/2016 11:59 PM

SORTING ▾

Outer Sort:	Extension
Inner Sort:	None
Display Navigation Tree:	Yes

● Screen ○ Printer ○ File ○ Email

The following screen displays CDR reports received during the compliance test.



Call Detail Report

Page: 1
Date: 2/17/2016
Time: 2:39:20PM

Call Date Range: 2/3/2016 00:00 to 2/17/2016 23:59

Billing ID	Date	Time	DAC	Dialed Number	Location	Count	Minutes	Cost
Date 2/3/2016								
1010	02/03/16	08:56 am	1	303-538-2324	BROOMFIELD, CO		0.1	$0.01
1080	02/03/16	08:57 am		Incoming	*		0.0	$0.00
72002	02/03/16	08:57 am	1	303-538-2324	BROOMFIELD, CO		0.0	$0.01
72002	02/03/16	08:57 am		Incoming	*42001		0.0	$0.00
72002	02/03/16	08:57 am		Incoming	*42001		0.3	$0.00
72002	02/03/16	08:57 am	1	303-538-2324	BROOMFIELD, CO		0.1	$0.01
72002	02/03/16	09:06 am		Incoming	*42001		0.4	$0.00
72002	02/03/16	09:06 am	1	303-538-2324	BROOMFIELD, CO		0.2	$0.01
72021	02/03/16	09:07 am		Incoming	*42001		0.2	$0.00
72021	02/03/16	09:07 am		Incoming	*42001		0.1	$0.00
72021	02/03/16	09:08 am	1	303-538-2324	BROOMFIELD, CO		0.0	$0.01
72021	02/03/16	09:30 am		72002			0.2	$0.00
72002	02/03/16	09:30 am		Incoming	*72021		0.2	$0.00
72021	02/03/16	09:30 am		Incoming	*72002		0.2	$0.00
72002	02/03/16	09:31 am		72021			0.8	$0.00
72021	02/03/16	09:31 am		Incoming	*72002		0.8	$0.00
72021	02/03/16	09:31 am		72002			0.8	$0.00
72022	02/03/16	09:31 am		72021			0.2	$0.00
72021	02/03/16	09:31 am		Incoming	*72022		0.2	$0.00
42001	02/03/16	09:33 am		72002			0.3	$0.00
72002	02/03/16	09:33 am		Incoming	*42001		0.3	$0.00

7. Verification Steps

The following steps may be used to verify the configuration:

- Check the CDR data, by accessing the CDR directory in Session Manager (Management).

```
 [root@avaya-asm7x cust]# cd /var/home/ftp/CDR
[root@avaya-asm7x CDR]# ls -l
total 56
-rw-r--r-- 1 root     root     16155 Dec  7 03:34 cleanup.log
drwxrwx--- 2 CDR_User CDR_User  4096 Sep 18 12:18 current
-rwxrw---- 1 root     CDR_User   241 Dec  2 10:44 S000A40-28E3-151202-10_44
-rwxrw---- 1 root     CDR_User   241 Dec  4 11:19 S000A40-28E3-151204-11_19
-rwxrw---- 1 root     CDR_User   241 Dec  4 11:24 S000A40-28E3-151204-11_24
-rwxrw---- 1 root     CDR_User   241 Dec  4 12:09 S000A40-28E3-151204-12_09
-rwxrw---- 1 root     CDR_User  1153 Dec  4 12:14 S000A40-28E3-151204-12_14
-rwxrw---- 1 root     CDR_User   469 Dec  4 12:19 S000A40-28E3-151204-12_19
-rwxrw---- 1 root     CDR_User   241 Dec  4 12:44 S000A40-28E3-151204-12_44
-rwxrw---- 1 root     CDR_User   697 Dec  4 12:49 S000A40-28E3-151204-12_49
-rwxrw---- 1 root     CDR_User   469 Dec  4 15:09 S000A40-28E3-151204-15_09
[root@avaya-asm7x CDR]#
```

- Verify from CommView in **Section 6.2**, where CDR data is reported.

8. Conclusion

These Application Notes describe the procedures for configuring @Comm CommView to collect call detail records from Avaya Aura® Session Manager. Testing was successful. Please refer to **Section 2.2** for test results and observation.

9. References

This section references the Avaya and @Comm documentation that are relevant to these Application Notes.

[1] *Avaya Aura® Session Manager Call Detail Recording Interface*, Issue 1.3.1, October2013, available at http://support.avaya.com.

The CommView Solution and Product information is available from @Comm. To obtain a document related to CommView, contact @Comm Support in **Section 2.3**.

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.