



Avaya Solution & Interoperability Test Lab

Application Notes for @Comm CommView with Avaya Aura® Communication 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® Communication Manager.

@Comm CommView is a call accounting software that interoperates with Avaya Aura® Communication Manager over the Avaya Reliable Session Protocol (RSP). Call records can be generated for various types of calls. @Comm CommView collects, and processes the call records.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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® Communication Manager 7.0. @Comm CommView (herein referred to as CommView) connects to Avaya Aura® Communication Manager over a local or wide area network using a CDR link running RSP. Avaya Aura® Communication Manager is configured to send CDR records to CommView using a specific port.

CommView is a call accounting solution that provides centralized administration and reporting with automated distribution of produced reports. CommView collects CDR data from Avaya Aura® Communication Manager by listening for connections on a specific TCP port.

Avaya Aura® Communication Manager communicates to @Comm CommView via an RSP session over the TCP/IP network. The RSP session provides a transport mechanism for reliable delivery of CDR records. Avaya Aura® Communication Manager generates and sends the call records out on the RSP session while CommView collects, stores and processes the records at the other end.

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 RSP protocol to collect the call records from Avaya Aura® Communication 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:

- A CDR link configuration on Avaya Aura® Communication Manager.
- CommView – A CDR link configuration on CommView.

2. General Test Approach and Test Results

The general test approach was to manually place intra-switch calls, inbound trunk calls, and outbound trunk calls for basic call, transfer, conference scenarios, authorization code and account code, and verify that CommView 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, Communication Manager was reset and CommView 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.

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 Communication Manager.

2.2. Test Results

All executed test cases passed, with the observations noted below. CommView successfully collected the CDR records from Communication Manager via a RSP connection for all types of calls generated including intra-switch calls, inbound/outbound PSTN trunk calls, inbound/outbound private IP trunk calls, transferred calls, conference calls, authorization and account code.

Note: During the intra-switch scenario, CommView collects from both extensions in the intra-switch form. Thus, CommView is collecting two CDR data for each intra-switch call scenario. CommView has an option on collecting one CDR data or two CDR data. During the compliance test, the option of collecting two CDR data was implemented.

For serviceability testing, CommView was able to resume collection of CDR records after failure recovery including buffered CDR records for calls that were placed during the outages.

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.

Note: Avaya S8300D Server with an Avaya G430 Media Gateway was included in the test only to provide an inter-switch scenario. Thus, there will not be any discussion on configuring Avaya S8300D Server with an Avaya G430 Media Gateway.

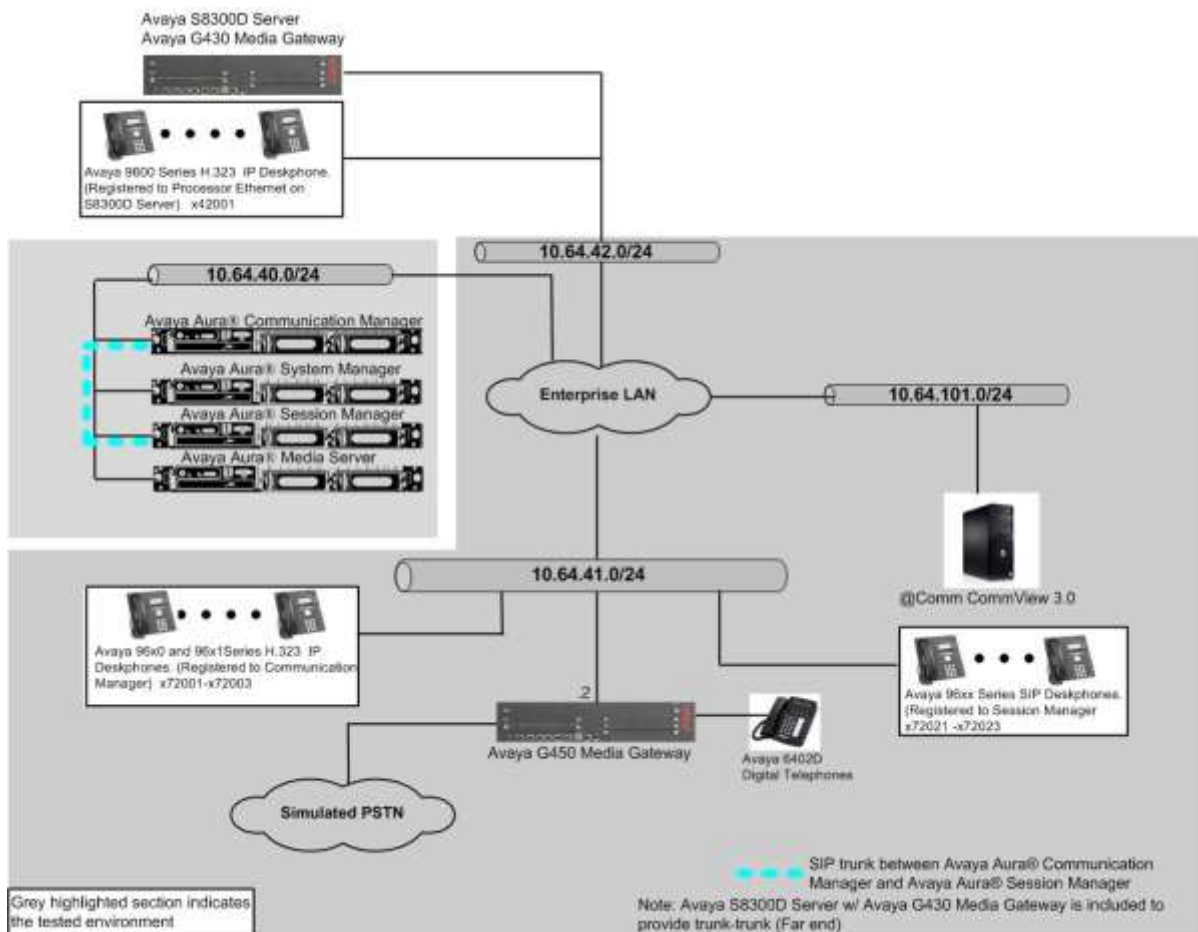


Figure 1. Test configuration of @Comm CommView with Avaya Aura® Communication Manager

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

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring call detail recording (CDR) and a SIP trunk in Communication Manager. These steps are performed through the System Access Terminal (SAT). Communication Manager is configured to generate CDR records using RSP over TCP/IP to the IP address of the server running CommView.

5.1. Configure CDR

Use the **change node-names ip** command to create a new node name, for example, **@comm**. This node name is associated with the IP Address of the server running the CommView application. Also, take note of the node name – “procr”. It will be used in the next step. The “procr” entry on this form was previously administered.

```
change node-names ip Page 1 of 2
```

IP NODE NAMES	
Name	IP Address
@comm	10.64.101.211
AMS	10.64.40.224
default	0.0.0.0
msgserver-ip	10.64.41.21
procr	10.64.40.221

Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, provide the following information:

- **Service Type:** “CDR1” [If needed, a secondary link can be defined by setting **Service Type** to CDR2.]
- **Local Node:** “procr”
- **Local Port:** “0” [The **Local Port** is fixed to 0 because Communication Manager initiates the CDR link.]
- **Remote Node:** “@comm” [The **Remote Node** is set to the node name previously defined in the **node-name ip** form.]
- **Remote Port:** “9000” [The **Remote Port** may be set to a value between 5000 and 64500 inclusive, and must match the port configured in CommView.]

```
change ip-services Page 1 of 4
```

IP SERVICES					
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port
AESVCS	y	procr	8765		
CDR1		procr	0	@comm	9000
CDR2		procr	0	rdtt-1	9004

On **Page 3** of the ip-services form, enable RSP for the CDR link by setting the **Reliable Protocol** field to “y”.

```
change ip-services Page 3 of 4
```

SESSION LAYER TIMERS						
Service Type	Reliable Protocol	Packet Timer	Resp Message	Session Connect Cntr	SPDU Cntr	Connectivity Timer
CDR1	<input checked="" type="checkbox"/>	30		3	3	60
CDR2	<input type="checkbox"/>	30		3	3	60

Enter the **change system-parameters cdr** command from the SAT to set the parameters for the type of calls to track and the format of the CDR data. The example below shows the settings used during the compliance test. Provide the following information:

- **CDR Date Format:** “month/day”
- **Primary Output Format:** “customized”
- **Primary Output Endpoint:** “CDR1”

The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See reference [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats:** “n” [Allows CDR formats to use 4.x CDR formats. If the field is set to “y”, then CDR formats utilize the 3.x CDR formats.]
- **Intra-switch CDR:** “y” [Allows call records for internal calls involving specific stations. Those stations must be specified in the **intra-switch cdr** form.]
- **Record Outgoing Calls Only:** “n” [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting:** “y” [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting:** “y” [Allows a separate call record for any portion of an incoming call that is transferred or conferenced.]
- **Call Account Code Length:** “6” [The length may be set to a value between 1 and 15. However, during the compliance test, “6” was used.]

```

change system-parameters cdr                                     Page 1 of 2
                                CDR SYSTEM PARAMETERS

Node Number (Local PBX ID): 1                                CDR Date Format: month/day
Primary Output Format: customized                            Primary Output Endpoint: CDR1
Secondary Output Format: customized                        Secondary Output Endpoint: CDR2
  Use ISDN Layouts? n                                     Enable CDR Storage on Disk? y
  Use Enhanced Formats? n                               Condition Code 'T' For Redirected Calls? n
  Use Legacy CDR Formats? n                             Remove # From Called Number? n
Modified Circuit ID Display? y                            Intra-switch CDR? y
  Record Outgoing Calls Only? n                          Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? n          Outg Attd Call Record? y
  Disconnect Information in Place of FRL? n              Interworking Feat-flag? n
  Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
  Calls to Hunt Group - Record: group-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n                           Record Agent ID on Outgoing? y
  Inc Trk Call Splitting? y                               Inc Attd Call Record? y
  Record Non-Call-Assoc TSC? n                           Call Record Handling Option: warning
  Record Call-Assoc TSC? n                               Digits to Record for Outgoing Calls: dialed
  Privacy - Digits to Hide: 0                            CDR Account Code Length: 6
Remove '+' from SIP Numbers? y

```

Since the format used for the compliance test is “customized”, the **system-parameters cdr** form will add the second page that describes the CDR format field. The following screen shows the customized format fields used during the compliance test.

```
change system-parameters cdr                                     Page 2 of 2
                                CDR SYSTEM PARAMETERS
```

Data Item - Length	Data Item - Length	Data Item - Length
1: time - 4	17: auth-code - 7	33: date - 6
2: space - 1	18: space - 4	34: space - 1
3: duration - 4	19: frl - 1	35: return - 1
4: space - 1	20: space - 1	36: line-feed - 1
5: cond-code - 1	21: in-crt-id - 3	37: null - 1
6: space - 1	22: space - 1	38: null - 1
7: code-dial - 4	23: out-crt-id - 3	39: null - 1
8: space - 1	24: space - 1	40: -
9: code-used - 4	25: feat-flag - 1	41: -
10: space - 1	26: space - 1	42: -
11: dialed-num - 15	27: attd-console - 2	43: -
12: space - 1	28: space - 1	44: -
13: calling-num - 10	29: in-trk-code - 4	45: -
14: space - 1	30: space - 1	46: -
15: acct-code - 15	31: node-num - 2	47: -
16: space - 1	32: space - 5	48: -

Record length = 115

If the **Intra-switch CDR** field is set to “y” on **Page 1** of the **system-parameters cdr** form, then use the **change intra-switch-cdr** command to define the extensions that will subject to call detail records. In the **Extension** field, enter the specific extensions whose usage will be tracked.

```
change intra-switch-cdr                                     Page 1 of 3
                                INTRA-SWITCH CDR
```

Extension	Assigned Members:	6	of 1000	administered
Extension	Extension	Extension	Extension	Extension
72001				
72002				
72003				
72021				
72022				
72023				

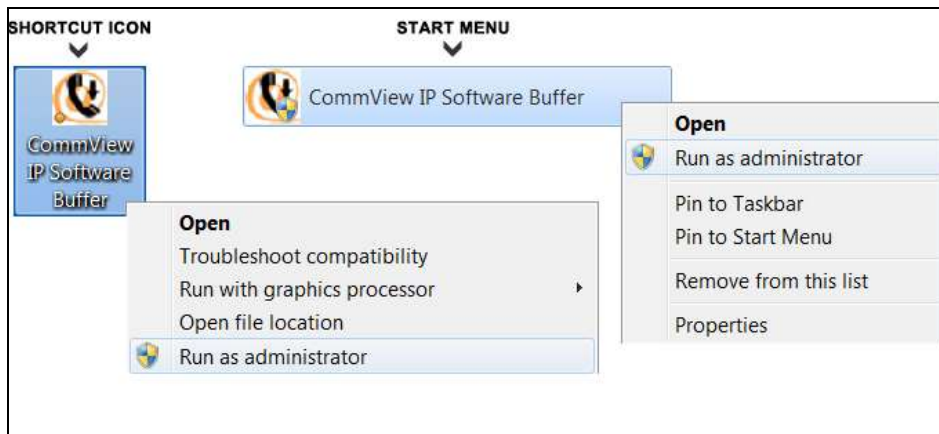
6. Configure @Comm CommView

This section describes the operation of CommView to receive CDR data from Communication 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 IP Software Buffer
- Start CommView Services
- View CommView CDR Report

6.1. Configure CommView IP Software Buffer

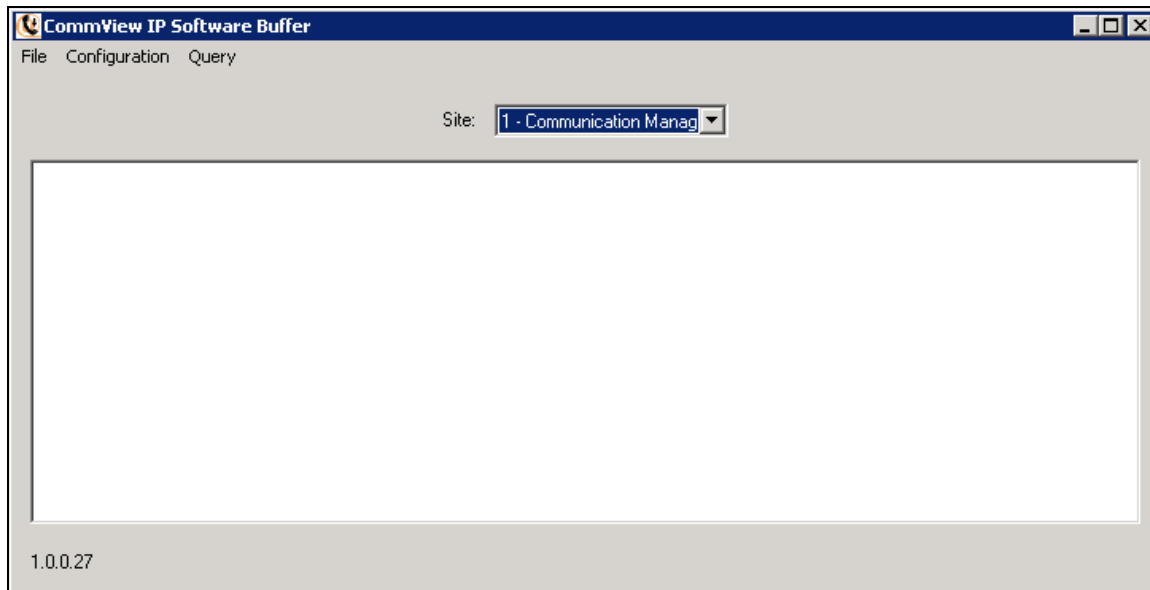
To configure CommView IP Software Buffer to communicate with Communication Manager, navigate to **SHORT CUT ICON** or **START MENU** → **CommView IP Software Buffer**. Right mouse click the icon and choose “Run as administrator”.



The **CommView IP Software Buffer** screen is displayed. Select “1 – Communication 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.



As a default, **Site Number** displays “1”, and **Site Name** displays “Communication Manager”. Select “Avaya Aura CM” for the **Source Type** field.

Click **OK**.

Input Configuration

Site Number: 1 Site Name: Communication Manager

Source Type: Avaya Aura CM

Serial COM Port:

Port: Baud Rate:

Parity: End of Record: Timeout:

TCP/IP:

Server: Port:

ODBC:

DSN: User: Password:

Poll Interval: Advanced

File Transfer:

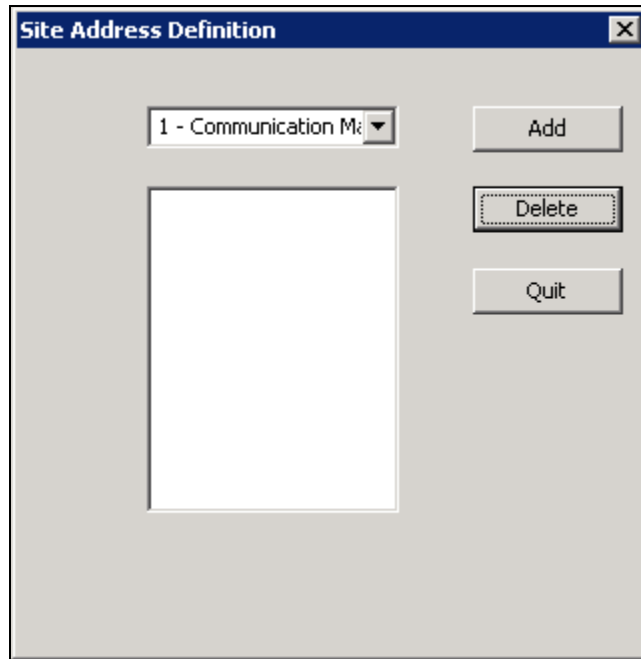
Path: File Mask: Browse Path Transfer Interval:

Start Date: 2/ 5/2016 Start Time: 10:48:21 AM

Delete Source Files: Last Transfer Time:

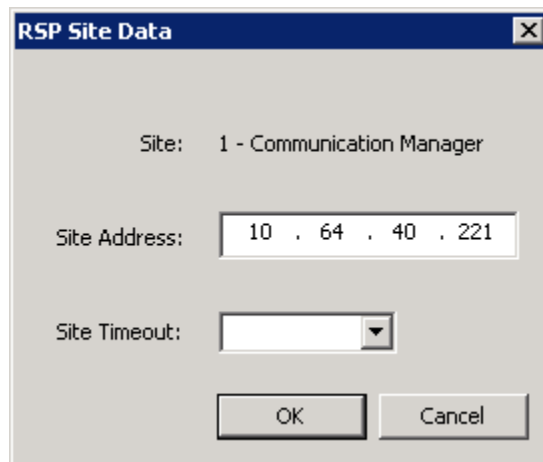
OK Cancel

From the **CommView IP Software Buffer** screen, navigate to **Configuration → RSP Setup → RSP Site Address**, and the **Site Address Definition** screen is displayed. Click the **Add** button to display the **RSP Site Data** screen.

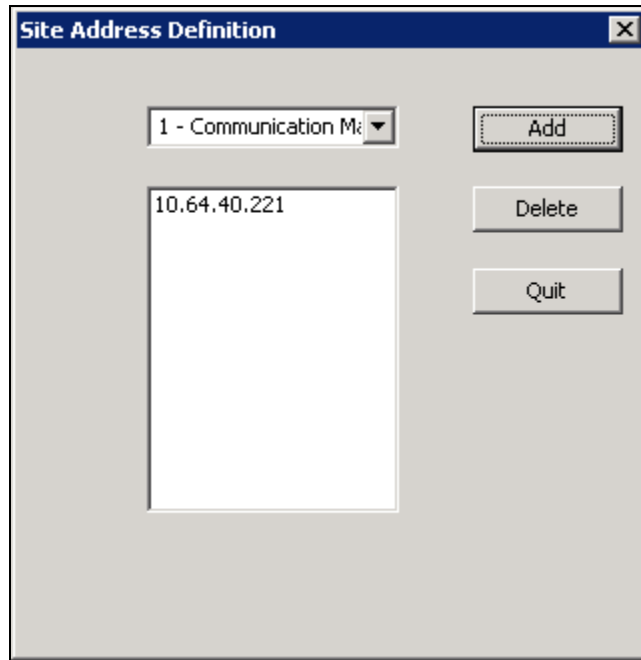


In the **RSP Site Data** screen, enter the IP address of Communication Manager on the **Site Address** field.

Click **OK**.

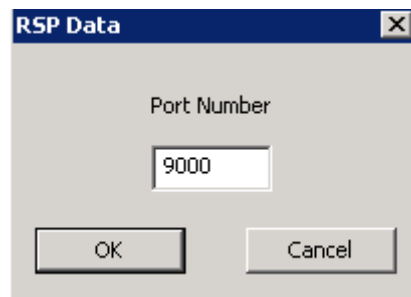


The following screen shows the **Site Address Definition** screen, after the IP address is configured.



From the **CommView IP Software Buffer** screen, navigate to **Configuration** → **RSP Setup** → **RSP Port**, and the **RSP Data** screen is displayed. Enter the listening port number for CDR data. This port number should match the port number from Avaya side in **Section 5.1**.

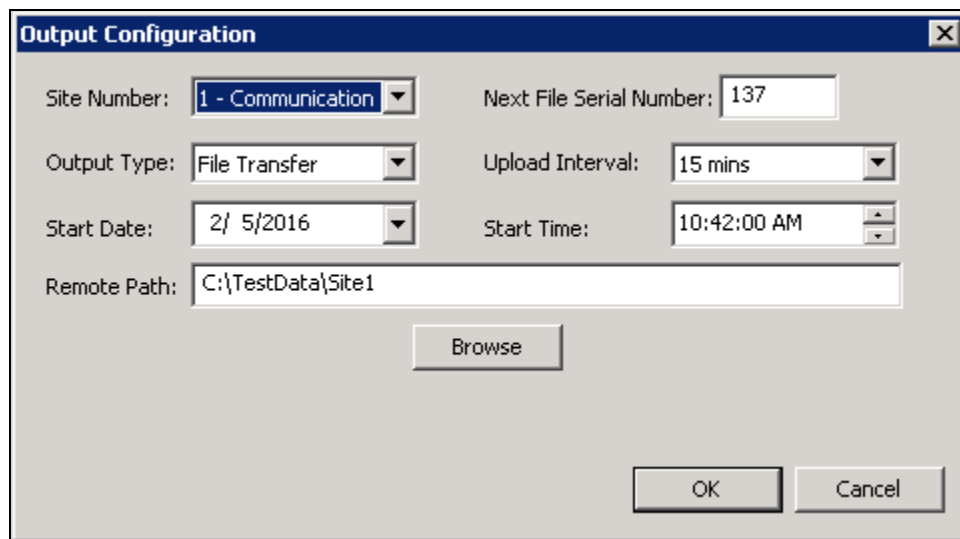
Click **OK**.



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, “15mins” was used.
- **Start Date:** Set the correct date.
- **Start Time:** Set the correct time.
- **Remote Path:** Specify the directory whether raw data is stored.

Click **OK**.



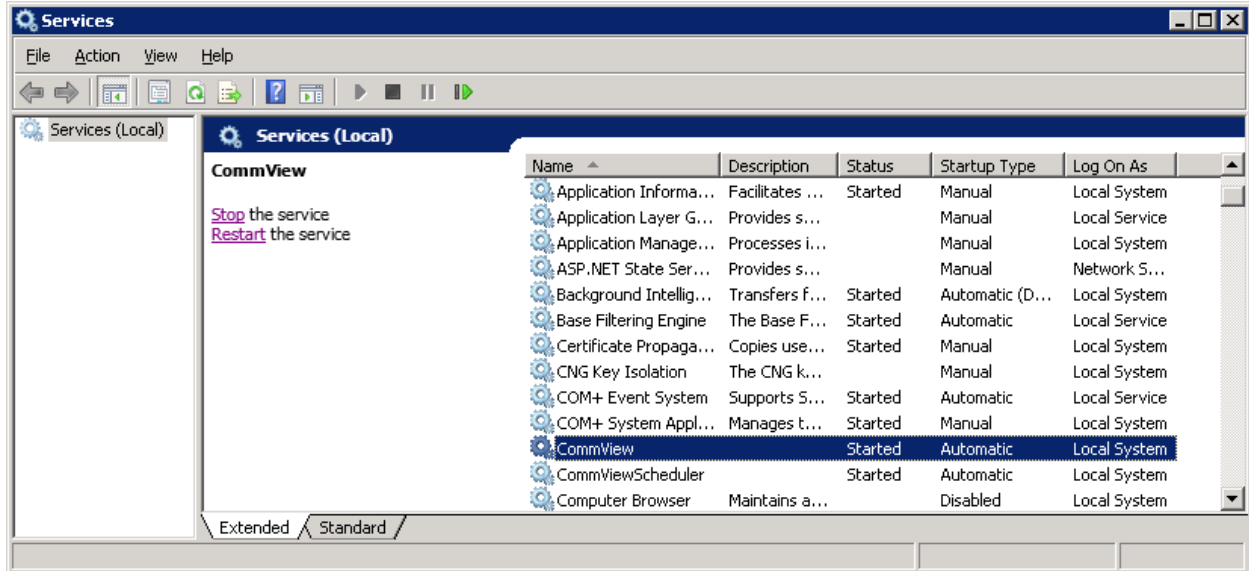
The screenshot shows the "Output Configuration" dialog box with the following settings:

Site Number:	1 - Communication	Next File Serial Number:	137
Output Type:	File Transfer	Upload Interval:	15 mins
Start Date:	2/ 5/2016	Start Time:	10:42:00 AM
Remote Path:	C:\TestData\Site1		

Buttons: Browse, OK, Cancel

6.2. Start CommView Services

To start CommView services, navigate to **Start → Administrative Tools → Services**. Verify **CommView** and **CommView Scheduler** services are started.



6.3. View CommView CDR Report

There are two ways to view CDR report:

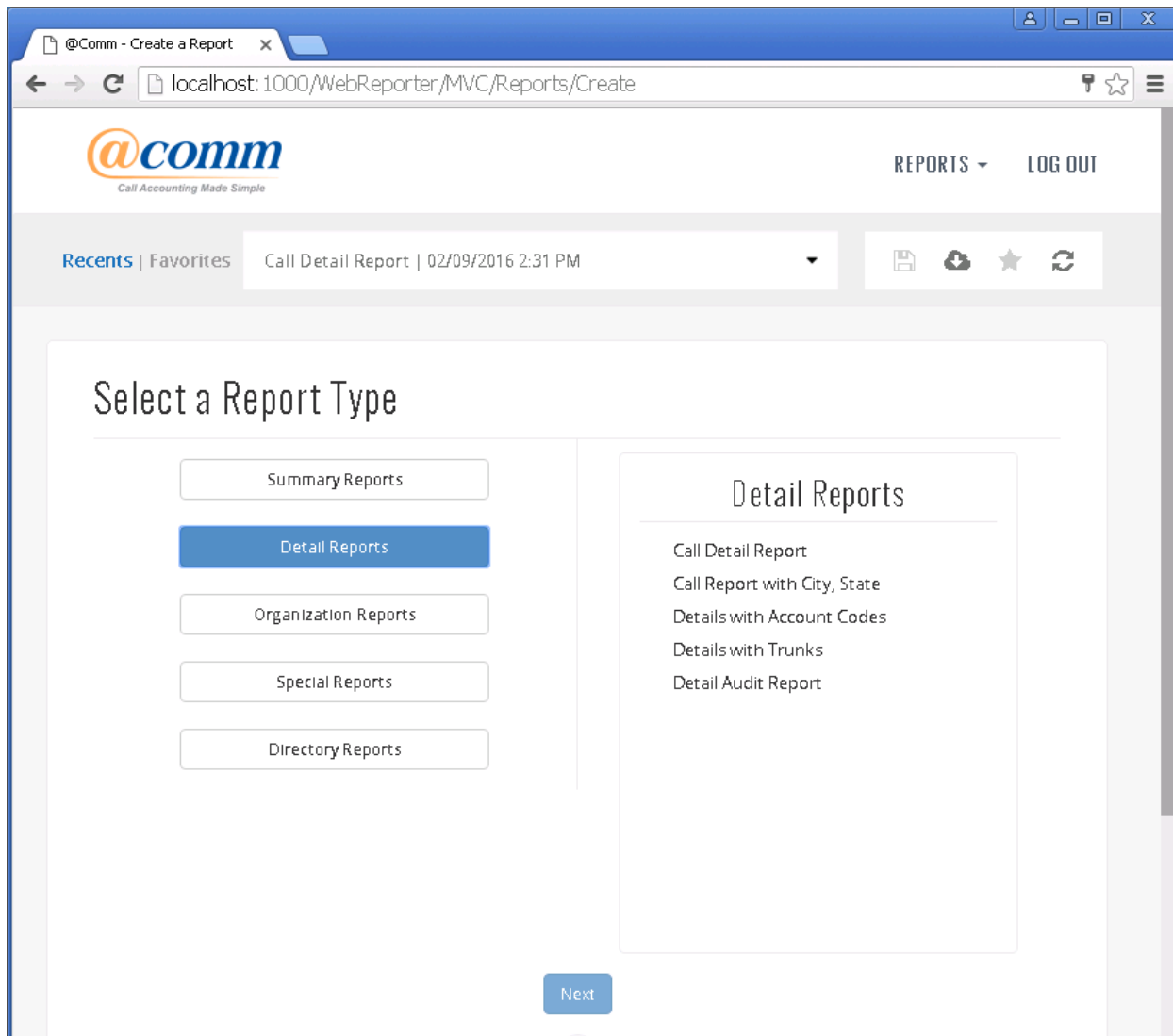
- CommView CDR Report
- WebReporter CDR Report

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.



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.

The screenshot shows the @comm web interface for creating a Call Detail Report. The page title is "Create a Call Detail Report" and it is part of a "Report Types" section. The interface includes a navigation bar with "Recents | Favorites" and "Call Detail Report | 02/09/2016 2:31 PM". The main content area is divided into two tabs: "Date Range" and "Report Sort Order". The "Date Range" tab is active, showing a "Select a date range" section with a "None" dropdown and a "Use most recent days?" checkbox. Below this are two rows of date and time inputs: "From" (02/03/2016, 12:00 AM) and "To" (02/17/2016, 11:59 PM). A checkbox labeled "Include all hours between dates?" is also present. To the right is a "Current Selections" panel showing the selected date range and sorting options: "Outer Sort", "Inner Sort", and "Display Navigation Tree". A "Reset" button is located below the "Current Selections" panel. At the bottom of the page, there are radio buttons for "Screen", "Printer", "File", and "Email", and two buttons: "Run report" and "Schedule".

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

@comm 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	0.0	\$0.01
1000	02/03/16	08:57 am		Incoming	*	0.0	0.0	\$0.00
72002	02/03/16	08:57 am	1	303-538-2324	BROOMFIELD, CO	0.0	0.0	\$0.01
72002	02/03/16	08:57 am		Incoming	+42001	0.0	0.0	\$0.00
72002	02/03/16	08:57 am		Incoming	+42001	0.3	0.0	\$0.00
72002	02/03/16	08:57 am	1	303-538-2324	BROOMFIELD, CO	0.1	0.0	\$0.01
72002	02/03/16	08:06 am		Incoming	+42001	0.4	0.0	\$0.00
72002	02/03/16	09:06 am	1	303-538-2324	BROOMFIELD, CO	0.2	0.0	\$0.01
72021	02/03/16	09:07 am		Incoming	+42001	0.2	0.0	\$0.00
72021	02/03/16	09:07 am		Incoming	+42001	0.1	0.0	\$0.00
72021	02/03/16	09:08 am	1	303-538-2324	BROOMFIELD, CO	0.0	0.0	\$0.01
72021	02/03/16	09:30 am		72002		0.2	0.0	\$0.00
72002	02/03/16	09:30 am		Incoming	+72021	0.2	0.0	\$0.00
72021	02/03/16	09:30 am		Incoming	+72002	0.2	0.0	\$0.00
72002	02/03/16	09:31 am		72021		0.8	0.0	\$0.00
72021	02/03/16	09:31 am		Incoming	+72002	0.0	0.0	\$0.00
72021	02/03/16	09:31 am		72002		0.8	0.0	\$0.00
72022	02/03/16	09:31 am		72021		0.2	0.0	\$0.00
72021	02/03/16	09:31 am		Incoming	+72022	0.2	0.0	\$0.00
42001	02/03/16	09:33 am		72002		0.3	0.0	\$0.00
72002	02/03/16	09:33 am		Incoming	+42001	0.3	0.0	\$0.00

7. Verification Steps

The following steps may be used to verify the configuration:

- Check the CDR status, by running the **status cdr-link** command in Communication Manager, and verify that the **Link State** is “up” and **Reason Code** is “OK”.

```

status cdr-link
                                CDR LINK STATUS
                                Primary                Secondary
Link State: up                    down
Number of Retries:                999
Date & Time: 2016/02/04 12:27:24  2016/02/05 11:44:02
Forward Seq. No: 18                0
Backward Seq. No: 0                0
CDR Buffer % Full: 0.00              0.05
Reason Code: OK                    CDR connection is closed
  
```

- Make several calls between two Communication Manager, and verify that call records were collected from CommView. The following raw data page may be used to verify. The raw data page is located in the **c:\TestData\Site1** directory.

```

Site100012.asc - Notepad
File Edit Format View Help
1534 0002 7 9 1080 13035382324 72002 0 005 0 1 020216
1534 0004 9 72002 42001 0 001 0 1010 1 020216
1535 0004 9 72002 42001 0 001 0 1010 1 020216
1535 0002 7 9 1080 13035382324 72002 0 005 0 1 020216
1539 0005 9 72002 42001 0 001 0 1010 1 020216
1539 0002 7 9 1080 13035382324 72002 0 005 0 1 020216
1539 0001 7 1010 42001 72002 0 006 0 1 020216
1539 0000 7 1010 42001 72021 0 006 0 1 020216
1539 0003 0 72002 72021 88888 0 005 0 1 020216
1544 0001 9 72002 42001 0 001 0 1010 1 020216
1545 0000 7 9 1080 13035382324 1010 0 001 005 0 1010 1 020216
1545 0000 9 1080 0 001 0 1010 1 020216
1545 0000 7 9 1080 13035382324 72002 0 001 005 4 1 020216
1545 0000 9 72002 42001 0 001 0 1010 1 020216
1552 0000 9 1080 0 001 0 1010 1 020216
1552 0000 7 9 1080 13035382324 1010 0 001 005 0 1010 1 020216
1552 0000 7 9 1080 13035382324 72002 88888 0 005 0 1 020216
00:00 02/03
0857 0001 7 9 1080 13035382324 1010 0 001 005 0 1010 1 020316
0857 0000 9 1080 0 001 0 1010 1 020316
0857 0000 7 9 1080 13035382324 72002 0 001 005 4 1 020316
0857 0000 9 72002 42001 0 001 0 1010 1 020316
0858 0001 7 9 1080 13035382324 72002 0 005 0 1 020316
Ln 1, Col 1
  
```

8. Conclusion

These Application Notes describe the procedures for configuring @Comm CommView to collect call detail records from Avaya Aura® Communication Manager. Testing was successful.

9. References

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

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 1 Release 7.0, August 2015, available at <http://support.avaya.com>.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 7.0, June 2015, Document 555-245-205, Issue 2 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**.

©2016 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.