Avaya Solution & Interoperability Test Lab

Application Notes for Configuring @Comm CommView Web with Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration procedures required to allow @Comm CommView Web to collect call detail records (CDR) from Avaya Communication Manager running on Avaya Media Servers using Avaya Reliable Session Protocol (RSP) over TCP/IP. The CommView Web collects, stores and processes these call records to provide usage analysis, call costing and billing capabilities.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describes a compliance-tested call detail recording (CDR) solution comprised of Avaya Communication Manager and @Comm CommView Web. The CommView Web is a call accounting software application that uses call detail records to provide reporting capabilities to business and IT managers to track and manage call usage and telecom expenses.

CommView Web is comprised of three components. The first component, the CommView Avaya Server application, resides on a Microsoft Windows PC at the customer's premises. Avaya Communication Manager communicates to this component via an Avaya Reliable Session Protocol (RSP) session over the local TCP/IP network. The CommView Avaya Server application runs as a background service that terminates the RSP protocol, collects the call records from Avaya Communication Manager, and stores the records in a text file.

The second component, the CommView Software Buffer also runs as a background service on the same PC as the CommView Avaya Server and acts as an SFTP Client. It periodically transmits the CDR data file collected by the CommView Avaya Server across the Internet via SFTP to a @Comm Hosted Server.

Once the file is on the @Comm-hosted server, it is available for processing by the third component, the CommView main application. The CommView main application periodically pulls the data from the text file, parses the data and places the information in a database. The database information is then used to provide the reporting capabilities. The resulting processing of the CDR data by the CommView Web is then made available to the user by a Web interface. From a standard web browser, using a @Comm provided account and password, the user can view call information and run reports on the CDR records collected from Avaya Communication Manager.

Avaya Communication Manager can generate call detail records for intra-switch calls, inbound trunk calls and outbound trunk calls. In addition, split records can be generated for transferred calls and conference calls. The CommView Web can support any CDR format provided by Avaya Communication Manager. As part of the CommView Web product registration process, @Comm technical support creates a custom PBX configuration file to accurately parse the CDR data. For the compliance testing, the expanded format was utilized.

Figure 1 illustrates a sample configuration that was used for the compliance test. The configuration consists of three Avaya Media Servers running Avaya Communication Manager. Site A is comprised of Avaya Communication Manager runs on Avaya S8700 Servers with an Avaya G650 Media Gateway. Site B is comprised of Avaya Communication Manager runs on an Avaya S8300 Server residing in an Avaya G700 Media Gateway. Each Avaya Communication Manager is connected to an IP network comprised of an Extreme Networks Summit 48 Layer III switch and Avaya C363T-PWR Converged Stackable Switch.

A Microsoft Windows 2000 PC running the CommView Avaya Server and CommView Software Buffer is also connected to the IP network. The CommView Avaya Server has a RSP session established to Avaya Communication Manager running on the Avaya S8700 and S8300 Servers to collect CDR records. This same PC has a second network interface card (NIC) that is connected to the Internet to provide connectivity to the @Comm Hosted Server.

The CommView Web can collect CDR data from multiple sources by using multiple instances of the CommView Software Buffer and CommView Avaya Server.

Each system has trunks and phones associated with it to generate calls. Avaya 4600 Series IP Telephones, Avaya 9600 Series IP Telephones, and Avaya 6400D Series Digital Telephones are registered to both Avaya S8700 and S8300 Servers. In addition, there is an H.323 IP trunk established between the two media servers.

Site C is comprised of an Avaya S8300 Server with an Avaya G350 Media Gateway, which has connections to an Avaya 4600 Series IP Telephone and Avaya 6400D Series Digital Telephone. The Avaya S8300 Server, installed with LSP license, is setup as a LSP to Site A.

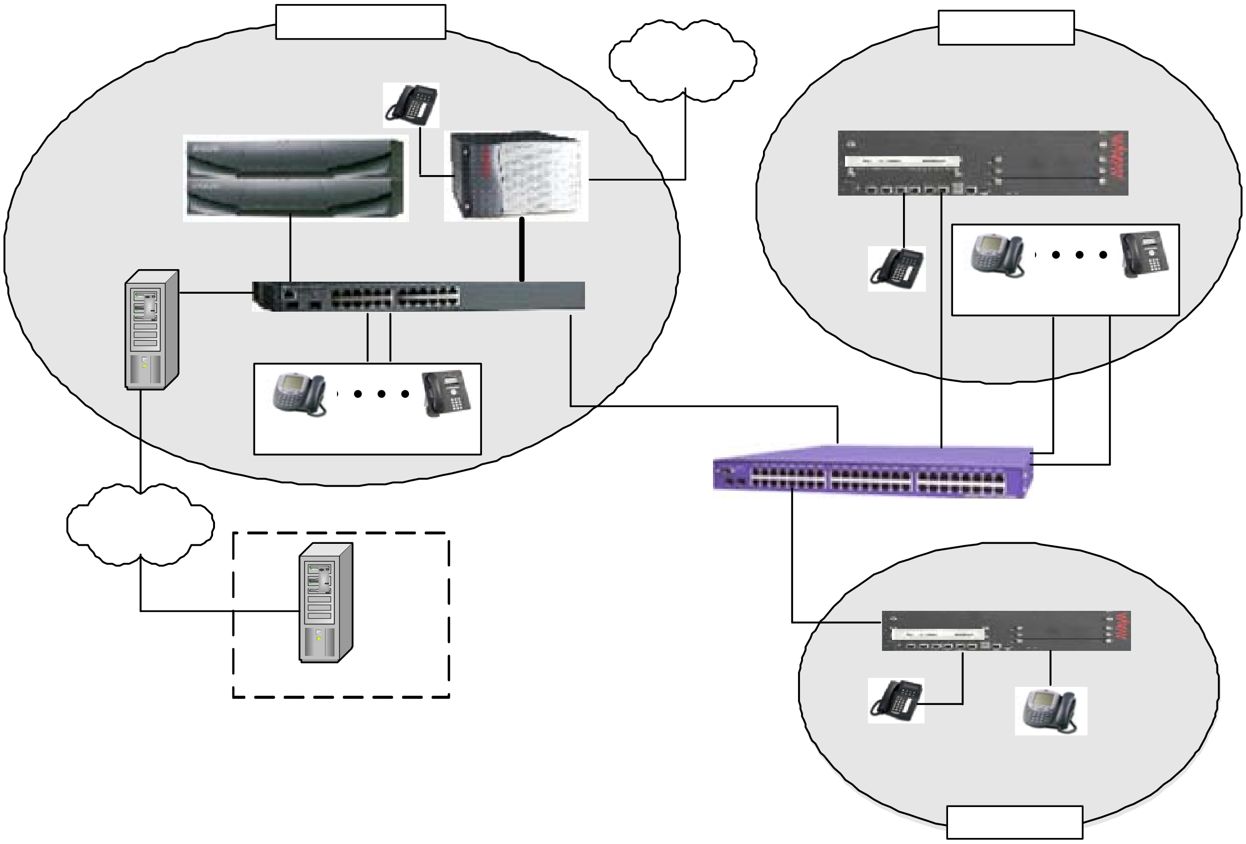


Figure 1: Test configuration collecting CDR data from multiple servers

2. Equipment and Software Validated

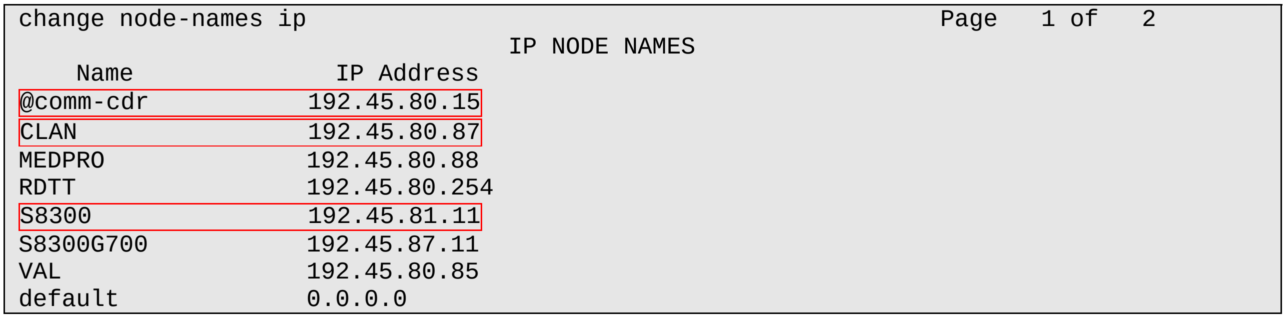
The following equipment and software/firmware were used for the test configuration provided.

Equipment		Software/Firmware
Avaya S8700 Servers		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface TN799DP CLAN Interface TN2302AP IP Media Processor TN2602AP IP Media Processor	HW11 FW030 HW01 FW017 HW20 FW108 HW02 FW007
Avaya S8300 Media Server with Avaya G700 Media Gateway		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya S8300 Media Server with Avaya G350 Media Gateway (with LSP license)		Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya 4600 Series IP Telephones		
	4620 (H.323) 4625 (H.323)	2.704 2.8
Avaya 9600 Series IP Telephones		
	9630 (H.323) 9650 (H.323)	1.5 1.5
Avaya 6400D Series Digital Telephones		-
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Networks Summit 48		4.1.21
@Comm CommView Web		2.02

3. Configure Avaya Communication Manager

This section describes the procedure for configuring call detail recording (CDR) in Avaya Communication Manager. These steps are performed through the System Access Terminal (SAT). These steps describe the procedure used for the Avaya S8700 Server. All steps are the same for the other media servers unless otherwise noted. Avaya Communication Manager will be configured to generate CDR records using RSP over TCP/IP to the IP address of the PC running the CommView Avaya Server. For the Avaya S8700 Server, the RSP link originates at the IP address of the CLAN board. For the Avaya S8300 Media Server, the RSP link originates at the IP address of the local media server (with node-name – “procr”).

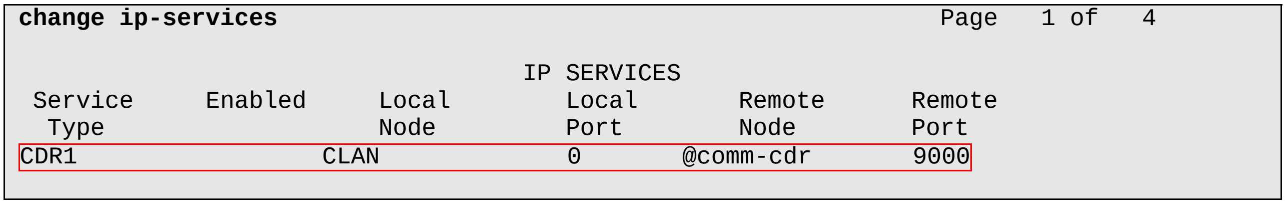
Use the **change node-names ip** command to create a new node name, for example, **@comm-cdr**. This node name is associated with the IP Address of the PC running the CommView Avaya Server application. Also, take note of the node name – "CLAN". It will be used in the next step. The CLAN entry on this form was previously administered. S8300 is an LSP licensed Avaya S8300 Server.



```
change node-names ip                                           Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
@comm-cdr               192.45.80.15
CLAN                    192.45.80.87
MEDPRO                  192.45.80.88
RDTT                    192.45.80.254
S8300                   192.45.81.11
S8300G700               192.45.87.11
VAL                     192.45.80.85
default                 0.0.0.0
```

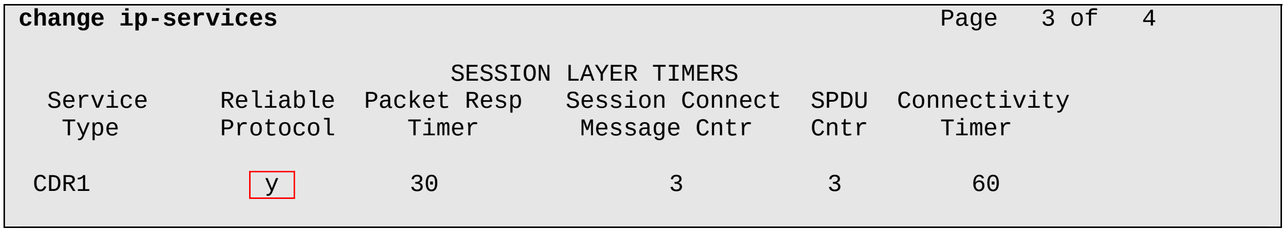
Use the **change ip-services** command to define the CDR link to use the RSP over TCP/IP. To define a primary CDR link, the following information should be provided:

- Service Type: **CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- Local Node: **CLAN** [For the Avaya S8700 Server, the Local Node is set to the node name of the CLAN board. If the Avaya S8300 Server was utilized, set the Local Node to **procr**.]
- Local Port: **0** [The Local Port is fixed to 0 because Avaya Communication Manager initiates the CDR link.]
- Remote Node: **@comm-cdr** [The Remote Node is set to the node name previously defined.]
- Remote Port: **9000** [The Remote Port may be set to a value between 5000 and 64500 inclusive, and must match the port configured in the CommView Avaya Server.]



```
change ip-services                                             Page   1 of   4

                                   IP SERVICES
 Service      Enabled      Local         Local        Remote       Remote
  Type                     Node          Port         Node         Port
CDR1                   CLAN              0        @comm-cdr        9000
```

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



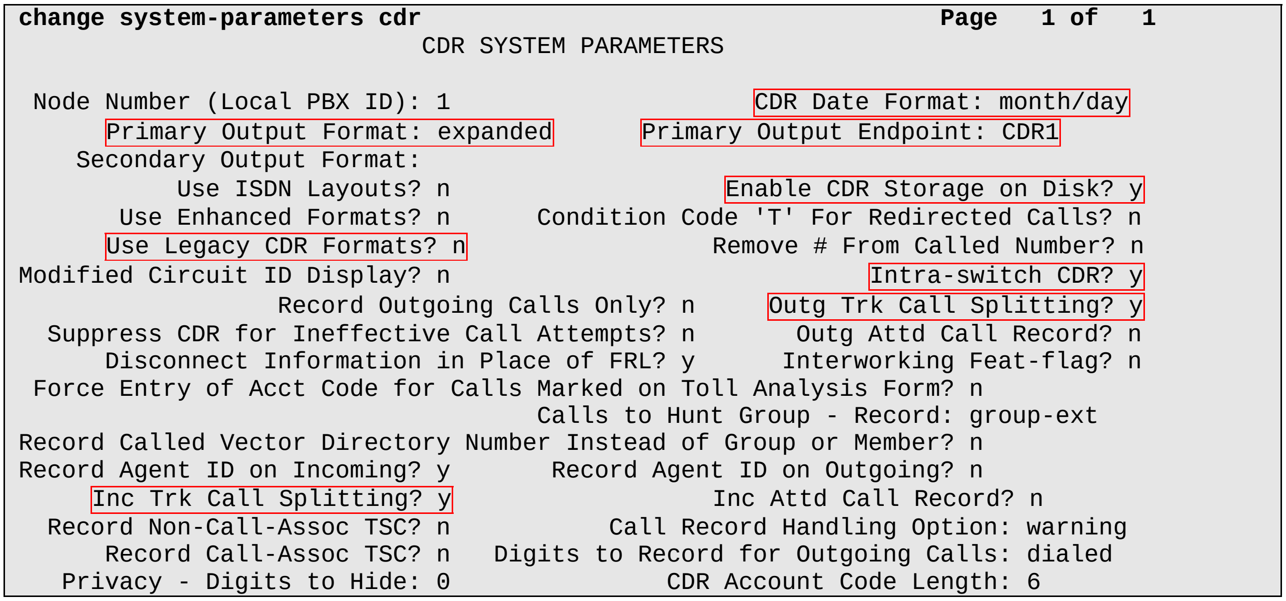
```
change ip-services                                             Page   3 of   4

                              SESSION LAYER TIMERS
  Service      Reliable  Packet Resp   Session Connect  SPDU  Connectivity
   Type        Protocol    Timer        Message Cntr    Cntr     Timer

 CDR1             y         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: **expanded**
- 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.

- Enable CDR Storage on Disk?: **y** [Enable the Survivable CDR feature. Default is **n**.]
- 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.]



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

 Node Number (Local PBX ID): 1                     CDR Date Format: month/day
      Primary Output Format: expanded      Primary Output Endpoint: CDR1
    Secondary Output Format:
           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? n                             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? n
      Disconnect Information in Place of FRL? y      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? y       Record Agent ID on Outgoing? n
     Inc Trk Call Splitting? y                  Inc Attd Call Record? n
  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
```

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 be subject to call detail records. In the Assigned Members field, enter the specific extensions whose usage will be tracked. To simplify the process of adding multiple extensions in the Assigned Members field, the “Intra-switch CDR by COS” feature may be utilized in the SPECIAL APPLICATIONS form under the system-parameters section. To utilize this feature, contact an authorized Avaya account representative to obtain the license.

```
change intra-switch-cdr                                          Page   1 of   2
                           INTRA-SWITCH CDR

Assigned Members:   4    of 5000   administered
  1: 22001    19:          37:          55:          73:           91:
  2: 22002    20:          38:          56:          74:           92:
  3: 22003    21:          39:          57:          75:           93:
  4: 22007    22:          40:          58:          76:           94:
  5:          23:          41:          59:          77:           95:
  6:          24:          42:          60:          78:           96:
  7:          25:          43:          61:          79:           97:
```

For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Use the **change trunk-group *n*** command, where ***n*** is the trunk group number, to verify that the CDR Reports field is set to **y**. This applies to all types of trunk groups.

```
change trunk-group 80                                            Page   1 of  20
                                TRUNK GROUP

Group Number: 80                  Group Type: isdn          CDR Reports: y
  Group Name: OUTSIDE CALL               COR: 1        TN: 1        TAC: 103
   Direction: two-way        Outgoing Display? y        Carrier Medium: PRI/BRI
 Dial Access? y                Busy Threshold: 255       Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n            TestCall ITC: rest
                         Far End Test Line No:
TestCall BCC: 4
TRUNK PARAMETERS
         Codeset to Send Display: 6     Codeset to Send National IEs: 6
        Max Message Size to Send: 260   Charge Advice: none
  Supplementary Service Protocol: a     Digit Handling (in/out): enbloc/enbloc

            Trunk Hunt: cyclical
                                                   Digital Loss Group: 13
Incoming Calling Number - Delete:     Insert:                Format:
             Bit Rate: 1200        Synchronization: async    Duplex: full
 Disconnect Supervision - In? y  Out? y
 Answer Supervision Timeout: 0
```

Repeat above steps for the Avaya S8300 Server running Avaya Communication Manager. The CDR format and port number used for the CDR link must be the same for each Avaya Communication Manager sending CDR records to the CommView Avaya Server.

4. Configure @Comm CommView Web

This section describes the configuration of @Comm CommView Web. It is comprised of three components: CommView Software Buffer, CommView Avaya Server and the CommView main application. The user installs CommView Software Buffer and CommView Avaya Server from a single software bundle which is downloaded from the @Comm website onto a local PC. Each of these two components is configured separately as shown below. The CommView main application resides on a server at a @Comm site and thus all installation and configuration is performed by @Comm for this component.

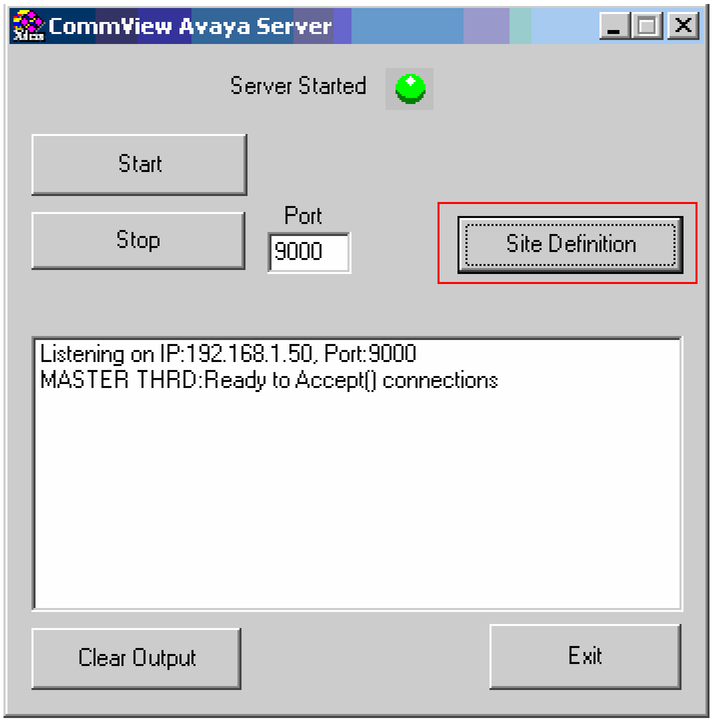
4.1. CommView Software Buffer

@Comm installs, configures, and customizes the CommView Software Buffer application for their end customers. @Comm engineer pre-configures which IP address (@Comm-hosted server) to send the raw data that is received from Avaya Communication manager. The protocol that is used to send raw data from the CommView Software Buffer to the @Comm-hosted server is SFTP. Thus, when the CommView bundled software is installed, the CommView Software Buffer application is automatically installed and configured.

4.2. CommView Avaya Server Application

This section describes the configuration steps for the CommView Avaya Server component of CommView Web. The CommView Avaya Server is installed as a service under Windows that will start automatically. When CommView Avaya Server starts running, the following window is displayed.

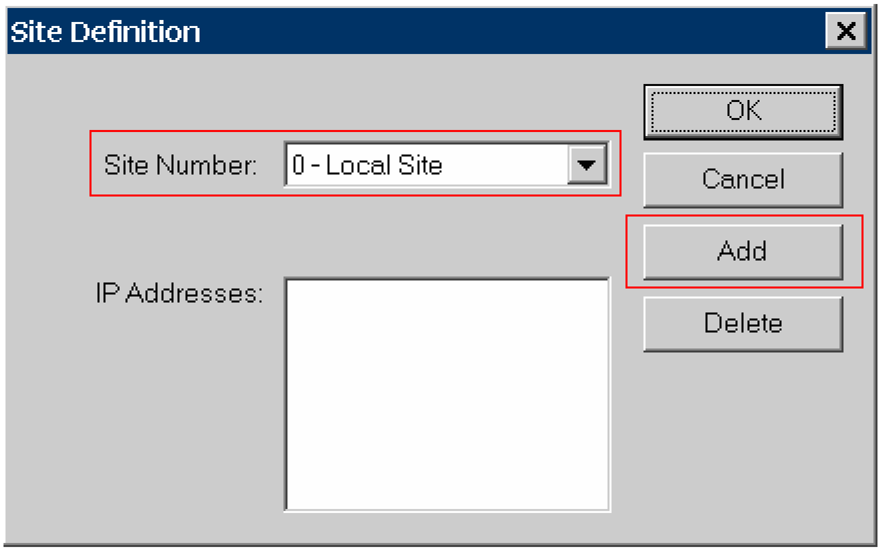
To begin configuration, select the **Site Definition** button.



Port: 9000

```
Listening on IP:192.168.1.50, Port:9000
MASTER THRD:Ready to Accept() connections
```

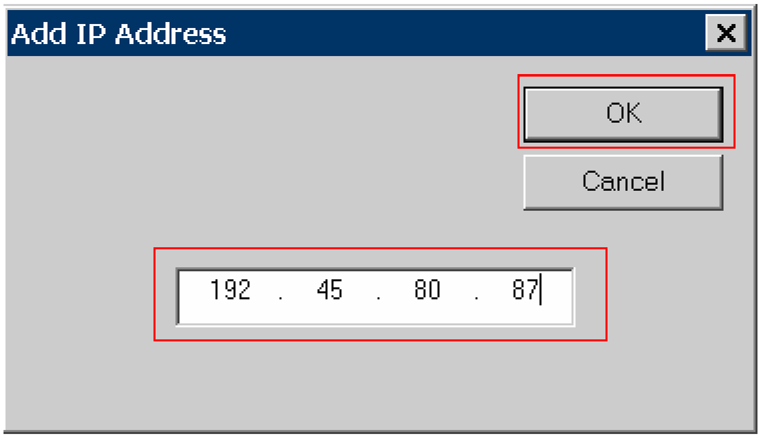
Using the drop-down menu, select **0 - Local Site** for the Site Number field. For the IP Address, enter the IP address of the local site by selecting the **Add** button.



Site Number: 0 - Local Site

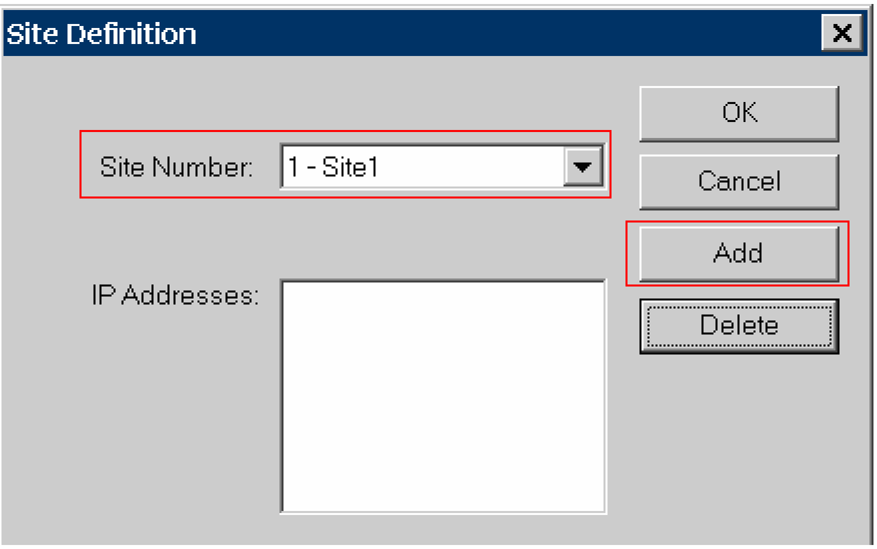
IP Addresses:

In the compliance test, this is the IP address of the Avaya S8700 Server which maps to node name "CLAN" in Avaya Communication Manager.
Select **OK**.



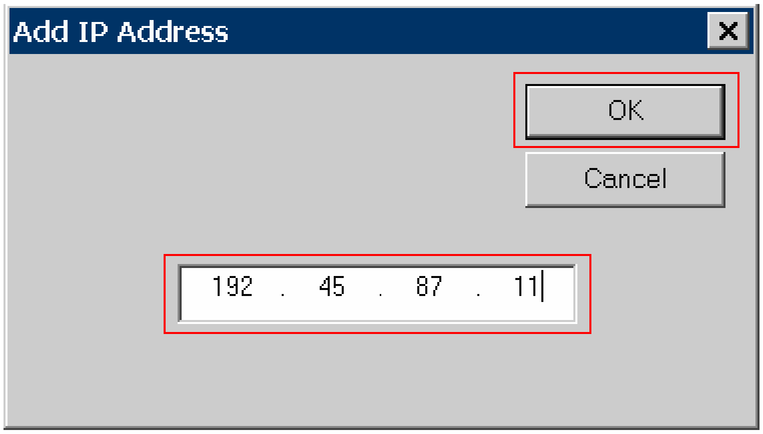
192 . 45 . 80 . 87

Repeat the previous step for the second site that was created. From the Site Number drop-down menu, select **1 – Site1**. For the IP Address, enter the IP address of the site named Site1 by selecting the **Add** button.



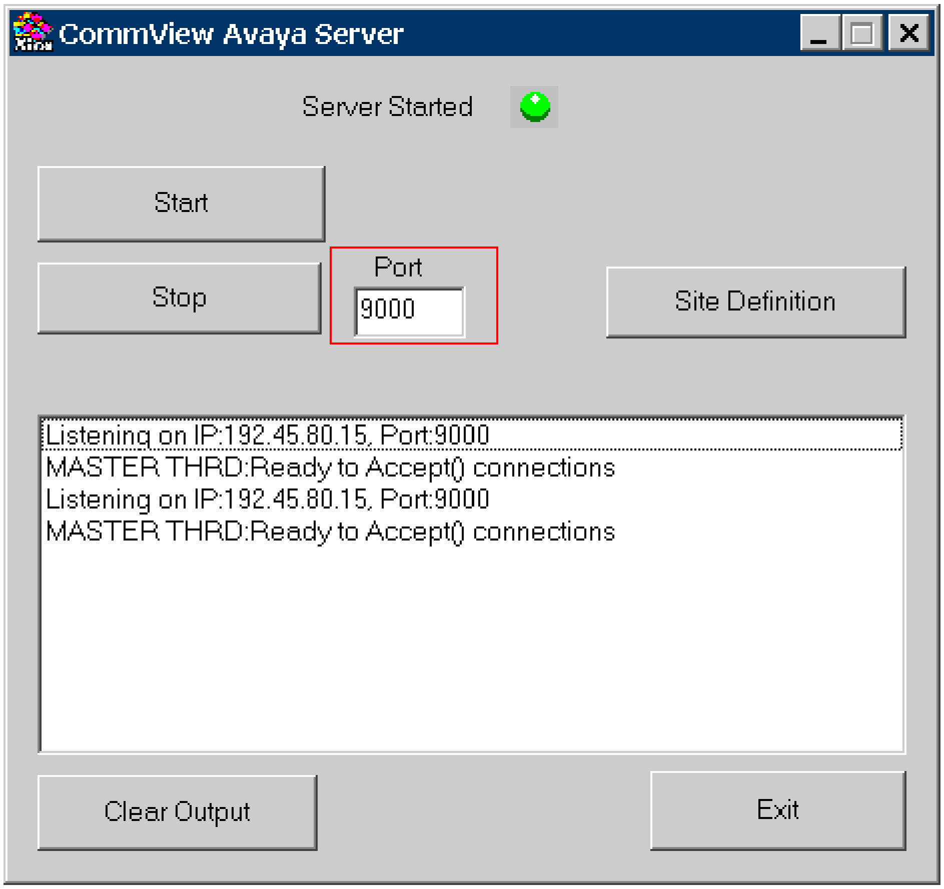
Site Number: 1 - Site1

In the compliance test, this is the IP address of the procr interface in the Avaya S8300 Server that is connected to this network.
Select **OK**.



192 . 45 . 87 . 11

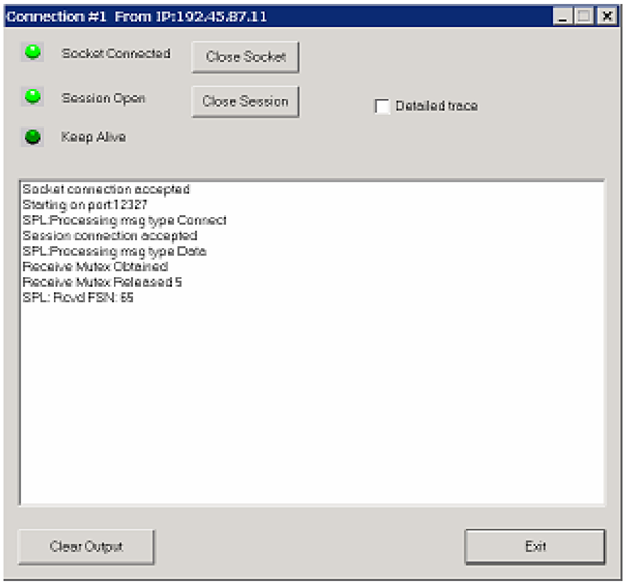
Set the port number to match the port number set on Avaya Communication Manager for use by the CDR link. Refer to Section 3. All sites must use the same port number.



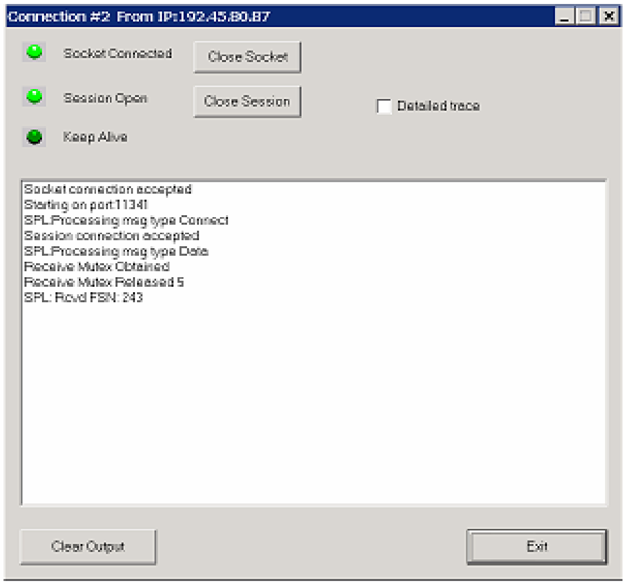
Port: 9000

```
Listening on IP:192.45.80.15, Port:9000
MASTER THRD:Ready to Accept() connections
Listening on IP:192.45.80.15, Port:9000
MASTER THRD:Ready to Accept() connections
```

The CommView Avaya Server will listen for connections from each site. The following window will appear for each site that has established a connection to the CommView Avaya Server. This window will remain open. Do not select **Exit**, otherwise the connection will drop.



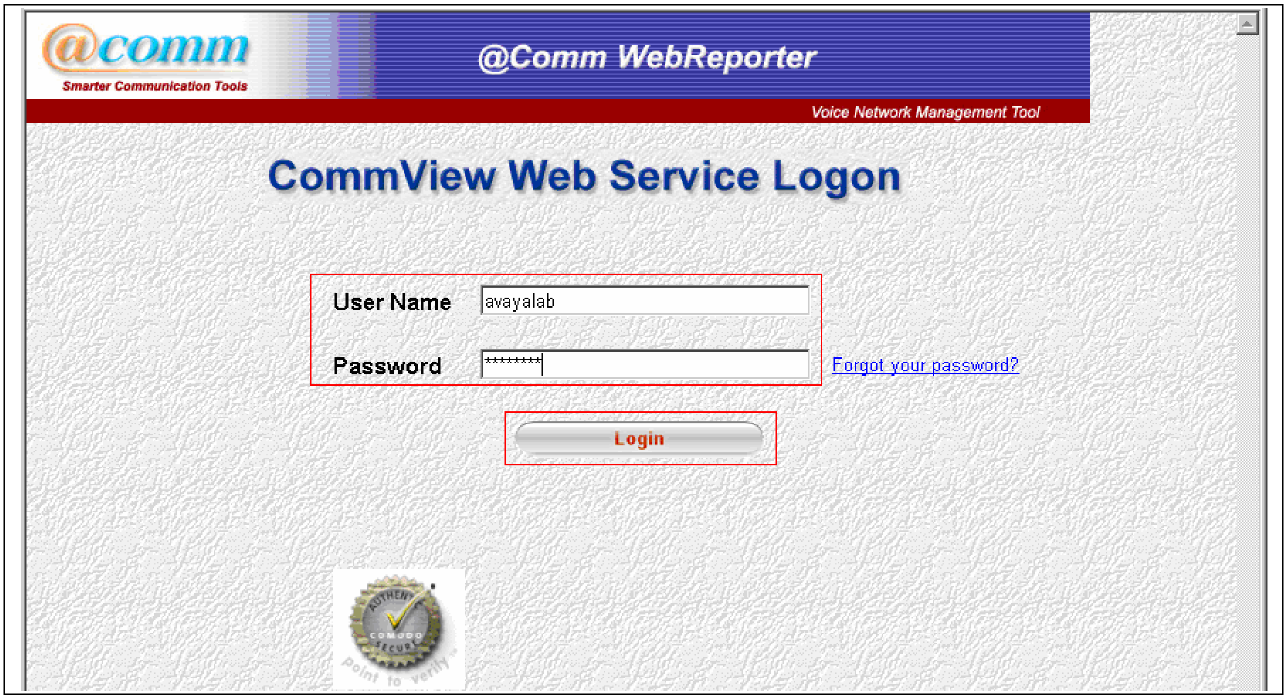
```
Socket connection accepted
Starting on port 12327
SPL:Processing msg type Connect
Session connection accepted
SPL:Processing msg type Data
Receive Mutex Obtained
Receive Mutex Released 5
SPL: Rcvd FSN: 65
```



```
Socket connection accepted
Starting on port 11341
SPL:Processing msg type Connect
Session connection accepted
SPL:Processing msg type Data
Receive Mutex Obtained
Receive Mutex Released 5
SPL: Rcvd FSN: 243
```

4.3. CommView Report

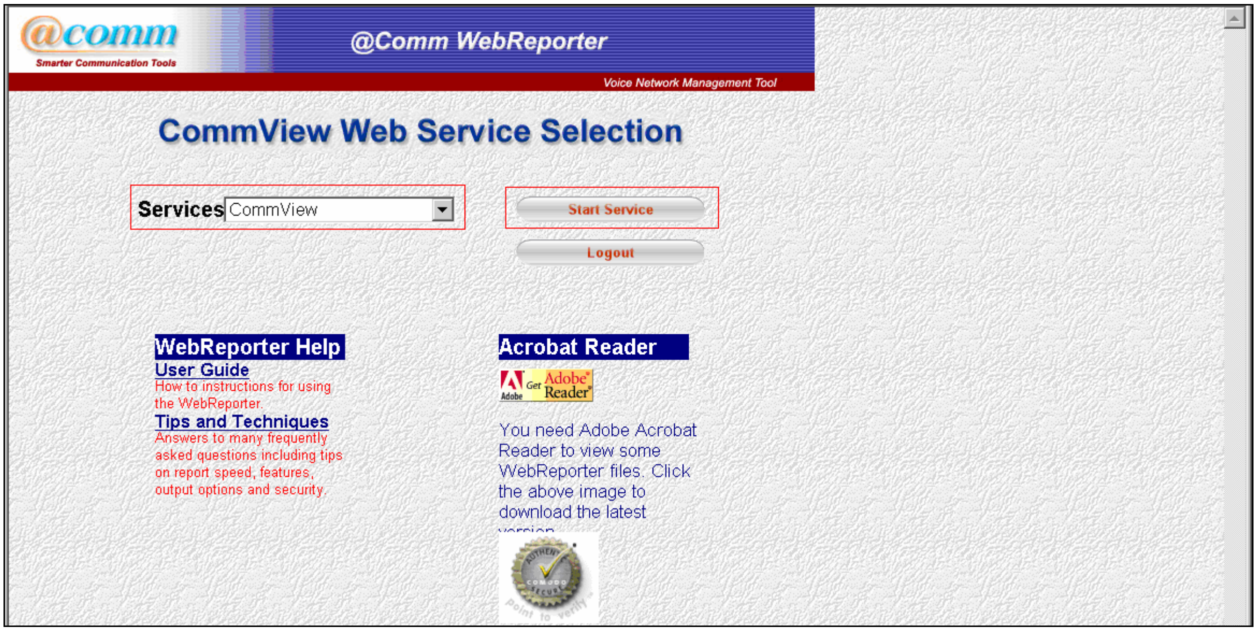
This section describes how to configure and generate report from the CommView reporter. Log in to the CommView Web Service website at http://webreporter.atcomm.com using the **User Name** and **Password** provided by @Comm. Select the **Login** button to continue


@comm
Smarter Communication Tools
@Comm WebReporter
Voice Network Management Tool
CommView Web Service Logon
Forgot your password?
Login

User Name: avayalab

Password: ********

After logging in, the following webpage will appear. Select **CommView** from the Services drop-down menu. Click the **Start Service** button.



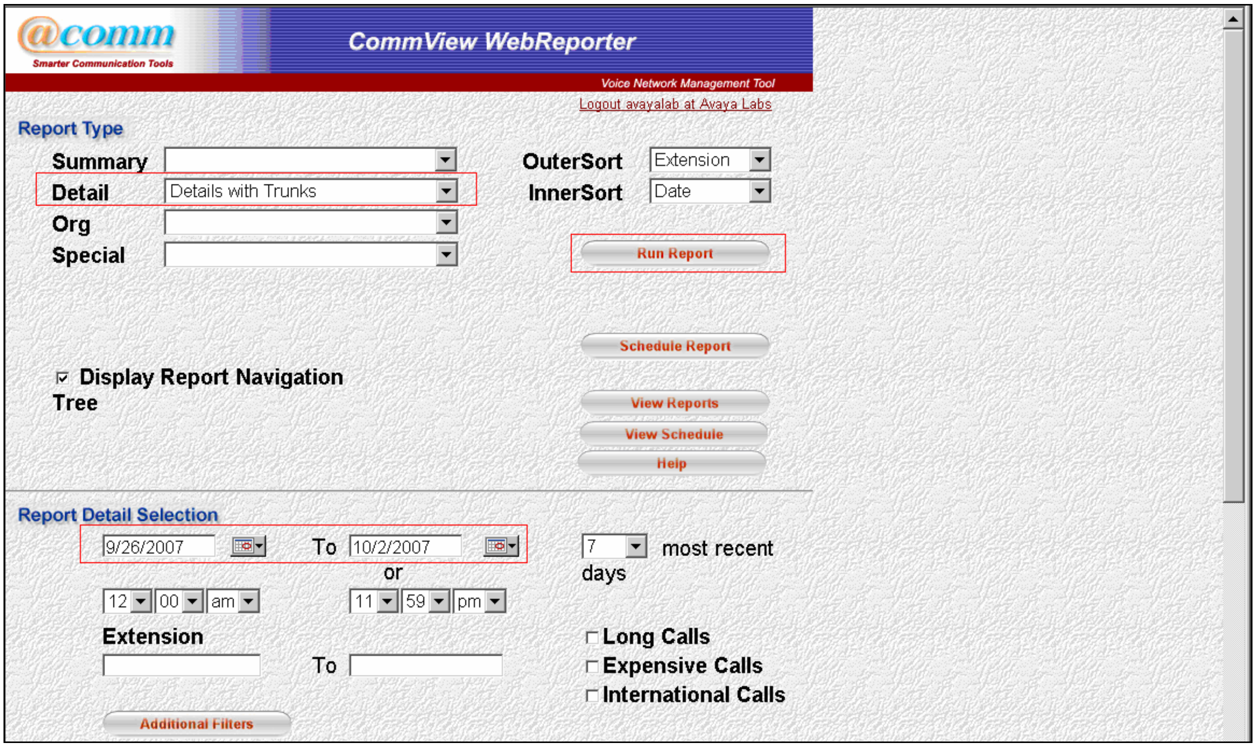
Services: CommView

How to instructions for using the WebReporter.

Answers to many frequently asked questions including tips on report speed, features, output options and security.

You need Adobe Acrobat Reader to view some WebReporter files. Click the above image to download the latest version.

The following screen shows a sample report configuration. Using the drop-down menu, select **Details with Trunks** for the Detail field. Provide a range of days under the Report Detail Selection section. Click the **Run Report** button.



Summary:
Detail: Details with Trunks
Org:
Special:
OuterSort: Extension
InnerSort: Date

☑ Display Report Navigation Tree

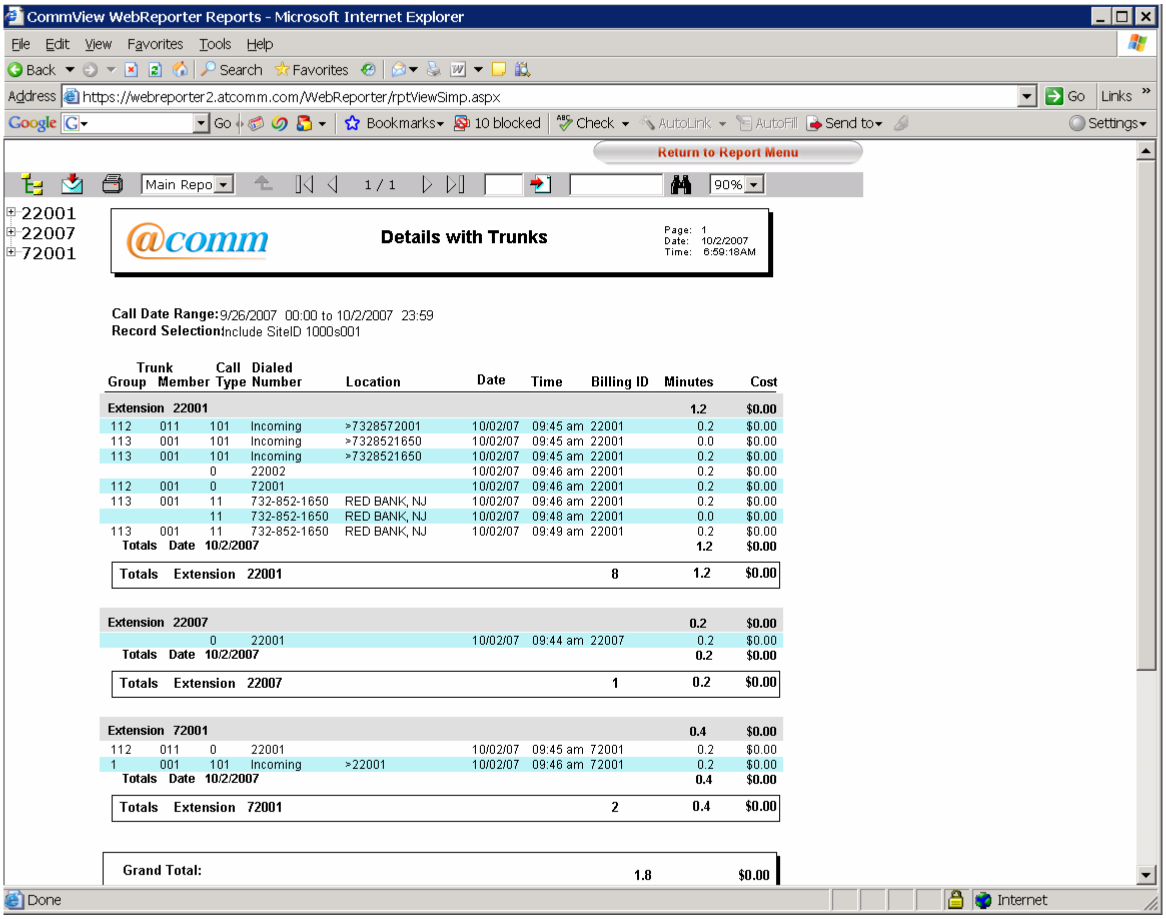
9/26/2007 To 10/2/2007 or 7 most recent days

12 00 am — 11 59 pm

Extension: To

□ Long Calls
□ Expensive Calls
□ International Calls

The following shows a sample report with **Details with Trunks**, as a report type.


CommView WebReporter Reports - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://webreporter2.atcomm.com/WebReporter/rptViewSimp.aspx
Go Links
Google G- Go Bookmarks 10 blocked Check AutoLink AutoFill Send to Settings
Return to Report Menu
Main Repo
1 / 1
90%
22001
22007
72001
@comm
Done
Internet

Details with Trunks

Page: 1
Date: 10/2/2007
Time: 6:59:18AM

Call Date Range: 9/26/2007 00:00 to 10/2/2007 23:59
Record Selection: Include SiteID 1000s001

Trunk		Call	Dialed						
Group	Member	Type	Number	Location	Date	Time	Billing ID	Minutes	Cost
Extension 22001								**1.2**	**$0.00**
112	011	101	Incoming	>7328572001	10/02/07	09:45 am	22001	0.2	$0.00
113	001	101	Incoming	>7328521650	10/02/07	09:45 am	22001	0.0	$0.00
113	001	101	Incoming	>7328521650	10/02/07	09:45 am	22001	0.2	$0.00
		0	22002		10/02/07	09:46 am	22001	0.2	$0.00
112	001	0	72001		10/02/07	09:46 am	22001	0.2	$0.00
113	001	11	732-852-1650	RED BANK, NJ	10/02/07	09:46 am	22001	0.2	$0.00
		11	732-852-1650	RED BANK, NJ	10/02/07	09:48 am	22001	0.0	$0.00
113	001	11	732-852-1650	RED BANK, NJ	10/02/07	09:49 am	22001	0.2	$0.00
Totals Date 10/2/2007								**1.2**	**$0.00**
Totals Extension 22001							**8**	**1.2**	**$0.00**
Extension 22007								**0.2**	**$0.00**
		0	22001		10/02/07	09:44 am	22007	0.2	$0.00
Totals Date 10/2/2007								**0.2**	**$0.00**
Totals Extension 22007							**1**	**0.2**	**$0.00**
Extension 72001								**0.4**	**$0.00**
112	011	0	22001		10/02/07	09:45 am	72001	0.2	$0.00
1	001	101	Incoming	>22001	10/02/07	09:46 am	72001	0.2	$0.00
Totals Date 10/2/2007								**0.4**	**$0.00**
Totals Extension 72001							**2**	**0.4**	**$0.00**
Grand Total:								**1.8**	**$0.00**

5. Configure the Avaya LSP Solution

This section describes how to configure the main Avaya Communication Manager and a LSP licensed Avaya Communication Manager to perform an Avaya LSP CDR solution. This section also includes the verification steps.

5.1. Configure the S8700 Server (Main) with G650 Media Gateway for the Avaya LSP Solution

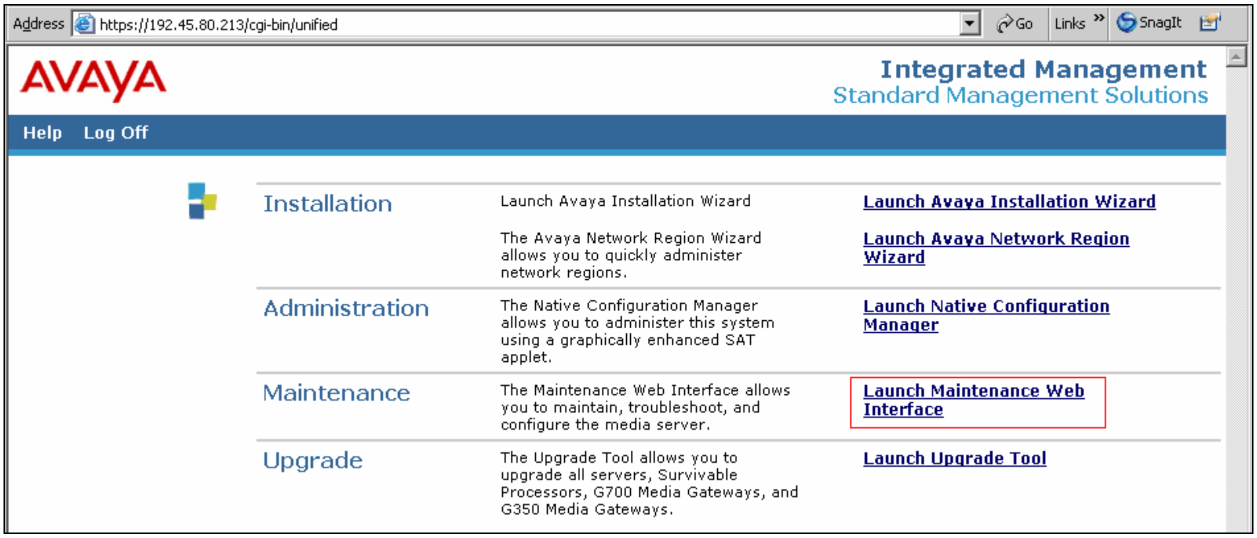
This section describes how to configure the S8700 Server with G650 Media Gateway for the Avaya LSP CDR Solution. The following steps must be performed:

- Create member credentials (username/password) for a SFTP account
- Change "survivable-processor <assigned Survivable Processor node-name>" form
- save translation all

5.1.1. CDR credentials for SFTP

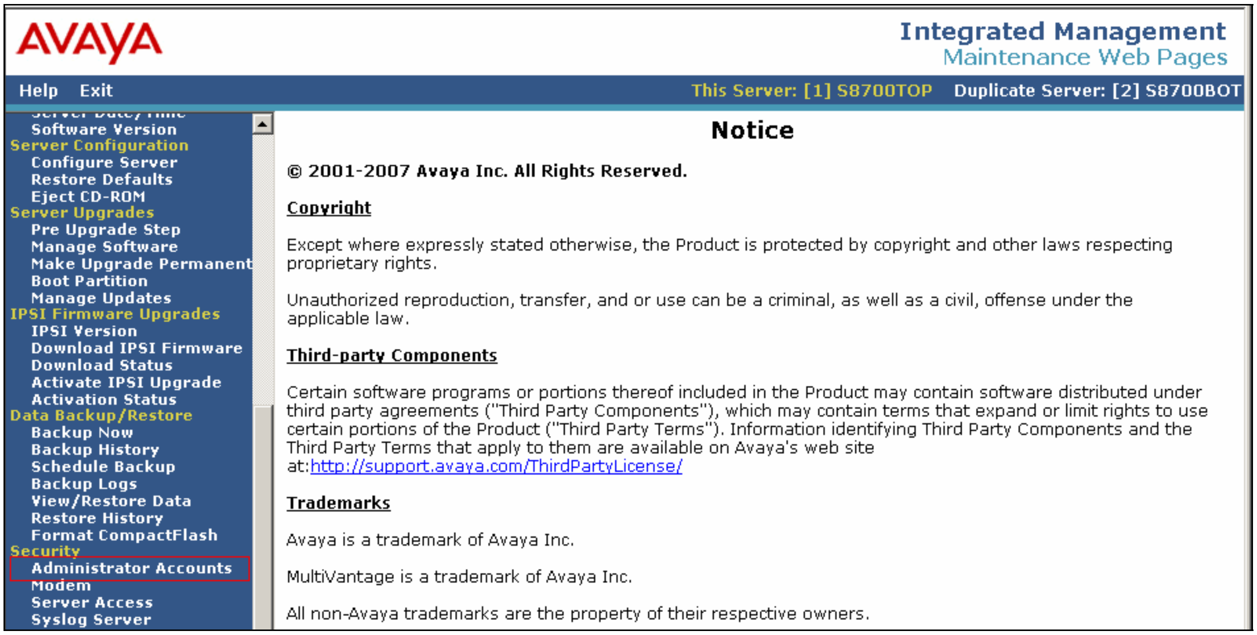
To create credentials, enter https://<IP address of Avaya S8700 Server> in the URL, and log in with the appropriate credentials for accessing the Integrated Management Standard Management Solutions pages.

Select **Launch Maintenance Web Interface** link.


Address https://192.45.80.213/cgi-bin/unified
Go
Links
SnagIt
AVAYA
Integrated Management
Standard Management Solutions
Help
Log Off

Installation	Launch Avaya Installation Wizard	Launch Avaya Installation Wizard
	The Avaya Network Region Wizard allows you to quickly administer network regions.	Launch Avaya Network Region Wizard
Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.	Launch Upgrade Tool

Select the **Administrator Accounts** link under the Security section.



Notice

© 2001-2007 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:http://support.avaya.com/ThirdPartyLicense/

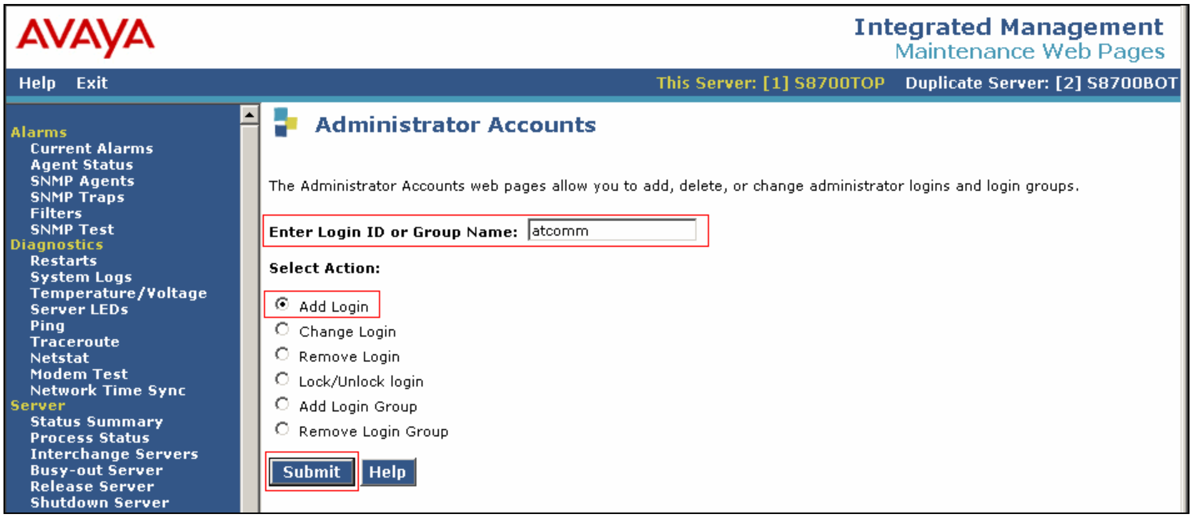
Trademarks

Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

In the Administrator Accounts page, provide a **Login ID** and click the **Add Login**.
Click the **Submit** button.



Administrator Accounts

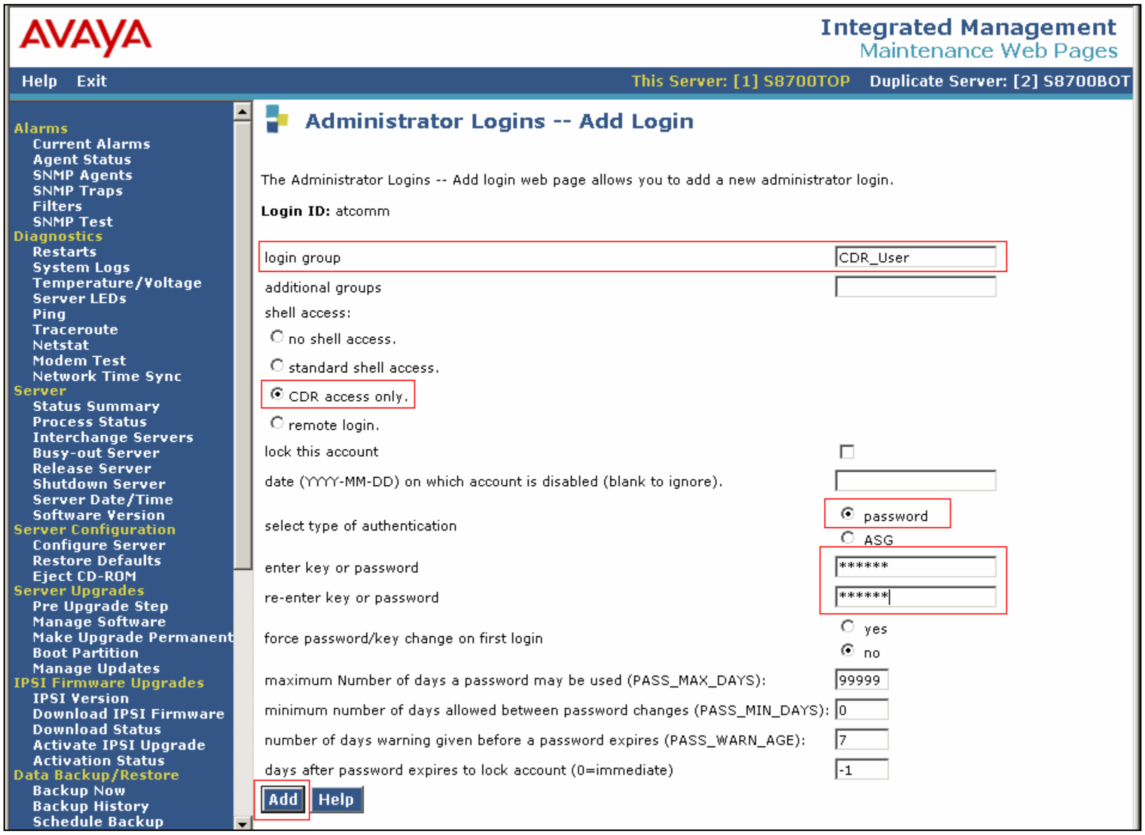
The Administrator Accounts web pages allow you to add, delete, or change administrator logins and login groups.

Enter Login ID or Group Name: atcomm

Select Action:

● Add Login
○ Change Login
○ Remove Login
○ Lock/Unlock login
○ Add Login Group
○ Remove Login Group

The CDR user has to be a part of the **CDR_User** group. Click the **CDR access only** for the shell access section. Click **Password** for the Select Type of Authentication field, and enter and reenter the password. Leave the default values for all other fields. Click the **Add** button.



Administrator Logins -- Add Login

The Administrator Logins -- Add login web page allows you to add a new administrator login.

Login ID: atcomm

login group: CDR_User

additional groups:

shell access:

○ no shell access.
○ standard shell access.
● CDR access only.
○ remote login.

lock this account □

date (YYYY-MM-DD) on which account is disabled (blank to ignore).

select type of authentication: ● password ○ ASG

enter key or password: ******

re-enter key or password: ******

force password/key change on first login: ○ yes ● no

maximum Number of days a password may be used (PASS_MAX_DAYS): 99999

minimum number of days allowed between password changes (PASS_MIN_DAYS): 0

number of days warning given before a password expires (PASS_WARN_AGE): 7

days after password expires to lock account (0=immediate): -1

5.1.2. Survivable-Processor Form

From the Avaya S8700 Server, enter the **change survivable-processor S8300** command, where S8300 is an LSP licensed Avaya S8300 Server, configured in Section 3. Change the Enabled field to **o**, and the Store to dsk field to **y**.

```
change survivable-processor S8300                              Page   2 of   3
                   SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local              Local    Remote             Remote
  Type              to dsk  Node               Port     Node               Port
  CDR1         o       y
```

After the Section 5.1.1 and 5.1.2 are completed, run the **save translation all** command, so that the translation in Avaya S8700 Server will be pushed to the LSP licensed Avaya S8300 Server.

5.2. Verification from the Avaya S8300 Server for the Avaya LSP Solution

This section describes how to verify the Avaya LSP CDR solution from the Avaya S8300 Server. Enter the **display ip-services** command. Notice that the Local Node field is changed to **procr**.

```
display  ip-services                                             Page   1 of   4

                                   IP SERVICES
 Service     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
CDR1                 procr            0       @comm-cdr       9000
```

Enter the **display survivable-processor S8300** command, and verify that the survivable-processor S8300 form in Avaya S8700 and S8300 Servers are identical.

```
display survivable-processor S8300                             Page   2 of   3
                   SURVIVABLE PROCESSOR - IP-SERVICES
 Service    Enabled Store   Local              Local    Remote             Remote
  Type              to dsk  Node               Port     Node               Port
  CDR1         o       y
```

6. Interoperability Compliance Testing

The interoperability compliance testing included feature, serviceability, performance, and LSP test. The feature testing evaluated the ability of the CommView Web to collect and process CDR records for various types of calls. The serviceability testing introduced failure scenarios to see if the CommView Web can resume CDR collection after failure recovery. The performance testing produced bulk call volumes to generate a substantial amount of CDR records. The Avaya LSP solution was tested by removing the CLAN board in the Avaya G650 Media Gateway.

6.1. General Test Approach

The general test approach was to manually place intra-switch calls, inbound trunk and outbound trunk calls to and from telephones attached to the Avaya Servers, and verifies the CommView Web 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, and media servers were reset. For performance testing, a call generator was used to place calls over an extended period of time. The LSP test was performed from the PC that CommView Avaya Server resides, using the SFTP command to the Avaya S8300 Server (LSP).

6.2. Test Results

All executed test cases passed. The CommView Web successfully collected the CDR records from Avaya 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, and conference calls. For serviceability testing, the CommView Web was able to resume collecting CDR records after failure recovery including buffered CDR records for calls that were placed during the outages. Performance tests verified that the CommView Web could collect call records during a sustained, high volume of calls.

The CommView Web also successfully collected the CDR records from the Avaya S8300 Server using the SFTP command.

7. Verification Steps

The following steps may be used to verify the configuration:

- On the SAT of each Avaya Media Server, enter the **status cdr-link** command and verify that the CDR link state is up.
- Place a call and verify that the CommView Web received the CDR record for the call. Compare the values of data fields in the CDR record with the expected values and verify that the values match.
- Place internal, inbound trunk, and outbound trunk calls to and from various telephones, generate an appropriate report in the CommView Web, and verify the report’s accuracy.

8. Support

Technical support for the CommView Web can be obtained by contacting @Comm via the support link at http://www.atcomm.com.

9. Conclusion

These Application Notes describe the procedures for configuring @Comm CommView Web to collect call detail records from Avaya Communication Manager running on Avaya Servers. The CommView Web successfully passed all compliance testing.

10. Additional References

The following Avaya product documentation can be found at http://support.avaya.com .

[1] Feature Description and Implementation For Avaya Communication Manager, Release, Issue 5, February 2007, Document Number 555-245-205

[2] Administrator Guide for Avaya Communication Manager, Issue 3.1, February 2007, Document Number 03-300509

The following CommView Web product documentation is available from @Comm. Visit the website at http://www.atcomm.com for company and product information.

[3] @Comm Web Reporter ASP Service User Guide, March 3, 2004

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.