



Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis VoIP Monitor with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis VoIP Monitor to interoperate with Avaya Aura® Communication Manager.

Prognosis VoIP Monitor is a purpose-built solution for the monitoring of voice quality in Avaya IP telephony environments. Prognosis VoIP Monitor provides best-in-class monitoring of voice quality from a telephony perspective as well as diagnostics for troubleshooting and service level analysis.

Prognosis VoIP Monitor integrates directly to Avaya Aura® Communication Manager using Secure Shell (SSH). At the same time, it processes Real-time Transport Control Protocol (RTCP) information from Avaya Aura® Communication Manager.

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

These Application Notes describe the compliance tested configuration used to validate Integrated Research Prognosis VoIP Monitor with Avaya Aura® Communication Manager.

Prognosis VoIP Monitor is designed to provide a comprehensive monitoring platform for Avaya IP telephony networks. It does this by collecting data, filtering it as required and then presenting it in a user-friendly format, all in real-time. An additional function allows for data to be used to generate email alerts when pre-defined conditions are exceeded.

In order to collect and present data, the Prognosis VoIP Monitor product must be installed on a dedicated server. The product has a web based configuration application and a PBX monitor application for users to configure the product and view the status of the monitored PBX using a web browser.

Prognosis VoIP Monitor uses the following methods to monitor Avaya Aura® Communication Manager.

- **System Access Terminal (SAT)** - The Prognosis VoIP Monitor uses a pool of SSH connections to the SAT to query system components configuration and the component status. In the test configuration, the solution establishes two concurrent SAT connections to Avaya Aura® Communication Manager and uses the connections to execute SAT commands.
- **RTCP Collection** - Prognosis VoIP Monitor collects RTCP information sent by the Avaya IP Media Processor (MEDPRO) boards, media gateways, IP Telephones and OneX® Communicator.
- **SNMP** – Prognosis VoIP Monitor uses SNMP V2c interface to query Avaya Server related information.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing.

The feature testing evaluated the ability of the Prognosis VoIP Monitor to correctly retrieve the configuration and status information from Communication Manager. In addition, the ability of Prognosis VoIP Monitor to receive and process RTCP information from Communication Manager was also validated.

The serviceability testing introduced failure scenarios to see if Prognosis VoIP Monitor is able to resume service after failure recovery and an Avaya Server interchange.

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 compliance test was performed in the following ways:

- PBX component information and status: Prognosis VoIP Monitor displays configuration and status information for major Communication Manager elements such as CLAN boards, Medpro boards, DS1 boards, main servers, survivable servers, network regions, phones, port networks, route patterns, and trunk groups. The displayed information on various Prognosis VoIP Monitor panels was compared with output from manually executed SAT commands and information accessible from Communication Manager web interface for accuracy.
- Quality of Service data for voice streams: Various types of calls including direct IP-to-IP, IP-to-digital, IP-analog, 3-party conference within a PBX, and 3-party conference across two PBXs were made with or without a network impairment device in the media path. For each call, the following from the Prognosis VoIP Monitor display was verified:
 - o Two voice streams were generated for each IP call leg
 - o Packet loss, latency, and jitter values were consistent with the values set on the network impairment device
- Serviceability testing focused on verifying the ability of Prognosis VoIP Monitor to recover from adverse conditions such as disconnecting and reconnecting the Communication Manager and Prognosis VoIP Monitor server from the network, rebooting Communication Manager and Prognosis VoIP Monitor server, and interchanging the Avaya Main Servers.

2.2. Test Results

The Prognosis VoIP Monitor successfully passed the compliance test. The following observations were made during testing:

- Trunk Group panel displayed incorrect medium information for SIP trunks groups.
- Signaling Group panel did not display Signaling Group number for SIP and H.323 trunk groups.
- OneX® Communicator Release 6.1 did not support RCTP functions.

2.3. Support

For technical support on Prognosis VoIP Monitor, contact the Integrated Research Support Team at:

- Phone: +61 (2) 9966 1066

- Fax: +61 (2) 9921-1042
- Email: support@prognosis.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Prognosis VoIP Monitor interoperability with Communication Manager. It consists of a Communication Manager simplex system running on a S8800 server with two Avaya G650 Media Gateways in Site 1, a Communication Manager duplex system running on a pair of Dell R610 servers with one Avaya G450 Media Gateway in Site 2, and Communication Manager Survivable Core software running on a pair of HP DL360G7 servers in Site 3 supporting the Site 2 Communication Manager system. The two Communication Manager systems have Avaya IP, digital and analog telephones, and Avaya One-X® Communicator users configured for making and receiving calls. Prognosis VoIP Monitor was installed on a VMWare virtual machine running Microsoft Windows Server 2008 R2 with Service Pack 1. All the systems and telephones are connected using an Avaya Layer2 and Layer 3 data infrastructure.

SIP Telephones are not supported by Prognosis VoIP Monitor and therefore are outside the scope of the testing.

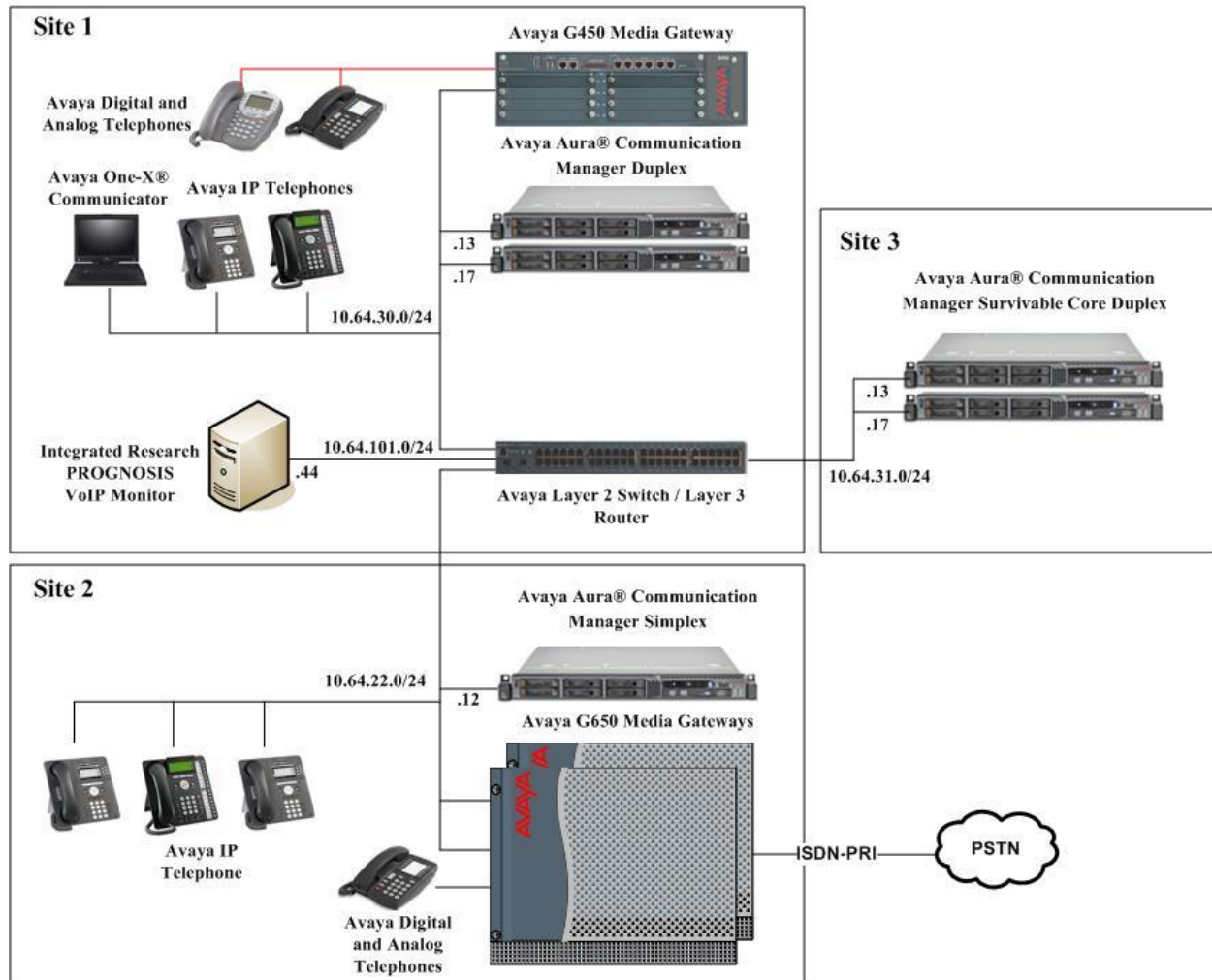


Figure 1: Test Configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Version
Avaya S8800 Server running Avaya Aura® Communication Manager	6.2 SP3 (Patch 20001)
G650 Media Gateway - TN2312BP IP Server Interface (x 2) - TN799DP C-LAN Interface (x 2) - TN2602AP IP Media Processor (x 2) - TN2302AP IP Media Processor (x 2) - TN464HP DS1 Interface - TN464F DS1 Interface (x 4) - TN793CP Analog Line - TN2224CP Digital Line	HW28, FW040 HW01/13, FW038 HW02 FW057/063 HW20 FW120 HW02, FW018 000010/18/20 HW10, FW009 HW03, FW008
Dell R610 Servers running Avaya Aura® Communication Manager Duplex	6.2 SP3 (Patch 20001)
HP DL360G7 Servers running Avaya Aura® Communication Manager Survivable Core	6.2 SP3 (Patch 20001)
G450 Media Gateway - MM712AP DCP MM - MM711AP Analog MM - MM710AP DS1 MM	31.20.0 HW07 FW011 HW31 FW095 HW04 FW018
96x0 Series IP Telephones	3.1.5 (H.323) 2.6.3 (SIP)
96x1 IP Telephone	6.0.2
2420 Digital Telephones	-
2500 analog phone	-
6211 analog phone	-
Desktop PC with Avaya one-X® Communicator	6.1
Integrated Research Prognosis VoIP Monitor running under Windows 2008 R2 SP1 on a VMWare virtual machine	4.0

5. Configure Avaya Aura® Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with Prognosis VoIP Monitor. This includes creating a SAT User Profile and a login account for Prognosis VoIP Monitor to access Communication Manager, enabling RTCP reporting, and enabling SNMP. The steps are repeated for each Communication Manager system in the test configuration.

5.1. Configure SAT User Profile

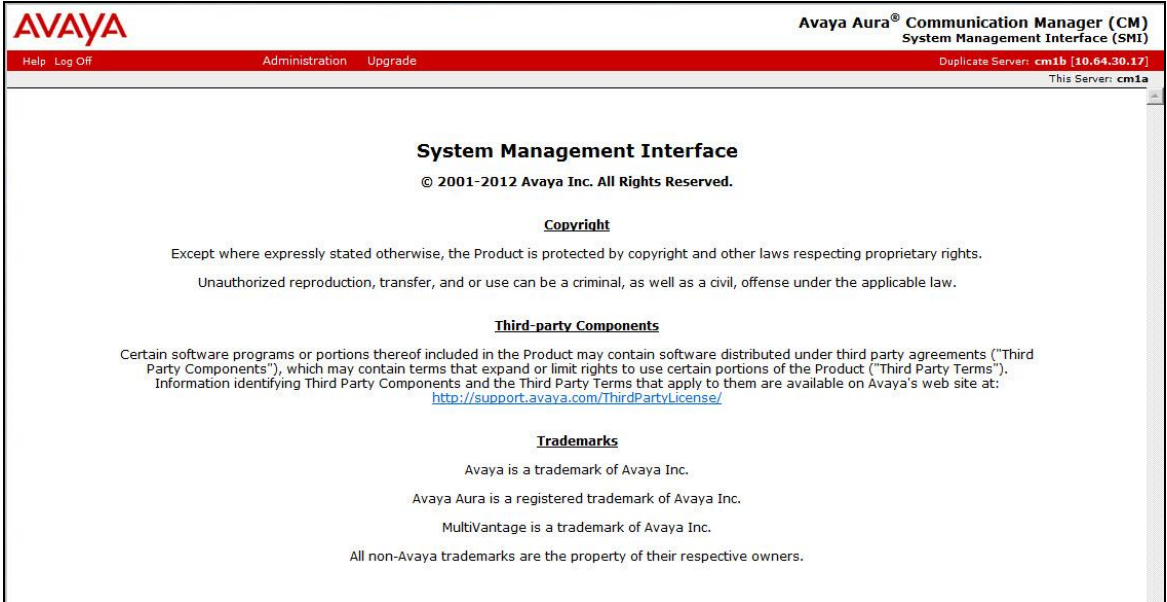
A SAT User Profile specifies which SAT screens may be accessed by the assigned user and the type of access to each screen. As Prognosis VoIP Monitor does not modify any system configuration, create a SAT User Profile with limited permissions for the Prognosis VoIP Monitor login account.

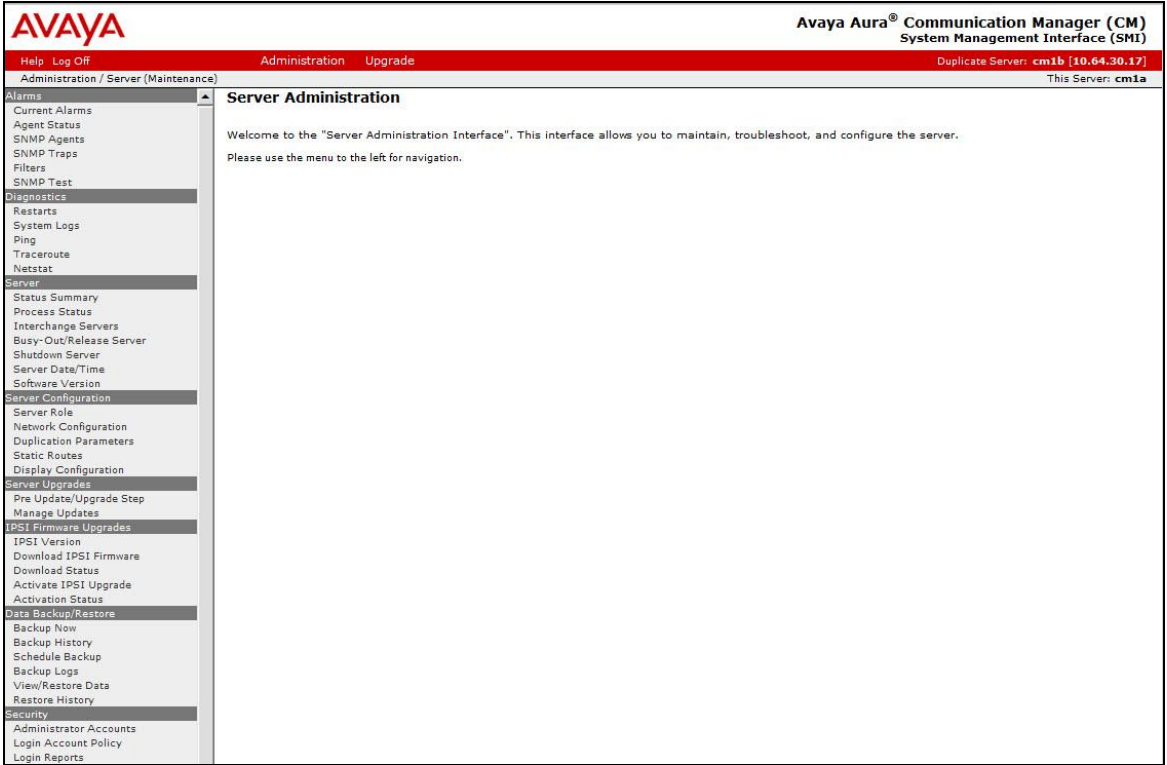
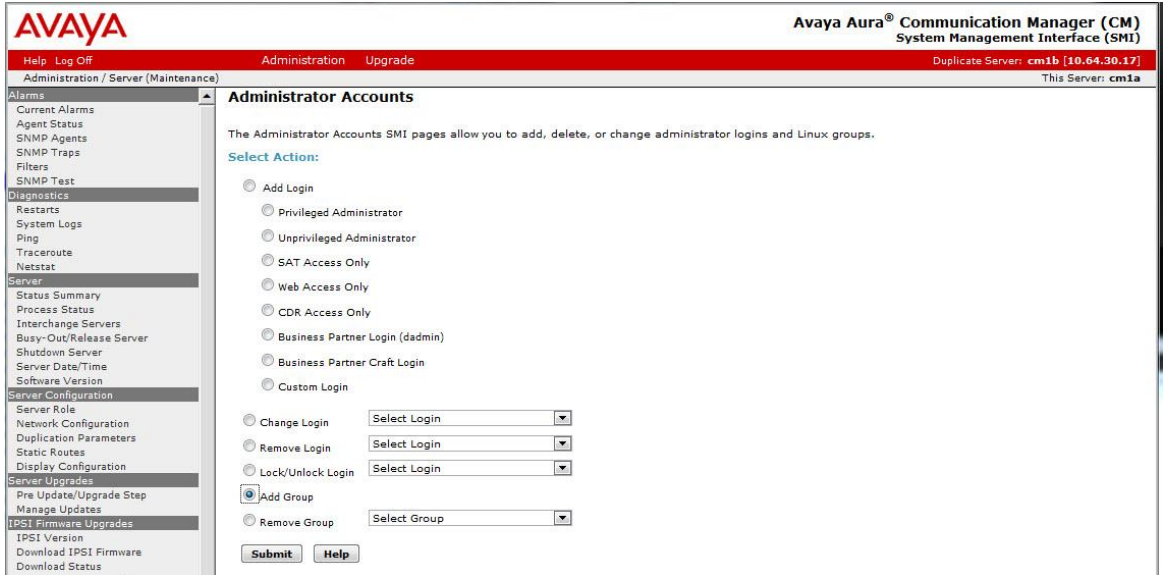
Step	Description
1.	<p>From the SAT command prompt, enter the add user-profile <i>n</i> command, where <i>n</i> is an unused profile number. Enter a descriptive name for User Profile Name and enable all categories by setting the Enbl field to y. In this configuration, the user profile 20 was created.</p> <pre>add user-profile 20 Page 1 of 41 USER PROFILE 20 User Profile Name: change user-profile 20 This Profile is Disabled? n Shell Access? n Facility Test Call Notification? n Acknowledgement Required? n Grant Un-owned Permissions? n Extended Profile? n Name Cat Enbl Name Cat Enbl Adjuncts A y Routing and Dial Plan J y Call Center B y Security K y Features C y Servers L y Hardware D y Stations M y Hospitality E y System Parameters N y IP F y Translations O y Maintenance G y Trunking P y Measurements and Performance H y Usage Q y Remote Access I y User Access R y</pre>

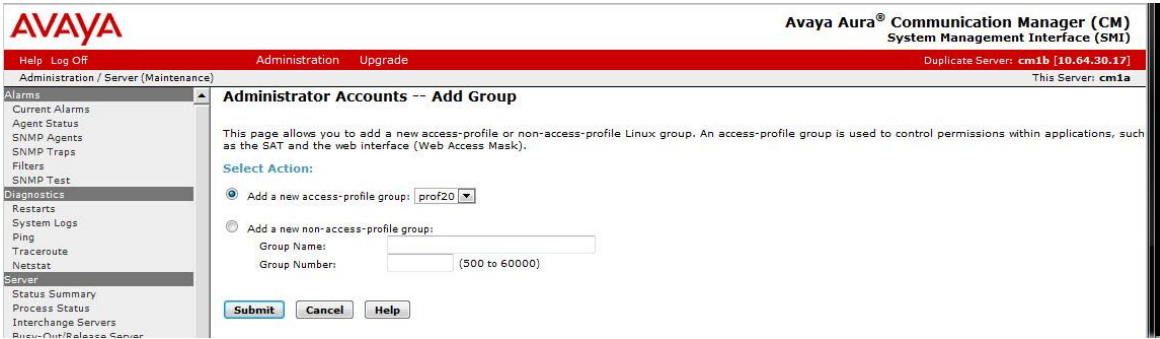
Step	Description																																													
2.	<p>On Pages 2 to 41 of the USER PROFILE form, set the permissions of all objects to rm (read and maintenance). This can be accomplished by typing rm into the Set All Permissions To field. Submit the form to create the user profile.</p>																																													
	<div><div>add user-profile 20</div><div>Page 2 of 41</div></div> <div><div>USER PROFILE 20</div><div>Set Permissions For Category: To: Set All Permissions To: '-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance</div><table><thead><tr><th>Name</th><th>Cat</th><th>Perm</th></tr></thead><tbody><tr><td>aar analysis</td><td>J</td><td>rm</td></tr><tr><td>aar digit-conversion</td><td>J</td><td>rm</td></tr><tr><td>aar route-chosen</td><td>J</td><td>rm</td></tr><tr><td>abbreviated-dialing 7103-buttons</td><td>C</td><td>rm</td></tr><tr><td>abbreviated-dialing enhanced</td><td>C</td><td>rm</td></tr><tr><td>abbreviated-dialing group</td><td>C</td><td>rm</td></tr><tr><td>abbreviated-dialing personal</td><td>C</td><td>rm</td></tr><tr><td>abbreviated-dialing system</td><td>C</td><td>rm</td></tr><tr><td>aca-parameters</td><td>P</td><td>rm</td></tr><tr><td>access-endpoint</td><td>P</td><td>rm</td></tr><tr><td>adjunct-names</td><td>A</td><td>rm</td></tr><tr><td>administered-connection</td><td>C</td><td>rm</td></tr><tr><td>aesvcs cti-link</td><td>A</td><td>rm</td></tr><tr><td>aesvcs interface</td><td>A</td><td>rm</td></tr></tbody></table></div>	Name	Cat	Perm	aar analysis	J	rm	aar digit-conversion	J	rm	aar route-chosen	J	rm	abbreviated-dialing 7103-buttons	C	rm	abbreviated-dialing enhanced	C	rm	abbreviated-dialing group	C	rm	abbreviated-dialing personal	C	rm	abbreviated-dialing system	C	rm	aca-parameters	P	rm	access-endpoint	P	rm	adjunct-names	A	rm	administered-connection	C	rm	aesvcs cti-link	A	rm	aesvcs interface	A	rm
Name	Cat	Perm																																												
aar analysis	J	rm																																												
aar digit-conversion	J	rm																																												
aar route-chosen	J	rm																																												
abbreviated-dialing 7103-buttons	C	rm																																												
abbreviated-dialing enhanced	C	rm																																												
abbreviated-dialing group	C	rm																																												
abbreviated-dialing personal	C	rm																																												
abbreviated-dialing system	C	rm																																												
aca-parameters	P	rm																																												
access-endpoint	P	rm																																												
adjunct-names	A	rm																																												
administered-connection	C	rm																																												
aesvcs cti-link	A	rm																																												
aesvcs interface	A	rm																																												

5.2. Configure Login Group

Use the Communication Manager web interface to create an Access-Profile Group to correspond to the SAT User Profile created in **Section 5.1**.

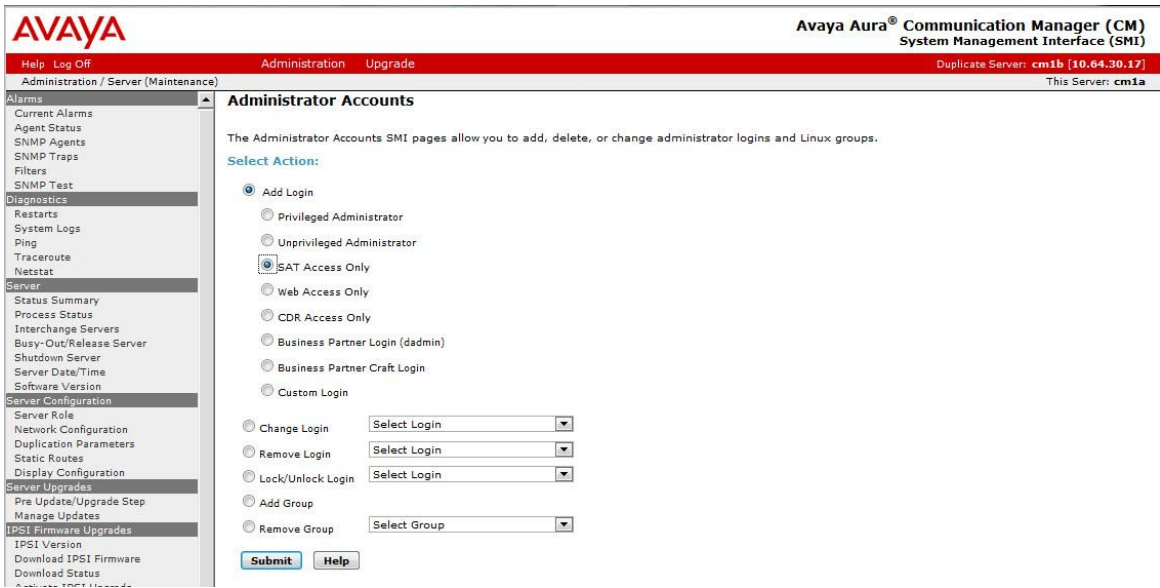
Step	Description
1.	<p>Using a web browser, enter https://<IP address of Avaya Server> to connect to the Avaya Server being configured and log in using appropriate credentials. A messages page will be displayed (not shown). Click Continue. A System Management Interface page will be displayed.</p> 

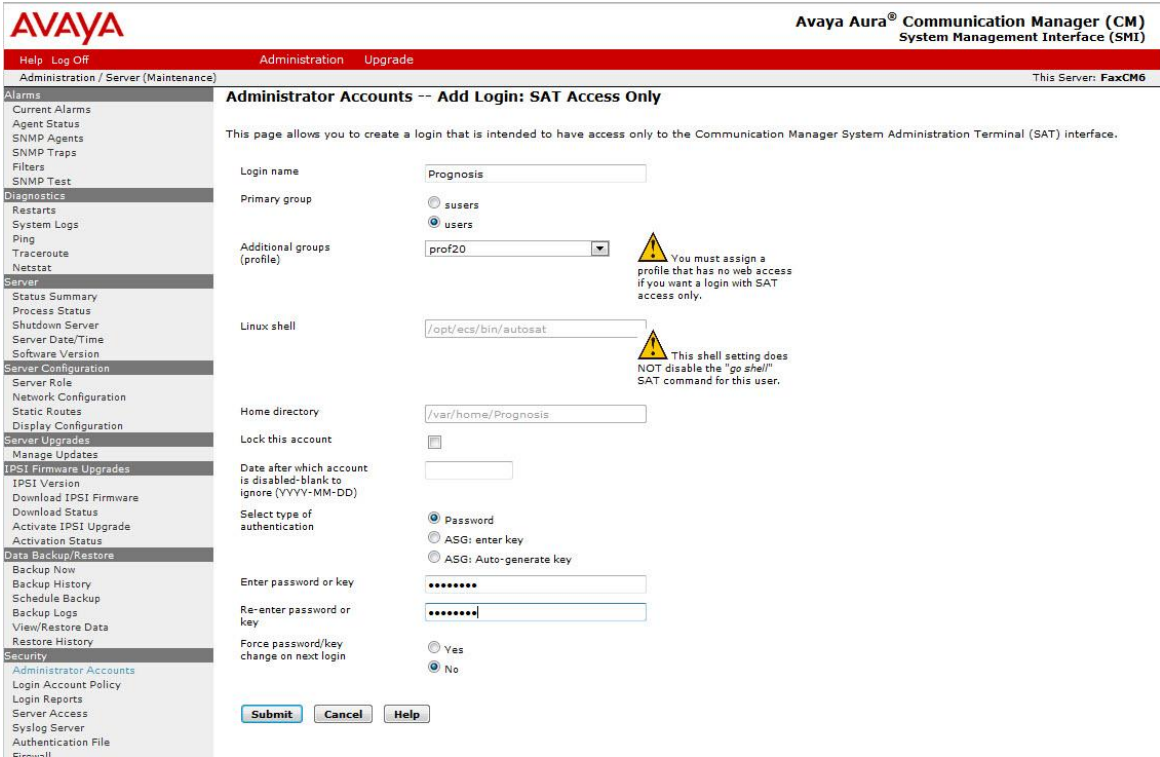
Step	Description
2.	<p>Click Administration → Server (Maintenance). This will open up the Server Administration page.</p> 
3.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Group and click Submit.</p> 

Step	Description
4.	<p>Select Add a new access-profile group and select “prof20” from the drop-down box which corresponds to the user-profile created in Section 5.1. Click Submit. This completes the creation of the login group.</p> 

5.3. Configure Login

From the Communication Manager web interface, create a login account for Prognosis VoIP Monitor to access the Communication Manager SAT.

Step	Description
1.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Login and SAT Access Only to create a new login account with SAT access privileges only. Click Submit.</p> 

Step	Description
2.	<p>Enter a login in the Login name field. In this configuration, the login “Prognosis” was created. Configure the other parameters for the login as follows:</p> <ul style="list-style-type: none"> • Primary group: “users” [Limits the permissions of the login] • Additional groups (profile): “prof20” [Select the login group created in Section 5.2.] • Select type of authentication: “Password” [Uses a password for authentication.] • Enter password or key / Re-enter password or key [Define the password] <p>Click Submit to continue. This completes the configuration of the login.</p> 

5.4. Configure RTCP Monitoring

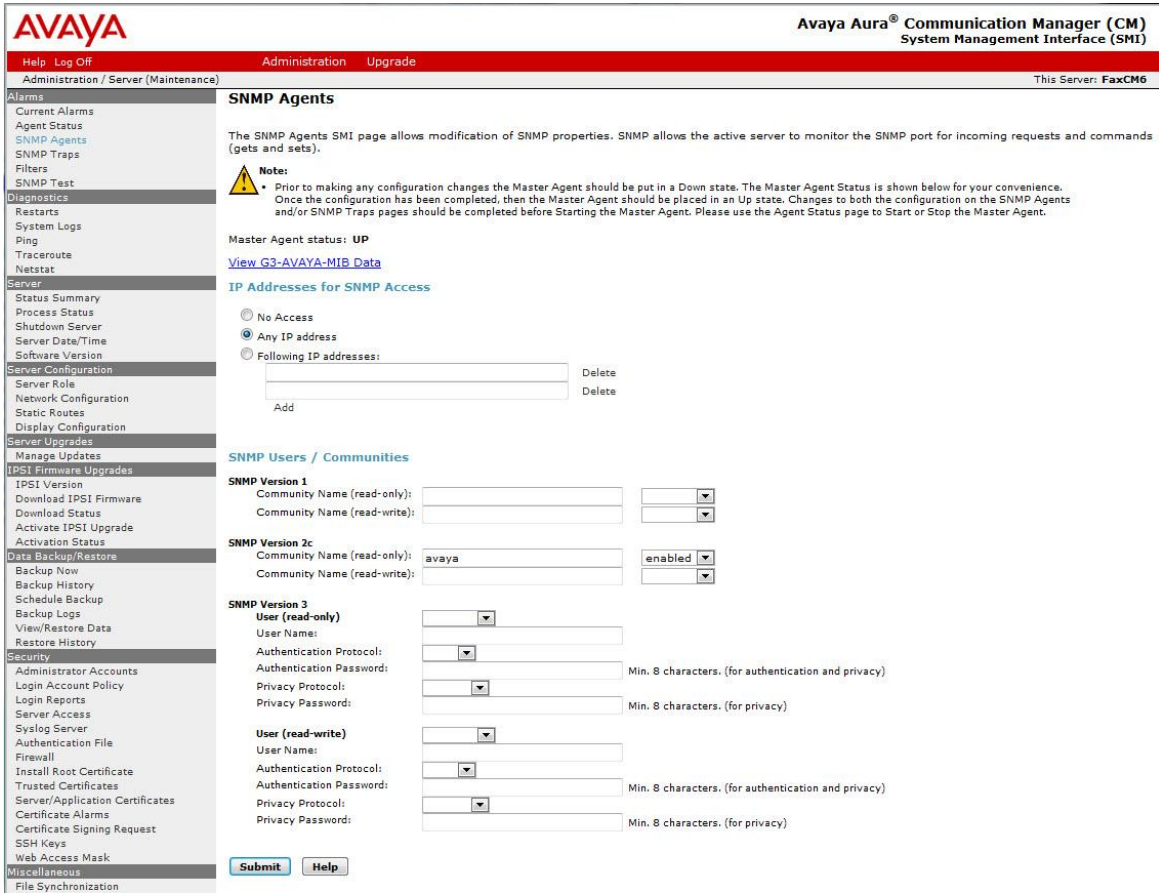
To allow Prognosis VoIP Monitor to monitor the quality of IP calls, configure Communication Manager to send RTCP reporting to the IP address of the Prognosis VoIP Monitor server.

Step	Description
1.	<p>From the SAT command prompt, enter the change system-parameters ip-options command. In the RTCP MONITOR SERVER section, set Server IPV4 Address to the IP address of the Prognosis VoIP Monitor server. Use the default values for the IPV4 Server Port field and the RTCP Report Period (secs) field.</p>

Step	Description
	<p>change system-parameters ip-options Page 1 of 4</p> <p style="text-align: center;">IP-OPTIONS SYSTEM PARAMETERS</p> <p>IP MEDIA PACKET PERFORMANCE THRESHOLDS</p> <p>Roundtrip Propagation Delay (ms) High: 800 Low: 400</p> <p>Packet Loss (%) High: 40 Low: 15</p> <p>Ping Test Interval (sec): 20</p> <p>Number of Pings Per Measurement Interval: 10</p> <p>Enable Voice/Network Stats? n</p> <p>RTCP MONITOR SERVER</p> <p>Server IPv4 Address: 10.64.101.44 RTCP Report Period(secs): 5</p> <p>IPv4 Server Port: 5005</p> <p>Server IPv6 Address:</p> <p>IPv6 Server Port: 5005</p> <p>AUTOMATIC TRACE ROUTE ON</p> <p>Link Failure? y</p> <p style="text-align: right;">H.323 IP ENDPOINT</p> <p>H.248 MEDIA GATEWAY Link Loss Delay Timer (min): 5</p> <p>Link Loss Delay Timer (min): 5 Primary Search Time (sec): 75</p> <p>Periodic Registration Timer (min): 20</p> <p>Short/Prefixed Registration Allowed? Y</p>
2.	<p>Enter the change ip-network-region <i>n</i> command, where <i>n</i> is IP network region number to be monitored. Set RTCP Reporting Enabled to “y” and Use Default Server Parameters to “y”.</p>
	<p>change ip-network-region 1 Page 2 of 20</p> <p style="text-align: center;">IP NETWORK REGION</p> <p>RTCP Reporting Enabled? y</p> <p>RTCP MONITOR SERVER PARAMETERS</p> <p>Use Default Server Parameters? y</p>
3.	Repeat Step 2 for all the IP network regions that are required to be monitored.

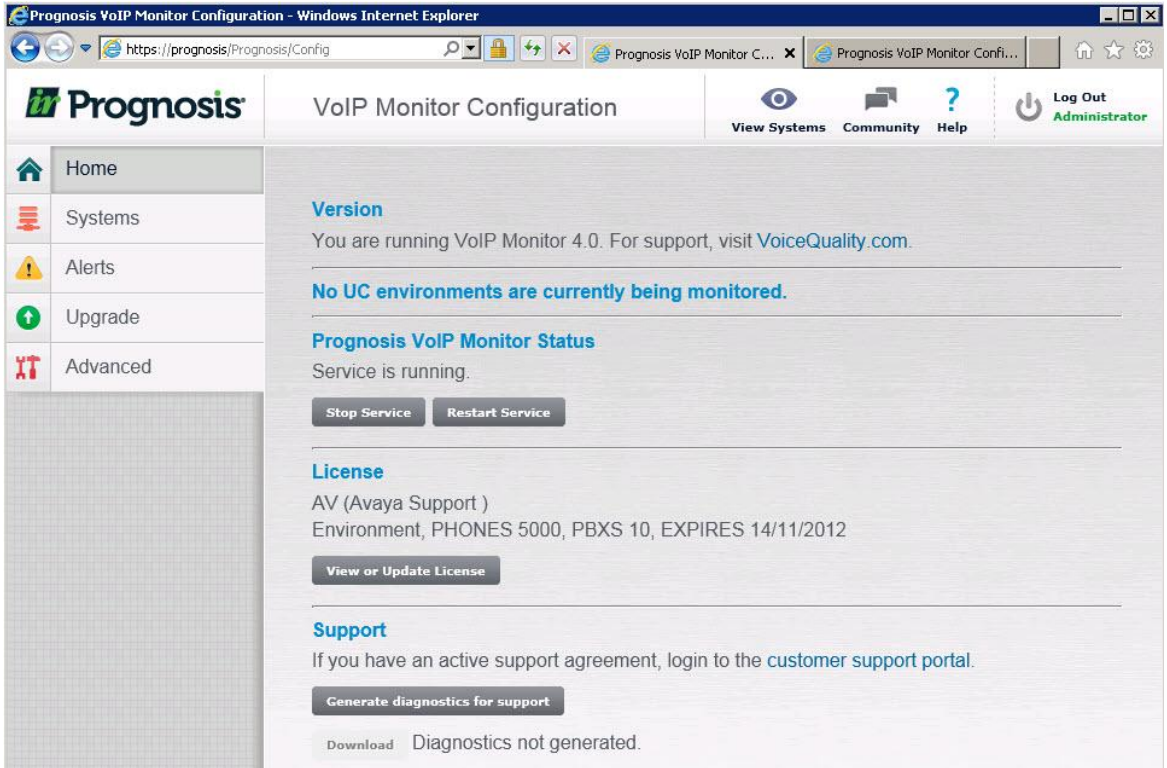
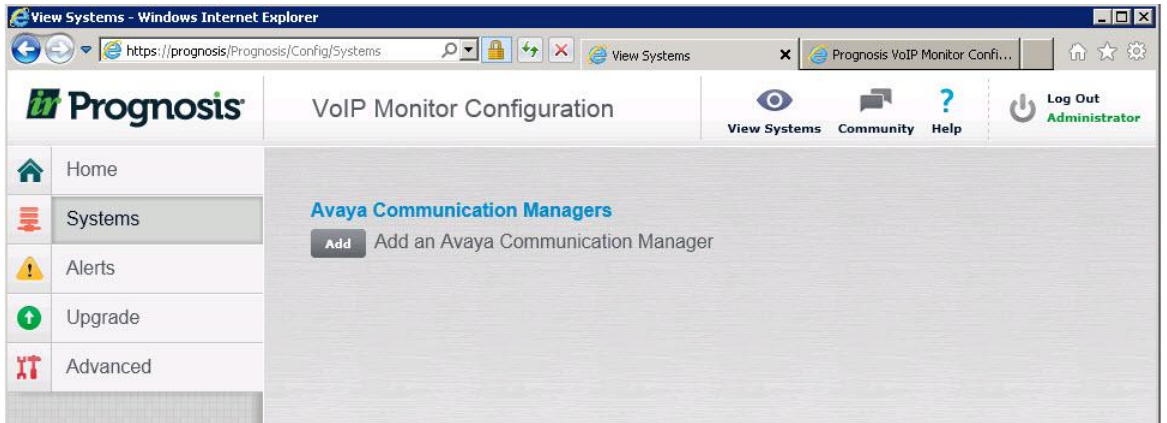
5.5. Configure SNMP

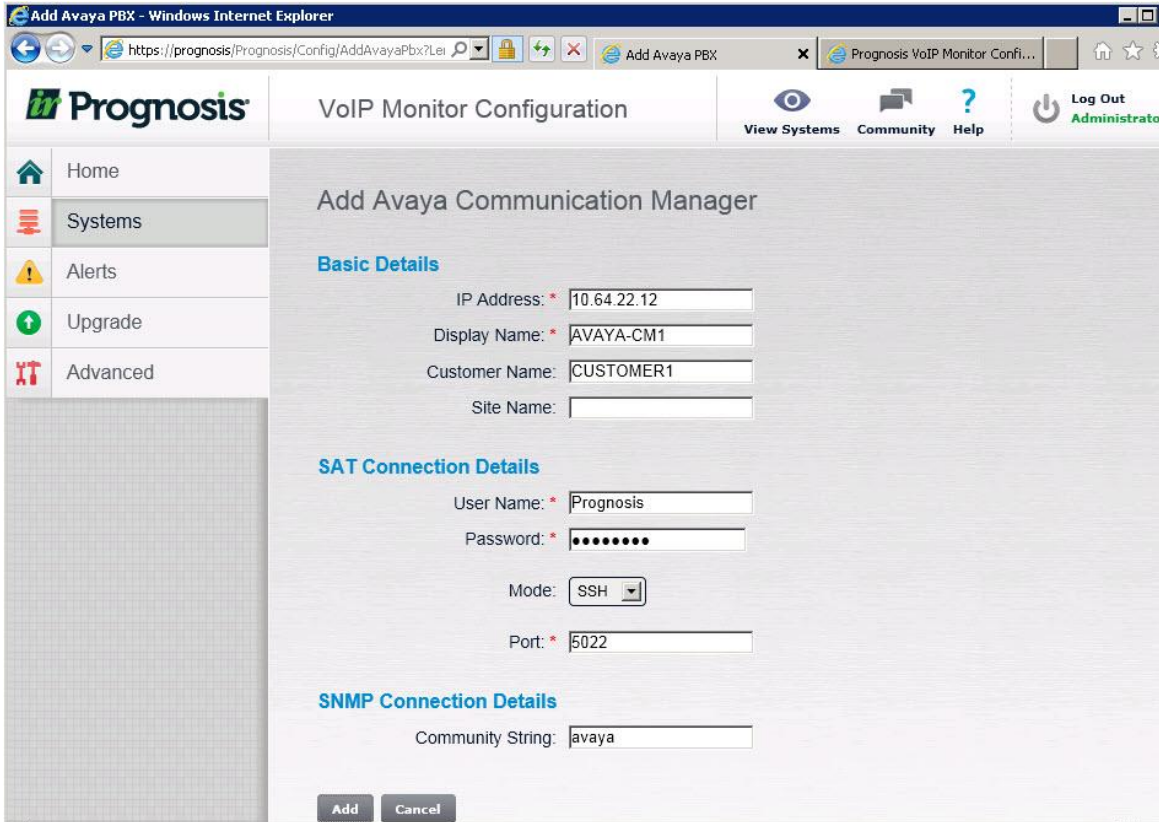
Enable SNMP for Prognosis VoIP Monitor to access.

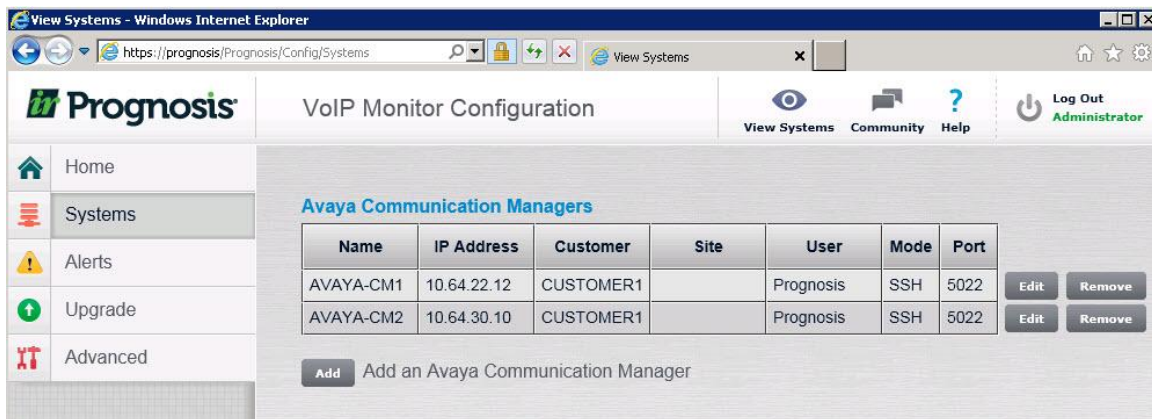
Step	Description
1.	<p>From the navigation panel on the left side, click SNMP Agents. The SNMP Agents page is displayed. Under IP Addresses for SNMP Access, select Any IP address. In the SNMP Users / Communities → SNMP Version 2c section, enter “avaya” in the Community Name (read-only) field and select “enabled”. Click Submit.</p> 

6. Configure Integrated Research Prognosis VoIP Monitor

This section describes the configuration of Prognosis VoIP Monitor required to interoperate with Communication Manager.

Step	Description
1.	<p>On the Prognosis VoIP Monitor server, click Start → All Programs → Prognosis VoIP Monitor → Configure to start the configuration application. Enter proper credentials to log in. The VoIP Monitor Configuration page is displayed.</p> 
2.	<p>To configure the Communication Manager systems to be monitored, click Systems on the left pane and click the Add button.</p> 

Step	Description
3.	<p>The Add Avaya Communication Manager page is displayed. Under Basic Details, enter the IP address of the Site 1 Communication Manager in the IP Address field and a descriptive name for the Communication Manager in the Display Name field. Specify a Customer Name for the PBX. Under SAT Connection Details, enter the login and password configured in Section 5.3 in the User Name and Password fields. Under SNMP Connection Details, enter the Community Name configured in Section 5.5 in the Community String field. The remaining fields may be left at their defaults. Click Add to effect the addition.</p>  <p>The screenshot shows a web browser window titled 'Add Avaya PBX - Windows Internet Explorer'. The address bar shows the URL 'https://prognosis/Prognosis/Config/AddAvayaPbx?Lei...'. The page header includes the Prognosis logo, 'VoIP Monitor Configuration', and navigation links for 'View Systems', 'Community', 'Help', and 'Log Out Administrator'. A left sidebar contains links for 'Home', 'Systems', 'Alerts', 'Upgrade', and 'Advanced'. The main content area is titled 'Add Avaya Communication Manager' and contains three sections: 'Basic Details' with fields for IP Address (10.64.22.12), Display Name (AVAYA-CM1), Customer Name (CUSTOMER1), and Site Name; 'SAT Connection Details' with fields for User Name (Prognosis), Password (masked), Mode (SSH), and Port (5022); and 'SNMP Connection Details' with a Community String (avaya). At the bottom are 'Add' and 'Cancel' buttons.</p>

Step	Description																											
4.	<p>Repeat Step 1 to 3 to add the Site 2 CM. The screenshot below shows the two CMs in the test configuration.</p>  <p>The screenshot shows the 'View Systems - Windows Internet Explorer' window with the URL 'https://prognosis/Prognosis/Config/Systems'. The page title is 'VoIP Monitor Configuration'. On the left is a navigation menu with links: Home, Systems (selected), Alerts, Upgrade, and Advanced. On the right, there are links for View Systems, Community, Help, and a Log Out Administrator button. The main content area is titled 'Avaya Communication Managers' and contains a table with the following data:</p> <table><thead><tr><th>Name</th><th>IP Address</th><th>Customer</th><th>Site</th><th>User</th><th>Mode</th><th>Port</th><th></th><th></th></tr></thead><tbody><tr><td>AVAYA-CM1</td><td>10.64.22.12</td><td>CUSTOMER1</td><td></td><td>Prognosis</td><td>SSH</td><td>5022</td><td>Edit</td><td>Remove</td></tr><tr><td>AVAYA-CM2</td><td>10.64.30.10</td><td>CUSTOMER1</td><td></td><td>Prognosis</td><td>SSH</td><td>5022</td><td>Edit</td><td>Remove</td></tr></tbody></table> <p>Below the table is an 'Add' button and the text 'Add an Avaya Communication Manager'.</p>	Name	IP Address	Customer	Site	User	Mode	Port			AVAYA-CM1	10.64.22.12	CUSTOMER1		Prognosis	SSH	5022	Edit	Remove	AVAYA-CM2	10.64.30.10	CUSTOMER1		Prognosis	SSH	5022	Edit	Remove
Name	IP Address	Customer	Site	User	Mode	Port																						
AVAYA-CM1	10.64.22.12	CUSTOMER1		Prognosis	SSH	5022	Edit	Remove																				
AVAYA-CM2	10.64.30.10	CUSTOMER1		Prognosis	SSH	5022	Edit	Remove																				

7. Verification Steps

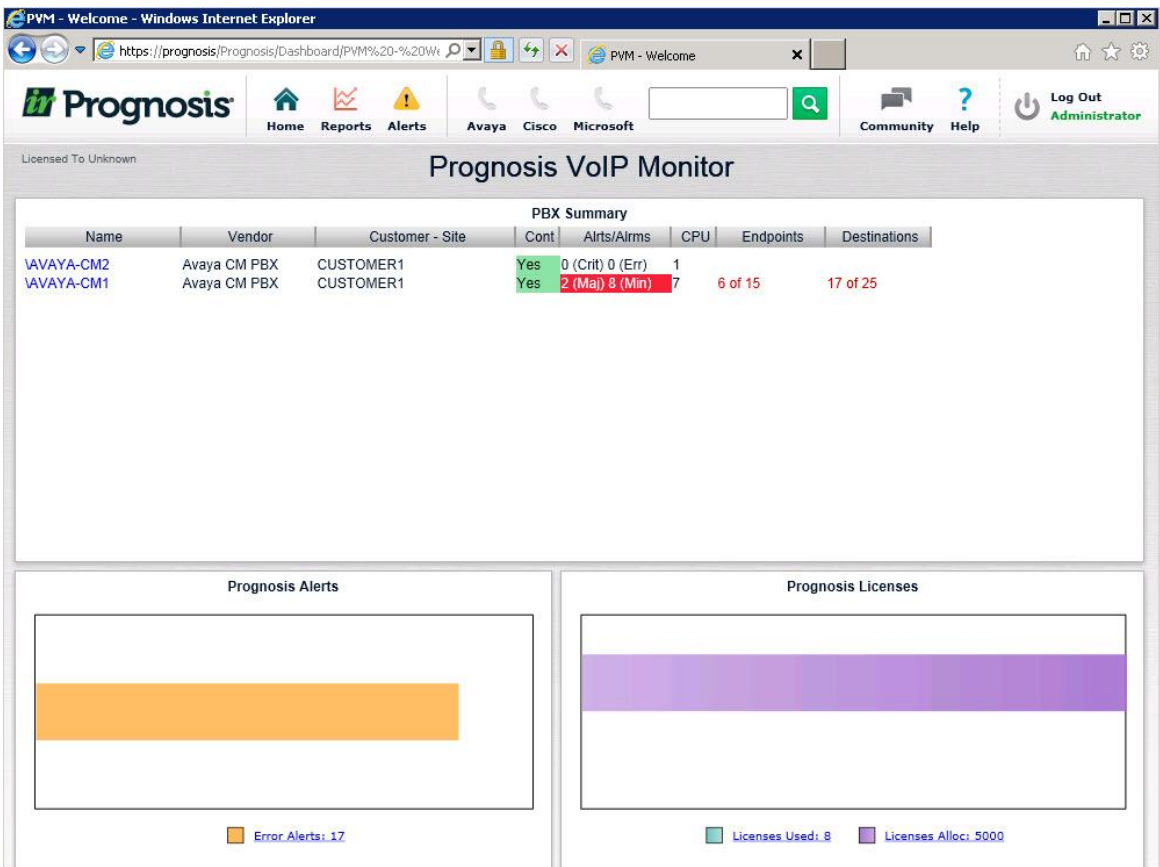
This section provides the steps that can be performed to verify proper configuration of Communication Manager and Prognosis VoIP Monitor.

7.1. Verify Communication Manager

Verify that Prognosis VoIP Monitor has established two concurrent SSH connections to the SAT by using the **status logins** command.

status logins				
COMMUNICATION MANAGER LOGIN INFORMATION				
Login	Profile	User's Address	Active Command	Session
Prognosi	20	10.64.101.44		1
Prognosi	20	10.64.101.44		3

7.2. Verify Integrated Research Prognosis VoIP Monitor

Step	Description
1.	<p>On the Prognosis VoIP Monitor server, click Start → All Programs → Prognosis VoIP Monitor → View Systems to start the Prognosis VoIP Monitor application. Enter proper credentials to log in. The Prognosis VoIP Monitor page is displayed.</p> 

Step	Description
2.	<p>Click \AVAYA-CM1. The Avaya PBX page for Avaya-CM1 is displayed. Verify that the SAT Connections field shows 2. Make IP calls between various Avaya telephones that trigger RTCP information to be sent to the Prognosis VoIP Monitor server. Verify that the Voice Quality (Streams) section shows correct number of voice streams and the quality of the voice streams.</p> <p>Repeat the step for \AVAYA-CM2.</p>

AV-PBX - Windows Internet Explorer

https://prognosis/Prognosis/Dashboard/AV-PBX?DefaultN

AV-PBX

Prognosis

Home

Reports

Alerts

Avaya

Cisco

Microsoft

Community

Help

Log Out Administrator

Licensed To Avaya Support

Avaya PBX

SAT Connections 2

Avaya PBXs

PBX

\AVAYA-CM1

\AVAYA-CM2

AVAYA-CM1

SAT Availability

Now

This Hr

Today

100.00

100.00

100.00

PROGNOSIS Raised Alerts

Severity

Alerts

Error

Warning

17

1

PBX Status

Type	Up	Down	Degr	Unkn	Total
Boards	7	5			12
Media Servers	1			1	1
Network Regions	2			248	250
Phones	6	4		5	15
Port Networks	1	1		2	2
Route Patterns	2	2	1	14	19
Trunk Groups	17	8			25

Major 2

Minor 8

CPU 3

PBX Busy Hour

Configuration

Worksheets

Voice Streams

Streams

Good

Fair

Poor

Unacceptable

58

58.00

100

80

60

40

20

0

15:28:30

15:25:50

15:27:50

Gd (58.00)

Fr (0.00)

Pr (0.00)

Un (0.00)

Processor

100

80

60

40

20

0

15:28:30

15:25:50

15:27:50

Call Processing (0 %)

Static (1 %)

System Management (2 %)

Step	Description
3.	<p>On the Avaya PBX page for Avaya-CM2, click Media Servers in the PBX Status box. The Avaya Media Servers page is displayed. Verify that the Cluster Status fields and Server fields are populated and the values are correct.</p>

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis VoIP Monitor to interoperate with Avaya Aura® Communication Manager. In the configuration described in these Application Notes, the Prognosis VoIP Monitor established SSH and SNMP connections to the SAT to view the configurations of Communication Manager and to monitor for status. Prognosis VoIP Monitor also processed the RTCP information to monitor the quality of IP calls.

9. Additional References

The following document can be found at <http://support.avaya.com>:

[1] *Avaya Aura® Communication Manager Feature Description and Implementation*, Release 6.2, Issue 9.0, July 2012, Document Number 555-245-205.

[2] *Administering Avaya Aura® Communication Manager*, Release 6.2, Issue 7.0, July 2012, Document Number 03-300509.

The following documentation is provided by Integrated Research.

[3] *Prognosis VoIP Monitor 4.0 Installation and Configuration Guide*, August 29, 2012

©2013 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.