



Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research PROGNOSIS IP Telephony Manager 9.6 with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research PROGNOSIS IP Telephony Manager 9.6 to interoperate with Avaya Aura® Communication Manager 6.0.1.

PROGNOSIS IP Telephony Manager is a performance management solution for multi-vendor IP telephony solutions. PROGNOSIS IP Telephony Manager provides visibility of Avaya and other vendor's IP Telephony solutions from a single console. Targeted at multi-site enterprises and managed service providers of IP telephony solutions, PROGNOSIS IP Telephony Manager offers a multi-customer, multi-PBX perspective, enabling a significant reduction in complexity when managing complex IP telephony environments.

PROGNOSIS integrates directly to Communication Manager using Secure Shell (SSH). At the same time, it processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from 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 IP Telephony Manager with Avaya Aura® Communication Manager.

The PROGNOSIS IP Telephony Manager is based on the PROGNOSIS product-family architecture for the scalable monitoring of business critical systems. The PROGNOSIS product consists of:

- One or more PROGNOSIS Monitoring Nodes (Server Nodes). These are servers used by the PROGNOSIS product to collect, relay and store information collected from Communication Manager.
- The PROGNOSIS GUI is a Microsoft Windows client program which is used to connect to a PROGNOSIS Monitoring Node and display the information collected by the Monitoring Node. The PROGNOSIS GUI may either be installed on a Monitoring Node or on a separate computer.

The PROGNOSIS IP Telephony Manager product uses three methods to monitor a Communication Manager system.

- System Access Terminal (SAT) - The PROGNOSIS IP Telephony Manager uses a pool of SSH connections to the SAT using the IP address of the Avaya Server. By default, the solution establishes three concurrent SAT connections to the Communication Manager system and uses the connections to execute SAT commands.
- Real Time Transport Control Protocol (RTCP) Collection - The PROGNOSIS IP Telephony Manager collects RTCP information sent by the Avaya IP Media Processor (MEDPRO) boards, media gateways, IP Telephones and IP Softphones.
- Call Detail Recording (CDR) Collection - The PROGNOSIS IP Telephony Manager collects CDR information sent by Communication Manager.

2. General Test Approach and Test Results

The general test approach was to use PROGNOSIS GUI to display the configurations of the Communication Manager systems and verify against what is displayed on the SAT interface. The SAT interface is accessed by using either telnet or Secure Shell (SSH) to the Avaya S8800 and S8300D Servers. Calls were placed between various Avaya endpoints and PROGNOSIS GUI was used to display the RTCP and CDR information collected.

2.1. Interoperability Compliance Testing

For feature testing, PROGNOSIS GUI was used to view the configurations of Communication Manager such as port networks, cabinets, media gateways, ESS, LSP, trunk groups, route patterns, CLAN, MEDPRO and DS1 boards, IP network regions, stations, processor occupancy, alarm and error information. During testing, a call generator was used to load the Communication Manager systems by placing incoming calls through two E1 ISDN-PRI trunks to the system in Site A and terminating the calls as IP stations on the system in Site B. For the collection of RTCP and CDR information, the endpoints included Avaya IP, digital and analog telephones, Avaya A175 Desktop Video Device and Avaya one-X® Communicator users. The types of calls made included intra-switch calls, inbound/outbound inter-switch IP trunk calls, transferred calls and conference calls.

For serviceability testing, reboots were applied to the PROGNOSIS IP Telephony Manager Server and Avaya Servers to simulate system unavailability. Interchanging of the Avaya S8800 Servers and failover to ESS and LSP were also performed during testing.

2.2. Test Results

All test cases passed successfully.

2.3. Support

For technical support on Integrated Research PROGNOSIS IP Telephony Manager, contact the Integrated Research Support Team at:

- Hotline: +61 (2) 9921 1524
- Email: support@prognosis.com

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Integrated Research PROGNOSIS IP Telephony Manager interoperability with Communication Manager. It consists of a Communication Manager system running on a pair of Avaya S8800 Servers with two Avaya G650 Media Gateways, an Avaya G430 Media Gateway with Avaya S8300D Server as a Local Survivability Processor (LSP) and an Avaya G250-BRI Media Gateway. An Enterprise Survivable Server (ESS) running on Avaya S8800 Server was also configured for failover testing. A second Communication Manager system runs on an Avaya S8300D Server with an Avaya G450 Media Gateway. Both systems have Avaya IP (H.323 and SIP), digital and analog telephones, and Avaya one-X[®] Communicator users configured for making and receiving calls. IP Trunks connect the two systems together to allow calls between them. Avaya Aura[®] System Manager and Avaya Aura[®] Session Manager provided SIP support to the Avaya SIP telephones and Avaya A175 Desktop Video Device. Integrated Research PROGNOSIS IP Telephony Manager was installed on a server running Microsoft Windows Server 2003 with Service Pack 2. Both the Monitoring Node and GUI software are installed on this server. The Avaya 4548GT-PWR Ethernet Routing Switch provides Ethernet connectivity to the servers, media gateways and IP telephones.

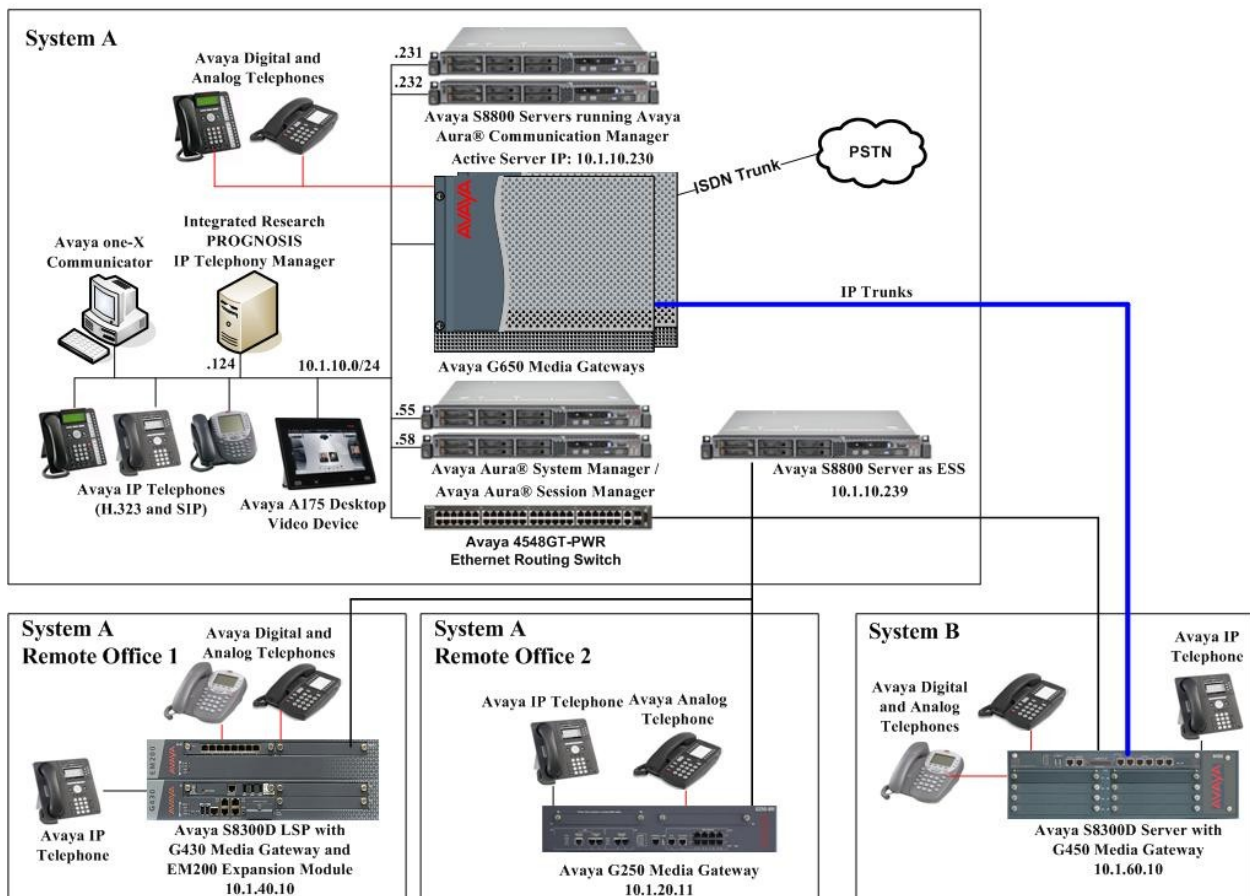


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Servers	Avaya Aura® Communication Manager 6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya G650 Media Gateways - TN2312BP IP Server Interface - TN799DP C-LAN Interface - TN2302AP IP Media Processor - TN2602AP IP Media Processor - TN2214CP Digital Line - TN793CP Analog Line - TN2464BP DS1 Interface - TN2464CP DS1 Interface	- HW07, FW053 and HW15 FW054 HW01, FW039 and HW01 FW040 HW20 FW121 and HW20 FW117 HW02 FW058 and HW02 FW041 HW08 FW015 HW09 FW010 HW05 FW024 HW02 FW024
Avaya G250-BRI Media Gateway	30.18.1
Avaya G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	31.18.1 HW04 FW009 HW04 FW073 HW31 FW093 HW05 FW021
Avaya S8300D Server as LSP	6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya S8800 Server as ESS	6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya S8300D Server	Avaya Aura® Communication Manager 6.0.1 (Service Pack 1.01 00.1.510.1-18857)
Avaya G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	31.18.1 HW01 FW008 HW07 FW009 HW10 FW093 HW03 FW009 HW11 FW049
Avaya Aura® System Manager	6.1 Service Pack 2
Avaya Aura® Session Manager	6.1 Service Pack 2
Avaya 9600 Series IP telephones - 9630, 9640, 9650, 9670G	3.1 SP2 (H.323) or 2.6 SP4 (SIP)
Avaya 1608 IP telephones	1.300B (H.323)
Avaya 6221 analog telephones	-

Equipment	Software
Avaya digital telephones - 1416 - 2420	SP1 -
Avaya A175 Desktop Video Device	1.0
Avaya one-X® Communicator	6.0 SP1 (H.323)
Avaya 4548GT-PWR Ethernet Routing Switch	V5.4.0.008
Integrated Research PROGNOSIS IP Telephony Manager	9.6.1 Patch 11

5. Configure Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with Integrated Research PROGNOSIS IP Telephony Manager. This includes creating a login account and a SAT User Profile for PROGNOSIS to access Communication Manager and enabling RTCP and CDR reporting. The steps are repeated for each Communication Manager system, ESS and LSP Servers.

5.1. Configure SAT User Profile

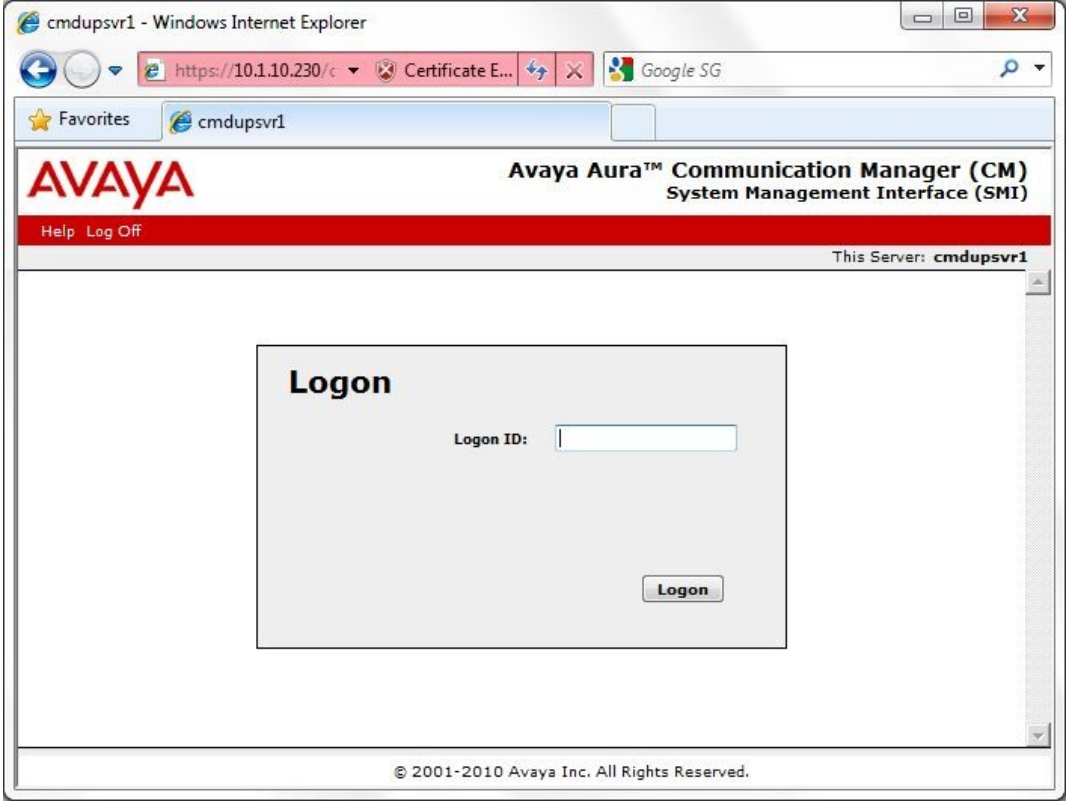
A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As PROGNOSIS IP Telephony Manager does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the PROGNOSIS login account.

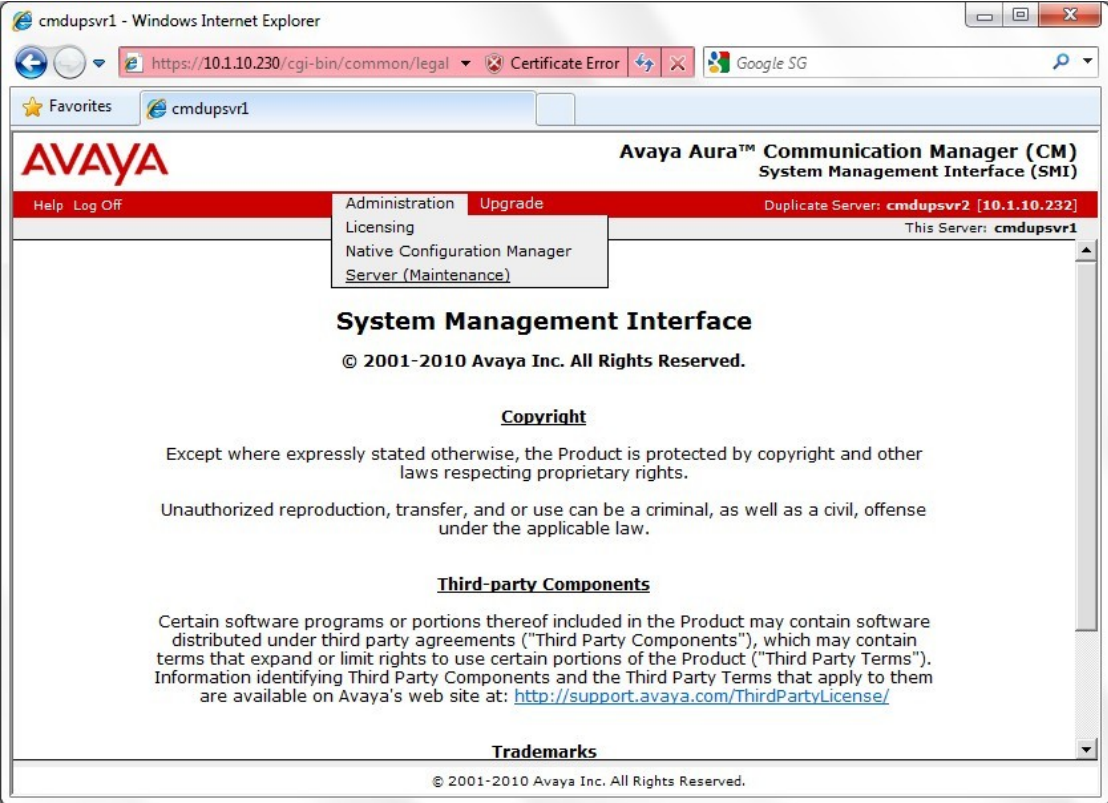
Step	Description
1.	Enter the add user-profile <i>n</i> command, where <i>n</i> is the next unused profile number. Enter a descriptive name for User Profile Name and enable all categories by setting the Enbl field to y . In this configuration, the user profile 21 is created.
	<pre> add user-profile 21 Page 1 of 41 USER PROFILE 21 User Profile Name: IPTM 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 <input checked="" type="checkbox"/> Routing and Dial Plan J <input checked="" type="checkbox"/> Call Center B <input checked="" type="checkbox"/> Security K <input checked="" type="checkbox"/> Features C <input checked="" type="checkbox"/> Servers L <input checked="" type="checkbox"/> Hardware D <input checked="" type="checkbox"/> Stations M <input checked="" type="checkbox"/> Hospitality E <input checked="" type="checkbox"/> System Parameters N <input checked="" type="checkbox"/> IP F <input checked="" type="checkbox"/> Translations O <input checked="" type="checkbox"/> Maintenance G <input checked="" type="checkbox"/> Trunking P <input checked="" type="checkbox"/> Measurements and Performance H <input checked="" type="checkbox"/> Usage Q <input checked="" type="checkbox"/> Remote Access I <input checked="" type="checkbox"/> User Access R <input checked="" type="checkbox"/> </pre>

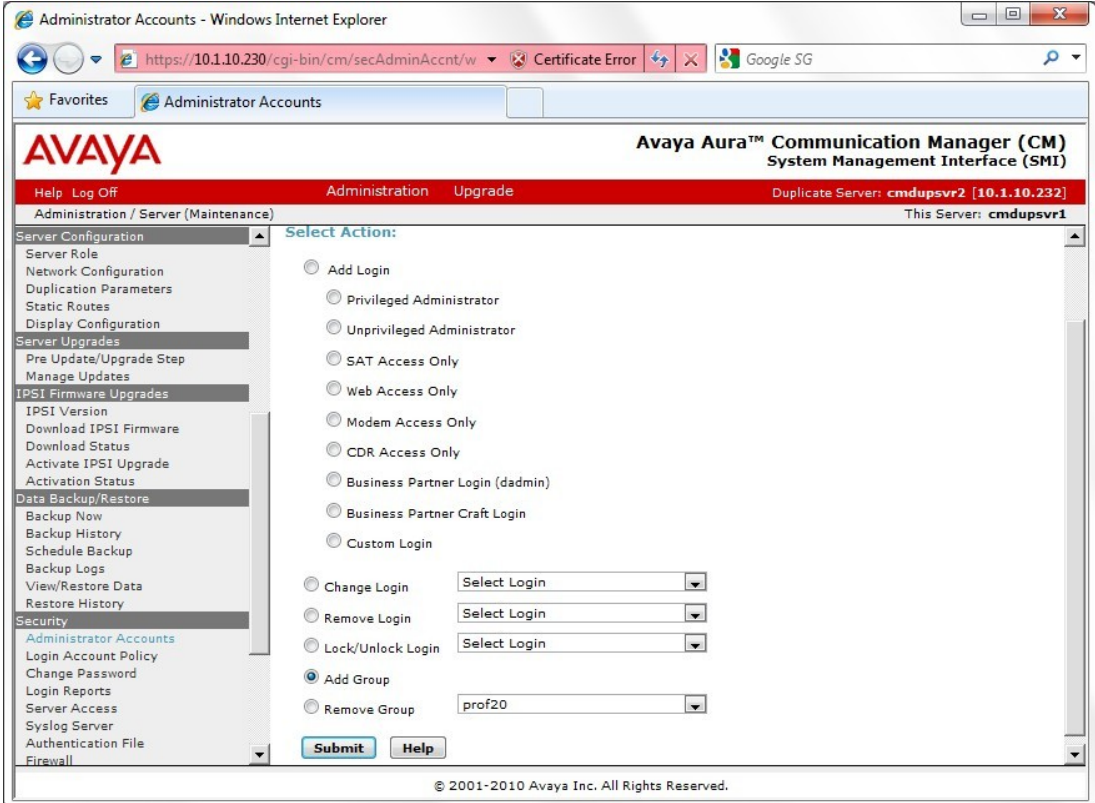
Step	Description
2.	<p>On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to rm (read and maintenance). This can be accomplished by typing rm into the field Set All Permissions To. Submit the form to create the user profile.</p>
	<pre> add user-profile 21 Page 2 of 41 USER PROFILE 21 Set Permissions For Category: To: Set All Permissions To: rm '-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance 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-endpoints P rm adjunct-names A rm administered-connections C rm aesvcs cti-link A rm aesvcs interface A rm </pre>


5.2. Configure Login Group

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 <code>https://<IP address of Avaya Server></code> to connect to the Avaya Server being configured and log in using appropriate credentials.</p> 

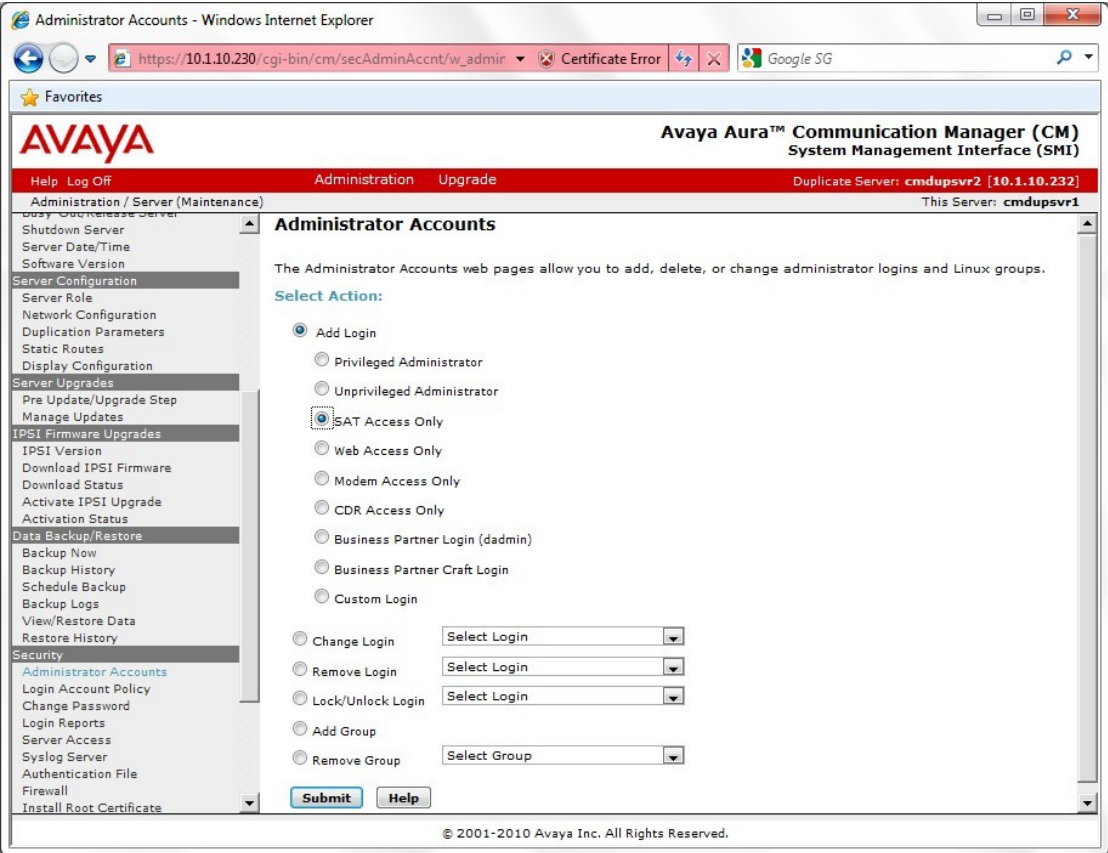
Step	Description
2.	<p>Click Administration > Server (Maintenance). This will open up the Server Administration Interface that will allow the user to complete the configuration process.</p>  <p>The screenshot shows a web browser window with the following details:</p> <ul style="list-style-type: none"> Browser: cmdupsvr1 - Windows Internet Explorer Address Bar: https://10.1.10.230/cgi-bin/common/legal Page Title: Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) Navigation Menu: Help, Log Off, Administration, Upgrade, Duplicate Server: cmdupsvr2 [10.1.10.232], This Server: cmdupsvr1 Sub-menu (under Administration): Licensing, Native Configuration Manager, Server (Maintenance) Main Content: <ul style="list-style-type: none"> System Management Interface © 2001-2010 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 © 2001-2010 Avaya Inc. All Rights Reserved.

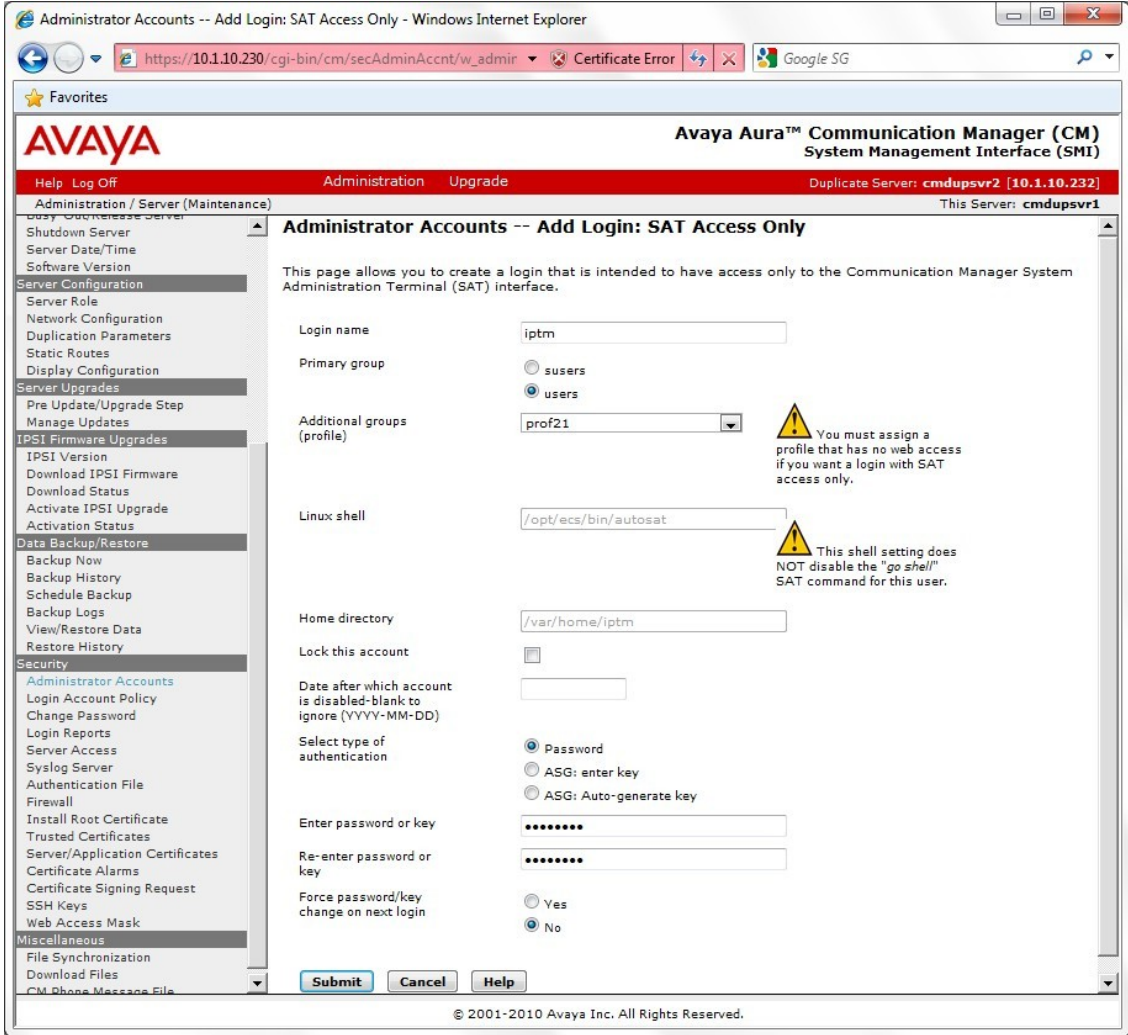
Step	Description
3.	<p>From the navigation panel on the left side, click Administrator Accounts under Security. Select Add Group and click Submit.</p>  <p>The screenshot shows the Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) in a Windows Internet Explorer browser. The page title is 'Administrator Accounts - Windows Internet Explorer'. The address bar shows 'https://10.1.10.230/cgi-bin/cm/secAdminAccnt/w'. The page header includes the Avaya logo and 'Avaya Aura™ Communication Manager (CM) System Management Interface (SMI)'. The navigation menu on the left is expanded to 'Security', and 'Administrator Accounts' is selected. The 'Select Action:' section has the 'Add Group' radio button selected. The 'Remove Group' dropdown menu is set to 'prof20'. The 'Submit' button is visible at the bottom of the form.</p>

Step	Description
4.	<p>Select Add a new access-profile group and select prof21 from the drop-down box to correspond to the user-profile created in Section 5.1 Step 1. Click Submit. This completes the creation of the login group.</p> 

5.3. Configure Login

Create a login account for PROGNOSIS 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>For the field Login name, enter a login to be used by PROGNOSIS. In this configuration, the login iptm is created. Configure the other parameters for the login as follows:</p> <ul style="list-style-type: none"> • Primary group: Select users [Limits the permissions of the login] • Additional groups (profile): prof21 [Select the login group created in Section 5.2 Step 4.] • Select type of authentication: Select Password [Uses a password for authentication.] • Enter password or key / Re-enter password or key [Define the password.] • Force password/key change on next login: Select No <p>Click Submit to continue. This completes the configuration of the login.</p> 

5.4. Configure RTCP Monitoring

To allow PROGNOSIS IP Telephony Manager to monitor the quality of IP calls, configure Communication Manager to send RTCP reporting to the IP address of the PROGNOSIS server. This is done through the SAT interface.

Step	Description
1.	<p>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 IP Telephony Manager server. Set IPV4 Server Port to 5005 and RTCP Report Period (secs) to 5.</p> <pre> change system-parameters ip-options Page 1 of 3 IP-OPTIONS SYSTEM PARAMETERS IP MEDIA PACKET PERFORMANCE THRESHOLDS Roundtrip Propagation Delay (ms) High: 800 Low: 400 Packet Loss (%) High: 40 Low: 15 Ping Test Interval (sec): 20 Number of Pings Per Measurement Interval: 10 Enable Voice/Network Stats? n RTCP MONITOR SERVER Server IPV4 Address: 10.1.10.124 RTCP Report Period(secs): 5 IPV4 Server Port: 5005 Server IPV6 Address: IPV6 Server Port: 5005 AUTOMATIC TRACE ROUTE ON Link Failure? y H.323 IP ENDPOINT H.248 MEDIA GATEWAY Link Loss Delay Timer (min): 5 Link Loss Delay Timer (min): 5 Primary Search Time (sec): 75 Periodic Registration Timer (min): 20 Short/Prefixed Registration Allowed? N </pre>
2.	<p>Enter the change ip-network-region n command, where n is IP network region number to be monitored. On Page 2, set RTCP Reporting Enabled to y and Use Default Server Parameters to y.</p> <p>Note: Only one RTCP MONITOR SERVER can be configured per IP network region.</p> <pre> change ip-network-region 1 Page 2 of 20 IP NETWORK REGION RTCP Reporting Enabled? y RTCP MONITOR SERVER PARAMETERS Use Default Server Parameters? Y </pre>
3.	Repeat Step 2 for all IP network regions that are required to be monitored.

5.5. Configure CDR Monitoring

To allow PROGNOSIS IP Telephony Manager to monitor the CDR information, configure Communication Manager to send CDR information to the IP address of the PROGNOSIS server.

Step	Description
1.	<p>Enter the change ip-interface procr command to enable the processor-ethernet interface on the Avaya Server. Set Enable Interface to y. This interface will be used by Communication Manager to send out the CDR information.</p> <pre> change ip-interface procr Page 1 of 2 IP INTERFACES Type: PROCR Target socket load: 19660 Enable Interface? y Allow H.323 Endpoints? y Allow H.248 Gateways? y Network Region: 1 Gatekeeper Priority: 5 IPV4 PARAMETERS Node Name: procr IP Address: 10.1.10.230 Subnet Mask: /24 </pre>
2.	<p>Enter the change node-names ip command to add a new node name for the PROGNOSIS server. In this configuration, the name iptm is added with the IP address specified as 10.1.10.124. Note also the node name procr which is automatically added.</p> <pre> change node-names ip Page 1 of 2 IP NODE NAMES Name IP Address CLAN-01a02 10.1.50.21 CLAN-01a03 10.1.50.22 CLAN-02a02 10.1.10.21 DefaultRouter 10.1.50.1 MEDPRO-01a07 10.1.50.31 MEDPRO-01a08 10.1.50.32 MEDPRO-01a09 10.1.50.33 MEDPRO-02a13 10.1.10.31 MEDPRO-02a14 10.1.10.32 VAL-01a11 10.1.50.41 cm6ess 10.1.10.239 default 0.0.0.0 iptm 10.1.10.124 procr 10.1.10.230 procr6 :: router10 10.1.10.1 </pre>

Step	Description																							
3.	<p>Enter the change ip-services command to define the CDR link. To define a primary CDR link, the following information should be provided:</p> <ul style="list-style-type: none"> • Service Type: CDR1 [Note: If needed, a secondary link can be defined by setting Service Type to CDR2.] • Local Node: procr [Note: Communication Manager will use the processor-ethernet interface to send out the CDR.] • Local Port: 0 [Note: The Local Port is set to 0 because Communication Manager initiates the CDR link.] • Remote Node: iptm [Note: The Remote Node is set to the node name previously defined in Step 1.] • Remote Port: 50000 [Note: The Remote Port may be set to a value between 5000 and 64500 inclusive. 50000 is the default port number used by PROGNOSIS and the PROGNOSIS server uses the same port number for all Avaya Servers sending CDR information to it.] 																							
<pre>change ip-services</pre> <p style="text-align: right;">Page 1 of 3</p> <table border="1"> <thead> <tr> <th colspan="7">IP SERVICES</th> </tr> <tr> <th>Service Type</th> <th>Enabled</th> <th>Local Node</th> <th>Local Port</th> <th>Remote Node</th> <th>Remote Port</th> <th></th> </tr> </thead> <tbody> <tr> <td>CDR1</td> <td></td> <td>procr</td> <td>0</td> <td>iptm</td> <td>50000</td> <td></td> </tr> </tbody> </table>		IP SERVICES							Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port		CDR1		procr	0	iptm	50000			
IP SERVICES																								
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																			
CDR1		procr	0	iptm	50000																			
<p>On Page 3 of the IP SERVICES form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the Reliable Protocol field to n.</p>																								
<pre>change ip-services</pre> <p style="text-align: right;">Page 3 of 3</p> <table border="1"> <thead> <tr> <th colspan="7">SESSION LAYER TIMERS</th> </tr> <tr> <th>Service Type</th> <th>Reliable Protocol</th> <th>Packet Timer</th> <th>Resp</th> <th>Session Message</th> <th>Connect Cntr</th> <th>SPDU Cntr</th> <th>Connectivity Timer</th> </tr> </thead> <tbody> <tr> <td>CDR1</td> <td>n</td> <td>30</td> <td></td> <td></td> <td>3</td> <td>3</td> <td>60</td> </tr> </tbody> </table>		SESSION LAYER TIMERS							Service Type	Reliable Protocol	Packet Timer	Resp	Session Message	Connect Cntr	SPDU Cntr	Connectivity Timer	CDR1	n	30			3	3	60
SESSION LAYER TIMERS																								
Service Type	Reliable Protocol	Packet Timer	Resp	Session Message	Connect Cntr	SPDU Cntr	Connectivity Timer																	
CDR1	n	30			3	3	60																	

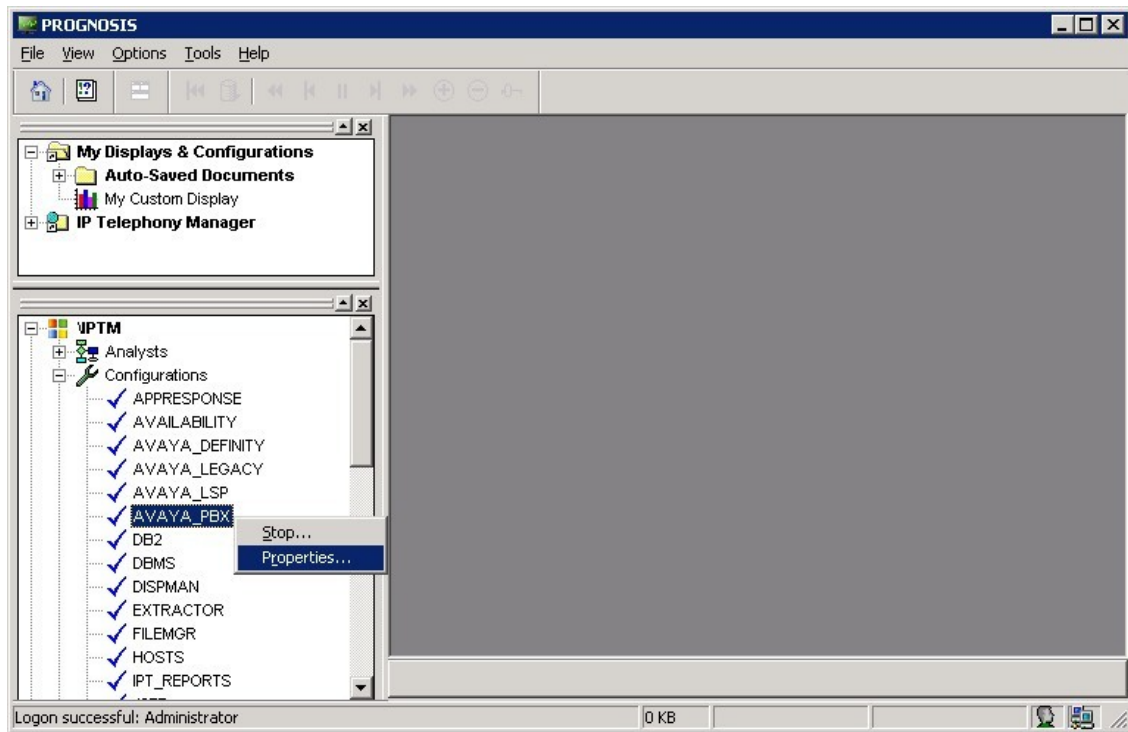
Step	Description
4.	<p>Enter the change system-parameters cdr command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test.</p> <ul style="list-style-type: none"> • CDR Date Format: month/day • Primary Output Format: unformatted [Note: This value is used to configure PROGNOSIS in Section 5 Step 3.] • Primary Output Endpoint: CDR1 <p>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.</p> <ul style="list-style-type: none"> • Use Legacy CDR Formats? y [Note: Specify the use of the Communication Manager 3.x (“legacy”) formats in the CDR records produced by the system.] • Intra-switch CDR: y [Note: 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 [Note: Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.] • Outg Trk Call Splitting? y [Note: Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.] • Inc Trk Call Splitting? n [Note: Do not allow a separate call record for any portion of an incoming call that is transferred or conferenced.]
	<pre> 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: unformatted Primary Output Endpoint: CDR1 Secondary Output Format: Secondary Output Endpoint: Use ISDN Layouts? n Enable CDR Storage on Disk? n Use Enhanced Formats? n Condition Code 'T' For Redirected Calls? n Use Legacy CDR Formats? y 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? y 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: member-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? 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: 15 </pre>

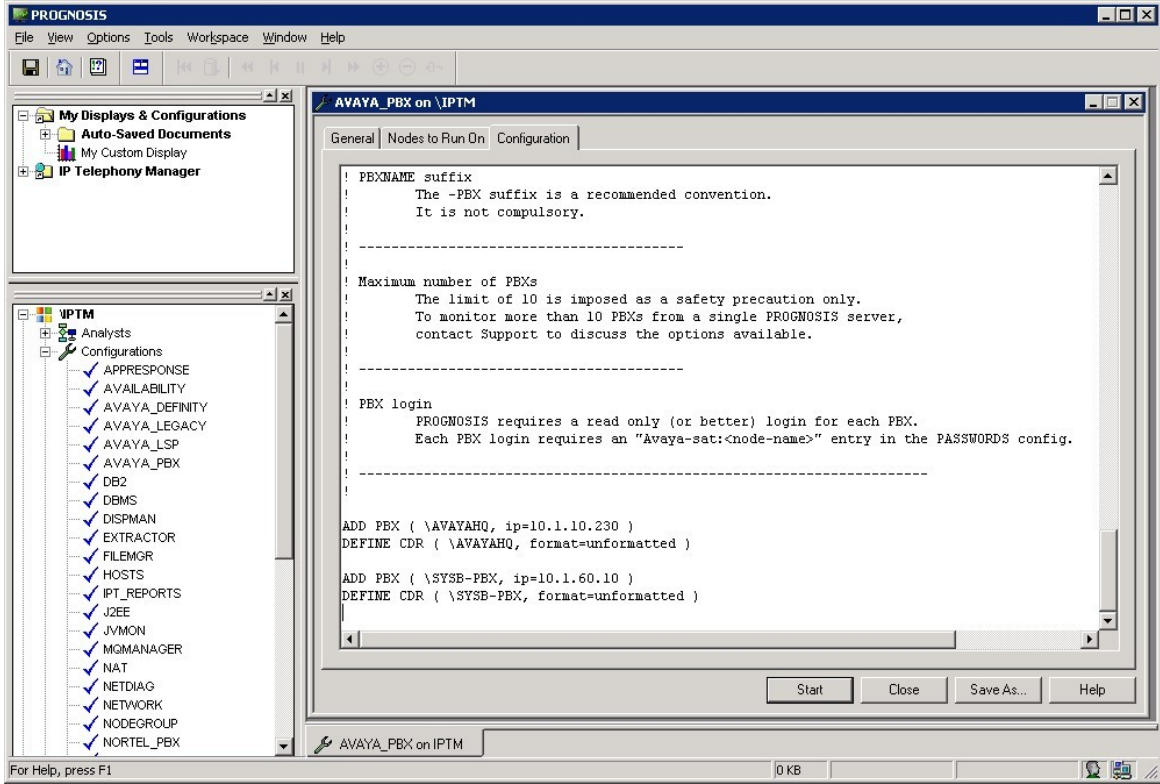
Step	Description
5.	<p>If the Intra-switch CDR field is set to y on Page 1 of the CDR SYSTEM PARAMETERS form, then enter the change intra-switch-cdr command to define the extensions that will be subjected to call detail recording. In the Assigned Members field, enter the specific extensions whose usage will be tracked with the CDR records.</p> <pre> change intra-switch-cdr Page 1 of 3 INTRA-SWITCH CDR Assigned Members: 8 of 5000 administered Extension Extension Extension Extension 10001 10002 10003 10004 10005 10006 10007 10008 </pre>
6.	<p>For each trunk group for which CDR records are desired, verify that CDR reporting is enabled. Enter the change trunk-group n command, where n is the trunk group number, to verify that the CDR Reports field is set to y. Repeat for all trunk groups to be reported.</p> <pre> change trunk-group 6 Page 1 of 21 TRUNK GROUP Group Number: 6 Group Type: sip CDR Reports: <input checked="" type="checkbox"/> Group Name: SIP Trunk to SM6 COR: 1 TN: 1 TAC: #06 Direction: two-way Outgoing Display? y Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Member Assignment Method: auto Signaling Group: 6 Number of Members: 20 </pre>

6. Configure Integrated Research PROGNOSIS IP Telephony Manager

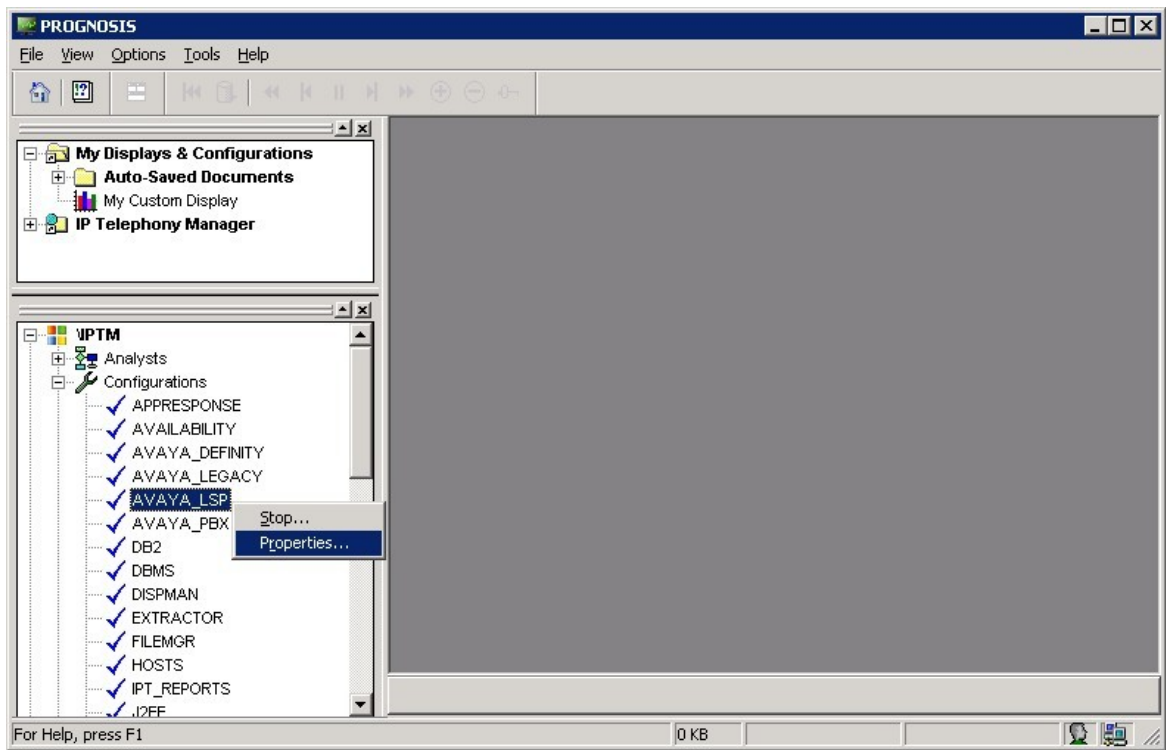
This section describes the configuration of PROGNOSIS IP Telephony Manager required to interoperate with Communication Manager.

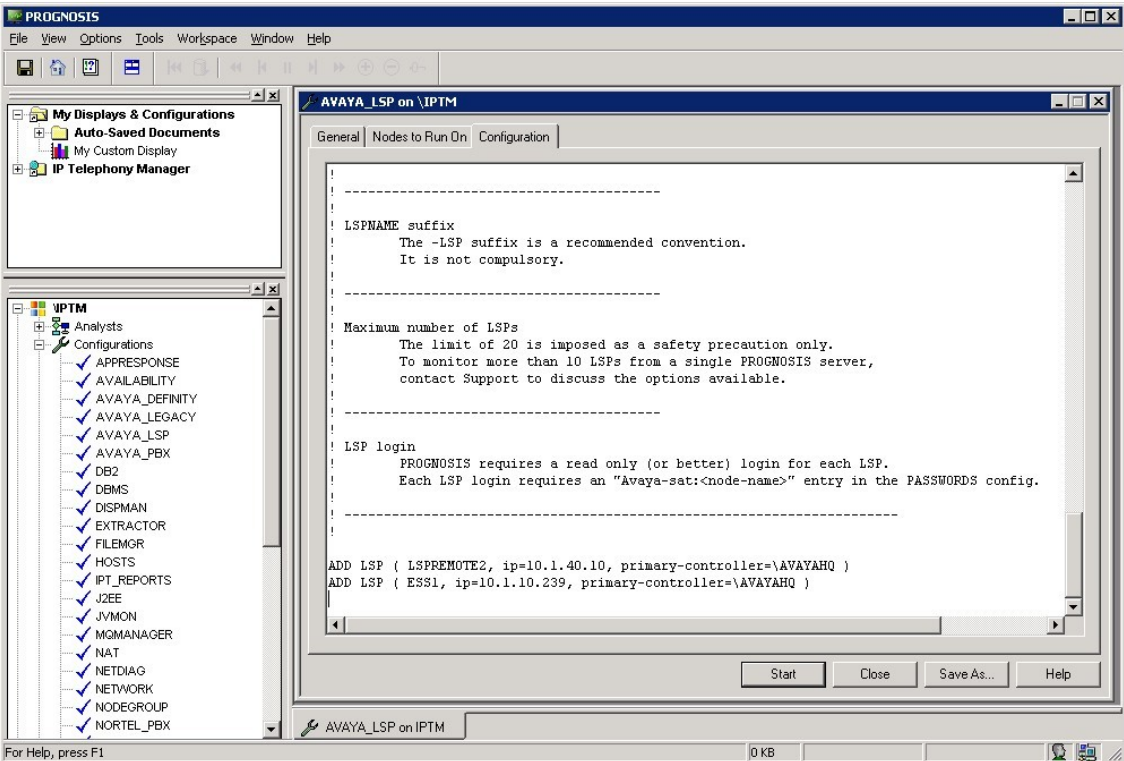
Step	Description
1.	On PROGNOSIS IP Telephony Manager server, click Start > All Programs > PROGNOSIS IP Telephony Manager > IP Telephony Manager GUI to start the IP Telephony Manager GUI application. Enter a valid Windows user account and password to log in.
2.	To configure the Communication Manager systems to be monitored, expand Configurations of the Monitoring Node, right-click on AVAYA_PBX and select Properties .

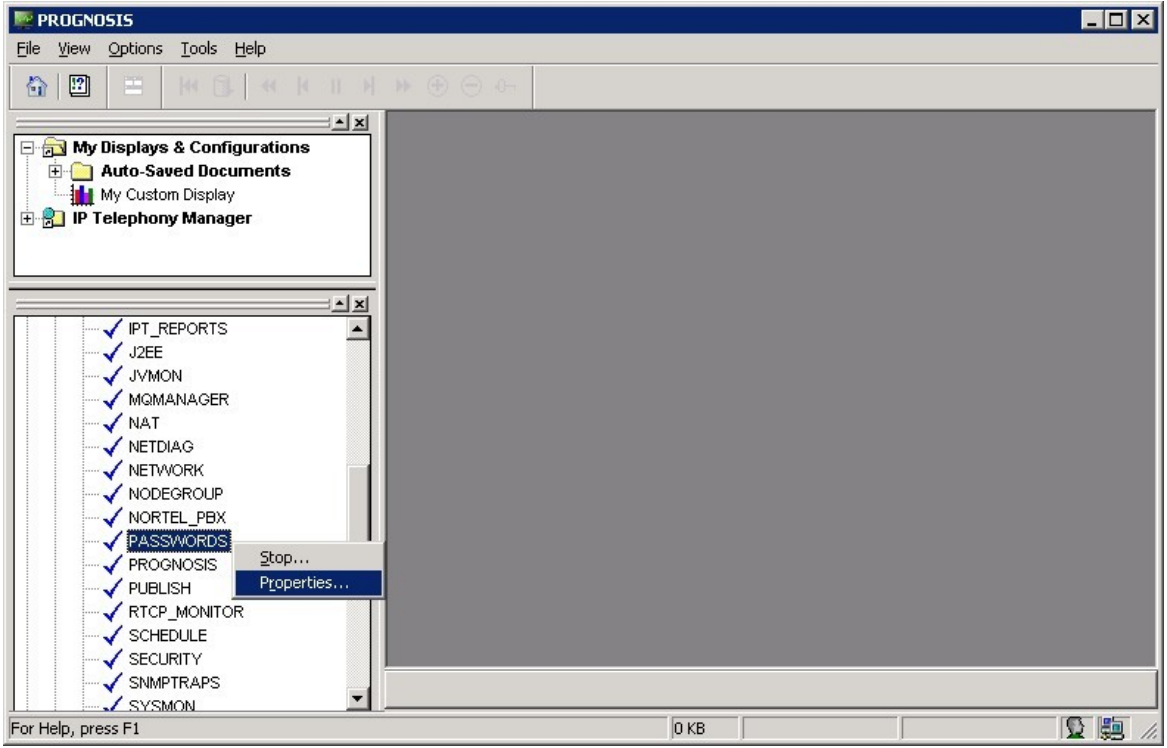


Step	Description
3.	<p>In the Configuration tab, add an entry for each Communication Manager system to be managed. The template to add a system is provided in the PROGNOSIS GUI application. In this test configuration, the following entries are added for the two Communication Manager systems with the names AVAYAHQ and SYSB-PBX and with the IP addresses of the Avaya Servers 10.1.10.230 and 10.1.60.10 respectively. The PROGNOSIS Monitoring Node will use SSH to connect to port 5022 of the Avaya Servers.</p> <p style="text-align: center;">ADD PBX (\AVAYAHQ, ip=10.1.10.230) ADD PBX (\SYSB-PBX, ip=10.1.60.10)</p> <p>Define the CDR format to match the settings configured on Communication Manager in Section 5.5 Step 2 and 3 respectively.</p> <p style="text-align: center;">DEFINE CDR (\AVAYAHQ, format=unformatted) DEFINE CDR (\SYSB-PBX, format=unformatted)</p> <p>Click Start to proceed.</p> 

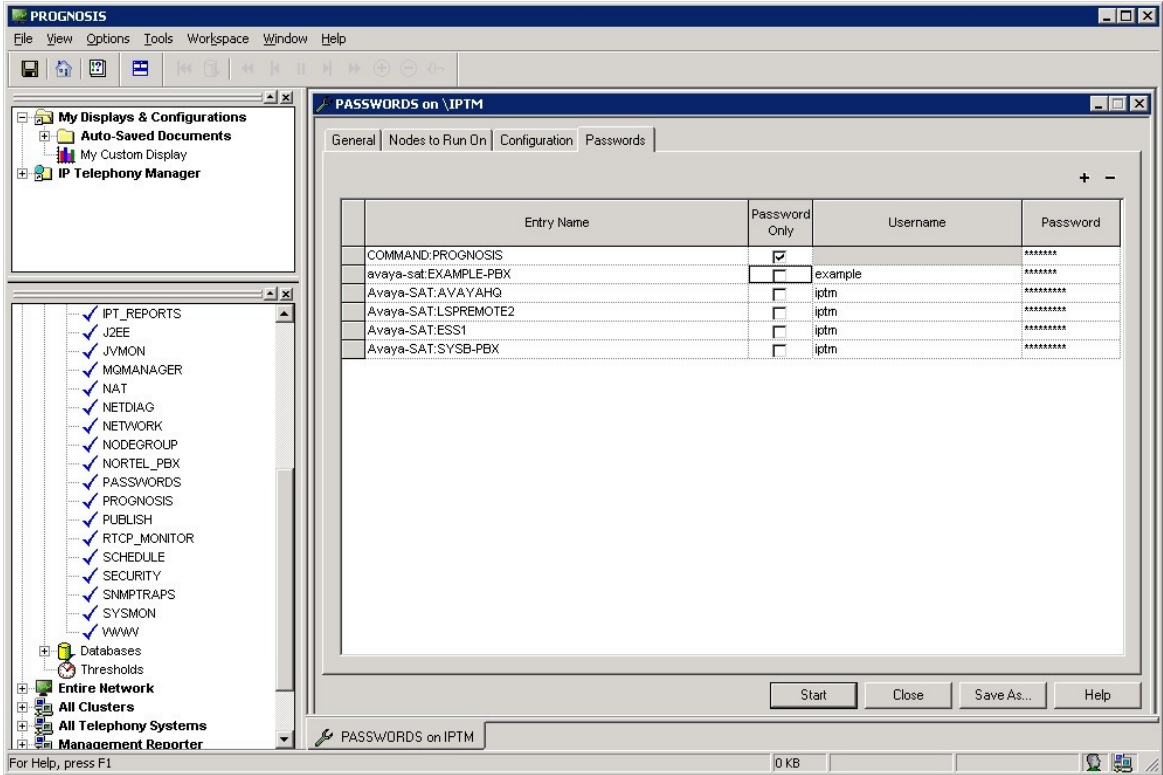
Step	Description
4.	To configure the ESS and LSP Servers to be monitored, expand Configurations of the Monitoring Node, right-click on AVAYA_LSP and select Properties .



Step	Description
5.	<p>In the Configuration tab, add an entry for each ESS or LSP Servers to be monitored. The template to add the server is provided in the PROGNOSIS GUI application. In this test configuration, the following entries are added for the ESS and LSP Servers with the names LSPREMOTE2 and ESS1 and with the IP addresses of 10.1.40.10 and 10.1.10.239 respectively, both belonging to the AVAYAHQ Communication Manager system.</p> <p style="padding-left: 40px;">ADD LSP (LSPREMOTE2, ip=10.1.40.10, primary-controller=\AVAYAHQ) ADD LSP (ESS1, ip=10.1.10.239, primary-controller=\AVAYAHQ)</p> <p>Click Start to proceed.</p> 

Step	Description
6.	<p>To configure the SAT login account and password, expand Configurations of the Monitoring Node, right-click on PASSWORDS and select Properties.</p> 

Step	Description
7.	<p>Click the + 'plus' button to add a new password entry for each of the configured systems in Steps 3 and 5. The Entry Name must be of the form Avaya-SAT:<pbx-name>. For the system with the name AVAYAHQ, enter Avaya-SAT:AVAYAHQ for Entry Name, uncheck Password Only, and enter the login account created in Section 5.3 for Username and Password. Repeat to add another three entries for the ESS and LSP Servers, and the second system SYSB-PBX. Click Start to proceed.</p>



The screenshot shows the PROGNOSIS application window. On the left is a tree view of system configurations, including 'IPT_REPORTS', 'J2EE', 'JVMON', 'MQMANAGER', 'NAT', 'NETDIAG', 'NETWORK', 'NODEGROUP', 'NORTEL_PBX', 'PASSWORDS', 'PROGNOSIS', 'PUBLISH', 'RTCP_MONITOR', 'SCHEDULE', 'SECURITY', 'SNMPTRAPS', 'SYSMON', 'WWW', 'Databases', and 'Thresholds'. The main window is titled 'PASSWORDS on \IPTM' and has tabs for 'General', 'Nodes to Run On', 'Configuration', and 'Passwords'. The 'Passwords' tab is active, showing a table with the following data:

Entry Name	Password Only	Username	Password
COMMAND:PROGNOSIS	<input checked="" type="checkbox"/>		*****
avaya-sat EXAMPLE-PBX	<input type="checkbox"/>	example	*****
Avaya-SAT:AVAYAHQ	<input type="checkbox"/>	iptm	*****
Avaya-SAT:LSPREMOTE2	<input type="checkbox"/>	iptm	*****
Avaya-SAT:ESS1	<input type="checkbox"/>	iptm	*****
Avaya-SAT:SYSB-PBX	<input type="checkbox"/>	iptm	*****

At the bottom of the window are buttons for 'Start', 'Close', 'Save As...', and 'Help'. The status bar at the bottom indicates '0 KB'.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Communication Manager and Integrated Research PROGNOSIS IP Telephony Manager.

7.1. Verify Communication Manager

Verify that PROGNOSIS IP Telephony Manager has established three 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
iptm	21	10.1.10.124	list measurements summary	1
iptm	21	10.1.10.124	list registered-ip-stations	3
iptm	21	10.1.10.124	stat trunk 10	4
*dadmin	2	10.1.10.99	stat logins	5

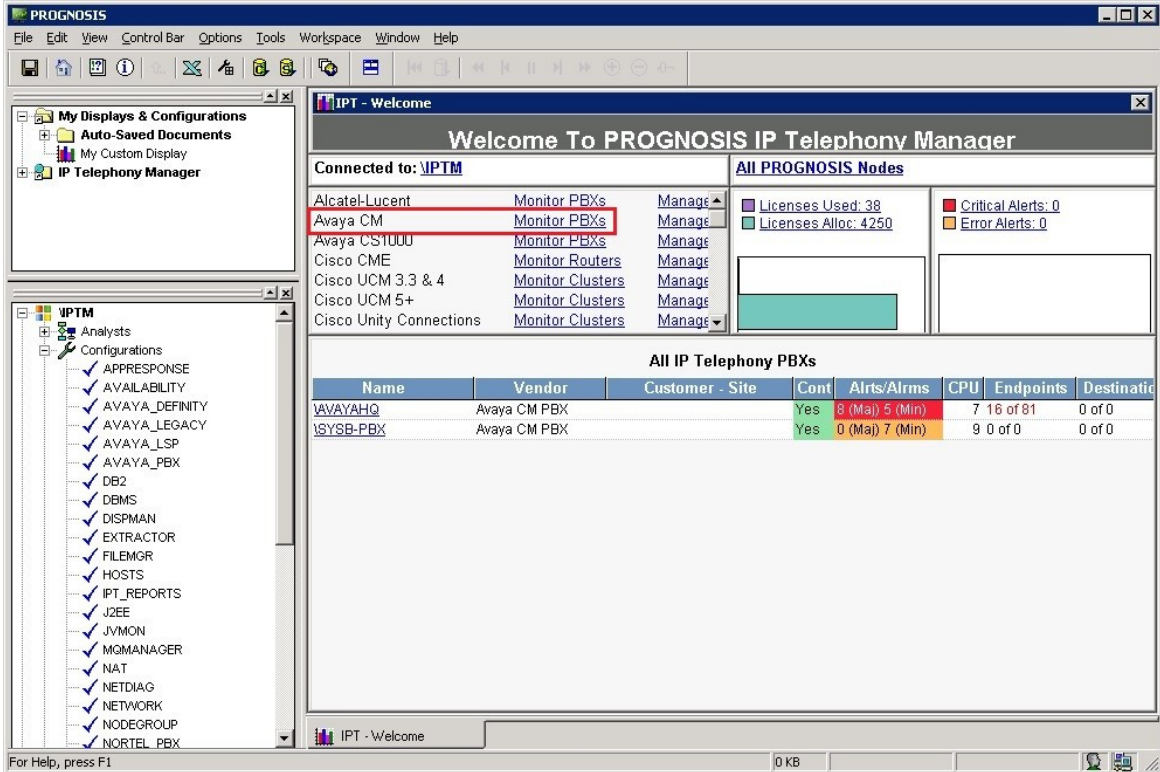
Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.5** shows **up**.

```
status cdr-link
```

CDR LINK STATUS	
Primary	Secondary
Link State: up	CDR not administered
Date & Time: 2011/04/14 17:16:20	0000/00/00 00:00:00
Forward Seq. No: 0	0
Backward Seq. No: 0	0
CDR Buffer % Full: 0.00	0.00
Reason Code: OK	

7.2. Verify Integrated Research PROGNOSIS IP Telephony Manager

The following steps are done using the PROGNOSIS GUI.

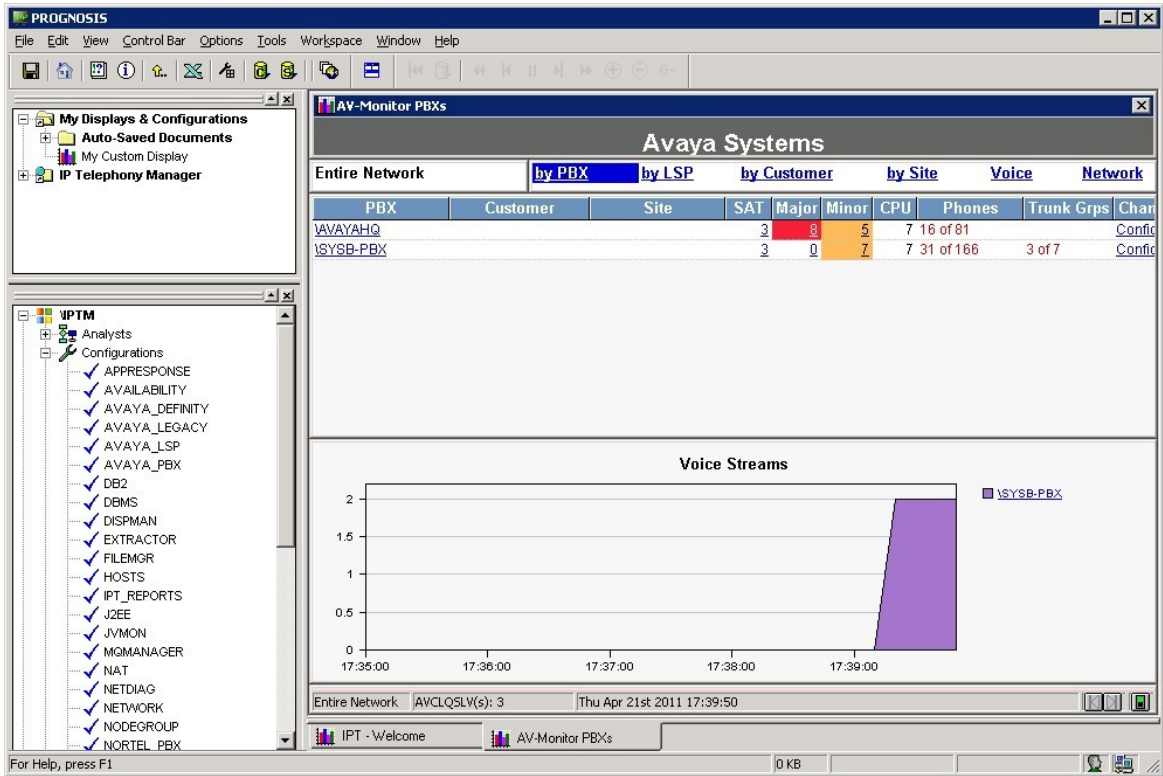
Step	Description																								
1.	<p>After logging into PROGNOSIS GUI, click on the Home button on the toolbar to display the Welcome screen. In the Monitor section, click Avaya CM > Monitor PBXs to display the list of Communication Manager Servers configured in Section 6.</p>  <p>The screenshot shows the PROGNOSIS GUI interface. The main window is titled 'IPT - Welcome' and displays 'Welcome To PROGNOSIS IP Telephony Manager'. On the left, there is a navigation tree with 'IP Telephony Manager' selected. The main content area shows a list of nodes connected to IPTM, including Alcatel-Lucent, Avaya CM, Avaya CS1000, Cisco CME, Cisco UCM 3.3 & 4, Cisco UCM 5+, and Cisco Unity Connections. The 'Avaya CM' node is highlighted with a red box, and its 'Monitor PBXs' link is also highlighted. Below this, there is a table titled 'All IP Telephony PBXs' with the following data:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Vendor</th> <th>Customer - Site</th> <th>Cont</th> <th>Alrts/Alrms</th> <th>CPU</th> <th>Endpoints</th> <th>Destinatio</th> </tr> </thead> <tbody> <tr> <td>WAWAYAHQ</td> <td>Avaya CM PBX</td> <td></td> <td>Yes</td> <td>8 (Max) 5 (Min)</td> <td>7</td> <td>16 of 81</td> <td>0 of 0</td> </tr> <tr> <td>WSYSB-PBX</td> <td>Avaya CM PBX</td> <td></td> <td>Yes</td> <td>0 (Max) 7 (Min)</td> <td>9</td> <td>0 of 0</td> <td>0 of 0</td> </tr> </tbody> </table>	Name	Vendor	Customer - Site	Cont	Alrts/Alrms	CPU	Endpoints	Destinatio	WAWAYAHQ	Avaya CM PBX		Yes	8 (Max) 5 (Min)	7	16 of 81	0 of 0	WSYSB-PBX	Avaya CM PBX		Yes	0 (Max) 7 (Min)	9	0 of 0	0 of 0
Name	Vendor	Customer - Site	Cont	Alrts/Alrms	CPU	Endpoints	Destinatio																		
WAWAYAHQ	Avaya CM PBX		Yes	8 (Max) 5 (Min)	7	16 of 81	0 of 0																		
WSYSB-PBX	Avaya CM PBX		Yes	0 (Max) 7 (Min)	9	0 of 0	0 of 0																		

Step	Description
2.	In the Avaya Systems page, verify that the SAT field for each configured Communication Manager shows 3 connections.

The screenshot shows the PROGNOSIS Avaya Systems interface. The main window displays a table titled 'Avaya Systems' with the following data:

Entire Network	by PBX	by LSP	by Customer	by Site	Voice	Network			
PBX	Customer	Site	SAT	Major	Minor	CPU	Phones	Trunk Grps	Chat
WVAYAHQ			3	8	5	2	16 of 81		Config
WYSB-PBX			3	0	7	2	31 of 166	3 of 7	Config

The SAT values (3) for both PBX entries are highlighted with a red box. Below the table is a 'Voice Streams' graph showing a flat line at 0.0 on the y-axis (ranging from 0 to 1) across the x-axis (ranging from 17:23:40 to 17:27:40). The status bar at the bottom indicates 'Entire Network AVCLQSLW(s): 1' and 'Thu Apr 21st 2011 17:28:30'.

Step	Description
3.	<p>Make a call between two Avaya IP telephones that belong to an IP Network Region that has been configured to send RTCP information to the PROGNOSIS server. Verify that the Voice Streams section shows two active voice streams reflecting the quality of the call.</p>  <p>The screenshot displays the PROGNOSIS application window. On the left, there is a tree view for 'My Displays & Configurations' and 'IPTM' (IP Telephony Manager) configurations. The main area shows 'Avaya Systems' monitoring data. A table lists PBX systems with columns for Customer, Site, SAT, Major, Minor, CPU, Phones, Trunk Grps, and Char. Below the table is a 'Voice Streams' graph showing a purple bar representing active streams for 'ISYSB-PBX' between 17:38:00 and 17:39:00. The status bar at the bottom indicates 'Entire Network: AVCLQSLW(s): 3' and the date 'Thu Apr 21st 2011 17:39:50'.</p>

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research PROGNOSIS IP Telephony Manager to interoperate with Avaya Aura® Communication Manager. In the configuration described in these Application Notes, PROGNOSIS IP Telephony Manager established SSH connections to the SAT to view the configurations of Communication Manager and to monitor for failures. PROGNOSIS IP Telephony Manager also processed the RTCP information to monitor the quality of IP calls and collected CDR information from the Communication Manager. During compliance testing, all test cases were completed successfully.

9. Additional References

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Release 6.0, Issue 8.0, June 2010, Document Number 555-245-205.

[2] *Administering Avaya Aura™ Communication Manager*, June 2010, Release 6.0, Issue 6.0, Document Number 03-300509.

The following PROGNOSIS documents are provided by Integrated Research.

[3] *PROGNOSIS IP Telephony Manager 9.6 Installation and Configuration Guide*, September 2010.

[4] *PROGNOSIS IP Telephony Manager 9.6 User Guide Online Help*.

©2011 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.

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>