



Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis IP Telephony Manager 9.6.1 with Avaya Aura® Communication Manager 6.2 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis IP Telephony Manager 9.6.1 to interoperate with Avaya Aura® Communication Manager 6.2.

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) or Telnet. 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 telnet/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.
- 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.

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

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 H323, SIP, digital and analog telephones, and Avaya One-X® Communicator users. The types of calls made included intra-switch calls, inbound/outbound inter-switch IP trunk calls, transfer 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, 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 2008 R2 with Service Pack 1. 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.

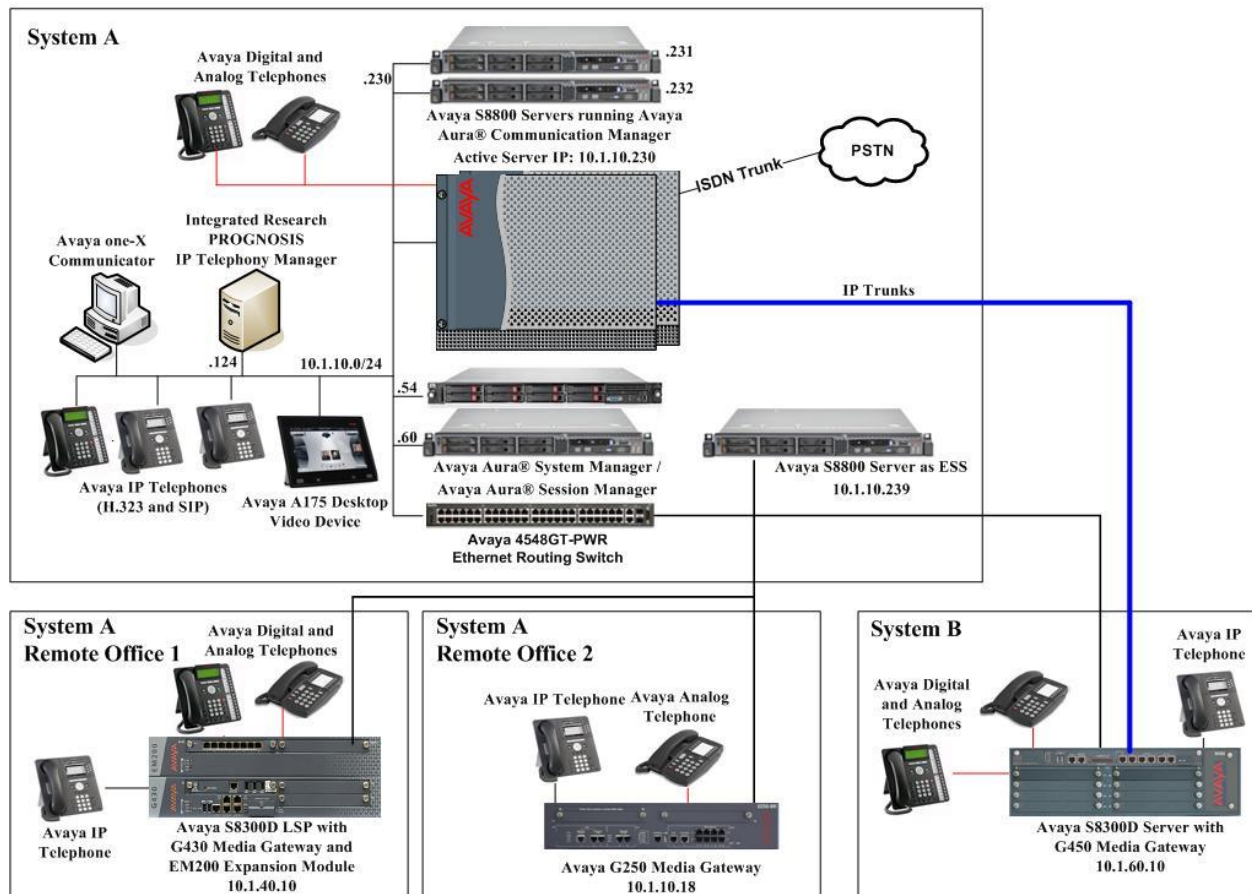


Figure 1: Test Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Avaya S8800 Servers (System A)	6.2 SP2.01
G650 Media Gateway - TN2312BP IP Server Interface (x 2) - TN799DP C-LAN Interface (x 4) - TN2602AP IP Media Processor (x 2) - TN2302AP IP Media Processor (x 2) - TN2464BP DS1 Interface - TN2464CP DS1 Interface - TN793CP Analog Line - TN2214CP Digital Line	HW07, FW054 and HW15, FW054 HW01, FW040 HW02, FW059 HW20, FW121 HW05, FW024 HW02, FW024 HW09, FW011 HW08, FW015
G250 Media Gateway	30.18.1
Avaya Aura® Communication Manager running on Avaya S8300D Server (G450 Media Gateway – System B)	6.2 SP2.01
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	31.22.0 HW01, FW008 HW07, FW011 HW10, FW095 HW03, FW011 HW11, FW049
Avaya Aura® Communication Manager running on Avaya S8300D Server (G430 Media Gateway - LSP)	6.2 SP2.01
G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	31.22.0 HW04, FW011 HW04, FW073 HW31, FW095 HW05, FW021
Avaya Aura® Communication Manager running on Avaya S8800 Server (ESS)	6.2 SP2.01
HP DL360 G7 running Avaya Aura® System Manager	6.2 SP2
Avaya S8800 Server running Avaya Aura® Session Manager	6.2 SP2

Equipment/Software	Release/Version
96xx Series IP Telephones - 9640 - 9620	3.1 SP3 (H323) or 2.6 SP8 (SIP)
96x1 Series IP Telephones - 9641G - 9611G	6.2 SP2 (H.323) or 6.0 SP3 (SIP)
1600 Series IP Telephones - 1616 - 1603SW	1.32 (H.323)
Avaya A175 Desktop Video Device	1.10 (SIP)
Digital Telephones - 1416 - 1408	SP1
Avaya Analog Phones	-
Desktop PC with Avaya one-X Communicator	6.1 SP5 (H.323)
Avaya 4548GT-PWR Ethernet Routing Switch	V5.6.1.052
IP Telephony Manager on Windows 2008 R2 SP1	9.6.1 Update 3

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.

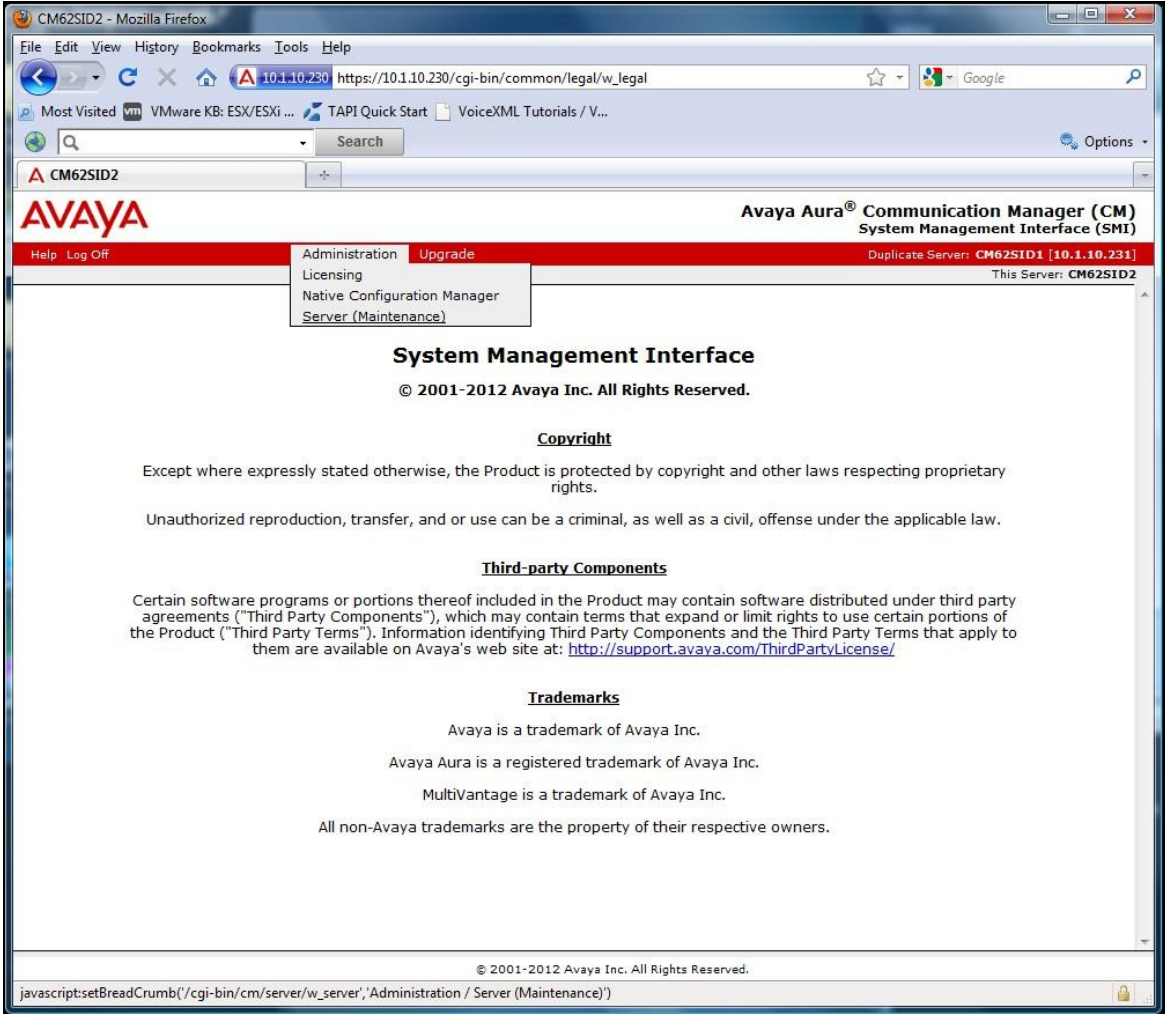
Step	Description
1.	<p>Enter the add user-profile <i>n</i> command, where <i>n</i> is the next unused profile number. Enter a descriptive name for User Profile Name and enable all categories by setting the Enbl field to y. In this test configuration, the user profile 21 is created.</p> <pre>add user-profile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

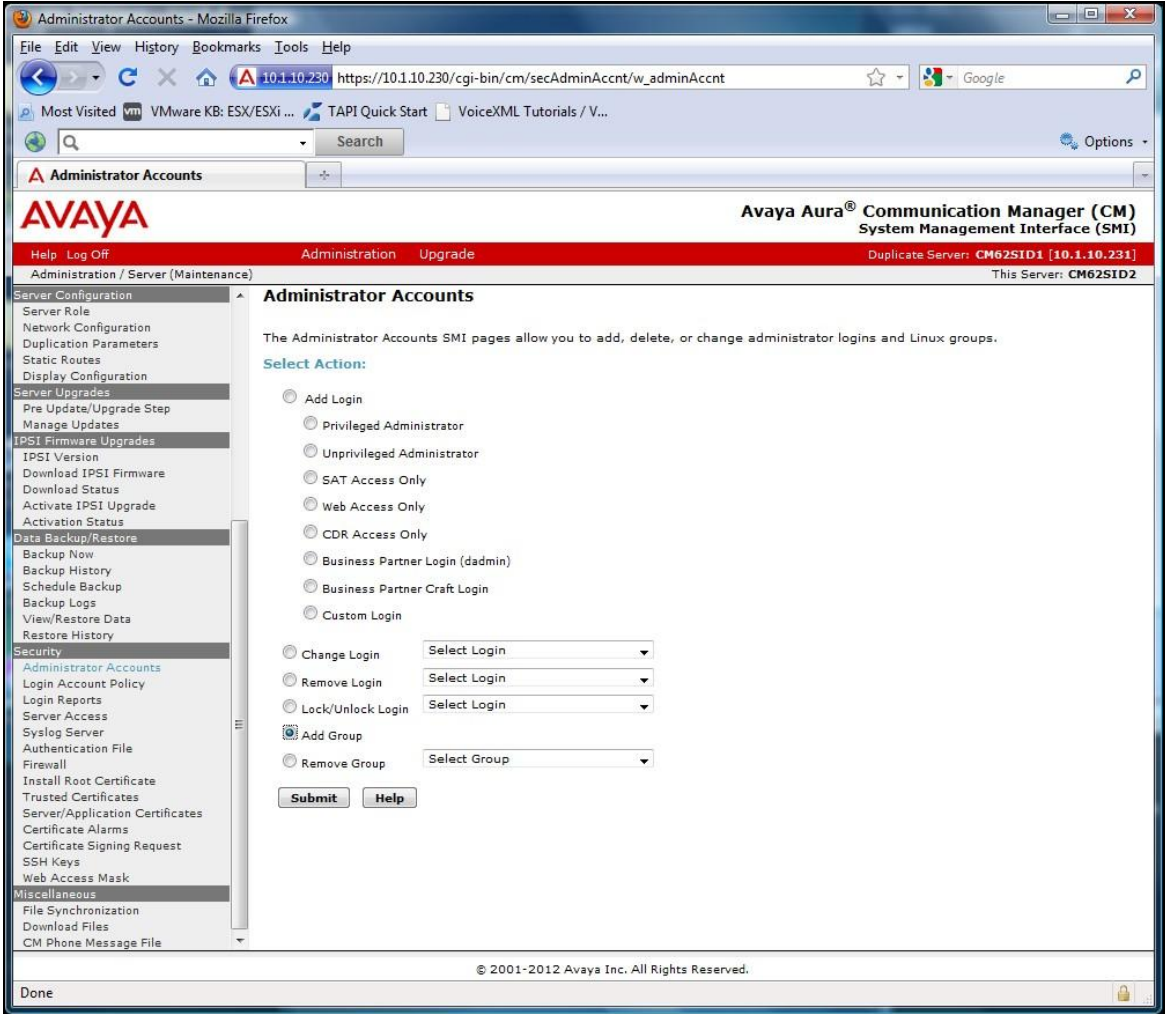
Step	Description																																													
2.	<p>On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to rm (read and maintenance). This can be accomplished by typing rm into the field Set All Permissions To. Submit the form to create the user profile.</p>																																													
	<div><div>add user-profile 21</div><div>Page 2 of 41</div></div> <div>USER PROFILE 21</div> <div>Set Permissions For Category: To: Set All Permissions To: <div>rm</div></div> <div>'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance</div> <table><tr><th>Name</th><th>Cat</th><th>Perm</th></tr><tr><td>aar analysis</td><td>J</td><td><div>rm</div></td></tr><tr><td>aar digit-conversion</td><td>J</td><td><div>rm</div></td></tr><tr><td>aar route-chosen</td><td>J</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing 7103-buttons</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing enhanced</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing group</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing personal</td><td>C</td><td><div>rm</div></td></tr><tr><td>abbreviated-dialing system</td><td>C</td><td><div>rm</div></td></tr><tr><td>aca-parameters</td><td>P</td><td><div>rm</div></td></tr><tr><td>access-endpoints</td><td>P</td><td><div>rm</div></td></tr><tr><td>adjunct-names</td><td>A</td><td><div>rm</div></td></tr><tr><td>administered-connections</td><td>C</td><td><div>rm</div></td></tr><tr><td>aesvcs cti-link</td><td>A</td><td><div>rm</div></td></tr><tr><td>aesvcs interface</td><td>A</td><td><div>rm</div></td></tr></table>	Name	Cat	Perm	aar analysis	J	<div>rm</div>	aar digit-conversion	J	<div>rm</div>	aar route-chosen	J	<div>rm</div>	abbreviated-dialing 7103-buttons	C	<div>rm</div>	abbreviated-dialing enhanced	C	<div>rm</div>	abbreviated-dialing group	C	<div>rm</div>	abbreviated-dialing personal	C	<div>rm</div>	abbreviated-dialing system	C	<div>rm</div>	aca-parameters	P	<div>rm</div>	access-endpoints	P	<div>rm</div>	adjunct-names	A	<div>rm</div>	administered-connections	C	<div>rm</div>	aesvcs cti-link	A	<div>rm</div>	aesvcs interface	A	<div>rm</div>
Name	Cat	Perm																																												
aar analysis	J	<div>rm</div>																																												
aar digit-conversion	J	<div>rm</div>																																												
aar route-chosen	J	<div>rm</div>																																												
abbreviated-dialing 7103-buttons	C	<div>rm</div>																																												
abbreviated-dialing enhanced	C	<div>rm</div>																																												
abbreviated-dialing group	C	<div>rm</div>																																												
abbreviated-dialing personal	C	<div>rm</div>																																												
abbreviated-dialing system	C	<div>rm</div>																																												
aca-parameters	P	<div>rm</div>																																												
access-endpoints	P	<div>rm</div>																																												
adjunct-names	A	<div>rm</div>																																												
administered-connections	C	<div>rm</div>																																												
aesvcs cti-link	A	<div>rm</div>																																												
aesvcs interface	A	<div>rm</div>																																												

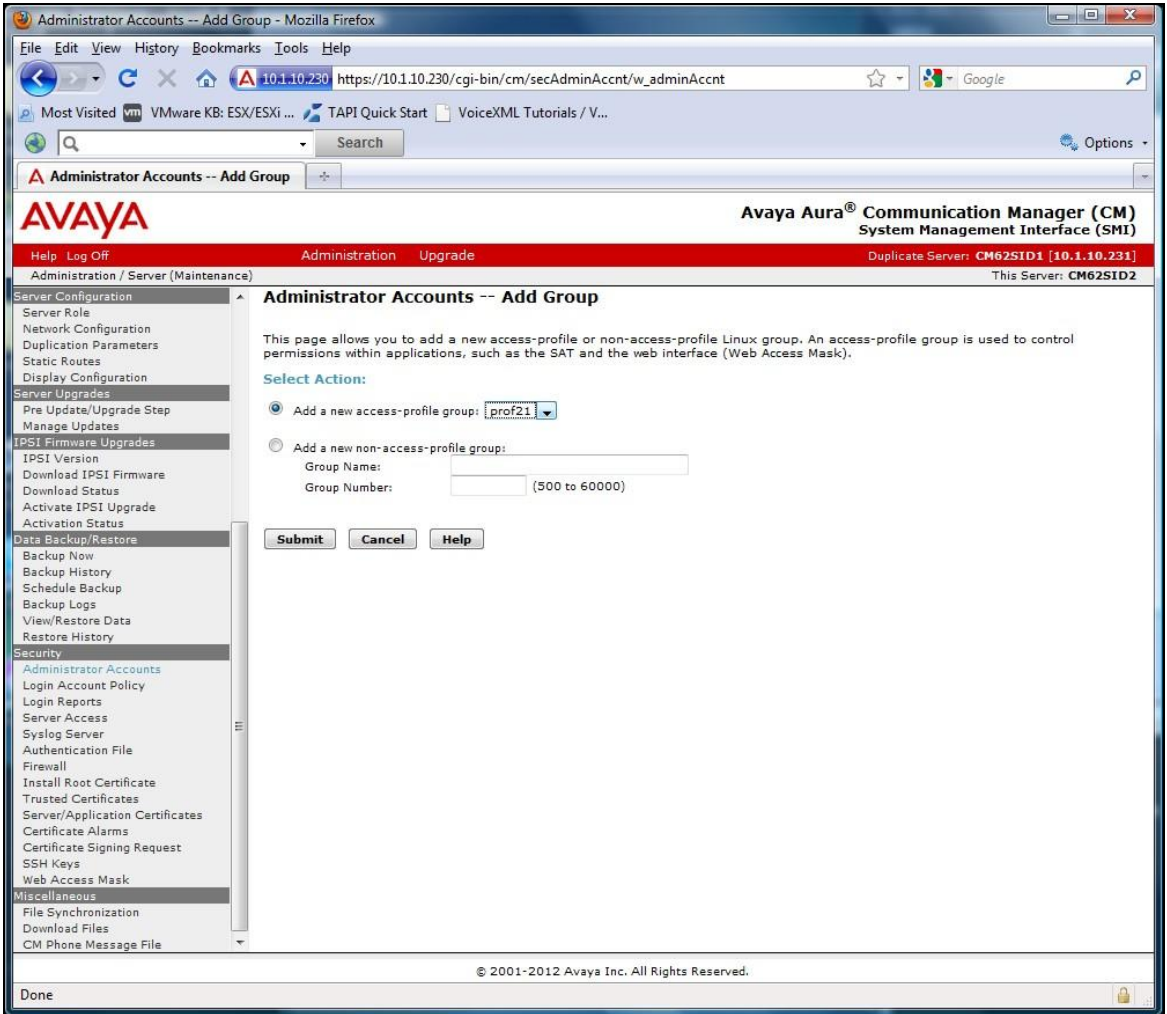
5.2. Configure Login Group

Create an Access-Profile Group on Communication Manager SMI 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 Communication Manager> to connect to the Communication Manager Server being configured and log in using appropriate credentials.</p> 

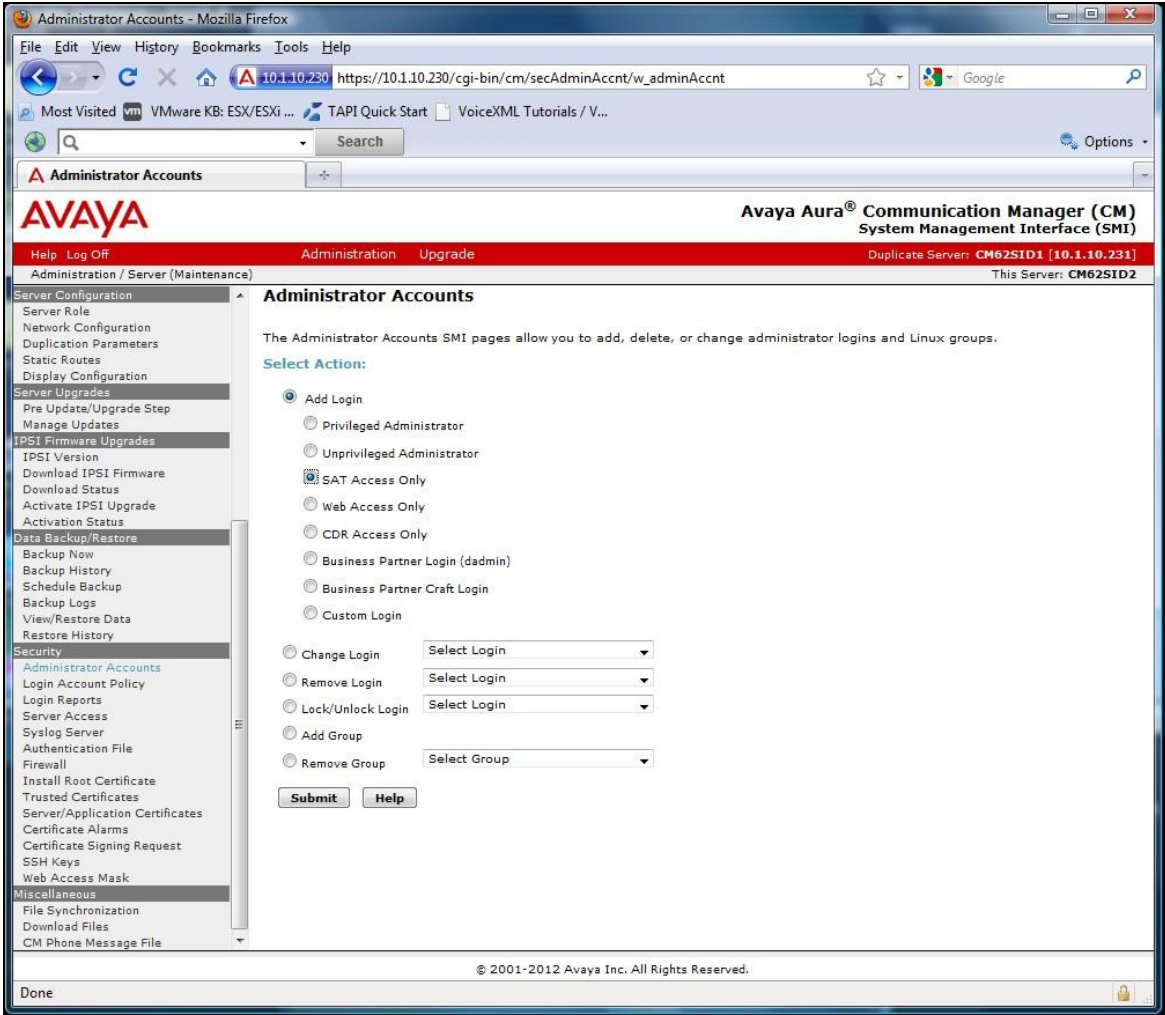
Step	Description
2.	<p>Click Administration → Server (Maintenance). This will open up the Server Administration Interface that will allow the user to complete the configuration process.</p>  <p>The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) in a Mozilla Firefox browser. The browser address bar displays the URL <code>https://10.1.10.230/cgi-bin/common/legal/w_legal</code>. The page title is "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)". The navigation menu includes "Administration", "Upgrade", "Licensing", "Native Configuration Manager", and "Server (Maintenance)". The main content area displays the "System Management Interface" with the following text:</p> <p>© 2001-2012 Avaya Inc. All Rights Reserved.</p> <p>Copyright</p> <p>Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.</p> <p>Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.</p> <p>Third-party Components</p> <p>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/</p> <p>Trademarks</p> <p>Avaya is a trademark of Avaya Inc.</p> <p>Avaya Aura is a registered trademark of Avaya Inc.</p> <p>MultiVantage is a trademark of Avaya Inc.</p> <p>All non-Avaya trademarks are the property of their respective owners.</p> <p>© 2001-2012 Avaya Inc. All Rights Reserved.</p> <p>The browser status bar at the bottom shows the JavaScript code: <code>javascript:setBreadCrumb('/cgi-bin/cm/server/w_server','Administration / Server (Maintenance)')</code></p>

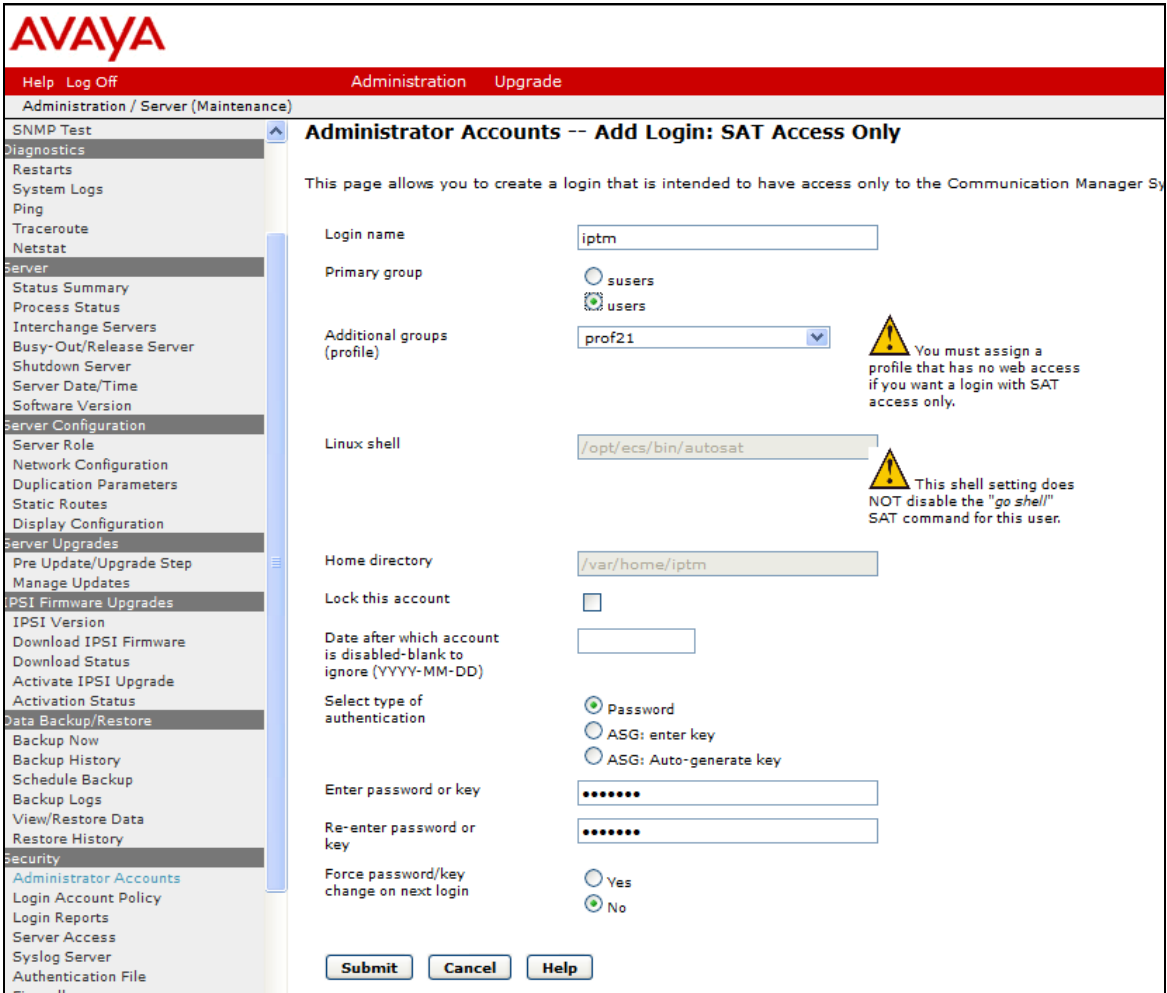
Step	Description
3.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Group and click Submit.</p> 

Step	Description
4.	<p>Select Add a new access-profile group and select 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 the login. 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: users [Limits the permissions of the login] • Additional groups (profile): prof21 [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 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 4 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 Primary Search Time (sec): 75 Periodic Registration Timer (min): 20 Short/Prefixed Registration Allowed? y </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: 1700 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 ESS 10.1.10.239 Gateway001 10.1.10.1 IPOffice 10.1.30.10 PC2 10.1.10.152 aes1 10.1.10.71 cms1 10.1.10.85 default 0.0.0.0 iptm 10.1.10.124 lsp-g430 10.1.40.10 msgserver 10.1.10.10 n 10.3.10.253 procr 10.1.10.230 procr6 :: s8300-siteB 10.1.20.10 (16 of 26 administered node-names were displayed) Use 'list node-names' command to see all the administered node-names Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name </pre>

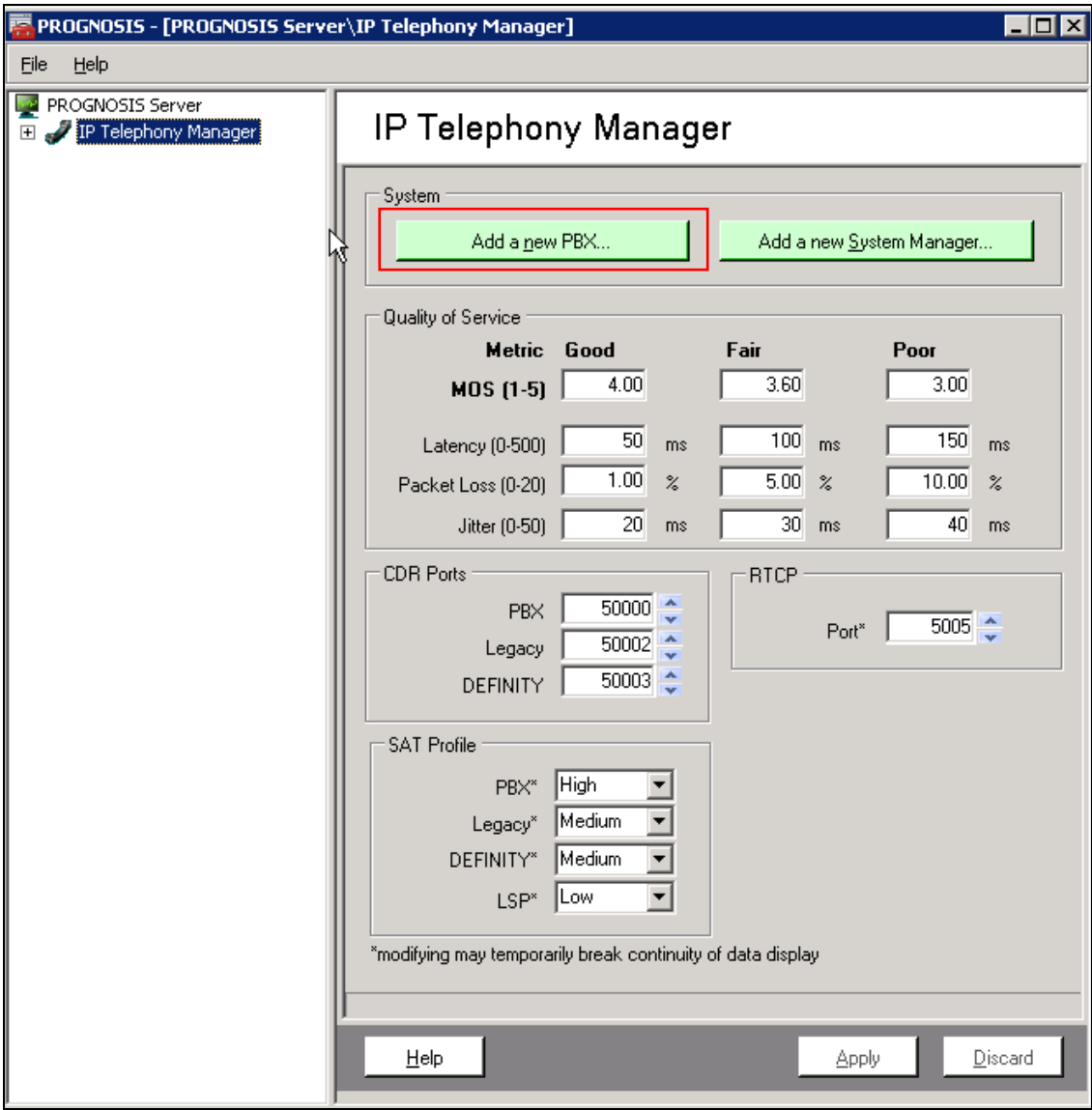
Step	Description																								
3.	<p>Enter the change ip-services command to define the CDR link. To define a primary CDR link, the following information should be provided:</p> <ul style="list-style-type: none">• Service Type: CDR1 [If needed, a secondary link can be defined by setting Service Type to CDR2.]• Local Node: procr [Communication Manager will use the processor-ethernet interface to send out the CDR]• Local Port: 0 [The Local Port is set to 0 because Communication Manager initiates the CDR link.]• Remote Node: iptm [The Remote Node is set to the node name previously defined in Step 2]• Remote Port: 50000 [The Remote Port may be set to a value between 5000 and 64500 inclusive. 50000 is the default port number used by Prognosis. Note that Prognosis server uses the same port number for all Avaya Servers sending CDR information to it.]																								
<div>change ip-services<div>Page1 of 4</div></div> <table><tr><th colspan="6">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></tr><tr><td>AESVCS</td><td>y</td><td>procr</td><td>8765</td><td></td><td></td></tr><tr><td>CDR1</td><td></td><td>procr</td><td>0</td><td>iptm</td><td>50000</td></tr></table>		IP SERVICES						Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port	AESVCS	y	procr	8765			CDR1		procr	0	iptm	50000
IP SERVICES																									
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote Port																				
AESVCS	y	procr	8765																						
CDR1		procr	0	iptm	50000																				
<p>On Page 3 of the form, disable the Reliable Session Protocol (RSP) for the CDR link by setting the Reliable Protocol field to n.</p>																									
<div>change ip-services<div>Page3 of 4</div></div> <table><tr><th colspan="6">SESSION LAYER TIMERS</th></tr><tr><th>Service Type</th><th>Reliable Protocol</th><th>Packet Resp Timer</th><th>Session Connect Message Cntr</th><th>SPDU Cntr</th><th>Connectivity Timer</th></tr><tr><td>CDR1</td><td>n</td><td>30</td><td>3</td><td>3</td><td>60</td></tr></table>		SESSION LAYER TIMERS						Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message Cntr	SPDU Cntr	Connectivity Timer	CDR1	n	30	3	3	60						
SESSION LAYER TIMERS																									
Service Type	Reliable Protocol	Packet Resp Timer	Session Connect Message 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 [This value is used to configure Prognosis in Section 6 Step 2 and 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 [Specify the use of the Communication Manager 3.x ("legacy") formats in the CDR records produced by the system.] • 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? n [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: 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? 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 SYSTEM-PARAMETERS CDR 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: 14 of 5000 administered Extension Extension Extension Extension 10001 10003 10004 10013 10016 10024 10049 10050 10099 10701 20000 481121 481122 481123 </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 7 Page 1 of 21 TRUNK GROUP Group Number: 7 Group Type: sip CDR Reports: y Group Name: SIP Trunk to SM1 COR: 1 TN: 1 TAC: #07 Direction: two-way Outgoing Display? n Dial Access? n Night Service: Queue Length: 0 Service Type: tie Auth Code? n Member Assignment Method: auto Signaling Group: 7 Number of Members: 14 </pre>

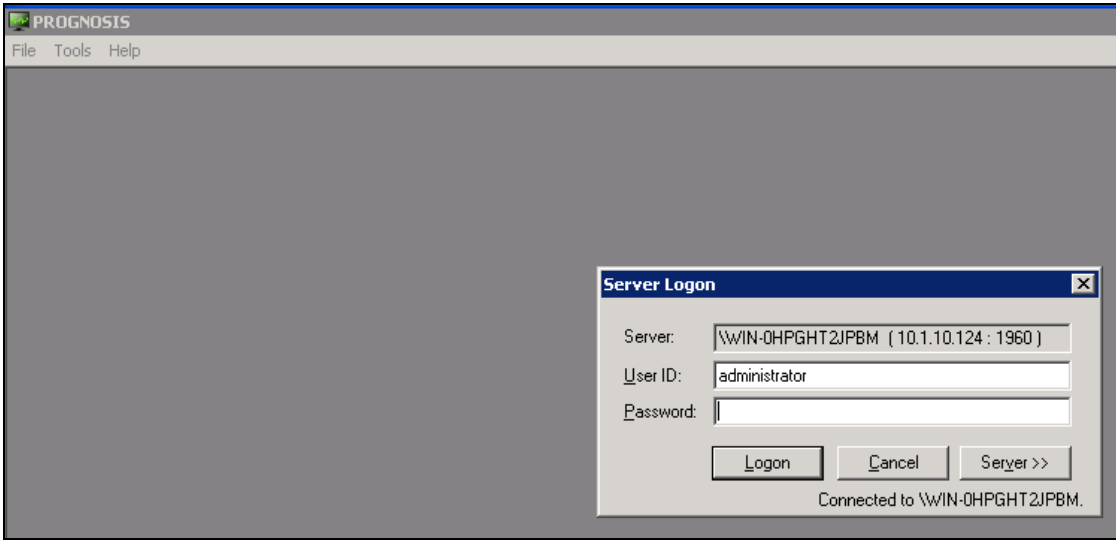
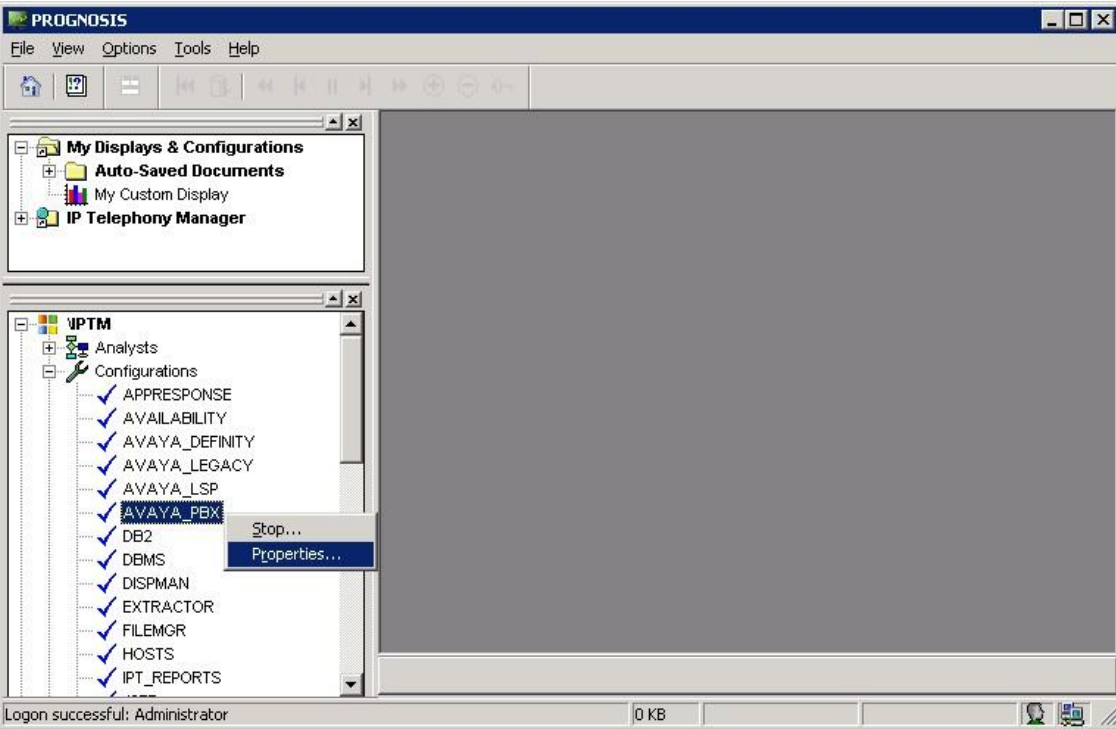
6. Configure Integrated Research Prognosis IP Telephony Manager

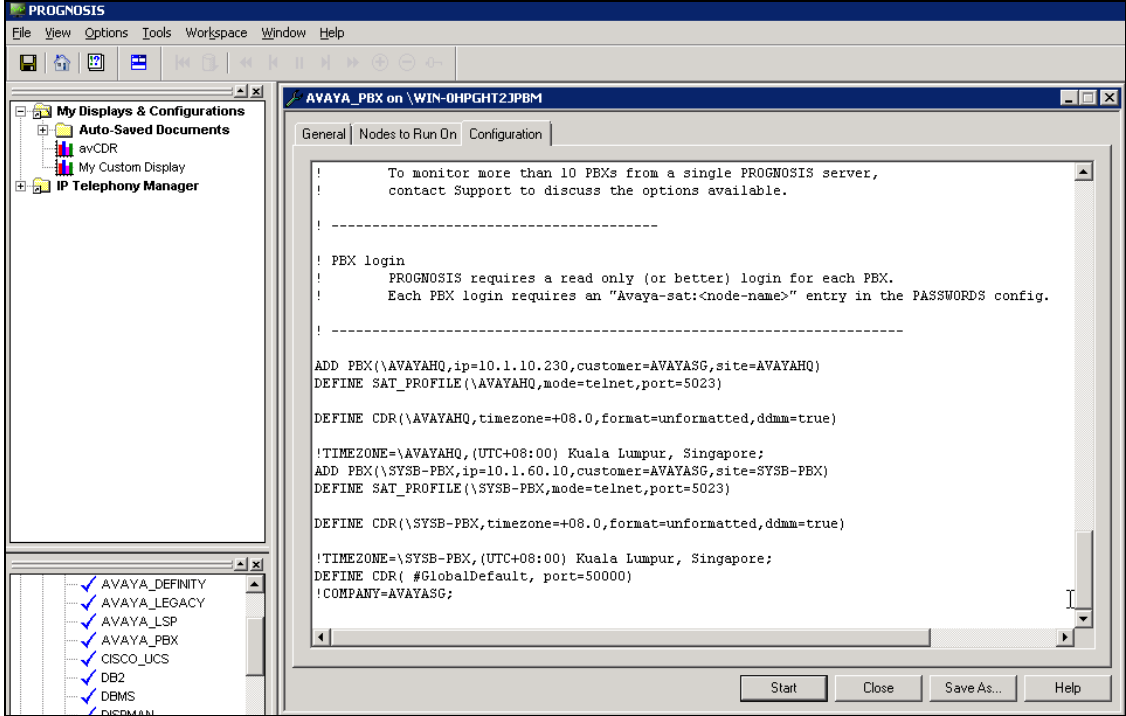
This section describes the configuration of Prognosis IP Telephony Manager required to interoperate with Communication Manager.

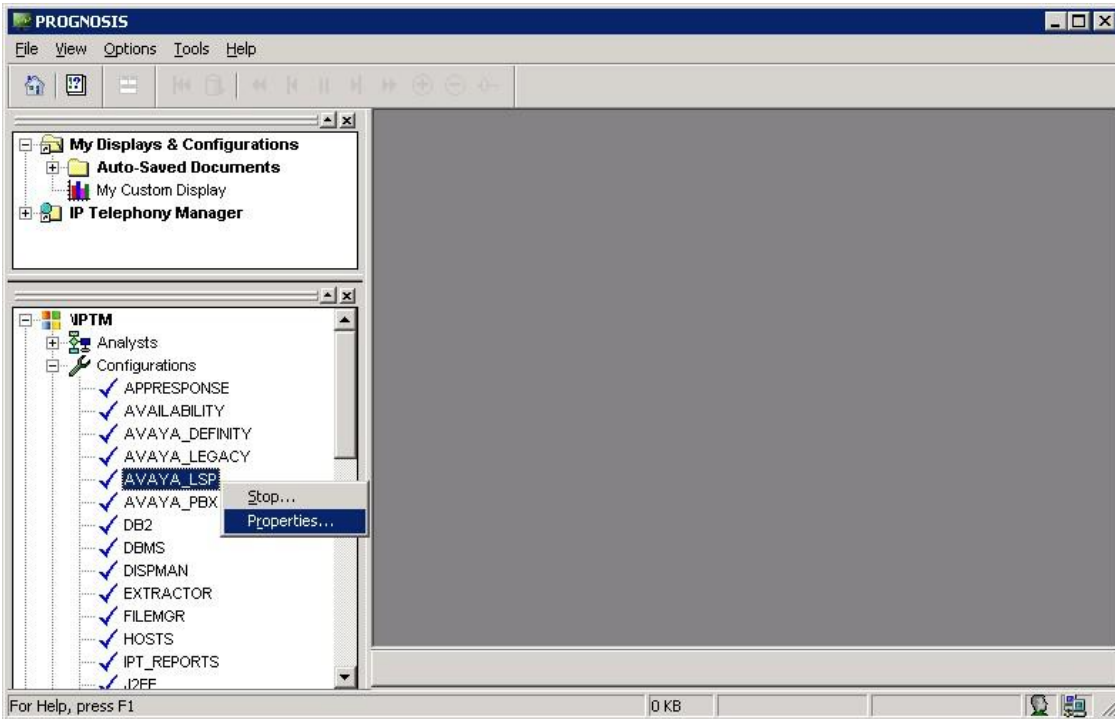
Step	Description
1.	<p>Log into the IP Telephony Manager Server with administrative privileges and configure the Communication Manager systems to be monitored, click Start → All Programs → Prognosis IP Telephony Manager → Configure Avaya Aura. Click Add a new PBX...</p> 

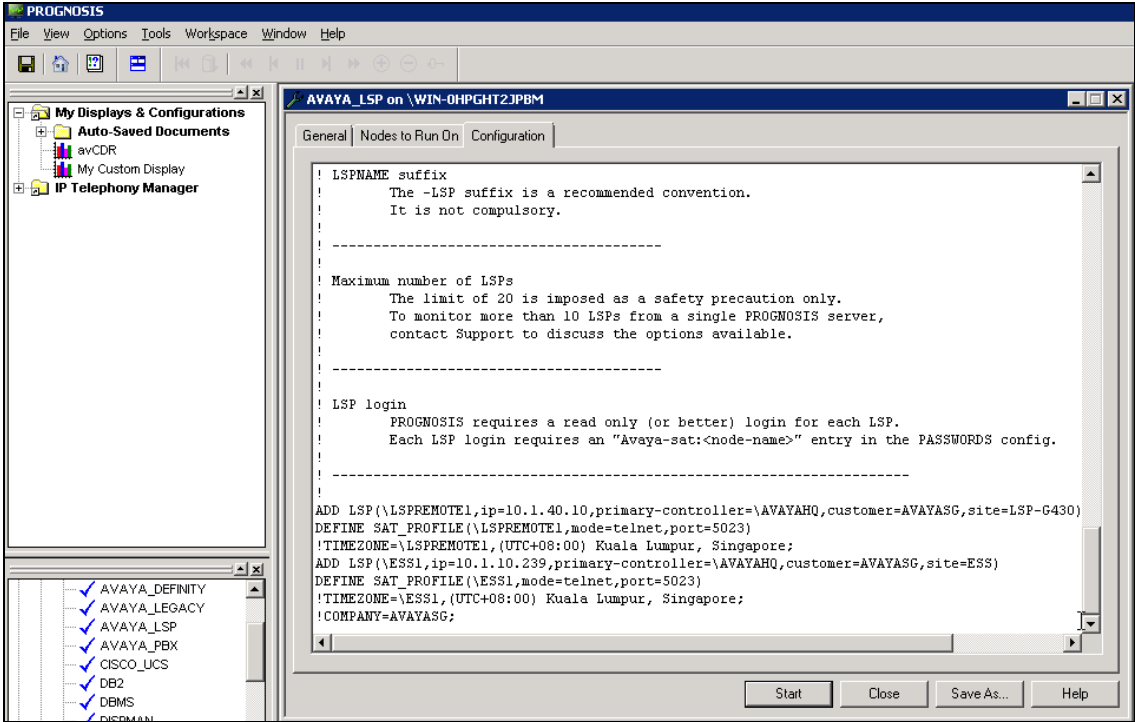
Step	Description
2.	<p>In this test configuration, the following entries are added for the two Communication Manager systems with the names AVAYAHQ and SYSB-PBX and with the IP addresses of the Avaya Servers 10.1.10.230 and 10.1.60.10 respectively.</p> <p>On the right pane, the following settings were used during the compliance test.</p> <ul style="list-style-type: none"> • Name: AVAYAHQ • Site: AVAYAHQ • IP address: 10.1.10.230 • User/Password: iptm [As configured in Section 5.3 Step 2] • Mode: telnet, 5023 [For secure connection, select ssh with port 5022] • Format: unformatted, dd-mm [as configured in Section 5.5 Step 4] <p>Click Apply to effect the addition. Repeat the above for the setup of SYSB-PBX.</p> <div data-bbox="527 751 1214 1675"> </div>

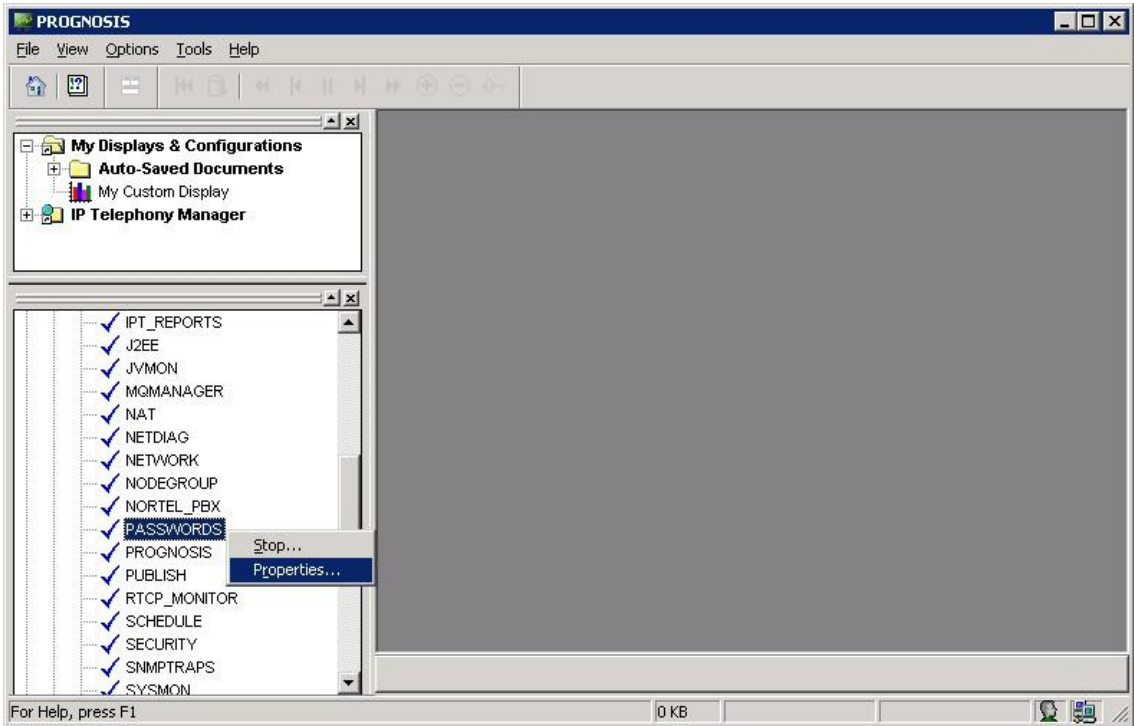
Step	Description
3.	<p>In this test configuration, the and Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS) Servers with the names LSPREMOTE1 and ESS1 and with the IP addresses of 10.1.40.10 and 10.1.10.239 respectively, both belonging to the AVAYAHQ Communication Manager system are also configured.</p> <p>Repeat Step 1 to add a new PBX. The following settings were used during the compliance test.</p> <ul style="list-style-type: none"> • Name: LSPREMOTE1 • Site: LSP-G430 • Controller PBX: AVAYAHQ • IP address: 10.1.40.10 • User/Password: iptm [As configured in Section 5.3 Step 2] • Mode: telnet, 5023 [For secure connection, select ssh with port 5022] • Format: unformatted, dd-mm [as configured in Section 5.5 Step 4] <p>Click Apply to effect the addition. Repeat the above for the setup of ESS1.</p> <div data-bbox="506 861 1219 1839"> <p>The screenshot shows the 'Avaya PBX' configuration dialog box. It has a title bar 'Avaya PBX'. Inside, there's a 'PBX' section with 'Name' set to 'LSPREMOTE1', 'Site' set to 'LSP-G430', and 'Controller PBX' set to 'AVAYAHQ'. Below that is a 'SAT Connectivity' section with 'IP address' set to '10.1.40.10', 'User' set to 'iptm', 'Password' masked with 'XXXXXXXX', 'Mode' set to 'telnet', and 'Port' set to '5023'. There's also an 'SNMP Community' field. Below that is a 'CDRs (optional)' section with 'Format' set to 'unformatted' and 'Time zone' set to a dropdown menu. At the bottom left is a 'Cancel Add' button. At the bottom right are 'Help', 'Apply', and 'Discard' buttons. A note at the bottom says 'The mode of SAT communication (default = ssh)'.</p> </div>

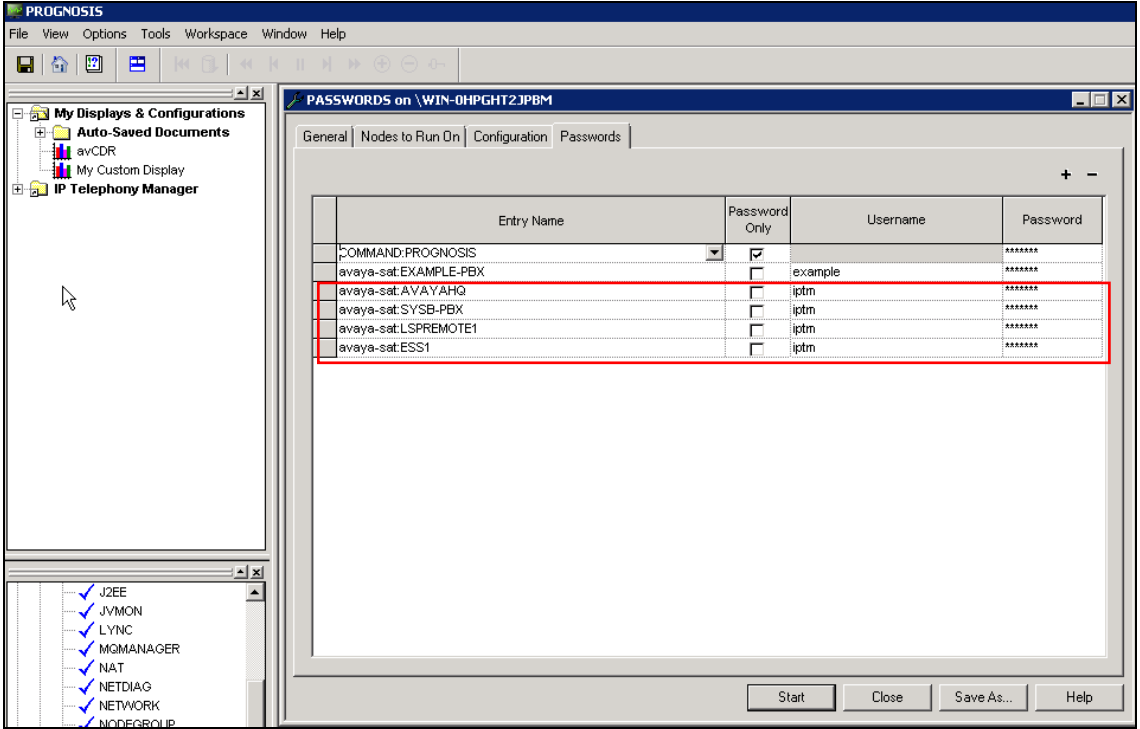
Step	Description
4.	<p>On Prognosis IP Telephony Manager server, click Start → All Programs → Prognosis IP Telephony Manager → IP Telephony Manager GUI to start the IP Telephony Manager GUI application. Enter a valid Windows user account and password to log in.</p> 
5.	<p>Expand Configurations of the Monitoring Node, right-click on AVAYA_PBX and select Properties.</p> 

Step	Description
6.	<p>Check the configurations for each of the Communication Manager and the corresponding CDR settings Step as configured in Step 2 earlier.</p> <pre> ADD PBX(\AVAYAHQ,ip=10.1.10.230,customer=AVAYASG,site=AVAYAHQ) DEFINE SAT_PROFILE(\AVAYAHQ,mode=telnet,port=5023) DEFINE CDR(\AVAYAHQ,timezone=+08.0,format=unformatted,ddmm=true) ADD PBX(\SYSB-PBX,ip=10.1.60.10,customer=AVAYASG,site=SYSB-PBX) DEFINE SAT_PROFILE(\SYSB-PBX,mode=telnet,port=5023) DEFINE CDR(\SYSB-PBX,timezone=+08.0,format=unformatted,ddmm=true) </pre> <p>Note that the default CDR port is 50,000 which correspond to the configurations set in Section 5.5 Step 3 is already created as default.</p> <pre> DEFINE CDR(#GlobalDefault, port=50000) </pre> 

Step	Description
7.	<p>To check the configurations of the ESS and LSP Servers to be monitored, expand Configurations of the Monitoring Node, right-click on AVAYA_LSP and select Properties.</p>  <p>The screenshot shows the PROGNOSIS application window. The left pane displays a tree structure under 'VPTM'. The 'Configurations' folder is expanded, showing a list of monitored services: APPRESPONSE, AVAILABILITY, AVAYA_DEFINITY, AVAYA_LEGACY, AVAYA_LSP, AVAYA_PBX, DB2, DBMS, DISPMAN, EXTRACTOR, FILEMGR, HOSTS, IPT_REPORTS, and I2FF. The 'AVAYA_LSP' item is selected, and a right-click context menu is open, showing 'Stop...' and 'Properties...' options. The 'Properties...' option is highlighted. The top pane shows 'My Displays & Configurations' with 'Auto-Saved Documents' and 'My Custom Display' listed. The bottom status bar indicates 'For Help, press F1' and '0 KB'.</p>

Step	Description
8.	<p>Check the configurations for each ESS and LSP Servers to be monitored as configured in Step 3 earlier.</p> <pre>ADD LSP(\LSPREMOTE1,ip=10.1.40.10,primary- controller=\AVAYAHQ,customer=AVAYASG,site=LSP-G430) DEFINE SAT_PROFILE(\LSPREMOTE1,mode=telnet,port=5023)</pre> <pre>ADD LSP(\ESS1,ip=10.1.10.239,primary- controller=\AVAYAHQ,customer=AVAYASG,site=ESS) DEFINE SAT_PROFILE(\ESS1,mode=telnet,port=5023)</pre> 

Step	Description
9.	<p>To check the SAT login account and password configured on Section 6 Step 2 and Step 3, expand Configurations of the Monitoring Node, right-click on PASSWORDS and select Properties.</p> 

Step	Description
10.	<p>The four entries for the AVAYAHQ, second system SYSB-PBX, LSP and ESS are listed on the right pane.</p> 

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
init	0	192.168.100.18		1
*init	0	10.1.10.151	stat logins	3
iptm	22	10.1.10.124		4
iptm	22	10.1.10.124		5
iptm	22	10.1.10.124		7

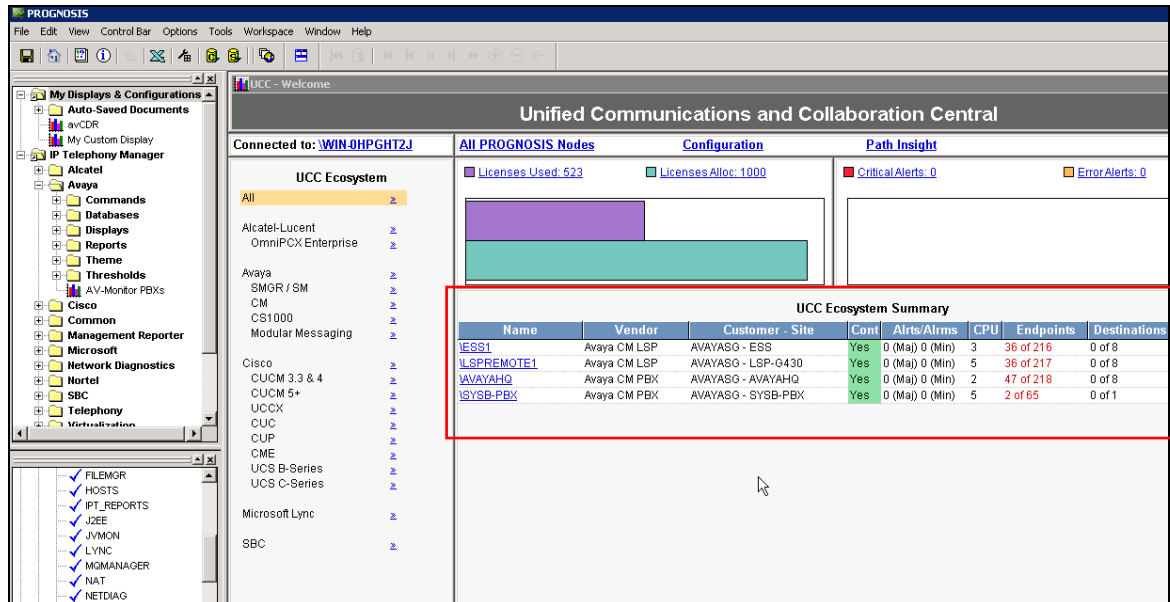
Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.5** shows **up**.

status cdr-link	
CDR LINK STATUS	
Primary	Secondary
Link State: up	CDR not administered
Date & Time: 2012/08/14 13:53:54	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

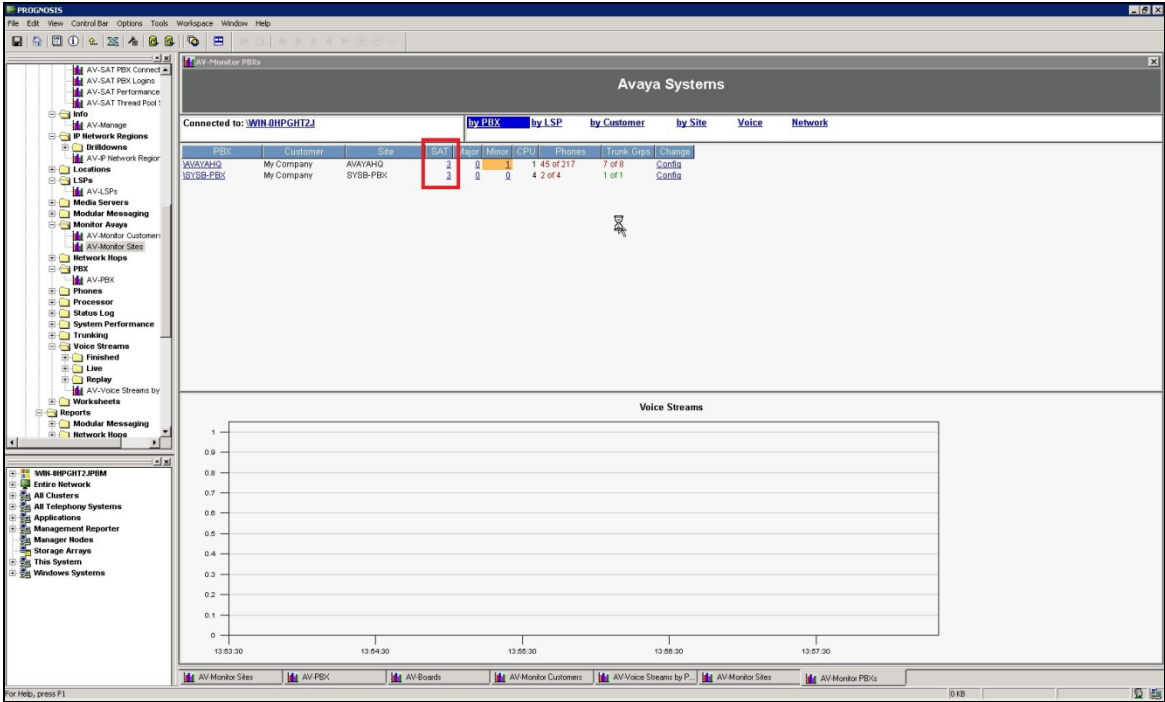
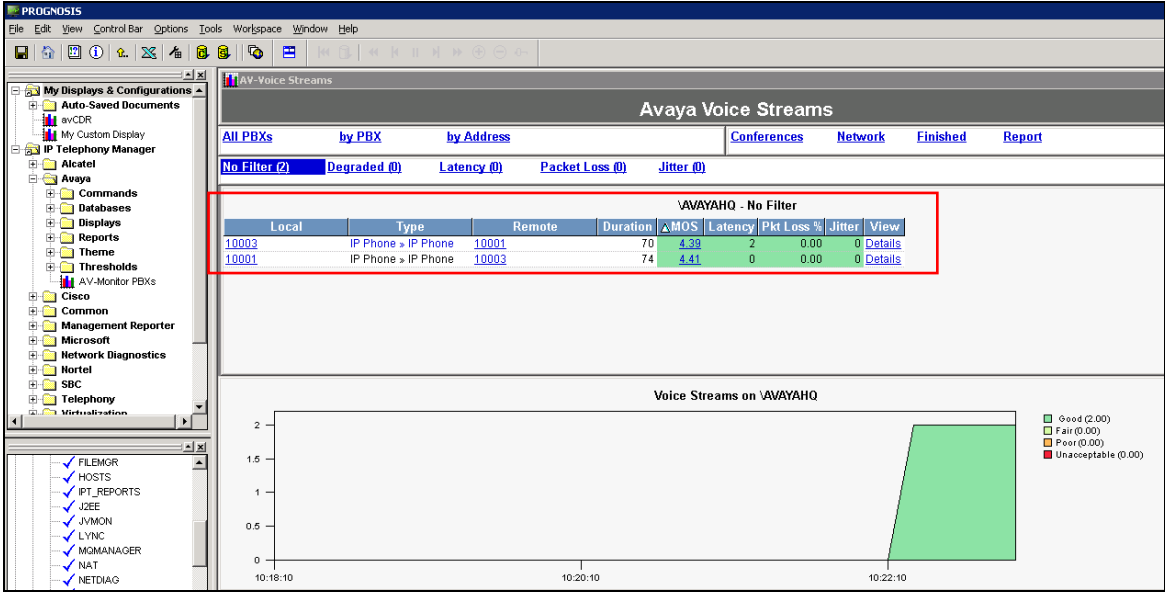
The following steps are done using the Prognosis GUI.

Step	Description
1.	After logging into Prognosis GUI, click on the Home button on the toolbar to display the Welcome screen. The list of Communication Manager Servers configured in Section 6 is displayed on the right pane.



The screenshot displays the PROGNOSIS UCC - Welcome interface. The left sidebar shows a tree view of 'My Displays & Configurations' with categories like Auto-Saved Documents, My Custom Display, IP Telephony Manager, Alcatel, Avaya, Cisco, and Microsoft. The main area is titled 'UCC - Welcome' and 'Unified Communications and Collaboration Central'. It shows 'Connected to: WINJHPGHTZJ' and 'All PROGNOSIS Nodes'. Below this is a 'UCC Ecosystem' section with a list of vendors and products. A red box highlights the 'UCC Ecosystem Summary' table, which contains the following data:

Name	Vendor	Customer - Site	Cont	Alerts/Alrms	CPU	Endpoints	Destinations
LESS1	Avaya CM LSP	AVAYASG - ESS	Yes	0 (Max) 0 (Min)	3	36 of 216	0 of 8
LSPREMOTE1	Avaya CM LSP	AVAYASG - LSP-G430	Yes	0 (Max) 0 (Min)	5	36 of 217	0 of 8
AVAYAHQ	Avaya CM PBX	AVAYASG - AVAYAHQ	Yes	0 (Max) 0 (Min)	2	47 of 218	0 of 8
SYSB-PBX	Avaya CM PBX	AVAYASG - SYSB-PBX	Yes	0 (Max) 0 (Min)	5	2 of 65	0 of 1

Step	Description
2.	<p>In the Avaya Systems page, verify that the SAT field for each configured Communication Manager shows 3 connections.</p> 
3.	<p>Make a call between two Avaya IP telephones that belong to an IP Network Region that is being 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> 

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 telnet 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

The following Avaya documentations can be obtained on the <http://support.avaya.com>.

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

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

The following Prognosis documentations are provided by Integrated Research in the package software for installation.

[3] *Prognosis IP Telephony Manager 9.6 Installation and Configuration Guide*, 3rd April 2012, IPTM 9.6.1 (Update 3).

[4] *Prognosis IP Telephony Manager 9.6.1 User Guide Online Help*.

©2012 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.