



Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research's Prognosis for Unified Communication 10 with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Prognosis for Unified Communication 10 (Prognosis) to interoperate with Avaya Aura® Communication Manager.

Prognosis provides real-time monitoring and management solutions for IP telephony networks. Prognosis provides visibility of Avaya and other vendor's IP Telephony solutions from a single console and enables a significant reduction in complexity when managing complex IP telephony environments.

Prognosis integrates directly to Communication Manager using Secure Shell (SSH) or Telnet and uses Simple Network Management Protocol (SNMP) to query Communication Manager. 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 Prognosis for Unified Communication 10 (herein after referred to as Prognosis) with Avaya Aura® Communication Manager.

The Prognosis product uses four methods to monitor a Communication Manager system.

- System Access Terminal (SAT) - The Prognosis 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 collects RTCP information sent by the Avaya IP Media Processor (MEDPRO) boards, media gateways, IP Telephones.
- Call Detail Recording (CDR) Collection - The Prognosis collects CDR information sent by Communication Manager.
- Simple Network Management Protocol (SNMP) – The Prognosis uses SNMP to collect configuration and status information from Communication Manager.

2. General Test Approach and Test Results

The general test approach was to use Prognosis web user interface (webui) 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 used in this testing. Note that other Communication Manager Servers are also supported. Calls were placed between various Avaya endpoints and Prognosis webui 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 webui 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. 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, outbound trunk calls, transfer and conference calls.

For serviceability testing, reboots were applied to the Prognosis Server and Avaya Servers to simulate system unavailability. Interchanging of the Avaya S8800 Servers and loss of network connections were also performed during testing.

2.2. Test Results

All test cases passed successfully.

2.3. Support

For technical support on Integrated Research Prognosis, 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 Prognosis interoperability with Communication Manager. It consists of a Communication Manager system (System A) 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 (System B) 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. Prognosis was installed on a server running Microsoft Windows Server 2008 R2 with Service Pack 1. Both the Monitoring Node and Web Application software are installed on this server. The Avaya 4548GT-PWR Ethernet Routing Switch provides Ethernet connectivity to the servers, media gateways and IP telephones.

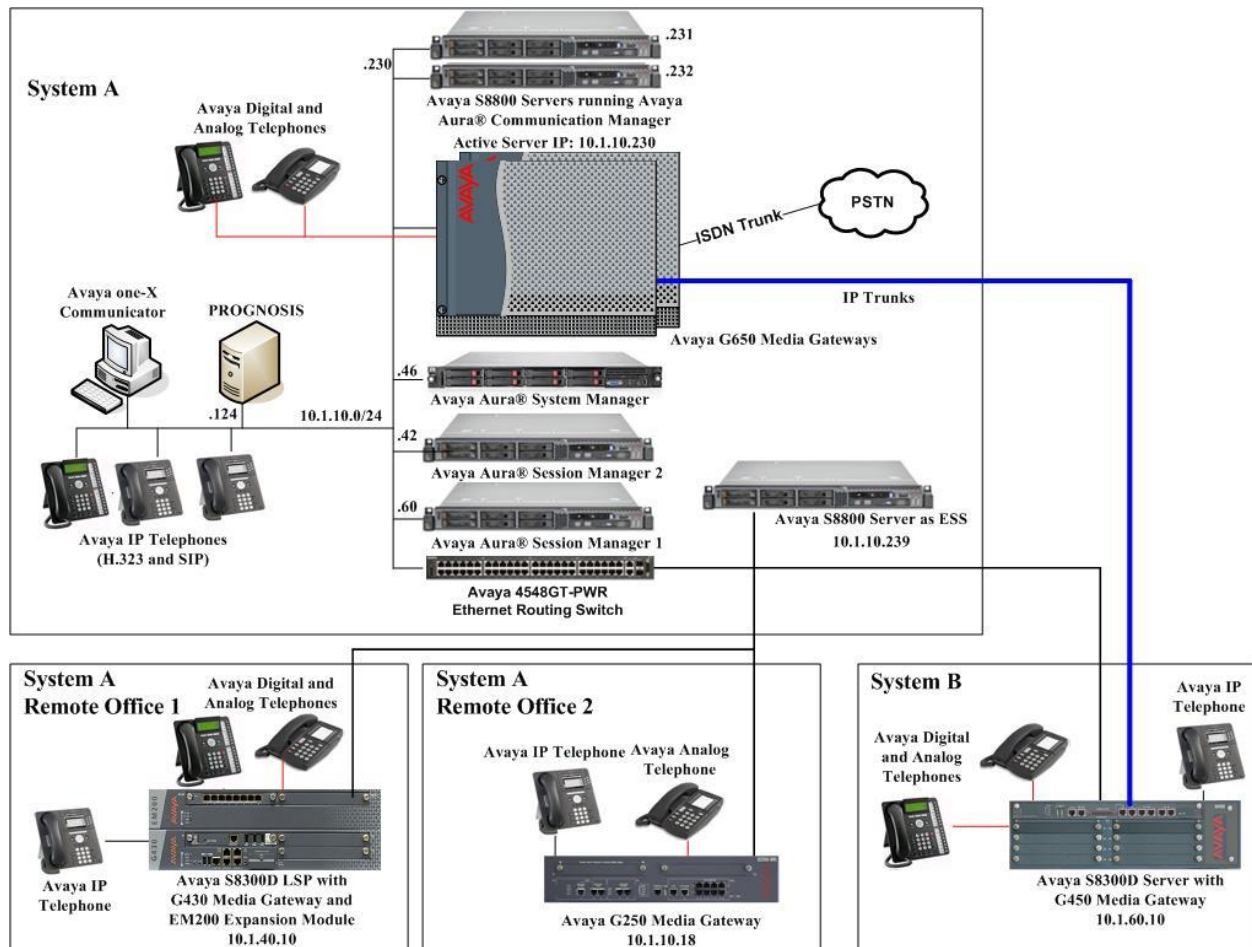


Figure 1: Test Configuration

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)	6.3 SP3
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, FW057 HW01, FW043 HW02 FW064 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW011 HW08, FW016
G250 Media Gateway	30.27.1
Avaya Aura® Communication Manager running on Avaya S8300D Server (G450 Media Gateway – System B)	6.3 SP3
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	34.5.1 HW01 FW008 HW07 FW015 HW10 FW098 HW03 FW015 HW11 FW052
Avaya Aura® Communication Manager running on Avaya S8300D Server (G430 Media Gateway - LSP)	6.3 SP3
G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	34.5.1 HW04 FW015 HW12 FW098 HW31 FW098 HW05 FW022
Avaya Aura® Communication Manager running on Avaya S8800 Server (ESS)	6.3 SP3
HP DL360 G7 running Avaya Aura® System Manager	6.3 SP5 Patch 1
Avaya S8800 Server running Avaya Aura® Session Manager 1	6.3 SP5
Avaya S8800 Server running Avaya Aura® Session Manager 2 on VMware 5.1	6.3 SP5
96xx Series IP Telephones - 9640 - 9620	2.6 SP11 (SIP) 3.2.1 (H323)

Equipment/Software	Release/Version
96x1 Series IP Telephones - 9641G - 9611G	6.3 (SIP) 6.3.1 (H323)
1600 Series IP Telephones - 1616 - 1603SW	1.34 (H.323)
Digital Telephones - 1416 - 1408	SP1
Avaya Analog Phones	-
Desktop PC with Avaya one-X Communicator	6.2 (H.323)
Avaya 4548GT-PWR Ethernet Routing Switch	V5.6.1.052
Prognosis on Windows 2008 R2 SP1	Windows 2008 R2 SP1

5. Configure Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with Prognosis. 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. Configuration of Session and System Manager can be referred from **Reference [4]** and will not be detailed here.

5.1. Configure SAT User Profile

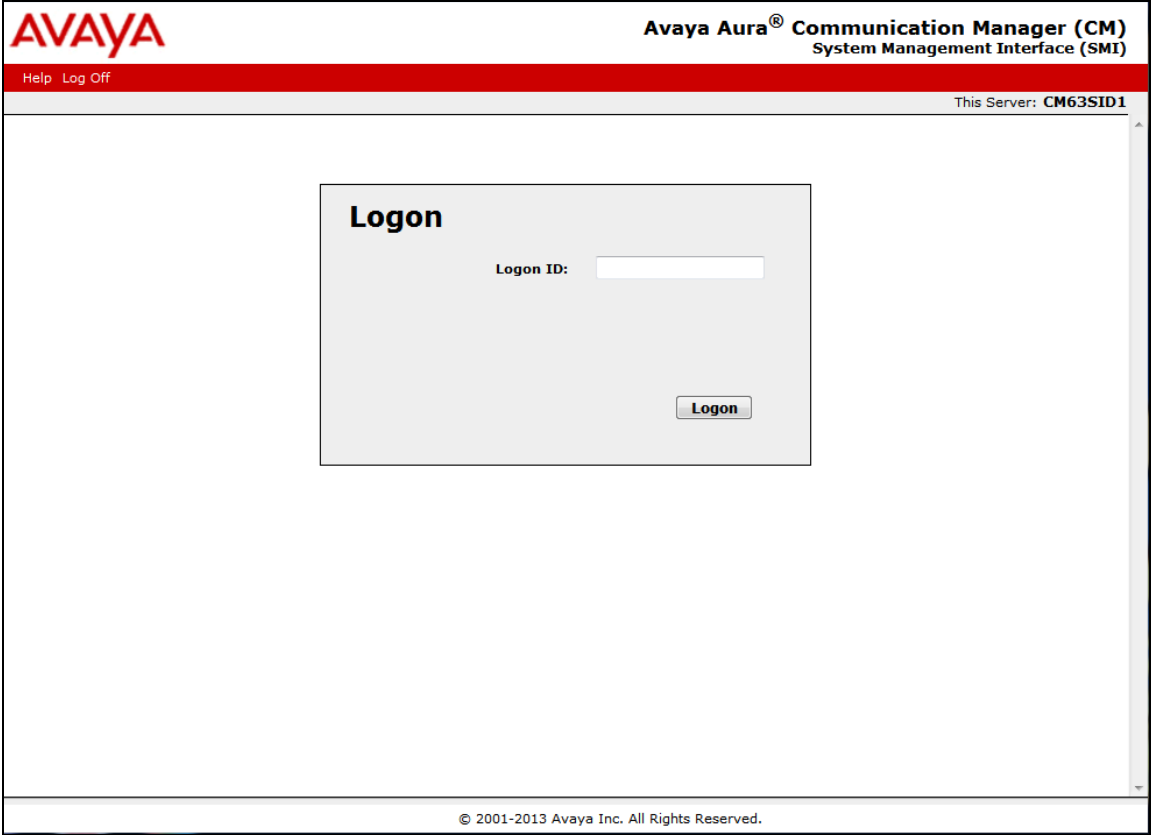
A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As Prognosis does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the Prognosis login account.

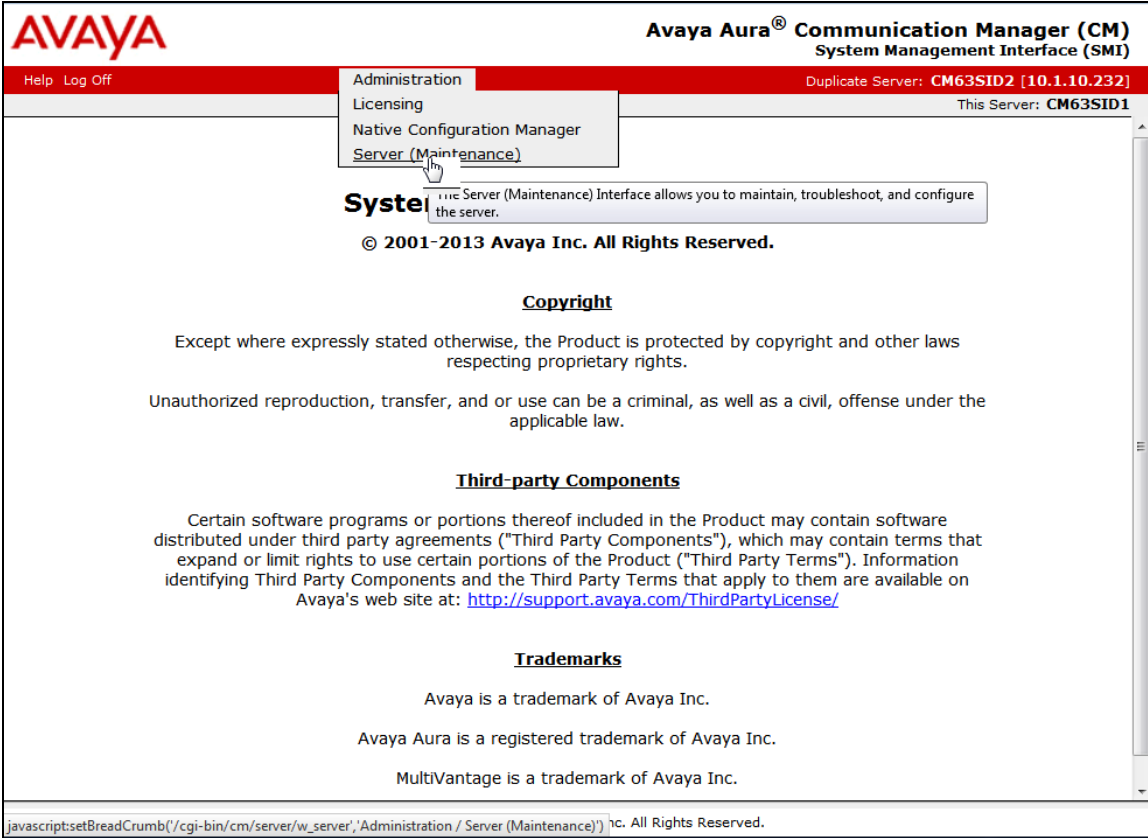
Step	Description
1.	<p>Enter the add user-profile <i>n</i> command, where <i>n</i> is the next unused profile number. Enter a descriptive name for User Profile Name and enable all categories by setting the Enbl field to y. In this test configuration, the user profile 22 is created.</p> <pre>add user-profile 22 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 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>

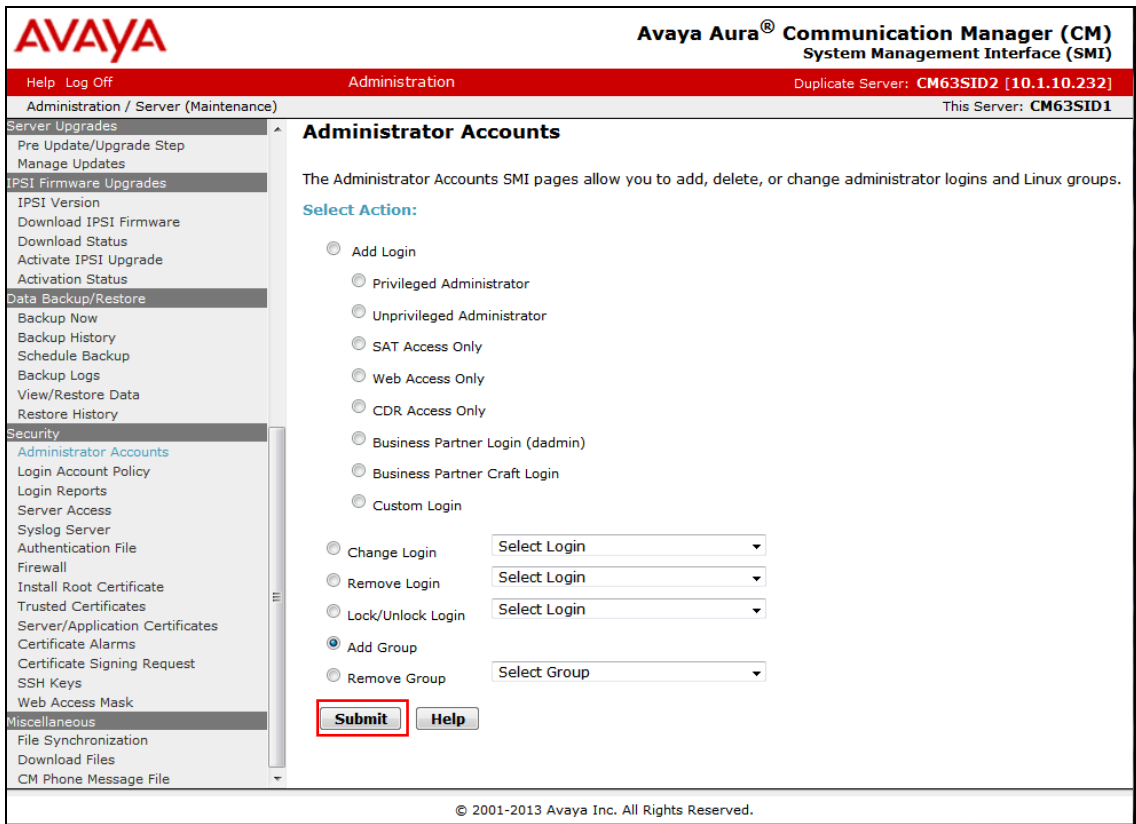
Step	Description																																													
2.	<p>On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to rm (read and maintenance). This can be accomplished by typing rm into the field Set All Permissions To. Submit the form to create the user profile.</p>																																													
	<div><div>add user-profile 22</div><div>Page 2 of 41</div></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></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>
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>																																												

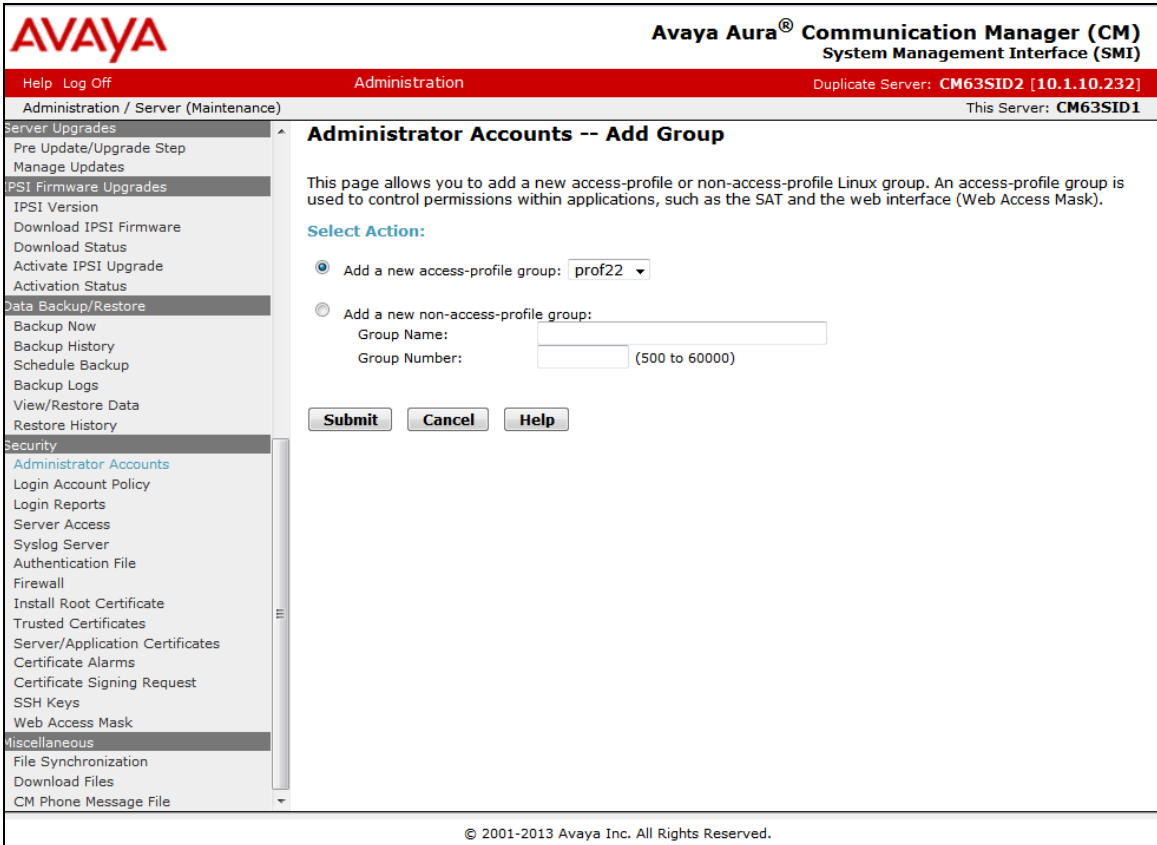
5.2. Configure Login Group

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> 

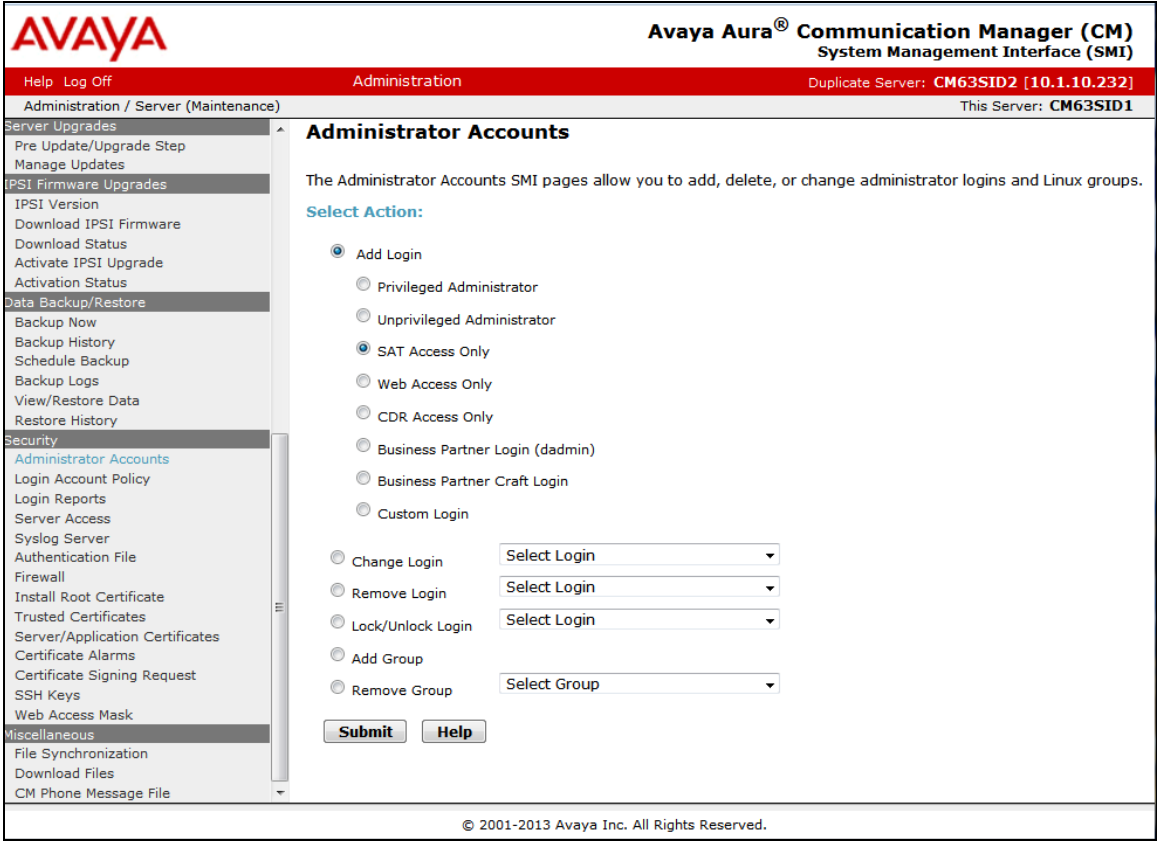
Step	Description
2.	<p>Click Administration → Server (Maintenance). This will open up the Server Administration Interface that will allow the user to complete the configuration process.</p>  <p>The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help' and 'Log Off' on the left, and 'Administration', 'Licensing', 'Native Configuration Manager', and 'Server (Maintenance)' in the center. The 'Server (Maintenance)' option is highlighted with a mouse cursor. To the right of the navigation bar, it shows 'Duplicate Server: CM63SID2 [10.1.10.232]' and 'This Server: CM63SID1'. Below the navigation bar, a message states: 'The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.' The main content area contains copyright information: '© 2001-2013 Avaya Inc. All Rights Reserved.' followed by sections for 'Copyright', 'Third-party Components', and 'Trademarks'. The footer of the interface shows a JavaScript breadcrumb trail: 'javascript:setBreadCrumb('/cgi-bin/cm/server/w_server/Administration / Server (Maintenance)') hc. All Rights Reserved.'</p>

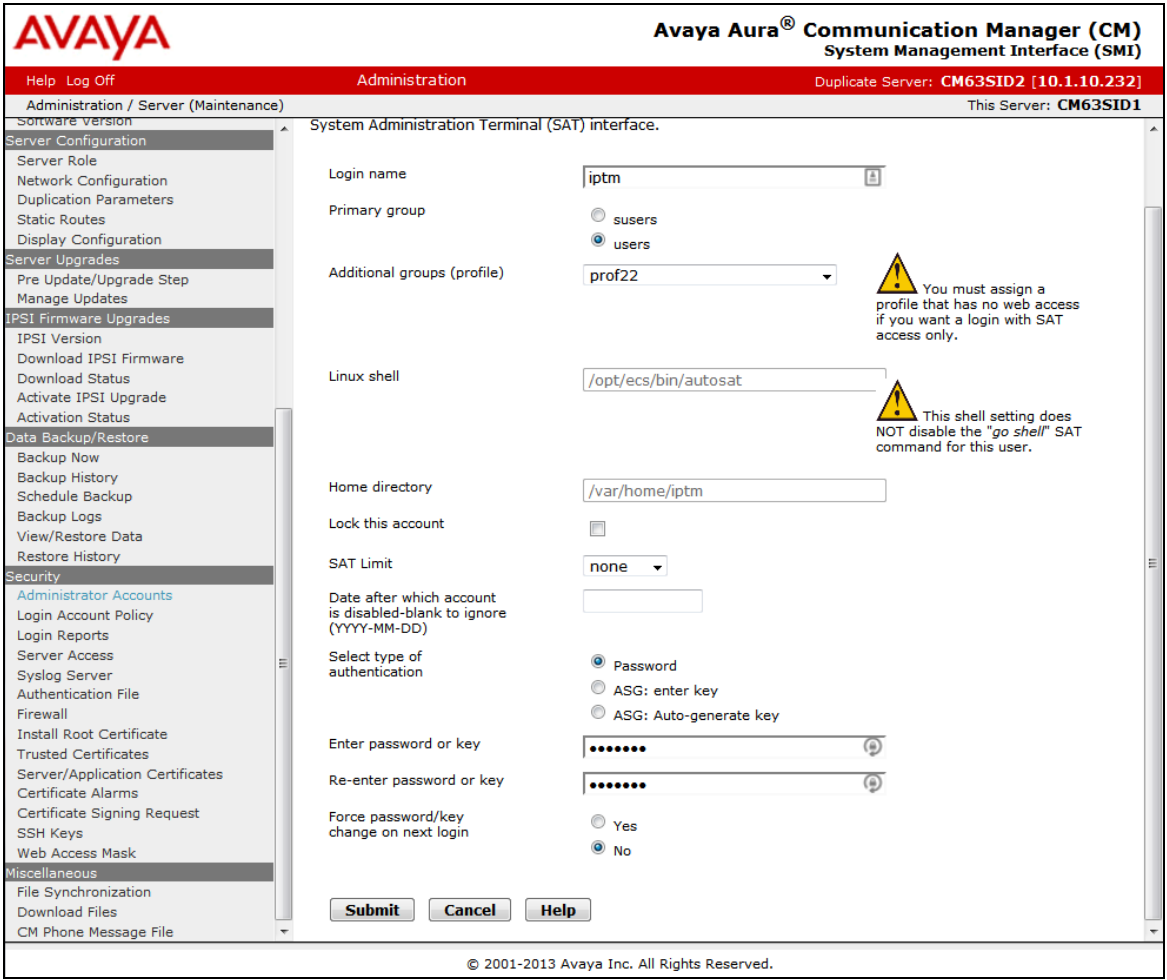
Step	Description
3.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Group and click Submit.</p>  <p>The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The left navigation pane is expanded to the 'Security' section, where 'Administrator Accounts' is selected. The main content area, titled 'Administrator Accounts', provides instructions and options for managing administrator logins and Linux groups. Under the 'Select Action:' heading, there are radio buttons for 'Add Login' and 'Add Group'. The 'Add Group' option is selected. Below these are four dropdown menus: 'Select Login' for 'Change Login', 'Remove Login', and 'Lock/Unlock Login', and 'Select Group' for 'Add Group' and 'Remove Group'. The 'Submit' button is highlighted with a red box, and a 'Help' button is also visible.</p>

Step	Description
4.	<p>Select Add a new access-profile group and select prof22 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>  <p>© 2001-2013 Avaya Inc. All Rights Reserved.</p>

5.3. Configure Login

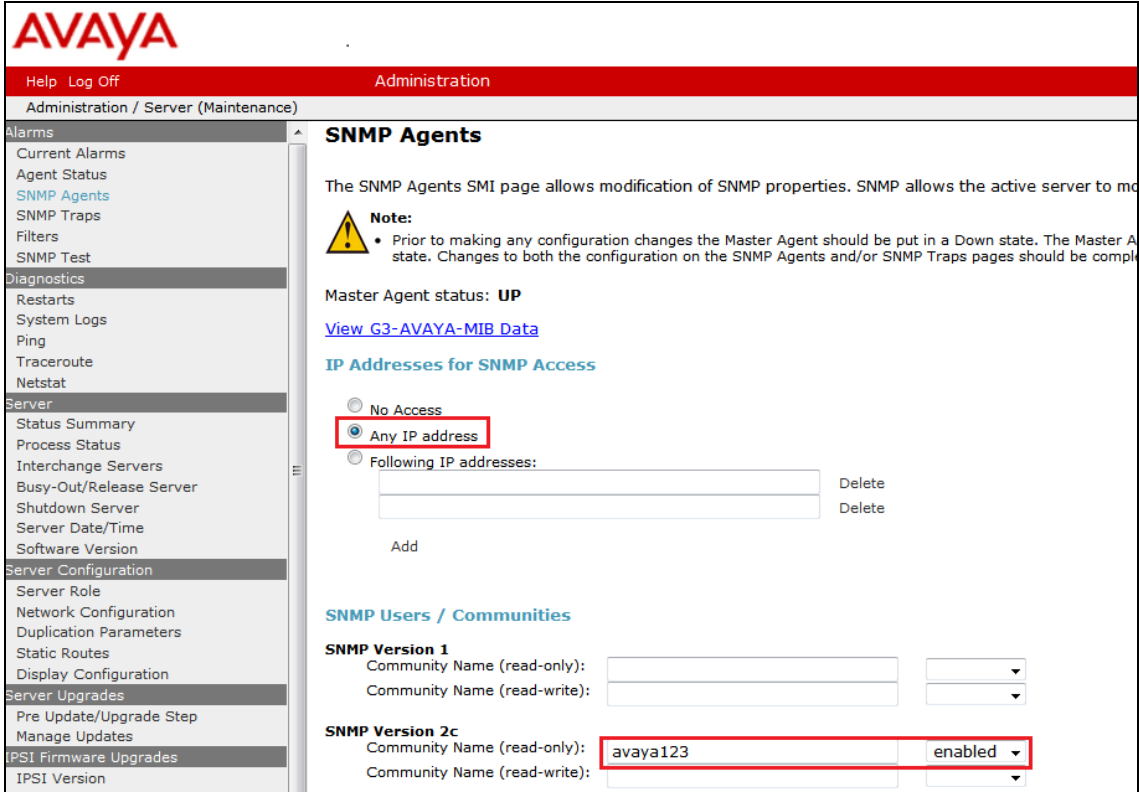
Create a login account for Prognosis to access the Communication Manager SAT. Repeat this for each Communication Manager including LSP and ESS.

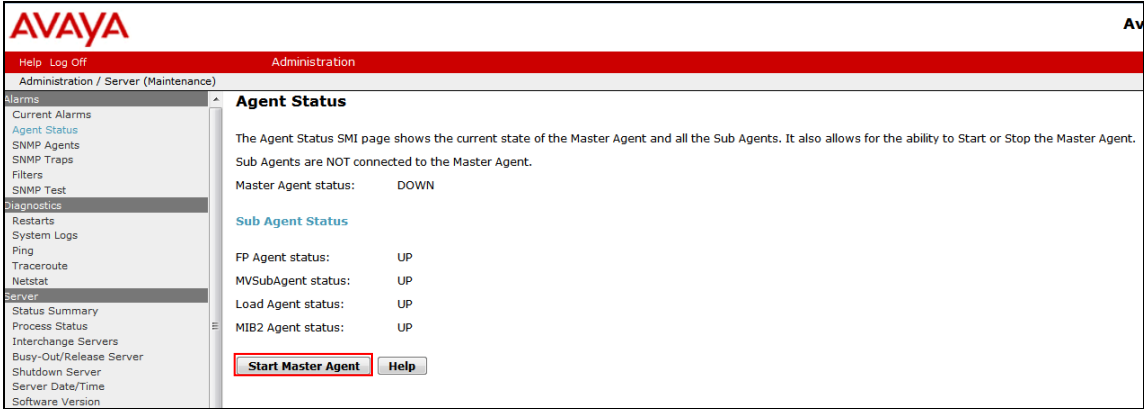
Step	Description
1.	<p>From the navigation panel on the left side, click Administrator Accounts. Select Add Login and SAT Access Only to create a new login account with SAT access privileges only. Click Submit.</p>  <p>The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The left-hand navigation pane is expanded to the 'Administrator Accounts' section. The main content area is titled 'Administrator Accounts' and includes a description: 'The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.' Under the 'Select Action:' heading, several radio button options are listed: 'Add Login' (selected), 'Privileged Administrator', 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. Below these options are five rows, each with a radio button and a text input field: 'Change Login' with a 'Select Login' dropdown, 'Remove Login' with a 'Select Login' dropdown, 'Lock/Unlock Login' with a 'Select Login' dropdown, 'Add Group' with a 'Select Group' dropdown, and 'Remove Group' with a 'Select Group' dropdown. At the bottom of the main content area are 'Submit' and 'Help' buttons. The footer of the interface reads '© 2001-2013 Avaya Inc. All Rights Reserved.'</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): prof22 [Select the access-profile 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 SNMP

Step	Description
1.	<p>Access the Communication Manager Interface as in Section 5.2 Step 1 and 2. Click on Alarms → Agent Status. Click Stop the Master Agent if the Master Agent status is UP to allow setup of SNMP Agent.</p> 

Step	Description
2.	<p>To allow Prognosis to use SNMP to collect configuration and status information from Communication Manager, navigate to Alarms → SNMP Agents in the left pane. Under IP Addresses for SNMP Access, select <i>Any IP address</i>. Under SNMP Users / Communities, configure the SNMP Version 2c section. Set the Community Name (read-only) field to avaya123 and the drop-down box to the right to enabled. Click Submit at the bottom of the web page (not shown in the figure).</p> 

Step	Description
3.	<p>Lastly, the SNMP agent must be started. Navigate to Alarms → Agent Status. If the Master Agent status is <i>Down</i>, then click the Start Master Agent button. If the Master Agent status is <i>Up</i>, then the agent must be stopped and restarted.</p> 

5.5. Configure RTCP Monitoring

To allow Prognosis 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 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>

Step	Description
2.	<p>Enter the change ip-network-region <i>n</i> command, where <i>n</i> is IP network region number to be monitored. On Page 2, set RTCP Reporting Enabled to <i>y</i> and Use Default Server Parameters to <i>y</i>.</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.

5.6. Configure CDR Monitoring

To allow Prognosis 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>

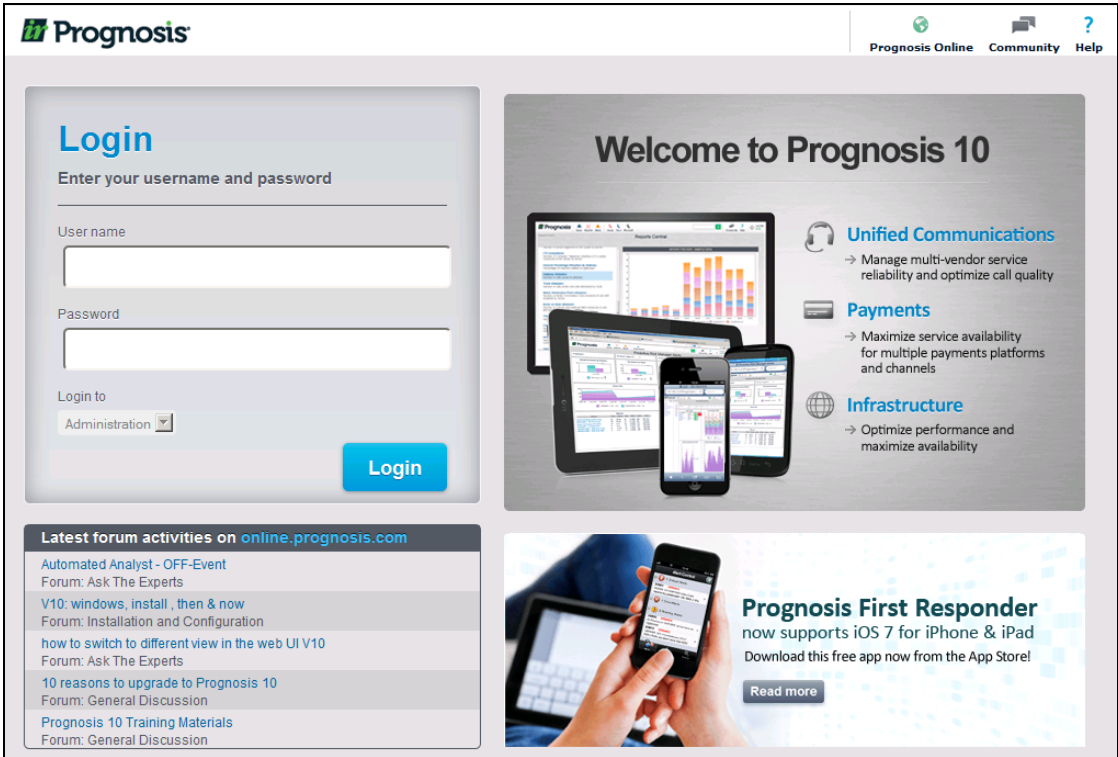
Step	Description																								
3.	<p>Enter the change ip-services command to define the CDR link. To define a primary CDR link, the following information should be provided:</p> <ul style="list-style-type: none">• Service Type: CDR1 [If needed, a secondary link can be defined by setting Service 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, disabled 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																				

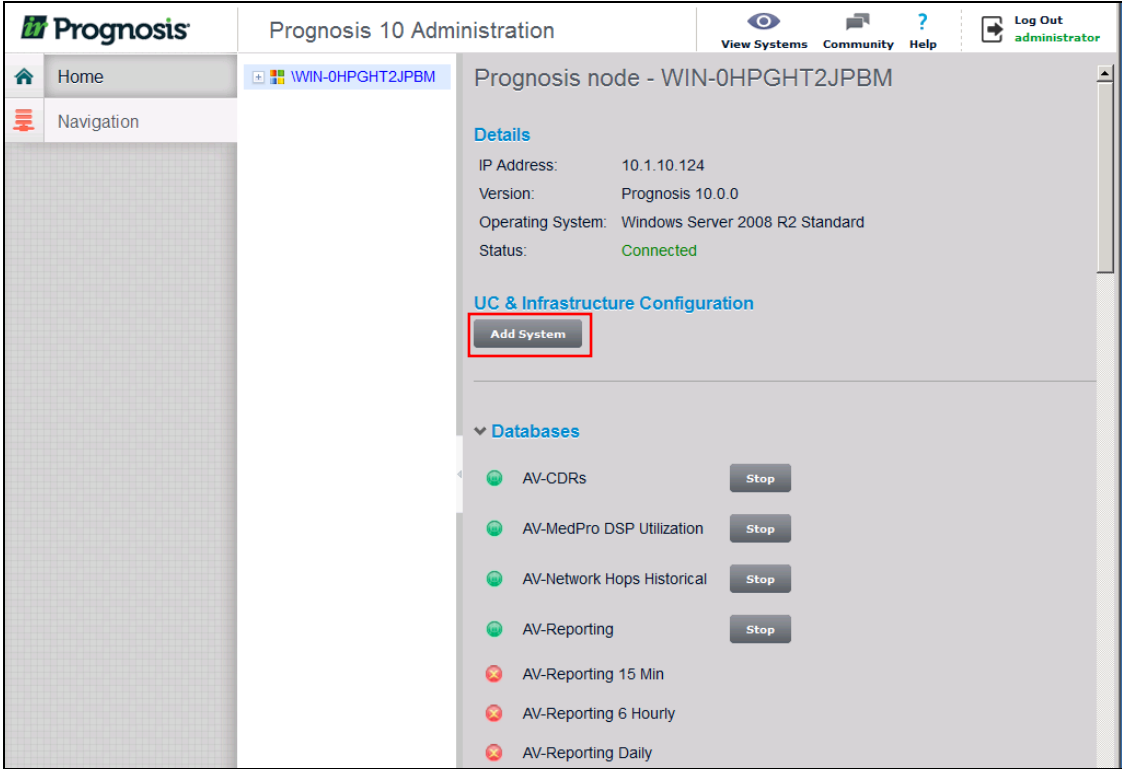
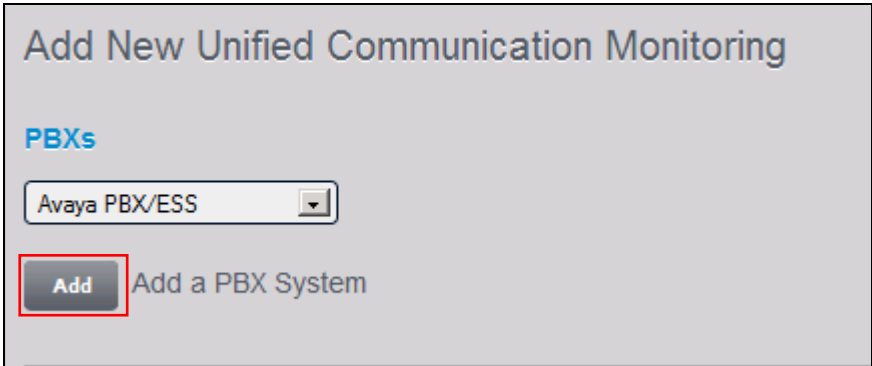
Step	Description
4.	<p>Enter the change system-parameters cdr command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test.</p> <ul style="list-style-type: none"> • CDR Date Format: month/day • Primary Output Format: unformatted [This value is used to configure Prognosis in Section 6 Step 4] • 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 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: 8 of 5000 administered Extension Extension Extension Extension 10001 10003 10005 10016 10018 20001 481121 481122 </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>
7.	<p>Enter save translation to save the changes made.</p> <pre> save translation SAVE TRANSLATION Command Completion Status Error Code Success 0 </pre>

6. Configure Prognosis

This section describes the configuration of Prognosis required to interoperate with Communication Manager. Configuration of Prognosis to interoperate with Session and System Manager can be referred from **Reference [4]** and will not be detailed here.

Step	Description
1.	<p>Log into the Prognosis with administrative privileges. Launch the Prognosis Administration by clicking Start → All Programs → Prognosis → Administration. Login with the appropriate password.</p> 

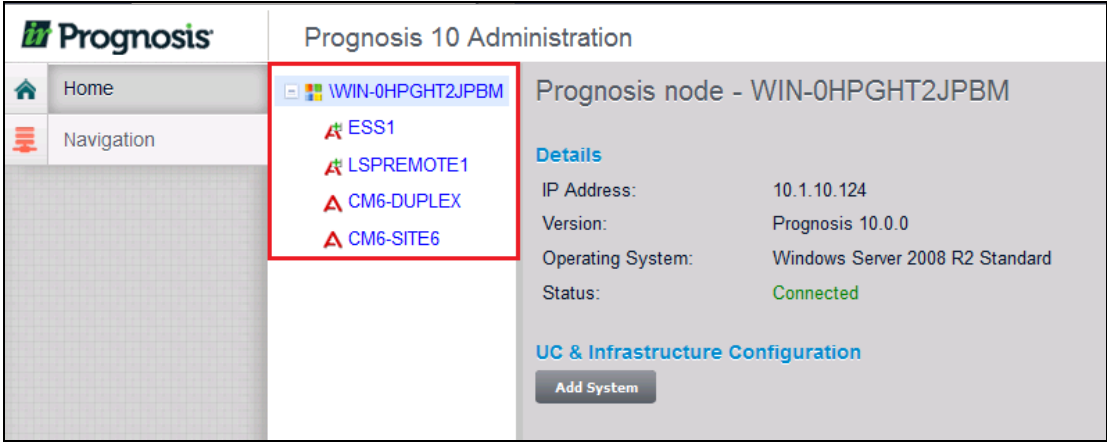
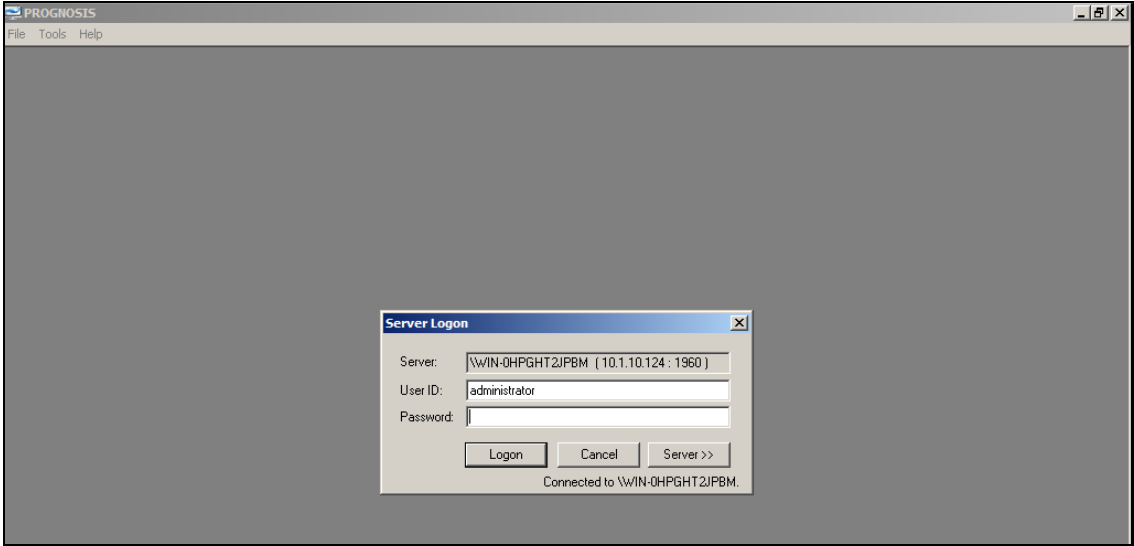
Step	Description
2.	<p>Click Add System.</p> 
3.	<p>Click Add to add a new Avaya PBX.</p> 

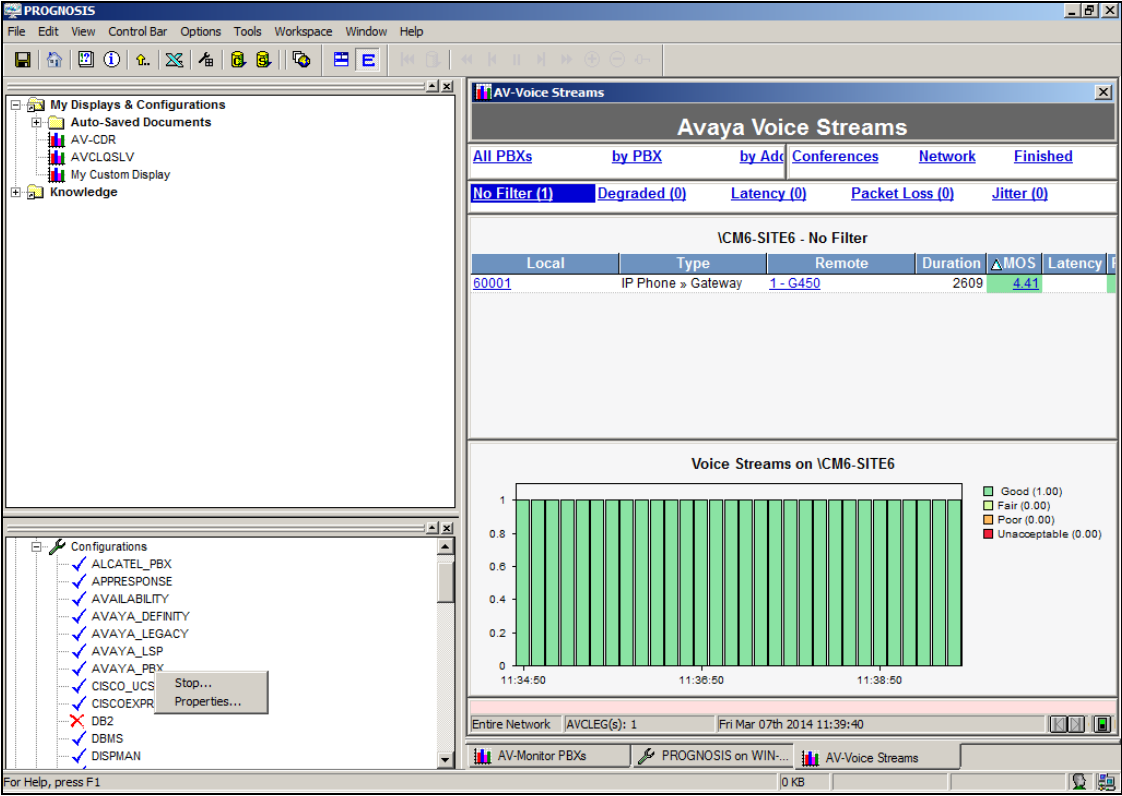
Step	Description
4.	<p>In this test configuration, the following entries are added for the two Communication Manager systems with the Display Name CM6-DUPLEX (System A) and CM6-SITE6 (System B) and with the IP addresses of the Avaya Servers 10.1.10.230 and 10.1.60.10 respectively. The Display Name must be the same name configured in Avaya Aura® System Manager.</p> <p>The following settings were used during the compliance test (see next page)</p> <p>Basic Details:</p> <ul style="list-style-type: none"> • IP address: 10.1.10.230 • Display Name: CM6-DUPLEX • Customer Name: Avaya • Site Name: DevConLab <p>SAT Connection Details:</p> <ul style="list-style-type: none"> • User Name/Password: iptm/[As configured in Section 5.3 Step 2] • Mode: Telnet • Port: 5023 [For secure connection, select SSH with port 5022] <p>CDR Configuration:</p> <ul style="list-style-type: none"> • Format: unformatted [as configured in Section 5.6 Step 4] • Date Format: mm-dd [as configured in Section 5.6 Step 4] <p>SNMP Connection Details:</p> <ul style="list-style-type: none"> • Select Use SNMP Version 2c • Community String: As configured in Section 5.4. <p>Leave the Databases and Thresholds as checked.</p> <p>Click Add to effect the addition. Repeat the above for the setup of CM6-SITE6.</p>

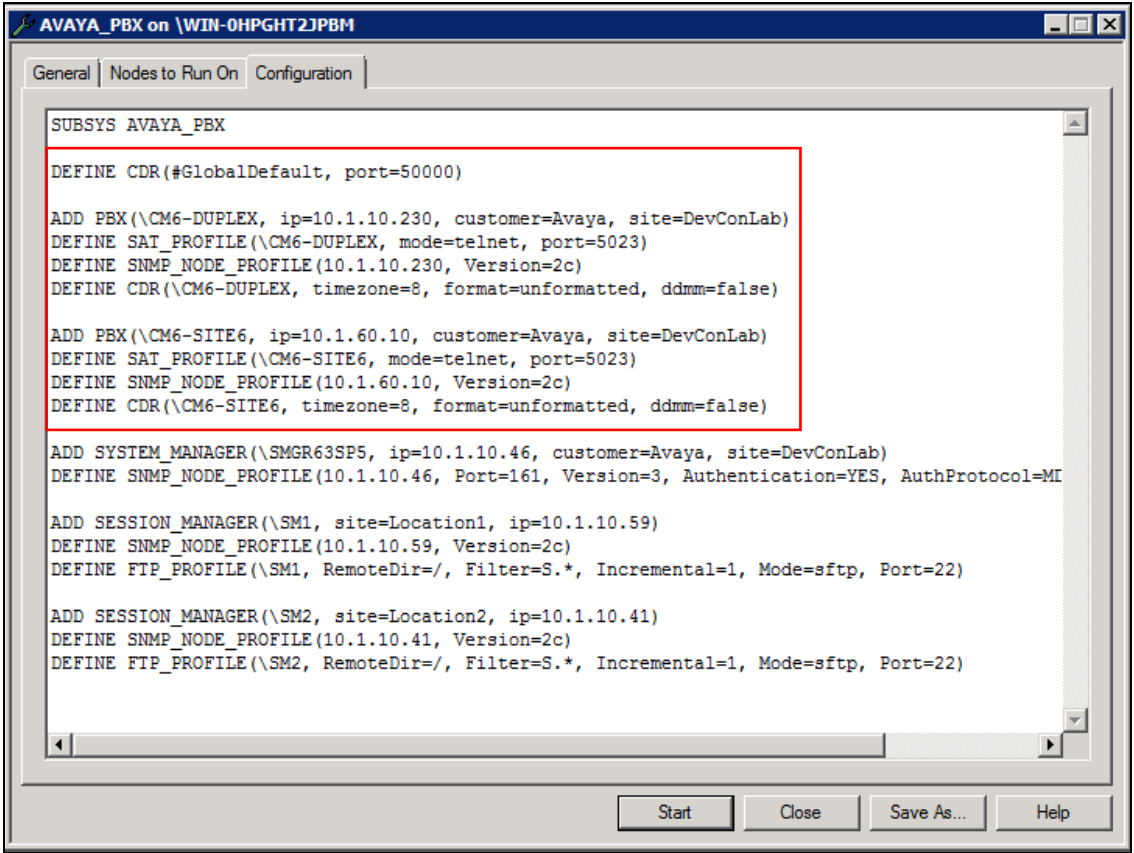
Step	Description
	<div> <h3>Add Avaya Communication Manager or Enterprise Survivable Server</h3> <h4>Basic Details</h4> <p>IP Address: * <input type="text" value="10.1.10.230"/></p> <p>Display Name: * <input type="text" value="CM6-DUPLEX"/></p> <p>Customer Name: <input type="text" value="Avaya"/></p> <p>Site Name: <input type="text" value="DevConLab"/></p> <h4>SAT Connection Details</h4> <p>User Name: * <input type="text" value="iptm"/></p> <p>Password: * <input type="password" value="••••••"/></p> <p>Mode: <input type="text" value="Telnet"/></p> <p>Port: * <input type="text" value="5023"/></p> <h4>CDR Configuration</h4> <p>Format: <input type="text" value="Unformatted"/></p> <p>Date Format: <input type="text" value="mm-dd"/></p> <p>Time Zone: <input type="text" value="(UTC+08:00) Kuala Lumpur, Singapore"/></p> <h4>SNMP Connection Details</h4> <p> <input type="radio"/> Do not use SNMP <input checked="" type="radio"/> Use SNMP Version 2c <input type="radio"/> Use SNMP Version 3 </p> <p>Community String: <input type="text" value="avaya123"/></p> <h4>Databases and Thresholds</h4> <p><input checked="" type="checkbox"/> Start standard databases and thresholds</p> <p> <input type="button" value="Add"/> <input type="button" value="Cancel"/> </p> </div>

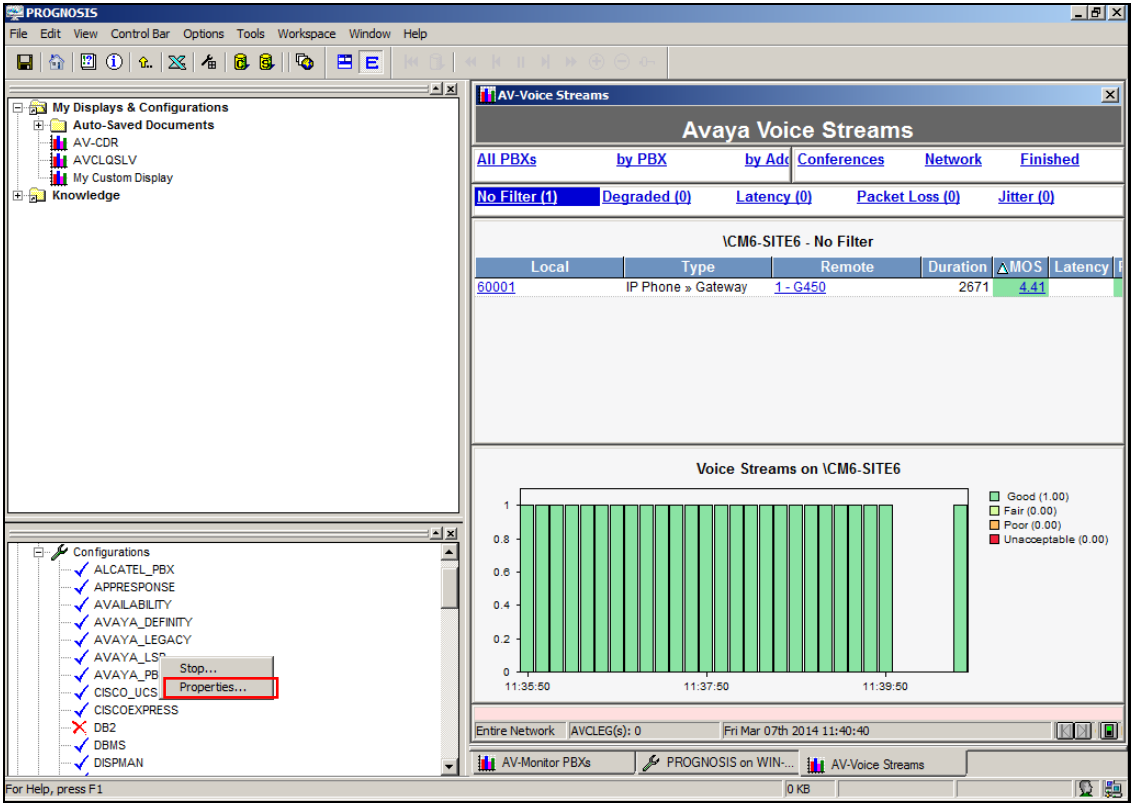
Step	Description
5.	<p>In this test configuration, the Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS) Servers with the names LSPREMOTE1 and ESS1 with the IP addresses of 10.1.40.10 and 10.1.10.239 respectively, both belonging to the CM6-DUPLEX Communication Manager system are also configured.</p> <p>Repeat Step 2 to add a new system and select Add to add a new Avaya LSP.</p> <div data-bbox="609 485 1133 766" data-label="Image"> <p>The screenshot shows a configuration window titled 'Survivable Appliances'. Inside, there is a dropdown menu currently displaying 'Avaya LSP'. Below this menu is a button labeled 'Add' which is highlighted with a red rectangular border. To the right of the 'Add' button, the text 'Add a Survivable Appliance' is visible.</p> </div>

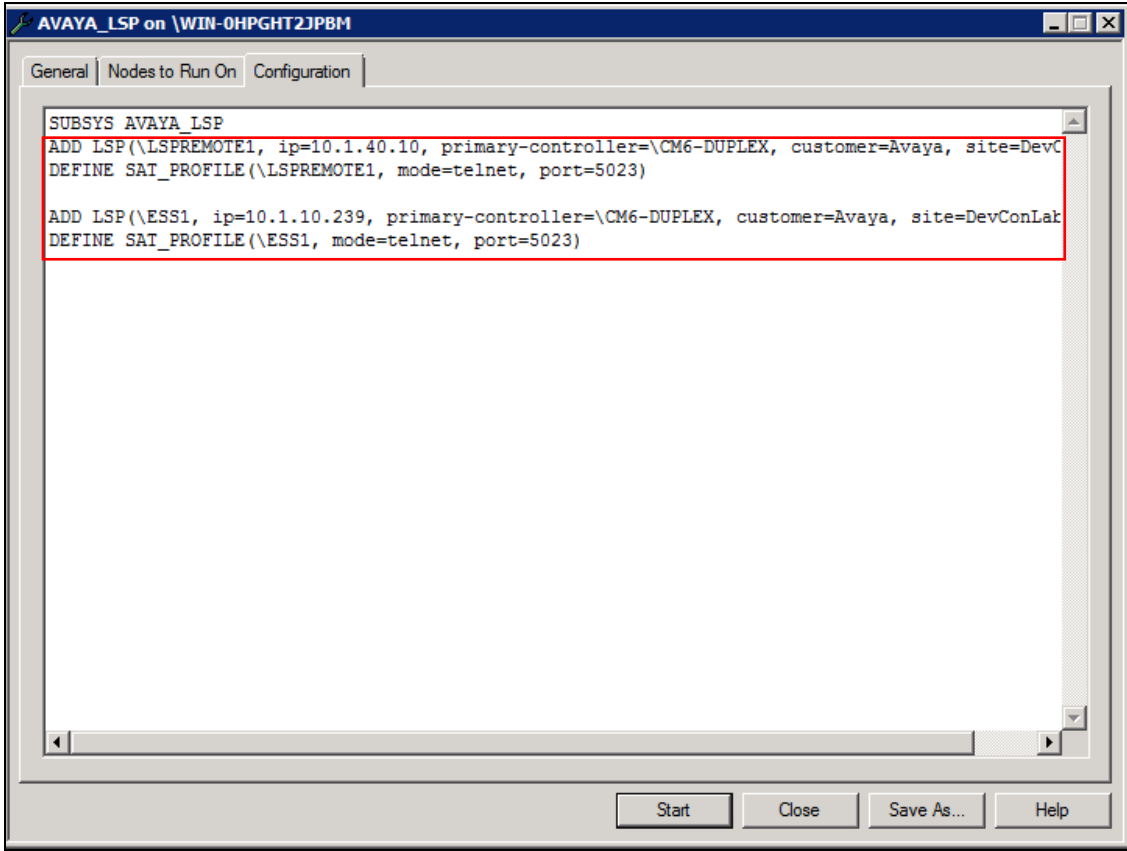
Step	Description
6.	<p>The following settings were used during the compliance test.</p> <p>Basic Details:</p> <ul style="list-style-type: none"> • IP address: 10.1.40.10 • Display Name: LSPREMOTE1 • Primary Controller: CM6-DUPLEX • Customer Name: Avaya • Site Name: DevConLab <p>SAT Connection Details:</p> <ul style="list-style-type: none"> • User/Password: iptm/[As configured in Section 5.3 Step 2] • Mode: Telnet • Port: 5023 [For secure connection, select SSH with port 5022] <p>Click Add to effect the addition. Repeat the above for the setup of ESS1.</p> <div data-bbox="420 831 1321 1864"> </div>

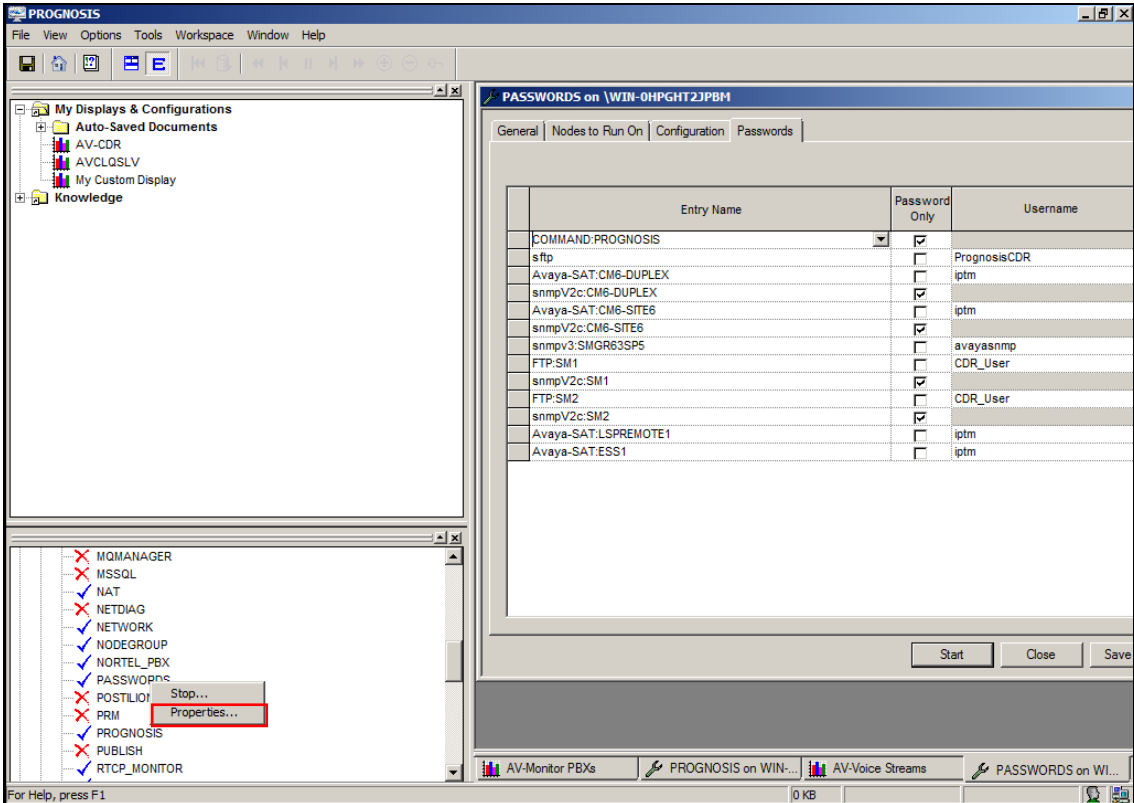
Step	Description
7.	<p>Below is the result of the additions of the 2 Communication Systems plus the LSP/ESS.</p>  <p>The screenshot shows the 'Prognosis 10 Administration' web interface. On the left is a navigation menu with 'Home' and 'Navigation'. The main content area displays 'Prognosis node - WIN-0HPGHT2JPBM'. Below this, there's a 'Details' section showing IP Address (10.1.10.124), Version (Prognosis 10.0.0), Operating System (Windows Server 2008 R2 Standard), and Status (Connected). A 'UC & Infrastructure Configuration' section with an 'Add System' button is at the bottom. A red box highlights a list of nodes: WIN-0HPGHT2JPBM, ESS1, LSPREMOTE1, CM6-DUPLEX, and CM6-SITE6.</p>
8.	<p>On Prognosis server, click Start → All Programs → Prognosis → Prognosis Client to start the Windows Client application. Log in with the appropriate credentials.</p>  <p>The screenshot shows the 'PROGNOSIS' client application window. A 'Server Logon' dialog box is open in the center. It has three input fields: 'Server' with the value '\\WIN-0HPGHT2JPBM (10.1.10.124 : 1960)', 'User ID' with the value 'administrator', and an empty 'Password' field. Below the fields are three buttons: 'Logon', 'Cancel', and 'Server >>'. At the bottom of the dialog, it says 'Connected to \\WIN-0HPGHT2JPBM.'.</p>

Step	Description
9.	<p>Expand Configurations of the Monitoring Node, right-click on AVAYA_PBX and select Properties.</p> 

Step	Description
10.	<p>Check the configurations for each of the Communication Manager and the corresponding CDR settings Step as configured in Step 4 earlier.</p> <pre> ADD PBX(\CM6-DUPLEX, ip=10.1.10.230, customer=Avaya, site=DevConLab) DEFINE SAT_PROFILE(\CM6-DUPLEX, mode=telnet, port=5023) DEFINE SNMP_NODE_PROFILE(10.1.10.230, Version=2c) DEFINE CDR(\CM6-DUPLEX, timezone=8, format=unformatted, ddmm=false) ADD PBX(\CM6-SITE6, ip=10.1.60.10, customer=Avaya, site=DevConLab) DEFINE SAT_PROFILE(\CM6-SITE6, mode=telnet, port=5023) DEFINE SNMP_NODE_PROFILE(10.1.60.10, Version=2c) DEFINE CDR(\CM6-SITE6, timezone=8, format=unformatted, ddmm=false) </pre> <p>Note that the default CDR port is 50,000 which correspond to the configurations set in Section 5.6 Step 3 is already created as default.</p> <pre> DEFINE CDR(#GlobalDefault, port=50000) </pre>  <p>The screenshot shows a window titled 'AVAYA_PBX on \WIN-0HPGHT2JPBM'. It has three tabs: 'General', 'Nodes to Run On', and 'Configuration'. The 'Configuration' tab is selected, showing a text area with the following configuration:</p> <pre> SUBSYS AVAYA_PBX DEFINE CDR(#GlobalDefault, port=50000) ADD PBX(\CM6-DUPLEX, ip=10.1.10.230, customer=Avaya, site=DevConLab) DEFINE SAT_PROFILE(\CM6-DUPLEX, mode=telnet, port=5023) DEFINE SNMP_NODE_PROFILE(10.1.10.230, Version=2c) DEFINE CDR(\CM6-DUPLEX, timezone=8, format=unformatted, ddmm=false) ADD PBX(\CM6-SITE6, ip=10.1.60.10, customer=Avaya, site=DevConLab) DEFINE SAT_PROFILE(\CM6-SITE6, mode=telnet, port=5023) DEFINE SNMP_NODE_PROFILE(10.1.60.10, Version=2c) DEFINE CDR(\CM6-SITE6, timezone=8, format=unformatted, ddmm=false) ADD SYSTEM_MANAGER(\SMGR63SP5, ip=10.1.10.46, customer=Avaya, site=DevConLab) DEFINE SNMP_NODE_PROFILE(10.1.10.46, Port=161, Version=3, Authentication=YES, AuthProtocol=MI ADD SESSION_MANAGER(\SM1, site=Location1, ip=10.1.10.59) DEFINE SNMP_NODE_PROFILE(10.1.10.59, Version=2c) DEFINE FTP_PROFILE(\SM1, RemoteDir=/, Filter=S.*, Incremental=1, Mode=sftp, Port=22) ADD SESSION_MANAGER(\SM2, site=Location2, ip=10.1.10.41) DEFINE SNMP_NODE_PROFILE(10.1.10.41, Version=2c) DEFINE FTP_PROFILE(\SM2, RemoteDir=/, Filter=S.*, Incremental=1, Mode=sftp, Port=22) </pre> <p>The first four lines of the configuration are highlighted with a red box. At the bottom of the window, there are buttons for 'Start', 'Close', 'Save As...', and 'Help'.</p>

Step	Description
11.	<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. On the left, the 'Configurations' tree is expanded, showing a list of configurations including 'ALCATEL_PBX', 'APPRESPONSE', 'AVAILABILITY', 'AVAYA_DEFINITY', 'AVAYA_LEGACY', 'AVAYA_LSP', 'AVAYA_PB', 'CISCO_UCS', 'CISCOEXPRESS', 'DB2', and 'DISPMAN'. The 'AVAYA_LSP' configuration is selected, and a context menu is open with 'Stop...' and 'Properties...' options. On the right, the 'AV-Voice Streams' window is open, displaying a table of voice streams for 'ICM6-SITE6 - No Filter'. The table has columns for 'Local', 'Type', 'Remote', 'Duration', 'MOS', and 'Latency'. A single entry is shown: '60001' (Local), 'IP Phone » Gateway' (Type), '1 - G450' (Remote), '2671' (Duration), '4.41' (MOS), and '4.41' (Latency). Below the table is a bar chart titled 'Voice Streams on ICM6-SITE6' showing MOS values over time. The legend indicates: Good (1.00) in green, Fair (0.00) in yellow, Poor (0.00) in orange, and Unacceptable (0.00) in red. The chart shows a series of green bars, indicating good quality. The status bar at the bottom shows 'Entire Network AVCLEG(s): 0 Fri Mar 07th 2014 11:40:40'.</p>

Step	Description
12.	<p>Check the configurations for each ESS and LSP Servers to be monitored as configured in Step 6 earlier.</p> <pre>ADD LSP(\LSPREMOTE1, ip=10.1.40.10, primary-controller=\CM6-DUPLEX, customer=Avaya, site=DevConLab) DEFINE SAT_PROFILE(\LSPREMOTE1, mode=telnet, port=5023)</pre> <pre>ADD LSP(\ESS1, ip=10.1.10.239, primary-controller=\CM6-DUPLEX, customer=Avaya, site=DevConLab) DEFINE SAT_PROFILE(\ESS1, mode=telnet, port=5023)</pre>  <p>The screenshot shows a window titled "AVAYA_LSP on \WIN-0HPGHT2JPBM". It has three tabs: "General", "Nodes to Run On", and "Configuration". The "Configuration" tab is active, displaying a text area with the following configuration:</p> <pre>SUBSYS AVAYA_LSP ADD LSP(\LSPREMOTE1, ip=10.1.40.10, primary-controller=\CM6-DUPLEX, customer=Avaya, site=DevC DEFINE SAT_PROFILE(\LSPREMOTE1, mode=telnet, port=5023) ADD LSP(\ESS1, ip=10.1.10.239, primary-controller=\CM6-DUPLEX, customer=Avaya, site=DevConLak DEFINE SAT_PROFILE(\ESS1, mode=telnet, port=5023)</pre> <p>The configuration text is highlighted with a red border. At the bottom of the window, there are four buttons: "Start", "Close", "Save As...", and "Help".</p>

Step	Description																																										
13.	<p>To check the SAT login account and password configured on Section 5.3, expand Configurations of the Monitoring Node and right-click on PASSWORDS and select Properties.</p>  <p>The screenshot shows the PROGNOSIS application window. On the left, a tree view under 'My Displays & Configurations' shows 'PASSWORDS' selected, with a context menu open showing 'Properties...'. The main pane displays the 'PASSWORDS on WIN-0HPGHT2JPBM' dialog box. The 'Passwords' tab is active, showing a table of entries:</p> <table border="1"> <thead> <tr> <th>Entry Name</th> <th>Password Only</th> <th>Username</th> </tr> </thead> <tbody> <tr> <td>COMMAND:PROGNOSIS</td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>sftp</td> <td><input type="checkbox"/></td> <td>PrognosisCDR</td> </tr> <tr> <td>Avaya-SAT:CM6-DUPLEX</td> <td><input type="checkbox"/></td> <td>iptm</td> </tr> <tr> <td>snmpV2c:CM6-DUPLEX</td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>Avaya-SAT:CM6-SITE6</td> <td><input type="checkbox"/></td> <td>iptm</td> </tr> <tr> <td>snmpV2c:CM6-SITE6</td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>snmpv3:SMGR63SP5</td> <td><input checked="" type="checkbox"/></td> <td>avayasnmp</td> </tr> <tr> <td>FTP-SM1</td> <td><input type="checkbox"/></td> <td>CDR_User</td> </tr> <tr> <td>snmpV2c:SM1</td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>FTP-SM2</td> <td><input type="checkbox"/></td> <td>CDR_User</td> </tr> <tr> <td>snmpV2c:SM2</td> <td><input checked="" type="checkbox"/></td> <td></td> </tr> <tr> <td>Avaya-SAT:LSPREMOTE1</td> <td><input type="checkbox"/></td> <td>iptm</td> </tr> <tr> <td>Avaya-SAT:ESS1</td> <td><input type="checkbox"/></td> <td>iptm</td> </tr> </tbody> </table> <p>Buttons at the bottom of the dialog are 'Start', 'Close', and 'Save'.</p>	Entry Name	Password Only	Username	COMMAND:PROGNOSIS	<input checked="" type="checkbox"/>		sftp	<input type="checkbox"/>	PrognosisCDR	Avaya-SAT:CM6-DUPLEX	<input type="checkbox"/>	iptm	snmpV2c:CM6-DUPLEX	<input checked="" type="checkbox"/>		Avaya-SAT:CM6-SITE6	<input type="checkbox"/>	iptm	snmpV2c:CM6-SITE6	<input checked="" type="checkbox"/>		snmpv3:SMGR63SP5	<input checked="" type="checkbox"/>	avayasnmp	FTP-SM1	<input type="checkbox"/>	CDR_User	snmpV2c:SM1	<input checked="" type="checkbox"/>		FTP-SM2	<input type="checkbox"/>	CDR_User	snmpV2c:SM2	<input checked="" type="checkbox"/>		Avaya-SAT:LSPREMOTE1	<input type="checkbox"/>	iptm	Avaya-SAT:ESS1	<input type="checkbox"/>	iptm
Entry Name	Password Only	Username																																									
COMMAND:PROGNOSIS	<input checked="" type="checkbox"/>																																										
sftp	<input type="checkbox"/>	PrognosisCDR																																									
Avaya-SAT:CM6-DUPLEX	<input type="checkbox"/>	iptm																																									
snmpV2c:CM6-DUPLEX	<input checked="" type="checkbox"/>																																										
Avaya-SAT:CM6-SITE6	<input type="checkbox"/>	iptm																																									
snmpV2c:CM6-SITE6	<input checked="" type="checkbox"/>																																										
snmpv3:SMGR63SP5	<input checked="" type="checkbox"/>	avayasnmp																																									
FTP-SM1	<input type="checkbox"/>	CDR_User																																									
snmpV2c:SM1	<input checked="" type="checkbox"/>																																										
FTP-SM2	<input type="checkbox"/>	CDR_User																																									
snmpV2c:SM2	<input checked="" type="checkbox"/>																																										
Avaya-SAT:LSPREMOTE1	<input type="checkbox"/>	iptm																																									
Avaya-SAT:ESS1	<input type="checkbox"/>	iptm																																									

Step	Description
------	-------------

14.	The four entries for the CM6-DUPLEX , second system CM6-SITE6 , LSPREMOTE1 and ESS1 are listed on the right pane.
-----	---

PASSWORDS on WIN-0HPGHT2JPBM

General | Nodes to Run On | Configuration | Passwords

Entry Name	Password Only	Username	Password
COMMAND:PROGNOSIS	<input checked="" type="checkbox"/>		*****
sftp	<input type="checkbox"/>	PrognosisCDR	*****
Avaya-SAT:CM6-DUPLEX	<input checked="" type="checkbox"/>	iptm	*****
snmpV2c:CM6-DUPLEX	<input checked="" type="checkbox"/>		*****
Avaya-SAT:CM6-SITE6	<input checked="" type="checkbox"/>	iptm	*****
snmpV2c:CM6-SITE6	<input checked="" type="checkbox"/>		*****
snmpv3:SMGR63SP5	<input type="checkbox"/>	avayasnmp	*****
FTP:SM1	<input type="checkbox"/>	CDR_User	*****
snmpV2c:SM1	<input checked="" type="checkbox"/>		*****
FTP:SM2	<input type="checkbox"/>	CDR_User	*****
snmpV2c:SM2	<input checked="" type="checkbox"/>		*****
Avaya-SAT:LSPREMOTE1	<input type="checkbox"/>	iptm	*****
Avaya-SAT:ESS1	<input type="checkbox"/>	iptm	*****

Start Close Save As... Help

7. Verification Steps

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

7.1. Verify Communication Manager

Verify that Prognosis has established three concurrent 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		1
iptm	21	10.1.10.124		3
iptm	21	10.1.10.124		4
*init	0	192.168.100.18	stat logins	5

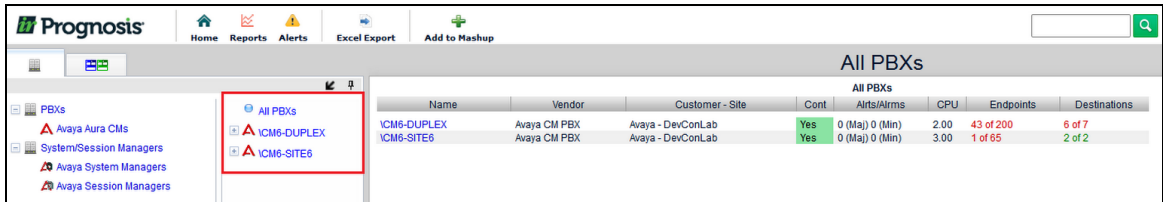
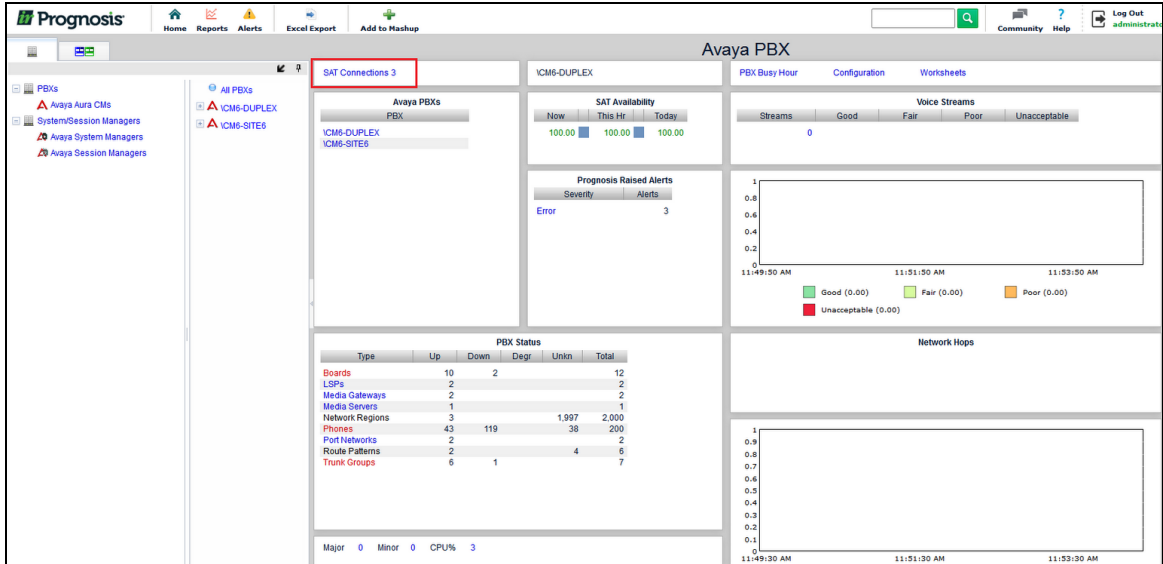
Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.6** shows **up**.

```
status cdr-link
```

CDR LINK STATUS	
Primary	Secondary
Link State: up	CDR not administered
Date & Time: 2014/03/06 12:16:53	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 Prognosis

This section provides the tests that can be performed to verify proper configuration of Prognosis. The following steps are done by accessing the Prognosis webui.

Step	Description
1.	<p>After logging into Prognosis webui, the list of Communication Manager Servers configured in Section 6 is displayed on the middle pane under All PBXs.</p> <div></div>
2.	<p>Select any of the PBX in the middle pane, verify that the SAT Connections field for each configured Communication Manager shows 3 connections. Repeat to check the other PBX.</p> <div></div>

Step	Description
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>

Prognosis

[Home](#)[Reports](#)[Alerts](#)[Excel Export](#)[Add to Mashup](#)

[Search](#)

[Community](#)[Help](#)[Log Out](#)[administrate](#)

PBXs

Avaya Aura CMs

System/Session Managers

Avaya Session Managers

All Aura CMs

ICMS-DUPLEX

ICMS-SITES

All PBXs

by PBX

by Address

Conferences

Network

Finished

No Filter (2)Degraded (0)Latency (0)Packet Loss (0)Jitter (0)

ICMS-DUPLEX - No Filter

Local	Type	Remote	Duration	MOS	Latency	Pkt Loss %	Jitter	View
10005	IP Phone to IP Phone	10001	5,726	4.39	5	0.00	0	Details
10001	IP Phone to IP Phone	10005	5,726	4.41	0	0.00	0	Details

Voice Streams on ICMS-DUPLEX

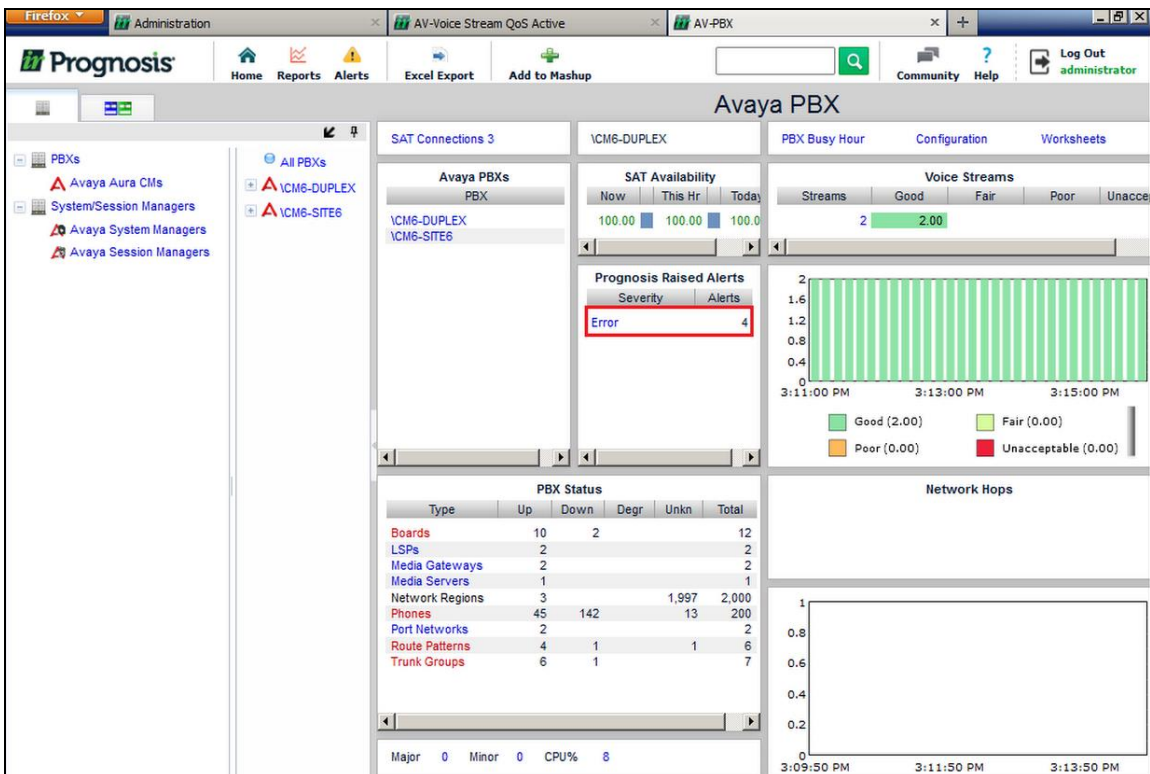
Good (2.00)

Fair (0.00)

Poor (0.00)

Unacceptable (0.00)

Step	Description
4.	Verify that the errors present in the Communication Manager are also reflected on the PBX screen below.



The screenshot displays the Prognosis Avaya PBX interface. The left sidebar shows a tree view of PBXs, including Avaya Aura CMs, System/Session Managers, Avaya System Managers, and Avaya Session Managers. The main content area is divided into several panels:

- SAT Connections 3:** Lists Avaya PBXs, including VCM6-DUPLEX and VCM6-SITE6.
- SAT Availability:** Shows a table with columns for Now, This Hr, and Today, all displaying 100.00.
- Prognosis Raised Alerts:** A table with columns for Severity and Alerts. It shows one 'Error' alert with a count of 4, which is highlighted with a red box.
- Voice Streams:** A bar chart showing streams over time, with a legend indicating Good (2.00), Fair (0.00), Poor (0.00), and Unacceptable (0.00).
- PBX Status:** A table showing the status of various components:

Type	Up	Down	Degr	Unkn	Total
Boards	10	2			12
LSPs	2				2
Media Gateways	2				2
Media Servers	1				1
Network Regions	3			1,997	2,000
Phones	45	142		13	200
Port Networks	2				2
Route Patterns	4	1		1	6
Trunk Groups	6	1			7

- Network Hops:** A bar chart showing network hops over time.

At the bottom, a status bar shows Major 0, Minor 0, and CPU% 8.

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis for Unified Communications 10 to interoperate with Avaya Aura® Communication Manager. In the configuration described in these Application Notes, Prognosis established telnet connections to the SAT to view the configurations of Communication Manager and to monitor for failures. Prognosis also processed the RTCP information to monitor the quality of IP calls and collected CDR information sent by 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 6.3, Issue 10.0, May 2013, Document Number 555-245-205.

[2] *Administering Avaya Aura® Communication Manager*, Release 6.3, Issue 9.0, October 2013, Document Number 03-300509.

[3] *Application Notes for Integrated Research Prognosis IP Telephony Manager 9.6.1 with Avaya Aura® Communication Manager 6.2*.

[4] *Application Notes for Integrated Research's Prognosis IP Telephony Manager 10 with Avaya Aura® Session Manager and Avaya Aura® System Manager*.

The following Prognosis documentations are provided by Integrated Research. Documents are also provided in the online help that comes with the software Package.

[3] *Prognosis 10 Deployment and Installation Guide*, 31st October 2013

©2014 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.