Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis for Unified Communication R11.4 with Avaya Aura® Communication Manager R7.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis for Unified Communication R11.4 to interoperate with Avaya Aura® Communication Manager R7.1.

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 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, Prognosis processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Communication Manager.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 R11.4 (herein after referred to as Prognosis) with Avaya Aura® Communication Manager R7.1.

The Prognosis product uses four integration 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 Communication Manager. By default, the solution establishes three concurrent SAT connections to each Communication Manager system and uses the connections to execute SAT commands.

- Real Time Transport Control Protocol (RTCP) collection - Prognosis collects RTCP information sent by Avaya resources including IP Media Processor (MEDPRO) boards, media gateways, media servers and IP Deskphones.

- Call Detail Recording (CDR) collection - Prognosis collects CDR information sent by Communication Manager.

- Simple Network Management Protocol (SNMP) –Prognosis uses SNMP to read Communication Manager name and IP address as these information cannot be collected via the standard SAT interface.

2. General Test Approach and Test Results

The general test approach was to use Prognosis web user interface (webui) to display the configurations of Communication Manager and verify against what is displayed on the SAT interface. The SAT interface is accessed by using Secure Shell (SSH) to Communication Manager running on VMware or Avaya Virtual Platform (AVP) used in this testing. Calls were placed between various Avaya endpoints and Prognosis webui was used to display the RTCP and CDR information collected. SNMP collection of Communication Manager's name and IP address were also verified from the Prognosis webui.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with these Application Notes, the interface between Avaya systems and Prognosis utilized capabilities of SSH for SAT access but not for CDR, RTCP and SNMP as requested by Integrated Research.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager. While this solution has successfully completed Compliance Testing for the specific release levels as described in this Application Note, Avaya does not generally recommend use the SAT interface as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the SAT interface in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using this SAT interface. Using the SAT interface in a programmatic manner may also result in a variety of operational issues, including performance impacts to the Avaya solution. If there are no other programmatic options available to obtain the required data or functionality, Avaya recommends that 3rd party applications only be executed during low call volume periods, and that real time delays be inserted between each command execution. NOTE: The scope of the compliance testing activities reflected in this Application Note explicitly did not include load or performance evaluation criteria, and no guarantees or assurances are made by Avaya that the 3rd party application has implemented these recommendations. The vendor of the 3rd party application using this interface remains solely responsible for verifying interoperability with all later Communication Manager Releases, including feature packs, service packs, and patches as issued by Avaya. For additional details see Avaya Product Support Notices PSN002884u, PSN005085u, and PSN020295u, available at www.avaya.com/support.

2.1. Interoperability Compliance Testing

For feature testing, Prognosis webui was used to view the configurations of Communication Manager via collected SAT data such as port networks, cabinets, media gateways, media servers, Enterprise Survivable Server (ESS), Local Survivable Processor (LSP), trunk groups, route patterns, CLAN, MEDPRO and DS1 boards, IP network regions, stations, processor occupancy, alarm and error information. Prognosis webui was also used to view the Communication Manager name and IP address collected via SNMP.

For the collection of RTCP and CDR information, the endpoints included Avaya H323, digital and analog endpoints, and Avaya one-X® Communicator user. 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 Prognosis and Communication Manager to simulate system unavailability. Interchanging of the duplex Communication Manager 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. The configuration consists of a duplex Communication Manager system (System A) with two Avaya G650 Media Gateways, an Avaya G430 Media Gateway with Avaya S8300D Server as a Local Survivability Processor (LSP) and a local Avaya G250-BRI Media Gateway. An Enterprise Survivable Server (ESS) was also configured for failover testing. A second Communication Manager system (System B) runs on a simplex Communication Manager system with an Avaya G450 Media Gateway. Both systems have Avaya H323, SIP, digital and analog endpoints, 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 endpoints. Prognosis was installed on a server running Microsoft Windows Server 2012 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.

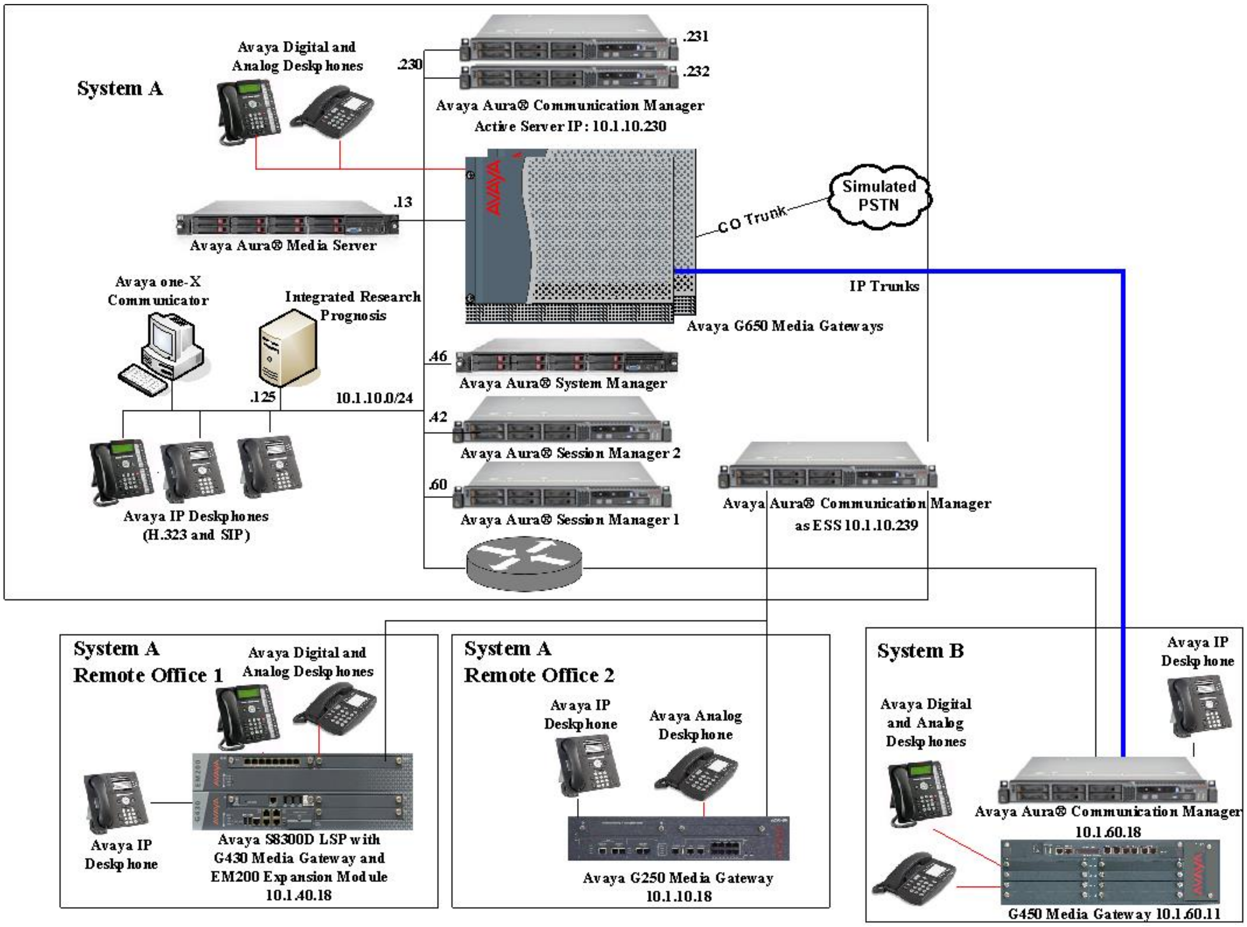

System A
Avaya Digital and Analog Deskphones
.230
.231
.232
Avaya Aura® Communication Manager Active Server IP: 10.1.10.230
.13
Avaya Aura® Media Server
Simulated PSTN
CO Trunk
IP Trunks
Avaya G650 Media Gateways
Avaya one-X Communicator
Integrated Research Prognosis
.125
10.1.10.0/24
.46
Avaya Aura® System Manager
.42
Avaya Aura® Session Manager 2
.60
Avaya Aura® Session Manager 1
Avaya IP Deskphones (H.323 and SIP)
Avaya Aura® Communication Manager as ESS 10.1.10.239
System A Remote Office 1
Avaya Digital and Analog Deskphones
Avaya IP Deskphone
Avaya S8300D LSP with G430 Media Gateway and EM200 Expansion Module 10.1.40.18
System A Remote Office 2
Avaya IP Deskphone
Avaya Analog Deskphone
Avaya G250 Media Gateway 10.1.10.18
System B
Avaya IP Deskphone
Avaya Digital and Analog Deskphones
Avaya Aura® Communication Manager 10.1.60.18
G450 Media Gateway 10.1.60.11

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 (System A)	7.1.2.0.0.532.24184
Avaya Aura® Media Server	7.8.0.333
Avaya G650 Media Gateway - TN2312BP IP Server Interface - TN799DP C-LAN Interface - TN2602AP IP Media Processor - TN2302AP IP Media Processor - TN2464BP DS1 Interface - TN2464CP DS1 Interface - TN793CP Analog Line - TN2214CP Digital Line - TN2501AP Announcement	 HW07, FW058 HW01, FW044 HW02 FW066 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW012 HW08, FW016 HW03 FW023
Avaya G250 Media Gateway	30.27.1
Avaya Aura® Communication Manager (G450 Media Gateway – System B)	7.1.2.0.0.532.24184
Avaya G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	39.5.0 HW01 FW008 HW07 FW015 HW10 FW099 HW03 FW015 HW11 FW053
Avaya Aura® Communication Manager using Avaya S8300D Server as Local Survivable Processor (LSP)	7.1.2.0.0.532.24184
Avaya G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	39.5.0 HW04 FW015 HW12 FW100 HW31 FW100 HW05 FW022
Avaya Aura® Communication Manager as Enterprise Survivable Server (ESS)	7.1.2.0.0.532.24184
Avaya Aura® System Manager	7.1.2.0 Build No.– 7.1.0.0.1125193
Avaya Aura® Session Manager (1)	7.1.2.0.712004
Avaya Aura® Session Manager (2)	7.1.2.0.712004
Avaya 96x1 Series IP Deskphones - 9641G - 9611G	 7.1.1.0 (SIP) 6.6506 (H323)

Equipment/Software	Release/Version
Avaya 1600 Series IP Deskphones - 1608-I - 1603SW-I	 1.3100 (H.323) 1.3100 (H.323)
Avaya Digital Deskphones - 1416 - 1408	 Rel 4 SP9 Rel 4 SP9
Avaya Analog Phones	-
Desktop PC with Avaya one-X Communicator	6.2.12.04-SP12 (H.323)
Prognosis running on Windows 2012 R2 SP1	11.4

Note: All Avaya Aura® systems runs on VMware 5.x except S8300D on Avaya Virtual Platform.

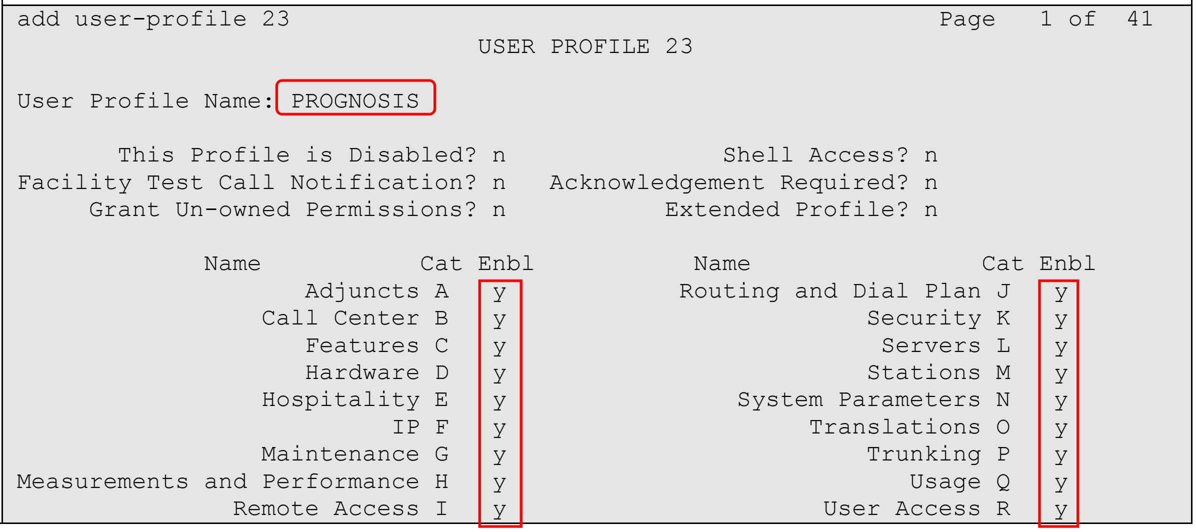
5. Configure Avaya Aura® Communication Manager

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 SNMP, RTCP and CDR reporting. The steps are repeated for Communication Manager in System B.

5.1. Configure SAT User Profile

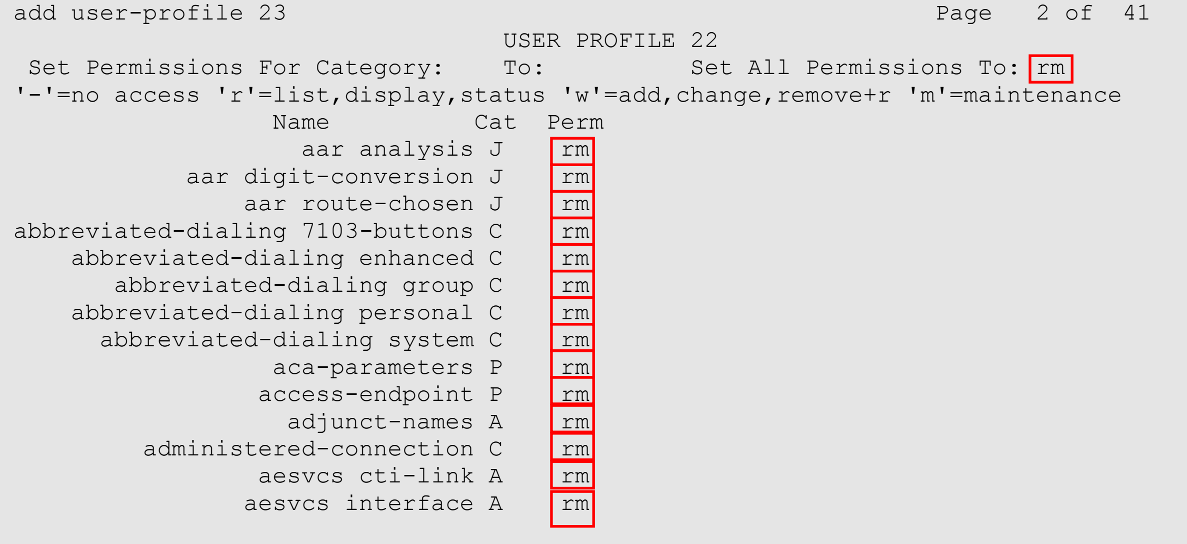
A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As Prognosis does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the Prognosis login account.

Step	Description
1.	Enter the **add user-profile *n*** command, where ***n*** 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 23 is created.



```
add user-profile 23                                             Page   1 of   41
                                USER PROFILE 23

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
```

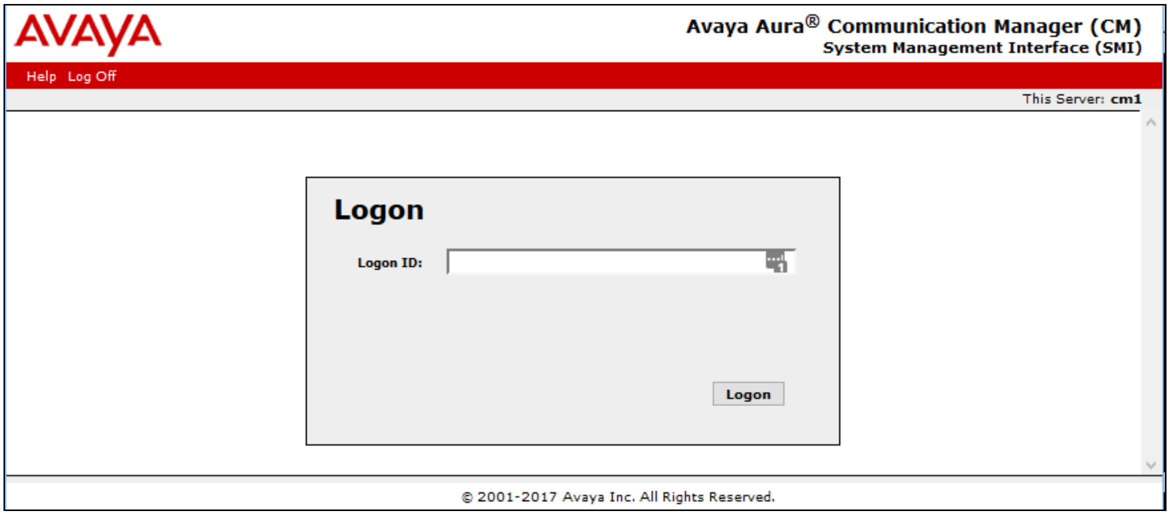
Step	Description
2.	On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the field **Set All Permissions To**. Submit the form to create the user profile.



```
add user-profile 23                                             Page   2 of  41
                                  USER PROFILE 22
 Set Permissions For Category:    To:          Set All Permissions To: rm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  Name          Cat  Perm
                    aar analysis J    rm
            aar digit-conversion J    rm
                aar route-chosen J    rm
abbreviated-dialing 7103-buttons C    rm
    abbreviated-dialing enhanced C    rm
       abbreviated-dialing group C    rm
    abbreviated-dialing personal C    rm
      abbreviated-dialing system C    rm
                  aca-parameters P    rm
                 access-endpoint P    rm
                   adjunct-names A    rm
         administered-connection C    rm
                 aesvcs cti-link A    rm
                aesvcs interface A    rm
```

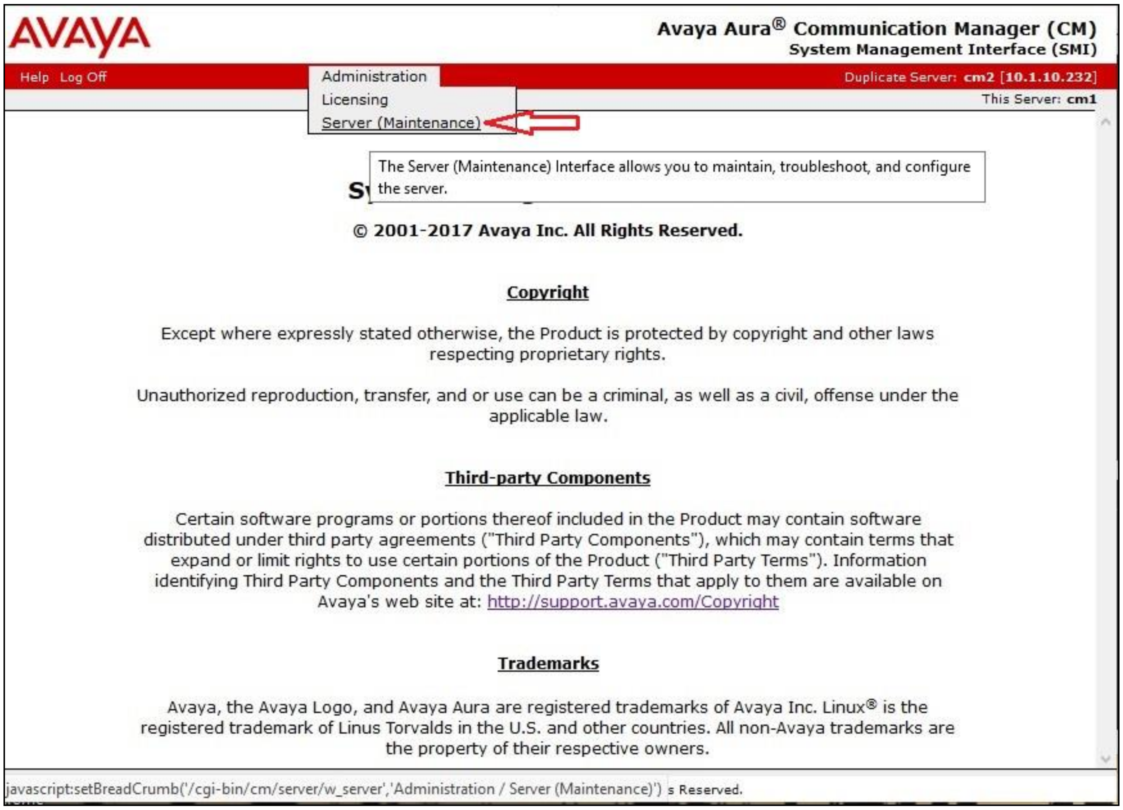
5.2. Configure Login Group

Create an Access-Profile Group on Communication Manager System Management Interface (SMI) to correspond to the SAT User Profile created in **Section 5.1**.

Step	Description
1.	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.  AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Help Log Off This Server: cm1 Logon Logon ID: Logon © 2001-2017 Avaya Inc. All Rights Reserved.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Click **Administration → Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow the user to complete the configuration process.



Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)

Duplicate Server: **cm2 [10.1.10.232]**
This Server: **cm1**

The Server (Maintenance) Interface allows you to maintain, troubleshoot, and configure the server.

© 2001-2017 Avaya Inc. All Rights Reserved.

Copyright

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

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

Third-party Components

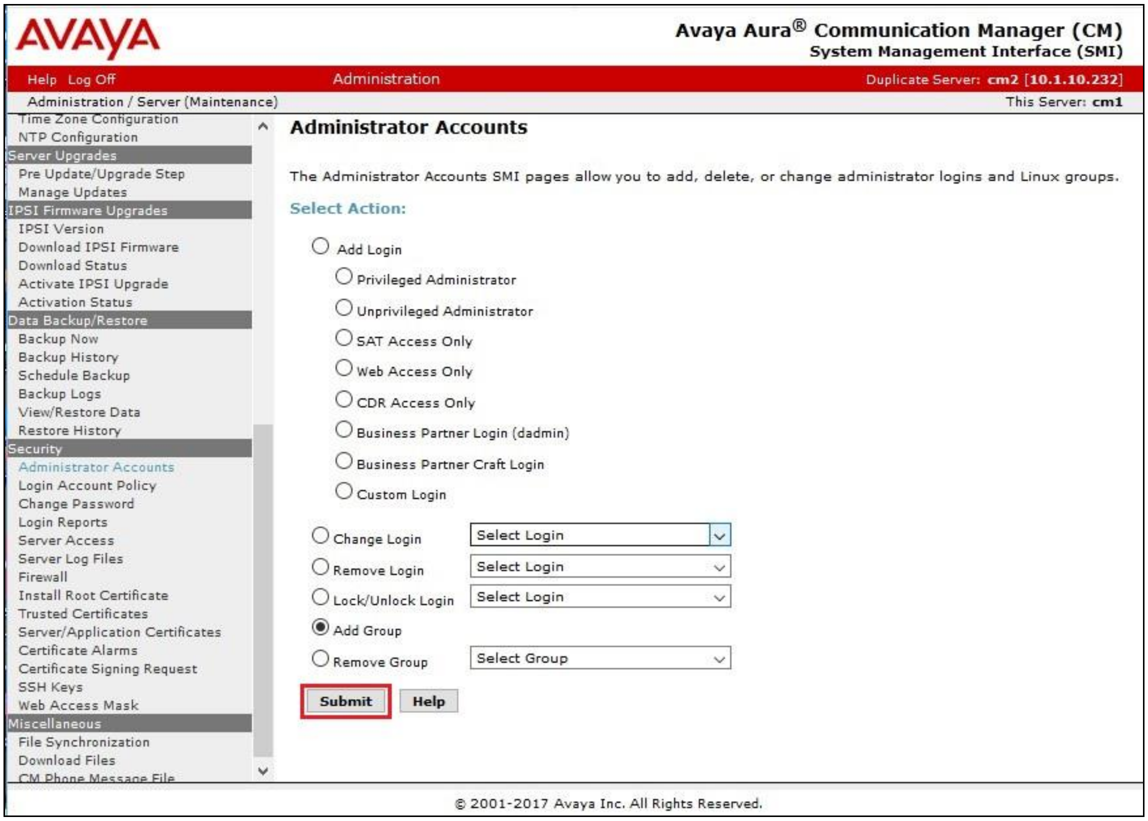
Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third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

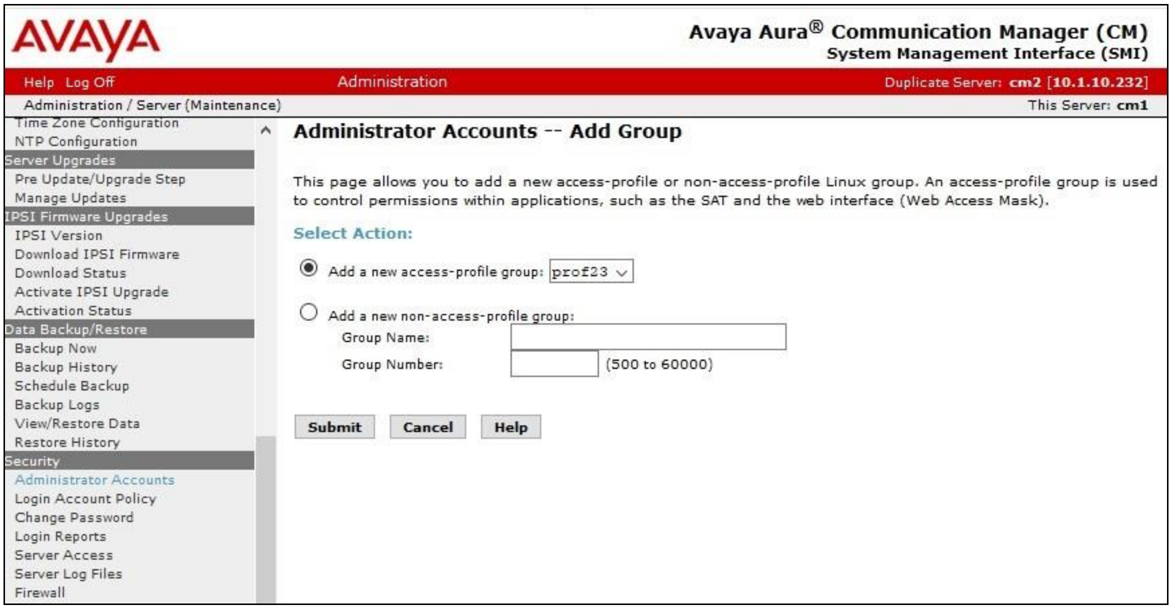
Trademarks

Avaya, the Avaya Logo, and Avaya Aura are registered trademarks of Avaya Inc. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries. All non-Avaya trademarks are the property of their respective owners.

javascript:setBreadCrumb('/cgi-bin/cm/server/w_server','Administration / Server (Maintenance)') s Reserved.

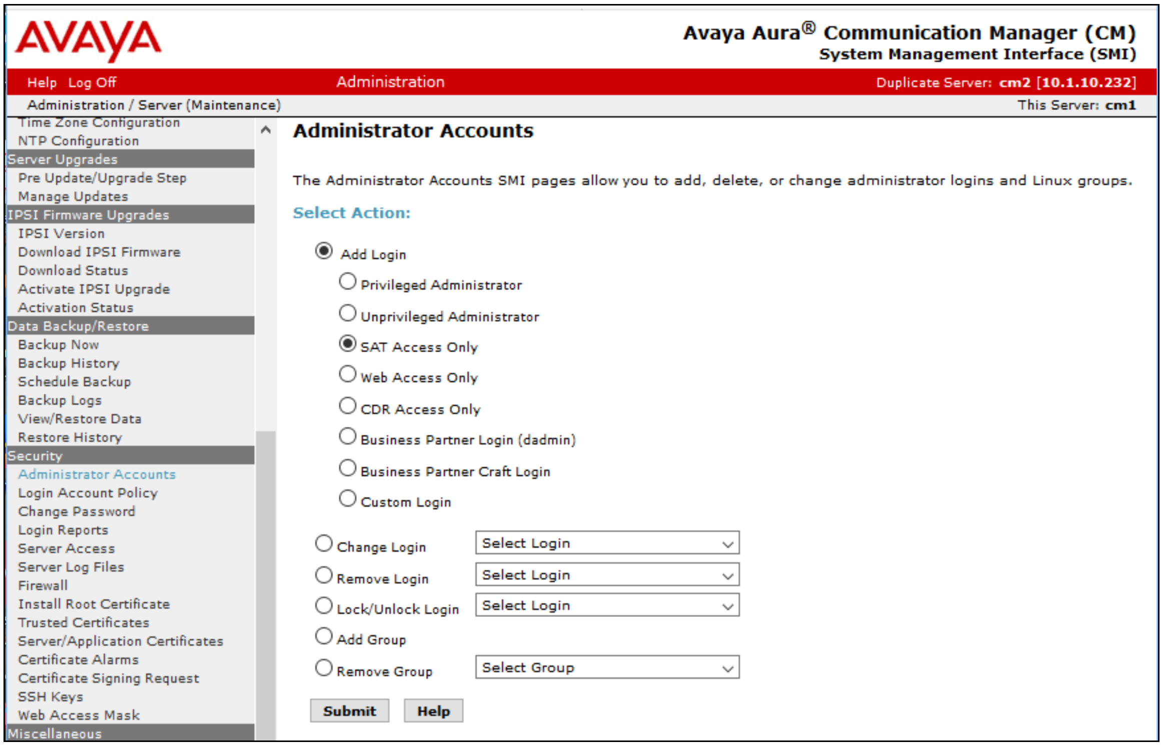
</td></tr>
</table>

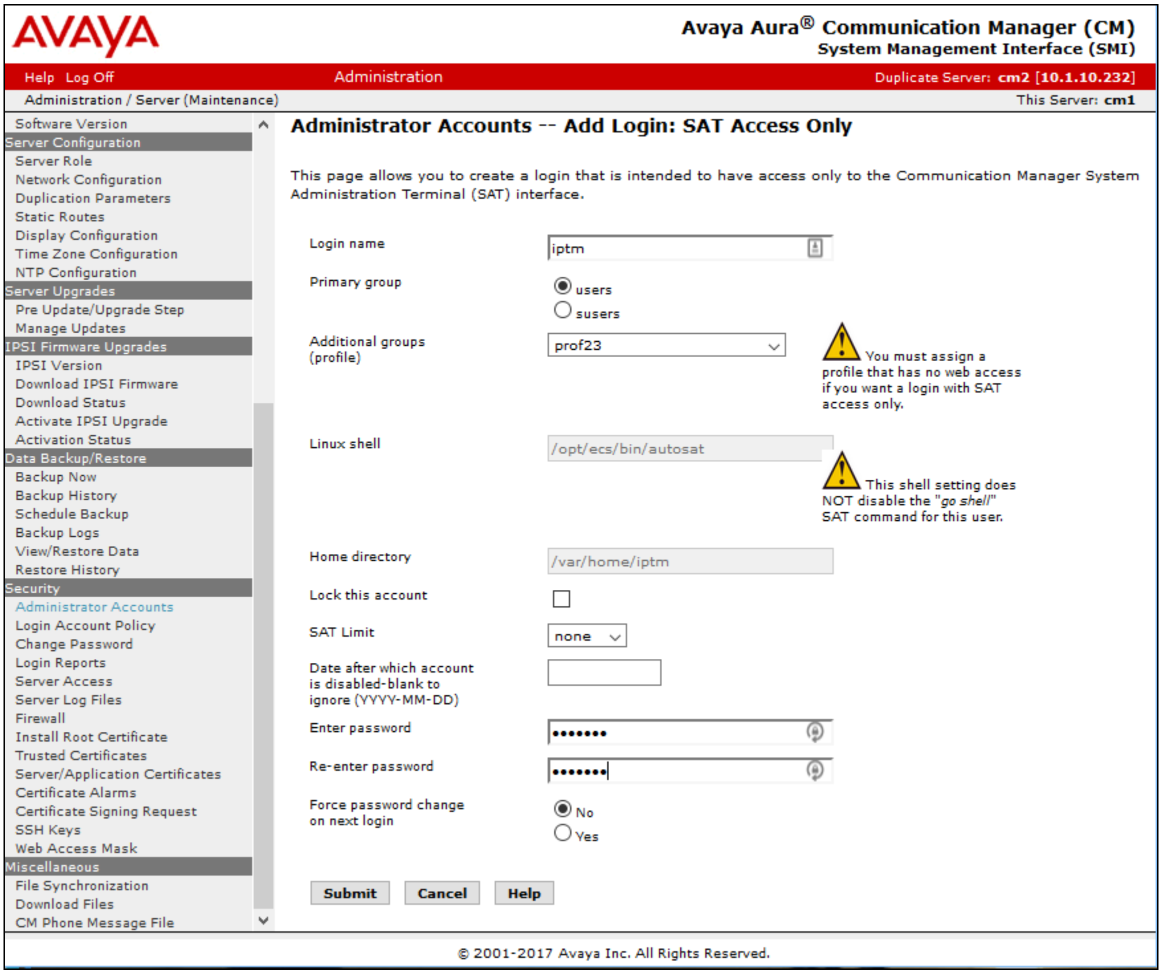
Step	Description
3.	From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Group** and click **Submit**.  AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Help Log Off Administration Duplicate Server: cm2 [10.1.10.232] Administration / Server (Maintenance) This Server: cm1 Time Zone Configuration NTP Configuration Server Upgrades Pre Update/Upgrade Step Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Security Administrator Accounts Login Account Policy Change Password Login Reports Server Access Server Log Files Firewall Install Root Certificate Trusted Certificates Server/Application Certificates Certificate Alarms Certificate Signing Request SSH Keys Web Access Mask Miscellaneous File Synchronization Download Files CM Phone Message File **Administrator Accounts** The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups. Select Action: ○ Add Login ○ Privileged Administrator ○ Unprivileged Administrator ○ SAT Access Only ○ Web Access Only ○ CDR Access Only ○ Business Partner Login (dadmin) ○ Business Partner Craft Login ○ Custom Login ○ Change Login [Select Login] ○ Remove Login [Select Login] ○ Lock/Unlock Login [Select Login] ● Add Group ○ Remove Group [Select Group] Submit Help © 2001-2017 Avaya Inc. All Rights Reserved.

Step	Description
4.	Select **Add a new access-profile group** and select **prof23** 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.  AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Help Log Off Administration Duplicate Server: cm2 [10.1.10.232] Administration / Server (Maintenance) This Server: cm1 Time Zone Configuration NTP Configuration Server Upgrades Pre Update/Upgrade Step Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Security Administrator Accounts Login Account Policy Change Password Login Reports Server Access Server Log Files Firewall Submit Cancel Help **Administrator Accounts -- Add Group** This page allows you to add a new access-profile or non-access-profile Linux group. An access-profile group is used to control permissions within applications, such as the SAT and the web interface (Web Access Mask). Select Action: ● Add a new access-profile group: prof23 ○ Add a new non-access-profile group: Group Name: Group Number: (500 to 60000)

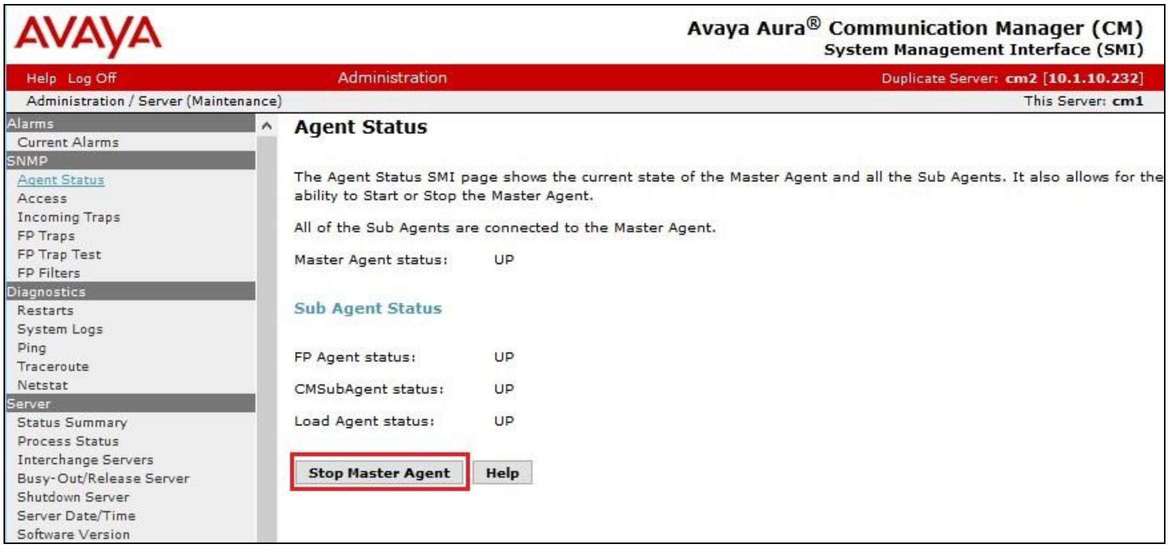
5.3. Configure Login

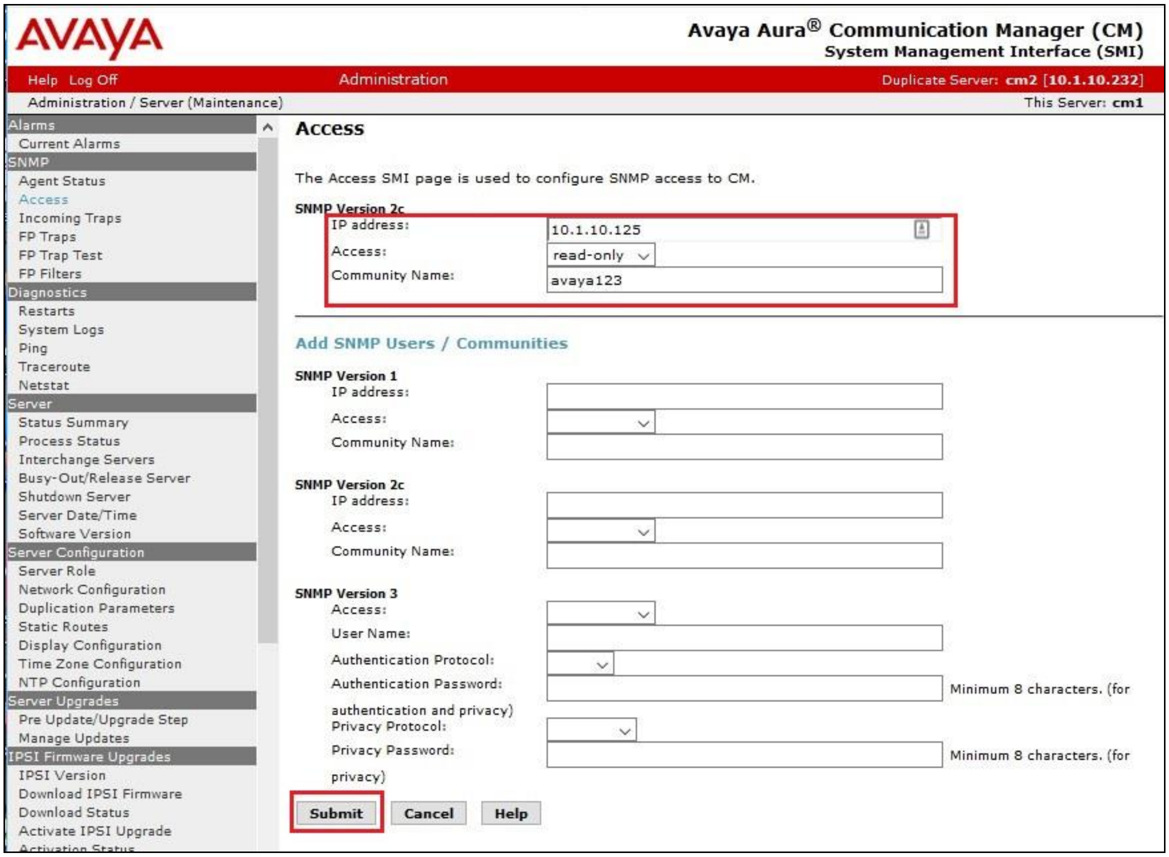
Create a login account for Prognosis to access the Communication Manager SAT. Repeat this for each Communication Manager.

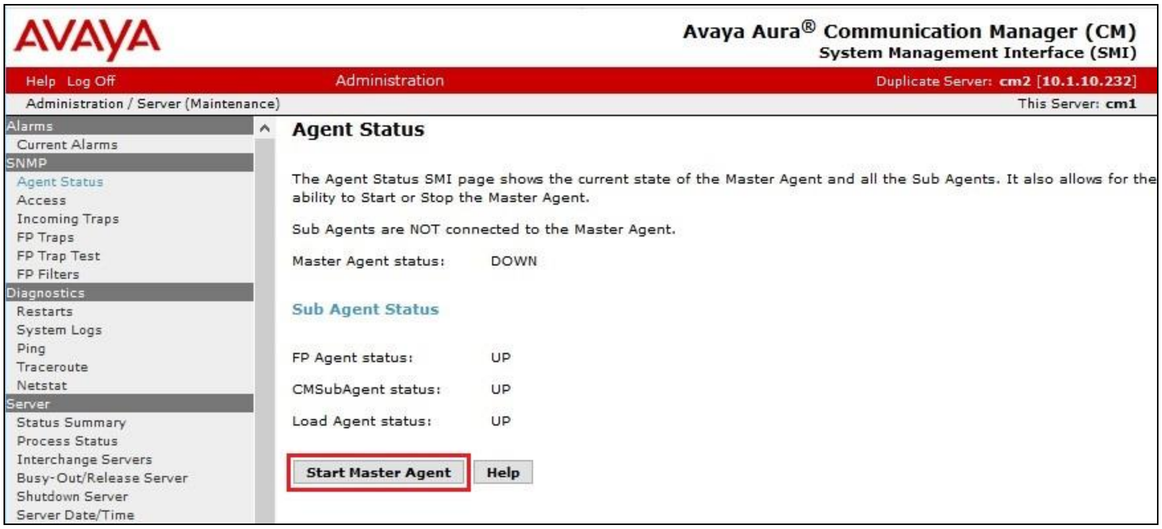
Step	Description
1.	From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Login** and **SAT Access Only** to create a new login account with SAT access privileges only. Click **Submit**.  AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Help Log Off Administration Duplicate Server: cm2 [10.1.10.232] Administration / Server (Maintenance) This Server: cm1 Time Zone Configuration NTP Configuration Server Upgrades Pre Update/Upgrade Step Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Security Administrator Accounts Login Account Policy Change Password Login Reports Server Access Server Log Files Firewall Install Root Certificate Trusted Certificates Server/Application Certificates Certificate Alarms Certificate Signing Request SSH Keys Web Access Mask Miscellaneous **Administrator Accounts** The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups. **Select Action:** ● Add Login ○ Privileged Administrator ○ Unprivileged Administrator ● SAT Access Only ○ Web Access Only ○ CDR Access Only ○ Business Partner Login (dadmin) ○ Business Partner Craft Login ○ Custom Login ○ Change Login Select Login ○ Remove Login Select Login ○ Lock/Unlock Login Select Login ○ Add Group ○ Remove Group Select Group

Step	Description
2.	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: - **Primary group**: **users** [Limits the permissions of the login] - **Additional groups (profile)**: **prof23** [Select the access-profile group created in **Section 5.2**. Ignore the warnings as SAT access is selected in Step 1.] - **Enter password / Re-enter password** [Define the password.] Click **Submit** to continue. This completes the configuration of the login.  AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Help Log Off Administration Duplicate Server: cm2 [10.1.10.232] Administration / Server (Maintenance) This Server: cm1 Software Version Server Configuration Server Role Network Configuration Duplication Parameters Static Routes Display Configuration Time Zone Configuration NTP Configuration Server Upgrades Pre Update/Upgrade Step Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Security Administrator Accounts Login Account Policy Change Password Login Reports Server Access Server Log Files Firewall Install Root Certificate Trusted Certificates Server/Application Certificates Certificate Alarms Certificate Signing Request SSH Keys Web Access Mask Miscellaneous File Synchronization Download Files CM Phone Message File **Administrator Accounts -- Add Login: SAT Access Only** This page allows you to create a login that is intended to have access only to the Communication Manager System Administration Terminal (SAT) interface. Login name: iptm Primary group: ● users ○ susers Additional groups (profile): prof23 You must assign a profile that has no web access if you want a login with SAT access only. Linux shell: /opt/ecs/bin/autosat This shell setting does NOT disable the "*go shell*" SAT command for this user. Home directory: /var/home/iptm Lock this account: □ SAT Limit: none Date after which account is disabled-blank to ignore (YYYY-MM-DD): Enter password: ••••••• Re-enter password: ••••••• Force password change on next login: ● No ○ Yes Submit Cancel Help © 2001-2017 Avaya Inc. All Rights Reserved.

5.4. Configure SNMP

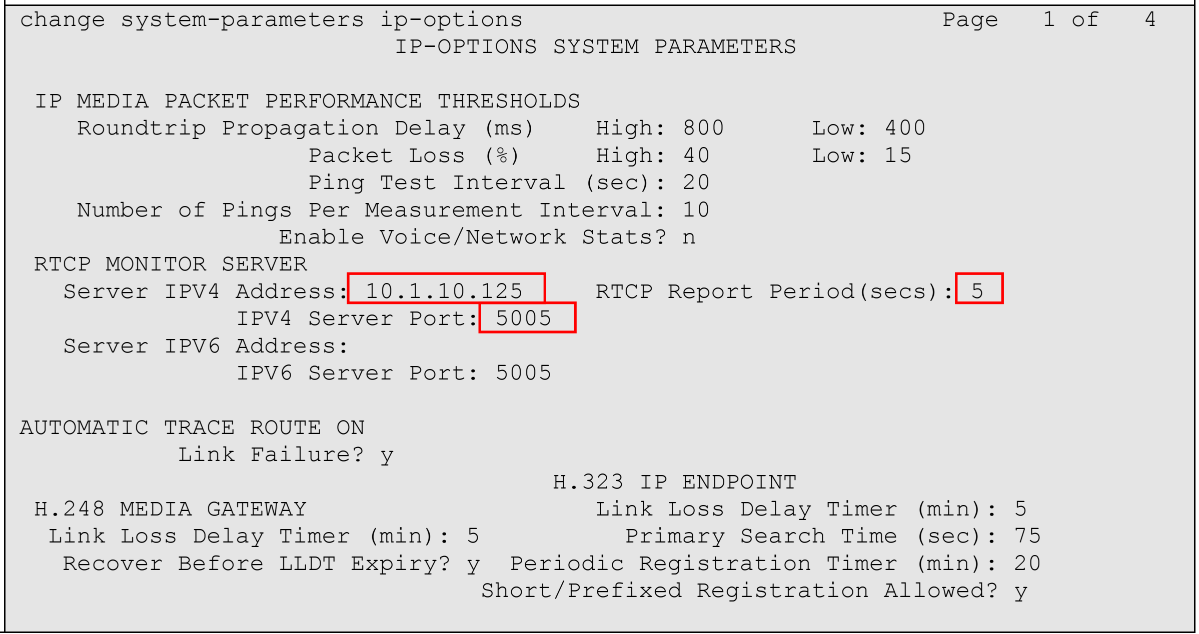
Step	Description
1.	Access the Communication Manager System Management Interface as in **Section 5.2 Step 1** and **2**. Click on **SNMP → Agent Status**. Click **Stop the Master Agent** if the **Master Agent status** is *UP* to allow setup of SNMP Agent.  AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Help Log Off Administration Duplicate Server: cm2 [10.1.10.232] Administration / Server (Maintenance) This Server: cm1 Alarms Current Alarms SNMP Agent Status Access Incoming Traps FP Traps FP Trap Test FP Filters Diagnostics Restarts System Logs Ping Traceroute Netstat Server Status Summary Process Status Interchange Servers Busy-Out/Release Server Shutdown Server Server Date/Time Software Version Stop Master Agent Help **Agent Status** The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent. All of the Sub Agents are connected to the Master Agent. Master Agent status: UP **Sub Agent Status** FP Agent status: UP CMSubAgent status: UP Load Agent status: UP

Step	Description
2.	To allow Prognosis to use SNMP to collect configuration and status information from Communication Manager, navigate to **SNMP → Access** in the left pane. Click **Add/Change** button (not shown). Configure the **SNMP Version 2c** section. Set the **IP address** to the Prognosis server and **Access** as **read-only** from the drop menu. Set also the **Community Name** field to say **avaya123**. Click **Submit** at the bottom of the web page.  AVAYA Help Log Off Administration Alarms Current Alarms SNMP Agent Status Access Incoming Traps FP Traps FP Trap Test FP Filters Diagnostics Restarts System Logs Ping Traceroute Netstat Server Status Summary Process Status Interchange Servers Busy-Out/Release Server Shutdown Server Server Date/Time Software Version Server Configuration Server Role Network Configuration Duplication Parameters Static Routes Display Configuration Time Zone Configuration NTP Configuration Server Upgrades Pre Update/Upgrade Step Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Submit Cancel Help Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Duplicate Server: **cm2 [10.1.10.232]** Administration / Server (Maintenance) This Server: **cm1** **Access** The Access SMI page is used to configure SNMP access to CM. **SNMP Version 2c** IP address: 10.1.10.125 Access: read-only Community Name: avaya123 **Add SNMP Users / Communities** **SNMP Version 1** IP address: Access: Community Name: **SNMP Version 2c** IP address: Access: Community Name: **SNMP Version 3** Access: User Name: Authentication Protocol: Authentication Password: Minimum 8 characters. (for authentication and privacy) Privacy Protocol: Privacy Password: Minimum 8 characters. (for privacy)

Step	Description
3.	Lastly, the SNMP agent must be started. Navigate to **SNMP → Agent Status**. If the **Master Agent status** is *DOWN***,** then click the **Start Master Agent** button. If the **Master Agent status** is *UP*, then the agent must be stopped and restarted.  AVAYA Avaya Aura® Communication Manager (CM) System Management Interface (SMI) Help Log Off Administration Duplicate Server: cm2 [10.1.10.232] Administration / Server (Maintenance) This Server: cm1 Alarms Current Alarms SNMP Agent Status Access Incoming Traps FP Traps FP Trap Test FP Filters Diagnostics Restarts System Logs Ping Traceroute Netstat Server Status Summary Process Status Interchange Servers Busy-Out/Release Server Shutdown Server Server Date/Time Start Master Agent Help **Agent Status** The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent. Sub Agents are NOT connected to the Master Agent. Master Agent status: DOWN **Sub Agent Status** FP Agent status: UP CMSubAgent status: UP Load Agent status: UP

5.5. Configure RTCP Monitoring

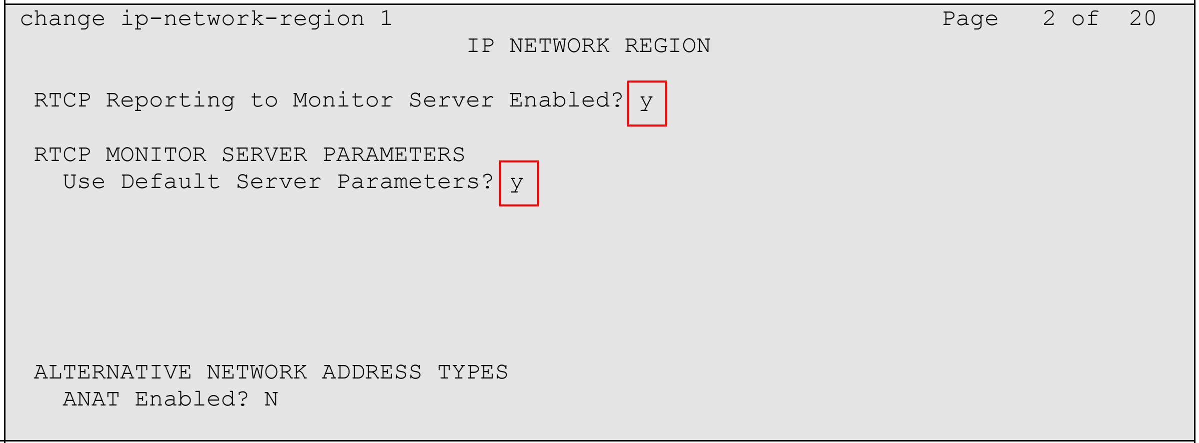
To allow Prognosis to monitor the quality of H.323 IP calls, configure Communication Manager to send RTCP reporting to the IP address of the Prognosis server. This is done through the SAT interface. But for Avaya SIP endpoints, refer to the reference **[3]** in Section 9.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>Enter the <b>change system-parameters ip-options</b> command. In the <b>RTCP MONITOR SERVER</b> section, set <b>Server IPV4 Address</b> to the IP address of the Prognosis server. Set <b>IPV4 Server Port</b> to <b><i>5005</i></b> and <b>RTCP Report Period (secs)</b> to <b><i>5</i></b>.

<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: 10.1.10.125   RTCP Report Period(secs): 5
               IPV4 Server Port: 5005
   Server IPV6 Address:
               IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                     H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY   Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5   Primary Search Time (sec): 75
   Recover Before LLDT Expiry? y Periodic Registration Timer (min): 20
                                Short/Prefixed Registration Allowed? y
</pre></td></tr>
</table>

Step	Description

2.	Enter the **change ip-network-region *n*** command, where ***n*** is IP network region number to be monitored. On Page 2, set **RTCP Reporting to Monitor Server Enabled** to ***y*** and **Use Default Server Parameters** to ***y***.
	
	Note: Only one RTCP MONITOR SERVER can be configured per IP network region.
	
	`change ip-network-region 1                                   Page   2 of  20`
	`                              IP NETWORK REGION`
	
	` RTCP Reporting to Monitor Server Enabled? y`
	
	` RTCP MONITOR SERVER PARAMETERS`
	`   Use Default Server Parameters? y`
	
	` ALTERNATIVE NETWORK ADDRESS TYPES`
	`   ANAT Enabled? N`

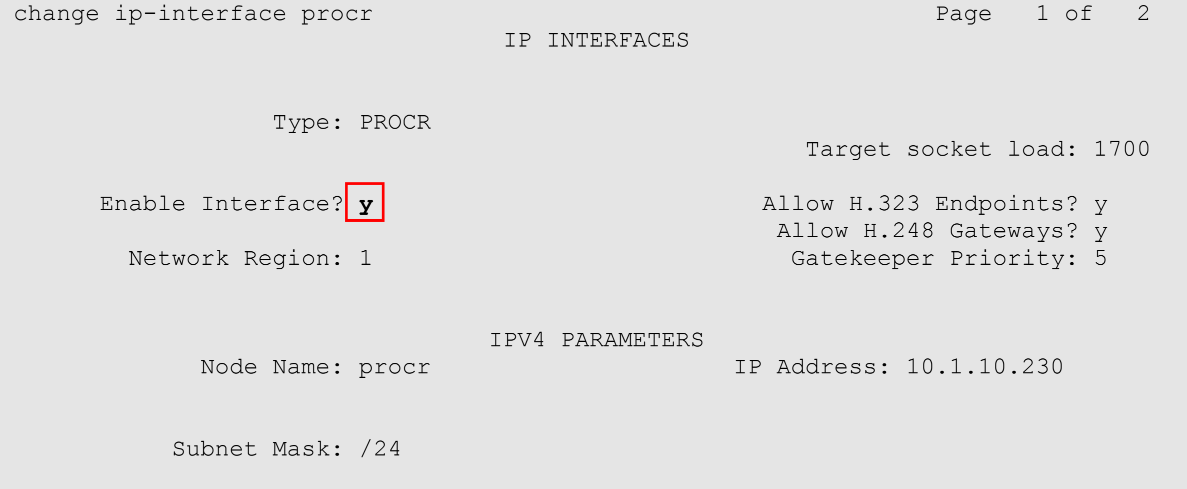
3.	Repeat **Step 2** for all IP network regions that are required to be monitored.

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.

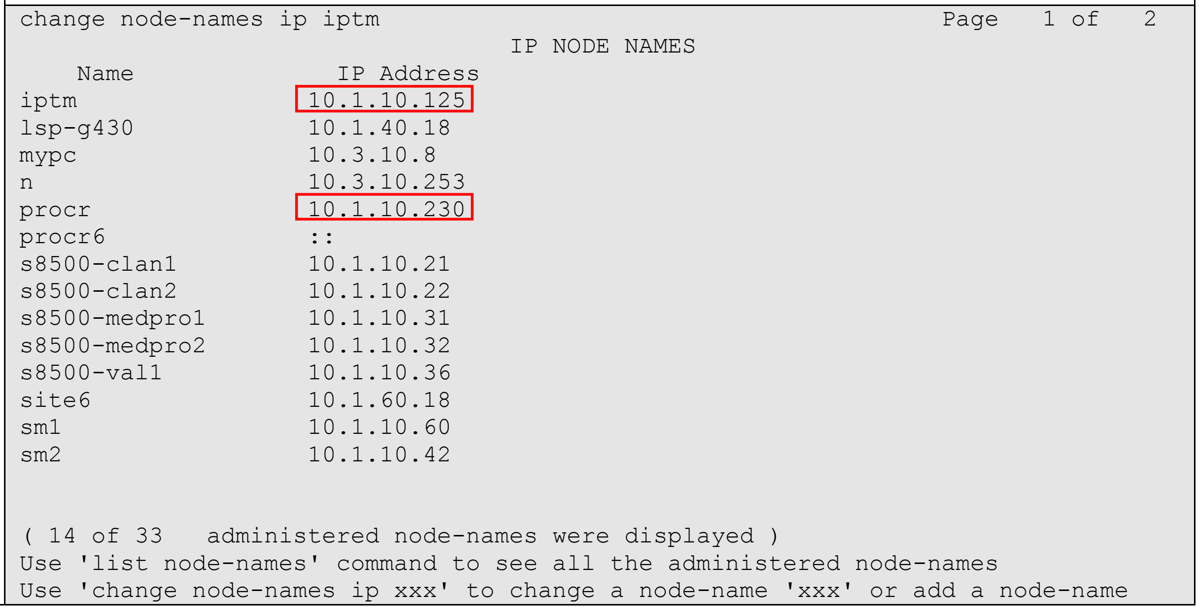
Step **Description**

1. Enter the **change ip-interface procr** command to enable the processor-ethernet interface on Communication Manager. Set **Enable Interface** to **y**. This interface will be used by Communication Manager to send out the CDR information.



```
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
```

2. Enter the **change node-names ip iptm** 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 **10.1.10.125**. Note also the node name **procr** which is automatically added.

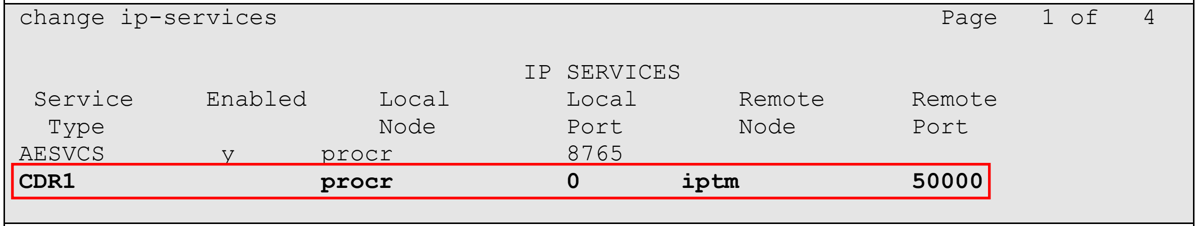


```
change node-names ip iptm                                       Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
iptm                    10.1.10.125
lsp-g430                10.1.40.18
mypc                    10.3.10.8
n                       10.3.10.253
procr                   10.1.10.230
procr6                  ::
s8500-clan1             10.1.10.21
s8500-clan2             10.1.10.22
s8500-medpro1           10.1.10.31
s8500-medpro2           10.1.10.32
s8500-val1              10.1.10.36
site6                   10.1.60.18
sm1                     10.1.10.60
sm2                     10.1.10.42


( 14 of 33   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
```

Step **Description**

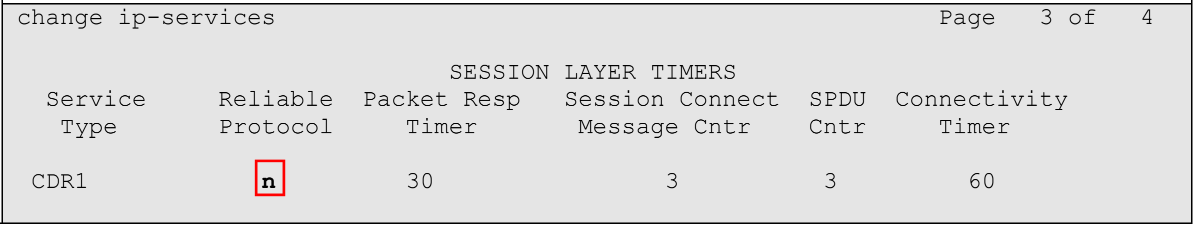
3. Enter the **change ip-services** command to define the CDR link. To define a primary CDR link, the following information should be provided:

- **Service Type: CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node: procr** [Communication Manager will use the processor-ethernet interface to send out the CDR. CLAN node could also be used.]
- **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 inclusively. **50000** is the default port number used by Prognosis. Note that Prognosis server uses the same port number for CDR integration with all Communication Manager systems.]



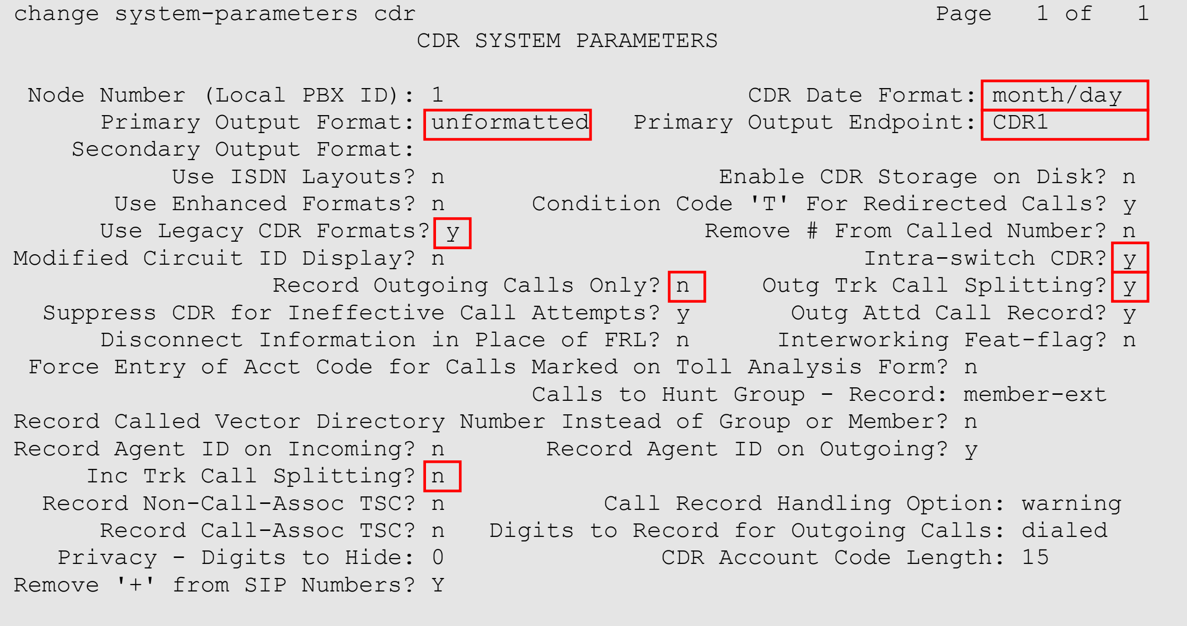
```
change ip-services                                             Page   1 of   4

                                    IP SERVICES
 Service      Enabled      Local        Local        Remote       Remote
  Type                     Node         Port         Node         Port
AESVCS          y      procr            8765
CDR1                   procr            0        iptm             50000
```

On Page 3 of the form, disabled the Reliable Session Protocol (RSP) for the CDR link by setting the **Reliable Protocol** field to **n**.



```
change ip-services                                             Page   3 of   4

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

 CDR1             n         30                3           3        60
```

Step	Description
4.	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. • **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** 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. • **Use Legacy CDR Formats? y** [Specify the use of 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.]



```
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? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? y
      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
Remove '+' from SIP Numbers? Y
```

Step **Description**

5. If the **Intra-switch CDR** field is set to **y** on Page 1 of the CDR SYSTEM PARAMETERS form, then enter the **change intra-switch-cdr** command to define the extensions that will be subjected to call detail recording. In the **Extension** column, enter the specific extensions whose usage will be tracked with the CDR records.

```
change intra-switch-cdr                                         Page   1 of   3
                           INTRA-SWITCH CDR

                                Assigned Members:   4    of 5000   administered
   Extension          Extension          Extension          Extension
   10001
   10002
   10005
   10007



Use 'list intra-switch-cdr' to see all members, 'add intra-switch-cdr' to add
new members and 'change intra-switch-cdr <ext>' to change/remove other members
```

6. 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.

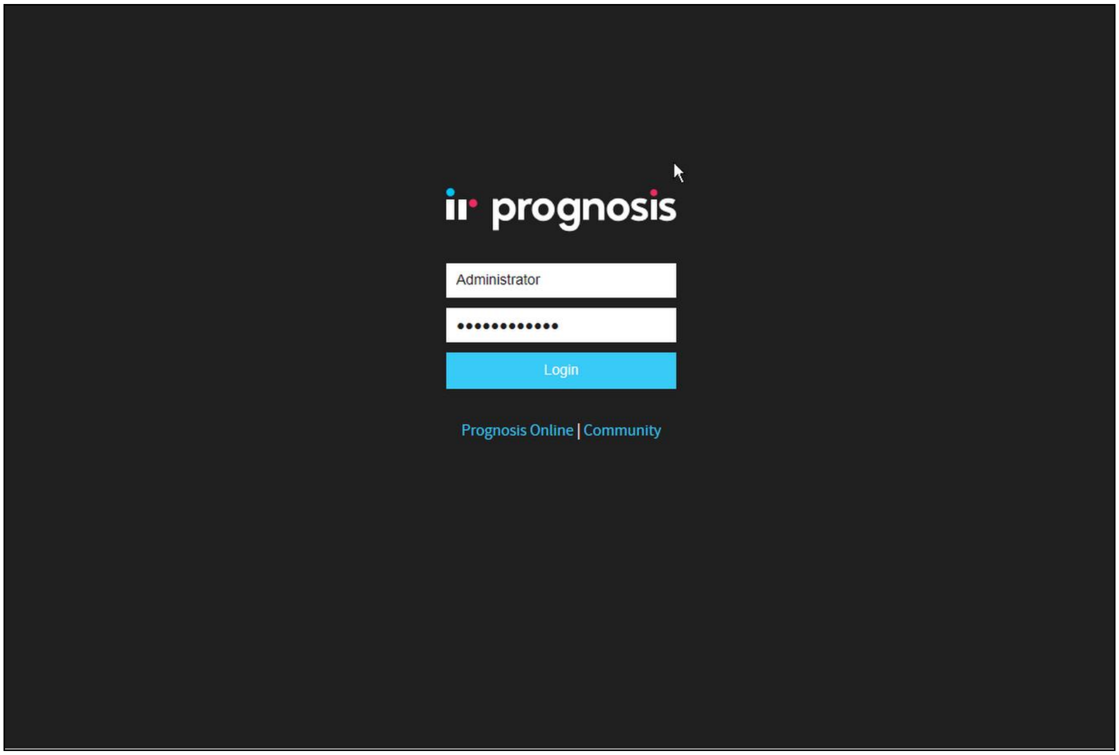
```
change trunk-group 7                                            Page   1 of  21
                                TRUNK GROUP

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
```

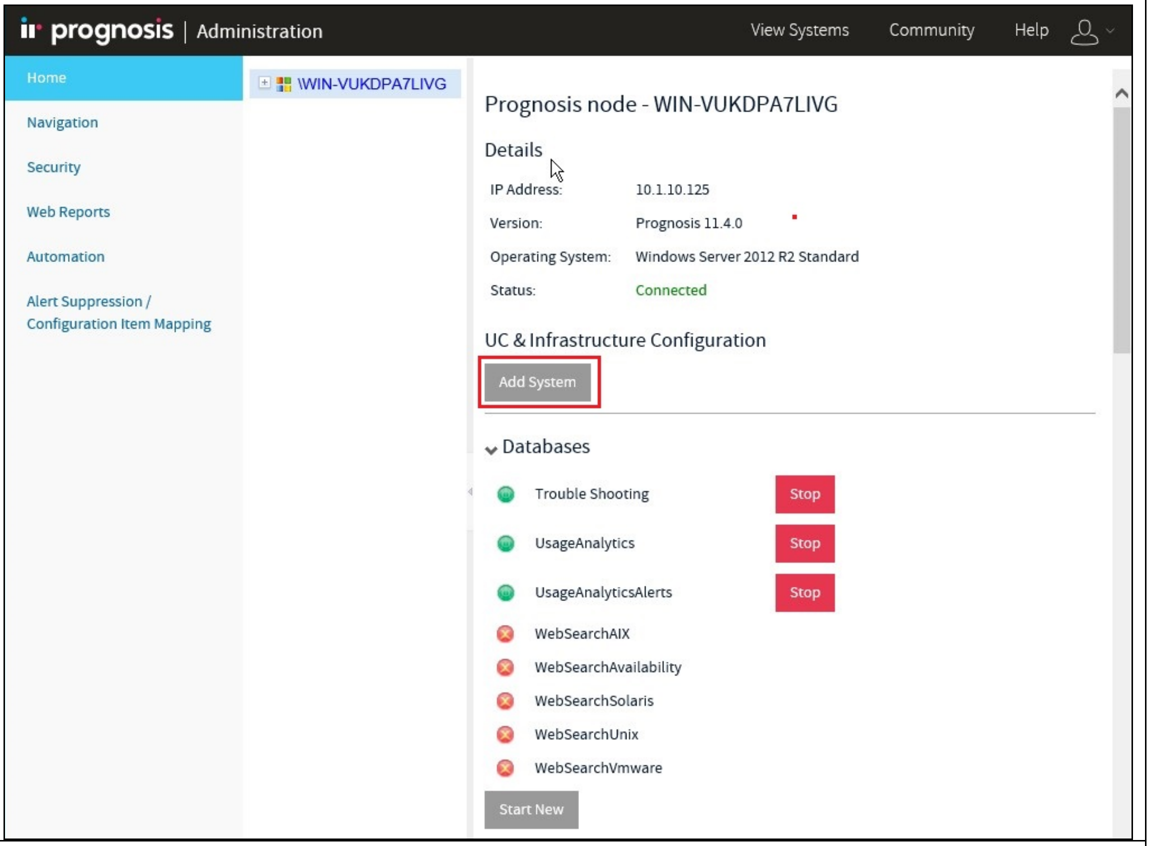
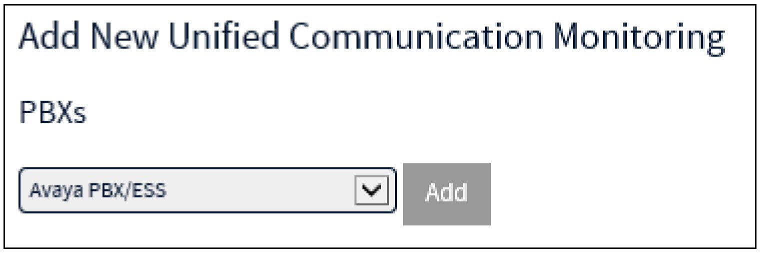
7. Enter **save translation** to save the changes made.

```
save translation

                               SAVE TRANSLATION

           Command Completion Status                                 Error Code

           Success                                                   0
```

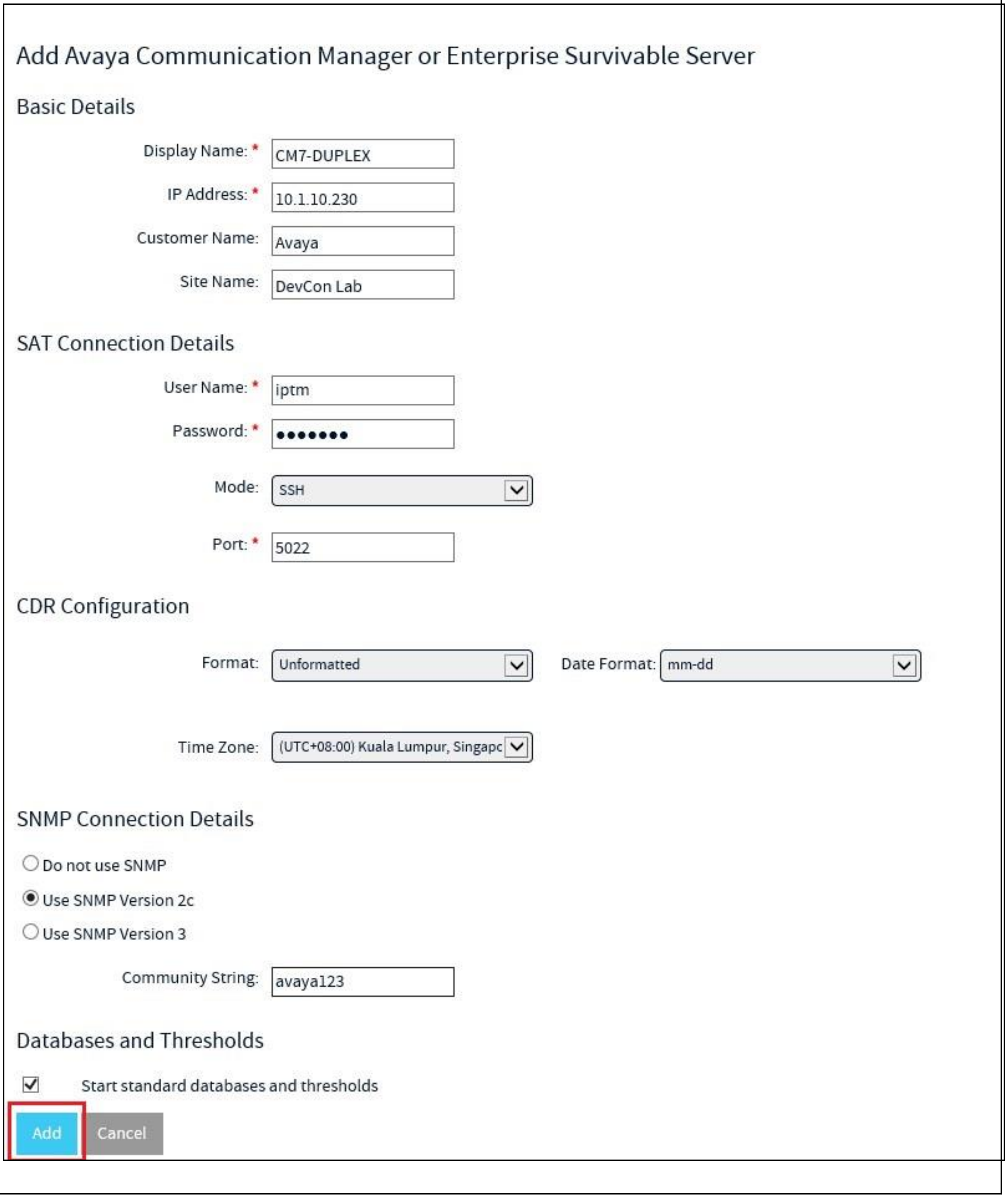
6. Configure Integrated Research Prognosis

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 [3]** and will not be detailed here.

Step	Description
1.	Log into the Prognosis server with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Administration**. Login with the appropriate password.  Administrator ••••••••••••

Step	Description
2.	Click **Add System**.  Prognosis node - WIN-VUKDPA7LIVG Details IP Address: 10.1.10.125 Version: Prognosis 11.4.0 Operating System: Windows Server 2012 R2 Standard Status: Connected UC & Infrastructure Configuration Databases Trouble Shooting Stop UsageAnalytics Stop UsageAnalyticsAlerts Stop WebSearchAIX WebSearchAvailability WebSearchSolaris WebSearchUnix WebSearchVmware prognosis | Administration View Systems Community Help Home Navigation Security Web Reports Automation Alert Suppression / Configuration Item Mapping \WIN-VUKDPA7LIVG Add System Start New
3.	Select **Avaya PBX/ESS** from drop-down menu. Click **Add** to add a new Avaya PBX.  Add New Unified Communication Monitoring PBXs Avaya PBX/ESS

Step	Description
4.	In this test configuration, the following entries are added for the two Communication Manager systems with display name of **CM7-DUPLEX** (System A) and **G450-CM** (System B) and with IP addresses of **10.1.10.230** and **10.1.60.18** respectively. The display name is matched with the naming of these systems on the System Manager SIP Entities. The following settings were used during the compliance test (see **next page**). **Basic Details:** • **Display Name: CM7-DUPLEX** • **IP address: 10.1.10.230** • **Customer Name: Avaya** • **Site Name: DevCon Lab** **SAT Connection Details:** • **User Name/Password: iptm/**[As configured in **Section 5.3 Step 2**] • **Mode: SSH** • **Port: 5022** **CDR Configuration:** • **Format: unformatted [**as configured in **Section 5.6 Step 4]** • **Date Format: mm-dd [**as configured in **Section 5.6 Step 4]** **SNMP Connection Details:** • Select **Use SNMP Version 2c** • **Community String:** As configured in **Section 5.4 Step 2** Leave the **Databases and Thresholds** as checked**.** Click **Add** to affect the addition**.** Repeat the above for the setup of **G450-CM**.

Step	Description
	

Add Avaya Communication Manager or Enterprise Survivable Server

Basic Details

Display Name: *	CM7-DUPLEX
IP Address: *	10.1.10.230
Customer Name:	Avaya
Site Name:	DevCon Lab

SAT Connection Details

User Name: *	iptm
Password: *	●●●●●●●
Mode:	SSH
Port: *	5022

CDR Configuration

Format:	Unformatted	Date Format:	mm-dd
Time Zone:	(UTC+08:00) Kuala Lumpur, Singapc		

SNMP Connection Details

○ Do not use SNMP

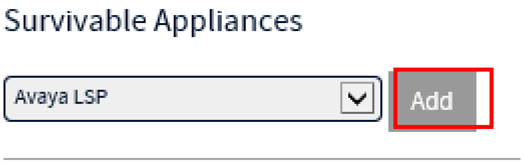
● Use SNMP Version 2c

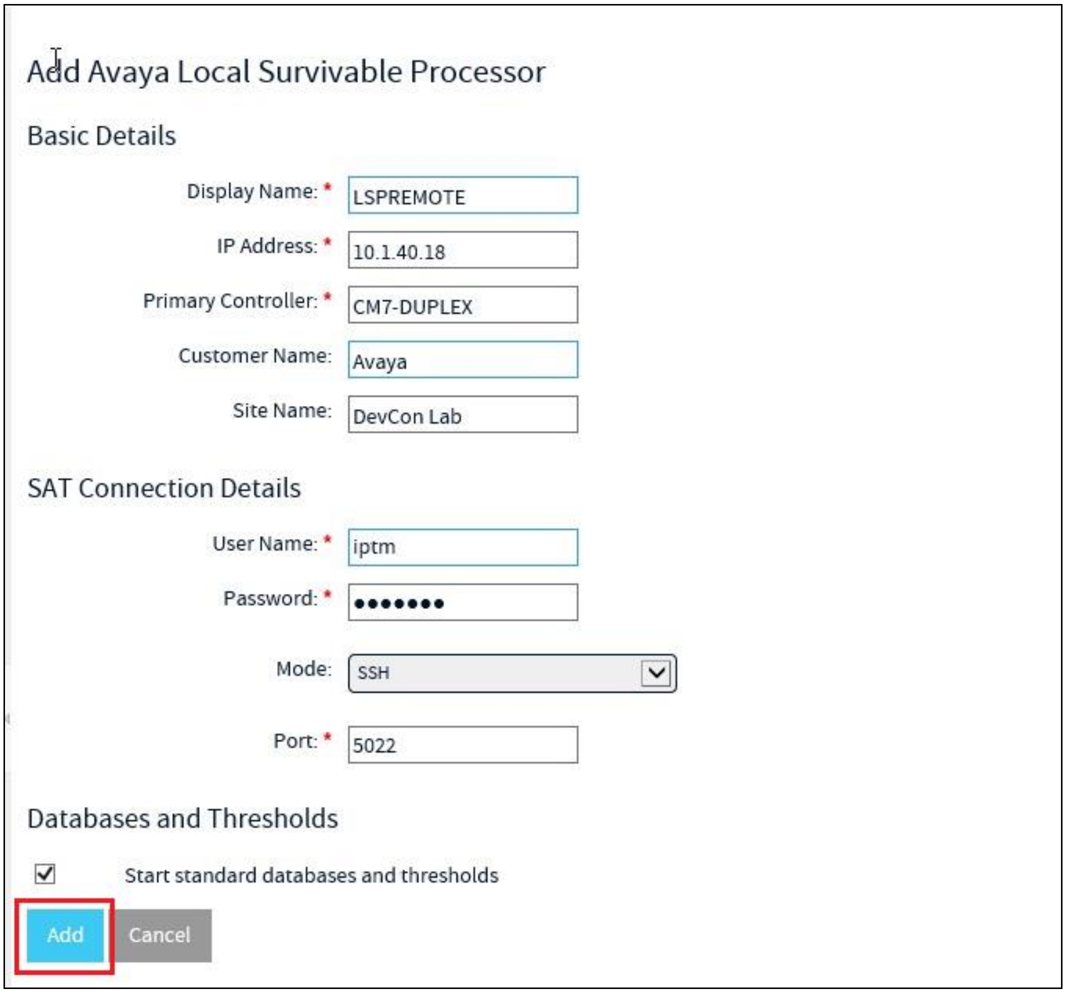
○ Use SNMP Version 3

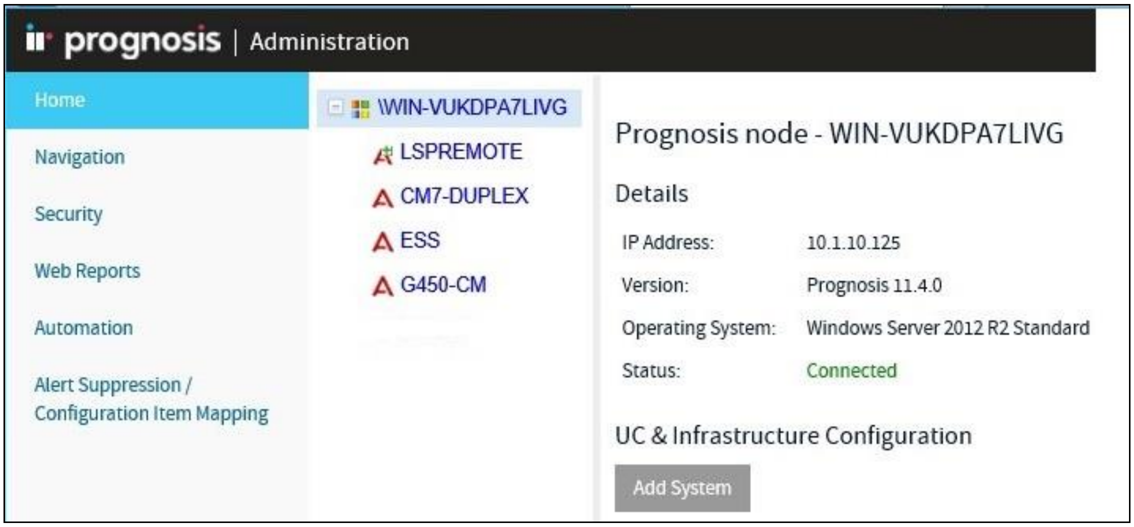
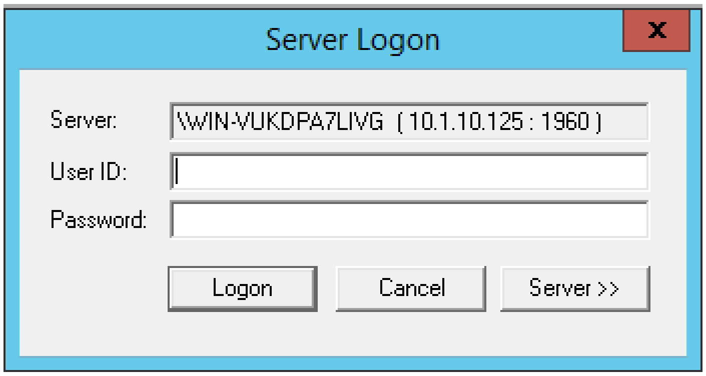
Community String: avaya123

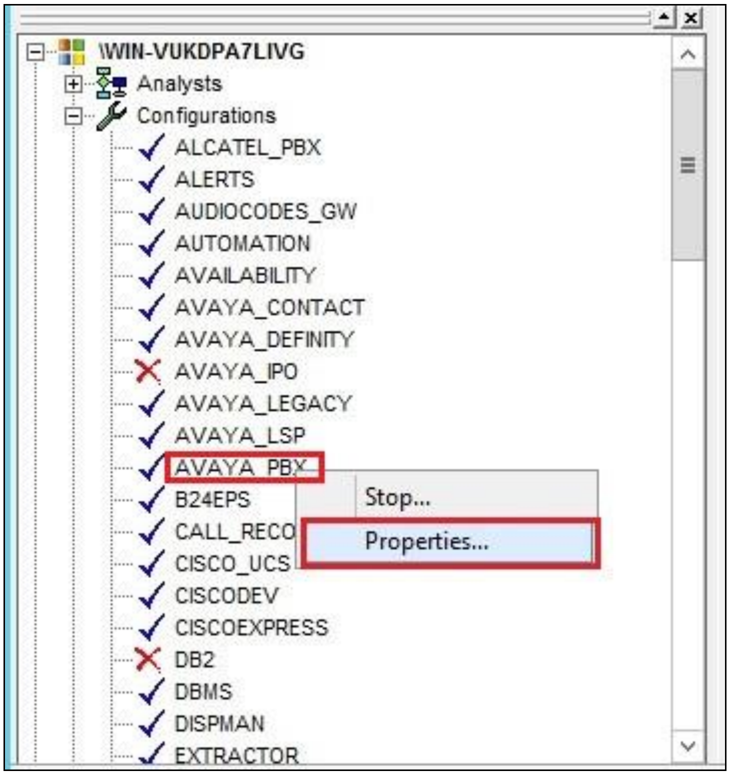
Databases and Thresholds

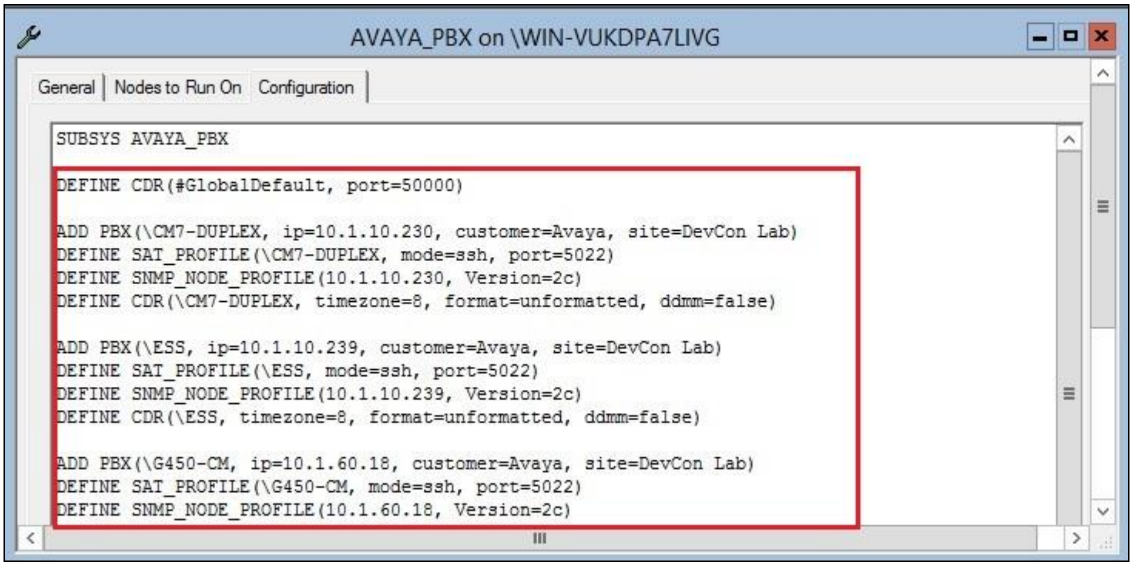
☑ Start standard databases and thresholds

Step	Description
5.	In this test configuration, the LSP and ESS servers with names of **LSPREMOTE** and **ESS** and IP addresses of **10.1.40.18** and **10.1.10.239** respectively, both belonging to the **CM7-DUPLEX** Communication Manager system are also configured. Repeat **Step 2** to add a new system and select **Add** to add a new **Avaya LSP**.  Survivable Appliances Avaya LSP Add

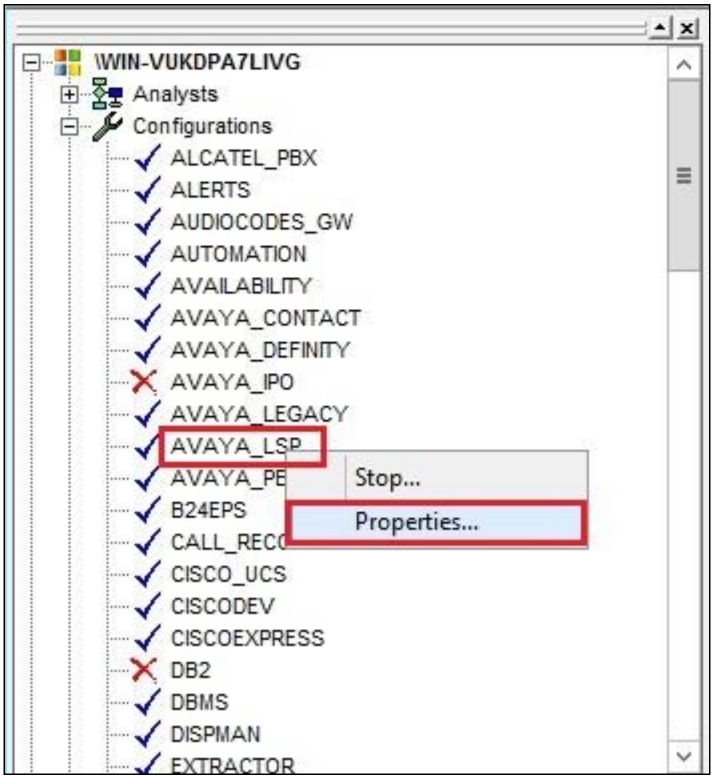
Step	Description
6.	The following settings were used during the compliance test. **Basic Details:** • **Display Name: LSPREMOTE** • **IP address: 10.1.40.18** • **Primary Controller: CM7-DUPLEX** • **Customer Name: Avaya** • **Site Name: DevCon Lab** **SAT Connection Details:** • **User/Password: iptm** [As configured in **Section 5.3 Step 2**] • **Mode: SSH** • **Port: 5022** Leave the **Databases and Thresholds** as checked**.** Click **Add** to affect the addition**.** Repeat the above for the setup of **ESS.**  Add Avaya Local Survivable Processor Basic Details Display Name: * LSPREMOTE IP Address: * 10.1.40.18 Primary Controller: * CM7-DUPLEX Customer Name: Avaya Site Name: DevCon Lab SAT Connection Details User Name: * iptm Password: * ••••••• Mode: SSH Port: * 5022 Databases and Thresholds ☑ Start standard databases and thresholds

Step	Description
7.	Below is the result of the additions of the two Communication Manager systems plus the LSP and ESS.  prognosis | Administration Home Navigation Security Web Reports Automation Alert Suppression / Configuration Item Mapping WIN-VUKDPA7LIVG LSPREMOTE CM7-DUPLEX ESS G450-CM Add System Prognosis node - WIN-VUKDPA7LIVG Details IP Address: 10.1.10.125 Version: Prognosis 11.4.0 Operating System: Windows Server 2012 R2 Standard Status: Connected UC & Infrastructure Configuration
8.	On Prognosis server, click **Start → All Programs → Prognosis → Prognosis Client** to start the Windows Client application. Log in with the appropriate credentials.  Server Logon Server: \WIN-VUKDPA7LIVG (10.1.10.125 : 1960) User ID: Password:

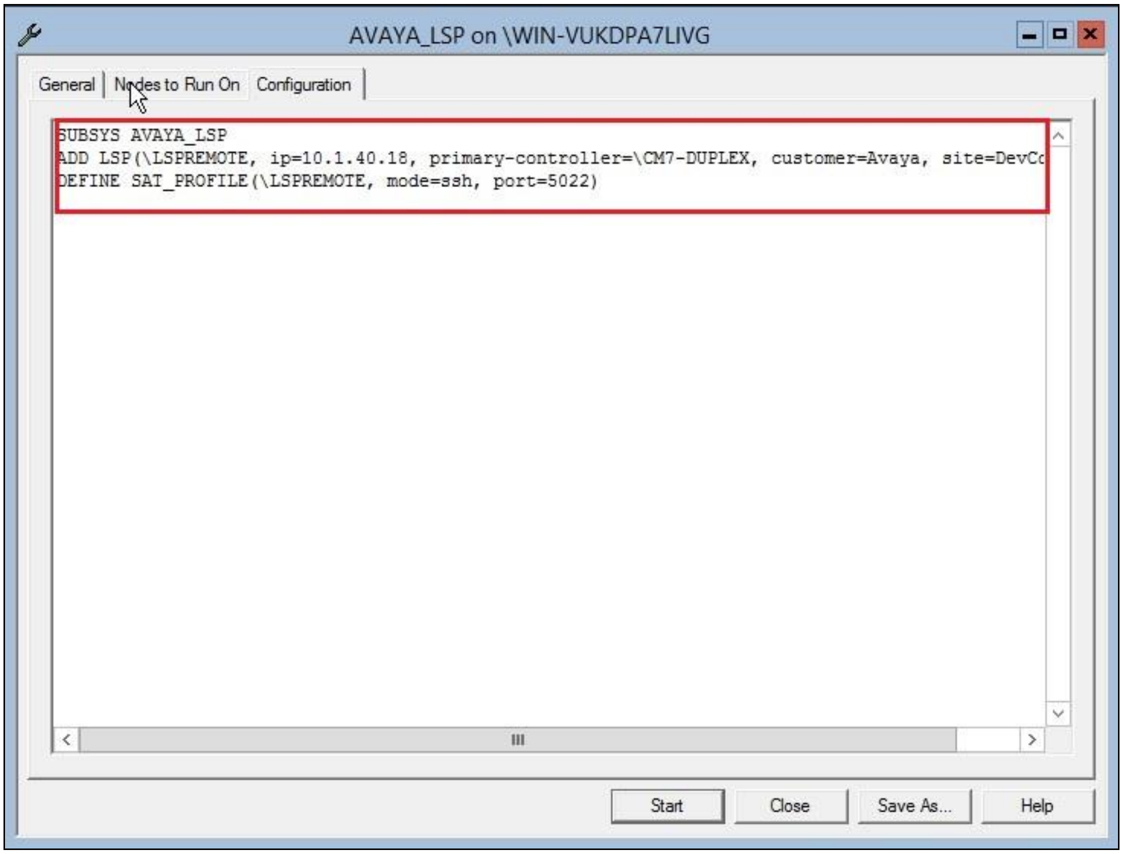
Step	Description
9.	To check the configurations of the Avaya PBX/ESS to be monitored, expand **Configurations** of the Monitoring Node, right-click on **AVAYA_PBX** and select **Properties**.  \WIN-VUKDPA7LIVG Analysts Configurations ALCATEL_PBX ALERTS AUDIOCODES_GW AUTOMATION AVAILABILITY AVAYA_CONTACT AVAYA_DEFINITY AVAYA_IPO AVAYA_LEGACY AVAYA_LSP AVAYA_PBX B24EPS CALL_RECO CISCO_UCS CISCODEV CISCOEXPRESS DB2 DBMS DISPMAN EXTRACTOR Stop... Properties...

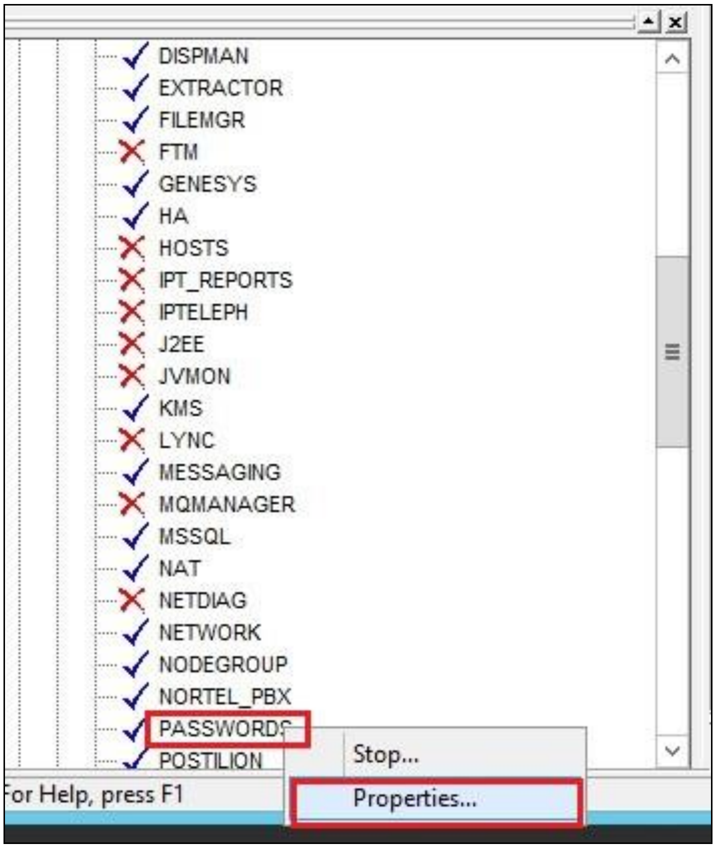
Step	Description
10.	Check the configurations for each Communication Manager and the corresponding CDR settings as configured in **Step 4** earlier. Note that the default CDR port is 50000 which correspond to the configurations set in **Section 5.6 Step 3** is already created as default. 

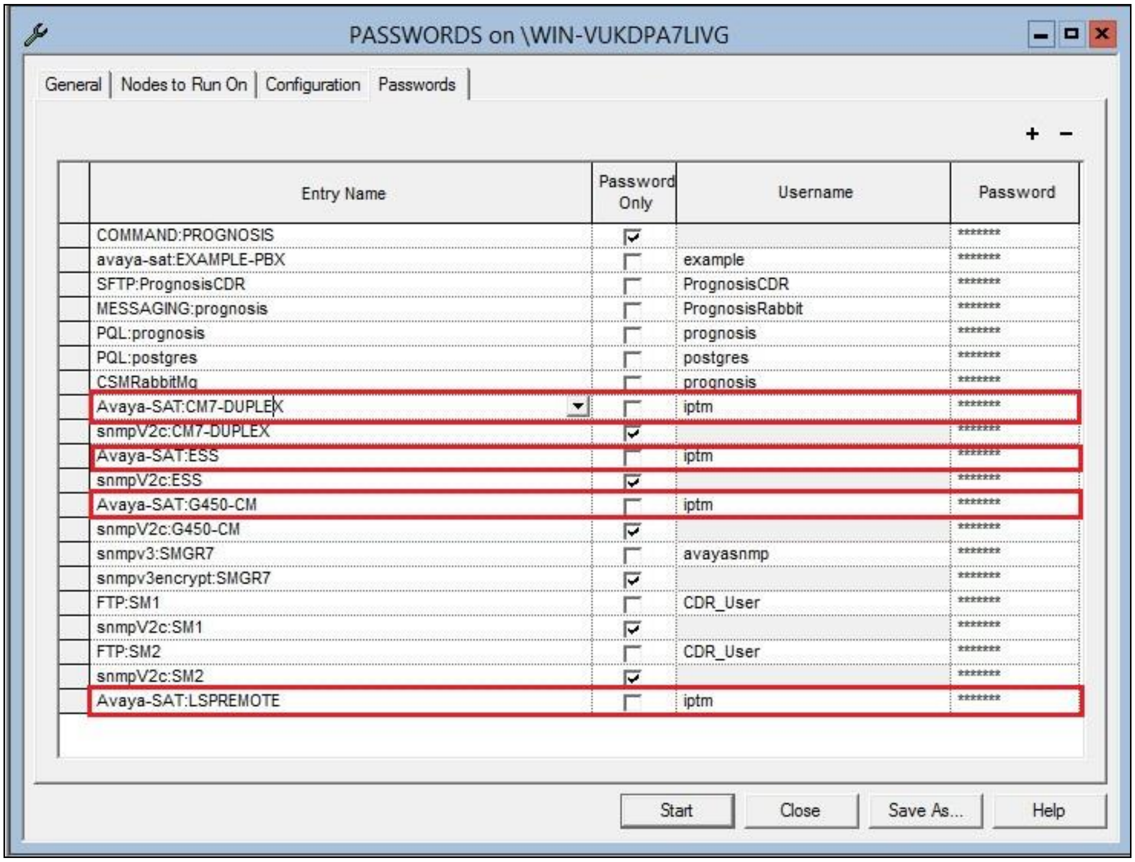
```
SUBSYS AVAYA_PBX

DEFINE CDR(#GlobalDefault, port=50000)

ADD PBX(\CM7-DUPLEX, ip=10.1.10.230, customer=Avaya, site=DevCon Lab)
DEFINE SAT_PROFILE(\CM7-DUPLEX, mode=ssh, port=5022)
DEFINE SNMP_NODE_PROFILE(10.1.10.230, Version=2c)
DEFINE CDR(\CM7-DUPLEX, timezone=8, format=unformatted, ddmm=false)

ADD PBX(\ESS, ip=10.1.10.239, customer=Avaya, site=DevCon Lab)
DEFINE SAT_PROFILE(\ESS, mode=ssh, port=5022)
DEFINE SNMP_NODE_PROFILE(10.1.10.239, Version=2c)
DEFINE CDR(\ESS, timezone=8, format=unformatted, ddmm=false)

ADD PBX(\G450-CM, ip=10.1.60.18, customer=Avaya, site=DevCon Lab)
DEFINE SAT_PROFILE(\G450-CM, mode=ssh, port=5022)
DEFINE SNMP_NODE_PROFILE(10.1.60.18, Version=2c)
```

Step	Description
11.	To check the configurations of the LSP server to be monitored, expand **Configurations** of the Monitoring Node, right-click on **AVAYA_LSP** and select **Properties**.  \WIN-VUKDPA7LIVG Analysts Configurations ALCATEL_PBX ALERTS AUDIOCODES_GW AUTOMATION AVAILABILITY AVAYA_CONTACT AVAYA_DEFINITY AVAYA_IPO AVAYA_LEGACY AVAYA_LSP AVAYA_PE B24EPS CALL_RECO CISCO_UCS CISCODEV CISCOEXPRESS DB2 DBMS DISPMAN EXTRACTOR Stop... Properties...

Step	Description

12.	Check the configurations for LSP server to be monitored as configured in **Step 6** earlier.
	
	 AVAYA_LSP on \WIN-VUKDPA7LIVG
	General
	Nodes to Run On
	Configuration
	Start
	Close
	Save As...
	Help
	`SUBSYS AVAYA_LSP`
	`ADD LSP(\LSPREMOTE, ip=10.1.40.18, primary-controller=\CM7-DUPLEX, customer=Avaya, site=DevC`
	`DEFINE SAT_PROFILE(\LSPREMOTE, mode=ssh, port=5022)`

Step	Description
13.	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**.  DISPMAN EXTRACTOR FILEMGR FTM GENESYS HA HOSTS IPT_REPORTS IPTELEPH J2EE JVMON KMS LYNC MESSAGING MQMANAGER MSSQL NAT NETDIAG NETWORK NODEGROUP NORTEL_PBX PASSWORDS POSTILION Stop... Properties... For Help, press F1

Step	Description
14.	The four Communication Manager entries **CM7-DUPLEX**, **G450-CM, LSPREMOTE** and **ESS** are listed below. 

PASSWORDS on \WIN-VUKDPA7LIVG

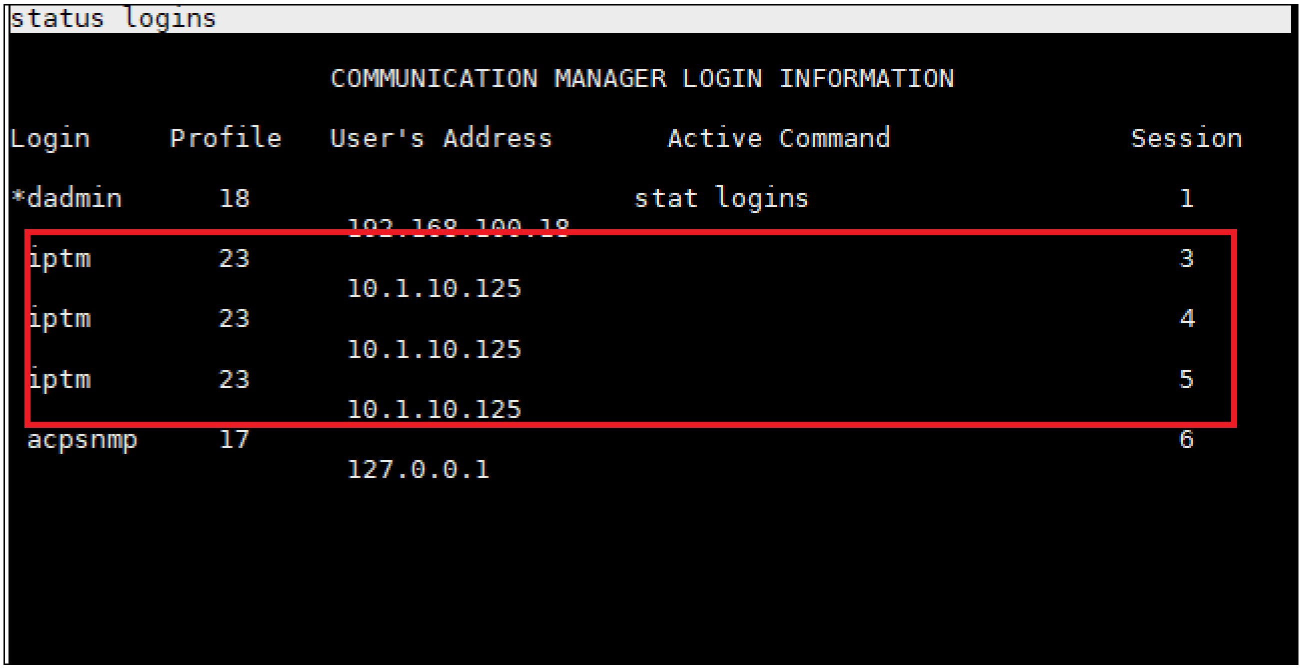
Entry Name	Password Only	Username	Password
COMMAND:PROGNOSIS	☑		*******
avaya-sat:EXAMPLE-PBX	☐	example	*******
SFTP:PrognosisCDR	☐	PrognosisCDR	*******
MESSAGING:prognosis	☐	PrognosisRabbit	*******
PQL:prognosis	☐	prognosis	*******
PQL:postgres	☐	postgres	*******
CSMRabbitMq	☐	prognosis	*******
Avaya-SAT:CM7-DUPLEX	☐	iptm	*******
snmpV2c:CM7-DUPLEX	☑		*******
Avaya-SAT:ESS	☐	iptm	*******
snmpV2c:ESS	☑		*******
Avaya-SAT:G450-CM	☐	iptm	*******
snmpV2c:G450-CM	☑		*******
snmpv3:SMGR7	☐	avayasnmp	*******
snmpv3encrypt:SMGR7	☑		*******
FTP:SM1	☐	CDR_User	*******
snmpV2c:SM1	☑		*******
FTP:SM2	☐	CDR_User	*******
snmpV2c:SM2	☑		*******
Avaya-SAT:LSPREMOTE	☐	iptm	*******

7. Verification Steps

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

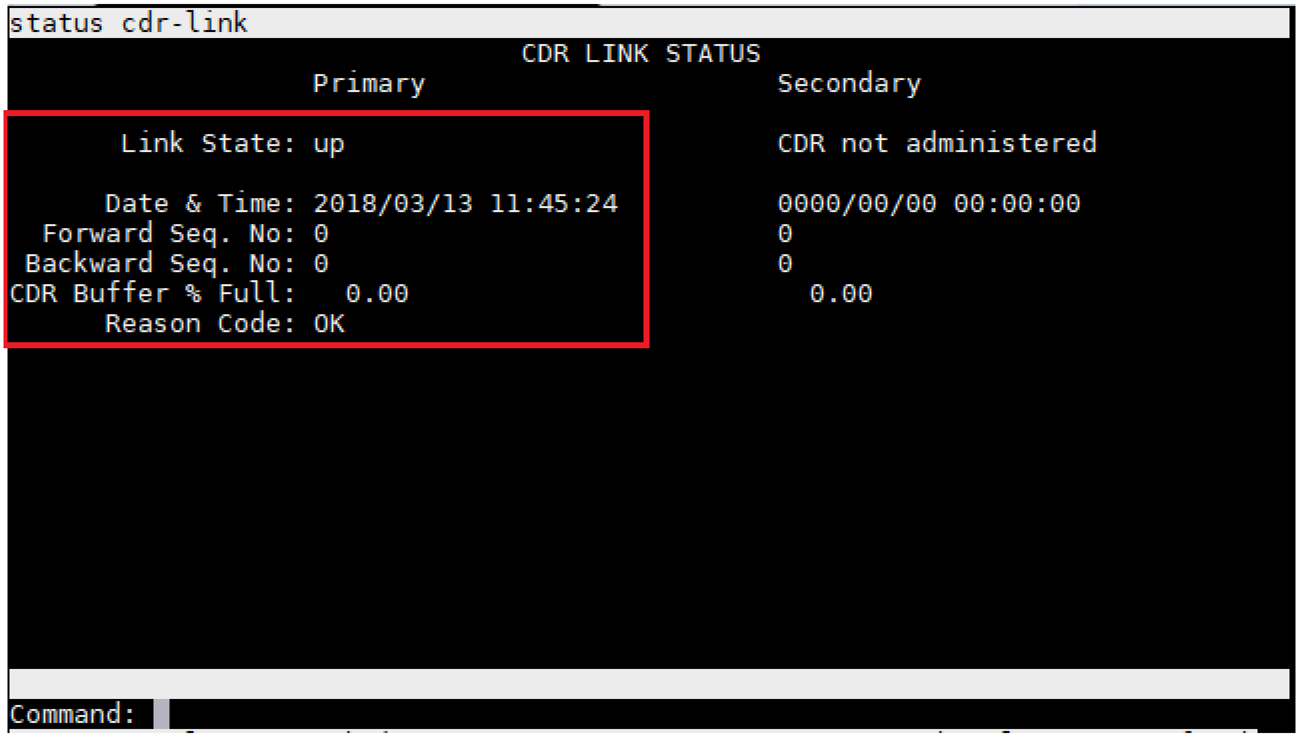
7.1. Verify Communication Manager

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

*dadmin      18                        stat logins                        1
                     192.168.100.18
 iptm        23                                                           3
                     10.1.10.125
 iptm        23                                                           4
                     10.1.10.125
 iptm        23                                                           5
                     10.1.10.125
 acpsnmp     17                                                           6
                     127.0.0.1
```

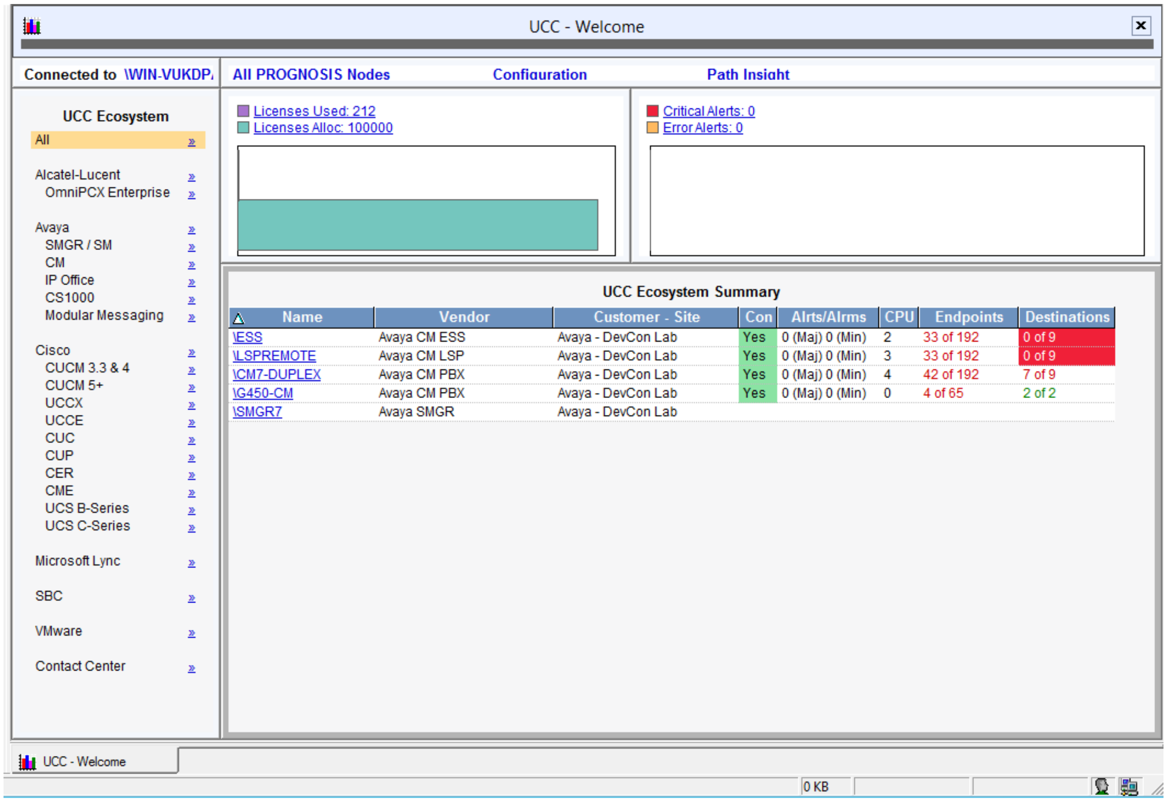
Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.6** shows **up**.



```
status cdr-link
                                 CDR LINK STATUS
                   Primary                        Secondary

       Link State: up                             CDR not administered

      Date & Time: 2018/03/13 11:45:24            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

Command:
```

7.2. Verify Prognosis

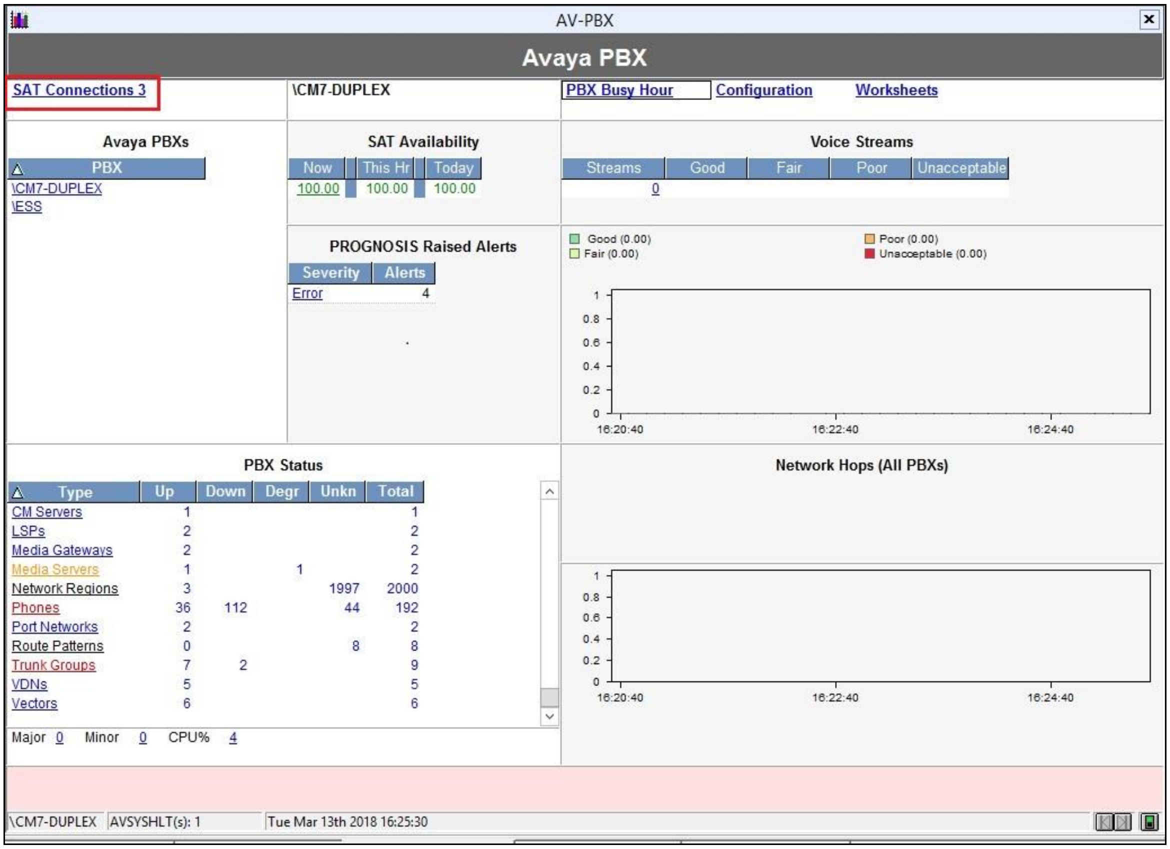
This section provides the tests that can be performed to verify proper configuration of Prognosis. The following steps are done by accessing the Prognosis webui.

Step	Description
1.	After logging into Prognosis webui and selecting the home screen icon above, the list of Communication Manager servers configured in **Section 6** is displayed on the right pane under **UC Ecosystem Summary**. 

Licenses Used: 212
Licenses Alloc: 100000
Critical Alerts: 0
Error Alerts: 0

UCC Ecosystem Summary

Name	Vendor	Customer - Site	Con	Alrts/Alrms	CPU	Endpoints	Destinations
\ESS	Avaya CM ESS	Avaya - DevCon Lab	Yes	0 (Maj) 0 (Min)	2	33 of 192	0 of 9
\LSPREMOTE	Avaya CM LSP	Avaya - DevCon Lab	Yes	0 (Maj) 0 (Min)	3	33 of 192	0 of 9
\CM7-DUPLEX	Avaya CM PBX	Avaya - DevCon Lab	Yes	0 (Maj) 0 (Min)	4	42 of 192	7 of 9
\G450-CM	Avaya CM PBX	Avaya - DevCon Lab	Yes	0 (Maj) 0 (Min)	0	4 of 65	2 of 2
\SMGR7	Avaya SMGR	Avaya - DevCon Lab					

Step	Description
2.	Select any of the PBX, verify that the **SAT Connections** field for each configured Communication Manager shows **3** connections. However, the number of SAT connections can be changed to 1 or 2. The instruction is found in the user guide in the software package installed. 

AV-PBX

Avaya PBX

SAT Connections 3 | \CM7-DUPLEX | PBX Busy Hour | Configuration | Worksheets

Avaya PBXs

PBX
\CM7-DUPLEX
\ESS

SAT Availability

Now	This Hr	Today
100.00	100.00	100.00

PROGNOSIS Raised Alerts

Severity	Alerts
Error	4

Voice Streams

Streams	Good	Fair	Poor	Unacceptable
0				

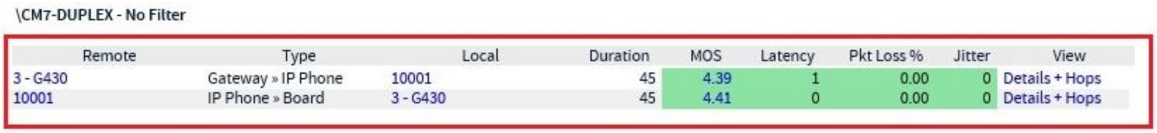
PBX Status

Type	Up	Down	Degr	Unkn	Total
CM Servers	1				1
LSPs	2				2
Media Gateways	2				2
Media Servers	1		1		2
Network Regions	3			1997	2000
Phones	36	112		44	192
Port Networks	2				2
Route Patterns	0			8	8
Trunk Groups	7	2			9
VDNs	5				5
Vectors	6				6

Major 0 Minor 0 CPU% 4

Network Hops (All PBXs)

\CM7-DUPLEX | AVSYSHLT(s): 1 | Tue Mar 13th 2018 16:25:30

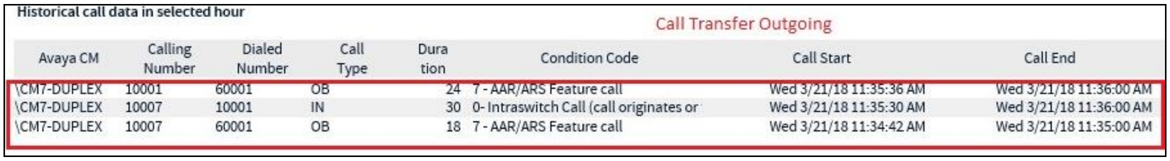
Step	Description
3.	Make a call between two Avaya IP telephones that belong to an IP Network Region that is being configured to send RTCP information to the Prognosis server. Verify that the **Voice Streams** section shows two active voice streams reflecting the quality of the call. 

\CM7-DUPLEX - No Filter

Remote	Type	Local	Duration	MOS	Latency	Pkt Loss %	Jitter	View
3 - G430	Gateway » IP Phone	10001	45	4.39	1	0.00	0	Details + Hops
10001	IP Phone » Board	3 - G430	45	4.41	0	0.00	0	Details + Hops

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

Verify the CDR data by making outbound and internal calls from Communication Manager System A to Communication Manager System B. Captured CDR data can be custom designed for the layout. Below is a sample of a captured CDR data.



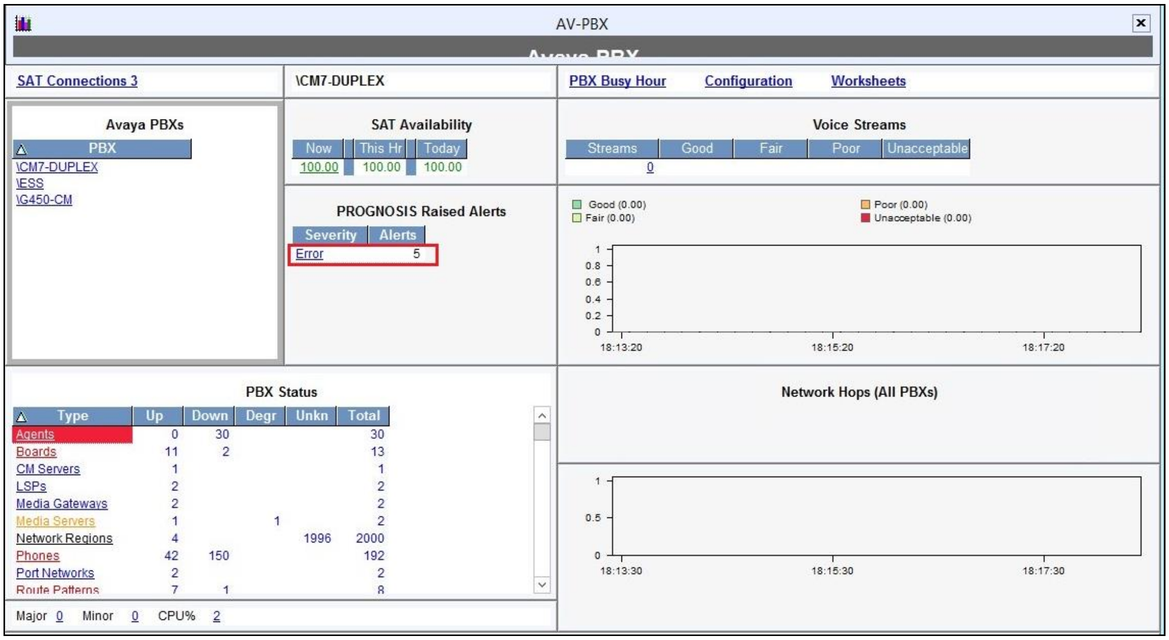
Historical call data in selected hour

Call Transfer Outgoing

<table>
<tr><th>Avaya CM</th><th>Calling Number</th><th>Dialed Number</th><th>Call Type</th><th>Duration</th><th>Condition Code</th><th>Call Start</th><th>Call End</th></tr>
<tr><td>\CM7-DUPLEX</td><td>10001</td><td>60001</td><td>OB</td><td>24</td><td>7 - AAR/ARS Feature call</td><td>Wed 3/21/18 11:35:36 AM</td><td>Wed 3/21/18 11:36:00 AM</td></tr>
<tr><td>\CM7-DUPLEX</td><td>10007</td><td>10001</td><td>IN</td><td>30</td><td>0- Intraswitch Call (call originates or</td><td>Wed 3/21/18 11:35:30 AM</td><td>Wed 3/21/18 11:36:00 AM</td></tr>
<tr><td>\CM7-DUPLEX</td><td>10007</td><td>60001</td><td>OB</td><td>18</td><td>7 - AAR/ARS Feature call</td><td>Wed 3/21/18 11:34:42 AM</td><td>Wed 3/21/18 11:35:00 AM</td></tr>
</table>

</td></tr>
<tr><td>5.</td><td>

Verify that the number of errors present in Communication Manager from the “display errors” command is also reflected on the PBX screen below.



AV-PBX

Avaya PBX

SAT Connections 3 | \CM7-DUPLEX | PBX Busy Hour | Configuration | Worksheets

Avaya PBXs

PBX
\CM7-DUPLEX
\ESS
\G450-CM

SAT Availability

Now	This Hr	Today
100.00	100.00	100.00

Voice Streams

Streams	Good	Fair	Poor	Unacceptable
0				

PROGNOSIS Raised Alerts

Severity	Alerts
Error	5

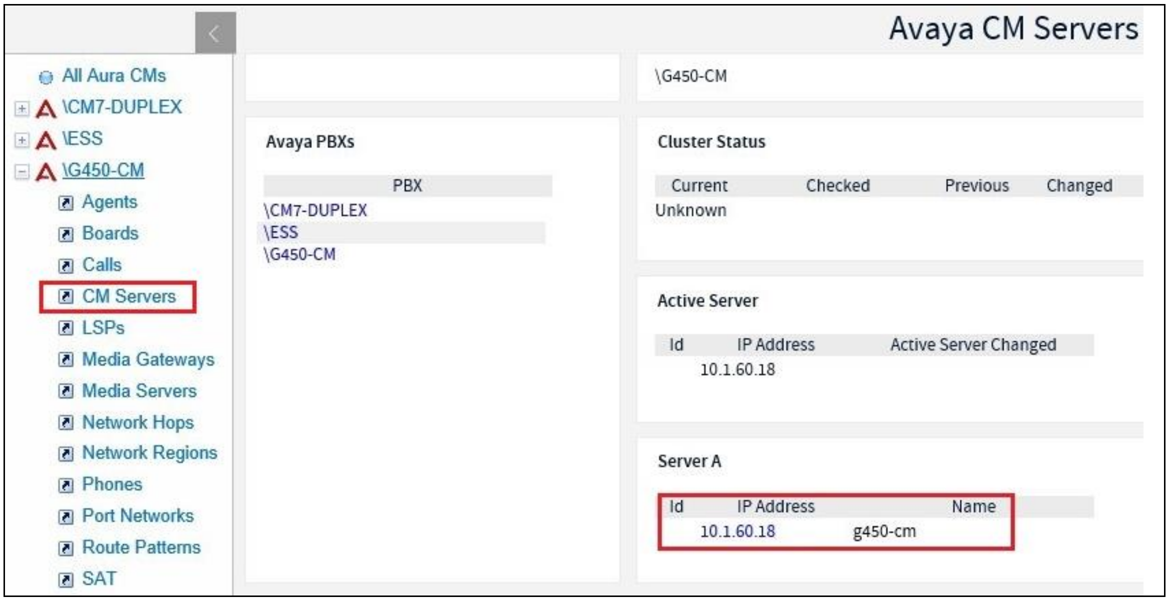
PBX Status

Type	Up	Down	Degr	Unkn	Total
Agents	0	30			30
Boards	11	2			13
CM Servers	1				1
LSPs	2				2
Media Gateways	2				2
Media Servers	1		1		2
Network Regions	4			1996	2000
Phones	42	150			192
Port Networks	2				2
Route Patterns	7	1			8

Major 0 Minor 0 CPU% 2

Network Hops (All PBXs)

</td></tr>
</table>

Step	Description
6.	Select any of the PBX, verify that the SNMP capture of the Communication Manager name and IP address is shown from the CM Servers link on the left pane of Communication Manager. 

Avaya CM Servers

\G450-CM

Avaya PBXs

PBX
\CM7-DUPLEX
\ESS
\G450-CM

Cluster Status

Current	Checked	Previous	Changed
Unknown			

Active Server

Id	IP Address	Active Server Changed
	10.1.60.18	

Server A

Id	IP Address	Name
	10.1.60.18	g450-cm

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis for Unified Communications R11.4 to interoperate with Avaya Aura® Communication Manager R7.1. In the configuration described in these Application Notes, Prognosis established SSH connections to the SAT to view the configurations of Communication Manager. Prognosis also processed the RTCP information to monitor the quality of IP calls and collected CDR information sent by Communication Manager. Prognosis also obtained the Communication Manager name and IP address from the SNMP information. 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 7.1.2, Issue 5, Feb 2018.
[2] *Administering Avaya Aura® Communication Manager*, Release 7.1.2, Issue 4, Jan 2018.
[3] *Application Notes for Integrated Research's Prognosis for Unified Communications 11.4 with Avaya Aura® Session Manager R7.1 and Avaya Aura® System Manager R7.1.*

Prognosis documentations are provided with the software Package.

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.