Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research's Prognosis for Unified Communication 10.5 with Avaya Aura® Communication Manager R7.0 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Prognosis for Unified Communication R10.5 (Prognosis) to interoperate with Avaya Aura® Communication Manager R7.0.

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.

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 10.5 (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, media servers and 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 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.

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, 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. 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 Communication Managers to simulate system unavailability. Interchanging of the duplex Communication Managers and loss of network connections were also performed during testing.

2.2. Test Results

All test cases passed successfully. The following was observed for media server introduced in Communication Manager R7.0:

- The correct voice streams were shown when a call is made through the media server. However, the "Type" field is marked with "Unknown" instead of Media Server. Enhancement to be made in the later release.

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 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 an 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 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. System Manager and 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.

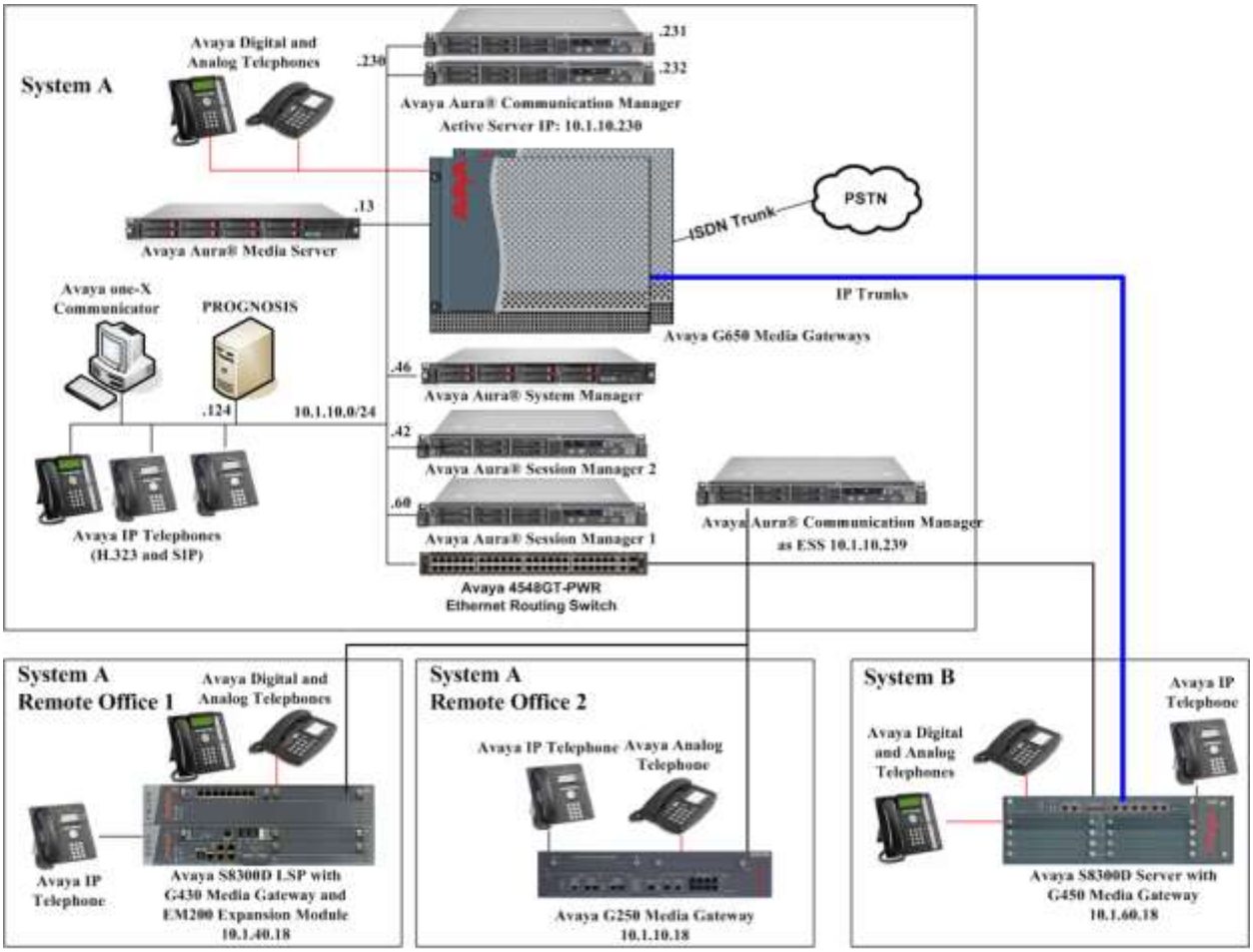


Figure 1: Test Configuration

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 (System A)	7.0 SP3.1
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, FW058 HW01, FW044 HW02 FW066 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW012 HW08, FW016
G250 Media Gateway	30.27.1
Avaya Aura® Communication Manager using Avaya S8300D Server (G450 Media Gateway – System B)	7.0 SP3.1
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	37.21.0 HW01 FW008 HW07 FW015 HW10 FW099 HW03 FW015 HW11 FW053
Avaya Aura® Communication Manager using Avaya S8300D Server as Local Survivable Processor (LSP)	7.0 SP3.1
G430 Media Gateway - MM712AP DCP MM - MM714AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	37.21.0 HW04 FW015 HW12 FW100 HW31 FW100 HW05 FW022
Avaya Aura® Communication Manager as Enterprise Survivable Server (ESS)	7.0 SP3.1
Avaya Aura® System Manager	7.0.0.2
Avaya Aura® Session Manager 1	7.0.0.2
Avaya Aura® Session Manager 2	7.0.0.2
96xx Series IP Telephones - 9640 - 9620	2.6.14 (SIP) 3.250A (H323)
96x1 Series IP Telephones - 9641G - 9611G	7.0.0.39 (SIP) 6.6029 (H323)

Equipment/Software	Release/Version
1600 Series IP Telephones - 1616 - 1603SW	1.390A (H.323)
Digital Telephones - 1416 - 1408	Rel 4 SP7
Avaya Analog Phones	-
Desktop PC with Avaya one-X Communicator	6.2.11.03 (H.323)
Avaya 4548GT-PWR Ethernet Routing Switch	V5.6.1.052
Prognosis running on Windows 2008 R2 SP1	10.5

Note: All Avaya Aura systems runs on VMware 5.x except S8300D on AVP.

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 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.

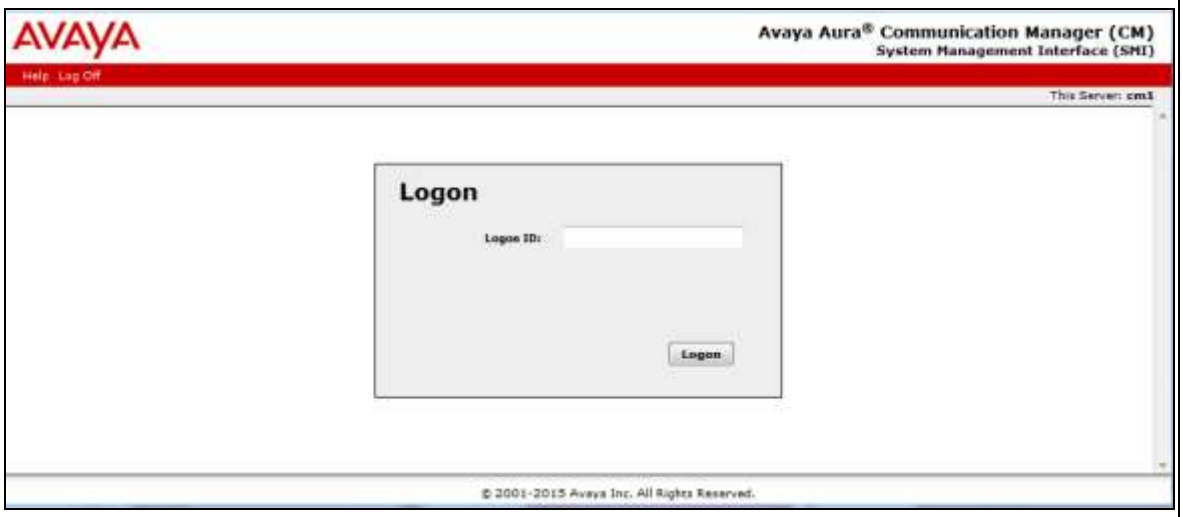
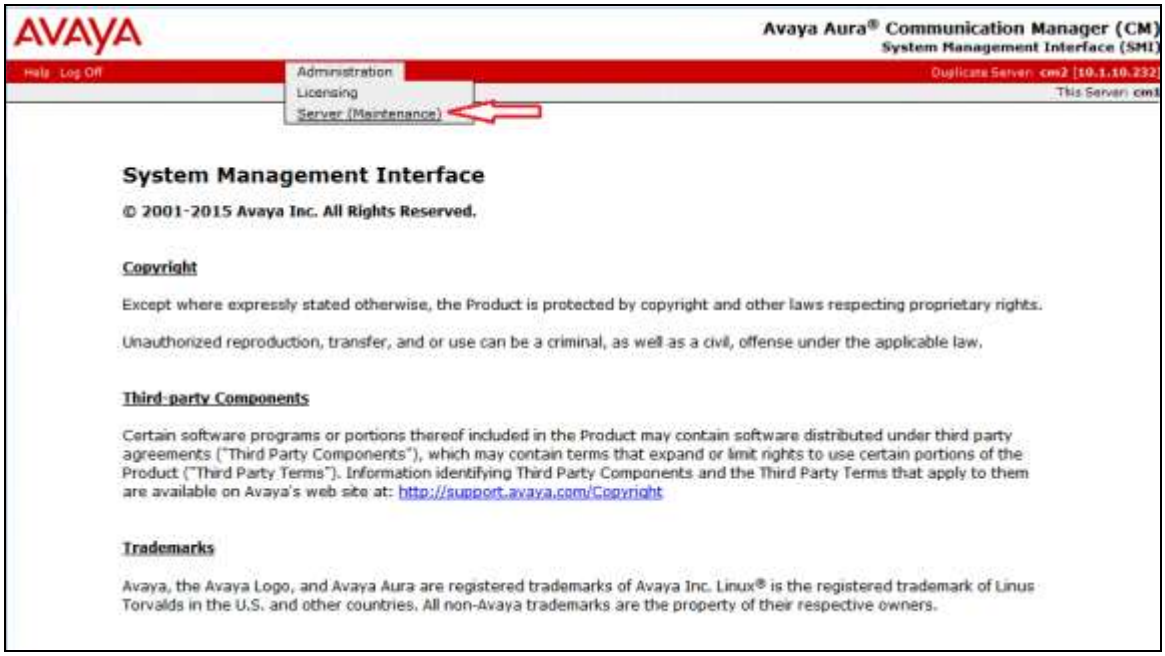
```
add user-profile 23                                          Page   1 of  41
                                 USER PROFILE 22

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
```

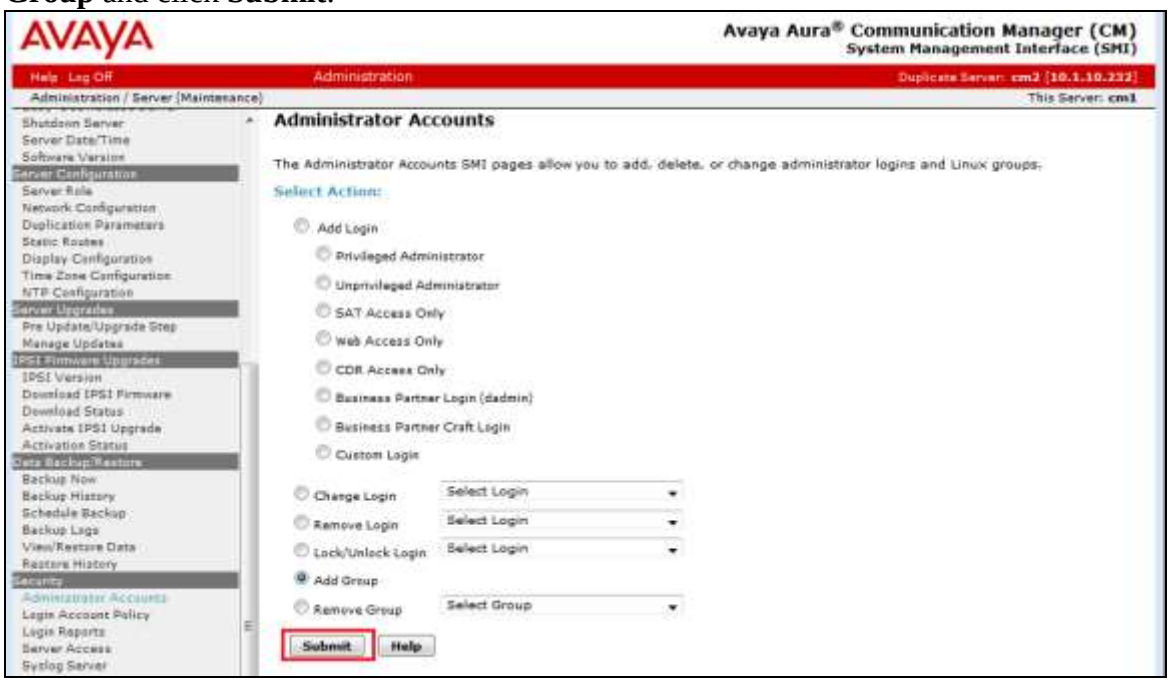
Step	Description
2.	On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the field **Set All Permissions To**. Submit the form to create the user profile.

```
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

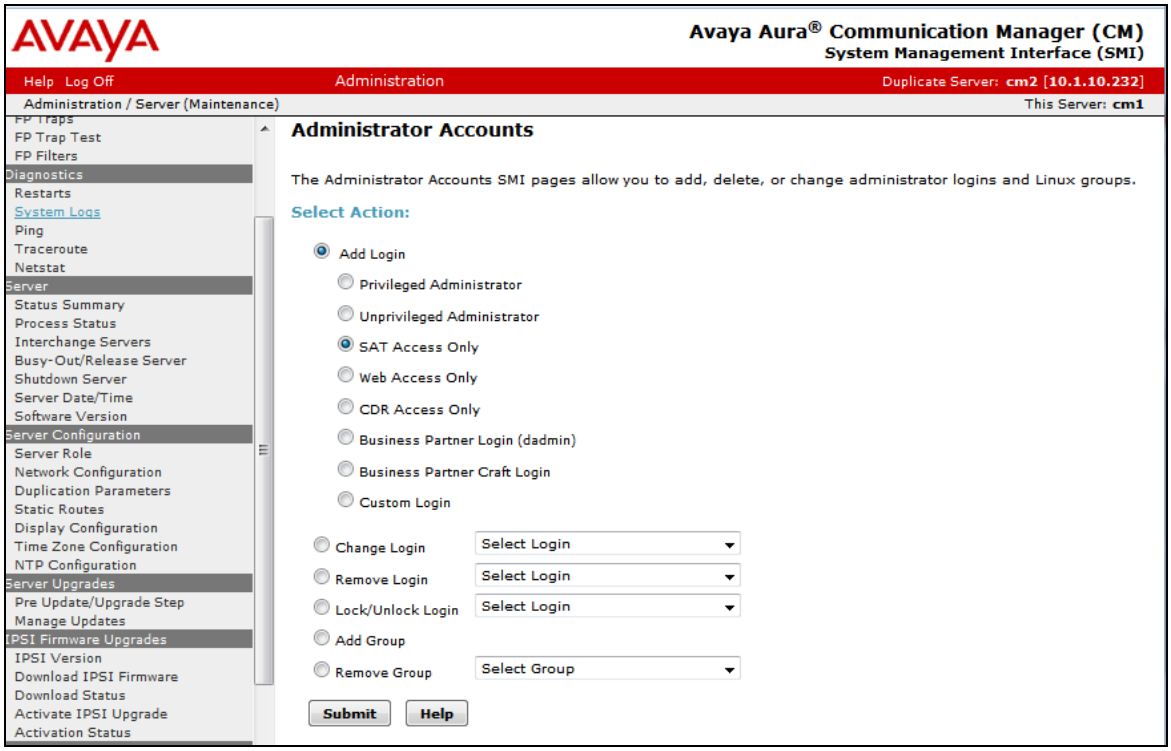
Create an Access-Profile Group on Communication Manager System Management Interface (SMI) to correspond to the SAT User Profile created in **Section 5.1**.

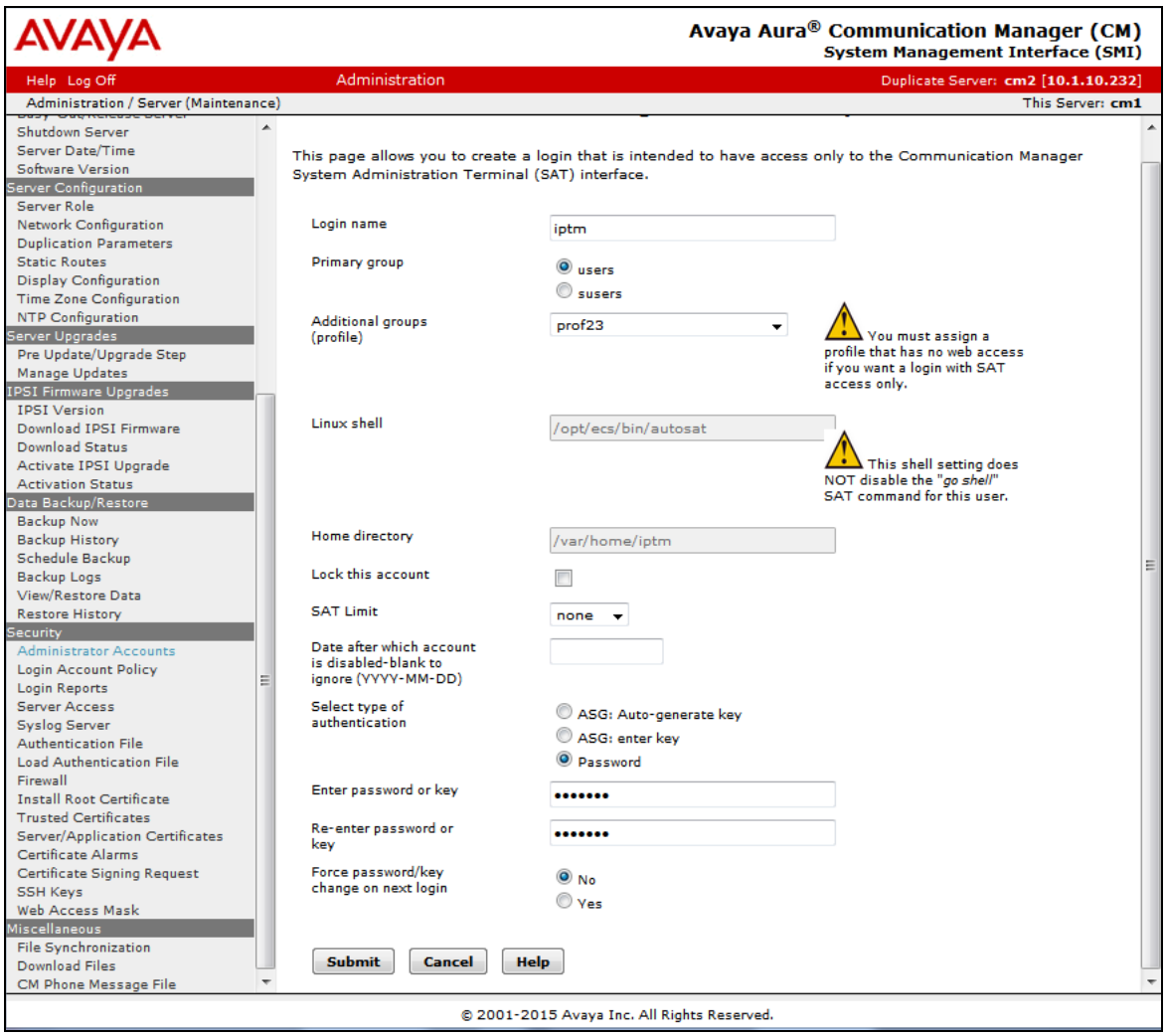
Step	Description
1.	Using a web browser, enter *https://<IP address of Communication Manager>* to connect to the Communication Manager Server being configured and log in using appropriate credentials. 
2.	Click **Administration → Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow the user to complete the configuration process. 

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

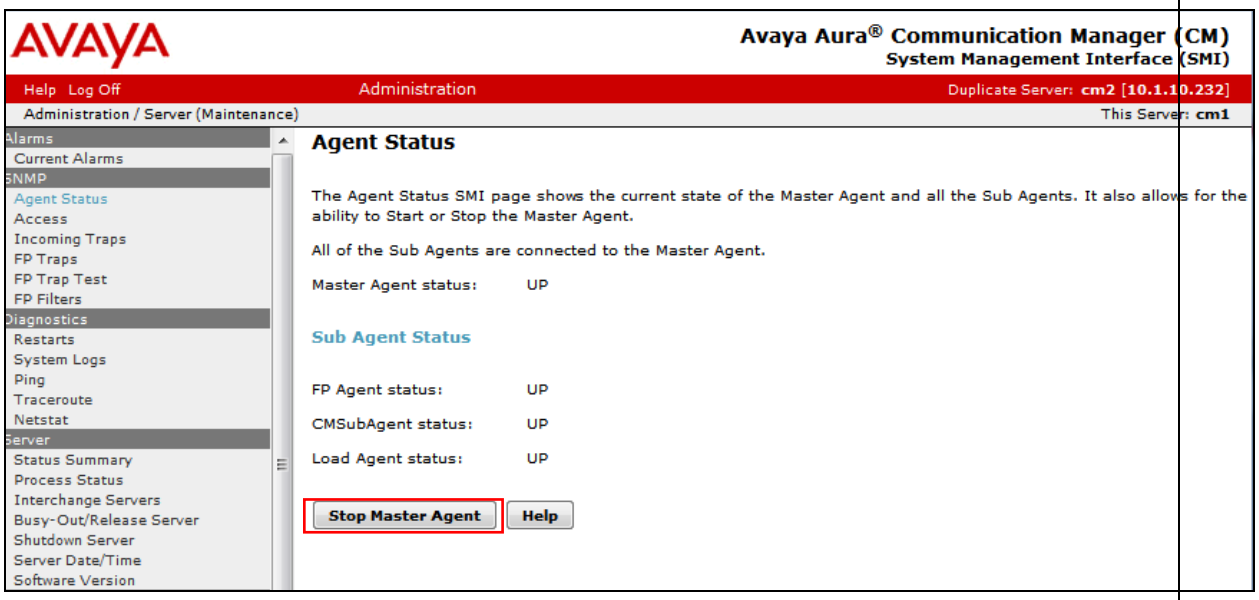
5.3. Configure Login

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

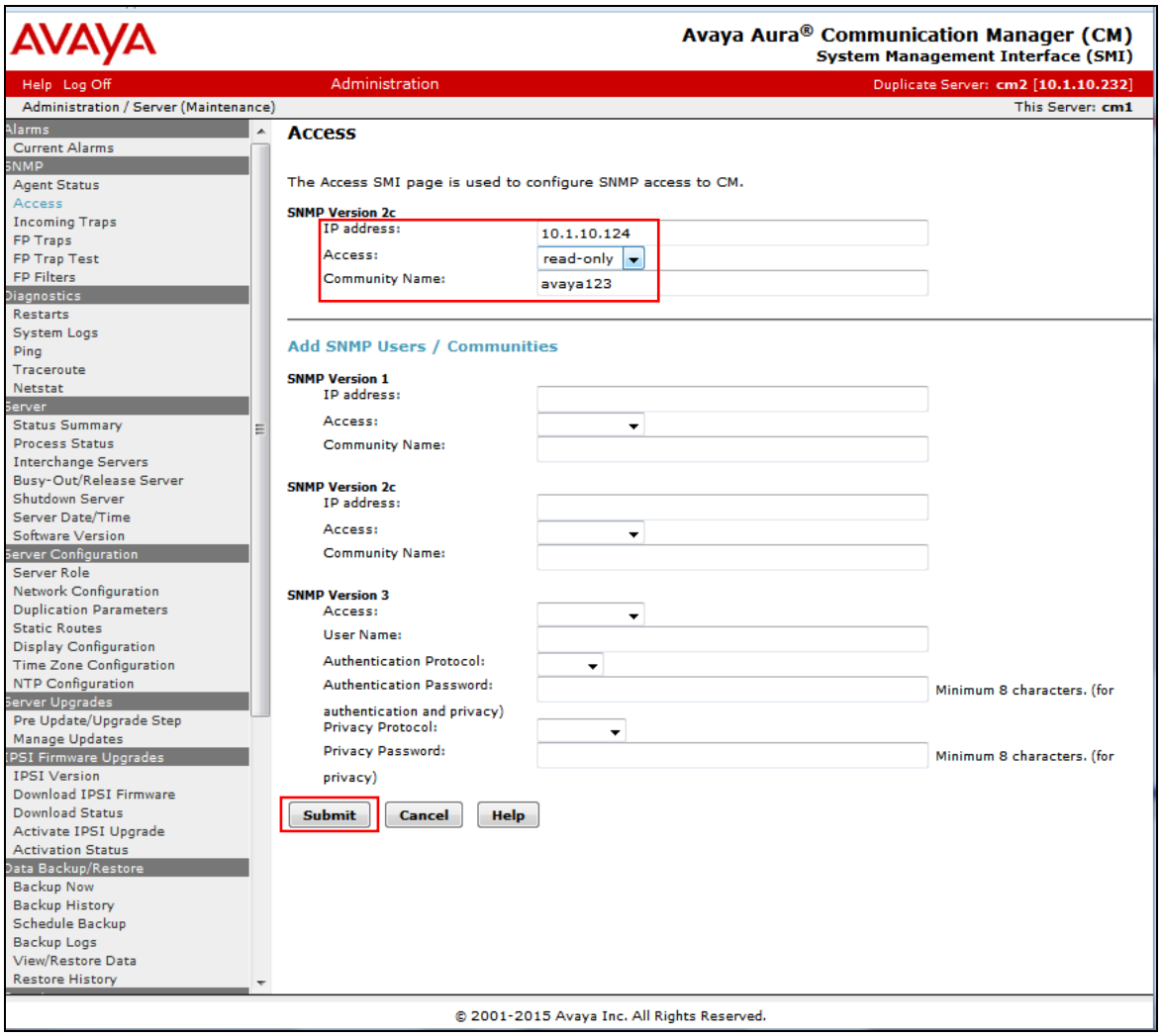
Step	Description
1.	From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Login** and **SAT Access Only** to create a new login account with SAT access privileges only. Click **Submit**. 

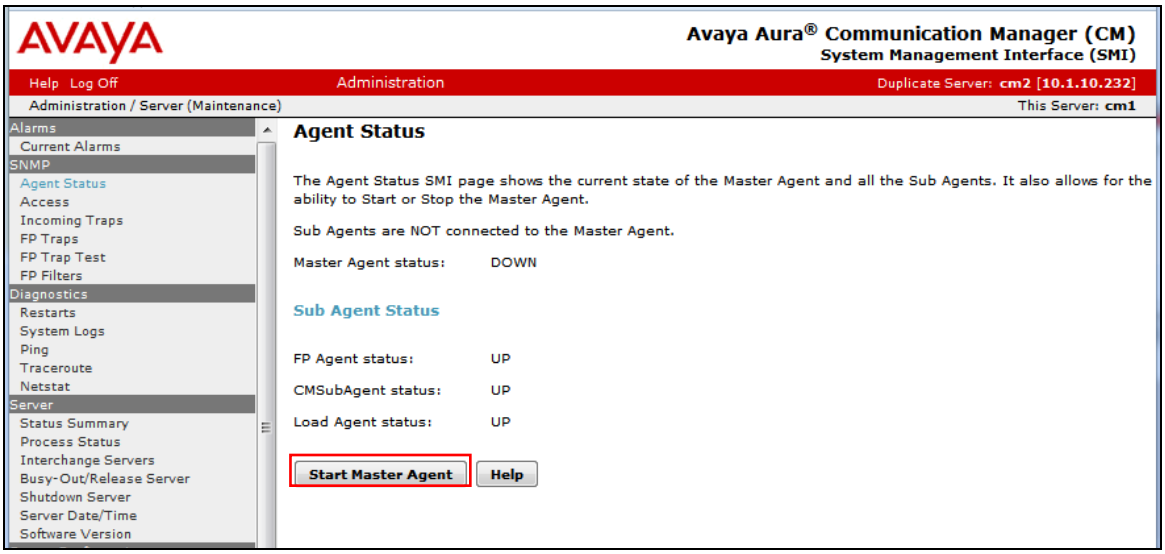
Step	Description
2.	For the field **Login name**, enter the login. In this configuration, the login **iptm** is created. Configure the other parameters for the login as follows: • **Primary group**: **users** [Limits the permissions of the login] • **Additional groups (profile)**: **prof23** [Select the access-profile group created in **Section 5.2**. Ignore the warnings as SAT access access is selected in Step 1.] • **Select type of authentication: Password** [Uses a password for authentication.] • **Enter password or key / Re-enter password or key** [Define the password.] Click **Submit** to continue. This completes the configuration of the login. 

5.4. Configure SNMP

Step	Description
1.	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. 

Step	Description
2.	To allow Prognosis to use SNMP to collect configuration and status information from Communication Manager, navigate to **Alarms → 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 **avaya123**. Click **Submit** at the bottom of the web page.



Step	Description
3.	Lastly, the SNMP agent must be started. Navigate to **Alarms → 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. 

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.	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***.

```
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
  Link Loss Delay Timer (min): 5         Primary Search Time (sec): 75
                                  Periodic Registration Timer (min): 20
                                Short/Prefixed Registration Allowed? Y
```

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 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 Enabled? y

 RTCP MONITOR SERVER PARAMETERS
   Use Default Server Parameters? Y
```

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 the Avaya Server. 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 **10.1.10.124**. Note also the node name **procr** which is automatically added.

```
change node-names ip                                               Page   1 of   2
                                 IP NODE NAMES
    Name                IP Address
iptm                  10.1.10.124
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 31   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] • **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.]

```
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 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.]

```
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 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.

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

                               Assigned Members:   7    of 5000   administered
   Extension          Extension          Extension          Extension
   10001
   10002
   10003
   10004
   10005
   10017
   20001


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
```

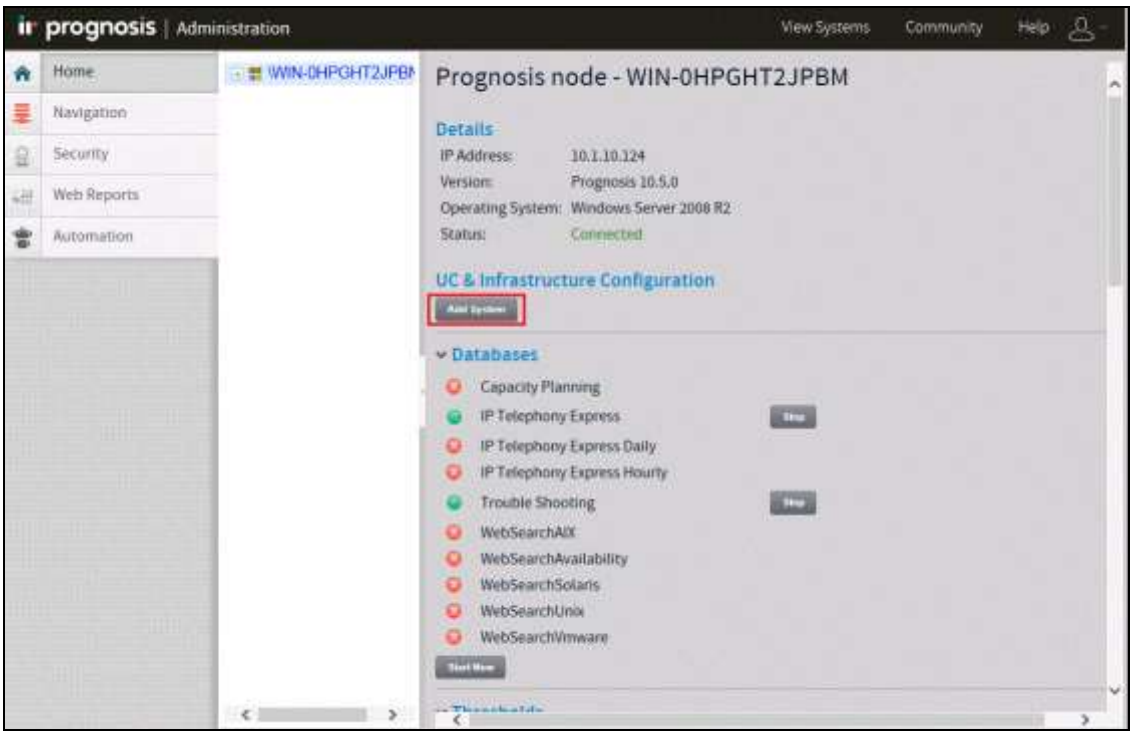
7.	Enter **save translation** to save the changes made.

```
save translation

                               SAVE TRANSLATION

           Command Completion Status                                Error Code

           Success                                                  0
```

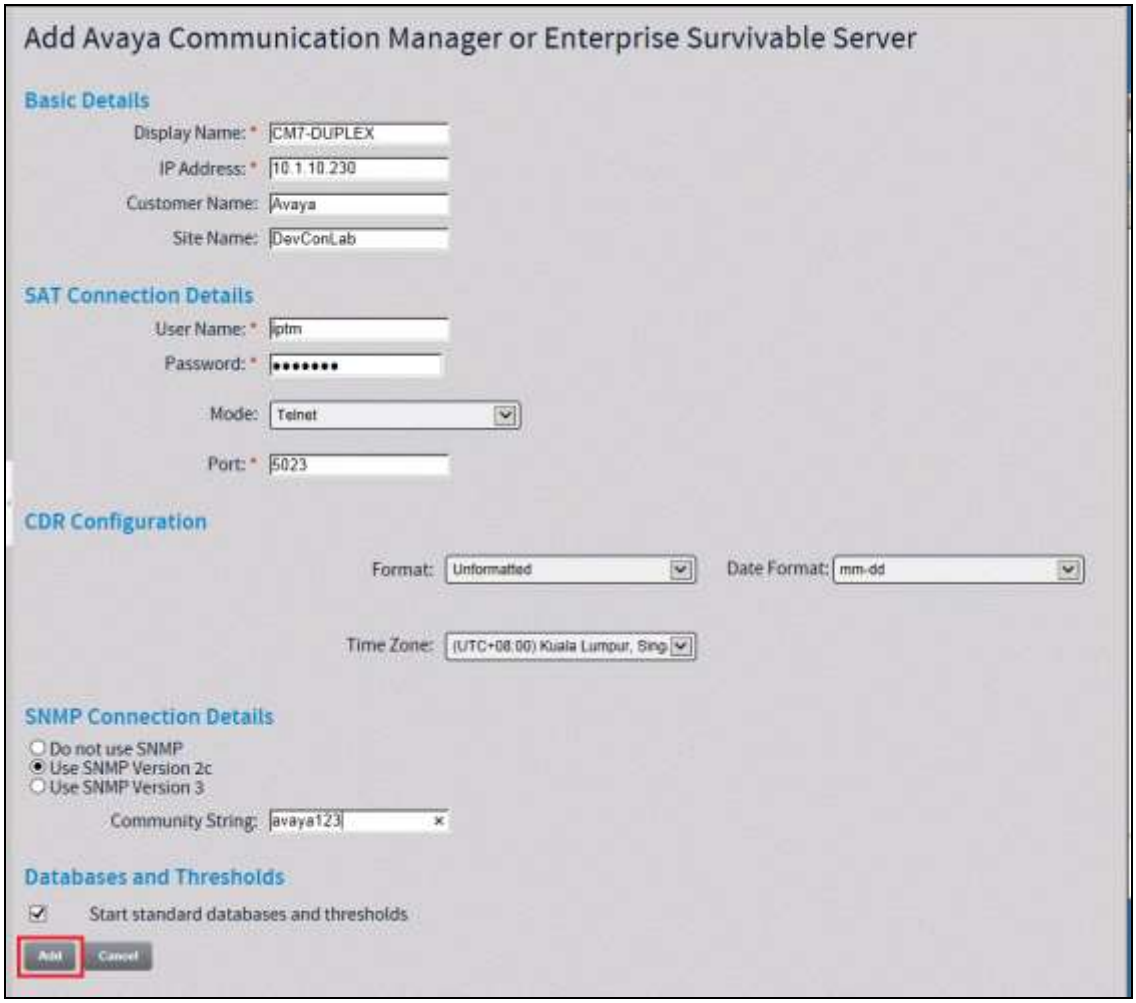
6. Configure Prognosis

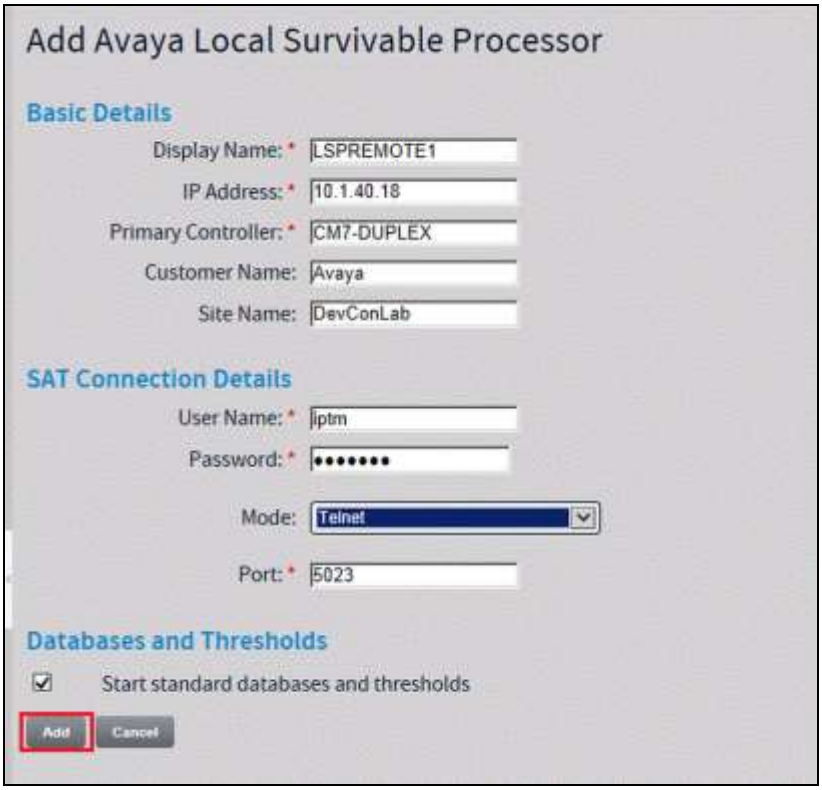
This section describes the configuration of Prognosis required to interoperate with Communication Manager. Configuration of Prognosis to interoperate with Session and System Manager can be referred from **Reference [6]** and will not be detailed here.

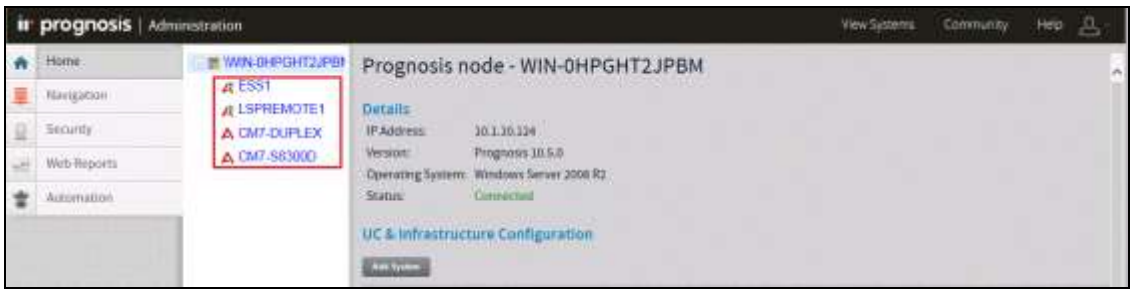
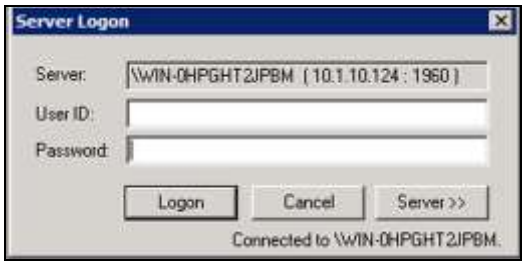
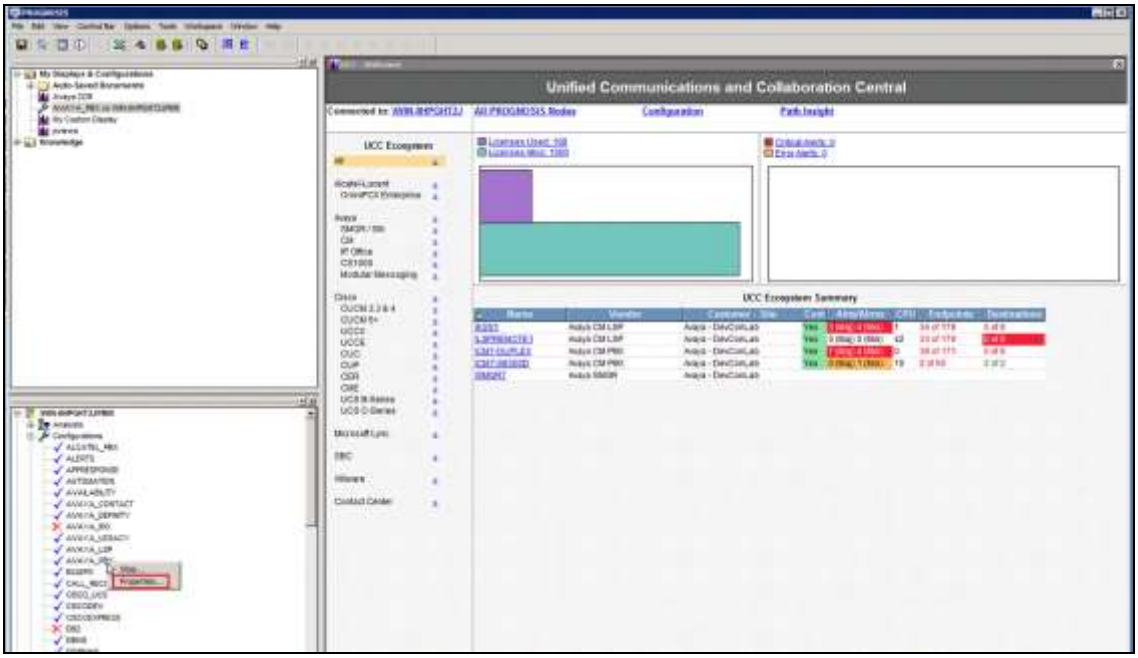
Step	Description
1.	Log into the Prognosis Server with administrative privileges. Launch the Prognosis Administration by clicking **Start → All Programs → Prognosis → Administration**. Login with the appropriate password. 

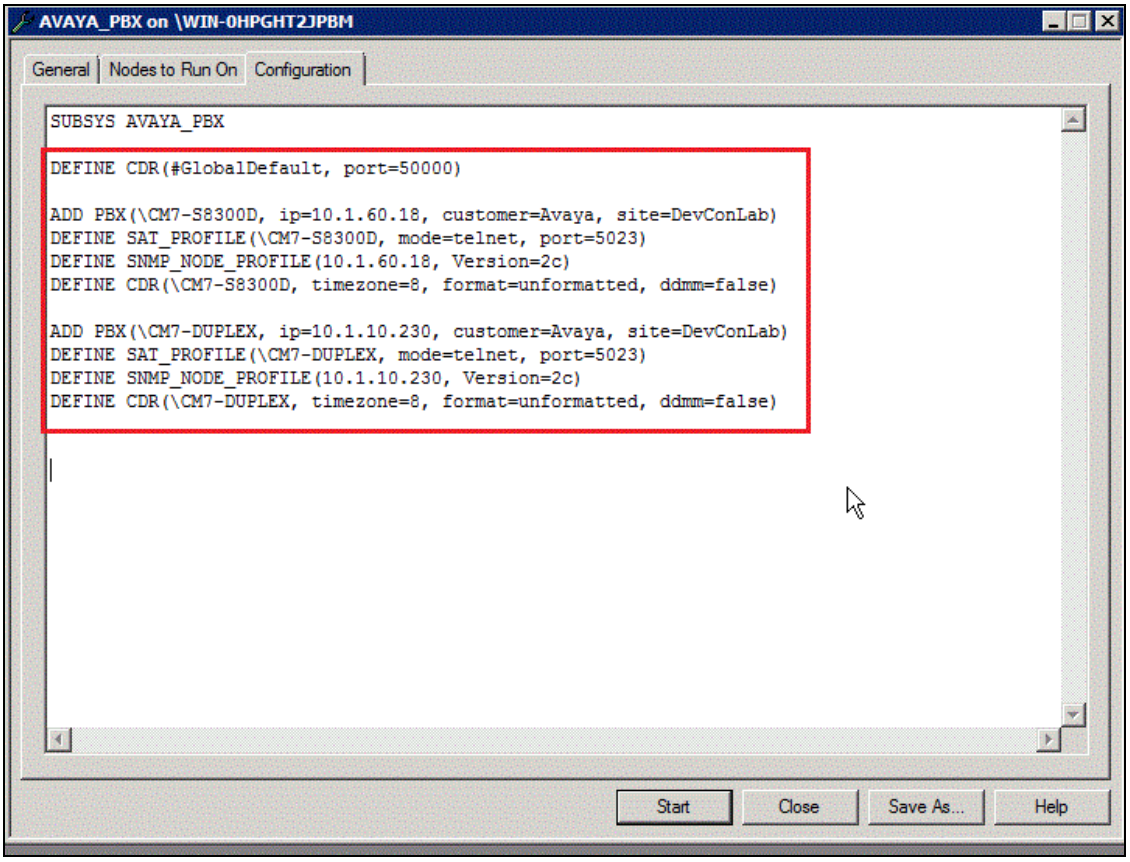
Step	Description
2.	Click **Add System**. 
3.	Click **Add** to add a new Avaya PBX. 

Step	Description
4.	In this test configuration, the following entries are added for the two Communication Manager systems with the Display Name **CM7-DUPLEX** (System A) and **CM7-S8300D** (System B) and with the IP addresses of the Avaya Servers **10.1.10.230** and **10.1.60.18** respectively. 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: DevConLab** **SAT Connection Details:** • **User Name/Password: iptm/**[As configured in **Section 5.3 Step 2**] • **Mode: Telnet** • **Port: 5023** [For secure connection, select SSH with 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.** Leave **the Databases and Thresholds** as checked**.** Click **Add** to effect the addition**.** Repeat the above for the setup of **CM7-S8300D**.

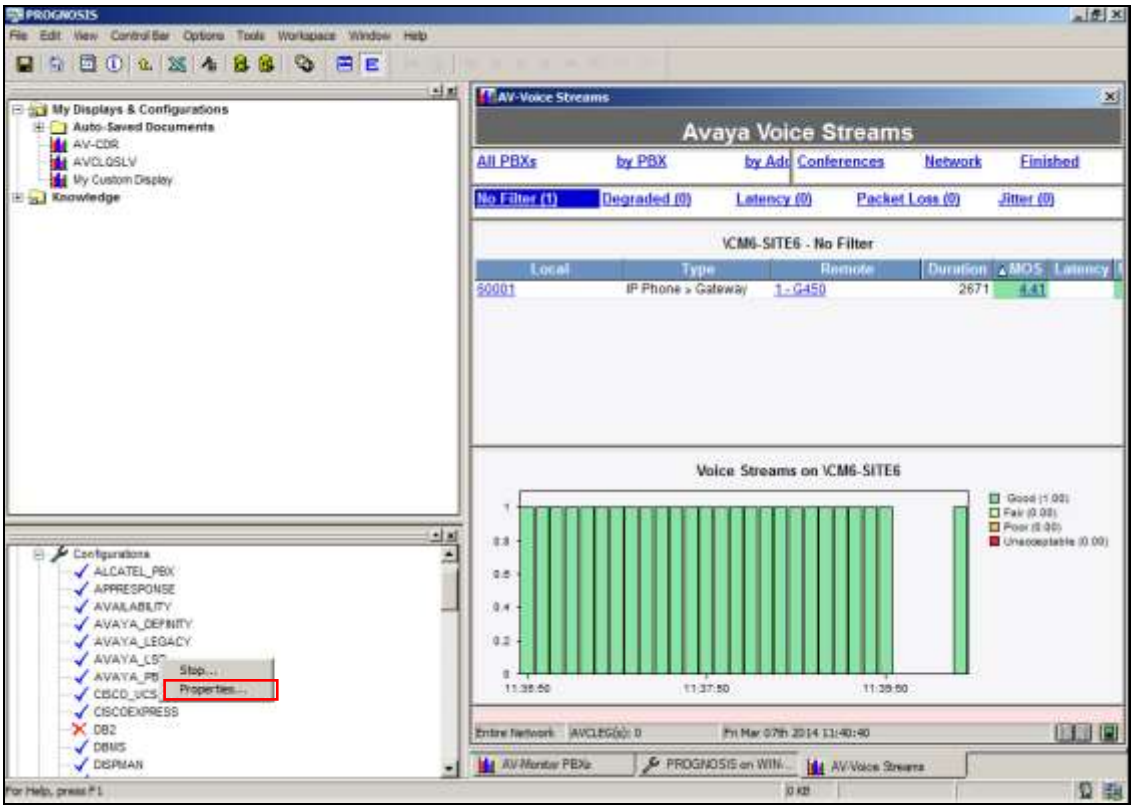
Step	Description
	
5.	In this test configuration, the Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS) Servers with the names **LSPREMOTE1** and **ESS1** with the IP addresses of **10.1.40.10** and **10.1.10.239** respectively, both belonging to the **CM7-DUPLEX** Communication Manager system are also configured. Repeat Step 2 to add a new system and select **Add** to add a new **Avaya LSP**. 

Step	Description
6.	The following settings were used during the compliance test. **Basic Details:** • **Display Name: LSPREMOTE1** • **IP address: 10.1.40.18** • **Primary Controller: CM7-DUPLEX** • **Customer Name: Avaya** • **Site Name: DevConLab** **SAT Connection Details:** • **User/Password: iptm/**[As configured in **Section 5.3 Step 2**] • **Mode: Telnet** • **Port: 5023** [For secure connection, select SSH with port 5022] Click **Add** to effect the addition**.** Repeat the above for the setup of **ESS1.** 

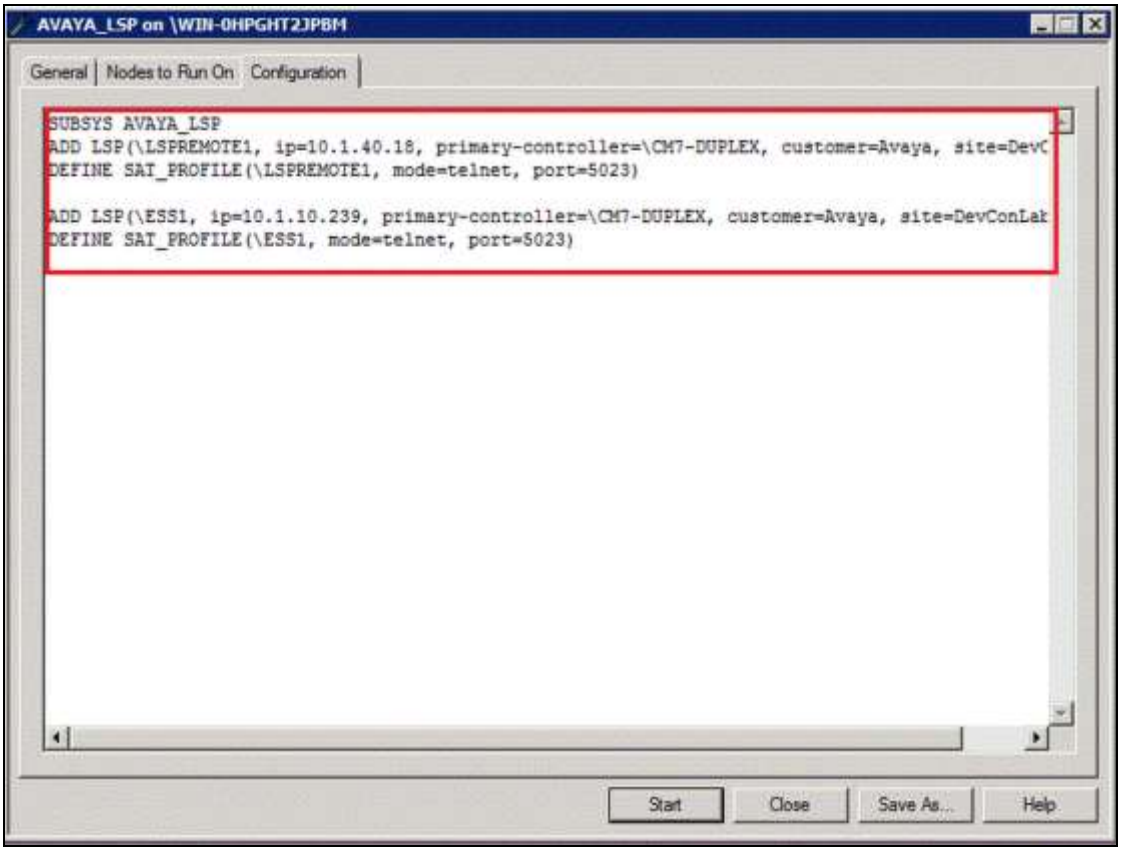
Step	Description
7.	Below is the result of the additions of the 2 Communication Systems plus the LSP/ESS. 
8.	On Prognosis server, click **Start → All Programs → Prognosis → Prognosis Client** to start the Windows Client application. Log in with the appropriate credentials. 
9.	Expand **Configurations** of the Monitoring Node, right-click on **AVAYA_PBX** and select **Properties**. 

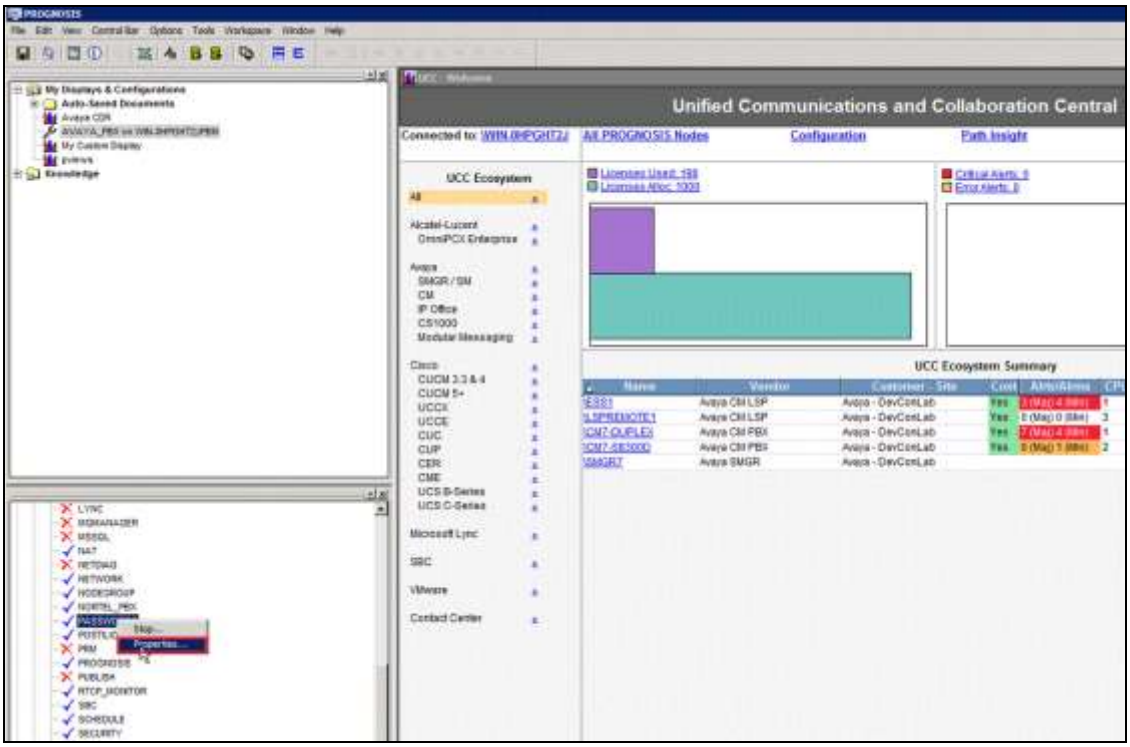
Step	Description
10.	Check the configurations for each of the Communication Manager and the corresponding CDR settings Step as configured in **Step** 4 earlier. Note that the default CDR port is 50000 which correspond to the configurations set in **Section 5.6 Step 3** is already created as default. 

Step	Description
11.	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**.

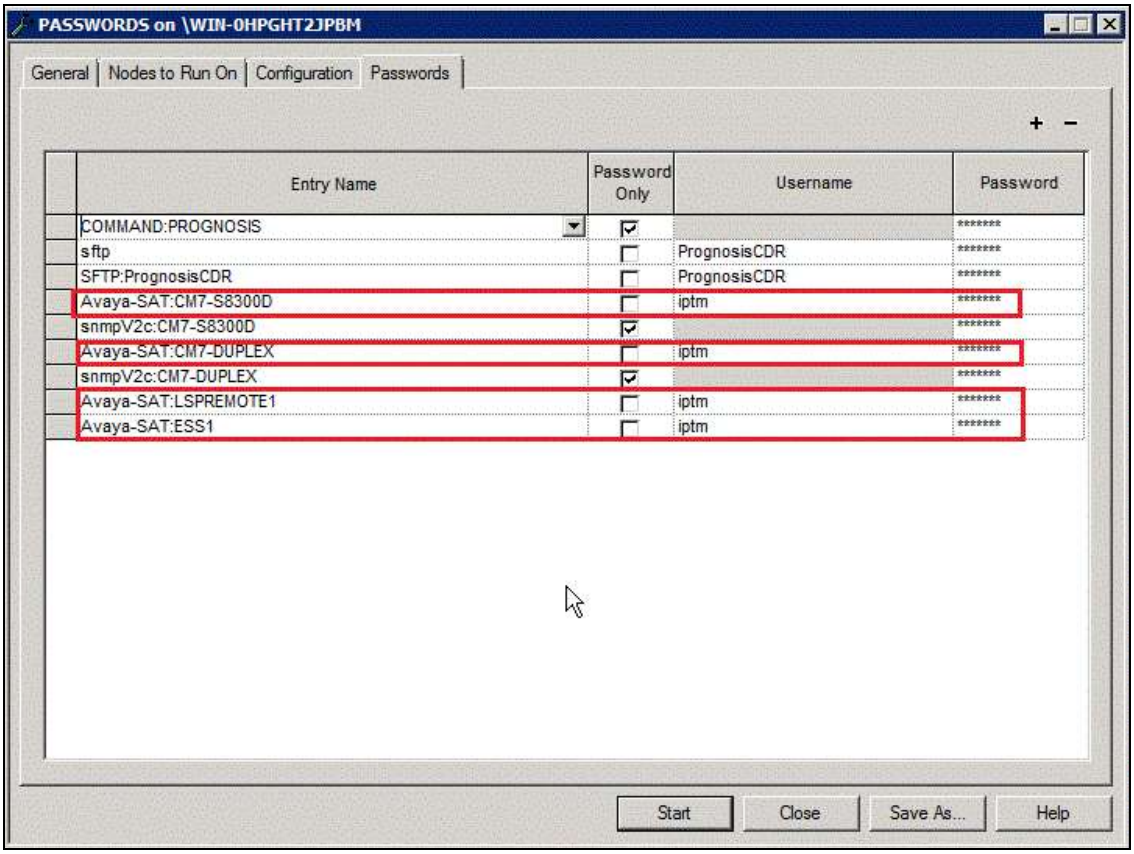


Step	Description
12.	Check the configurations for each ESS and LSP Servers to be monitored as configured in **Step 6** earlier.



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**. 

Step	Description
14.	The four entries for the **CM7-DUPLEX**, second system **CM7-S8300D, LSPREMOTE1** and **ESS1** are listed on the right pane.



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.

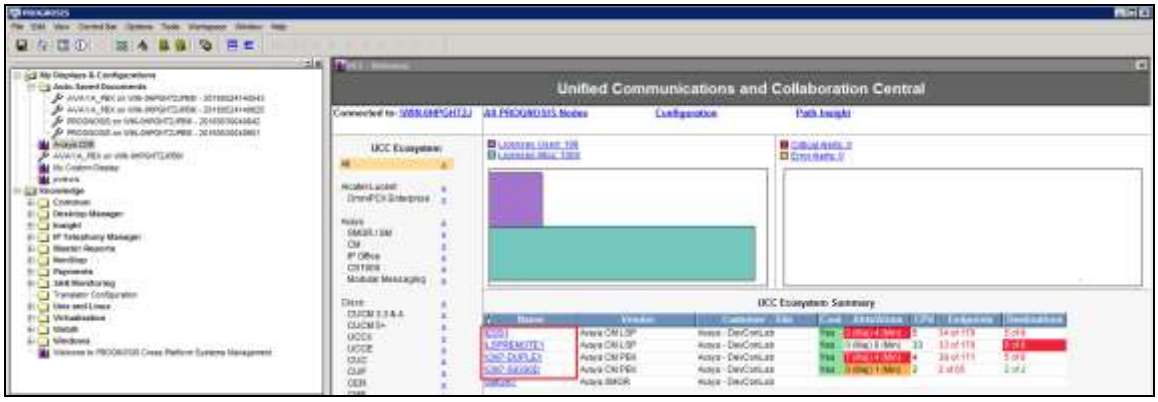
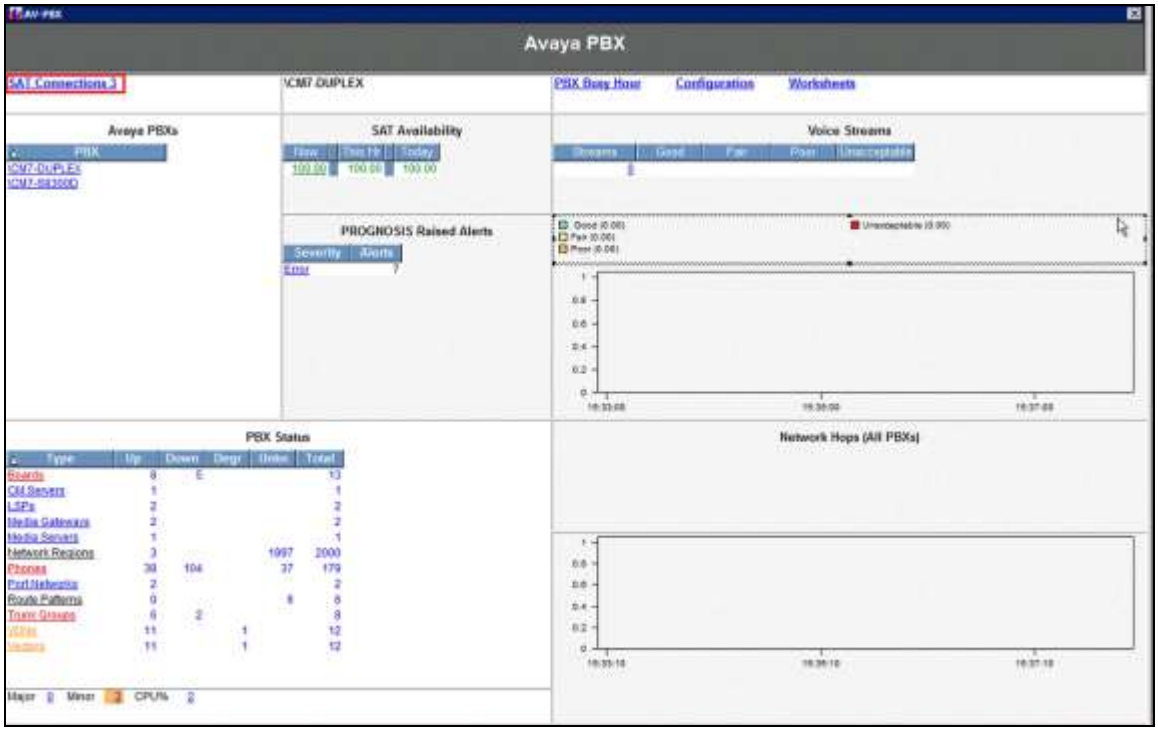
```
status logins

                    COMMUNICATION MANAGER LOGIN INFORMATION

Login     Profile   User's Address       Active Command              Session

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

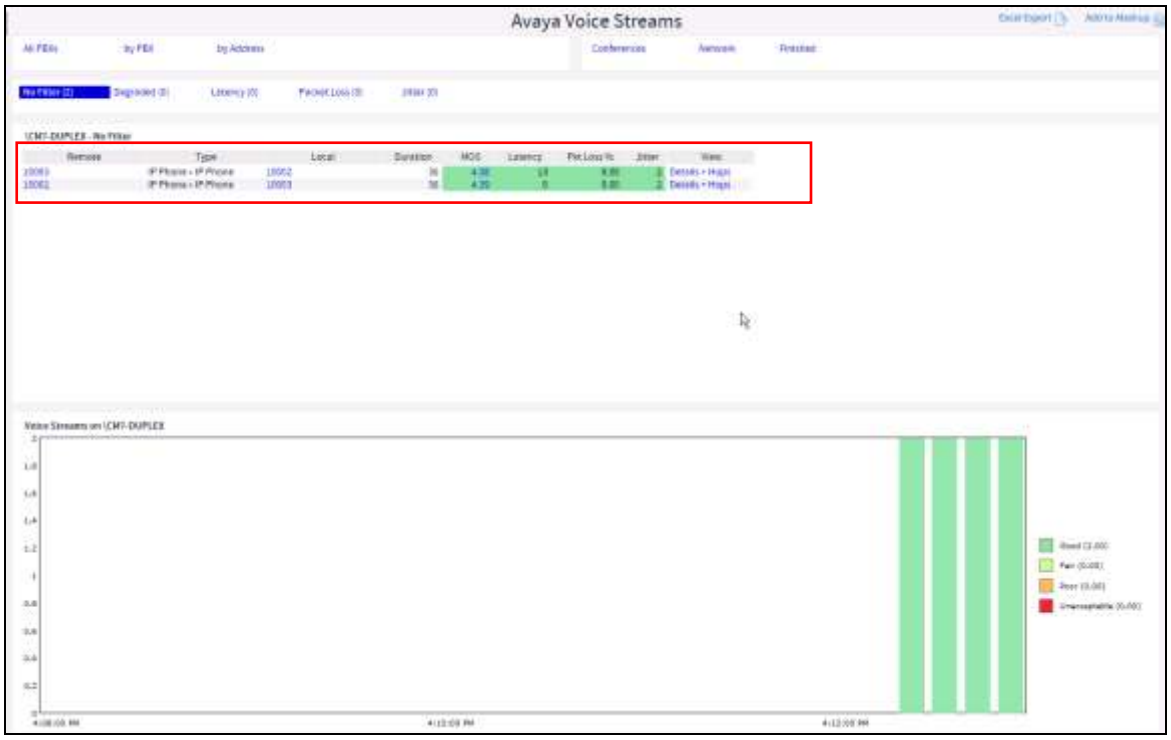
Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 5.7** shows **up**.

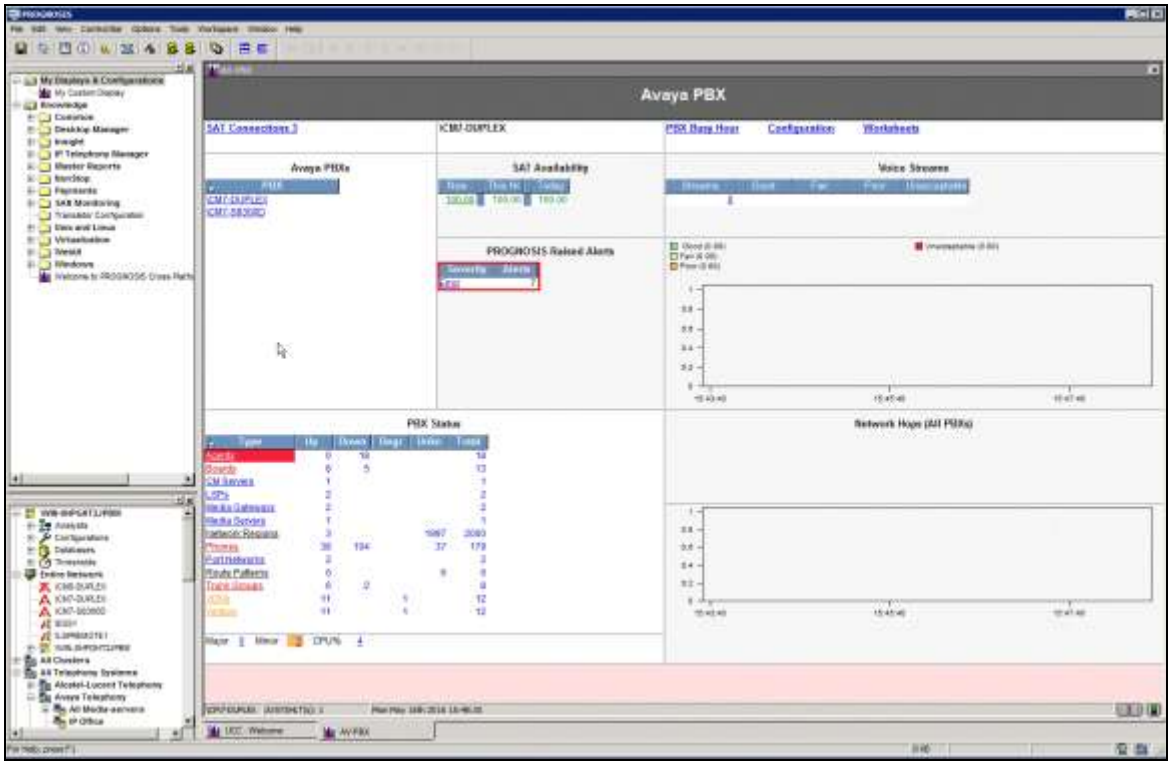
```
status cdr-link
                                CDR LINK STATUS
                    Primary                      Secondary

       Link State: up                            CDR not administered

      Date & Time: 2016/05/16 14:56:10           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.	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**. 
2.	Select any of the PBX, verify that the **SAT Connections** field for each configured Communication Manager shows **3** connections. Repeat to check the other PBX. 

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. 

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

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis for Unified Communications 10.5 to interoperate with Avaya Aura® Communication Manager R7.0. In the configuration described in these Application Notes, Prognosis established telnet connections to the SAT to view the configurations of Communication Manager and SNMP 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 with observations in **Section 2.2**.

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 7.0.1, Issue 2, May 2016, Document Number 555-245-205.
[2] *Administering Avaya Aura® Communication Manager*, Release 7.0.1, Issue 2, May 2016, Document Number 03-300509.
[3] *Application Notes for Integrated Research's Prognosis for Unified Communications 10.5 with Avaya Aura® Session Manager R7.0 and Avaya Aura® System Manager R7.0.*

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

[4] *Prognosis Deployment and Installation Guide 10.5*, 22nd Feb 2016
[5] *Prognosis for Unified Communications Avaya Aura Communication Manager User Guide, Prognosis 10.5*, 21 Dec 2015
[6] *Prognosis for Unified Communications Avaya Aura System and Session Manager User Guide, Prognosis 10.5*, 21 Dec 2015

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.