Avaya Solution & Interoperability Test Lab

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

Abstract

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

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

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

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Integrated Research PROGNOSIS IP Telephony Manager with Avaya Aura™ Communication Manager.

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

- One or more **PROGNOSIS Monitoring Nodes** (Server Nodes). These are servers used by the PROGNOSIS product to collect, relay and store information collected from Communication Manager.

- The **PROGNOSIS GUI** is a Microsoft Windows client program which is used to connect to a PROGNOSIS monitoring node and display the information collected by the monitoring node. The PROGNOSIS GUI may either be installed on a monitoring node or on a separate computer.

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

- **System Access Terminal (SAT)** - The PROGNOSIS IP Telephony Manager uses a pool of SSH connections to the SAT using the IP address of the Avaya Server. By default, the solution establishes three concurrent SAT connections to the Communication Manager system and uses the connections to execute SAT commands.

- Real Time Transport Control Protocol **(RTCP) Collection** - The PROGNOSIS IP Telephony Manager collects RTCP information sent by the Avaya IP Media Processor (MEDPRO) boards, media gateways, IP Telephones and IP Softphones.

- **Call Detail Recording (CDR) Collection** - The PROGNOSIS IP Telephony Manager collects CDR information sent by Communication Manager.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing evaluated the ability of the PROGNOSIS IP Telephony Manager to correctly retrieve the configuration, performance, alarms and errors from Communication Manager. In addition, the ability of PROGNOSIS IP Telephony Manager to receive and process both RTCP and CDR information from Communication Manager was also validated.

The serviceability testing introduced failure scenarios to see if PROGNOSIS IP Telephony Manager is able to resume service after failure recovery and an Avaya Server interchange.

1.2. Support

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

- Phone: +61 (2) 9966 1066
- Fax: +61 (2) 9921-1042
- Email: support@prognosis.com

2. Reference Configuration

Figure 1 illustrates the test configuration used to verify Integrated Research PROGNOSIS IP Telephony Manager interoperability with Communication Manager. It consists of a Communication Manager system running on a pair of Avaya S8720 Servers with two Avaya G650 Media Gateways, an Avaya G450 Media Gateway, an Avaya G430 Media Gateway with EM200 Expansion Module, an Avaya G700 Media Gateway with Avaya S8300 Server as a Local Survivability Processor (LSP) and an Avaya G250-BRI Media Gateway. An Enterprise Survivable Server (ESS) running on Avaya S8500C Server was also configured for failover testing. A second Communication Manager system runs on an Avaya S8300 Server with an Avaya G350 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. Integrated Research PROGNOSIS IP Telephony Manager was installed on a server running Microsoft Windows Server 2003 Standard Edition with Service Pack 2. Both the Monitoring Node and GUI software are installed on this server. All the systems and telephones are connected using an Avaya C364T-PWR Converged Stackable Switch for network connectivity.

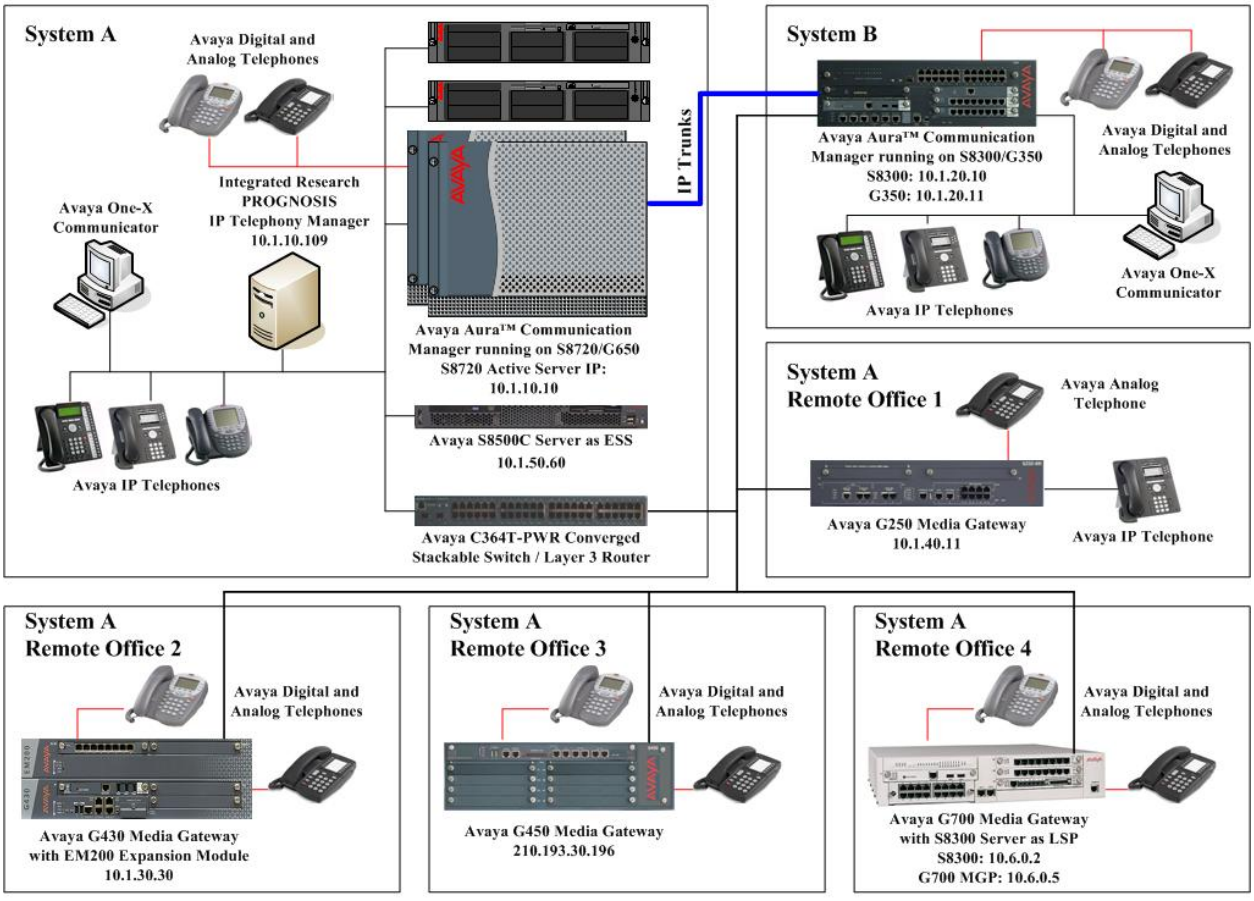


Figure 1: Test Configuration

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8720 Servers	Avaya Aura™ Communication Manager 5.2 (Service Pack 02.0.947.3-17294)
Avaya G650 Media Gateway - TN2312BP IP Server Interface - TN799DP C-LAN Interface - TN2302AP IP Media Processor - TN2602AP IP Media Processor - TN2214CP Digital Line - TN793CP Analog Line - TN2464BP DS1 Interface - TN2464CP DS1 Interface	- HW07 FW046 and HW15 FW042 HW01 FW032 and HW01 FW026 HW20 FW120 and HW20 FW117 HW02 FW048 and HW02 FW041 HW08 FW015 HW09 FW010 HW05 FW024 HW02 FW024
Avaya G250-BRI Media Gateway	29.23.0
Avaya G450 Media Gateway	29.23.0
Avaya G430 Media Gateway	29.23.0
Avaya S8300 Server as LSP	5.2 (Service Pack 02.0.947.3-17294)
Avaya G700 Media Gateway	29.23.0
Avaya S8500C Server as ESS	5.2 (Service Pack 02.0.947.3-17294)
Avaya S8300 Server	Communication Manager 5.2 (Service Pack 02.0.947.3-17294)
Avaya G350 Media Gateway - MM710BP DS1 Media Module - MM714AP Analog Media Module	29.23.0 HW11 FW047 HW04 FW073
Avaya 9600 Series IP telephones - 9630, 9640, 9650	3.002 (H.323) Service Pack 1
Avaya 9670 IP telephones	2.0 (H.323)
Avaya 1608 IP telephones	1.100 (H.323)
Avaya 6221 analog telephones	-
Avaya 2420 digital telephones	-
Avaya One-X® Communicator	R1.010-SP1-15895
Avaya C364T-PWR Converged Stackable Switch	4.5.18
Integrated Research PROGNOSIS IP Telephony Manager	9.5.2 Patch 2

4. Configure Communication Manager

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

4.1. Configure SAT User Profile

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

Step	Description
1.	Enter the **add user-profile *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 configuration, the user profile 20 is created.

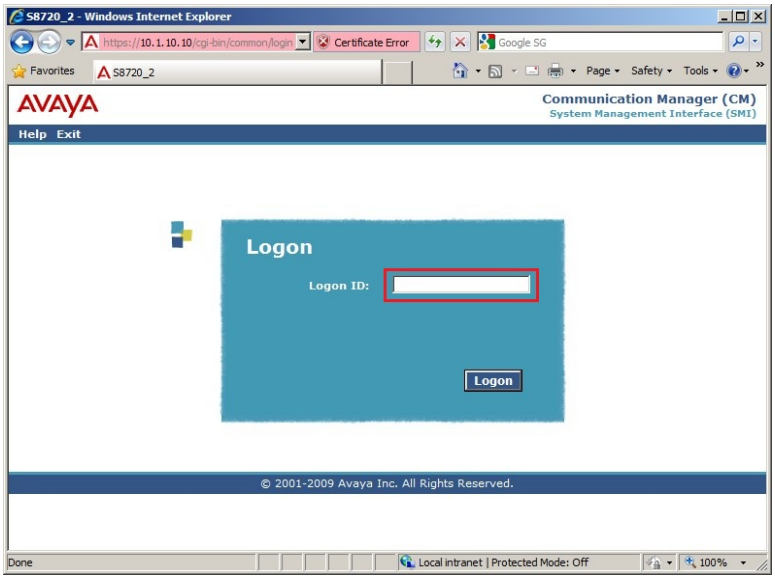
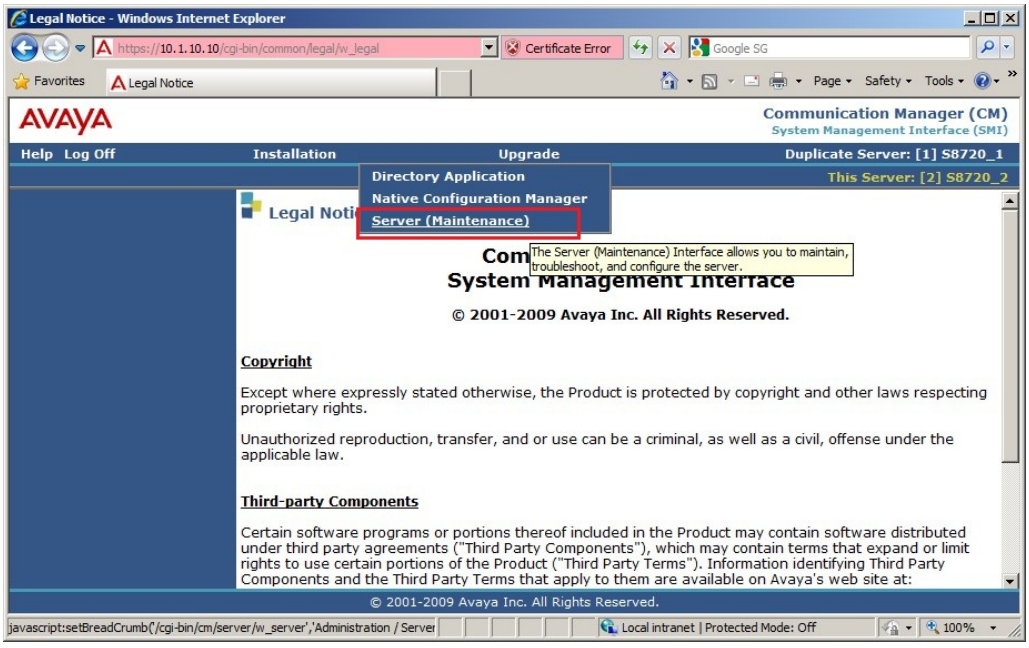
```
add user-profile 20                                          Page   1 of  41
                                USER PROFILE 20

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
```

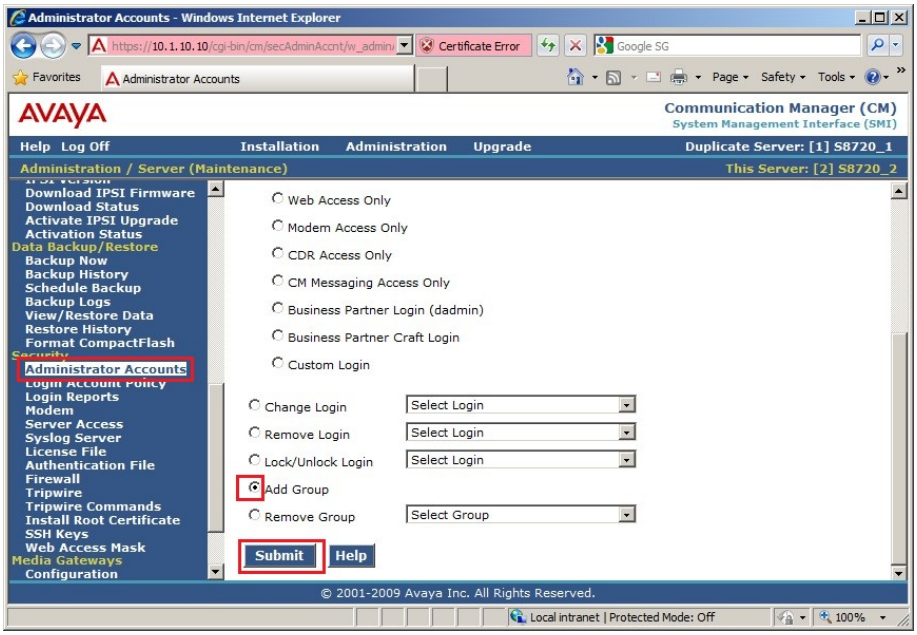
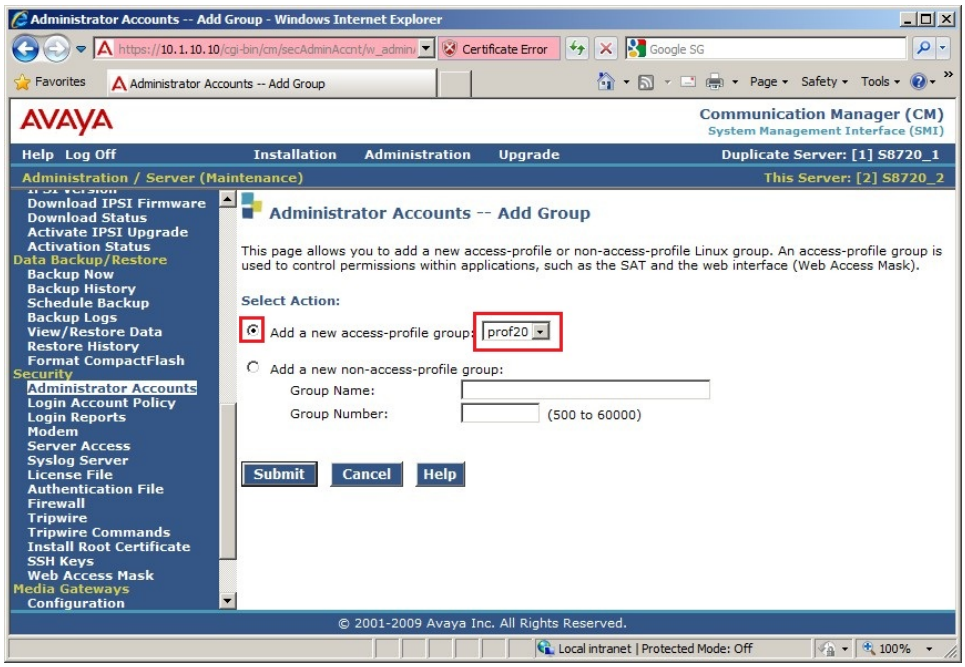
Step	Description
2.	On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the field **Set All Permissions To**. Submit the form to create the user profile.

```
add user-profile 20                                          Page   2 of  41
                                 USER PROFILE 20
 Set Permissions For Category:    To:          Set All Permissions To: rm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                   Name          Cat  Perm
                     aar analysis J    rm
              aar digit-conversion J    rm
                  aar route-chosen J    rm
abbreviated-dialing 7103-buttons C    rm
    abbreviated-dialing enhanced C    rm
       abbreviated-dialing group C    rm
    abbreviated-dialing personal C    rm
      abbreviated-dialing system C    rm
                  aca-parameters P    rm
                access-endpoints P    rm
                   adjunct-names A    rm
        administered-connections C    rm
                  aesvcs cti-link A    rm
                aesvcs interface A    rm
```

4.2. Configure Login Group

Create an Access-Profile Group to correspond to the SAT User Profile created in **Section 4.1**.

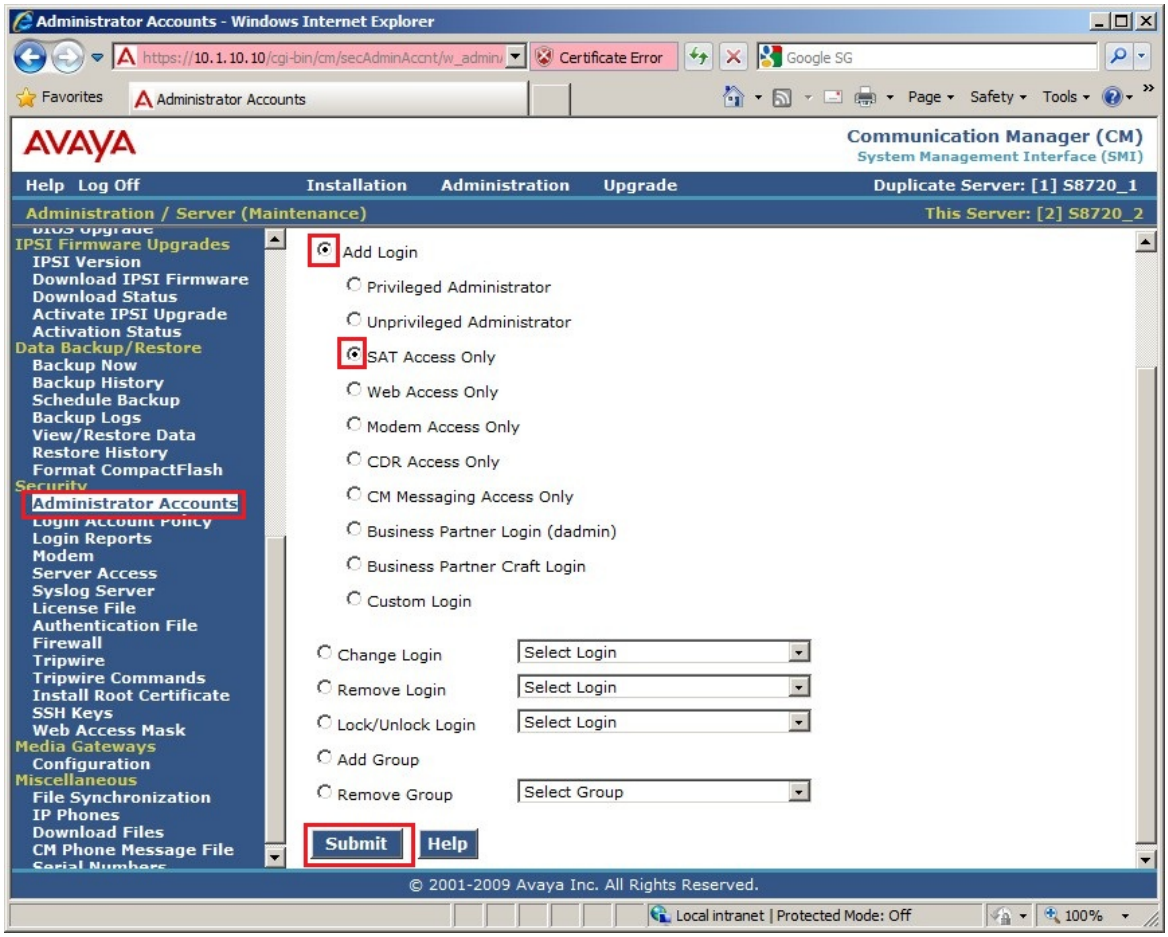
Step	Description
1.	Using a web browser, enter https://<IP address of Avaya Server> to connect to the Avaya Server being configured and log in using appropriate credentials. 
2.	Click **Administration > Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow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

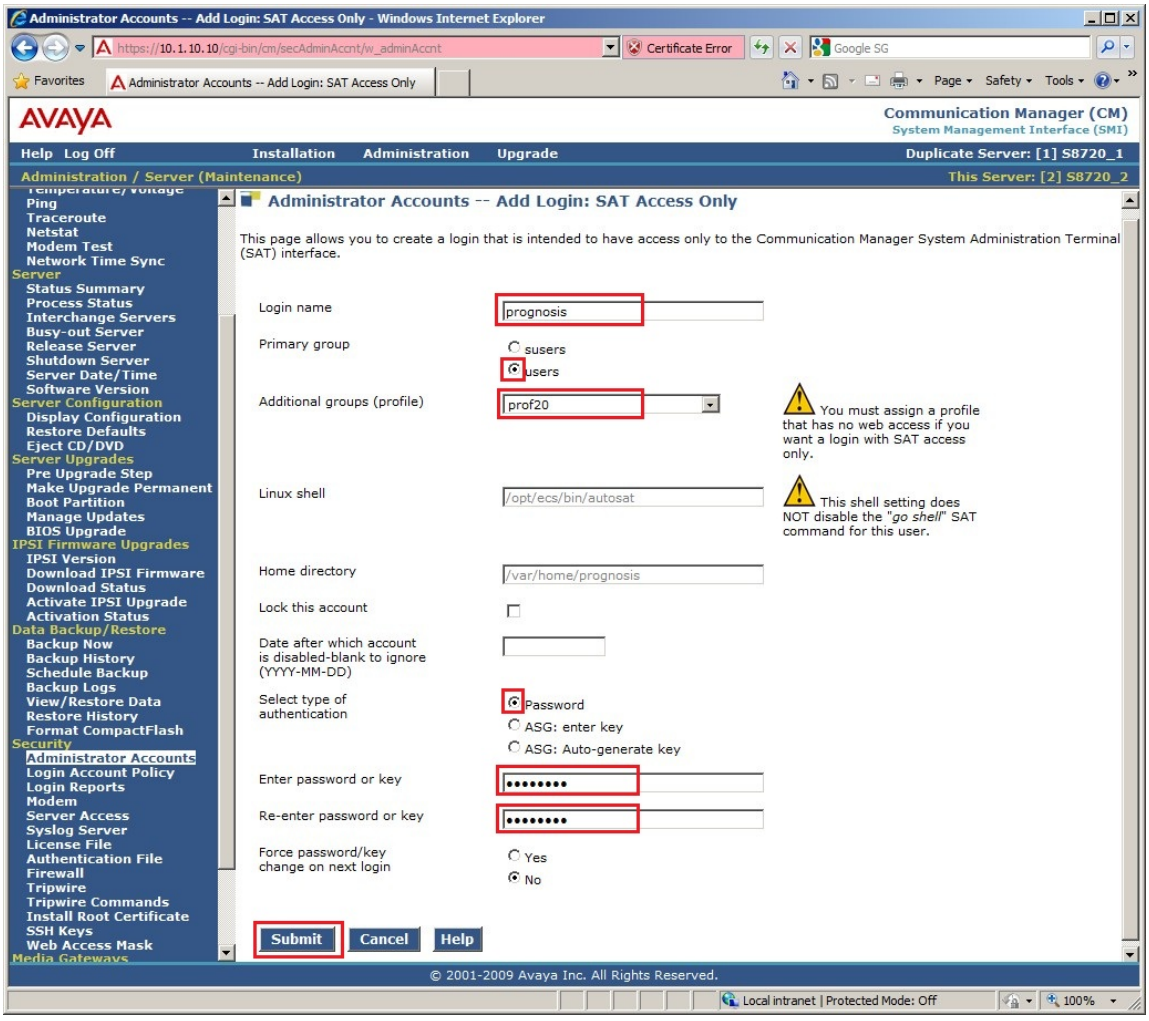
Step	Description
3.	From the navigation panel on the left side, click **Administrator Accounts**. Select **Add Group** and click **Submit**. 
4.	Select **Add a new access-profile group** and select **prof20** from the drop-down box to correspond to the user-profile created in **Section 4.1 Step 1**. Click **Submit**. This completes the creation of the login group. 

4.3. Configure Login

Create a login account for PROGNOSIS to access the Communication Manager SAT.

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 **prognosis** is created. Configure the other parameters for the login as follows: • **Primary group**: **users** [Limits the permissions of the login] • **Additional groups (profile)**: **prof20** [Select the login group created in **Section 4.2**.] • **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. 

4.4. Configure RTCP Monitoring

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

Step	Description
1.	Enter the **change system-parameters ip-options** command. In the **RTCP MONITOR SERVER** section, set **Default Server IP Address** to the IP address of the PROGNOSIS IP Telephony Manager server. Set **Default Server Port** to ***5005*** and **Default RTCP Report Period (secs)** to ***5***.

```
change system-parameters ip-options                              Page   1 of   3
                          IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                   Packet Loss (%)      High: 40       Low: 15
                   Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10

 RTCP MONITOR SERVER
         Default Server IP Address: 10 .1  .10 .109
               Default Server Port: 5005
  Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
           Link Failure? y

 H.248 MEDIA GATEWAY                  H.323 IP ENDPOINT
  Link Loss Delay Timer (min): 5       Link Loss Delay Timer (min): 5
                                         Primary Search Time (sec): 75
                                  Periodic Registration Timer (min): 20
```

Step	Description
2.	Enter the **change ip-network-region *n*** command, where ***n*** is IP network region number to be monitored. 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   1 of  19
                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain:
    Name: Local
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? y
   UDP Port Max: 65535
DIFFSERV/TOS PARAMETERS                  RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                       RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

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

4.5. Configure CDR Monitoring

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

Step	Description
1.	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   1
                                  IP INTERFACES


                 Type: PROCR
                                                  Target socket load: 19200

      Enable Interface? y                       Allow H.323 Endpoints? y
                                                 Allow H.248 Gateways? y
        Network Region: 1                         Gatekeeper Priority: 5



                                 IPV4 PARAMETERS
             Node Name: procr
           Subnet Mask: /24
```

2.	Enter the **change node-names ip** command to add a new node name for the PROGNOSIS server. In this configuration, the name **prognosis** is added with the IP address specified as **10.1.10.109**. Note also the node name **procr** which is automatically added.

```
change node-names ip                                         Page   1 of   2
                                  IP NODE NAMES
    Name                  IP Address
clan1                  10.1.10.21
clan2                  10.1.10.22
default                0.0.0.0
medpro1                10.1.10.31
medpro2                10.1.10.32
procr                  10.1.10.10
val1                   10.1.10.41
prognosis              10.1.10.109
```

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 this CLAN to send out the CDR] • **Local Port: 0** [The Local Port is set to 0 because Communication Manager initiates the CDR link.] • **Remote Node: prognosis** [The Remote Node is set to the node name previously defined in Step 1.] • **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
CDR1                    procr           0       prognosis      50000
```

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

```
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
```

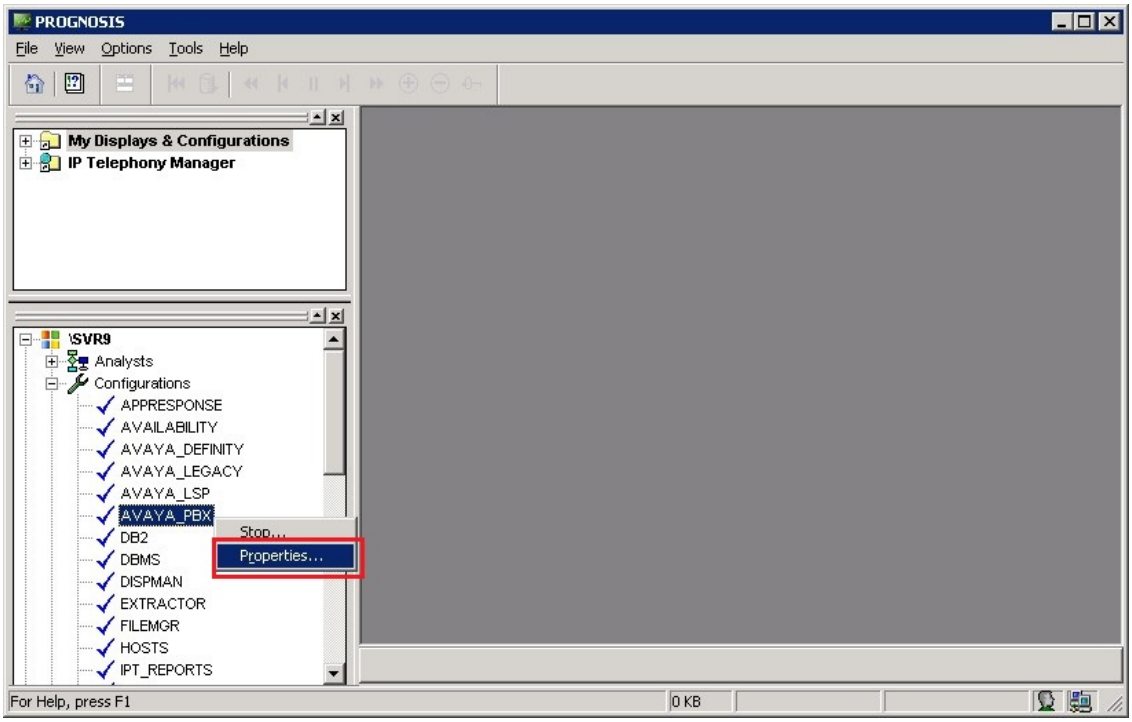
Step	Description
4.	Enter the **change system-parameters cdr** command to set the parameters for the type of calls to track and the format of the CDR data. The following settings were used during the compliance test. • **CDR Date Format**: **month/day** • **Primary Output Format**: **unformatted** [This value is used to configure PROGNOSIS in **Section 5 Step 3**.] • **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.]

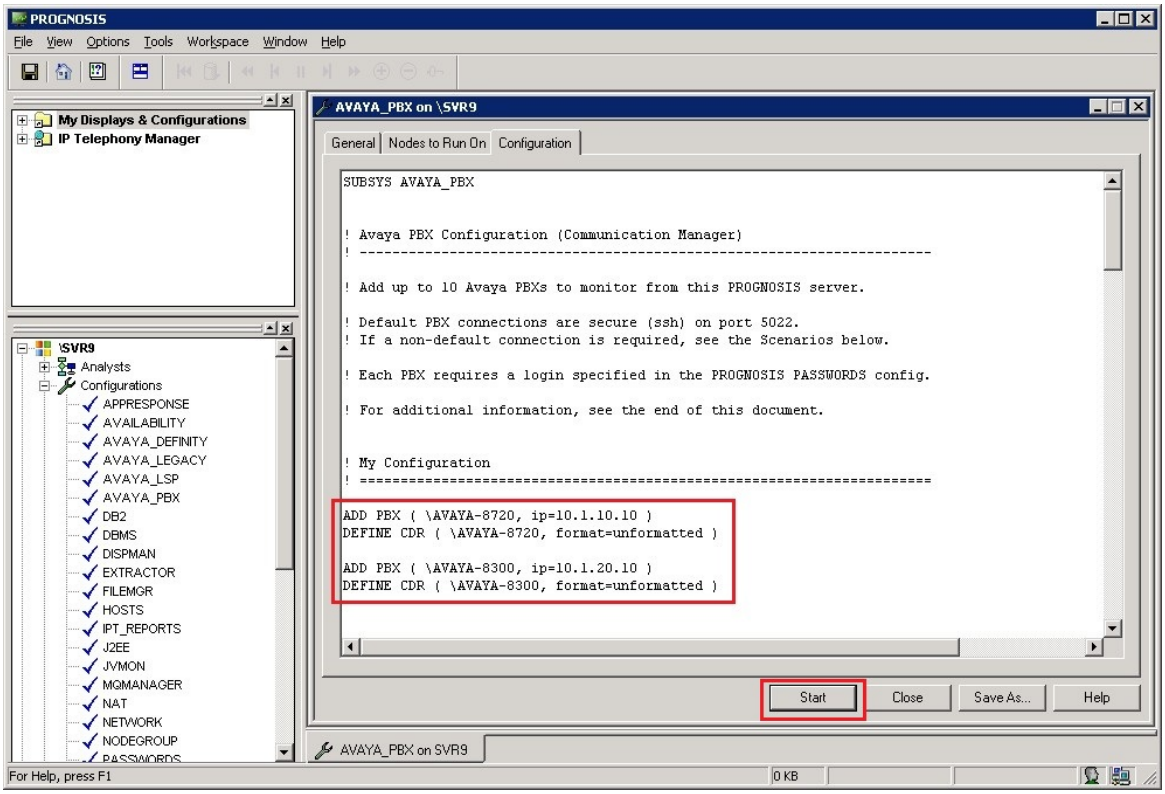
```
change system-parameters cdr                                    Page   1 of   1
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID):                        CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format:              Secondary Output Endpoint:
           Use ISDN Layouts? n                    Enable CDR Storage on Disk? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? n
      Use Legacy CDR Formats? y                 Remove # From Called Number? n
Modified Circuit ID Display? n                              Intra-switch CDR? y
                  Record Outgoing Calls Only? n     Outg Trk Call Splitting? y
  Suppress CDR for Ineffective Call Attempts? y       Outg Attd Call Record? y
      Disconnect Information in Place of FRL? n      Interworking Feat-flag? n
 Force Entry of Acct Code for Calls Marked on Toll Analysis Form? n
                                   Calls to Hunt Group - Record: member-ext
Record Called Vector Directory Number Instead of Group or Member? n
Record Agent ID on Incoming? n       Record Agent ID on Outgoing? y
     Inc Trk Call Splitting? n
  Record Non-Call-Assoc TSC? n           Call Record Handling Option: warning
      Record Call-Assoc TSC? n   Digits to Record for Outgoing Calls: dialed
   Privacy - Digits to Hide: 0               CDR Account Code Length: 15
```

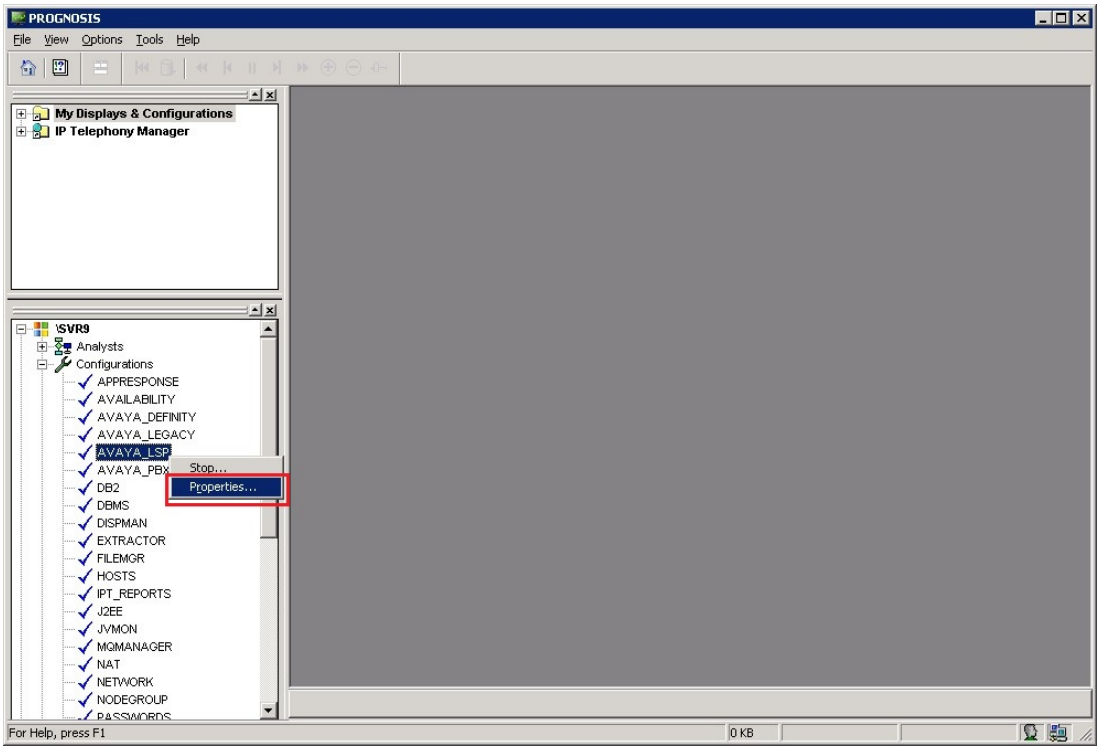
Step	Description
5.	If the **Intra-switch CDR** field is set to **y** on Page 1 of the CDR SYSTEM PARAMETERS form, then enter the **change intra-switch-cdr** command to define the extensions that will be subjected to call detail recording. In the **Assigned Members** field, enter the specific extensions whose usage will be tracked with the CDR records.
	`change intra-switch-cdr` Page 1 of 3 INTRA-SWITCH CDR Assigned Members: 8 of 5000 administered Extension Extension Extension Extension **10001** **10002** **10003** **10004** **10005** **10006** **10007** **10008**
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 2` Page 1 of 21 TRUNK GROUP Group Number: 2 Group Type: isdn CDR Reports: **y** Group Name: ISDN-BRI to PSTN COR: 95 TN: 1 TAC: 702 Direction: two-way Outgoing Display? n Carrier Medium: PRI/BRI Dial Access? y Busy Threshold: 255 Night Service: Queue Length: 0 Service Type: public-ntwrk Auth Code? n TestCall ITC: rest Far End Test Line No: TestCall BCC: 4

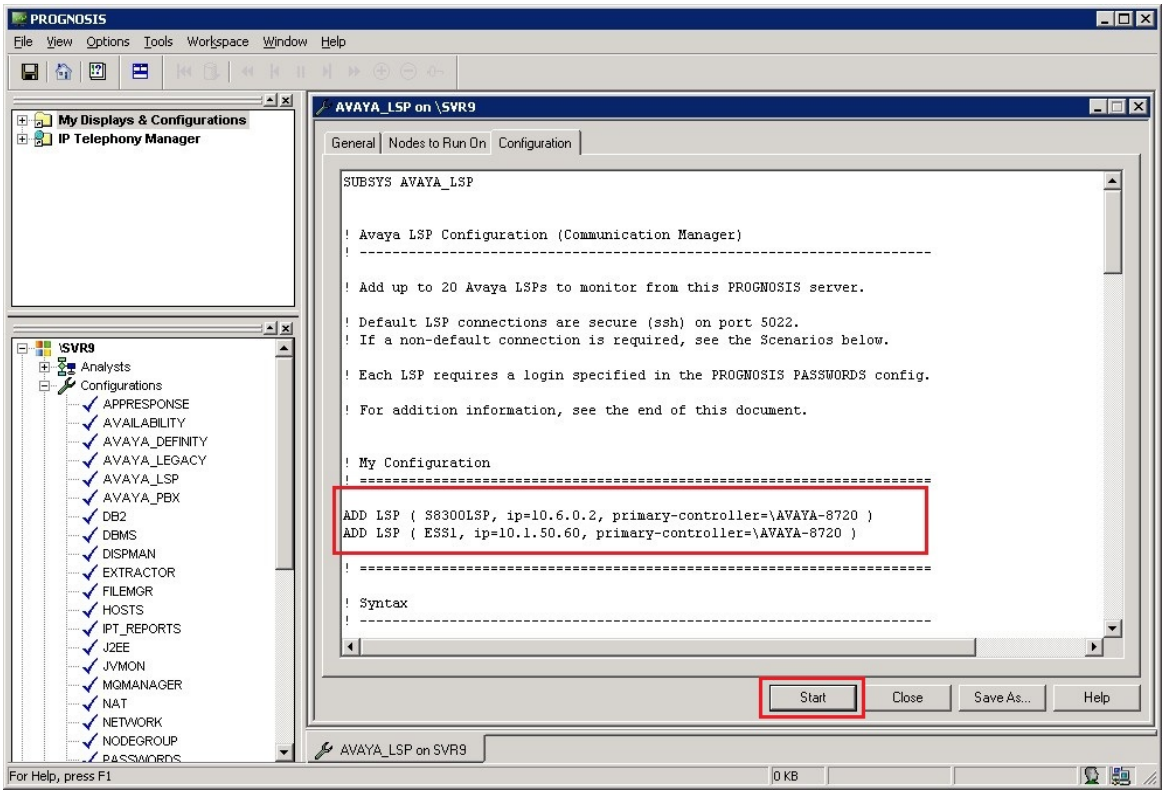
5. Configure Integrated Research PROGNOSIS IP Telephony Manager

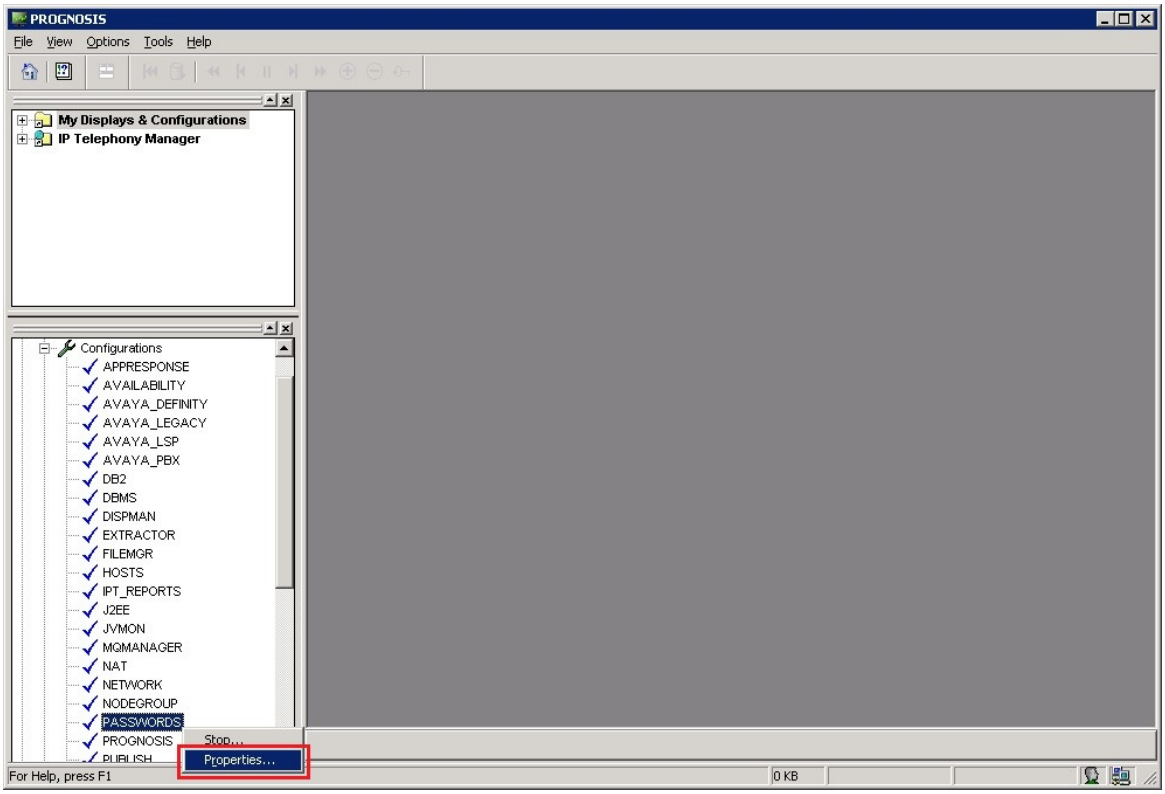
This section describes the configuration of Integrated Research PROGNOSIS IP Telephony Manager required to interoperate with Communication Manager.

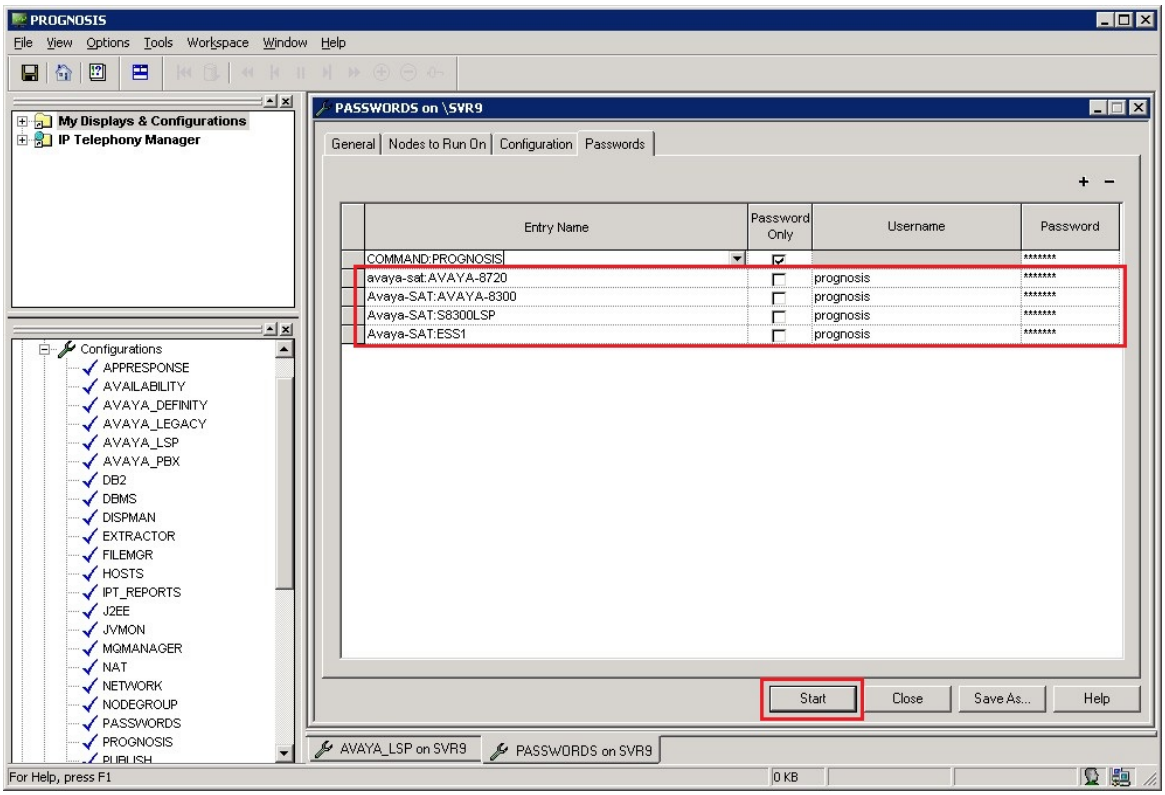
Step	Description
1.	On the Integrated Research PROGNOSIS IP Telephony Manager server, click **Start > All Programs > PROGNOSIS IP Telephony Manager > IP Telephony Manager GUI** to start the IP Telephony Manager GUI application. Enter a valid Windows user account and password to log in.
2.	To configure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

Step	Description
3.	In the **Configuration** tab, add an entry for each Communication Manager system to be managed. The template to add a system is provided in the PROGNOSIS GUI application. In this test configuration, the following entries are added for the two Communication Manager systems with the names **AVAYA-S8720** and **AVAYA-S8300** and with the IP addresses of the Avaya Servers **10.1.10.10** and **10.1.20.10** respectively. The PROGNOSIS Monitoring Node will use SSH to connect to port 5022 of the Avaya Servers by default. ADD PBX (\AVAYA-S8720, ip=10.1.10.10) ADD PBX (\AVAYA-S8300, ip=10.1.20.10) Define the CDR format to match the settings configured on Communication Manager in **Section 4.5 Step 2 and 3** respectively. DEFINE CDR (\AVAYA-S8720, format=unformatted) DEFINE CDR (\AVAYA-S8300, format=unformatted) Click **Start** to proceed. 

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

Step	Description
5.	In the **Configuration** tab, add an entry for each ESS or LSP Servers to be monitored. The template to add the server is provided in the PROGNOSIS GUI application. In this test configuration, the following entries are added for the ESS and LSP Servers with the names **ESS1** and **S8300LSP** and with the IP addresses of **10.1.50.60** and **10.6.0.2** respectively, both belonging to the **AVAYA-S8720** Communication Manager system. ADD LSP (S8300LSP, ip=10.6.0.2, primary-controller=\AVAYA-S8720) ADD LSP (ESS1, ip=10.1.50.60, primary-controller=\AVAYA-S8720) Click **Start** to proceed. 

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

Step	Description
7.	Click the **+ 'plus'** button to add a new password entry for each of the configured systems in **Steps 3** and **5**. The **Entry Name** must be of the form avaya-sat:<pbx-name>. For the system with the name **S8720**, enter **avaya-sat:S8720** for **Entry Name**, uncheck **Password Only**, and enter the login account created in **Section 4.3** for **Username** and **Password**. Repeat to add another three entries for the second system **S8300**, the ESS and LSP Servers. Click **Start** to proceed. 

6. General Test Approach and Test Results

The general test approach was to use PROGNOSIS GUI to display the configurations of the Communication Manager systems and verify against what is displayed on the SAT interface. The SAT interface is accessed by using either telnet or Secure Shell (SSH) to the Avaya S8720 and S8300 Servers. Calls were placed between various Avaya endpoints and PROGNOSIS GUI was used to display the RTCP and CDR information collected.

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

For serviceability testing, reboots were applied to the PROGNOSIS IP Telephony Manager Server and Avaya Servers to simulate system unavailability. Interchanging of the Avaya S8720 Servers and failover to ESS and LSP were also performed during testing.

All test cases passed successfully. The following observation was made during testing:

1. The RTCP information sent out by the TN2602AP IP MEDPRO board did not include the correct IP address of the board. This caused PROGNOSIS IP Telephony Manager to classify voice streams from conference calls incorrectly when using this board.

7. Verification Steps

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

7.1. Verify Communication Manager

Verify that PROGNOSIS IP Telephony Manager has established three concurrent SSH connections to the SAT by using the **status logins** command.

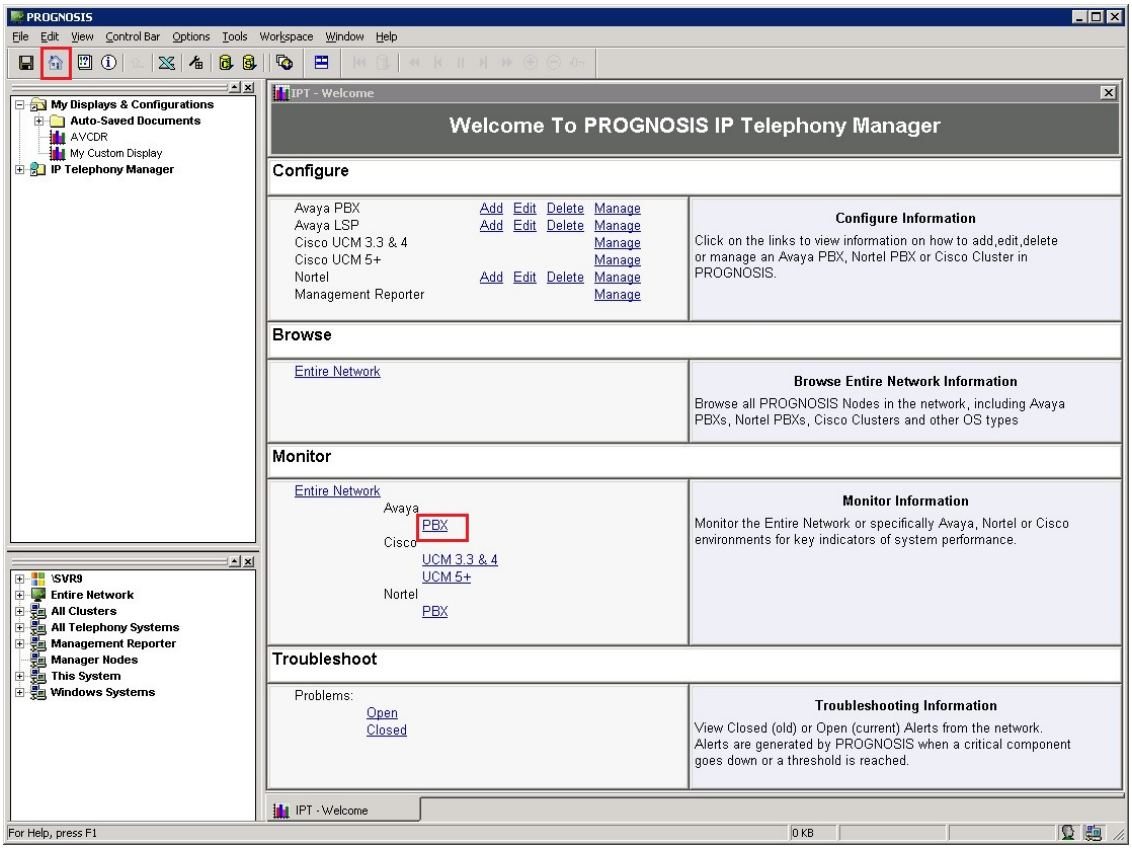
```
status logins

                    COMMUNICATION MANAGER LOGIN INFORMATION

Login     Profile   User's Address       Active Command               Session

*dadmin      2       10.1.10.152       stat logins                      1
 prognosi    20      10.1.10.109       list measurements summary        3
 prognosi    20      10.1.10.109       list registered-ip-stations      4
 prognosi    20      10.1.10.109       stat trunk 10                    5
```

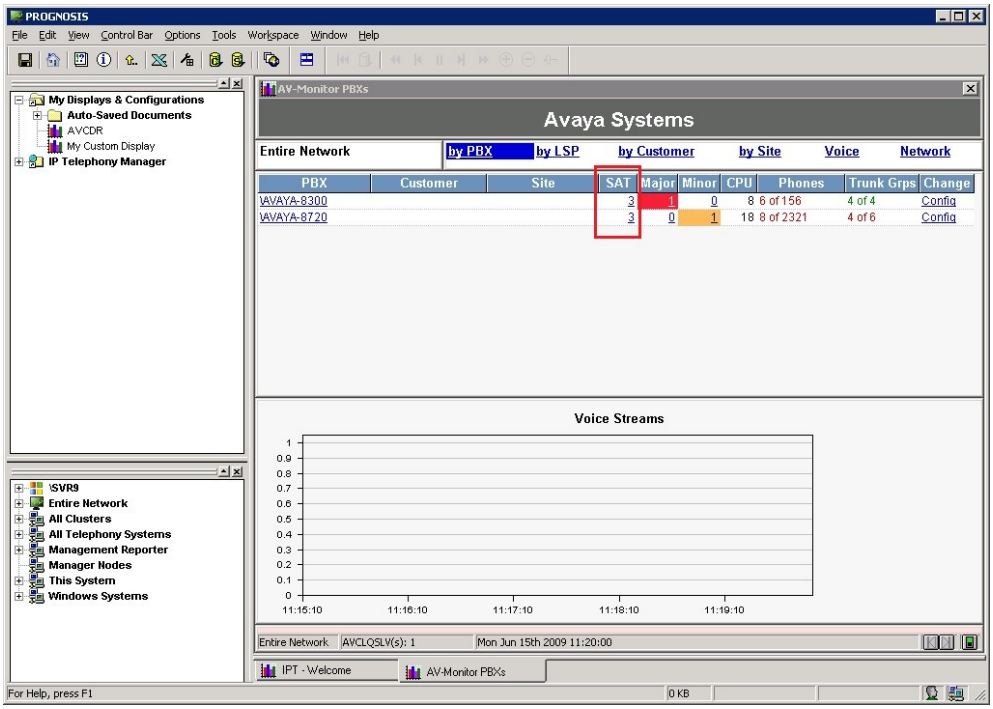
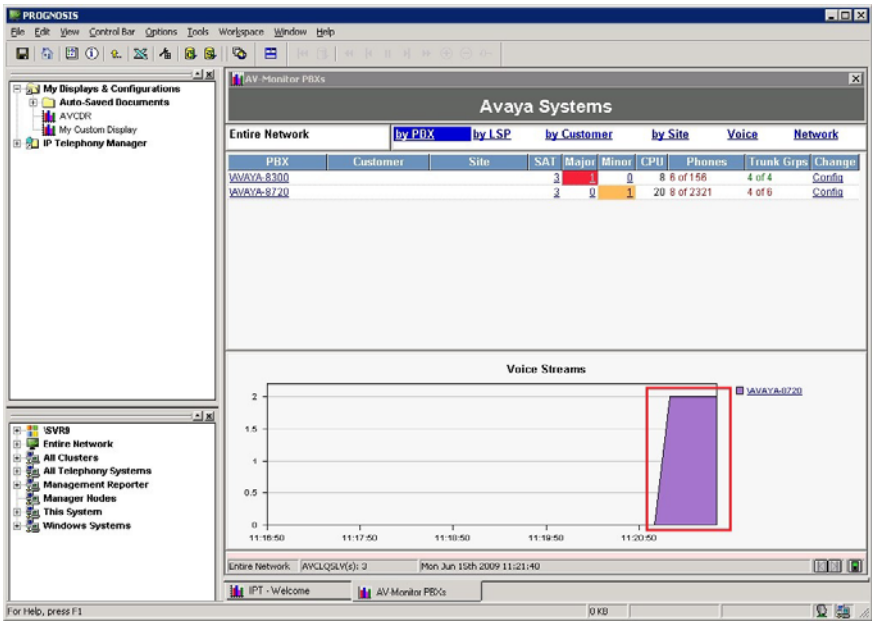
Using the **status cdr-link** command, verify that the **Link State** of the primary CDR link configured in **Section 4.5** shows **up**.

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

       Link State: up                             CDR not administered

      Date & Time: 2009/7 /15 11:27:48            0   /0 /0  0 :0 :0
  Forward Seq. No: 0                              0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.02                           0.00
      Reason Code: OK
```

7.2. Verify Integrated Research PROGNOSIS IP Telephony Manager

The following steps are done using the PROGNOSIS GUI.

Step	Description
1.	After logging into PROGNOSIS GUI, click on the **Home** button on the toolbar to display the **Welcome** screen. In the **Monitor** section, click **Entire Network** > **Avaya** > **PBX** to display the list of Communication Manager Servers configured in **Section 5**. 

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

8. Conclusion

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

9. Additional References

The following document can be found at http://support.avaya.com:

[1] *Avaya Aura™ Communication Manager Feature Description and Implementation*, Release 5.2, Issue 7, May 2009, Document Number 555-245-205.
[2] *Administering Avaya Aura™ Communication Manager*, Release 5.2, Issue 5.0, May 2009, Document Number 03-300509.

The following PROGNOSIS documentations are provided by Integrated Research.

[3] *PROGNOSIS IP Telephony Manager 9.5 Installation Guide*, April 2009
[4] *PROGNOSIS IP Telephony Manager 9.5 User Guide*, April 2009

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.