Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the procedures for configuring Integrated Research PROGNOSIS IP Telephony Manager to interoperate with Avaya 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 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 multiple IP Telephony vendors.

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

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 9.0.1 with Avaya Communication Manager 4.0.1.

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 the monitored systems. In some case the monitoring node may actually exist as an agent running on the monitored system but in the case of Avaya Communication Manager, all monitoring nodes are separate servers.

- 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 two methods to monitor an Avaya Communication Manager system.

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

- **RTCP Collection** - The PROGNOSIS IP Telephony Manager collects RTCP information sent by Avaya Communication Manager IP Media Processor boards, media gateways and IP Telephones.

Figure 1 illustrates the test configuration used to verify Integrated Research PROGNOSIS IP Telephony Manager interoperability with Avaya Communication Manager. It consists of an Avaya Communication Manager system running on a pair of Avaya S8720 Servers with an Avaya G650 Media Gateway and a second system running on an Avaya S8300 Server with an Avaya G700 Media Gateway. Both systems have Avaya IP, Digital and analog telephones, and Avaya IP Softphone and Avaya IP Agent users configured for making and receiving calls. IP Trunks connects 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 with Service Pack 1. Both the Monitoring Node and GUI software are installed on this server. All the systems and telephones are connected using two Avaya C364T-PWR Converged Stackable Switches for network connectivity.

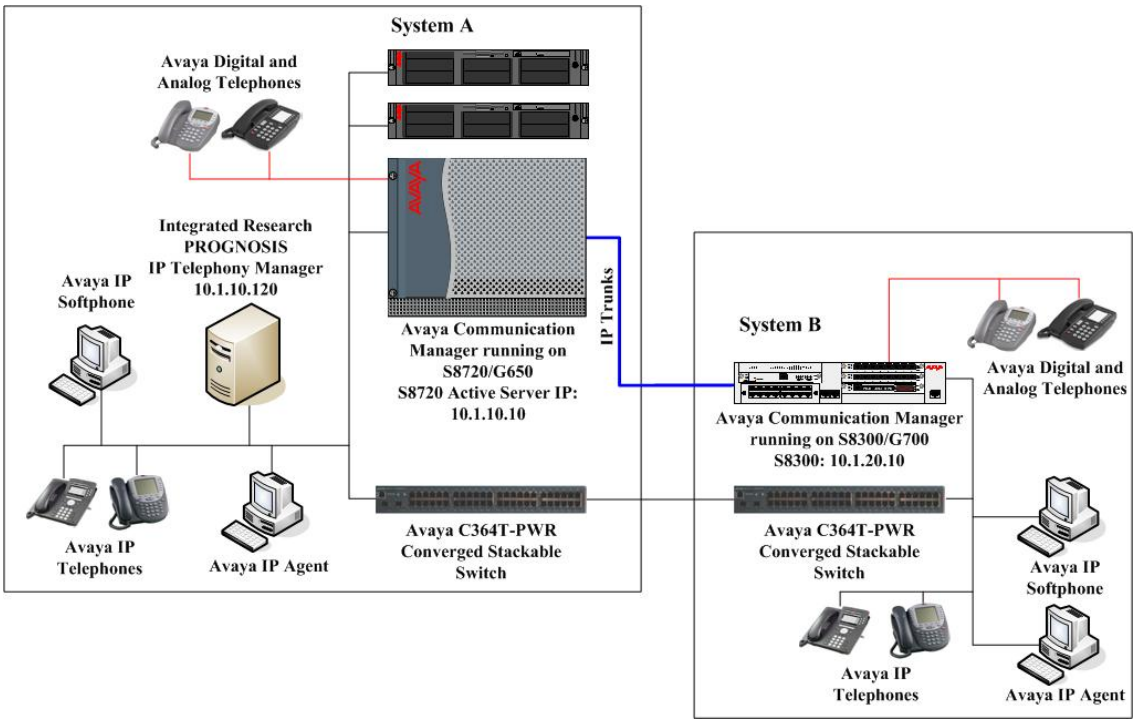


Figure 1: Test Configuration

2. Equipment and Software Validated

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

Equipment	Software
Avaya S8720 Servers	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2) with Service Pack 2 (00.1.731.2-14878)
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	- HW15, FW042 HW01, FW026 HW20, FW117 HW02, FW033 HW08, FW015 HW09, FW010
Avaya S8300 Server	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2) with Service Pack 2 (00.1.731.2-14878)
Avaya G700 Media Gateway • MM760AP VOIP Media Module • MM714AP Analog Media Module	26.36.0 HW01, FW072 HW04, FW071

Avaya 4600 Series IP telephones	2.8.3 (H.323)
Avaya 9600 Series IP telephones	1.5 (H.323)
Avaya 6200 Series analog telephones	-
Avaya 2400 Series digital telephones	-
Avaya IP Softphone	6.0 Service Pack 2
Avaya IP Agent	7.0.23.116
Avaya C364T-PWR Converged Stackable Switches	4.5.18
Integrated Research PROGNOSIS IP Telephony Manager	9.0.1 Patch 14
Microsoft Windows Server 2003 Standard	Service Pack 1

3. Configure Avaya Communication Manager

This section describes the steps needed to configure Avaya Communication Manager to interoperate with Integrated Research PROGNOSIS IP Telephony Manager. This section describes the steps to create a login account and a SAT User Profile for PROGNOSIS to access Avaya Communication Manager and the steps to enable RTCP reporting. The steps are repeated for each Avaya Communication Manager system.

3.1. 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
```

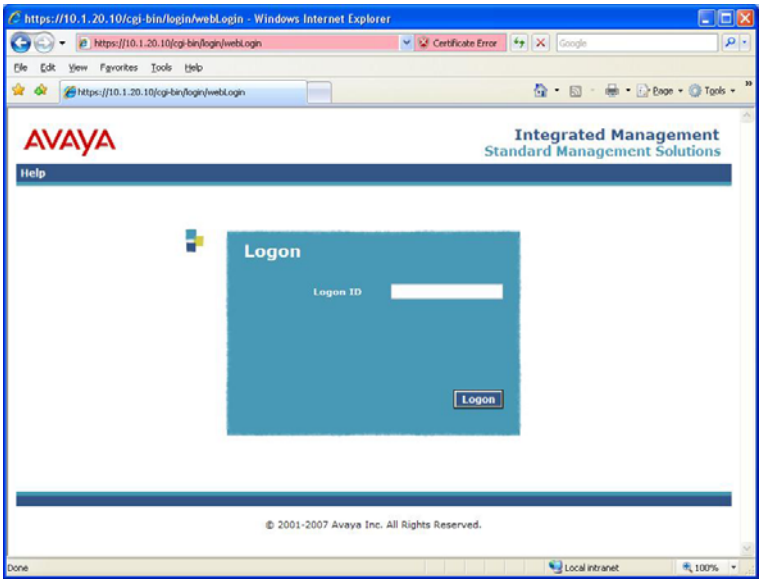
Step	Description
2.	On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to **rm** (read and maintenance). This can be accomplished by typing **rm** into the field **Set All Permissions To**. Submit the form to create the user profile.

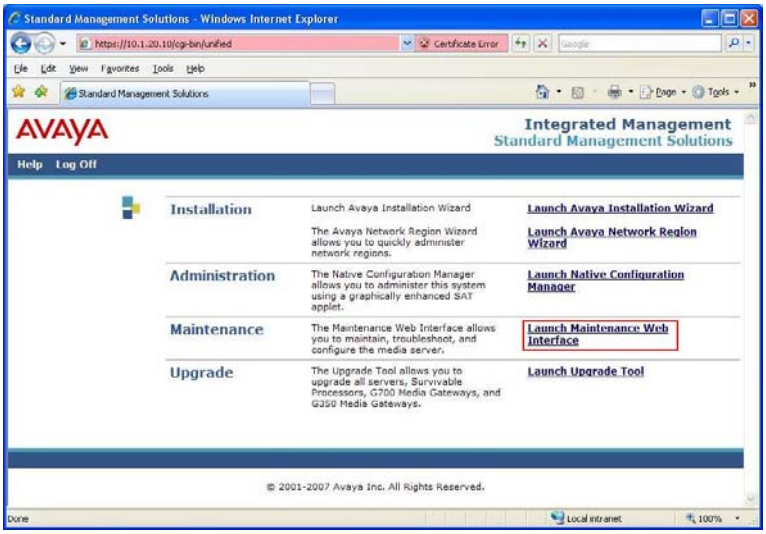
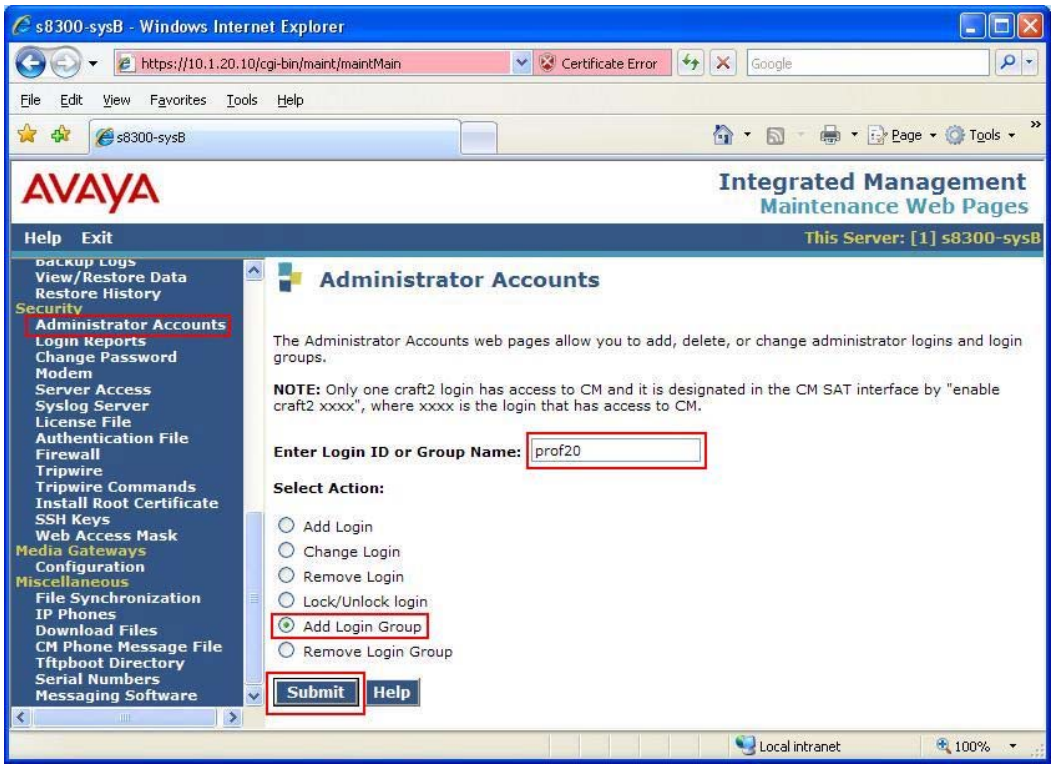
```
add user-profile 20                                          Page   2 of  41
                                USER PROFILE 20
 Set Permissions For Category:    To:          Set All Permissions To: rm

                   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
```

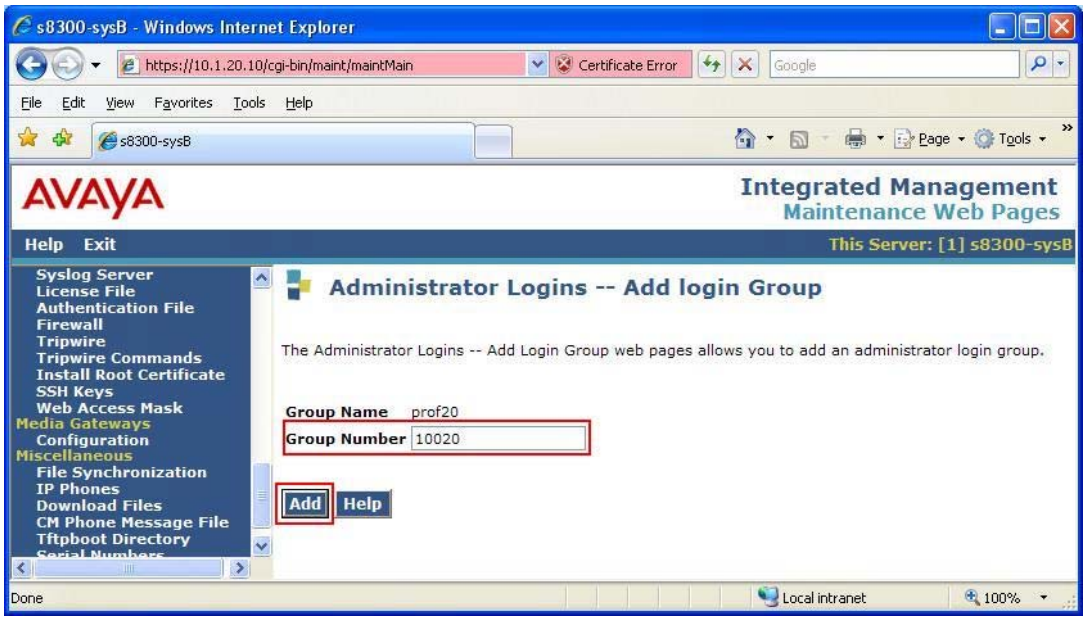
3.2. Configure Login Group

Create a Login Group in the range 10,020 - 10,069 to correspond to the SAT User Profile created in **Section 3.1**.

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.

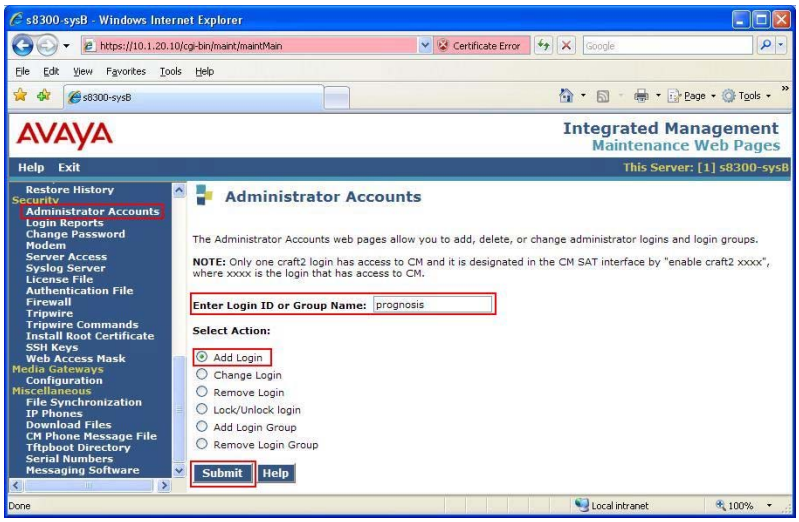


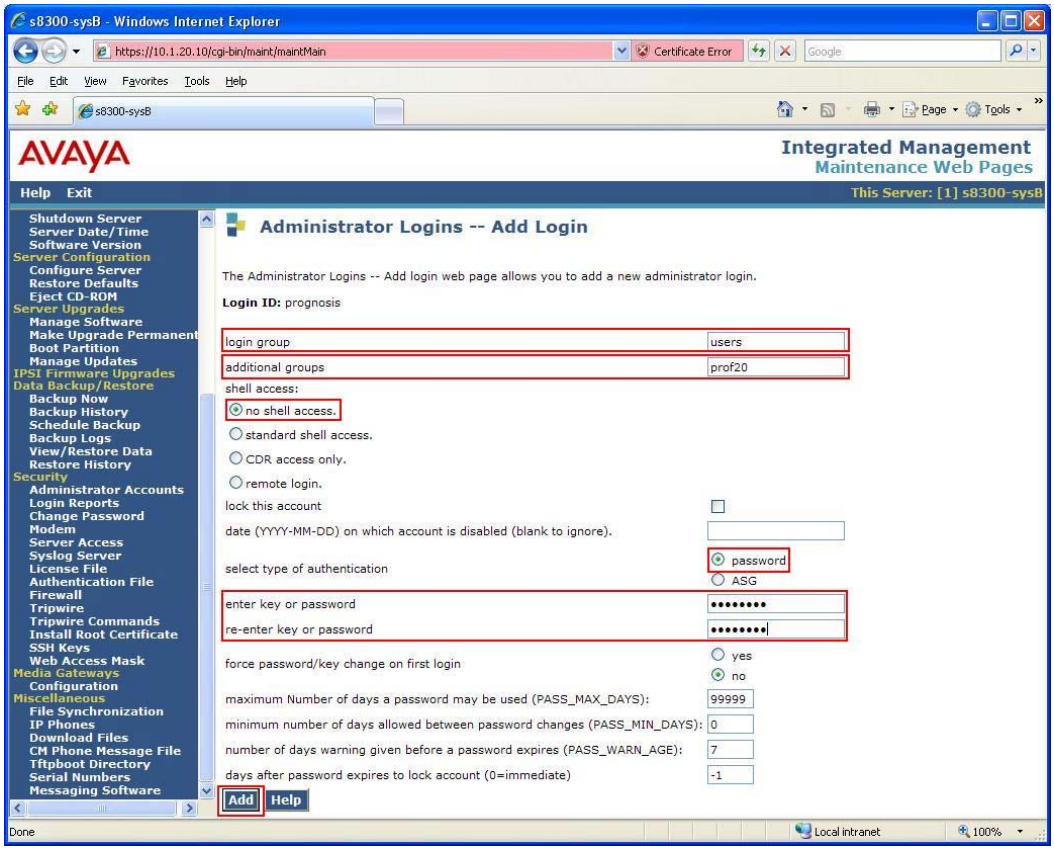
Step	Description
2.	Click **Launch Maintenance Web Interface**. This will open up the **Maintenance Web Pages** in a new window that will allow the user to complete the configuration process. 
3.	From the navigation panel on the left side, click **Administrator Accounts**. For the field **Enter Login ID or Group Name**, Avaya recommends the group name be in the form prof<nn> where nn is the group number. In this configuration, the group **prof20** is created to correspond to the user profile 20. Select **Add Login Group** and click **Submit**. 

Step	Description
4.	For the Group Number field, enter the value **10020**, which is obtained by adding the Access Mask Base (default value of 10000) to the user profile number. Click **Add**. This completes the creation of the login group. 

3.3. Configure Login

Create a login account for PROGNOSIS to access the SAT.

Step	Description
1.	From the navigation panel on the left side, click **Administrator Accounts**. For the field **Enter Login ID or Group Name**, enter the login to be created. In this configuration, the login **prognosis** is created. Select **Add Login** and click **Submit**. 

Step	Description
2.	On the Administrator Logins -- Add Login page, configure the login as follows: • **login group**: **users** [Limits the permissions of the login] • **additional groups**: **prof20** [Enter the login group created in **Section 3.2**.] • **shell access: no shell access** [Shell access not required.] • **select type of authentication: password** [Uses a password for authentication.] • **enter key or password / re-enter key or password** [Define the password] Click **Add** to continue. This completes the configuration of the login. 

3.4. Configure RTCP Monitoring

To allow PROGNOSIS IP Telephony Manager to monitor the quality of IP calls, configure Avaya Communication Manager to send RTCP reporting to the IP address of the PROGNOSIS server.

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 .120
               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
```

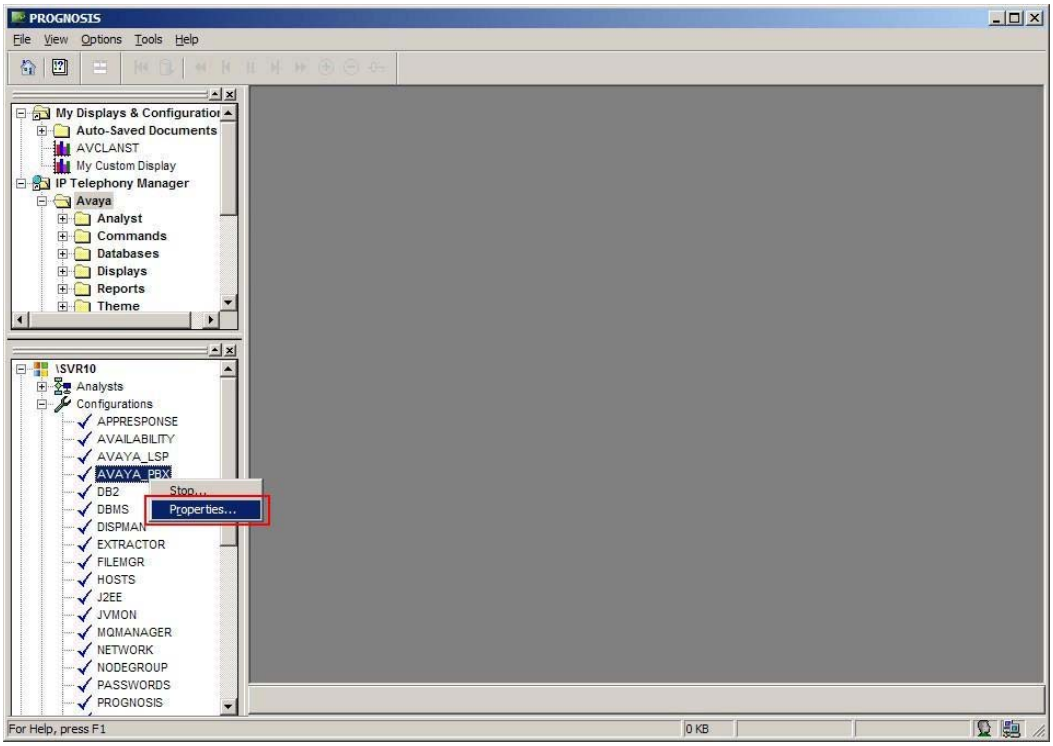
2.	Enter the **change ip-network-region *n*** command, where ***n*** is IP network region number to be monitored. Set **RTCP Reporting Enabled** to ***y*** and **Use Default Server Parameters** to ***y***. Note: Only one RTCP MONITOR SERVER can be configured per IP network region.

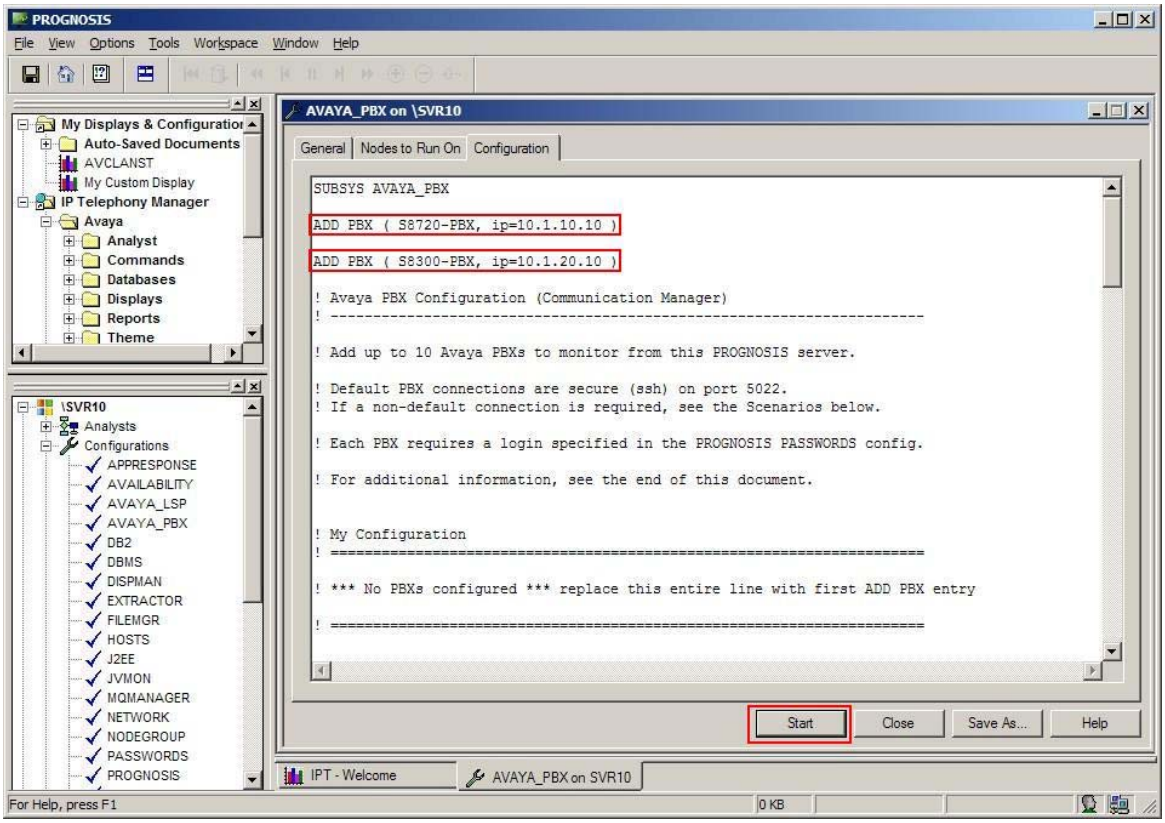
```
change ip-network-region 1                                       Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain:
    Name: Local
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              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
```

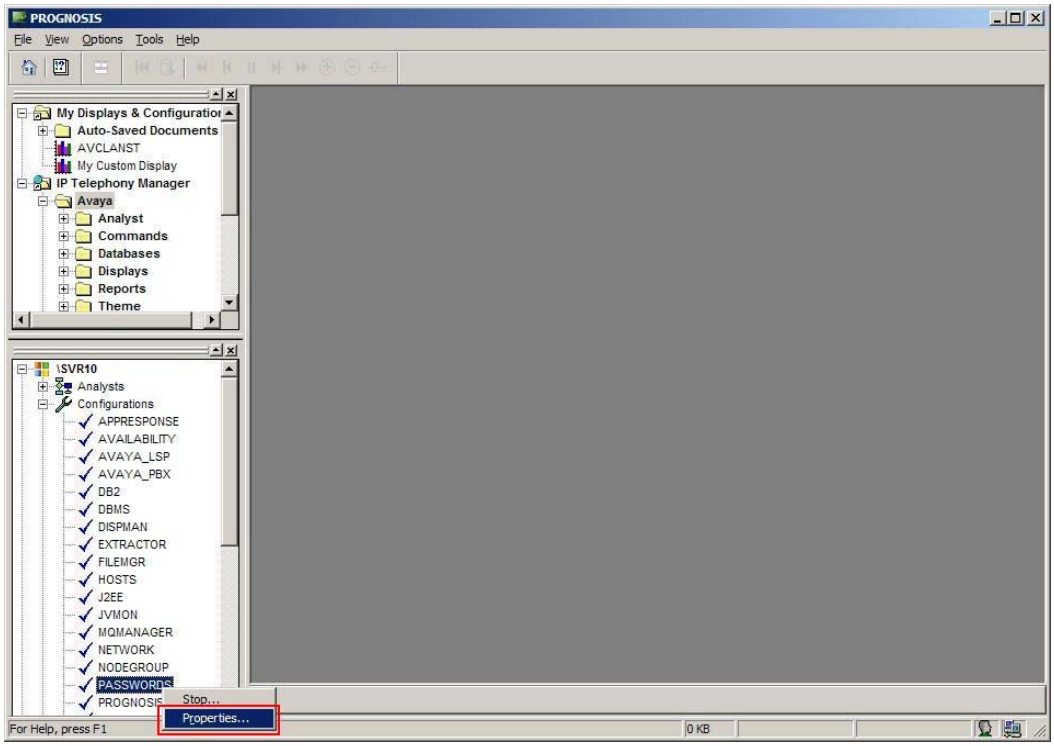
Step	Description
3.	Repeat **Step 2** for all IP network regions that are required to be monitored.

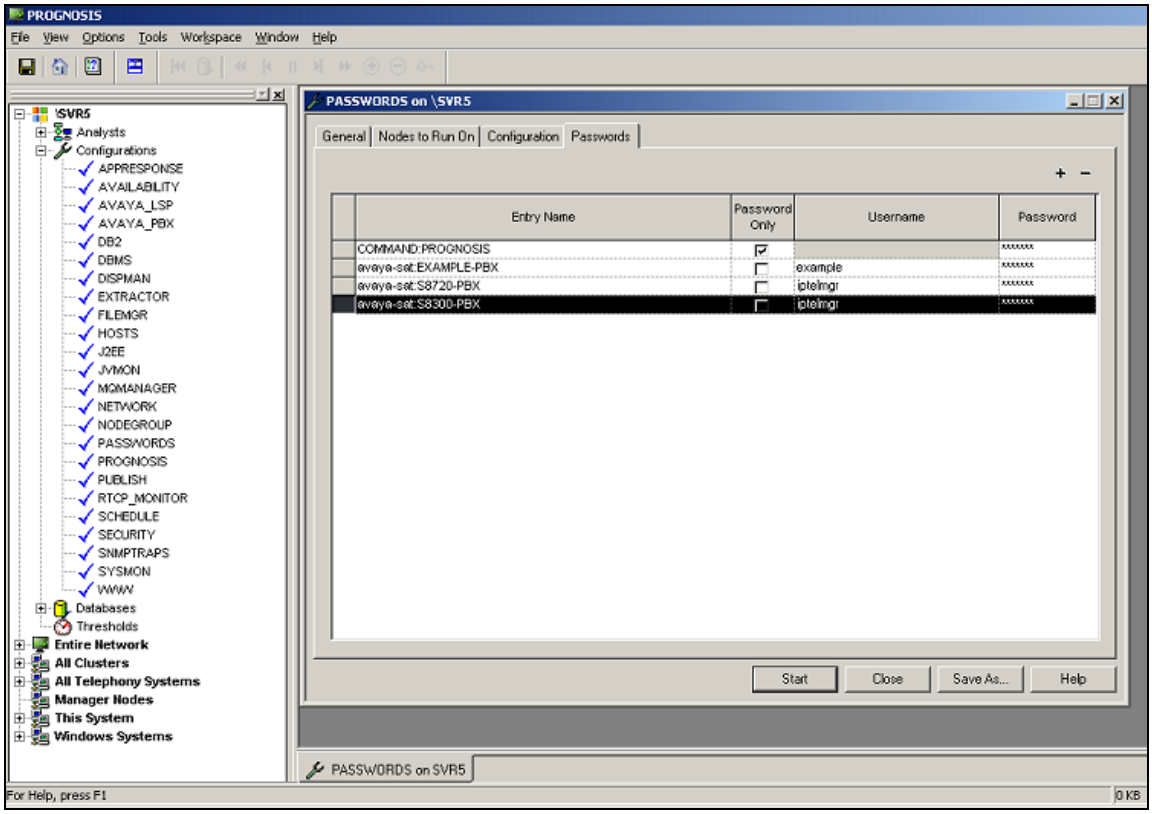
4. Configure Integrated Research PROGNOSIS IP Telephony Manager

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

Step	Description
1.	On the Integrated Research PROGNOSIS IP Telephony Manager server, click **Start > All Programs > PROGNOSIS IP Telephony Manager > PROGNOSIS GUI** to start the PROGNOSIS GUI application. Enter a valid Windows user account and password to log in.
2.	To configure the Avaya 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 **Configurations** tab, add an entry for each Avaya Communication Manager system to be managed. The template to add a system is provided in the PROGNOSIS GUI application. In this sample configuration, the following entries are added for the two Avaya Communication Manager systems with the names **S8720-PBX** and **S8300-PBX** 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 (\S8720-PBX, ip=10.1.10.10) ADD PBX (\S8300-PBX, ip=10.1.20.10) Click **Start** to proceed. 

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

Step	Description
5.	Click the **+ 'plus'** button to add a new password entry for each of the configured system in **Step 3**. The **Entry Name** must be of the form avaya-sat:<pbx-name>. For the system with the name **S8720-PBX**, enter **avaya-sat:S8720-PBX** for **Entry Name**, uncheck **Password Only**, and enter the login account created in **Section 3.3** for **Username** and **Password**. Repeat to add another entry for the second system **S8300-PBX**. Click **Start** to proceed. This completes the configuration for PROGNOSIS IP Telephony Manager. 

5. 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 an Avaya Communication Manager system. In addition, the ability of PROGNOSIS IP Telephony Manager to receive and process RTCP information from Avaya Communication Manager and Avaya IP endpoints 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 Avaya Server interchange.

5.1. General Test Approach

The general test approach was to use the PROGNOSIS GUI to display the configurations of Avaya 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 the PROGNOSIS GUI was used to display the RTCP information collected.

For feature testing, PRONOSIS GUI was used to view the configurations of Avaya Communication Manager such as media gateways, cabinets, port networks, 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. For the collection of RTCP information, the endpoints included Avaya IP, digital and analog telephones, and Avaya IP Softphone and IP Agent users.

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 was also performed during testing.

5.2. Test Results

All test cases passed successfully. Integrated Research PROGNOSIS IP Telephony Manager successfully interoperates with Avaya Communication Manager.

6. Verification Steps

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

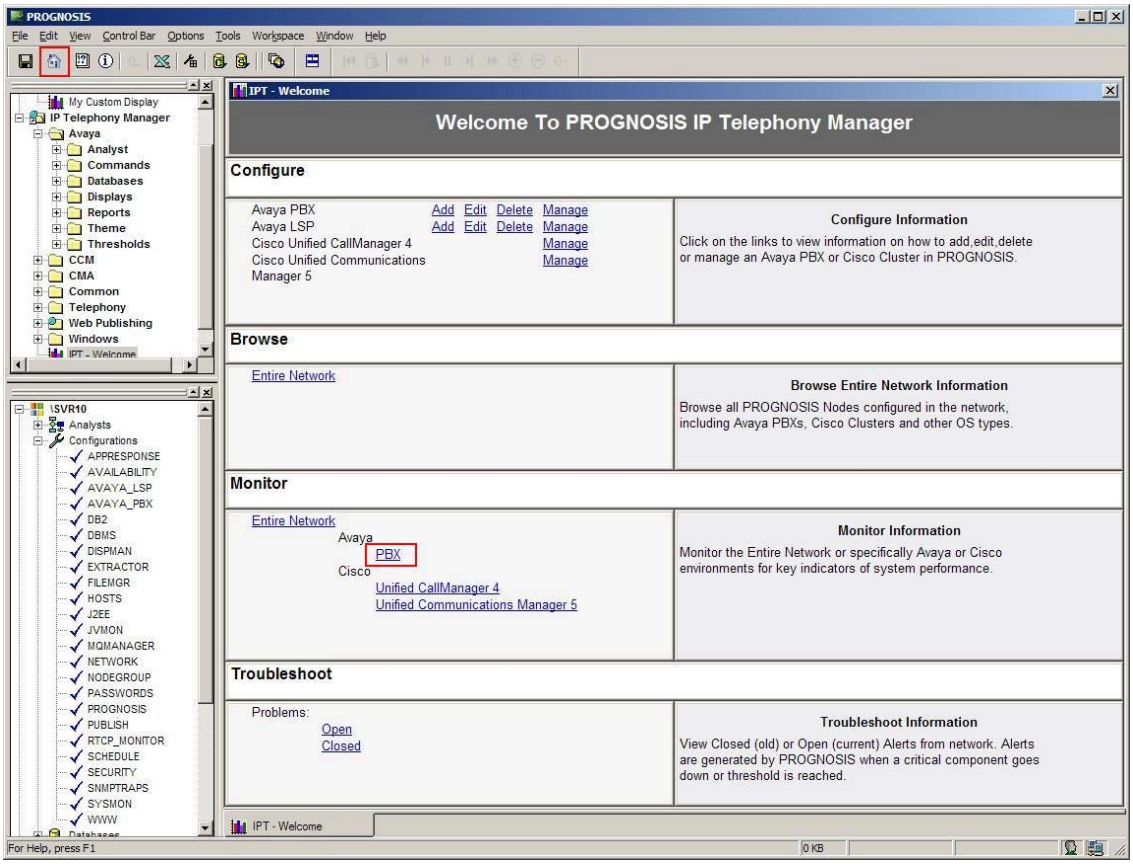
6.1. Verify Avaya Communication Manager

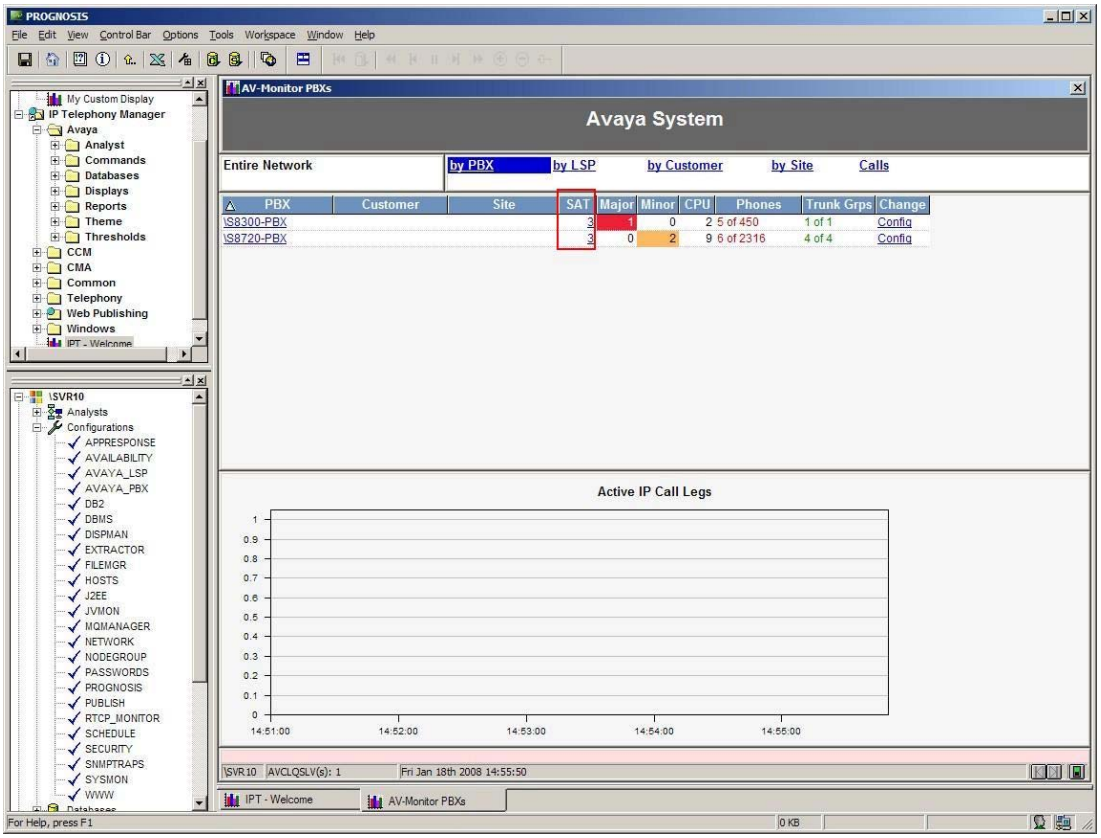
Verify that PROGNOSIS IP Telephony Manager has established three concurrent SSH connections to the SAT by using the **status logins** command.

```
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      10.1.10.120       list measurements summary         3
 prognosi    20      10.1.10.120       list registered-ip-stations       4
 prognosi    20      10.1.10.120       stat trunk 10                     5
```

6.2. 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 Avaya Communication Manager Servers configured in **Section 4**. 

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

7. 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

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research PROGNOSIS IP Telephony Manager 9.0.1 to interoperate with Avaya Communication Manager Release 4.0.1. In the configuration described in these Application Notes, the PROGNOSIS IP Telephony Manager established SSH connections to the SAT to view the configurations of Avaya Communication Manager and to monitor for failures. PROGNOSIS IP Telephony Manager also processed the RTCP information to monitor the quality of IP calls. During compliance testing, all test cases were completed successfully.

9. Additional References

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

[1] *Feature Description and Implementation For Avaya Communication Manager*, Release 4.0, Issue 5, February 2007, Document Number 555-245-205.
[2] *Administrator Guide for Avaya Communication Manager*, Release 4.0, Issue 3, February 2007, Document Number 03-300509.

The following PROGNOSIS documentations are provided by Integrated Research.

[3] *Installation Guide for PROGNOSIS IP Telephony Manager 9.0*
[4] *User Guide for PROGNOSIS IP Telephony Manager 9.0*

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.