



## Avaya Solution & Interoperability Test Lab

# **Application Notes for Integrated Research's Collaborate - Prognosis Server 12.1 with Avaya Aura® Communication Manager R10.1 - Issue 1.0**

## **Abstract**

These Application Notes describe the procedures for configuring Collaborate Prognosis Server R12.1 (Prognosis) to interoperate with Avaya Aura® Communication Manager R10.1.

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

Prognosis integrates directly to Communication Manager using Secure Shell (SSH) or Telnet and uses Simple Network Management Protocol (SNMP) to query Communication Manager. At the same time, Prognosis processes Real-time Transport Control Protocol (RTCP) and Call Detail Recording (CDR) information from Communication Manager.

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

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

# 1. Introduction

These Application Notes describe the compliance tested configuration used to validate Collaborate - Prognosis Server R12.1 (herein after referred to as Prognosis) with Avaya Aura® Communication Manager R10.1.

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

- System Access Terminal (SAT) - The Prognosis uses a pool of Telnet/SSH connections to the SAT using the IP address of Communication Manager. By default, the solution establishes three concurrent SAT connections to each Communication Manager system and uses the connections to execute SAT commands.
- Real Time Transport Control Protocol (RTCP) collection - Prognosis collects RTCP information sent by Avaya resources including IP Media Processor (MEDPRO) boards, media gateways, media servers and IP Deskphones.
- Call Detail Recording (CDR) collection - Prognosis collects CDR information sent by Communication Manager.
- Simple Network Management Protocol (SNMP) - Prognosis uses SNMP to read Communication Manager name and IP address as this information cannot be collected via the standard SAT interface.

## 2. General Test Approach and Test Results

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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

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

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

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

## **2.1. Interoperability Compliance Testing**

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

For the collection of RTCP and CDR information, the endpoints included Avaya H323, SIP, digital and analog endpoints and Avaya Workplace Client and Avaya Agent for Desktop user. The types of calls made included intra-switch calls, inbound/outbound inter-switch IP trunk calls, outbound trunk calls, transfer and conference calls.

For serviceability testing, reboots were applied to Prognosis and Communication Manager to simulate system unavailability. Interchanging of the duplex Communication Manager and loss of network connections were also performed during testing.

## **2.2. Test Results**

All test cases passed successfully with observations below:

- a. Load testing is not within the scope and so it was not conducted.
- b. Firmware compatibility check with Communication Manager R10.1 is not available in this version of Prognosis software.
- c. System Capacities displayed for percentage used in Software Entities, Physical Devices and Call Center Counts are not calculated.

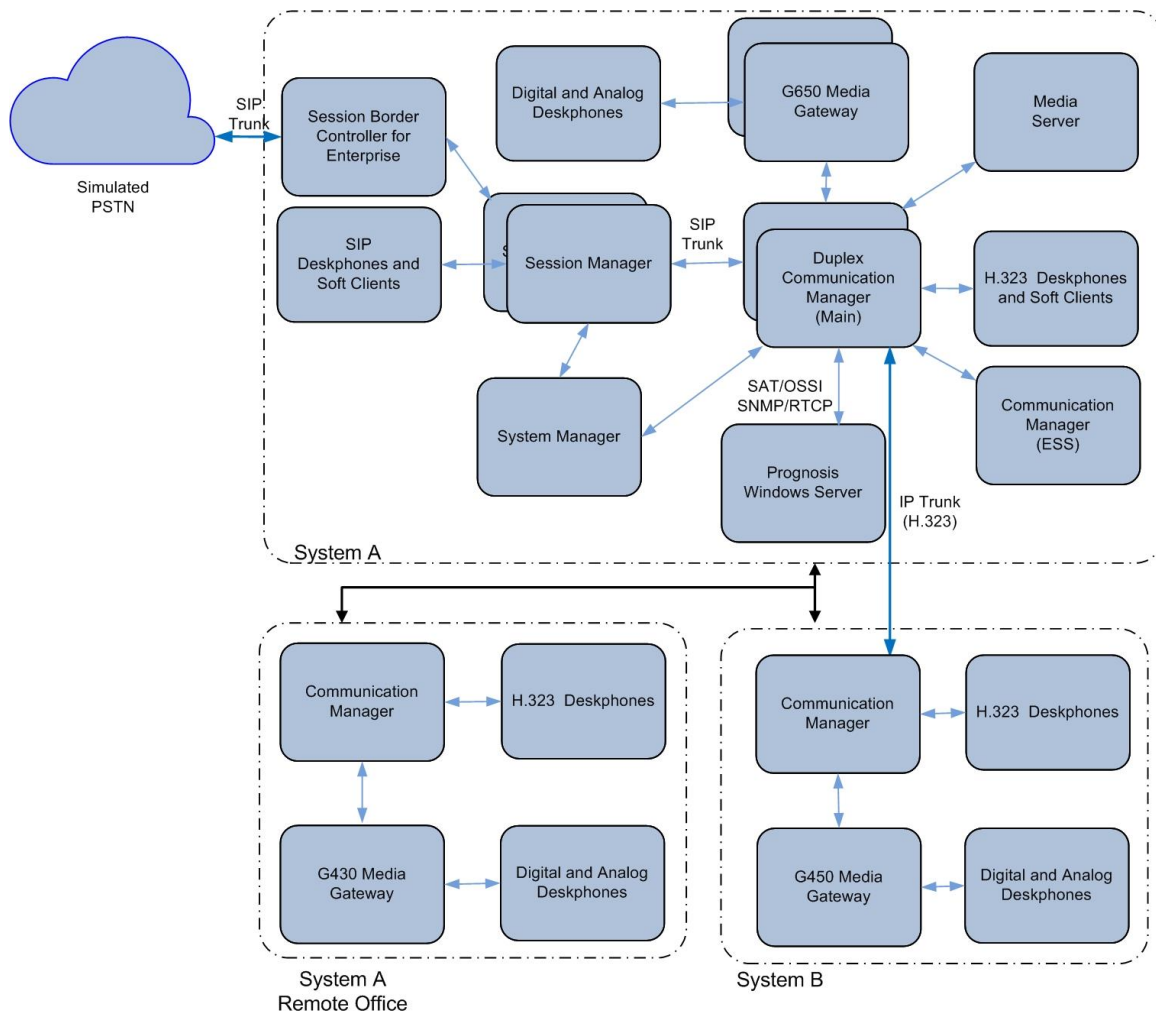
## **2.3. Support**

For technical support on Integrated Research Prognosis, contact the Integrated Research Support Team at:

- Hotline: +61 (2) 9966 1066
- Email: [support@ir.com](mailto:support@ir.com)

### 3. Reference Configuration

**Figure 1** illustrates the test configuration used to verify Prognosis interoperability with Communication Manager. The configuration consists of a duplex Communication Manager system (System A) with two Avaya G650 Media Gateways and an Avaya G430 Media Gateway with Communication Manager as a Local Survivability Processor (LSP). A simplex Enterprise Survivable Server (ESS) was also configured for failover testing. A second Communication Manager system (System B) runs on a simplex Communication Manager system with an Avaya G450 Media Gateway. Both systems have Avaya H323, SIP, digital and analog endpoints, Avaya Workplace Client (SIP) and Avaya Agent for Desktop (H.323) user configured for making and receiving calls. IP trunks connect the two systems together to allow calls between them. Avaya Aura® System Manager and Avaya Aura® Session Manager provided SIP support to the Avaya SIP endpoints. Prognosis was installed on Microsoft Windows Server 2019. Both the Monitoring Node and Web Application software are installed on this server. Avaya Session Border Controller for Enterprise was used to complete a SIP trunk connection to simulate a PSTN connection to the Enterprise solution.



**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)	10.1 (10.1.0.0.0.974.27293)
Avaya Aura® Media Server	8.0.2.218
G650 Media Gateway - TN2312BP IP Server Interface - TN799DP C-LAN Interface - TN2602AP IP Media Processor - TN2302AP IP Media Processor - TN2464BP DS1 Interface - TN2464CP DS1 Interface - TN793CP Analog Line - TN2214CP Digital Line - TN2501AP Announcement	HW07, FW058 HW01, FW044 HW02 FW067 HW20 FW121 HW05, FW025 HW02 FW025 HW09, FW012 HW08, FW016 HW03 FW023
Avaya Aura® Communication Manager (LSP)	10.1 (10.1.0.0.0.974.27293)
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	42.4.0 HW01 FW008 HW10 FW0104 HW03 FW015 HW11 FW054
Avaya Aura® Communication Manager (System B)	10.1 (10.1.0.0.0.974.27293)
G430 Media Gateway - MM712AP DCP MM - MM716AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	42.4.0 HW04 FW015 HW12 FW104 HW31 FW104 HW05 FW022
Avaya Aura® Communication Manager (ESS)	10.1 (10.1.0.0.0.974.27293)
Avaya Aura® System Manager	10.1 Build No. - 10.1.0.0.537353 Software Update Revision No: 10.1.0.0.0614119
Avaya Aura® Session Manager	10.1 (10.1.0.0.1010019)
J100 Series IP Telephones - J179 - J129	4.0.11.0 (SIP) 6.8511 (H323)
96x1 Series IP Telephones - 9611G - 9641G	6.8511 (H323)

Equipment/Software	Release/Version
Avaya Workplace Client for Windows	3.26 (SIP)
1600 Series IP Telephones - 1616 - 1603SW	1.312 (H.323)
Digital Telephones - 1400 Series	R48
Avaya Analog Phones	-
Avaya Agent for Desktop	2.0.6.20.3007 (H.323)
Collaborate – Prognosis Server running on Microsoft Windows Server 2019	12.1

**Note:** All Avaya Aura® systems and Prognosis run on VMware 6.7 virtual platform.

## 5. Configure Avaya Aura® Communication Manager

This section describes the steps needed to configure Communication Manager to interoperate with Prognosis. This includes the following:

1. Configure SAT user profile
2. Configure login group
3. Configure login
4. Configure SNMP
5. Configure RTCP monitoring
6. Configure CDR monitoring

These 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.

Enter the **add user-profile *n*** command, where *n* is the next unused profile number. Enter a descriptive name for **User Profile Name** and enable all categories by setting the **Enbl** field to **y**. In this test configuration, the user profile 23 is created.

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

User Profile Name: PROGNOSIS

This Profile is Disabled? n      Shell Access? n
Facility Test Call Notification? n Acknowledgement Required? n
Grant Un-owned Permissions? n    Extended Profile? n

Name      Cat  Enbl      Name      Cat  Enbl
Adjuncts  A    y      Routing and Dial Plan J    y
Call Center B    y      Security      K    y
Features  C    y      Servers      L    y
Hardware  D    y      Stations     M    y
Hospitality E    y      System Parameters N    y
IP        F    y      Translations  O    y
Maintenance G    y      Trunking     P    y
Measurements and Performance H    y      Usage       Q    y
Remote Access I    y      User Access  R    y
```



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 23

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**.

Using a web browser, enter *https://<IP address of Communication Manager>* to connect to the Communication Manager server being configured and log in using appropriate credentials.

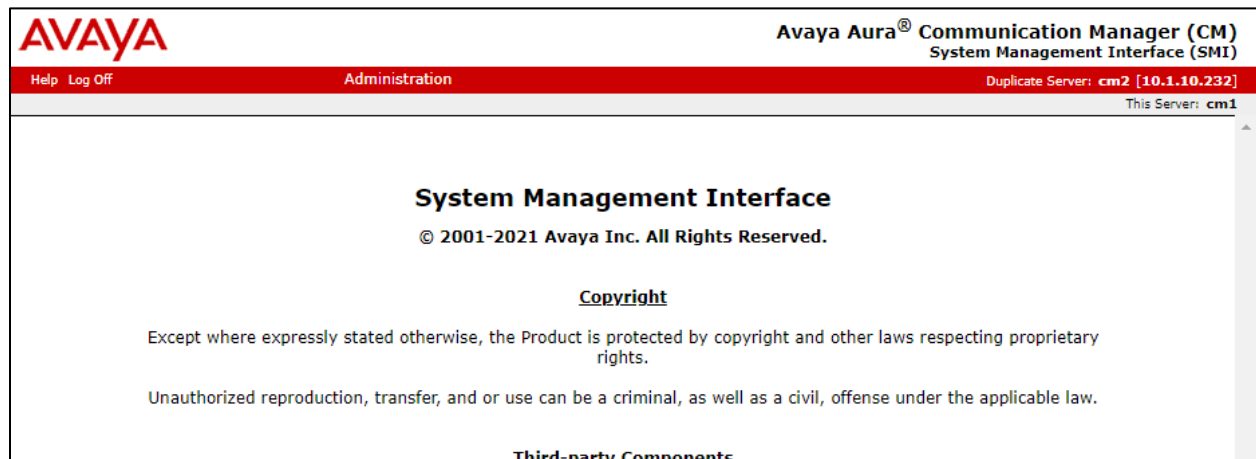
**AVAYA** Avaya Aura® Communication Manager (CM)  
System Management Interface (SMI)

Help Log Off This Server: cm1

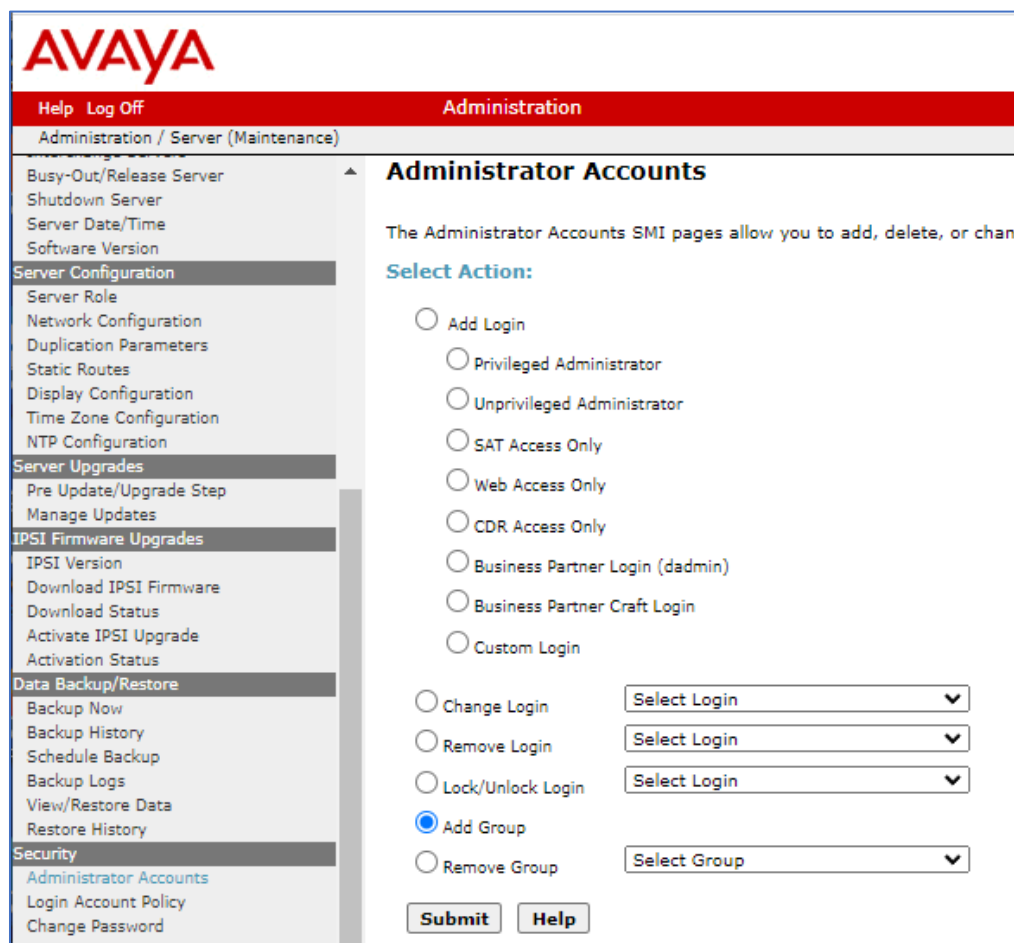
**Logon**

Logon ID:

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



From the navigation panel on the left side, click **Security** → **Administrator Accounts**. Select **Add Group** and click **Submit**.



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**. Click **Submit**. This completes the creation of the login group.

The screenshot shows the Avaya Administration web interface. At the top is the Avaya logo. Below it is a red navigation bar with 'Help' and 'Log Off' links, and the title 'Administration'. Underneath is a grey breadcrumb trail: 'Administration / Server (Maintenance)'. On the left is a sidebar menu with categories: 'FP Trap Test', 'FP Filters', 'Diagnostics' (with sub-items: Restarts, System Logs, Ping, Traceroute, Netstat), 'Server' (with sub-items: Status Summary, Process Status, Interchange Servers, Busy-Out/Release Server, Shutdown Server, Server Date/Time, Software Version), 'Server Configuration', and 'Server Role'. The main content area is titled 'Administrator Accounts -- Add Group'. It contains a description: 'This page allows you to add a new access-profile or non-access-profile Linux group. An access-profile g'. Below this is a 'Select Action:' section with two radio buttons. The first is selected and labeled 'Add a new access-profile group: prof23'. The second is labeled 'Add a new non-access-profile group:'. Below the second option are input fields for 'Group Name:' and 'Group Number:' (with a range '(500 to 60000)'). At the bottom are three buttons: 'Submit' (highlighted with a red box), 'Cancel', and 'Help'.

### 5.3. Configure Login

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

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

The screenshot displays the Avaya Administration web interface. On the left is a navigation pane with categories like Alarms, SNMP, Diagnostics, Server, Server Configuration, and Server Upgrades. The main area is titled 'Administrator Accounts' and includes a description: 'The Administrator Accounts SMI pages allow you to add, delete, or change administrator accounts.' Below this is a 'Select Action:' section with radio buttons for 'Add Login', 'Change Login', 'Remove Login', 'Lock/Unlock Login', 'Add Group', and 'Remove Group'. Under 'Add Login', there are several options: 'Privileged Administrator', 'Unprivileged Administrator', 'SAT Access Only' (which is selected), 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. To the right of the 'Change Login', 'Remove Login', 'Lock/Unlock Login', and 'Remove Group' options are dropdown menus labeled 'Select Login' and 'Select Group'. At the bottom of the 'Add Login' section, the 'Submit' button is highlighted with a red rectangular box, and a 'Help' button is located next to it.

For the field **Login name**, enter a descriptive name. 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**].
- **Enter password / Re-enter password** [Define the password].

Click **Submit** to continue. This completes the configuration of the login.

The screenshot shows the Avaya Administration web interface. The top navigation bar includes 'Help', 'Log Off', and 'Administration'. Below this, a breadcrumb trail reads 'Administration / Server (Maintenance)'. The left sidebar contains a tree view with categories like 'System Logs', 'Server', 'Server Configuration', 'Server Upgrades', 'Data Backup/Restore', and 'Security'. The 'Administrator Accounts' link under 'Security' is selected. The main content area is titled 'Administrator Accounts -- Add Login: SAT Access Only'. It contains a descriptive text: 'This page allows you to create a login that is intended to have access only to the Communication Manager System'. The form fields are as follows: 'Login name' (text box with 'iptm'), 'Primary group' (radio buttons for 'users' and 'susers', with 'users' selected), 'Additional groups (profile)' (dropdown menu with 'prof23' selected), 'Linux shell' (text box with '/opt/ecs/bin/autosat'), 'Home directory' (text box with '/var/home/iptm'), 'Lock this account' (checkbox, unchecked), 'SAT Limit' (dropdown menu with 'none' selected), 'Date after which account is disabled-blank to ignore (YYYY-MM-DD)' (text box, empty), 'Enter password' (password field with 6 dots), 'Re-enter password' (password field with 6 dots), and 'Force password change on next login' (radio buttons for 'No' and 'Yes', with 'No' selected). There are two warning icons: one for the 'Additional groups (profile)' field stating 'You must assign a profile that has no web access if you want a login with SAT access only.', and another for the 'Linux shell' field stating 'This shell setting does NOT disable the "go shell" SAT command for this user.' At the bottom, there are three buttons: 'Submit' (highlighted with a red box), 'Cancel', and 'Help'.

## 5.4. Configure SNMP

Access the Communication Manager System Management Interface as in **Section 5.2**. Click on **SNMP → Agent Status**. Click **Stop the Master Agent** if the **Master Agent status** is *UP* to allow setup of SNMP Agent.

The screenshot displays the Avaya Communication Manager System Management Interface. The top navigation bar includes the Avaya logo, 'Help', 'Log Off', and 'Administration'. Below this, a breadcrumb trail shows 'Administration / Server (Maintenance)'. A left-hand menu lists various system management options, including 'Alarms', 'SNMP', 'Diagnostics', and 'Server'. The 'SNMP' section is expanded, and 'Agent Status' is selected. The main content area, titled 'Agent Status', provides information about the current state of the Master Agent and Sub Agents. It states that all Sub Agents are connected to the Master Agent and lists the status of the Master Agent, FP Agent, CMSubAgent, and Load Agent, all of which are 'UP'. A red rectangular box highlights the 'Stop Master Agent' button, which is located next to a 'Help' button.

Agent Status	
The Agent Status SMI page shows the current state of the Master Agent.	
All of the Sub Agents are connected to the Master Agent.	
Master Agent status:	UP
<b>Sub Agent Status</b>	
FP Agent status:	UP
CMSubAgent status:	UP
Load Agent status:	UP
<b>Stop Master Agent</b>	<b>Help</b>

To allow Prognosis to use SNMP to collect configuration and status information from Communication Manager, navigate to **SNMP → Access** in the left pane. Click **Add/Change** button (not shown).

Configure the **SNMP Version 2c** section. Set the **IP address** to the Prognosis server and **Access** as **read-only** from the drop menu. Also set the **Community Name** field to say **avaya123**. Click **Submit** at the bottom of the web page.

**AVAYA**

Help Log Off Administration

Administration / Server (Maintenance)

Agent Status

Access

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Interchange Servers

Busy-Out/Release Server

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Duplication Parameters

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Pre Update/Upgrade Step

Manage Updates

IPSI Firmware Upgrades

IPSI Version

Download IPSI Firmware

Download Status

Activate IPSI Upgrade

Activation Status

Base Backup/Restore

### Access

The Access SMI page is used to configure SNMP access to CM.

**SNMP Version 2c**

IP address: 10.1.10.124

Access: read-only

Community Name: avaya123

#### Add SNMP Users / Communities

**SNMP Version 1**

IP address:

Access:

Community Name:

**SNMP Version 2c**

IP address:

Access:

Community Name:

**SNMP Version 3**

Access:

User Name:

Authentication Protocol:

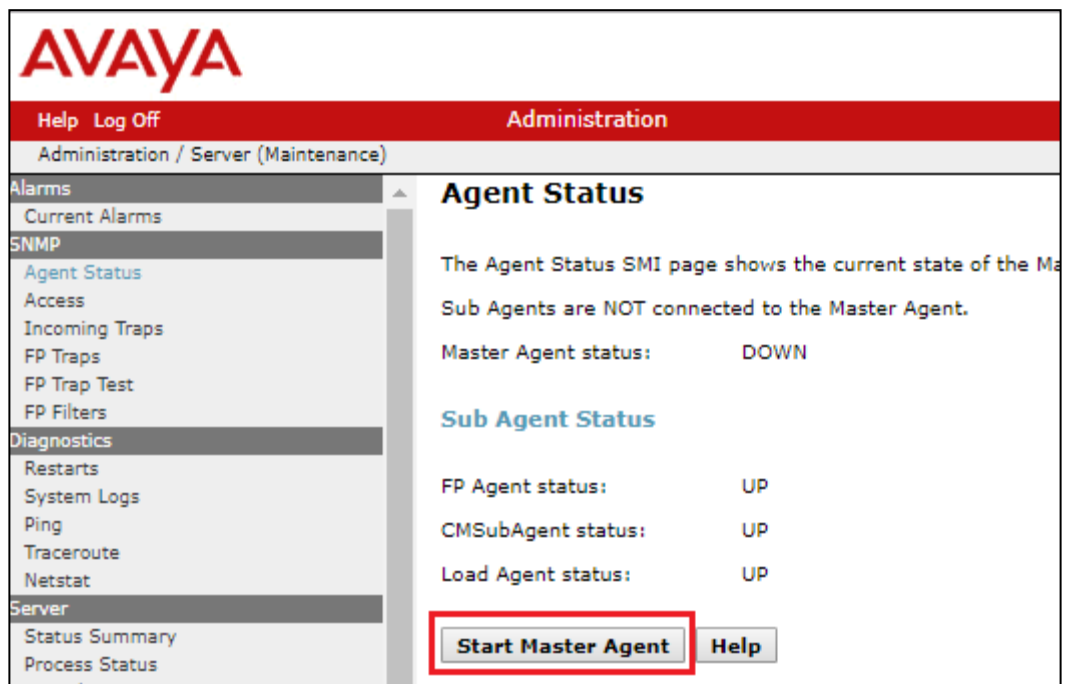
Authentication Password: Minimum 8 characters. (for authentication)

Privacy Protocol:

Privacy Password: Minimum 8 characters. (for privacy)

**Submit** **Cancel** **Help**

Lastly, the SNMP agent must be started. Navigate to **SNMP → Agent Status**. If the Master Agent status is *DOWN*, then click the **Start Master Agent** button. If the Master Agent status is *UP*, then the agent must be stopped and restarted.





## 5.5. Configure RTCP Monitoring

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

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

AUTOMATIC TRACE ROUTE ON
  Link Failure? y

                                H.323 IP ENDPOINT
H.248 MEDIA GATEWAY
  Link Loss Delay Timer (min): 5
  Primary Search Time (sec): 75
  Recover Before LLDT Expiry? y
  Periodic Registration Timer (min): 20
  Short/Prefixed Registration Allowed? y
```

Enter the **change ip-network-region *n*** command, where *n* is IP network region number to be monitored. On **Page 2**, set **RTCP Reporting to Monitor Server Enabled** to **y** and **Use Default Server Parameters** to **y**.

**Note:** Only one RTCP MONITOR SERVER can be configured per IP network region.

```
change ip-network-region 1                                           Page 2 of 20
                                IP NETWORK REGION

RTCP Reporting to Monitor Server Enabled? y

RTCP MONITOR SERVER PARAMETERS
  Use Default Server Parameters? y

ALTERNATIVE NETWORK ADDRESS TYPES
  ANAT Enabled? n
```

Repeat above 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.

Enter the **change ip-interface procr** command to enable the processor-ethernet interface on Communication Manager. Check **Enable Interface** is set 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
                                                           Gatekeeper Priority: 5

Network Region: 1

                                                           IPV4 PARAMETERS
Node Name: procr                                           IP Address: 10.1.10.230

Subnet Mask: /24
```

Enter the **change node-names ip** command to add a new node name for the Prognosis server. In this configuration, the name **iptm** is added with the IP address specified as **10.1.10.125**. Note that the node name **procr** which is automatically added.

```
change node-names ip                                         Page 1 of 2
                                                           IP NODE NAMES

Name                IP Address
iptm               10.1.10.125
lsp-g430            10.1.40.18
mypc                10.3.10.8
n                   10.3.10.253
procr             10.1.10.230
procr6             ::
s8500-clan1         10.1.10.21
s8500-clan2         10.1.10.22
s8500-medpro1       10.1.10.31
s8500-medpro2       10.1.10.32
s8500-vall          10.1.10.36
site6              10.1.60.18
sm1                 10.1.10.60
sm2                 10.1.10.42

( 14 of 34 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
```

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

- **Service Type: CDR1** [If needed, a secondary link can be defined by setting Service Type to CDR2.]
- **Local Node: procr** [Communication Manager will use the processor-ethernet interface to send out the CDR. CLAN node can also be used.]
- **Local Port: 0** [The Local Port is set to 0 because Communication Manager initiates the CDR link.]
- **Remote Node: iptm** [The Remote Node is set to the Prognosis node name previously defined earlier.]
- **Remote Port: 50000** [The Remote Port may be set to a value between 5000 and 64500 inclusively. 50000 is the default port number used by Prognosis. Note that Prognosis server uses the same port number for CDR integration with all Communication Manager systems.]

change ip-services						Page 1 of 4
IP SERVICES						
Service Type	Enabled	Local Node	Local Port	Remote Node	Remote 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 Type	Reliable Protocol	Packet Timer	Resp	Session Message	Connect Cntr	SPDU Cntr	Connectivity Timer
CDR1	n	30			3	3	60

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]
- **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 [2] for a full explanation of each field. The test configuration used some of the more common fields described below.

- **Use Legacy CDR Formats? y** [Specify the use of Communication Manager 3.x (“legacy”) formats in the CDR records produced by the system.]
- **Intra-switch CDR: y** [Allows call records for internal calls involving specific stations. Those stations must be specified in the **intra-switch-cdr** form.]
- **Record Outgoing Calls Only? n** [Allows incoming trunk calls to appear in the CDR records along with the outgoing trunk calls.]
- **Outg Trk Call Splitting? y** [Allows a separate call record for any portion of an outgoing call that is transferred or conferenced.]
- **Inc Trk Call Splitting? y** [Allow a separate call record for any portion of an incoming call that is transferred or conferenced.]

<b>change system-parameters cdr</b>		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:		
CDR Retention (days): 20		
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? n	
Inc Trk Call Splitting? y	Inc Attd Call Record? y	
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		

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

<b>change intra-switch-cdr</b>		Page 1 of 3
INTRA-SWITCH CDR		
	Assigned Members: 5	of 5000 administered
Extension	Extension	Extension
10001		
10002		
10004		
10010		
10016		

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 4
                                     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? y
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
```

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

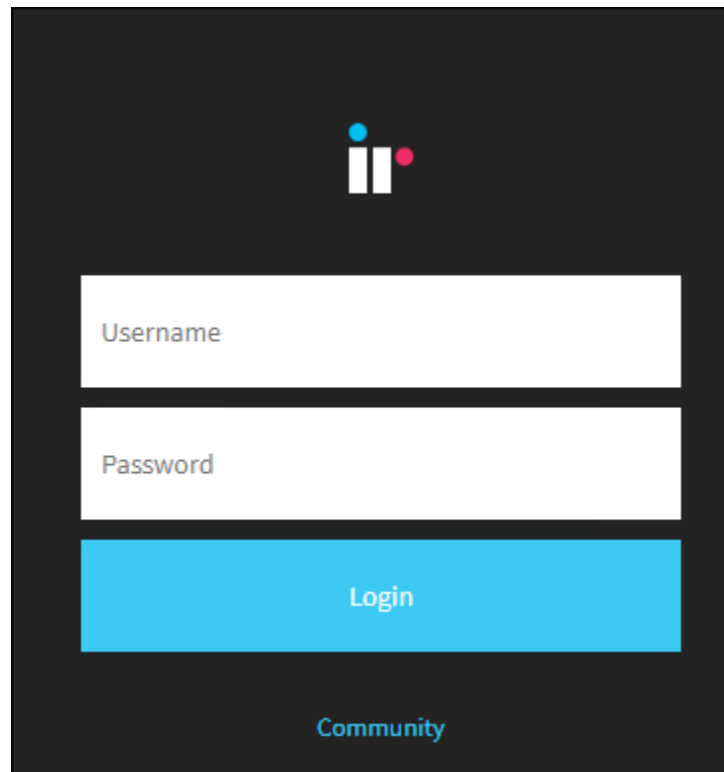
```
save translation
                                     SAVE TRANSLATION
Command Completion Status          Error Code
Success                            0
```

## 6. Configure Integrated Research Prognosis

This section describes the configuration of Prognosis required to interoperate with Communication Manager. Configuration of Prognosis to interoperate with System Manager and Session Manager, please refer to **Section 9**.

### 6.1. Configure Main Server

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

The image shows a login form for the Prognosis Administration interface. It has a dark gray background. At the top center is a logo consisting of three vertical bars of different heights and colors (blue, white, and red). Below the logo are two white input fields. The first field is labeled 'Username' in a light gray font. The second field is labeled 'Password' in a light gray font. Below these fields is a large blue button with the word 'Login' in white text. At the bottom center, there is a link labeled 'Community' in a light blue font.

Click **Add System**.

The screenshot shows the 'Administration' page for a Prognosis node. The left sidebar contains a navigation menu with options: Home, Call Recording Assurance, Assured Users, Tenants, Navigation, Security, Web Reports, Automation, Configuration Item Mapping, Alert Suppression, and High Availability. The main content area is titled 'Prognosis node - WIN-KKHMESF8NFQ'. It includes a 'Details' section with the following information: IP Address: 10.1.10.125, Version: Prognosis 12.1.0, Operating System: Windows Server 2019 Standard, and Status: Connected. Below this is the 'UC & Infrastructure Configuration' section, which features a red-bordered 'Add System' button. Further down is a 'Manage Prognosis Regions' button. At the bottom, there is a 'Databases' section with a list of databases and their status: AV-CDRs, AV-Contact Center Elite, AV-MedPro DSP Utilization, AV-Network Hops Historical, and AV-Reporting. Each database has a green status icon and a red 'Stop' button.

Select **Avaya PBX/ESS** from drop-down menu. Click **Add** to add a new Avaya PBX.

The form is titled 'Add New Unified Communication Monitoring'. It has a section for 'PBXs' with a drop-down menu showing 'Avaya PBX/ESS' and a blue 'Add' button.

In this test configuration, the following entries are added for the two Communication Manager systems with display name of **CM10-DUPLEX** (System A) and **G450-CM10** (System B) and with IP addresses of **10.1.10.230** and **10.1.60.18** respectively. The display name must match with the naming of these systems on the *System Manager SIP Entities*.

The following settings were used during the compliance test (see **next page**).

Basic Details:

- **Display Name: CM10-DUPLEX**
- **IP address: 10.1.10.230**
- **Customer Name: Avaya**
- **Site Name: DevCon Lab**

SAT Connection Details:

- **User Name/Password: iptm** [As configured in **Section 5.3**]
- **Mode: SSH**
- **Port: 5022**

CDR Configuration:

- **Format: unformatted** [as configured in **Section 5.6**]
- **Date Format: mm-dd** [as configured in **Section 5.6**]

SNMP Connection Details:

- **Select Use SNMP Version 2c**
- **Community String: As configured in Section 5.4**

Leave the **Databases and Thresholds** (not shown) at the bottom as checked and click **Add** (not shown) to affect the addition. Repeat the above for the setup of Communication Manager System B i.e., **G450-CM10**.



### Basic Details

Display Name: CM10-DUPLEX

IP Address: \* 10.1.10.230

Customer Name: Avaya

Site Name: DevCon Lab

### SAT Connection Details

User Name: \* iptm

Password: \* \*\*\*\*\*

Mode: SSH

Port: \* 5022

### CDR Configuration

Format: Unformatted

Date Format: dd-mm

Time Zone: (UTC+08:00) Kuala Lumpur, Singa...

### SNMP Connection Details

☐ Do not use SNMP

☒ Use SNMP Version 2c

☐ Use SNMP Version 3

Community String: \*\*\*\*\*

### Configure G700 Media Gateways

Configure

## 6.2. Configure Local Survivable Processor (LSP) and Enterprise Survivable Server (ESS)

In this test configuration, the LSP and ESS with names of **LSPREMOTE** and **ESS** with IP addresses of **10.1.40.18** and **10.1.10.239** respectively, both belonging to the **CM10-DUPLEX** Communication Manager system are also configured.

Select **Add System** (not shown) from home screen and select **Avaya LSP** from the drop-down menu. Click **Add** to add a new LSP.



The screenshot shows a web interface titled "Survivable Appliances". Below the title is a dropdown menu currently displaying "Avaya LSP" with a downward arrow icon. To the right of the dropdown is a blue button labeled "Add", which is highlighted by a red rectangular border.

The following settings were used during the compliance test.

Basic Details:

- **Display Name: LSPREMOTE**
- **IP address: 10.1.40.18**
- **Primary Controller: CM10-DUPLEX**
- **Customer Name: Avaya**
- **Site Name: DevCon Lab**

SAT Connection Details:

- **User/Password: iptm** [As configured in **Section 5.3**]
- **Mode: SSH**
- **Port: 5022**

Leave the **Databases and Thresholds** as checked. Click **Add** to affect the addition. Repeat the above for the setup of ESS.

Below show the screenshot after addition.

### Basic Details

Display Name: LSPREMOTE

IP Address: \*

Customer Name:

Site Name:

Primary Controller: \*

### SAT Connection Details

User Name: \*

Password: \*

Mode:

Port: \*

### Databases and Thresholds

☐ Start standard databases and thresholds

UpdateRemoveCancel

Below is the result of the additions of the two Communication Manager systems plus the LSP and ESS.

WIN-KKHMESF8NFQ

LSPREMOTE

CM10-DUPLEX

ESS

G450-CM10

## Prognosis node - WIN-KKHMESF8NFQ

### Details

IP Address:	10.1.10.125
Version:	Prognosis 12.1.0
Operating System:	Windows Server 2019 Standard
Status:	Connected

### UC & Infrastructure Configuration

Add System

Do you have Microsoft Skype for Business? [Why do I need this?](#)

Manage Prognosis Regions

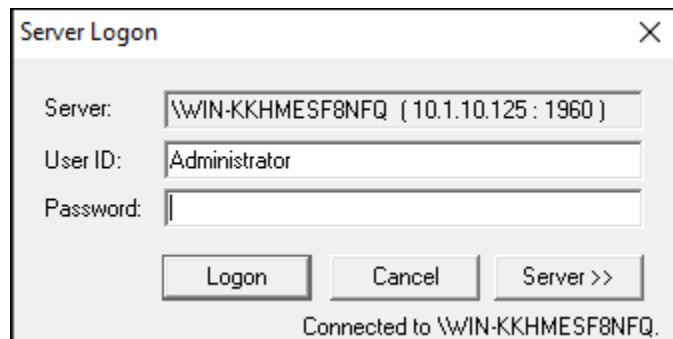
### ▼ Databases

AV-CDRs

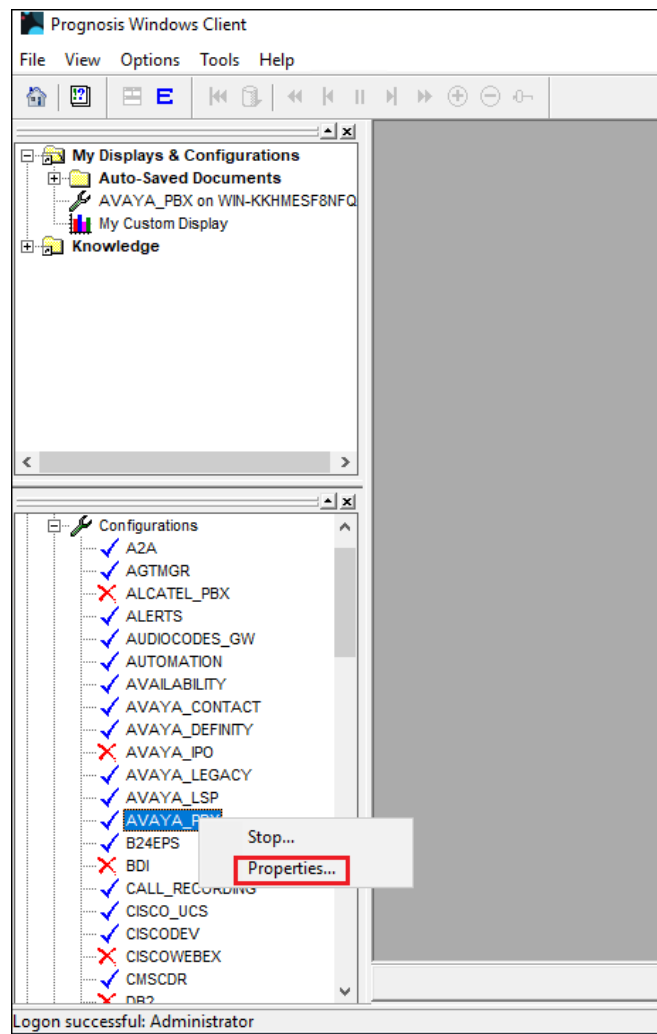
Stop

### 6.3. Verifying Configurations with Prognosis Client

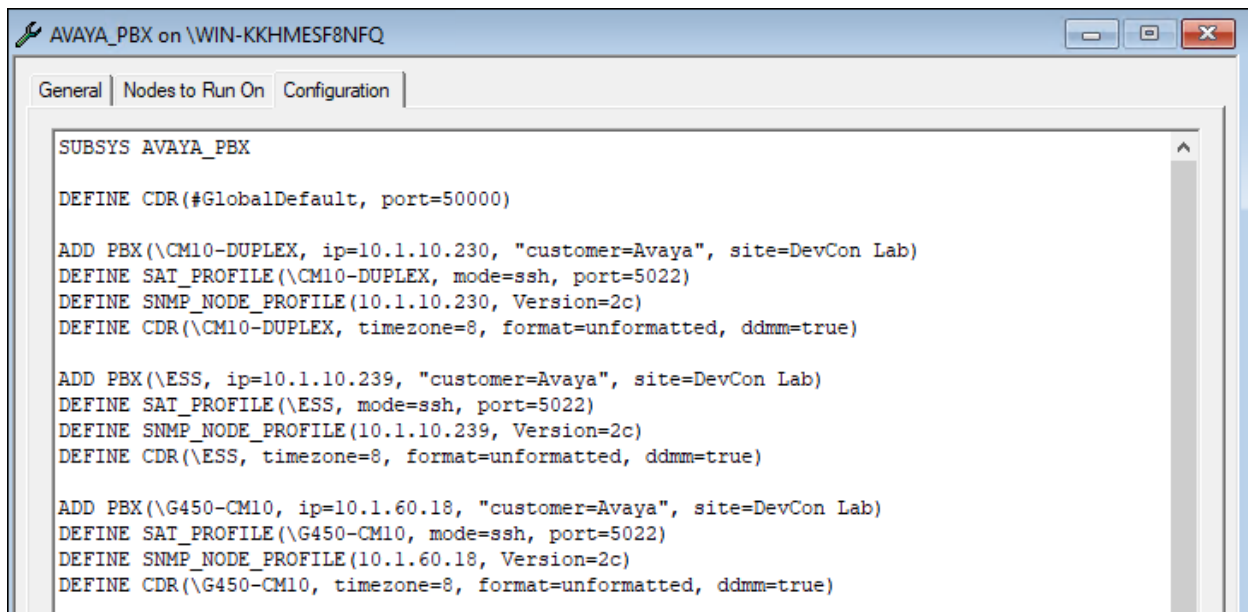
On Prognosis server, click **Start** → **All Programs** → **Prognosis** → **Prognosis Client** to start the Windows Client application. Log in with the appropriate credentials.



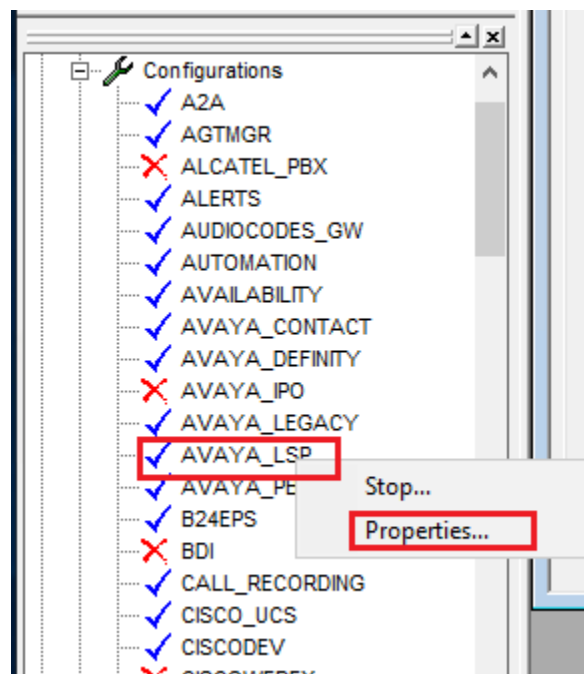
To check the configurations of the Avaya PBX/ESS to be monitored, expand **Configurations** of the Monitoring Node, right-click on **AVAYA\_PBX** and select **Properties**.



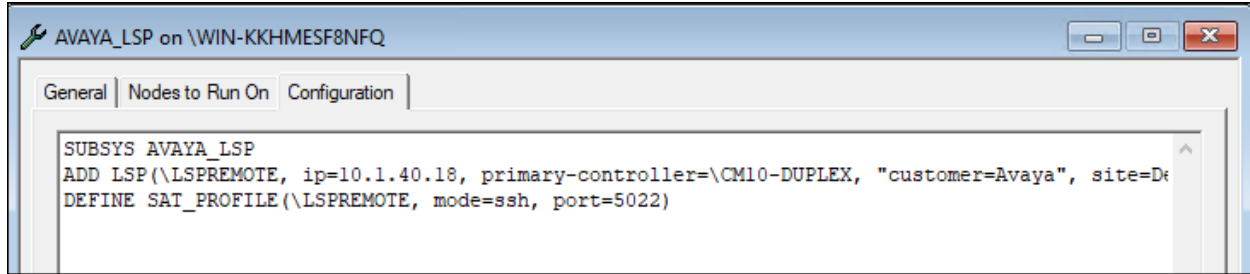
Check the configurations for each Communication Manager and the corresponding CDR settings configured in **Section 6.1**. Note that the default CDR port is **50000** which correspond to the configurations set in **Section 5.6** is already created as default.



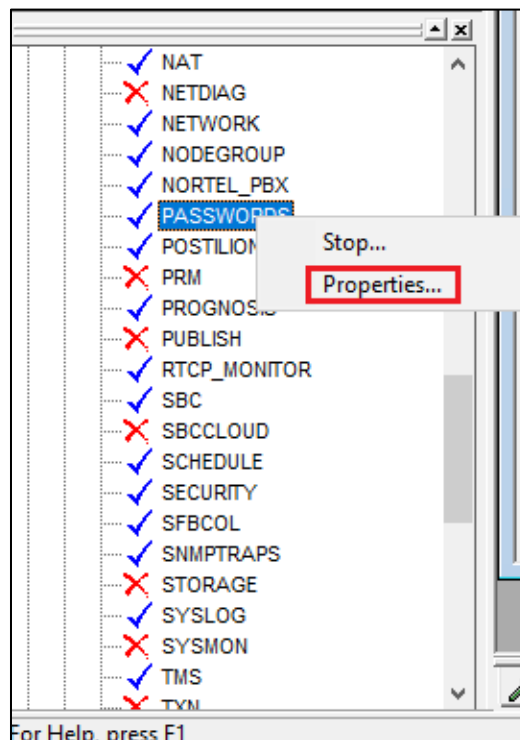
To check the configurations of the LSP server to be monitored, expand **Configurations** of the Monitoring Node, right-click on **AVAYA\_LSP** and select **Properties**.



Check the configurations for LSP server to be monitored as configured in **Section 6.2** earlier.



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**.



The four Communication Manager entries **CM10-DUPLEX**, **G450-CM10**, **LSPREMOTE** and **ESS** are listed below.

Entry Name	Password Only	Username	Password
CSMRabbitMq	<input type="checkbox"/>	prognosis	*****
Avaya-SAT:CM10-DUPLEX	<input type="checkbox"/>	iptm	*****
snmpV2c:CM10-DUPLEX	<input checked="" type="checkbox"/>		*****
Avaya-SAT:ESS	<input type="checkbox"/>	iptm	*****
snmpV2c:ESS	<input checked="" type="checkbox"/>		*****
Avaya-SAT:G450-CM10	<input type="checkbox"/>	iptm	*****
snmpV2c:G450-CM10	<input checked="" type="checkbox"/>		*****
snmpv3:SMGR10	<input type="checkbox"/>	avayasnmp	*****
snmpv3encrypt:SMGR10	<input checked="" type="checkbox"/>		*****
FTP:SM1	<input type="checkbox"/>	CDR_User	*****
snmpV2c:SM1	<input checked="" type="checkbox"/>		*****
FTP:SM2	<input type="checkbox"/>	CDR_User	*****
snmpV2c:SM2	<input checked="" type="checkbox"/>		*****
Avaya-SAT:LSPREMOTE	<input type="checkbox"/>	iptm	*****
snmpV2c:AES10	<input checked="" type="checkbox"/>		*****
soap:AAEP81	<input type="checkbox"/>	outcall	*****
snmpV2c:AAEP81	<input checked="" type="checkbox"/>		*****
SmgrWebAPI:SMGR10	<input type="checkbox"/>	admin	*****
snmpv3:SBCE10	<input type="checkbox"/>	Prognosis	*****
snmpv3encrypt:SBCE10	<input checked="" type="checkbox"/>		*****



## 7. Verification Steps

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

### 7.1. Verify Communication Manager

Verify that Prognosis has established three concurrent connections to the SAT by using the **status logins** command.

```
status logins
```

COMMUNICATION MANAGER LOGIN INFORMATION				
Login	Profile	User's Address	Active Command	Session
*dadmin	18	10.1.10.155	stat logins	1
iptm	23	10.1.10.125		3
iptm	23	10.1.10.125		4
iptm	23	10.1.10.125		5
acpsnmp	17	127.0.0.1		7

```
Command successfully completed  
Command:
```

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

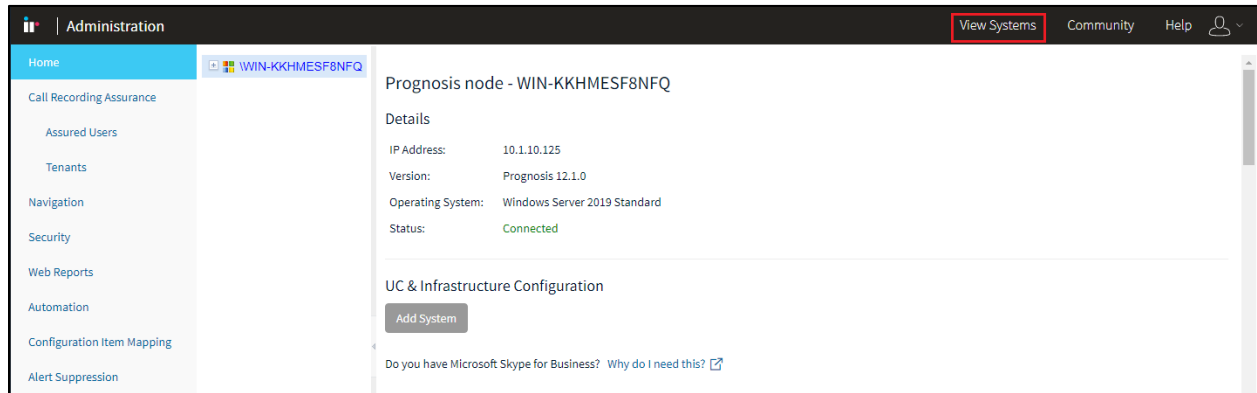
```
status cdr-link
```

CDR LINK STATUS	
Primary	Secondary
Link State: up	CDR not administered
Date & Time: 2022/06/28 16:08:10	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	

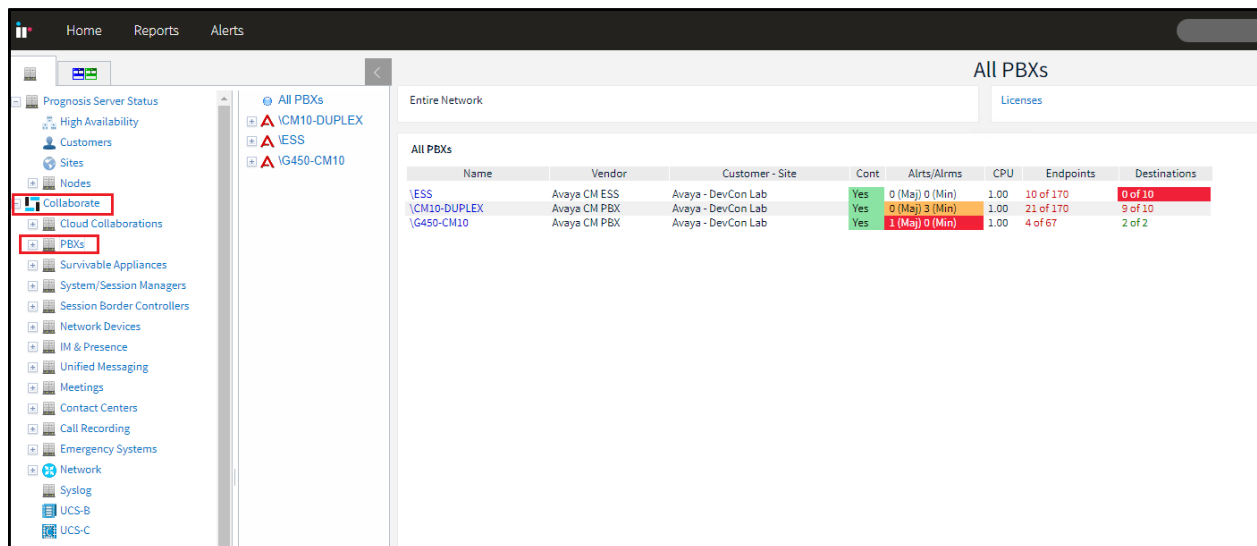
## 7.2. Verify Prognosis

This section provides the tests that can be performed to verify proper configuration of Prognosis. The following steps are done by accessing the Prognosis as in **Section 6.1**.

At the selecting the home screen, click on the **View Systems** on the top right.

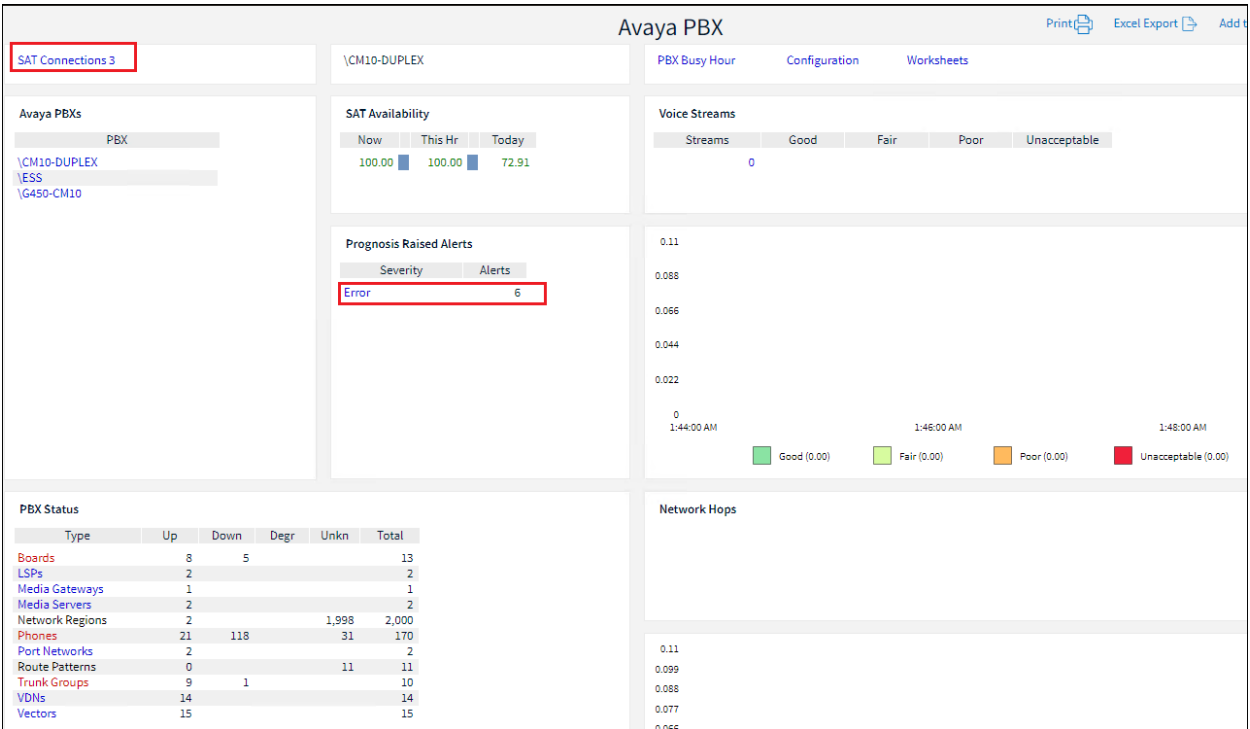


Select **Collaborate** → **PBXs** from the left pane and a list of Communication Manager servers configured in **Section 6** is displayed on the middle pane with details on the right pane.

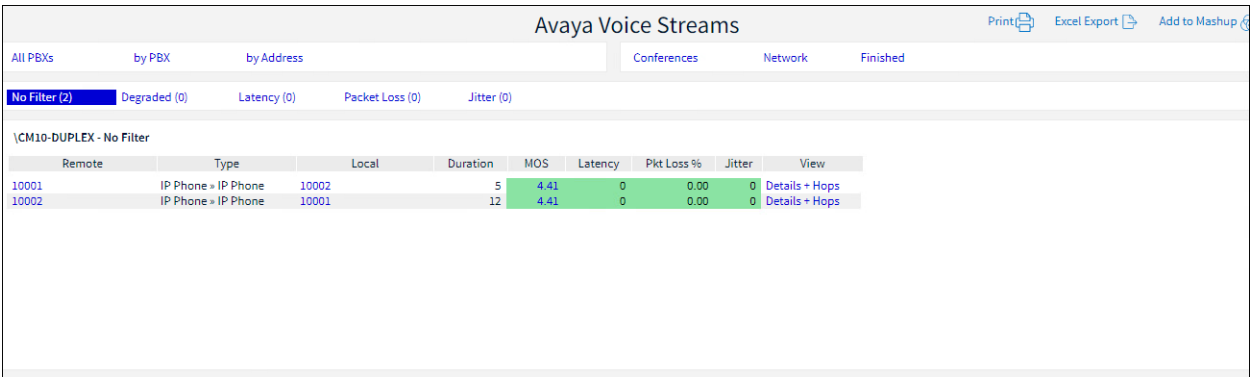


Select any of the PBX, verify that the **SAT Connections** field for each configured Communication Manager shows **3** connections. However, the number of SAT connections can be changed to 1 or 2. The instruction is found in the user guide in the software package installed.

Verify that the number of errors present in Communication Manager from the “display errors” command is also reflected below under the **Prognosis Raised Alerts**.



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. **Streams** count under Voice Streams in the above screen will be increased. Click on the count and verify that the **Avaya Voice Streams** section shows two active voice streams reflecting the quality of the call.



Verify the CDR data by making outbound and inbound calls from Communication Manager System B to Communication Manager System A, as well intra call within Communication Manager A. Captured CDR data can be custom designed for the layout. Below is a sample of a captured CDR data.

From: 2022-06-28 13:00:00-07:00 (Tue)  
To: 2022-06-28 20:00:00-07:00 (Tue)

Historical call data in selected hour

Avaya CM	Calling Number	Dialed Number	Call Type	Duration	Condition Code	Call Start	Call End	In Trunk Group	In Trunk Member	Out Trunk Group	Out Trunk Member	VDN	Vect ID	Calling Agent	Dialed Agent
\CM10-DUPLEX 10002	10001	10001	IN	12	0 - Intraswitch Call (call originates)	Tue 6/28/22 7:02:48 PM	Tue 6/28/22 7:03:00 PM	0	0	0	0			11002	
\CM10-DUPLEX 10001	60001	60001	OB	12	7 - AAR/ARS Feature call	Tue 6/28/22 7:02:48 PM	Tue 6/28/22 7:03:00 PM	0	10	4	4			11002	
\CM10-DUPLEX 10002	60001	60001	OB	12	7 - AAR/ARS Feature call	Tue 6/28/22 7:02:48 PM	Tue 6/28/22 7:03:00 PM	0	10	4	4			11002	
\CM10-DUPLEX 60001	10004	10004	IB	12	9 - Incoming or Tandem Calls	Tue 6/28/22 6:58:48 PM	Tue 6/28/22 6:59:00 PM	10	32	0	0				
\CM10-DUPLEX 60001	10001	10001	IB	12	9 - Incoming or Tandem Calls	Tue 6/28/22 6:58:48 PM	Tue 6/28/22 6:59:00 PM	10	32	0	0				

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

Avaya CM Servers

\CM10-DUPLEX

Avaya PBXs

PBX

\CM10-DUPLEX

ESS

IG450-CM10

Cluster Status

Current	Checked	Previous	Changed	Id	Type	Registration/State	ESS
Unknown							no

Active Server

Id	IP Address	Active Server Changed
10.1.10.231		

Updates

Software Vers	Translations Updated
R020x.01.0.974.0	2022-06-28 15:53:2

Server A

Id	IP Address	Name
10.1.10.231		cm1

Server B

Id	IP Address	Name
10.1.10.232		cm2

PBX Status

Type	Dn	Tot
Agents	29	30
Boards	5	13
CM Servers		
LSPs		2
Media Gateways		1
Media Servers		2
Network Regions		2,000
Phones	143	170
Port Networks		2
Route Patterns	1	11
Trunk Groups	1	10
VDNs		14

Recent Interchanges

Time	Text

## 8. Conclusion

These Application Notes describe the procedures for configuring Integrated Research's Collaborate - Prognosis Server R12.1 to interoperate with Avaya Aura® Communication Manager R10.1. In the configuration described in these Application Notes, Prognosis established SSH connections to the SAT to view the configurations of Communication Manager. Prognosis also processed the RTCP information to monitor the quality of IP calls and collected CDR information sent by Communication Manager. Prognosis also obtained the Communication Manager name, IP address and software versions from the SNMP information. Compliance test was successfully completed with observations noted 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 10.1, Issue 1, Feb 2022.
- [2] *Administering Avaya Aura® Communication Manager*, Release 10.1.x, Issue 1, Dec 2021.
- [3] *Application Notes for Integrated Research's Collaborate - Prognosis Server R12.1 with Avaya Aura® System Manager R10.1*.
- [4] *Application Notes for Integrated Research's Collaborate - Prognosis Server R12.1 with Avaya Aura® Session Manager R10.1*.

Prognosis documentations are provided with the software package.

---

**©2022 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at [devconnect@avaya.com](mailto:devconnect@avaya.com).