Avaya Solution & Interoperability Test Lab

Application Notes for Integrated Research Prognosis for Unified Communication R11.7 with Avaya Aura® Communication Manager R8.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Integrated Research Prognosis for Unified Communication R11.7 to interoperate with Avaya Aura® Communication Manager R8.1.

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

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

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

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

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Prognosis for Unified Communication R11.7 (herein after referred to as Prognosis) with Avaya Aura® Communication Manager R8.1.

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

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

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

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

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

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager. While this solution has successfully completed Compliance Testing for the specific release levels as described in 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.

2.1. Interoperability Compliance Testing

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

For the collection of RTCP and CDR information, the endpoints included Avaya H323, SIP, digital and analog endpoints, Avaya IX Workplace and Avaya one-X® Communicator user. The types of calls made included intra-switch calls, inbound/outbound inter-switch IP trunk calls, outbound trunk calls, transfer and conference calls.

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

2.2. Test Results

All test cases passed successfully with observations below:

a. ‘Unknown type’ was displayed for Avaya IX Workplace which is a SIP endpoint in voice stream capture.
b. Firmware compatibility check for 1600 series IP Phones is wrong as logic of comparison is not correct. This is because of the change in format for the firmware. 1.3120 (1.3.12.0) is actually a later firmware as compare to 1.3.8.
c. G430 MGP firmware 41.16.0 was indicated as not supported for Communication Manager 8.0 though it is actually supported. It was indicated as supported for Communication Manager 8.1 though.

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

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, and Avaya one-X® Communicator 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 2016. 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.

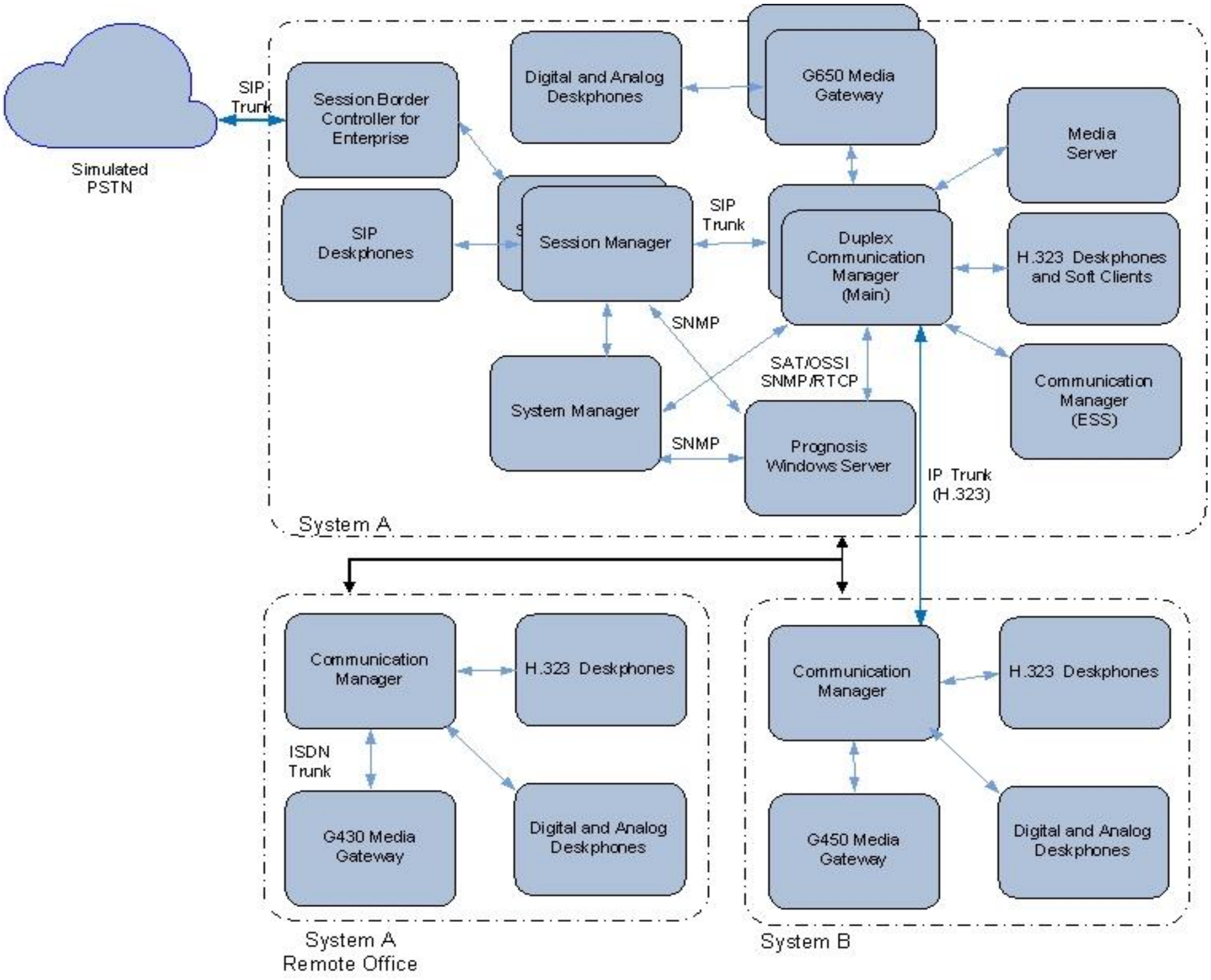


Figure 1: Test Configuration

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	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
Avaya Aura® Media Server	R8.0.1.121
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	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
G450 Media Gateway - MM722AP BRI Media Module (MM) - MM712AP DCP MM - MM714AP Analog MM - MM717AP DCP MM - MM710BP DS1 MM	41.16.0 HW01 FW008 HW07 FW015 HW10 FW0104 HW03 FW015 HW11 FW054
Avaya Aura® Communication Manager	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
G430 Media Gateway - MM712AP DCP MM - MM716AP Analog MM - MM711AP Analog MM - MM710AP DS1 MM	41.16.0 HW04 FW015 HW12 FW104 HW31 FW104 HW05 FW022
Avaya Aura® Communication Manager	R018x.01.0.890.0 R8.1.1.0.0 – FP1 Update ID 01.0.890.0-25763
Avaya Aura® System Manager	System Manager 8.1.1.0 Build No. – 8.1.0.0.733078 Software Update Revision No: 8.1.1.0.0310912 Feature Pack 1
Avaya Aura® Session Manager	Session Manager R8.1 FP1 Build No. – 8.1.0.0.810021

Equipment/Software	Release/Version
J100 Series IP Telephones - J179 - J129	 4.0.2.1.3 (SIP) 6.8202 (H323)
96x1 Series IP Telephones - 9641G - 9611G	 7.1.6.1.3 (SIP) 6.8202 (H323)
Avaya IX Workplace	3.7.0.102.3 (SIP)
1600 Series IP Telephones - 1616 - 1603SW	1.312 (H.323)
Digital Telephones - 9408	 R20
Avaya Analog Phones	-
Desktop PC with Avaya one-X Communicator	6.2.13.04 SP13 (H.323)
Prognosis running on Microsoft Windows Server 2016	11.7

Note: All Avaya Aura® systems and Prognosis runs on VMware 6.x 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:

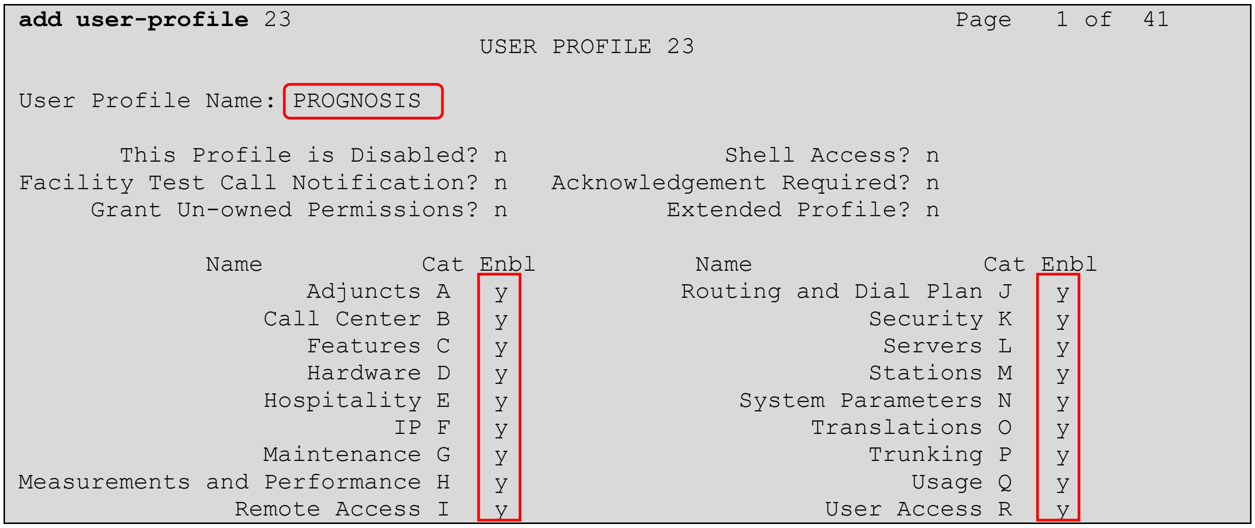
1. Configure SAT user profile
2. Configure login group
3. Configure login
4. Configure SNMP
5. Configure RTCP monitoring
6. Configure CDR monitoring

The steps are repeated for Communication Manager in System B.

5.1. Configure SAT User Profile

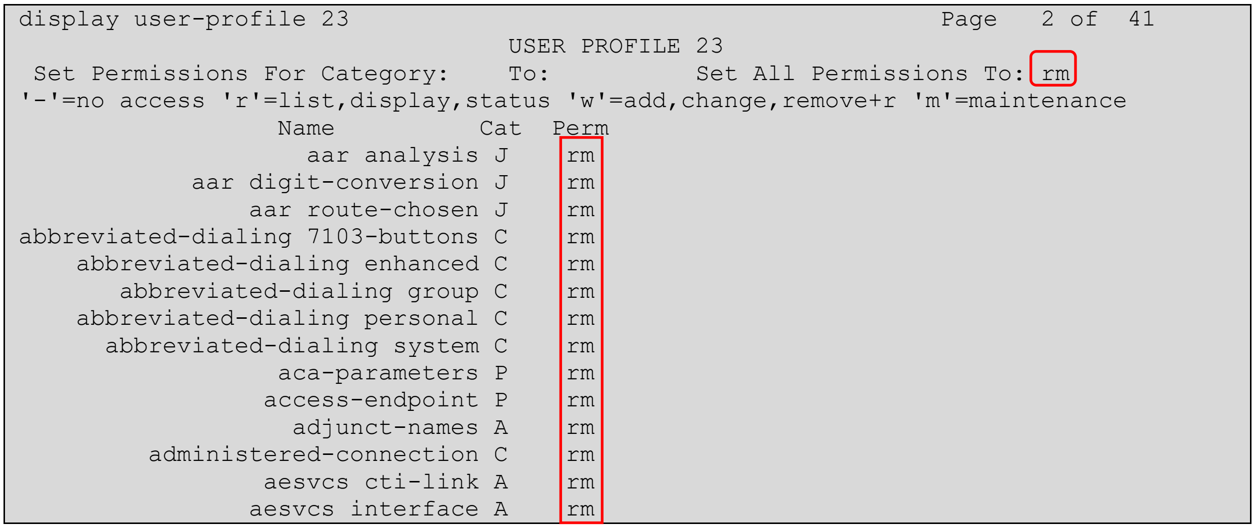
A SAT User Profile specifies which SAT screens may be accessed by the user assigned the profile and the type of access to each screen. As Prognosis does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the Prognosis login account.

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.

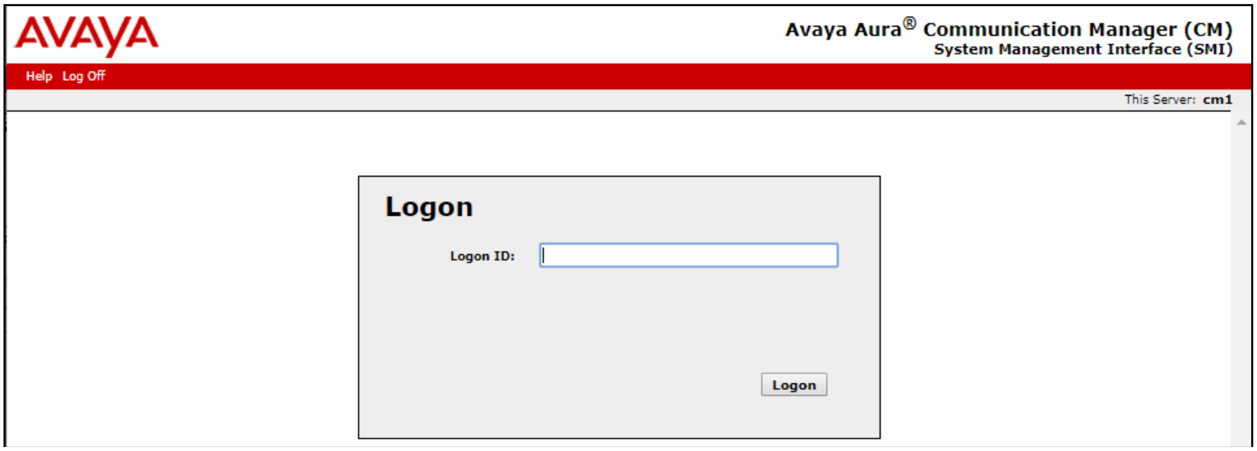


```
display user-profile 23                                                Page   2 of  41
                                  USER PROFILE 23
 Set Permissions For Category:    To:           Set All Permissions To: rm
'-'=no access 'r'=list,display,status 'w'=add,change,remove+r 'm'=maintenance
                  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
```

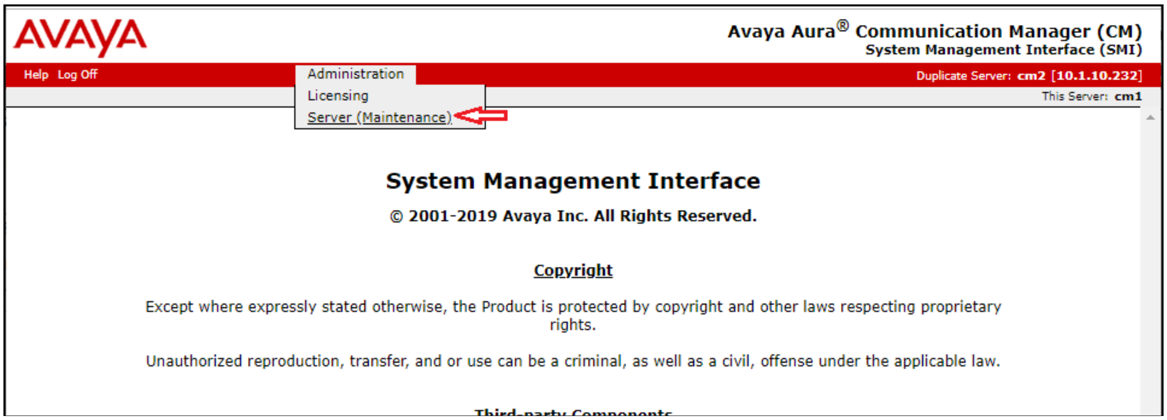
5.2. Configure Login Group

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:
Logon

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



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

Duplicate Server: cm2 [10.1.10.232]
This Server: cm1

System Management Interface

© 2001-2019 Avaya Inc. All Rights Reserved.

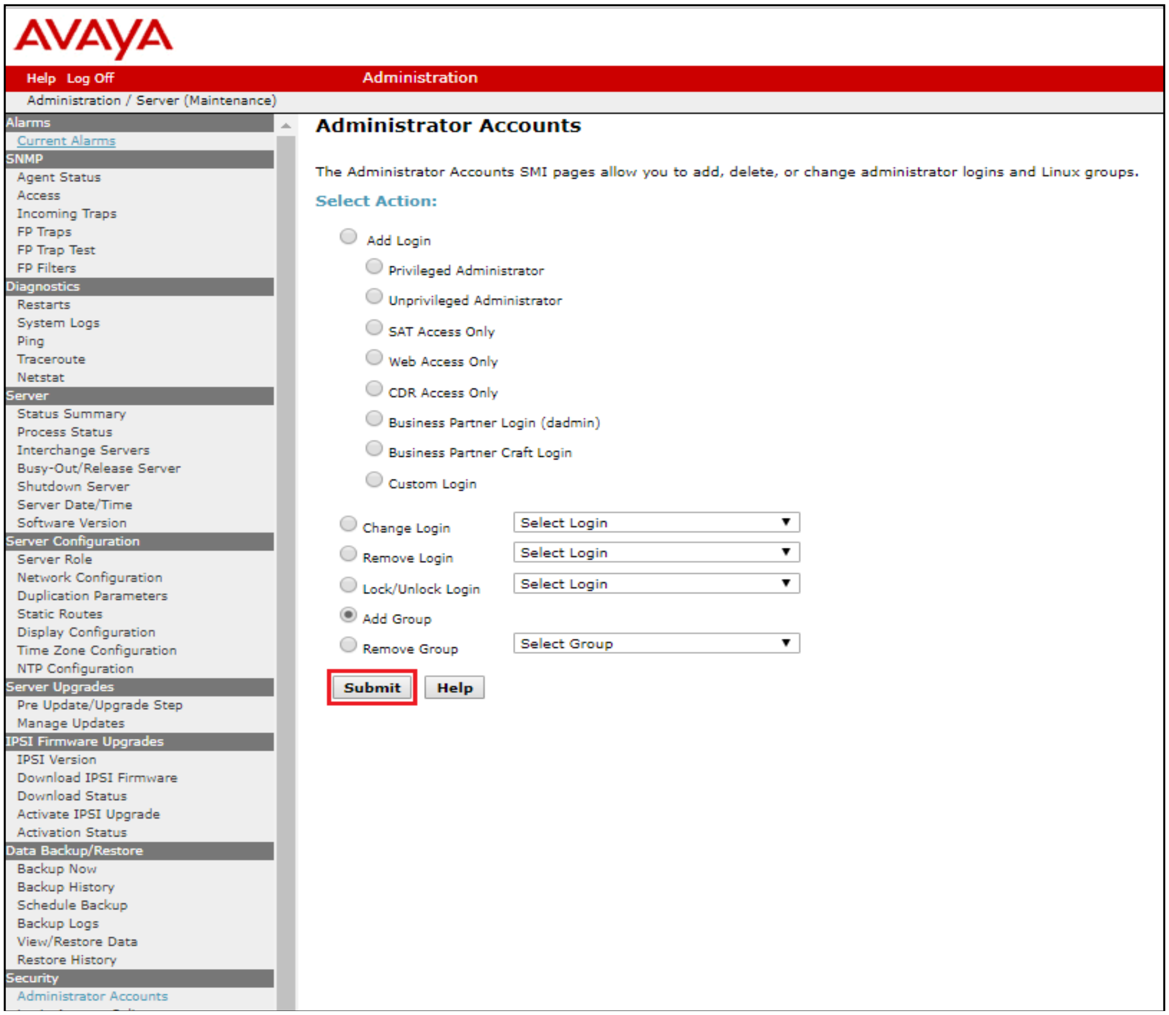
Copyright

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

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

Third-party Components

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



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.

Select Action:

○ Add Login
- ○ Privileged Administrator
- ○ Unprivileged Administrator
- ○ SAT Access Only
- ○ Web Access Only
- ○ CDR Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

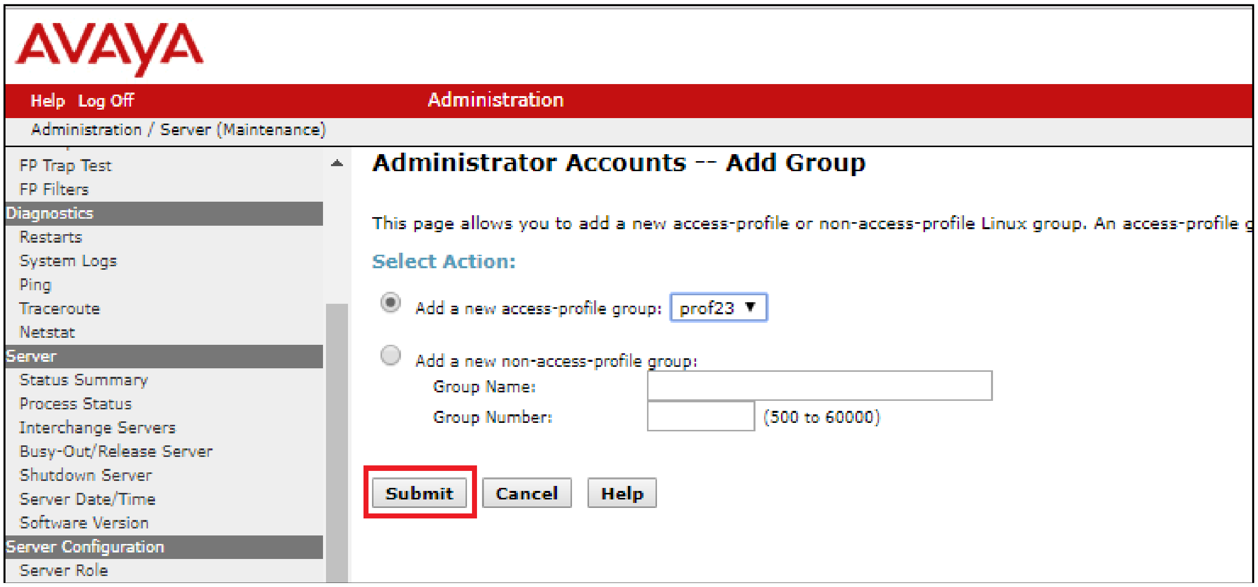
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

● Add Group

○ Remove Group — Select Group

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.



Administrator Accounts -- Add Group

This page allows you to add a new access-profile or non-access-profile Linux group. An access-profile g

Select Action:

● Add a new access-profile group: prof23 ▼

○ Add a new non-access-profile group:

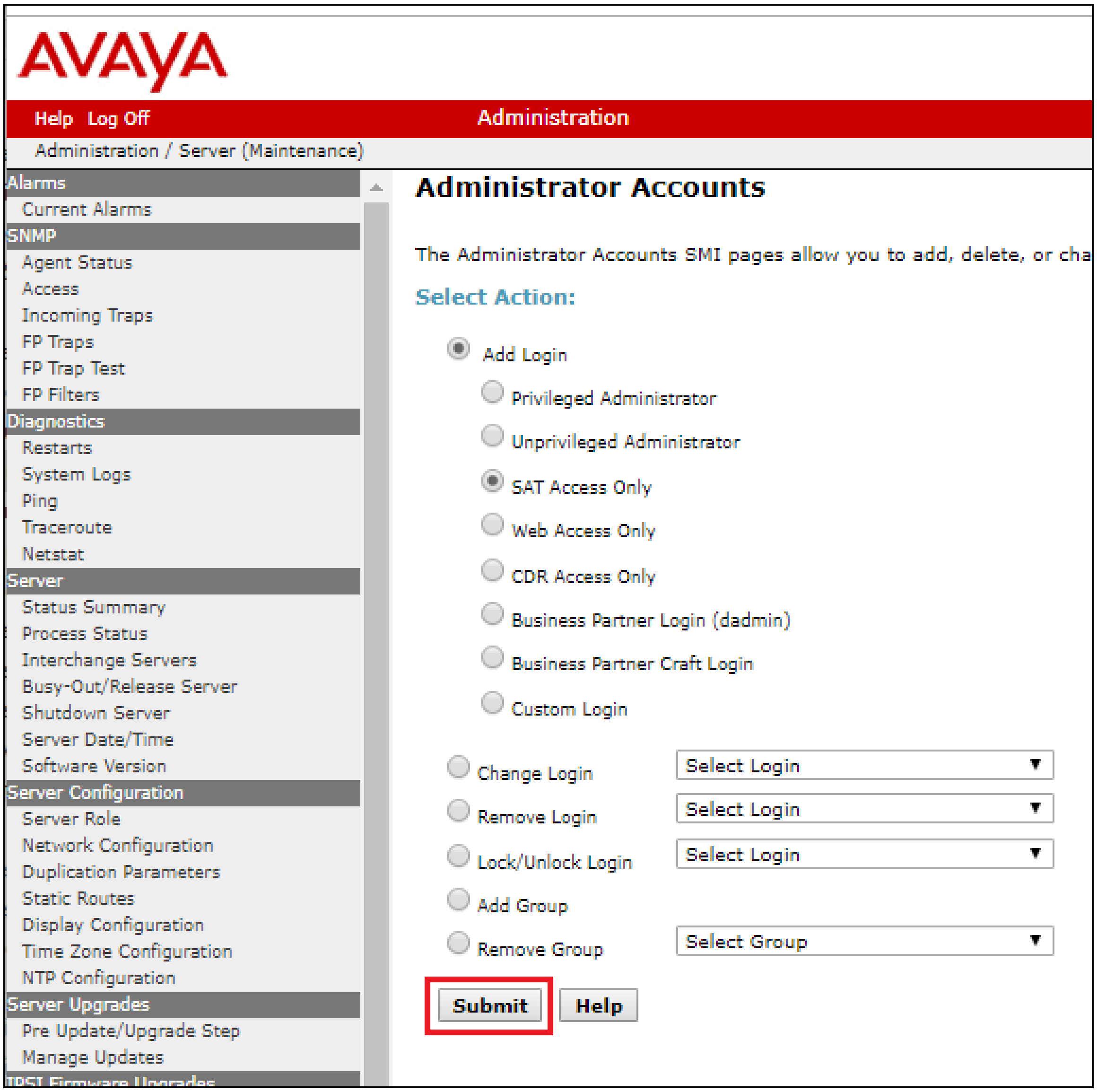
Group Name:

Group Number: (500 to 60000)

5.3. Configure Login

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

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**.



Administrator Accounts

The Administrator Accounts SMI pages allow you to add, delete, or cha

Select Action:

● Add Login

  ○ Privileged Administrator

  ○ Unprivileged Administrator

  ● SAT Access Only

  ○ Web Access Only

  ○ CDR Access Only

  ○ Business Partner Login (dadmin)

  ○ Business Partner Craft Login

  ○ Custom Login

○ Change Login Select Login ▼

○ Remove Login Select Login ▼

○ Lock/Unlock Login Select Login ▼

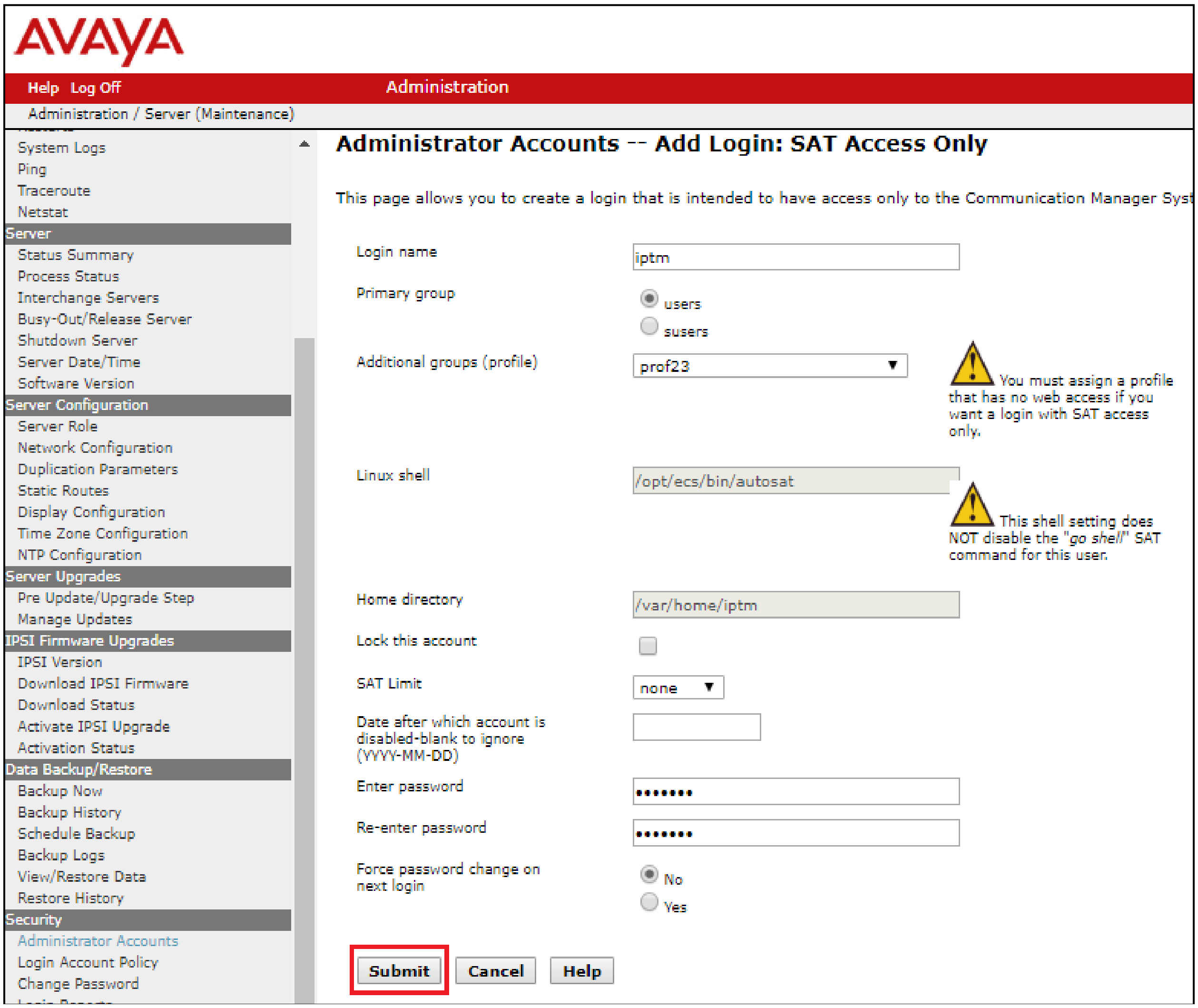
○ Add Group

○ Remove Group Select Group ▼

For the field **Login name**, enter the login. In this configuration, the login **iptm** is created. Configure the other parameters for the login as follows:

- **Primary group**: users [Limits the permissions of the login].
- **Additional groups (profile)**: **prof23** [Select the access-profile group created in **Section 5.2**].
- **Enter password / Re-enter password** [Define the password].

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



Administrator Accounts -- Add Login: SAT Access Only

This page allows you to create a login that is intended to have access only to the Communication Manager Syst

Login name: iptm

Primary group: ● users ○ susers

Additional groups (profile): prof23

You must assign a profile that has no web access if you want a login with SAT access only.

Linux shell: /opt/ecs/bin/autosat

This shell setting does NOT disable the "*go shell*" SAT command for this user.

Home directory: /var/home/iptm

Lock this account: □

SAT Limit: none

Date after which account is disabled-blank to ignore (YYYY-MM-DD):

Enter password: •••••••

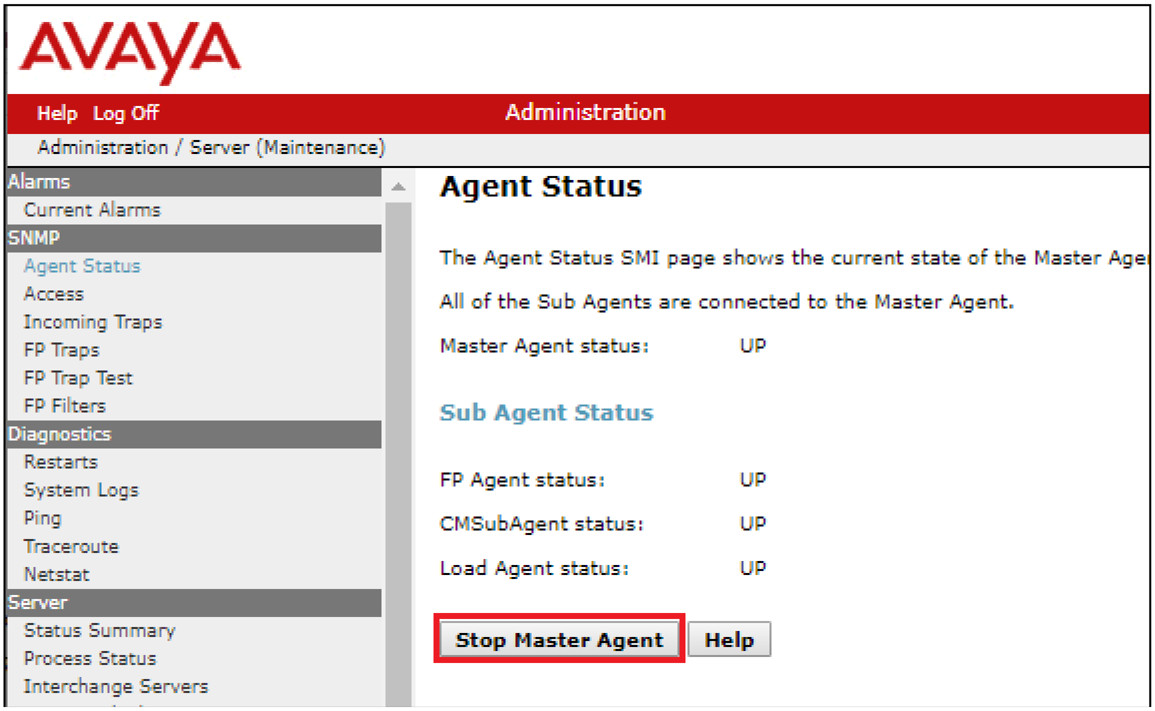
Re-enter password: •••••••

Force password change on next login: ● No ○ Yes

Submit | Cancel | Help

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.



Agent Status

The Agent Status SMI page shows the current state of the Master Age

All of the Sub Agents are connected to the Master Agent.

Master Agent status: UP

Sub Agent Status

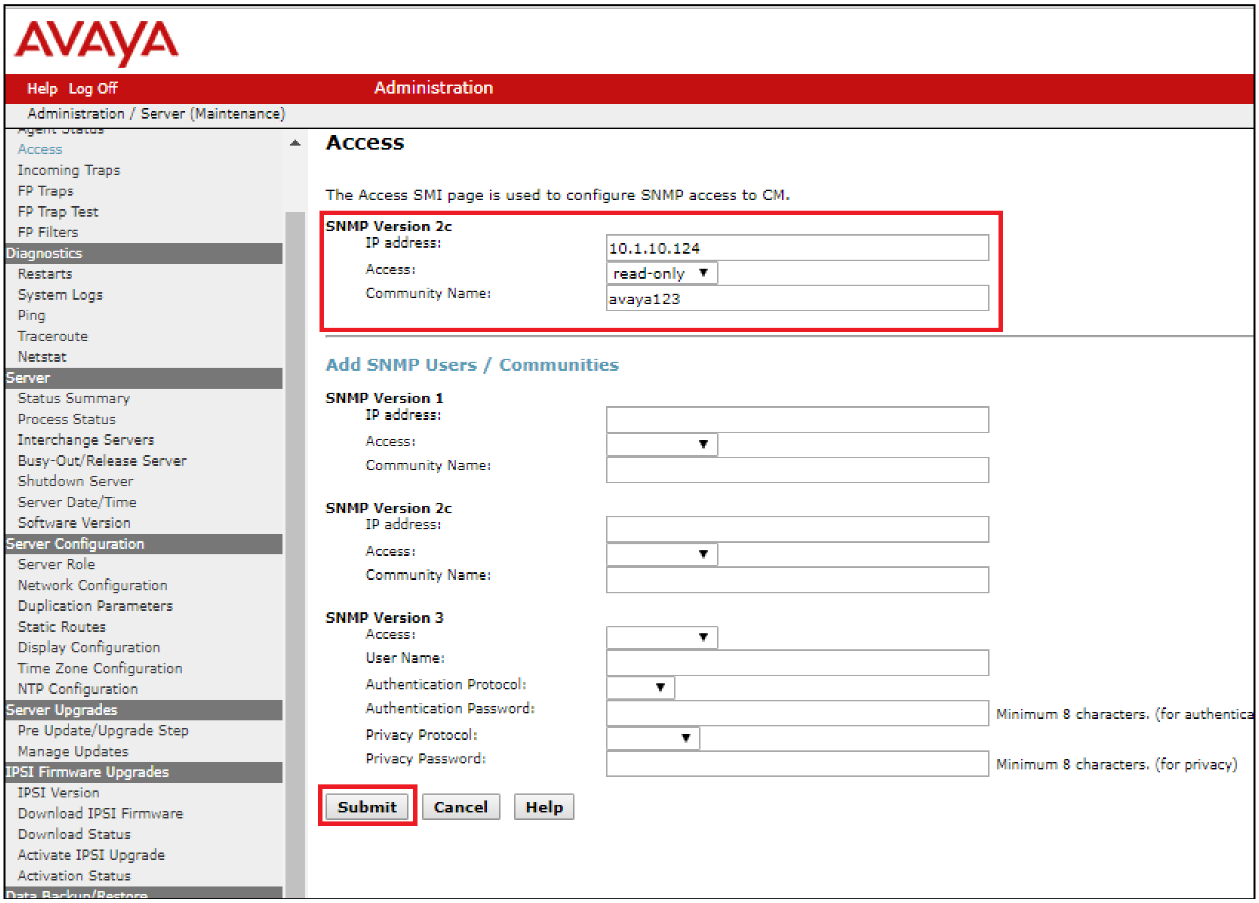
FP Agent status: UP

CMSubAgent status: UP

Load Agent status: UP

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

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



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:

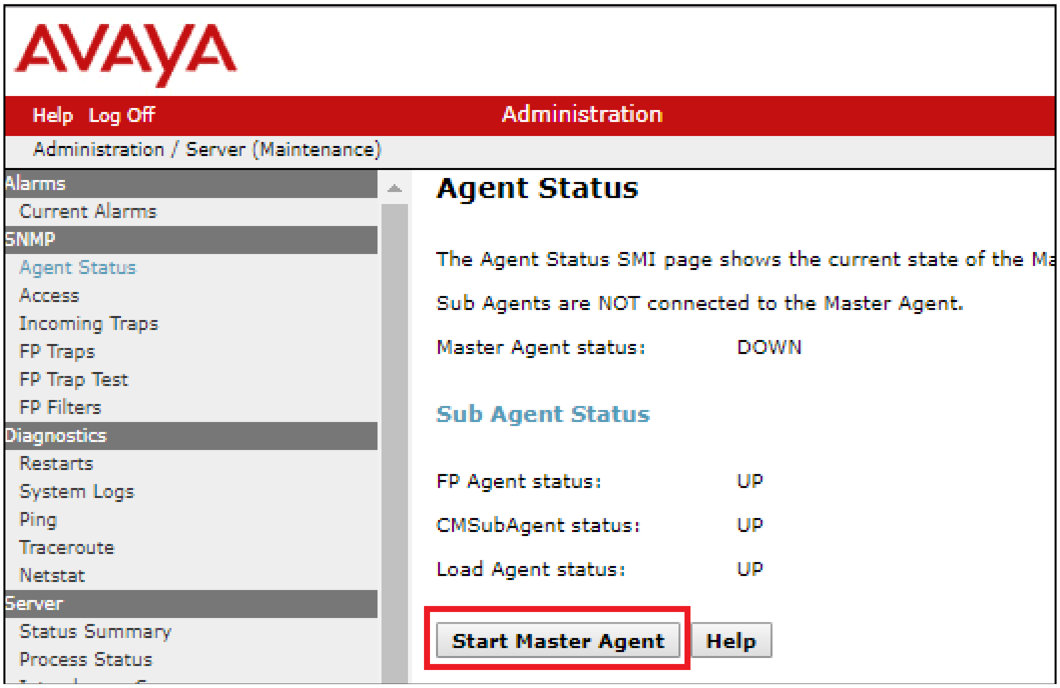
Authentication Protocol:

Authentication Password: Minimum 8 characters. (for authentica

Privacy Protocol:

Privacy Password: Minimum 8 characters. (for privacy)

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.



Agent Status

The Agent Status SMI page shows the current state of the Ma

Sub Agents are NOT connected to the Master Agent.

Master Agent status: DOWN

Sub Agent Status

FP Agent status: UP

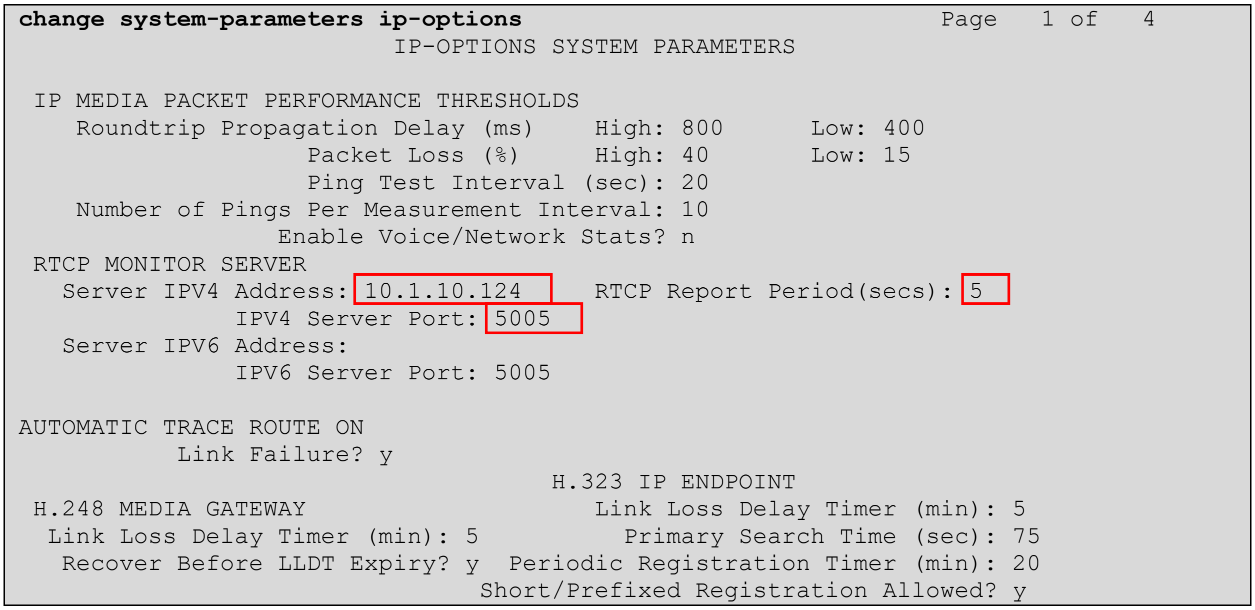
CMSubAgent status: UP

Load Agent status: UP

5.5. Configure RTCP Monitoring

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

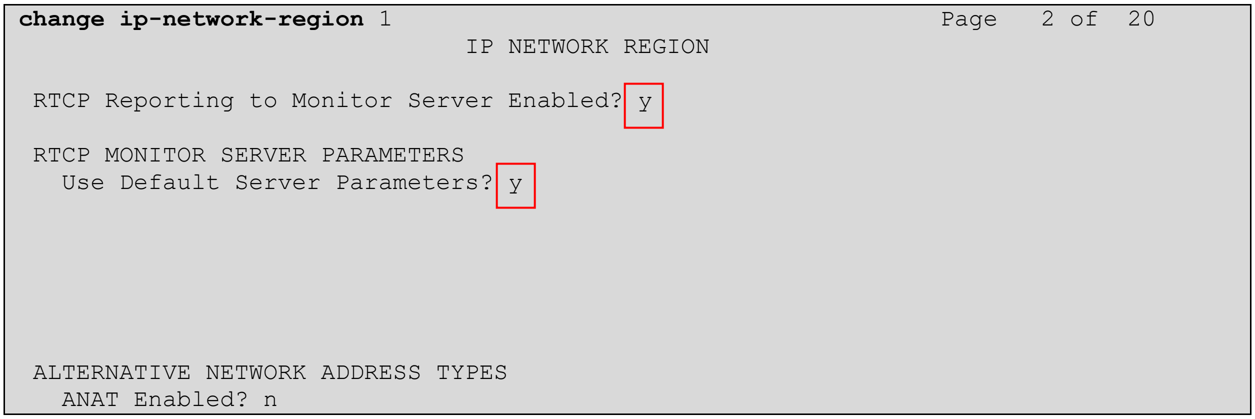
Enter the **change system-parameters ip-options** command. In the **RTCP MONITOR SERVER** section, set **Server IPV4 Address** to the IP address of the Prognosis server. Set **IPV4 Server Port** to **5005** and **RTCP Report Period (secs)** to **5**.



```
change system-parameters ip-options                             Page   1 of   4
                          IP-OPTIONS SYSTEM PARAMETERS

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                    Packet Loss (%)     High: 40       Low: 15
                    Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10
                  Enable Voice/Network Stats? n
 RTCP MONITOR SERVER
   Server IPV4 Address: 10.1.10.124     RTCP Report Period(secs): 5
               IPV4 Server Port: 5005
   Server IPV6 Address:
               IPV6 Server Port: 5005

AUTOMATIC TRACE ROUTE ON
           Link Failure? y
                                     H.323 IP ENDPOINT
 H.248 MEDIA GATEWAY                    Link Loss Delay Timer (min): 5
  Link Loss Delay Timer (min): 5          Primary Search Time (sec): 75
   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.



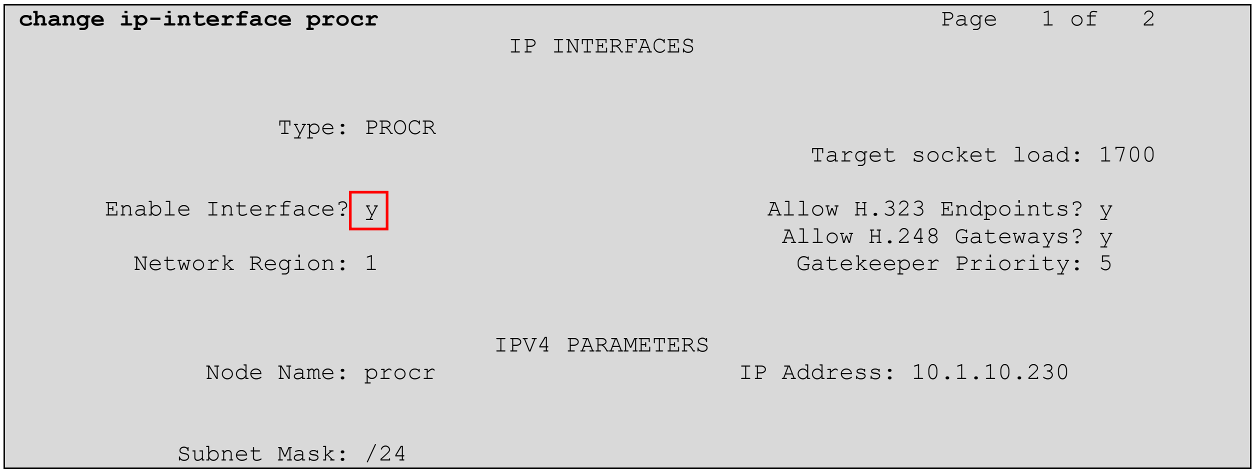
```
change ip-network-region 1                                      Page   2 of  20
                               IP NETWORK REGION

 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

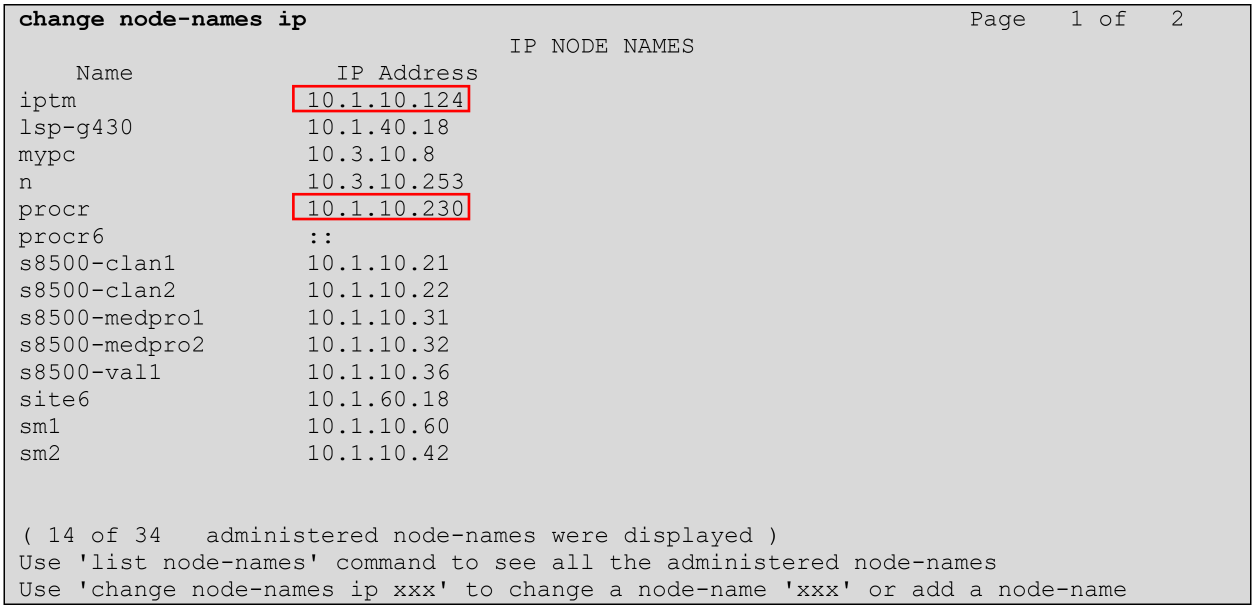
To allow Prognosis to monitor the CDR information, configure Communication Manager to send CDR information to the IP address of the Prognosis server.

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



```
change ip-interface procr                                      Page   1 of   2
                                  IP INTERFACES


                  Type: PROCR
                                                       Target socket load: 1700

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


                                 IPV4 PARAMETERS
             Node Name: procr                       IP Address: 10.1.10.230


           Subnet Mask: /24
```

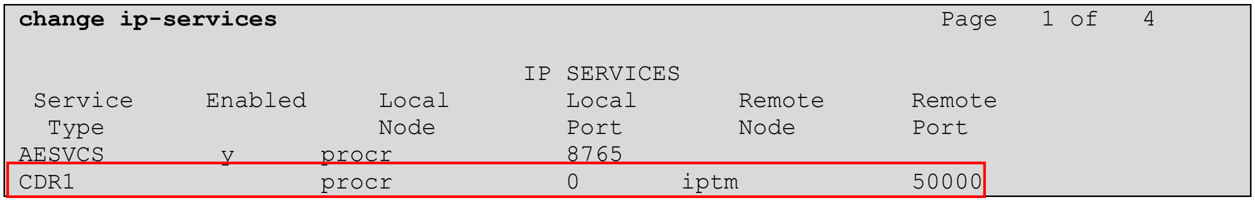
Enter the **change node-names ip** command to add a new node name for the Prognosis server. In this configuration, the name **iptm** is added with the IP address specified as **10.1.10.124**. Note also the node name **procr** which is automatically added.



```
change node-names ip                                             Page   1 of   2
                                  IP NODE NAMES
    Name                 IP Address
iptm                    10.1.10.124
lsp-g430                10.1.40.18
mypc                    10.3.10.8
n                       10.3.10.253
procr                   10.1.10.230
procr6                  ::
s8500-clan1             10.1.10.21
s8500-clan2             10.1.10.22
s8500-medpro1           10.1.10.31
s8500-medpro2           10.1.10.32
s8500-val1              10.1.10.36
site6                   10.1.60.18
sm1                     10.1.10.60
sm2                     10.1.10.42


( 14 of 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
```

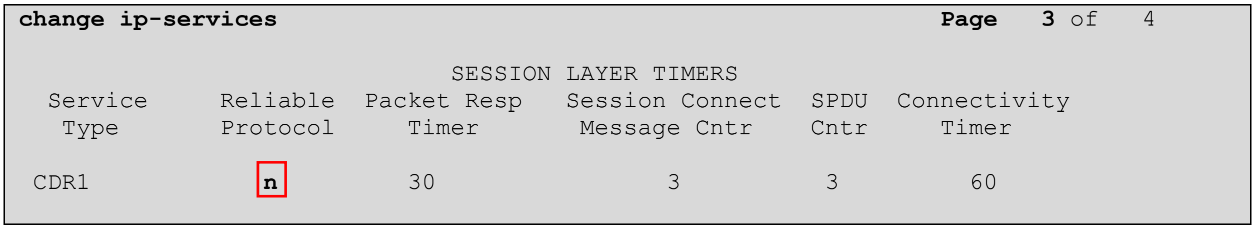
Enter the **change ip-services** command to define the CDR link. To define a primary CDR link, the following information should be provided:

- **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 could also be used.]
- **Local Port: 0** [The Local Port is set to 0 because Communication Manager initiates the CDR link.]
- **Remote Node: iptm** [The Remote Node is set to the node name previously defined 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     Enabled     Local        Local       Remote      Remote
  Type                   Node         Port        Node        Port
AESVCS        y      procr            8765
CDR1                 procr            0       iptm            50000
```

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



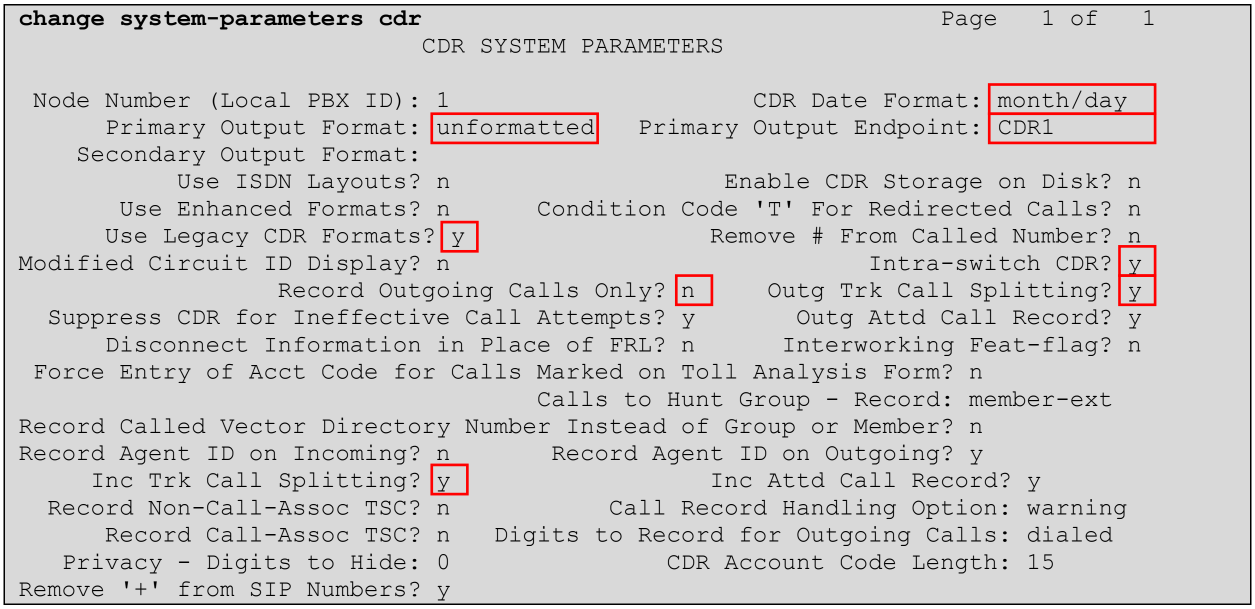
```
change ip-services                                              Page   3 of   4

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

 CDR1            n         30                3          3         60
```

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**

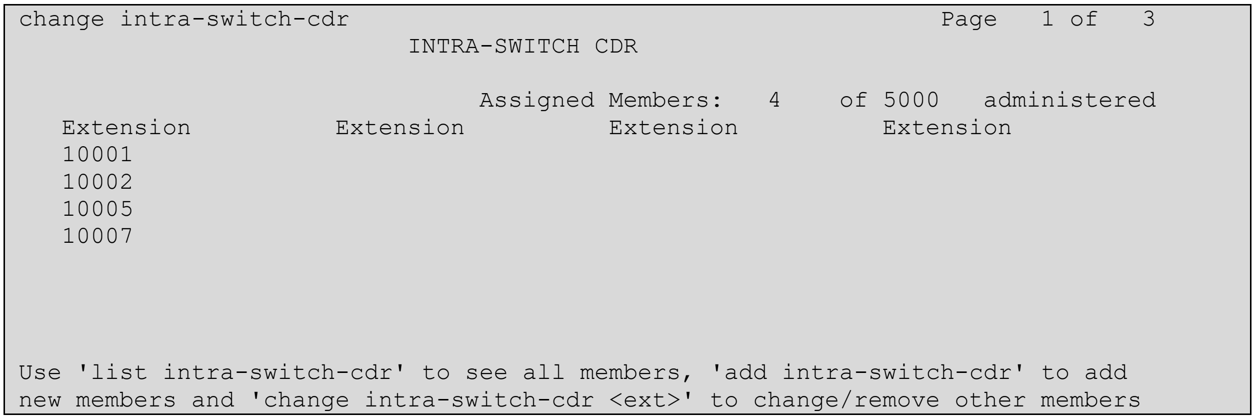
The remaining parameters define the type of calls that will be recorded and what data will be included in the record. See **Reference [2]** for a full explanation of each field. The test configuration used some of the more common fields described below.

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



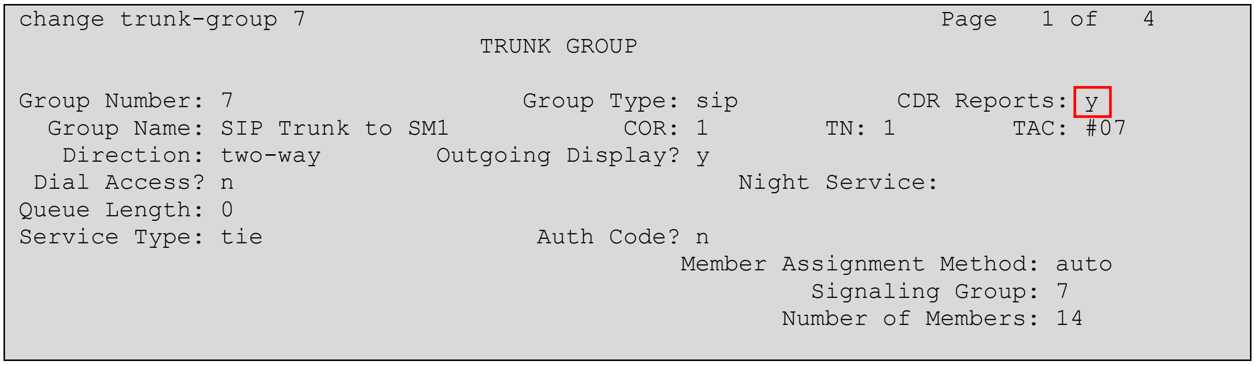
```
change system-parameters cdr                                    Page   1 of   1
                            CDR SYSTEM PARAMETERS

 Node Number (Local PBX ID): 1                     CDR Date Format: month/day
      Primary Output Format: unformatted   Primary Output Endpoint: CDR1
    Secondary Output Format:
           Use ISDN Layouts? n                   Enable CDR Storage on Disk? n
       Use Enhanced Formats? n      Condition Code 'T' For Redirected Calls? 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? 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.



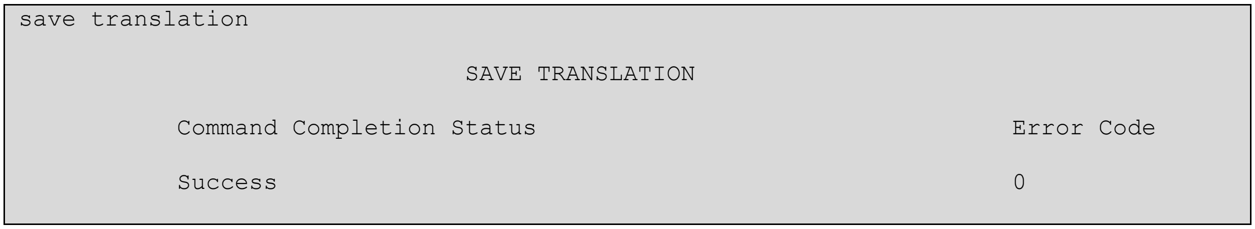
```
change intra-switch-cdr                                         Page   1 of   3
                           INTRA-SWITCH CDR

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





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

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.



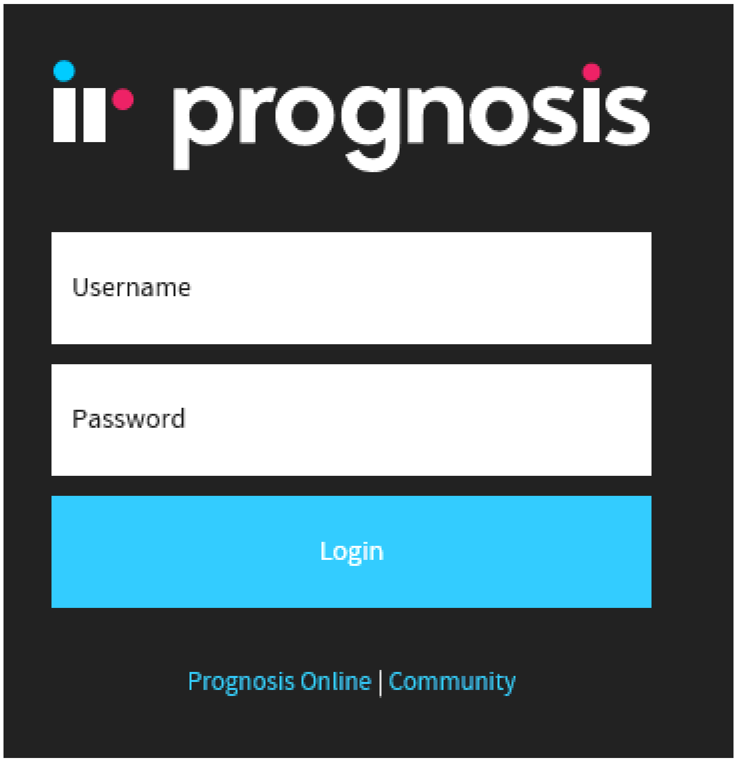
```
save translation

                               SAVE TRANSLATION

           Command Completion Status                                 Error Code

           Success                                                   0
```

6. Configure Integrated Research Prognosis

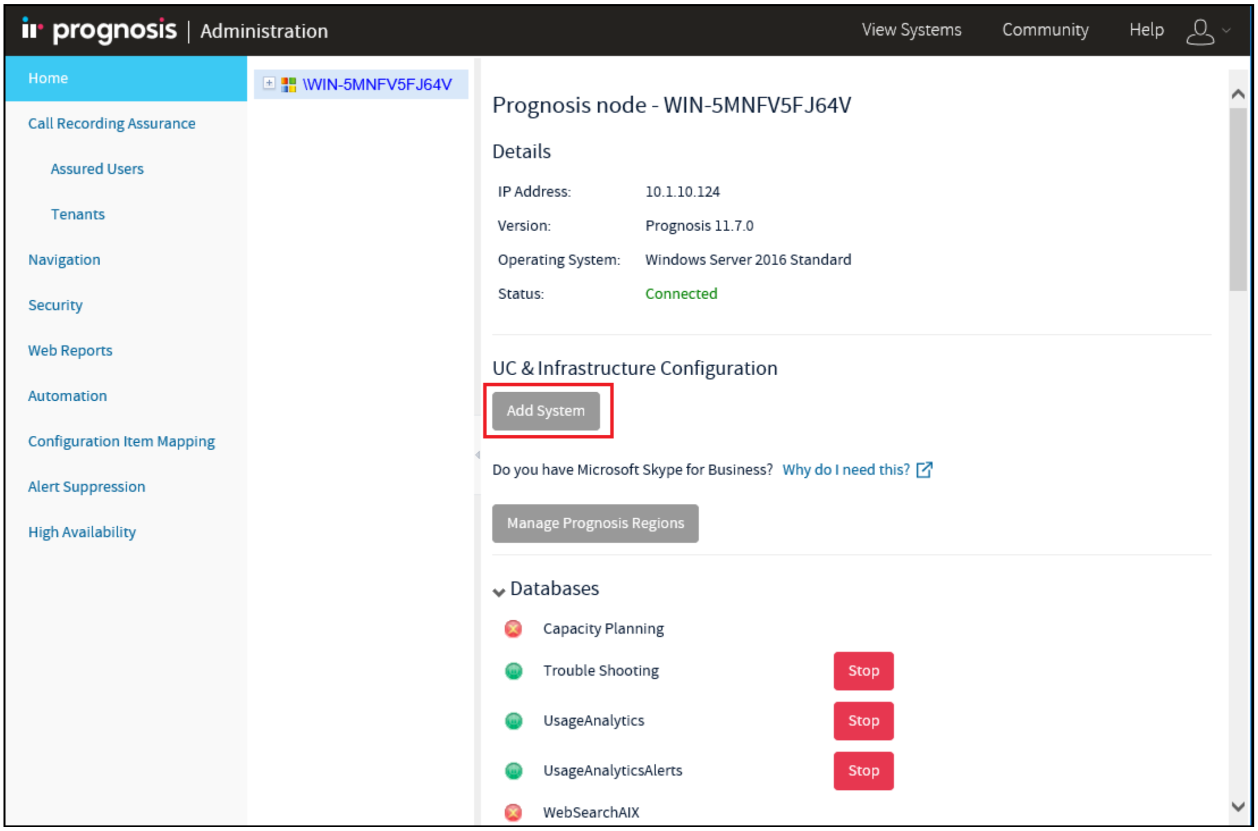
This section describes the configuration of Prognosis required to interoperate with Communication Manager. Configuration of Prognosis to interoperate with Session and System Manager can be referred from **Reference [3]** and will not be detailed here.

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.



Click **Add System**.



Prognosis node - WIN-5MNFV5FJ64V

Details

IP Address: 10.1.10.124

Version: Prognosis 11.7.0

Operating System: Windows Server 2016 Standard

Status: Connected

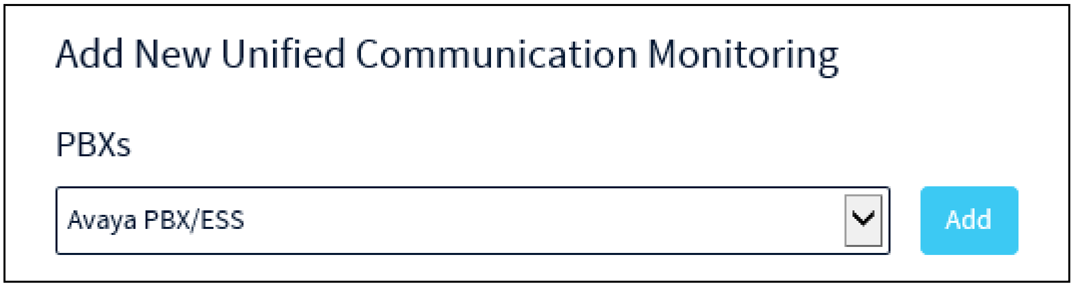
UC & Infrastructure Configuration

Do you have Microsoft Skype for Business? Why do I need this?

Databases

Capacity Planning	
Trouble Shooting	Stop
UsageAnalytics	Stop
UsageAnalyticsAlerts	Stop
WebSearchAIX	

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



Add New Unified Communication Monitoring

PBXs

Avaya PBX/ESS

In this test configuration, the following entries are added for the two Communication Manager systems with display name of **CM8-DUPLEX** (System A) and **G450-CM** (System B) and with IP addresses of **10.1.10.230** and **10.1.60.18** respectively. The display name is matched with the naming of these systems on the System Manager SIP Entities.

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

Basic Details:

- **Display Name: CM8-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:

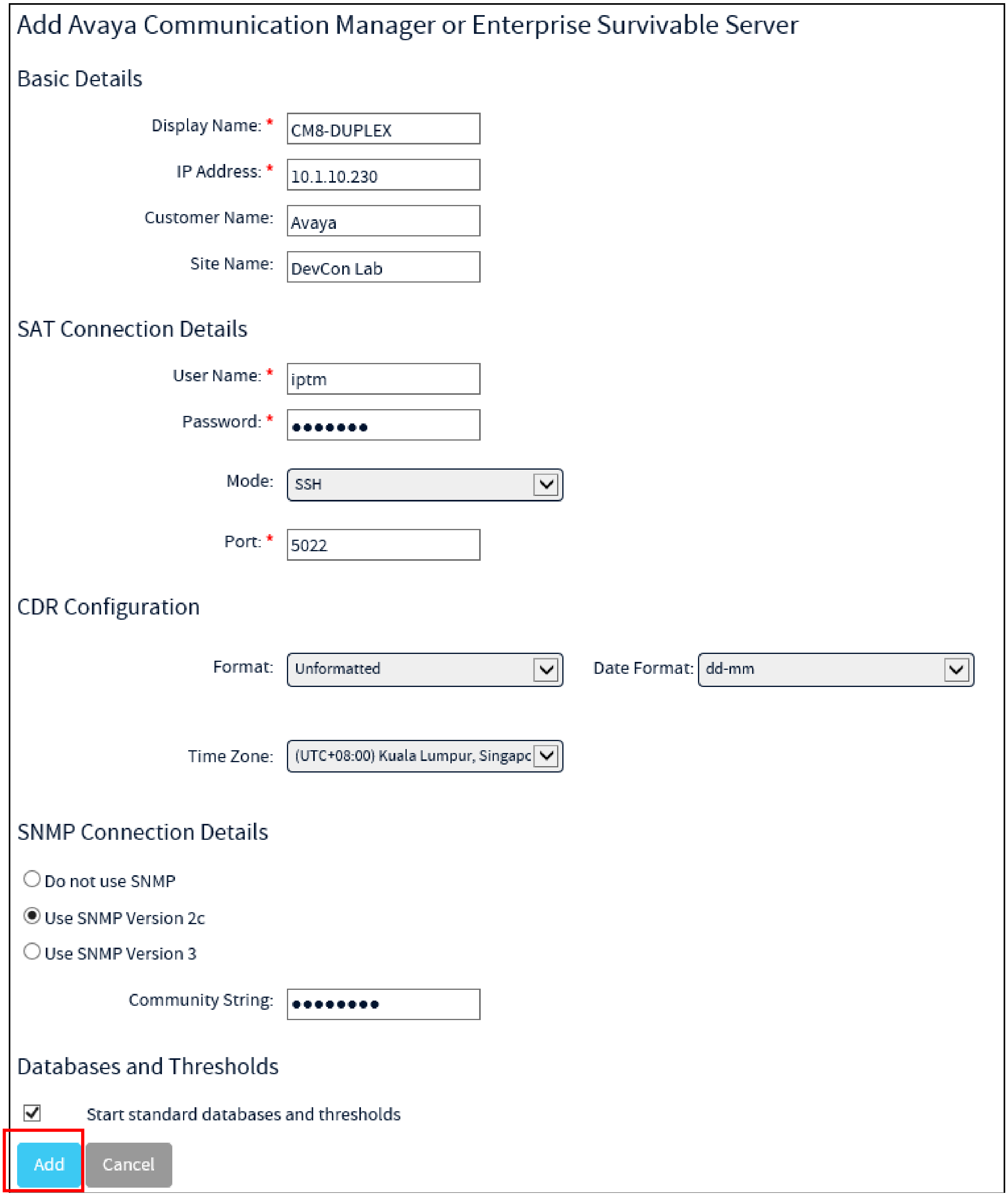
- **Format: unformatted [**as configured in **Section 5.6]**
- **Date Format: mm-dd [**as configured in **Section 5.6]**

SNMP Connection Details:

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

Leave the **Databases and Thresholds** as checked.

Click **Add** to affect the addition**.** Repeat the above for the setup of Communication Manager System B i.e., **G450-CM**.



Add Avaya Communication Manager or Enterprise Survivable Server

Basic Details

Display Name: * CM8-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, Singapc

SNMP Connection Details

○ Do not use SNMP

● Use SNMP Version 2c

○ Use SNMP Version 3

Community String: ••••••••

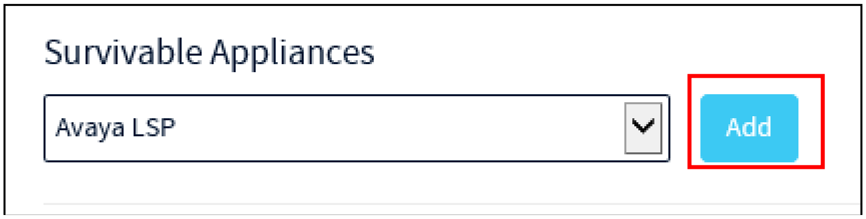
Databases and Thresholds

☑ Start standard databases and thresholds

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** and IP addresses of **10.1.40.18** and **10.1.10.239** respectively, both belonging to the **CM8-DUPLEX** Communication Manager system are also configured.

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



The following settings were used during the compliance test.

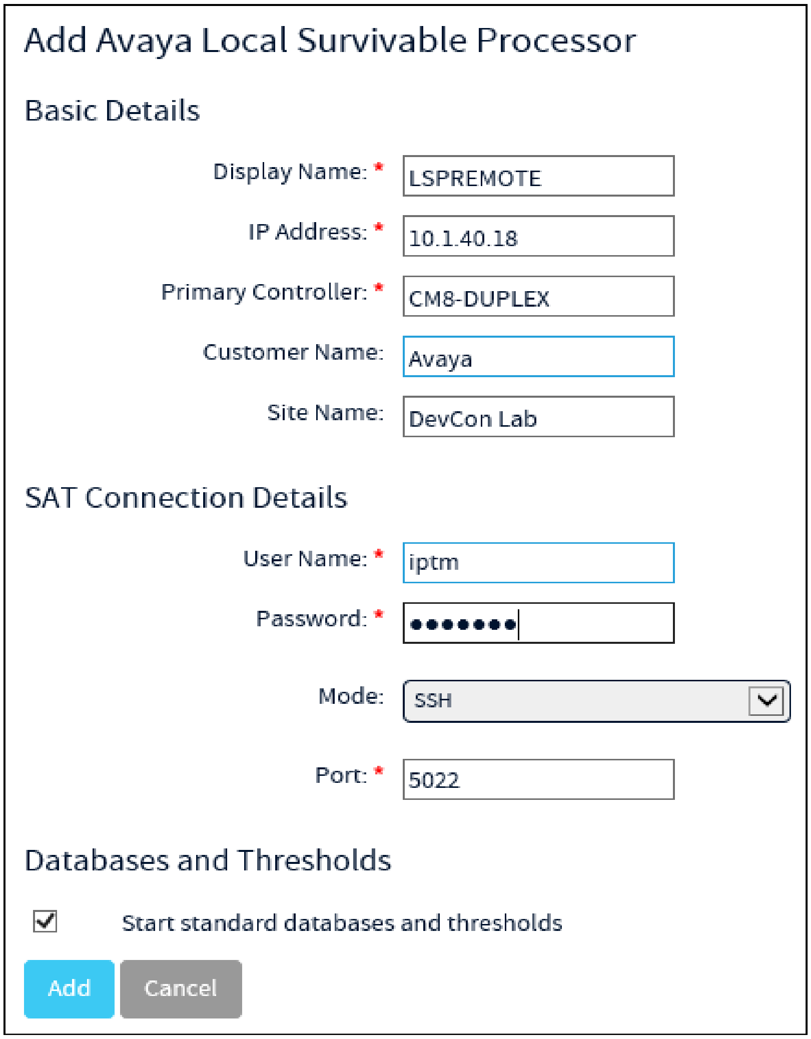
Basic Details:

- **Display Name: LSPREMOTE**
- **IP address: 10.1.40.18**
- **Primary Controller: CM8-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.



Add Avaya Local Survivable Processor

Basic Details

Display Name: *	LSPREMOTE
IP Address: *	10.1.40.18
Primary Controller: *	CM8-DUPLEX
Customer Name:	Avaya
Site Name:	DevCon Lab

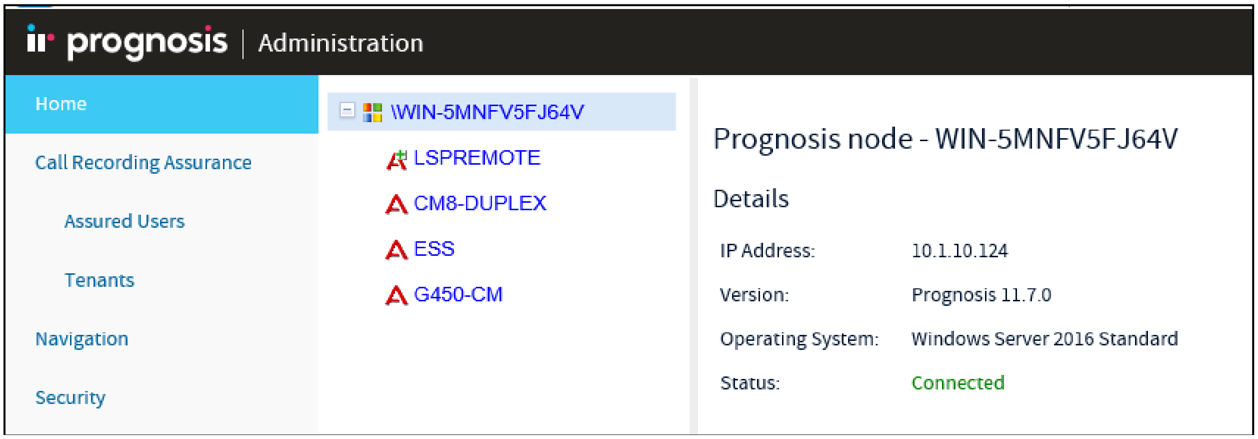
SAT Connection Details

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

Databases and Thresholds

☑ Start standard databases and thresholds

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



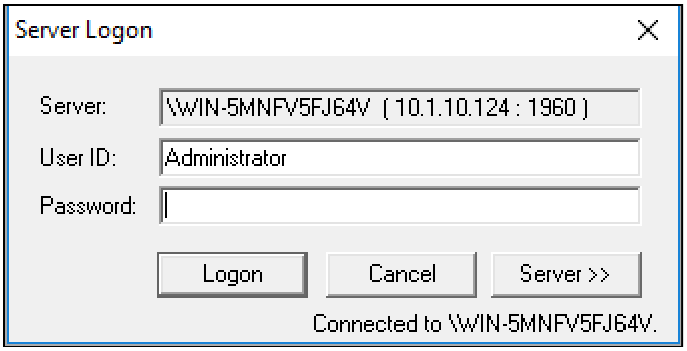
Prognosis node - WIN-5MNFV5FJ64V

Details

IP Address:	10.1.10.124
Version:	Prognosis 11.7.0
Operating System:	Windows Server 2016 Standard
Status:	Connected

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.



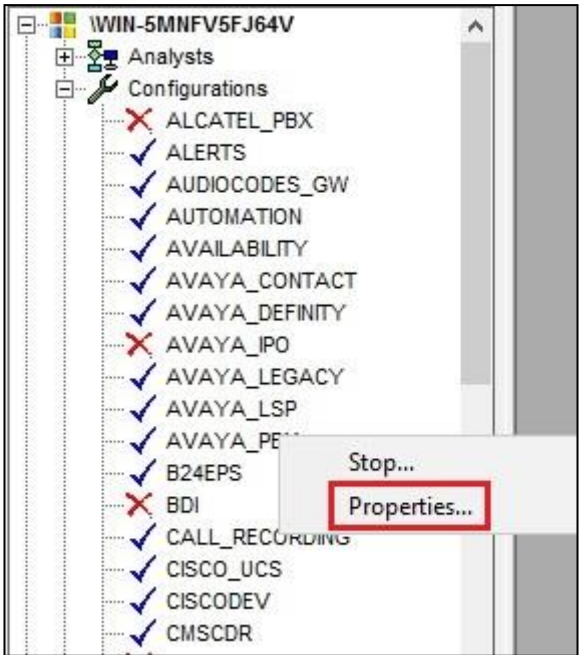
Server: \\WIN-5MNFV5FJ64V (10.1.10.124 : 1960)

User ID: Administrator

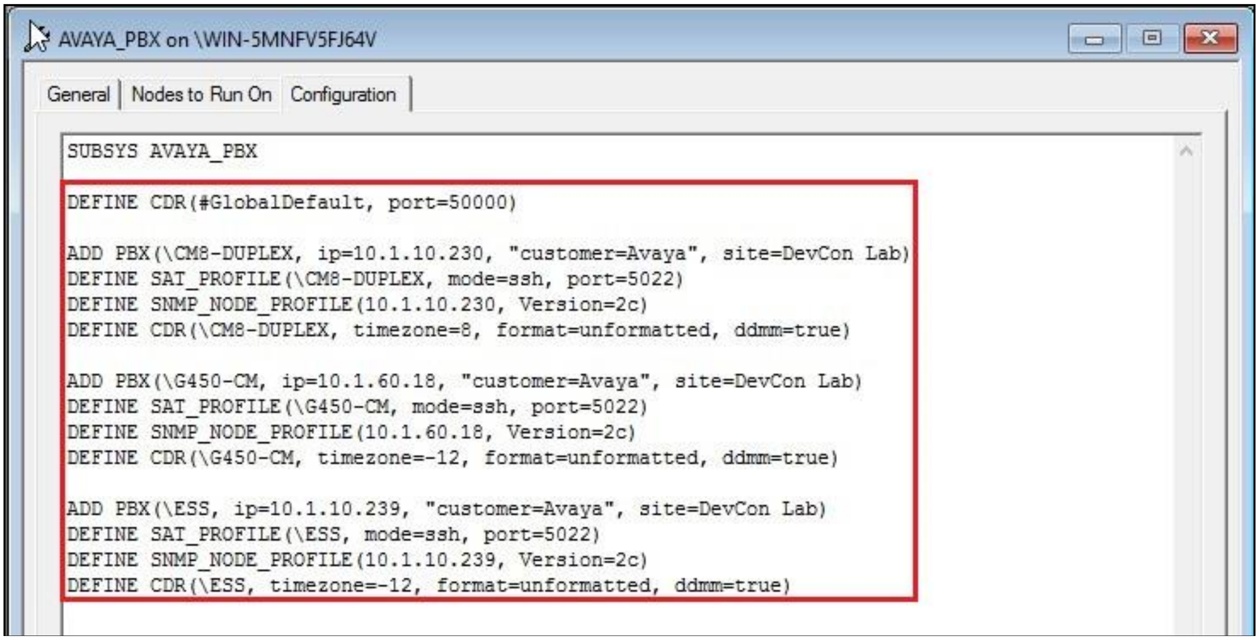
Password:

Connected to \\WIN-5MNFV5FJ64V.

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**.

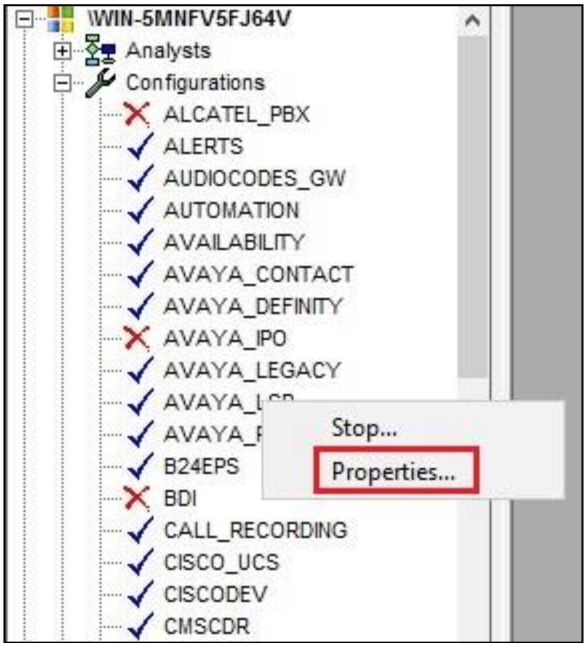


Check the configurations for each Communication Manager and the corresponding CDR settings configured in **Section 6.1**. Note that the default CDR port is **50000** which correspond to the configurations set in **Section 5.6** is already created as default.

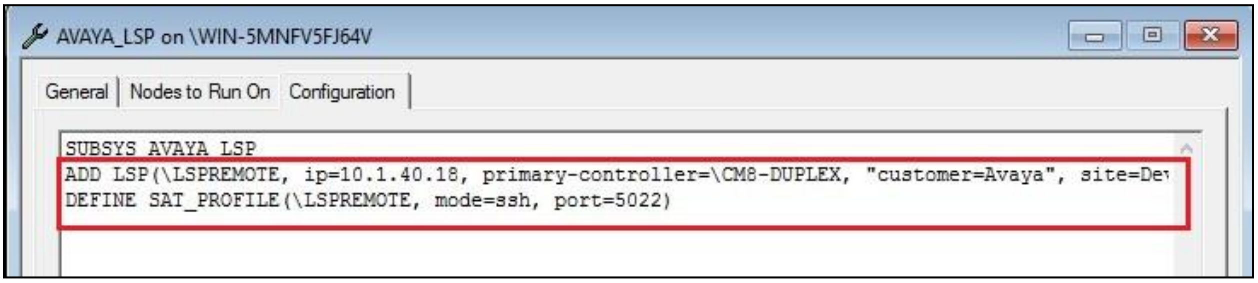


```
SUBSYS AVAYA_PBX

DEFINE CDR(#GlobalDefault, port=50000)

ADD PBX(\CM8-DUPLEX, ip=10.1.10.230, "customer=Avaya", site=DevCon Lab)
DEFINE SAT_PROFILE(\CM8-DUPLEX, mode=ssh, port=5022)
DEFINE SNMP_NODE_PROFILE(10.1.10.230, Version=2c)
DEFINE CDR(\CM8-DUPLEX, timezone=8, format=unformatted, ddmm=true)

ADD PBX(\G450-CM, ip=10.1.60.18, "customer=Avaya", site=DevCon Lab)
DEFINE SAT_PROFILE(\G450-CM, mode=ssh, port=5022)
DEFINE SNMP_NODE_PROFILE(10.1.60.18, Version=2c)
DEFINE CDR(\G450-CM, timezone=-12, format=unformatted, ddmm=true)

ADD PBX(\ESS, ip=10.1.10.239, "customer=Avaya", site=DevCon Lab)
DEFINE SAT_PROFILE(\ESS, mode=ssh, port=5022)
DEFINE SNMP_NODE_PROFILE(10.1.10.239, Version=2c)
DEFINE CDR(\ESS, timezone=-12, format=unformatted, ddmm=true)
```

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**.

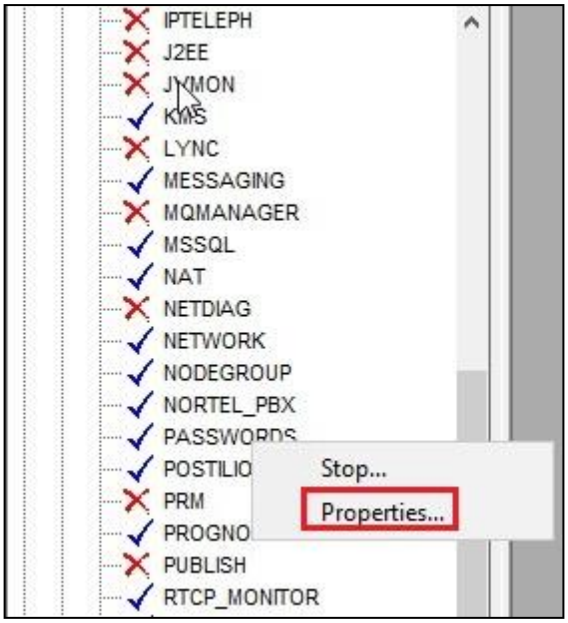


Check the configurations for LSP server to be monitored as configured in **Section 6.2** earlier.

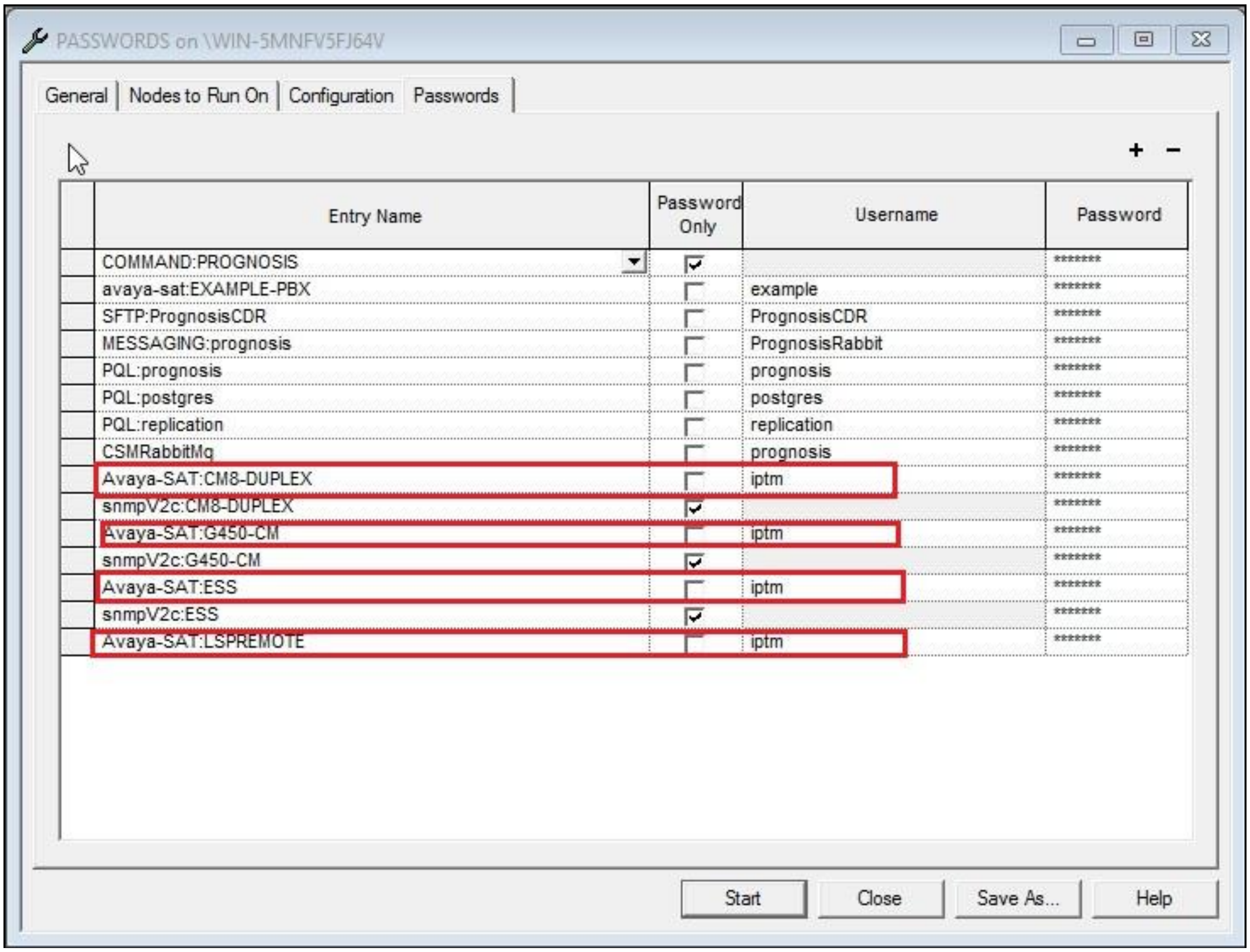


```
SUBSYS AVAYA_LSP
ADD LSP(\LSPREMOTE, ip=10.1.40.18, primary-controller=\CM8-DUPLEX, "customer=Avaya", site=De
DEFINE SAT_PROFILE(\LSPREMOTE, mode=ssh, port=5022)
```

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 **CM7-DUPLEX**, **G450-CM, LSPREMOTE** and **ESS** are listed below.



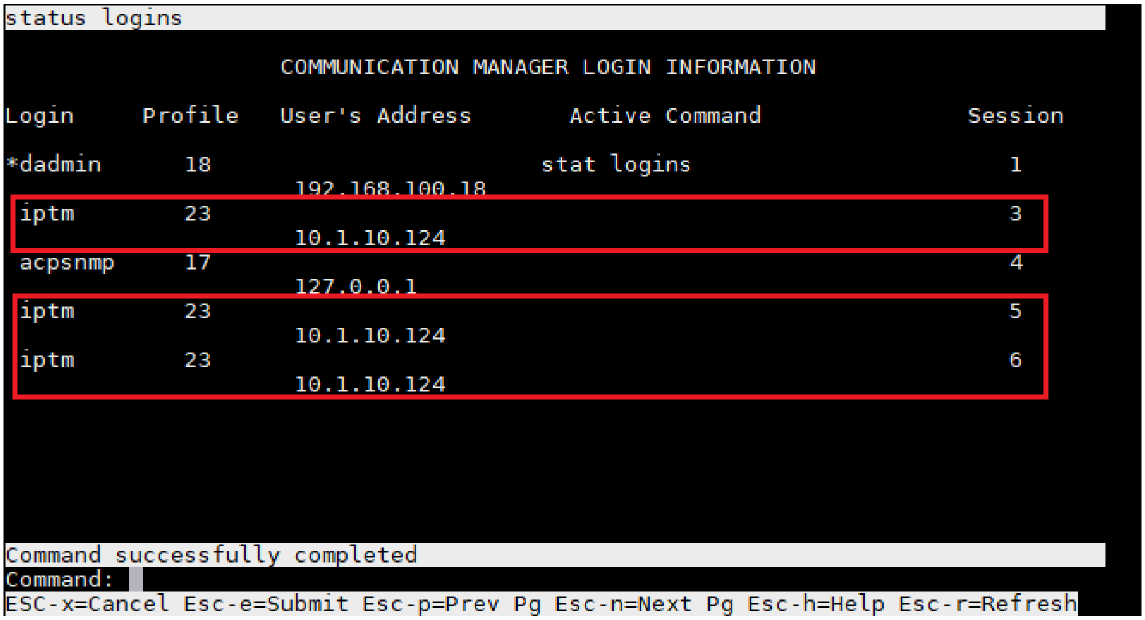
Entry Name	Password Only	Username	Password
COMMAND:PROGNOSIS	☑		********
avaya-sat:EXAMPLE-PBX	□	example	********
SFTP:PrognosisCDR	□	PrognosisCDR	********
MESSAGING:prognosis	□	PrognosisRabbit	********
PQL:prognosis	□	prognosis	********
PQL:postgres	□	postgres	********
PQL:replication	□	replication	********
CSMRabbitMq	□	prognosis	********
Avaya-SAT:CM8-DUPLEX	□	iptm	********
snmpV2c:CM8-DUPLEX	☑		********
Avaya-SAT:G450-CM	□	iptm	********
snmpV2c:G450-CM	☑		********
Avaya-SAT:ESS	□	iptm	********
snmpV2c:ESS	☑		********
Avaya-SAT:LSPREMOTE	□	iptm	********

7. Verification Steps

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

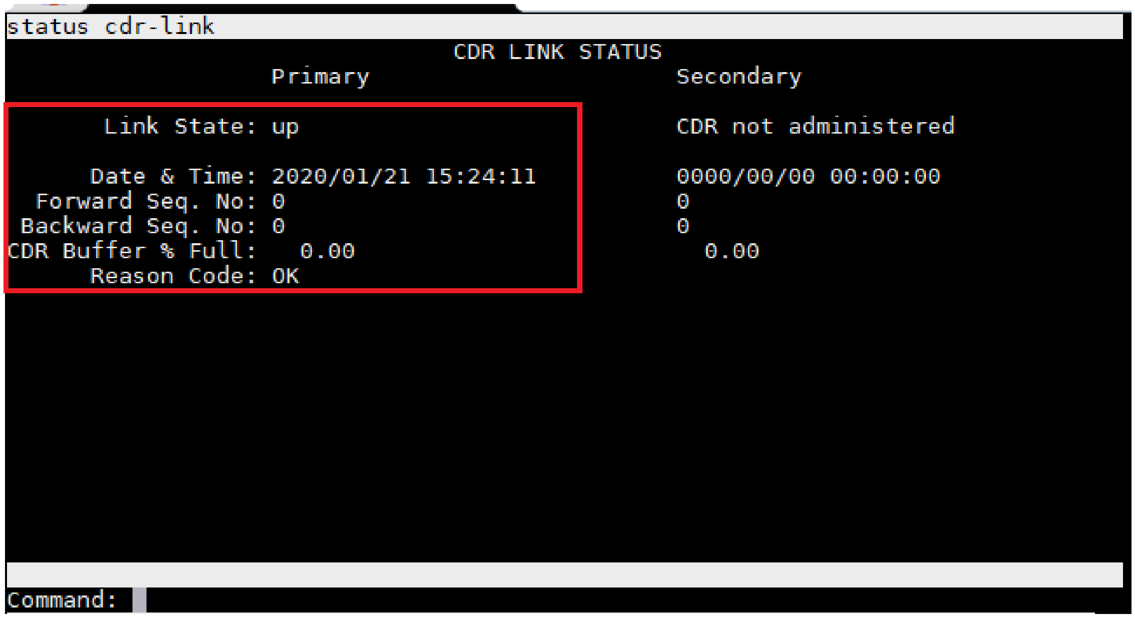
7.1. Verify Communication Manager

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



```
status logins

                    COMMUNICATION MANAGER LOGIN INFORMATION

Login     Profile   User's Address       Active Command              Session

*dadmin      18                        stat logins                      1
                     192.168.100.18
 iptm        23                                                         3
                     10.1.10.124
 acpsnmp     17                                                         4
                     127.0.0.1
 iptm        23                                                         5
                     10.1.10.124
 iptm        23                                                         6
                     10.1.10.124




Command successfully completed
Command:
ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh
```

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

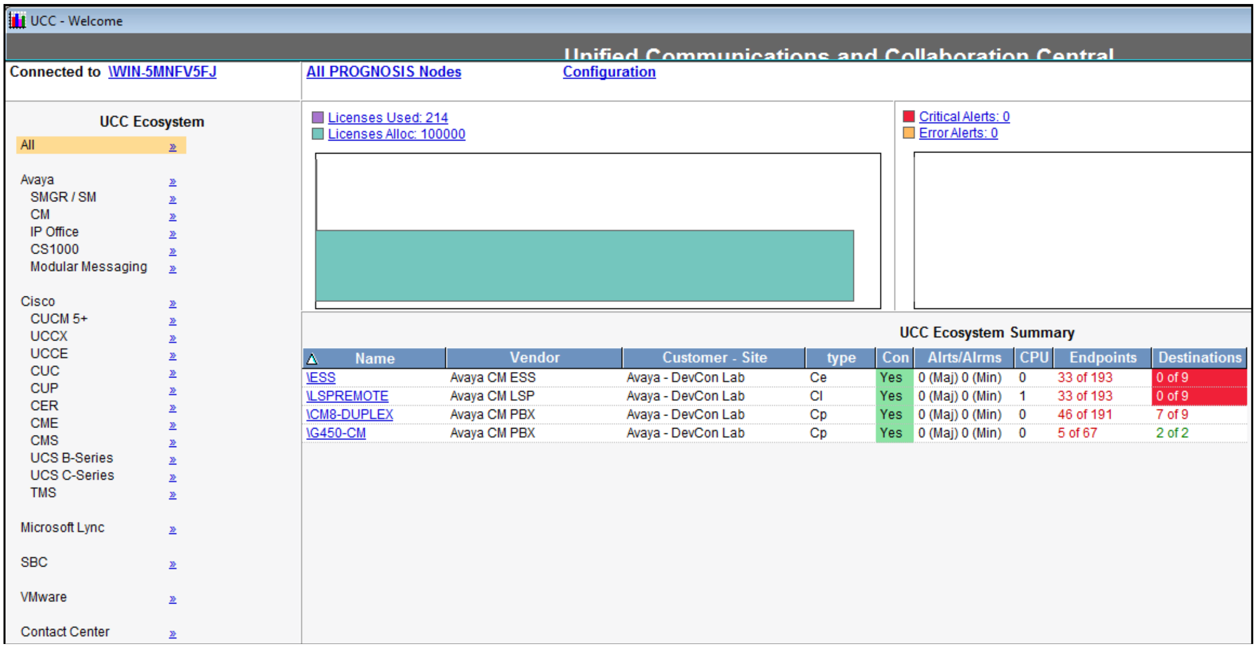


```
status cdr-link
                              CDR LINK STATUS
                   Primary                        Secondary

       Link State: up                             CDR not administered

      Date & Time: 2020/01/21 15:24:11            0000/00/00 00:00:00
  Forward Seq. No: 0                              0
 Backward Seq. No: 0                              0
CDR Buffer % Full:   0.00                           0.00
      Reason Code: OK









Command:
```

7.2. Verify Prognosis

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

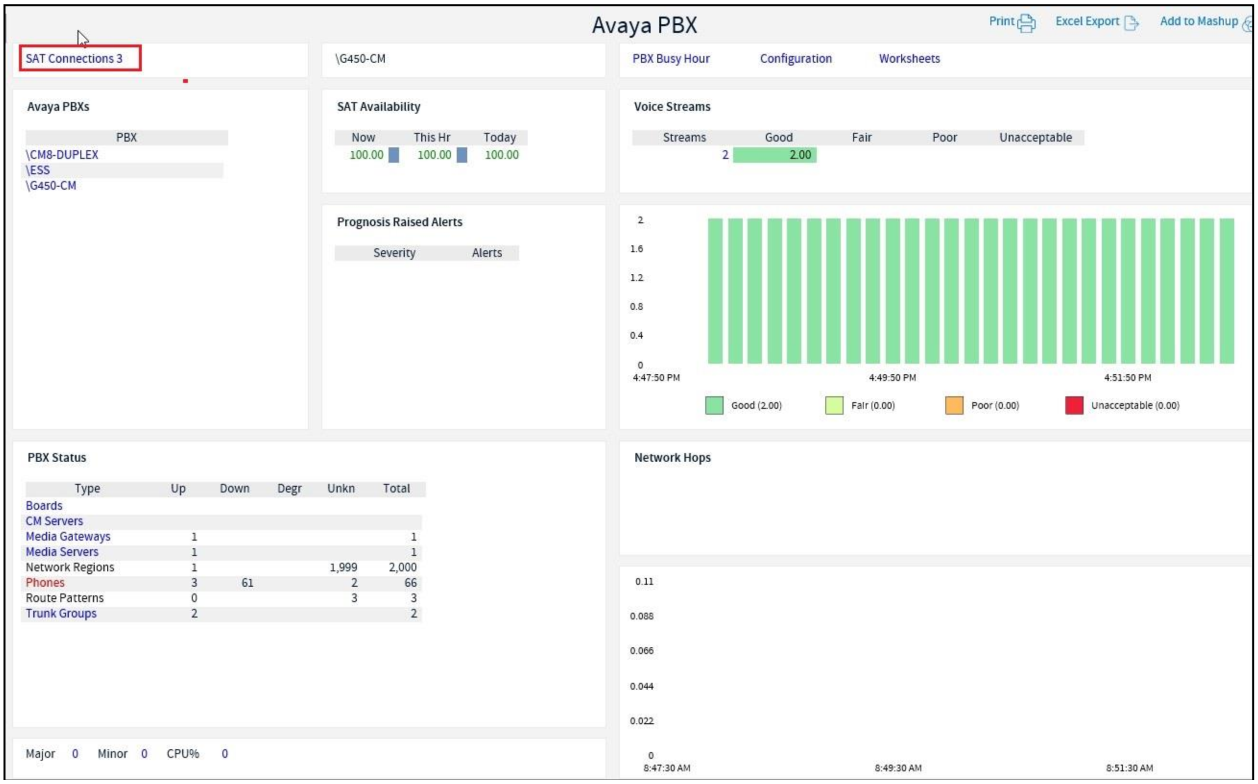
After logging into Prognosis webui and selecting the home screen icon above, the list of Communication Manager servers configured in **Section 6** is displayed on the right pane under **UC Ecosystem Summary**.



UCC Ecosystem Summary

△ Name	Vendor	Customer - Site	type	Con	Alrts/Alrms	CPU	Endpoints	Destinations
\ESS	Avaya CM ESS	Avaya - DevCon Lab	Ce	Yes	0 (Maj) 0 (Min)	0	33 of 193	0 of 9
\LSPREMOTE	Avaya CM LSP	Avaya - DevCon Lab	Cl	Yes	0 (Maj) 0 (Min)	1	33 of 193	0 of 9
\CM8-DUPLEX	Avaya CM PBX	Avaya - DevCon Lab	Cp	Yes	0 (Maj) 0 (Min)	0	46 of 191	7 of 9
\G450-CM	Avaya CM PBX	Avaya - DevCon Lab	Cp	Yes	0 (Maj) 0 (Min)	0	5 of 67	2 of 2

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



PBX
\CM8-DUPLEX
\ESS
\G450-CM

Now	This Hr	Today
100.00	100.00	100.00

Severity	Alerts

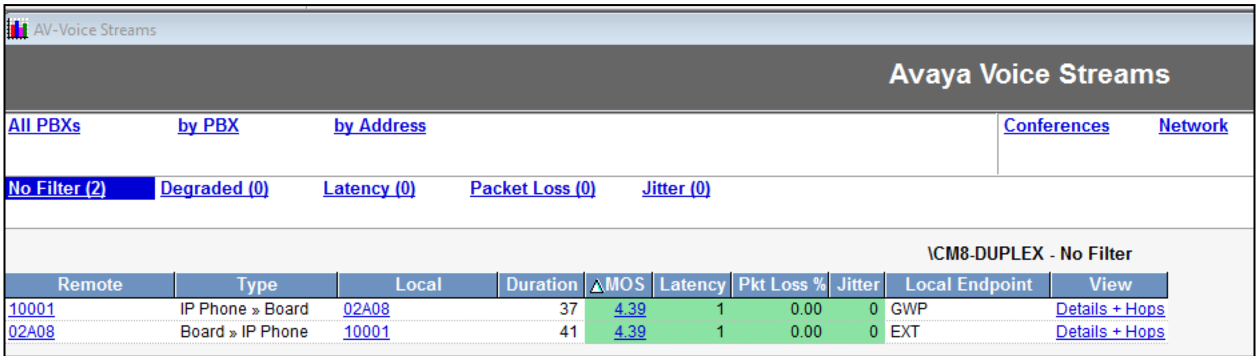
Streams	Good	Fair	Poor	Unacceptable
2	2.00			

PBX Status

Type	Up	Down	Degr	Unkn	Total
Boards					
CM Servers					
Media Gateways	1				1
Media Servers	1				1
Network Regions	1			1,999	2,000
Phones	3	61		2	66
Route Patterns	0			3	3
Trunk Groups	2				2

Major 0 Minor 0 CPU% 0

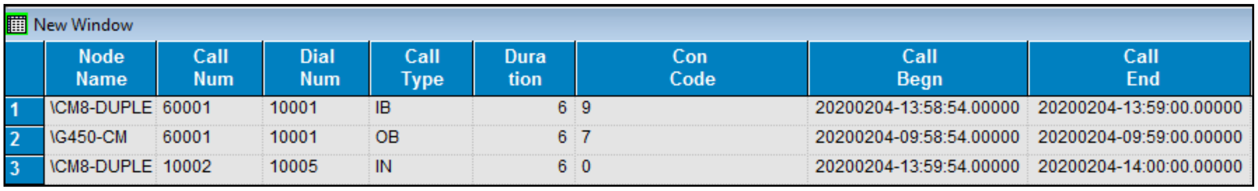
Make a call between two Avaya IP telephones that belong to an IP Network Region that is being configured to send RTCP information to the Prognosis server. Verify that the **Voice Streams** section shows two active voice streams reflecting the quality of the call.



\CM8-DUPLEX - No Filter

Remote	Type	Local	Duration	ΔMOS	Latency	Pkt Loss %	Jitter	Local Endpoint	View
10001	IP Phone » Board	02A08	37	4.39	1	0.00	0	GWP	Details + Hops
02A08	Board » IP Phone	10001	41	4.39	1	0.00	0	EXT	Details + Hops

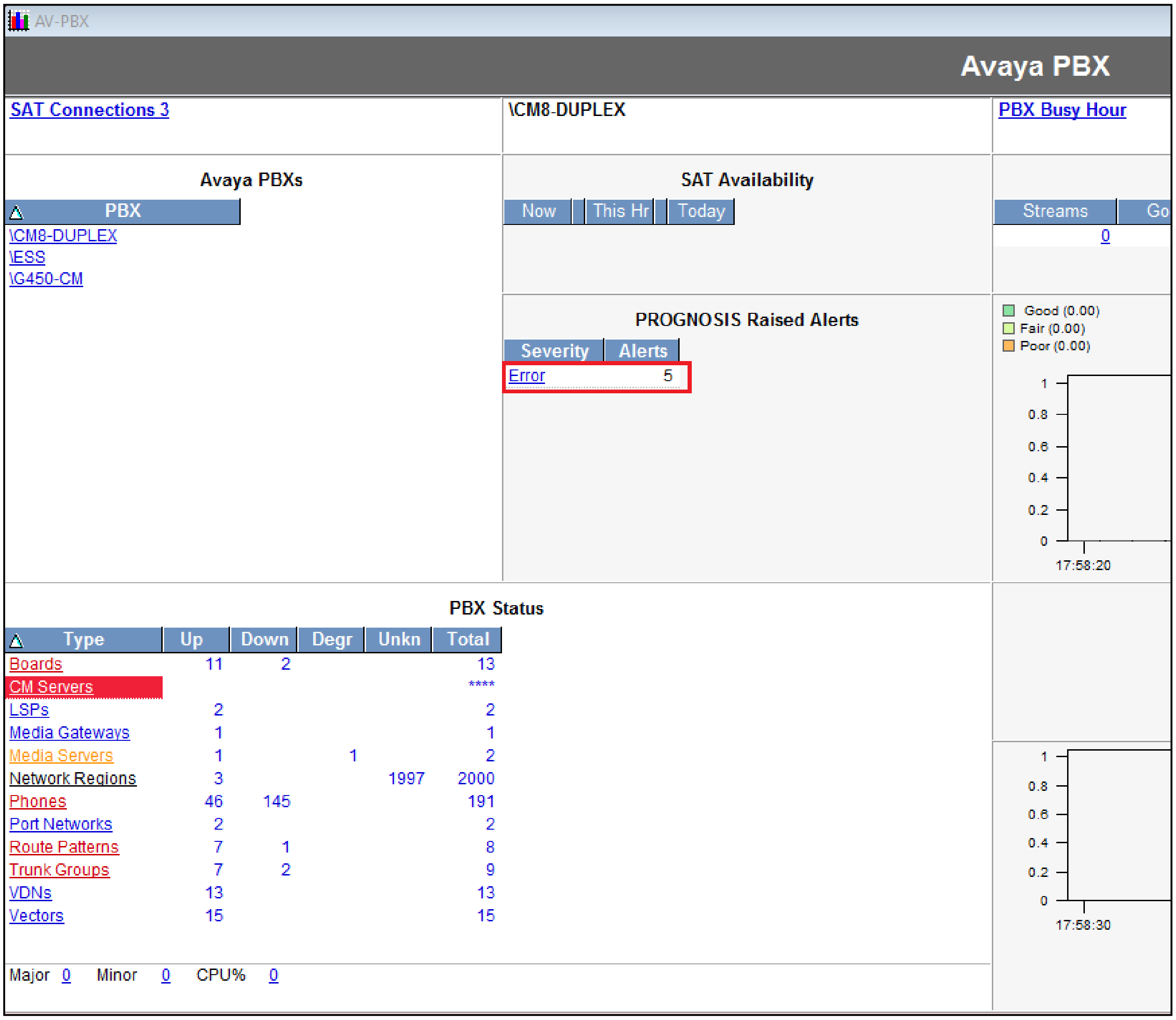
Verify the CDR data by making outbound and inbound calls from Communication Manager System B to Communication Manager System A as well intra call within Communication Manager A. Captured CDR data can be custom designed for the layout. Below is a sample of a captured CDR data.



New Window

	Node Name	Call Num	Dial Num	Call Type	Duration	Con Code	Call Begn	Call End
1	\CM8-DUPLE	60001	10001	IB	6	9	20200204-13:58:54.00000	20200204-13:59:00.00000
2	\G450-CM	60001	10001	OB	6	7	20200204-09:58:54.00000	20200204-09:59:00.00000
3	\CM8-DUPLE	10002	10005	IN	6	0	20200204-13:59:54.00000	20200204-14:00:00.00000

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



Avaya PBX

SAT Connections 3

\CM8-DUPLEX

PBX Busy Hour

Avaya PBXs

PBX
\CM8-DUPLEX
\ESS
\G450-CM

SAT Availability

Now	This Hr	Today

Streams	Go
0	

PROGNOSIS Raised Alerts

Severity	Alerts
Error	5

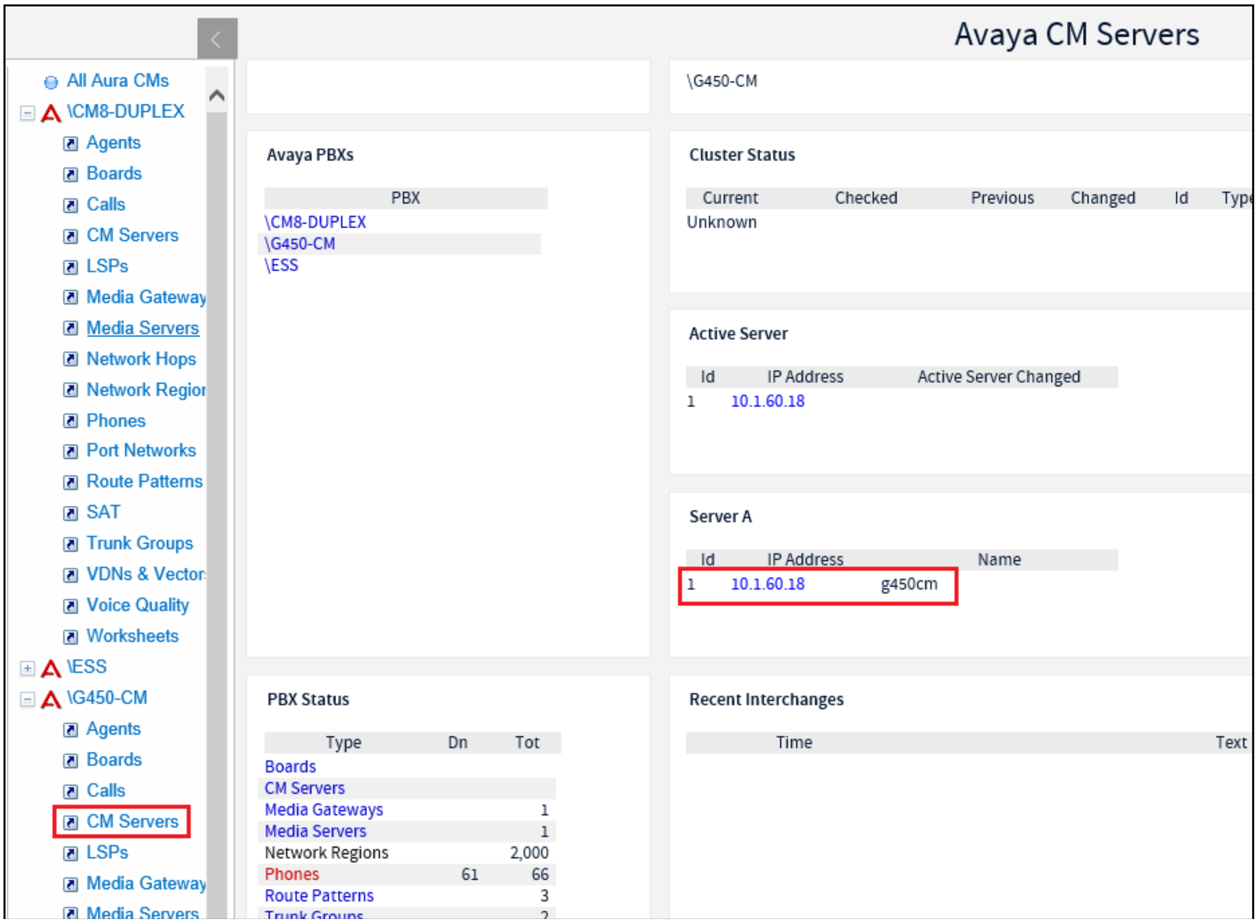
🟩 Good (0.00)
🟨 Fair (0.00)
🟧 Poor (0.00)

PBX Status

Type	Up	Down	Degr	Unkn	Total
Boards	11	2			13
CM Servers					****
LSPs	2				2
Media Gateways	1				1
Media Servers	1		1		2
Network Regions	3			1997	2000
Phones	46	145			191
Port Networks	2				2
Route Patterns	7	1			8
Trunk Groups	7	2			9
VDNs	13				13
Vectors	15				15

Major 0 Minor 0 CPU% 0

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



Avaya CM Servers

\G450-CM

Avaya PBXs

PBX
\CM8-DUPLEX
\G450-CM
\ESS

Cluster Status

Current	Checked	Previous	Changed	Id	Type
Unknown					

Active Server

Id	IP Address	Active Server Changed
1	10.1.60.18	

Server A

Id	IP Address	Name
1	10.1.60.18	g450cm

PBX Status

Type	Dn	Tot
Boards		
CM Servers		
Media Gateways		1
Media Servers		1
Network Regions		2,000
Phones	61	66
Route Patterns		3
Trunk Groups		2

Recent Interchanges

Time	Text

8. Conclusion

These Application Notes describe the procedures for configuring the Integrated Research Prognosis for Unified Communications R11.7 to interoperate with Avaya Aura® Communication Manager R8.1. In the configuration described in these Application Notes, Prognosis established SSH connections to the SAT to view the configurations of Communication Manager. Prognosis also processed the RTCP information to monitor the quality of IP calls and collected CDR information sent by Communication Manager. Prognosis also obtained the Communication Manager name and IP address from the SNMP information. 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 8.1, Issue 5, Dec 2019.

[2] *Administering Avaya Aura® Communication Manager*, Release 8.1.x, Issue 5, Nov 2019.

[3] *Application Notes for Integrated Research's Prognosis for Unified Communications 11.7 with Avaya Aura® Session Manager R8.1 and Avaya Aura® System Manager R8.1.*

Prognosis documentations are provided with the software package.

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.