



Avaya Solution & Interoperability Test Lab

Application Notes for Nectar Unified Communications Management Platform (UCMP) Version 7.3 and Avaya Aura® Communication Manager 7.1 - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Nectar UCMP to interoperate with Avaya Aura® Communication Manager. Nectar UCMP integrates directly to Communication Manager using Secure Shell (SSH) or Telnet. At the same time, it processes Simple Network Management Protocol (SNMP) and Real-time Transport Control Protocol (RTCP) information from Communication Manager, Gateways and Avaya Endpoints.

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 Nectar UCMP with Avaya Aura® Communication Manager.

Nectar's Unified Communications Management Platform (UCMP) is a multi-vendor UC operations management platform enabling enterprises and service providers to deliver great user experiences with monitoring, troubleshooting and reporting tools. UCMP provides actionable visibility across the platform, network and endpoint health domains to enable: proactive issue avoidance based on contextual monitoring, significantly faster root cause analysis & issue correlation, and powerful insight & reporting on critical health factors that contribute to user experience.

For Avaya Communication Manager, Nectar delivers inventory, contextual alarms, resource consumption, and performance metrics. Nectar also captures and reports on real-time RTCP call quality data from: H.323 endpoints, Avaya Media Gateways and MedPros, Avaya Aura® Media Server, and Avaya soft clients including Equinox.

Nectar UCMP uses three methods below to monitor a Communication Manager system.

- System Access Terminal (SAT) – Nectar UCMP uses telnet/SSH connections to the SAT using the IP address of Communication Manager. By default, the solution establishes 3 concurrent SAT connections to the Communication Manager system and uses the connections to execute SAT commands.
- Real Time Transport Control Protocol (RTCP) Collection – Nectar UCMP collects RTCP information sent by the Communication Manager, media gateways, and IP Telephones. The call quality metrics including RTD, packet loss, jitter and DSCP are collected and from these metrics, the MOS (mean opinion score) is computed, which measures overall call quality.
- Simple Network Management Protocol (SNMP) Collection – Nectar UCMP uses SNMP to collect configuration and status information and SNMP traps from Communication Manager.

2. General Test Approach and Test Results

The general test approach was to configure the Avaya equipment and verify Nectar UCMP interoperability as on a customer site. The interoperability compliance test included both feature and functionality testing.

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 the Nectar UCMP did not include use of any specific encryption features as requested by Nectar. Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

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 this Application Note, 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 this Application Note 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, Nectar used Java-based Remote Intelligent Gateway (RIG) Client application to view the configurations of Communication Manager including: trunk groups, route patterns, IP network regions, stations, processor occupancy, SNMP alarm and error information...etc. For the collection of RTCP information, the endpoints included Avaya H323, SIP, Media Server, Media Gateway, Equinox soft client, digital and analog telephones. The types of calls made

included intra-switch calls, inbound/outbound PSTN calls, inbound/outbound inter-switch IP trunk calls, transfer and conference calls.

For serviceability testing, reboots were applied to the Nectar server and Avaya Servers to simulate system unavailability.

2.2. Test Results

The tests were all functional in nature and performance testing was not included. All the test cases passed successfully.

2.3. Support

For technical support on Nectar UCMP, contact the Nectar Support Team at:

- Email: support@nectarcorp.com
- Phone: 1-888-811-8647

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Nectar interoperability with Communication Manager, G450 Media Gateway, Media Server, Session Manager, and System Manager. Nectar UCMP connected on the same LAN as the Avaya equipment and collects relevant information using SAT and SNMP from Communication Manager. Nectar also monitors RTCP. A variety of Avaya telephones were configured and used to make calls to be monitored. A simulated PSTN was also configured to allow incoming and outgoing calls.

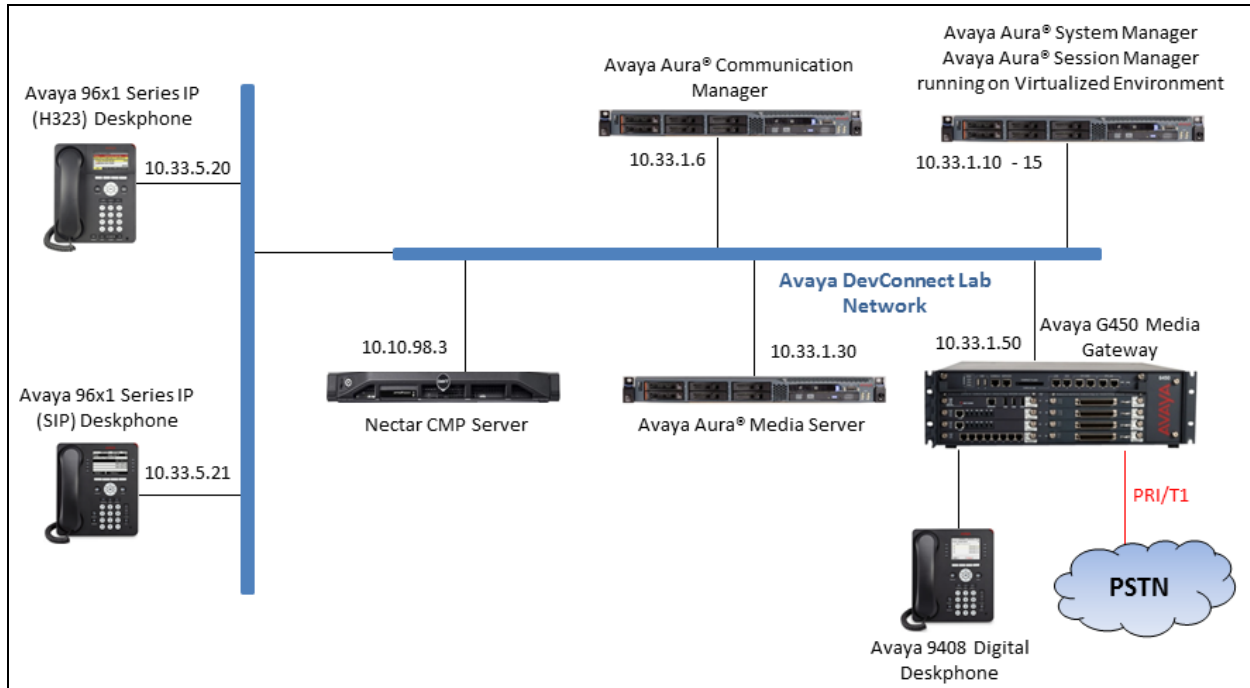


Figure 1: Test Configuration Diagram

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 running on Virtual Environment	7.1.3.0 (7.1.3.0.0.532.24515)
Avaya Aura® Session Manager running on Virtual Environment	7.1.3.0 (7.1.3.0.713014)
Avaya Aura® System Manager running on Virtual Environment	7.1.3.0 (7.1.3.0.037763)
Avaya Aura® Media Server running on Virtual Environment	7.8.0.333
Avaya G450 Media Gateway	39 .12 .0
Avaya Telephones	
9641GS (H323)	6.6604
9611G (H323)	6.6604
9608G (SIP)	7.1.3
9641G (SIP)	7.1.3
Avaya Digital 1416 Telephone	FW1
Nectar UCMP running on Windows 2012	7.3-CMP7413

5. Configure Avaya Aura® Communication Manager

Configuration and verification operations on Communication Manager illustrated in this section were all performed using Avaya Site Administrator Emulation Mode. The information provided in this section describes the configuration of Communication Manager for this solution. It is implied a working system is already in place. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 12**. The configuration described in this section can be summarized as follows:

- Configure SAT User Profile
- Configure Login Group
- Configure SNMP on Avaya Aura® Communication Manager
- Configure RTCP Monitoring

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 Nectar UCMP does not modify any system configuration, create a SAT User Profile with limited permissions to assign to the Nectar UCMP login account.

Use 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 20 is created.

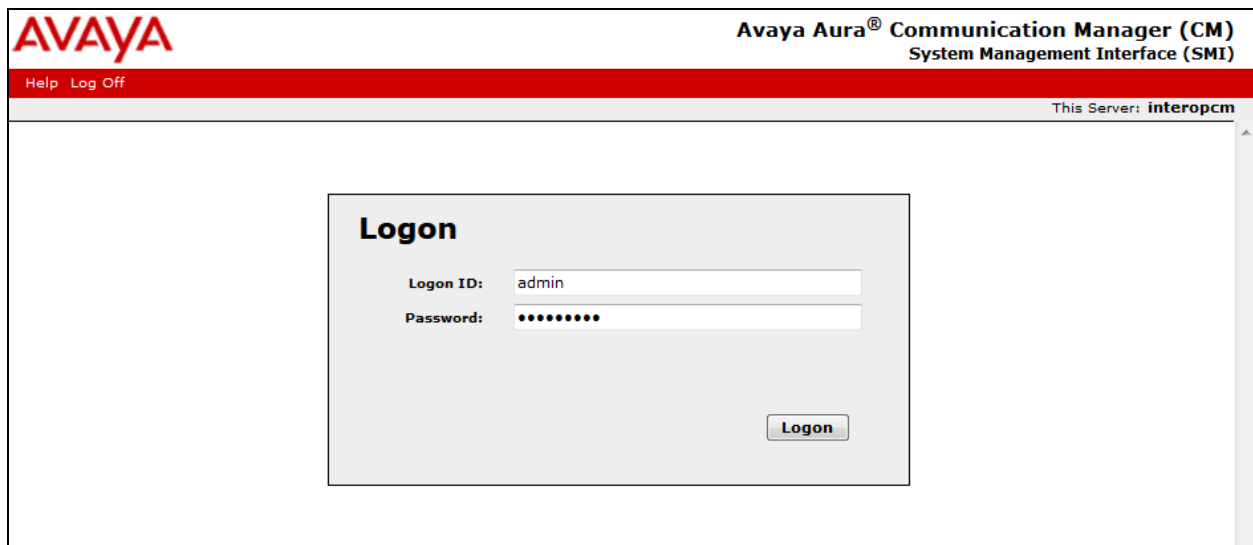
add user-profile-by-category 20						Page 1 of 39	
USER PROFILE 20							
User Profile Name: Nectar							
This Profile is Disabled? n				Shell Access? n			
Facility Test Call Notification? n				Acknowledgement Required? n			
Grant Un-owned Permissions? y				Extended Profile? n			
Name	Cat	Enbl	Name	Cat	Enbl		
Adjuncts	A	y	Routing and Dial Plan	J	y		
Call Center	B	y	Security	K	n		
Features	C	y	Servers	L	y		
Hardware	D	y	Stations	M	y		
Hospitality	E	y	System Parameters	N	y		
IP	F	y	Translations	O	n		
Maintenance	G	y	Trunking	P	y		
Measurements and Performance	H	y	Usage	Q	y		
Remote Access	I	n	User Access	R	n		

On Pages 2 to 41 of the USER PROFILE forms, set the permissions of all objects to as shown in the table below. Submit the form to create the user profile.

add user-profile 20			Page 2 of 41	
USER PROFILE BY CATEGORY 20				
Set Permissions For Category:		To:	Set All Permissions To:	
'-'=no access 'r'=list,display,status		'w'=add,change,remove+r	'm'=maintenance	
Name	Cat	Perm		
adjunct-names	A	r-		
aesvcs cti-link	A	r-		
aesvcs interface	A	r-		
aesvcs link	A	r-		
aesvcs-server	A	r-		
intra-switch-cdr	A	r-		
communication-interface links	A	r-		
mis	A	r-		
comm-intf proc-chan	A	r-		
processor-ip-interface	A	r-		

5.2. Configure Login Group

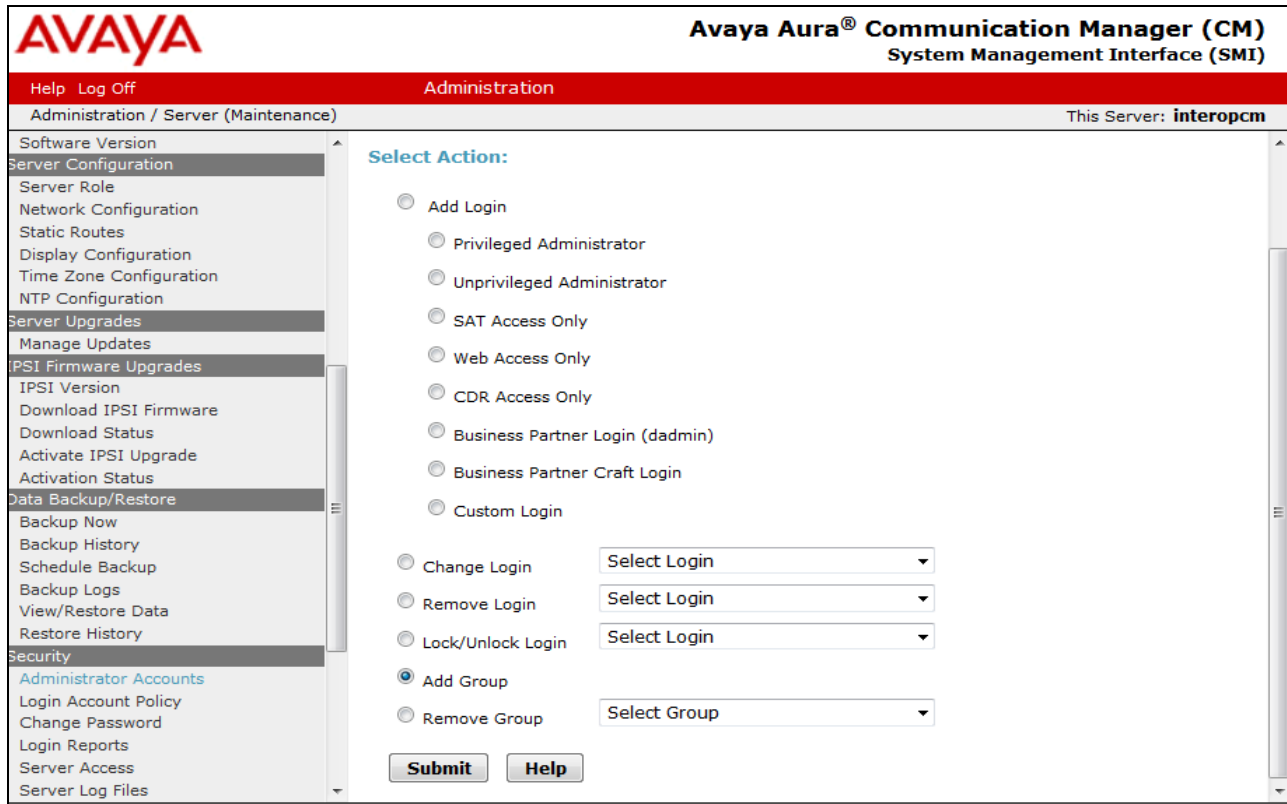
Create an Access-Profile Group on Communication Manager System Management Interface (SMI) to correspond to the SAT User Profile created in **Section 5.1**. Using a web browser, enter `https://<IP address of Communication Manager>` to connect to the Communication Manager Server being configured and log in using appropriate credentials.



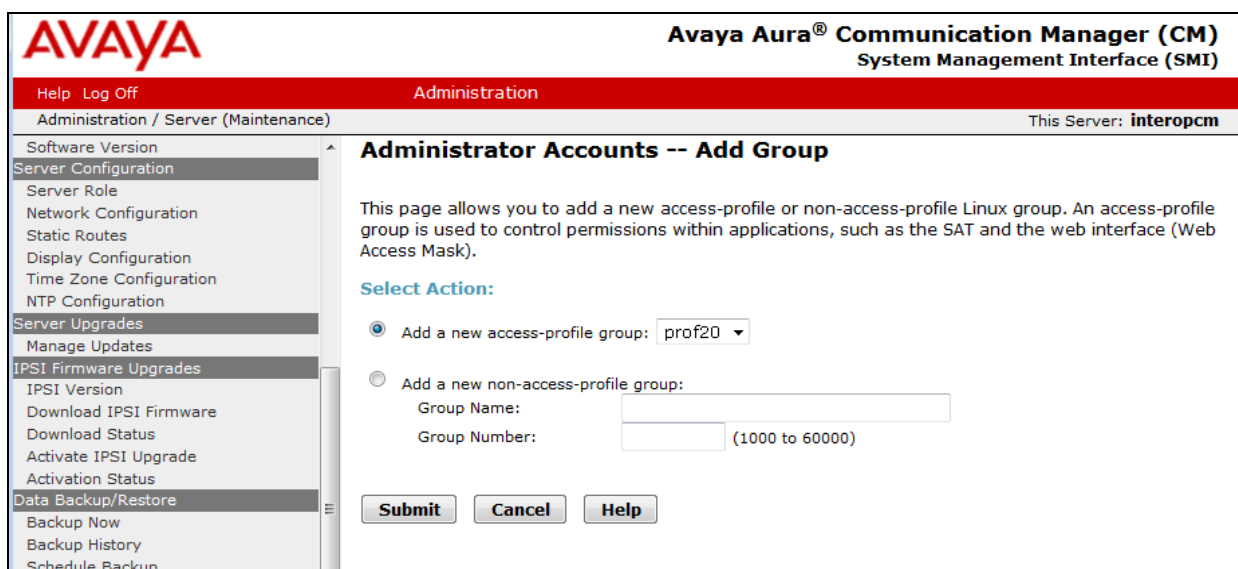
Click **Administration** → **Server (Maintenance)**. This will open up the **Server Administration Interface** that will allow the user to complete the configuration process.



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



Select **Add a new access-profile group** and select **prof20** from the drop down list to correspond to the user-profile created in **Section 5.1**. Click **Submit**. This completes the creation of the login group.



5.3. Configure Login User

Create a login account for Nectar UCMP to access the Communication Manager SAT. 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**.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes the Avaya logo, the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)", and links for "Help" and "Log Off". Below this, a red banner indicates the current section is "Administration".

The left-hand navigation pane lists various system management tasks, including "Server Configuration", "Server Upgrades", "Data Backup/Restore", and "Security". The "Administrator Accounts" option under the "Security" section is highlighted.

The main content area is titled "Administrator Accounts" and contains the following information:

- A description: "The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups."
- A "Select Action:" section with radio button options:
 - ☒ 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
- Form fields for actions:
 - ☐ Change Login: Select Login (dropdown)
 - ☐ Remove Login: Select Login (dropdown)
 - ☐ Lock/Unlock Login: Select Login (dropdown)
 - ☐ Add Group
 - ☐ Remove Group: Select Group (dropdown)
- Buttons for "Submit" and "Help" at the bottom.

In the subsequent page enter the following:

- **Login name** Enter an informative name (i.e. rig)
- **Primary group** Click on the **users** radio button
- **Additional groups (profile)** Select **prof20** from the drop down list (the **login group** created in **Section 5.2**)
- **Sat Limit** Select **None** from the drop down list
- **Select type of authentication** Click on the **Password** radio button
- **Enter password or key** Enter a password
- **Re-enter password or key** Re-enter the password
- **Force password/Key change on next login** Click on the **No** radio button



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

Administration

This Server: **interopcm**

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 System Administration Terminal (SAT) interface.

Login name	<input type="text" value="rig"/>	
Primary group	<input type="radio"/> users <input checked="" type="radio"/> susers	
Additional groups (profile)	<input type="text" value="prof20"/>	 You must assign a profile that has no web access if you want a login with SAT access only.
Linux shell	<input type="text" value="/opt/ecs/bin/autosat"/>	 This shell setting does NOT disable the "go shell" SAT command for this user.
Home directory	<input type="text" value="/var/home/rig"/>	
Lock this account	<input type="checkbox"/>	
SAT Limit	<input type="text" value="none"/>	
Date after which account is disabled-blank to ignore (YYYY-MM-DD)	<input type="text"/>	
Enter password	<input type="password" value="....."/>	
Re-enter password	<input type="password" value="....."/>	
Force password change on next login	<input checked="" type="radio"/> No <input type="radio"/> Yes	

5.4. Configure SNMP on Communication Manager

Note that the following needs to be configured per Communication Manager. If a duplex system is to be configured, complete these steps on each side of the Communication Manager.

To configure SNMP on Communication Manager navigate to **Administration → Server Administration** (not shown) and select **Agent Status**. Click **Stop Master Agent** if the **Master Agent status** is **UP** to allow setup of the SNMP Agent.

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top header includes the Avaya logo and the text "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)". Below this is a red navigation bar with "Help Log Off" and "Administration". The main content area is titled "Administration / Server (Maintenance)" and "This Server: interopcm". On the left, a sidebar menu lists various categories: Alarms, SNMP, Diagnostics, and Server. The "Agent Status" page is selected under the SNMP category. The main content area shows the "Agent Status" title, a description of the page, and the current status of the Master Agent and Sub Agents. The Master Agent status is "UP". The Sub Agent Status section shows the status of the FP Agent, CMSubAgent, and Load Agent, all of which are "UP". At the bottom, there are two buttons: "Stop Master Agent" and "Help".

Category	Sub-category	Status
Agent Status	Master Agent status:	UP
	Sub Agent Status	
	FP Agent status:	UP
Sub Agent Status	CMSubAgent status:	UP
	Load Agent status:	UP

To allow Nectar UCMP to use SNMP to collect configuration and status information from Communication Manager, Select **Access** in the left pane and enter the following in the **SNMP Version 2c** section.

- **IP address** Enter the Nectar UCMP IP address 10.10.98.3
- **Access** Select “read-only” from the list
- **Community Name** Enter a name, e.g. “public”

Click the **Submit** button at the bottom of the page (not shown).

The screenshot displays the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The top navigation bar includes 'Help', 'Log Off', and 'Administration'. The left sidebar lists various system management categories: Alarms, SNMP, Diagnostics, Server, Server Configuration, and Server Upgrades. The 'Access' page is selected under the SNMP category. The main content area is titled 'Access' and contains the following sections:

- SNMP Version 1**: Fields for IP address, Access (dropdown), and Community Name.
- SNMP Version 2c**: Fields for IP address (10.10.98.3), Access (read-only dropdown), and Community Name (public).
- SNMP Version 3**: Fields for Access (dropdown), User Name, Authentication Protocol (dropdown), Authentication Password (with a 'Minimum 8 characters' note), Privacy Protocol (dropdown), and Privacy Password (with a 'Minimum 8 characters' note).

At the bottom of the form are three buttons: 'Submit', 'Cancel', and 'Help'.

Select **FP Traps** in navigation panel on the left side and click the **Add/Change** button (not shown). In the subsequent page enter the following in the **SNMP Version 2c**:

- **IP address** Enter the IP address of Nectar UCMP e.g. **10.10.98.3**
- **Notification** Select **trap** from the drop down list
- **Community Name** Enter **public**

Click the **Submit** button at the bottom of the page.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The left navigation panel is expanded to 'FP Traps'. The main content area is titled 'Add Trap Destination' and contains three sections for configuring SNMP traps: 'SNMP Version 1', 'SNMP Version 2c', and 'SNMP Version 3'. The 'SNMP Version 2c' section is active, showing fields for IP address (10.10.98.3), Notification (trap), and Community Name (public). The 'Port' field is set to 162. At the bottom, there are 'Submit', 'Cancel', and 'Help' buttons. The footer indicates '© 2001-2017 Avaya Inc. All Rights Reserved.'

To start the SNMP agent, select **Agent Status** in navigation panel on the left side. 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.

The screenshot shows the 'Agent Status' page in the Avaya Aura Communication Manager (CM) System Management Interface (SMI). The left navigation panel is expanded to 'Agent Status'. The main content area displays the current state of the Master Agent and all Sub Agents. It shows that the Master Agent status is 'DOWN' and Sub Agents are 'NOT connected to the Master Agent'. Below this, there is a 'Sub Agent Status' section showing 'FP Agent status: UP', 'CMSubAgent status: UP', and 'Load Agent status: UP'. At the bottom, there is a 'Start Master Agent' button and a 'Help' button.

5.5. Configure RTCP Monitoring

To allow Nectar UCMP to monitor the quality of IP calls, configure Communication Manager to send RTCP reporting to the IP address of the Nectar UCMP server. This is done through the SAT interface. Use the **change system-parameters ip-options** command and enter the following:

- **Server IPV4 Address** Enter the IP address of the Nectar UCMP server
10.10.98.3
- **RTCP Report Period (secs)** Enter **5**
- **IPV4 Server Port** Enter **5005**

```
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: 10.10.98.3      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? n
```

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

Note: Only one RTCP MONITOR SERVER can be configured per IP network region. Repeat this step for all IP network regions that are required to be monitored.

```
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
```


6. Configure Nectar UCMF

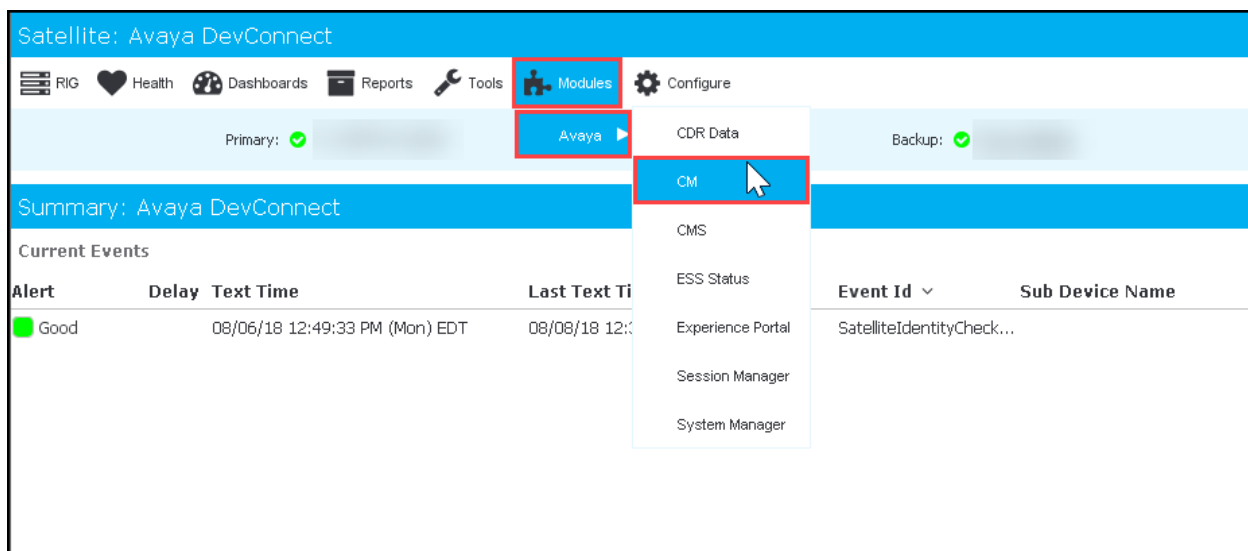
This section describes the configuration required for Nectar UCMF to interoperate with Communication Manager. It assumes that the application and all required software components have been installed and properly licensed.

Note: The installation and configuration of Nectar UCMF is carried out by Nectar personnel and the following section only details a summary of the configuration used during compliance testing

6.1. Connect Avaya CM

Follow these steps to connect the Avaya CM:

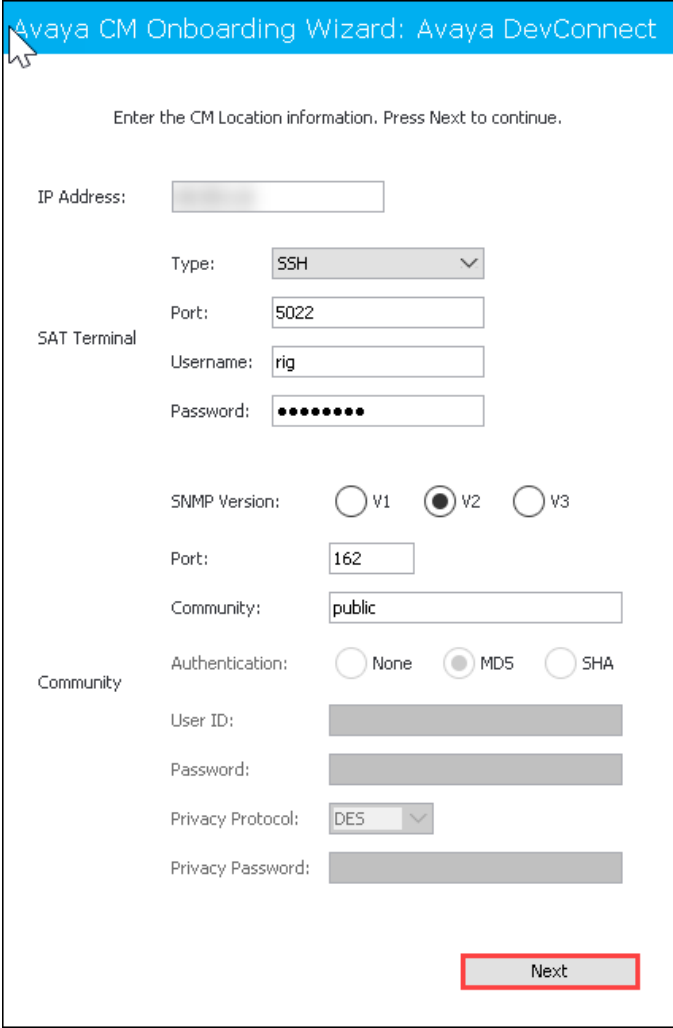
1. Navigate to **Modules** → **Avaya** → **CM**:



2. In the left pane, select **CM Connection Wizard**:



The following **Avaya CM Onboarding Wizard** dialog box appears.



The image shows a screenshot of the 'Avaya CM Onboarding Wizard: Avaya DevConnect' dialog box. The title bar is blue with white text. Below the title bar, there is a instruction: 'Enter the CM Location information. Press Next to continue.' The form is divided into several sections with labels on the left: 'IP Address:', 'SAT Terminal', and 'Community'. The 'IP Address:' section has a text input field. The 'SAT Terminal' section includes a 'Type:' dropdown menu set to 'SSH', a 'Port:' text input field with '5022', a 'Username:' text input field with 'rig', and a 'Password:' text input field with masked characters. The 'Community' section includes an 'SNMP Version:' section with radio buttons for 'V1', 'V2' (selected), and 'V3'; a 'Port:' text input field with '162'; a 'Community:' text input field with 'public'; an 'Authentication:' section with radio buttons for 'None', 'MD5' (selected), and 'SHA'; and three text input fields for 'User ID:', 'Password:', and 'Privacy Password:', each with a greyed-out background. A 'Privacy Protocol:' dropdown menu is set to 'DES'. A 'Next' button is located at the bottom right, highlighted with a red border.

Avaya CM Onboarding Wizard: Avaya DevConnect

Enter the CM Location information. Press Next to continue.

IP Address:

Type:

Port:

SAT Terminal Username:

Password:

SNMP Version: ☐ V1 ☒ V2 ☐ V3

Port:

Community:

Authentication: ☐ None ☒ MD5 ☐ SHA

User ID:

Password:

Privacy Protocol:

Privacy Password:

Next

3. Enter the following details relating to the location of the Avaya CM you are onboarding to UCMP; then click **Next**.

Parameter	Description
IP Address	Enter the IP address for the Avaya CM to be onboarded.
Type	Select connection type using the drop-down: <ul style="list-style-type: none">• SSH• Telnet
Port	Enter the port, such as 5022 or 5023 , depending on the connection type.
Username/Password	Enter the Username and Password for accessing the Avaya CM.
SNMP Version	Select the SNMP version from one of the following: <ul style="list-style-type: none">• V1• V2• V3
Port	Enter the SNMP port, such as 161 .
Community	Enter the community string previously configured.
Authentication	Select the authentication from one of the following: <ul style="list-style-type: none">• None• MD5• SHA
User ID	Enter the User ID previously set up for the SNMP read only community string.
Password	Enter the password previously set up for the SNMP read only community string.
Privacy Protocol	Select the protocol from one of the following: <ul style="list-style-type: none">• None• DES• AES• AES-192• AES-256 <i>Note: Enabled for SNMP V3 only.</i>
Privacy Password	Enter the password for the Privacy Protocol. <i>Note: Enabled for SNMP V3 only.</i>

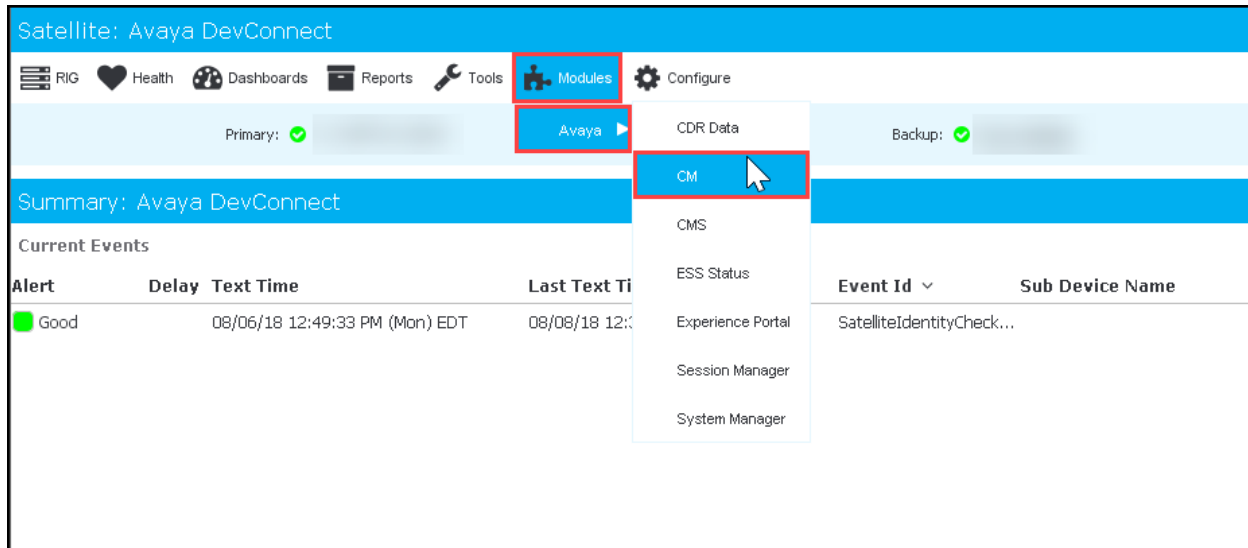
UCMP contacts the Avaya CM server to obtain version and survivable processor information.

4. Inspect the processors for inclusion; then click **Next**.

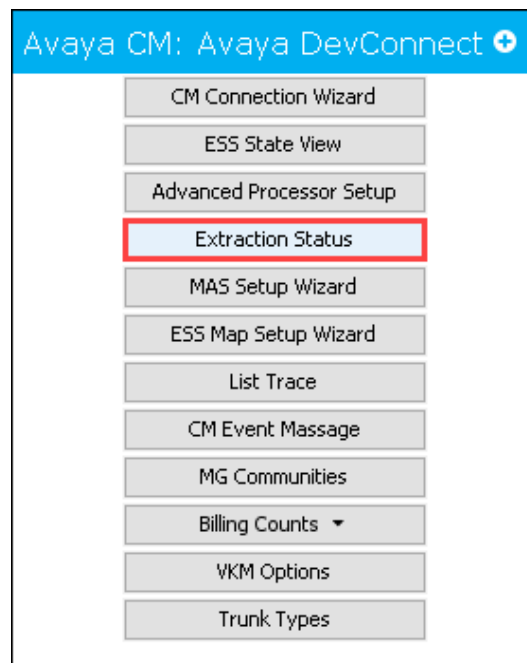
6.2. Confirm Connectivity

Follow these steps to view a list of data collection extractions for a particular Avaya CM server:

1. Navigate to **Modules** → **Avaya** → **CM**:



2. In the left pane, select **Extraction Status**:



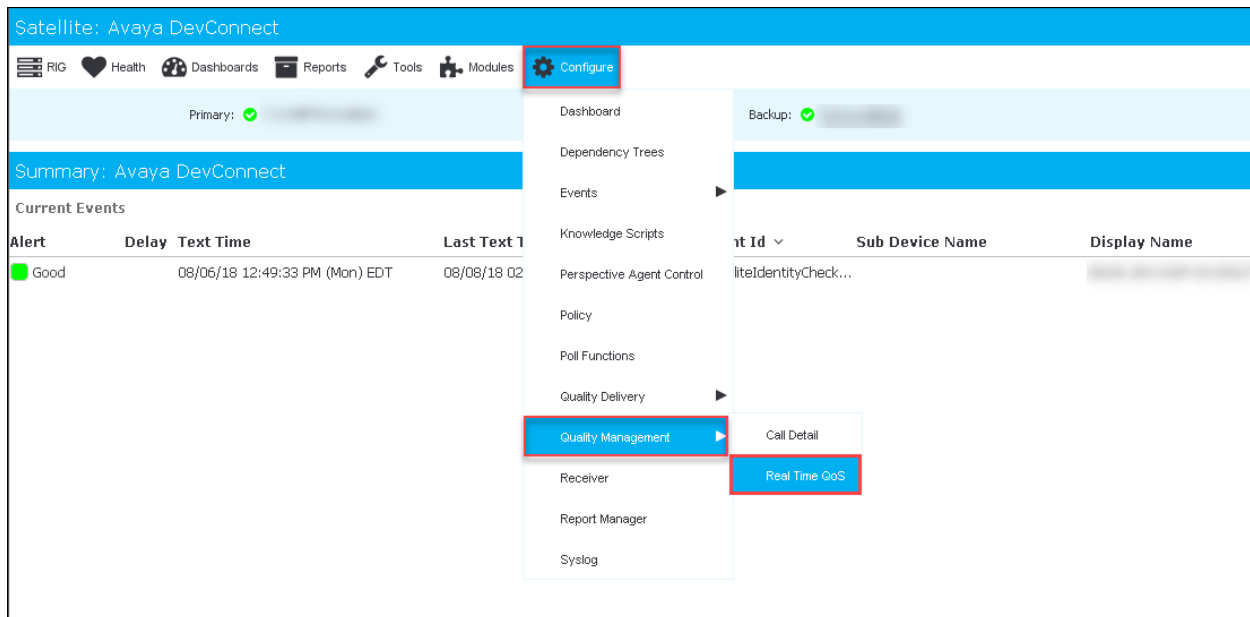
When connected (proper IP address and credentials) you will see extractions begin to populate this window:

Avaya Extraction Status Avaya DevConnect								
Process	Enable	Status	Auto	Synch St... ^	Hour To Run	Frequency	Last Time	
portCard	true	idle	true	In Synch	23		08/07/18 ...	
ipNetworkMap	true	idle	true	In Synch	23		08/07/18 ...	
mediaGateways	true	idle	true	In Synch	23		08/07/18 ...	
mediaServers	true	idle	true	In Synch	23		08/07/18 ...	
ipInterface	true	idle	true	In Synch	23		08/07/18 ...	
nodeNames	true	idle	true	In Synch	23		08/07/18 ...	
capacities	true	idle	true	In Synch	23	60	08/08/18 ...	
regions	true	idle	true	In Synch	23		08/07/18 ...	
23 rows								
Process		Status	Synch St... ^	Auto	Last Time			
CMPings		idle	synched	true	07/18/18 ...			
TrunkPollers		idle	synched	true	07/18/18 ...			
ProcessorPollers		idle	synched	true	07/18/18 ...			
ClanPollers		idle	synched	true	07/18/18 ...			
MGDSPPollers		idle	synched	true	07/18/18 ...			
ESSDependencyTree		idle	synched	true	07/18/18 ...			
ClanDependencyTrees		idle	synched	true	07/18/18 ...			
TrunkDependencyTrees		idle	synched	true	07/18/18 ...			
MedProDependencyTrees		idle	synched	true	07/18/18 ...			
ValBoardDependencyTrees		idle	synched	true	07/18/18 ...			
EventControlReset		idle	synched	true	07/18/18 ...			
ChassisBoardDependencyTrees		idle	synched	true	07/18/18 ...			
InterRegionAlignment		idle	synched	true	07/18/18 ...			
AESAlignment		idle	synched	true	07/18/18 ...			
19 rows								

6.3. Configure Real Time QoS

Follow these steps to configure Real Time QoS for your Avaya CM VKM:

1. Navigate to **Configure → Quality Management → Real Time QoS**:



The **Real Time QoS** dialog box appears where you can make a variety of configurations:

RTCP Receiver	Start
Status: <input checked="" type="checkbox"/> Enabled	Stop
Configure RTCP Categories	Configure
Status:	
Enable Traces	<input checked="" type="checkbox"/> True
Receiver Interface: 10.10.21.36 Receiver Port: 5005	Edit
Default Codec: G.711	Configure
Hop Name Lookup: <input checked="" type="checkbox"/> Enabled	Disable
Threshold Normalization: <input type="checkbox"/> Disabled	Enable

Note: You may start the receiver module after you have confirmed the settings described below.

2. Configure the **RTCP Categories**.
 - a. The Avaya collections must be completely extracted for this to work. Specifically, make sure the **ipNetworkMap** and **region** tables are complete.
3. Set **Enable Traces** to **True**.
4. Set **Receiver Interface** to the RIG IP address.
5. Leave the **Receiver Port** set to **5005**.
6. The **Default Codec** is used to calculate the Mean Opinion Score (MOS) when sessions are encrypted, and the codec is not known to Nectar. If using encryption, set this to the codec that applies to encrypted sessions.
7. Set **Hop Name Lookup** to **Enabled**. This will use DNS to show layer-3 device names in the trace routes in addition to their IP addresses.
8. When **Threshold Normalization** is disabled, each metric in the **Real-Time QoS Detail** window has an absolute Y-axis scale. (The maximum values are: MOS=5, RTD=500ms, Jitter=500ms, Loss=100%.) If enabled, each metric has a relative Y-axis scale, with the maximum observed value becoming the maximum Y-axis value. This setting is your default view. You can toggle between the absolute and relative Y-axis scales using the gear icon in the **Real-Time QoS Detail** window.
9. Start the **RTCP Receiver**.

7. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya and Nectar solution.

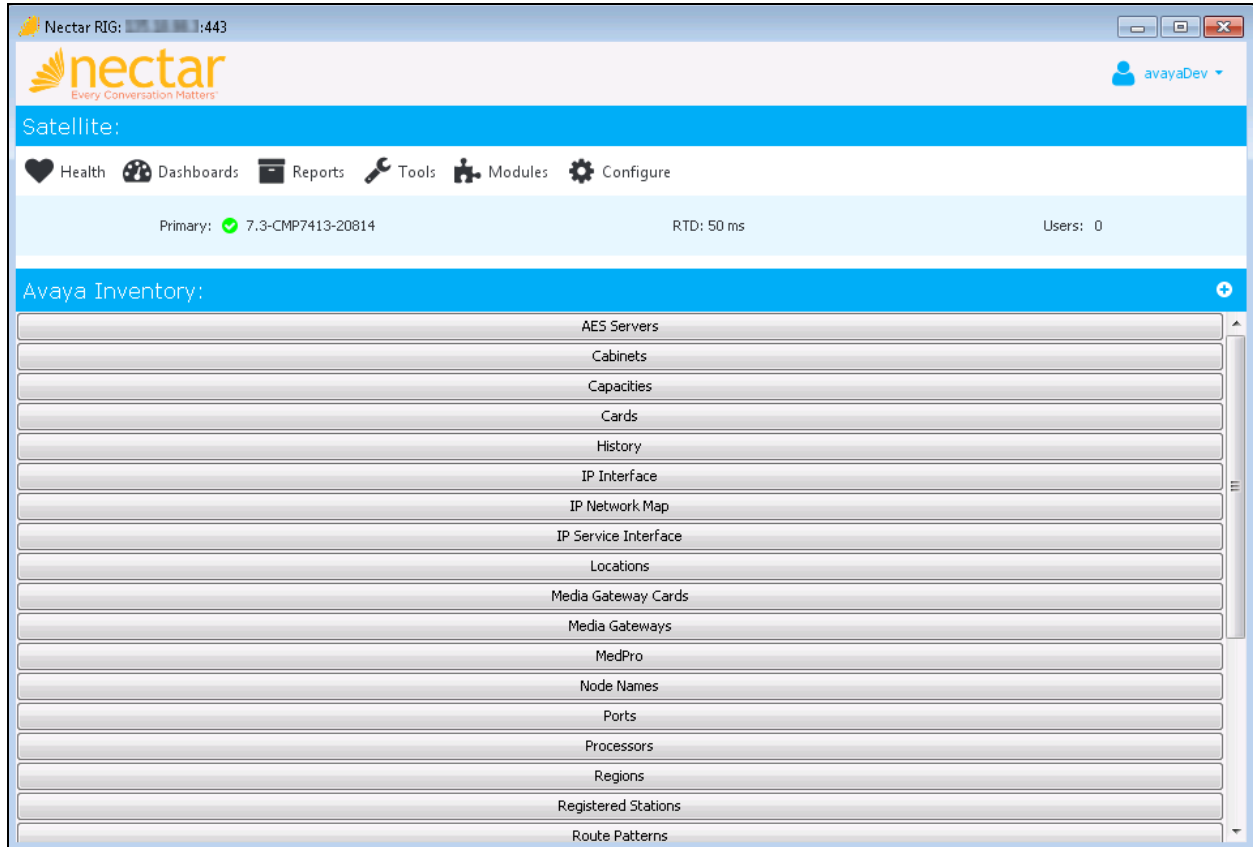
7.1. Verify Communication Manager

Verify Nectar UCMP 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
rig	20	10.10.98.3		3
rig	20	10.10.98.3		4
rig	20	10.10.98.3		5
*admin	18	10.10.98.86	stat logins	6

7.2. Verify Inventory of Communication Manager on Nectar RIG client

On the Nectar RIG client, navigate to **Reports** → **Inventory** → **Avaya** → **CM** (not shown) the Avaya Inventory window displays the inventory of Communication Manager.



7.3. Verify Event of Communication Manager on Nectar RIG client

On the Nectar RIG client, navigate to **Health** → **Summary** (not shown), the **Summary** window displays current events of Communication Manager with level of alert.

The screenshot shows the Nectar RIG client interface. At the top, the title bar reads "Nectar RIG: 7.3-CMP7413-20814". The main header features the Nectar logo and the tagline "Every Conversation Matters". Below the header, a navigation bar includes icons for Health, Dashboards, Reports, Tools, Modules, and Configure. A status bar displays "Primary: 7.3-CMP7413-20814", "RTD: 51 ms", and "Users: 0".

The "Summary" window is open, showing a table of "Current Events". The table has the following columns: Alert, Delay, Text Time, Last Text Time, Event Id, Sub Device Name, and Display Name. The events listed are as follows:

Alert	Delay	Text Time	Last Text Time	Event Id	Sub Device Name	Display Name
Minor		07/30/18 07:47:51 AM (Mon) EDT	07/30/18 07:47:51 AM (Mon) EDT	DependencyTree		CMControlChange
Good		07/27/18 03:22:36 PM (Fri) EDT	07/27/18 03:22:36 PM (Fri) EDT	DependencyTree		LocalRIGStatus
No Activity		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_11-OUTSIDE
No Activity		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_10-CS1K-H3
No Activity		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_9-H323-2-IF
Warning		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_8-PRI-2_CS:
No Activity		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_5-PRI-SIP-2
No Activity		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_3-OUTSIDE
Warning		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_7-OUTSIDE
No Activity		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_6-KP-CM_to
No Activity		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		Trunk_Group_1-Private_Ti
Critical		07/27/18 03:22:34 PM (Fri) EDT	07/27/18 03:22:34 PM (Fri) EDT	DependencyTree		CMProcessorControl

At the bottom left of the table, it indicates "20 rows".

7.4. Verify RCTP on Nectar RIG client

On the Nectar RIG client, navigate to **Health** → **Quality Management** → **Real Time QoS** (not shown), the **Real Time QoS** portion displays below the main menu. To open the **Real Time QoS** in a separate window, click on the plus sign (+) on the right side.

Nectar RIG: 443

nectar
Every Conversation Matters

avayaDev

Satellite:

Health Dashboards Reports Tools Modules Configure

Primary: 7.3-CMP7413-20814 RTD: 53 ms Users: 1

Real Time QoS: +

All Phone Perspective

Traces Search Debug Configure

Categories

Category	Alert	Total
All Calls	Good	2
General	Good	2
NR_1_Loc-1	No Activity	0

3 rows

Media Processor Search Filter

Search For: * Search

You can search by IP or Extension.

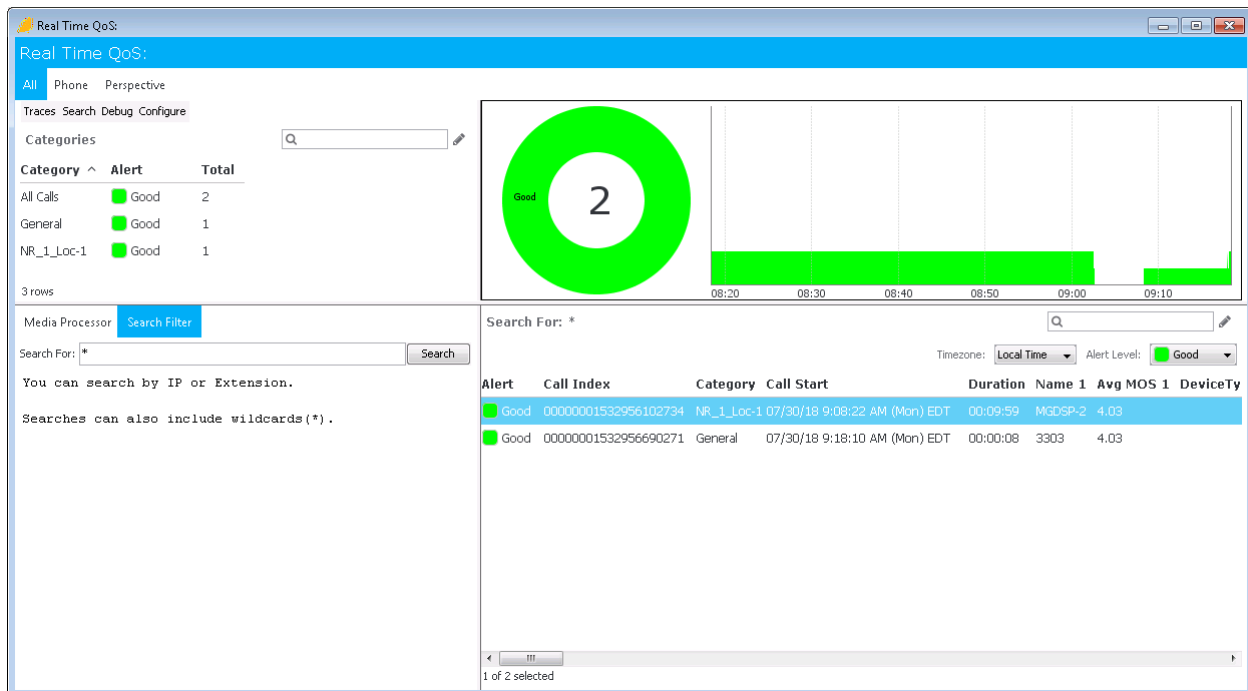
Searches can also include wildcards(*) .

Search For: * Timezone: Local Time Alert Level: Good

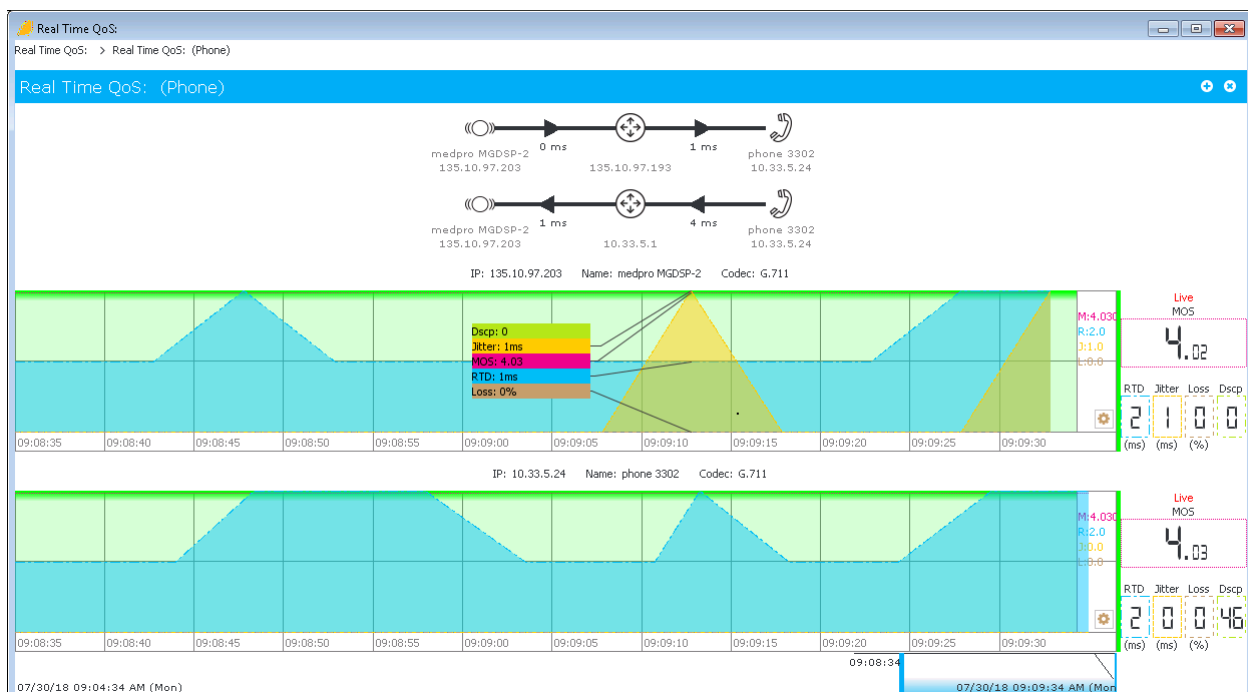
Alert	Call Index	Category	Call Start	Duration
Good	00000001532953107014	General	07/30/18 8:18:26 AM (Mon) EDT	00:33:3
Good	00000001532953098401	General	07/30/18 8:18:18 AM (Mon) EDT	00:33:4

2 rows

The Real Time QoS window is displayed with RTCP information of real time calls. Select a call to look at it in detail.



The detail of call is displayed with QoS information including trace route end-to-end, MOS, RTD (Latency), Jitter, Packet Loss and DSCP.



8. Conclusion

These Application Notes describe the steps required to configure Nectar UCMP to interoperate with Avaya Aura® Communication Manager. All test cases have passed and met the objectives outlined in **Section 2.1**.

9. Additional References

These documents form part of the Avaya official technical reference documentation suite. Further information may be had from <http://support.avaya.com> or from your Avaya representative.

- [1] *Administering Avaya Aura® Communication Manager (Release 7.1.2, Issue 5, February 2018)*
- [2] *Administering Network Connectivity on Avaya Aura® Communication Manager (Release 7.1.1, Issue 2, August 2017), 555-233-504*
- [3] *Avaya Aura® Communication Manager Feature Description and Implementation (Release 7.1.2, Issue 4, January 2018)*
- [4] *Avaya Aura® Communication Manager Screen Reference (Release 7.1.1, Issue 2, August 2017), 03-602878*
- [5] *Avaya Aura® Communication Manager SNMP Administration and Reference Guide (Release 7.1, Issue 1, May 2017), 03-602013*
- [6] *Administering Avaya Aura® Session Manager (Release 7.1.2, Issue 3, December 2017)*

Nectar documentation can be obtained directly from the Nectar website
<https://www.nectarcorp.com/solutions/nectar-for-avaya/>

©2018 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.