



Avaya Solution & Interoperability Test Lab

Application Notes for Nectar for Avaya with Avaya Aura® Communication Manager, Avaya G430/G450 Media Gateway, Avaya Aura® Media Server, Avaya Aura® Application Enablement Services, and Avaya Session Border Controller for Enterprise - Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Nectar for Avaya 2022 with Avaya Aura® Communication Manager 10.1, Avaya G430/G450 Media Gateway, Avaya Aura® Media Server, Avaya Aura® Application Enablement Services 10.1, and Avaya Session Border Controller for Enterprise 10.1. Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It automatically captures system inventory, alarms, resource utilization and status data, and real-time call quality metrics. Nectar for Avaya monitors Avaya Aura® Communication Manager, Avaya Media Gateways, Avaya Aura® Media Server, Avaya Session Border Controller for Enterprise, and VoIP calls using SNMP, RTCP, System Access Terminal (SAT) interface, and Avaya Aura® Application Enablement Services System Management Service (SMS) Web Services. Avaya Session Border Controller for Enterprise relays RTCP call quality metrics from SIP Remote Workers to Nectar for Avaya. Alarms, inventory reports, resource utilization and status, and RTCP call quality metrics are displayed on the Nectar Remote Intelligence Gateway (RIG) client.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the 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.

Table of Contents

1. Introduction.....	4
2. General Test Approach and Test Results.....	5
2.1. Interoperability Compliance Testing.....	7
2.2. Test Results	7
2.3. Support	8
3. Reference Configuration.....	9
4. Equipment and Software Validated	10
5. Configure Avaya Aura® Communication Manager	11
5.1. Launch System Management Interface	11
5.2. Configure SAT Login.....	12
5.2.1. Configure Login Group.....	12
5.2.2. Configure Login User	14
5.2.3. Configure SAT User Profile	16
5.3. Configure SNMP.....	17
5.3.1. Administer FP Traps	17
5.3.2. Restart SNMP Master Agent	19
5.4. Configure RTCP Reporting.....	20
5.4.1. Enable Unencrypted SRTCP.....	21
6. Configure Avaya Aura® Application Enablement Services	22
7. Configure Avaya G430/G450 Media Gateway.....	23
7.1. Configure SNMP Traps.....	23
7.1.1. Configure SNMPv1 or v2c Traps	23
7.1.2. Configure SNMPv3 Traps	23
7.2. Configure SNMP Polling	24
7.2.1. Configure SNMPv1 or V2c Polling.....	24
7.2.2. Configure SNMPv3 Polling.....	24
8. Configure Avaya Aura® Media Server	25
8.1. Configure SNMP.....	25
8.2. Configure RTCP.....	29
9. Configure Avaya Session Border Controller for Enterprise	30
9.1. Launch EMS Web Interface.....	30
9.2. Configure SNMP.....	31
9.3. Configure RTCP Relay Service	34

10.	Configure Avaya SIP Endpoints	37
10.1.	Configure Device Settings Groups in System Manager	37
10.2.	Configure 46xxsettings.txt File	41
11.	Configure Nectar for Avaya.....	43
11.1.	Launch the RIG Client.....	43
11.2.	Configure Communication Manager SAT Access and SNMP Polling.....	44
11.3.	Configure SBCE SNMP Polling	47
11.4.	Configure SNMP Traps	52
11.5.	Configure Real-Time Quality Monitoring.....	54
12.	Verification Steps.....	55
13.	Conclusion	64
14.	Additional References.....	64

1. Introduction

These Application Notes describe the configuration steps required to integrate Nectar for Avaya with Avaya Aura® Communication Manager, Avaya G430/G450 Media Gateway, Avaya Aura® Media Server, Avaya Aura® Application Enablement Services, and Avaya Session Border Controller for Enterprise. Nectar for Avaya is a performance monitor that provides a comprehensive view of unified communications and contact center environments. It automatically captures system inventory, alarms, resource utilization and status data, and real-time call quality metrics. Nectar for Avaya monitors Avaya Aura® Communication Manager, Avaya Media Gateways, Avaya Aura® Media Server, Avaya Session Border Controller for Enterprise, and VoIP calls using SNMP, RTCP, System Access Terminal (SAT) interface, and Avaya Aura® Application Enablement Services System Management Service (SMS) Web Services. Avaya Session Border Controller for Enterprise (SBCE) relays RTCP call quality metrics from SIP Remote Workers to Nectar for Avaya. Alarms, inventory reports, resource utilization and status, and RTCP call quality metrics are displayed on the Nectar Remote Intelligence Gateway (RIG) client.

Nectar automatically collects the following Communication Manager Inventory using a SAT login, SNMP polling, and Application Enablement Services SMS Web Service. Nectar may use both SNMP and/or SMS Web Service to retrieve all data for a particular category. SAT login is only used to collect Media Server data, because it is not available via SNMP or SMS Web Service.

ACD Agent	IP Network Region	Stations
AES CTI Links	IP Server Interfaces	System Information
Announcements	Locations	Trunk Groups
Audio Groups	Media Gateways	Trunk Member Status
Cabinets	Media Servers	VDNs
Capacities Product ID	MedPro Boards	VDN Variables
Cards	MG DSP Usage	Vectors
CTI Links	Node Names	Vector Events
Events	Registered Stations	Vector Steps
History	Route Patterns	Vector Variables
Init Causes	Route Pattern Details	
IP Interfaces	Survivable Processors	
IP Network Map	Signal Group Status	

Nectar performs SNMP polling against Avaya Media Gateway to retrieve Fan Speeds, Ambient Temperature Sensor, and MG DSP Usage. No SNMP polling is performed for Media Server.

Nectar performs SNMP polling against SBCE to retrieve data related to calls, registrations, and other data.

Nectar also serves as an SNMP trap receiver for Communication Manager, Avaya Media Gateway, Media Server, and SBCE.

The following table specifies the SNMP versions supported between Nectar and Avaya Aura® Communication Manager, media resources, and SBCE for SNMP traps and polls.

Avaya Product	Data Type	SNMP Version(s)
Avaya Aura® Communication Manager	SNMP Traps	SNMPv1, v2c, v3
	SNMP Polling	SNMPv1, v2c, v3
Avaya Media Gateway	SNMP Traps	SNMPv1, v2c, v3
	SNMP Polling	SNMPv1, v2c, v3
Avaya Aura® Media Server	SNMP Traps	SNMPv1, v2c, v3
Avaya Session Border Controller for Enterprise	SNMP Traps	SNMPv3
	SNMP Polling	SNMPv3

Nectar captures RTCP call quality metrics from Avaya H.323 Deskphones, Avaya SIP Deskphones, Avaya Workplace Client for Windows, G430/G450 Media Gateway, Media Server, and SBCE. SBCE forwards RTCP received by SIP remote workers.

Nectar data collection schedule is configurable, but on-demand data collection is also supported.

2. General Test Approach and Test Results

The interoperability compliance test included feature and serviceability testing. The feature testing focused on Nectar monitoring Communication Manager and its associated media resources using SNMP traps and polling, RTCP collection, a SAT login, and SMS Web Service to provide resource utilization, system inventory, call quality metrics, and alarm events in the RIG client.

SNMP traps were generated on Communication Manager, Media Gateway, Media Server and SBCE and sent to Nectar. Nectar displayed these SNMP traps in the Events log in the RIG client.

SNMP polling, a SAT login, and SMS Web Service were used by Nectar to capture system inventory and other platform data from Communication Manager, Media Gateways, and SBCE.

RTCP was used by Nectar to provide call quality metrics for VoIP calls. The general approach was to place calls between Avaya H.323, SIP, digital and analog phones and injecting errors using a network impairment tool to simulate network delay and packet loss conditions on the LAN. In addition, SIP remote workers sent RTCP to SBCE, which in turn relayed them to Nectar.

The serviceability testing focused on verifying that Nectar came back into service after re-connecting the Ethernet cable (i.e., restoring network connectivity) and restarting Nectar.

This solution uses the System Access Terminal (SAT) interface to interact with Avaya Aura® Communication Manager or the Telnet/SSH interface to interact with other Avaya products.

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 of these interfaces as a programmatic approach to integration of 3rd party applications. Avaya may make changes or enhancements to the interfaces in any subsequent release, feature pack, service pack, or patch that may impact the interoperability of 3rd party applications using these interfaces. Using these interfaces 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 Avaya Product 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.

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 Nectar for Avaya utilized encryption capabilities of SNMPv3.

2.1. Interoperability Compliance Testing

Interoperability compliance testing covered the following Nectar features and functionality.

- Collecting Communication Manager Inventory (i.e., managed objects, such as IP Network Regions, Stations, and Trunks) using SNMP polling, a SAT login session, and Application Enablement Services SMS Web Service and displaying the data in the RIG client.
- Verifying inventory updates on the RIG client after making configuration changes on Communication Manager.
- Verifying resource utilization (e.g., MG DSP Usage) captured from Media Gateway via SNMP polling.
- Collecting call and registration information from SBCE via SNMP polling.
- Capturing SNMP traps and providing events for alarm conditions on Communication Manager, G430/450 Media Gateways, Media Server, and SBCE.
- Tracking the registration status of Avaya H.323 Deskphones.
- Capturing RTCP from Avaya H.323 Deskphones, Avaya SIP Deskphones Avaya Workplace, Media Gateway, and Media Server and displaying call quality metrics on the RIG client.
- Capturing RTCP data from SIP remote Workers registered to Session Manager through SBCE. In this case, SIP remote worker sends RTCP to SBCE and then relays them to Nectar.
- Verifying proper system recovery after a restart of Nectar and loss of IP network connectivity.

2.2. Test Results

The compliance test passed with the following observations:

- If SRTP is used for SIP calls, unencrypted SRTCP must be used so that G430/G450 Media Gateway sends RTCP to Nectar.
- In the **Real-Time QoS** window of the RIG client, there is no call path information for Avaya SIP Deskphones or Media Server, because they don't provide call path (or call trace) information to Nectar. In addition, for J100 Series SIP Deskphones, the IP address and name may be blank in the Real-Time QoS detail window on the RIG. However, the SIP endpoint information is correctly displayed in the Real-Time call summary window.
- Nectar may log SNMP traps from Communication Manager against the wrong agent, and therefore, SNMP traps may not be reflected in the Dependency Tree. This is caused by an IP address being assigned to agents automatically added in the background by Nectar, which cannot be removed by a user. Nectar is investigating this issue.
- If there are no Audio Groups or IP Network Map configured, the data collection status for those data items will indicate as *Failed* in the Collections window on the RIG. If data exists, the data collection status will be *Success*, if the data was retrieved successfully.

- If Audio Groups or IP Network Map configuration is removed, Nectar continues to display the last retrieved data.

2.3. Support

For technical support and information on Nectar for Avaya, contact Nectar Support at:

- Phone: +1 (888) 811-8647 (US)
+1 (631) 270-1077 (outside the US)
- Website: <https://support.nectarcorp.com>
- Email: support@nectarcorp.com

3. Reference Configuration

Figure 1 illustrates a sample configuration consisting of Nectar for Avaya with an Avaya SIP-based network. Nectar for Avaya was used to:

- Retrieve Communication Manager Inventory using SNMP polling, a SAT interface, and Application Enablement Services SMS Web Service.
- Monitor Communication Manager, G430/G450 Media Gateways, and Media Server using SNMP (no SNMP polling for Media Server).
- Capture RTCP call quality metrics from Avaya H.323 and SIP endpoints, media resources, and SBCE.
- Display alarms, inventory reports, and call quality metrics on the RIG client.

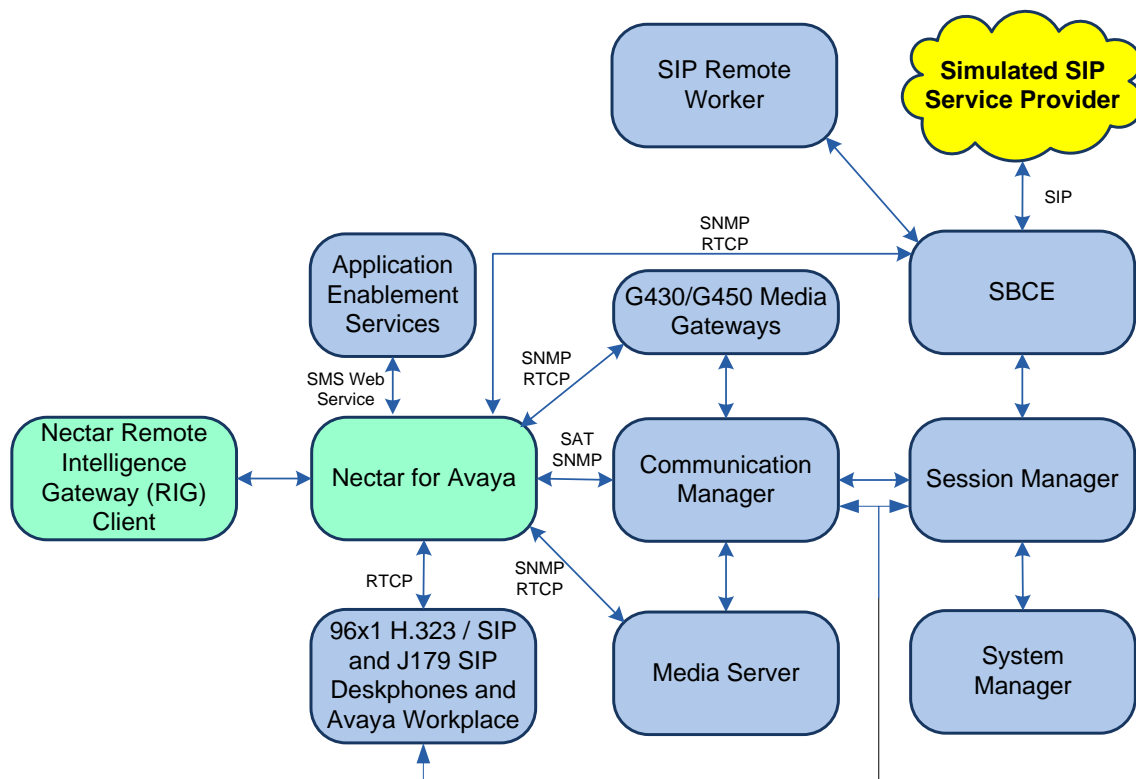


Figure 1: Nectar for Avaya with Avaya SIP-based Network

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	10.1.0.1.0-SP1
Avaya G430 Media Gateway	FW 42.4.0 Vintage 1
Avaya G450 Media Gateway	FW 42.7.0 Vintage 3
Avaya Aura® Media Server	10.1.0.77
Avaya Aura® System Manager	10.1.0.1 Build No. – 10.1.0.0.537353 Software Update Revision No: 10.1.0.1.0614394 Service Pack 1
Avaya Aura® Session Manager	10.1.0.1.1010105
Avaya Aura® Application Enablement Services	10.1.0.0.0.11-0
Avaya Session Border Controller for Enterprise	10.1.1.0-35-21872
Avaya 96x1 Series IP Deskphones	6.8.5.3.2 (H.323) 7.1.13.0.4 (SIP)
Avaya J179 SIP Deskphone	4.0.13.0.6
Avaya Workspace Client for Windows	3.24.0.84
Avaya 9404 Digital Phone	12.0
Avaya Analog Phone	N/A
Nectar for Avaya	2022.1-21422
Nectar Remote Intelligence Gateway (RIG) Client	2022.1-20314

5. Configure Avaya Aura® Communication Manager

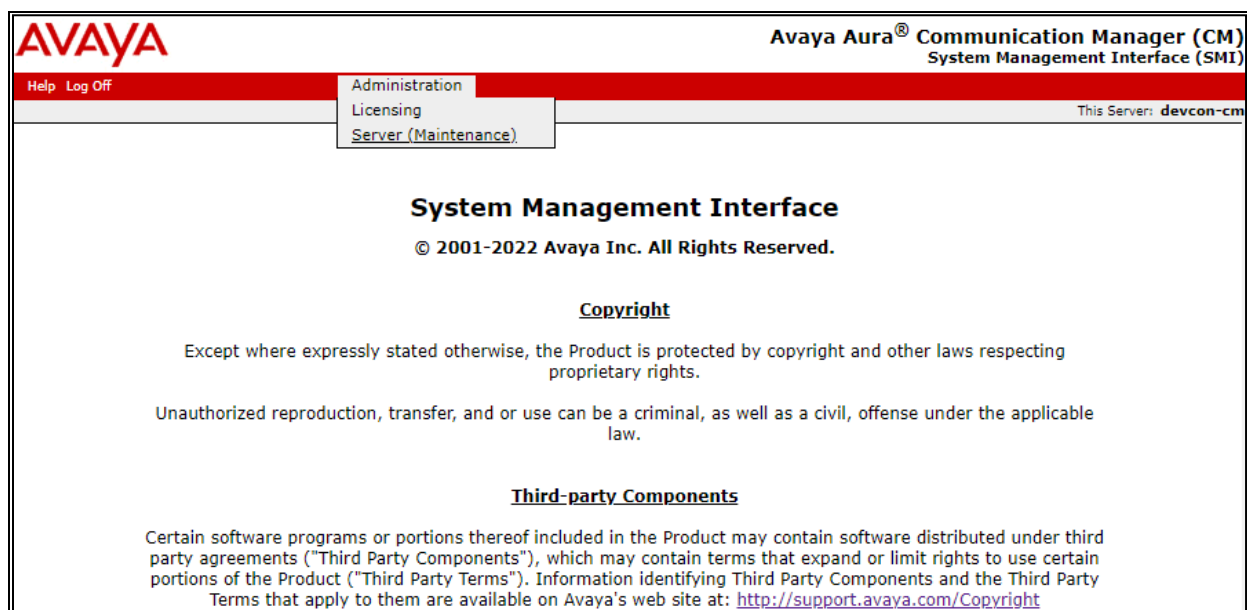
This section provides the procedure for configuring SNMP, RTCP Reporting, and SAT access. The procedures include the following areas:

- Launch System Management Interface
- Configure SAT Login
- Configure SNMP
- Configure RTCP Reporting

5.1. Launch System Management Interface

Access the Communication Manager System Manager Interface by using the URL **Error! Hyperlink reference not valid.** in an Internet browser, where *<ip-address>* is the Communication Manager IP address. Log in using the appropriate credentials.

In the subsequent webpage, select **Administration → Server (Maintenance)** from the top menu as shown below. The **Server Administration** webpage is displayed as shown in the following section.



5.2. Configure SAT Login

This section covers the configuration of a SAT user account for Nectar and its associated permissions. The SAT interface is used by Nectar to retrieve Media Server data from Communication Manager.

5.2.1. Configure Login Group

Create an Access-Profile Group. Navigate to **Security → Administrator Accounts**. In the **Administrator Accounts** webpage, select **Add Group**, and then click **Submit**.

The screenshot shows the Avaya Aura Communication Manager (CM) System Management Interface (SMI) Administrator Accounts page. The page has a red header with the Avaya logo and the title "Avaya Aura® Communication Manager (CM) System Management Interface (SMI)". Below the header is a navigation bar with "Help" and "Log Off" links, and a "Administration" tab. The main content area is titled "Administrator Accounts" and contains a description: "The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups." Below this is a "Select Action:" section with radio buttons for "Add Login", "Privileged Administrator", "Unprivileged Administrator", "SAT Access Only", "Web Access Only", "CDR Access Only", "Business Partner Login (dadmin)", "Business Partner Craft Login", and "Custom Login". There are also buttons for "Change Login", "Remove Login", "Lock/Unlock Login", "Add Group", and "Remove Group", each with a dropdown menu. At the bottom are "Submit" and "Help" buttons. A left sidebar contains a tree view of the system management interface, with "Administrator Accounts" selected under the "Security" category.

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

Help Log Off Administration This Server: devcon-cm

Administration / Server (Maintenance)

Server Date/Time
Software Version
Server Configuration
Server Role
Network Configuration
Static Routes
Display Configuration
Time Zone Configuration
NTP Configuration
Server Upgrades
Manage Updates
IPSI Firmware Upgrades
IPSI Version
Download IPSI Firmware
Download Status
Activate IPSI Upgrade
Activation Status
Data Backup/Restore
Backup Now
Backup History
Schedule Backup
Backup Logs
View/Restore Data
Restore History
Security
Administrator Accounts
Login Account Policy
Login Reports
Server Access
Server Log Files
Firewall
Trusted Certificates
Server/Application Certificates
Certificate Alarms
Certificate Signing Request
SSH Keys
Web Access Mask
Renew Certificates
Miscellaneous
File Synchronization
Download Files
CM Phone Message File

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

☐ Remove Login

☐ Lock/Unlock Login

☒ Add Group

☐ Remove Group

In the **Administrator Accounts – Add Group** webpage, select *prof20* from the drop-down list of the **Add a new access-profile** group field. Click **Submit**.

Administrator Accounts -- Add Group

This page allows you to add a new access-profile or non-access-profile Linux group. An access-profile group is used to control permissions within applications, such as the SAT and the web interface (Web Access Mask).

Select Action:

☒ Add a new access-profile group: prof20 ▼

☐ Add a new non-access-profile group:

Group Name:

Group Number: (1000 to 60000)

Submit **Cancel** **Help**

5.2.2. Configure Login User

Create a login account for Nectar to access the Communication Manager SAT. Navigate to **Security → Administrator Accounts** and select *SAT Access Only*. Click **Submit**.

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 contains a tree view with categories like 'Server Configuration', 'Server Upgrades', 'Data Backup/Restore', 'Security', and 'Miscellaneous'. The 'Security' category is expanded, showing 'Administrator Accounts' as the selected option. The main content area is titled 'Administrator Accounts' and includes a description: 'The Administrator Accounts SMI pages allow you to add, delete, or change administrator logins and Linux groups.' Below this, a 'Select Action:' section contains several radio button options: 'Add Login' (selected), 'Privileged Administrator', 'Unprivileged Administrator', 'SAT Access Only', 'Web Access Only', 'CDR Access Only', 'Business Partner Login (dadmin)', 'Business Partner Craft Login', and 'Custom Login'. There are also three radio button options for 'Change Login', 'Remove Login', and 'Lock/Unlock Login', each followed by a 'Select Login' dropdown menu. Additionally, there are radio button options for 'Add Group' and 'Remove Group', each followed by a 'Select Group' dropdown menu. At the bottom of the form are 'Submit' and 'Help' buttons.

In the **Administrator Accounts – Add Login: SAT Access Only** webpage, provide the **Login name** (e.g., *rig*), password, and accept all other default values. Click **Submit**.

AVAYA

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

[Help](#) [Log Off](#) **Administration**

Administration / Server (Maintenance) This Server: devcon-cm

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Manage Updates

IPSI Firmware Upgrades

IPSI Version

Download IPSI Firmware

Download Status

Activate IPSI Upgrade

Activation Status

Data Backup/Restore

Backup Now

Backup History

Schedule Backup

Backup Logs

View/Restore Data

Restore History

Security

Administrator Accounts

Login Account Policy

Login Reports

Server Access

Server Log Files

Firewall

Trusted Certificates

Server/Application Certificates

Certificate Alarms

Certificate Signing Request

SSH Keys

Web Access Mask

Renew Certificates

Miscellaneous

File Synchronization

Download Files

CM Phone Message File

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

nectar

Primary group

☒ susers
☐ users

Additional groups (profile)

prof20

Linux shell

/opt/ecs/bin/autosat

Home directory

/var/home/nectar

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


☒ Yes
☐ No

Submit

Cancel

Help

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

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

JAO; Reviewed:
SPOC 10/6/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

15 of 65
Nectar-Aura10

5.2.3. 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. Since Nectar doesn't modify any system configuration, create a SAT User Profile with limited permissions.

Use the **add user-profile-by-category 20** command, where **20** was the user profile configured in **Section 5.2.2**. Enter a descriptive name for **User Profile Name** (e.g., *Nectar Admin*) and enable the categories shown below. For the compliance test, user profile 20 was created.

add user-profile-by-category 20 Page 1 of 39

USER PROFILE 20

User Profile Name: Nectar Admin

This Profile is Disabled? n Shell Access? y

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	n
Maintenance	G	y	Trunking	P	y
Measurements and Performance	H	y	Usage	Q	y
Remote Access	I	n	User Access	R	n

On Page 2, **Set Permissions For Category** according to the table below.

Category	Permission
A	r-
B	r-
C	rm
D	r-
E	r-
F	rm
G	rm
H	r-
J	r-
history K	r-
L	rm
M	rm
N	r-
P	rm
Q	r-

5.3. Configure SNMP

This section covers the configuration of SNMP on Communication Manager. The steps required include:

- Administer FP Traps
- Administer SNMP Access
- Restart SNMP Master Agent
- Configure RTCP Reporting

5.3.1. Administer FP Traps

To configure Communication Manager to send SNMP traps to Nectar, navigate to **SNMP → FP Traps**. The **FP Traps** webpage is displayed as shown below. In the sample configuration below, SNMP traps using SNMPv1, v2c, and v3 are configured simultaneously for informational purposes. Note that only *one* SNMP version needs to be configured.


For SNMPv1 or v2c, configure the following fields:

IP Address:	Set to the Nectar IP address (e.g., <i>10.64.102.113</i>).
Port:	Use the default port 162 for SNMP traps.
Notification:	Set to <i>trap</i> .
Community Name:	Set to appropriate community string (e.g., <i>public</i>).

For SNMPv3, configure the following fields:

IP Address:	Set to the Nectar IP address (e.g., <i>10.64.102.113</i>).
User Name:	Specify a user name (e.g., <i>nectar</i>).
Authentication Protocol:	Set to <i>SHA</i> .
Authentication Password:	Set to a valid password to be used by Nectar.
Privacy Protocol:	Set to <i>AES128</i> .
Privacy Password:	Set to a valid password to be used by Nectar.

Once completed, press the **Submit** button.



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

Help Log Off
Administration

Administration / Server (Maintenance)
This Server: **devcon-cm**

Alarms

Current Alarms

SNMP

Agent Status

Access

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Server Date/Time

Software Version

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Manage Updates

FP Traps

The FP Traps page allows specification of the alarms to be sent as traps.

Add Trap Destination

SNMP Version 1
IP address:
Notification:
Community Name:

Port:

SNMP Version 2c
IP address:
Notification:
Community Name:

Port:

SNMP Version 3
IP address:
Notification:
User Name:
Authentication Protocol:
Authentication Password:
Privacy Protocol:
Privacy Password:
Engine ID:

Port:

Minimum 8 characters. (for authentication and privacy)
Minimum 8 characters. (for privacy)

5.3.2. Administer SNMP Access

To configure Communication Manager to respond to SNMP polling, navigate to **SNMP → Access**. The **Access** webpage is displayed as shown below. In the sample configuration below, SNMP polling using SNMPv1, v2c, and v3 are configured simultaneously for informational purposes. Note that only *one* SNMP version needs to be configured.

For SNMPv1 or v2c, configure the following fields:

IP Address: Set to the Nectar IP address (e.g., *10.64.102.113*).
Access: Set to *read-only*.
Community Name: Set to appropriate community string (e.g., *public*).

For SNMPv3, configure the following fields:

IP Address: Set to the Nectar IP address (e.g., *10.64.102.113*).
User Name: Specify a user name (e.g., *nectar*).
Authentication Protocol: Set to *SHA*.
Authentication Password: Set to a valid password to be used by Nectar.
Privacy Protocol: Set to *AES128*.
Privacy Password: Set to a valid password to be used by Nectar.

Once completed, press the **Submit** button.

JAO; Reviewed:
SPOC 10/6/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

18 of 65
Nectar-Aura10

AVAYA

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

Help Log Off

Administration

Administration / Server (Maintenance)

This Server: devcon-cm

Alarms

Current Alarms

SNMP

Agent Status

Access

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Server Configuration

Server Role

Network Configuration

Static Routes

Display Configuration

Time Zone Configuration

NTP Configuration

Server Upgrades

Access

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

Add SNMP Users / Communities

SNMP Version 1

IP address: 10.64.102.113

Access: read-only

Community Name: public

SNMP Version 2c

IP address: 10.64.102.113

Access: read-only

Community Name: public

SNMP Version 3

Access: read-only

User Name: nectar

Authentication Protocol: SHA

Authentication Password: nectar123

Privacy Protocol: AES128

Privacy Password: nectar123

Submit Cancel Help

5.3.3. Restart SNMP Master Agent

Select **SNMP → Agent Status** from the left pane to display the **Agent Status** webpage and restart the SNMP agent. Click the **Stop Master Agent** button followed by the **Start Master Agent** button.

AVAYA

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

Help Log Off

Administration

Administration / Server (Maintenance)

This Server: devcon-cm

Alarms

Current Alarms

SNMP

Agent Status

Access

Incoming Traps

FP Traps

FP Trap Test

FP Filters

Diagnostics

Restarts

System Logs

Ping

Traceroute

Netstat

Server

Status Summary

Process Status

Shutdown Server

Agent Status

The Agent Status SMI page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent.

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

Stop Master Agent Help

5.4. Configure RTCP Reporting

Nectar can monitor the quality of IP calls using RTCP reporting. Communication Manager should be configured to provide RTCP settings to Avaya H.323 Deskphones and G430/G450 Media Gateway. The RTCP settings specify where to send the RTCP data and the frequency. This configuration is performed through the SAT interface. Use the **change system-parameters ip-options** command to set the following RTCP Monitor Server parameters:

Server IPV4 Address: Enter the Nectar IP address (e.g., *10.64.102.113*).
IPV4 Server Port: Set to *5005*.
RTCP Report Period (secs): Set to *5*.

```
change system-parameters ip-options                               Page 1 of 5
                        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: 10.64.102.113   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
```

Use the **change-ip-network-region** command to enable RTCP reporting for H.323 deskphones and G430/G450 Media Gateways. For the compliance test, IP network region 1 was used. Set the **RTCP Reporting to Monitor Server Enabled** field to *y*. To use the RTCP parameters configured system-wide in the System-Parameters IP-Options above, set **Use Default Server Parameters** to *y* or set this field to *n* to set different RTCP parameters on a network region basis.

```
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
```

5.4.1. Enable Unencrypted SRTCP

For SIP calls using SRTP and G430/G450 Media Gateway for media resources, ensure that unencrypted SRTCP is enforced. If encrypted SRTCP is used, Media Gateway won't send RTCP to Nectar. Note that Avaya H.323 Deskphones do not support encrypted SRTCP.

Enforcing unencrypted SRTCP can be done in the following ways: enforce unencrypted SRTCP in the IP codec set or disable ENCRYPT_SRTCP in the 46xxsettings file as shown below.

In the IP codec set below, **Encrypted SRTCP** is set to *enforce-unenc-srtcp*. The default of *best-effort* may be used if unencrypted SRTCP is enforced in the 46xxsettings file for Avaya SIP Deskphones.

```
change ip-codec-set 1                                     Page 1 of 2

                                IP MEDIA PARAMETERS

Codec Set: 1

Audio      Silence      Frames      Packet
Codec      Suppression   Per Pkt    Size (ms)
1: G.711MU          n           2          20
2:
3:
4:
5:
6:
7:

Media Encryption                                Encrypted SRTCP: enforce-unenc-srtcp
1: 1-srtp-aescm128-hmac80
2: 2-srtp-aescm128-hmac32
3: none
4:
5:
```

If the IP codec set above allows *best-effort* for **Encrypted SRTCP**, then unencrypted SRTCP may be enforced in the 46xxsettings file by setting **ENCRYPT_SRTCP** to 0 as shown below. Unencrypted SRTCP is the default.

```
## ENCRYPT_SRTCP specifies whether RTCP packets are encrypted or not. SRTCP is only
## used if SRTP is enabled using
## MEDIAENCRYPTION (values other than 9 (none) are configured).
## This parameter controls RTCP encryption for RTCP packets exchanged between peers.
## RTCP packets sent to Voice Monitoring Tools are always sent unencrypted.
## Value Operation
## 0 SRTCP is disabled (default).
## 1 SRTCP is enabled.
## This parameter is supported by:
## J129 SIP R1.0.0.0 (or R1.1.0.0), J169/J179 SIP R1.5.0, J100 SIP R2.0.0.0 and
## later, J139 SIP R3.0.0.0 and later, J159 SIP R4.0.3.0 and later, J189 SIP R4.0.6.1 and
## later
## Avaya IX Workplace 3.1.2 and later
## 96x1 SIP R7.1.0.0 and later
## Avaya Vantage Connect Application SIP R1.0.0.0 and later
SET ENCRYPT_SRTCP 0
```

6. Configure Avaya Aura® Application Enablement Services

This section covers the configuration of SMS Properties, which is used by the SMS web service to access managed objects on Communication Manager. Nectar only requests read-only access to managed objects via the SMS web service and will provide the Communication Manager login credentials to Application Enablement Services configured in **Section 5.2**.

Access the OAM web-based interface by using the URL “https://<ip-address>” in an Internet browser window, where <ip-address> is the IP address of Application Enablement Services. Log in using the appropriate credentials (not shown).

Navigate to **AE Services → SMS → SMS Properties**. In **SMS Properties**, configure the following fields:

- **Default CM Host Address:** Set to the CM IP address (e.g., *10.64.102.115*).
- **Max Session per CM:** Default is 1 (can be set to 1-5).
- **SAT Login Keepalive:** Set to *360*.
- **CM Terminal Type:** Set to *OSSIE*.

Use default values for the other fields.

The screenshot displays the Avaya Application Enablement Services Management Console. At the top right, a welcome message for user 'cust' is shown, including login details and system status. The main navigation bar includes 'AE Services | SMS | SMS Properties' and links for 'Home | Help | Logout'. The left sidebar lists various services, with 'SMS Properties' selected under the 'SMS' category. The main content area, titled 'SMS Properties', contains several configuration fields: 'Default CM Host Address' (10.64.102.115), 'Default CM Admin Port' (5022), 'CM Connection Protocol' (SSH), 'SMS Logging' (NORMAL), 'SMS Log Destination' (apache), 'CM Proxy Trace Logging' (NORMAL), 'Max Sessions per CM' (5), 'Proxy Shutdown Timer' (1800 seconds), 'SAT Login Keepalive' (360 seconds), 'CM Terminal Type' (OSSIE), and 'Proxy Log Destination' (/var/log/avaya/aes/ossicm.log). At the bottom of the configuration area are three buttons: 'Apply Changes', 'Restore Defaults', and 'Cancel'.

7. Configure Avaya G430/G450 Media Gateway

This section covers the G430/G450 Media Gateway configuration to send SNMP traps to Nectar and allow Nectar SNMP polling.

Note: Pre-defined SNMP Groups and Views mentioned in this section already exist by default in G430/G450 Media Gateways with newer firmware. Use the **show snmp group** or **show snmp view** commands to view them. Use the **show snmp userToGroup** command to view the group mapped to a user.

7.1. Configure SNMP Traps

This section covers the configuration of the G450 Media Gateway to enable SNMP traps. Log into the Media Gateway command line interface with the appropriate credentials using SSH (not shown).

7.1.1. Configure SNMPv1 or v2c Traps

At the command prompt, enter one of the commands shown below. In the **snmp-server host** command specify the Nectar IP address, specify *v1* or *v2c* in the command depending on the SNMP version desired, and *public* as the community name. The **show snmp** command may be used to view the SNMP configuration.

```
snmp-server host 10.64.102.113 traps v1 public
-or-
snmp-server host 10.64.102.113 traps v2c public
```

7.1.2. Configure SNMPv3 Traps

To configure SNMPv3 traps, create a new SNMP Group in the Media Gateway using the command below. This new SNMP Group assigns the pre-defined *iso* SNMP View as the group's Read View and Notify View.

```
snmp-server group v3ReadViewG v3 priv read iso notify iso
```

Next, configure a SNMP User for Nectar using the command below. This new SNMP user assigns the SNMP Group created above. After the command is entered, the user will be prompted for passwords.

```
snmp-server user nectar v3ReadViewG v3 auth sha priv aes128
```

Finally, enable SNMPv3 traps with the command below, which specifies the Nectar IP address, SNMP version and the SNMP User (i.e., *nectar*) created above.

```
snmp-server host 10.64.102.113 traps v3 priv nectar
```

7.2. Configure SNMP Polling

This section covers the configuration on the Media Gateway to allow SNMP Polls. Log into the Media Gateway command line interface with the appropriate credentials using SSH (not shown).

7.2.1. Configure SNMPv1 or V2c Polling

To allow SNMPv1 or v2c polling, use the following command to set the community strings.

```
snmp-server community read-only public read-write private
```

7.2.2. Configure SNMPv3 Polling

To allow SNMPv3 polling, use the following command to create a SNMP user, *nectar123*, assigned to the pre-defined *v3ReadOnlyG* SNMPv3 group. After the command is entered, the user will be prompted for passwords.

```
snmp-server user nectar123 v3ReadOnlyG v3 auth sha priv aes128
```


8. Configure Avaya Aura® Media Server

This section covers the configuration to allow SNMP traps and RTCP to be sent to Nectar. Access the Media Server web management interface by using a web browser and entering the URL **Error! Hyperlink reference not valid.**, where *<ip-address>* is the Media Server IP address. Log in using the appropriate credentials.

8.1. Configure SNMP

This section covers SNMP trap configuration. Navigate to **System Configuration → Network Settings → SNMP → Users** to add a SNMP user. The Users webpage is displayed below. Click **Add**.

The screenshot shows the 'SNMP Users' configuration page in the Avaya Aura® Media Server web interface. The left sidebar contains a navigation menu with options like System Status, Applications, Cluster Configuration, System Configuration, Server Profile, Network Settings, General Settings, IP Interface Assignment, Name Resolution, SNMP, Users, Agent Settings, Destinations, Advanced Settings, and Signaling Protocols. The main content area displays a table of existing SNMP users. At the top of the table are buttons for 'Add...', 'Edit...', and 'Delete...'. The table has columns for 'Security Name', 'Security Model', 'Authentication Mode', 'Privacy Mode', and 'Access'. One user named 'nectar' is listed with Security Model 'v3', Authentication Mode 'SHA', Privacy Mode 'AES128', and Access 'Read-only'.

<input type="checkbox"/>	Security Name ▲	Security Model	Authentication Mode	Privacy Mode	Access
<input type="checkbox"/>	nectar	v3	SHA	AES128	Read-only
<input type="checkbox"/>					
<input type="checkbox"/>					

In the **Add User** webpage, configure a SNMPv1/v2c or SNMPv3 user. Below is a SNMPv1/v2c user.

The screenshot shows the 'Add SNMP User' configuration page in the Avaya Aura® Media Server web interface. The left sidebar is the same as in the previous screenshot. The main content area contains a form for adding a new SNMP user. The form fields are: 'Security name' (text input with value 'nectar' and a note '(Allowed characters: a-zA-Z0-9_-)'), 'Description' (text input with value 'Nectar for Avaya'), 'Version' (dropdown menu with value 'v1/v2c'), and 'Access rights' (dropdown menu with value 'read-only'). At the bottom of the form are 'Save' and 'Cancel' buttons.

Security name: (Allowed characters: a-zA-Z0-9_-)
Description:
Version:
Access rights:

The webpage below shows the configuration of a SNMPv3 user.

The screenshot shows the Avaya Aura Media Server web interface. The top header includes the Avaya logo, the product name "Avaya Aura® Media Server", and links for "Help", "Sign Out", and the user "admin". Below the header, a breadcrumb trail indicates the current path: "Home > System Configuration > Network Settings > SNMP > Users > Add User". The main content area is titled "Add SNMP User" and contains a form with the following fields:

- Security name: (Allowed characters: a-zA-Z0-9_-)
- Description:
- Version:
- Access rights:
- Authentication Mode:
- Authentication Password: (8 - 128 characters)
- Confirm Authentication Password: (8 - 128 characters)
- Privacy Mode:
- Privacy Password: (8 - 128 characters)
- Confirm Privacy Password: (8 - 128 characters)

At the bottom right of the form are "Save" and "Cancel" buttons. On the left side of the interface is a navigation menu with the following items:

- + System Status
- + Applications
- + Cluster Configuration
- System Configuration
 - + Server Profile
 - Network Settings
 - General Settings
 - IP Interface Assignment
 - Name Resolution
 - SNMP
 - Users
 - Agent Settings
 - Destinations
 - + Advanced Settings
- + Signaling Protocols
- + Media Processing
- + Application Interpreters
- + Monitoring Settings
- + Session Detail Records
- + Content Store
- Logging Settings

To allow Media Server to send SNMP traps to Nectar, navigate to **System Configuration → Network Settings → SNMP → Destinations**. The **Traps Destinations** webpage is displayed as shown below.

AVAYA

Avaya Aura® Media Server
[Help](#) | [Sign Out](#) **admin**

+ System Status
+ Applications
+ Cluster Configuration
- System Configuration
 + Server Profile
 - Network Settings
 - General Settings
 - IP Interface Assignment
 - Name Resolution
 - **SNMP**
 - Users
 - Agent Settings
 - Destinations
 + Advanced Settings
+ Signaling Protocols
+ Media Processing
+ Application Interpreters
+ Monitoring Settings
+ Session Detail Records
+ Content Store
- Logging Settings
+ Debug Tracing
- Engineering Parameters
- Element Manager Settings
- Licensing
 - General Settings
 - Monitoring
 - Utilization Threshold
+ Tools
+ Security
+ Account Management

Managing: devcon-ams.avaya.com, 10.64.102.118
[Home](#) » [System Configuration](#) » [Network Settings](#) » [SNMP](#) » Destinations

Trap Destinations

This task allows administrators to configure SNMP trap configuration, destinations, and routes.

[General Settings](#) | [Trap Destinations](#) | [Trap Routes](#)

General Settings

SNMP Alarm Delivery Traps ☒

SNMP Event Log Delivery Traps ☐

Trap Destinations

Add... Edit... Delete

<input type="checkbox"/>	Destination Address ▲	Destination Port

Trap Routes

Add... Edit... More Actions ▼

<input type="checkbox"/>	Destination Address ▲	Destination Port	Security Name

Save Cancel Restore Defaults

Copyright © 2006-2022 Avaya Inc.

In **Add Trap Destination**, provide the Nectar IP address for the **Destination address** and set the **Destination port** to *162*. Click **Save**.

The screenshot shows the Avaya Aura Media Server web interface. The top header includes the AVAYA logo, the title 'Avaya Aura® Media Server', and links for 'Help', 'Sign Out', and 'admin'. Below the header, a breadcrumb trail reads: 'Home > System Configuration > Network Settings > SNMP > Destinations > Add Trap Destination'. The left sidebar contains a tree view with categories like System Status, Applications, Cluster Configuration, System Configuration, Server Profile, Network Settings, and SNMP. The main content area is titled 'Add Trap Destination' and contains two input fields: 'Destination address' with the value '10.64.102.113' and 'Destination port' with the value '162'. At the bottom right of the form are 'Save' and 'Cancel' buttons.

In the **Traps Routes** section of the **Traps Destination** webpage, click **Add**. The following webpage shows the **Route Destination** configuration for SNMPv1/v2c traps.

The screenshot shows the Avaya Aura Media Server web interface for the 'Add Trap Route Destination' page. The top header and breadcrumb trail are identical to the previous screenshot. The left sidebar is also the same. The main content area is titled 'Add Trap Route Destination' and contains several configuration options: 'Destination address' is a dropdown menu showing '10.64.102.113:162'; 'Trap unlocked' is a checked checkbox; 'Version' is a dropdown menu showing 'v1/v2c'; 'User' is a dropdown menu showing 'nectar'; and 'Description' is a text input field containing 'Nectar for Avaya'. 'Save' and 'Cancel' buttons are located at the bottom right of the form.

The following webpage shows the **Route Destination** configuration for SNMPv3 traps.

The screenshot shows the Avaya Aura Media Server web interface. The top header includes the Avaya logo, the title 'Avaya Aura® Media Server', and links for 'Help' and 'Sign Out admin'. Below the header, a breadcrumb trail reads: 'Home > System Configuration > Network Settings > SNMP > Destinations > Add Route Destination'. The left sidebar contains a tree view with categories like System Status, Applications, Cluster Configuration, System Configuration, Server Profile, Network Settings, Signaling Protocols, Media Processing, Music, ICE, Media Security, ACI, Advanced Settings, Application Interpreters, Monitoring Settings, Session Detail Records, Content Store, and Logging Settings. The main content area is titled 'Add Trap Route Destination' and contains the following fields: 'Destination address' (a dropdown menu showing '10.64.102.113:162'), 'Trap unlocked' (a checked checkbox), 'Version' (a dropdown menu showing 'v3'), 'User' (a dropdown menu showing 'nectar'), and 'Description' (a text field containing 'Nectar for Avaya'). At the bottom right of the form are 'Save' and 'Cancel' buttons.

8.2. Configure RTCP

This section covers the configuration for reporting RTCP to Nectar. Navigate to **System Configuration → Media Processing → General Settings** and scroll down to the **Dual Unicast Monitor** section to set the **Monitoring Server IP** to the Nectar IP address and **Monitoring Server Port** to **5005**, the RTCP receiver port configured on Nectar. Click **Save**.

The screenshot shows the Avaya Aura Media Server web interface. The top header includes the Avaya logo, the title 'Avaya Aura® Media Server', and links for 'Help' and 'Sign Out admin'. Below the header, a breadcrumb trail reads: 'Home > System Configuration > Media Processing > General Settings'. The left sidebar contains a tree view with categories like System Status, Applications, Cluster Configuration, System Configuration, Server Profile, Network Settings, Signaling Protocols, Media Processing, Music, ICE, Media Security, ACI, Advanced Settings, Application Interpreters, Monitoring Settings, Session Detail Records, Content Store, and Logging Settings. The main content area is titled 'Dual Unicast Monitoring' and contains the following fields: 'Dual Unicast Monitoring' (a checked checkbox with a refresh and power icon), 'Monitoring Server IP' (a text field containing '10.64.102.113' with a refresh and power icon, and a character count '(1 - 256 characters)'), and 'Monitoring Server Port' (a text field containing '5005' with a refresh and power icon, and a character count '(0 - 65535)'). Below these fields is a section titled 'Compositor Resource' with a 'Compositor Nodes' text field and a 'Clear All' button. At the bottom right of the form are 'Save', 'Cancel', and 'Restore Defaults' buttons.

9. Configure Avaya Session Border Controller for Enterprise

This section provides the procedure for configuring SNMP and RTCP relay service. The procedures include the following areas:

- Launch EMS Web Interface
- Configure SNMP
- Configure RTCP Relay Service

It is assumed that the initial installation and configuration of SBCE has already been completed. For more information on configuring SBCE, refer to [6].

9.1. Launch EMS Web Interface

Access the Session Border Controller web management interface by using a web browser and entering the URL **Error! Hyperlink reference not valid.**, where *<ip-address>* is the EMS IP address. Log in using the appropriate credentials.

Once logged in, the **Dashboard** screen is presented as shown below. Change the **Device** in the title bar from *EMS* to *SBCE*.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web management interface. The top navigation bar includes 'Device: EMS', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. The left sidebar lists 'EMS Dashboard' with sub-links: 'Software Management', 'Device Management', 'System Administration', 'Templates', 'Backup/Restore', and 'Monitoring & Logging'. The central dashboard area is titled 'Dashboard' and contains several sections: 'Information' (System Time, Version, GUI Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count, Last Logged in at, Failed Login Attempts), 'Installed Devices' (EMS, SBCE), 'Active Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (None found), and 'Notes' (No notes found). An 'Add' button is located next to the 'Incidents' section.

9.2. Configure SNMP

This section covers the configuration of SNMP on SBCE. Navigate to **Monitoring & Logging** → **SNMP**. The **SNMP** webpage is displayed as shown below. In the **SNMP v3** tab, click **Add**.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes 'Device: SBCE', 'Alarms', 'Incidents', 'Status', 'Logs', 'Diagnostics', 'Users', 'Settings', 'Help', and 'Log Out'. The main header displays 'Session Border Controller for Enterprise' and the 'AVAYA' logo. The left sidebar lists various management sections, with 'Monitoring & Logging' expanded to show 'SNMP'. The main content area is titled 'SNMP: SBCE' and features three tabs: 'SNMP v3' (selected), 'Management Servers', and 'Trap Severity Settings'. An 'Add' button is located in the top right of the table area. The table lists SNMP v3 configurations with columns for User Name, Auth Schema, Auth Protocol, Priv Protocol, Privilege, and Traps. One entry is visible: 'nectar' with 'authPriv' authentication, 'SHA' protocol, 'AES' privacy, 'READ' privilege, and '10.64.102.113:162 [default]' traps. Action links 'Clone', 'Edit', and 'Delete' are provided for each entry.

User Name	Auth Schema	Auth Protocol	Priv Protocol	Privilege	Traps	
nectar	authPriv	SHA	AES	READ	10.64.102.113:162 [default]	Clone Edit Delete

In the **Add User** dialog box, configure the following fields to add Nectar as the SNMP trap receiver:

- **User Name:** Provide a user name (e.g., *nectar*).
- **Authentication Scheme:** Select SNMPv3 authentication scheme (e.g., *authPriv*).
- **AuthPassPhrase:** Enter authentication password, if required.
- **Confirm AuthPassPhrase:** Re-enter authentication password, if required.
- **Authentication Protocol:** Select *SHA*, if authentication protocol is used.
- **PrivPassPhrase:** Enter privacy password, if required.
- **Confirm PrivPassPhrase:** Re-enter privacy password, if required.
- **Privacy Protocol:** Select privacy protocol, if required (e.g., *AES*).
- **Privilege:** Select *Read*.
- **Trap IP Address:** Set to Nectar IP address (e.g., *10.64.102.113*).
- **Port:** Set to SNMP trap port *162*.
- **Trap Profile:** Use the *default* trap profile. To view default trap profile, navigate to **Configuration Profiles → SNMP Traps**.

Add User X

User Name:

Authentication Scheme: ☐ noAuthNoPriv ☐ authNoPriv ☒ authPriv

AuthPassPhrase:

Confirm AuthPassPhrase:

Authentication Protocol: ☒ SHA ☐

PrivPassPhrase:

Confirm PrivPassPhrase:

Privacy Protocol: ☒ AES ☐ DES

Privilege: ☒ Read ☐ Read/Write

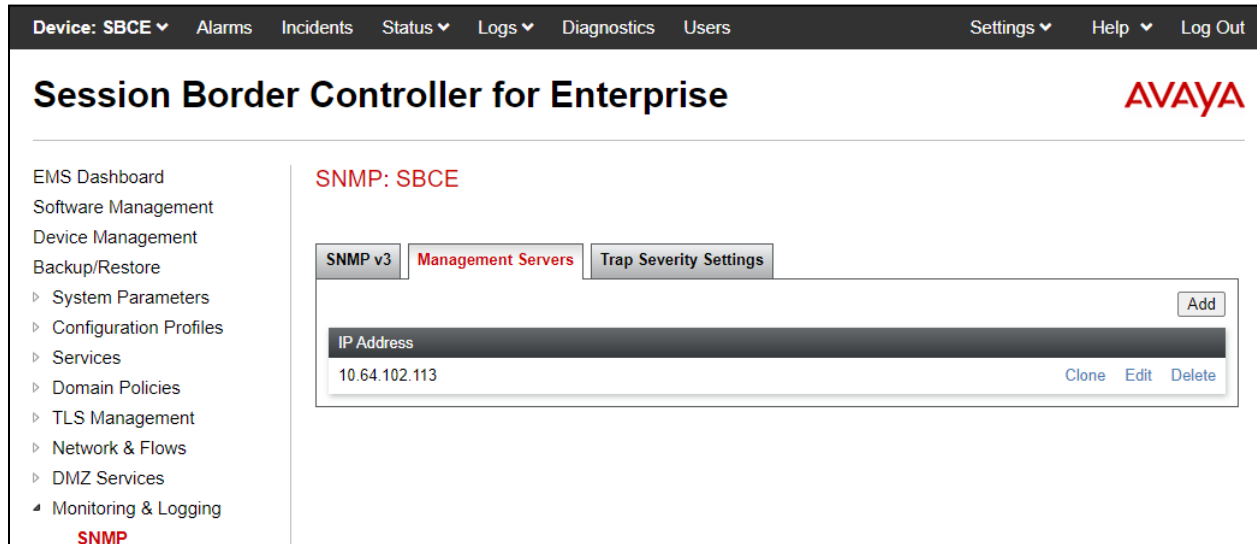
Add

Trap IP Address	Port	Trap Profile
<input type="text" value="10.64.102.113"/>	<input type="text" value="162"/>	<input type="text" value="default"/> ▼

Delete

Finish

Select the **Management Servers** tab and click **Add**.



In the **Add IP Address** dialog box, enter the Nectar IP address (e.g., *10.64.102.113*).



The default **Trap Severity Settings** were used, where all trap severities were enabled.

9.3. Configure RTCP Relay Service

This section describes the SBCE configuration to relay RTCP to Nectar. This configuration supports SIP remote workers that register to Session Manager through SBCE.

Navigate to **DMZ Services** → **Relay**. The **Relay Services: SBCE** webpage is displayed as shown below. In the **Application Relay** tab, click **Add**.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The top navigation bar includes links for Device, Alarms, Incidents, Status, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various management options, with 'DMZ Services' and 'Relay' highlighted. The main content area is titled 'Relay Services: SBCE' and features four tabs: 'Application Relay' (selected), 'Reverse Proxy', 'XMPP', and 'H248 Relay'. An 'Add' button is located in the top right corner of the table area. The table lists the configured relay service:

Name	Type	Remote IP/FQDN:Port	Remote Transport	Listen IP:Port Network	Listen Transport	Connect IP Network	
Remote-Worker-RTCP	RTCP	10.64.102.113:5005	UDP	10.64.101.102:5005 Public-B1 (B1, VLAN 0)	UDP	10.64.102.108 Private-A1 (A1, VLAN 0)	View Edit Delete

The **Add Application Relay** dialog box is displayed as shown below. To add an **Application Relay** to relay RTCP from SIP remote workers to Nectar, provide the following configuration.

In the **General Configuration** section, provide a descriptive **Name** (e.g., *Remote-Worker-RTCP*) and set the **Service Type** is set to *RTCP*.

In the **Remote Configuration** section, set the **Remote IP/FQDN** is set to the Nectar IP address (e.g., *10.64.102.113*). For RTCP, port *5005* and *UDP* transport is used.

In the **Device Configuration** section, set the **Listen IP** to the SBCE public IP address (e.g., *10.64.101.102*), which remote SIP endpoints use as the SIP proxy IP address, and set the **Connect IP** to the SBCE private IP address (e.g., *10.64.102.108*). For RTCP, port *5005* and *UDP* transport is used.

In the **Additional Configuration** section, set the **Options** to *RTCP Monitoring* → *Hop-by-Hop Traceroute*.

Add Application RelayX

General Configuration

Name

Remote-Worker-RTCP

Service Type

RTCP ▾

Remote Configuration

Remote IP/FQDN

10.64.102.113

Remote Port

5005

Remote Transport

UDP ▾

Device Configuration

Listen IP

Public-B1 (B1, VLAN 0) ▾

10.64.101.102 ▾

Listen Port

5005

Connect IP

Private-A1 (A1, VLAN 0) ▾

10.64.102.108 ▾

Listen Transport

UDP ▾

Additional Configuration

Whitelist Flows

☐

Use Relay Actors

☒

Options

Use Ctrl+Click to select or deselect multiple items.

RTCP Monitoring

End-to-End Rewrite

Hop-by-Hop Traceroute

Bridging

Finish

JAO; Reviewed:
SPOC 10/6/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

35 of 65
Nectar-Aura10

Navigate to **Network & Flows** → **Advanced Options** to display the Advanced Options webpage. In the **RTCP Monitoring** tab, enable **RTCP Monitoring Relay**, set the **Node Type** to **Core**, and set the **Relay IP** to the private SBCE interface (e.g., *10.64.102.108*).

Device: SBCE
Alarms
Incidents
Status
Logs
Diagnostics
Users
Settings
Help
Log Out

Session Border Controller for Enterprise

AVAYA

EMS Dashboard

Software Management

Device Management

Backup/Restore

System Parameters

Configuration Profiles

Services

Domain Policies

TLS Management

Network & Flows

DMZ Services

Monitoring & Logging

Network Management

Media Interface

Signaling Interface

End Point Flows

Session Flows

Advanced Options

Advanced Options

Periodic Statistics

Feature Control

SIP Options

Network Options

Port Ranges

RTCP Monitoring

Load Monitoring

Changes to the settings below take effect immediately and will impact sessions that are using them. It is recommended to change these values only during a maintenance window.

RTCP Monitoring Configuration

RTCP Monitoring Relay

Node Type

Core

Relay IP

Private-A1 (A1, VLAN 0)

10.64.102.108

Port

5005

RTCP Monitoring Report Generation

SBCE Interface IP

None

None

SBCE Interface Port

Monitoring server IP/FQDN and Port

IP:Port

Monitoring Frequency based on RTCP Report

2

Monitoring interval in absence of RTCP Report

10

seconds

Save

JAO; Reviewed:
SPOC 10/6/2022

Solution & Interoperability Test Lab Application Notes
©2022 Avaya Inc. All Rights Reserved.

36 of 65
Nectar-Aura10

10. Configure Avaya SIP Endpoints

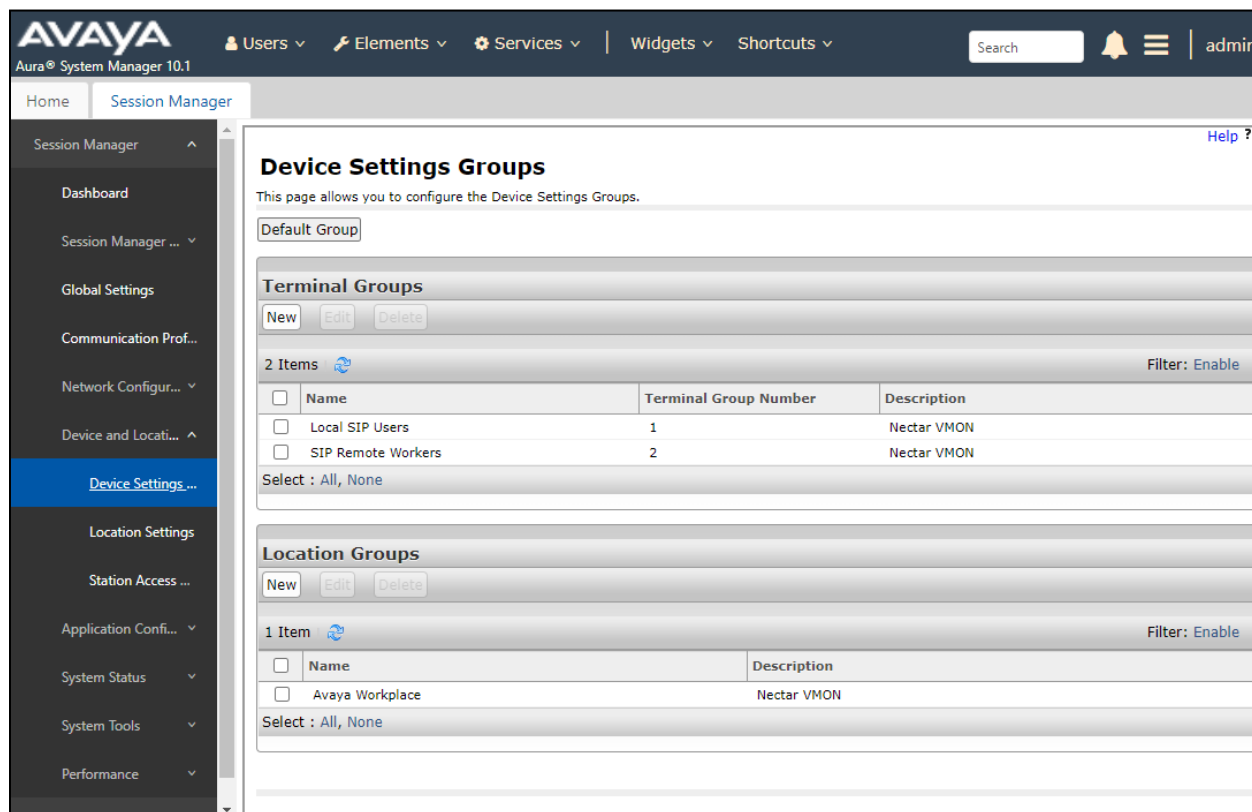
This section covers the methods for providing Avaya SIP 96x1 and J100 Series SIP Deskphones and Avaya Workplace with RTP settings. The two methods include the use of **Device Settings Groups** on System Manager and the **46xxsettings.txt** file.

10.1. Configure Device Settings Groups in System Manager

There are two types of **Device Settings Groups**, **Terminal Groups** and **Location Groups**. A terminal group will allow configuration parameters, such as RTP settings, to be assigned on a SIP user basis. Configuration settings specified in a location group can be assigned to SIP users in a specified location. Note that Terminal Groups take precedence for Location Groups.

Device Settings Groups are configured in System Manager. To access the System Manager web interface, use the URL **Error! Hyperlink reference not valid.** in an Internet browser window, where *<ip-address>* is the System Manager IP address. Log in using the appropriate credentials.

Navigate to **Elements** → **Session Manager** → **Device and Location Configuration** → **Device Settings Groups**. The following webpage shows that two terminal groups exist, one for local SIP users and another one for SIP remote workers. As a different example, one location group was created for Workplace.



The screenshot displays the Avaya System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, a search bar, and user information (admin). The left sidebar shows the navigation menu with options like Home, Session Manager, Dashboard, and various settings menus. The main content area is titled "Device Settings Groups" and contains two sections: "Terminal Groups" and "Location Groups".

Terminal Groups

Name	Terminal Group Number	Description
Local SIP Users	1	Nectar VMON
SIP Remote Workers	2	Nectar VMON

Location Groups

Name	Description
Avaya Workplace	Nectar VMON

To create a terminal group, click **New** in the **Terminal Groups** section. In the **General** section, provide a descriptive **Name** (e.g., *Local SIP Users* or *SIP Remote Workers*) and **Description**. The **Group Type** is automatically set to *Terminal Group*. Assign a **Terminal Group Number**. Number 1 was assigned for local SIP users and number 2 was assigned for SIP remote workers.

In the **VoIP Monitoring Manager** section, the **IP Address** was set to the Nectar IP address (i.e., *10.64.102.113*) for local SIP users and to the SBCE public IP address (i.e., *10.64.101.102*) for SIP remote workers. For SIP remote workers, RTCP will be relayed from SBCE to Nectar. The default values for **RTCP Port** and **Reporting Period** were used. Click **Save**.

The following webpage displays Terminal Group 1 for local SIP users.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar shows a tree view with 'Session Manager' selected, and 'Device Settings Group' highlighted. The main content area is titled 'Device Settings Group' and includes 'Restore', 'Cancel', and 'Save' buttons. Below the title is a breadcrumb trail: 'General | Endpoint Timer | Maintenance Settings | VoIP Monitoring Manager | Volume Settings | VLAN Parameters | DIFFSERV/QOS Parameters | 802.1 P/Q Parameters |'. The 'General' section is expanded, showing fields for 'Name' (Local SIP Users), 'Description' (Nectar VMON), 'Group Type' (Terminal Group selected), and 'Terminal Group Number' (1). Other sections like 'Endpoint Timer', 'Maintenance Settings', 'VoIP Monitoring Manager' (with IP Address 10.64.102.113, Port 5005, and Reporting Period 5), 'Volume Settings', 'VLAN Parameters', 'DIFFSERV/QOS Parameters', and '802.1 P/Q Parameters' are collapsed. 'Restore', 'Cancel', and 'Save' buttons are at the bottom right.

The following webpage displays the Terminal Group 2 for SIP Remote Workers.

The screenshot shows the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, 'Aura® System Manager 10.1', and tabs for Users, Elements, Services, Widgets, and Shortcuts. A search bar and a user profile 'admin' are also present. The left sidebar contains a menu with 'Session Manager' selected, and sub-items like Dashboard, Session Manager Admin, Global Settings, Communication Profile, Network Configuration, Device and Location, and Device Settings Group (highlighted). The main content area is titled 'Device Settings Group' and includes tabs for General, Endpoint Timer, Maintenance Settings, VoIP Monitoring Manager, Volume Settings, VLAN Parameters, DIFFSERV/QOS Parameters, and 802.1 P/Q Parameters. The 'General' tab is active, showing fields for Name (SIP Remote Workers), Description (Nectar VMON), Group Type (Terminal Group selected), and Terminal Group Number (2). Buttons for Restore, Cancel, and Save are visible at the top right and bottom right of the form.

To assign a terminal group number to a SIP user, navigate to the SIP user **CM Endpoint Profile Editor**, and in the **Feature Options** tab, set **IP Phone Group ID** to the desired terminal group number.

To create a location group, click **New** in the **Location Groups** section in the **Device Settings Groups** page. In the **General** section, provide a descriptive **Name** (e.g., *Avaya Workplace*) and **Description**. The **Group Type** is automatically set to *Location Group*.

In the **VoIP Monitoring Manager** section, the **IP Address** was set to the Nectar IP address (i.e., *10.64.102.113*). The default values for **RTCP Port** and **Reporting Period** were used. Click **Save** (not shown). Next, this location group will be assigned to a **Location**.

The screenshot displays the Avaya Aura System Manager 10.1 interface. The top navigation bar includes the Avaya logo, user information, and various menu items like Users, Elements, Services, Widgets, and Shortcuts. The left sidebar shows a tree view of the system configuration, with 'Device Settings Groups' selected. The main panel is titled 'Device Settings Group' and contains several tabs for configuration. The 'General' tab is active, showing fields for 'Name' (Avaya Workplace), 'Description' (Nectar VMON), and 'Group Type' (Location Group). Other tabs include 'Server Timer', 'Assigned Locations', 'Endpoint Timer', 'Maintenance Settings', 'VoIP Monitoring Manager' (with IP Address 10.64.102.113, Port 5005, and Reporting Period 5), 'Volume Settings', 'VLAN Parameters', 'DIFFSERV/QOS Parameters', and '802.1 P/Q Parameters'.

To assign the previously configured location group to a **Location**, select **Location Settings** in the left pane. Assign the **Location Group** to a **Location** as shown below. In this example, the *Avaya Workplace* location group was assigned to the **Thornton** location. Note that this method of assigning configuration settings could also have been used for local SIP users (e.g., 96x1 and J100 Series SIP Deskphones) that are local or remote workers.

The screenshot displays the Avaya Aura System Manager 10.1 web interface. The top navigation bar includes the Avaya logo, user information (Users), and various configuration menus (Elements, Services, Widgets, Shortcuts). A search bar and notification icons are also present. The left sidebar shows the navigation menu with options like Home, Session Manager, Dashboard, and Global Settings. The main content area is titled "Location Settings" and contains a table with two columns: "Name" and "Device Setting Group". The table lists two entries: "Thornton" and "Thornton-SBC", both assigned to the "Avaya Workplace" group. A "Save" button is visible above the table.

Name	Device Setting Group
Thornton	Avaya Workplace
Thornton-SBC	

10.2. Configure 46xxsettings.txt File

Alternatively, the Avaya 96x1 and J100 Series SIP Deskphones can derive the RTCP settings from the **46xxsettings.txt** file. The **RTCP Monitoring** parameters for local SIP users can be configured as follows in the file. Note that **RTCPMON** was set to the Nectar IP address.

```
##### RTCP MONITORING #####
##
## The RTCP monitor
## One RTCP monitor (VMM server) IP address in dotted-decimal format or DNS name
## format (0 to 15 characters).
SET RTCPMON 10.64.102.113
##
## RTCPMONPORT sets the port used to send RTCP information to the IP address specified
## in the RTCPMON parameter. The default value is 5005.
SET RTCPMONPORT 5005
##
## RTCP Monitor Report Period
## Specifies the interval for sending out RTCP monitoring reports (5-30 seconds).
## Default is 5 seconds.FG
SET RTCPMONPERIOD 5
##
```

SIP remote workers, assigned to Group 4, can be provided the RTCP Monitoring settings as follows. Note that **RTCPMON** was set to the public SBCE interface. SBCE will relay RTCP to Nectar as configured in **Section 0**.

```
#####  
# GROUP_4  
##### Add SET Statements for GROUP 4 below #####  
  
SET RTCPMON 10.64.102.113  
SET RTCPMONPORT 5005  
SET RTCPMONPERIOD 5  
  
##### END OF GROUP 4 SETTINGS #####  
GOTO END
```

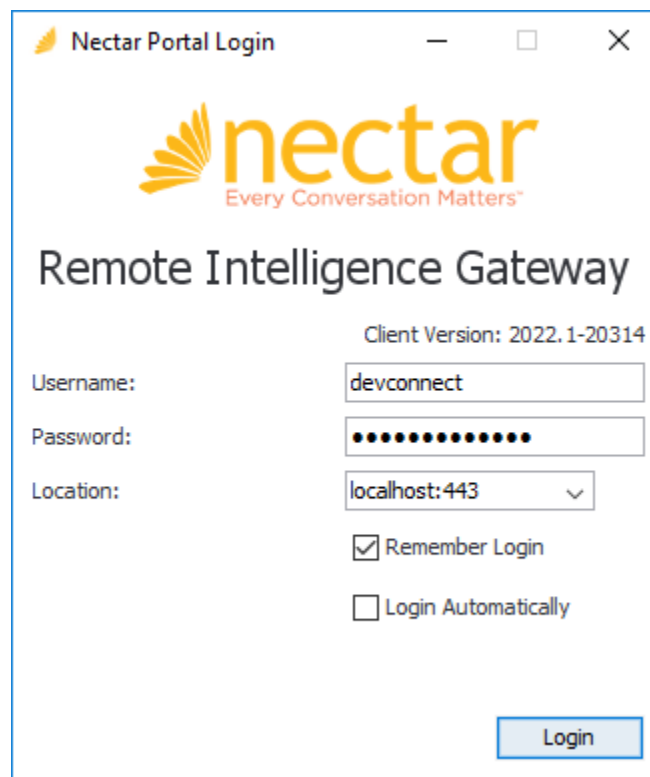
11. Configure Nectar for Avaya

This section covers the Nectar configuration to monitor Communication Manager, Media Gateways, Media Server and Avaya IP Deskphones using SNMP, RTCP, the SAT interface, and Application Enablement Services SMS Web Service. The configuration was performed via the **RIG client**. The procedure covers the following areas:

- Launch the RIG Client
- Configure Communication Manager SAT Access and SNMP Polling
- Configure SBCE SNMP Polling
- Configure SNMP Traps
- Configure Real-Time Quality Monitoring

11.1. Launch the RIG Client

In an Internet browser, enter the Nectar IP address in the URL field. The RIG client software is downloaded. Install and run the RIG client. In the **Nectar Portal Login** screen, enter the user credentials and click **Login**.



Nectar Portal Login

nectar
Every Conversation Matters™

Remote Intelligence Gateway

Client Version: 2022.1-20314

Username: devconnect

Password: ●●●●●●●●●●

Location: localhost:443

☒ Remember Login

☐ Login Automatically

Login

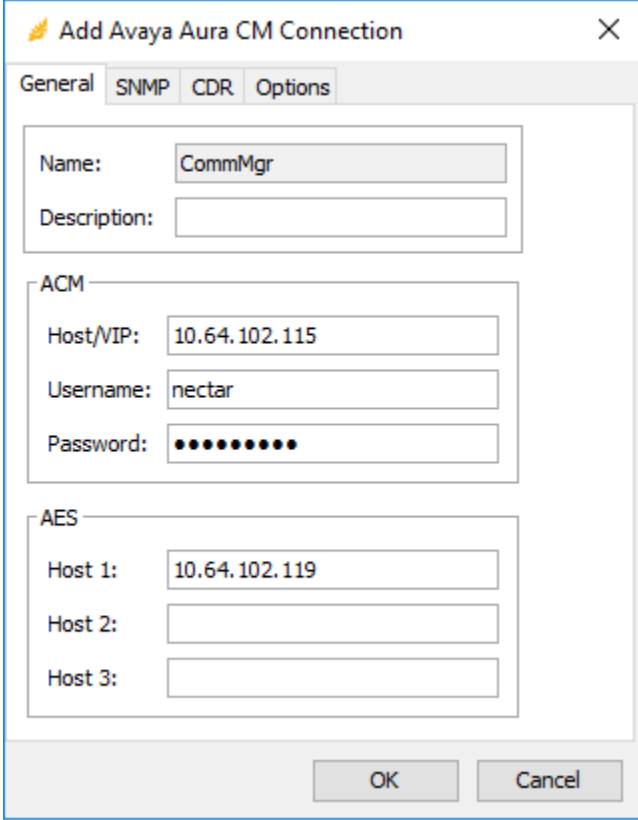
11.2. Configure Communication Manager SAT Access and SNMP Polling

Navigate to **Modules** → **Avaya** → **Aura CM (r7.0 or above)** to display the **Avaya Aura CM (r7.0 or above) Setup** windows as shown below. Click **Add**.

The screenshot shows the Nectar RIG interface. At the top, the title bar reads "Nectar RIG: localhost:443". Below it is the Nectar logo with the tagline "Every Conversation Matters". A user profile icon labeled "devconnect" is in the top right. A blue header bar contains the word "Satellite:". Below this is a navigation menu with icons and labels for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. A status bar shows "Primary: 2022.1-21422", "RTD: 3 ms", and "Users: 0". The main content area is titled "Avaya Aura CM (r7.0 or above) Setup:". Below the title are tabs for "Configurations", "Settings", and "VKM Options". A search bar is on the right. Below the search bar are links for "Add", "Edit", "Remove", "Enable", "Disable", "Collections", "Timer Tasks", "Capacity Pollers", and "SNMP Configuration". A table displays the configuration for the "CommMgr" system. The table has columns for System Name, Description, Enable, Host/VIP, Server 1 IP, Server 2 IP, and AES Host. The data row shows "CommMgr" with "true" enabled, host "10.64.102.115", and server IPs "10.64.102.115". A scrollbar at the bottom indicates "1 row".

System Name	Description	Enable	Host/VIP	Server 1 IP	Server 2 IP	AES Host
CommMgr		true	10.64.102.115			10.64.102.119

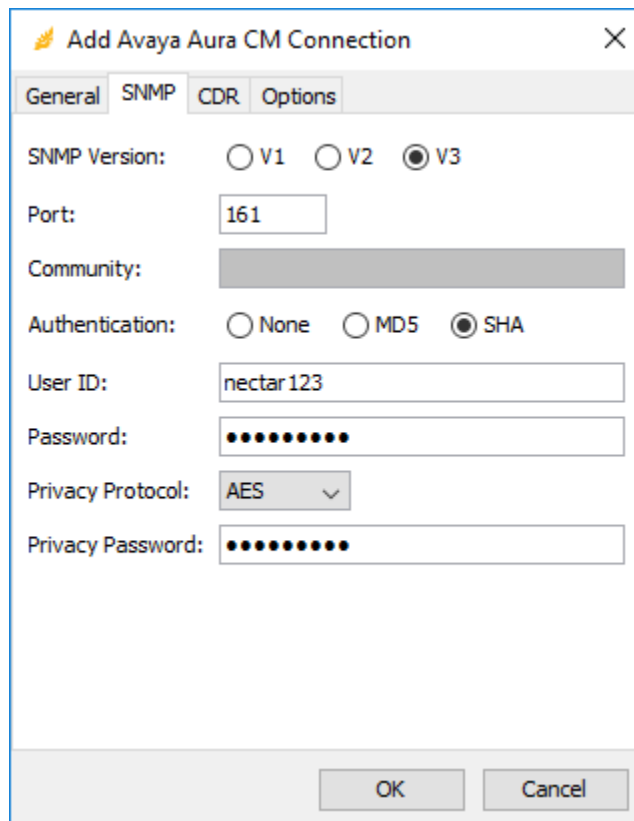
In **Add Avaya Aura CM Connection**, select the **General** tab. Specify a descriptive name (e.g., *CommMgr*) in the **Name** field. In the **ACM** section, set **Host/VIP** to the Communication Manager IP address and specify the SAT login credentials, configured in **Section 5.2**, in the **Username** and **Password** fields. In the **AES** section, specify the IP address of Application Enablement Service in **Host 1** used to direct requests to SMS Web Service. Note that the Communication Manager credentials specified in the **ACM** section are also used by Nectar when making requests via the SMS Web Service.



The screenshot shows a dialog box titled "Add Avaya Aura CM Connection" with a close button (X) in the top right corner. The dialog has four tabs: "General", "SNMP", "CDR", and "Options". The "General" tab is selected. Inside the "General" tab, there are three main sections: "Name", "ACM", and "AES". The "Name" section has a "Name:" label and a text field containing "CommMgr", and a "Description:" label with an empty text field. The "ACM" section has a "Host/VIP:" label and a text field containing "10.64.102.115", a "Username:" label and a text field containing "nectar", and a "Password:" label and a text field filled with dots. The "AES" section has a "Host 1:" label and a text field containing "10.64.102.119", a "Host 2:" label with an empty text field, and a "Host 3:" label with an empty text field. At the bottom right of the dialog are "OK" and "Cancel" buttons.

In the **SNMP** tab, configure SNMP polling access. In this example, SNMPv3 polling was configured as shown in **Section 5.3.2**. SNMPv1 or v2c may also be used by specifying the **Community** instead. These SNMP credentials are also used for SNMP polling of the Media Gateways and should match the configuration in **Section 7.2**. Click **OK**.

Note: SNMP credentials for Communication Manager and the Media Gateways should be the same.



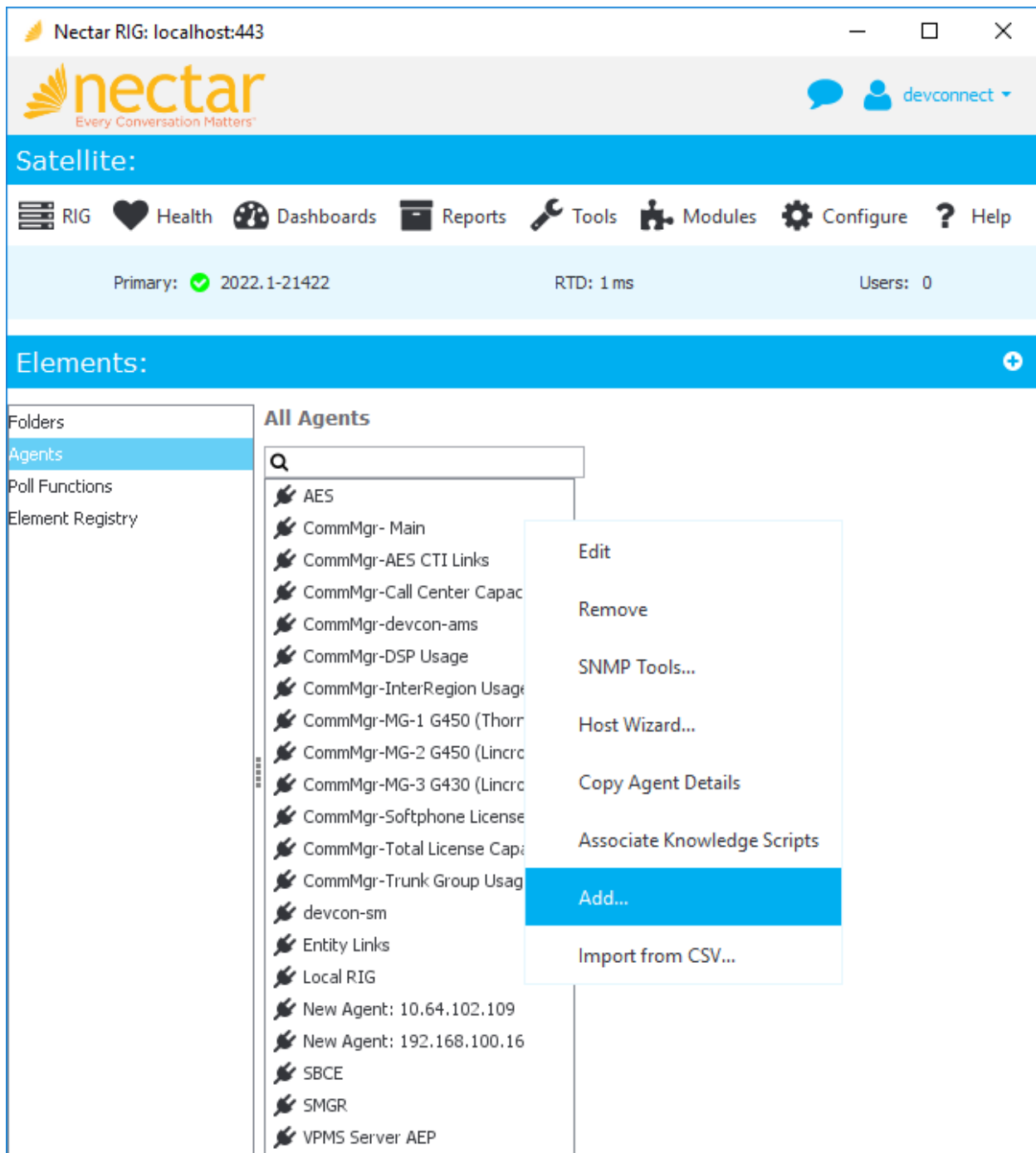
The screenshot shows a dialog box titled "Add Avaya Aura CM Connection" with a close button (X) in the top right corner. The dialog has four tabs: "General", "SNMP", "CDR", and "Options". The "SNMP" tab is currently selected. The configuration fields are as follows:

- SNMP Version:** Three radio buttons are present: "V1", "V2", and "V3". The "V3" radio button is selected.
- Port:** A text input field containing the value "161".
- Community:** A text input field that is currently empty.
- Authentication:** Three radio buttons are present: "None", "MD5", and "SHA". The "SHA" radio button is selected.
- User ID:** A text input field containing the value "nectar123".
- Password:** A text input field filled with ten black dots, indicating a masked password.
- Privacy Protocol:** A dropdown menu with "AES" selected and a downward arrow.
- Privacy Password:** A text input field filled with ten black dots, indicating a masked password.

At the bottom right of the dialog, there are two buttons: "OK" and "Cancel".

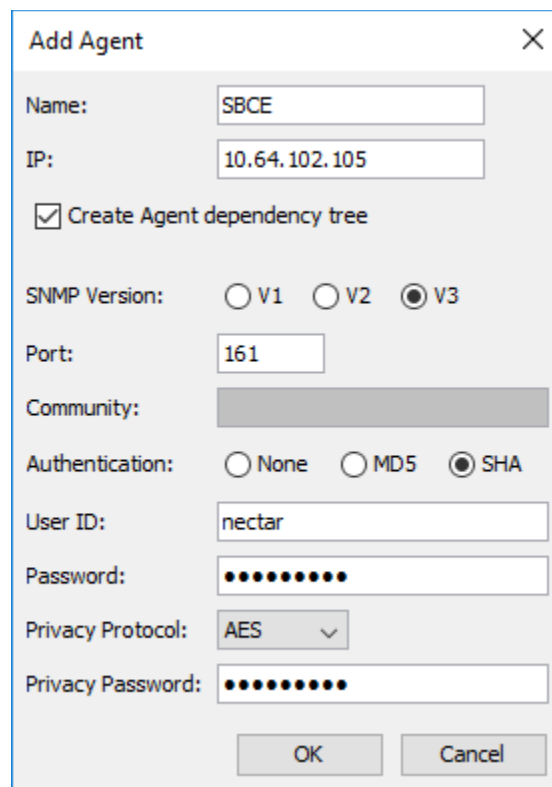
11.3. Configure SBCE SNMP Polling

Navigate to **Health** → **Elements**, and then select **Agents** in the left pane. In the **All Agents** section, right-mouse click and select **Add** as shown below.



In the **Add Agent** dialog box, configure the following fields to add an SBCE agent. The SNMP credentials must match the SNMP configuration for the SBCE. Refer to **Section 9.2**.

- Name: Specify the agent name (e.g., *SBCE*).
- IP: Specify the SBCE IP address (e.g., *10.64.102.105*).
- Create Agent dependency tree: Select this option.
- SNMP Version: Set to V3.
- Port: Set to SNMP polling port *161*.
- Authentication: Specify authentication protocol (e.g., *SHA*).
- User ID: Specify user ID (e.g., *nectar*).
- Password: Specify authentication password, if required.
- Privacy Protocol: Specify privacy protocol (e.g., *AES*).
- Privacy Password: Specify privacy password, if required.



The screenshot shows the 'Add Agent' dialog box with the following configuration:

- Name: SBCE
- IP: 10.64.102.105
- ☒ Create Agent dependency tree
- SNMP Version: V1 ☐ V2 ☒ V3
- Port: 161
- Community: (empty field)
- Authentication: None ☐ MD5 ☐ SHA ☒
- User ID: nectar
- Password: (masked with dots)
- Privacy Protocol: AES (dropdown menu)
- Privacy Password: (masked with dots)
- Buttons: OK, Cancel

In the **Poll Functions** section, right-mouse click and select **Add** as shown below.

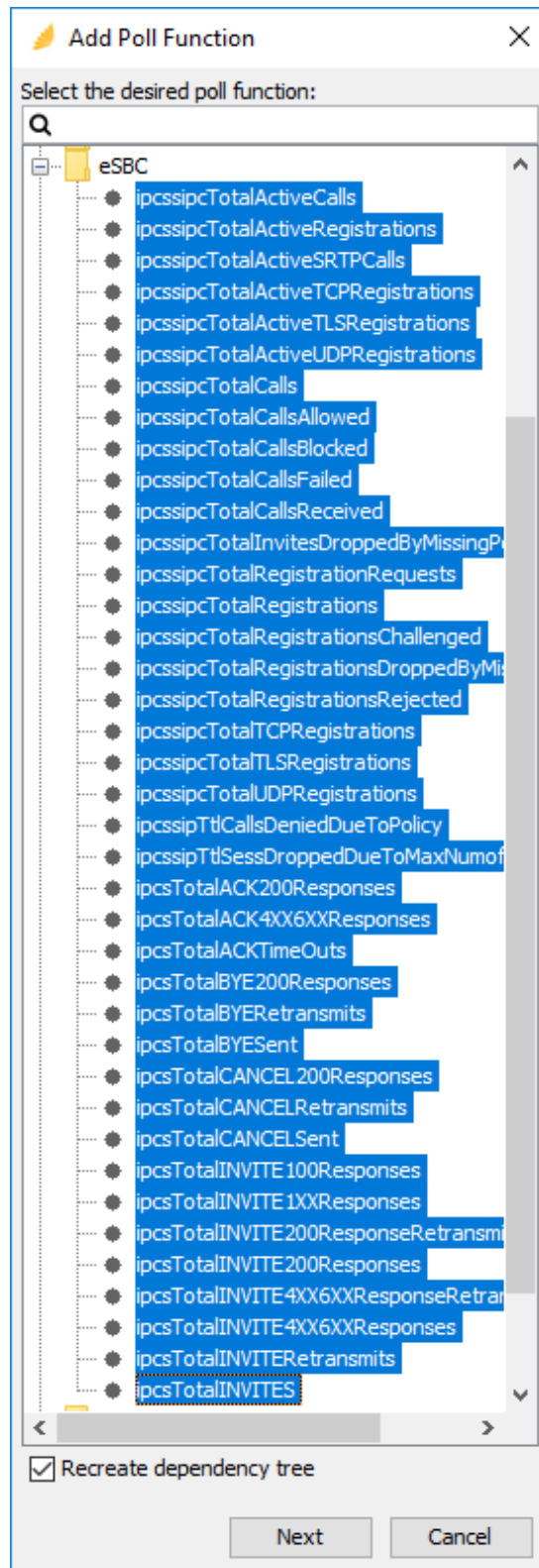
The screenshot shows the Nectar RIG web interface. The top navigation bar includes the Nectar logo, user profile 'devconnect', and a menu with options: RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. Below this, a status bar shows 'Primary: 2022.1-21422', 'RTD: 3 ms', and 'Users: 0'.

The main content area is titled 'Elements:' and contains a tabbed interface. The 'Poll Functions' tab is active. On the left, there is a list of 'All Agents' including AES, CommMgr-Main, CommMgr-AES CTI Links, CommMgr-Call Center Capacities, CommMgr-devcon-ams, CommMgr-DSP Usage, CommMgr-InterRegion Usage, CommMgr-MG-1 G450 (Thornton), CommMgr-MG-2 G450 (Lincroft), CommMgr-MG-3 G430 (Lincroft), CommMgr-Softphone License Usage, CommMgr-Total License Capacity, CommMgr-Trunk Group Usage, devcon-sm, Entity Links, Local RIG, New Agent: 10.64.102.109, New Agent: 192.168.100.16, SBCE, and SMGR. The 'SBCE' agent is selected.

The 'Poll Functions' table has two columns: 'Description' and 'Function'. A right-click context menu is open over the 'Add...' option in the 'Function' column. The menu options are: View, Add..., Edit..., Remove, Enable, Disable, Export Poll Metrics..., and Copy to Clipboard. The table shows 39 rows of data.

Description	Function
Number of SIP ACK 200 Responses	ipcsTotalACK
Number of SIP ACK 4XX 6XX Responses	ipcsTotalACK
Number of ACK Time outs	ipcsTotalACK
Number of SIP active calls.	ssipcTotal/
Number of SIP active registrat	ssipcTotal/
Number of SIP active SRTP ca	ssipcTotal/
Number of SIP active TCP reg	ssipcTotal/
Number of SIP active TLS reg	ssipcTotal/
Number of SIP active UDP reg	ssipcTotal/
Number of SIP BYE 200 Respo	sTotalBYE:
Number of SIP BYE Retransmi	sTotalBYEI
Number of SIP BYE	sTotalBYE:
Number of SIP CANCEL 200 R	sTotalCAN

In the **Add Poll Function** window, expand **eSBC** and select the desired poll functions. Click **Next**.



In the next **Add Poll Functions** window, click **Add**.

The screenshot shows the 'Add Poll Functions' window with the 'Single Targets' tab selected. On the left, a list of functions is shown, with 'TotalACK200Responses' highlighted. The main area is divided into 'Parameters' and 'Thresholds' tabs, with 'Parameters' currently active. Under 'Parameters', there is an 'Address' section with 'Inherited' set to '10.64.102.105' and an empty 'Override' field. Below this is an 'SNMP' section with two sub-panels. The top sub-panel is for 'Inherited' and has the following settings: 'SNMP Version' set to 'V3', 'Port' set to '161', 'Community' is empty, 'Authentication' set to 'SHA', 'User ID' set to 'nectar', 'Password' is masked with dots, 'Privacy Protocol' set to 'AES', and 'Privacy Password' is masked with dots. The bottom sub-panel is for 'Override' (indicated by an unchecked checkbox) and has the following settings: 'SNMP Version' set to 'V1', 'Port' set to '161', 'Community' is empty, 'Authentication' set to 'None', and 'User ID' is empty. At the bottom right of the window are 'Cancel' and 'Add' buttons.

Add Poll Functions

Single Targets

Function:

- TotalACK200Responses
- TotalACK4XX6XXRespon:
- TotalACKTimeOuts
- TotalActiveCalls
- TotalActiveRegistrations
- TotalActiveSRTPCalls
- TotalActiveTCPRegistrat
- TotalActiveTLSRegistrati
- TotalActiveUDPRegistrat
- TotalBYE200Responses
- TotalBYERetransmits
- TotalBYESent
- TotalCANCEL200Respon
- TotalCANCELRetransmit:
- TotalCANCELSent
- TotalCalls
- TotalCallsAllowed

Parameters Thresholds

Address

Inherited: 10.64.102.105

Override:

SNMP

Inherited:

SNMP Version: ☐ V1 ☐ V2 ☒ V3

Port: 161

Community:

Authentication: ☐ None ☐ MD5 ☒ SHA

User ID: nectar

Password:

Privacy Protocol: AES

Privacy Password:

☐ Override:

SNMP Version: ☒ V1 ☐ V2 ☐ V3

Port: 161

Community:

Authentication: ☒ None ☐ MD5 ☐ SHA

User ID:

Cancel Add

11.4. Configure SNMP Traps

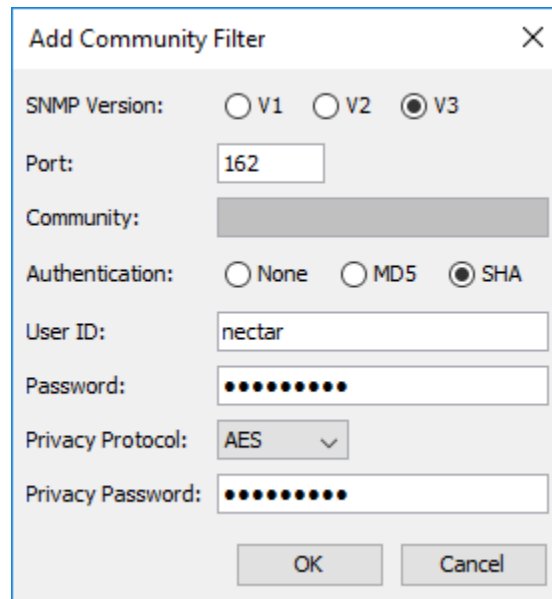
Navigate to **Configure → Receiver** and select the **Community Filter** tab. The Community Filter serves two purposes:

- Filter SNMPv1 and v2c traps based on community name (optional).
- Configure credentials for SNMPv3 traps (required).

This section covers the configuration of credentials for SNMPv3 traps. The SNMPv3 trap credentials were configured the same in Communication Manager, Media Gateways, Media Server, and SBCE so only one entry was required. Click **Add**.

The screenshot shows the Nectar RIG interface for a device named 'localhost:443'. The top navigation bar includes 'RIG', 'Health', 'Dashboards', 'Reports', 'Tools', 'Modules', 'Configure', and 'Help'. Below this, a status bar shows 'Primary: 2022.1-21422', 'RTD: 7 ms', and 'Users: 0'. The main section is titled 'Receiver:' and contains three tabs: 'Traps', 'Post Process', and 'Community Filter'. The 'Community Filter' tab is active, showing a search bar and a checkbox labeled 'Filter incoming traps based on SNMP community strings...'. Below this, there are 'Add', 'Edit', and 'Remove' buttons. A table with the header 'Community Name' contains one row with the value 'V3/nectar/SHA/...../AES/.....'. The table indicates '1 row'.

In **Add Community Filter**, set the **SNMP Version** to *V3*, the **Port** to *162*, and specify the credentials as configured on the Avaya products. Click **OK**.



The image shows a dialog box titled "Add Community Filter" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- SNMP Version:** Three radio buttons are present: ☐ V1, ☐ V2, and ☒ V3.
- Port:** A text input field containing the value "162".
- Community:** A text input field that is currently empty.
- Authentication:** Three radio buttons are present: ☐ None, ☐ MD5, and ☒ SHA.
- User ID:** A text input field containing the value "nectar".
- Password:** A text input field filled with ten black dots (••••••••••).
- Privacy Protocol:** A dropdown menu showing "AES" with a downward arrow.
- Privacy Password:** A text input field filled with ten black dots (••••••••••).

At the bottom of the dialog are two buttons: "OK" and "Cancel".

11.5. Configure Real-Time Quality Monitoring

Navigate to **Configure → Quality Management → Real Time QoS** and configure the following fields:

RTCP Receiver:	Set to <i>Enabled</i> .
Traces:	Set to <i>Enabled</i> .
Receiver Interface:	Set to the Nectar IP address (e.g., <i>10.64.102.113</i>).
Receiver Port:	Set to <i>5005</i> .
Default Codec:	Set to <i>G.711</i> .
Hop Name Lookup:	Set to <i>Enabled</i> .

Click **Apply** to start the **RTCP Receiver**.

The screenshot shows the Nectar RIG web interface. The top header includes the Nectar logo and the text 'Every Conversation Matters'. Below the header is a navigation bar with icons for RIG, Health, Dashboards, Reports, Tools, Modules, Configure, and Help. A status bar below the navigation bar shows 'Primary: 2022.1-21422', 'RTD: 4 ms', and 'Users: 0'. The main content area is titled 'Configure Real Time QoS' and has three tabs: 'General', 'Categories', and 'Endpoint Names'. The 'General' tab is selected, showing a list of configuration fields with dropdown menus or checkboxes. The fields are: 'RTCP Receiver' (Enabled), 'Traces' (Enabled), 'Receiver Interface' (10.64.102.113), 'Receiver Port' (5005), 'Default Codec' (G.711), 'Hop Name Lookup' (Enabled), 'Threshold Normalization' (Disabled), 'Use PQOS RTCP Remote Address' (Disabled), and 'Report PQOS RTCP via Agent' (Disabled). At the bottom of the configuration area are two buttons: 'Configure Categories' and 'Apply'.

Nectar RIG: localhost:443	
nectar Every Conversation Matters	
Satellite:	
RIG Health Dashboards Reports Tools Modules Configure ? Help	
Primary: 2022.1-21422 RTD: 4 ms Users: 0	
Configure Real Time QoS :	
General Categories Endpoint Names	
RTCP Receiver:	Enabled
Traces:	Enabled
Receiver Interface:	10.64.102.113
Receiver Port:	5005
Default Codec:	G.711
Hop Name Lookup:	Enabled
Threshold Normalization:	Disabled
Use PQOS RTCP Remote Address:	Disabled
Report PQOS RTCP via Agent:	Disabled
Configure Categories Apply	

12. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Nectar with Communication Manager, Media Gateways, Media Server, and SBCE.

1. Generate alarm conditions in any Avaya server. Navigate to **Health** → **Events** to view SNMP traps and events.

Nectar RIG: localhost:443

nectar
Every Conversation Matters

Satellite:

RIG Health Dashboards Reports Tools Modules Configure ? Help

Primary: 2022.1-21422 RTD: 3 ms Users: 0

Events:

Current Events

Alert	Text Time	Delay	Last Text Time	Event Id
Warning	08/15/22 05:02:11 PM (Mon) EDT	⌚	08/15/22 05:02:11 PM (Mon) EDT	avCmAlmServCmgWarning
Warning	08/15/22 09:53:10 AM (Mon) EDT		08/15/22 09:53:10 AM (Mon) EDT	cmgCertErrorNearExpiry
Good	08/15/22 09:23:38 AM (Mon) EDT		08/15/22 09:23:38 AM (Mon) EDT	avCmAlmServCmgResolved
Good	08/15/22 09:23:33 AM (Mon) EDT		08/15/22 09:23:33 AM (Mon) EDT	cmgDs1Layer2Up
Warning	08/15/22 09:23:33 AM (Mon) EDT		08/15/22 09:23:33 AM (Mon) EDT	cmgH248LinkUp
Warning	08/15/22 09:23:33 AM (Mon) EDT		08/15/22 09:23:33 AM (Mon) EDT	cmgModuleInsertSuccess
Warning	08/15/22 09:23:33 AM (Mon) EDT		08/15/22 09:23:33 AM (Mon) EDT	cmgModuleInsertSuccess

3,970 rows

UnknownTraps

0
0
3
0
0
0
0

All Events Start Time: Monday, August 15, 2022 4:46:36 PM EDT End Time: Monday, August 15, 2022 5:01:36 PM EDT Setup Filter Search

Event Id	Location	Display Name	Device Name
TotalRegistrationsDroppedByMissingPolicyevent	SBCE	Number of SIP total registrations dropped by missing policy.	Poll-33-33
TotalRegistrationsDroppedByMissingPolicyevent	SBCE	Number of SIP total registrations dropped by missing policy.	Poll-33-33
TotalRegistrationsDroppedByMissingPolicyevent	SBCE	Number of SIP total registrations dropped by missing policy.	Poll-33-33
TotalRegistrationsDroppedByMissingPolicyevent	SBCE	Number of SIP total registrations dropped by missing policy.	Poll-33-33
cmTrkMbrOosNe	CommMgr-ISDN	TRK0004	CommMgr-ISDN-TRK0004
cmTrkMbrOosNe	CommMgr-ISDN	TRK0003	CommMgr-ISDN-TRK0003
cmTrkMbrOosNe	CommMgr-ISDN	TRK0005	CommMgr-ISDN-TRK0005

2. Navigate to **Health → Agents** and then select a Media Gateway under **All Agents** to view the data collected using SNMP polling, including MG DSP Usage, Fan Speed, and Ambient Temperature Sensor.

Nectar RIG: localhost:443

nectar

Every Conversation Matters

devconnect

Satellite:

RIG
Health
Dashboards
Reports
Tools
Modules
Configure
Help

Primary: 2022.1-21422
RTD: 5 ms
Users: 0

Elements:

Folders

Agents

Poll Functions

Element Registry

All Agents

Q

AES

CommMgr- Main

CommMgr-AES CTI Links

CommMgr-Call Center Capacities

CommMgr-devcon-ams

CommMgr-DSP Usage

CommMgr-InterRegion Usage

CommMgr-MG-1 G450 (Thornton)

CommMgr-MG-2 G450 (Lincroft)

CommMgr-MG-3 G430 (Lincroft)

CommMgr-Softphone License Usage

CommMgr-Total License Capacities

CommMgr-Trunk Group Usage

devcon-sm

Entity Links

Local RIG

New Agent: 10.64.102.109

New Agent: 192.168.100.16

SBCE

SMGR

VPMS Server AEP

Poll Functions

Trap Groups

Interfaces

VKM Collections

Poll Functions

Q

Description

Function

Sub Function

Enabled

Current Value

Max Value

Base Fan 0 OperStatus

pushData

true

1

DSP State Slot 102

pushData

true

2

Ambient Temperature Sensor OperStatus

pushData

true

1

DSP State Slot 101

pushData

true

2

DSP Usage

pushData

true

0

120

Ping MG 192.168.100.16

Ping

true

47

ESS Control

pushData

true

1

Base Fan 2

pushData

true

4350

Base Fan 1 OperStatus

pushData

true

1

Base Fan 2 OperStatus

pushData

true

1

<

>

10 rows

3. Navigate to **Health** → **Agents** and then select the SBCE under **All Agents** to view the data collected via SNMP polling.

Nectar RIG: localhost:443

nectar
Every Conversation Matters™

Satellite:

RIG Health Dashboards Reports Tools Modules Configure ? Help

Primary: ● 2022.1-21422 RTD: 3 ms Users: 0

Elements:

Folders Agents Poll Functions Element Registry

All Agents

Q

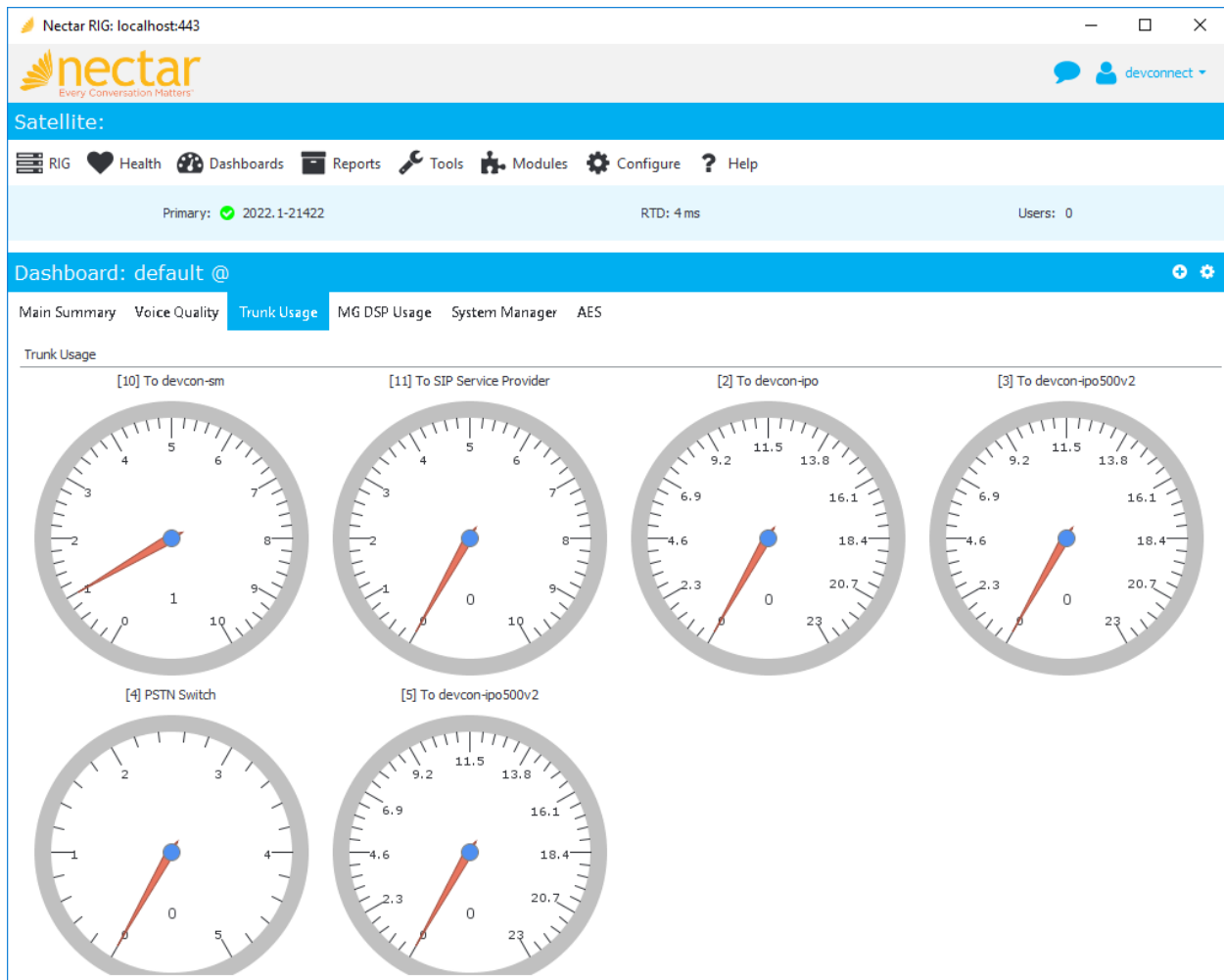
- AES
- CommMgr- Main
- CommMgr-AES CTI Links
- CommMgr-Call Center Capacities
- CommMgr-devcon-ams
- CommMgr-DSP Usage
- CommMgr-InterRegion Usage
- CommMgr-MG-1 G450 (Thornton)
- CommMgr-MG-2 G450 (Lincroft)
- CommMgr-MG-3 G430 (Lincroft)
- CommMgr-Softphone License Usage
- CommMgr-Trunk Group Usage
- devcon-sm
- Entity Links
- Local RIG
- New Agent: 10.64.102.109
- New Agent: 192.168.100.16
- SBCE**
- SMGR
- VPMS Server AEP

Poll Functions

Description	Function	Sub Function Enabled	Current Value
Number of SIP ACK 200 Responses	ipcsTotalACK200Respon...	true	110
Number of SIP ACK 4XX 6XX Responses	ipcsTotalACK4XX6XXRes...	true	42
Number of ACK Time outs	ipcsTotalACKTimeOuts	true	0
Number of SIP active calls.	ipcssipcTotalActiveCalls	true	0
Number of SIP active registrations.	ipcssipcTotalActiveRegis...	true	0
Number of SIP active SRTP calls.	ipcssipcTotalActiveSRTP...	true	0
Number of SIP active TCP registrations.	ipcssipcTotalActiveTCPR...	true	0
Number of SIP active TLS registrations.	ipcssipcTotalActiveTLRS...	true	0
Number of SIP active UDP registrations.	ipcssipcTotalActiveUDPR...	true	0
Number of SIP BYE 200 Responses	ipcsTotalBYE200Respon...	true	72
Number of SIP BYE Retransmits	ipcsTotalBYERetransmits	true	0
Number of SIP BYE	ipcsTotalBYESent	true	74
Number of SIP CANCEL 200 Responses	ipcsTotalCANCEL200Res...	true	28

< 78 rows >

4. Navigate to **Dashboards → Dashboard**. Note that the Dashboard is customizable. For the compliance test, gauges for trunk and MG DSP usage were created. The following window shows trunk usage.



The following window shows MG DSP usage.



5. Navigate to **Reports → Inventory → Avaya → Aura CM (r7.0 or above)** to view the inventory information. The following window shows the Communication Manager inventory list available.

Nectar RIG: localhost:443

nectar

Every Conversation Matters™

devconnect

Satellite:

RIG

Health

Dashboard

Reports

Tools

Modules

Configure

Help

Primary: ✓ 2022.1-21422

RTD: 5 ms

Users: 0

Avaya Aura CM (r7.0 or above) Inventory: +

ACD Agents

AES CTI Links

Announcements

Audio Groups

Cabinets

Capacities

Capacities Product ID

Cards

CTI Links

Events

History

Init Causes

IP Interfaces

IP Network Map

IP Network Region

IP Server Interfaces

Locations

Media Gateways

Media Servers

MedPro Boards

MG DSP Usage

Node Names

Registered Stations

Route Patterns

Route Pattern Details

Survivable Processors

Signal Group Status

Stations
System Information
Trunk Groups
Trunk Member Status
VDNs
VDN Variables
Vectors
Vector Events
Vector Steps
Vector Variables

As an example, click on **Media Gateways** to display the list of Media Gateways.

Nectar RIG: localhost:443

nectar

Every Conversation Matters

devconnect

Satellite:

RIG
Health
Dashboards
Reports
Tools
Modules
Configure
Help

Primary: 2022.1-21422
RTD: 3 ms
Users: 0

Avaya Aura CM (7.0 or above) Inventory: > Listing: avayaAuraCM:MEDIA_GATEWAYS

Avaya Aura CM (

ACD Agents

AES CTI Links

Announcements

Audio Groups

Cabinets

Capacities

Capacities Produ...

Cards

CTI Links

Events

History

Init Causes

IP Interfaces

IP Network Map

IP Network Region

IP Server Interf...

Locations

Media Gateways

Listing: avayaAuraCM:MEDIA_GATEWAYS

Avaya Aura CM Systems

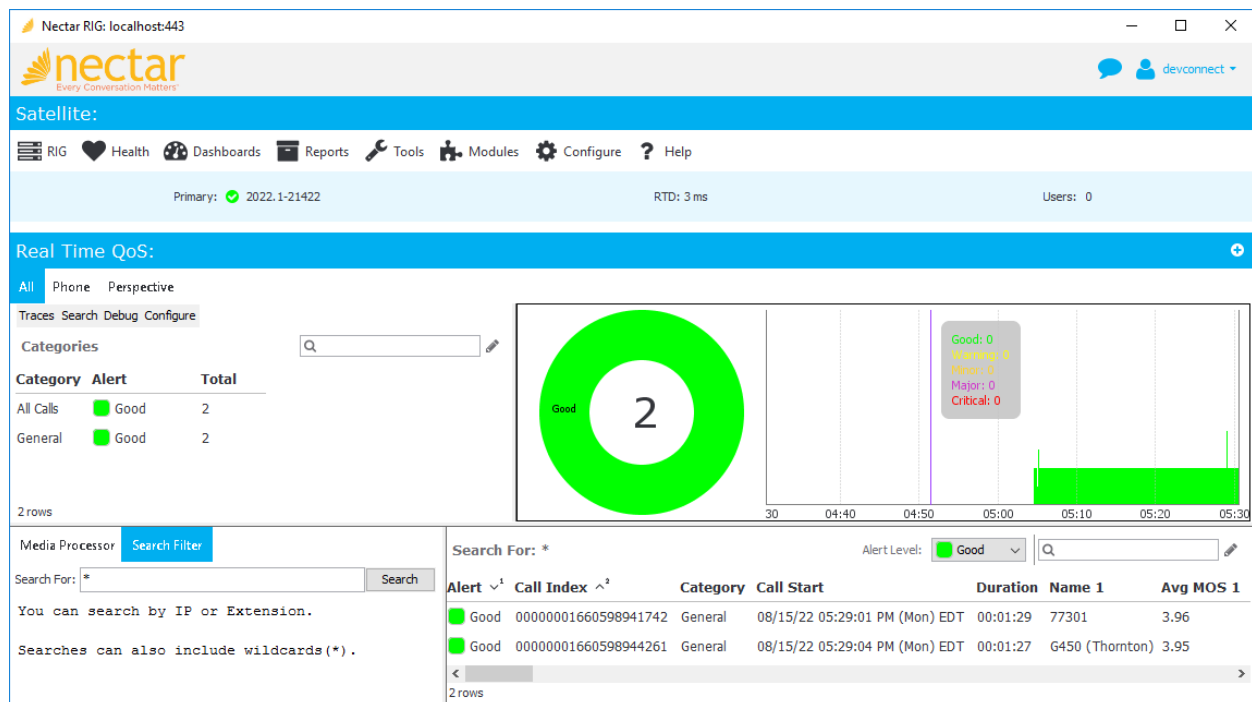
All

Q

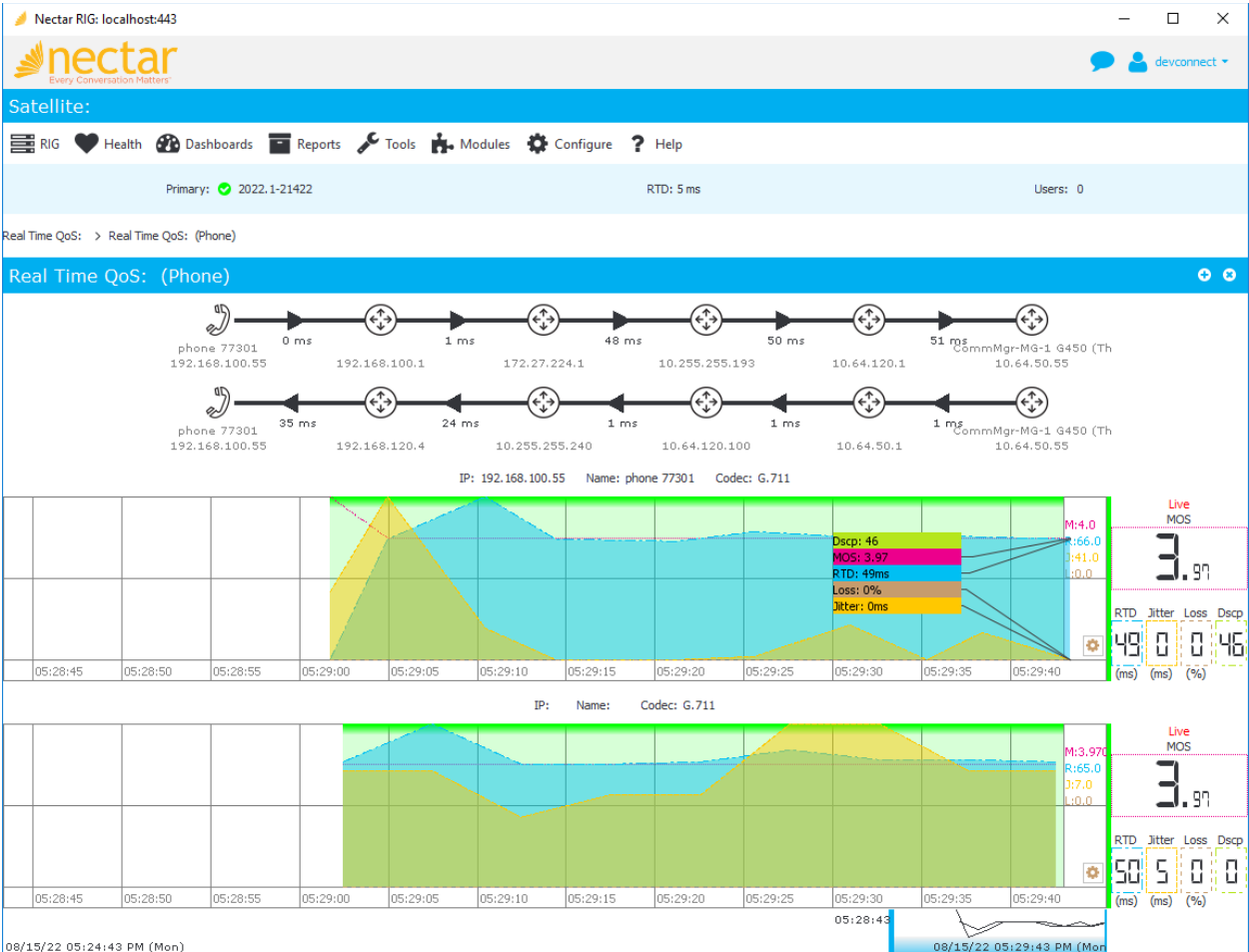
System Name	Number	Name	Serial Number	Version/Vintage	Recovery	Rule	IP Address	Control Address	Type	Region	Registered
CommMgr	1	G450 (Thornton)	14TG44050921	42.7 .0 /3	none		10.64.50.55	10.64.102.115	g450	1	y
CommMgr	2	G450 (Lincroft)	11N515752594	41.24 .0 /2	none		192.168.100.15		g450	1	n
CommMgr	3	G430 (Lincroft)	11N511742478	42.4 .0 /1	none		192.168.100.16		g430	1	n

3 rows

- Establish a call between two Avaya IP Deskphones. Navigate to **Health → Quality Management → Real-Time QoS** to view the active calls as shown below. Double-click on one of the calls to view the **Real-Time QoS metrics**.



The real-time QoS metrics and call path information for the phone are displayed as shown below. Note that there is a call path from a H.323 phone to the media resource and vice versa. There would not be any call path for Avaya SIP Deskphones or Media Server as mentioned in **Section 2.2**.



13. Conclusion

These Application Notes described the configuration steps required to integrate Nectar for Avaya with Avaya Aura® Communication Manager, Avaya G430/G450 Media Gateway, Avaya Aura® Media Server, Avaya Session Border Controller for Enterprise using SNMP, RTCP, the SAT interface, and Avaya Aura® Application Enablement Services System Management Service Web Service. The compliance test passed with observations noted in **Section 2.2**.

14. Additional References

This section references the Avaya documentation relevant to these Application Notes available at <http://support.avaya.com>.

- [1] *Administering Avaya Aura® Communication Manager*, Release 10.1, Issue 3, August 2022.
- [2] *Administering Avaya Aura® System Manager*, Release 10.1.x, Issue 6, June 2022.
- [3] *Administering Avaya Aura® Session Manager*, Release 10.1.x, Issue 3, April 2022.
- [4] *Administering Avaya G430 Branch Gateway*, Release 10.1, Issue 2, July 2022.
- [5] *Administering Avaya G450 Branch Gateway*, Release 10.1, Issue 2, July 2022.
- [6] *Administering Avaya Session Border Controller for Enterprise*, Release 10.1, Issue 1, December 2021.
- [7] *Administering Avaya Aura® Application Enablement Services*, Release 10.1.x, Issue 4, April 2022.

©2022 Avaya Inc. All Rights Reserved.

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

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