Avaya Solution & Interoperability Test Lab

Application Notes for configuring Nectar's Unified Communication Management Platform Version 7.3 with Avaya Aura® Session Manager and Avaya Aura® System Manager Release 7.1 - Issue 1.0

Abstract

These Application Notes describe the compliance tested configuration used to validate Nectar's Unified Communications Management Platform (UCMP) with Avaya Aura® Session Manager and Avaya Aura® System Manager.

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

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

1. Introduction

These Application Notes describe the compliance tested configuration used to validate Nectar's Unified Communications Management Platform (UCMP) with Avaya Aura® Session Manager and Avaya Aura® System Manager.

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

For Avaya Aura® System Manager and Avaya Aura® Session Manger, Nectar delivers inventory, registered stations, contextual alarms and performance metrics. Nectar also captures and reports on real-time RTCP call quality data from SIP endpoints registered to Session Manager, including through Avaya Session Border Controller for Enterprise (SBCE) and soft clients such as Avaya one-X® Communicator and Avaya Equinox™.

2. General Test Approach and Test Results

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

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

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

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

For the testing associated with these Application Notes, the interface between Avaya systems and the Nectar UCMP did not include use of any specific encryption features as requested by Nectar. Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

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

2.1. Interoperability Compliance Testing

For feature testing, Nectar used Java-based Remote Intelligent Gateway (RIG) Client application to view the inventory of Session Manage including: SIP entity, Entity Links, Locations, Session Manager status, Session Manager Instances, SIP Registrations...etc.

For the collection of real-time RTCP call quality: the endpoints included Avaya SIP 96x1, Avaya Equinox™, Avaya one-X® Communicator (SIP), remote worker SIP endpoint registering through Avaya SBC. The types of calls made included intra-switch calls, inbound/outbound PSTN calls, inbound/outbound inter-switch IP trunk calls, transfer and conference calls.

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

2.2. Test Results

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

2.3. Support

For technical support on Nectar's Unified Communication Management Platform, contact the Nectar Support Team at:

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

3. Reference Configuration

Figure 1 illustrates the test configuration used to verify Nectar interoperability with Session Manager and System Manager. Nectar UCMP server connected on the same LAN as the Avaya equipment and collects relevant information and monitors RTCP of SIP endpoint. A verity of Avaya telephones were configured and used to make calls from/to SIP endpoint. The remote worker SIP endpoint registers to Session Manager through the public interface of Avaya Session Border Controller for Enterprise. A simulated PSTN via PRI trunk was also configured to allow incoming and outgoing calls.

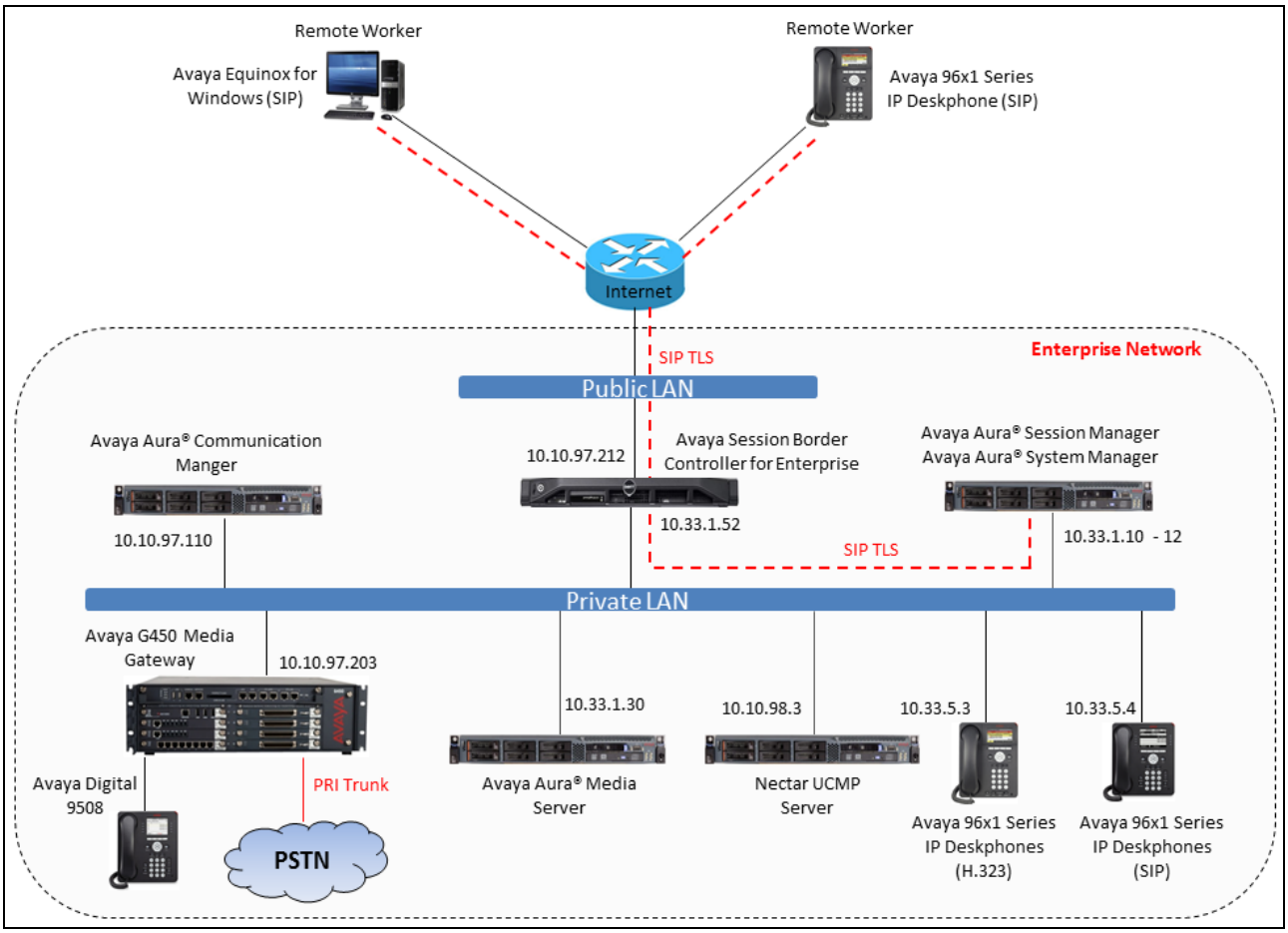


Figure 1: Test Configuration Diagram

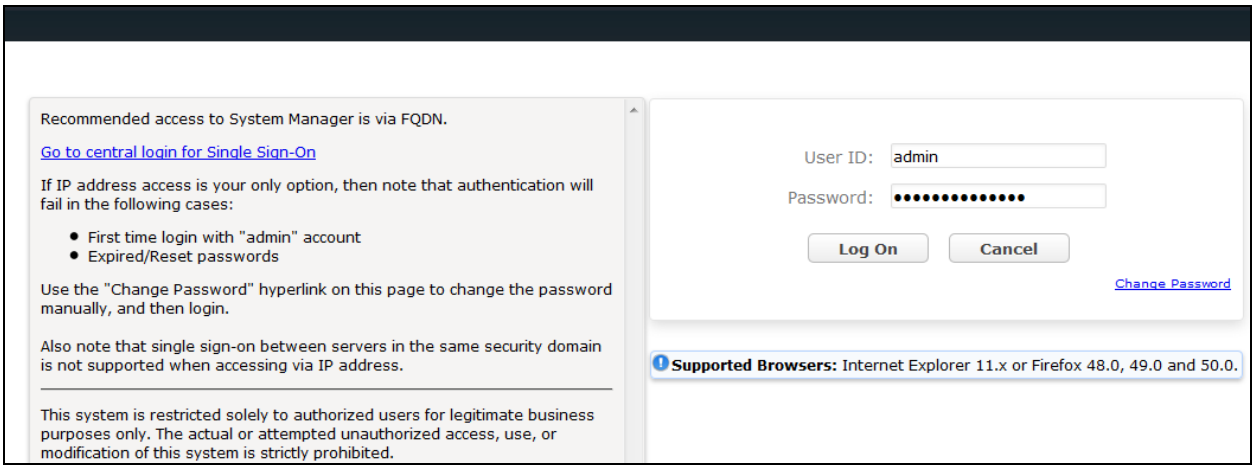
4. Equipment and Software Validated

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

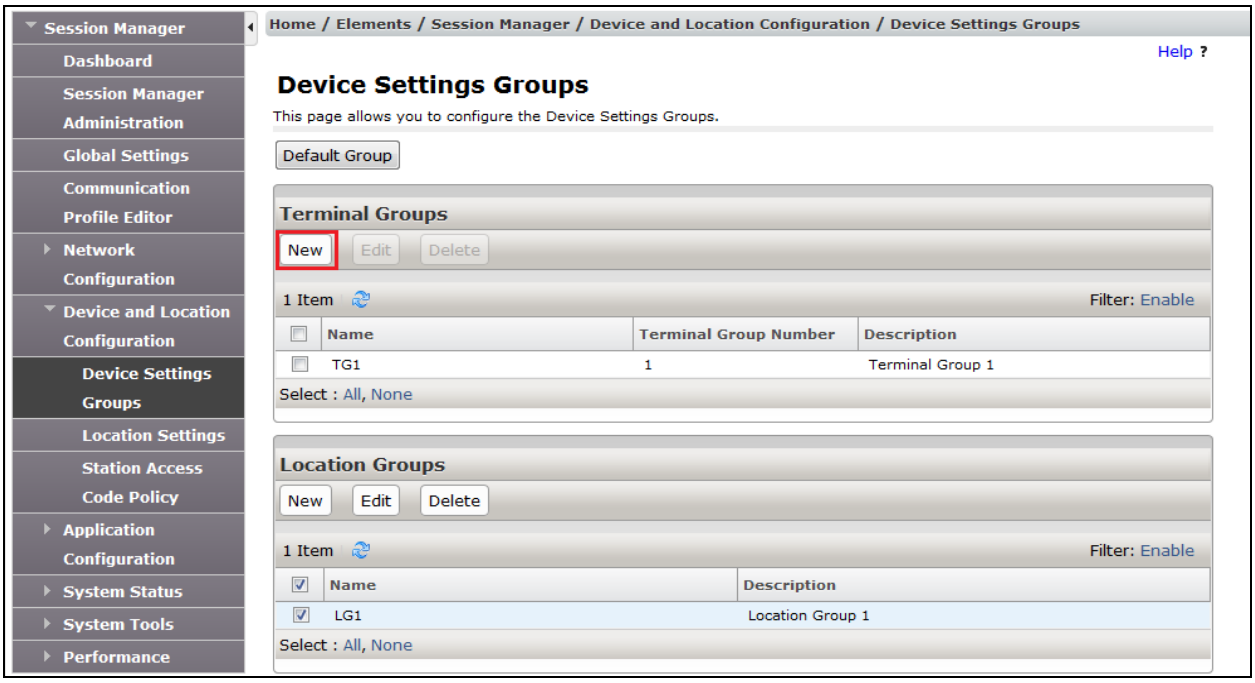
Equipment/Software	Release/Version
Avaya Aura® Communication Manager running on Virtual Environment	7.1.3.0 (7.1.3.0.0.532.24515)
Avaya Aura® Session Manager running on Virtual Environment	7.1.3.0 (7.1.3.0.713014)
Avaya Aura® System Manager running on Virtual Environment	7.1.3.0 (7.1.3.0.037763)
Avaya Aura® Media Server running on Virtual Environment	7.8.0.333
Avaya G450 Media Gateway	39 .12 .0
Avaya Session Border Controller for Enterprise	7.2.2
Avaya Equinox™	3.4.1
Avaya one-X® Communicator	6.2.12.04-SP12
Avaya Telephones 9641GS (H323) 9611G (H323) 9608G (SIP) 9641G (SIP) Avaya Digital 1416 Telephone	 6.6604 6.6604 7.1.3.0.8 7.1.3.0.8 FW1
Nectar's Unified Communication Management Platform running on Windows 2012	7.3-CMP7413

5. Configure Avaya Aura® Session Manager

The configuration of Session Manager is configured through System Manager, to access the System Manager web interface by using the URL "https://ip-address" in an Internet browser window, where "ip-address" is the IP address of System Manager. Log in using the appropriate credentials.



Select **Session Manager** from the **Elements** section (not shown) and navigate to **Device and Location Configuration → Device Settings Groups** in the navigation panel on the left and click the **New** button to add a **Terminal Group**.



On the subsequent page enter the following:

General Section

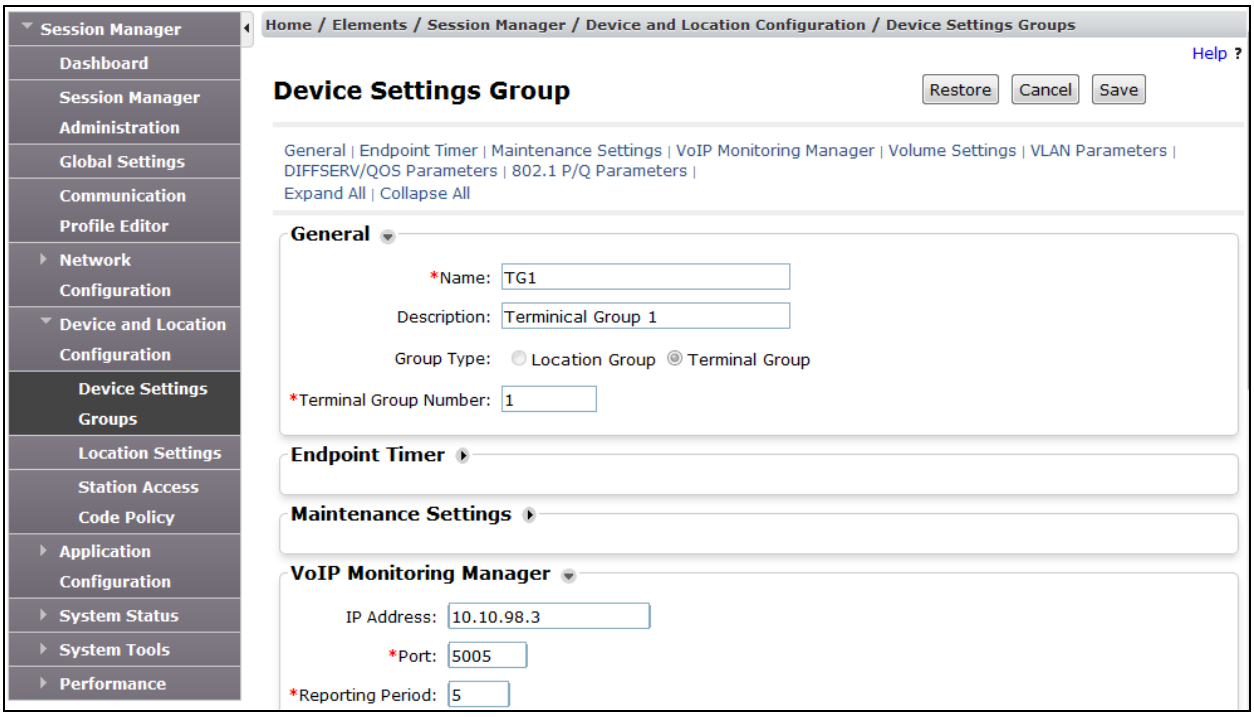
- **Name** Enter an appropriate name
- **Terminal Group** Click the radio button
- **Terminal Group Number** Enter an appropriate Terminal Group Number

Note: The Terminal group number needs to be configured on each telephone to be monitored using the **Group procedure**. The actual procedure is outside the scope of these Application Notes.

VoIP Monitoring Manager Section

- **IP Address** Enter the IP address of the Nectar UCMP server **10.10.98.3**
- **Port** Enter **5005**
- **Reporting Period** Enter **5**

Click **Save** to submit the changes.



In the **Device Settings Groups**, click **New** button in the **Location Groups** to add a new location group.

On the subsequent page enter the following:

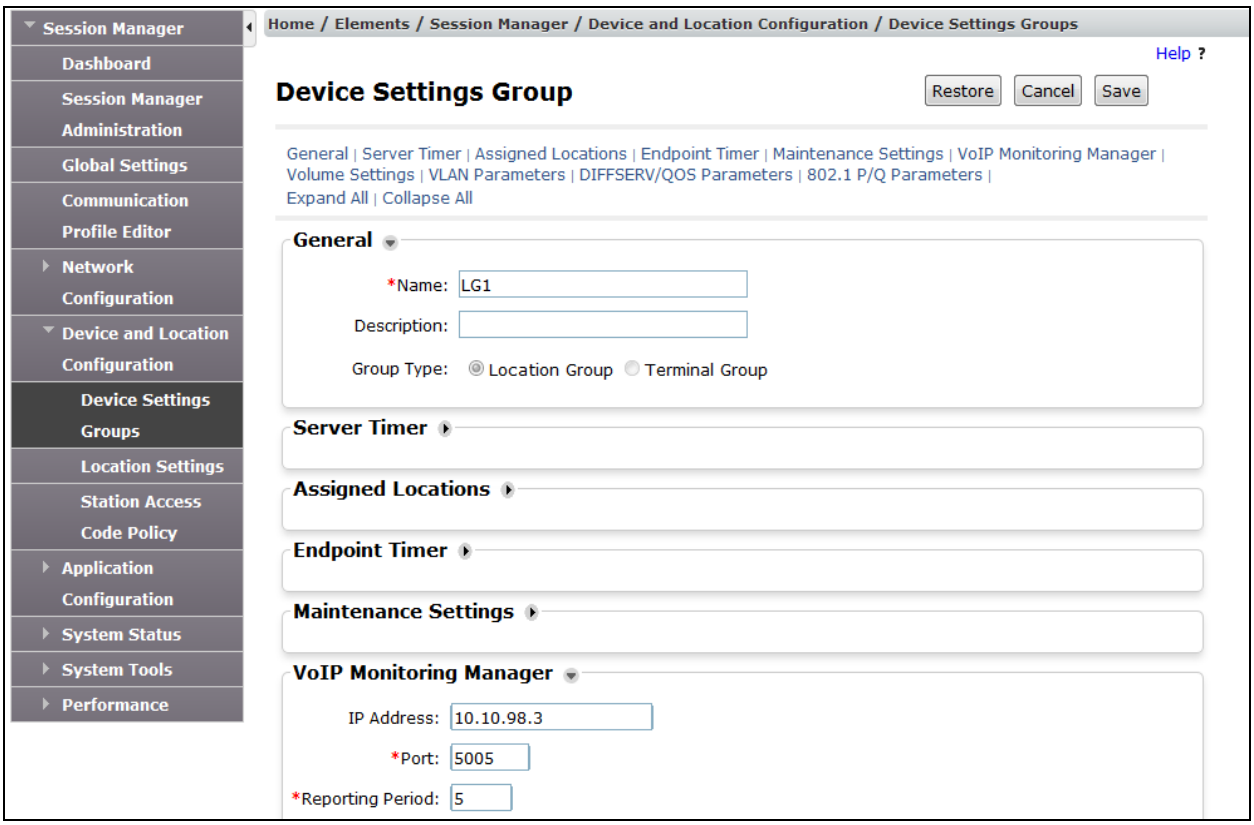
General Section

- **Name** Enter an appropriate name
- **Group Type** Select radio button **Location Group**

VoIP Monitoring Manager Section

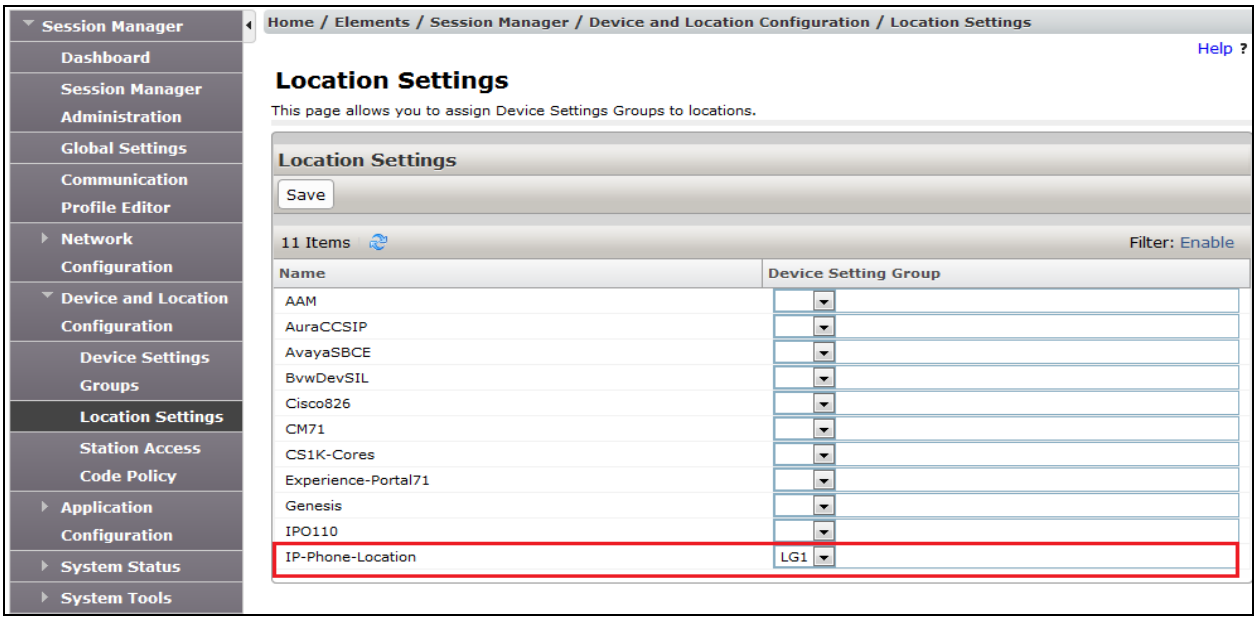
- **IP Address** Enter the IP address of the Nectar UCMP server **10.10.98.3**
- **Port** Enter **5005**
- **Reporting Period** Enter **5**

Click **Save** to submit the changes.



Navigate to **Device and Location Configuration → Location Settings** in the navigation panel on the left and the **Location Settings** is displayed in the right hand side. In the list of Location Settings, select the location group **LG1** configured above in the **IP-Phone-Location** to assign the location group LG1to this location. Note that the **IP-Phone-Location** is previously configured in **Locations** section of **Routing**.

Click on **Save** button to save the change.

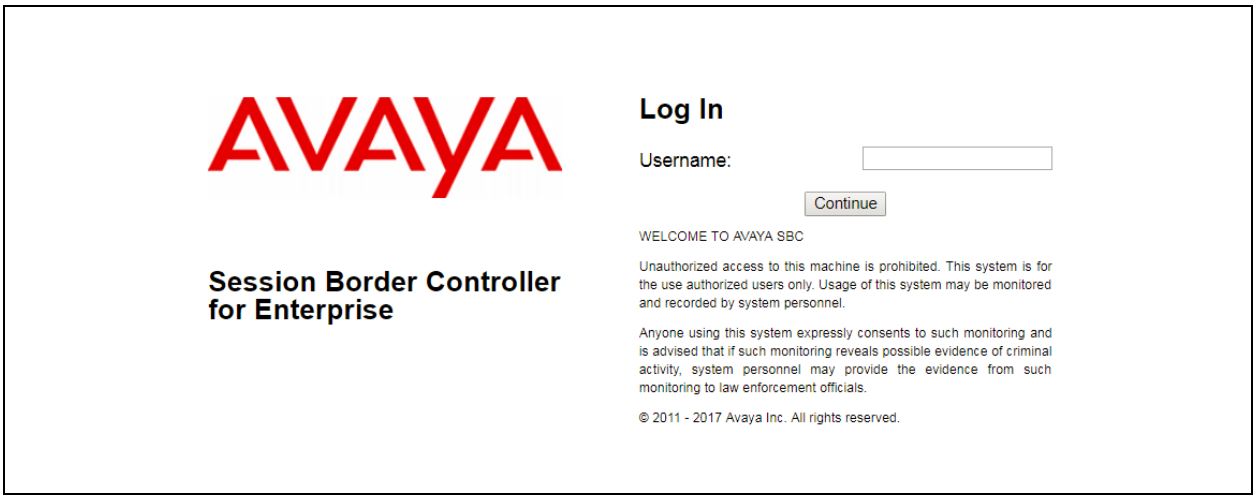


6. Configure Avaya Session Border Controller for Enterprise

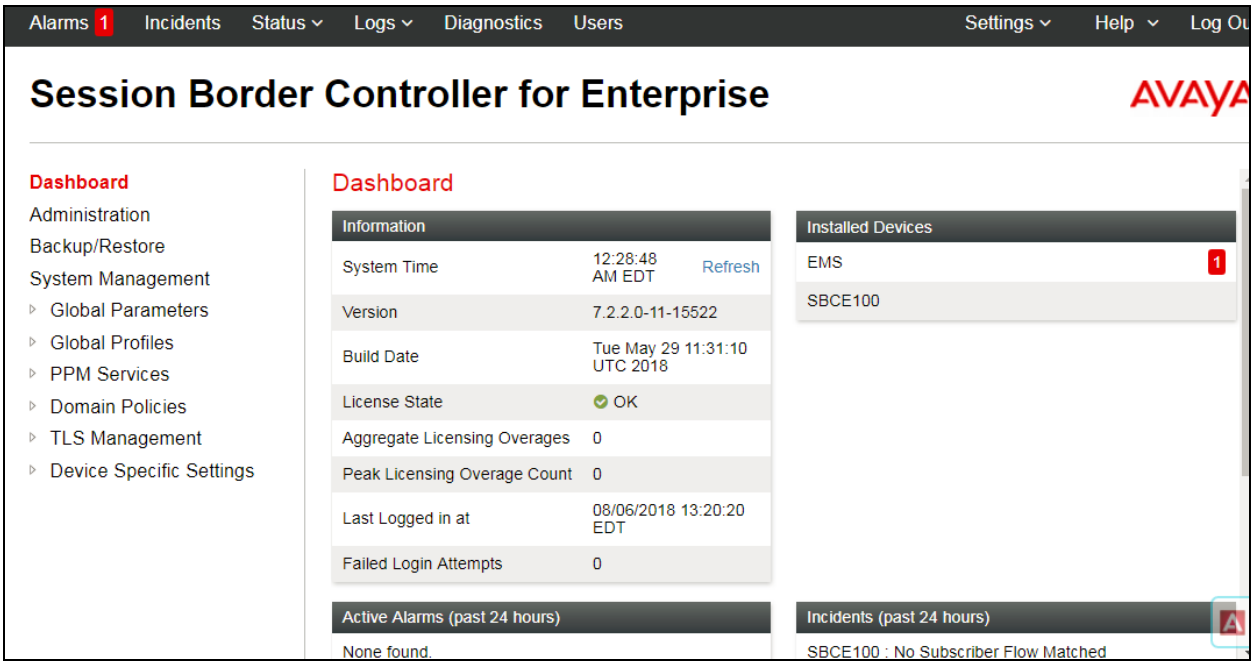
This section describes the RTCP configuration for remote worker SIP endpoint registering to Session Manager through Avaya SBCE. It is assumed that the initial installation of the Avaya SBCE, the assignment of the management interface IP Address and license installation have already been completed; hence these tasks are not covered in these Application Notes. For more information on the installation and initial provisioning of the Avaya SBCE consult the Avaya SBCE documentation in the **Additional References** section.

6.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.

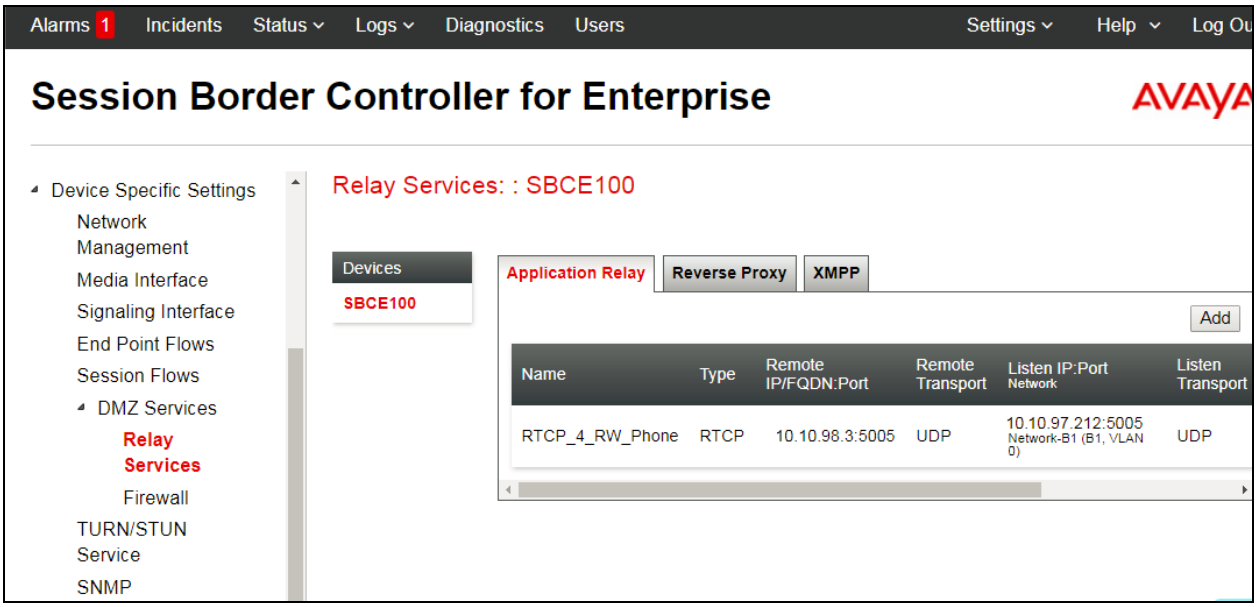


Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE. Verify that the status of the **License State** field is **OK**, indicating that a valid license is present. Contact an authorized Avaya sales representative if a license is needed.

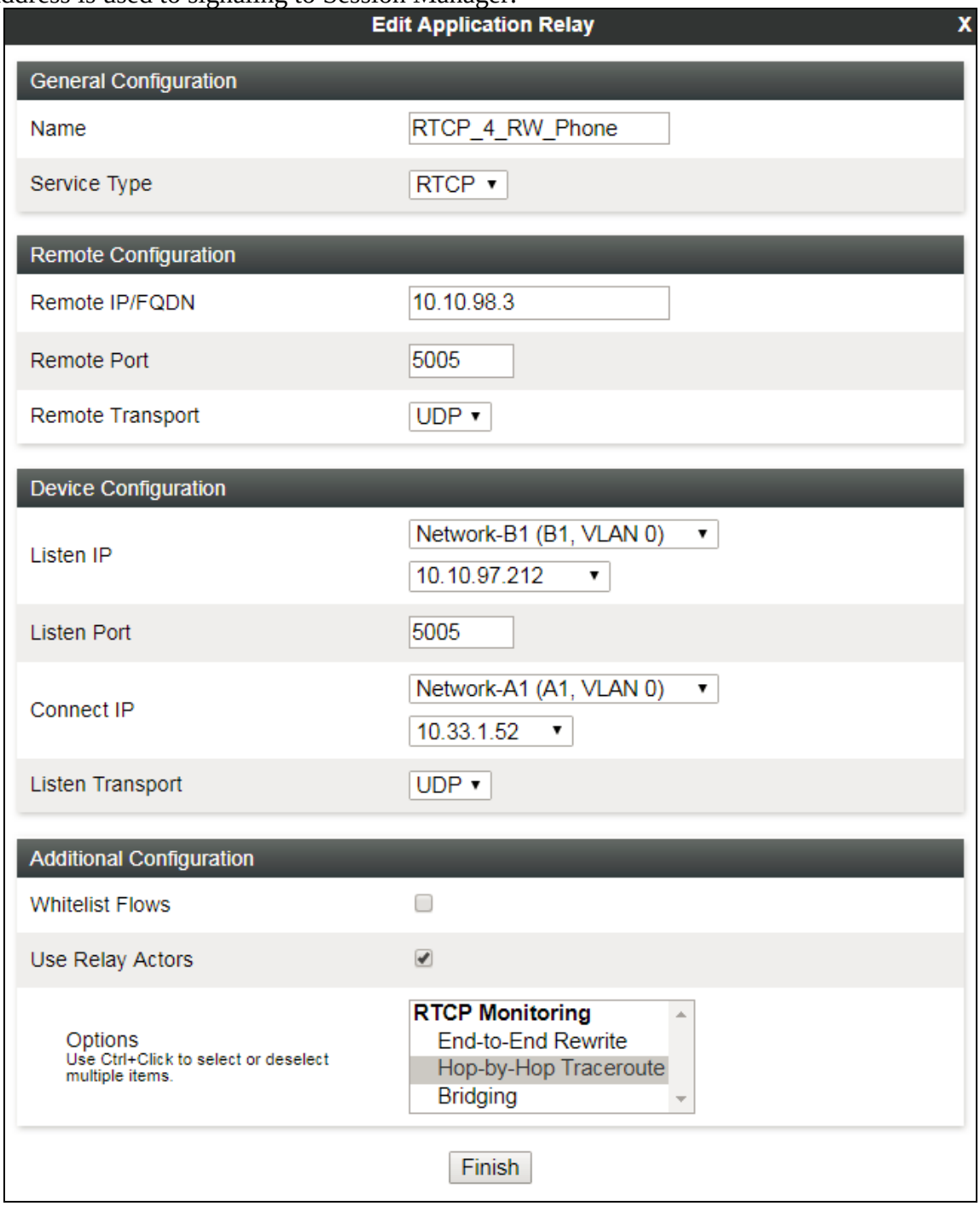


6.2. Configure Relay Services for RTCP

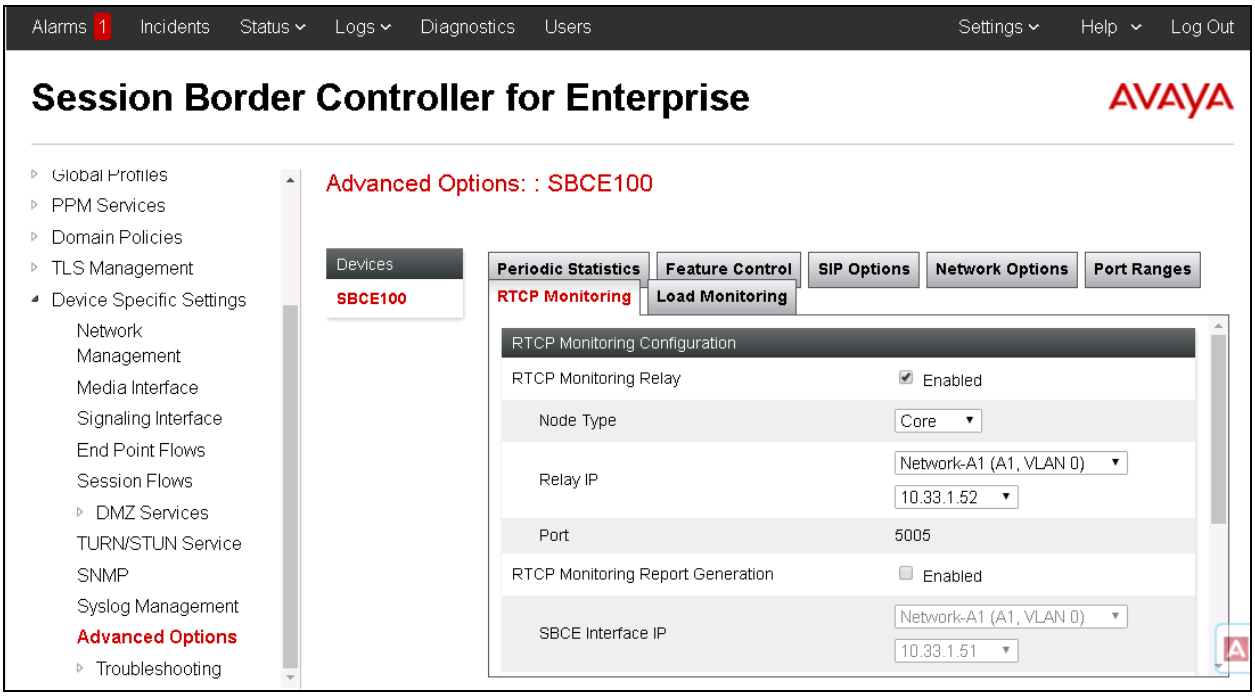
From the left navigation menu, navigate to **Devices Specific Settings → DMZ Services →Relay Services**. The Replay Services portion is displayed in the right hand of the window.



Select **Add** button on the **Application Replay** tab to create a new application. The screenshot below shows all values used in the previously created **Application Relay** for the remote worker SIP endpoint using RTCP service. The remote IP is set to Nectar UCMP server **10.10.98.3**, the **Listen IP** is set to public IP address of Avaya SBCE **10.10.97.212** which SIP endpoint uses as SIP proxy IP address and the **Connect IP** is set to private of Avaya SBCE **10.33.1.52** the private IP address is used to signaling to Session Manager.



Continue to navigate to **Devices Specific Settings → DMZ Services →Advanced Options**. The **Advanced Options** portion is displayed in the right hand of the window. Select the **RTCP Monitoring** tab, in the **RTCP Monitoring Configuration** section checks **Enabled** checkbox on the **RTCP Monitoring Relay**, select **Core** in the **Node Type** and **Relay IP** as the inside IP address **10.33.1.52** as the same as configured above.



6.3. Configure 46xxsettings file for remote worker

The following parameters need to be enabled in the 46xxsetting file for remote worker SIP endpoint.

```
SET RTCPCONT 1
SET RTCPMON 10.10.97.213 (the public IP address of SBCE Relay IP
towards the remote worker SIP phone)
SET RTCPMONPORT "5005"
SET RTCPMONPERIOD 5
```

7. Configure Nectar UCMP

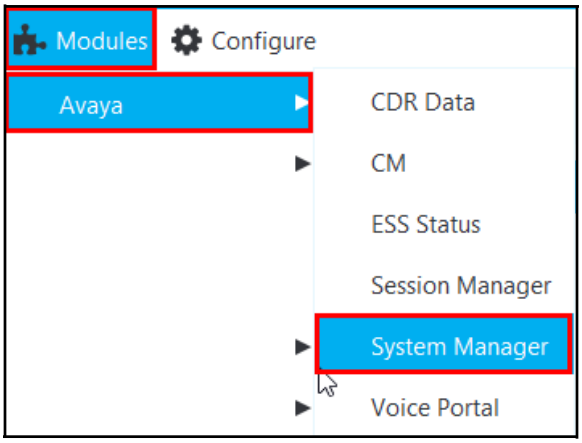
This section describes the configuration required for Nectar UCMP to interoperate with Avaya Aura® Session Manager and Avaya Aura® System Manager. It assumes that the application and all required software components have been installed and properly licensed.

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

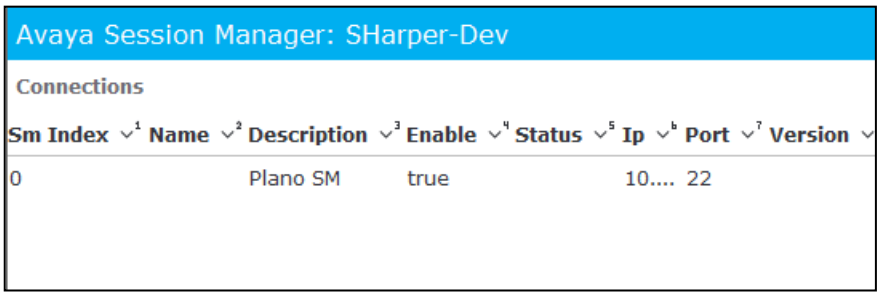
7.1. Add a System Manager Connection

Follow these steps to add a System Manager connection using the VKM:

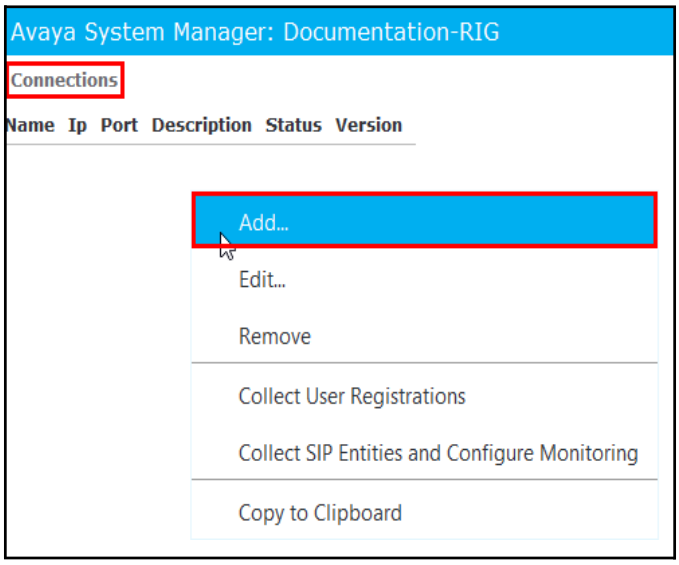
1. Navigate to **Modules** > **Avaya** > **System Manager**.



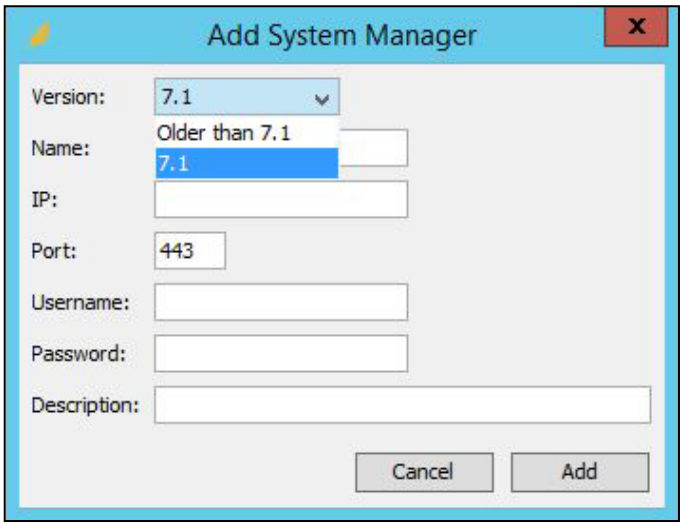
The **Avaya System Manager - Connections** window appears.



2. Right-click in the **Connections** pane and select **Add**.



The **Add System Manager** dialog box appears.



3. Enter the following information.

Field	Enter…
Version	Select the Version that your system is presently using.
Name	Name for the System Manager connection.
IP	IP address of the System Manager connection.
Port	Connection port for the System Manager, such as ***443***, which is the default value.
Username	Username for connecting to the System Manager.
Password	Password associated with the Username.
Description	Description of the System Manager.

4. Click **Add**.

7.2. Collection Verification

After the **System Manager** connection is added, right-click on it and select **View Collections** (graphic not shown) from the drop-down menu.

The list of **Collections** will appear.

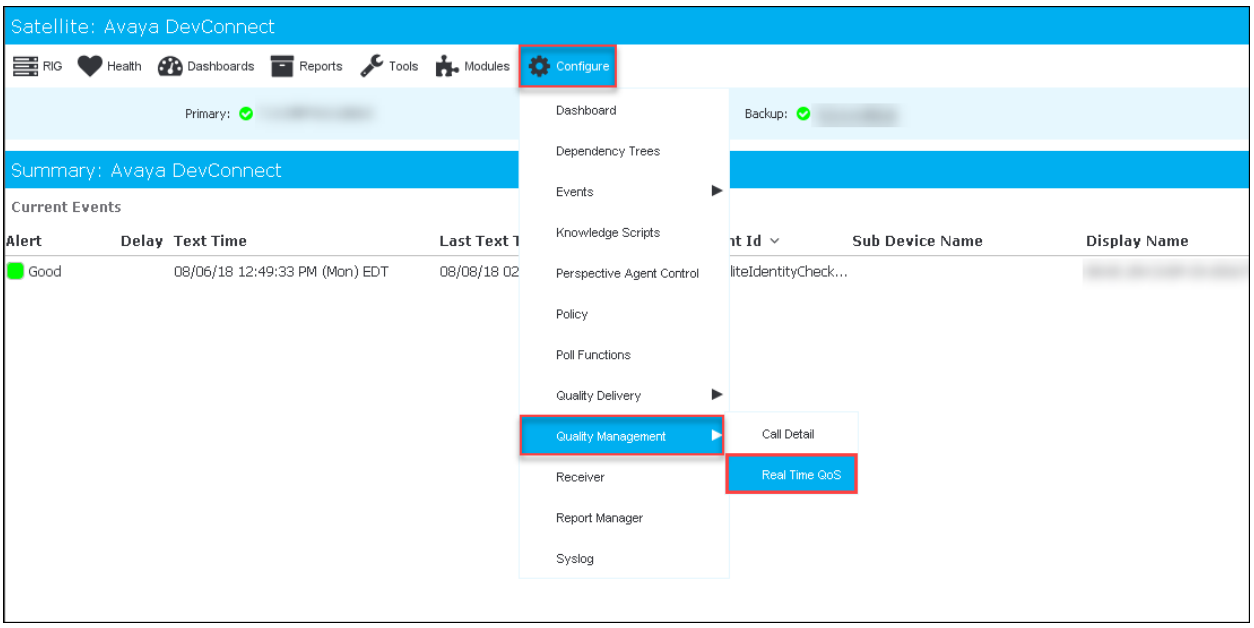
Collections

Name	Enabled	Status	Schedule	Last Execution	Last Execution Duration
Session Manager Status for agent 0	Yes	Success	0 0 0 ? * *	08/01/18 12:00:...	0 min, 1 sec, 057 ms.
Registrations for agent 0	Yes	Success	0 0 * ? * *	08/01/18 03:00:...	0 min, 10 sec, 971 ms.
SIP Entity Links for agent 0	Yes	Success	0 0 0 ? * *	08/01/18 12:00:...	0 min, 3 sec, 142 ms.
SIP Entities for agent 0	Yes	Success	0 0 0 ? * *	08/01/18 12:00:...	0 min, 3 sec, 147 ms.
Locations for agent 0	Yes	Success	0 0 0 ? * *	08/01/18 12:00:...	0 min, 1 sec, 793 ms.
ASM Instance for agent 0	Yes	Success	0 0 0 ? * *	08/01/18 12:00:...	0 min, 1 sec, 217 ms.

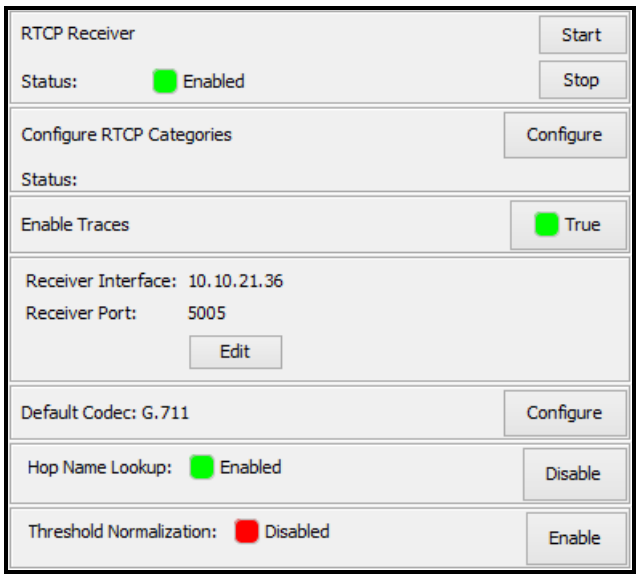
7.3. Configure RTCP

If you are deploying Nectar Real-Time Quality Monitoring, we must enable that functionality. Follow these steps to configure Real Time QoS for your Avaya CM VKM:

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



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



Note: Do not start the receiver module until you have confirmed the settings described below.

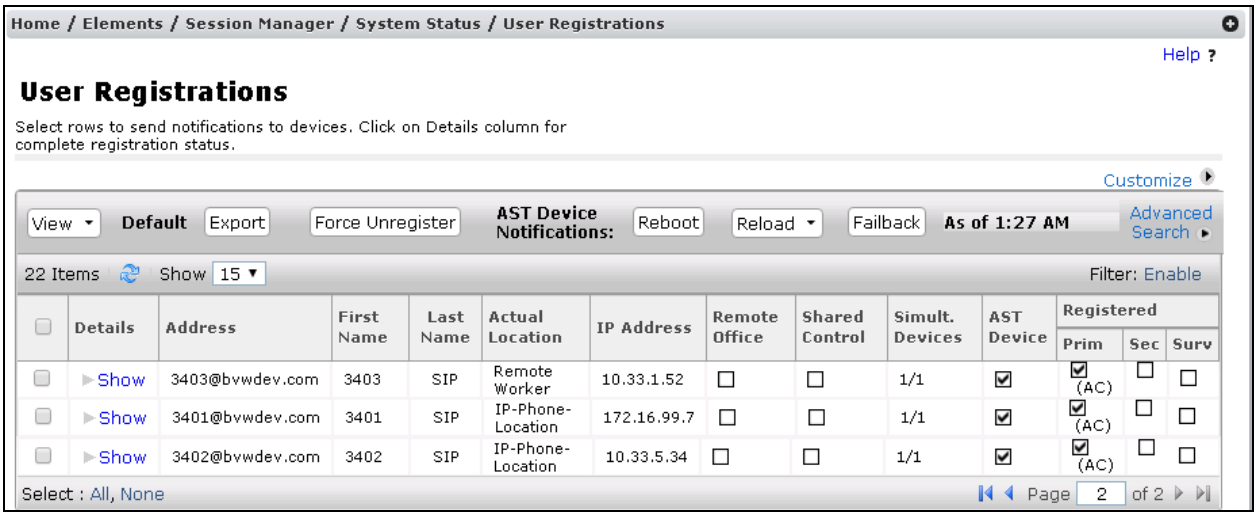
2. Configure the **RTCP Categories**.
    a. Press Configure. This is related to Communication Manager IP-network-regions and presumes that you are currently integrated to and monitoring the Communication Manager system.
3. Set **Enable Traces** to **True**.
4. Set **Receiver Interface** to the RIG IP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

8. Verification Steps

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

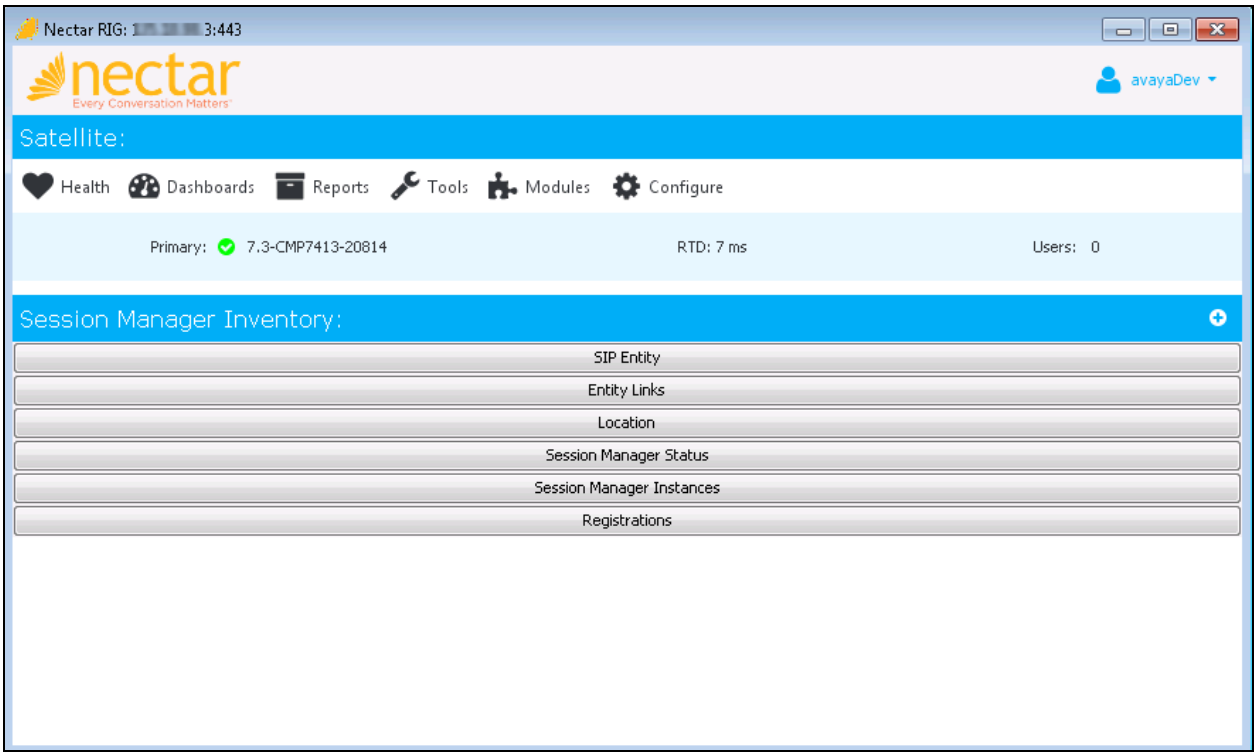
8.1. Verify SIP Endpoints on Session Manager

From the home page of System Manager, navigate to **Elements → Session Manager →System Status → User Registrations**. The **User Registrations** section is displayed in the right hand of the window, there are 3 SIP endpoints register to Session Manager shown in the list and have its actual location displayed in the Actual Location column. The SIP 3403 registers to Session Manager through Avaya SBCE having the private IP address of SBCE 10.33.1.52 and the actual location as Remote Worker.

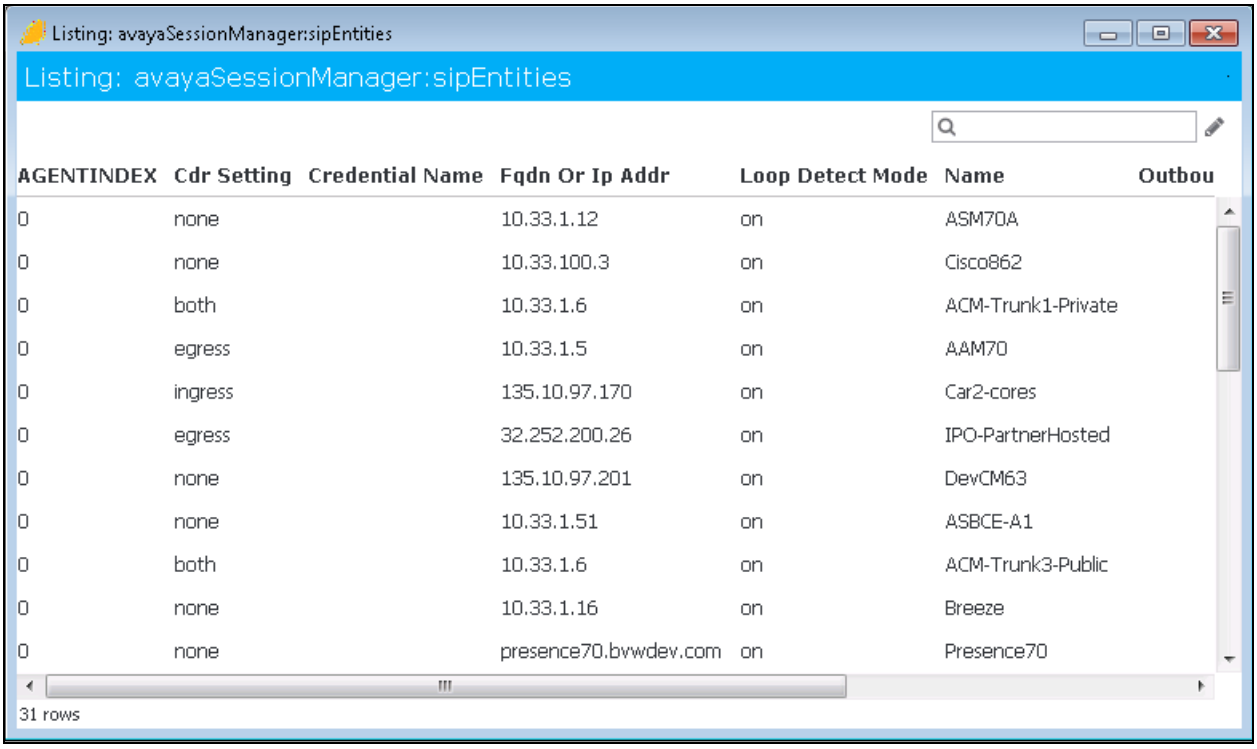


8.2. Verify Inventory of Session Manager on Nectar RIG client

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



Click on **SIP Entity**.

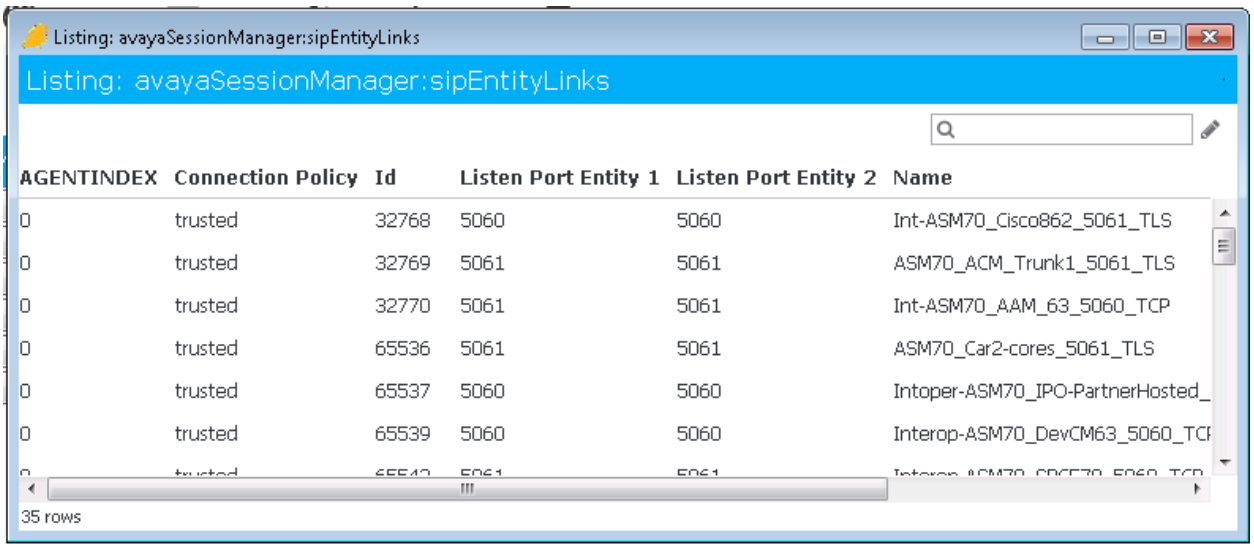


Listing: avayaSessionManager:sipEntities

AGENTINDEX	Cdr Setting	Credential Name	Fqdn Or Ip Addr	Loop Detect Mode	Name	Outbou
0	none		10.33.1.12	on	ASM70A	
0	none		10.33.100.3	on	Cisco862	
0	both		10.33.1.6	on	ACM-Trunk1-Private	
0	egress		10.33.1.5	on	AAM70	
0	ingress		135.10.97.170	on	Car2-cores	
0	egress		32.252.200.26	on	IPO-PartnerHosted	
0	none		135.10.97.201	on	DevCM63	
0	none		10.33.1.51	on	ASBCE-A1	
0	both		10.33.1.6	on	ACM-Trunk3-Public	
0	none		10.33.1.16	on	Breeze	
0	none		presence70.bvwdev.com	on	Presence70	

31 rows

Click on **Entity Links**.



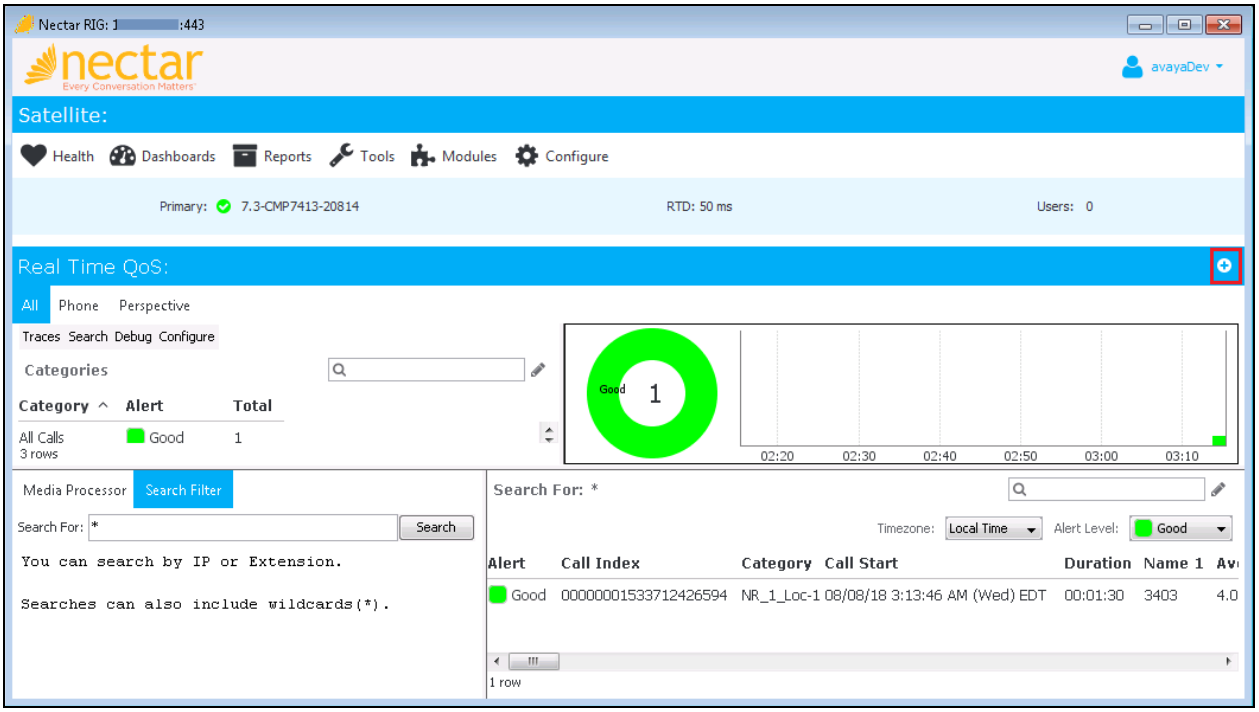
Listing: avayaSessionManager:sipEntityLinks

AGENTINDEX	Connection Policy	Id	Listen Port Entity 1	Listen Port Entity 2	Name
0	trusted	32768	5060	5060	Int-ASM70_Cisco862_5061_TLS
0	trusted	32769	5061	5061	ASM70_ACM_Trunk1_5061_TLS
0	trusted	32770	5061	5061	Int-ASM70_AAM_63_5060_TCP
0	trusted	65536	5061	5061	ASM70_Car2-cores_5061_TLS
0	trusted	65537	5060	5060	Intoper-ASM70_IPO-PartnerHosted_
0	trusted	65539	5060	5060	Interop-ASM70_DevCM63_5060_TCI

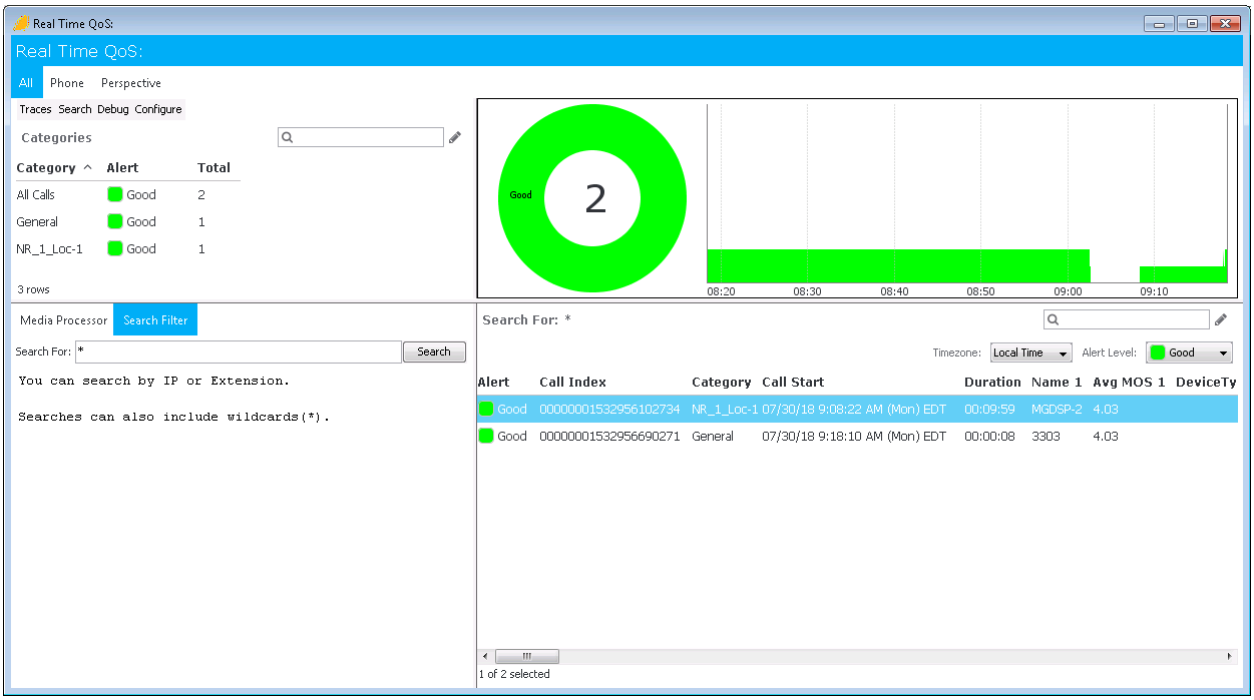
35 rows

8.3. Verify RCTP on Nectar RIG client

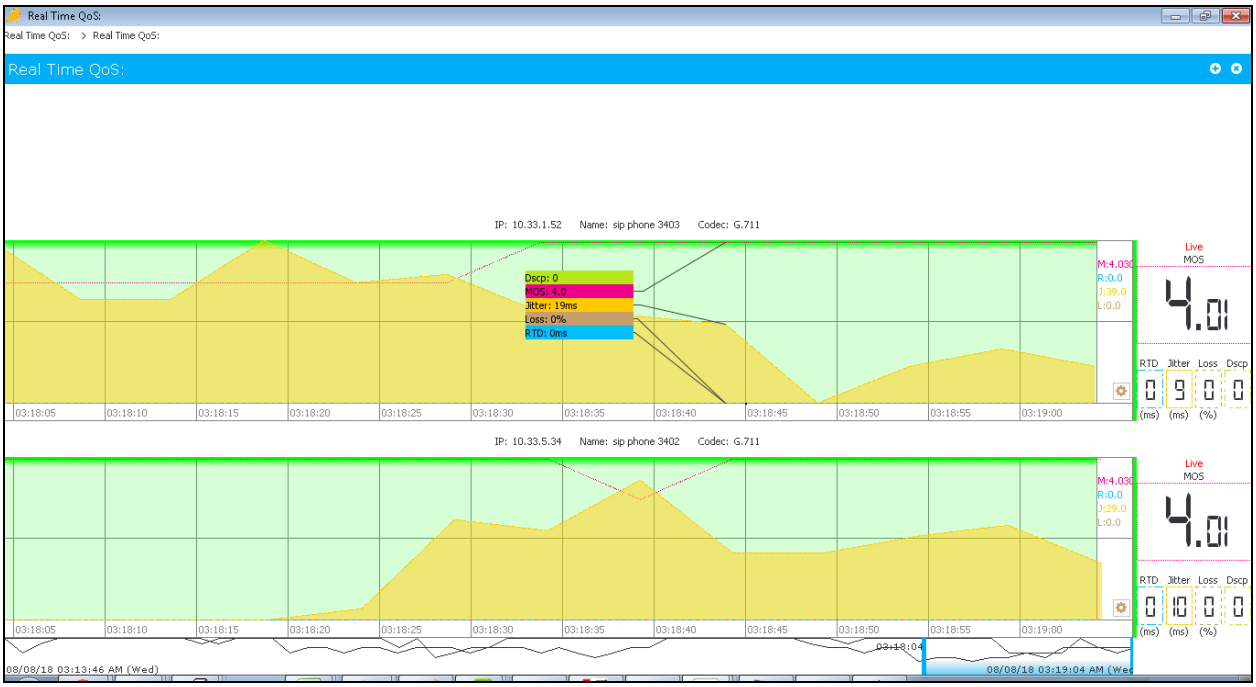
On the Nectar RIG client, navigate to **Health → Quality Management → Real Time QoS** (not shown), the **Real Time QoS** portion displays below the main menu. To open the **Real Time QoS** in a separate window, click on the plus sign (+) on the right side.



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



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



9. Conclusion

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

10. Additional References

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

[1] Administering Avaya Aura® Communication Manager (Release 7.1.2, Issue 5, February 2018)

[2] Administering Network Connectivity on Avaya Aura® Communication Manager (Release 7.1.1, Issue 2, August 2017), 555-233-504

[3] Avaya Aura® Communication Manager Feature Description and Implementation (Release 7.1.2, Issue 4, January 2018)

[4] Avaya Aura® Communication Manager Screen Reference (Release 7.1.1, Issue 2, August 2017), 03-602878

[5] Administering Avaya Session Border Controller for Enterprise, Issue 10 June 2018

[6] Administering Avaya Aura® Session Manager (Release 7.1.2, Issue 3, December 2017)

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

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.