Avaya Solution & Interoperability Test Lab

Application Notes for Nectar Converged Management Platform with Avaya Aura® Communication Manager - Issue 1.0

Abstract

These Application Notes describe the configuration procedures required for the Nectar Converged Management Platform to interoperate with Avaya Aura® Communication Manager. Nectar Converged Management Platform is an intelligent platform that converges monitoring and management of the different layers of a network and system infrastructure to provide a unified business service view of an entire application or its delivery system.

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 configuration procedures required for Nectar Converged Management Platform (CMP) to interoperate with Avaya Aura® Communication Manager. The purpose of the testing was to verify that Nectar Converged Management Platform (CMP) recorded each phone call's performance metrics. Nectar Converged Management Platform (CMP) is a Network Management Platform that is delivered as a service. In a converged architecture, the interoperable framework is designed with many individual parts working together for overall network functionality. Nectar Converged Management Platform (CMP) is an intelligent platform that converges monitoring and management of the different layers of a network and system infrastructure to provide a unified business service view of an entire application or its delivery system, regardless of how many parts it is composed of.

2. General Test Approach and Test Results

The general approach was to place various types of calls to and from stations, collect VoIP call quality data from Nectar CMP, and compare collected values with Avaya IP telephone's Network Audio Quality values. For feature testing, the types of calls included internal calls, inbound trunk calls, outbound trunk calls, transferred calls, conferenced calls. During the compliance test, a VoIP impairment tool was utilized to simulate VoIP delay and packet drop. For serviceability testing, failures such as cable pulls and resets were applied. Verification of each call was made by performing queries into the Nectar CMP meta data, and looking at the results recorded in the Nectar CMP internal logs.

2.1. Interoperability Compliance Testing

The interoperability compliance testing included feature and serviceability testing. The feature testing evaluated the ability of Nectar CMP to provide quality of calls placed to and from stations. The serviceability testing introduced failure scenarios to see if Nectar CMP can resume monitoring and recording after failure recovery. Hardware failures were generated in order to confirm the ability of Nectar CMP to collect SNMP alarms and use SAT commands to get further details about hardware outages.

2.2. Test Results

Nectar CMP successfully provided VoIP call quality data on various types of calls. For serviceability testing, Nectar CMP was able to resume collecting VoIP call quality data after restoration of connectivity to the CLAN, and after resets of Nectar CMP and Avaya Media.

Further, the Nectar CMP solution was able to discover and report on the configuration and health of components in the configured systems including media servers, gateways and boards using the SNMP capabilities of Communication Manager. The Nectar CMP solution successfully reported alarms when resources were taken out of service including SNMP alarms and refined details provided by utilizing automated SAT terminal discovery methods.

2.3. Support

Technical support for the CMP can be obtained by contacting Nectar Support via the support link at http://www.nectarcorp.com/support or by calling support at (888) 8-N-E-C-T-A-R.

3. Reference Configuration

Figure 1 illustrates the network configuration used to verify the Nectar CMP solution. The figure shows two separate communication systems, each running Avaya Aura® Communication Manager on separate Avaya servers. Site A was comprised of an S8300 Server with a G450 Media Gateway, which had 9600 Series IP Telephones registered to it. Site B was comprised of an S8500 Server and two G650 Media Gateways, with 9600 Series IP Telephones registered to it. An IP trunk connected the two Avaya Aura® Communication Manager systems. A Nectar CMP server was located in the Site A, and had IP connection to all devices. A Packet Storm network device was used in various places on the network during the tests in order to inject delays and packet loss to verify phone and Nectar CMP properly measured network performance.

The primary focus of this test was to verify interoperability with Avaya Aura® Communication Manager R6 at Site A. Site B was present primarily for the ability to connect external calls to the endpoints at Site A. The Nectar CMP solution was previously tested with R5 and re-testing was not the focus of this effort. For details on configuration with Communication Manager R5, refer to the *Application Notes for Nectar Converged Management Platform with Avaya Communication Manager dated November, 2008*.

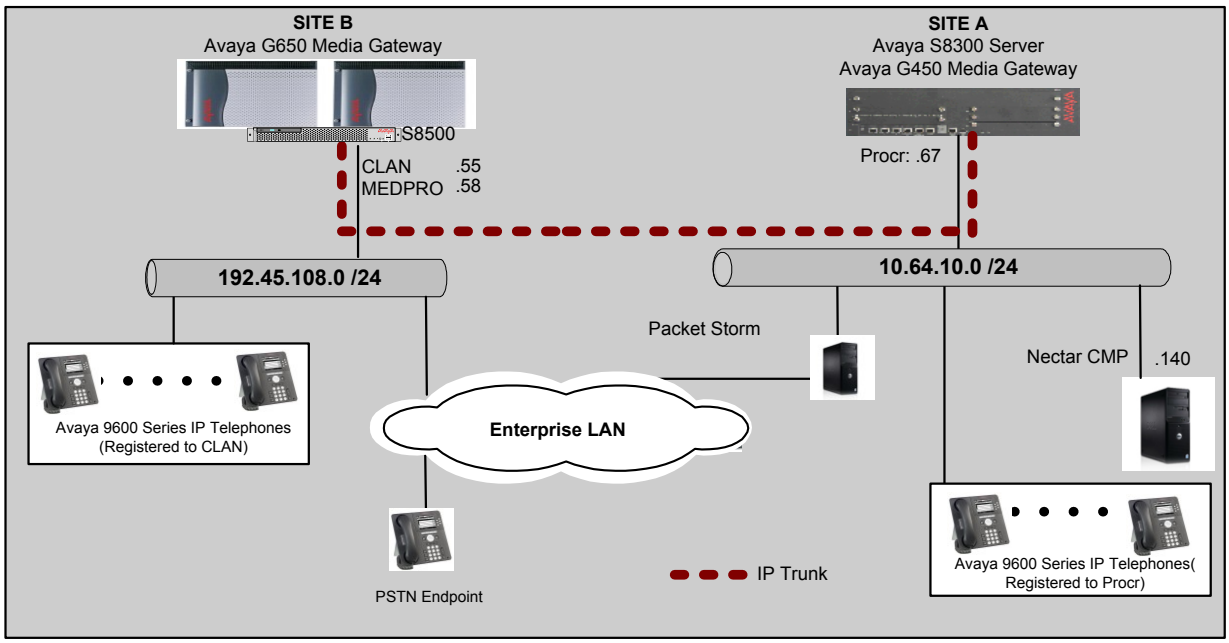


Figure 1 - Test configuration of Nectar CMP with Avaya Aura® Communication Manager

4. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8500 Server		Avaya Aura® Communication Manager 5.2.1 (02.1.016.4) with Patch # 18475
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface TN799DP C-LAN Interface TN2602AP IP Media Processor	HW28 FW040 HW01 FW038 HW02 FW57
Avaya S8300 Server with Avaya G450 Media Gateway		Avaya Aura® Communication Manager 6.0 (R016x.00.0.345.0)
Avaya 9600 Series IP Telephones		
	9630 (H.323) 9650 (H.323)	3.11 3.11
Nectar CMP OS –Windows 2008R2 Server		2.1

5. Configuring Avaya Aura® Communication Manager

Nectar CMP utilizes a combination of the following three methods to collect data for generating a report on VoIP devices.

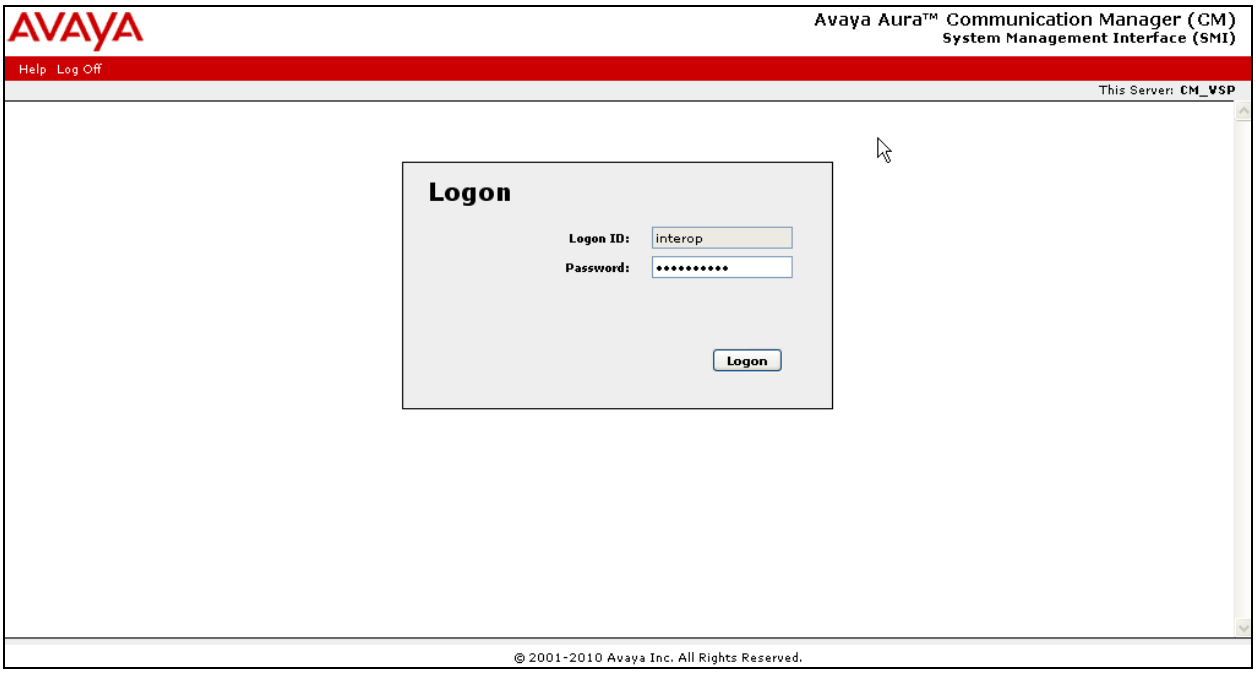
- System Access Terminal (SAT) – Nectar CMP utilizes a SAT connection to collect resource information in Avaya Aura® Communication Manager. In order for Nectar CMP to perform the resource collection, credentials were provided.
- RTCP Monitor Server – Nectar CMP receives RTCP reports from endpoints or media processor (medpro) boards to provide VoIP path and call quality information.
- SNMP/TRAP – Nectar CMP queries Avaya Aura® Communication Manager utilizing SNMP walk, to collect status information. Nectar CMP was set up as a trap receiver, and thus received alarms from Avaya Aura® Communication Manager.

This section provides the procedures used for configuring the above mentioned methods in Avaya Aura® Communication Manager.

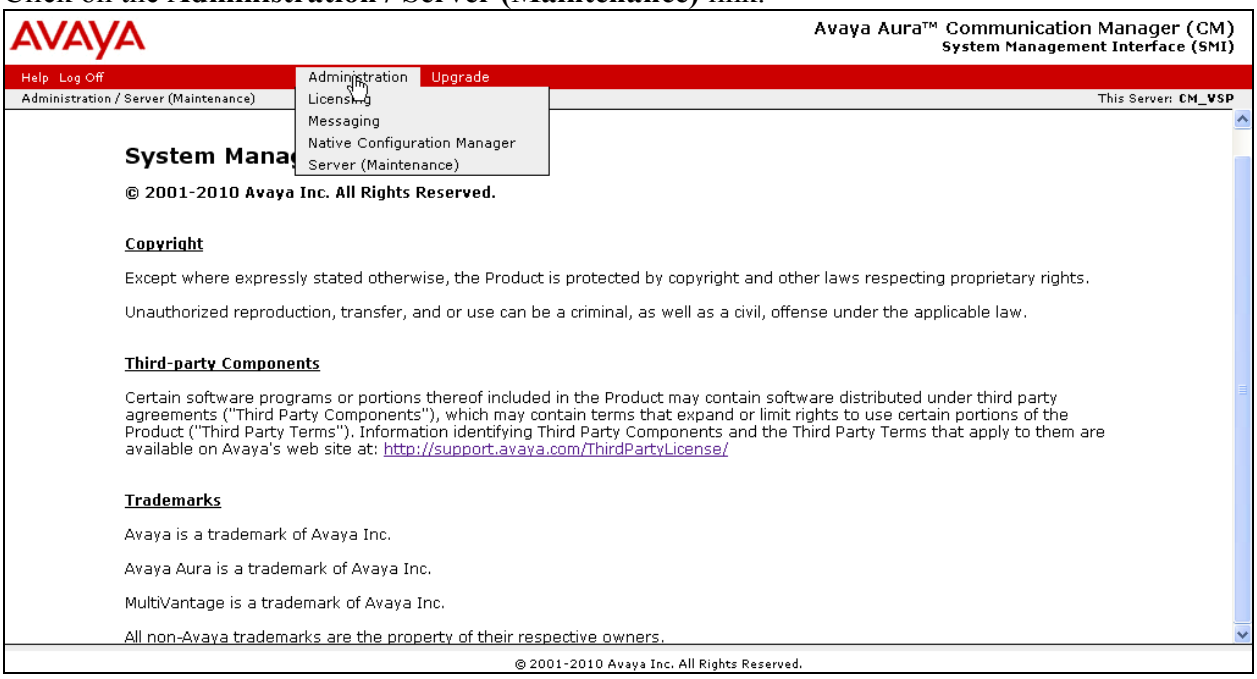
5.1. Configuring System Access Terminal (SAT) Access

This section describes how to create credentials for Nectar CMP to login to a Communication Manager.

Launch a web browser and connect to the Communication Manager by entering https://< IP address>. Supply proper credentials.

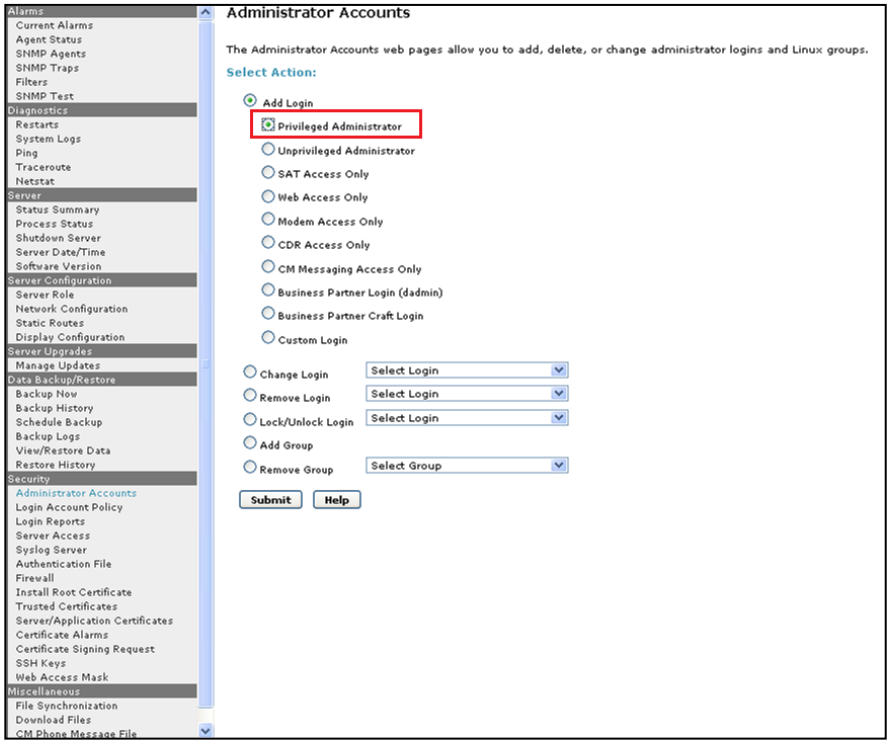


Click on the **Administration / Server (Maintenance)** link.



Click on the **Administrator Accounts** link under the **Security** section on the left pane.

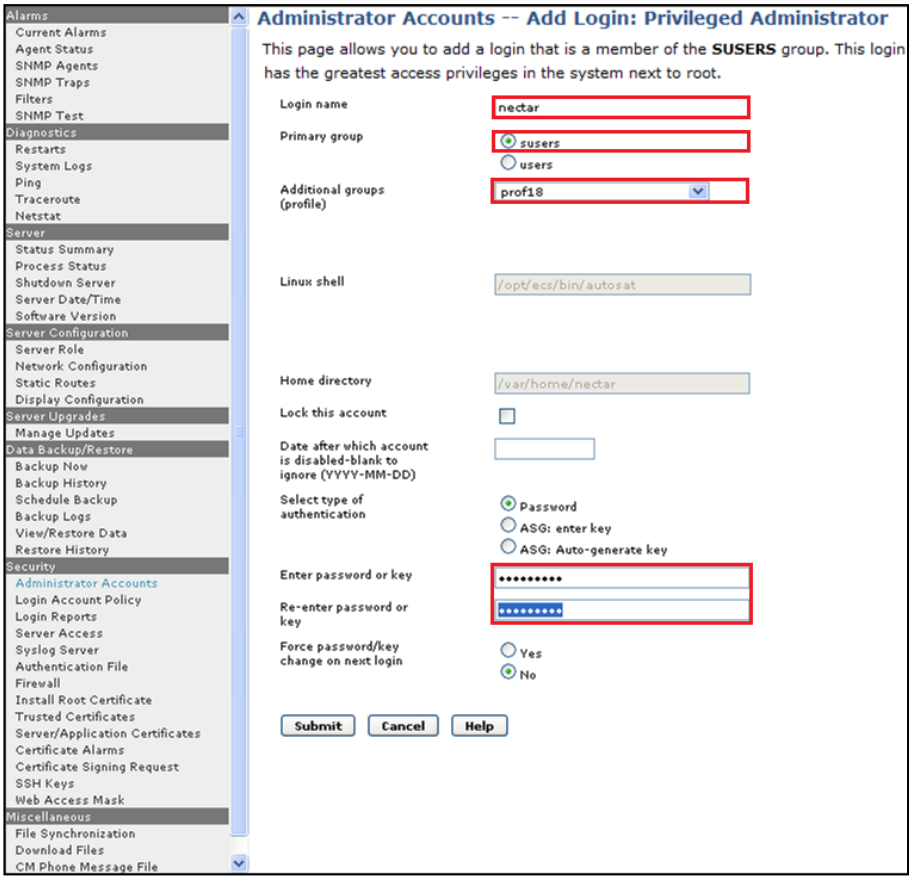
On the **Administrator Accounts** page, select the **Add Login** radio button. Click the **Privileged Administrator** radio button under **Add Login** section. Click on the **Submit** button.



Note: Although Nectar CMP leverages a privileged login, it does not issue any change commands to the Avaya system. The privileged login is required to review critical information associated with distributed gateway and ESS/LSP components of a Communication Manager system.

Provide a **Login name** and select the **susers** radio button under the **Primary group** section. Select '**prof18'** for the **Additional groups** option. Finally, provide a password for the new account in the **Enter password or key** and **Re-enter password or key** fields.

Click on the **Submit** button. Default values may be used in the remaining fields.



5.2. Creating the RTCP Monitor Server

Since Nectar CMP utilizes RTCP packet to calculate and report the call path and quality of the call stream, a RTCP monitor server need to be configured in Communication Manager. The following screen describes the setting of the RTCP monitor server. Login to the SAT and use the **change system-parameters ip-options** command to configure the RTCP monitor server. Provide the following information:

- **Enable Voice/Network Stats?** – Set to **y** to enable RTCP
- **Server IPV4 Address** - IP address of the Nectar CMP server
- **IPV4 Server Port** – Default value of **5005 was used** [This port number must match with the Nectar CMP RTCP Receiver Port configured in **Section 6.1**]
- **RTCP Report Period (secs)** – Default value of **5** was used [The report period indicates Avaya endpoints forward RTCP packet to the RTCP monitor server, which is the Nectar CMP server.]

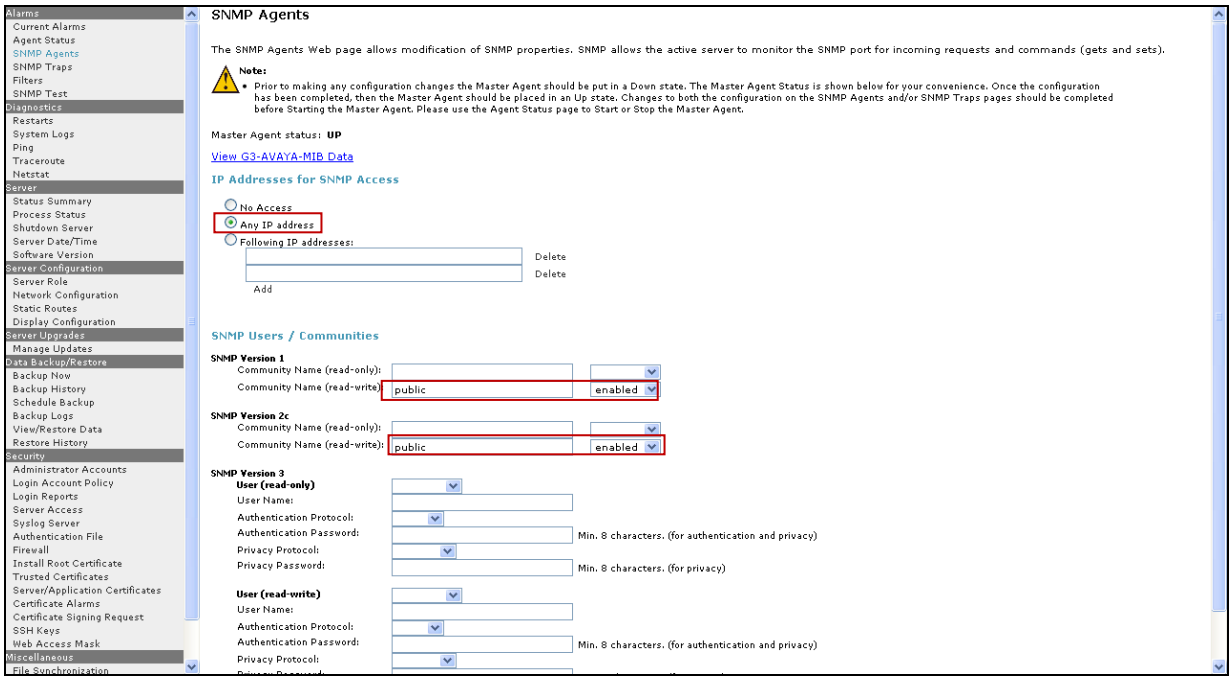
Default values may be used in the remaining fields.

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

 IP MEDIA PACKET PERFORMANCE THRESHOLDS
    Roundtrip Propagation Delay (ms)    High: 800      Low: 400
                    Packet Loss (%)     High: 40       Low: 15
                    Ping Test Interval (sec): 20
    Number of Pings Per Measurement Interval: 10
                  Enable Voice/Network Stats? y
 RTCP MONITOR SERVER
   Server IPV4 Address: 10.64.10.140    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
                                Periodic Registration Timer (min): 20
                              Short/Prefixed Registration Allowed? n
```

5.3. Configuring SNMP / TRAP Agents

For Nectar CMP to query the status information on Communication Manager, the SNMP and TRAP services need to be enabled. Enabling the SNMP service is configured through the Communication Manager's web interface. From the Communication Manager web System Management Interface, Click on the **SNMP Agents** link under the Alarms section, on the left pane, to display the **SNMP Agents** page.

On the **SNMP Agents** page, select the **Any IP Address** radio button under the **IP Addresses for SNMP Access** section. This implies that any device can perform SNMP request to the Communication Manager. Enable **SNMP Version 1** and **SNMP Version 2c** by selecting **enabled** from the list in each of these sections. Set the **Community Name** (read-only) field to **public** on both versions of SNMP. The community name configured here must match entries on the Nectar CMP configuration. Click on the **Submit** button (not shown) at the bottom of the page.



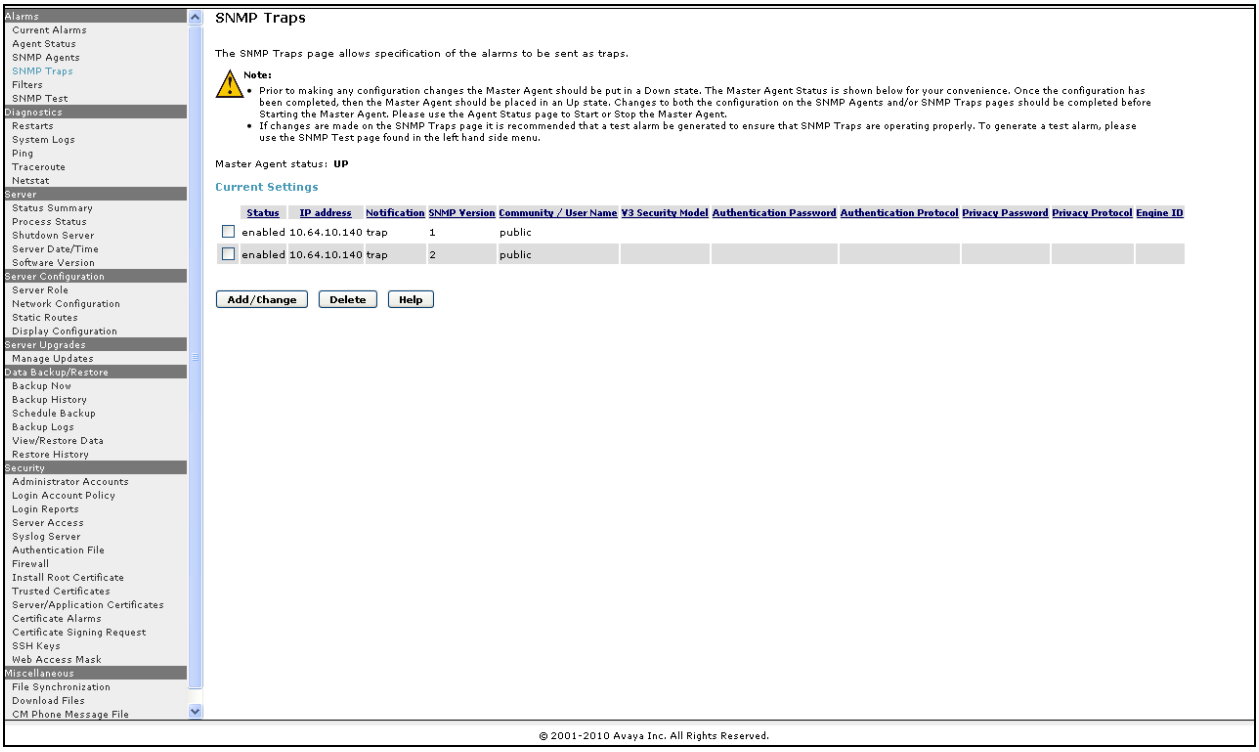
5.3.1. Confirming SNMP / TRAP Firewall Services

The firewall in the Avaya server must allow SNMP on UDP port 161 and SNMPTRAP on UDP port 162. Nectar CMP utilizes this service to obtain health statistics about the Media Server hardware that hosts the Communication Manager software.

In Communication Manager 6 and later, Firewall rules are configured by a privileged user (root for example) as operating system modifications. For this test, no modifications were required to the default configuration. Modifications would be documented in Linux operating system guides and are beyond the scope of these Application Notes.

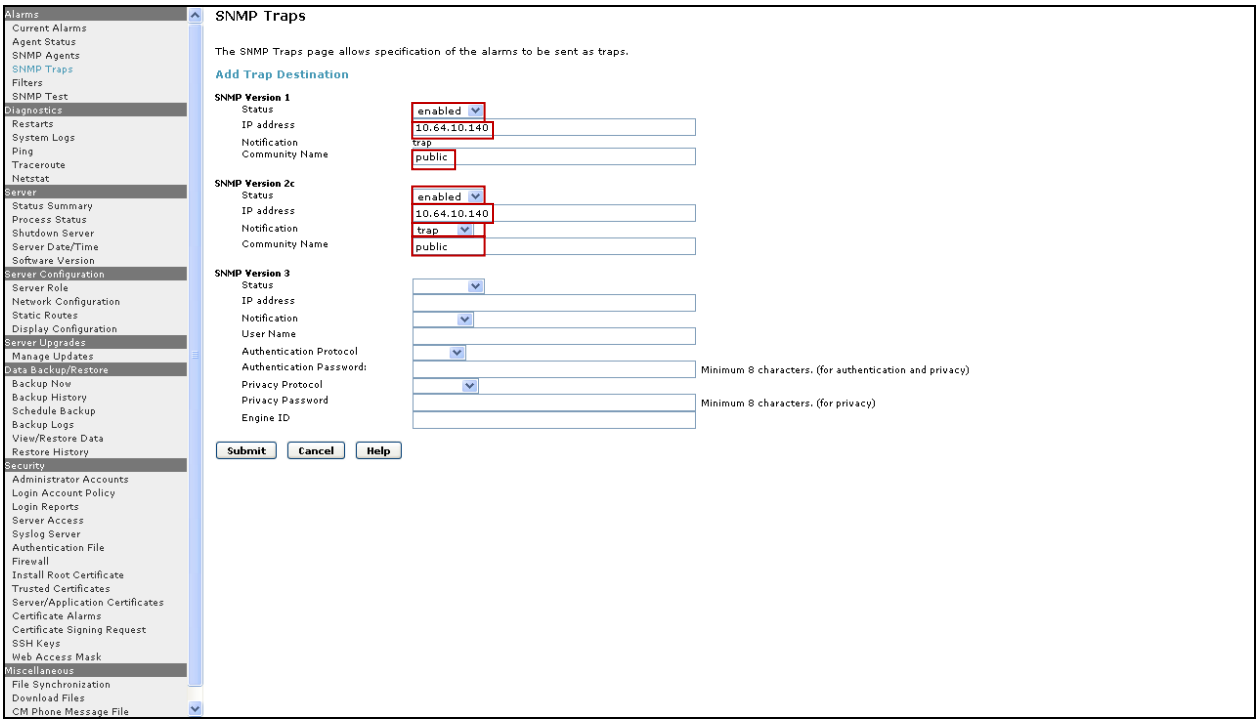
5.3.2. Configure SNMP TRAP Destination

This section describes how to create a trap destination. Navigate to the **SNMP Traps** link under the **Alarms** section. In the screenshot below, the SNMP traps had been configured previously. The following steps will demonstrate the configuration. Click on the **Add/Change** button to configure or modify the SNMP traps.

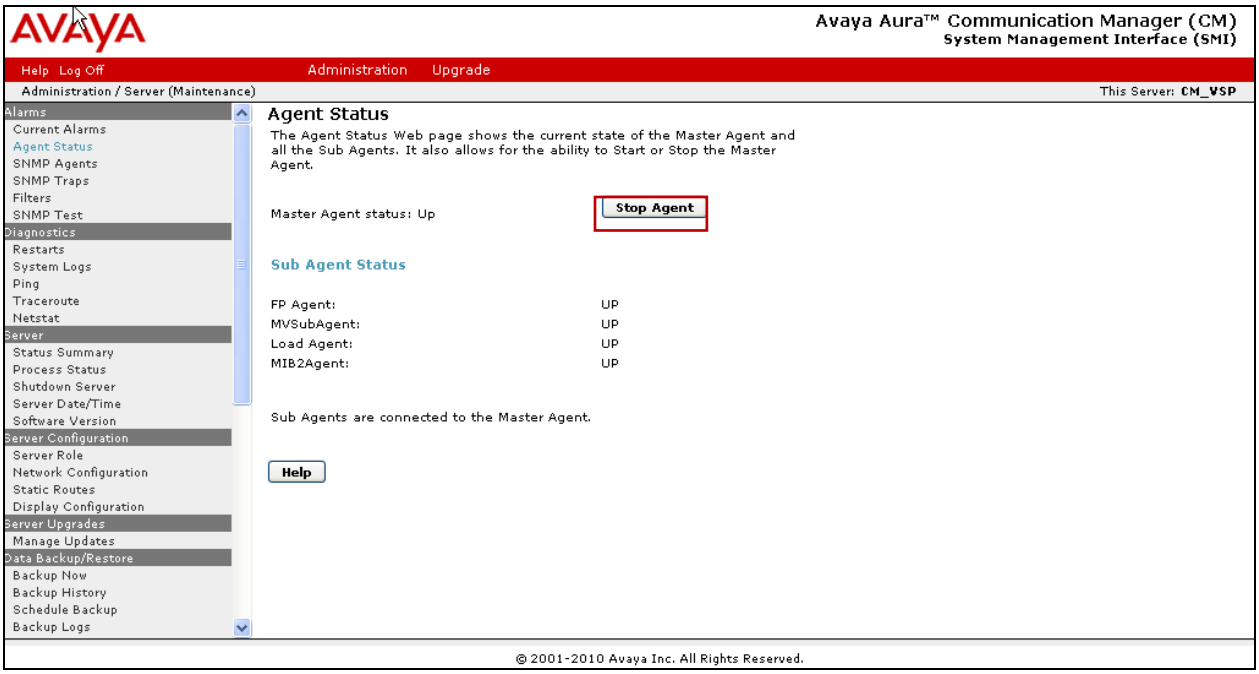


In the **Add Trap Destination** section, in the SNMP Version 1 section, select **enabled** for the **Status** selection and enter the trap destination **IP address** (the Nectar CMP IP Address). Also enter the **Community Name** (**public** was used in the test).

In the **SNMP Version 2c** section, select **enabled** for the **Status** selection and enter the trap destination **IP address** (the Nectar CMP IP Address). Select **trap** for the **Notification** option, and enter the **Community Name** (**public** was used in the test). Click **Submit** to commit these entries.



Before proceeding to the next step, restart the Agent Status (SNMP Stop/SNMP Start) before configuring the trap filter. Click on the **Agent Status** link in the Alarms section on the navigation panel. Stop the SNMP Master Agent by clicking the **Stop Agent** button. After the Master Agent status shows **down**, the **Stop Agent** button will now display **Start Agent**. Click on the **Start Agent** (not shown) button to start the Master Agent.

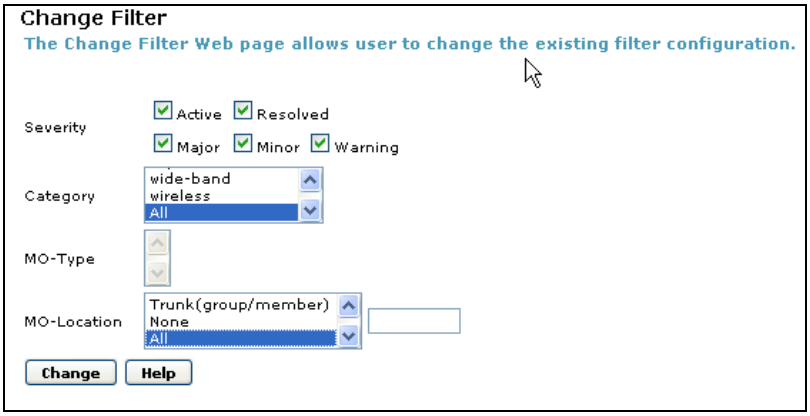


5.3.3. Configure Alarm Filters

Navigate to the **Filters** link under the Alarms section. Click on the **Add** button to add filter associated to the trap message. By default, the Customer Alarm Reporting Options field is set to **Report All Communication Manager alarms**.

In the illustrations below, the Filters were already configured, so the Change option is used below to demonstrate the settings previously configured.

On the **Change Filter** page, all Severity check boxes were checked during the compliance test. Select **All** for the **Category** field. Click on the **Change** button.

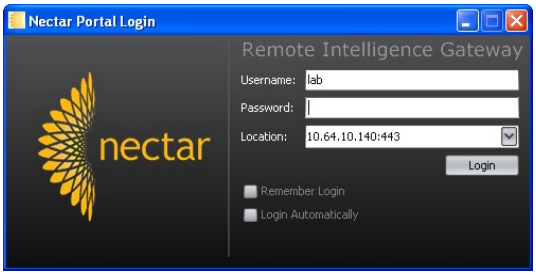


6. Configuring the Nectar CMP Remote Intelligence Gateway

The steps in this section describe the configuration of Nectar CMP that receives RTCP packets from the VoIP endpoint, and recording performance metrics. Additionally, the Communication Manager, and other servers must be administered. For additional information on configuring Nectar CMP, refer to [2], [3] and [4].

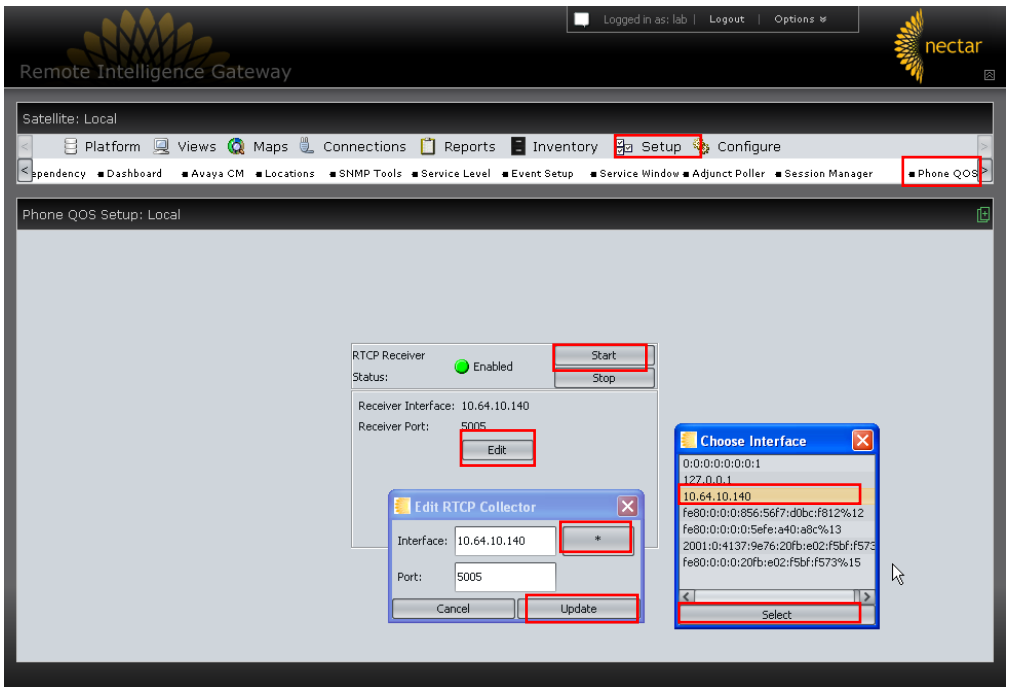
6.1. Configure Nectar CMP to receive RTCP Packets

Launch a web browser and connect to Nectar CMP by entering http://<Nectar CMP IP address> to login to the Nectar Portal Login page. Provide credentials.



Navigate to **Setup >Phone QOS** and edit the RTCP Receiver settings.

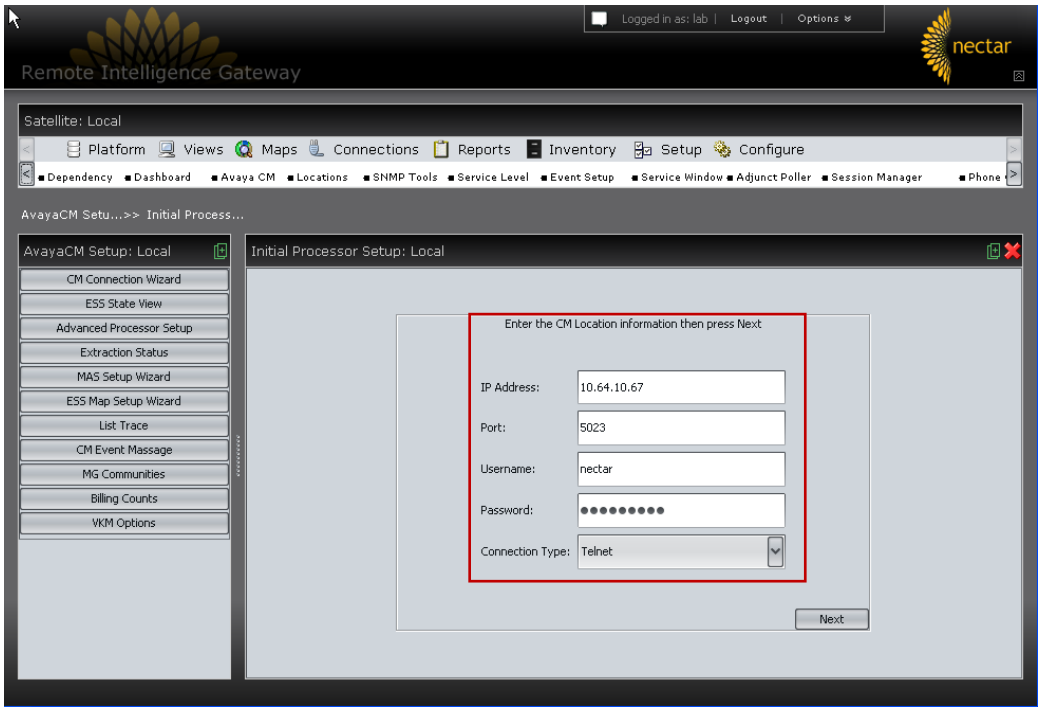
- Click **Edit** to set the **Receiver Interface** and **Receiver Port**.
- Choose the Interface by clicking the * icon, highlighting the address of the server and click on the **Select** button.
- On the **Edit RTCP Collector** dialog, select **Update** to commit the changes.
- Click **Start** to enable the server to start collection RTCP data.



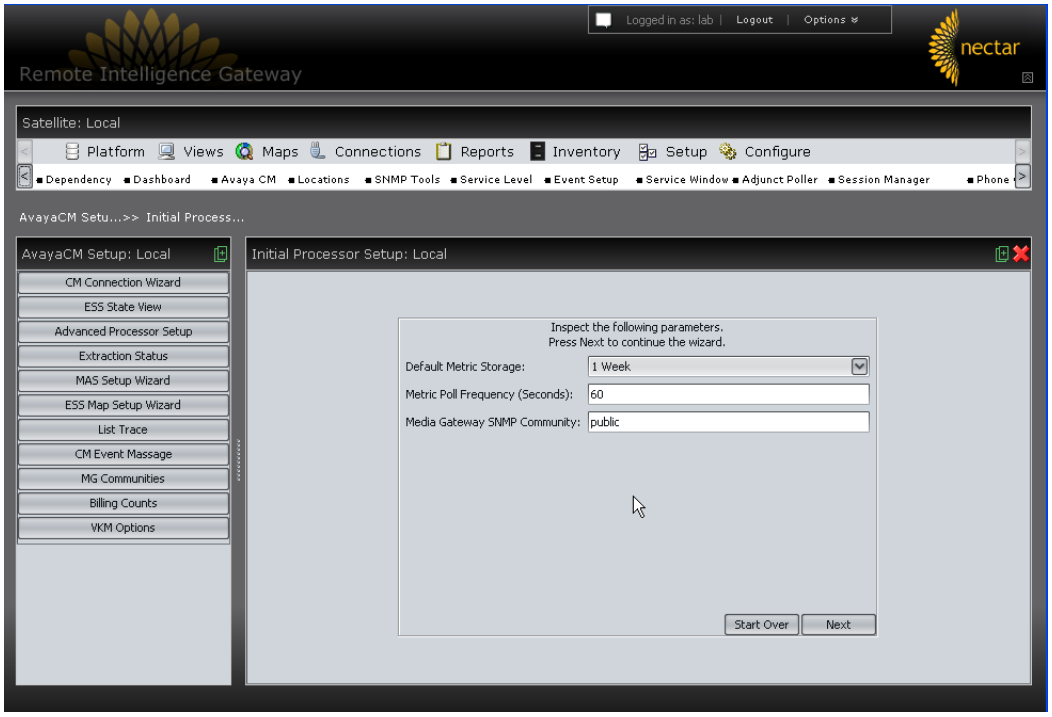
Then press the **Start** button to enable the RTCP receiver.

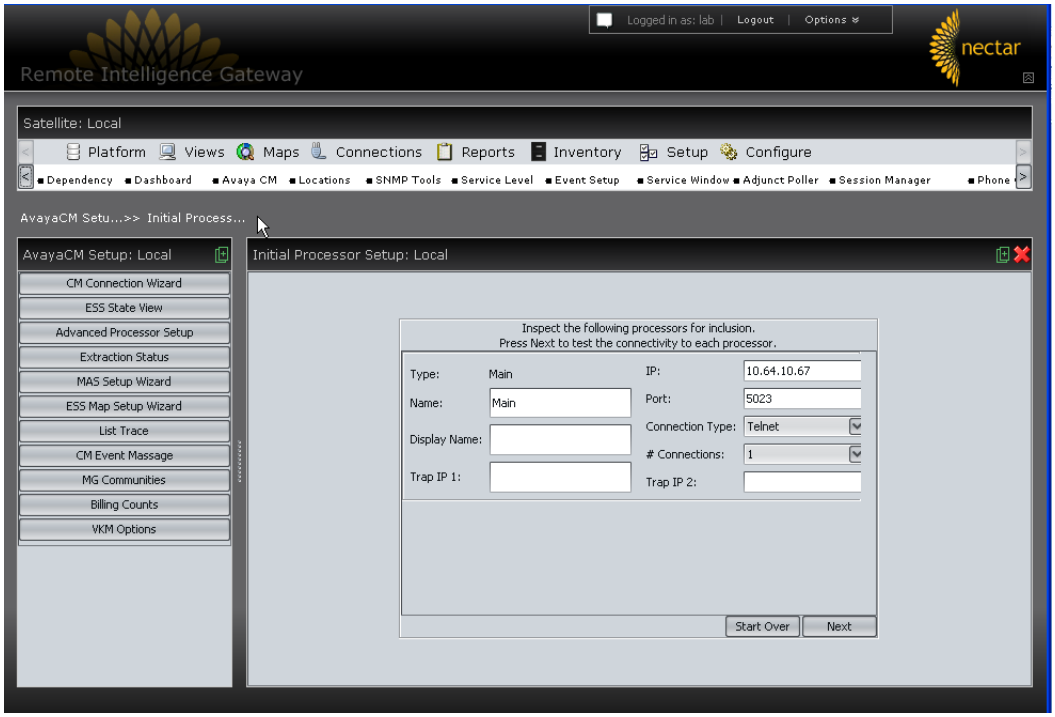
6.2. Add the Communication Manager to the Configuration

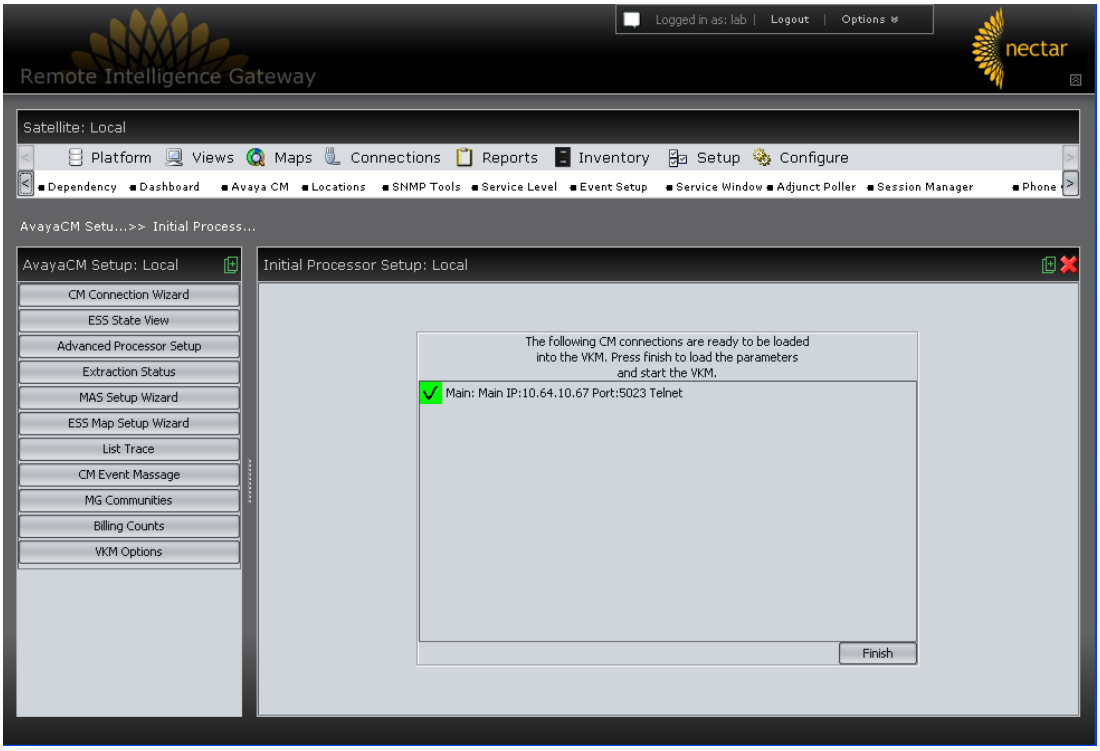
Navigate to **Setup > Avaya CM** to enter the address and login credentials (which must match those created in section 4.1 above). Click **Next** to proceed.

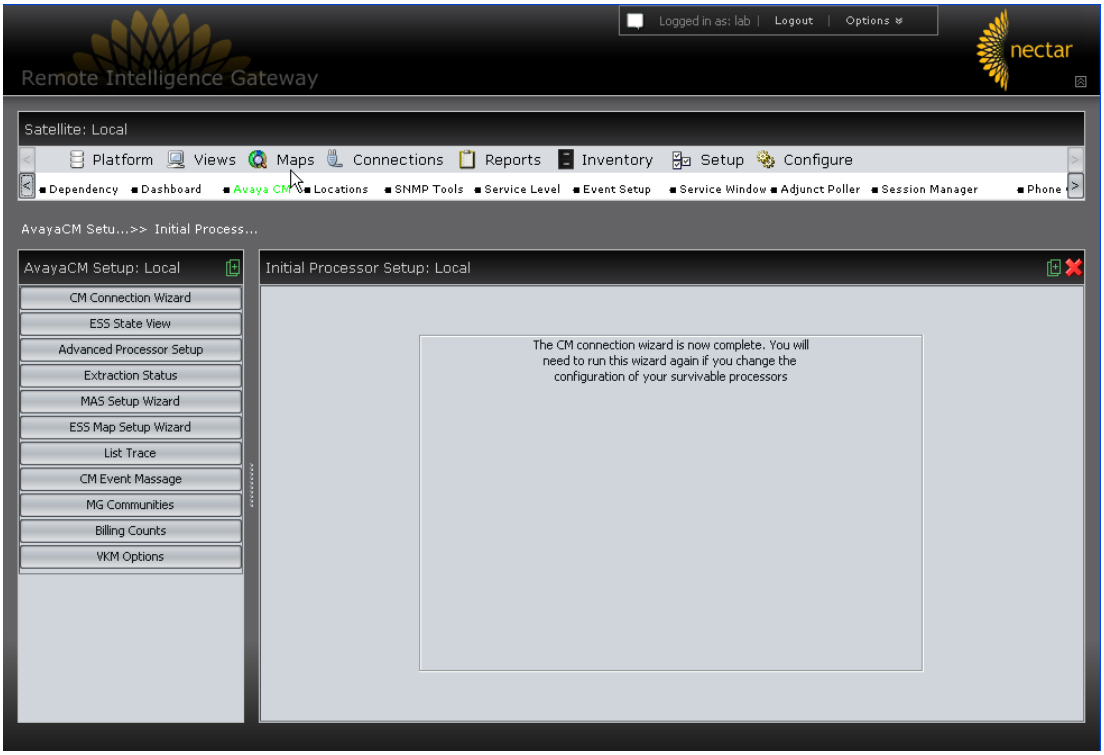


Navigate through the remaining screens to confirm the default parameters.









7. Verification Steps

The following steps were used to verify the configuration.

- Use the **ping** command to verify connectivity from Nectar CMP to all devices.
- Verify that calls can be successfully completed between the IP and Digital telephones.
- Compare VoIP quality data from the following sources:
    - A VoIP impairment tool
    - Avaya IP telephone's Network Audio Quality data
    - Nectar CMP

8. Conclusion

These Application Notes illustrate the procedures for configuring Nectar CMP to monitor and correctly provide VoIP call quality statistics on various types of calls. In the configuration described in these Application Notes, Nectar CMP employs a combination of the following three methods to collect data for generating a report on VoIP devices:

- System Access Terminal (SAT)
- RTCP Monitor Server
- SNMP/TRAP

During compliance testing, CMP successfully monitored call streams, correctly provided VoIP call quality data, and received traps from VoIP devices and media servers.

9. References

This section references the Avaya and Nectar documentation that are relevant to these Application Notes.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administering Avaya Aura™ Communication Manager*, Issue 6.0, June 2010, Document Number 03-300509

Nectar provided the following documentation. For additional product and company information, visit http://www.nectarcorp.com.

[2] *Nectar CMP Supplement – Avaya CM VKM Preparing Avaya Communications Manager (IP Enabled) for CMP Interaction*, September 2010, Document Version 2.0
[3] *Nectar CMP Administrator Technical Guide Central Intelligence Platform (CIP),* July 2010, Document Version 2.3
[4] *Nectar CMP Operator Technical Guide Central Intelligence Platform (CIP),* July 2010, Document Version 2.3

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.