Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the configuration procedures required for the Nectar Converged Management Platform (CMP) to interoperate with Avaya Communication Manager. Nectar CMP is an intelligent platform that converges monitoring and management of the different layers of your network and system's 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 CMP to interoperate with Avaya Communication Manager. The purpose of the testing was to verify that Nectar CMP recorded each phone call's performance metrics, and these performance metrics match those from the endpoints. In addition, it was verified that Nectar CMP could discover and properly identify the devices in the lab, including making a determination of which phones were registered to which call server.

Nectar 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 CMP is an intelligent platform that converges monitoring and management of the different layers of a network and system's 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.

Figure 1 illustrates the network configuration used to verify the Nectar CMP solution. The figure shows two separate communication systems, each running Avaya Communication Manager on separate Avaya servers. Site A is comprised of Avaya S8720 Servers and an Avaya G650 Media Gateway, which has connections to the following: Avaya 4600 Series IP Telephones, Avaya 9600 Series IP Telephones, and an Avaya 6400 Series Digital Telephone. Site B is comprised of an Avaya S8300 Server with an Avaya G700 Media Gateway, which has connections to Avaya 4600 Series IP Telephones, an Avaya 9600 Series IP Telephone, and an Avaya 6400 Series Digital Telephone. Site C is comprised of an Avaya S8300 Server with an Avaya G350 Media Gateway, which has connections to an Avaya 4600 Series IP Telephone and an Avaya 6400 Series Digital Telephone. Site C is setup as a Local Survivable Processor (LSP) to Site A. An IP trunk connects the two Avaya Communication Manager systems in Site A and Site B. Nectar CMP was located in Site D, and has IP connectivity to all devices.

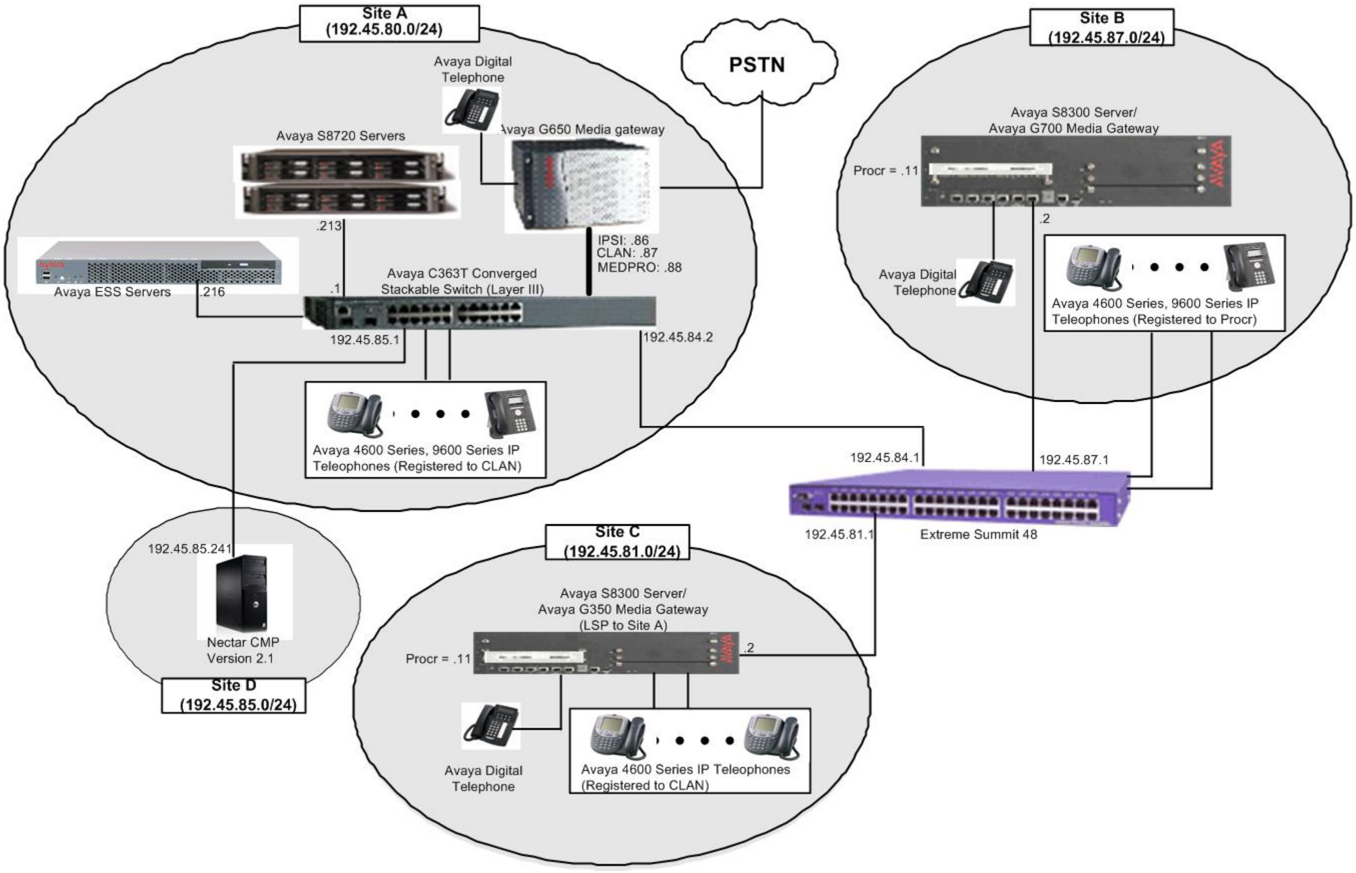


Figure 1. Test configuration of Nectar CMP with Avaya Communication Manager

2. Equipment and Software Validated

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

Equipment		Software/Firmware
Avaya S8720 Servers		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya G650 Media Gateway		
	TN2312BP IP Server Interface	HW11 FW030
	TN799DP C-LAN Interface	HW20 FW017
	TN2302AP IP Media Processor	HW01 FW108
Avaya S8300 Server with Avaya G700 Media Gateway		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya S8500 Server (ESS Mode)		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya S8300 Server with Avaya G350 Media Gateway (LSP Mode)		Avaya Communication Manager 5.1 (01.0.414.3) with SP # 15842
Avaya 4600 Series IP Telephones		
	4620 (H.323)	2.8
	4625 (H.323)	2.8
Avaya 4600 Series IP Telephones		
	9630 (H.323)	1.5
	9650 (H.323)	1.5
Avaya 6400 Series Digital Telephones		-
Analog Telephones		-
Avaya C363T-PWR Converged Stackable Switch		4.5.14
Extreme Summit 48		4.1.21
Nectar CMP OS –Windows 2003 Server with SP 2		2.1

3. Configuring Avaya Communication Manager

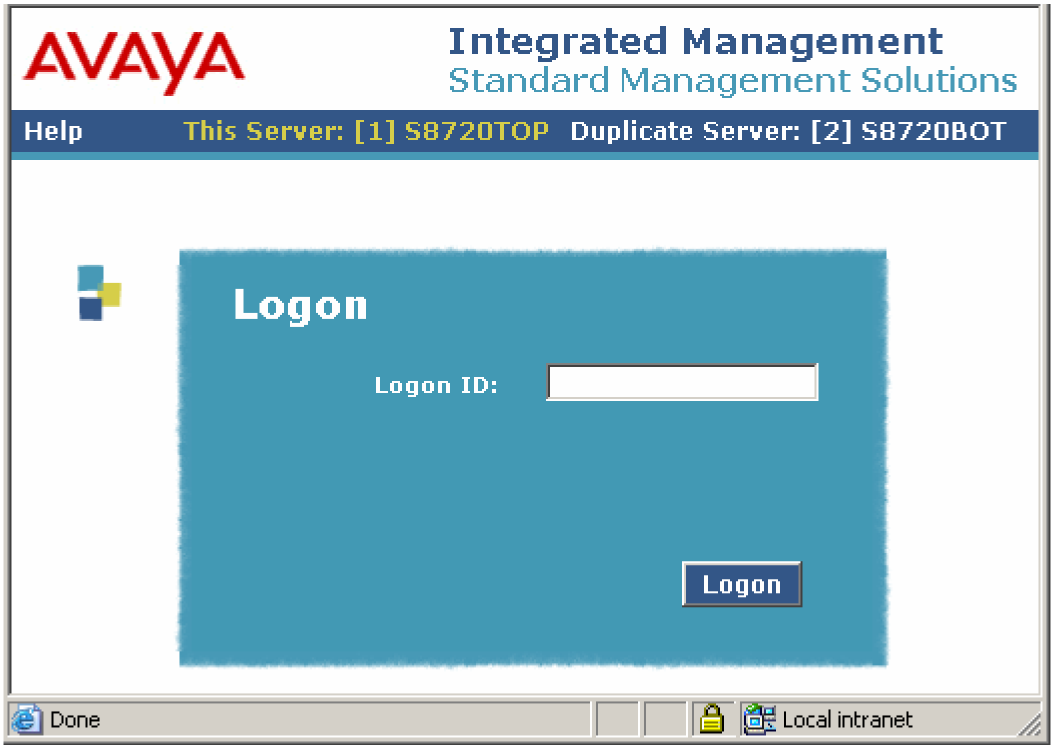
Nectar CMP utilizes a combination of the following three methods to collect data for generating a report on VoIP devices.

- System Access Terminal (SAT) – Nectar CMP utilize SAT to collect resource information in Avaya Communication Manager. In order for Nectar CMP to perform the resource collection, credentials should be provided.
- RTCP Monitor Server – Nectar CMP receives RTCP reports from the endpoints or the media processor (medpro) board to provide the VoIP path and call quality information.
- SNMP/TRAP – Nectar CMP queries Avaya Communication Manager and other Avaya VoIP devices, utilizing SNMPwalk, to collect status information. Nectar CMP is set up as a trap receiver, and thus receives alarms from Avaya Communication Manager and other Avaya VoIP devices.

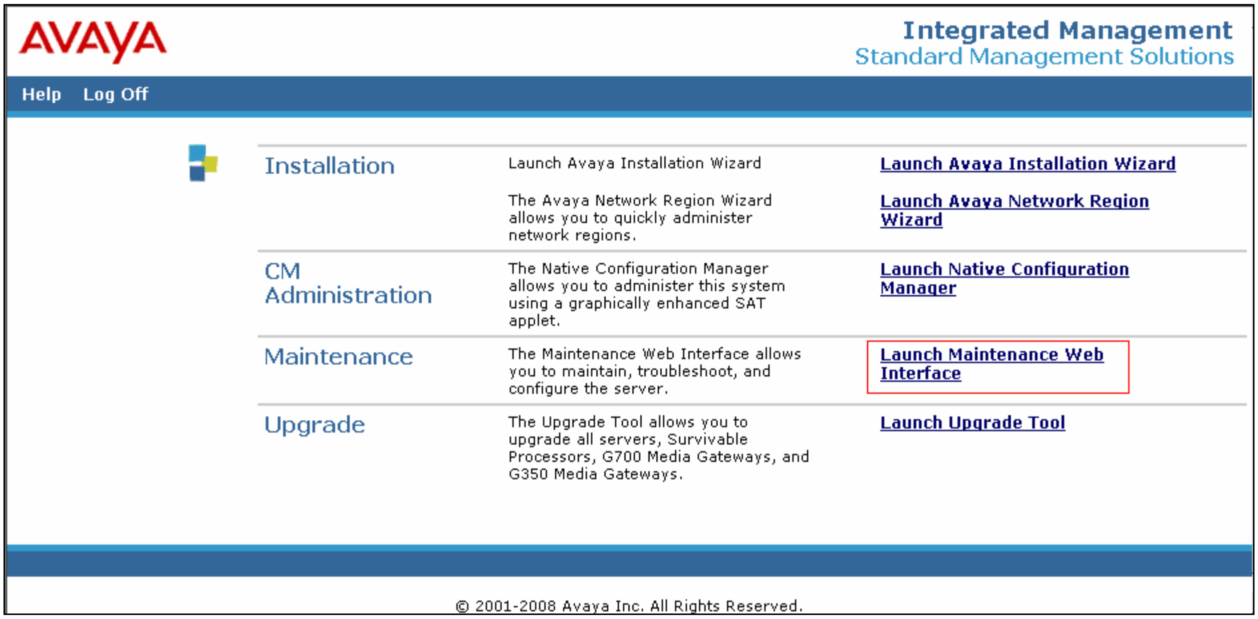
This section provides the procedures for configuring the above mentioned methods in Avaya Communication Manager.

3.1. Creating Nectar CMP credentials

This section describes how to create credentials for Nectar CMP to log in to an Avaya Communication Manager. Launch a web browser and connect to the media server by entering https://<media server IP address>. Supply proper credentials to access the Integrated Management Standard Management Solutions page.


AVAYA
Integrated Management
Standard Management Solutions
Help
This Server: [1] S8720TOP
Duplicate Server: [2] S8720BOT
Logon
Logon ID:
Logon
Done
Local intranet

Click on the **Launch Maintenance Web Interface** link.


AVAYA
Integrated Management
Standard Management Solutions
Help
Log Off
Installation
Launch Avaya Installation Wizard
Launch Network Region Wizard
CM Administration
Launch Native Configuration Manager
Maintenance
Launch Maintenance Web Interface
Upgrade
Launch Upgrade Tool

Launch Avaya Installation Wizard

The Avaya Network Region Wizard allows you to quickly administer network regions.

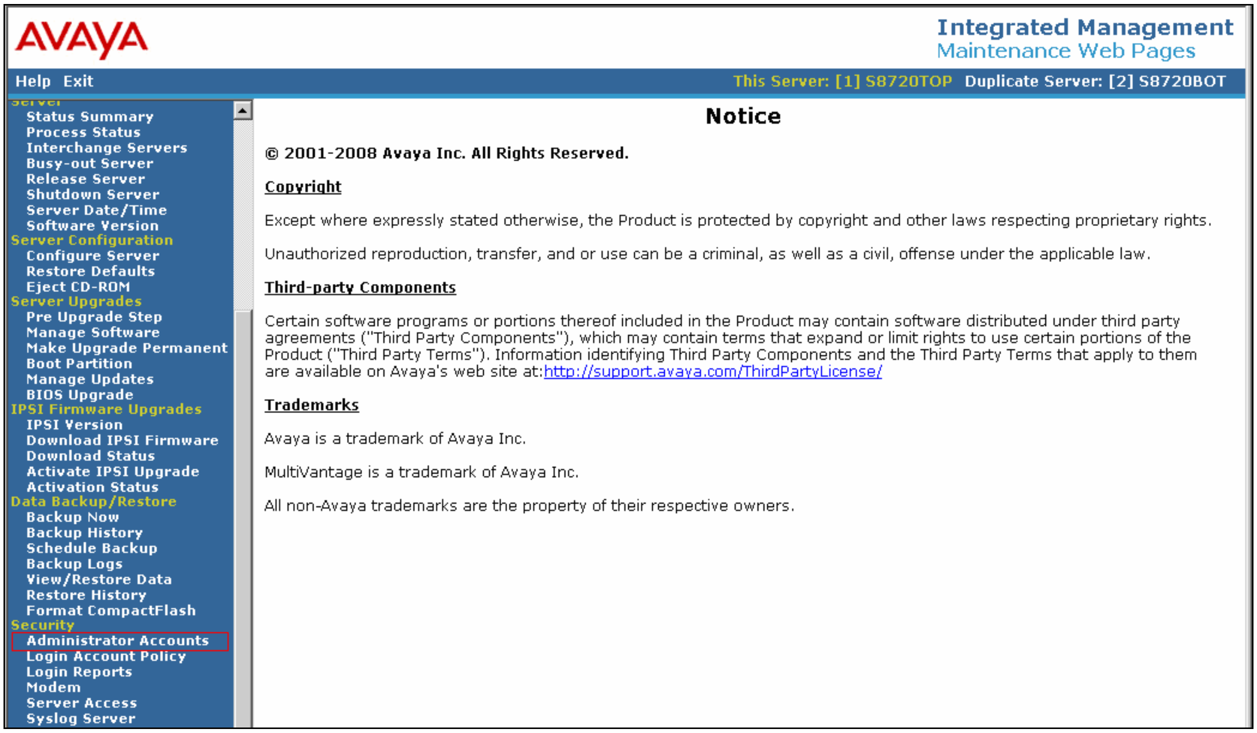
The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.

The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the server.

The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.

© 2001-2008 Avaya Inc. All Rights Reserved.

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



Notice

© 2001-2008 Avaya Inc. All Rights Reserved.

Copyright

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

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

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:http://support.avaya.com/ThirdPartyLicense/

Trademarks

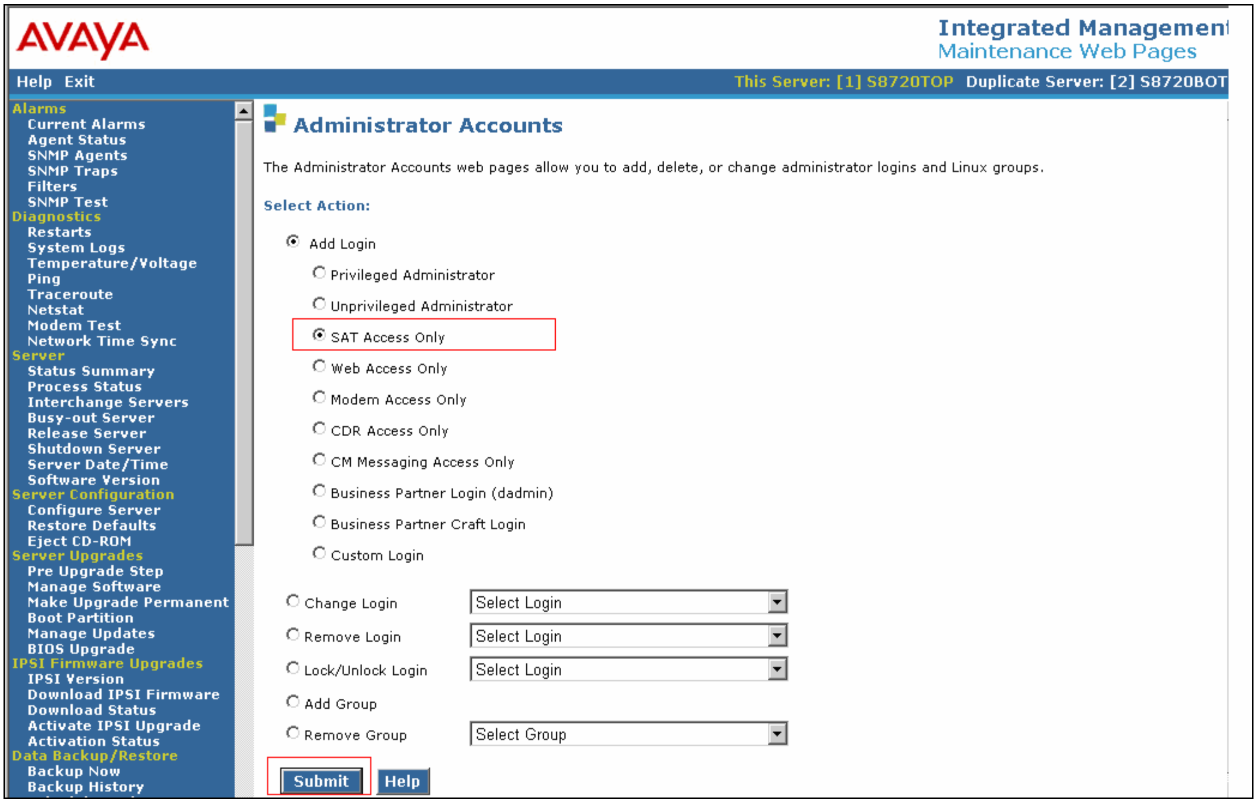
Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

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

Note: *For Nectar CMP to perform the resource collection, the login account only need to be a permission level of* ***SAT Access Only****.*



AVAYA

Integrated Management
Maintenance Web Pages

Help Exit

This Server: [1] S8720TOP Duplicate Server: [2] S8720BOT

Alarms
- Current Alarms
- Agent Status
- SNMP Agents
- SNMP Traps
- Filters
- SNMP Test

Diagnostics
- Restarts
- System Logs
- Temperature/Voltage
- Ping
- Traceroute
- Netstat
- Modem Test
- Network Time Sync

Server
- Status Summary
- Process Status
- Interchange Servers
- Busy-out Server
- Release Server
- Shutdown Server
- Server Date/Time
- Software Version

Server Configuration
- Configure Server
- Restore Defaults
- Eject CD-ROM

Server Upgrades
- Pre Upgrade Step
- Manage Software
- Make Upgrade Permanent
- Boot Partition
- Manage Updates
- BIOS Upgrade

IPSI Firmware Upgrades
- IPSI Version
- Download IPSI Firmware
- Download Status
- Activate IPSI Upgrade
- Activation Status

Data Backup/Restore
- Backup Now
- Backup History

Administrator Accounts

The Administrator Accounts web 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
- ○ Modem Access Only
- ○ CDR Access Only
- ○ CM Messaging Access Only
- ○ Business Partner Login (dadmin)
- ○ Business Partner Craft Login
- ○ Custom Login

○ Change Login — Select Login

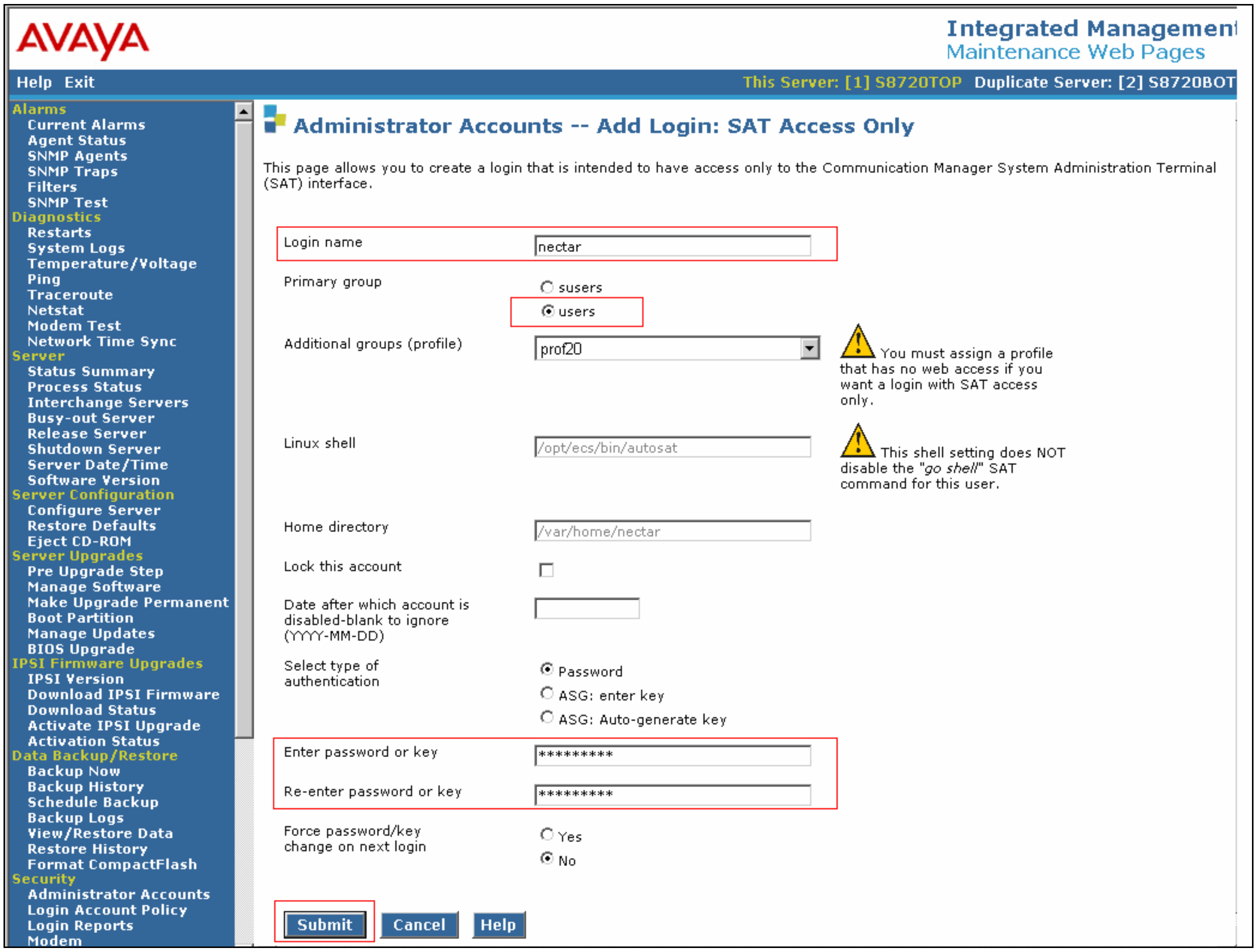
○ Remove Login — Select Login

○ Lock/Unlock Login — Select Login

○ Add Group

○ Remove Group — Select Group

Provide Login name and password, and select the **users** radio button under the Primary group section. Click on the **Submit** button. Default values may be used in the remaining fields.



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

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

Linux shell: /opt/ecs/bin/autosat

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

Home directory: /var/home/nectar

Lock this account: □

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

Select type of authentication: ● Password ○ ASG: enter key ○ ASG: Auto-generate key

Enter password or key: *********

Re-enter password or key: *********

Force password/key change on next login: ○ Yes ● No

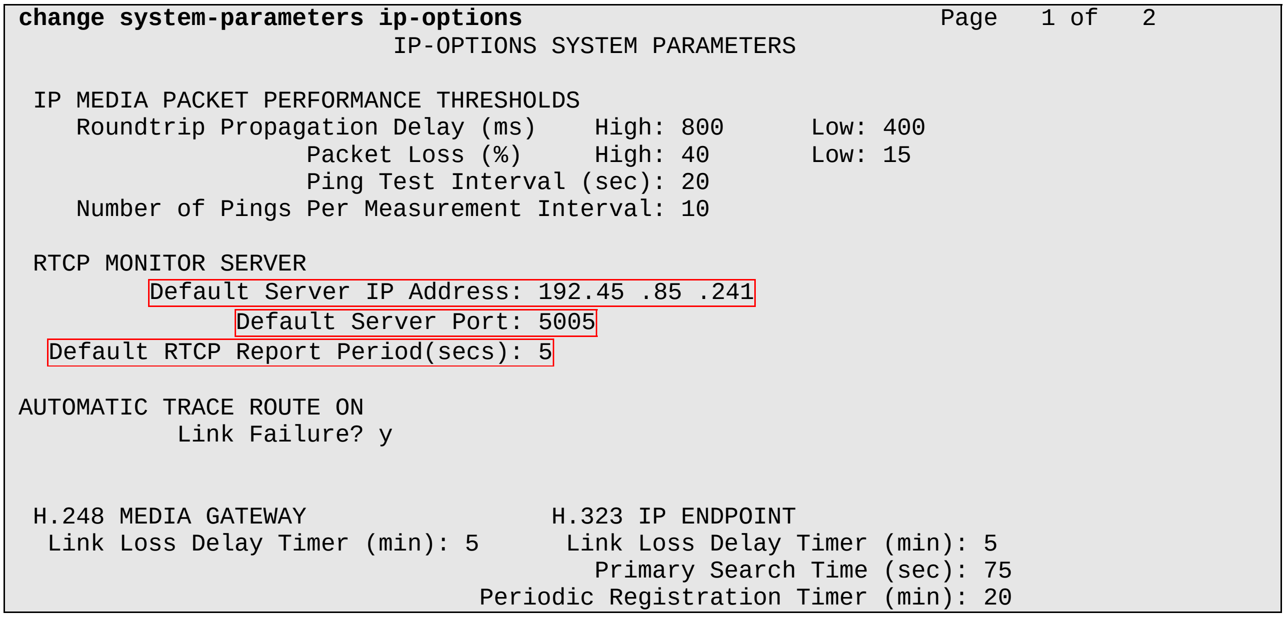
Submit Cancel Help

3.2. Creating RTCP Monitor Server

Since Nectar CMP utilizes RTCP packets to calculate and report the call path and quality of the call stream, a RTCP monitor server needs to be created in Avaya Communication Manager. The following screen describes the setting of the RTCP monitor server. All the configuration changes in Avaya Communication Manager are performed through the System Access Terminal (SAT). Log into the SAT and use the **change system-parameters ip-options** command to configure the RTCP monitor server. Provide the following information:

- **Default Server IP Address** - IP address of the Nectar CMP server
- **Default Server Port** – 5005 [This port number must match with the Nectar CMP RTCP Listening Port. The default value for the Default Server Port field is 5005]
- **Default RTCP Report Period (secs)** – 5 [The report period indicates Avaya endpoints forward RTCP packet to the RTCP monitor server, which is the Nectar CMP server. The default value for the Default RTCP Report Period(secs) field is 5]

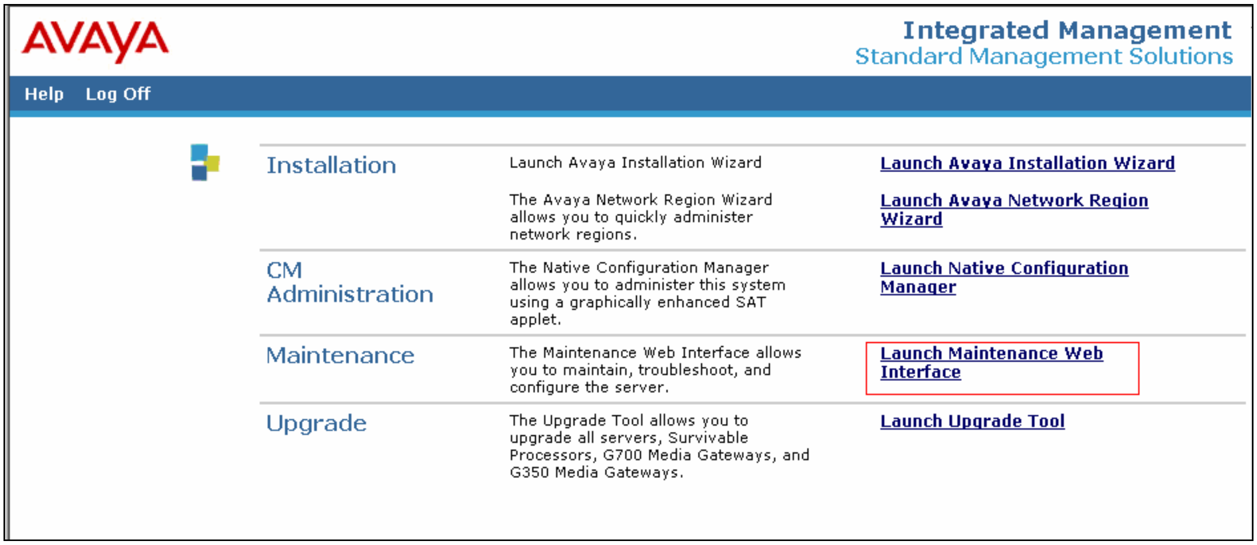
Default values may be used in the remaining fields.



```
change system-parameters ip-options                           Page   1 of   2
                          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

 RTCP MONITOR SERVER
         Default Server IP Address: 192.45 .85 .241
               Default Server Port: 5005
  Default RTCP Report Period(secs): 5

AUTOMATIC TRACE ROUTE ON
           Link Failure? y


 H.248 MEDIA GATEWAY                 H.323 IP ENDPOINT
  Link Loss Delay Timer (min): 5      Link Loss Delay Timer (min): 5
                                        Primary Search Time (sec): 75
                                 Periodic Registration Timer (min): 20
```

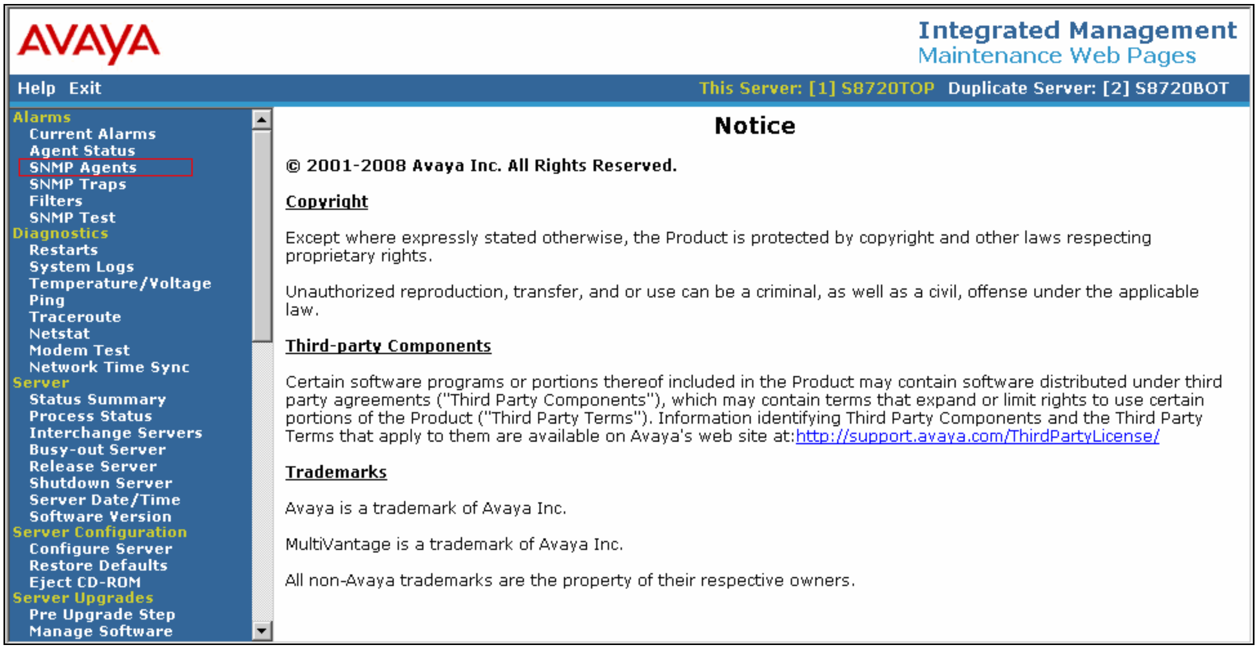
3.3. Enabling SNMP / TRAP Service

For Nectar CMP to query the status information on Avaya Communication Manager, the SNMP and TRAP services need to be enabled on the Avaya S8720 and S8300 Media Servers. Once SNMP is enabled, Nectar CMP utilizes SNMPwalk to extract information from Avaya Communication Manager. Enabling the SNMP service for the Avaya S8720 and S8300 Media Servers can be configured through the server's web interface. Launch a web browser and connect to the media server by entering https://<media server IP address>. Supply the login and password for an account with super-user privileges. For an S8720 Media Server pair, the SNMP trap destinations need to be configured on each media server. Select **Launch Maintenance Web Interface** from the screen.



Installation	Launch Avaya Installation Wizard	Launch Avaya Installation Wizard
	The Avaya Network Region Wizard allows you to quickly administer network regions.	Launch Avaya Network Region Wizard
CM Administration	The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet.	Launch Native Configuration Manager
Maintenance	The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the server.	Launch Maintenance Web Interface
Upgrade	The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways.	Launch Upgrade Tool

Click on the **SNMP Agents** link under the Alarms section, on the left pane, to display the SNMP Agent page.



Notice

© 2001-2008 Avaya Inc. All Rights Reserved.

Copyright

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

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

Third-party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them are available on Avaya's web site at:http://support.avaya.com/ThirdPartyLicense/

Trademarks

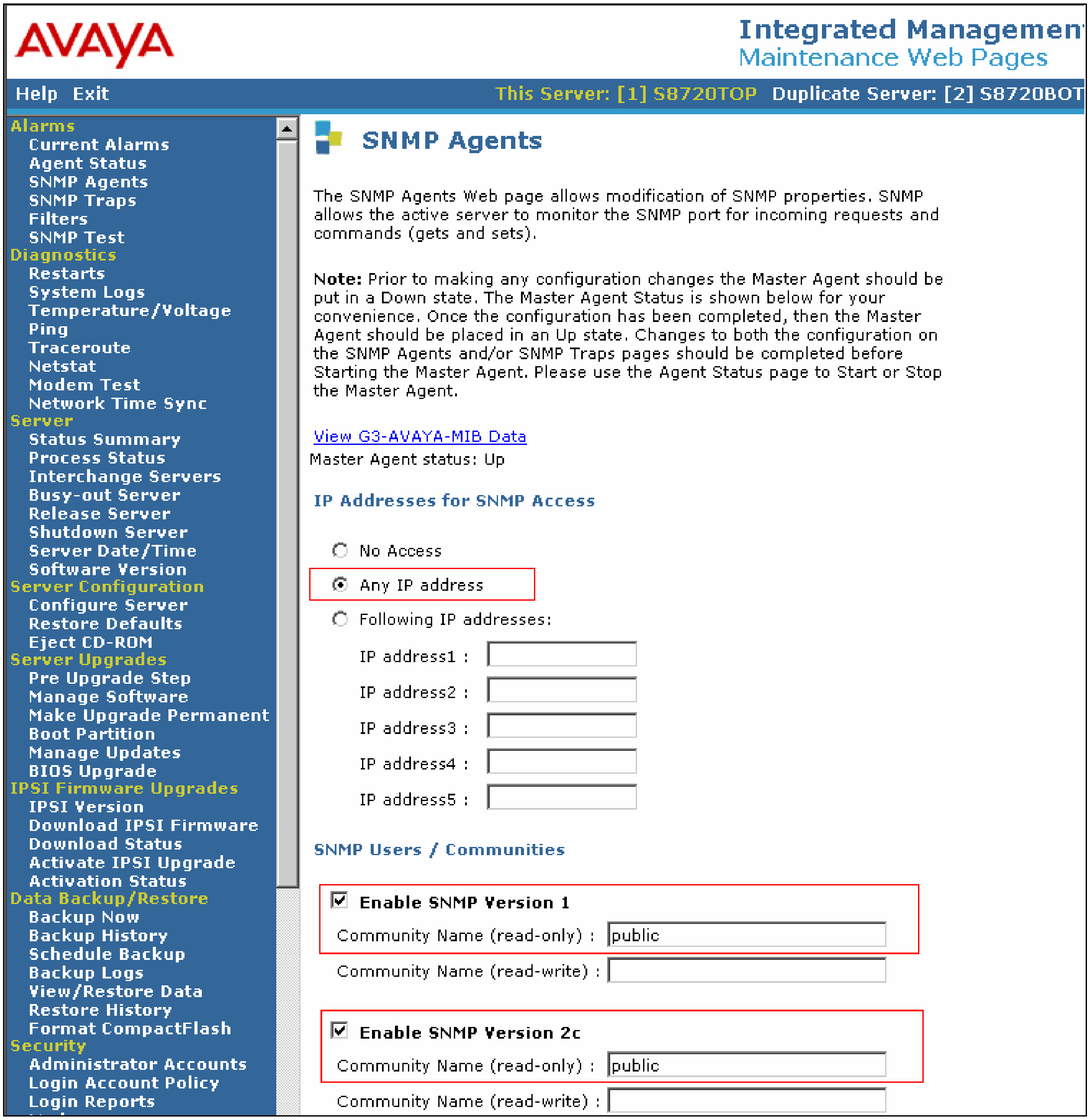
Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

In the SNMP Agent page, select the **Any IP Address** radio button under the **IP Addresses for SNMP Access** section. This implies that any device can perform a SNMP request to the Avaya media servers. For the security purpose, an administrator may restrict the access by specifying IP address(s) under the **Following IP addresses** field for the SNMP access section. Enable SNMP version 1 and version 2c by checking on the check boxes. Provide the Community Name (read-only) field to **public** on both versions of SNMP. The community name configured in the Avaya media server has to match with Nectar CMP.

Click on the **Submit** button (not shown) at the bottom of the page to submit the form.



SNMP Agents

The SNMP Agents Web page allows modification of SNMP properties. SNMP allows the active server to monitor the SNMP port for incoming requests and commands (gets and sets).

Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

View G3-AVAYA-MIB Data

Master Agent status: Up

IP Addresses for SNMP Access

○ No Access

● Any IP address

○ Following IP addresses:

IP address1 :

IP address2 :

IP address3 :

IP address4 :

IP address5 :

SNMP Users / Communities

☑ **Enable SNMP Version 1**

Community Name (read-only) : public

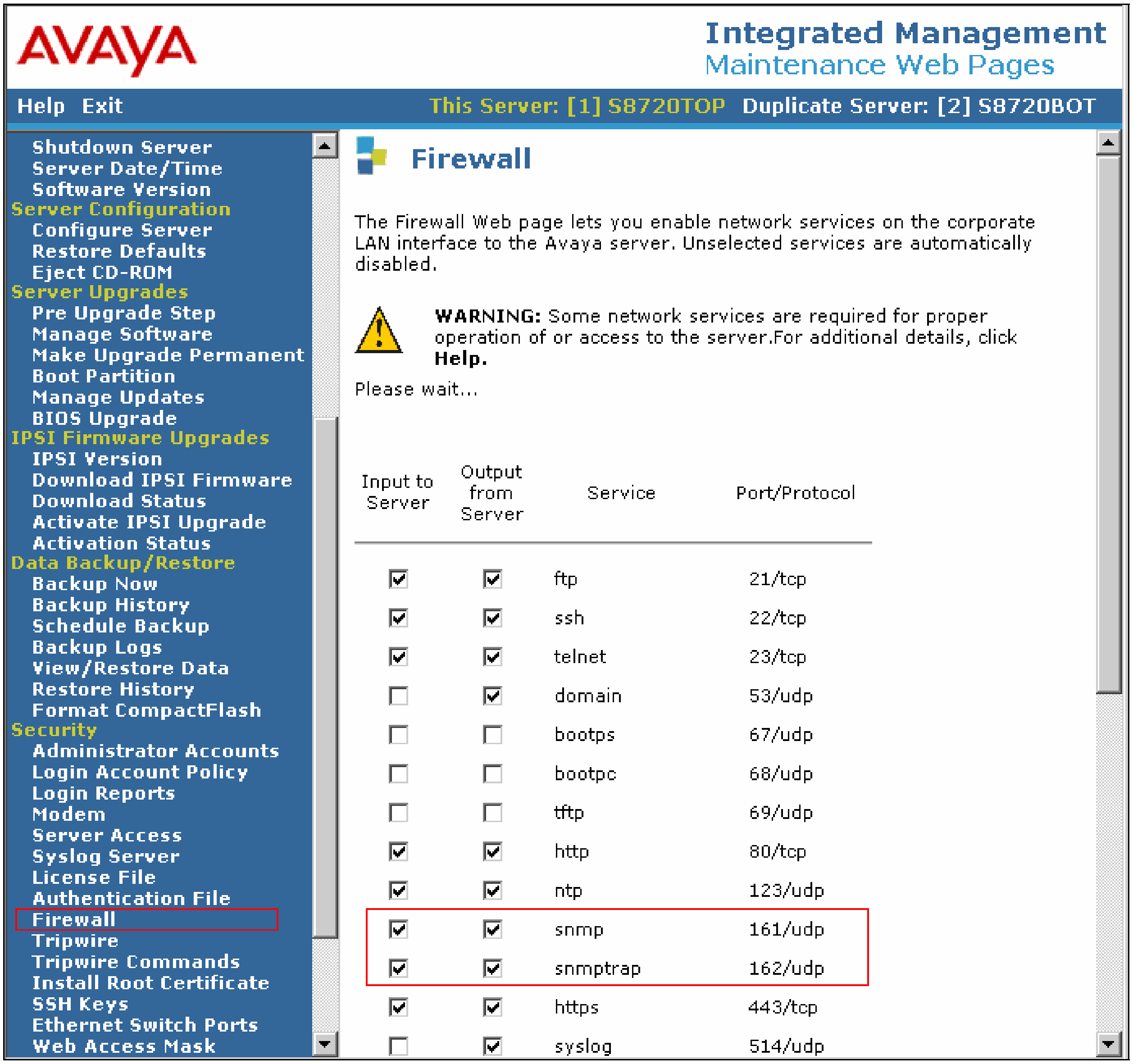
Community Name (read-write) :

☑ **Enable SNMP Version 2c**

Community Name (read-only) : public

Community Name (read-write) :

The firewall in the Avaya server must allow SNMP on UDP port 161 and SNMPTRAP on UDP port 162. Click on the **Firewall** link under the Security section to display the Firewall page. Make sure that **snmp** (Input to Server 161/udp) and **snmptrap** (Output from Server 162/udp) are selected (the example below shows, both inbound and outbound are enabled on both ports). SNMP allows for operating system and host queries to be made against Avaya Communication Manager from an external system. Nectar CMP utilizes this service to obtain health statistics about the S8720 hardware that hosts the Avaya Communication Manager software. Click on the **Submit** button (not shown) at the bottom of the page to submit the form.



Firewall

The Firewall Web page lets you enable network services on the corporate LAN interface to the Avaya server. Unselected services are automatically disabled.

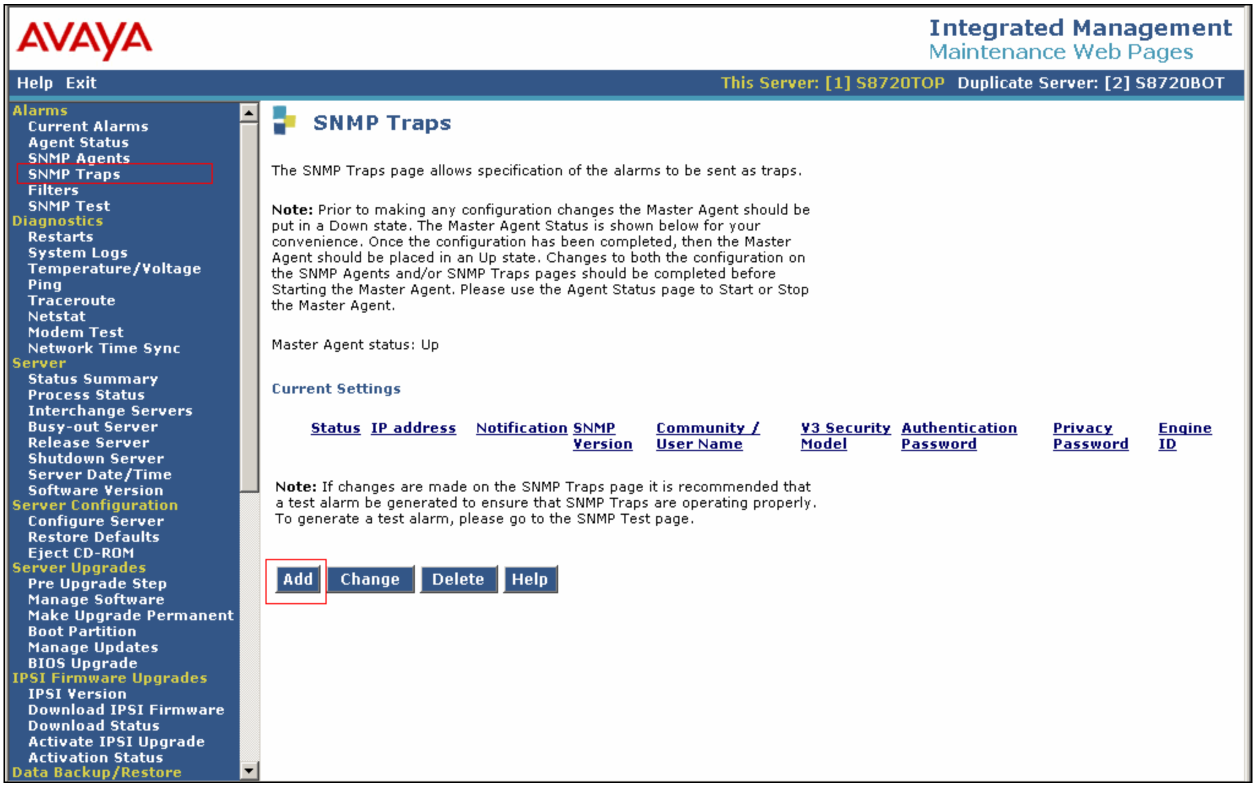
WARNING: Some network services are required for proper operation of or access to the server.For additional details, click **Help.**

Please wait...

Input to Server	Output from Server	Service	Port/Protocol
☑	☑	ftp	21/tcp
☑	☑	ssh	22/tcp
☑	☑	telnet	23/tcp
☐	☑	domain	53/udp
☐	☐	bootps	67/udp
☐	☐	bootpc	68/udp
☐	☐	tftp	69/udp
☑	☑	http	80/tcp
☑	☑	ntp	123/udp
☑	☑	snmp	161/udp
☑	☑	snmptrap	162/udp
☑	☑	https	443/tcp
☐	☑	syslog	514/udp

3.4. Configure SNMP TRAP Destination

This section describes how to create a trap destination. Navigate to the **SNMP Traps** link under the Alarms section. Click on the **Add** button to start configuring a trap destination.



SNMP Traps

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

Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

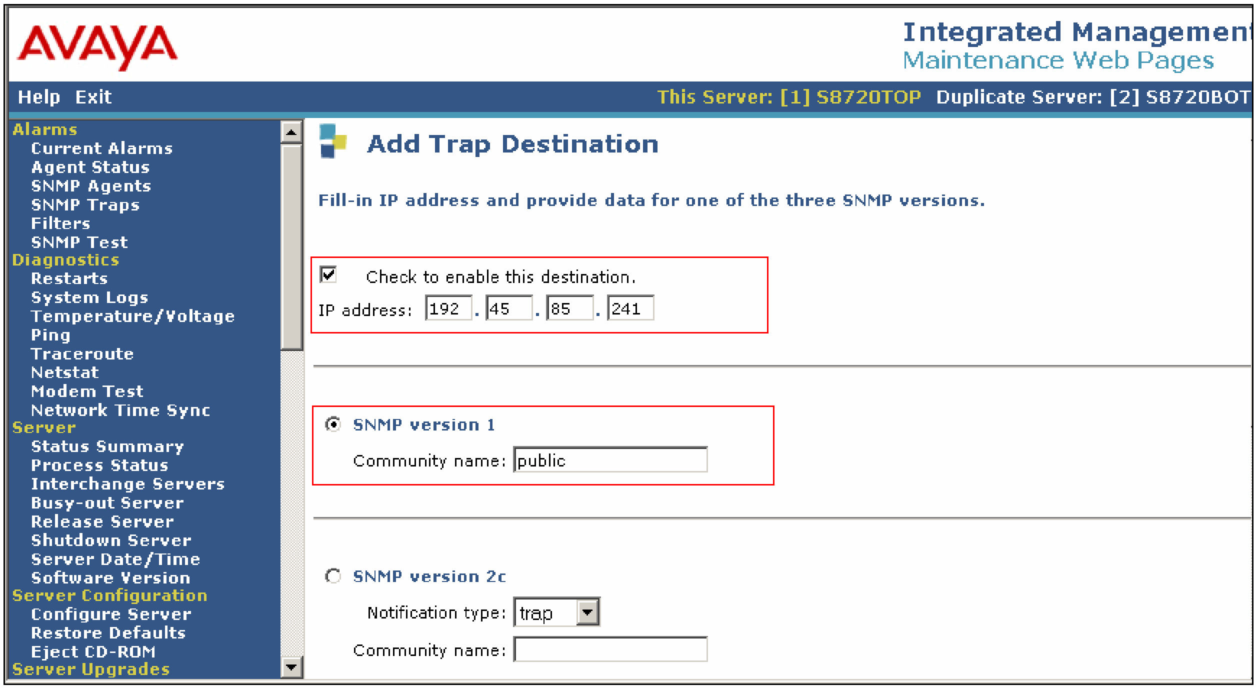
Master Agent status: Up

Current Settings

Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Privacy Password	Engine ID

Note: If changes are made on the SNMP Traps page it is recommended that a test alarm be generated to ensure that SNMP Traps are operating properly. To generate a test alarm, please go to the SNMP Test page.

From the Add Trap Destination page, check the trap destination check box to enable the trap service, and provide the trap destination IP address (Nectar CMP IP address). Click on the SNMP version 1 radio button, and provide the community name. Click on the **Add** button (not shown) at the bottom of the page to submit the form



Add Trap Destination

Fill-in IP address and provide data for one of the three SNMP versions.

☑ Check to enable this destination.

IP address: 192 . 45 . 85 . 241

● SNMP version 1

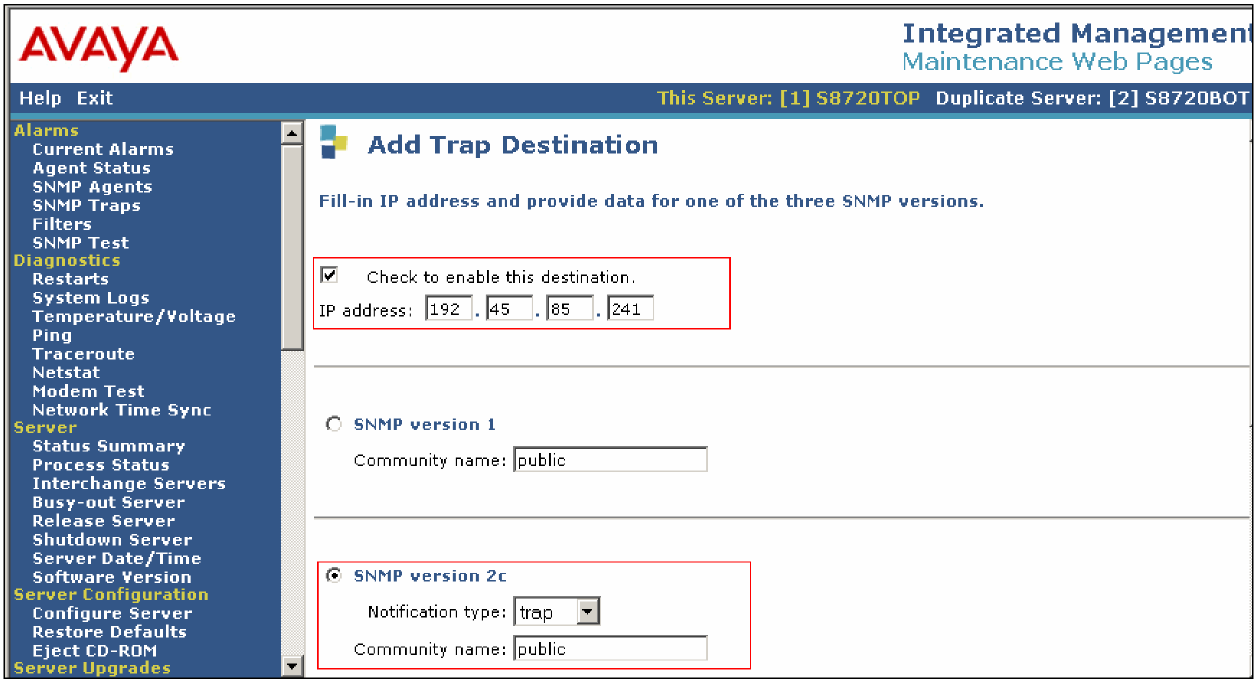
Community name: public

○ SNMP version 2c

Notification type: trap

Community name:

Using the previous steps in **Section 3.4**, add trap destination for the SNMP version 2c. Set Notification type to **trap**, using the drop-down menu.



Add Trap Destination

Fill-in IP address and provide data for one of the three SNMP versions.

☑ Check to enable this destination.

IP address: 192 . 45 . 85 . 241

○ SNMP version 1

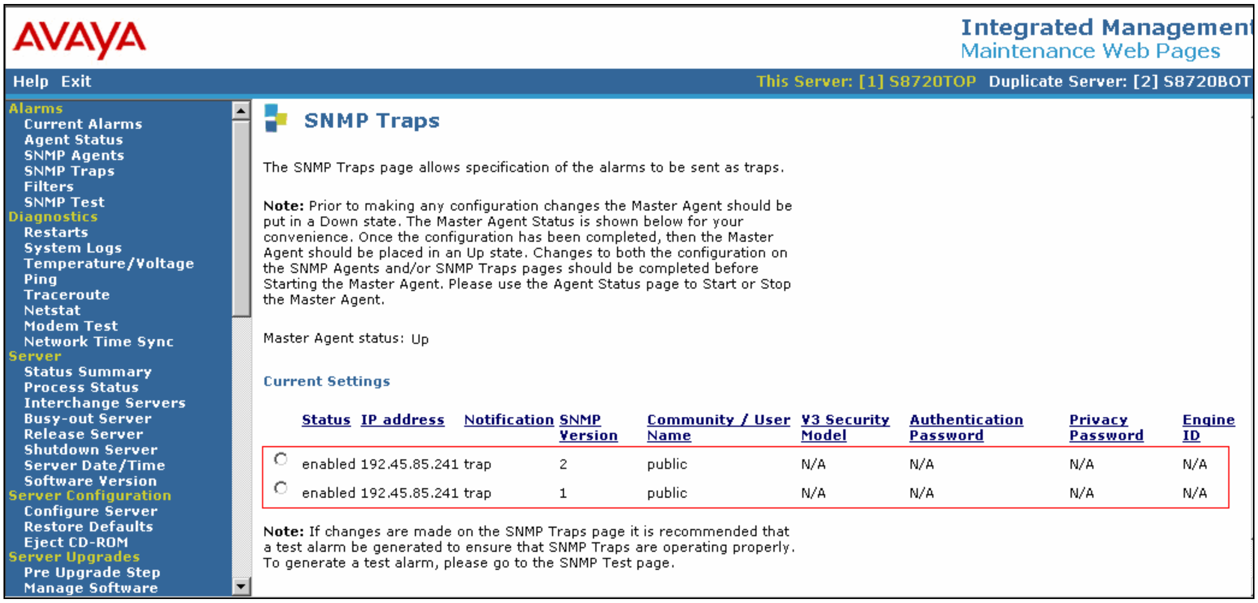
Community name: public

● SNMP version 2c

Notification type: trap

Community name: public

The following screen shows the completion of the trap destination setup for SNMP version 1 and 2.



SNMP Traps

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

Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP Agents and/or SNMP Traps pages should be completed before Starting the Master Agent. Please use the Agent Status page to Start or Stop the Master Agent.

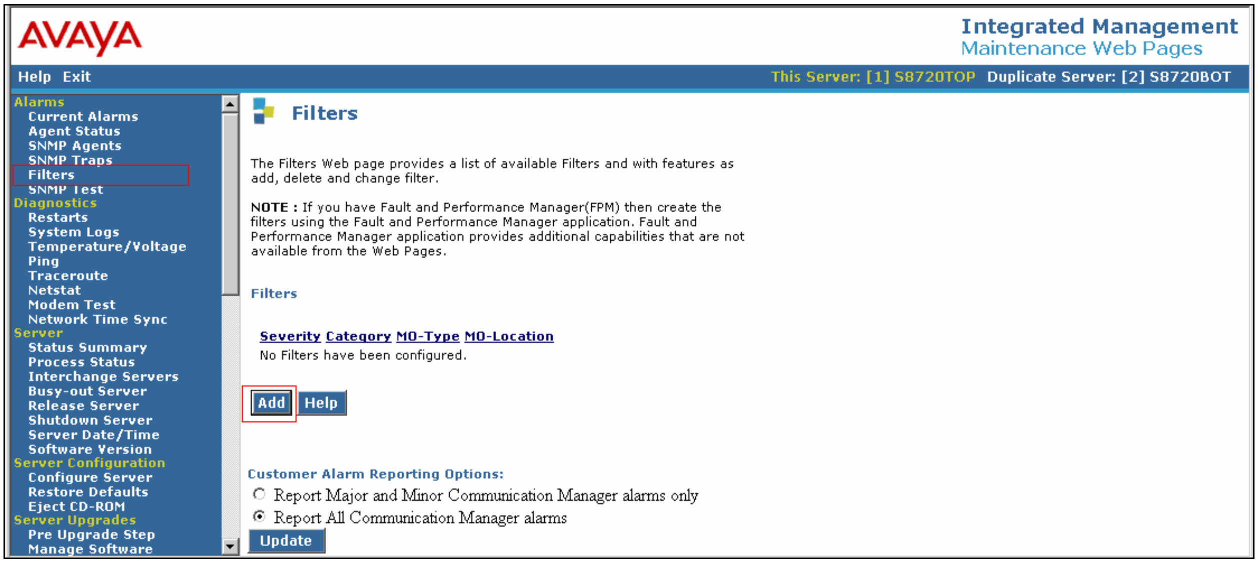
Master Agent status: Up

Current Settings

	Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Privacy Password	Engine ID
○	enabled	192.45.85.241	trap	2	public	N/A	N/A	N/A	N/A
○	enabled	192.45.85.241	trap	1	public	N/A	N/A	N/A	N/A

Note: If changes are made on the SNMP Traps page it is recommended that a test alarm be generated to ensure that SNMP Traps are operating properly. To generate a test alarm, please go to the SNMP Test page.

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.



Filters

The Filters Web page provides a list of available Filters and with features as add, delete and change filter.

NOTE : If you have Fault and Performance Manager(FPM) then create the filters using the Fault and Performance Manager application. Fault and Performance Manager application provides additional capabilities that are not available from the Web Pages.

Filters

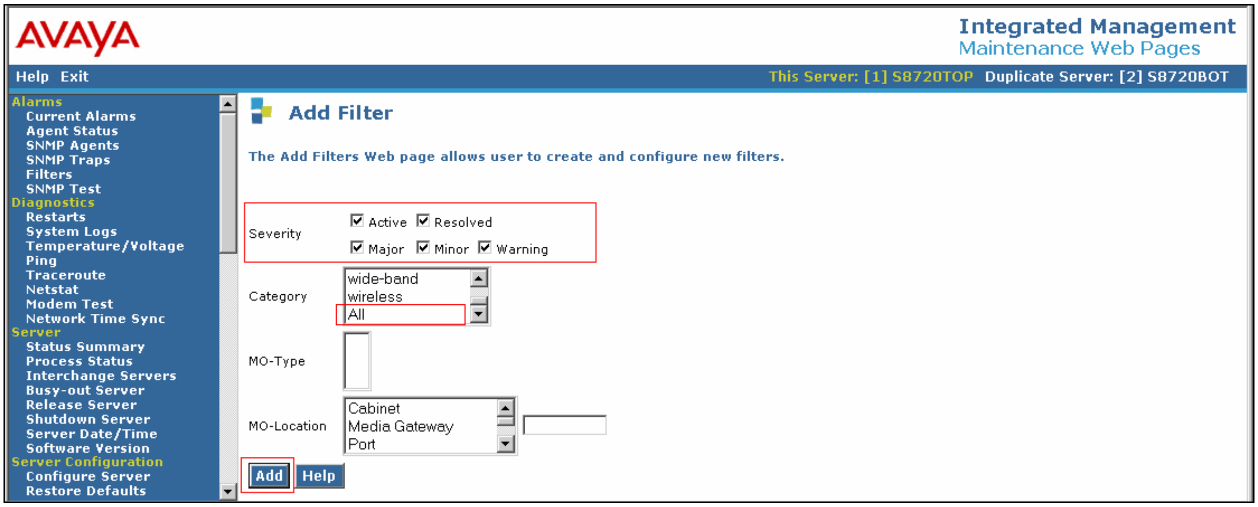
Severity	Category	MO-Type	MO-Location

No Filters have been configured.

Customer Alarm Reporting Options:

○ Report Major and Minor Communication Manager alarms only
● Report All Communication Manager alarms

On the Add Filter page, all severity check boxes were checked during the compliance test. Using the drop-down menu, select **All** for the Category field. Click on the **Add** button.



Add Filter

The Add Filters Web page allows user to create and configure new filters.

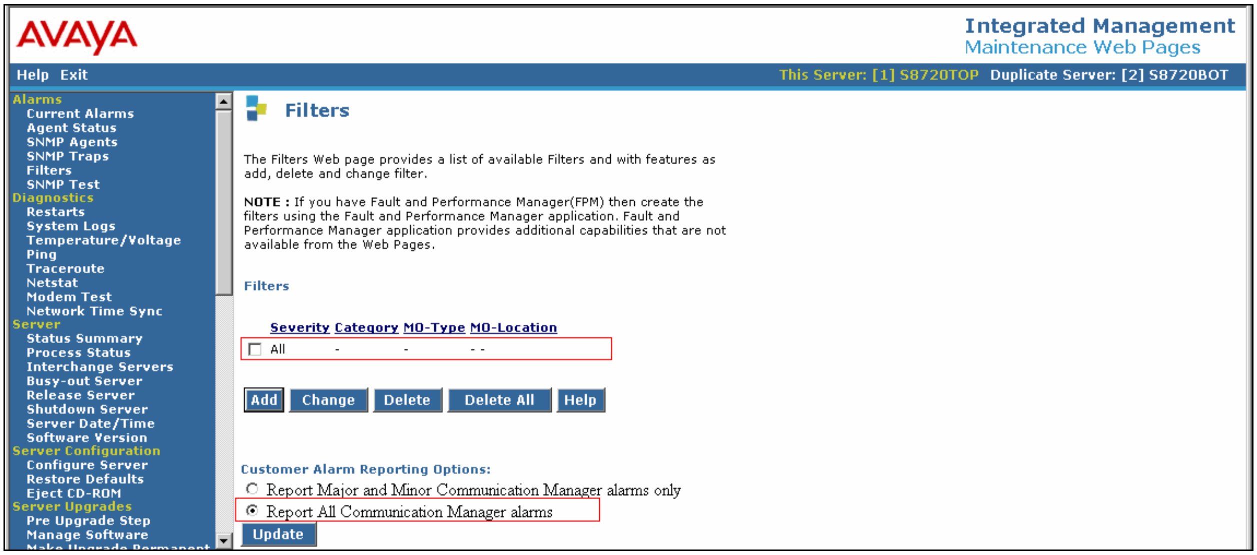
Severity ☑ Active ☑ Resolved ☑ Major ☑ Minor ☑ Warning

Category wide-band / wireless / All

MO-Type

MO-Location Cabinet / Media Gateway / Port

The following screen shows the filters page after the completion of the filter settings.



Filters

The Filters Web page provides a list of available Filters and with features as add, delete and change filter.

NOTE : If you have Fault and Performance Manager(FPM) then create the filters using the Fault and Performance Manager application. Fault and Performance Manager application provides additional capabilities that are not available from the Web Pages.

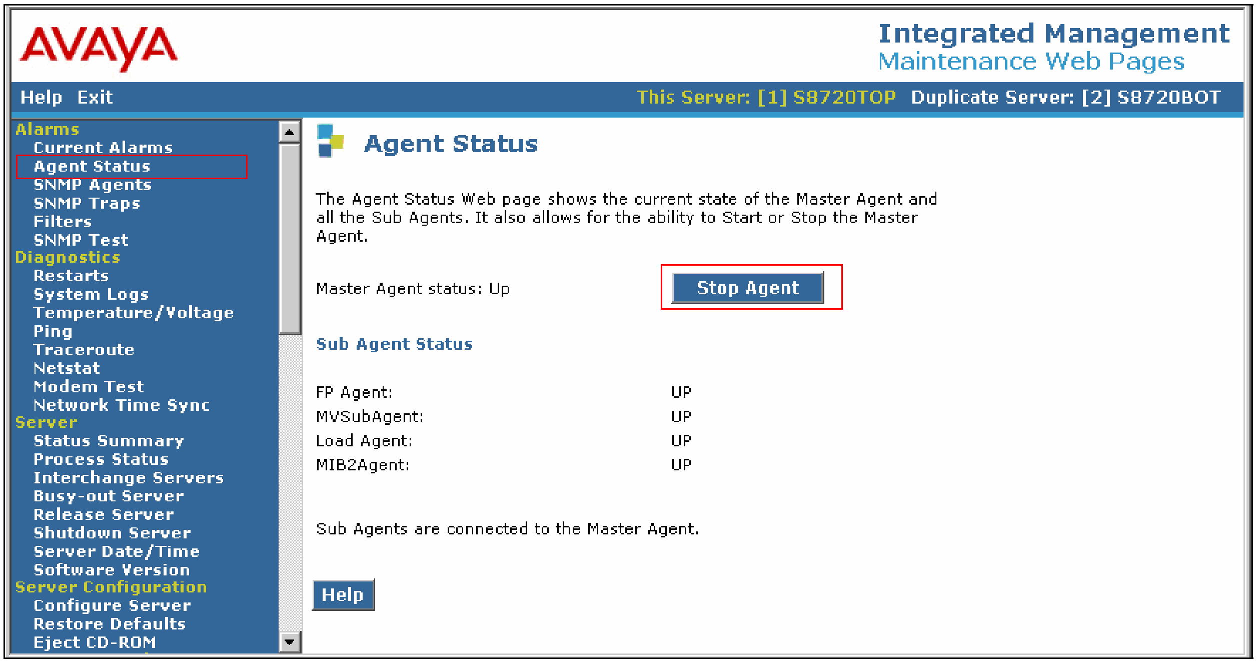
Filters

	Severity	Category	MO-Type	MO-Location
□	All	-	-	- -

Customer Alarm Reporting Options:

○ Report Major and Minor Communication Manager alarms only
● Report All Communication Manager alarms

Click on the **Agent Status** link under the Alarms section, on the left pane, stop the SNMP Master Agent by clicking the **Stop Agent** button. After the Master Agent status shows **down**, click on the **Start Agent** button to start the Master Agent.



Agent Status

The Agent Status Web 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.

Master Agent status: Up

Sub Agent Status

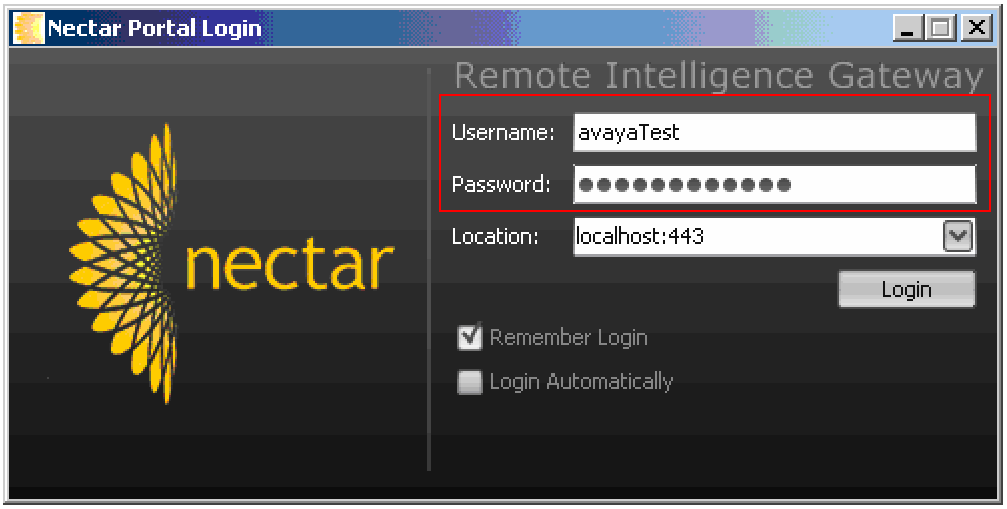
FP Agent:	UP
MVSubAgent:	UP
Load Agent:	UP
MIB2Agent:	UP

Sub Agents are connected to the Master Agent.

4. Configuring the CMP

The steps in this section describe the configuration of Nectar CMP that receives RTCP packets from the VoIP endpoint, and record performance metrics. For additional information on configuring Nectar CMP, refer to [3] and [4].

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



Username: avayaTest

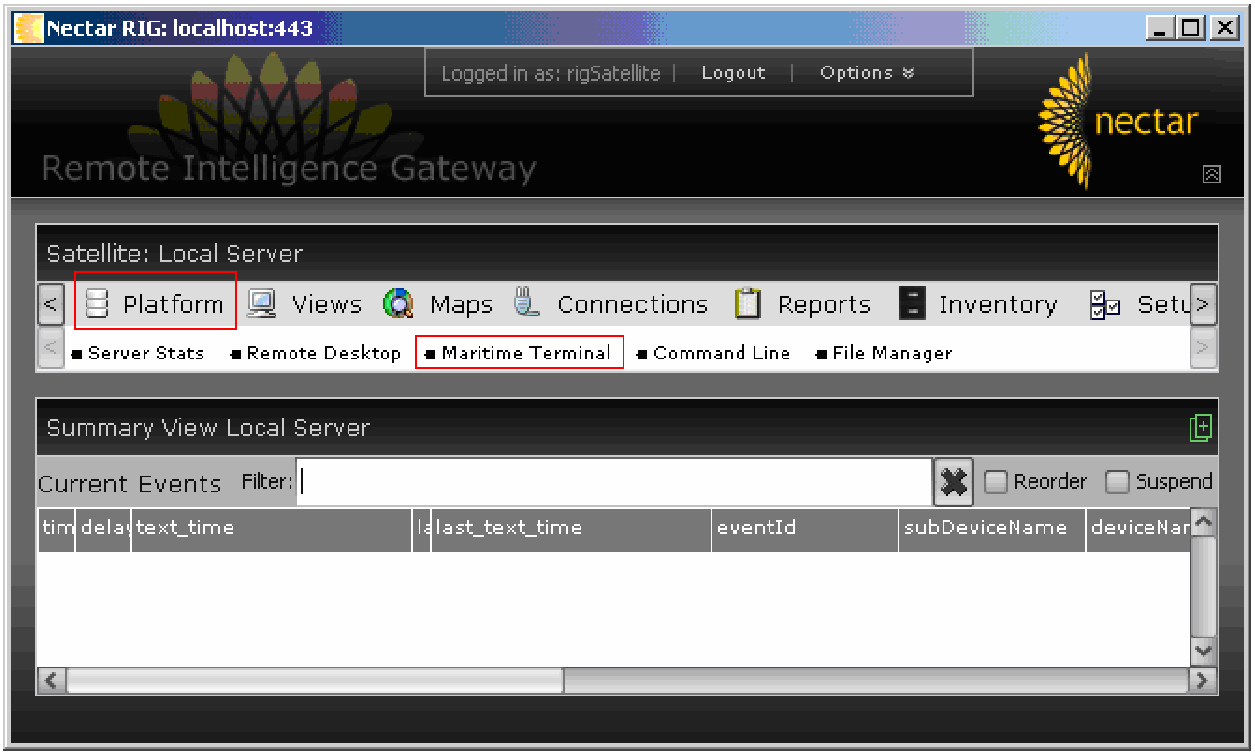
Password: ●●●●●●●●●●●●●

Location: localhost:443

☑ Remember Login

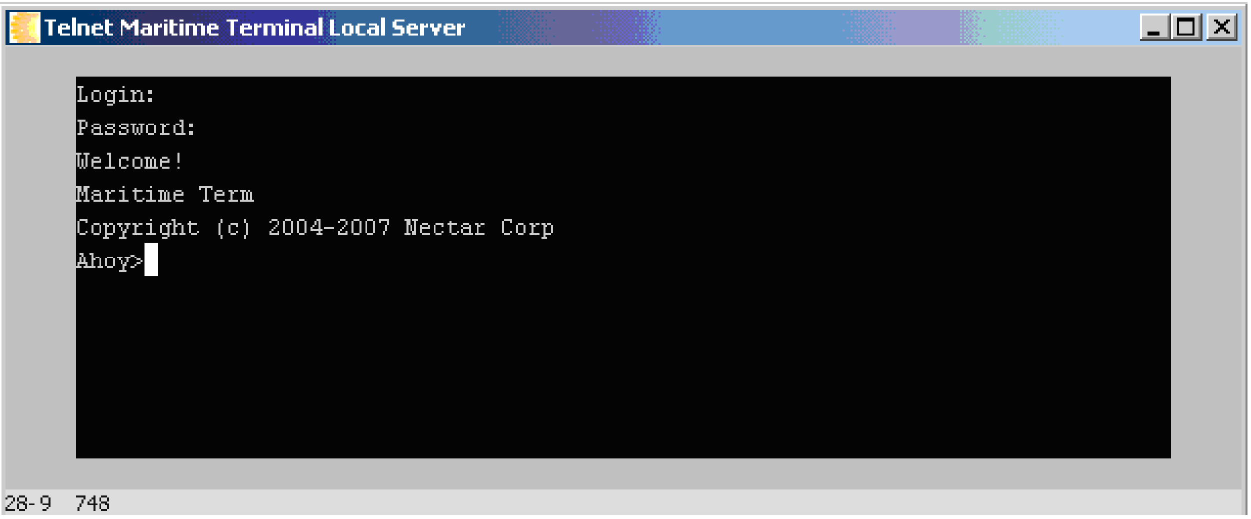
☐ Login Automatically

Select **Platform → Maritime Terminal**. Once the operation is completed, the **Telnet Maritime Terminal Local Server** window will be appeared.



To configure a RTCP receiver, type the following commands in the Telnet Maritime Terminal Local Server window:

- **avayaphone rtcp setreceiverip 192.45.85.241**
- **avayaphone rtcp setport 5005**
- **avayaphone rtcp enable**



```
Login:
Password:
Welcome!
Maritime Term
Copyright (c) 2004-2007 Nectar Corp
Ahoy>
```

5. 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.

5.1. General Test Approach

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.

5.2. Test Results

Nectar CMP successfully provided VoIP call quality data on various types of calls discussed in Section 5.1. 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 S8720 Servers.

6. 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

7. 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 the support telephone number at (888) 8-N-E-C-T-A-R.

8. Conclusion

These Application Notes illustrate the procedures for configuring Nectar CMP to monitor and correctly provide VoIP call quality statistics on the various types of calls placed to and from stations. 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.

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] *Administration for Network Connectivity for Avaya Communication Manager*, Issue 10, June 2005, Document Number 555-233-504.

[2] *Administrator Guide for Avaya Communication Manager*, Issue 1, June 2005, Document Number 03-300509

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

[3] *Nectar CMP V2.1 Vendor Knowledge Module (VKM) for Avaya Communication Manager (IP Enabled)*, August 2008, Document Version 1.5

[4] *Nectar CMP V2.1 Technical Overview Briefing*, August 2008, Document Version 1.5

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.