Avaya Solution & Interoperability Test Lab

Application Notes for TONE Software's ReliaTel with Avaya Communication Manager – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for the TONE Software Corporation's ReliaTel Monitoring and Management platform to interoperate with Avaya Communication Manager. ReliaTel is a monitoring and management solution that can monitor and maintain groups of telephone switches, PBX systems, and other devices from a single control point. In the compliance testing, ReliaTel used the SNMP interfaces from Avaya Communication Manager to provide alarm monitoring.

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 steps required for the TONE Software Corporation's ReliaTel Monitoring and Management platform to interoperate with Avaya Communication Manager. ReliaTel is a monitoring and management solution that can monitor and maintain groups of telephone switches, PBX systems, and other devices from a single control point. In the compliance testing, ReliaTel used the SNMP interfaces from the Avaya S8500 Server and the Avaya G250 Media Gateway to provide alarm monitoring.

Upon detection of a failure, the Avaya S8500 Server or the Avaya G250 Media Gateway can raise alarms and send SNMP traps to ReliaTel. ReliaTel collects and stores the alarm information from the Avaya Communication Manager SNMP traps, and presents the alarms on the monitoring screen. The integration uses SNMP version 2c.

1.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the following with ReliaTel: generation of SNMP traps on the Avaya S8500 Server, generation of SNMP traps on the Avaya G250 Media Gateway, display of received SNMP traps on the ReliaTel web-based alarm monitoring screen, and comparison of the displayed SNMP trap information with a protocol analyzer.

The serviceability testing focused on verifying the ability of ReliaTel to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet cable to ReliaTel.

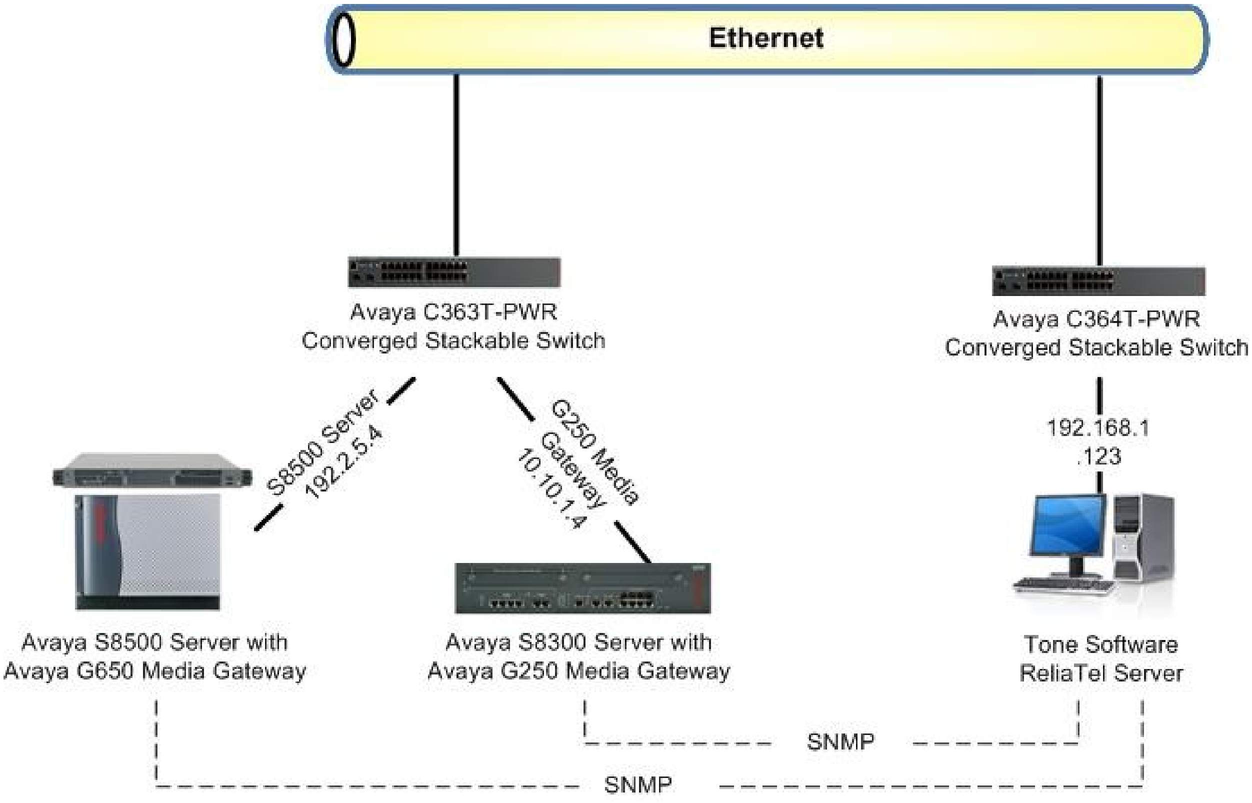
1.2. Support

Technical support on ReliaTel can be obtained through the following:

- **Phone:** (800) 833-8663
- **Email:** info@tonesoft.com
- **Web:** http://www.tonesoft.com/support/portal2.html

2. Reference Configuration

Avaya Communication Manager provides SNMP interfaces for the Avaya S8xxx Servers and the Avaya G250/G350/G450 Media Gateways. The test configuration used two Avaya Communication Manager systems – one system with an Avaya S8500 Server and an Avaya G650 Media Gateway, and the other system with an Avaya S8300 Server and an Avaya G250 Media Gateway. In the compliance testing, the ReliaTel server used the SNMP interfaces to monitor the alarms on the Avaya S8500 Server and on the Avaya G250 Media Gateway. The results in these Application Notes should be applicable to other Avaya S8xxx Servers and the Avaya G350 Media Gateway.



3. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server with Avaya G650 Media Gateway	Avaya Communication Manager 5.1.2, R015x.01.2.416.4
Avaya S8300 Server with Avaya G250 Media Gateway	Avaya Communication Manager 5.1.2, R015x.01.2.416.4
TONE Software Corporation's ReliaTel	2.5.2

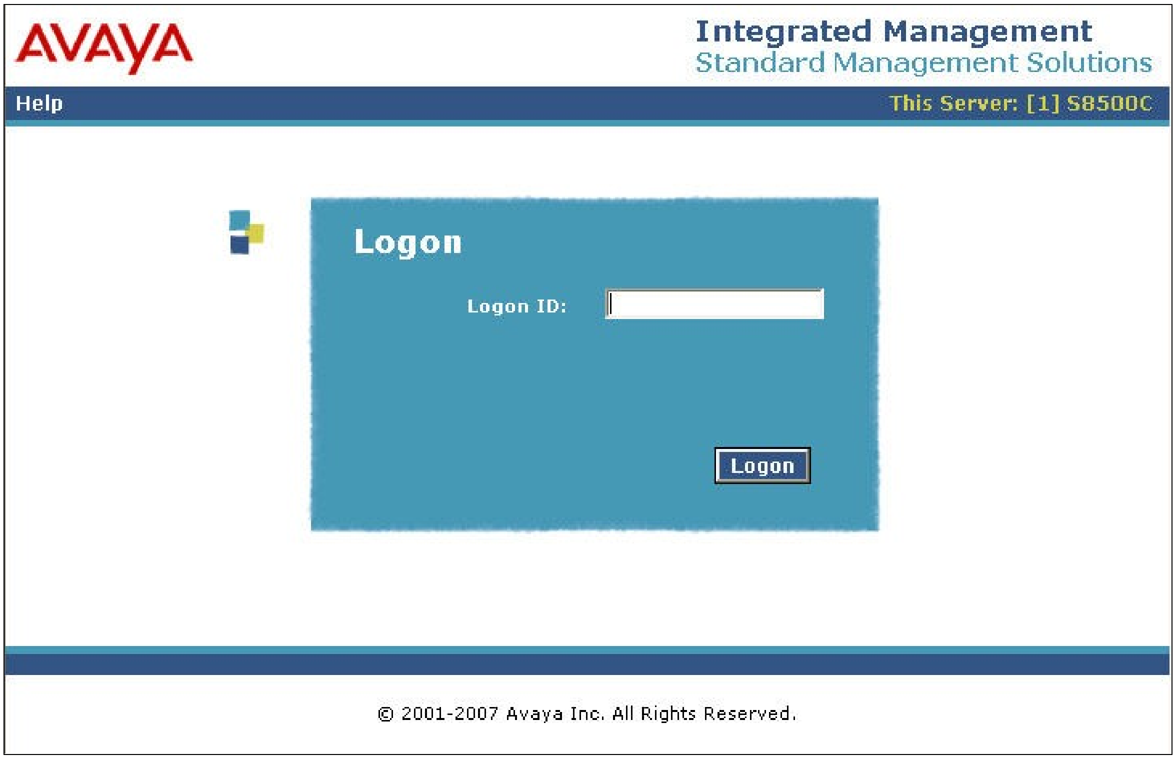
4. Configure Avaya Communication Manager S8500 Server

This section provides the procedures for configuring SNMP on the Avaya Communication Manager S8500 Server. The procedures include the following areas:

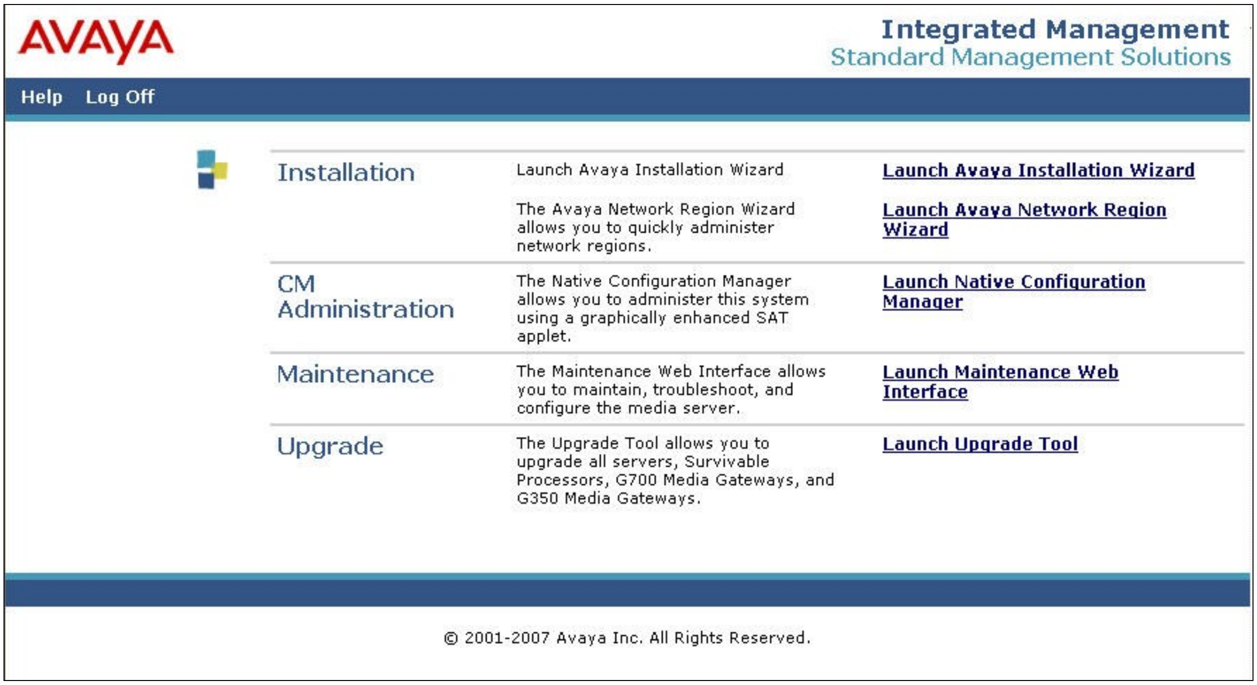
- Launch maintenance web interface
- Administer firewall
- Administer SNMP traps

4.1. Launch Maintenance Web Interface

Access the Avaya Communication Manager web interface by using the URL "http://ip-address" in an Internet browser window, where "ip-address" is the IP address of Avaya Communication Manager. Log in with the appropriate credentials.


AVAYA
Integrated Management
Standard Management Solutions
Help
This Server: [1] S8500C
Logon
Logon ID:
Logon
© 2001-2007 Avaya Inc. All Rights Reserved.

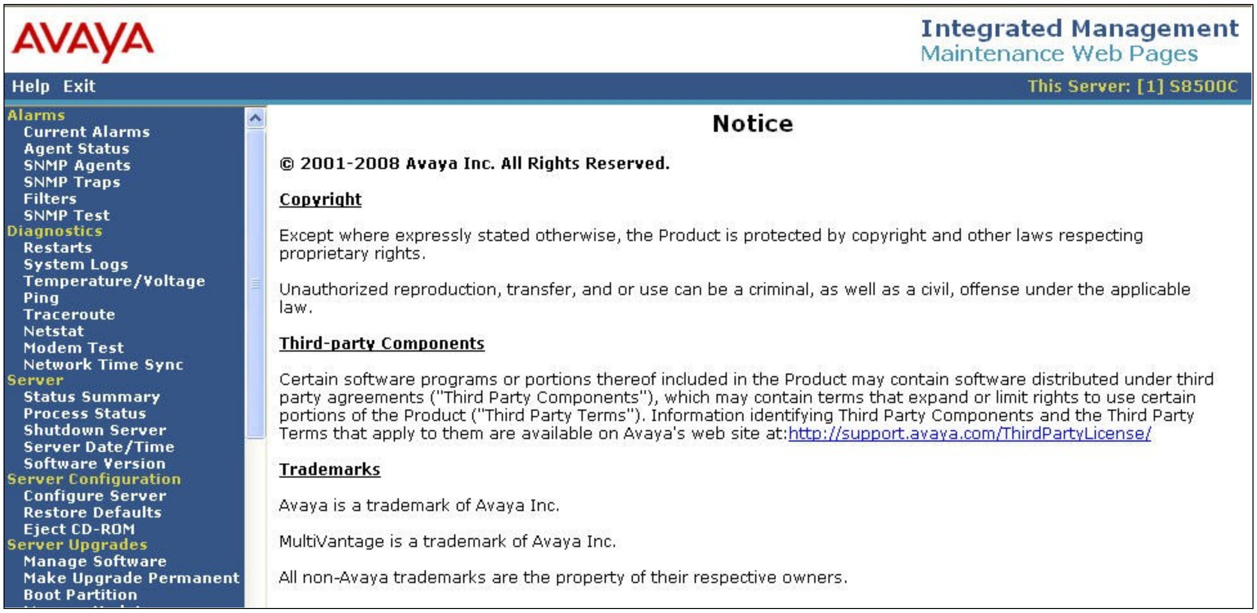
In the subsequent screen, select **Launch Maintenance Web Interface**.



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 media 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

© 2001-2007 Avaya Inc. All Rights Reserved.

The **Notice** screen is displayed next.



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

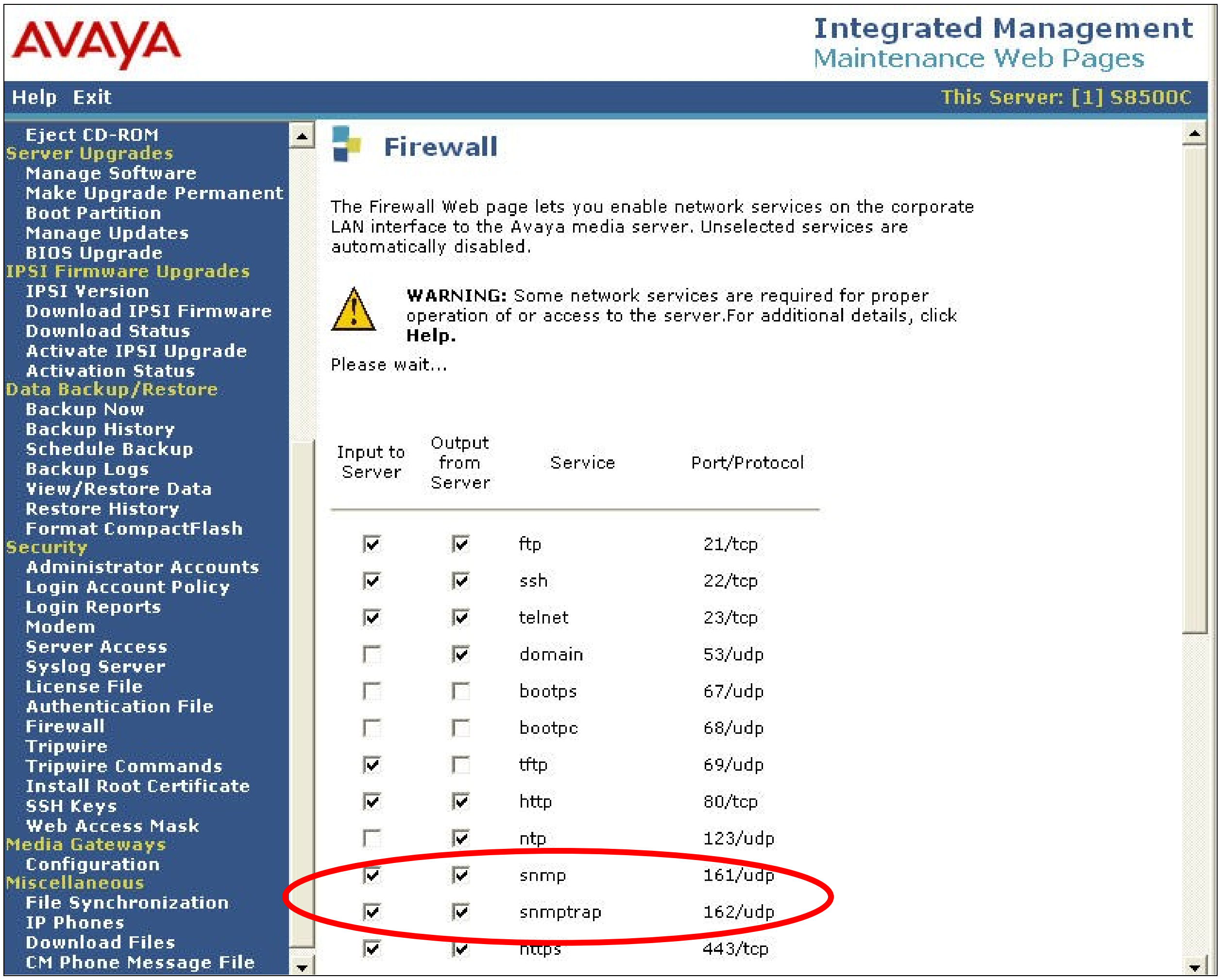
Avaya is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

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

4.2. Administer Firewall

Select **Security > Firewall** from the left pane. The **Firewall** screen is displayed. Check the **Input to Server** and **Output from Server** fields for **snmp** and **snmptrap**, as shown below.



Firewall

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

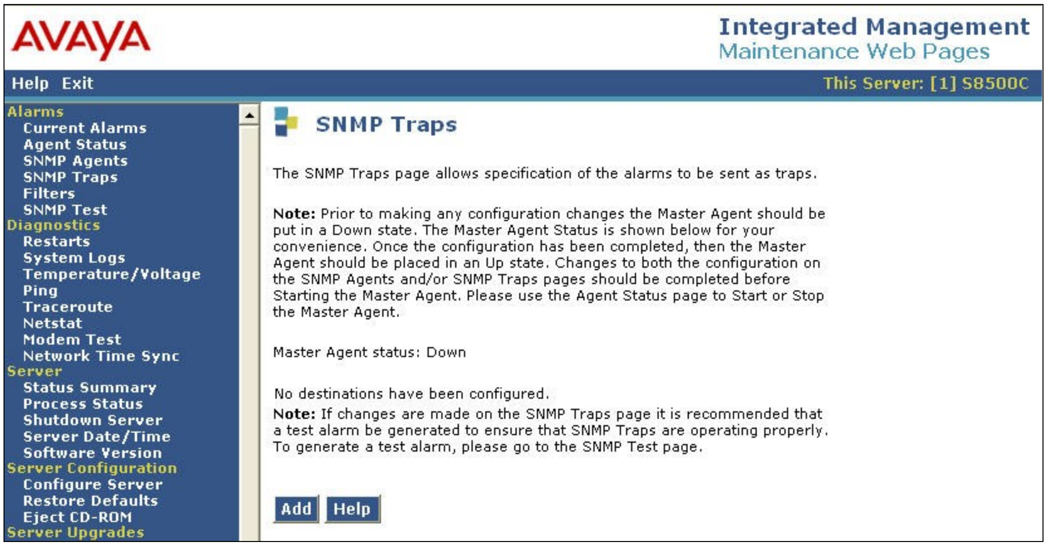
WARNING: Some network services are required for proper operation of or access to the server.For additional details, click **Help.**

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

4.3. Administer SNMP Traps

Select **Alarms > SNMP Traps** from the left pane. The **SNMP Traps** screen is displayed. Click **Add**.



SNMP Traps

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

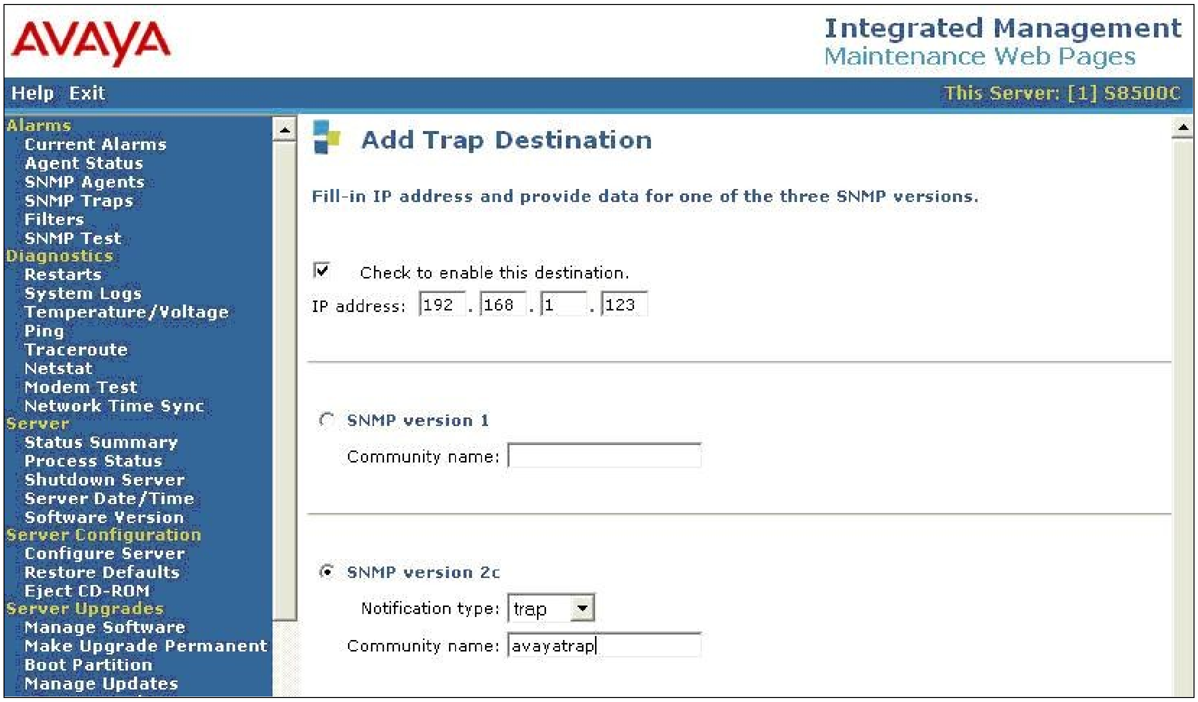
Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP 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: Down

No destinations have been configured.

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.

The **Add Trap Destination** screen is displayed next. Check the **Check to enable this destination** field, and enter the IP address of the ReliaTel server into the **IP address** field. Select the radio button for **SNMP version 2c**, and enter a desired string for **Community name**. Note that the community name is not used by ReliaTel, but still needs to be configured. Retain the default values in the remaining fields.



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 . 168 . 1 . 123

○ SNMP version 1

Community name:

● SNMP version 2c

Notification type: trap

Community name: avayatrap

5. Configure Avaya Communication Manager G250 Media Gateway

This section provides the procedures for configuring SNMP on the Avaya Communication Manager G250 Media Gateway. The procedures include the following areas:

- Administer community
- Administer SNMP traps
- Show SNMP

5.1. Administer Community

Access the G250 Media Gateway CLI interface, and log in with the appropriate credentials. Use the "set snmp community" command shown below to set the SNMP community and the access level. Note that the community can be set to any desired string, and "avayatrap" was used in the compliance testing.

```
G250-001(super)# set snmp community read-only avayatrap
SNMP read-only community string set.
```

5.2. Administer SNMP Traps

Use the "snmp-server host" command shown below to enable SNMP traps and notifications to ReliaTel. In the compliance testing, "192.168.1.123" is the IP address of the ReliaTel server, and "avayatrap" is the community string from **Section 5.1**.

```
G250-001(super)# snmp-server host 192.168.1.123 traps v2c avayatrap udp-port
162 all
Done!
```

5.3. Show SNMP

The “show snmp” command shown below can be used to display the list of SNMP receivers.

```
G250-001(super)# show snmp

Authentication trap disabled

Community-Access     Community-String
----------------     ----------------
read-only            *****


SNMPv3 Notifications Status
-----------------------------
Traps:  Enabled
Informs:  Enabled         Retries: 3   Timeout: 3 seconds


SNMP-Rec-Address Model  Level   Notification   Trap/Inform      User name
---------------- ----- ------- --------------- ----------- ------------------

192.168.1.123     v2c  noauth  all              trap       ReadCommN
 UDP port: 162
```

6. Configure TONE Software ReliaTel

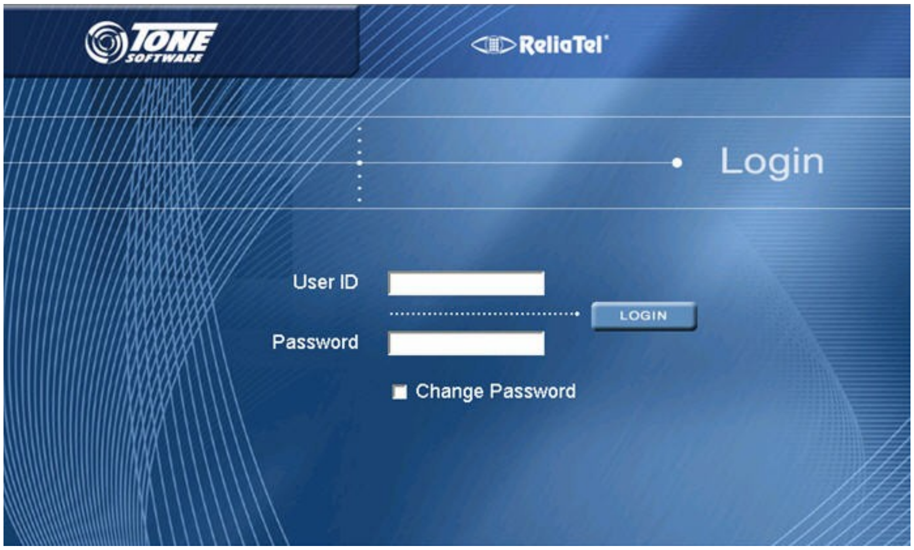
This section provides the procedures for configuring TONE Software ReliaTel. The procedures include the following areas:

- Launch web interface
- Administer centers
- Administer entities
- Administer IP address

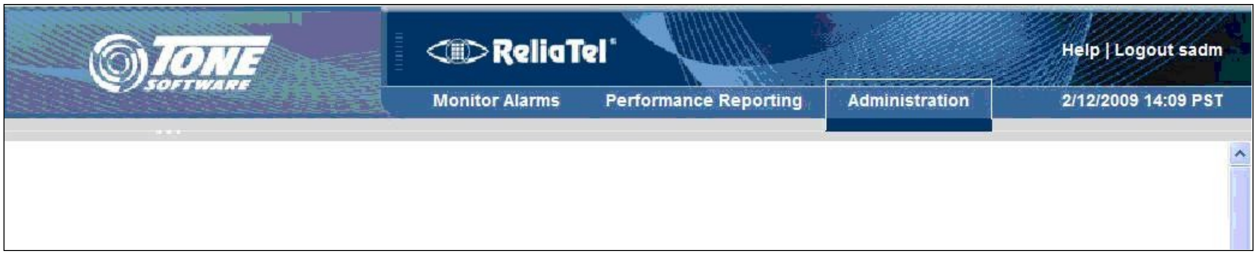
The configuration of ReliaTel is typically performed by TONE Software technicians. The procedural steps are presented in these Application Notes for informational purposes.

6.1. Launch Web Interface

Access the ReliaTel web interface by using the URL "http://ip-address:8080/ems/app" in an Internet browser window, where "ip-address" is the IP address of the ReliaTel server. Log in with the appropriate credentials.

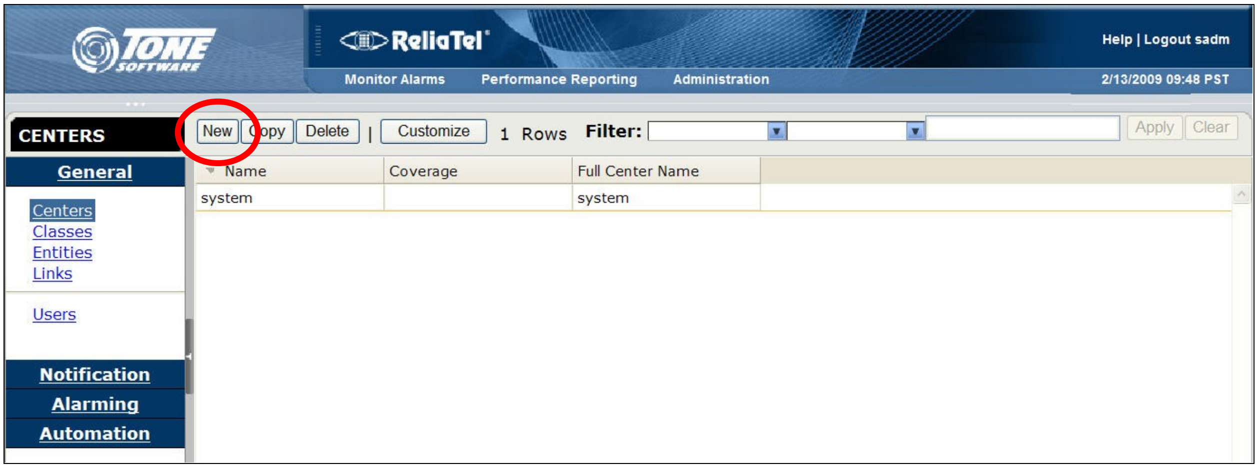


In the subsequent screen, select **Administration** from the top menu, as shown below.



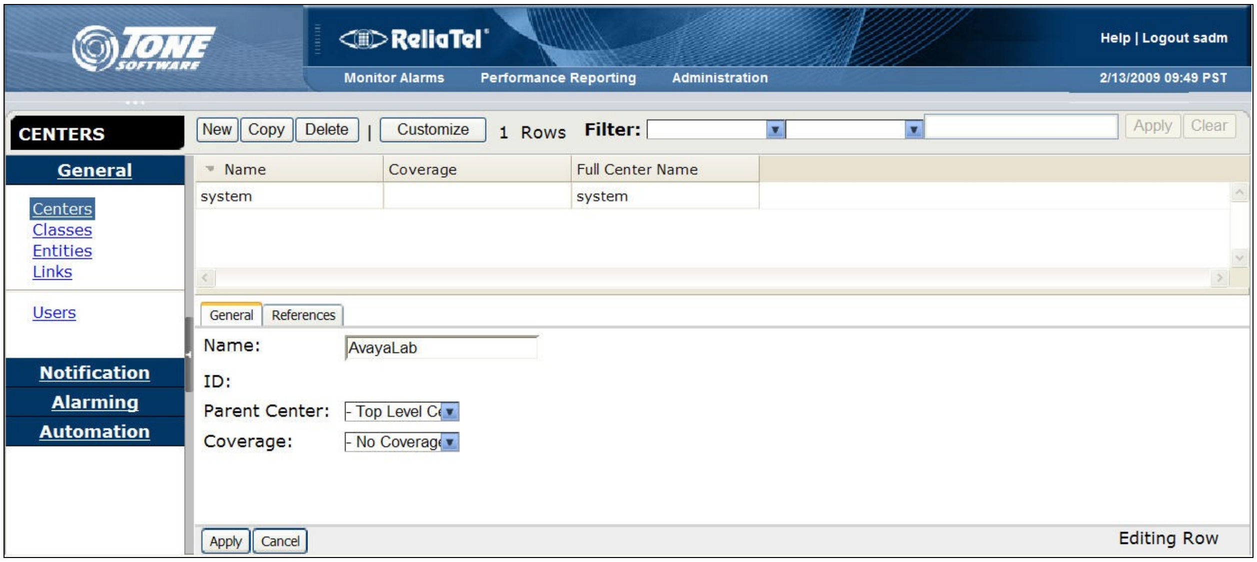
6.2. Administer Centers

From the ReliaTel screen, select **General > Centers** in the left pane to display a list of centers in the right pane. Click **New** to create a new center.



Name	Coverage	Full Center Name
system		system

In the lower portion of the screen, select the **General** tab. Enter a descriptive **Name**. Retain the default values in the remaining fields, and click **Apply**.

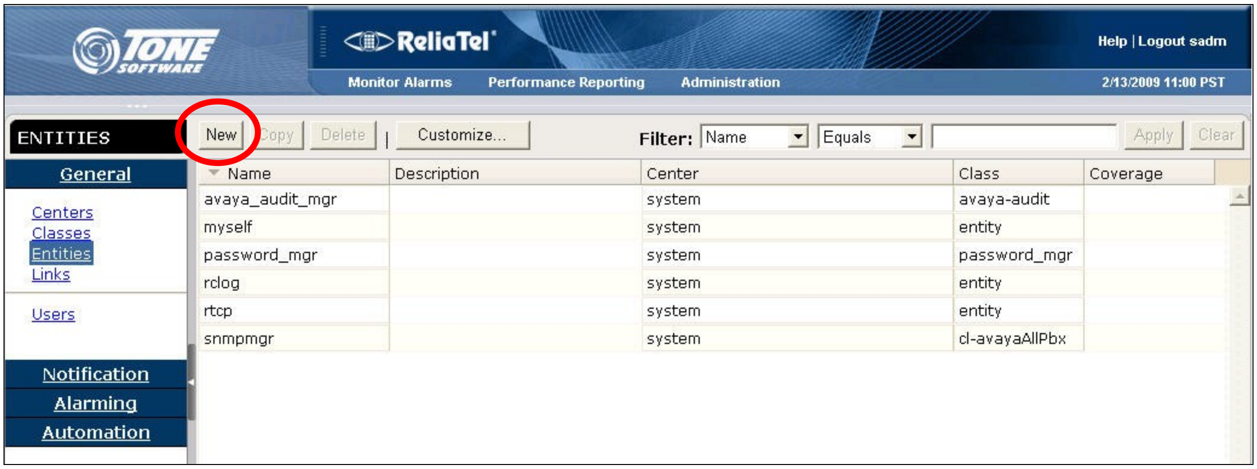


Name	Coverage	Full Center Name
system		system

Name: AvayaLab
ID:
Parent Center: - Top Level Ce
Coverage: - No Coverag

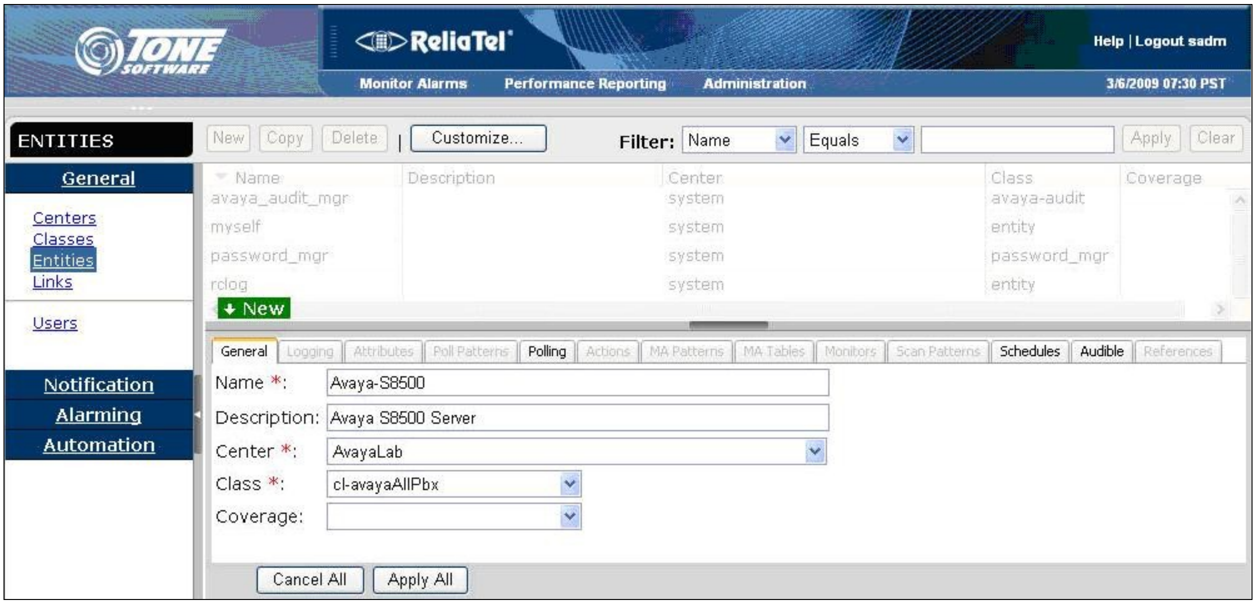
6.3. Administer Entities

From the ReliaTel screen, select **General > Entities** in the left pane to display a list of entities in the right pane. Click **New** to create a new entity.



Name	Description	Center	Class	Coverage
avaya_audit_mgr		system	avaya-audit	
myself		system	entity	
password_mgr		system	password_mgr	
rclog		system	entity	
rtcp		system	entity	
snmpmgr		system	cl-avayaAllPbx	

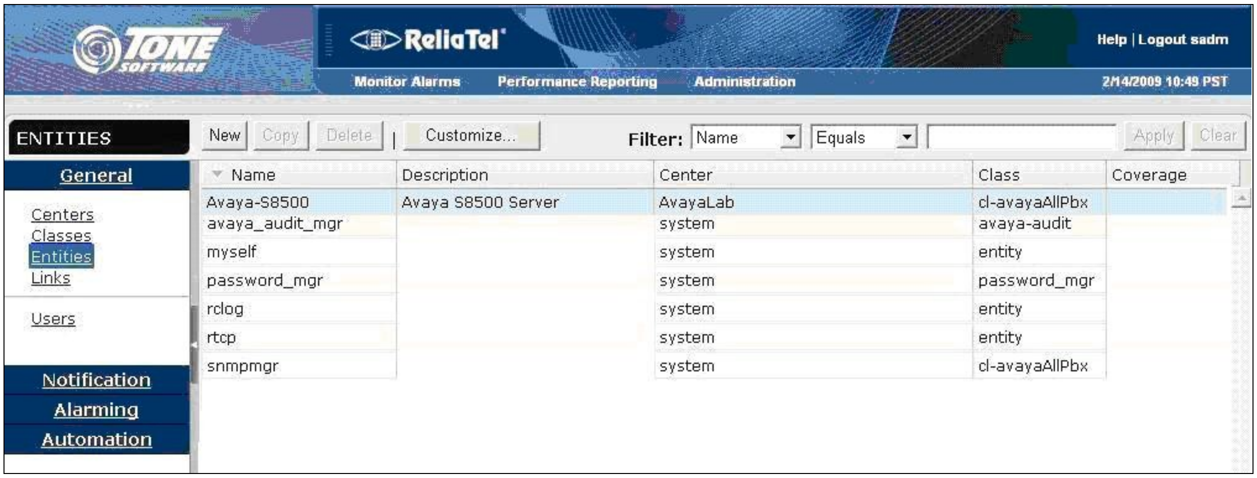
In the lower portion of the screen, select the **General** tab. Enter a descriptive **Name** and **Description** for the Avaya S8500 Server. For **Center**, select the center name from **Section 6.2**, in this case "AvayaLab". For **Class**, select "cl-avayaAllPbx" from the drop-down list, as shown below. Click **Apply All**.



Name	Description	Center	Class	Coverage
avaya_audit_mgr		system	avaya-audit	
myself		system	entity	
password_mgr		system	password_mgr	
rclog		system	entity	

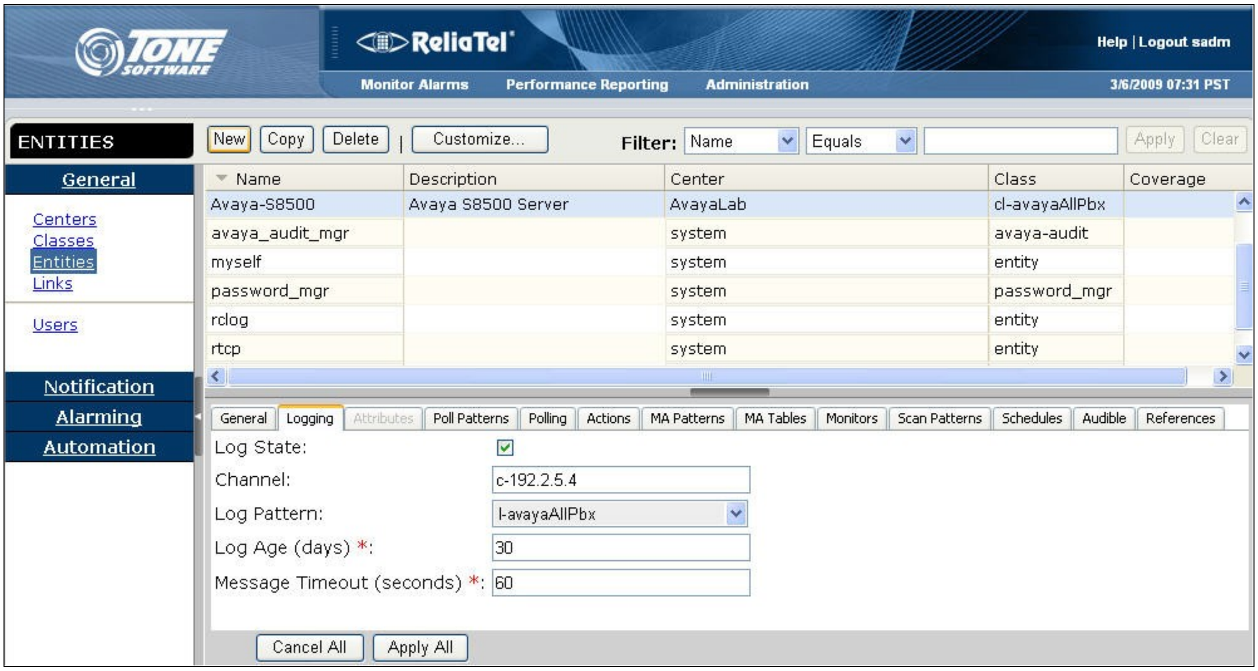
Name *: Avaya-S8500
Description: Avaya S8500 Server
Center *: AvayaLab
Class *: cl-avayaAllPbx
Coverage:

The ReliaTel screen is refreshed and shows the newly added entity. Double click on the new entity, in this case “Avaya-S8500”.



Name	Description	Center	Class	Coverage
Avaya-S8500	Avaya S8500 Server	AvayaLab	cl-avayaAllPbx	
avaya_audit_mgr		system	avaya-audit	
myself		system	entity	
password_mgr		system	password_mgr	
rclog		system	entity	
rtcp		system	entity	
snmpmgr		system	cl-avayaAllPbx	

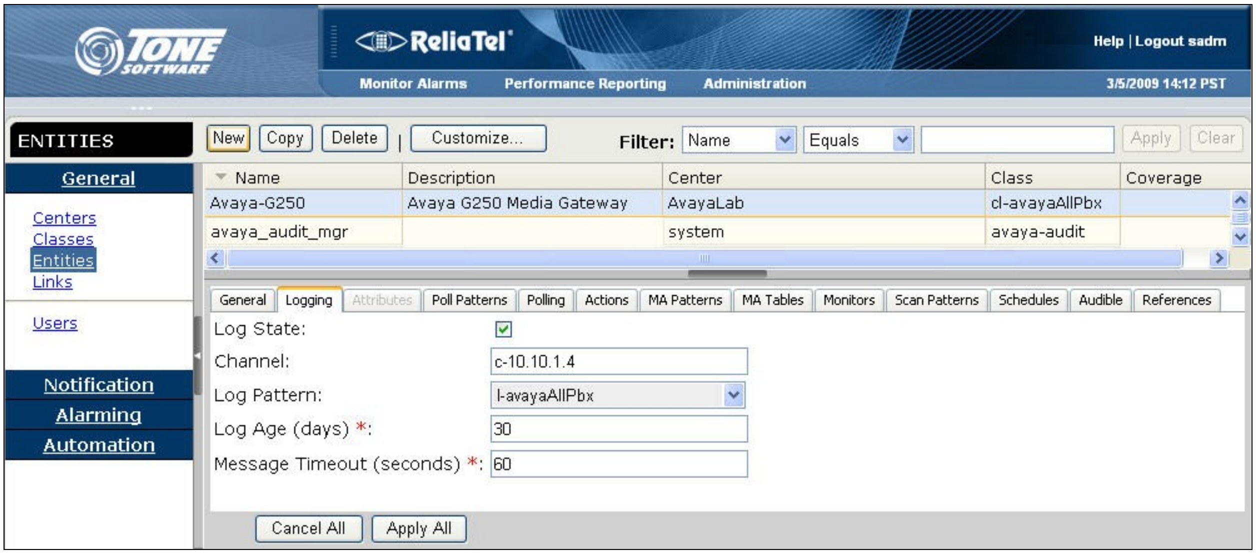
In the lower portion of the screen, select the **Logging** tab. Check the **Log State** field to enable logging. Enter a descriptive name for **Channel**. Retain the default values in the remaining fields, and click **Apply All**.



Name	Description	Center	Class	Coverage
Avaya-S8500	Avaya S8500 Server	AvayaLab	cl-avayaAllPbx	
avaya_audit_mgr		system	avaya-audit	
myself		system	entity	
password_mgr		system	password_mgr	
rclog		system	entity	
rtcp		system	entity	

Log State: ☑
Channel: c-192.2.5.4
Log Pattern: l-avayaAllPbx
Log Age (days) *: 30
Message Timeout (seconds) *: 60

Repeat the procedures in this section to create an entity for the Avaya G250 Media Gateway. In the compliance testing, the Avaya G250 Media Gateway entity was configured with “Avaya-G250” as the name and “c-10.10.1.4” as the channel, as shown below.



Name	Description	Center	Class	Coverage
Avaya-G250	Avaya G250 Media Gateway	AvayaLab	cl-avayaAllPbx	
avaya_audit_mgr		system	avaya-audit	

Log State: ☑
Channel: c-10.10.1.4
Log Pattern: l-avayaAllPbx
Log Age (days) *: 30
Message Timeout (seconds) *: 60

6.4. Administer IP Address

Log in to the Linux shell of the TONE Software ReliaTel server with administrative rights. Navigate to the "conf" directory to edit the "cdata.conf" file, as shown below.

```
[xx@yy ~]# cd /export/home/ems/etc/conf

[xx@yy conf]# vi cdata.conf
```

Scroll to the end of the file, and add new lines to associate the IP address of the Avaya S8500 Server and the Avaya G250 Media Gateway with the channel names from **Section 6.3**, as shown below. Save the file.

```
[c-snmpmgr]
chanType = SNMPMGR
account  =
port     = 1162

[c-192.2.5.4]
chanType = SNMPMGR
account  = 192.2.5.4

[c-10.10.1.4]
chanType = SNMPMGR
account  = 10.10.1.4
```

In the Linux prompt, issue the "pkill" command to restart the necessary components.

```
[xx@yy conf]# pkill -HUP dapmgr
```

7. General Test Approach and Test Results

The feature test cases were performed manually. Different SNMP traps were generated on the Avaya S8500 Server and the Avaya G250 Media Gateway and verified on the ReliaTel web-based alarm monitoring screen. The verification also included the use of a protocol analyzer to view the SNMP traps sent from Avaya Communication Manager. The different SNMP traps included the following:

- Avaya S8500 Server reboot
- Avaya S8500 Server SNMP agent restart
- Avaya S8500 Server test SNMP command
- Avaya S8500 Server IPSI circuit pack disconnect/reconnect
- Avaya G250 Media Gateway media module reset
- Avaya G250 Media Gateway VoIP engine reset
- Avaya G250 Media Gateway VoIP engine busyout/release
- Avaya G250 Media Gateway failed authentication

The serviceability test cases were performed manually by disconnecting/reconnecting Ethernet cable to the ReliaTel server.

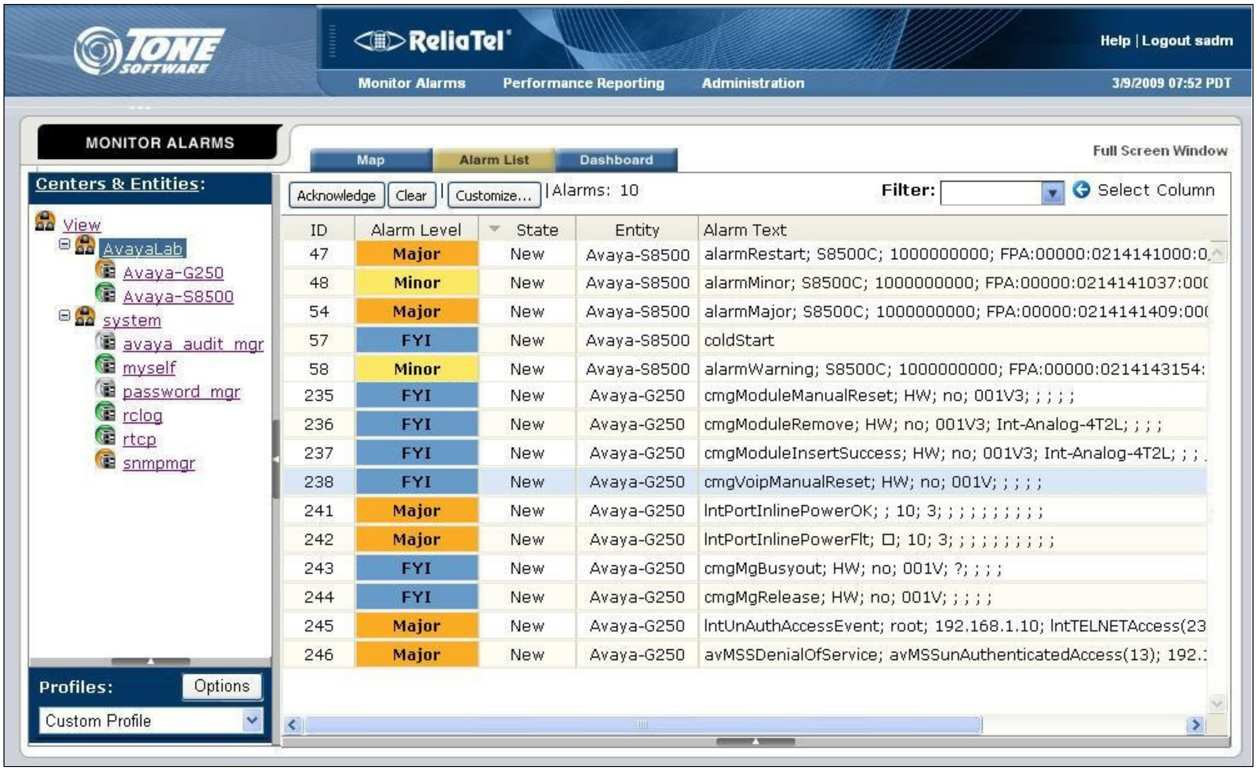
All test cases were executed and passed.

8. Verification Steps

This section provides the test that can be performed to verify proper configuration of Avaya Communication Manager and ReliaTel.

Generate alarm events on the Avaya S8500 Server and on the Avaya G250 Media Gateway. With a protocol analyzer, verify that SNMP traps are sent to the ReliaTel server.

In the ReliaTel screen, select **Monitor Alarms** from the top menu. Select **View > AvayaLab** in the left pane, where "AvayaLab" is the name of the center from **Section 6.2**. Verify that the new alarms are displayed in the right pane, as shown below.



ID	Alarm Level	State	Entity	Alarm Text
47	Major	New	Avaya-S8500	alarmRestart; S8500C; 1000000000; FPA:00000:0214141000:0
48	Minor	New	Avaya-S8500	alarmMinor; S8500C; 1000000000; FPA:00000:0214141037:00
54	Major	New	Avaya-S8500	alarmMajor; S8500C; 1000000000; FPA:00000:0214141409:00
57	FYI	New	Avaya-S8500	coldStart
58	Minor	New	Avaya-S8500	alarmWarning; S8500C; 1000000000; FPA:00000:0214143154:
235	FYI	New	Avaya-G250	cmgModuleManualReset; HW; no; 001V3; ; ; ; ;
236	FYI	New	Avaya-G250	cmgModuleRemove; HW; no; 001V3; Int-Analog-4T2L; ; ; ;
237	FYI	New	Avaya-G250	cmgModuleInsertSuccess; HW; no; 001V3; Int-Analog-4T2L; ; ;
238	FYI	New	Avaya-G250	cmgVoipManualReset; HW; no; 001V; ; ; ; ;
241	Major	New	Avaya-G250	IntPortInlinePowerOK; ; 10; 3; ; ; ; ; ; ; ; ; ;
242	Major	New	Avaya-G250	IntPortInlinePowerFlt; □; 10; 3; ; ; ; ; ; ; ; ; ;
243	FYI	New	Avaya-G250	cmgMgBusyout; HW; no; 001V; ?; ; ; ;
244	FYI	New	Avaya-G250	cmgMgRelease; HW; no; 001V; ; ; ; ;
245	Major	New	Avaya-G250	IntUnAuthAccessEvent; root; 192.168.1.10; IntTELNETAccess(23
246	Major	New	Avaya-G250	avMSSDenialOfService; avMSSunAuthenticatedAccess(13); 192.

9. Conclusion

These Application Notes describe the configuration steps required ReliaTel to successfully interoperate with Avaya Communication Manager. All feature and serviceability test cases were completed.

10. Additional References

This section references the product documentation relevant to these Application Notes.

1. *Administrator Guide for Avaya Communication Manager*, Document 03-300509, Issue 4.0, Release 5.0, January 2008, available at http://support.avaya.com.

2. *Administration for the Avaya G250 and G350 Media Gateways*, Document 03-300436, Issue 5, June 2008, available at http://support.avaya.com.

3. *ReliaTel Monitoring and Management Solution Installation and Configuration Guide*, Version 2 Release 5 Modification 0, contact ReliaTel support at info@tonesoft.com.

4. *ReliaTel Monitoring and Management Solution User's Guide*, Version 2 Release 5 Modification 2, contact ReliaTel support at info@tonesoft.com.

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.