



Avaya Solution & Interoperability Test Lab

Application Notes for TONE Software's ReliaTel with Avaya SIP Enablement Services – 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 SIP Enablement Services. 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 interface from Avaya SIP Enablement Services 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 SIP Enablement Services (SES). 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 interface from Avaya SES to provide alarm monitoring.

Upon detection of a failure, Avaya SES raises an alarm and sends a SNMP trap to ReliaTel. ReliaTel collects and stores the alarm information from the Avaya SES SNMP trap, and presents the alarm 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 Avaya SES, display of received SNMP traps on the ReliaTel web-based alarm monitoring screen, and comparison of the displayed SNMP trap 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.

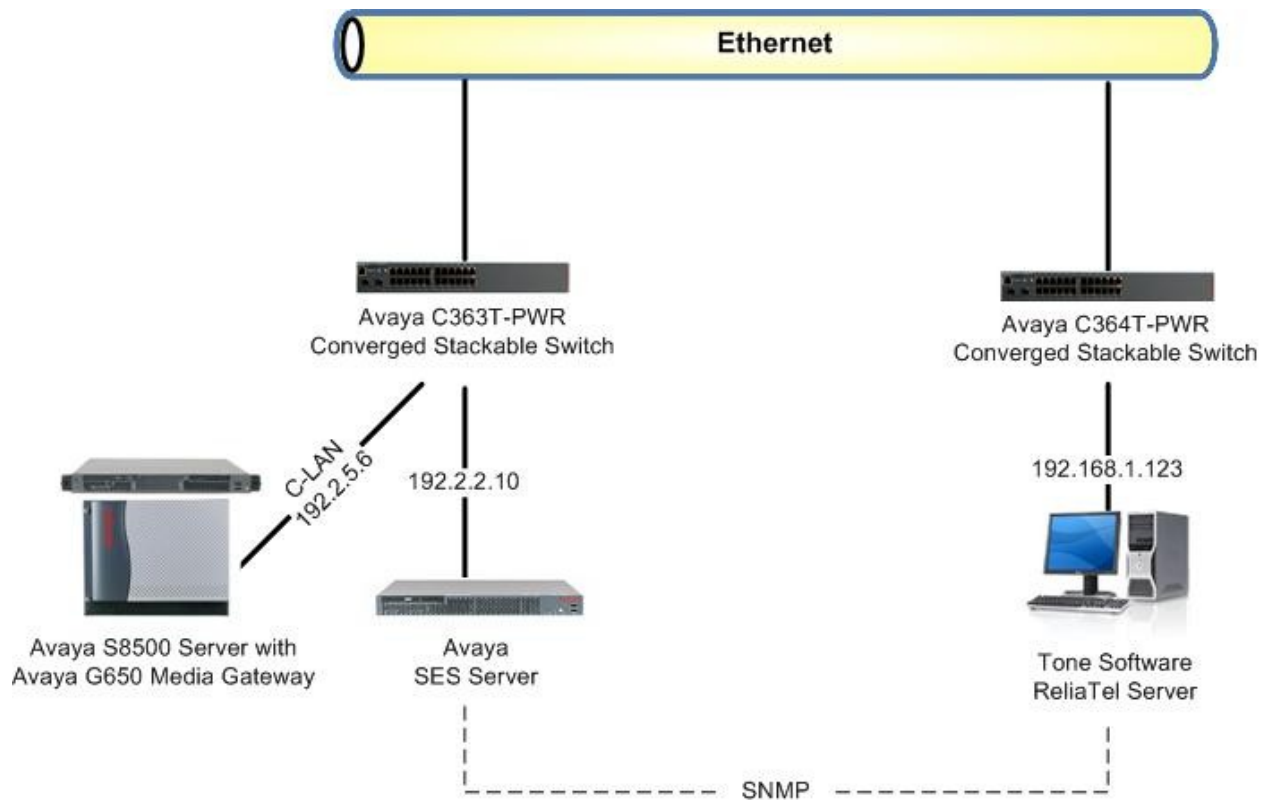
1.2. Support

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

The test configuration used for the compliance testing is shown below.



3. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server	Avaya Communication Manager 5.0, R015x.00.0.825.4
Avaya G650 Media Gateway <ul style="list-style-type: none">• TN799DP C-LAN Circuit Pack	HW13 FW021
Avaya SIP Enablement Services	5.0, SES-5.0.0.0-825.31
TONE Software Corporation's ReliaTel	2.5.2

4. Configure Avaya SIP Enablement Services

The detailed administration of basic connectivity between Avaya Communication Manager and Avaya SES is not the focus of these Application Notes and will not be described. This section provides the procedures for the following:

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

4.1. Launch Maintenance Web Interface

Access the SES web interface by using the URL “http://ip-address/admin” in an Internet browser window, where “ip-address” is the IP address of the SES server. Log in with the appropriate credentials.




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

AVAYA

Integrated Management
Standard Management Solutions

Help Log Off



SES
Administration

The Administration Web Interface allows you to administer this SES server.

[Launch SES Administration Interface](#)

Maintenance

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

[Launch Maintenance Web Interface](#)

The **Notice** screen is displayed next.

AVAYA

Integrated Management
Maintenance Web Pages

Help Exit

This Server: [1] mprsipserver

Alarms

- Current Alarms
- SNMP Traps

Diagnostics

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

Server

- Status Summary
- Process Status
- Shutdown Server
- Server Date/Time
- Software Version

Server Configuration

- Configure Server
- Eject CD-R/DW

Server Upgrades

- Manage Software
- Make Upgrade Permanent
- Boot Partition
- Manage Updates
- BIOS Upgrade

Data Backup/Restore

- Backup Now
- Backup History
- Schedule Backup
- Backup Logs
- View/Restore Data

Notice

© 2001-2007 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.

AVAYA Integrated Management Maintenance Web Pages
This Server: [1] mprsipserv

Help Exit

Alarms
Current Alarms
SNMP Traps

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

Server
Status Summary
Process Status
Shutdown Server
Server Date/Time
Software Version

Server Configuration
Configure Server
Eject CD-ROM

Server Upgrades
Manage Software
Make Upgrade Permanent
Boot Partition
Manage Updates
BIOS Upgrade

Data Backup/Restore
Backup Now
Backup History
Schedule Backup

Server Upgrades
Manage Software
Make Upgrade Permanent
Boot Partition
Manage Updates
BIOS Upgrade

Data Backup/Restore
Backup Now
Backup History
Schedule Backup
Backup Logs
View/Restore Data
Restore History
Format CompactFlash

Security
Administrator Accounts
Login Account Policy
Login Reports
Modem
Server Access
Syslog Server
Authentication File
Firewall
Tripwire
Tripwire Commands
Install Root Certificate
SSH Keys
Web Access Mask

Miscellaneous
File Synchronization
Download Files

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
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ftp	21/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	ssh	22/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	telnet	23/tcp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	domain	53/udp
<input type="checkbox"/>	<input type="checkbox"/>	bootps	67/udp
<input type="checkbox"/>	<input type="checkbox"/>	bootpc	68/udp
<input checked="" type="checkbox"/>	<input type="checkbox"/>	tftp	69/udp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	http	80/tcp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ntp	123/udp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	snmp	161/udp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	snmptrap	162/udp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	https	443/tcp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	syslog	514/udp
<input type="checkbox"/>	<input type="checkbox"/>	ldap	389/tcp
<input type="checkbox"/>	<input type="checkbox"/>	ldaps	636/tcp
<input type="checkbox"/>	<input type="checkbox"/>	radius	1812/udp
<input type="checkbox"/>	<input type="checkbox"/>	securID	5500/udp
<input type="checkbox"/>	<input type="checkbox"/>	safeword	5030/tcp
<input checked="" type="checkbox"/>	<input type="checkbox"/>	http-iphone	81/tcp
<input checked="" type="checkbox"/>	<input type="checkbox"/>	https-iphone	411/tcp
<input checked="" type="checkbox"/>	<input type="checkbox"/>	hp-sshd	2222/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	secure-sat	5022/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	def-sat	5023/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	echo-request	8/icmp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	unknown	61613/tcp
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	unknown	61616/tcp
<input type="checkbox"/>	<input checked="" type="checkbox"/>	unknown	1024:65535/udp

4.3. Administer SNMP Traps

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



AVAYA Integrated Management Maintenance Web Pages
This Server: [1] mprsiserver

Help Exit

SNMP Traps

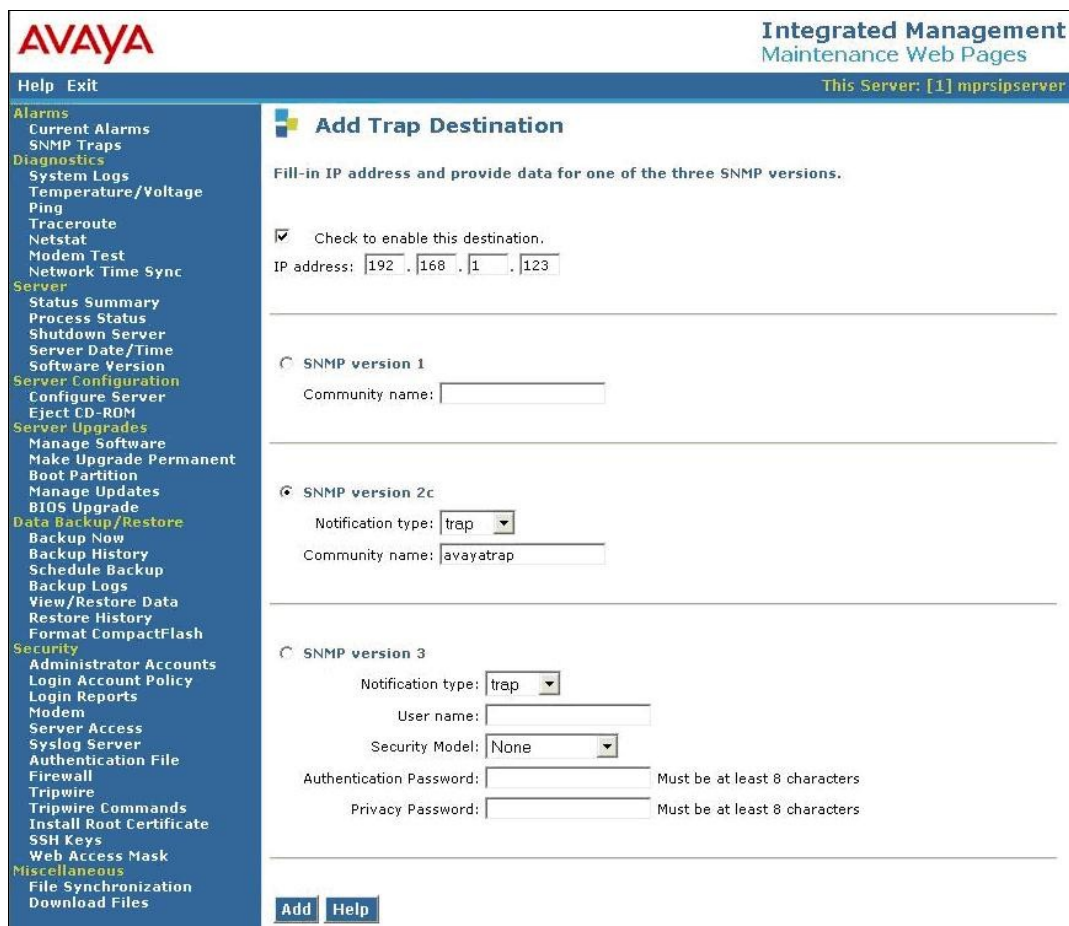
The SNMP Traps page allows specification of the alarms to be sent as traps.

Current Settings

Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Privacy Password
No destinations have been configured.							

Add **Help**

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 on Avaya SES. Retain the default values in the remaining fields.



AVAYA Integrated Management Maintenance Web Pages
This Server: [1] mprsiserver

Help Exit

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]

☐ SNMP version 3
Notification type: [trap]
User name: []
Security Model: [None]
Authentication Password: [] Must be at least 8 characters
Privacy Password: [] Must be at least 8 characters

Add **Help**

5. Configure TONE Software Corporation's ReliaTel Solution

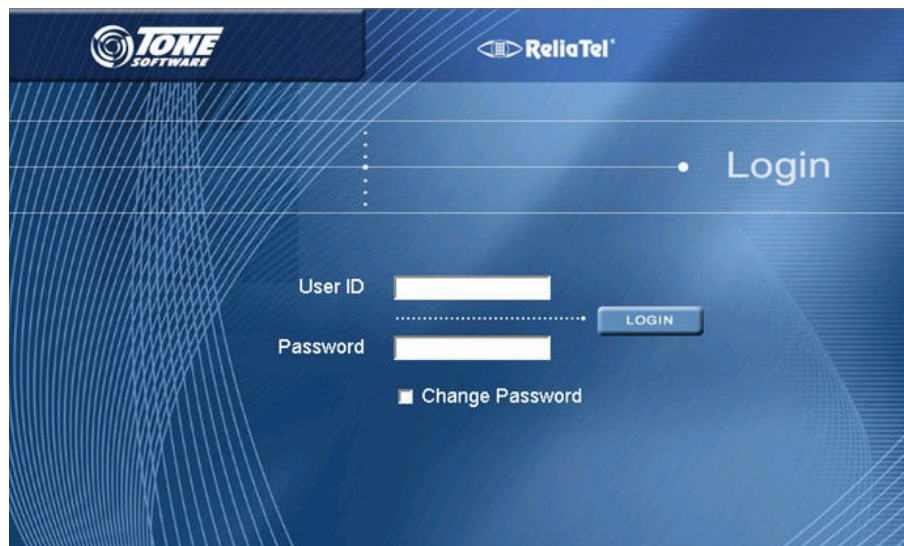
This section provides the procedures for configuring TONE Software Corporation's ReliaTel solution. The procedures include the following areas:

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

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

5.1. 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.



5.2. 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.

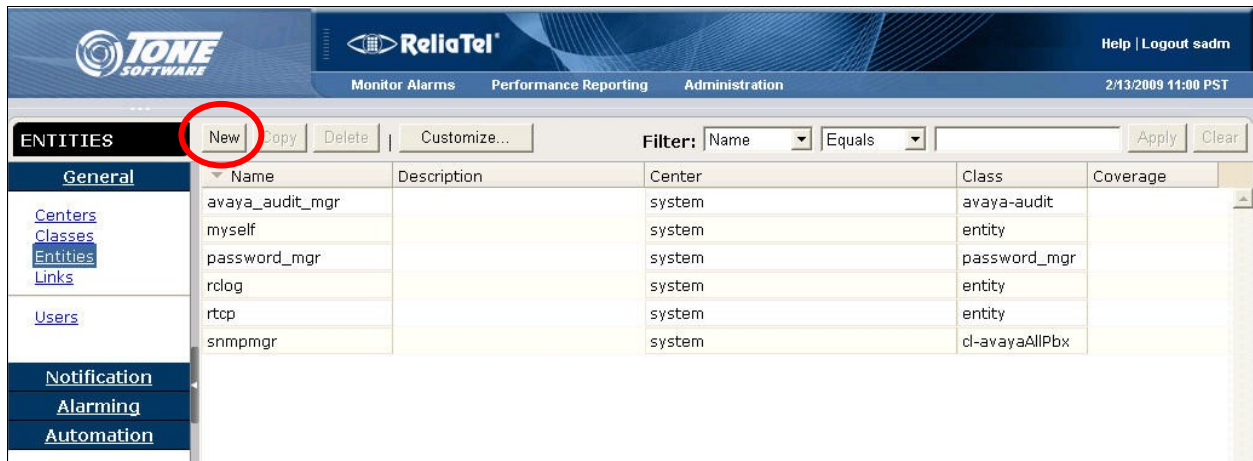
The screenshot shows the ReliaTel Administration interface. The top navigation bar includes the TONE SOFTWARE logo, the ReliaTel logo, and links for Monitor Alarms, Performance Reporting, and Administration. The user is logged in as 'sadm' on 2/13/2009 at 09:48 PST. The left sidebar shows the 'CENTERS' menu with sub-items: General, Centers, Classes, Entities, Links, Users, Notification, Alarming, and Automation. The 'New' button in the top toolbar is circled in red. The main area displays a table with one row: 'system' under the 'Name' column, and 'system' under the 'Full Center Name' column. The table has columns for Name, Coverage, and Full Center Name.

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

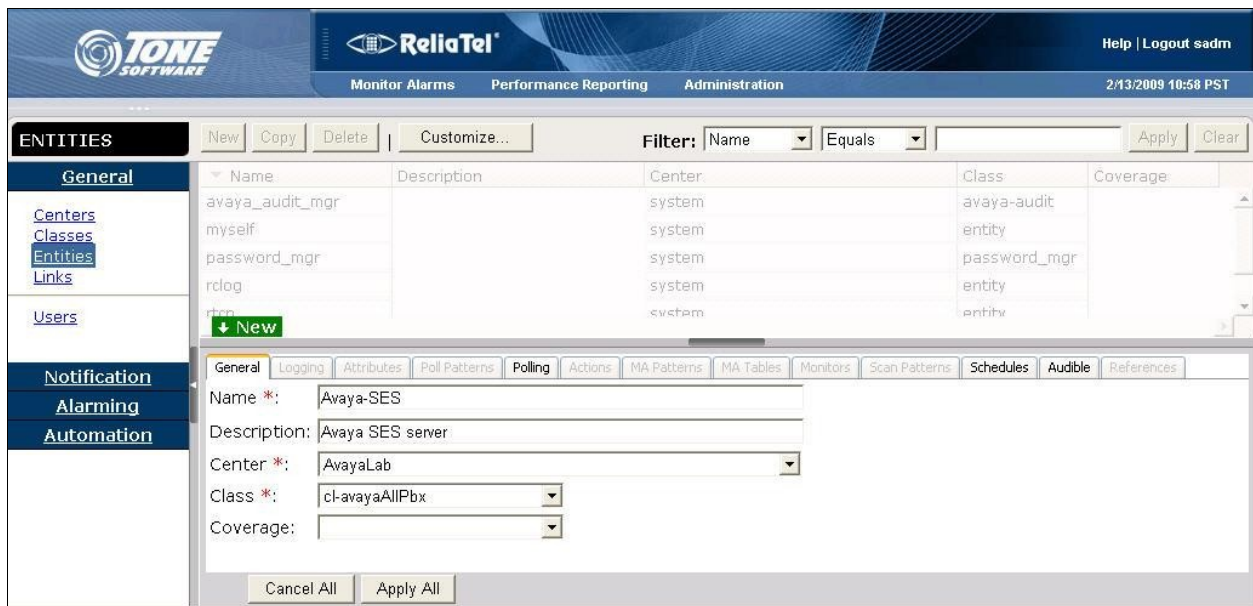
The screenshot shows the ReliaTel Administration interface with the 'General' tab selected for a new center. The top navigation bar and sidebar are the same as in the previous screenshot. The main area displays a form with the following fields: Name (AvayaLab), ID (empty), Parent Center (Top Level C), and Coverage (No Coverage). The 'Apply' button is visible at the bottom left, and the 'Editing Row' status is shown at the bottom right.

5.3. 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.



In the lower portion of the screen, select the **General** tab. Enter a descriptive **Name** and **Description**. For **Center**, select the center name from **Section 5.2**, in this case “AvayaLab”. For **Class**, select “cl-avayaAllPbx” from the drop-down list, as shown below. Click **Apply All**.



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

The screenshot shows the ReliaTel Administration interface. The 'ENTITIES' tab is selected. A table lists several entities, with 'Avaya-SES' highlighted. The table has columns for Name, Description, Center, Class, and Coverage.

Name	Description	Center	Class	Coverage
Avaya-SES	Avaya SES 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**.

The screenshot shows the 'Logging' configuration for the 'Avaya-SES' entity. The 'Log State' checkbox is checked. The 'Channel' field is set to 'c-192.2.2.10'. The 'Log Pattern' is set to 'l-avayaAllPbx'. The 'Log Age (days)' is set to 30, and the 'Message Timeout (seconds)' is set to 60.

Log State	Channel	Log Pattern	Log Age (days) *	Message Timeout (seconds) *
<input checked="" type="checkbox"/>	c-192.2.2.10	l-avayaAllPbx	30	60

5.4. Administer IP Address

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

```
[ReliaTel ~]# cd /export/home/ems/etc/conf  
[ReliaTel conf]# vi cdata.conf
```

Scroll to the end of the file, and add three new lines to associate the IP address of the Avaya SES server with the channel name from **Section 5.3**, as shown below. Save the file.

```
[c-snmppmgr]  
chanType = SNMPMGR  
account  =  
port     = 1162  
  
[c-192.2.2.10]  
chanType = SNMPMGR  
account  = 192.2.2.10
```

In the Linux prompt, issue the “pkill” command to restart all necessary components.

```
[ReliaTel conf]# pkill -HUP dapmgr
```

6. General Test Approach and Test Results

The feature test cases were performed manually. Different SNMP traps were generated on Avaya SES 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 SES. The different SNMP traps included Avaya SES reboot, expired Avaya SES license, and multiple login failures.

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

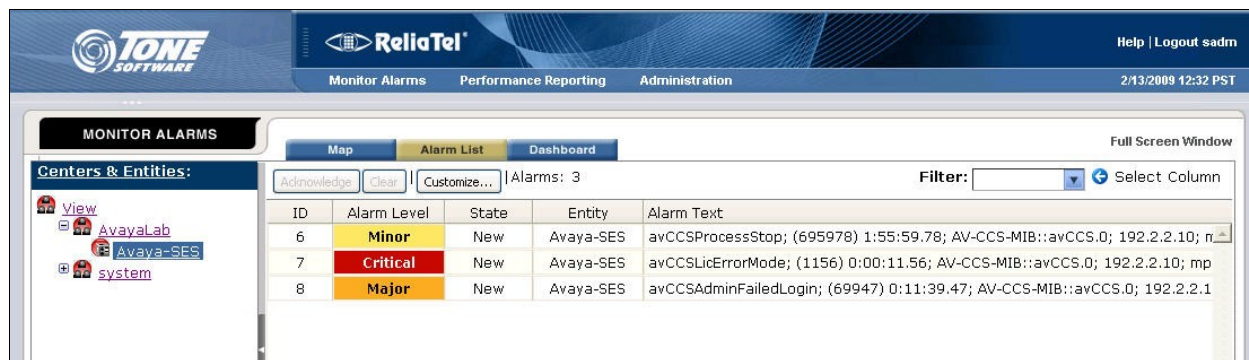
All test cases were executed and passed.

7. Verification Steps

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

Generate an alarm event on the Avaya SES, such as reboot the Avaya SES server, have an expired license, or attempt multiple logins to the Avaya SES Linux shell with invalid credentials. 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 > Avaya-SES** in the left pane, where “AvayaLab” is the name of the center from **Section 5.2**, and “Avaya-SES” is the name of the entity from **Section 5.3**. Verify that the new alarms are displayed in the right pane, as shown below.



The screenshot displays the ReliaTel web interface for monitoring alarms. The top navigation bar includes the TONE SOFTWARE logo, the ReliaTel logo, and links for Help and Logout. The main menu has options for Monitor Alarms, Performance Reporting, and Administration. The left sidebar shows a tree view of Centers & Entities, with 'AvayaLab' selected. The main content area is titled 'MONITOR ALARMS' and contains a table of active alarms. The table has columns for ID, Alarm Level, State, Entity, and Alarm Text. Three alarms are listed, all with a 'New' state and 'Avaya-SES' as the entity.

ID	Alarm Level	State	Entity	Alarm Text
6	Minor	New	Avaya-SES	avCCSProcessStop; (695978) 1:55:59.78; AV-CCS-MIB::avCCS.0; 192.2.2.10; n...
7	Critical	New	Avaya-SES	avCCSLicErrorMode; (1156) 0:00:11.56; AV-CCS-MIB::avCCS.0; 192.2.2.10; mp
8	Major	New	Avaya-SES	avCCSAdminFailedLogin; (69947) 0:11:39.47; AV-CCS-MIB::avCCS.0; 192.2.2.1

8. Conclusion

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

9. 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. *Installing, Administering, Maintaining, & Troubleshooting SIP Enablement Services*, Document 03-600768, Issue 5.0, January 2008, available at <http://support.avaya.com>.
3. *SIP Support in Avaya Communication Manager Running on Avaya S8xxx Servers*, Document 555-245-206, Issue 8, January 2008, available at <http://support.avaya.com>.
4. *ReliaTel Monitoring and Management Solution Installation and Configuration Guide*, Version 2 Release 5 Modification 0, contact ReliaTel support at info@tonesoft.com.
5. *ReliaTel Monitoring and Management Solution User's Guide*, Version 2 Release 5 Modification 2, contact ReliaTel support at info@tonesoft.com.

©2009 Avaya Inc. All Rights Reserved.

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

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