



Avaya Solution & Interoperability Test Lab

Application Notes for TONE Software ReliaTel with Avaya Aura® Communication Manager Using SNMP – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TONE Software ReliaTel to interoperate with Avaya Aura® Communication Manager using SNMP. 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 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 TONE Software ReliaTel to interoperate with Avaya Aura® Communication Manager using SNMP. 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 Communication Manager to provide alarm monitoring.

Upon detection of a failure, Communication Manager can raise alarms and send SNMP traps to ReliaTel. ReliaTel collects and stores the alarm information from SNMP traps, and presents the information on web-based alarm monitoring screen. The compliance testing used SNMP version 2c.

2. General Test Approach and Test Results

The feature test cases were performed manually. Different SNMP traps were generated on Avaya S8800 Server and Avaya G450 Media Gateway and verified on the ReliaTel web-based alarm monitoring screen.

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

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing.

The feature testing focused on verifying the proper reporting of SNMP traps by ReliaTel. The SNMP traps generated and verified for Avaya S8800 Server included server reboot, test SNMP command, and IPSI circuit pack disconnect/reconnect. The SNMP traps generated and verified for Avaya G450 Media Gateway included media module reset, VoIP engine reset, and VoIP engine busyout/release.

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

2.2. Test Results

All test cases were executed and passed.

2.3. Support

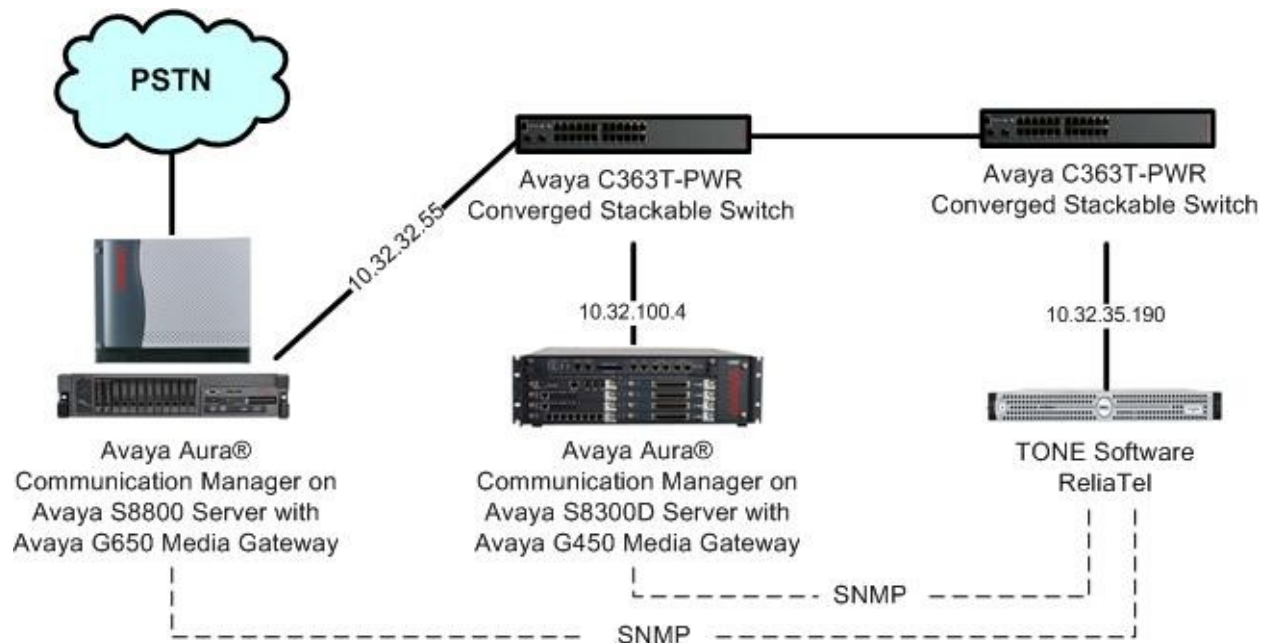
Technical support on ReliaTel can be obtained through the following:

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

3. Reference Configuration

As shown in the test configuration below, the compliance testing used two Communication Manager systems – one with Avaya S8800 Server and Avaya G650 Media Gateway, and the other with Avaya S8300D Server and Avaya G450 Media Gateway.

In the compliance testing, ReliaTel used the SNMP interface to monitor alarms on Avaya S8800 Server and Avaya G450 Media Gateway. The results in these Application Notes should be applicable to other Avaya S8xx0 Servers and to the Avaya G430 Media Gateway.



4. Equipment and Software Validated

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

| Equipment | Software |
|---|------------------------------|
| Avaya Aura® Communication Manager on Avaya S8800 Server with Avaya G650 Media Gateway | 6.0 (R016x.00.0.345.0-18246) |
| Avaya Aura® Communication Manager on S8300D Server with Avaya G450 Media Gateway | 6.0 (R016x.00.0.345.0-18246) |
| TONE Software ReliaTel | 3.1.0 |

5. Configure Avaya S8800 Server

This section provides the procedures for configuring SNMP for the Avaya S8800 Server. The procedures include the following areas:

- Launch maintenance web interface
- Administer SNMP traps

5.1. Launch Maintenance Web Interface

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

The screenshot shows the Avaya Aura™ Communication Manager (CM) System Management Interface (SMI) login page. The page has a red header bar with the Avaya logo on the left and the text "Avaya Aura™ Communication Manager (CM) System Management Interface (SMI)" on the right. Below the header bar, there is a red bar with "Help Log Off" on the left and "This Server: S8800-CM" on the right. The main content area is white and contains a gray box with the title "Logon". Inside the gray box, there are two input fields: "Logon ID:" and "Password:". Below the input fields is a "Logon" button. At the bottom of the page, there is a footer bar with the text "© 2001-2010 Avaya Inc. All Rights Reserved."

In the subsequent screen, select **Administration > Server (Maintenance)** from the top menu.

AVAYA

Avaya Aura™ Communication Manager (CM)
System Management Interface (SMI)

Help Log OffAdministrationUpgrade

This Server: S8800-CM

System Management Interface

© 2001-2010 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.

Avaya Aura is a trademark of Avaya Inc.

MultiVantage is a trademark of Avaya Inc.

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

© 2001-2010 Avaya Inc. All Rights Reserved.

The **Server Administration** screen is displayed.

AVAYA

Avaya Aura™ Communication Manager (CM)
System Management Interface (SMI)

Help Log OffAdministrationUpgrade

Administration / Server (Maintenance)This Server: S8800-CM

Alarms

Current Alarms

Agent Status

SNMP Agents

SNMP Traps

Filters

SNMP Test

Diagnostics

Restarts

System Logs

Ping

Server Administration

Welcome to the "Server Administration Interface". This interface allows you to maintain, troubleshoot, and configure the server.

Please use the menu to the left for navigation.

5.2. Administer SNMP Traps

Select **Alarms > SNMP Traps** from the left pane, to display the **SNMP Traps** screen. Click **Add/Change** to add a new trap destination.

AVAYA Avaya Aura™ Communication Manager (CM)
System Management Interface (SMI)

Help Log Off Administration Upgrade

Administration / Server (Maintenance) This Server: **S8800-CM**

Alarms

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

Diagnostics

- Restarts
- System Logs
- Ping
- Traceroute
- Netstat

Server

- Status Summary
- Process Status
- Shutdown Server
- Server Date/Time
- Software Version
- Server Configuration
- Server Role
- Network Configuration

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.
- 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 use the SNMP Test page found in the left hand side menu.

Master Agent status: **UP**

Current Settings

No trap destinations have been configured.

Add/Change **Delete** **Help**

The **SNMP Traps** screen is updated as shown below. In the **SNMP Version 2c** sub-section, configure the fields as shown, where “10.32.35.190” is the IP address of the ReliaTel server, and **Community Name** can be any desired string.

Note that **Community Name** is required to be configured on Communication Manager, and not used by ReliaTel.

AVAYA Avaya Aura™ Communication Manager (CM)
System Management Interface (SMI)

Help Log Off Administration Upgrade

Administration / Server (Maintenance) This Server: **S8800-CM**

Alarms

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

Diagnostics

- Restarts
- System Logs
- Ping
- Traceroute
- Netstat

Server

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

SNMP Traps

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

Add Trap Destination

SNMP Version 1

Status
IP address
Notification
Community Name

SNMP Version 2c

Status
IP address
Notification
Community Name

6. Configure Avaya G450 Media Gateway

This section provides the procedures for configuring SNMP on the Avaya G450 Media Gateway. The procedures include the following areas:

- Administer community string
- Administer SNMP traps
- Show SNMP

6.1. Administer Community String

Use the “snmp-server community” command shown below to set the desired community strings for read-only and read-write access, where “public” and “private” can be any desired community string. Note that the community strings are required to be set on the G450 Media Gateway, and not used by ReliaTel.

```
G450-001 (super) # snmp-server community read-only public read-write private
Done!
```

6.2. Administer SNMP Traps

Use the “snmp-server host” command shown below to enable SNMP traps and notifications to ReliaTel, where “10.32.35.190” is the IP address of the ReliaTel server, and “public” is the read-only community string from **Section 6.1**.

```
G450-001 (super) # snmp-server host 10.32.35.190 traps v2c public udp-port 162 all
Done!
```

6.3. Show SNMP

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

```
G450-001 (super) # show snmp

Authentication trap disabled

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

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

SNMP-Rec-Address Model  Level  Notification  Trap/Inform  User name
-----
10.32.100.1          v1    noauth  all           trap         ReadCommN    UDP
port: 162 DM

10.32.35.190        v2c noauth all         trap        ReadCommN   UDP
port: 162

G450-001 (super) #
```

7. Configure TONE Software ReliaTel

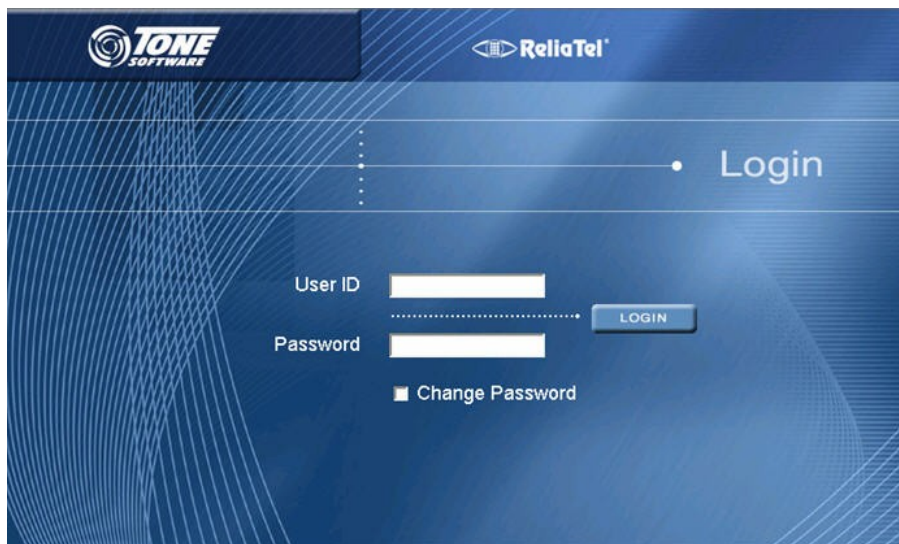
This section provides the procedures for configuring TONE Software ReliaTel. The procedures include the following areas:

- Launch web interface
- Administer centers
- Administer DAPs
- Administer entities

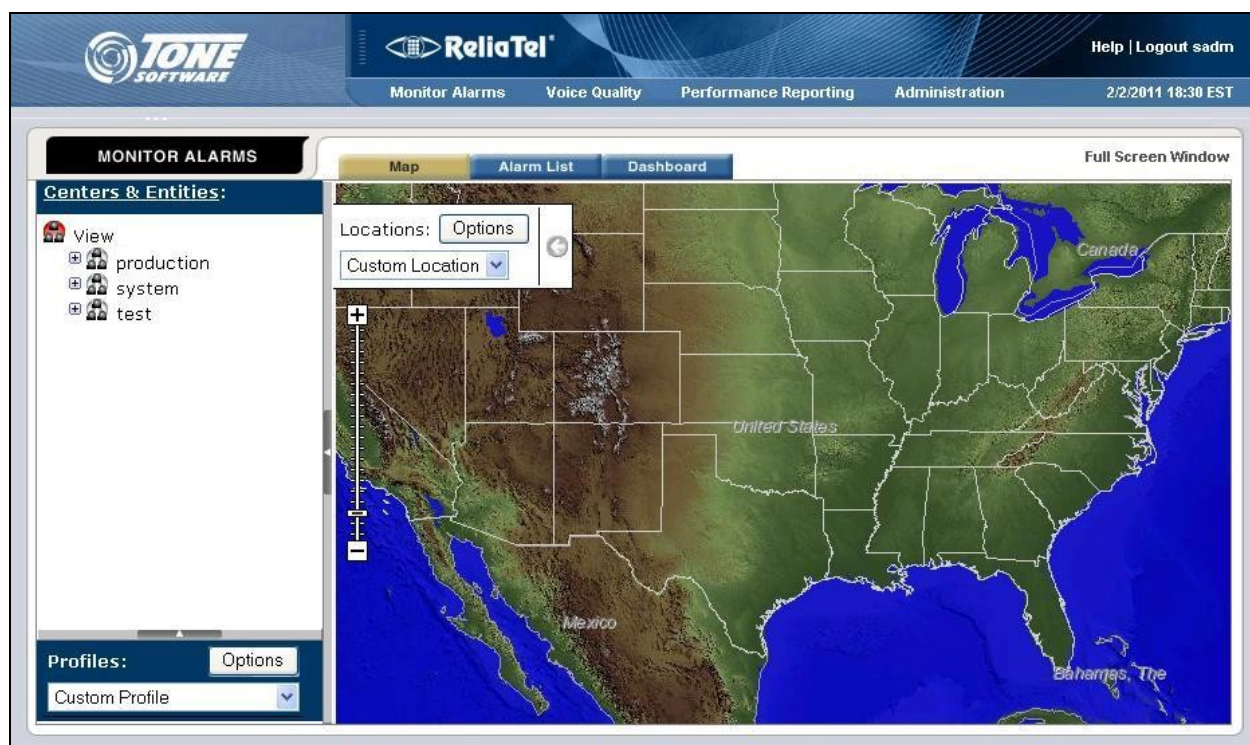
The configuration of ReliaTel is typically performed by TONE Software technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. 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 using the appropriate credentials.



The **ReliaTel** screen is displayed. Select **Administration > General Administration** from the top menu.

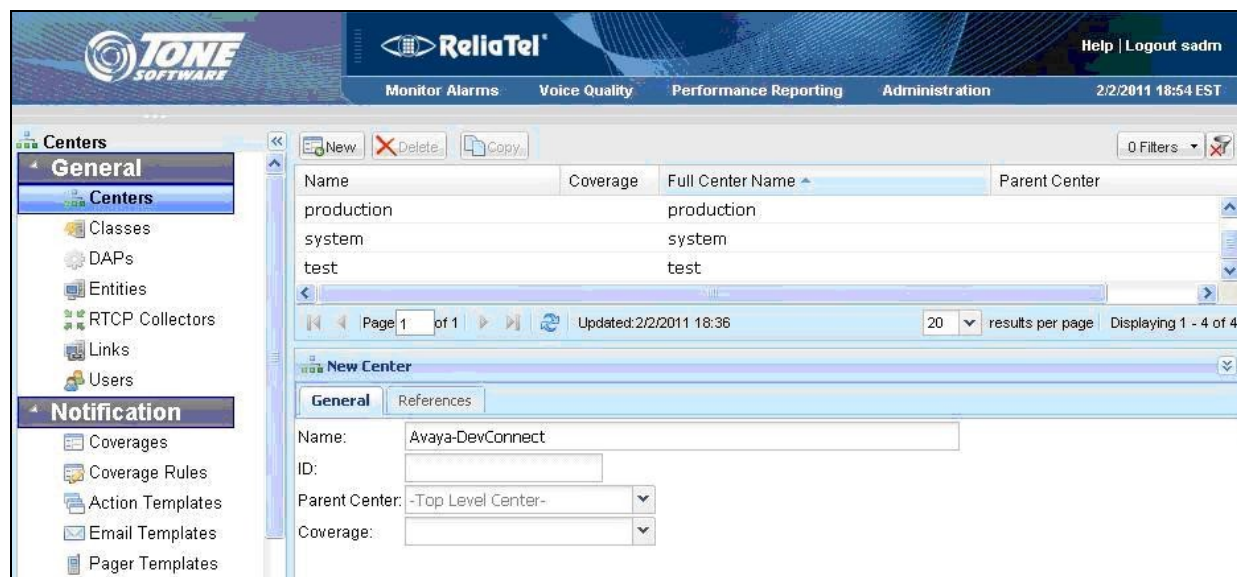


7.2. Administer Centers

The **ReliaTel** screen is updated as shown below. Select **General > Centers** in the left pane to display a list of centers in the right pane. Click **New** to add a new center.

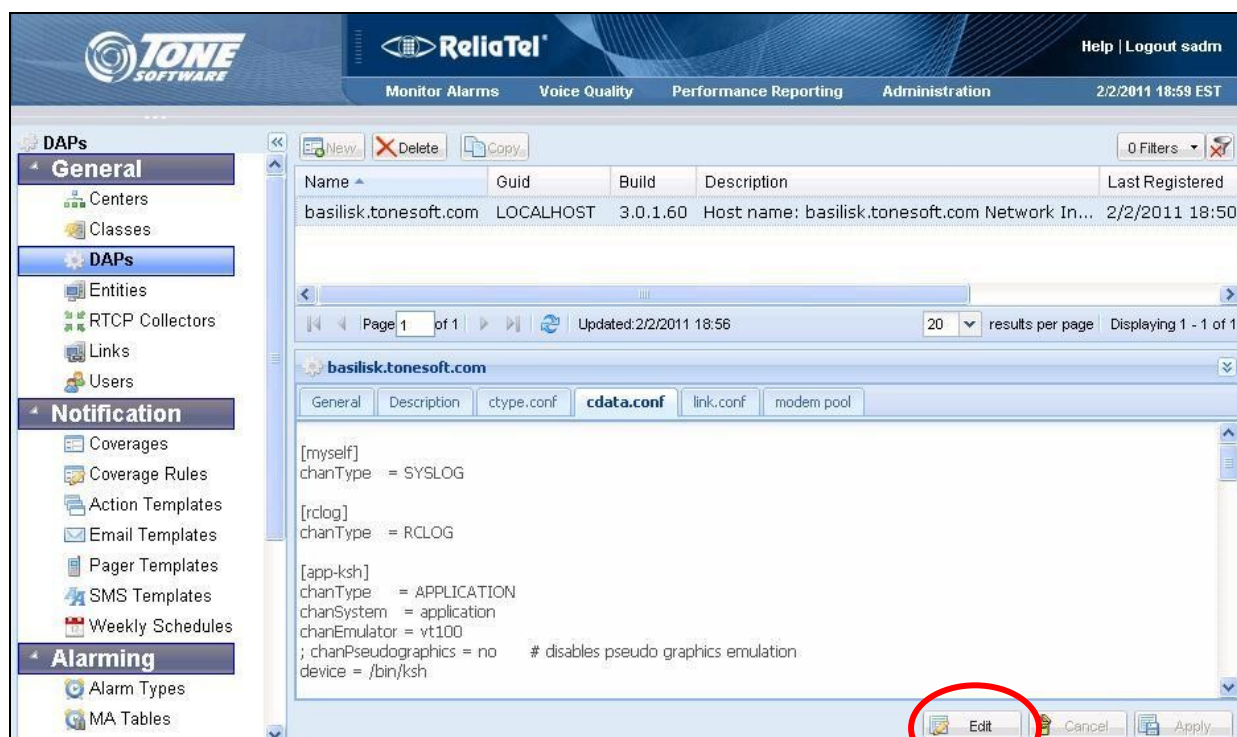


In the lower portion of the screen, select the **General** tab. Enter a descriptive **Name**, and retain the default values in the remaining fields.



7.3. Administer DAPs

Select **General > DAPs** in the left pane to display the pre-configured DAPs. Select the applicable DAP in the upper pane, followed by the **cdata.conf** tab in the lower pane. Click **Edit**.



Scroll the lower pane to the bottom, and add the entries shown below for connectivity to Avaya S8800 Server and Avaya G450 Media Gateway.

In the examples shown below, “devconnect-s8800” and “Avaya S8800” can be any desired string to denote the Avaya S8800 Server, and “devconnect-g450” and “Avaya G450” can be any desired strings to denote the Avaya G450 Media Gateway.

Use the values shown below for **chanType**, **chanEmulator**, and **chanSilent**. For **account**, use the IP address of the Avaya S8800 Server and Avaya G450 Media Gateway respectively.

The screenshot displays the ReliaTel administration web interface. The left sidebar contains a navigation menu with categories: DAPs (General, Centers, Classes, DAPs, Entities, RTP Collectors, Links, Users), Notification (Coverages, Coverage Rules, Action Templates, Email Templates, Pager Templates, SMS Templates, Weekly Schedules), and Alarming (Alarm Types, MA Tables). The main content area shows a table of DAPs with columns: Name, Guid, Build, Description, and Last Registered. A single entry is visible: 'basilisk.tonesoft.com' with Guid 'LOCALHOST' and Build '3.0.1.60'. Below the table, there is a configuration section for 'basilisk.tonesoft.com' with tabs for General, Description, ctype.conf, cdata.conf, link.conf, and modem pool. The 'cdata.conf' tab is active, showing configuration for two DAPs: [devconnect-s8800] and [devconnect-g450].

| Name | Guid | Build | Description | Last Registered |
|-----------------------|-----------|----------|--|-----------------|
| basilisk.tonesoft.com | LOCALHOST | 3.0.1.60 | Host name: basilisk.tonesoft.com Network In... | 2/2/2011 18:50 |

Page 1 of 1 | Updated: 2/2/2011 18:56 | 20 results per page | Displaying 1 - 1 of 1

basilisk.tonesoft.com

General | Description | ctype.conf | **cdata.conf** | link.conf | modem pool

[devconnect-s8800]
chanType = SNMPMGR
chanSystem = Avaya S8800
chanEmulator = 4410
account = 10.32.32.55
chanSilent = 259200

[devconnect-g450]
chanType = SNMPMGR
chanSystem = Avaya G450
chanEmulator = 4410
account = 10.32.100.4
chanSilent = 259200

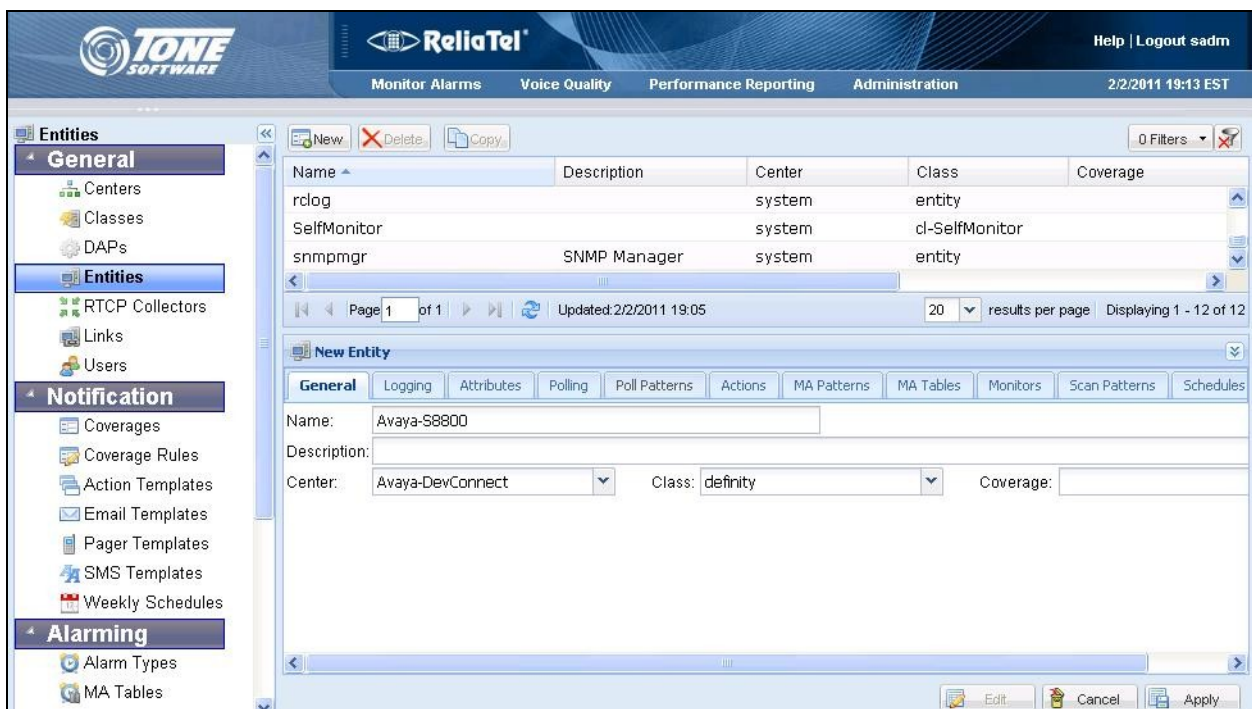
Edit | Cancel | Apply

7.4. 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 add a new entity.



In the lower portion of the screen, select the **General** tab. Enter a descriptive **Name** for the Avaya S8800 Server. For **Center**, select the center name from **Section 7.2**, in this case “Avaya-DevConnect”. For **Class**, select “definity” from the drop-down list, as shown below.



In the lower portion of the screen, select the **Logging** tab. Check **Log State**, enter a descriptive **Channel**, and select “l-avayamdsrv” for **Log Pattern**, as shown below. Retain the default values in the remaining fields.

The screenshot shows the ReliaTel administration interface. On the left, the 'Entities' menu is expanded, and the 'Logging' tab is selected for the 'Avaya-S8800' entity. The configuration fields are as follows:

| Name | Description | Center | Class | Coverage |
|-------------|--------------|--------|----------------|----------|
| rlog | | system | entity | |
| SelfMonitor | | system | cl-SelfMonitor | |
| snmpmgr | SNMP Manager | system | entity | |

Below the table, the 'Logging' configuration for 'Avaya-S8800' is shown:

- Log State: ☒
- Channel: devconnect-s8800
- Log Pattern: l-avayamdsrv
- Log Age (Days): 30
- Message Timeout (Seconds): 10

Repeat the procedures in this section to create another entity for the Avaya G450 Media Gateway. In the compliance testing, the “Avaya-S8800” entity shown below was created for the Avaya S8800 Media Server, and the “Avaya-G450” entity was created for the Avaya G450 Media Gateway.

The screenshot shows the ReliaTel administration interface with the 'Entities' menu expanded. The table below lists the entities created:

| Name | Description | Center | Class | Coverage |
|------------------|--------------|------------------|----------------|----------|
| Avaya-G450 | | Avaya-DevConnect | definity | |
| Avaya-S8800 | | Avaya-DevConnect | definity | |
| def_password_mgr | | system | password_mgr | |
| myself | | system | entity | |
| password_mgr | | system | password_mgr | |
| rlog | | system | entity | |
| SelfMonitor | | system | cl-SelfMonitor | |
| snmpmgr | SNMP Manager | system | entity | |

8. Verification Steps

This section provides the tests that can be performed to verify proper configuration of Avaya S8800 Server, Avaya G450 Media Gateway, and TONE Software ReliaTel.

Prior to verification, generate alarms on Avaya S8800 Server and Avaya G450 Media Gateway.

From the **ReliaTel** screen, select **Monitor Alarms** from the top menu. Select **View > Avaya-DevConnect > Avaya-S8800** in the left pane, and verify that the new alarms from Avaya S8800 Server are displayed in the right pane, as shown below.

The screenshot shows the ReliaTel web interface with the 'Monitor Alarms' section active. The left pane shows the 'Centers & Entities' tree with 'Avaya-S8800' selected. The main pane displays a table of 8 alarms.

| ID | Alarm Level | State | Entity | Alarm Text | Count |
|------|-------------|-------|-------------|---|-------|
| 1001 | FYI | New | Avaya-S8800 | Enterprise Specific 6 RFC1155-SMI::enterprise | 1 |
| 1002 | FYI | New | Avaya-S8800 | Cold Start | 2 |
| 1003 | FYI | New | Avaya-S8800 | WRN "CUSTOMER ALARM TEST" | 1 |
| 1004 | Major | New | Avaya-S8800 | MAJ "PN 01" EXP-PN Problem is Off Board | 2 |
| 1005 | Major | New | Avaya-S8800 | MAJ "" TTR-LEV Problem is Off Board | 2 |
| 1006 | Major | New | Avaya-S8800 | MAJ "1" ADJ-IP Problem is Off Board | 1 |
| 1009 | Minor | New | Avaya-S8800 | MIN "01A04" IPMEDPRO Problem is On Board | 1 |
| 1010 | Minor | New | Avaya-S8800 | MIN "01A1333" ETH-PT Problem is Off Board | 1 |

Select **View > Avaya-DevConnect > Avaya-G450** in the left pane, and verify that the new alarms from Avaya G450 Media Gateway are displayed in the right pane, as shown below.

The screenshot shows the ReliaTel web interface with the 'Monitor Alarms' section active. The left pane shows the 'Centers & Entities' tree with 'Avaya-G450' selected. The main pane displays a table of 2 alarms.

| ID | Alarm Level | State | Entity | Alarm Text | Count |
|------|-------------|-------|------------|-------------------------------|-------|
| 1007 | FYI | New | Avaya-G450 | cmgMgBusyout; HW; no; ; ; ; ; | 1 |
| 1008 | FYI | New | Avaya-G450 | cmgMgRelease; HW; no; ; ; ; ; | 1 |

9. Conclusion

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

10. Additional References

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

1. *Administering Avaya Aura™ Communication Manager*, Document 03-300509, Issue 6.0, Release 6.0, June 2010, available at <http://support.avaya.com>.
2. *Avaya G450 CLI Reference*, Document 03-602056, Issue 3, May 2009, available at <http://support.avaya.com>.
3. *ReliaTel Monitoring and Management Solution Installation and Configuration Guide*, Version 3 Release 1 Modification 0, contact ReliaTel support at info@tonesoft.com.
4. *ReliaTel Monitoring and Management Solution User's Guide*, Version 3 Release 1 Modification 0, contact ReliaTel support at info@tonesoft.com.

©2011 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.