



Application Notes for TONE Software ReliaTel Fault and Performance Management 4.6 with Avaya Aura® Communication Manager 7.0 using SNMP – Issue 1.0

Abstract

These Application Notes describe the configuration steps required for TONE Software ReliaTel Fault and Performance Management 4.6 to interoperate with Avaya Aura® Communication Manager 7.0 using SNMP. TONE Software ReliaTel Fault and Performance Management 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, TONE Software ReliaTel Fault and Performance Management used the SNMP interface from Avaya Aura® Communication Manager to provide alarm monitoring.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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 Fault and Performance Management 4.6 to interoperate with Avaya Aura® Communication Manager 7.0 using SNMP. TONE Software ReliaTel Fault and Performance Management 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.

Upon detection of failures, Avaya Aura® Communication Manager raised alarms and sent SNMP traps to TONE Software ReliaTel Fault and Performance Management. The application collected and stored information from the SNMP traps, and presented the information on web-based alarm monitoring screen. The compliance testing used SNMP version 2c.

In the compliance testing, TONE Software ReliaTel Fault and Performance Management used the SNMP interface to monitor alarms on an Avaya Server in a virtual environment and an Avaya G430 Media Gateway. The results in these Application Notes should be applicable to other Avaya Servers and to the Avaya G450 Media Gateway.

2. General Test Approach and Test Results

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

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

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

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 Server included server reboot, test SNMP, SNMP agent restart, and login failure. The SNMP traps generated and verified for Avaya Media Gateway included media module reset, VoIP engine reset, VoIP engine busyout/release, and login failure.

The serviceability testing focused on verifying the ability of ReliaTel to recover from adverse conditions, such as disconnecting/reconnecting the Ethernet connection 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:** support@tonesoft.com
- **Web:** <http://www.tonesoft.com/tone-secure/support-home/login-reliatel/>

3. Reference Configuration

As shown in **Figure 1**, ReliaTel has SNMP connections to the Avaya Server and to the Avaya Media Gateway.

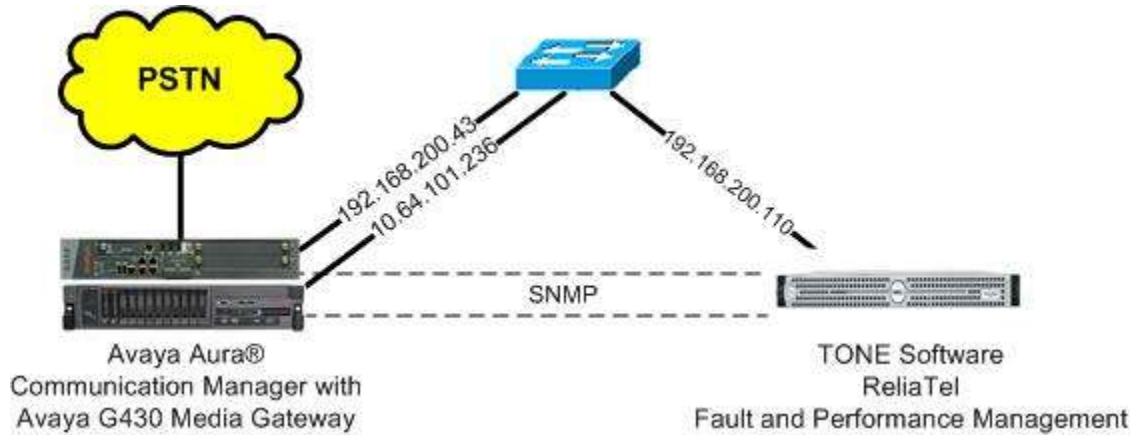


Figure 1: Compliance Testing Configuration

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Aura® Communication Manager in Virtual Environment	7.0 SP 3.1 (7.0.0.3.1.441.22903)
Avaya G430 Media Gateway	37.20.0
TONE Software ReliaTel Fault and Performance Management	4.6.1.164

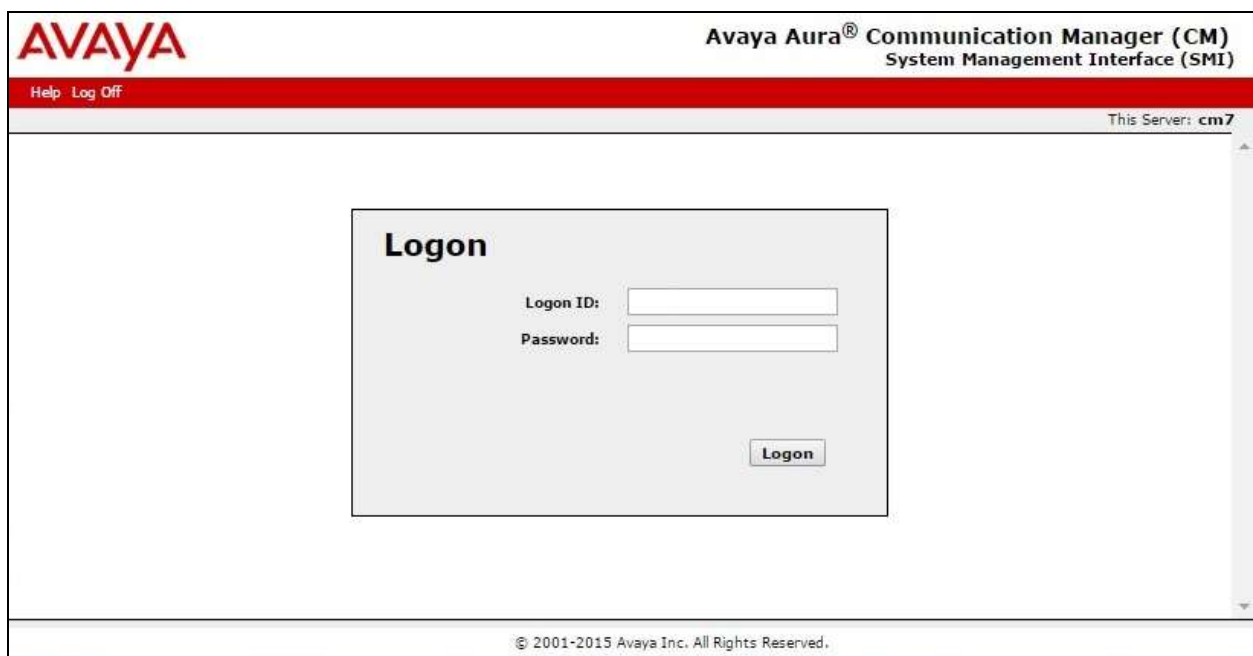
5. Configure Avaya Server

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

- Launch maintenance web interface
- Administer SNMP traps

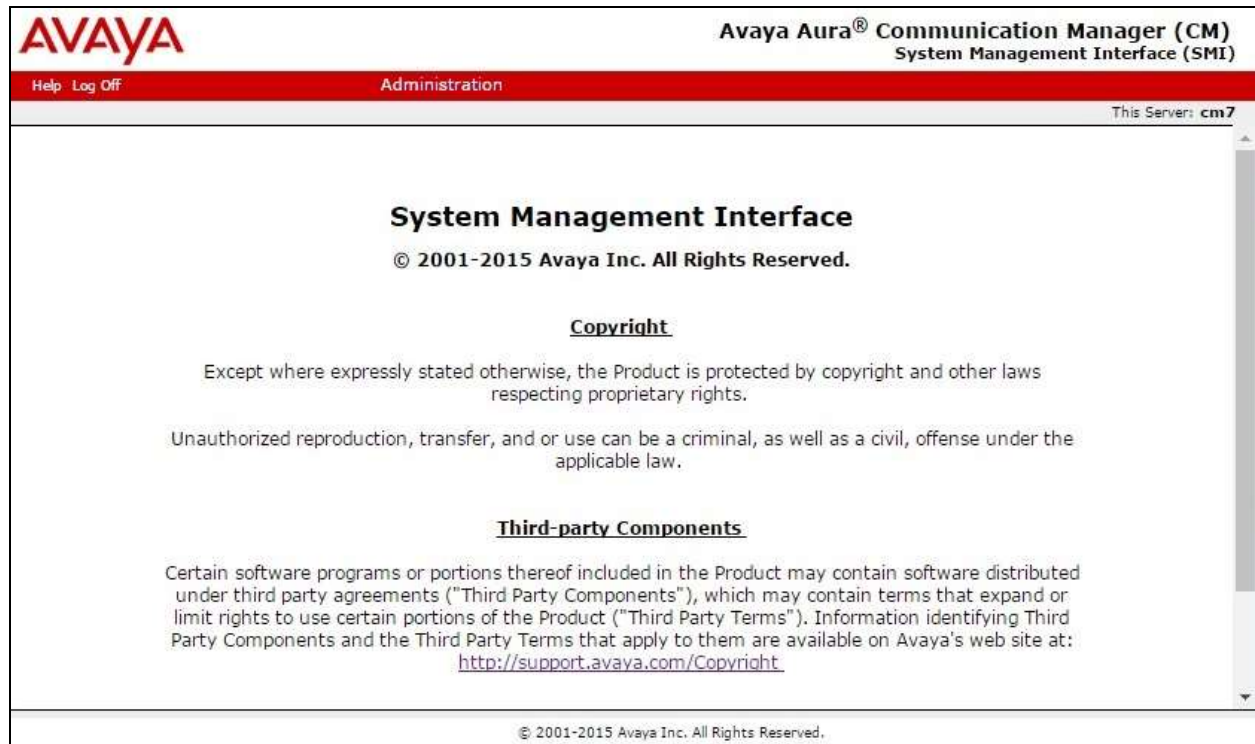
5.1. Launch Maintenance Web Interface

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 displays the Avaya Aura® Communication Manager (CM) System Management Interface (SMI) login page. The page features 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, a red bar contains the links "Help" and "Log Off". The main content area is white and contains a central gray box titled "Logon". Inside this box, there are two input fields: "Logon ID:" and "Password:". Below these fields is a "Logon" button. The text "This Server: cm7" is visible in the top right corner of the main content area. At the bottom of the page, a footer bar contains the copyright notice "© 2001-2015 Avaya Inc. All Rights Reserved."

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



The **Server Administration** screen is displayed.




5.2. Administer SNMP Traps

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



The **FP Traps** screen is updated as shown below. In the **SNMP Version 2c** sub-section, configure the fields as shown, where “192.168.200.110” is the IP address of the ReliaTel server, and **Community Name** can be any desired string. Retain the default value in the remaining fields.

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



6. Configure Avaya Media Gateway

This section provides the procedures for configuring SNMP on the Avaya G430 Media Gateway. The procedures include the following areas:

- Administer community string
- Administer SNMP traps
- Commit configuration

6.1. Administer Community String

Use the “snmp-server community” command 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 Media Gateway, although not used by ReliaTel.

```
G430-001 (super) # snmp-server community read-only public read-write private
```

6.2. Administer SNMP Traps

Use the “snmp-server host” command shown below to enable SNMP traps and notifications to ReliaTel, where “192.168.200.110” is the IP address of the ReliaTel server, and “public” is the read-only community string from **Section 6.1**.

```
G430-001 (super) # snmp-server host 192.168.200.110 traps v2c public udp-port 162 all
```

6.3. Commit Configuration

Use the “copy” command below to commit the current configuration.

```
G430-001 (super) # copy running startup-config
```


7. Configure TONE Software ReliaTel Fault and Performance Management

This section provides the procedures for configuring 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” in an Internet browser window, where “ip-address” is the IP address of the ReliaTel server. Log in using the appropriate credentials.

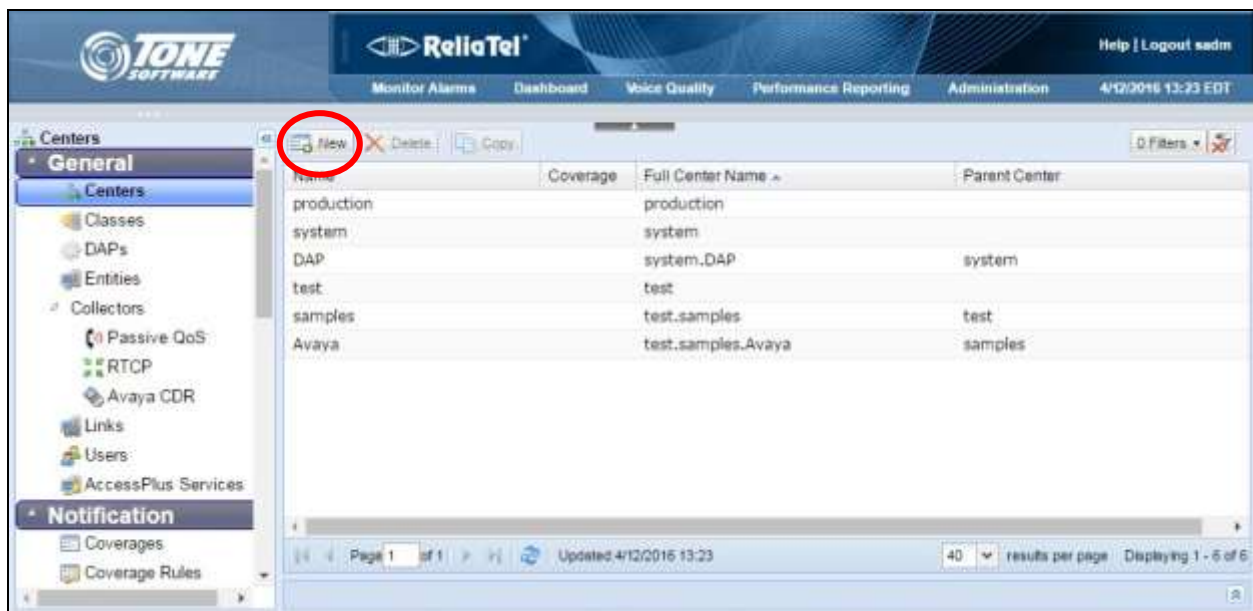


7.2. Administer Centers

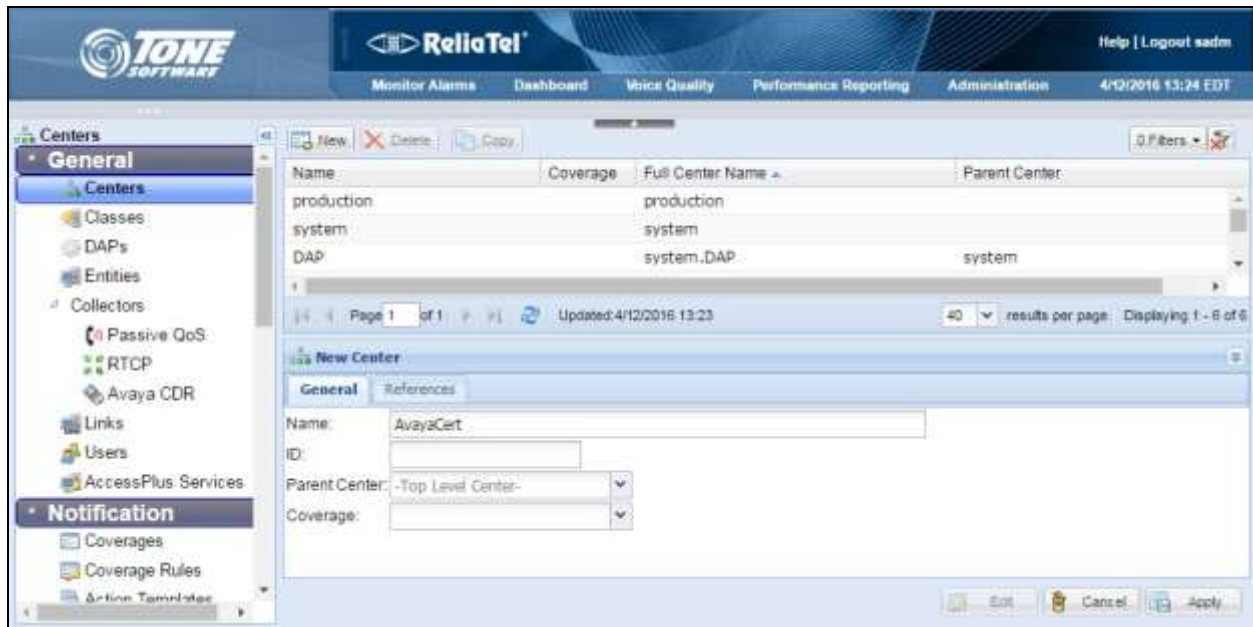
The **ReliaTel** screen is displayed. Select **Administration** → **General Administration** from the top menu.



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



The screen is updated with a bottom pane, as shown below. In the bottom pane, select the **General** tab. Enter a descriptive **Name**, and retain the default values in the remaining fields.



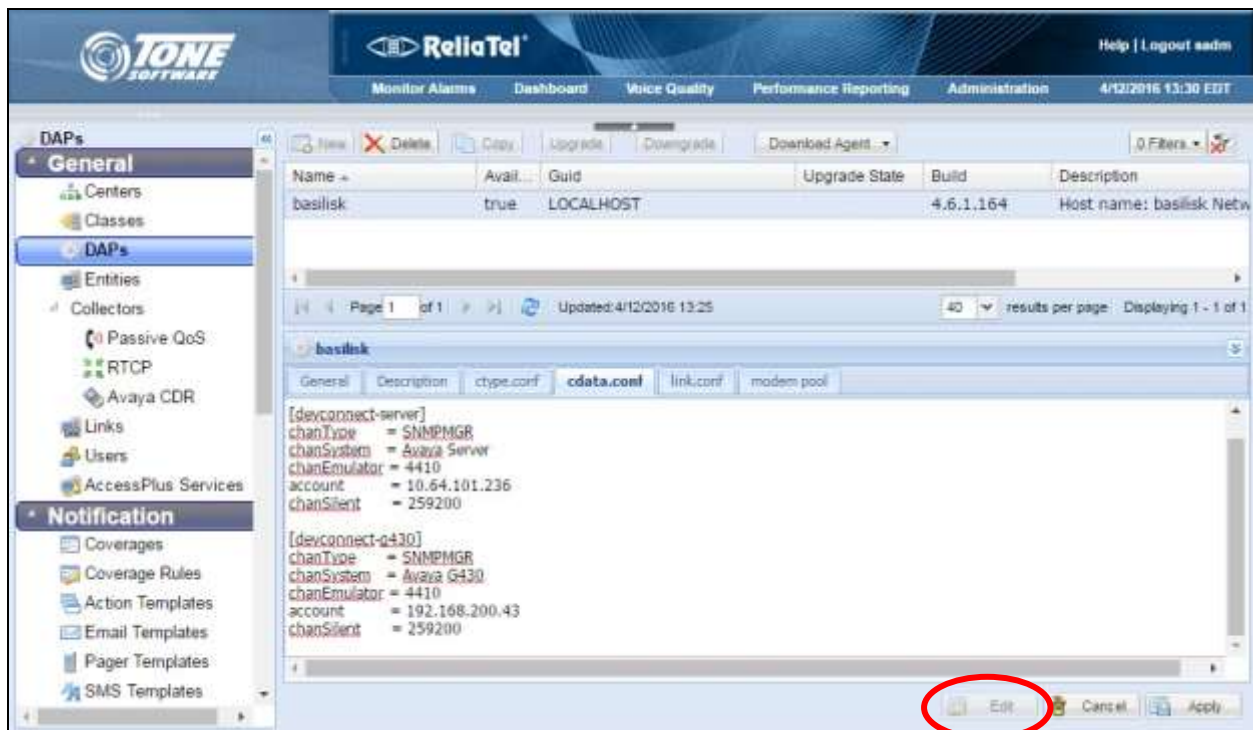
7.3. Administer DAPs

Select **General** → **DAPs** from the left pane to display the screen below. Select the displayed entry in the right pane.



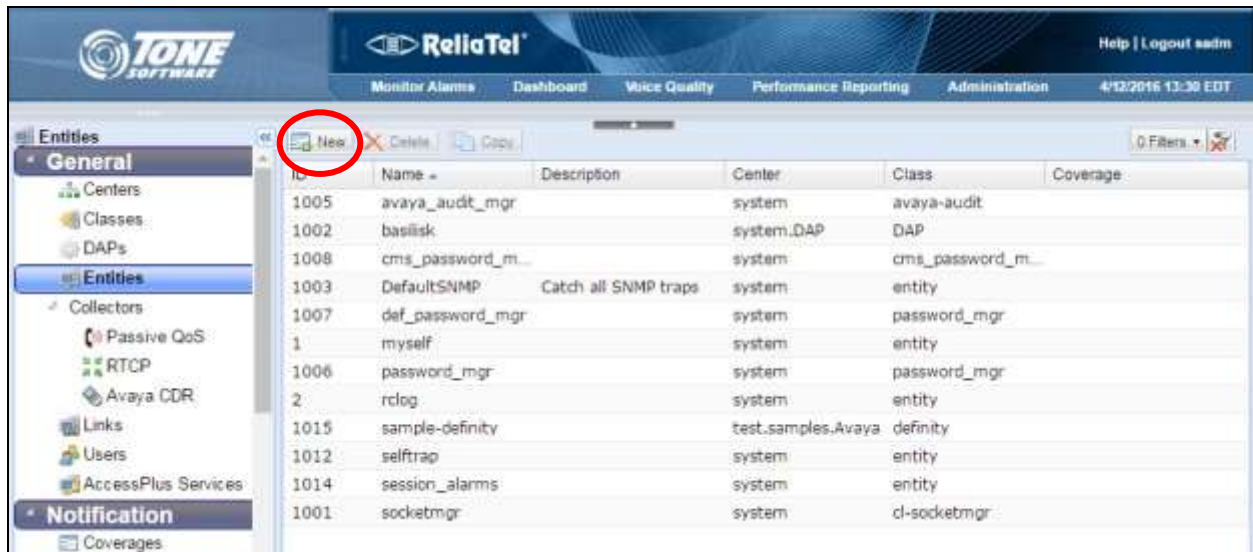
The screen is updated with details in the bottom pane. Select the **cdata.conf** tab and click **Edit**. Scroll down the bottom pane, and add entries at the end for Avaya Server and Avaya Media Gateway, as shown below.

Use descriptive channel names within the brackets, descriptive **chanSystem**, and the IP address of Avaya Server and Avaya Media Gateway for **account**. Enter all other entry lines exactly as shown.



7.4. Administer Entities

Select **General** → **Entities** from the left pane to display a list of entities in the right pane. Click **New** to add a new entity.



The screen is updated with a bottom pane, as shown below. In the bottom pane, select the **General** tab. Enter a descriptive **Name** for the Avaya Server. For **Center**, select the center name from **Section 7.2**. For **Class**, select “definity”.



Select the **Logging** tab. Check the **Log State** field. For **Channel**, enter the corresponding channel name from **Section 7.3**. For **Log Pattern**, select “l-avayamdsrv” from the drop-down list. Retain the default values in the remaining fields.

The screenshot shows the 'New Entity' form in the ReliaTel TONE Software. The 'Logging' tab is selected. The form contains the following fields:

- Log State:** ☒
- Channel:** devconnect-server
- Log Pattern:** l-avayamdsrv
- Log Age (days):** 30
- Message Timeout (seconds):** 10

Repeat this section to create another entity for the Avaya Media Gateway. In the compliance testing, the “Avaya-Server” entity shown below was created for the Avaya Server, and the “Avaya-G430” entity was created for the Avaya Media Gateway.

The screenshot shows the 'Entities' list in the ReliaTel TONE Software. The list contains the following entities:

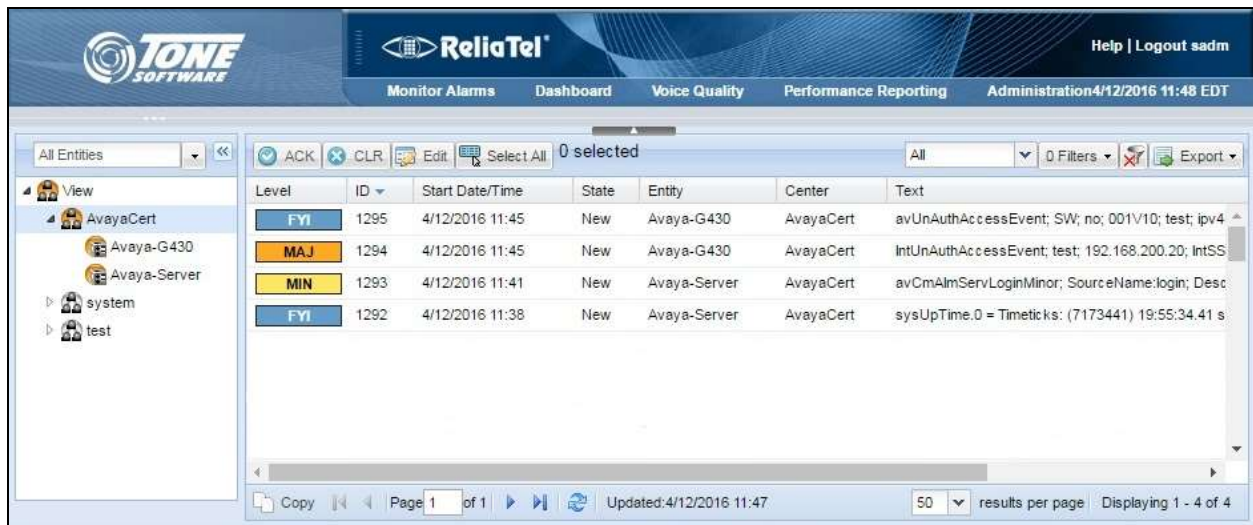
ID	Name	Description	Center	Class	Coverage
1005	avaya_audit_mgr		system	avaya-audit	
1020	Avaya-G430		AvayaCert	definity	
1019	Avaya-Server		AvayaCert	definity	
1002	basilisk		system.DAP	DAP	
1008	cms_password_mgr		system	cms_password_mgr	
1003	DefaultSNMP	Catch all SNMP traps	system	entity	
1007	def_password_mgr		system	password_mgr	
1	myself		system	entity	
1006	password_mgr		system	password_mgr	
2	rclog		system	entity	
1015	sample-definity		test.samples.Avaya	definity	

8. Verification Steps

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

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

On the **ReliaTel** screen, select **Monitor Alarms** → **Alarm List** from the top menu. Select **View** → **AvayaCert** in the left pane, where **AvayaCert** is the center name from **Section 7.2**. Verify that the new traps are displayed in the right pane, as shown below.



The screenshot displays the ReliaTel web interface for monitoring alarms. The top navigation bar includes 'Monitor Alarms', 'Dashboard', 'Voice Quality', 'Performance Reporting', and 'Administration'. The left sidebar shows a tree view with 'AvayaCert' selected. The main area displays a table of alarms with columns: Level, ID, Start Date/Time, State, Entity, Center, and Text. The table contains four rows of alarm data.

Level	ID	Start Date/Time	State	Entity	Center	Text
FYI	1295	4/12/2016 11:45	New	Avaya-G430	AvayaCert	avUnAuthAccessEvent; SW: no; 001V10; test; ipv4
MAJ	1294	4/12/2016 11:45	New	Avaya-G430	AvayaCert	IntUnAuthAccessEvent; test; 192.168.200.20; IntSS
MIN	1293	4/12/2016 11:41	New	Avaya-Server	AvayaCert	avCmAlmServLoginMinor; SourceName:login; Desc:
FYI	1292	4/12/2016 11:38	New	Avaya-Server	AvayaCert	sysUpTime.0 = Timeticks: (7173441) 19:55:34.41 s

The interface also includes a search bar, a '0 selected' status, and a footer with 'Page 1 of 1', 'Updated: 4/12/2016 11:47', and 'Displaying 1 - 4 of 4'.

9. Conclusion

These Application Notes describe the configuration steps required TONE Software ReliaTel Fault and Performance Management 4.6 to successfully interoperate with Avaya Aura® Communication Manager 7.0 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*, Release 7.0, Issue 1, August 2015, available at <http://support.avaya.com>.
2. *ReliaTel Release 4.6.0 Administrator Guide*, Guide Version 1.0, available via the ReliaTel web interface.
3. *ReliaTel Operator Guide Release 4.6.0*, Guide Version 1.0, available via the ReliaTel web interface.

©2016 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.