Avaya Solution & Interoperability Test Lab

Application Notes for TONE Software ReliaTel with Avaya Aura® Communication Manager 6.2 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 6.2 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 Avaya Aura® 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 6.2 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 Avaya Aura® Communication Manager to provide alarm monitoring.

Upon detection of a failure, Avaya Aura® Communication Manager can raise alarms and send SNMP traps to ReliaTel. ReliaTel collects and stores 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 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 cable to the ReliaTel server.

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 command, 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:** info@tonesoft.com
- **Web:** http://www.tonesoft.com/support/portal2.html

3. Reference Configuration

In the compliance testing, ReliaTel used the SNMP interface to monitor alarms on Avaya S8300D Server and Avaya G430 Media Gateway. The results in these Application Notes should be applicable to other Avaya S8xx0 Servers and to the Avaya G450 Media Gateway.

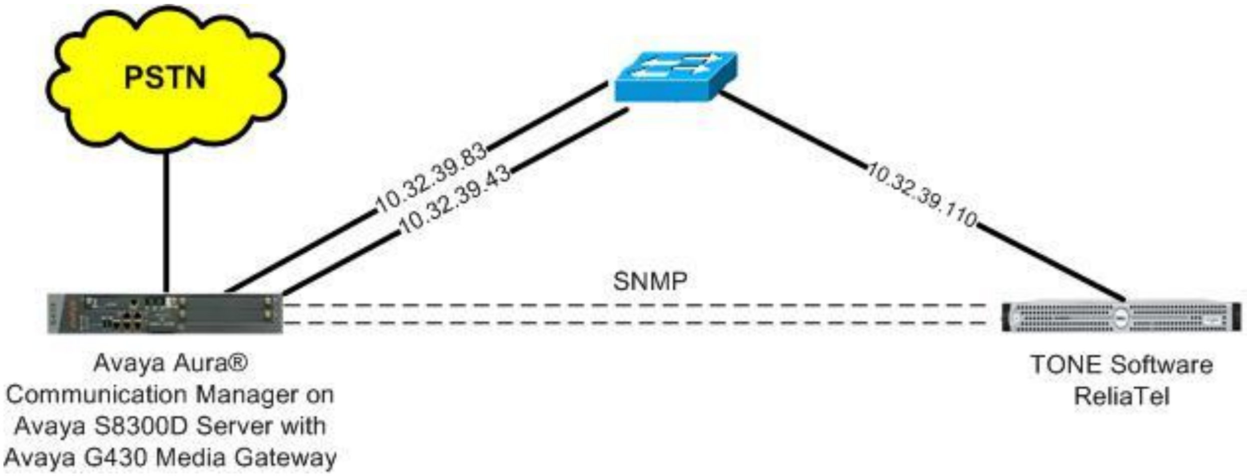

PSTN
10.32.39.83
10.32.39.43
10.32.39.110
SNMP
Avaya Aura® Communication Manager on Avaya S8300D Server with Avaya G430 Media Gateway
TONE Software ReliaTel

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 on Avaya S8300D Server with Avaya G430 Media Gateway	6.2 SP3 (R016x.02.0.823.0-20001)
TONE Software ReliaTel	4.1.0

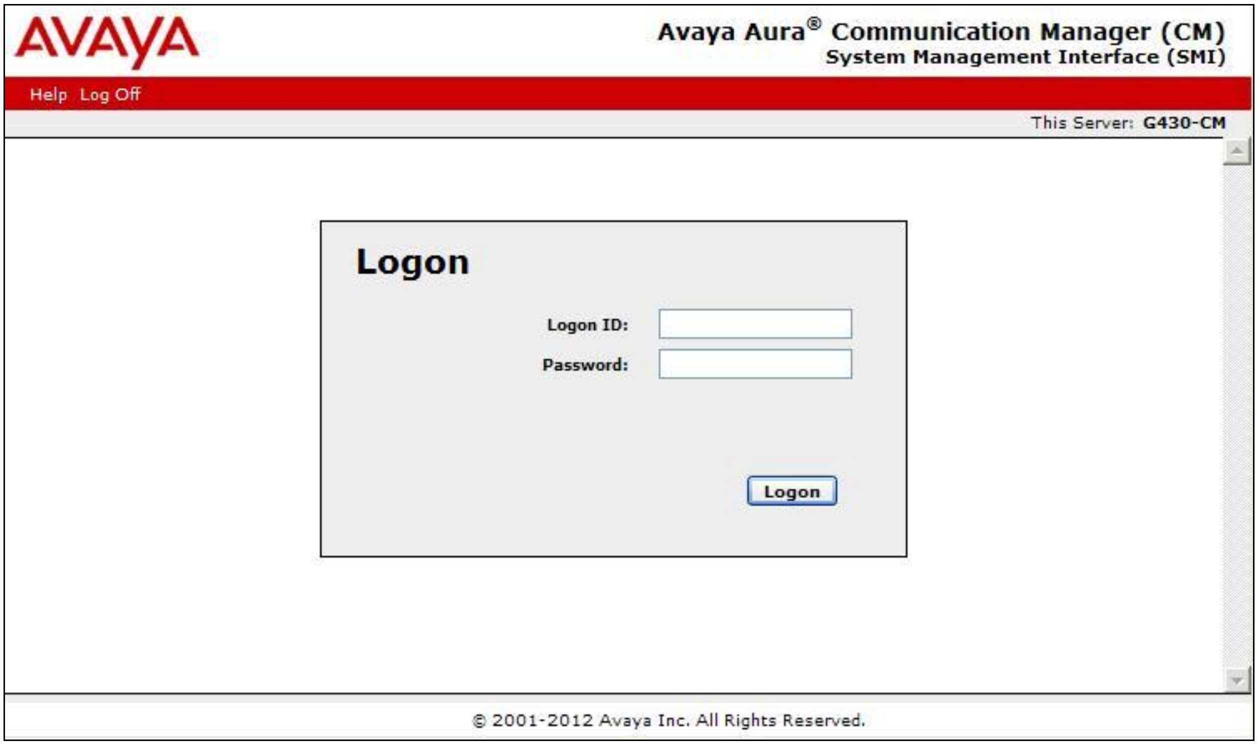
5. Configure Avaya Server

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

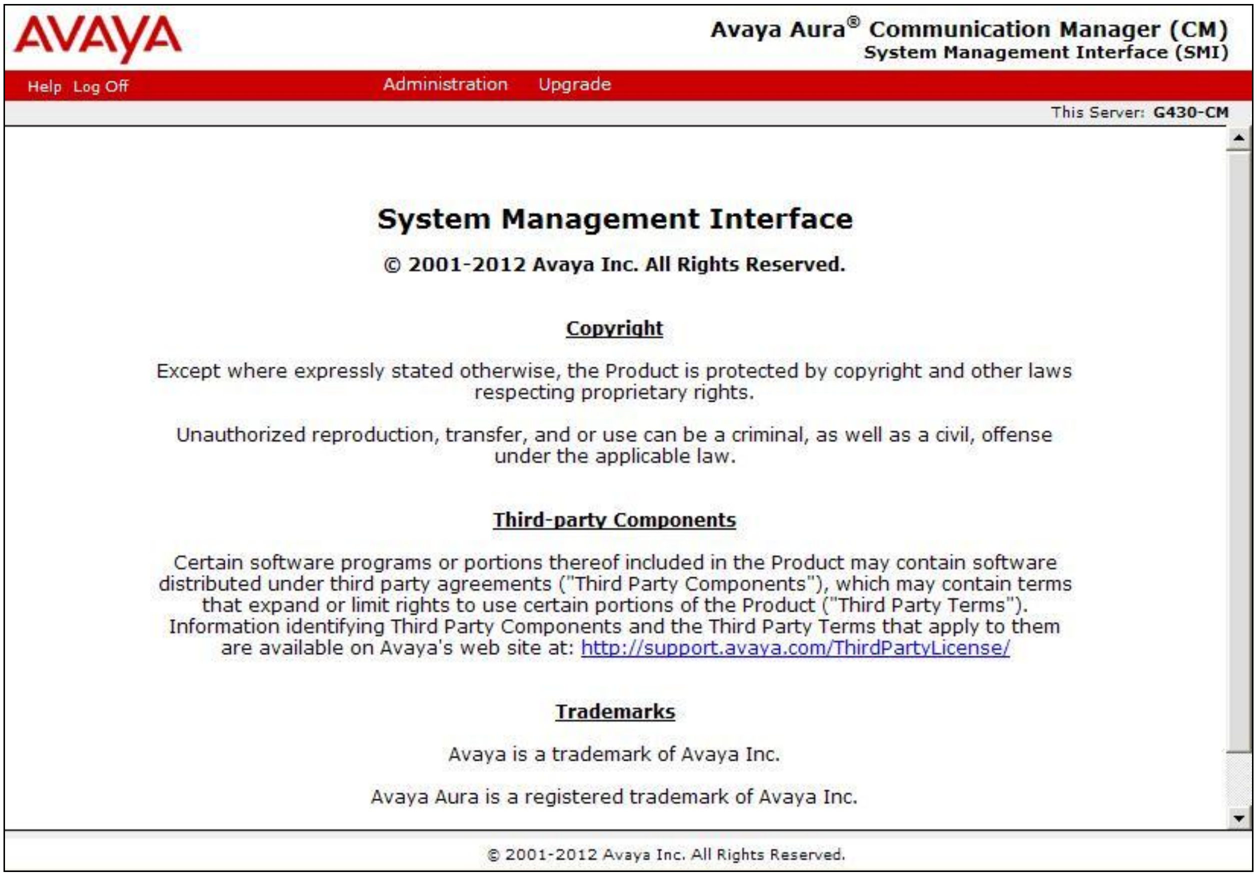
5.1. Launch Maintenance Web Interface

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.



AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help
Log Off
This Server: G430-CM
Logon
Logon ID:
Password:
Logon
© 2001-2012 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 Off
Administration Upgrade
This Server: G430-CM

System Management Interface

© 2001-2012 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/

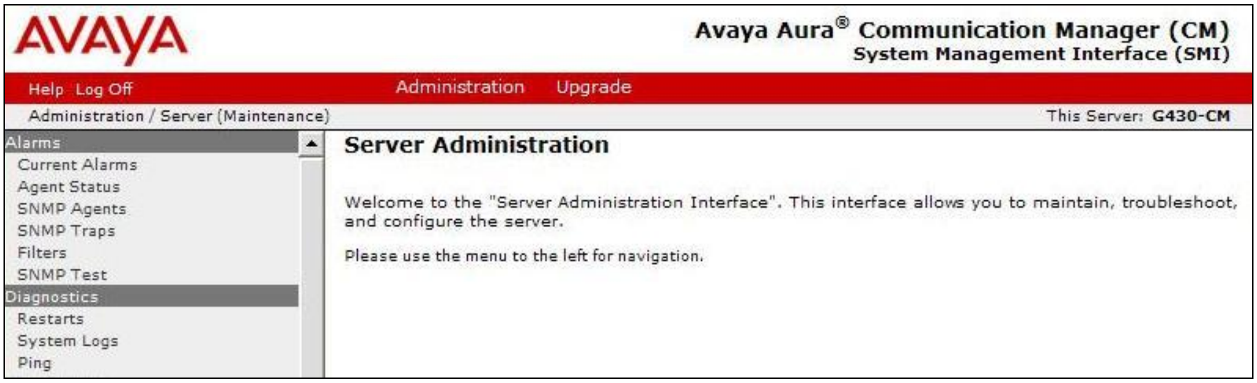
Trademarks

Avaya is a trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

© 2001-2012 Avaya Inc. All Rights Reserved.

The **Server Administration** screen is displayed.



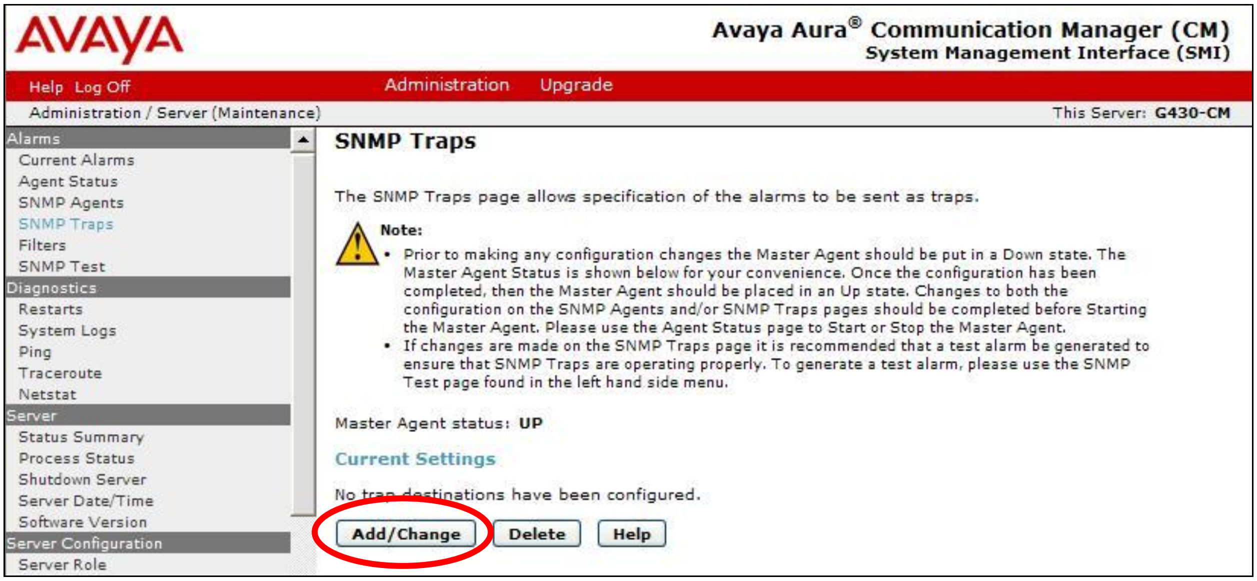
Server Administration

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.



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

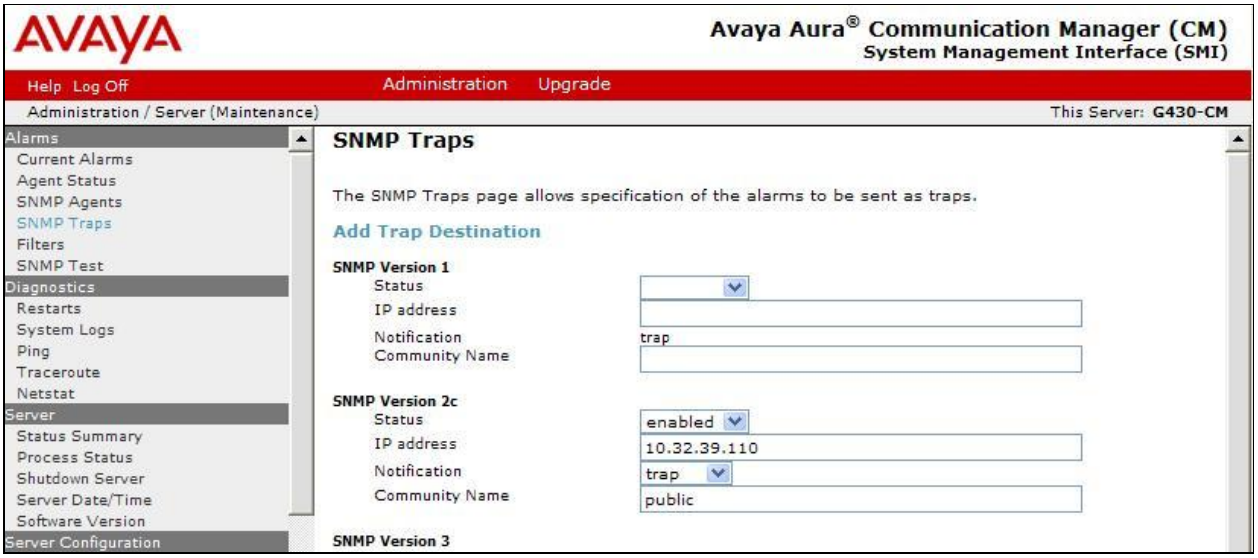
Note:
- Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP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

No trap destinations have been configured.

The **SNMP Traps** screen is updated as shown below. In the **SNMP Version 2c** sub-section, configure the fields as shown, where "10.32.39.110" 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, although not used by ReliaTel.



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

SNMP Version 1
Status:
IP address:
Notification: trap
Community Name:

SNMP Version 2c
Status: enabled
IP address: 10.32.39.110
Notification: trap
Community Name: public

SNMP Version 3

6. Configure Avaya Media Gateway

This section provides the procedures for configuring SNMP on the Avaya 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 Media Gateway, although not used by ReliaTel.

```
G430-001(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 “10.32.39.110” 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 10.32.39.110 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.

```
G430-001(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
---------------- ----- ------- --------------- ----------- --------------------

10.32.39.83       v1   noauth  all              trap       ReadCommN            UDP
port: 162 DM

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

7. Configure TONE Software ReliaTel

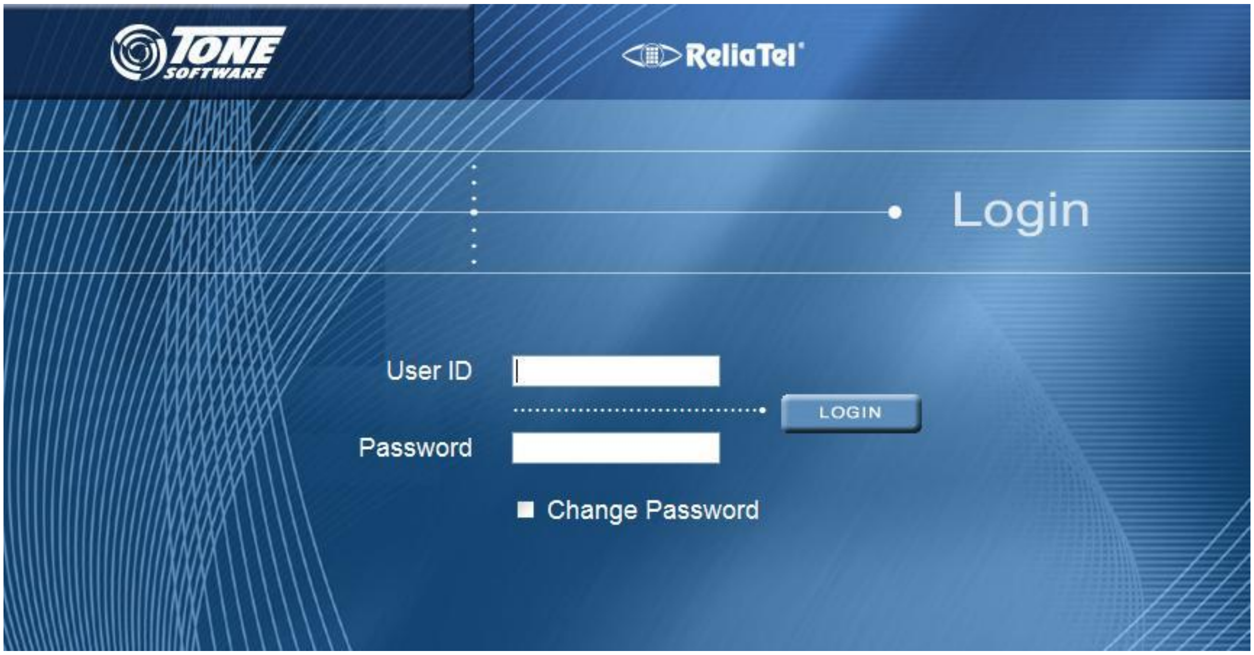
This section provides the procedures for configuring ReliaTel. The procedures include the following areas:

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

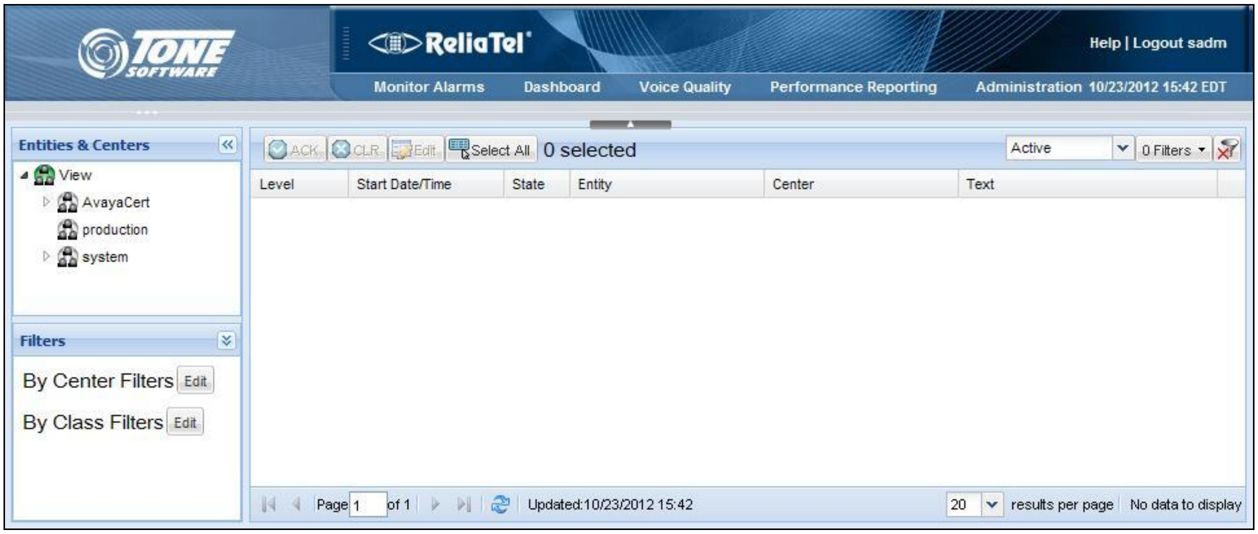
The configuration of ReliaTel is typically performed by TONE Software technicians. The procedural steps are presented in these Application Notes for informational purposes.

7.1. Launch Web Interface

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

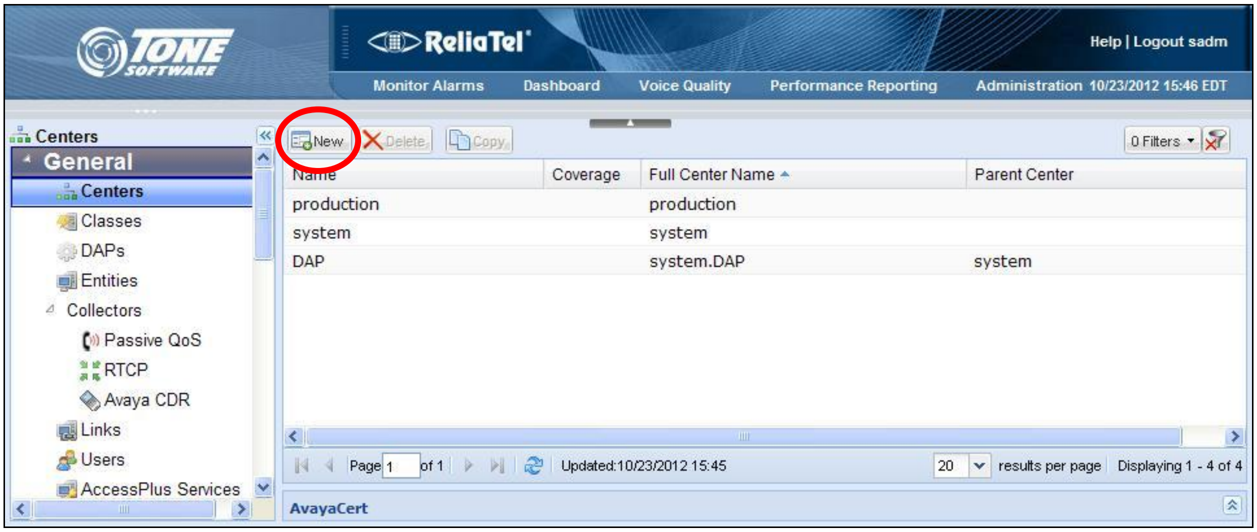


The **ReliaTel** screen is displayed. Select **Administration** > **General Administration** from the top menu.



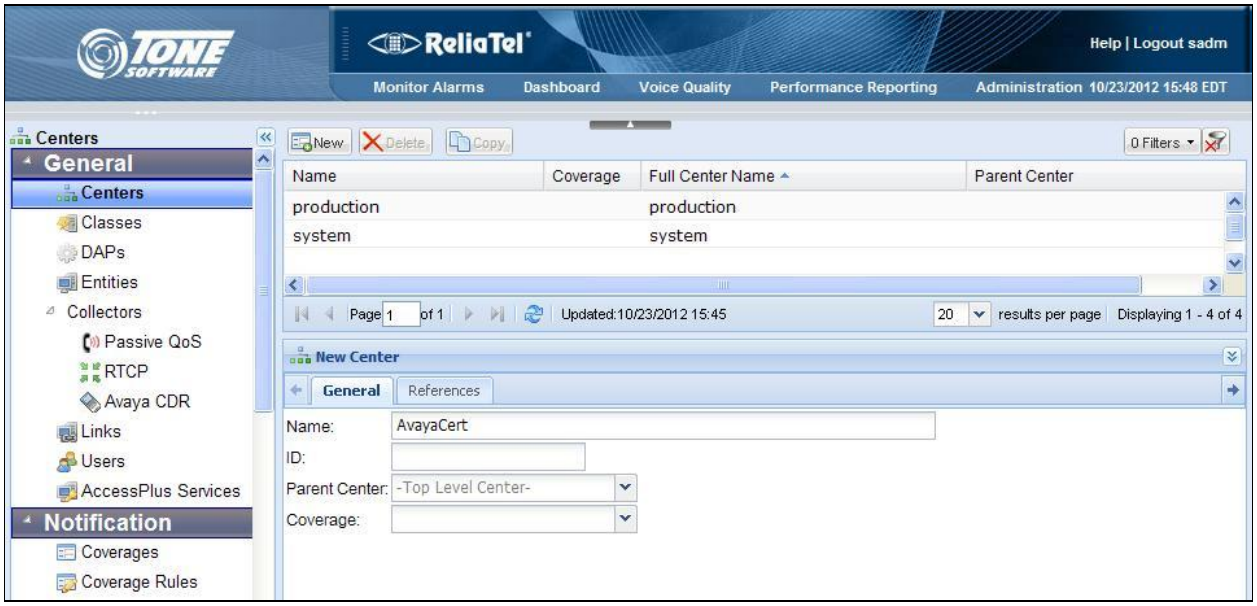
7.2. Administer Centers

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.



Name	Coverage	Full Center Name	Parent Center
production		production	
system		system	
DAP		system.DAP	system

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

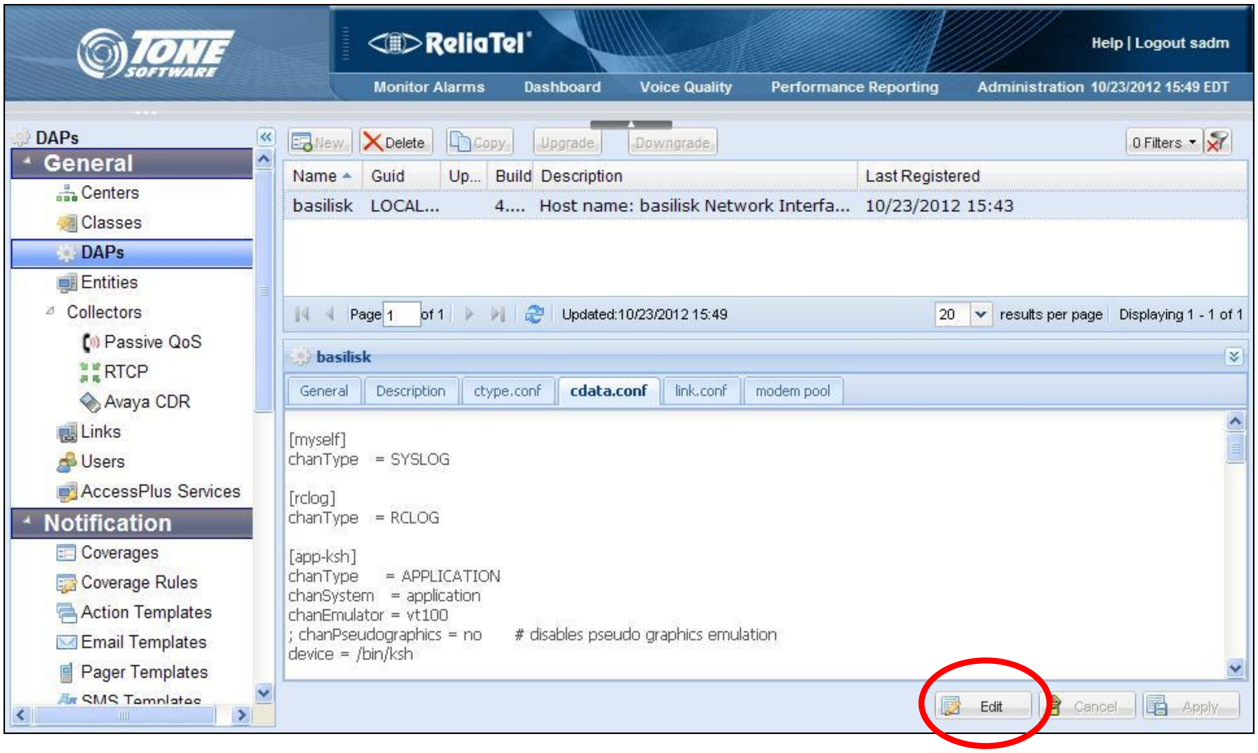


Name	Coverage	Full Center Name	Parent Center
production		production	
system		system	

Name: AvayaCert
ID:
Parent Center: -Top Level Center-
Coverage:

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**.



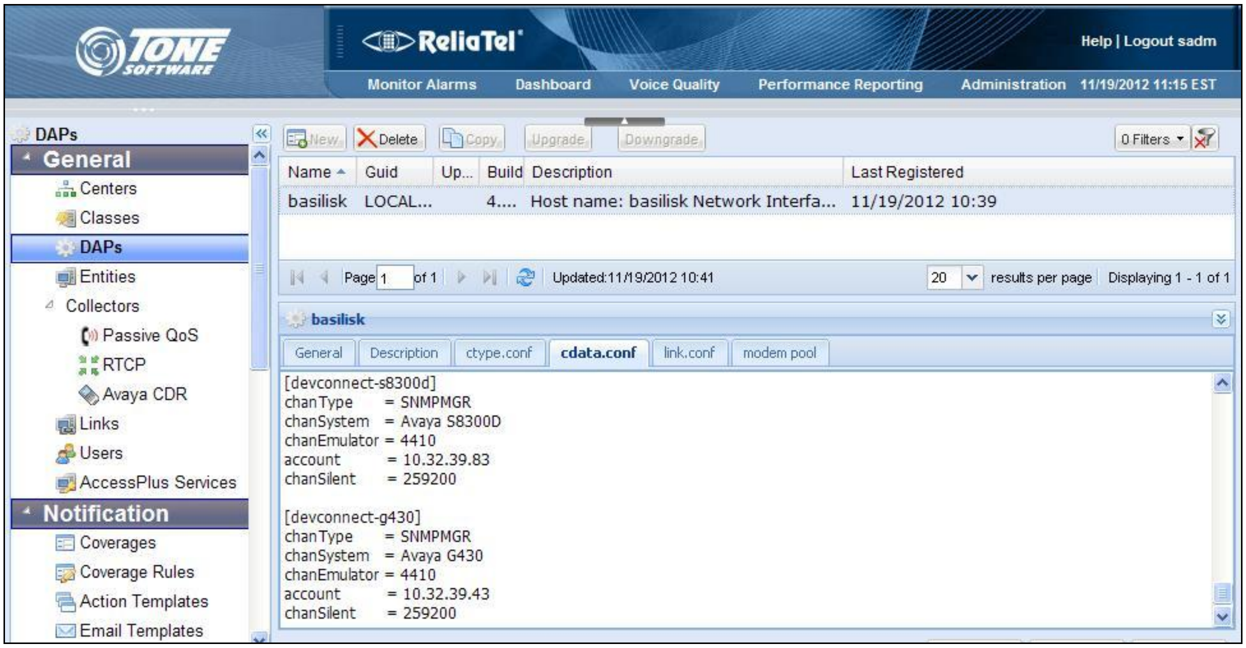
Name	Guid	Up...	Build	Description	Last Registered
basilisk	LOCAL...		4....	Host name: basilisk Network Interfa...	10/23/2012 15:43

```
[myself]
chanType   = SYSLOG

[rclog]
chanType   = RCLOG

[app-ksh]
chanType     = APPLICATION
chanSystem   = application
chanEmulator = vt100
; chanPseudographics = no      # disables pseudo graphics emulation
device = /bin/ksh
```

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

In the examples shown below, “devconnect-s8300d” can be any desired string to denote the Avaya Server, and “devconnect-g430” can be any desired strings to denote the Avaya Media Gateway.

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

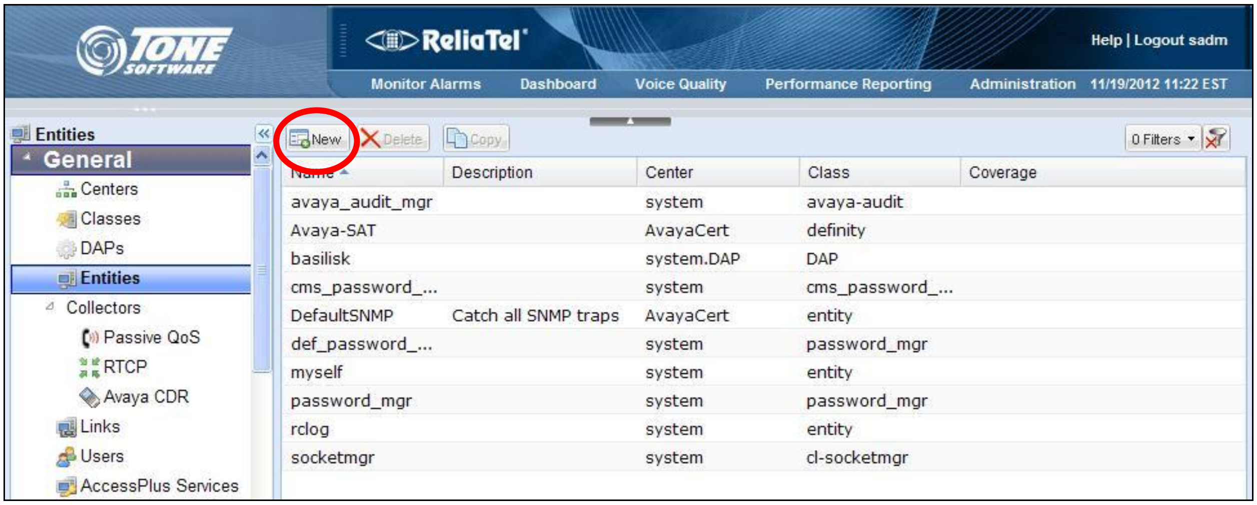


Name	Guid	Up...	Build	Description	Last Registered
basilisk	LOCAL...		4....	Host name: basilisk Network Interfa...	11/19/2012 10:39

```
[devconnect-s8300d]
chanType     = SNMPMGR
chanSystem   = Avaya S8300D
chanEmulator = 4410
account      = 10.32.39.83
chanSilent   = 259200

[devconnect-g430]
chanType     = SNMPMGR
chanSystem   = Avaya G430
chanEmulator = 4410
account      = 10.32.39.43
chanSilent   = 259200
```

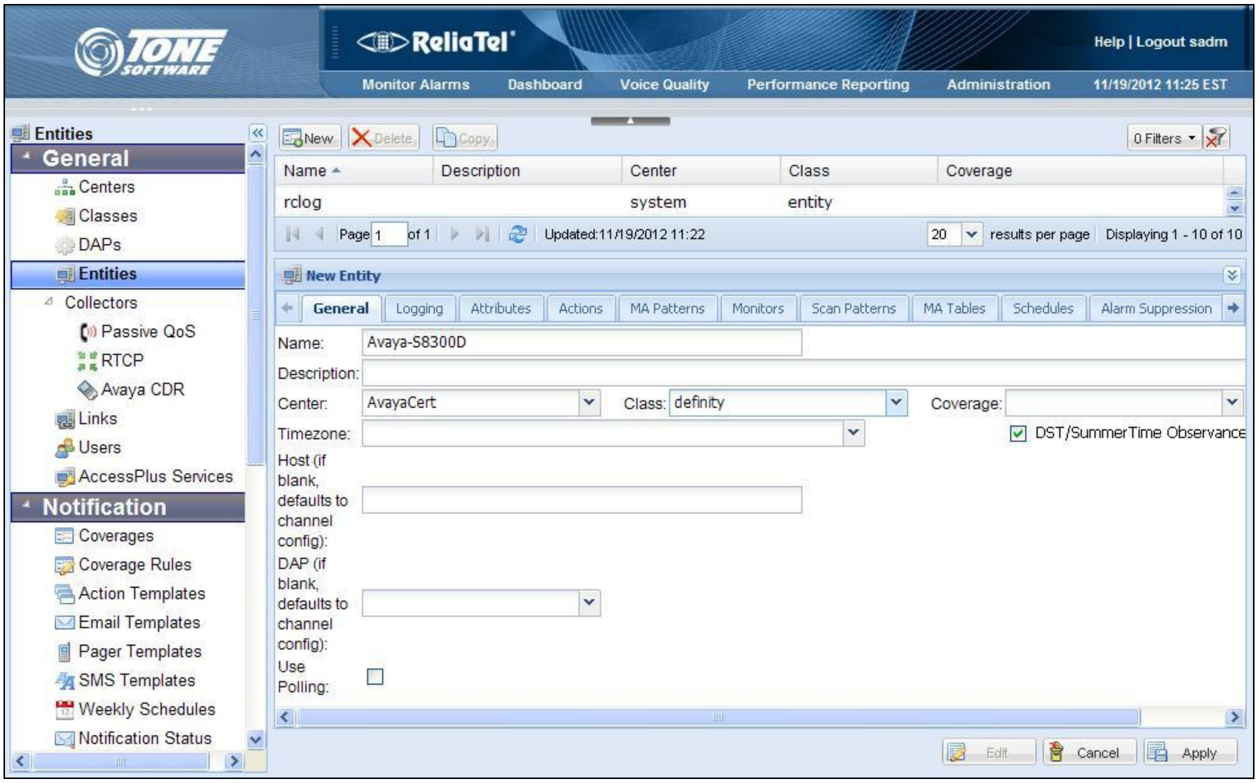
7.4. Administer Entities

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.



Name	Description	Center	Class	Coverage
avaya_audit_mgr		system	avaya-audit	
Avaya-SAT		AvayaCert	definity	
basilisk		system.DAP	DAP	
cms_password_...		system	cms_password_...	
DefaultSNMP	Catch all SNMP traps	AvayaCert	entity	
def_password_...		system	password_mgr	
myself		system	entity	
password_mgr		system	password_mgr	
rclog		system	entity	
socketmgr		system	cl-socketmgr	

In the lower portion of the screen, select the **General** tab. Enter a descriptive **Name** for Communication Manager. For **Center**, select the center name from **Section 7.2**, in this case "AvayaCert". For **Class**, select "definity" from the drop-down list, as shown below.



Name	Description	Center	Class	Coverage
rclog		system	entity	

Name: Avaya-S8300D

Description:

Center: AvayaCert

Class: definity

Coverage:

Timezone:

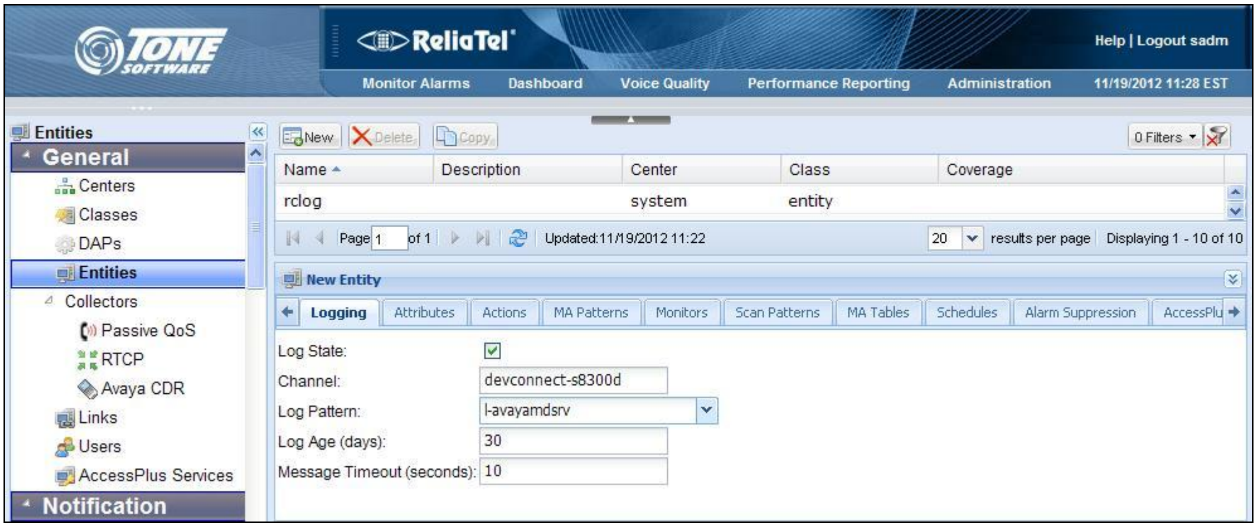
☑ DST/SummerTime Observance

Host (if blank, defaults to channel config):

DAP (if blank, defaults to channel config):

Use Polling: ☐

In the lower portion of the screen, select the **Logging** tab. Check **Log State**. For **Channel**, enter the same string that denotes Communication Manager from **Section 7.3**. For **Log Pattern**, select "l-avayamdsrv" as shown below. Retain the default values in the remaining fields.



Name	Description	Center	Class	Coverage
rclog		system	entity	

Log State: ☑

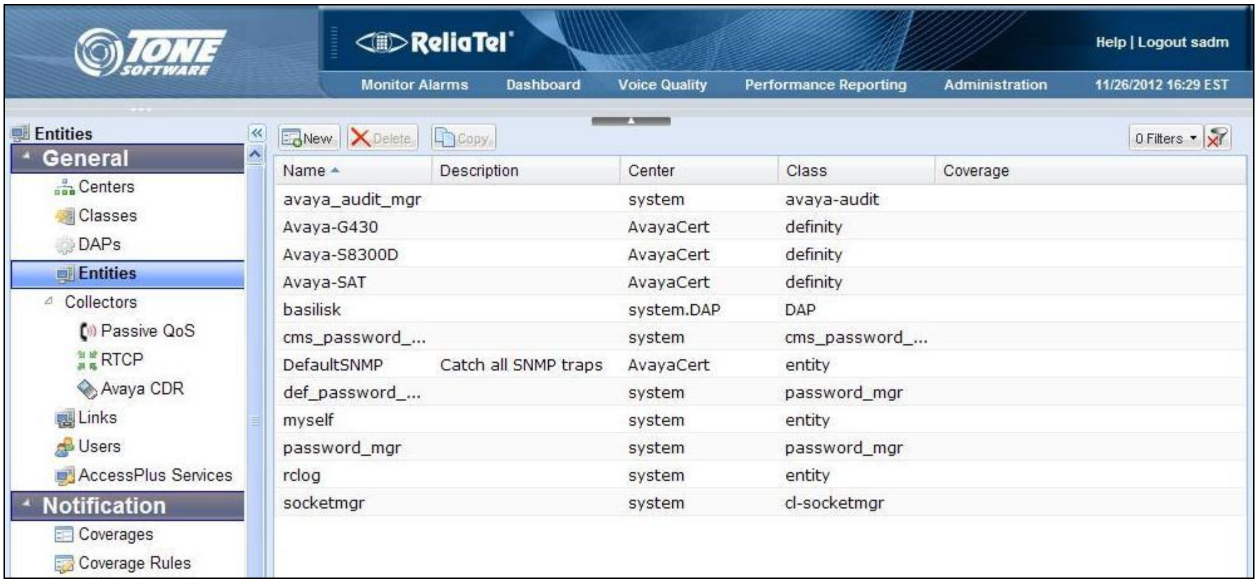
Channel: devconnect-s8300d

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 Media Gateway. In the compliance testing, the "Avaya-S8300D" entity shown below was created for the Avaya Server, and the "Avaya-G430" entity was created for the Avaya Media Gateway.



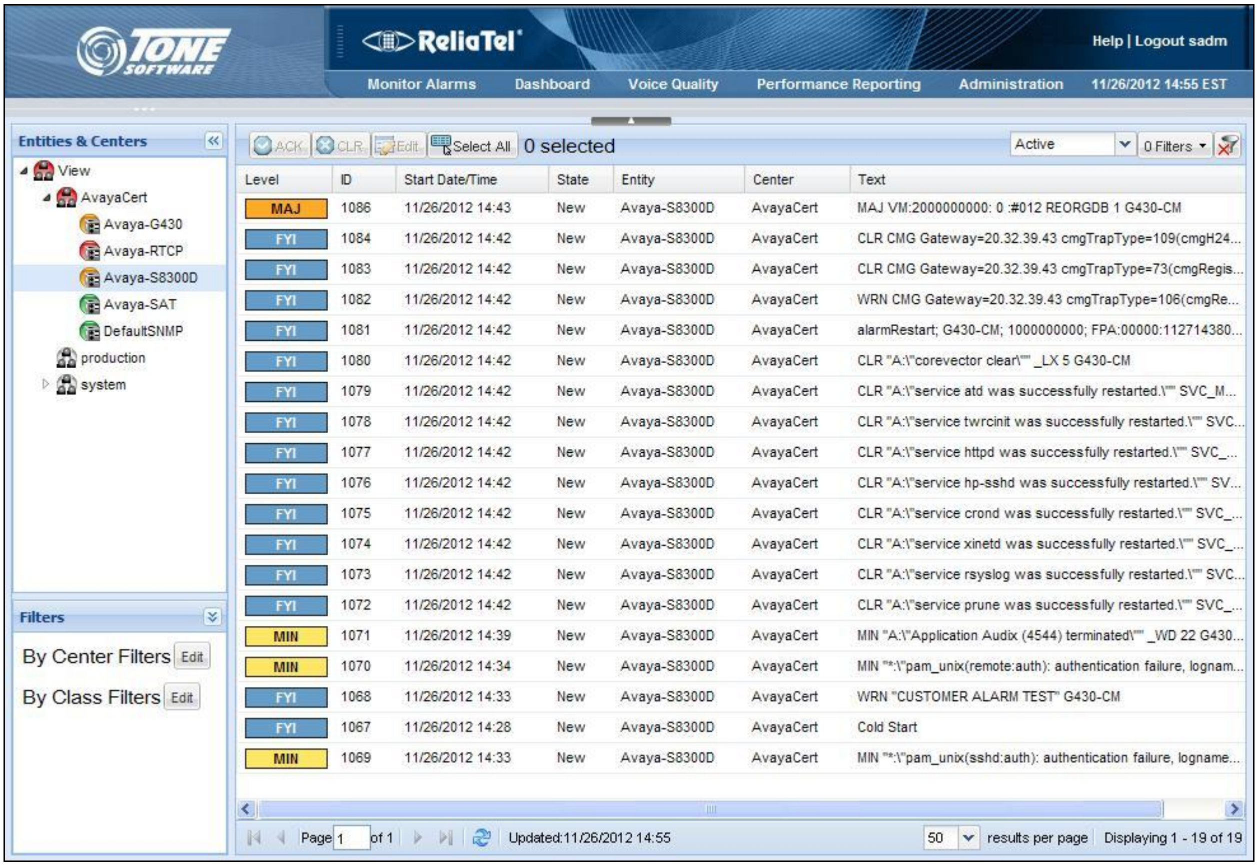
Name	Description	Center	Class	Coverage
avaya_audit_mgr		system	avaya-audit	
Avaya-G430		AvayaCert	definity	
Avaya-S8300D		AvayaCert	definity	
Avaya-SAT		AvayaCert	definity	
basilisk		system.DAP	DAP	
cms_password_...		system	cms_password_...	
DefaultSNMP	Catch all SNMP traps	AvayaCert	entity	
def_password_...		system	password_mgr	
myself		system	entity	
password_mgr		system	password_mgr	
rclog		system	entity	
socketmgr		system	cl-socketmgr	

8. Verification Steps

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

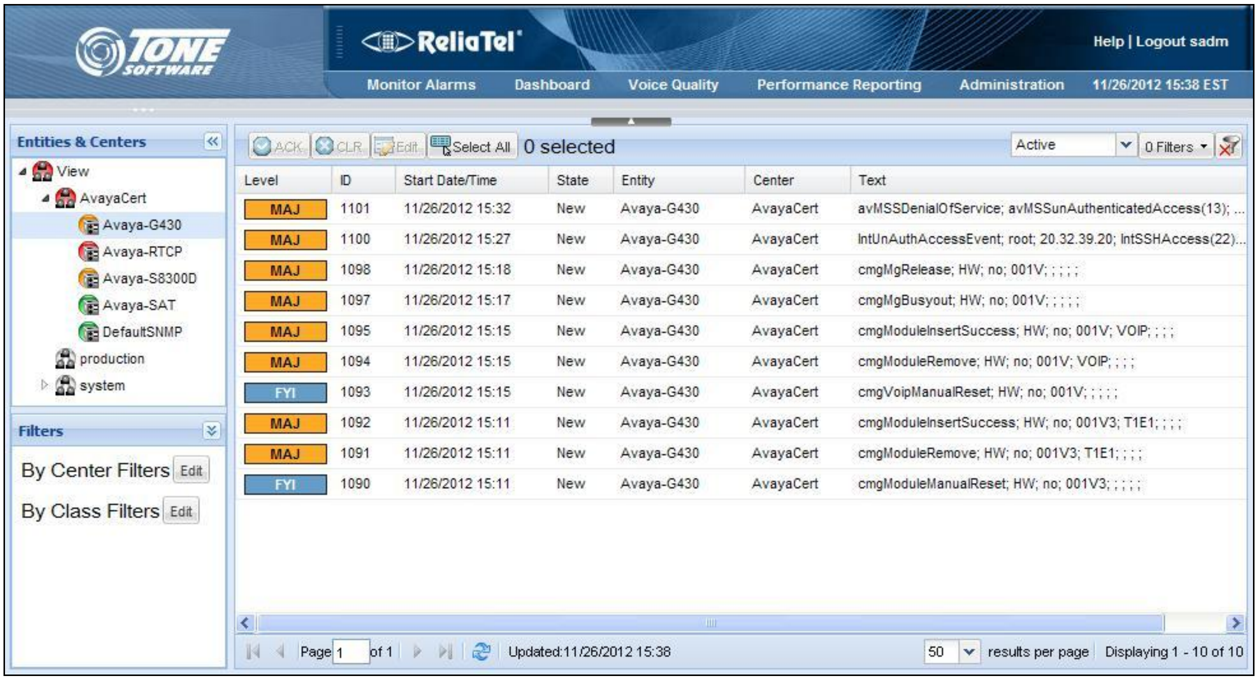
Prior to verification, generate alarms on the Server and Media Gateway.

From the **ReliaTel** screen, select **Monitor Alarms** from the top menu. Select **View > Avaya-Cert > Avaya-S8300D** in the left pane, where **Avaya-S8300D** is the entity name for the Avaya Server from **Section 7.4**. Verify that the new alarms are displayed in the right pane, as shown below.



Level	ID	Start Date/Time	State	Entity	Center	Text
MAJ	1086	11/26/2012 14:43	New	Avaya-S8300D	AvayaCert	MAJ VM:2000000000: 0 :#012 REORGDB 1 G430-CM
FYI	1084	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR CMG Gateway=20.32.39.43 cmgTrapType=109(cmgH24...
FYI	1083	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR CMG Gateway=20.32.39.43 cmgTrapType=73(cmgRegis...
FYI	1082	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	WRN CMG Gateway=20.32.39.43 cmgTrapType=106(cmgRe...
FYI	1081	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	alarmRestart; G430-CM; 1000000000; FPA:00000:112714380...
FYI	1080	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"corevector clear\"" _LX 5 G430-CM
FYI	1079	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service atd was successfully restarted.\"" SVC_M...
FYI	1078	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service twrcinit was successfully restarted.\"" SVC...
FYI	1077	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service httpd was successfully restarted.\"" SVC_...
FYI	1076	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service hp-sshd was successfully restarted.\"" SV...
FYI	1075	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service crond was successfully restarted.\"" SVC_...
FYI	1074	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service xinetd was successfully restarted.\"" SVC_...
FYI	1073	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service rsyslog was successfully restarted.\"" SVC...
FYI	1072	11/26/2012 14:42	New	Avaya-S8300D	AvayaCert	CLR "A:\"service prune was successfully restarted.\"" SVC_...
MIN	1071	11/26/2012 14:39	New	Avaya-S8300D	AvayaCert	MIN "A:\"Application Audix (4544) terminated\"" _WD 22 G430...
MIN	1070	11/26/2012 14:34	New	Avaya-S8300D	AvayaCert	MIN "*:\"pam_unix(remote:auth): authentication failure, lognam...
FYI	1068	11/26/2012 14:33	New	Avaya-S8300D	AvayaCert	WRN "CUSTOMER ALARM TEST" G430-CM
FYI	1067	11/26/2012 14:28	New	Avaya-S8300D	AvayaCert	Cold Start
MIN	1069	11/26/2012 14:33	New	Avaya-S8300D	AvayaCert	MIN "*:\"pam_unix(sshd:auth): authentication failure, logname...

Select **View > Avaya-Cert > Avaya-G430** in the left pane, where **Avaya-G430** is the entity name for the Avaya Media Gateway from **Section 7.4**. Verify that the new alarms are displayed in the right pane, as shown below.



Level	ID	Start Date/Time	State	Entity	Center	Text
MAJ	1101	11/26/2012 15:32	New	Avaya-G430	AvayaCert	avMSSDenialOfService; avMSSunAuthenticatedAccess(13); ...
MAJ	1100	11/26/2012 15:27	New	Avaya-G430	AvayaCert	IntUnAuthAccessEvent; root; 20.32.39.20; IntSSHAccess(22)...
MAJ	1098	11/26/2012 15:18	New	Avaya-G430	AvayaCert	cmgMgRelease; HW; no; 001V; ; ; ; ;
MAJ	1097	11/26/2012 15:17	New	Avaya-G430	AvayaCert	cmgMgBusyout; HW; no; 001V; ; ; ; ;
MAJ	1095	11/26/2012 15:15	New	Avaya-G430	AvayaCert	cmgModuleInsertSuccess; HW; no; 001V; VOIP; ; ; ;
MAJ	1094	11/26/2012 15:15	New	Avaya-G430	AvayaCert	cmgModuleRemove; HW; no; 001V; VOIP; ; ; ;
FYI	1093	11/26/2012 15:15	New	Avaya-G430	AvayaCert	cmgVoipManualReset; HW; no; 001V; ; ; ; ;
MAJ	1092	11/26/2012 15:11	New	Avaya-G430	AvayaCert	cmgModuleInsertSuccess; HW; no; 001V3; T1E1; ; ; ;
MAJ	1091	11/26/2012 15:11	New	Avaya-G430	AvayaCert	cmgModuleRemove; HW; no; 001V3; T1E1; ; ; ;
FYI	1090	11/26/2012 15:11	New	Avaya-G430	AvayaCert	cmgModuleManualReset; HW; no; 001V3; ; ; ; ;

9. Conclusion

These Application Notes describe the configuration steps required TONE Software ReliaTel to successfully interoperate with Avaya Aura® Communication Manager 6.2 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 7.0, Release 6.2, July 2012, available at http://support.avaya.com.

2. *CLI Reference Avaya Branch Gateway G430*, Document 03-603234, Issue 3, February 2011, available at http://support.avaya.com**.**

3. *ReliaTel Operator Guide*, Release 4.1, Guide Version 1.0, October 2012, 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.