# Application Notes for Unique Communications CAIRS Fault Management with Avaya Aura® Communication Manager - Issue 1.0

## Abstract

These Application Notes describe the configuration steps required for Unique Communications CAIRS Fault Management to successfully interoperate with Avaya Aura® Communication Manager.

Unique Communications CAIRS is an umbrella solution which includes various subcomponents (Accounting Management, Fault Management, Performance Management, Configuration Management, and IP Discovery). These Application Notes only cover the Fault Management component.

Unique Communications CAIRS Fault Management is a SNMP TRAP receiver that receives alarm from Avaya S8300D server and the Avaya Media Gateway.

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

The overall objective of this interoperability compliance testing is to verify that Unique Communications CAIRS Fault Management (CAIRS Fault Management) can interoperate with Avaya Aura® Communication Manager 6.3.

Unique Communications CAIRS Fault Management is a SNMP TRAP receiver that receives alarm from the Avaya S8300D server and the Avaya Media Gateway.

Unique Communications CAIRS Fault Management is configured to receive SNMP traps from Avaya Aura® Communication Manager, to display the data in a web interface and to execute actions based on the alarm type.

During the test, SIP endpoints were included. SIP endpoints registered with Avaya Aura® Session Manager. An assumption is made that Avaya Aura® Session Manager and Avaya Aura® System Manager are already installed and basic configuration have been performed.

Only steps relevant to this compliance test will be described in this document. In these Application Notes, the following topics will be described:

- Avaya S8300D Server – SNMP TRAP configuration
- Avaya G450 Media Gateway – SNMP TRAP configuration
- Unique Communications CAIRS Fault Management– SNMP TRAP receiver configuration

# 2. General Test Approach and Test Results

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

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 testing included features tests. The focus of the compliance testing was primarily on verifying the proper reporting of SNMP traps by CAIRS Fault Management. SNMP Traps generated by Avaya Server included SNMP Test, server reboot, server login fail, and SNMP agent restart. The SNMP traps generated by Avaya Media Gateway included media module reset, VoIP engine reset, VoIP engine busyout/release, and login failure.

## 2.2. Test Results

All executed test cases passed.

CAIRS Fault Management successfully received various types of traps from the Avaya S8300D Server and Avaya G450 Media Gateway.

## 2.3. Support

Technical support for CAIRS Fault Management can be obtained through the following:

- support@unique.net
- (702) 216 – 0266 opt 1
- www.unique.net/support

## 3. Reference Configuration

**Figure 1** illustrates a configuration used during the compliance test. For completeness, Avaya 96xx Series SIP IP Deskphones on the Avaya S8300D Server and Avaya G450 Media Gateway side have been registered to Session Manager, and are included in **Figure 1** to demonstrate calls between the SIP endpoints that are going through the IP/PRI trunk between two Communication Manager. The solution described herein is also extensible to other Avaya Servers and Media Gateways.

***Note:*** *Avaya S8300D Server with an Avaya G430 Media Gateway was included in the test only to provide an inter-switch scenario. Thus, there will not be any discussion on configuring Avaya S8300D Server with an Avaya G430 Media Gateway.*

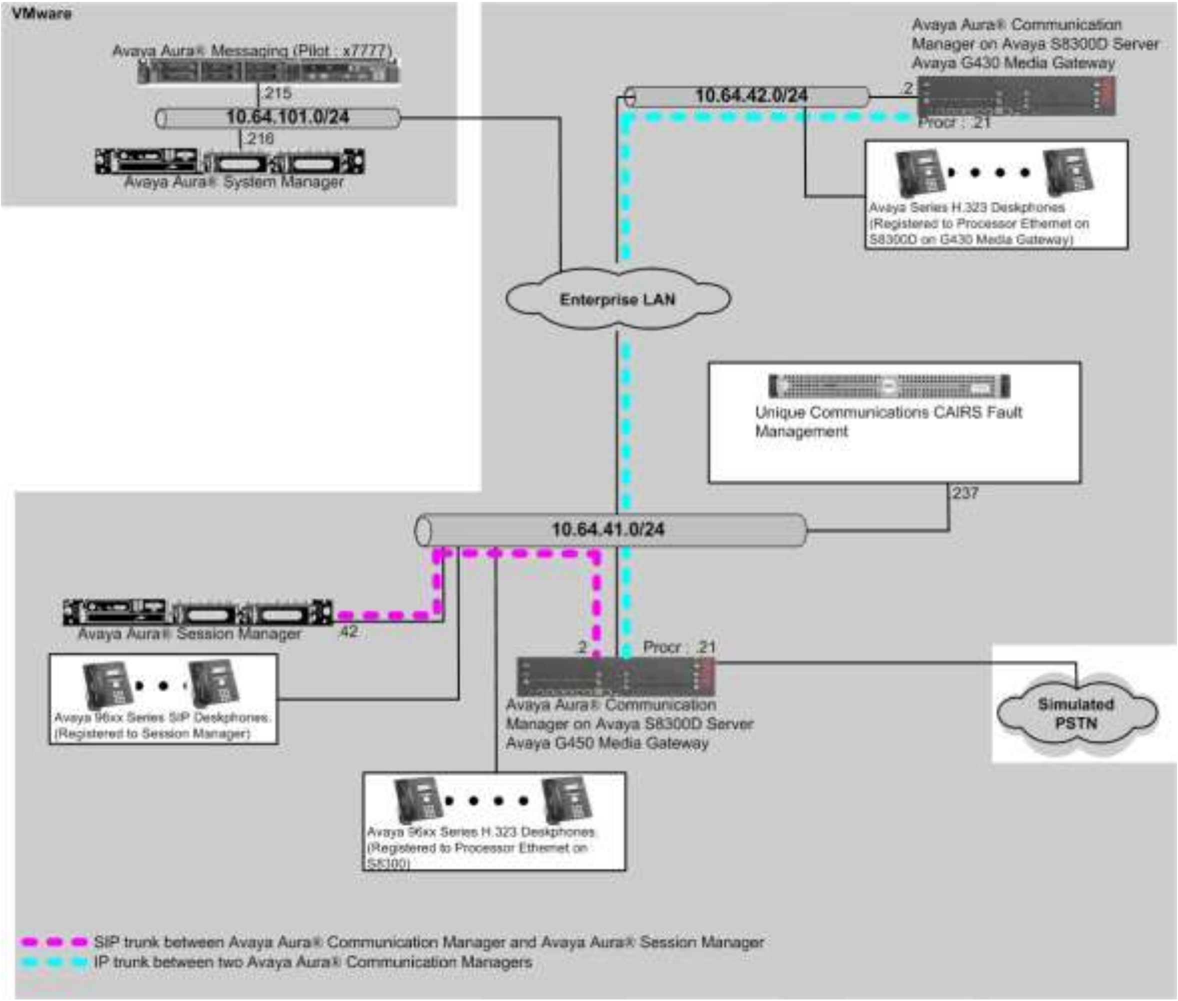

VMware
Avaya Aura® Messaging (Pilot : x7777)
.215
10.64.101.0/24
.216
Avaya Aura® System Manager
Avaya Aura® Communication Manager on Avaya S8300D Server Avaya G430 Media Gateway
.2
10.64.42.0/24
Procr : .21
Avaya Series H.323 Deskphones (Registered to Processor Ethernet on S8300D on G430 Media Gateway)
Enterprise LAN
Unique Communications CAIRS Fault Management
.237
10.64.41.0/24
Avaya Aura® Session Manager
.42
.2
Procr : .21
Avaya 96xx Series SIP Deskphones. (Registered to Session Manager)
Avaya Aura® Communication Manager on Avaya S8300D Server Avaya G450 Media Gateway
Simulated PSTN
Avaya 96xx Series H.323 Deskphones. (Registered to Processor Ethernet on S8300)
SIP trunk between Avaya Aura® Communication Manager and Avaya Aura® Session Manager
IP trunk between two Avaya Aura® Communication Managers

**Figure 1. Test configuration of Unique Communications CAIRS Fault Management with Avaya Aura® Communication Manager**

## 4. Equipment and Software Validated

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

| Equipment/Software | | Release/Version |
|---|---|---|
| Avaya S8300D Server with Avaya G450 Media Gateway | | Avaya Aura® Communication Manager 6.3 (R016x.03.0.124.0) with Patch 03.0.124.0-21754 |
| Avaya Aura® System Manager | | 6.3.13 |
| Avaya Aura® Session Manager | | 6.3.13.0.631304 |
| Avaya 9600 Series SIP IP Deskphone | | |
| | 9620<br>9641G | 2.6.12<br>6.5 |
| Avaya 9600 and 96X1 Series H.323 IP Deskphone | | |
| | 9620<br>9621G<br>9650 | 3.22<br>6.23<br>3.23 |
| | | |
| Unique Communications CAIRS Fault Management on Windows 8.1 Enterprise | | 4.0 |

# 5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring SNMP in Communication Manager. These steps describe the procedure used for the Avaya S8300D Server and Avaya G450 Media Gateway. All steps are the same for the other Avaya Servers and Avaya Media Gateways.

In this section, the following topics will be discussed:

- SNMP TRAP Configuration (Avaya Server)
- SNMP TRAP Configuration (Avaya Media Gateway)

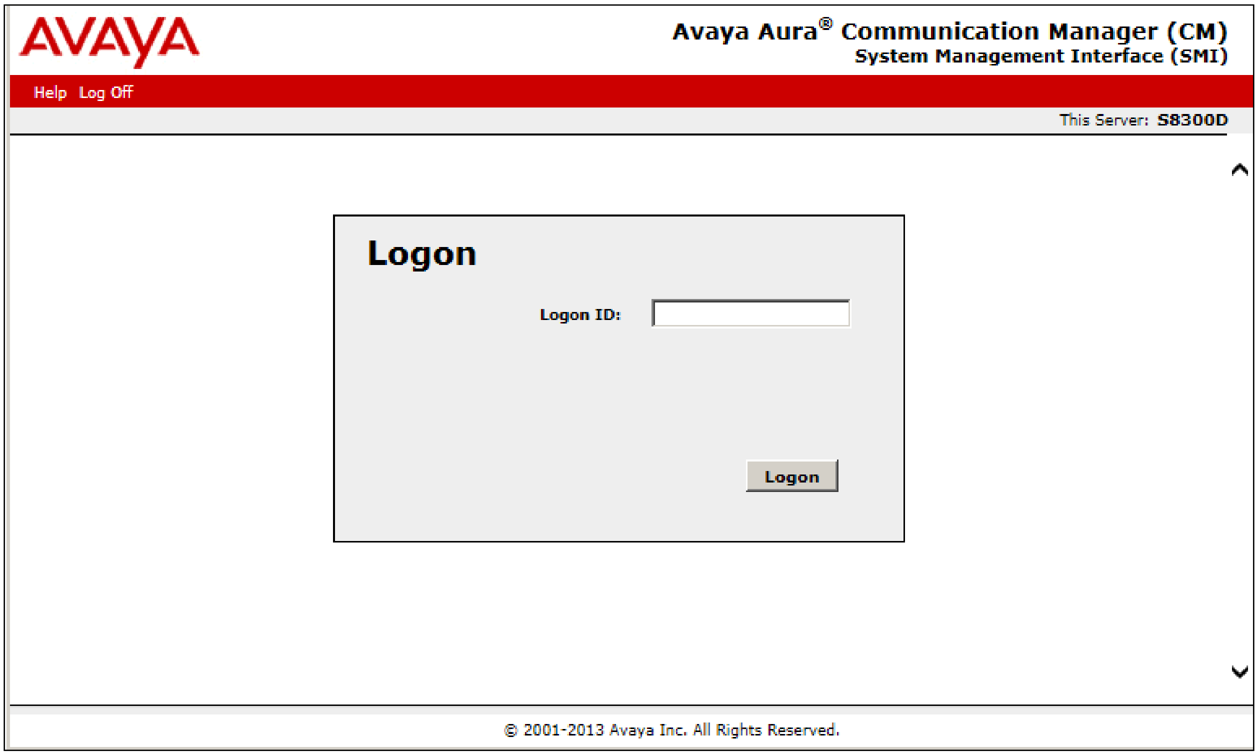
## 5.1. Configure Avaya S8300D Server

The procedures include the following areas:

- Launch maintenance web interface
- Administer SNMP traps

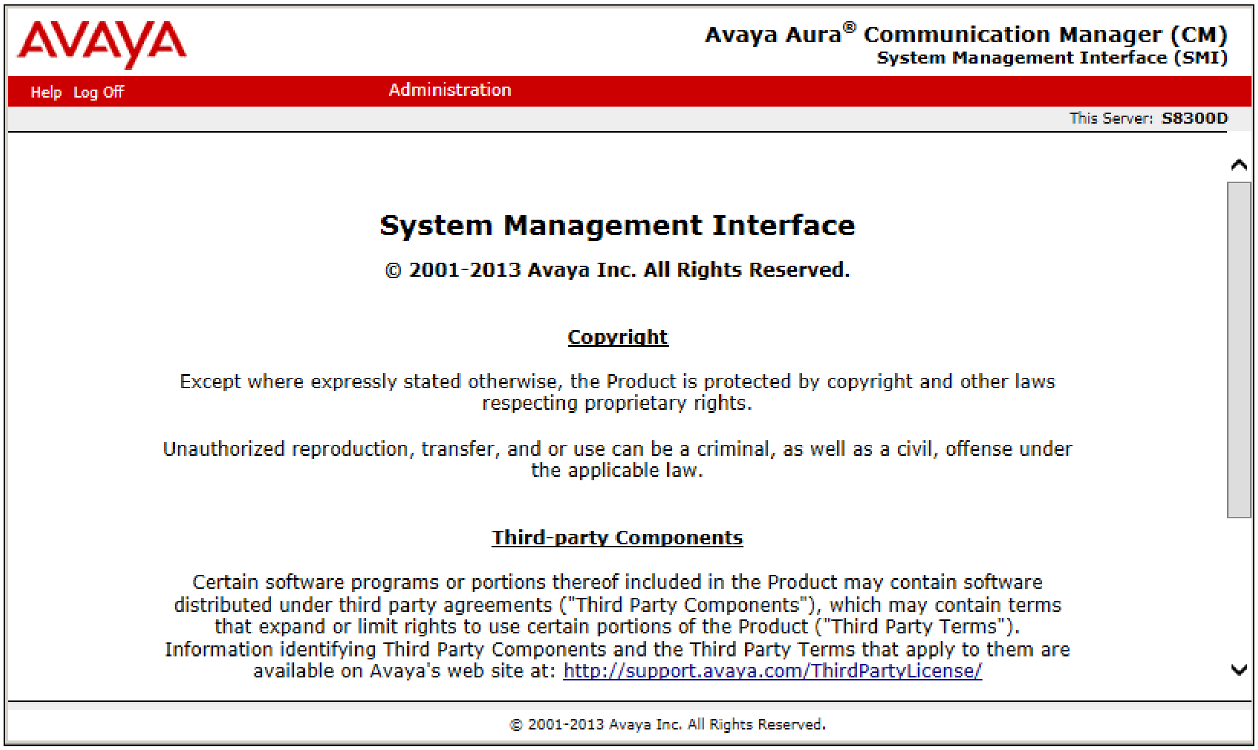
### 5.1.1. Launch Maintenance Web Interface

Launch a web browser, enter **http://<IP address of Communication Manager>** in the URL, and log in with the appropriate credentials.



AVAYA
Avaya Aura® Communication Manager (CM)
System Management Interface (SMI)
Help
Log Off
This Server: S8300D
Logon
Logon ID:
Logon
© 2001-2013 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
This Server: S8300D

System Management Interface

© 2001-2013 Avaya Inc. All Rights Reserved.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights.

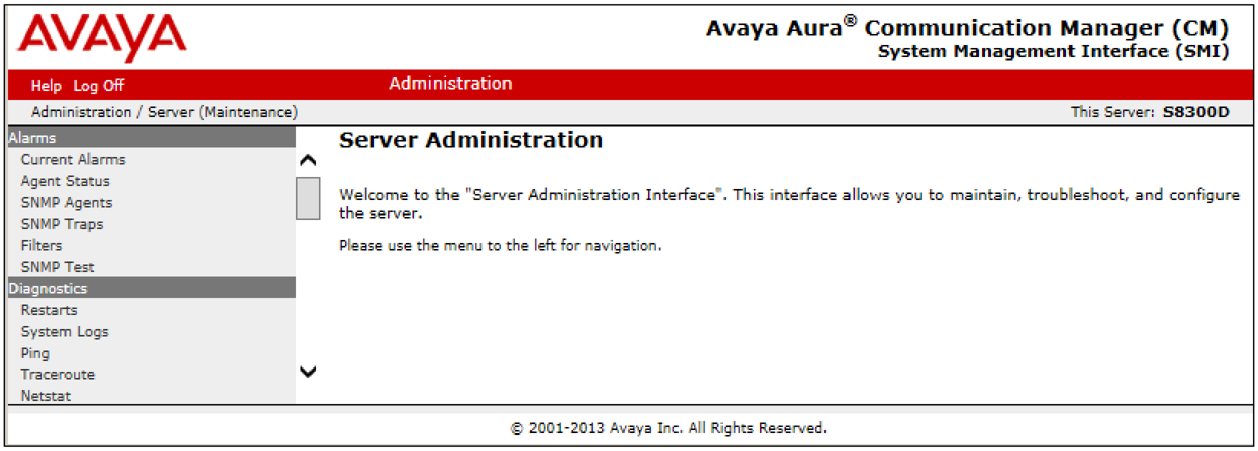
Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

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/

© 2001-2013 Avaya Inc. All Rights Reserved.

The **Server Administration** screen is displayed.



Server Administration

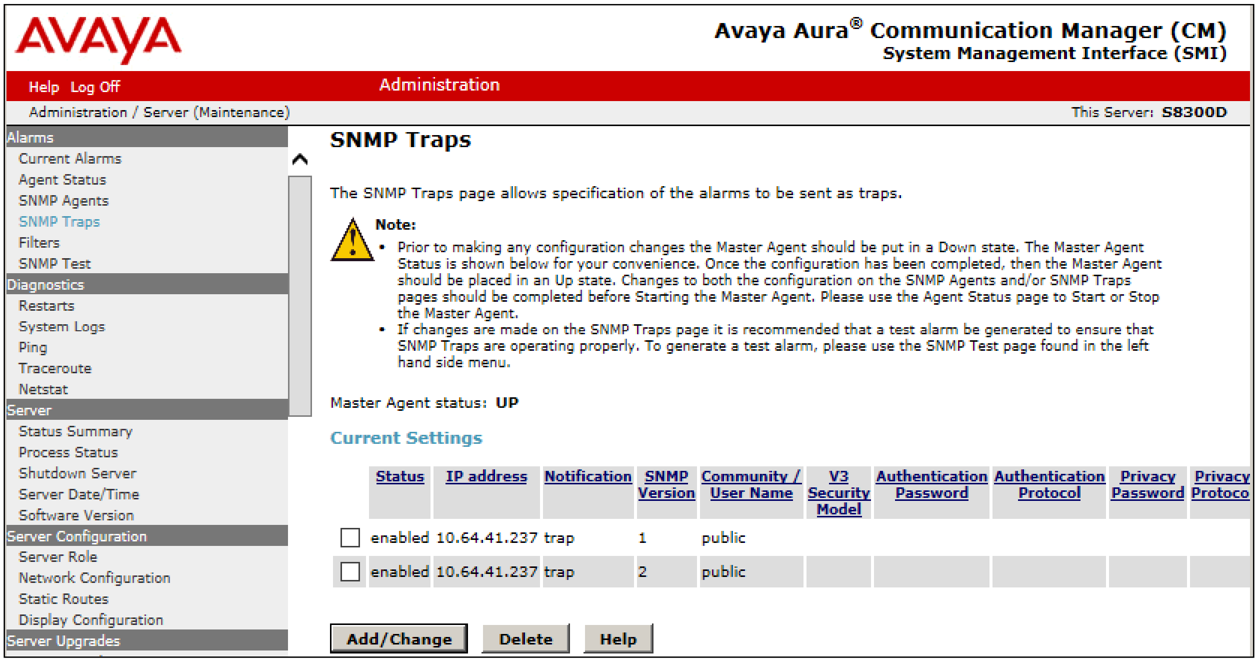
Welcome to the "Server Administration Interface". This interface allows you to maintain, troubleshoot, and configure the server.

Please use the menu to the left for navigation.

© 2001-2013 Avaya Inc. All Rights Reserved.

### 5.1.2. 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.



**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.

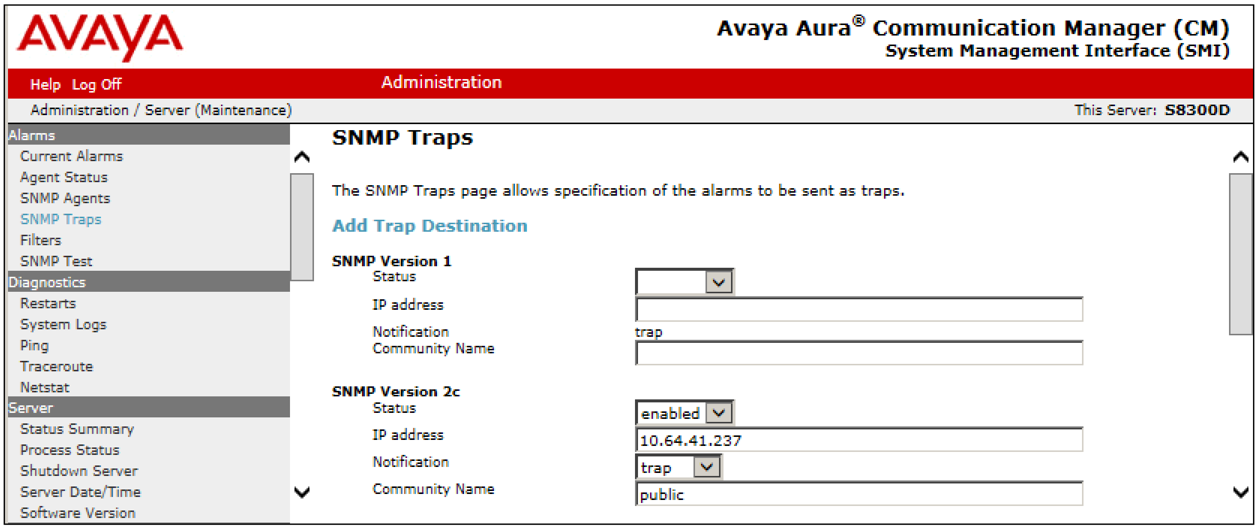
Master Agent status: **UP**

**Current Settings**

| | Status | IP address | Notification | SNMP Version | Community / User Name | V3 Security Model | Authentication Password | Authentication Protocol | Privacy Password | Privacy Protoco |
|---|---|---|---|---|---|---|---|---|---|---|
| □ | enabled | 10.64.41.237 | trap | 1 | public | | | | | |
| □ | enabled | 10.64.41.237 | trap | 2 | public | | | | | |

The **SNMP Traps** screen is updated as shown below. In the **SNMP Version 2c** sub-section, configure the fields as shown, where “10.64.41.237” is the IP address of CAIRS Fault Management, and **Community Name** can be any desired string.

Note that **Community Name** is required to be configured on Communication Manager. The Community Name will be utilized by CAIRS Fault Management.



**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 | trap |
| Community Name | |

**SNMP Version 2c**

| | |
|---|---|
| Status | enabled |
| IP address | 10.64.41.237 |
| Notification | trap |
| Community Name | public |

## 5.2. 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:

- Configure community string
- Configure SNMP Traps

### 5.2.1. Configure 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. The community name will be utilized by CAIRS Fault Management.

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

### 5.2.2. Configure SNMP Traps

Use the “snmp-server host” command shown below to enable SNMP traps and notifications to CAIRS Fault Management, where “10.64.41.237” is the IP address of the CAIRS Fault Management server, and “public” is the read-only community string from **Section 5.1.2**.

```
G450-001(super)#
G450-001(super)# snmp-server host 10.64.41.237 traps v1 public
Done!
G450-001(super)
```

# 6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager as provisioned in the reference configuration. Session Manager is comprised of two functional components: the Session Manager server and the System Manager server. All SIP call provisioning for Session Manager is performed through the System Manager Web interface and is then downloaded into Session Manager.

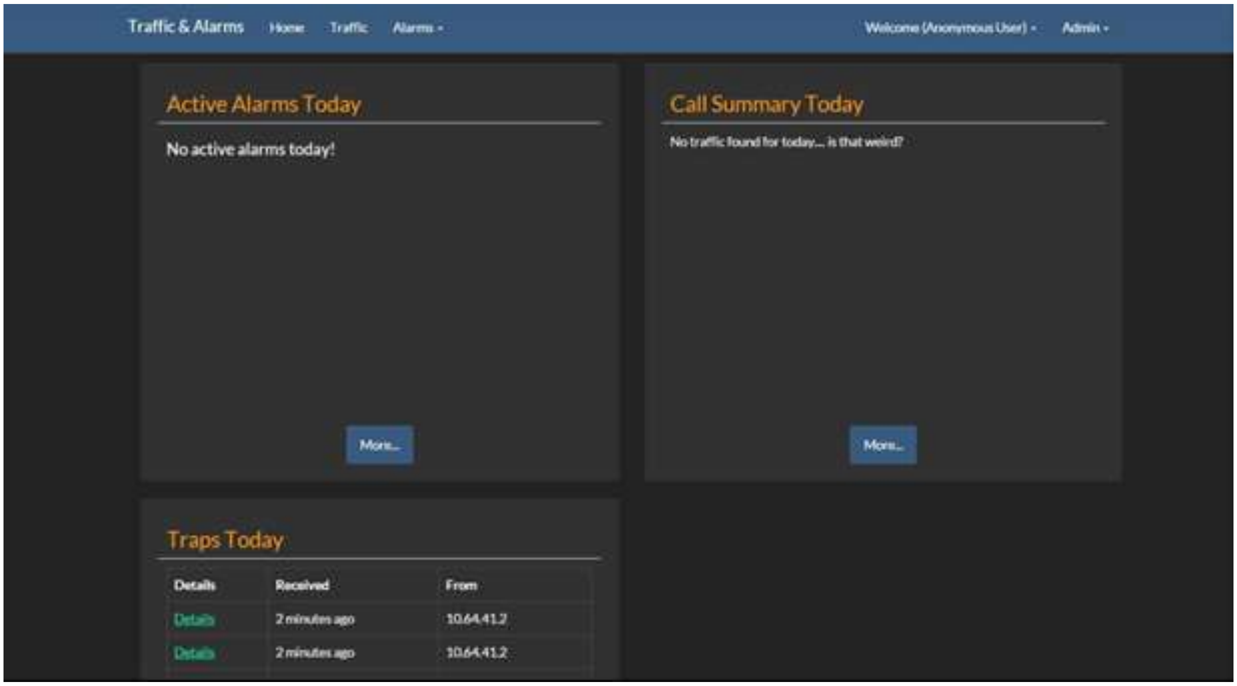
It is assumed that Session Manager and System Manager have been installed, network connectivity exists between Communication Manager and Session Manager, and following topics are already configured in System Manager:

- **SIP Domains**
- **Locations**
- **SIP Entities**
- **Entity Links**
- **Time Ranges**
- **Routing Policy**
- **Dial Patterns**
- **Manage Element**
- **Applications**
- **Application Sequence**
- **Manage Users**

# 7. Configure Unique Communications CAIRS Fault Management

This section describes the operation of Unique Communications CAIRS Fault Management to receive SNMP traps from Avaya Server and Avaya Media Gateways. Installation of the CAIRS Fault Management software was performed by a Unique Communications engineer prior to the actual compliance test.

To configure CAIRS Fault Management, navigate to http://<ip-address> in an Internet browser window, where "ip-addrss" is the IP address of the CAIRS Fault Management server. The **Traffic & Alarms** window is displayed.



Active Alarms Today

No active alarms today!

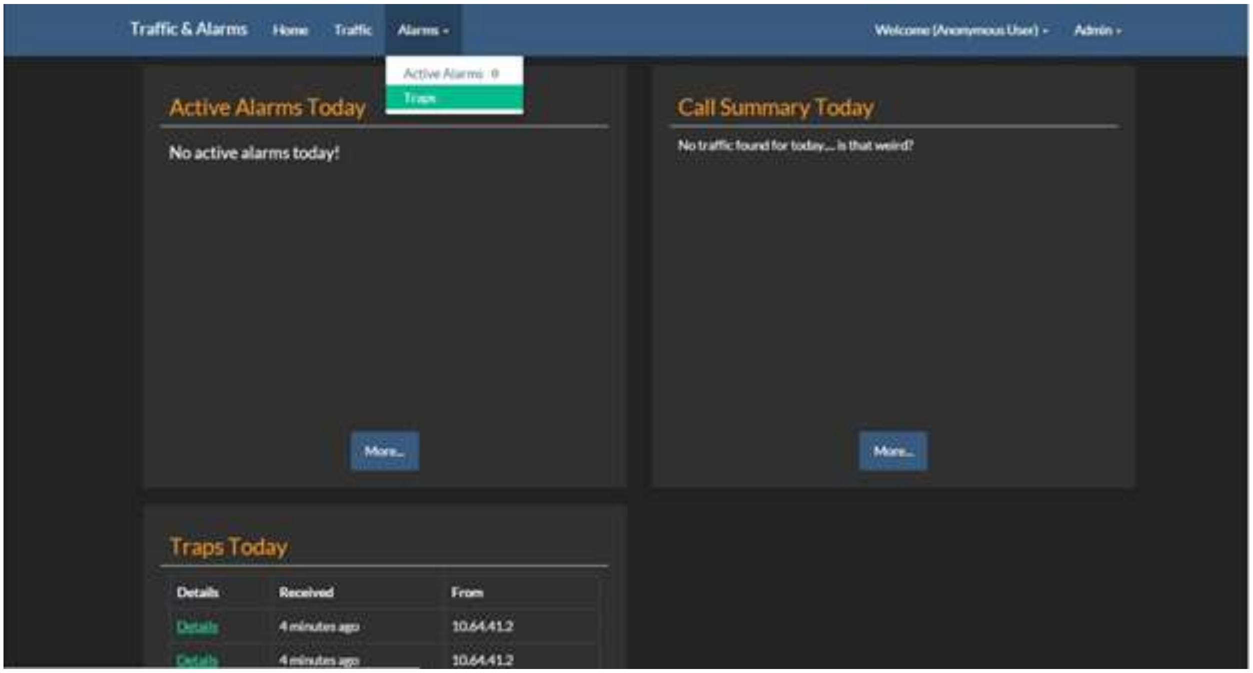
Call Summary Today

No traffic found for today.... is that weird?

Traps Today

| Details | Received | From |
|---|---|---|
| Details | 2 minutes ago | 10.64.41.2 |
| Details | 2 minutes ago | 10.64.41.2 |

On the **Traffic & Alarms** window, select **Alarm → Traps**



Active Alarms Today

No active alarms today!

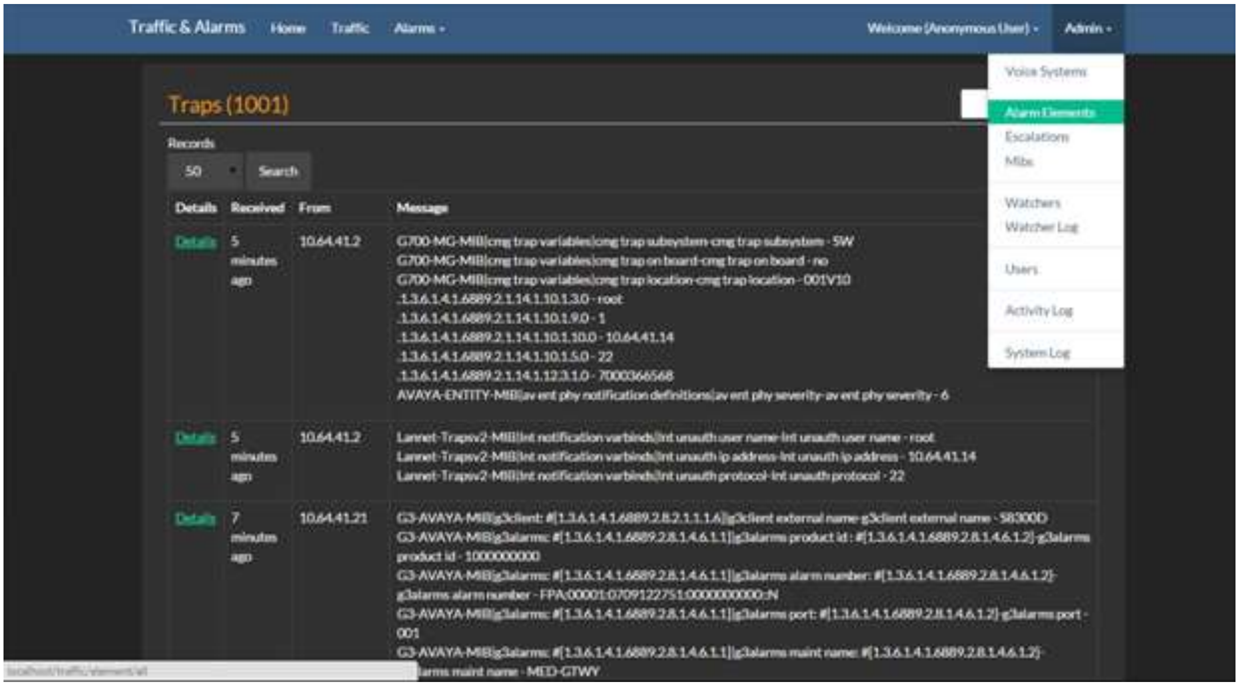
Call Summary Today

No traffic found for today.... is that weird?

Traps Today

| Details | Received | From |
|---|---|---|
| Details | 4 minutes ago | 10.64.41.2 |
| Details | 4 minutes ago | 10.64.41.2 |

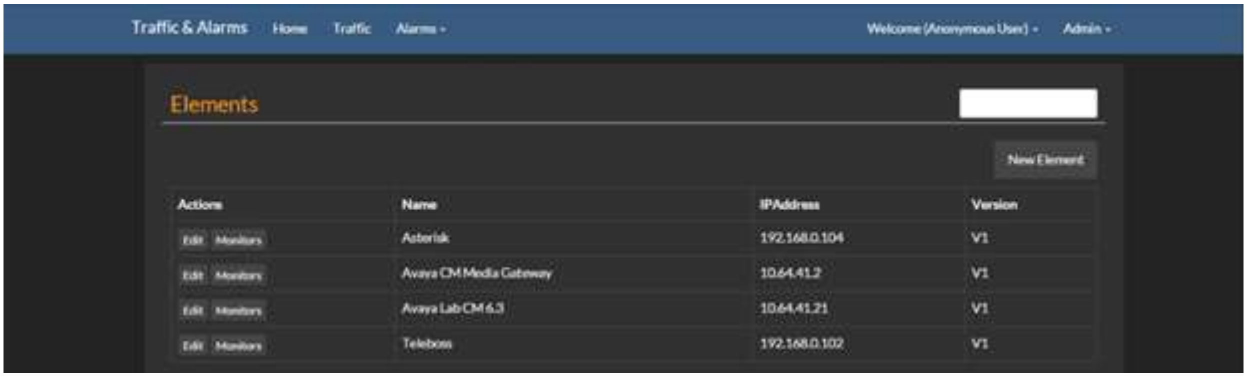
The **Traps** sub-page is displayed.  On the **Traps** page, select **Admin → Alarm Elements**.



Traps (1001)

| Details | Received | From | Message |
|---|---|---|---|
| Details | 5 minutes ago | 10.64.41.2 | G700-MG-MIB\|cmg trap variables\|cmg trap subsystem-cmg trap subsystem - SW<br>G700-MG-MIB\|cmg trap variables\|cmg trap on board-cmg trap on board - no<br>G700-MG-MIB\|cmg trap variables\|cmg trap location-cmg trap location - 001V10<br>.1.3.6.1.4.1.6889.2.1.14.1.10.1.3.0 - root<br>.1.3.6.1.4.1.6889.2.1.14.1.10.1.9.0 - 1<br>.1.3.6.1.4.1.6889.2.1.14.1.10.1.10.0 - 10.64.41.14<br>.1.3.6.1.4.1.6889.2.1.14.1.10.1.5.0 - 22<br>.1.3.6.1.4.1.6889.2.1.14.1.12.3.1.0 - 7000366568<br>AVAYA-ENTITY-MIB\|av ent phy notification definitions\|av ent phy severity-av ent phy severity - 6 |
| Details | 5 minutes ago | 10.64.41.2 | Lannet-Trapsv2-MIB\|lnt notification varbinds\|lnt unauth user name-lnt unauth user name - root<br>Lannet-Trapsv2-MIB\|lnt notification varbinds\|lnt unauth ip address-lnt unauth ip address - 10.64.41.14<br>Lannet-Trapsv2-MIB\|lnt notification varbinds\|lnt unauth protocol-lnt unauth protocol - 22 |
| Details | 7 minutes ago | 10.64.41.21 | G3-AVAYA-MIB\|g3client: #[1.3.6.1.4.1.6889.2.8.2.1.1.1.6]\|g3client external name-g3client external name - S8300D<br>G3-AVAYA-MIB\|g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]\|g3alarms product id : #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms product id - 1000000000<br>G3-AVAYA-MIB\|g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]\|g3alarms alarm number: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms alarm number - FPA:00001:0709122751:0000000000:N<br>G3-AVAYA-MIB\|g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]\|g3alarms port: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms port - 001<br>G3-AVAYA-MIB\|g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]\|g3alarms maint name: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-<br>larms maint name - MED-GTWY |

The **Elements** page is displayed.  To create a new element, click the **New Element** tab.

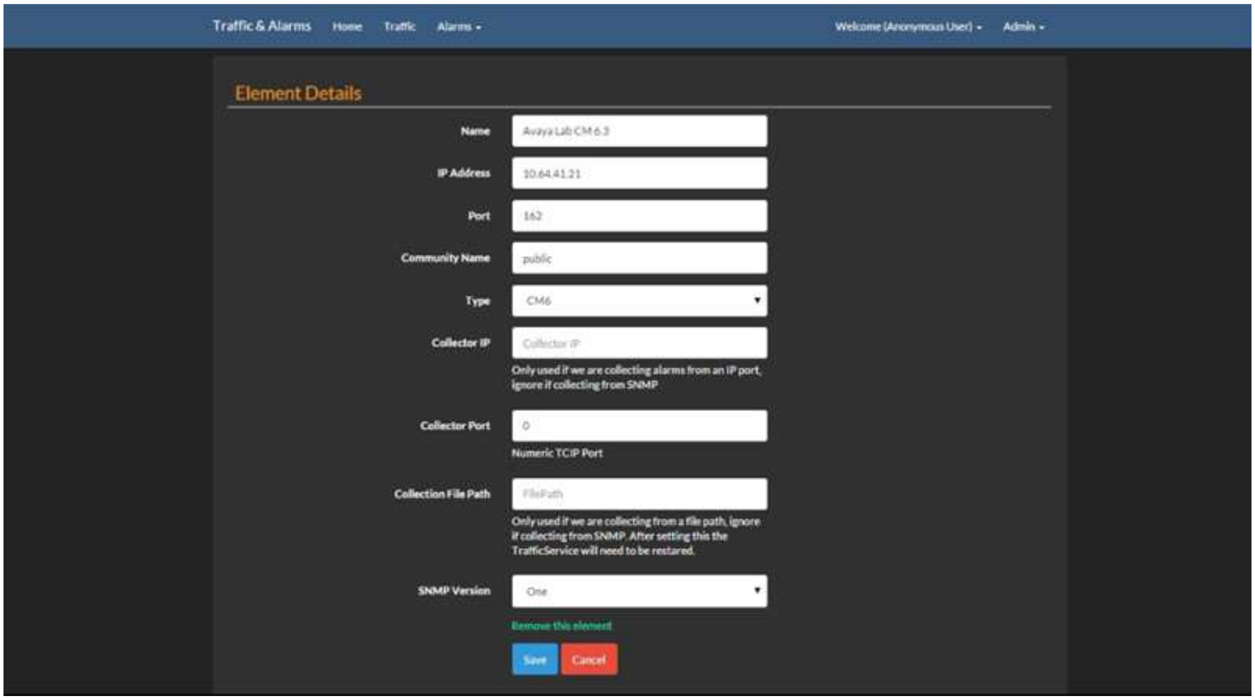


| Actions | Name | IPAddress | Version |
|---|---|---|---|
| Edit Monitors | Asterisk | 192.168.0.104 | V1 |
| Edit Monitors | Avaya CM Media Gateway | 10.64.41.2 | V1 |
| Edit Monitors | Avaya Lab CM 6.3 | 10.64.41.21 | V1 |
| Edit Monitors | Telebons | 192.168.0.102 | V1 |

On the **Element Details** screen, provide the following information:

- Provide a descriptive element name for the **Name** field.
- **IP Address** – IP address of Communication Manager.
- **Port** – the default trap port is used.
- **Community Name** – During the compliance test, public and private are used for read-only and read-write.
- **Type** – Select "CM6" using the drop-down menu.
- **SNMP Version** – Select the SNMP version using the drop-down menu.

Click **Save**.



Name: Avaya Lab CM 6.3

IP Address: 10.64.41.21

Port: 162

Community Name: public

Type: CM6

Collector IP: Collector IP
Only used if we are collecting alarms from an IP port, ignore if collecting from SNMP

Collector Port: 0
Numeric TCIP Port

Collection File Path: FilePath
Only used if we are collecting from a file path, ignore if collecting from SNMP. After setting this the TrafficService will need to be restared.

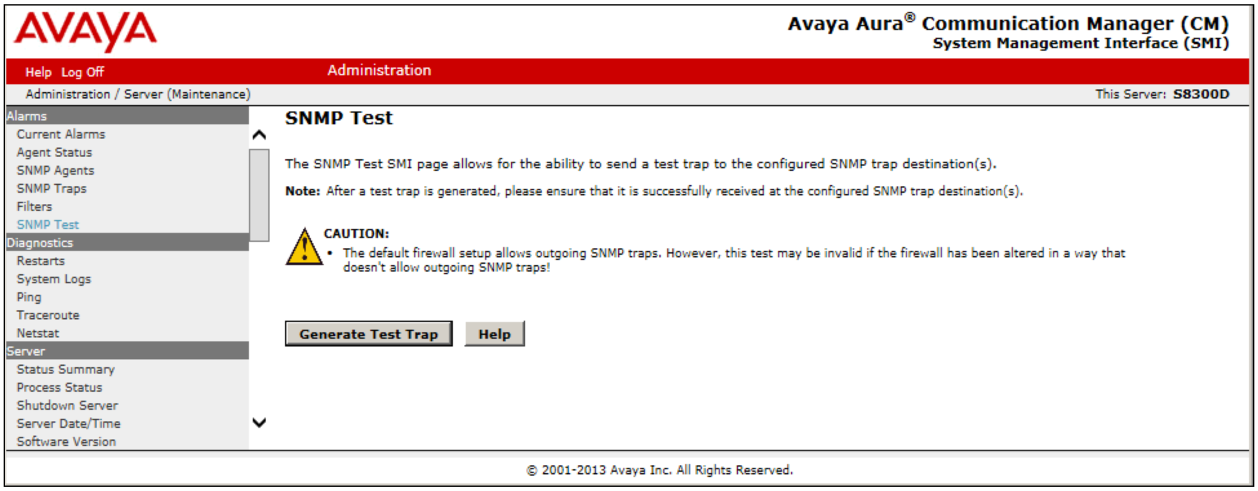
SNMP Version: One

Repeat above process for all SNMP devices, including Avaya Media Gateway.

# 8. Verification Steps

The following steps may be used to verify the configuration:

From the Communication Manager **Maintenance Web Interface** page, navigate to **Alarms → SNMP Test**, and click the **Generate Test Trap** tab**.**



SNMP Test

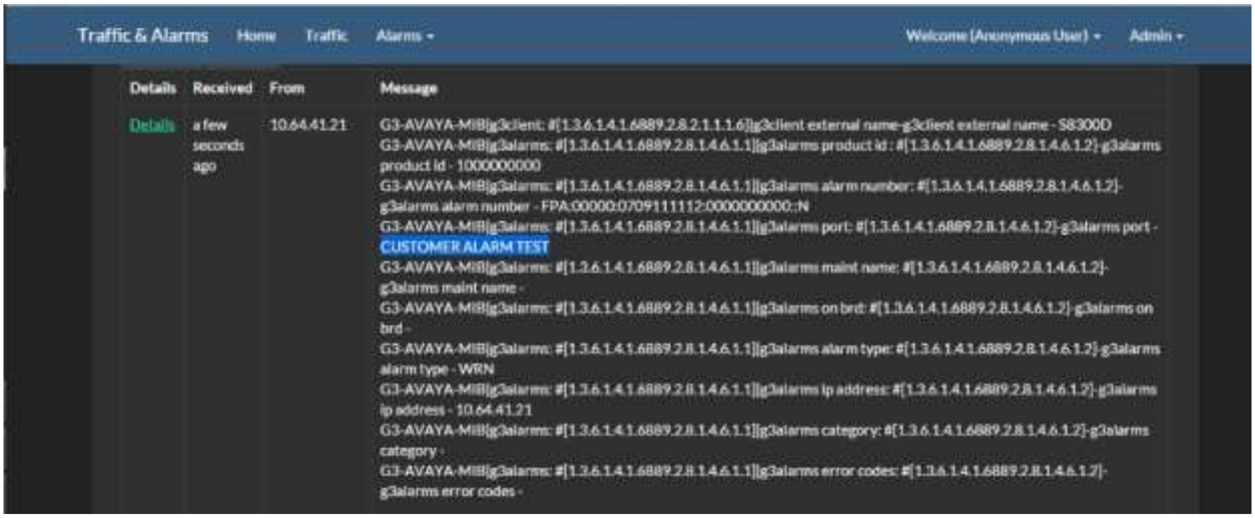
The SNMP Test SMI page allows for the ability to send a test trap to the configured SNMP trap destination(s).

**Note:** After a test trap is generated, please ensure that it is successfully received at the configured SNMP trap destination(s).

**CAUTION:**

- The default firewall setup allows outgoing SNMP traps. However, this test may be invalid if the firewall has been altered in a way that doesn't allow outgoing SNMP traps!

Verify the alarm from the CAIRS Fault Management application.



| Details | Received | From | Message |
|---|---|---|---|
| Details | a few seconds ago | 10.64.41.21 | G3-AVAYA-MIB[g3client: #[1.3.6.1.4.1.6889.2.8.2.1.1.1.6]]g3client external name-g3client external name - S8300D<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms product id : #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms product id - 1000000000<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms alarm number: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms alarm number - FPA:00000:0709111112:0000000000::N<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms port: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms port - CUSTOMER ALARM TEST<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms maint name: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms maint name -<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms on brd: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms on brd -<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms alarm type: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms alarm type - WRN<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms ip address: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms ip address - 10.64.41.21<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms category: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms category -<br>G3-AVAYA-MIB[g3alarms: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.1]]g3alarms error codes: #[1.3.6.1.4.1.6889.2.8.1.4.6.1.2]-g3alarms error codes - |

# 9. Conclusion

These Application Notes describe the configurations steps required for Unique Communications CAIRS Fault Management to successfully interoperate with Avaya Aura® Communication Manager.  Testing was successful.

# 10. References

This section references the Avaya and CAIRS Solution documentation that are relevant to these Application Notes.

[1] *Administering Avaya Aura® Communication Manager*, Document 03-300509, Issue 10 Release 6.3, August 2015, available at http://support.avaya.com.

[2] *Avaya Aura® Communication Manager Feature Description and Implementation*, Document 555-245-205, Release 6.3, October 2013, available at http://support.avaya.com.

The following CAIRS Fault Management information was provided by a Unique Communications engineer at the time of the compliance test.  To obtain the document, contact the CAIRS support, mentioned in **Section 2.3**.

[3]*Unique Traffic and Alarms – Admin Guide to Fault Configuration*

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.