Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Tone Software ReliaTel SNMP Management Application with Avaya Communication Manager and Avaya SIP Enablement Services - Issue 1.0

Abstract

These Application Notes detail the configuration steps to enable interoperability between Avaya Communication Manager, Avaya SIP Enablement Services and Tone Software ReliaTel SNMP management application. Information in these Application Notes has been obtained through Developer*Connection* compliance testing. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab in Lincroft, NJ.

1. Introduction

Supporting and maintaining network infrastructure equipment is an important issue many network administrators face. As IP telephony continues to grow and become more commonplace the requirement to manage the IP telephony infrastructure becomes a critical component within any network. Tone Software Reliatel is an SNMP management application capable of providing network administrators monitoring and alarming for both non-telephony and IP telephony network devices.

1.1. Network Diagram

The network diagram shown in **Figure 1** illustrates the testing environment used for compliance testing. The network consists of multiple Avaya Communication Manager systems, multiple Avaya Media Gateways, an Avaya SIP Enablement Services (SES) and Tone Software ReliaTel SNMP management software.

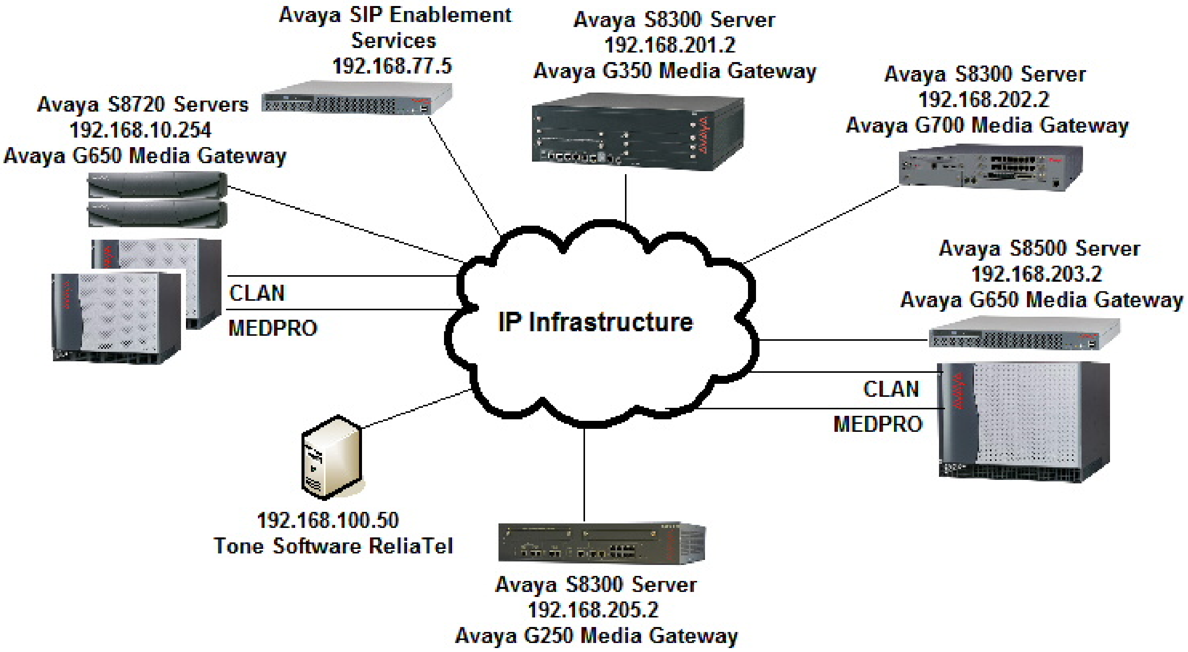


Figure 1: Sample Network Diagram

2. Equipment and Software Validated

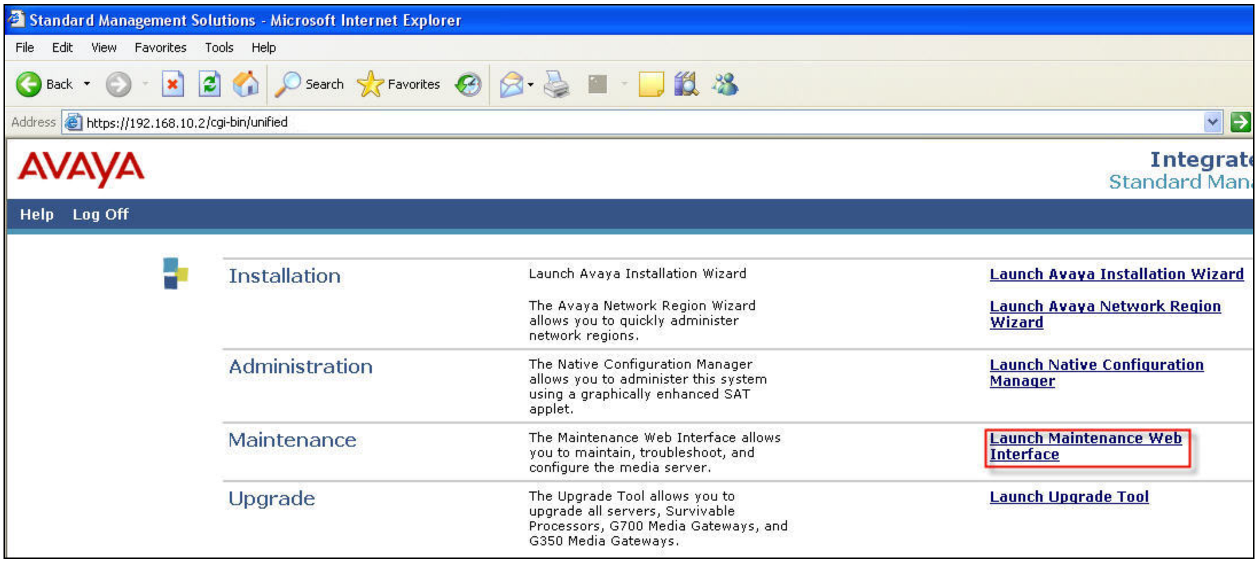
The following equipment and software were used for the sample configuration provided:

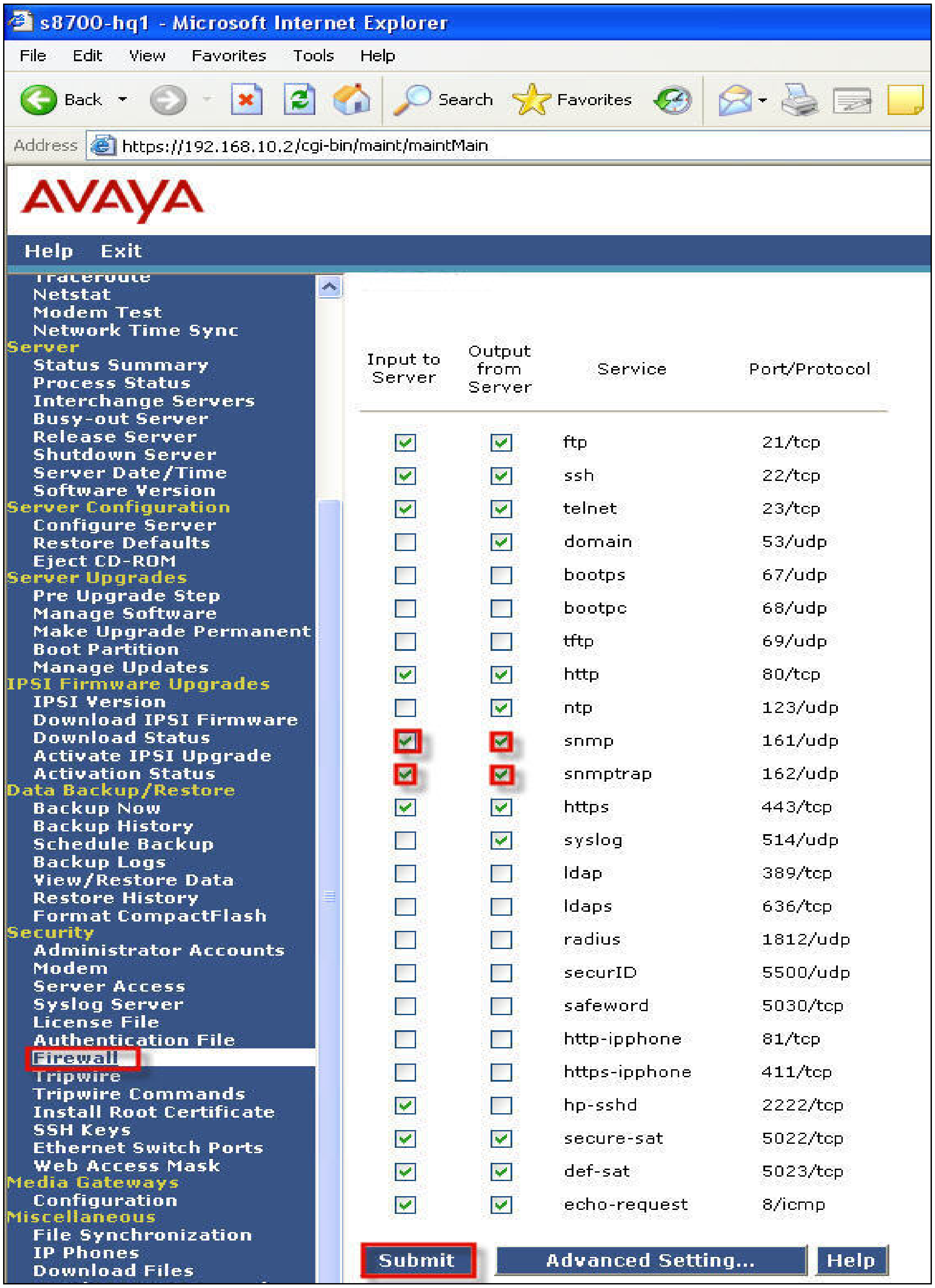
Equipment	Software
Avaya S8300 Server	Avaya Communication Manager 4.0 (R014x.00.0.730.5) Patches – 12514 and 13566
Avaya G250 Media Gateway	26.31.0
Avaya S8300 Server	Avaya Communication Manager 3.1 (R013x.01.0.628.6)
Avaya G350 Media Gateway	25.33.0
Avaya S8300 Server	Avaya Communication Manager 4.0 (R014x.00.0.730.5) Patches – 12514 and 13566
Avaya G700 Media Gateway	26.31.0
Avaya S8500 Server	Avaya Communication Manager 4.0 (R014x.00.0.730.5) Patches – 12514 and 13566
Avaya G650 Media Gateway	TN2312BP HW3 / FW 39
Avaya S8710 Server	Avaya Communication Manager 4.0 (R014x.00.0.730.5) Patches – 12514 and 13566
Avaya G650 Media Gateway	TN2312BP HW12 / FW 39
Avaya SIP Enablement Services	3.1.2 (SES-3.1.2.0-309.0)
Tone Software ReliaTel Red Hat Enterprise Linux AS release 4 (Nahant Update 5) Kernel 2.6.9-55.ELsmp on an i686	2.4.0

3. Avaya Communication Manager SNMP Configuration

Enabling an SNMP management system is a four-step process: enable SNMP to pass through the Avaya Communication Manager firewall, configure SNMP agents, configure SNMP traps, and restarting the SNMP agent. This process is the same for the Avaya Server 8300, 8500 and 8710.

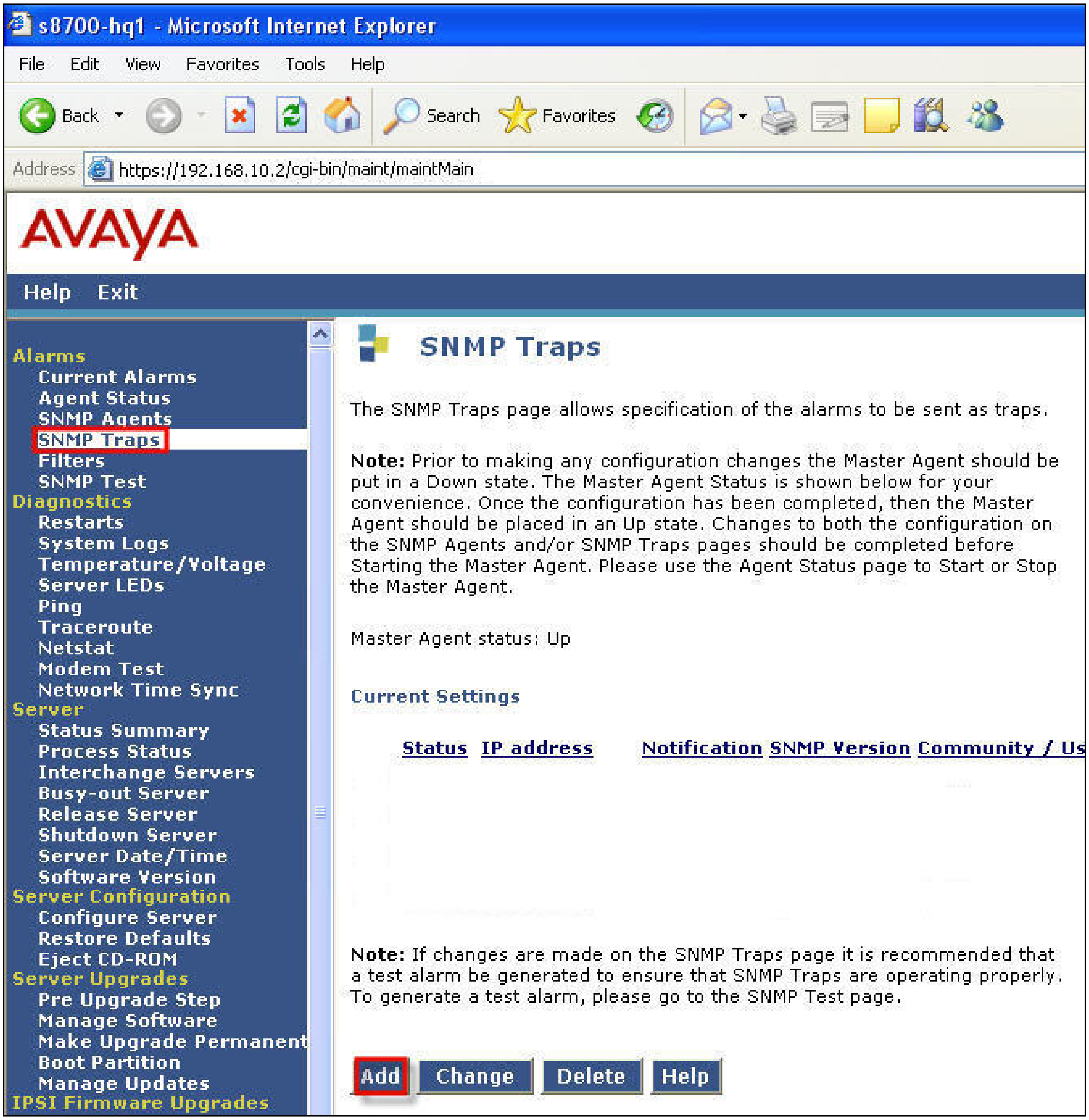
Use any web browser to connect and log into Avaya Communication Manager. For complete details on how to access Avaya Communication Manager from a web interface, refer to **Section 10** [**1**].

Step	Description
1.	After logging into Avaya Communication Manager, the user is presented with the following screen. Click **Launch Maintenance Web Interface**.  Standard Management Solutions - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://192.168.10.2/cgi-bin/unified AVAYA Integrat Standard Man Help Log Off Installation — Launch Avaya Installation Wizard — Launch Avaya Installation Wizard The Avaya Network Region Wizard allows you to quickly administer network regions. — Launch Avaya Network Region Wizard Administration — The Native Configuration Manager allows you to administer this system using a graphically enhanced SAT applet. — Launch Native Configuration Manager Maintenance — The Maintenance Web Interface allows you to maintain, troubleshoot, and configure the media server. — Launch Maintenance Web Interface Upgrade — The Upgrade Tool allows you to upgrade all servers, Survivable Processors, G700 Media Gateways, and G350 Media Gateways. — Launch Upgrade Tool

Step	Description
2.	Navigate to the **Firewall** web page by clicking **Firewall** found on the left side of the web page within the blue background. Check the **snmp** and **snmptrap** check boxes for both **Input to Server** and **Output from Server**. Click **Submit**. 

Address https://192.168.10.2/cgi-bin/maint/maintMain

Input to Server	Output from Server	Service	Port/Protocol
☑	☑	ftp	21/tcp
☑	☑	ssh	22/tcp
☑	☑	telnet	23/tcp
□	☑	domain	53/udp
□	□	bootps	67/udp
□	□	bootpc	68/udp
□	□	tftp	69/udp
☑	☑	http	80/tcp
□	☑	ntp	123/udp
☑	☑	snmp	161/udp
☑	☑	snmptrap	162/udp
☑	☑	https	443/tcp
□	☑	syslog	514/udp
□	□	ldap	389/tcp
□	□	ldaps	636/tcp
□	□	radius	1812/udp
□	□	securID	5500/udp
□	□	safeword	5030/tcp
□	□	http-ipphone	81/tcp
□	□	https-ipphone	411/tcp
☑	□	hp-sshd	2222/tcp
☑	☑	secure-sat	5022/tcp
☑	☑	def-sat	5023/tcp
☑	☑	echo-request	8/icmp

Step	Description
3.	Navigate to the **SNMP Traps** web page by clicking **SNMP Traps** found on the left side of the web page within the blue background. Click **Add**. 

SNMP Traps

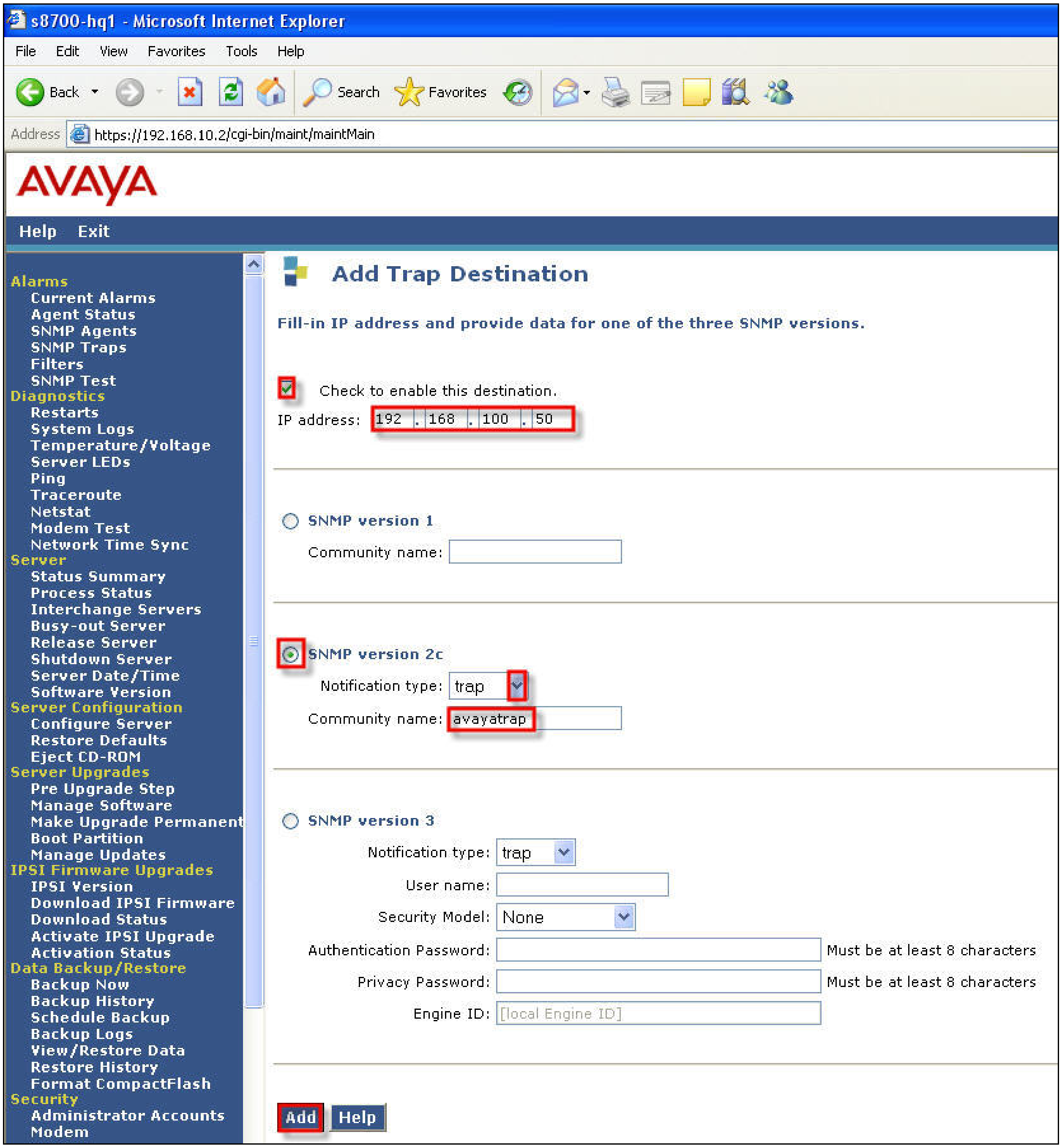
The SNMP Traps page allows specification of the alarms to be sent as traps.

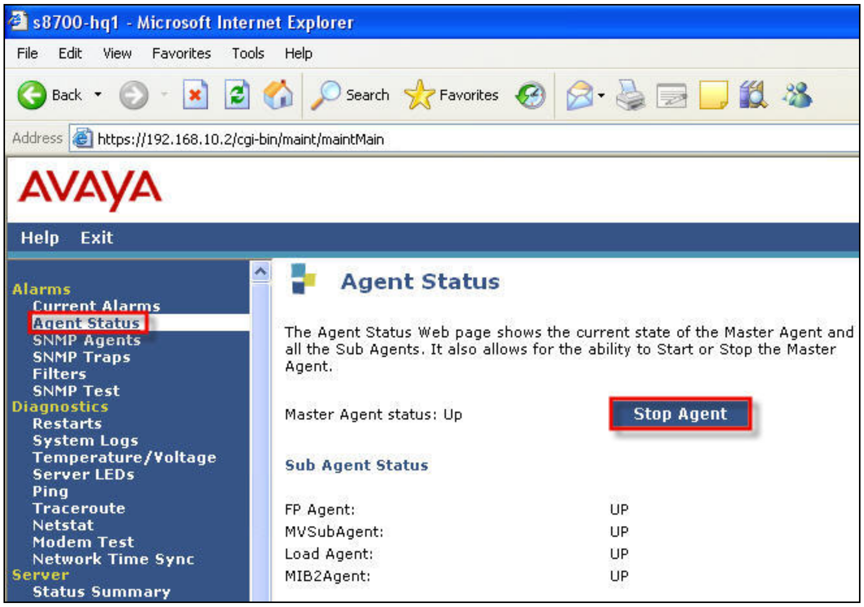
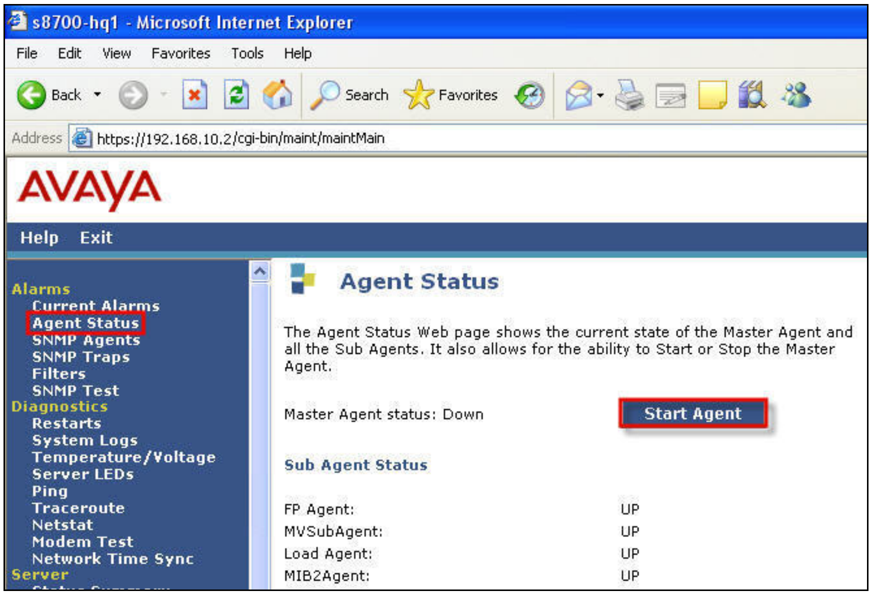
Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP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

Master Agent status: Up

Current Settings

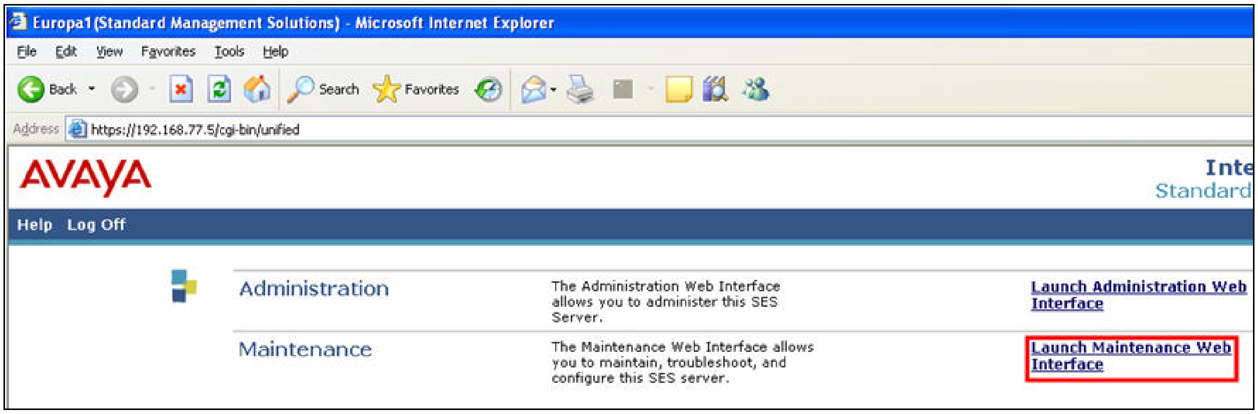
Note: If changes are made on the SNMP Traps page it is recommended that a test alarm be generated to ensure that SNMP Traps are operating properly. To generate a test alarm, please go to the SNMP Test page.

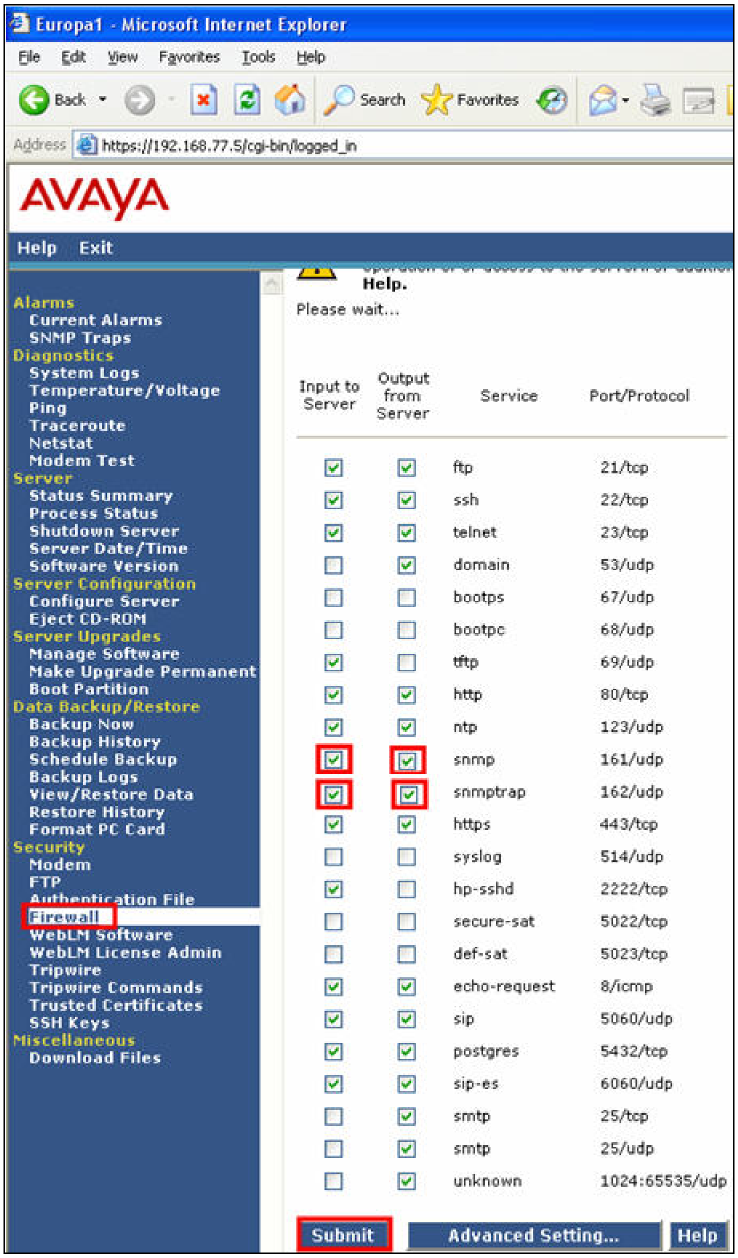
Step	Description
4.	From the **Add Trap Destination** web page, enter the information displayed below. Check the **Check to enable this destination** check box. Configure the IP address assigned to the Tone Software ReliaTel SNMP management application (see **Figure 1**) into the **IP address** field. Select the **SNMP version 2c** radio-button. Use the drop-down list for **Notification type** and select "trap". The **Community name** can be any descriptive text. In the sample configuration "avayatrap" was used for the **Community name**. Click **Add**. After making any changes to the SNMP configuration, the SNMP Agent needs to be restarted.  s8700-hq1 - Microsoft Internet Explorer Address https://192.168.10.2/cgi-bin/maint/maintMain 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 . 100 . 50 ○ 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 Engine ID: [local Engine ID] Add Help File Edit View Favorites Tools Help Back Search Favorites AVAYA Help Exit Alarms Current Alarms Agent Status SNMP Agents SNMP Traps Filters SNMP Test Diagnostics Restarts System Logs Temperature/Voltage Server LEDs Ping Traceroute Netstat Modem Test Network Time Sync Server Status Summary Process Status Interchange Servers Busy-out Server Release Server Shutdown Server Server Date/Time Software Version Server Configuration Configure Server Restore Defaults Eject CD-ROM Server Upgrades Pre Upgrade Step Manage Software Make Upgrade Permanent Boot Partition Manage Updates IPSI Firmware Upgrades IPSI Version Download IPSI Firmware Download Status Activate IPSI Upgrade Activation Status Data Backup/Restore Backup Now Backup History Schedule Backup Backup Logs View/Restore Data Restore History Format CompactFlash Security Administrator Accounts Modem

Step	Description
5.	Navigate to the **Agent Status** web page by clicking **Agent Status** found on the left side of the web page within the blue background. Click **Stop Agent**. Return to the **Agent Status** web page and then click **Start Agent**. Repeat all these steps on each Avaya Communication Manager.  s8700-hq1 - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://192.168.10.2/cgi-bin/maint/maintMain AVAYA Help Exit Alarms Current Alarms Agent Status SNMP Agents SNMP Traps Filters SNMP Test Diagnostics Restarts System Logs Temperature/Voltage Server LEDs Ping Traceroute Netstat Modem Test Network Time Sync Server Status Summary Stop Agent Agent Status The Agent Status Web page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent. Master Agent status: Up Sub Agent Status FP Agent: UP MVSubAgent: UP Load Agent: UP MIB2Agent: UP  s8700-hq1 - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://192.168.10.2/cgi-bin/maint/maintMain AVAYA Help Exit Alarms Current Alarms Agent Status SNMP Agents SNMP Traps Filters SNMP Test Diagnostics Restarts System Logs Temperature/Voltage Server LEDs Ping Traceroute Netstat Modem Test Network Time Sync Server Start Agent Agent Status The Agent Status Web page shows the current state of the Master Agent and all the Sub Agents. It also allows for the ability to Start or Stop the Master Agent. Master Agent status: Down Sub Agent Status FP Agent: UP MVSubAgent: UP Load Agent: UP MIB2Agent: UP

4. Avaya SIP Enablement Services Configuration

Administering the SNMP configuration for Avaya SIP Enablement Services is similar to the process for Avaya Communication Manager. One difference between the two configurations is that the SNMP Agent does not need to be restarted on Avaya SIP Enablement Services. For complete reference on the SNMP configuration for Avaya SIP Enablement Services refer to **Section 10** [**2**].

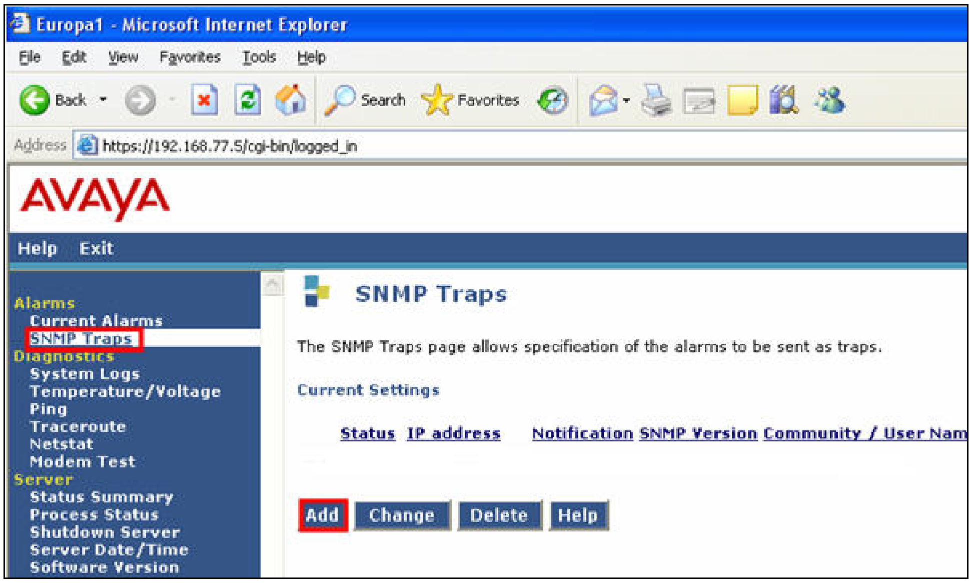
Step	Description
1.	After logging on to the web interface for Avaya SIP Enablement Services, the user is presented with the following screen. Click **Launch Maintenance Web Interface**.  Europa1 (Standard Management Solutions) - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://192.168.77.5/cgi-bin/unified AVAYA Inte Standard Help Log Off Administration – The Administration Web Interface allows you to administer this SES Server. – Launch Administration Web Interface Maintenance – The Maintenance Web Interface allows you to maintain, troubleshoot, and configure this SES server. – Launch Maintenance Web Interface

Step	Description
2.	Navigate to the **Firewall** web page by clicking **Firewall** found on the left side of the web page within the blue background. Check the **snmp** and **snmptrap** check boxes for both **Input to Server** and **Output from Server**. Click **Submit**. 

Help.

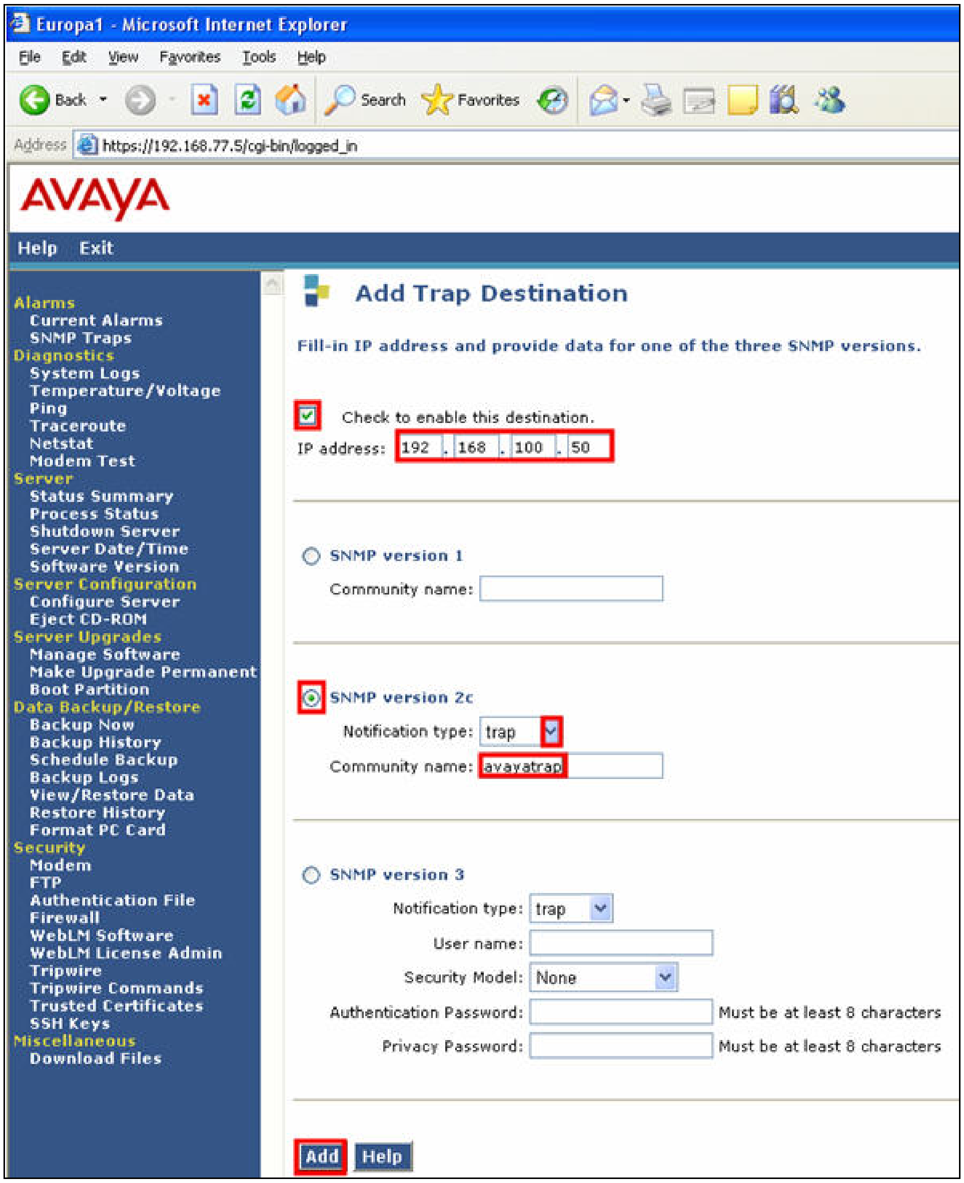
Please wait...

Input to Server	Output from Server	Service	Port/Protocol
☑	☑	ftp	21/tcp
☑	☑	ssh	22/tcp
☑	☑	telnet	23/tcp
□	☑	domain	53/udp
□	□	bootps	67/udp
□	□	bootpc	68/udp
☑	□	tftp	69/udp
☑	☑	http	80/tcp
☑	☑	ntp	123/udp
☑	☑	snmp	161/udp
☑	☑	snmptrap	162/udp
☑	☑	https	443/tcp
□	□	syslog	514/udp
☑	□	hp-sshd	2222/tcp
□	□	secure-sat	5022/tcp
□	□	def-sat	5023/tcp
☑	☑	echo-request	8/icmp
☑	☑	sip	5060/udp
☑	☑	postgres	5432/tcp
☑	☑	sip-es	6060/udp
□	☑	smtp	25/tcp
□	☑	smtp	25/udp
□	☑	unknown	1024:65535/udp

Step	Description
3.	Navigate to the **SNMP Traps** web page by clicking **SNMP Traps** found on the left side of the web page within the blue background. Click **Add**.  Europa1 - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address https://192.168.77.5/cgi-bin/logged_in AVAYA Help Exit Alarms Current Alarms SNMP Traps Diagnostics System Logs Temperature/Voltage Ping Traceroute Netstat Modem Test 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. Current Settings Status IP address Notification SNMP Version Community / User Nam Add Change Delete Help

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

From the **Add Trap Destination** web page, enter the information displayed below. Check the **Check to enable this destination** check box. Configure the IP address assigned to the Tone Software ReliaTel SNMP management application (see **Figure 1**) into the **IP address** field. Select the **SNMP version 2c** radio-button. Use the drop-down list for **Notification type** and select “trap”. The **Community name** can be any descriptive text. In the sample configuration “avayatrap” was used for the **Community name**. Click **Add**.



Address: https://192.168.77.5/cgi-bin/logged_in

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 . 100 . 50

○ 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

</td></tr>
</table>

5. Tone Software ReliaTel Configuration

Tone Software ReliaTel is a software application that runs on a Linux platform. Tone Software ReliaTel is a bundled software application sold with server hardware. The configurations can be performed directly on the server or via a telnet or ssh connection. Before systems are delivered to customer locations, Tone Software engineers pre-configure the system with information obtained from customers. The information provided by customers includes the IP address(es), class, channel type and channel system names. In the sample configuration the information displayed below was provided to Tone Software in order to provision the system.

• **IP address**	= “192.168.100.50”
• **Channel Type**	= “SNMPMGR”
• **Channel System**	= “Avaya”
• **Center**	= “AvayaDevConnect”
• **Class**	= “cl-avayamdsrv”

Step	Description
1.	Using a keyboard and monitor directly connected to the Tone Software ReliaTel server login using default credentials, see **Section 10** [**3**]. Once logged on, users will be presented with the Command Line Interface (CLI) of the Linux Operating System. Navigate to the “etc/conf/” directory by using the “cd” commands displayed below. Use the “vi” text editor and open up the **cdata.conf** text file.

```
=~=~=~=~=~=~=~=~=~= PuTTY log 2007.06.21 13:37:35 ~=~=~=~=~=~=~=~=
Red Hat Enterprise Linux AS release 4 (Nahant Update 5)
Kernel 2.6.9-55.ELsmp on an i686
login: xxxxx
Password: xxxxx
-sh-3.00$ cd etc
-sh-3.00$ cd conf
-sh-3.00$ vi cdata.conf
```

Step **Description**

2. Using “vi”, a text editing program included as part of Red Hat Linux, enter the information displayed below. The cdata.conf file houses the channel configuration information for Tone Software ReliaTel. Channels are added into the system by creating a **Channel** entry. A channel in the text file must follow the following format. A **Channel** name begins with the open bracket and ends with the closed bracket. The entity name must start with “c-“ and uses the following format: c-**NAME** where **NAME** can be any text value. In the sample configuration the IP address of the device being added to the database was used as the **NAME**. The **chanType** and **chanSystem** fields are Tone Software ReliaTel provided information. These parameters distinguish what software process receives information and how that information is processed by Tone Software ReliaTel. The **chanEmulator** must be set to “4410” when an Avaya Communication Manager is being managed. The **account** field is the IP address of the system being managed. The **acc_device** field is a combination of the IP address of the system, a colon and the communication port of the access method used when accessing the device from Tone Software ReliaTel. For example, a device with an IP address of “192.168.10.2” and an access method using direct System Administration Terminal (SAT) telnet access (which uses port 5023) would be “192.168.10.2:5023”. Other supported access methods include telnet and ssh. Telnet uses the standard port 23. In order to use ssh Tone Software will need to provide the user with the correct path and string needed to invoke ssh. All three access methods were tested (telnet, ssh and SAT telnet). Additional entries are created using the exact same format. Repeat this process for every Avaya Communication Manager being managed. For Avaya 87XX Servers remember to add all three IP addresses associated to the redundant systems. This includes both physical addresses assigned to each individual 87XX Server and the virtual IP address assigned to both systems.

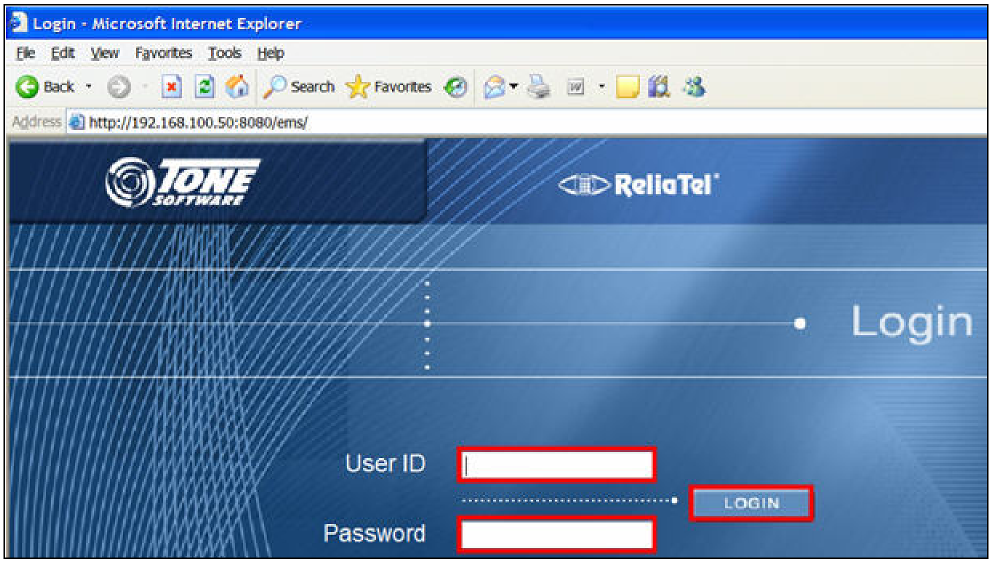
```
# Avaya Development Connect Lab channels configuration
[c-192.168.10.254]
chanType     = SNMPMGR
chanSystem   = Avaya
chanEmulator = 4410
account      = 192.168.10.254
acc_device   = 192.168.10.254:5023
```

3. Once the changes to the **cdata.conf** text file have been made, the user must re-initialize the application using the procedure listed below. Repeat this process for each new device added to the system.

```
=~=~=~=~=~=~=~=~=~=~= PuTTY log 2007.06.21 13:37:35 ~=~=~=~=~=~=~=~=~=
Red Hat Enterprise Linux AS release 4 (Nahant Update 5)
Kernel 2.6.9-55.ELsmp on an i686
-sh-3.00$ pkill –HUP dapmgr
-sh-3.00$ rc-cent rctype=n center=AvayaDevConnect
-sh-3.00$ rc-ent rctype=new entity=192.168.10.254 center=AvayaDevConnect
class=cl-avayamdsrv
-sh-3.00$ restore-log 192.168.10.254
```

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

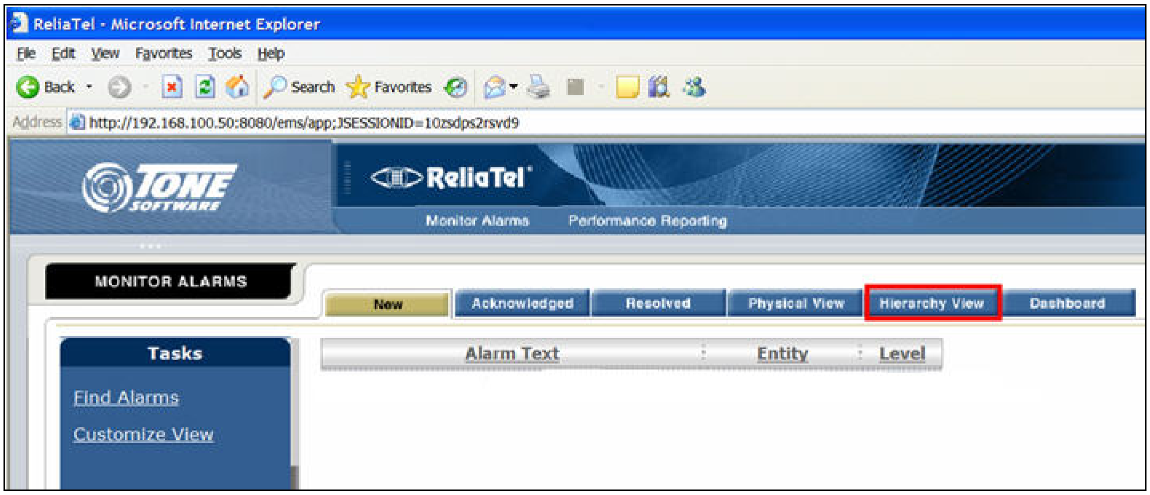
Using a web browser, open a connection to the Tone Software ReliaTel. For example, in the sample configuration the IP address of “192.168.100.50” was assigned to Tone Software ReliaTel server and the following URL was used to access the system http://192.168.100.50:8080/ems. The user will need to provide a login and password in order to access Tone Software ReliaTel. Refer to **Section 10** [**3**] for information such as default credentials used for Tone Software ReliaTel.



http://192.168.100.50:8080/ems/

</td></tr>
<tr><td>5.</td><td>

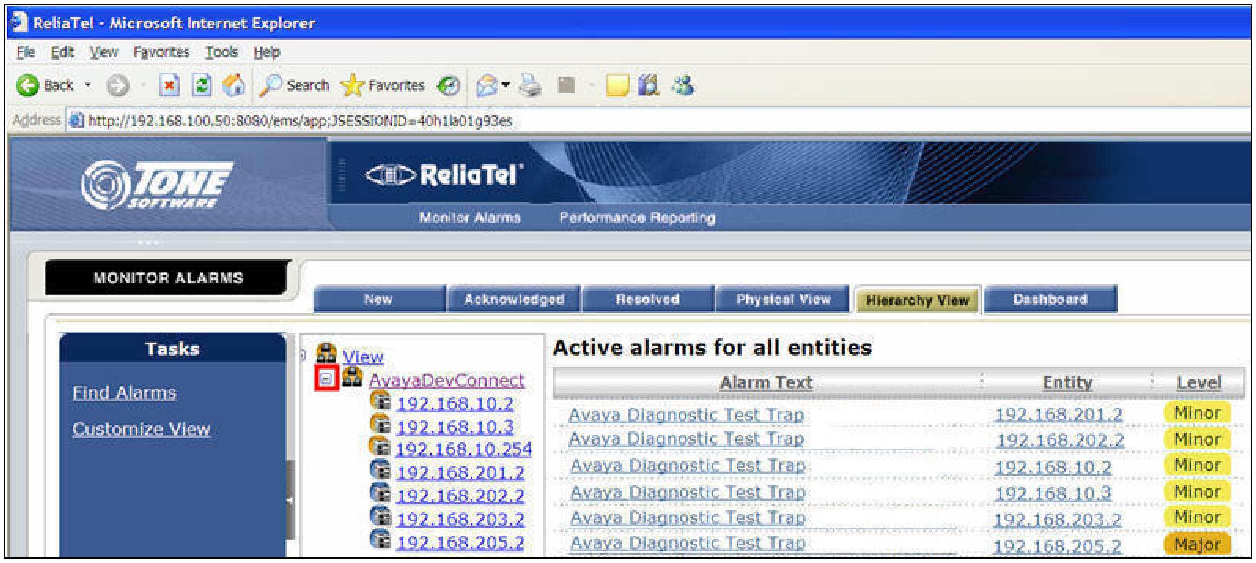
The user is presented with the **MONITOR ALARMS** web page. Click **Hierarchy View**.



http://192.168.100.50:8080/ems/app;JSESSIONID=10zsdps2rsvd9

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>6.</td><td>The user is presented with the <b>Hierarchy View</b> web page. This page displays the active alarms that have been received. Tone Software ReliaTel provides default pattern matching on traps sent from Avaya Communication Manager, however, the default parameters for any trap can be modified. To demonstrate this feature the test trap generated from every system in the test was relabeled “Avaya Diagnostic Test Trap” and the specific trap from host “192.168.205.2” was modified such that the <b>Level</b> would be interpreted as <b>Major</b> over <b>Minor</b>.

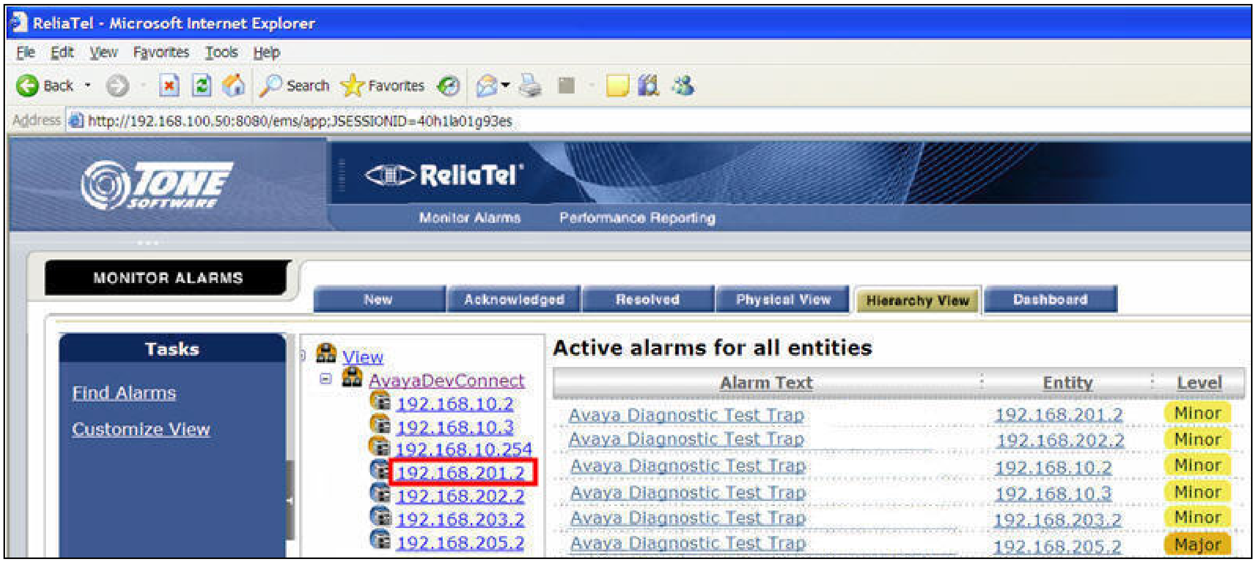


http://192.168.100.50:8080/ems/app;JSESSIONID=40h1la01g93es

View
AvayaDevConnect
192.168.10.2
192.168.10.3
192.168.10.254
192.168.201.2
192.168.202.2
192.168.203.2
192.168.205.2

Active alarms for all entities

<table>
<tr><th>Alarm Text</th><th>Entity</th><th>Level</th></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.201.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.202.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.10.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.10.3</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.203.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.205.2</td><td>Major</td></tr>
</table>
</td></tr>
<tr><td>7.</td><td>From the <b>Hierarchy View</b> page, the user can click on any of the specific device entities to obtain more detailed SNMP information or to access the device (based on the access type defined from <b>Step 1</b>).

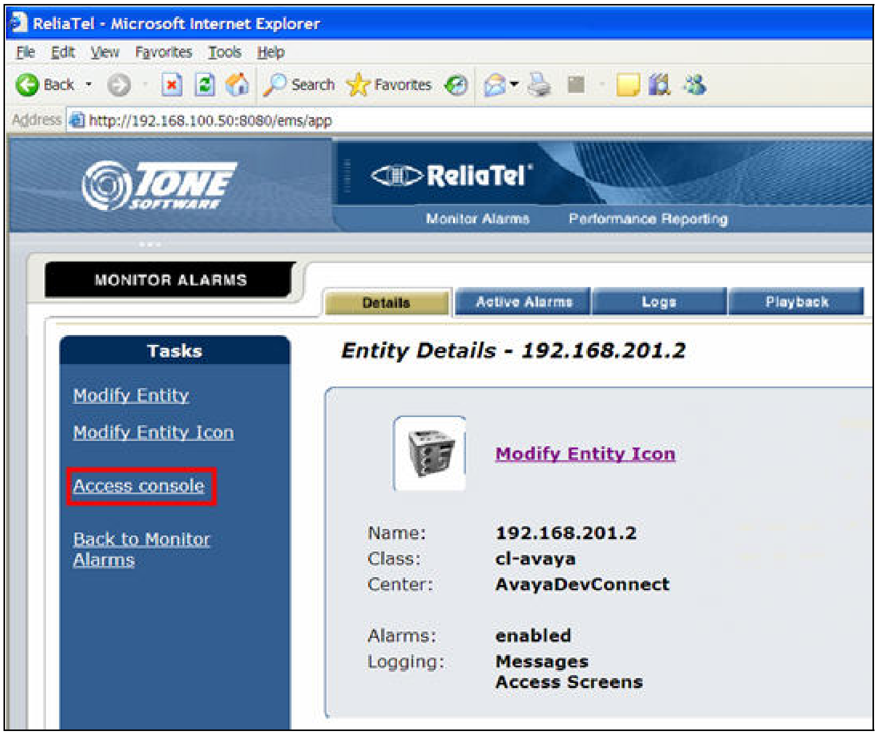


http://192.168.100.50:8080/ems/app;JSESSIONID=40h1la01g93es

View
AvayaDevConnect
192.168.10.2
192.168.10.3
192.168.10.254
192.168.201.2
192.168.202.2
192.168.203.2
192.168.205.2

Active alarms for all entities

<table>
<tr><th>Alarm Text</th><th>Entity</th><th>Level</th></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.201.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.202.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.10.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.10.3</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.203.2</td><td>Minor</td></tr>
<tr><td>Avaya Diagnostic Test Trap</td><td>192.168.205.2</td><td>Major</td></tr>
</table>
</td></tr>
</table>

Step	Description
8.	From the **Entity Details** web page, the user can click the **Access console** text to open up an additional window (not shown) with access to the system based on the access type configured in **Step 1**.  ReliaTel - Microsoft Internet Explorer File Edit View Favorites Tools Help Back Search Favorites Address http://192.168.100.50:8080/ems/app TONE SOFTWARE ReliaTel Monitor Alarms Performance Reporting MONITOR ALARMS Details Active Alarms Logs Playback Tasks Modify Entity Modify Entity Icon Access console Back to Monitor Alarms Modify Entity Icon Entity Details - 192.168.201.2 Name: 192.168.201.2 Class: cl-avaya Center: AvayaDevConnect Alarms: enabled Logging: Messages Access Screens

6. Interoperability Compliance Testing

The interoperability testing focused on verifying Tone Software ReliaTel capability to receive and interpret SNMP version 2c traps from Avaya Communication Manager and Avaya SIP Enablement Services.

6.1. General Test Approach

The general test approach was to configure the Tone Software ReliaTel database to monitor the systems depicted in **Figure 1**. SNMP version 2c was used and test traps were generated from each system and verified to be properly interpreted by Tone Software ReliaTel. Tone Software ReliaTel was verified to be capable of performing in-band access to the devices monitored using telnet or ssh.

6.2. Test Results

Tone Software ReliaTel passed all test cases. Tone Software ReliaTel was verified to be capable of receiving and interpreting SNMP version 2c traps from Avaya Communication Manager and Avaya SIP Enablement Services. Tone Software ReliaTel was verified to be capable of in-band access using telnet or ssh to Avaya Communication Manager and Avaya SIP Enablement Services.

7. Verification Steps

This section describes some of the verification steps that can be taken to validate the configuration used for testing.

- Verify the Tone Software ReliaTel management station has IP connectivity to the devices being monitored. This can be done on the console of Tone Software ReliaTel by issuing the "ping" command from a terminal window.
- Verify the entity details configured for the device being monitored. See **Section 5 Step 2**.

8. Support

Technical support for Tone Software ReliaTel can be obtained through the following:

- **Phone:** 1-800-833-8663
- **Email:** info@tonesoft.com

9. Conclusion

These Application Notes demonstrate how to configure Tone Software ReliaTel to interoperate with Avaya Communication Manager and Avaya SIP Enablement Services using SNMP version 2c. These Application Notes also demonstrate how to configure Tone Software ReliaTel to support multiple Avaya Communication Manager and/or Avaya SIP Enablement Services systems.

10. Additional References

The documents referenced below were used for additional support and configuration information. The Avaya documentation was obtained from http://support.avaya.com. The Tone Software documentation was obtained from http://www.tonesoft.com (access to Tone Software documentation may require a support account).

[1] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3.1, Document Number 03-300509

[2] *Installing & Administering SIP Enablement Services*, March 2007, Issue 2.1, Document Number 03-600768

[3] *Administrator's Guide for Tone Software ReliaTel*, June 2007, Issue 1.0

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 Developer*Connection* Program at devconnect@avaya.com.