Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Manager and Intuity Audix (IA 770) for Remote INADS Alarming using ASG Defender – Issue 1.0

Abstract

These Application Notes describe the steps required for configuring Avaya Communication Manager and Intuity Audix (IA 770) to support Simple Network Management Protocol (SNMP) traps to the ASG Defender. The ASG Defender forwards the alarm indications to Avaya Global Services in the required Initialization and Administration System (INADS) format.

Information in these Application Notes has been obtained through compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps required for configuring Avaya Communication Manager and Intuity Audix (IA 770) to support Simple Network Management Protocol (SNMP) traps to the ASG Defender. The ASG Defender forwards the alarm indications to Avaya Global Services in the required Initialization and Administration System (INADS) format. The ASG Defender dials out to the PSTN and establishes a point-to-point (PPP) session in order to forward SNMP-INADS notification, to Avaya Global Services.

These Application Notes do not cover the configuration of any of the software applications installed at Avaya Global Services or configuring or the logins and passwords on the ASG Defender.

The ASG Defender is an Avaya Branded product from ION Networks. (The ION Networks ASG Guard II was the previous product in this space.)

The ASG Defender sends the INADS alarms in the proper format (as shown below) for the Avaya Remote Alarm Fault Manager (AFM).

INADS Format for SNMP Alarms
< Product_ID><day>/<hour>:<minute> <Emergency_transfer_status>.<status> | <alarm_1>;<alarm_2>;…;<alarm_n>

When AFM receives the alarm, the *Product_ID* contained in the alarm is checked against a local database and an acknowledgement is sent back to the ASG Defender. The AFM then determines which of the following actions will be taken.

1. The alarm is forwarded to the Maestro ticketing system. A case is either created or updated.
2. The alarm is processed by the Agent Event Tracker (AET) application.

In the network configuration in **Figure 1**, the ASG Defender is connected to Avaya Communication Manager via the LAN. When the ASG Defender receives an alarm, it places a call via a modem to Avaya Global Services and establishes a PPP session. Once the PPP session is established, alarms travel from the ASG Defender and acknowledgements come to it.

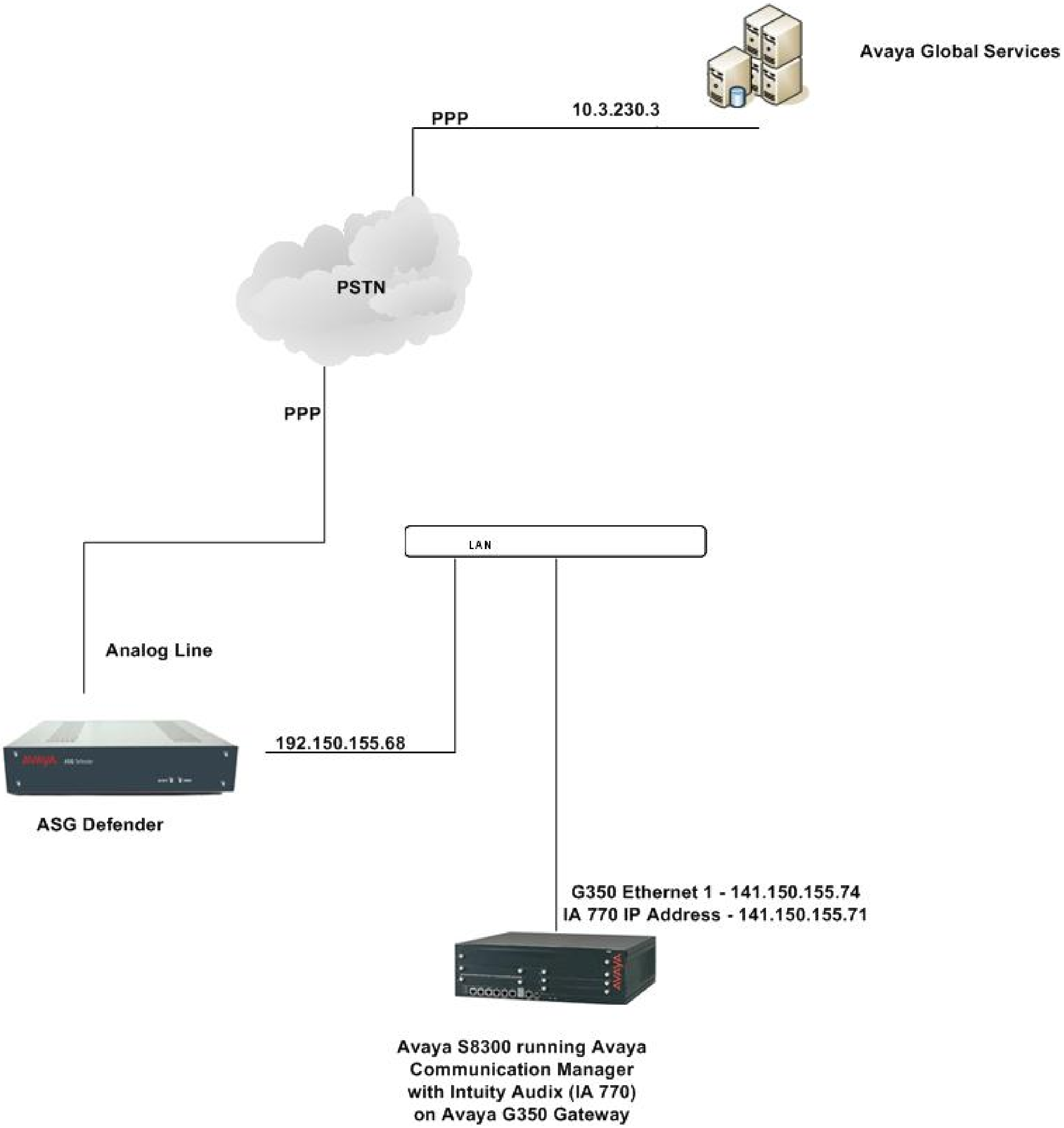

Avaya Global Services
PPP
10.3.230.3
PSTN
PPP
LAN
Analog Line
192.150.155.68
ASG Defender
G350 Ethernet 1 - 141.150.155.74
IA 770 IP Address - 141.150.155.71
Avaya S8300 running Avaya Communication Manager with Intuity Audix (IA 770) on Avaya G350 Gateway

Figure 1: Tested Configuration

2. Equipment and Software Validated

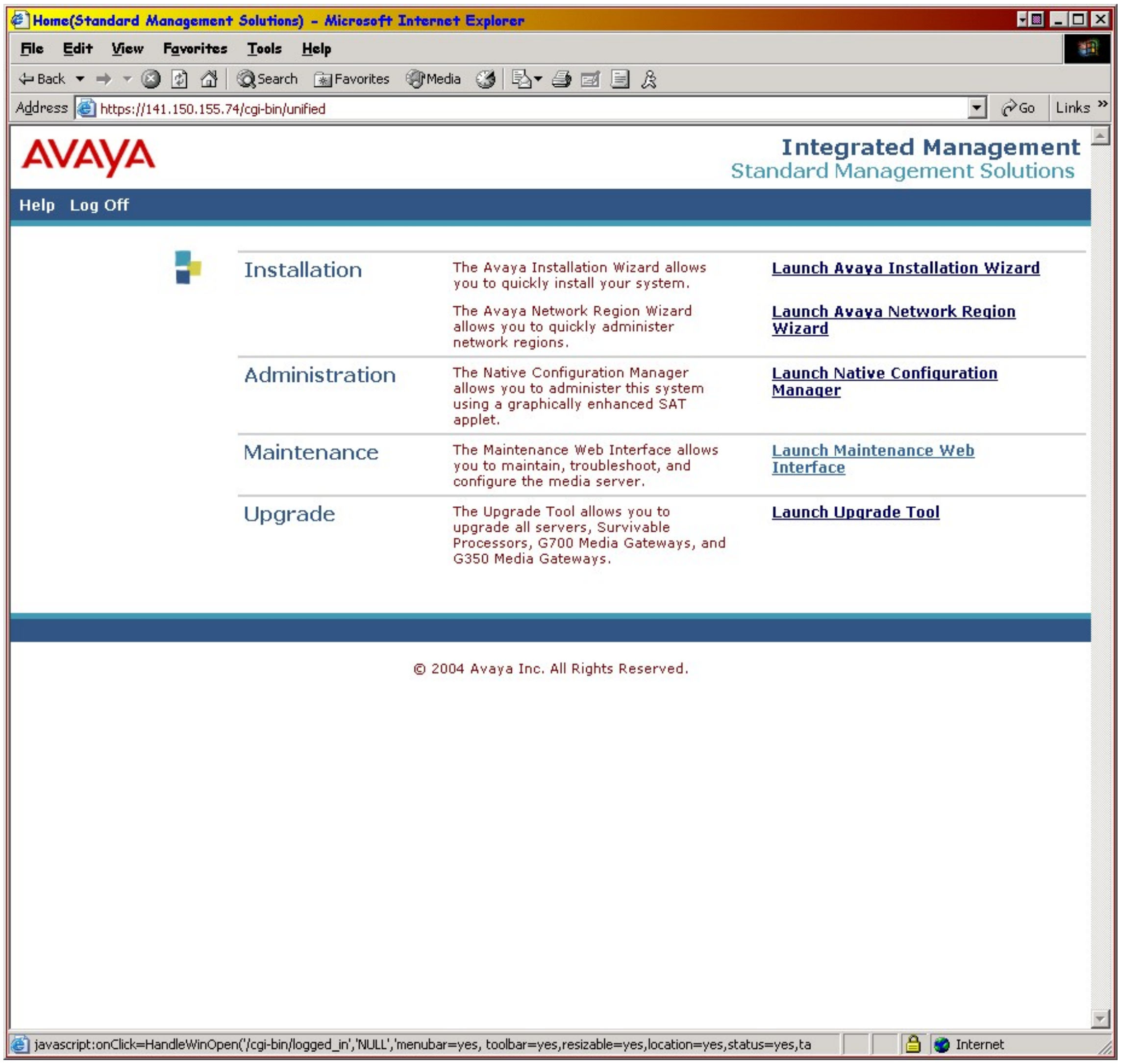
The following equipment and software were used for the sample configuration provided:

Equipment	Software
Avaya S8300 Media Server	Avaya Communication Manager R3.1.1 (R013x.01.0.626.0)
Avaya G350 Media Gateway	25.28
Avaya Intuity Audix (IA 770)	3.1.2
ASG Defender	RoHS Version 1.0.4

3. Configure Avaya Communication Manager

The following steps details the configuration for Avaya Communication Manager. The Avaya Intuity Audix (IA 770) sends SNMP alarms to the same IP address as Avaya Communication Manager, so there are no additional steps needed.

Enabling SNMP traps for the Avaya S8300 Media Server can be configured through the server's web interface. To access the web interface, launch a web browser and connect to the media server by entering the URL https://<media server IP address>. Supply the login and password for an account with super-user privileges. After logging in, a window is displayed with four options. Select the **Maintenance** option.

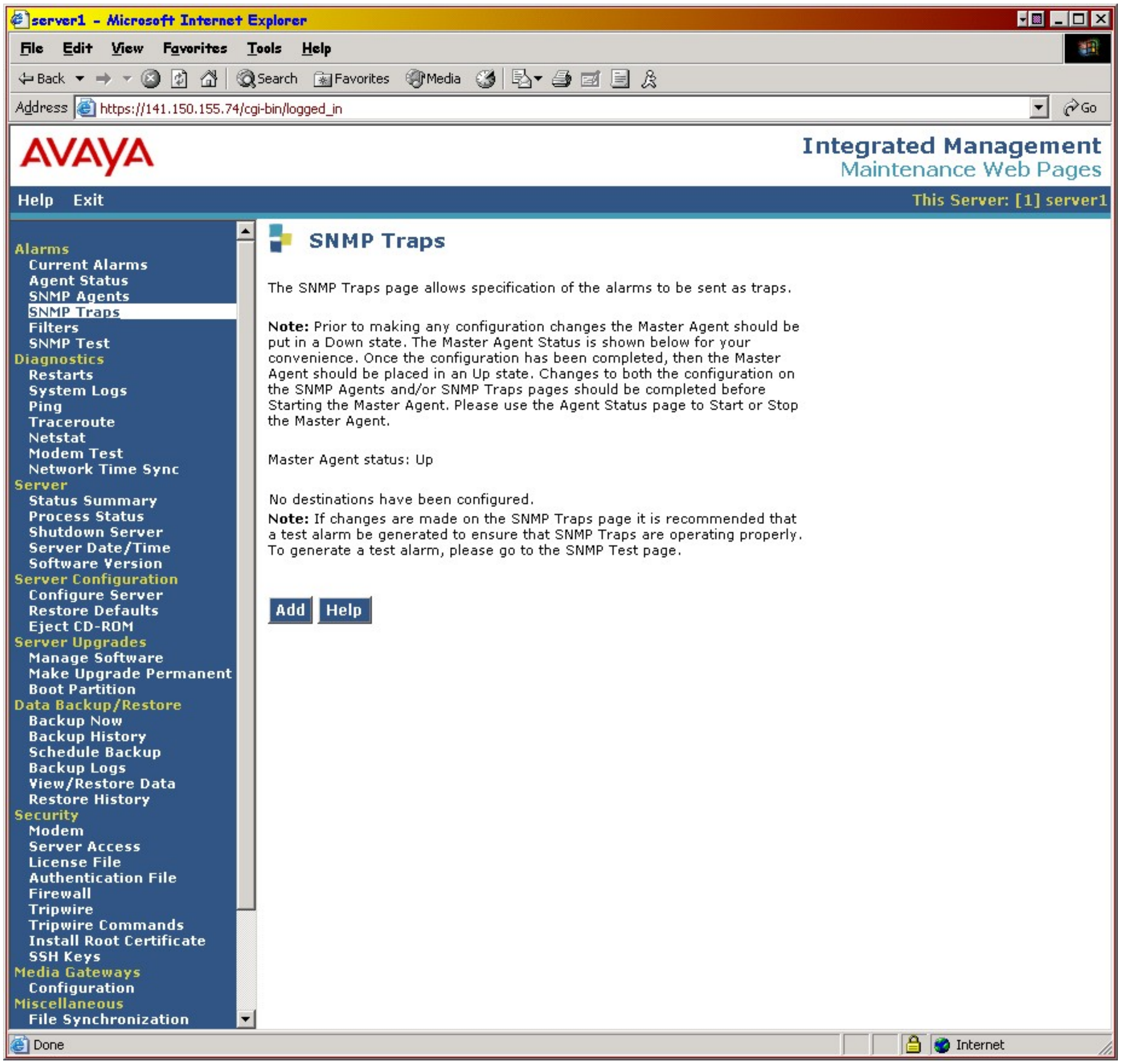

Home(Standard Management Solutions) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://141.150.155.74/cgi-bin/unified
Go Links
AVAYA
Integrated Management
Standard Management Solutions
Help Log Off

Installation	The Avaya Installation Wizard allows you to quickly install your system.	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

© 2004 Avaya Inc. All Rights Reserved.

javascript:onClick=HandleWinOpen('/cgi-bin/logged_in','NULL','menubar=yes, toolbar=yes,resizable=yes,location=yes,status=yes,ta

1. *Add the SNMP trap information*. In the left panel, select **Alarms → SNMP Traps**. Press the **Add** button.



SNMP Traps

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

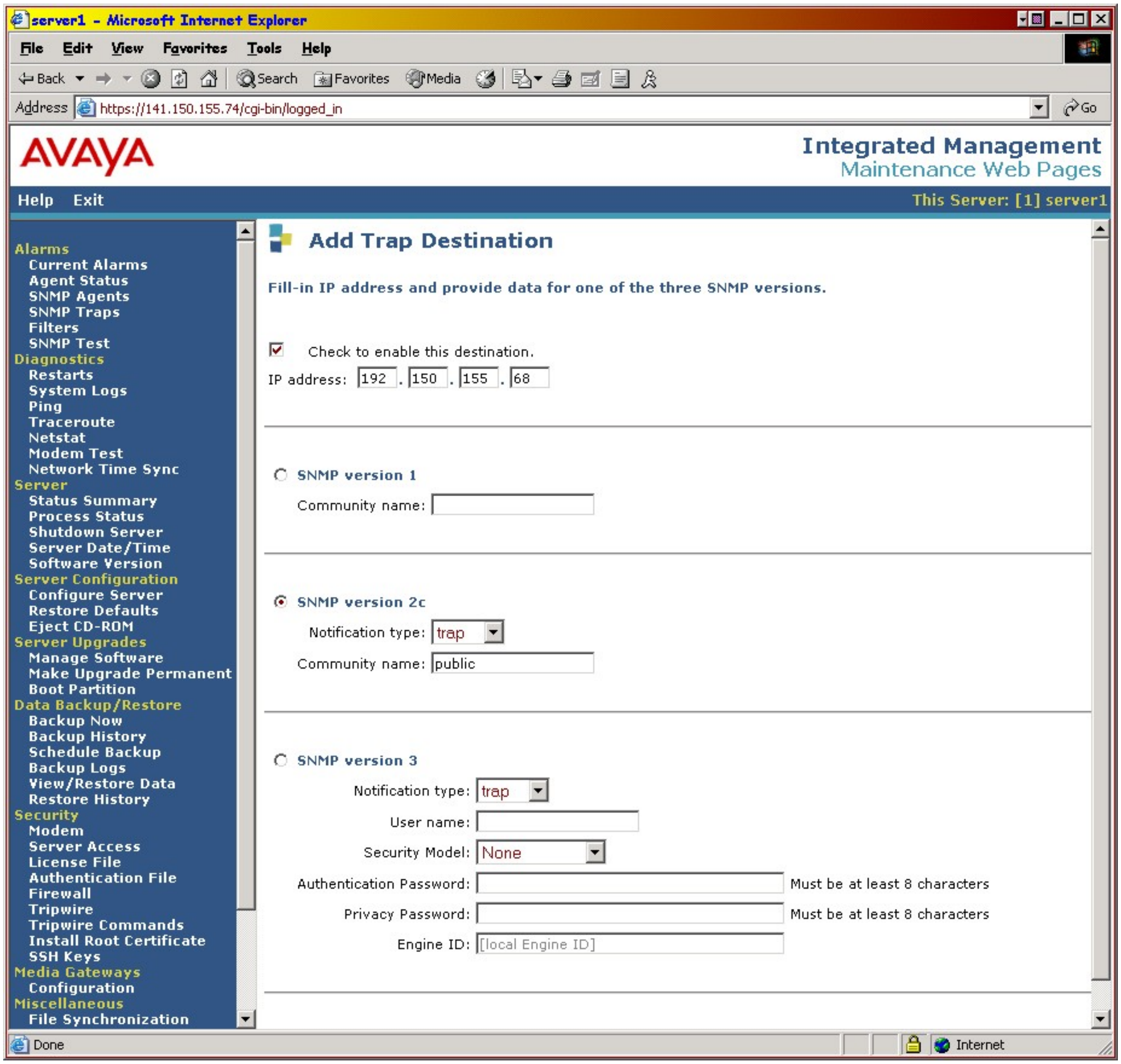
Note: Prior to making any configuration changes the Master Agent should be put in a Down state. The Master Agent Status is shown below for your convenience. Once the configuration has been completed, then the Master Agent should be placed in an Up state. Changes to both the configuration on the SNMP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

No destinations have been configured.

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.

2. *Configure the SNMP Trap information.* Check the **Check to enable this destination** box. Enter the IP Address of the ASG Defender in the **IP address** field. Select the **SNMP version2c** option and enter the same name used for the **SNMP Get Community Name** from Step 2 in Section 5 in the **Community name** field. Scroll down and press the **Add** button.



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 . 150 . 155 . 68

○ SNMP version 1

Community name:

● SNMP version 2c

Notification type: trap

Community name: public

○ SNMP version 3

Notification type: trap

User name:

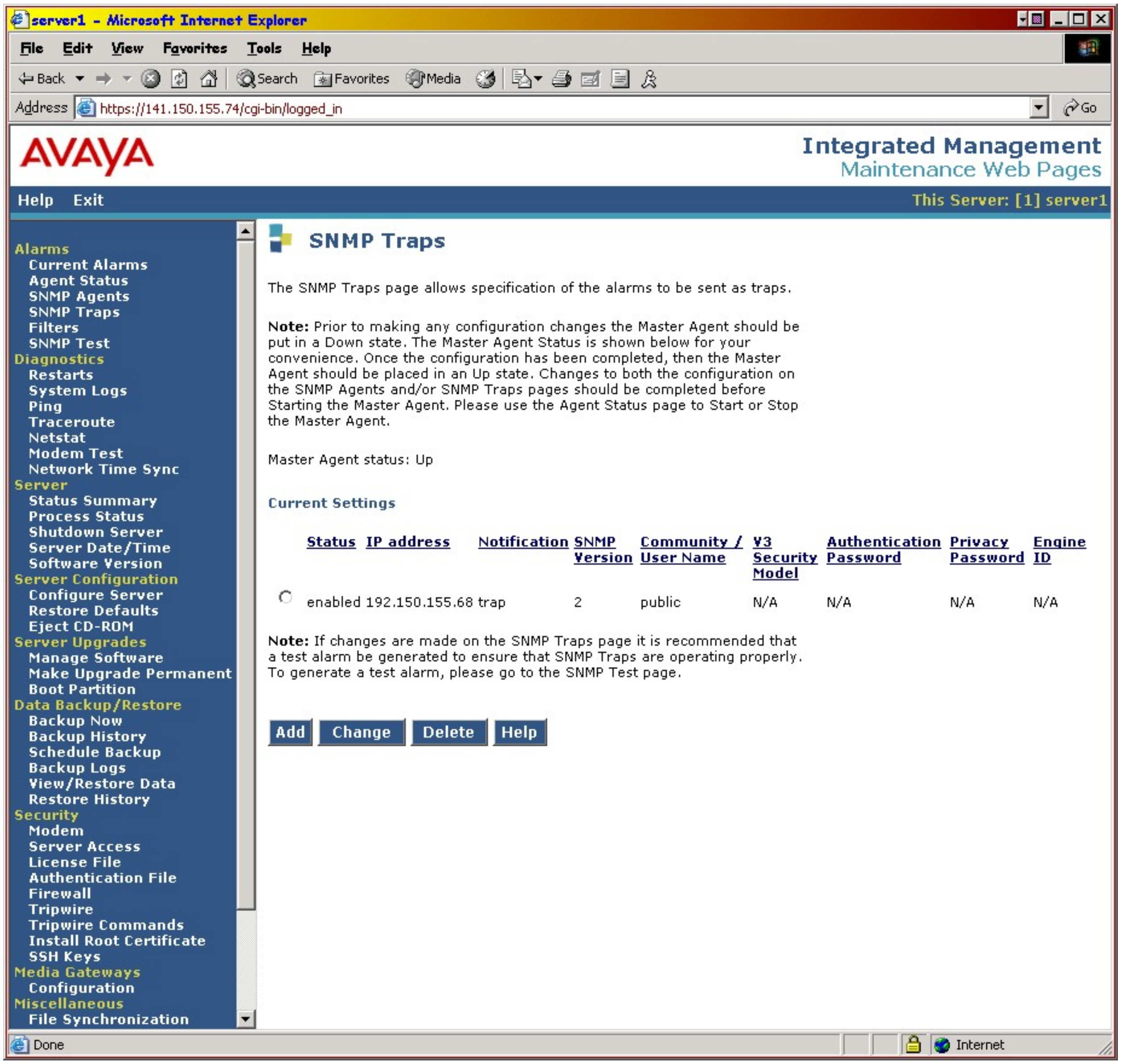
Security Model: None

Authentication Password: Must be at least 8 characters

Privacy Password: Must be at least 8 characters

Engine ID: [local Engine ID]

The following screen shows the SNMP Trap IP Address successfully administered.



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.

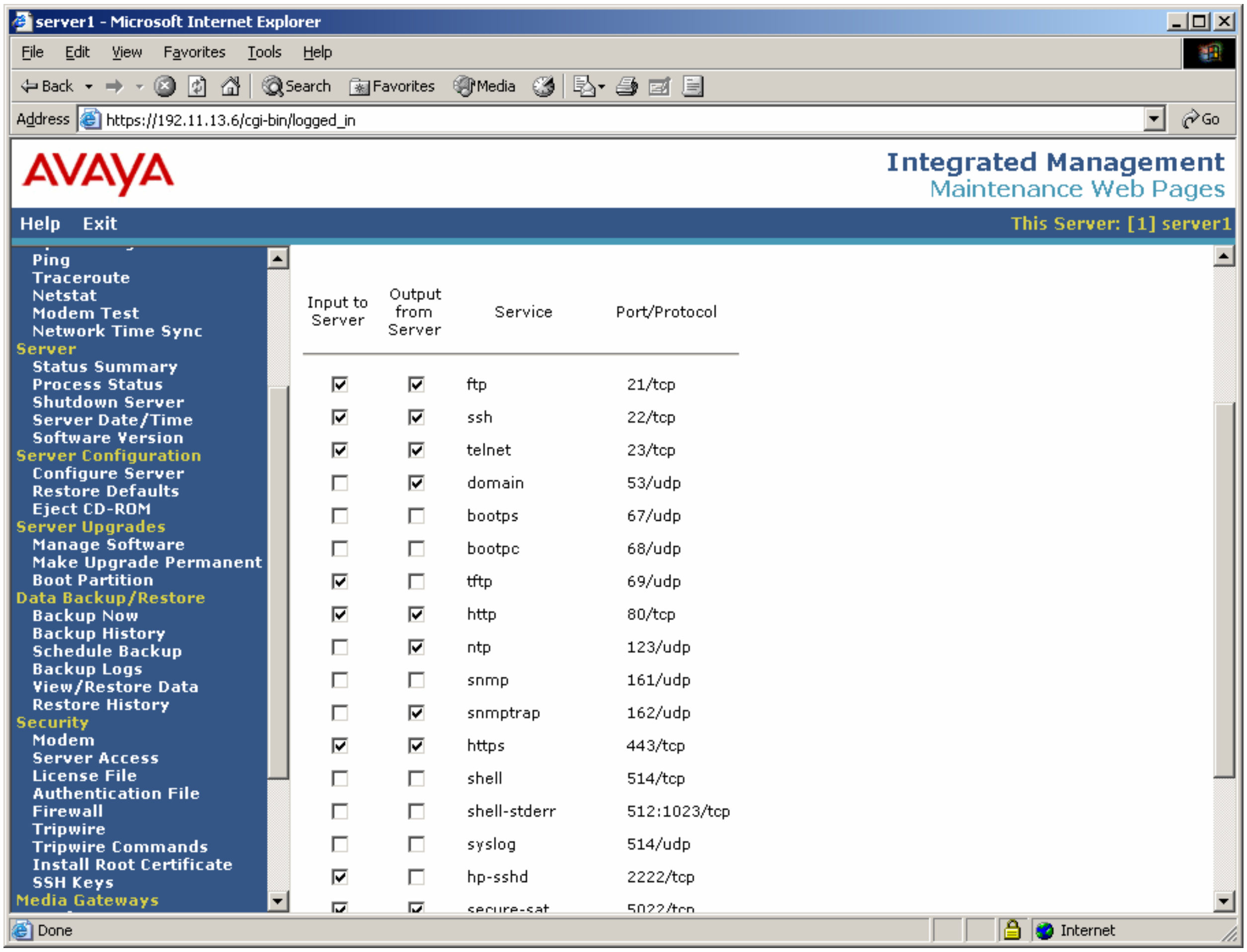
Master Agent status: Up

Current Settings

	Status	IP address	Notification	SNMP Version	Community / User Name	V3 Security Model	Authentication Password	Privacy Password	Engine ID
○	enabled	192.150.155.68	trap	2	public	N/A	N/A	N/A	N/A

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.

3. *Configure the S8300 firewall to allow SNMP traps to be sent.* The firewall in the Avaya Media Server must allow SNMP traps to be sent on UDP port 162. Select **Security** → **Firewall.** Check the box in the **Output from Server** column for the **snmptrap** entry. Scroll down and press the **Submit** button.



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
☐	☐	shell	514/tcp
☐	☐	shell-stderr	512:1023/tcp
☐	☐	syslog	514/udp
☑	☐	hp-sshd	2222/tcp
☑	☑	secure-sat	5022/tcp

4. *Configure the alarm reporting options.* This is done via the SAT. Log in with the appropriate credentials. Ensure that the alarms the customer would like to have reported are set to **[y]**es. Enter the **set options** command and check the Major and Minor columns for each alarm type. When the Major or Minor column is set to **[w]**arning, **[r]**eporting, or **[n]**o, then that alarm type has either been downgraded to warning severity or alarm reporting has been suppressed.

```
set options                                                    Page   1 of  22
                               ALARM REPORTING OPTIONS
                                                     Major   Minor
                                On-board Station Alarms: w    w
                               Off-board Station Alarms: w    w
                  On-board Trunk Alarms (Alarm Group 1): y    y
                 Off-board Trunk Alarms (Alarm Group 1): w    w
                  On-board Trunk Alarms (Alarm Group 2): w    w
                 Off-board Trunk Alarms (Alarm Group 2): w    w
                  On-board Trunk Alarms (Alarm Group 3): w    w
                 Off-board Trunk Alarms (Alarm Group 3): w    w
                  On-board Trunk Alarms (Alarm Group 4): w    w
                 Off-board Trunk Alarms (Alarm Group 4): w    w
                           On-board Adjunct Link Alarms: w    w
                          Off-board Adjunct Link Alarms: w    w
                             Off-board MASI Link Alarms:      w
                                   Off-board DS1 Alarms: w    w
```

4. Configure Avaya G350 Media Gateway

This section describes the procedure for configuring the Avaya G350 Media Gateway to report alarms to an SNMP trap destination. By default, the Avaya G350 Media Gateway forwards all alarms to the media server, configured in Section 3. In the compliance test, the Avaya G350 Media Gateway registered with the Avaya S8300 Media Server. All alarms were sent to the Avaya S8300 Media Server (192.150.155.71).

An administrator may configure another SNMP trap destination by using the following command:

G350-001(super)# snmp-server host <host-addr> <traps|informs> <v1|v2c> <community-name>

The following screen, obtained from the Command Line Interface of the Avaya G350 Media Gateway, displays the SNMP trap configuration used for the compliance test.

```
G350-003(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
---------------- ----- ------- --------------- ----------- ------------------
-
192.150.155.74      v2c   noauth  all              trap       ReadCommN
 UDP port: 162 DM
G350-003(super)#
```

5. Configure ASG Defender

This section provides the procedures for configuring the ASG Defender, which includes:

1. Configuring the IP Address
2. Configuring the SNMP parameters
3. Adding the Avaya devices
4. Configuring the modem dial out information

Start a terminal emulation program and connect to the ASG Defender via the AUX port. Log in with the appropriate credentials. In all the screens below, press **Enter** to advance to the next field.

1. *Configure the IP Address for the ASG Defender*. At the command prompt, type **snp**, which stands for Set Network Parameters. At the **Select Group** prompt type **1.** Enter **No** for **Restore Factory Defaults**. Advance to the **External Address** field. Enter the **IP Address** of the ASG Defender. Press **Enter** and type in the **Mask** and **Default Gateway**. Press **Enter** to advance to the prompt.

```
5010000000>snp
--- Set Network Params ---
1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params
4 = PPP Params
5 = Telnet Params
Select Group -->1
Restore Factory Defaults ?         No
Internal Interface                 Auto Sensing
Internal Address
         Mask                      255.255.255.0
External Interface                 Auto Sensing
External Address                   192.150.155.68
         Mask                      255.255.255.0
Default Gateway                    192.150.155.74
Nameserver
PPP Address                        10.28.11.11
PPP Peer Address                   10.28.11.12
10/19/06 12:48:56 8856 {I} [AUX:22] Set Network Params
5010000000>
```

2. *Configure the SNMP parameters.* At the command prompt, type **snp**. At the **Select Group Prompt**, type **2.** Enter **No** for **Restore Factory Defaults**. Configure the following fields as illustrated in the picture below.
    - **Trap Format**
    - **SNMP Trap Community Name**
    - **SNMP Get Community Name –** this must match the **Community name** administered on Avaya Communication Manager from Step 2 of Section 3.

```
5010000000>snp
--- Set Network Params ---
1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params
4 = PPP Params
5 = Telnet Params
Select Group -->2
Restore Factory Defaults ?          No
-- SNMP Manager Parameters --
PPP link needed for trap?           No
Trap format                         Standard
SNMP Trap Community Name            SNMP_trap
SNMP Set Community Name             private
SNMP Get Community Name             public
Enable reboot via SNMP              No
-- IP Addresses for SNMP Managers (name or IP address) --
  Manager 1
  Manager 2
  Manager 3
  Manager 4
  Manager 5
5010000000>
```

3. *Add in Avaya Communication Manager to the Avaya IP connection list.* At the command prompt, type **aaip**, which stands for Add Avaya IP Device. Enter a unique name in the **Device Name** field. Enter the IP address of the G350 Media Gateway in the **IP Address** field. Enter the IP Address of the Avaya Global Services System that will be accessing the Avaya Communication Manager in the **Avaya IP Address** field. Avaya Global Services will provide this. Select Telnet for the **Terminal Connection Type** field. The **Ports** field will be automatically populated when the **Terminal Connection Type** field is selected. This can be left as the default. Select **S8500** for the **Host Equipment Type** field. The **Comments** field may be left blank.

   Note: The S8500 choice for Host Equipment Type is used when the Avaya Media Server is either an S8300 or S8500.

```
5010000000>aaip
Device name                  Avaya Communication Manager
IP Address                  192.150.155.74
Avaya IP Address                10.3.230.3
Terminal Connection Type          Telnet
Ports                      80,443,21,23,5023
Host Equipment Type              8500
Comments
Reinitializing rules for Avaya devices...
```

4. *Add in Avaya Intuity Audix (IA 770) to the Avaya IP connection list.* At the command prompt, type **aaip**. Enter a unique name in the **Device Name** field. Enter the IP address of Intuity Audix (IA 770) in the **IP Address** field. Enter the IP Address of the Avaya Global Services System that will be accessing Intuity Audix (IA 770) in the **Avaya IP Address** field. Avaya Global Services will provide this. Select **SSH** for the **Terminal Connection Type** field. The **Ports** field will be automatically populated when the **Terminal Connection Type** field is selected. This can be left as the default. Select **S8500** for the **Host Equipment Type** field. The **Comments** field may be left blank.

```
5010000000>aaip
Device name                   IA 770
IP Address                  192.150.155.71
Avaya IP Address                10.3.230.3
Terminal Connection Type          SSH
Ports                      8443,80,443,21,22,5022
Host Equipment Type              8500
Comments
Reinitializing rules for Avaya devices...
```

5. *Configure the dial out telephone number*. At the command prompt, type **ssp**. At the **Select Group** prompt type **3.** Advance to the **Home Phone Number 1 (Default)** field. Enter the telephone number that will be used to connect to the INADS system. Advance to the **Report Multiple Alarms** field and select **Yes**. Leave all other fields as default.

```
5010000000>ssp
--- Set System Parameters ---
1 = Site Information
2 = Scheduling Params
3 = Action Routine Params
Select Group -->3
-- Action Routine Parameters --
Home Phone Number 1 (Default)        17325554321
Home Phone Number 2
Home Phone Number 3
Home IP Address
Delay Before Transmit (sec)          5
Report Multiple Alarms ?            Yes
Default Pager Number
Default Pin Number
Default Pager Message
Default Action Routine Modem
5010000000>
```

6. Interoperability Compliance Testing

The following section describes the compliance testing approach and results for the ASG Defender.

6.1. General Test Approach

Using the network illustrated in **Figure 1**, the ASG Defender was configured to receive SNMP INADS alarms from Avaya Communication Manager and Avaya Intuity Audix (IA 770). Avaya Communication Manager was configured to send test alarms to the ASG Defender. Alarms were generated on Avaya Communication Manager and Avaya Intuity Audix (IA 770) and sent to the ASG Defender, which placed a call to Avaya Global Services in Denver. The Product ID was verified in Denver for Avaya Communication Manager and Avaya Intuity Audix (IA 770). The Acknowledgement of the alarm that was sent from INADS to the ASG Defender was verified. The remote administration and maintenance of Avaya Communication Manager and Avaya Intuity Audix (IA 770) through the ASG Defender PPP connection was also verified. Both single and multiple alarm scenarios were tested.

6.2. Test Results

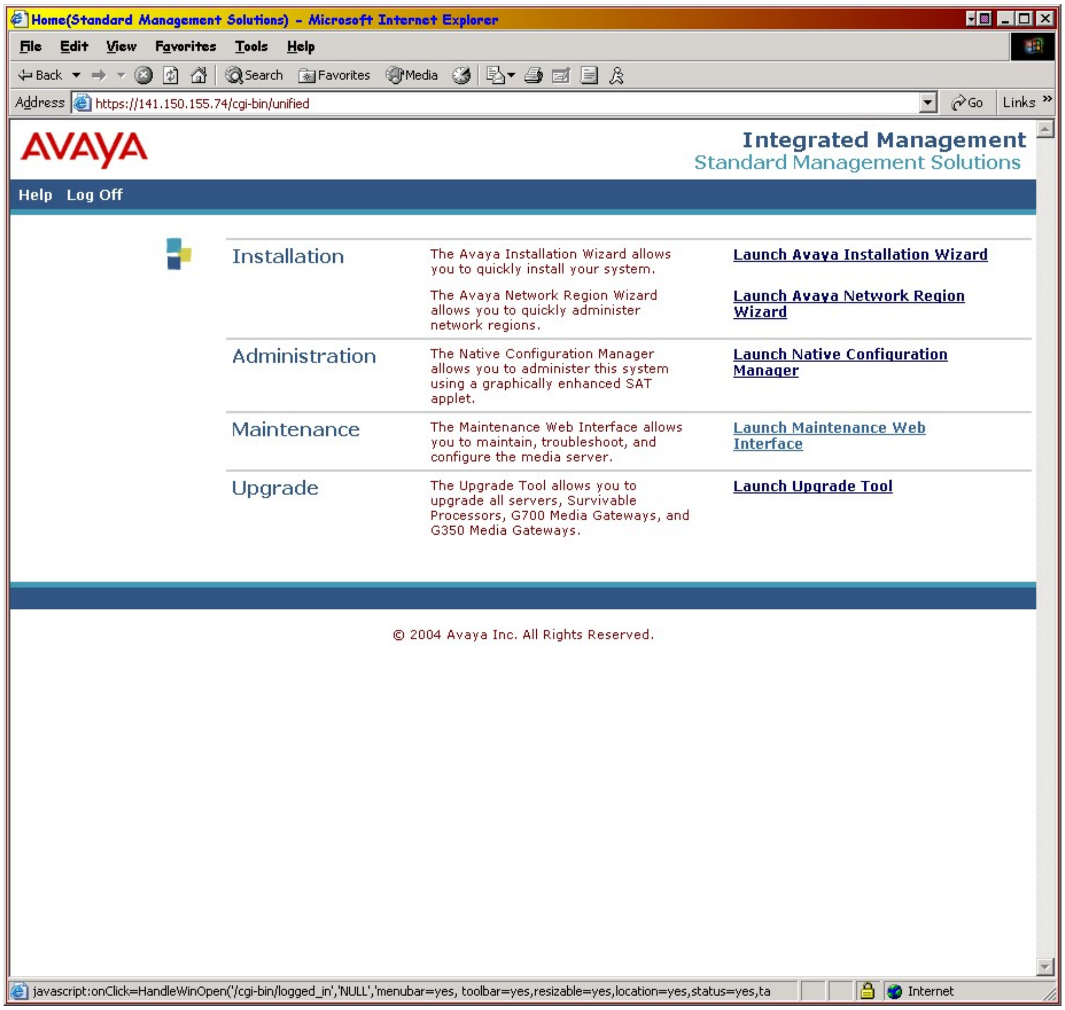
The following features for the ASG Defender were successfully verified during the compliance testing:

- Avaya Global Services access to Avaya Communication Manager and Avaya Intuity Audix (IA 770) via dial-up PPP session through PSTN
- Alarming forwarding and generation from ASG Defender to Avaya Global Services
- Notification of trap receipt status to Avaya Communication Manager and Avaya Intuity Audix (IA 770)

7. Verification Steps

7.1. Avaya Communication Manager

Test Alarms can be generated by performing the following steps. To access the web interface, launch a web browser and connect to the media server by entering the URL https://<media server IP address>. Supply the login and password for an account with super-user privileges. After logging in, a window is displayed with four options. Select the **Maintenance** option.

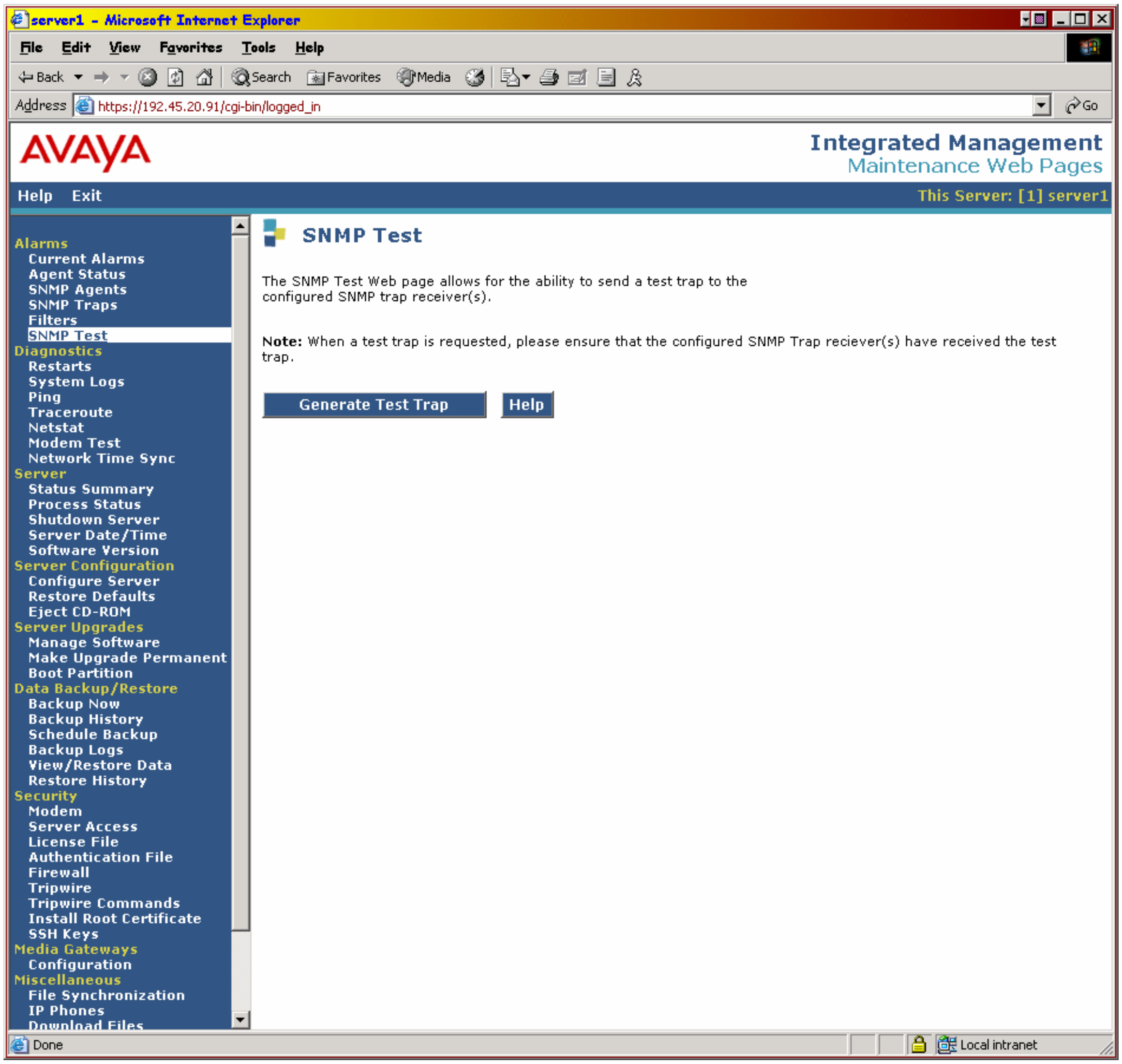

Home(Standard Management Solutions) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://141.150.155.74/cgi-bin/unified
Go Links
AVAYA
Integrated Management
Standard Management Solutions
Help Log Off

Installation	The Avaya Installation Wizard allows you to quickly install your system.	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

© 2004 Avaya Inc. All Rights Reserved.

javascript:onClick=HandleWinOpen('/cgi-bin/logged_in','NULL','menubar=yes, toolbar=yes,resizable=yes,location=yes,status=yes,ta

1. Select the **Alarms** → **SNMP Test** option. Press the **Generate Test Trap** button.



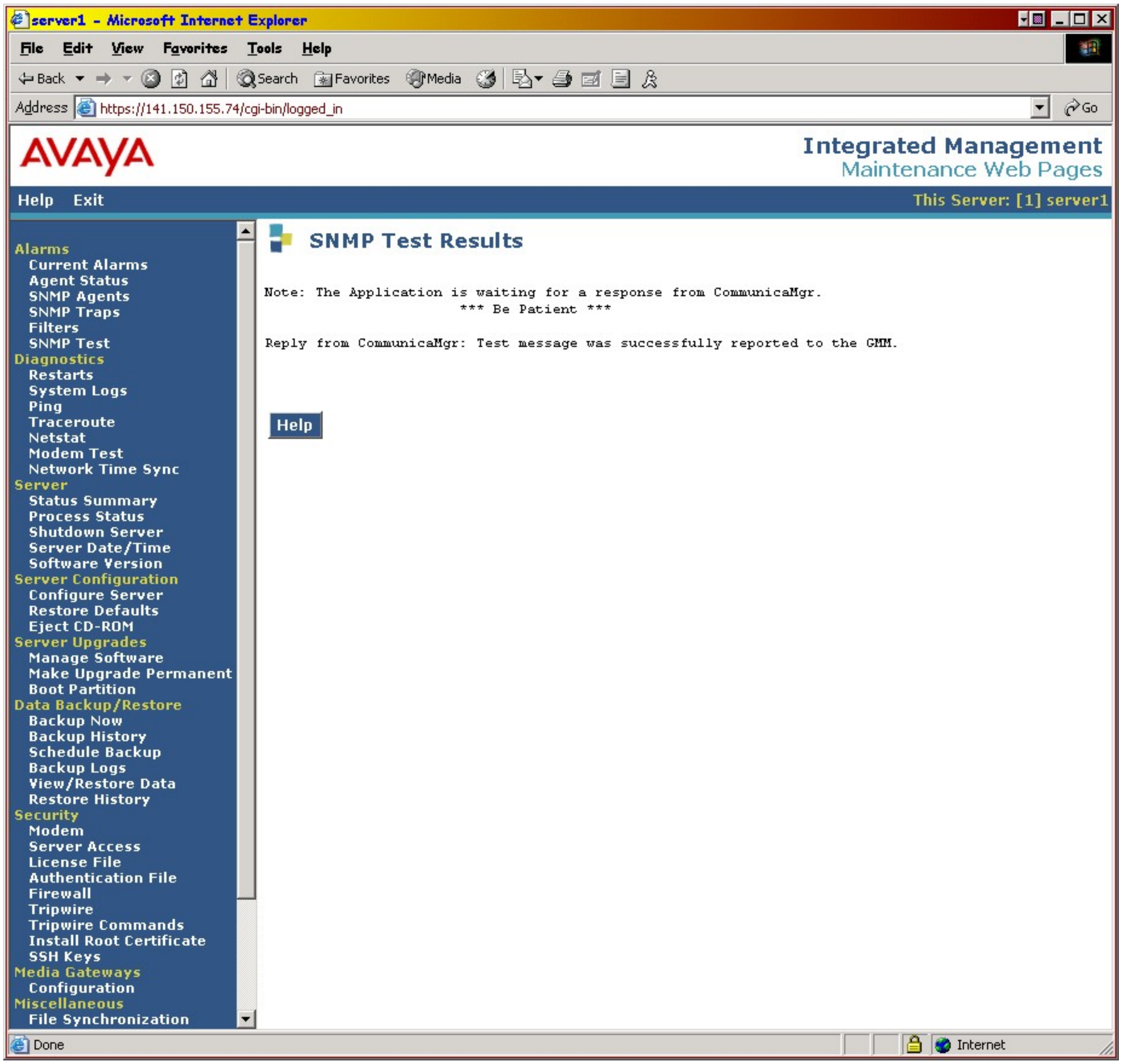
Address https://192.45.20.91/cgi-bin/logged_in

SNMP Test

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

Note: When a test trap is requested, please ensure that the configured SNMP Trap reciever(s) have received the test trap.

The following is displayed.



SNMP Test Results

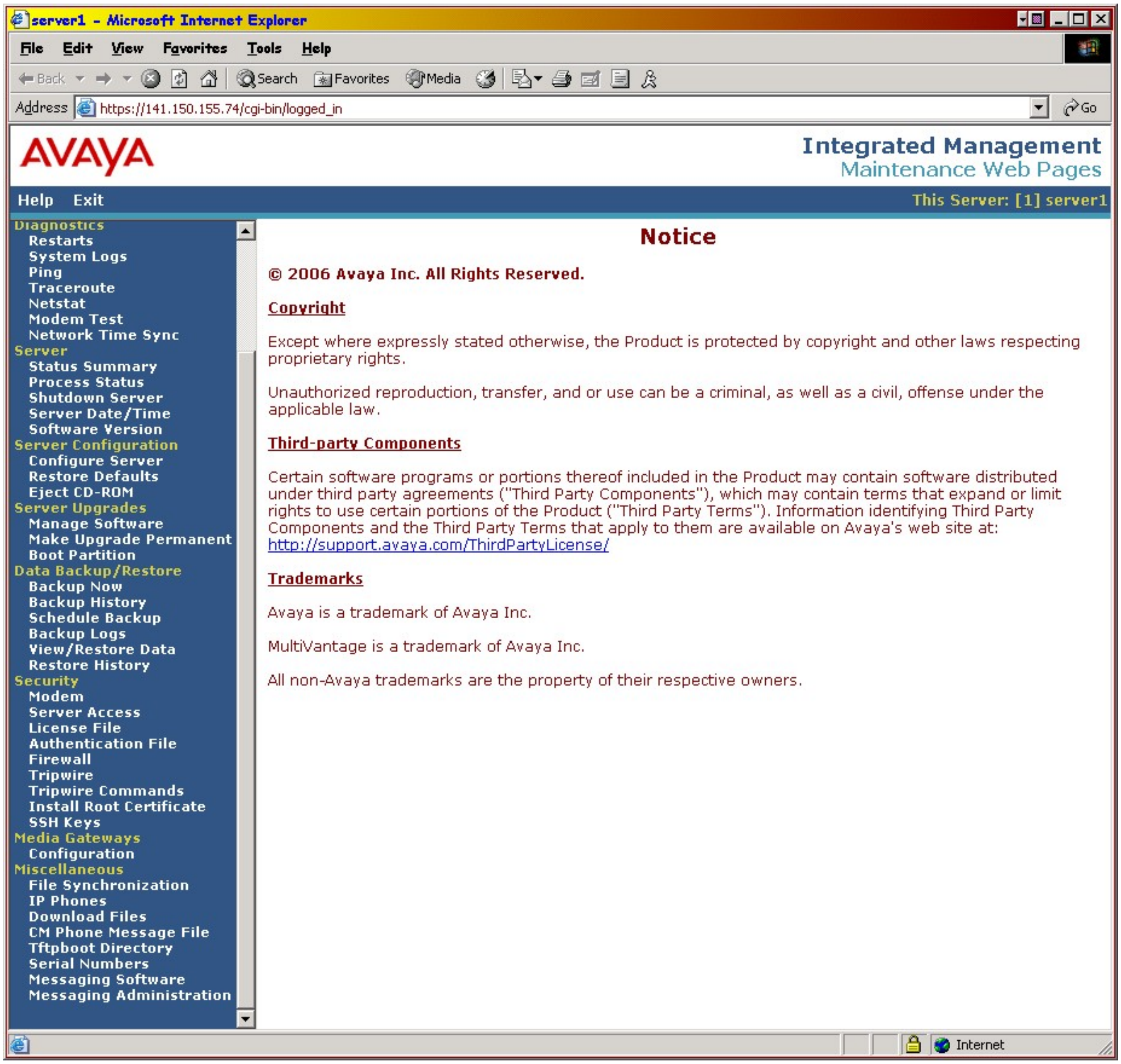
```
Note: The Application is waiting for a response from CommunicaMgr.
                       *** Be Patient ***

Reply from CommunicaMgr: Test message was successfully reported to the GMM.
```

To view alarms, select the **Alarms** → **Current Alarms** option.

7.2. Avaya Intuity Audix (IA 770)

Test Alarms can be generated by performing the following steps. To access the web interface, launch a web browser and connect to the media server by entering the URL https://<media server IP address>. Supply the login and password for an account with super-user privileges. After logging in, a window is displayed with four options. Select the **Maintenance** option.

1. Select the **Miscellaneous** → **Messaging Administration** option.



Notice

© 2006 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/

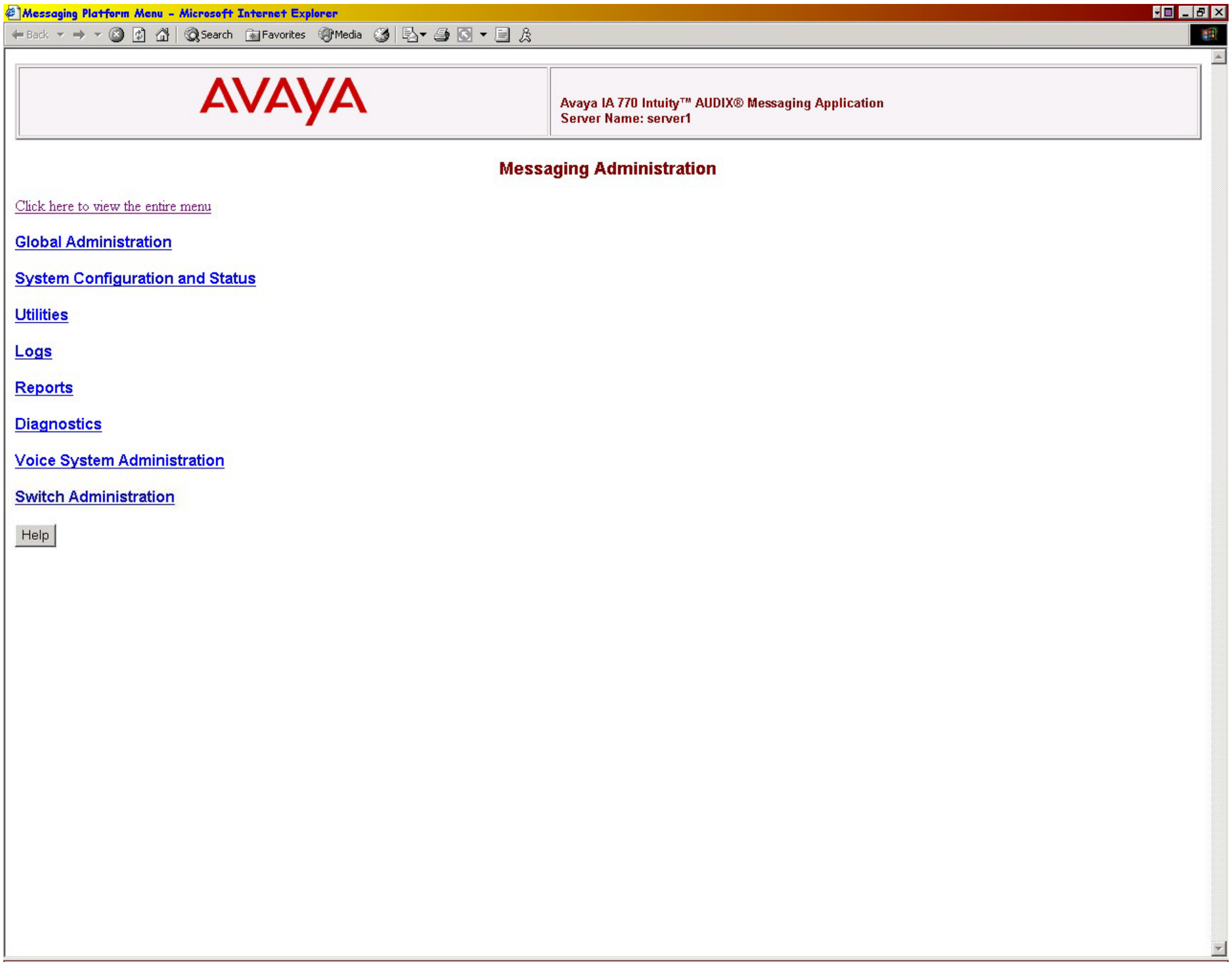
Trademarks

Avaya is a trademark of Avaya Inc.

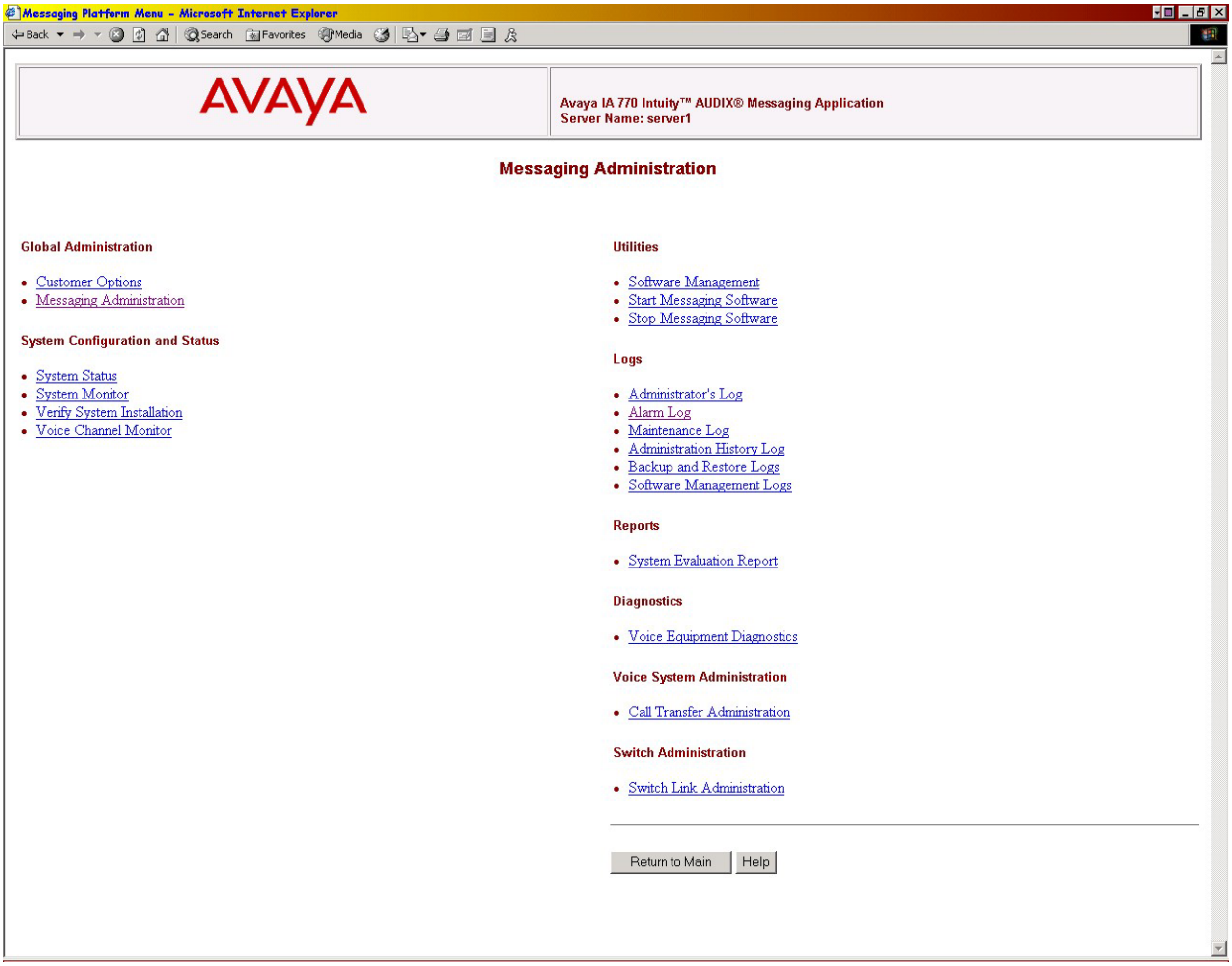
MultiVantage is a trademark of Avaya Inc.

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

2. Select the **Click here to view the entire menu** option.


Messaging Platform Menu - Microsoft Internet Explorer
Back
Search
Favorites
Media
AVAYA
Avaya IA 770 Intuity™ AUDIX® Messaging Application
Server Name: server1
Messaging Administration
Click here to view the entire menu
Global Administration
System Configuration and Status
Utilities
Logs
Reports
Diagnostics
Voice System Administration
Switch Administration
Help

3. Select the **Messaging Administration** option and log in with the appropriate credentials.



Avaya IA 770 Intuity™ AUDIX® Messaging Application
Server Name: server1

Messaging Administration

Global Administration

- Customer Options
- Messaging Administration

System Configuration and Status

- System Status
- System Monitor
- Verify System Installation
- Voice Channel Monitor

Utilities

- Software Management
- Start Messaging Software
- Stop Messaging Software

Logs

- Administrator's Log
- Alarm Log
- Maintenance Log
- Administration History Log
- Backup and Restore Logs
- Software Management Logs

Reports

- System Evaluation Report

Diagnostics

- Voice Equipment Diagnostics

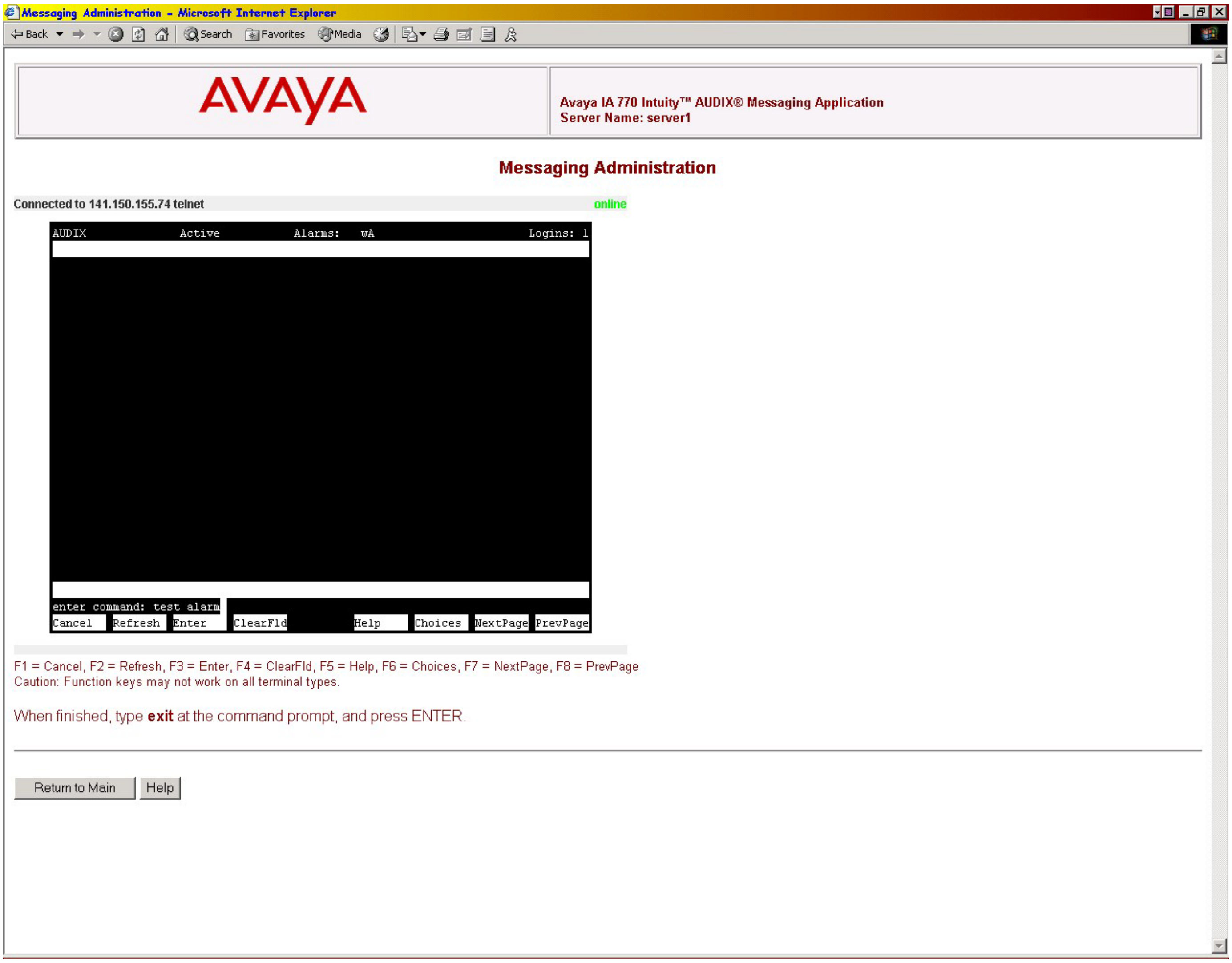
Voice System Administration

- Call Transfer Administration

Switch Administration

- Switch Link Administration

4. At the prompt, type in **test alarm** and press **Enter**.



Avaya IA 770 Intuity™ AUDIX® Messaging Application
Server Name: server1

Messaging Administration

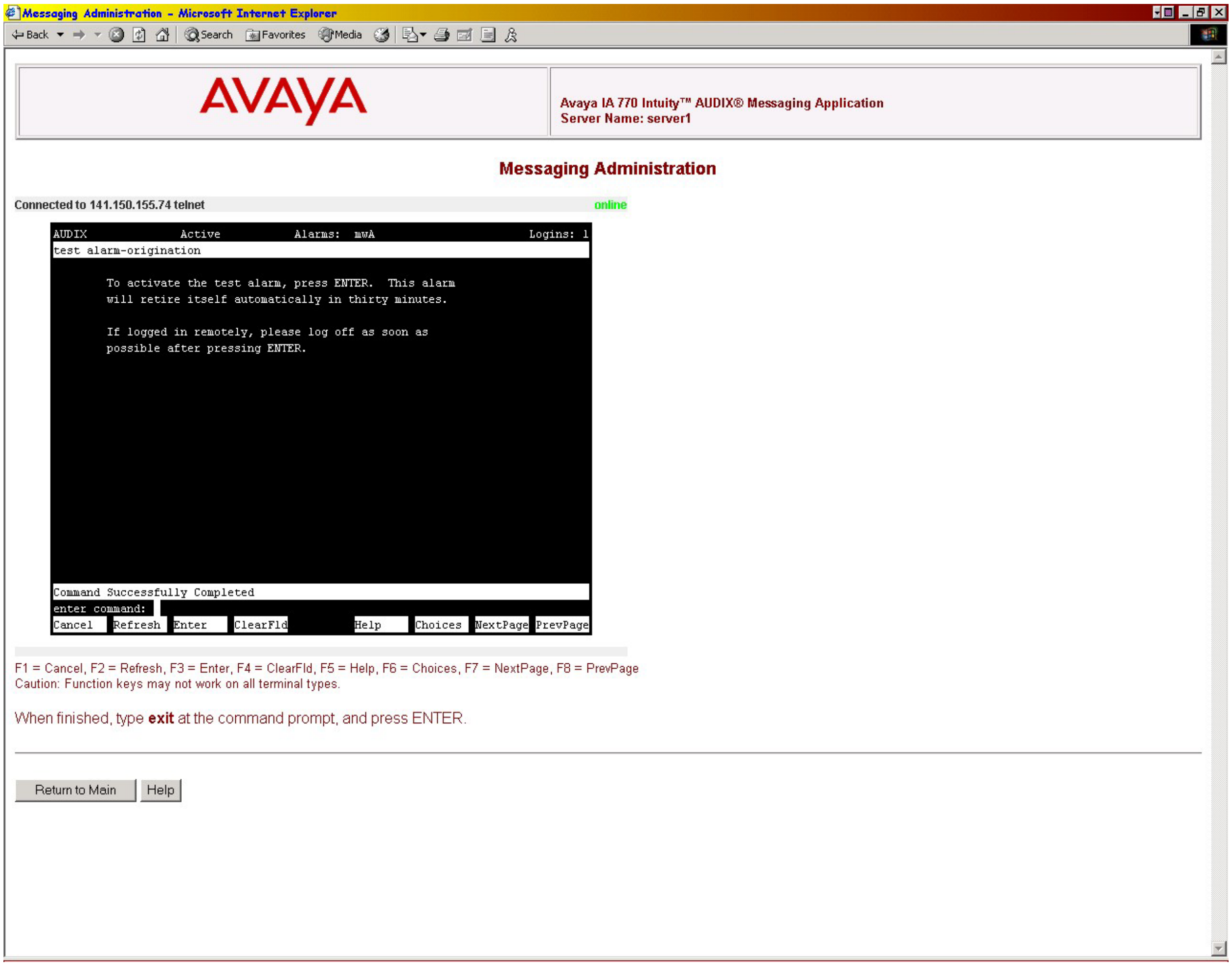
Connected to 141.150.155.74 telnet online

```
AUDIX              Active          Alarms:    wA                 Logins: 1

enter command: test alarm
Cancel   Refresh  Enter    ClearFld           Help     Choices  NextPage PrevPage
```

F1 = Cancel, F2 = Refresh, F3 = Enter, F4 = ClearFld, F5 = Help, F6 = Choices, F7 = NextPage, F8 = PrevPage
Caution: Function keys may not work on all terminal types.

When finished, type **exit** at the command prompt, and press ENTER.

5. Press the **F3** button when the following screen is displayed:


Messaging Administration - Microsoft Internet Explorer
Back
Search
Favorites
Media
AVAYA
Avaya IA 770 Intuity™ AUDIX® Messaging Application
Server Name: server1
Messaging Administration
online
Return to Main
Help

Connected to 141.150.155.74 telnet

```
AUDIX               Active            Alarms:  mwA                  Logins: 1
test alarm-origination

        To activate the test alarm, press ENTER.  This alarm
        will retire itself automatically in thirty minutes.

        If logged in remotely, please log off as soon as
        possible after pressing ENTER.

Command Successfully Completed
enter command:
Cancel   Refresh  Enter    ClearFld           Help     Choices  NextPage PrevPage
```

F1 = Cancel, F2 = Refresh, F3 = Enter, F4 = ClearFld, F5 = Help, F6 = Choices, F7 = NextPage, F8 = PrevPage
Caution: Function keys may not work on all terminal types.

When finished, type **exit** at the command prompt, and press ENTER.

7.3. ASG Defender

The logs on the ASG Defender can be used to verify the ASG Defender activity. At the prompt, type **lh**. Enter **Info** for the **Enter Lowest Severity to display** field. Below is a partial view of the log. The log will provide information about why the alarm failed, in this case the modem did not receive dial tone.

```
5010000000>lh


--- Log History ---
Enter Lowest Severity to display (Info=All)  Info
09/26/06 09:31:18 F1BA {I} SYSTEM RESTART:  Diagnostic code 00
09/26/06 09:31:18 6521 {I} ASG DEFENDER v1.0.4 - Reset
09/26/06 09:31:18 6CA9 {I} Serial Number: 062H0833976
.
.
.
09/26/06 09:34:57 D081 {I} [M1:] PHONTRAP: #SENDALL /tmp/trapYSHInG
09/26/06 09:35:05 E4BF {E} [M1:] PHONTRAP Fail: NO DIALTONE - Retry Scheduled
.
.
.
10/26/06 09:15:58 B1C2 {I} [AUX:23] Log History
10/26/06 09:15:58 B06F {I} Network init OK
```

8. Conclusion

These Application Notes describe the configuration steps required for configuring Avaya Communication Manager version 3.1.1 with a co-resident Intuity Audix (IA 770) to send SNMP alarms to Avaya Global Services through the ASG Defender version 1.0.4. All feature functionality and serviceability test cases were completed successfully.

9. Support

For technical support on the ASG Defender, visit http://support.avaya.com.

10. Additional References

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

- Feature Description and Implementation For Avaya Communication Manager, Issue 4.0, Feb 2006, Document Number 555-245-205.
- *ASG Defender Administrator's Guide*, Version 1.0.0, February 10, 2006

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.