ASG Guard II

Integration Guide for Linux-Based Duplex & Simplex Servers (S8700, S8500 & S8300)

Comcode XXXXXXX
Issue 1.0
October 2003

Printed in U.S.A.

Notice
Every effort was made to ensure that the information in this book was complete and accurate at the time of printing. However, information is subject to change.

Preventing Toll Fraud
Toll Fraud is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or working on your company.s behalf). Be aware that there is a risk of toll fraud associated with your system and that, if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Fraud Intervention
If you *suspect that you are being victimized* by toll fraud and you need technical assistance or support, call the Technical Service Center's Toll Fraud Intervention Hotline at 1-800-643-2353.

Providing Telecommunications Security
Telecommunications security of voice, data, and/or video communications is the prevention of any type of intrusion to, that is, either unauthorized or malicious access to or use of, your company's telecommunications equipment by some party.
Your company's telecommunications equipment includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or working on your company's behalf. Whereas, a "malicious party" is anyone, including someone who may be otherwise authorized, who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time multiplexed and/or circuit-based) or asynchronous (character-, message-, or packet-based) equipment or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll-facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent).

Be aware that there may be a risk of unauthorized or malicious intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company, including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs.

Your Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - an Avaya customer's system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure your:

- Avaya provided telecommunications system and their interfaces
- Avaya provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

To Get Help
If you need assistance with administration of the ASG Guard call Avaya, Inc. at **1 800-242-2121**, or your local Authorized Dealer. Our technical support staff is available 24 hours. This call may be billable.

FCC Notices

United States Users
Part 15. Subpart A: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio operations. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

European Users
This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Safety Warnings
1. Read and understand all instructions in the user's manual.
2. Observe all warnings and instructions marked on this product.
3. Unplug the product from wall outlets and telephone jacks before cleaning. Clean exposed parts with a soft, damp cloth. Do not use liquid or aerosol cleaners and never immerse in water.
4. Do not use the product near water or when you are wet. If the product comes in contact with any liquids, unplug the power and line cords immediately. Do not plug the product back in until it has been dried thoroughly.
5. Install this product securely on a stable surface. Damage may result if the product falls.
6. Install this product in a protected location, where no one can step on or trip over power and line cords. Do not place objects that may cause damage or abrasion on the cords.
7. Do not allow anything to rest on the power cord. Do not install this product where people walking on it will abuse the cord. Do not overload wall outlets, this can result in the risk of fire or electric shock.
8. Never push objects of any kind into this product through housing opening because they may touch dangerous voltage points or short out parts, resulting in possible fire or electric shock.
9. If this product does not operate normally, you cannot solve the problem, or if the product is damaged, report the trouble to Avaya, Inc. Do not open the product; opening the product can expose you to dangerous voltage or other risks.
10. During thunderstorms, avoid using telephones, except cordless modes. There is a slight chance of electric shock from lightning.
11. Never install telephone wiring during a lightning storm.
12. Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
13. Never touch telephone wires, network wires, or terminals unless they have been disconnected from the service provider.
14. Use caution when installing or modifying telephone lines.
15. Do not use a telephone in the vicinity of a gas leak. If you suspect a gas leak, report it immediately, but use a telephone away from the area where gas is leaking.
16. This product should be operated from the power source indicated on the power transformer (see item 17 below). If you are not sure of the type of power supplied to your business or home, consult your local power company.
17. Use only a UL Listed wall plug-in power transformer that has the following characteristics:
    Input Rating: 120 V AC ± 10% 60 Hz
    Output Rating: 16 V AC at 2063 milliamps
    The power transformer supplied with this product has these characteristics.

Changes or modifications to the ASG Guard and the devices that are not expressly approved by Avaya, Inc. will void the user's authority to operate the equipment.

Trademarks
The Avaya S8300 and S8700 Media Servers are trademarks of Avaya, Inc.

Table of Contents

Table of Figures

1 INTRODUCTION

This section covers the following topics:

1.1 Document Overview

The purpose of this document is to describe the integration between the ASG Guard II (referred to as the "Guard" or "Guard II" throughout this document) and the Avaya S8x000 series media servers.

The Guard II provides both secure remote access and device monitoring of Avaya IP enabled devices such as the S8x00 series media servers. Using a built in firewall, the Guard II offers remote access to the management interfaces of IP-enabled devices, while limiting connectivity to any other device located on the same network. The Guard II provides a secure access path to the various management ports of the S8x00 through a PPP dialup session. Individuals who access the Guard use a DES-based, two-factor authentication token called the ASG Key, which is available both as a software and hardware token.

The S8x00 Media Servers generate SNMP traps containing INADS alarms that are sent to the ASG Guard II. The ASG Guard II converts the SNMP traps to the Avaya alarm receiver format, and forwards the alarms to INADS via PSTN. Upon successful delivery and acknowledgement of the alarm, the Guard II sends a confirmation SNMP trap back to the originating S8x00 device.

The diagram below illustrates an example of the integration of the S8700 and Guard II. Any incoming Web, Telnet, SSH and FTP sessions are proxied by the Guard to the target device.

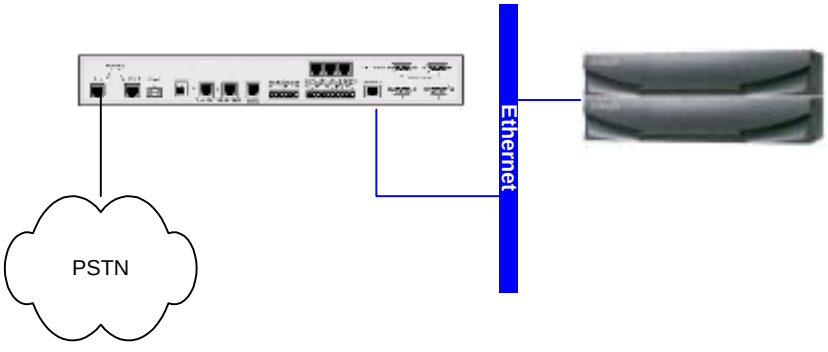

Figure 1-1: ASG Guard II and S8700 Integration

1.2 Audience Assumptions

This document is intended to assist Avaya field technicians and/or other authorized individuals who are responsible for the physical installation and configuration of ASG Guard II security appliances. Customer care center and technical service organization support associates should also refer to this document for assistance when working with field technicians to commission a customer site using ASG Guard II appliances.

1.3 Related Reading Material

ASG Guard and Avaya product documentation are supplemental to this installation guide and can be found at the Avaya website: http://www.avaya.com.

1.4 Getting Help

For assistance with commissioning the ASG Guard and the equipment it is protecting, contact the Avaya Customer Account Support Team at 1-800-248-1111.

2 HARDWARE OVERVIEW

This chapter covers the following topics:

2.1 ASG Guard II Introduction

The ASG Guard II is a security appliance that combines secure console, alarm, sensor, and power management functions. It can be deployed as a single layer solution or as a secure administrative gateway for other ASG Guards and Avaya products. The ASG Guard II protects serial and IP connected devices within the infrastructure, as well as monitors the health and configuration of the network, performs preventive and routine maintenance, manages the flow of information, and performs data collection and analysis from one central point. The ASG Guard II can also monitor environmental conditions surrounding infrastructure elements, using analog sensors that measure conditions such as temperature, humidity, and battery voltage.

2.2 ASG Guard II Physical Features

There are three basic types of devices with the ASG Guard II family, differentiated by the type of host port interface (RJ45 vs. DB9), and number of host port connections (4, 16, 28). See the table below for a list of features unique to each ASG Guard II category. A list of shared physical features and functionality follows the table.

RJ45: *16-port/28-port*	**DB9: *4-port***
• RJ-45 host port connectivity. • RJ-45 AUX port located on rear panel. • One RJ-11 modem connector that supports up to two PCMCIA modems. • One 10/100 “Internal” Ethernet connector that supports one LAN interface. • One 10/100 “External” router interface. • PC Cable power supply. • “Power” and “Activity” LEDs located on front panel. • Power button located on rear panel.	• DB-9 host port connectivity. • DB-9 AUX ports, located on front and rear of unit. • Two RJ-11 modem ports that support up to two PCMCIA modems. • One “10 Base-T” port for external Ethernet connectivity. • Three internal 10 Base-T” Ethernet ports of internal IP connectivity. • 16 VAC connector for standard power supply. • Power key located on front panel. • Various Power, System, and Port LEDs located on front panel.

Additional features include:

- Five contact closure inputs
- One Analog Sensor, 0-5 Volts
- Two Temperature Sensor Inputs
- Two Mechanical Relays, 1 latching/1 non-latching
- One Ram Disk with up to 32 MB of memory
- Integrated VPN router that securely carries administrative traffic through an intranet or public network from an administrator's desktop to each network connected device.

2.2.1 ASG Guard II 4-Port (DB 9) Panel Diagrams

Figure 2-1: ASG Guard II 4-Port Front Panel

ASG Guard II 4-Port Front Panel Features	
Aux Port connector	The user can administer ASG Guard II via a PC or a terminal connected to the front 9-pin AUX connector.
Key switch	The key switch is used to turn ASG Guard II on and off. The key can be removed in either the on or off position. The 4-port ASG Guard II cannot be turned on or off without a key.
LEDs	The LEDs display status messages. When the unit is operating properly, the pulse LED will flash.

Figure 2-2: ASG Guard II 4-Port Rear Panel

ASG Guard II 4-Port Rear Panel Features	
LINE 1 / 2	A standard RJ11 connector is used to connect up to two internal PCMCIA modems.
16 VAC	The 4-Port ASG Guard II utilizes a standard 120VAC 60Hz or 220VAC 50Hz power source input, and transforms it to a 16V output with a 6-pin modular jack connection.
SENSOR INPUTS	The 4-Port ASG Guard II provides three RJ45 sensor inputs: two temperature probes and one 0-5V analog input. A 6-pin Euroblock connector for the 2 simple relay outputs and a 10-pin Euroblock connector for the 5 contact closure inputs are also supported.
10 Base T	The 10-Base T connector provides Ethernet connectivity, while the three RJ45 connectors located above the contact closure inputs support up to three internal LAN interfaces.
HOST PORTS	The 4-Port ASG Guard II provides a standard 9-pin RS-232 (female) interface for up to four serially connected devices such as PBXs and routers.

2.2.2 ASG Guard II 16/28 Port (RJ45) Panel Diagrams

Figure 2-3: ASG Guard II 16/28 Port Front Panel

ASG Guard II 16/28-Port Front Panel Features	
LEDs	The LEDs display power and activity status. When the unit is operating properly, the Power LED is steadily illuminated, and the Activity LED will pulse.

Figure 2-4: ASG Guard II 16-Port Rear Panel

Figure 2-5: ASG Guard II 28-Port Rear Panel

ASG Guard II 16/28-Port Rear Panel Features	
POWER INPUT	The 16/28-Port ASG Guard II utilizes a standard PC cable power source input.
POWER BUTTON/LED	The Power button is located on the rear panel, adjacent to the power source input. When the Guard is powered on, the green LED beneath the button is illuminated.
SENSOR INPUTS	The 16/28-Port ASG Guard II provides three RJ45 sensor inputs: two temperature probes and one 0-5V analog input. A 6-pin Euroblock connector for the 2 simple relay outputs and a 10-pin Euroblock connector for the 5 contact closure inputs are also supported.
AUX PORT	The 16/28-Port ASG Guard II provides an RJ45 AUX port connector for local administrative access to the device. A standard 9-pin RS232 serial cable, with the enclosed modular RJ45 adapter, is used to connect a PC or terminal to the Guard.
HOST PORTS	The 16/28-Port ASG Guard II provides an RJ45 interface for up to 28 serially connected devices such as PBXs and routers. Host ports 1 through 4 are located directly beneath the contact closure inputs, while the remaining host ports are located on the right of the rear panel.
MODEMS	The MODEMS connector provides single RJ11 connectivity for up to two internal PCMCIA modems.
10/100 ETHERNET	The “External” 10/100 Ethernet port provides connectivity to a router interface. The “Internal” 10/100 Ethernet port provides connectivity for one internal LAN interface, but can also be connected to a hub for increased IP port density.

2.3 Package Contents

Every ASG Guard II ships with the following package contents:

- ✓ PROCOMM for Windows CD
- ✓ K003 Cable Kit, which includes:
  - One 9-pin to 9-pin straight cable for Intuity, Conversant, CMS
  - One 9-pin to 25-pin straight cable for Definity INADS (marked DCE)
  - One 9-pin to 25-pin null cable for Definity SAT terminal – MAP D
- ✓ One 9-pin to 25-pin short cable
- ✓ 16/28 Port Guard II's only: one RJ11 Y-Cable
- ✓ Temperature probe
- ✓ Documentation CD containing comprehensive product documents
- ✓ Printed documentation: this document, and the ASG Guard Connectivity Guide

2.4 Supported Avaya Products

In addition to Avaya S8x00 Media Servers, the ASG Guard II is certified to integrate with the following Avaya products:

- Definity G3R
- Definity G3SI Prologix
- Intuity Audix RMB, including: Intuity Conversant, RMB, Avaya IR, UCS 1000, MMU
- Definity MapD
- Definity SAT Terminal
- OCTEL Aria and Serenade
- Merlin Magix and Legend

NOTE: Refer to the **ASG Guard Connectivity Guide** for detailed information.

3 ASG GUARD II INSTALLATION

This chapter covers the following topics:

3.1 Pre-Installation Checklist

Obtain the following material and information prior to installation:

✓ **Determine where the Guard II will be installed**, and obtain the appropriate rack mount equipment if necessary.

✓ **Make sure you have the appropriate cables** required to connect the Guard II to the S8x00. This includes obtaining a CAT5 Ethernet cable of appropriate length for the Guard, as well as the S8x00, if necessary.

✓ **Provision a POTS line at the site**. Obtain the appropriate RJ11 cables, depending on the number of phone line jacks and modem ports located on the rear panel of the Guard II. Refer to the table below:

One Modem Port *(16/28-port ASG Guard II)*	• One RJ11 cable to connect a single phone line that supports two modems. *OR* • One RJ11 compatible Y-cable to connect the Guard to two separate phone lines.
Two Modem Ports *(4-port ASG Guard II)*	• One RJ11 compatible Y-cable to for one phone line provisioned to support two modems. *OR* • Two RJ11 cables to connect each phone line to each modem.

✓ **Obtain the modem phone number(s):**

Modem #1 _____

Modem #2 _____

✓ **Obtain network provisioning information** for the ASG Guard II. This information will be used to configure the External Address of the Guard II IP interface. This information is typically provided by the customer's network provisioning personnel.

IP Address _____

Subnet Mask _____

Gateway _____

✓ Obtain the PPP address that Avaya will use when dialing into the Guard II and establishing a PPP session. This information is obtained from Avaya.

PPP Address _____

✓ **Obtain Avaya device IP address** information for each device to be protected by the Guard II. The first entry is for example purposes only. The Avaya IP address is obtained by contacting Avaya, and the Customer IP Address is typically obtained from the customer's network provisioning personnel.

NOTE: When integrating a single S8x00 Media server with an ASG Guard II, you are actually establishing connectivity between the Guard and three separate Customer IP addresses. S8x00 Media Servers are deployed as a set of two servers for redundancy. Each server is assigned a real and unique IP address, as well as one virtual IP address that is used by the active server. **Each address must be defined as a separate device.** This procedure is covered in Chapter 4.

	Device Name	**Avaya IP Address**	**Customer IP Address**
Ex.	***S8700SRV1***	***10.1.1.37***	***192.1.1.4***
1			
2			
3			
4			

✓ **Obtain a laptop with a terminal application and appropriate cable** to connect to the AUX port of the ASG Guard.

3.2 ASG Guard II Physical Installation

To install the ASG Guard:

1. Place the Guard in the selected location.

   NOTE: To rack-mount the unit, perform the following:

   - Place a "wing" on each side panel of the ASG Guard/ASG Guard Plus.
   - Secure the wings by inserting and tightening two screws in the front panel wing and two screws in the bottom panel wing. The wings are now attached. (NOTE: a. says side panel and b. says front and bottom)
   - Place the Guard in the rack.

2. Connect the PC or terminal to the AUX port using a standard 9-pin RS-232C serial cable:

   - Connect the serial cable to a serial port on the terminal or computer.
   - Connect the serial cable to the AUX Port connector on the ASG Guard/ASG Guard Plus. Both the ASG Guard and ASG Guard Plus are equipped with AUX Ports located on the front panel. The ASG Guard Plus also has an AUX Port located on its rear panel.

3. If you are serially connecting any protected equipment, refer to the ASG Guard Connectivity guide for the appropriate cabling and connection instructions. Serial connectivity is not related to the S8x00 Media Server integration, and is not covered in this document.
4. Connect analog telephone lines to the appropriate RJ11 modem port(s).
5. Connect a CAT5 network cable to the 10-Base-T port on the 4-port Guard II, or the "External" Ethernet port on the 16/28-port Guard II. If you are installing a unit with the HUB Expansion Option (material code 174007), connect the network cable and appropriate devices to one of the RJ 45 connectors on the back of the HUB.
6. Connect the power supply.

NOTE: The ASG Guard II supports physical connectivity of networked devices to its internal Ethernet port. The ASG Guard II and S8x00 Media Server integration require VIRTUAL connections only; therefore, this type of connectivity is not covered in this document. For more information on connecting networked devices to the Guard II internal Ethernet port(s), refer to the user documentation.

3.3 Powering Up the ASG Guard II

Four Port ASG Guard II

Turn the key on the front panel of the Guard clockwise to the horizontal position. The red Power LED lights immediately and the System and Port LED lights during the power-up sequence. After about three seconds, the LEDs flash three times. A few seconds later, the host port LEDs sequentially light. After thirty to ninety seconds (depending on the number of host ports), initialization is complete. The Power, Clear for Alarm/Event/File and host port DTR LEDs remain lit to indicate the Guard's status. The Pulse LED (labeled with a heart) flashes periodically, indicating that the device is operating properly.

Sixteen and Twenty-Eight Port Guards

Press the "power" button located on the rear panel of the device. The "Power" LED located on the front panel flashes briefly and then stays on when the initialization sequence is complete.

NOTE: To power a Guard that supports a 16V AC power supply:

- Connect the 6-pin modular jack on one end of the wall pack cable to the 16 VAC POWER connector located on the rear panel of the ASG Guard/ASG Guard Plus.
- Connect the power supply to a standard 120-volt AC power source or to a standard 220 VAC power source.
- If the unit has the optional Grounding location on the back panel, indicated by the ground symbol or the abbreviation 'GND', the unit may be grounded to the equipment frame in which it is installed. Ground the unit to the equipment frame with an appropriate wire or braided strap, #8 lock washer, and a screw size #8 - #32 with a length not to exceed 0.5 inches.

3.4 Connecting to the AUX Port

Once you have physically installed the appliance, you should connect your laptop to the AUX port and start a terminal application, such as Hyperterm or ProComm that will allow you to communicate serially with the Guard.

Four Port Guard II

Connect a 9-pin RS232 cable from the appropriate COM port on your computer to the AUX port, located on the front panel of the device. Start the terminal application. If the Guard is already powered on, press ENTER several times until you are prompted to log in as the default user. Answer YES to proceed.

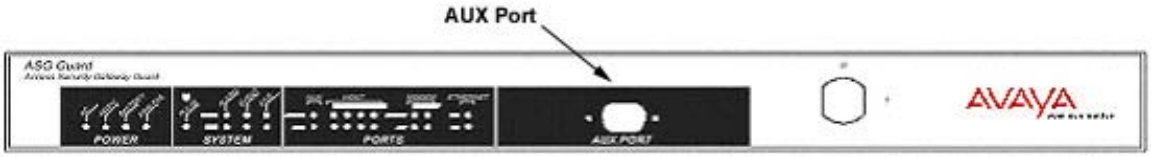

Figure 3-1: AUX Port, located on the four port ASG Guard II

Sixteen and Twenty-Eight Port Guards

Connect an RJ45 to 9-Pin serial cable to the RJ45 AUX port located on the back of the Guard. Connect the 9-Pin end to the COM port of your computer.

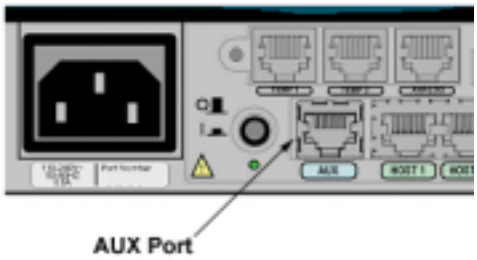

Figure 3-2: AUX Port, located on the sixteen and twenty-eight port ASG Guard II

3.5 International Modem Setup

Installations in the domestic United States do not require modifications to the modem settings. For international installations, you must set the modem to operate using the country codes that correspond to the location in which it is installed. To do this, you simply change a modem setting.

To set up a modem for international use:

1. Access the Guard by connecting to the AUX port as described in Section 3.5.
2. At the Guard's prompt, type the command SM and the modem number. The Set Modem Port Parameters dialog begins.
3. Press Enter to bypass each parameter that you are not modifying.
4. At the "Country" parameter, use the Space key to select the country in which the Guard is, or will be installed.
5. Press Enter to bypass the rest of the parameters and accept your changes.

NOTE: For more information on configuring modem port parameters, refer to the ASG Guard User's Guide.

3.6 Host Port Connectivity

Connectivity between the ASG Guard II host ports and other Avaya products as listed in Section 2.4 “Supported Avaya Products” is covered in detail in the ASG Guard Connectivity Guide that should have been enclosed with this document.

4 ASG GUARD II CONFIGURATION

This chapter covers the following topics:

4.1 Setting Network Parameters

In this section, you will learn how to manually set the basic network parameters needed to use the ASG Guard II. In some cases, the Guard II may be administered by ASG Guardian or PRIISMS management software. If this applies to you, refer to the Appendix "Using the Guard II Configuration Wizard."

As part of the installation process, you should have connected a PC or terminal to the AUX port of the appliance. You can also configure the appliance by connecting to it with a modem or via telnet. For the purpose of these instructions, configuration is performed through the Guard's AUX port.

To set network parameters:

1. Type the command SNP (*Set Network Parameters*) and press Enter; the **Set Network Params** dialog begins.
2. Select Group #1 "Network Initialization Params."
3. Answer "NO" when prompted to restore factory defaults and press Enter.
4. Press Enter to accept the defaults for *Internal Address*, *Mask*, and *Gateway*. Note that the Gateway field is typically blank, and can remain that way.
5. Type the *External Address*, *Mask*, and *Gateway* you specified in Section 3.1, pressing Enter after each entry. This is the actual LAN address of the Guard II.
6. Use one of the methods below to obtain the address used to establish a PPP session upon dialing into the Guard II.

For New Installations	The PPP address is included within the installation script provided by the ART registration system. The output will look like this: **RAS IP address: 10.1.8.199**
For Existing Installations	At one of the media servers, execute the following command: **Less /etc/ppp/ipaddrs** The output will look like this: **10.1.1.37:10.1.1.38** Use the first IP address.

7. Press Enter through the rest of the parameters in the group. When finished, the Guard II returns to a command prompt.

```
Restore Factory Defaults ?          No
Internal Address                    192.168.0.1
         Mask                       255.255.255.0
         Gateway
External Address                    10.10.2.137
         Mask                       255.255.0.0
         Gateway                    10.10.1.1
PPTP Local Address                  192.168.1.1
    Remote Addresses                192.168.1.2-50
    Authentication Class            NONE
PPP Address                         192.9.200.3
```

Figure 4-1: Set Network Parameters

4.2 Enabling Alarm Delivery

The ASG Guard II consists of several system parameters that define how the Guard is expected to function. System Parameters commands are located in the "System" family of commands, whose menu is displayed by pressing "S" at the command prompt of the Guard. To enable alarm delivery from the S8x00 devices to Avaya Expert Systems, a "Home Phone Number" parameters must be specified.

NOTE: Refer to the ASG Guard II User's Guide for additional information on setting system parameters.

To specify a home phone number:

1. At the command prompt, type SSP; a list of system parameter categories displays.
2. Select Group 3, "Action Routine Parameters" and press Enter; the **Action Routine Parameters** dialog displays.
3. Enter the phone number for the Avaya Alarm Receiver; ensure that the formatting of the telephone number adheres to the proper format. Refer to the table below to determine which phone number to use:

EMEA COE	080012345679
USA	1-800-535-3573

The numbers listed below can be used to verify alarm reception. They are NOT the alarm receiver numbers.

U.S. 1-800-242-2121, prompt 3 Australia - +612-9352-9151 Bahrain - +973-218-266; Budapest +36-1238-8334 Hong Kong +852-3121-6423; Japan +813-5575-8800	Carribean/Latin America: +786-331-0860 Canada: +1 800 387-4268 Moscow: +7-095-363-6780 France: +33-241-534-000 UK: +44 1483-308-000 Singapore +65-6872-8686;

4. Press Enter through the remaining parameters to save your settings.

4.3 Configuring Avaya Device IP Addresses

The ASG Guard II contains a special set of commands and action routines that enables you to configure Avaya IP-connected devices like the S8x00 series. Locate these commands by pressing "X" followed by Enter at the command prompt; a list of "User Commands" for the S8x00 displays. The table below provides an overview of these commands.

Command	Description
CONT	Provides connectivity to Avaya IP devices via telnet.
AAIP	Add Avaya IP device. **NOTE:** The customer must assign this address, and only CMASTER level users can actually add an Avaya IP address.
CAIP	Change Avaya IP device.
XAIP	Delete Avaya IP device.
LAIP	List Avaya IP devices.
TRAPTASK	An action routine that is used to start or stop the SNMP Trap Proxy. It can also be invoked as a command using the following syntax: TRAPTASK START (or STOP).
AINIT	An action routine that initializes proxy rules. This is part of the Guard II default configuration. No action is necessary.
ADDUMP	Download a file that contains the parameters set for the Avaya IP devices.
ADCONFIG	Load a file that contains configuration information for Avaya IP devices.

4.4 Administering an Avaya IP Device

NOTE: Only CMASTER level users can add Avaya IP devices.

To add an Avaya IP device:

1. Type the command AAIP (Add Avaya IP Device) and press Enter; the **Add Avaya IP Device** dialog begins.
2. Type a unique alphanumeric device name and press Enter.
3. Enter the actual IP address of the S8x00. You should have already obtained this information from the customer's network provisioning personnel.
4. Enter the Avaya IP address you should have already obtained from Expert Systems staff. The Avaya IP address is translated into the actual IP address when Expert Systems connects through PPP.
5. Specify the ports that should be forwarded to the Avaya device. Port numbers can be comma or space delimited. By default, the following ports are specified: 23 and 5023 (telnet), 21 (FTP), 80 (HTTP), and 443 (HTTPS/SSL). These ports may need to be removed, as specified by the customer. Ports 23 and 5023 are treated differently: attempt to telnet to these ports will be redirected to ASG Guard II login. Once authenticated into ASG Guard II, use command CONT to actually telnet to the Avaya devices.

   TIP: Use the command CAIP (*Change Avaya IP Device*) to modify the parameters set when you added an IP device. Use the XAIP (*Delete Avaya IP Device*) command to remove the record for a particular IP device. Use the LAIP (List Avaya IP Device) command to list information for any Avaya IP devices that have already been defined.

4.5 Enabling Telnet on the ASG Guard II

Before you can telnet to devices protected by the ASG Guard II, you must first ensure that the telnet capability of the appliance is enabled.

To enable telnet:

1. Type SNP at the command prompt, and select option #5 “Telnet Params.”
2. At the “Telnet Service Type” parameters, use the Space key to select “Both” from the available options. This enables telnet on the Guard II for as both a telnet client and telnet server.
3. Press Enter to save your settings.

4.6 Connecting to IP Devices

Syntax: CONT (device_name | avaya_ip_addr), [port=23]

The first argument can be either device name or Avaya IP address, as defined by AAIP command. The second argument specifies IP port. If not specified, telnet connection will be established to port 23. Only ports administered for the device will be accessible.

The CONT command enables you to establish a telnet session with an Avaya IP device. CONT sessions are subject to session buffering, if that option is enabled in the user’s profile. The session is also subject to command filter if enabled with the commands SHFP (*Set Host Command Filter Parameters*) or AHFS (*Add Host Filter String*).

NOTE: Refer to the ASG Guard II User’s Guide for more information on these additional commands.

To connect to an Avaya IP device:

1. Execute the CONT command using one of the following methods:
   - Type CONT and press Enter. When prompted, type the Avaya IP device name and press enter to invoke telnet.

     OR
   - Type the following command syntax and press Enter:

     Syntax: CONT (device_name | avaya_ip_addr), [port=23]

     NOTE: The first argument can be either device name or Avaya IP address, as defined by AAIP command. The second argument specifies IP port. If not specified, telnet connection will be established to port 23. Only ports administered for the device will be accessible.

2. Once telnet is invoked, proceed with the login process on the Avaya IP device.

```
Ser5011224286>cont

--- Telnet to Avaya device ---
   Name             Comment
   ================ ================
   S87MCA           Primary 8700
   S87MCB           Secondary 8700

Device name                        s87mca
Invoking telnet. Type ^A to exit
```

Figure 4-2: CONT Example

4.7 Saving and Loading Avaya IP Device Information

The ADDUMP command enables you to download a delimited list of IP address and port information for each Avaya IP device defined on the ASG Guard II. The ADCONFIG command enables you to load a list of predefined Avaya IP devices onto an ASG Guard II.

4.7.1 Using the ADDUMP Command

To save a list of Avaya IP devices from an ASG Guard II:

1. At the command prompt, type the command ADDUMP and press Enter; the Dump Avaya Devices dialog begins.
2. Press Enter to receive the configuration dump; the ASG Guard II dumps a delimited list containing the Avaya and external IP addresses, ports to be forwarded, and any comments.
3. Capture the text and save it to a file.

4.7.2 Using the ADCONFIG Command

To load a list of Avaya IP devices to an ASG Guard II:

1. If the predefined list of Avaya IP devices resides in a text file, XMODEM the file to the ASG Guard II. Refer to the ASG Guard II User's Guide for more information on sending files via XMODEM.
2. At the command prompt, type ADCONFIG <filename>. The contents of the file are loaded onto the ASG Guard II.
3. Type the command LAIP to list the Avaya IP devices you just loaded onto the Guard.

4.8 Provisioning the ASG Guard II

Once you have physically installed the ASG Guard and either physically or virtually connected the protected equipment, you must contact the TSO/COE at 1-800-248-1111 to provision the Guard. Follow the prompts to reach a member of the Account Support Team.

As part of the provisioning process, the TSO/COE will perform such functions as:

- Build the customer's Equipment and Guard records in proprietary Avaya systems.
- Dial into the Guard and install a standard configuration script.
- Add default TSO/COE user table to Guard for remote support.
- Set specific system parameters.

4.9 Modifying the Avaya S8X00 Platform to Work With the ASG Guard II

In some cases you may need to modify particular settings on the protected platform to ensure proper functionality. Use the chart below to determine whether or not the platform you are connecting requires additional modifications.

Product	Modification
S8300	The "SNMP Manager" should be set to the external IP address of the ASG Guard II.
S8700	

5 ADDITIONAL CONFIGURATION

This chapter covers the following topics:

5.1 Adding a CMaster User

This section provides basic instructions for adding a CMaster access level user. Refer to the ASG Guard II User's Guide for additional information on modifying the user database.

To add a CMaster user:

1. At the prompt, enter the AU (Add User) command. The "Add User" dialog begins.
2. Specify a unique user name and press enter; do not use spaces.
3. Use the Space key to select the CMASTER access level. Refer to the ASG Guard User's Guide for a definition of the various types of access levels.
4. Press Enter to bypass the Block Access, Sessions Allowed, and User Expiration Date parameters.
5. Use the Space key to select from one of the following Primary Authentication Methods: *ASG Key*, *Pager*, or *Password/Callback*.

   NOTE: See Section 5.2 for information on setting up an ASG Key.
6. Press Enter to bypass the Secondary Authentication Method, Auto Execute Command, Comments, and Options parameters.
7. When prompted, enter the additional information required for the authentication method you chose. Press Enter after each entry until complete. A log will display above the prompt indicating that the user was added successfully.

   NOTE: When adding a customer user, remember to advise the user of his/her user ID and authentication information.

```
Ser#2090114746>au
--- Add User ---
User Name                                Guard-CMaster
Access Class                          CMaster
Block Access                          No
Sessions Allowed (blank=unlimited)
User Expiration Date                  MM/DD/YY
Primary Authentication Method         ASG Key
Secondary Authentication Method       None
Auto Execute Command
Comments:
Options:

-- ASGKey Details --
Encryption Key Source                 Randomly Generated
Enter These Digits as Key1 or Key2: 6576 4334 =  3520 4215 =  4040 =
Test Challenge: 1234567 ...Reply:  421-7876

Press <ENTER> to Continue
06/04/03 10:32:14 4B33 [T1] User: GUARD-CMASTER Added - O.K.
Ser#2090114746>
```

Figure 5-1: Add User Example

5.2 ASG Key Setup

If you are adding a CMASTER user who will user an ASG Key to authenticate to the Guard, you must configure the ASG Key with the secret key that is generated by the ASG Guard when you created the user's profile.

To configure an ASG Key:

1. Press the ***ON/C key***. The 0 displays, indicating it is in calculator mode.
2. Press the ***M+ key***. This places the ASG Key into the Set PIN mode. At this point, the screen should display **"SET PIN 1"**. If it does not, the key has been previously programmed. To reinitialize the ASG Key for programming, remote the battery for 30 seconds.
3. Enter the digits of your **PIN**. A PIN may have from 4 to 8 digits. Check the display to see that your PIN has been entered correctly. If a mistake has been made, do not proceed to the next step. Press the ***CE key*** and re-enter the **PIN**.
4. Press the **= *key***. This sets your PIN into your ASG Key.
5. When the ASG Key prompts for a **second PIN**, press the **= *key***.
6. The screen will now prompt for the **SET KEY 1**. This should be the same secret key entered into the ASG Guard/ASG Guard Plus. Entering the secret key is a 3-step process as follows: Enter the first 8 digits of the secret key as entered into the ASG Guard/ASG Guard Plus. There is no need to enter the ***"-"***. Press the ***"=" sign*** as indicated. The screen will now prompt for the **SET KEY 1.** Enter the second 8 digits of the secret key. Press the ***"=" sign*** as indicated. The screen will now prompt for the **SET KEY 1.** Enter the final 4 digits of the secret key. Press the ***"=" sign*** as indicated.
7. After the first secret key has been entered, the ASG Key will prompt to **SET KEY 2**. Press the **= *key***.
8. At this point, the ASG Key has been programmed. To test that the key has been properly programmed, use the test challenge.
9. Turn on the ASG Key.
10. Press the ***RED key***.
11. Enter your PIN followed by the **= *key***.
12. Enter the test challenge of **1234567** followed by the **= *key***.
13. The ASG Key will give a response, which should match the response given by the ASG Guard/ASG Guard Plus. If they match, the ASG Key has been properly programmed.

    NOTE: If the responses do not match, retry the test challenge. If it they do not match again reset the ASG Key by removing the batteries. Then reprogram the ASG Key as outlined above

6 APPENDIX

This chapter covers the following topics:

6.1 Using the ASG Guard II Configuration Wizard

The ASG Guard II provides a Configuration Wizard that enables you to quickly and easily configure the appliance's network settings. For the purposes of configuring ASG Guard II network parameters for use with ASG Guardian software, you must select the "Secure Proxy" configuration option.

NOTE: Throughout these instructions and the prompts on the appliance, *PRIISMS* is synonymous with *ASG Guardian*.

To configure the ASG Guard II for Secure Proxy:

1. At the prompt, type WIZARD. The **Initial Setup Wizard** displays.
2. Select "Secure Proxy," using the space key and press Enter. The Wizard prompts you for the external IP address (*IP Address*), network mask (*Mask*) and default gateway (*Gateway*).

IP Address	10.50.20.20
Mask	255.255.0.0
Default Gateway	10.50.1.1
PPP Address	192.9.200.3

3. Enter the addresses you noted in Section 3.1, pressing Enter after each entry.
4. Next, you are prompted whether or not to accept the default PRIISMS IPSec key. If you answer NO you will be prompted to select an authorization type and enter the corresponding key. If you wish to specify your own PRIISMS IPSec key, you must select the "Secret" authorization type, and then enter the secret key.
5. Answer YES when asked to use the default PRIISMS IPSec Key. If you answer NO you must ensure that PRIISMS is configured with the same Secret Key you create for the ASG Guard II.
6. Specify the date and time format, pressing Enter after each entry.
7. After the last date entry option, you will be informed that the new settings will be applied. If you are ready to proceed, answer "Yes" when prompted. A "Configuration Successful" prompt displays when the process is complete.

   TIP: It is important that you configure the router/firewall that routes the management subnet to block Telnet traffic emanating from any IP address other than the ASG Guard II.

6.2 Determining the ASG Guard II Configuration File Version

There may be cases where you need to determine the version of the configuration file loaded on the ASG Guard II.

To check the configuration file version:

1. Type the command SAI; the **Schedule Action Item** dialog displays.
2. Use the Space key to select "VERSION" and press Enter through the rest of the parameters, accepting the defaults. Version information displays in the log above the command prompt of the ASG Guard II.

```
Ser5011224286>sai

--- Schedule Action Item ---

Action Routine                VERSION
Parameters
Schedule Date (<ENTER> = today, MM/DD/YY
 or 'nn' days from today)
Schedule Time (<ENTER> = now, hh:mm
or 'nn' minutes from now)
Event                         SysOp Generated
Comment
Severity                      Info

06/26/03 09:49:35 545E {I} [T1:24] Schedule Action Item
06/26/03 09:49:52 71AE {I} [T1:24] Schedule Action Item - O.K.
06/26/03 09:49:53 3592 {I} ** Avaya **,I
06/26/03 09:49:53 64E3 {I} ** CONFIG FILE: A8700.CFG 03/24/2003 Ver. 1.0**
06/26/03 09:49:53 D53F {I} ** For ASG Guard II ver 5.1.4+ **
Ser5011224286>
```

Figure 6-1: Schedule Action Item (Version) Example

6.3 How Automated Alarm Delivery Works

The ASG Guard II is pre-configured with action items that automate the delivery of SNMP alarms generated by the S8x00 media server to Avaya Expert Systems. *Action Items* utilize specific *Action Routines* to respond to events that are triggered on the ASG Guard II.

The S8x00 Media Server generates SNMP traps that contain alarms and sends them to the ASG Guard II. The Guard II's trap proxy receives the alarms and stores the IP address, timestamp, and alarm message in a file and generates the event, **#SENDALL <filename>**. The PHONTRAP action routine runs when this event is generated, and delivers the alarm to Expert Systems. Upon receipt of the alarm, Expert Systems sends a delivery acknowledgment to the Guard II, which generates an **.ACKTRAP <filename>** event. The XMLACK action routine runs when this event is generated, which sends a delivery confirmation to the S8x00 Media Server. If delivery confirmation is not received from Expert Systems, a .NACKTRAP event is generated. In both cases, these events are logged on the Guard II.

To view the list of predefined action routines on the Guard II, type the command LA (*List Action Items*). See the example, below:

```
Ser5011224286>la
--- List Action Items ---
     Alarm:           Routine: Parameters:
                      Severity: Comments:

  1) #SENDALL         PHONTRAP
                      Info
  2) #SENDERR         LOG
                      E
  3) .ACKTRAP         XMLACK
                      Info
  4) .COPROC.INITOK   DOLIST
                      Info
  5) .COPROC.INITOK.1 AINIT
                      Info     Initialize rules for Avaya
  6) .COPROC.INITOK.2 TRAPTASK START
                      Info     Start trap capture
-- End of List --

06/30/03 16:16:29 57B9 {I} [T1:26] List Action Items
Ser5011224286>
```

Figure 6-2: LA (List Action Item) Example

The following subsections provide instructions for defining action items for alarm delivery action routines. To create a new action item, type the command AA (*Add Action Item*).

6.3.1 AINIT – Initialize Rules for Avaya Devices

The AINIT action routine initializes the IP rules for all defined Avaya IP devices. This includes rules for forwarding IP ports, redirecting telnet ports to the ASG Guard II, and forwarding SNMP traps for dialup delivery to Avaya Expert Systems.

NOTE: Both the AINIT and TRAPTASK action routine (discussed in Section 6.3.2) should run when the .COPROC.INITOK event is generated. To make this happen, you must first create an action item that utilizes the "DOLIST" action routine. See the example below:

```
ASG_GuardII>aa

 --- Add Action Item ---

Alarm                    .COPROC.INITOK
Action Routine           DOLIST
Routine Parameters
Comment
Severity                 Info
```

Figure 6-3: DOLIST Action Item

To create an action item that utilizes the AINIT action routine:

- Specify the event **.COPROC.INITOK.1** in the "Alarm" parameter.
- Leave the "Routine Parameters" field blank.
- Enter comments, if desired.
- Use the Space key to select **Info** for the "Severity" parameter.

See the example below:

```
ASG_GuardII>aa

 --- Add Action Item ---

Alarm                    .COPROC.INITOK.1
Action Routine           AINIT
Routine Parameters
Comment                  Initialize IP Rules
Severity                 Info
```

Figure 6-4: AINIT Action Item

6.3.2 TRAPTASK - Start/Stop SNMP Trap Proxy

The TRAPTASK action routine is used to start or stop the SNMP Trap Proxy. SNMP traps are generated by the S8x00 Media Server, received by the ASG Guard II, and written to a file. Like the AINIT action routine discussed in Section 6.3.1, TRAPTASK should be scheduled to run on the .COPROC.INITOK event.

To create an action item that utilizes the TRAPTASK action routine:

- Specify the event **.COPROC.INITOK.2** in the "Alarm" parameter.
- Enter **START** in the "Routine Parameters" field.
- Enter comments, if desired.
- Use the Space key to select **Info** as the "Severity" parameter.

See below for an example:

```
ASG_GuardII>aa

 --- Add Action Item ---

Alarm                    .COPROC.INITOK.2
Action Routine           TRAPTASK
Routine Parameters       START
Comment                  Start/stop SNMP Trap
                         Proxy
Severity                 Info
```

Figure 6-5: TRAPTASK Action Item

NOTE: This action item can also be invoked as a command by using the following syntax: **TRAPTASK START** (or STOP).

6.3.3 PHONTRAP – Deliver S8x00 Alarms

The PHONTRAP action routine dials the Avaya Expert Systems server and delivers the S8x00 alarm with the message specified in the filename field. The Avaya Expert Systems phone number is specified using the SSP (Set System Parameter) command. (See Section 4.2 of this document, "Enabling Alarm Delivery.") An **.ACKTRAP <filename>** event is generated upon successful alarm delivery, and a **.NACKTRAP <filename>** event is generated if alarm delivery has failed. When scheduling an action item that utilizes the PHONTRAP action routine, specify the event #SENDALL and select "Info" for the Severity parameter. See below for an example:

```
ASG_GuardII>aa

 --- Add Action Item ---

Alarm                    #SENDALL
Action Routine           PHONTRAP
Routine Parameters
Comment
Severity                 Info
```

Figure 6-6: PHONTRAP Action Item

6.3.4 XMLACK – Sends Alarm Delivery Confirmation

Upon successful delivery of an alarm to Avaya Expert Systems, an .ACKTRAP event and a response SNMP trap are generated. The XMLACK action routine runs when the .ACKTRAP event is generated, and delivers the SNMP trap back to the S8x00, confirming successful alarm delivery.

See below for an example:

```
ASG_GuardII>aa

 --- Add Action Item ---

Alarm                    .ACKTRAP
Action Routine           XMLACK
Routine Parameters
Comment
Severity                 Info
```

Figure 6-7: XMLACK Action Item