



ASG Defender Setup/Integration Guide

Version 1.0.0

2/10/06

Avaya, Inc.
211 Mt. Airy Rd.
Basking Ridge, NJ 07920
www.avaya.com

2006 Avaya Inc.
All Rights Reserved
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 Defender 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:	Defender 2-Port: 95-250 V AC @ 0.6A, 47-63 Hz
	Defender 4-Port: 100-240 V AC @ 1.8A, 50-60 Hz

The power transformer supplied with this product has these characteristics.

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

Table of Contents

- 1. Introduction 1-1**
 - 1.1 Document Overview 1-1
 - 1.2 Audience Assumptions 1-2
- 2. Hardware Overview 2-1**
 - 2.1 ASG Defender Introduction 2-1
 - 2.2 ASG Defender Features 2-1
 - 2.3 ASG Defender Package Contents 2-5
 - 2.4 Supported Avaya Products 2-6
- 3. ASG Defender Installation 3-1**
 - 3.1 ASG Defender Installation Checklist 3-2
 - 3.2 Collect Information to Prepare for Defender Setup/Installation 3-3
 - 3.3 ASG Defender Physical Installation 3-5
 - 3.4 Start a Local Admin Session on the AUX Port 3-7
 - 3.5 Setup ASG Defender with Avaya Ethernet Products 3-12
 - 3.6 Setup ASG Defender with Avaya Serial Products 3-21
 - 3.7 Register the ASG Defender with the Global Technical Services Group 3-24
- Appendix A: Defender to Avaya Equipment Cable and Port RequirementsA-1**
- Appendix B: Cable and Connector PinoutsB-1**
 - B.1 AUX and Host Port Pinouts B-1
 - B.2 Standard Serial Cables B-2

List of Figures

Figure 1-1: ASG Defender Faceplate	1-2
Figure 2-1: ASG Defender Front Panel	2-2
Figure 2-2: Defender 4-Port Rear Panel	2-3
Figure 2-3: Defender 2-Port Rear Panel	2-4
Figure 3-1: Defender Wall-mount Unit	3-5
Figure 3-2: Cable Connections	3-6
Figure 3-3: ASG Defender Banner	3-8
Figure 3-4: Set Date and Time	3-9
Figure 3-5: Add user example	3-11
Figure 3-6: Set Network Parameters	3-13
Figure 3-7: Set Networking Services Screen	3-15
Figure 3-8: Administering an Avaya IP Device Screen	3-17
Figure 3-9: Connecting to an Avaya IP Device using the CONHOST Command	3-20
Figure 3-10: Setting Host Port Parameters	3-22
Figure B-1: RJ-45 Serial Pinout	B-1

List of Tables

Table 2-1: ASG Defender Hardware	2-1
Table 2-2: Defender 4-Port Rear Panel Features	2-3
Table 2-3: Defender 2-Port Rear Panel Features	2-4
Table 2-4: Defender Package Contents	2-5
Table 3-1: Defender Installation Checklist	3-2
Table 3-2: Avaya IP Commands	3-16
Table 3-3: ASG Defender Host Port Settings	3-21

1. Introduction

This section covers the following topics:

- Document Overview
- Audience Assumptions
- Getting Help

1.1 Document Overview

The purpose of this document is to:

- Present an easy-to-follow guide for installation of the ASG Defender (referred to as the “Defender” throughout this document).
- Provide integration procedures between the ASG Defender and Avaya devices.

This document is an abbreviated guide. Additional information can be found in the *ASG Defender Administrator Guide*.

The Defender provides both secure remote access and device monitoring of Avaya devices such as the S8xx0 series media servers, Modular Messaging, Definity, Intuity, etc. Using a built-in firewall, the Defender offers remote access to the management interfaces of IP-enabled devices, while limiting connectivity to any other device located on the same network. The Defender provides a secure access path to the various management ports of Avaya devices through both PPP dialup sessions or IP connections. Individuals who access the Defender use a DES-based, two-factor authentication token called the ASG Key, which is available both as a software and hardware token.

The S8xx0 Media Servers and Modular Messaging generate SNMP traps containing INADS alarms that are sent to the ASG Defender. The ASG Defender 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 Defender sends a confirmation SNMP trap back to the originating S8xx0 device.

Devices, such as Definity, stream INADS alarms through a serial port. The Defender captures and forwards the alarms over dialup connections.

Figure 1-1 illustrates an example of the integration of the S8xx0 and Defender. The Defender will proxy any incoming Telnet, SSH, Web (thru PPP) and FTP sessions to the target device.

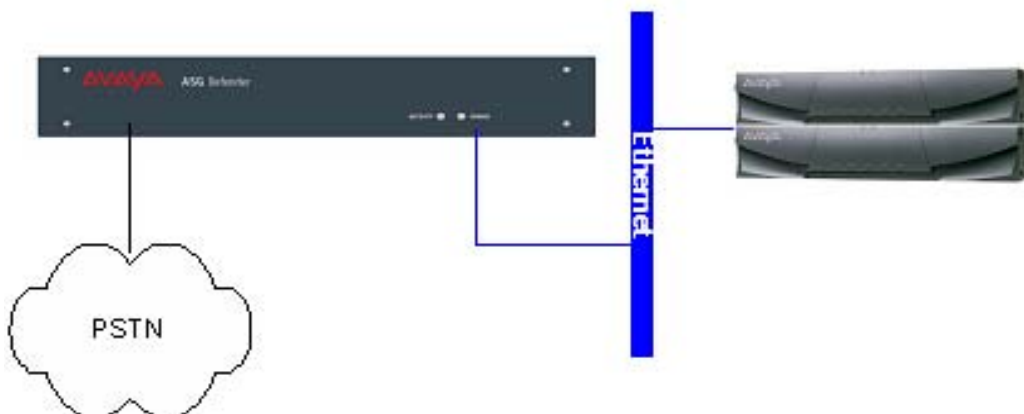


Figure 1-1: ASG Defender Faceplate

1.2 Audience Assumptions

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

1.2.1 Getting Help

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

Note: International sites should contact their regional Avaya Support Team.

2. Hardware Overview

This section covers the following topics:

- ASG Defender Introduction
- ASG Defender Physical Features
- Package Contents
- Supported Avaya Products

2.1 ASG Defender Introduction

The ASG Defender can securely access and manage S8xx0 switches. The ASG Defender is equipped with VPN access and a firewall for Avaya customers to define and restrict access to S8xx0 switches. In addition to securing Avaya's IP switches, the ASG Defender is certified to secure serially connected Definity, Octel, MAPD, CMS, etc. The ASG Defender can also monitor environmental conditions surrounding infrastructure elements by using analog sensors that measure conditions such as temperature, and humidity.

2.2 ASG Defender Features

Table 2-1 lists all Defender hardware configurations.

Table 2-1: ASG Defender Hardware

Features	Defender 2-Port	Defender 4-Port
Ethernet ports (10/100)	2	2
Modem	1-V92 56K bps	1-V92 56K bps
Host ports	2	4
Local Console Ports (AUX)	1	1
Maximum concurrent user sessions	16	16
Environmental monitoring	N/A	5 contact closures (sold separately) 1 Temperature probe is included
Power Requirements	100-240V~, 1.5 amp, 50-60 Hz	100-240V~, 1.5 amp, 50-60 Hz

Table 2-1: ASG Defender Hardware

Features	Defender 2-Port	Defender 4-Port
User Data Storage	A maximum of 94 Mb (This depends on the number of versions stored on the device.)	A maximum of 94 Mb (This depends on the number of versions stored on the device.)
USB ports	4 - for possible future use	4 - for possible future use
Wall Mount/Rack Mount	Wall Mount kit included Shelf required for rack mount	Wall Mount kit included Shelf required for rack mount
Weight	6 LBS	6 LBS
Dimensions (WxHxD)	Unit: 12" x 2.1" x 11" Box: 16" x 6" x 14"	Unit: 12" x 2.1" x 11" Box: 16" x 6" x 14"
Operating Temperature	32°F - 113°F (-4°C - °45 C)	32°F - 113°F (-4°C - °45 C)
Storage Temperature	-4°F - 140°F (-20°C - 60°C)	-4°F - 140°F (-20°C - 60°C)

2.2.1 ASG Defender Front Panel

The Defender Front Panel has Activity and Power LED indicators.



Figure 2-1: ASG Defender Front Panel

ASG Defender Front Panel Features	
LEDs	The LEDs display power and activity status. When the unit is operating properly, the blue Power LED is steadily illuminated; the amber Activity LED will light on initial startup. After startup, the Activity LED no longer illuminates.

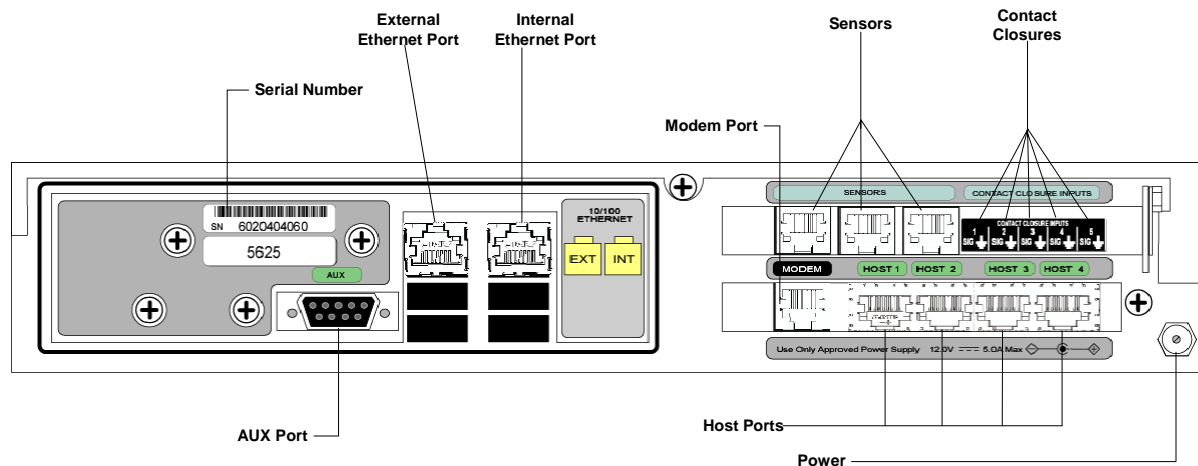


Figure 2-2: Defender 4-Port Rear Panel

Table 2-2: Defender 4-Port Rear Panel Features

Power Input	The Defender 4-Port utilizes a standard 120V PC cable power source input.
Sensor Inputs (Optional)	The Defender 4-Port provides five contact closures and three temperature probe inputs (one temperature probe is included).
AUX Port	The Defender 4-Port provides a DB-9 AUX port connector for local administrative access to the device. A standard 9-pin RS232 serial cable with a Null modem adapter is used to connect a PC or terminal to the Defender 4-Port.
Host Ports	The ASG Defender 4-Port provides an RJ-45 interface for up to four serially connected endpoints such as PBXs and routers, or two for the 2-Port.
Modem	The Modem connector provides single RJ-11 connectivity with one modem.
External Ethernet	This Ethernet port connects to the Enterprise network (such as a corporate LAN).
Internal Ethernet	This Ethernet port provides a secure subnet for endpoint network interfaces. An IP table's firewall secures traffic between the external and internal interface.

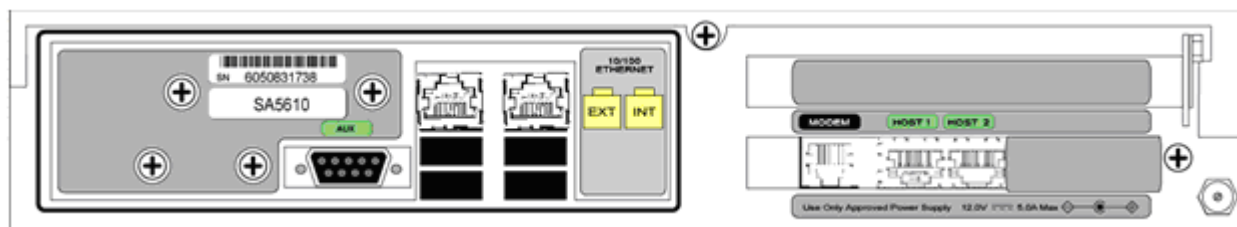


Figure 2-3: Defender 2-Port Rear Panel

Table 2-3: Defender 2-Port Rear Panel Features

Power Input	The Defender 2-Port utilizes a standard 120V PC cable power source input.
AUX Port	The Defender 2-Port provides a DB-9 AUX port connector for local administrative access to the device. A standard 9-pin RS232 serial cable with a Null modem adapter is used to connect a PC or terminal to the Defender.
Host Ports	The ASG Defender 2-Port provides an RJ-45 interface for up to two serially connected endpoints such as PBXs and routers.
Modem	The Modem connector provides single RJ-11 connectivity with one modem.
External Ethernet	This Ethernet port connects to the Enterprise network (such as a corporate LAN).
Internal Ethernet	This Ethernet port provides a secure subnet for endpoint network interfaces. An IP table's firewall secures traffic between the external and internal interface.

2.3 ASG Defender Package Contents

Table 2-4: Defender Package Contents

Product Part Number	Quantity	Description
ASG-K003-RJ45	1	ASG Cable Kit
Cable 1 (Assembled w/items below)	1	
WG-RJ45E9M	2	Adapter-RJ45 EIA to DB9 RS233
WC-CAT5S7G	1	Cable RJ45 CAT5 STR 7ft Green
WG-9FF	1	Gender Changer DB9 F-F
Cable 2 (Assembled w/items below)	1	
WG-RJ45E9M	1	Adapter-RJ45 EIA to DB9 RS233
WC-CAT5S7G	1	Cable RJ45 CAT5 STR 7ft Green
WG-RJ45E25M	1	Adapter-RJ45 EIA to DB25 RS232
Cable 3 (Assembled w/items below)	1	
WG-RJ45E9M	1	Adapter-RJ45 EIA to DB9 RS233
WC-CAT5S7G	1	Cable RJ45 CAT5 STR 7ft Green
WG-RJ45E25NM	1	Adapter-RJ45 EIA to DB25 RS232 NULL
TMP-56	1	5600 Temperature Sensor (ASG Defender 4-Port only)
Defender Standard Kit	1	
ZC-CBLCLAMP	1	Cable Clamp
WC-9MF6S	1	Cable DB9M to DB9F 6ft UL
ZZ-NULLMDM	1	NULL Modem coupler
WC-45E9MF7	1	RJ45EIA to DB9 RS232 CONV Female
WL-TEL7LNR	1	LCORD telephone 7ft
WC-45E9F	1	RJ45EIA to DB9 RS232 CONV CBL
Power supply	1	NA

Table 2-4: Defender Package Contents

Product Part Number	Quantity	Description
Power cord	1	NA
Wall mounts	2	NA
Black screws	4	NA
Avaya Documentation		
Integration/Setup Guide in hard copy form	1	
CD with all ASG GUARD II and Defender Documentation	1	
Note: Global shipments also include:		
IEC-UK	1	Power Cord UK
IEC-CE	1	Power Cord Europe

Note: The ASG Defender may be shipped with additional adapter kits and cables. These cables are for connecting additional serially connected devices. The number of cables included will vary across different sites.

2.4 Supported Avaya Products

In addition to Avaya S8xx0 Media Servers, the ASG Defender is certified to integrate with the following Avaya products:

- S8xx0 Media Servers (Communications Manager)
- Intuity Audix
- Intuity LX
- Definity G3r
- Definity G3si
- Prologix
- Definity MAPD
- Definity SAT Terminal
- CentreVue (CMS)
- IR
- Avaya Dialer
- Modular Messaging
- IP Office

3. ASG Defender Installation

This section covers the following topics:

- ASG Defender Installation Checklist
- Collecting Information for Defender Setup/Installation
- ASG Defender Physical Installation
- Starting a Local Admin Session on the AUX Port
- Setting up ASG Defender with Avaya Ethernet Products
- Setting up ASG Defender with Avaya Serial Products
- Registering the ASG Defender with the Global Technical Services (GTS) Group

3.1 ASG Defender Installation Checklist

Table 3-1: Defender Installation Checklist

Number	Description	Section	Complete	Technician Initials
1	Collect Information to prepare for Defender setup and installation. Eight steps including accessing the Automatic Registration Tool (ART).	Section 3.2		
2	ASG Defender Physical Installation	Section 3.3		
3	Start a Local Admin Session on the AUX Port	Section 3.4		
	Set Date and Time	Section 3.4.1		
	Add a CMaster user	Section 3.4.2		
	International Modem Setup (Optional)	Section 3.4.3		
4	Setup ASG Defender with Avaya Ethernet Products (S8xx0, Modular Messaging/Avaya Dialer) (Connections may be performed out of sequence.)	Section 3.5		
	Set Network Parameters (SNP)	Section 3.5.1		
	Set Network Services (SNS)	Section 3.5.2		
	Add Avaya IP (AAIP)	Section 3.5.3		
	Set Alarming Configuration (INADS delivery)	Section 3.5.5		
	Verify Connectivity of IP Devices	Section 3.5.6		
5	Setup ASG Defender with Avaya Serial Products for: Definity, Intuity, CMS, Prologix/IR	Section 3.6		
	Configure Defender host ports	Section 3.6.1		
	Modify the Avaya platform to interoperate with the ASG Defender (Optional)	Section 3.6.2		
	Verify Connectivity of Serial Devices	Section 3.6.3		
6	Register the ASG Defender with the Global Technical Services (GTS) Group	Section 3.7		

3.2 Collect Information to Prepare for Defender Setup/Installation

Obtain the following material and information prior to installation:

1. Determine where the Defender will be installed.
2. Determine which Avaya products will be connected to the Defender and ensure that you have the correct cables. Avaya products that are protected by the Defender are known as endpoints.
 - a. **For Avaya Serial Endpoints:** Appendix A lists each serial Avaya product and the necessary cables.
 - b. **For Avaya Ethernet Endpoints:** Typical installation connects both the Defender and the Avaya product to the customer LAN. Consult the appropriate Network Administration personnel on how to connect to this LAN.
3. Provision one POTS line at the site using the provided RJ-11 cable.
4. Obtain the modem phone number(s):

Modem 1	
---------	--

5. Obtain network-provisioning information for the ASG Defender. This information will be used to configure the External Address of the Defender IP interface. The customer's network provisioning personnel typically provide this information.

IP Address	
Subnet Mask	
Gateway	

6. Access the Automatic Registration Tool (ART) to obtain a Product ID (PID) and PPP address for the Defender
<http://ssdp.dr.avaya.com:7001/art/fwd/ARTstart.cgi?lang=en&country=US>

You will need the Sold To (FL) for the location the ASG Defender equipment will be associated with. You will also need the phone number for the maintenance line (INADS) connected to the ASG Defender for remote maintenance purposes.

Note: It is critical to use the ART tool to register any IP-connected device such as an S8xx0 prior to configuring the ASG Defender, in order to get the Product ID number. The PID number will be used when setting up the equipment in the ASG Defender. You must also get the PPP or RAS for S8700 Servers A and B, or the S8500.

PPP Address	
PPP Peer Address	

- Obtain Avaya device IP address information for each device to be protected by the Defender. (The first entry in the table below 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 S8xx0 Media server with an ASG Defender, you must actually establish connectivity between the Defender and three separate Customer IP addresses. S8xx0 Media Servers are deployed as a set of two servers for redundancy. Each server is assigned a real, 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 in the ASG Defender Avaya IP Table.

The Avaya IP table in the Defender can support up to 30 IP devices.

	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 or a dumb terminal to connect to the AUX port of the ASG Defender. The laptop will need a terminal application program such as Hyperterm and at least 1 COM port.

3.3 ASG Defender Physical Installation

To install the ASG Defender:

1. Place the ASG Defender on a rack shelf or wall-mount the unit. To wall-mount the unit, perform the following:
 - a. Place a "bracket" on each side panel of the Defender and insert and tighten two screws.
 - b. Mount the Defender on the wall with four appropriate wood screws. A wall-mount unit is shown in Figure 3-1.



Figure 3-1: Defender Wall-mount Unit

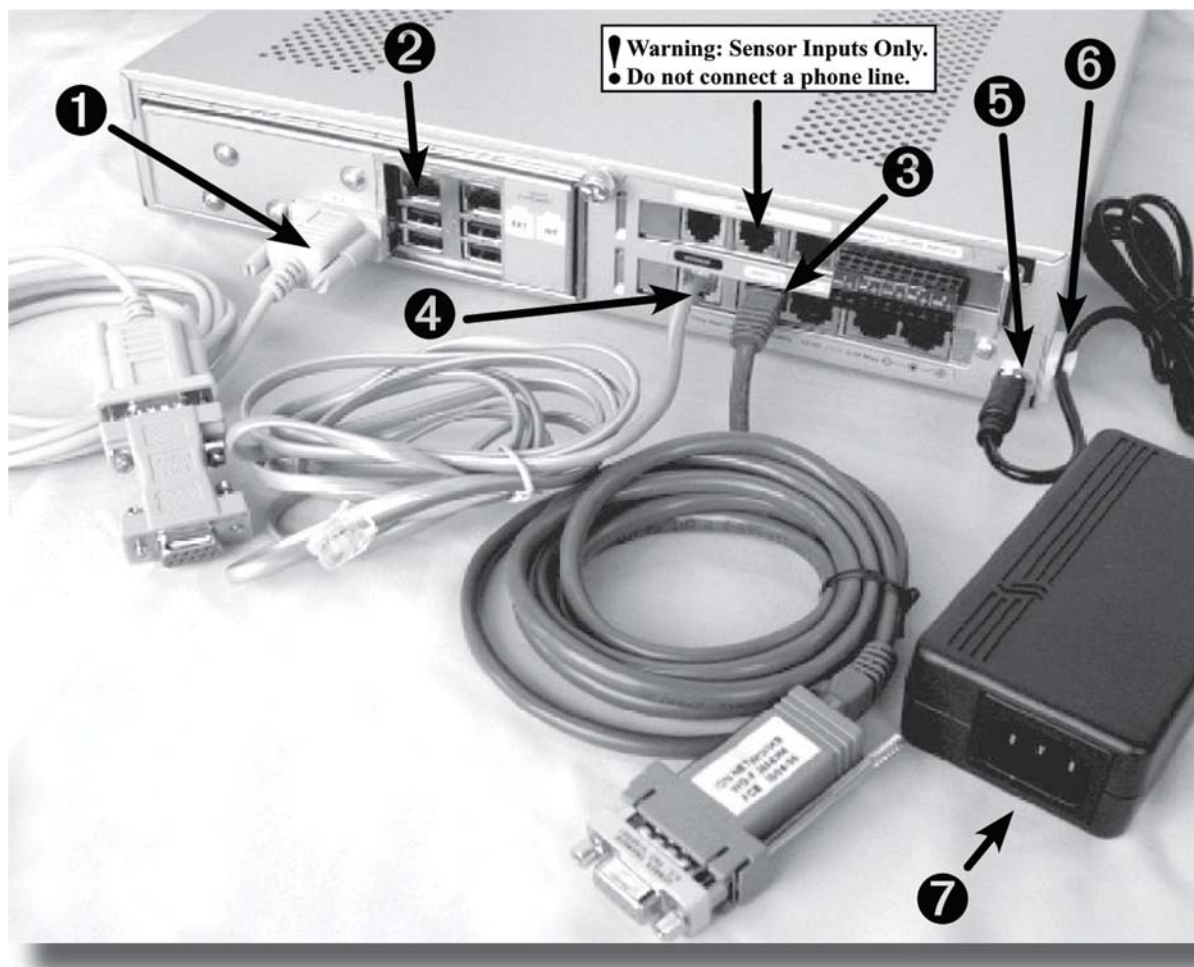


Figure 3-2: Cable Connections

To connect the ASG Defender:

1. Use the AUX port cable to connect the PC or terminal. This connection is used to configure the Defender and can be disconnected after the unit is installed.
2. Typical installation connects the External Interface port to a LAN with a CAT5 cable. Consult your Network Administration personnel to verify the correct placement in your network.
3. If you are administering equipment with a serial interface, then connect each device to one of the Defender host ports.
4. Connect one analog telephone line to the modem port on the back of the Defender.
5. Connect the power supply to the power plug located on the back of the Defender.

6. Place the cord into the cable clamp.
7. Plug the power cord into a standard AC outlet (100-240V~, 1.5A, 50/60 Hz).
8. **Note:** The blue “Power” LED illuminates and the amber “Activity” LED flashes as the device starts. The system’s banner displays on the terminal screen.

3.4 Start a Local Admin Session on the AUX Port

The Defender can be administered locally by connecting a PC or dumb terminal to the AUX port of the unit.

1. Connect a PC or dumb terminal to the AUX port.

To connect a PC:

- a. Connect the female end of the DB9 cable (see # 1 in Figure 2-4) to the AUX port of the Defender. Tighten the thumbscrews.
- b. Connect the male end of the DB9 cable to the NULL connector (already pre-assembled when shipped).
- c. Connect the DB9 male end with the NULL connector to the PC COM port. Tighten the screws.
- d. Open a terminal emulator program such as Hyperterm, configured with the following settings: 9600 bps, 8 data bits, no parity, 1 stop bit, and flow control = Xon/Xoff.

To connect a dumb terminal:

- a. Connect the female end of the DB9 cable (see # 1 in Figure 2-4) to the AUX port of the Defender. Tighten the thumbscrews.
- b. Remove the NULL connector from the DB9 cable.
- c. Connect the male end of the DB9 cable to the serial port of the terminal.
Note: A female-to-female DB9 gender changer may be required if the terminal serial port is a DB9 male connector.
- d. Configure the terminal with the following settings: 9600 bps, 8 data bits, no parity, 1 stop bit, and flow control = Xon/Xoff.
Note: Do not disconnect the AUX connection until you have verified the operation of the unit.

Your PC or dumb terminal is now ready to communicate with the ASG Defender. When the unit is turned ON in the next step, the boot up messages will display on the screen.

2. Power ON the unit:
 - a. Plug the female end of the power cord into the power supply pictured in Figure 2-4. Plug the male end of the power cord into a standard AC outlet

- (100-240V~, 1.5A, 50/60Hz).
- b. Plug the other end of the power supply into the Defender power connector shown in Figure 2-4.
The Defender unit will turn ON.
3. Observe the boot-up sequence when power is applied to the Defender:
- a. The LED labeled “Power” on the front of the unit will turn ON and the amber LED labeled “Activity” will flash on/off on initial startup (refer to Figure 2-1).
 - b. The unit will generate a Power ON beep when power is applied.
 - c. The system’s banner will display on the terminal screen as shown in Figure 3-3.
Note: If the banner does not display, you can “wake up” the AUX session by pressing <ENTER> several times until you are prompted to “Begin AUX Port Session.” Use the <SPACE BAR> to select “YES.” When prompted to connect as the Default User, use the <SPACE BAR> to select “YES”. The appliance system prompt will eventually display.
 - d. If the banner still does not display, check for connectivity problems between your AUX and terminal ports.

At this point, your local admin session has been successfully started.

```
-----  
- -                ASG DEFENDER 4-Port v1.0.0                - -  
- -                                                        - -  
- -                                                        - -  
-----  
11/09/05 16:11:00 F0EB {I} [AUX:12] User: AUX_Default -  
Connected to AUX  
11/09/05 16:11:01 C72E {I} [H] Host 1 Ready for: Definity  
11/09/05 16:11:01 E03C {I} [H] Host 2 Idle  
11/09/05 16:11:01 586B {I} [H] Host 3 Idle  
11/09/05 16:11:01 E7AF {I} [H] Host 4 Idle  
11/09/05 16:11:01 995A {I} [] TRAPTASK Started  
11/09/05 16:11:08 0334 {I} Network init OK  
11/09/05 16:11:10 3E1F {I} [M1:] Modem Idle  
Ser5600G12345>
```

Figure 3-3: ASG Defender Banner

3.4.1 Set the Date and Time

By default, ASG Defender units are set to Eastern Time. It may be necessary to adjust time settings to match the site's geographic location.

To set the date and time:

The Set Date and Time (SDT) command allows you to set the date format to one of ten options and to set the time.

1. At the system prompt type "SDT" and press <ENTER>. The Set Date and Time screen displays as shown in Figure 3-4.

```
Ser5600G12345>sdt

--- Set Date and Time ---
Date Format                MM/DD/YY
Current Date              03/22/05
Current Time              16:45
GMT Offset (e.g. '-05:00') -05:00

03/22/05 16:45:51 C880 {I} [T2:120] Set Date and Time
03/22/05 16:46:08 A89C {I} [T2:120] Set Date and Time - O.K.
```

Figure 3-4: Set Date and Time

The default date format is shown in Figure 3-4. By using the <SPACE BAR>, you can change the format to one of ten date formats. All areas within the ASG Defender reflect the change in format. For example, if an action item is scheduled to occur (in the default format) on 11/29/05, and you change the format to a four-digit year, the Action Item date will contain a four-digit year.

2. Press the <SPACE BAR> at the Date Format prompt to show the next format. Continue pressing the <SPACE BAR> until the desired format is listed, then press <ENTER>.

The ten formats available in the ASG Defender are:

MM/DD/YY	MM-DD-YY
MM/DD/YYYY	MM-DD-YYYY
YYYY/MM/DD	YYYY-MM-DD
YY/MM/DD	YY-MM-DD
DD/MM/YYYY	DD-MM-YYYY

3. After setting the format, enter the current date and press <ENTER>.
4. Enter the current time using the 24-hour (Military) time format and press <ENTER>.
5. Enter the GMT Offset used for setting time zones.
The system responds with a confirmation.

3.4.2 Add a CMASTER User

This section provides basic instructions for adding a CMASTER access level user. Refer to the *ASG Defender Administrator Guide* for additional information on modifying the user database.

Note: A CMASTER user may issue the Block Avaya Administration (BAA) command to restrict Avaya users from administering the customer user table. If this restriction is in effect, you will not be able to add a CMASTER user.

To add a CMASTER user:

1. At the system prompt type "AU" (Add User) and press <ENTER>.
2. When prompted, type the user "name" (or use the one line command AU "name") and press <ENTER>.
3. Use the <SPACE BAR> to select the CMASTER access level. Refer to the *ASG Defender Administrator 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 BAR> to select from one of the following Primary Authentication Methods: ASG Key, Pager, or Password/Callback.
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. Your screen should look similar to Figure 3-5.

Note: When adding a customer user, remember to advise the user of his/her user ID and authentication information. If the customer decides to implement restrictions such as the BAA command or Allow/Deny for Avaya personnel, it could result in voiding the SLA's in the contract.

```

Ser5600G12345>au pager
--- Add User ---
User Name                Defender-CMaster
Access Class             CMaster
Allow Concurrent Logins  No
Log Session Activity     No
Block Access             No
Sessions Allowed (blank=unlimited)
                        MM/DD/YY
User Expiration Date
Primary Authentication Method  ASG Key
Secondary Authentication Method  None
Auto Execute Command
Comments:
Options:

-- ASG Key Details --
Encryption Key Source      Randomly Generated
Enter These Digits as Key1 or Key2: 7363 2265 = 6723 2076 =
0520 =
Test Challenge: 1234567 ...Reply: 493-3790

Press <ENTER> to Continue

11/30/05 09:33:58 F070 {I} [T1:8] Add User
11/30/05 09:34:40 8BB4 {I} [T1:8] User: DEFENDER-CMASTER Added
- O.K.
Ser5625123456>

```

Figure 3-5: Add user example

3.4.3 International Modem Setup (Optional)

Installations in the domestic United States do not require modification 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 configure a modem for international use:

1. Access the Defender by connecting to the AUX port.
2. At the system prompt type "SM" and the modem number and press <ENTER>. The Set Modem Port Parameters table displays.
3. Press <ENTER> to move down the table until you reach the country parameter.
4. At the "Country" parameter, use the <SPACE BAR> to select the country in which the Defender is located, or will be installed.

5. Press <ENTER> to move to the end of the table. Press <ENTER> once more to accept your changes.

Note: For more information on configuring modem port parameters, refer to the *ASG Defender Administrator Guide*.

3.5 Setup ASG Defender with Avaya Ethernet Products

Endpoints are network elements (a router, server, voice switch, data processing equipment) that are protected by Avaya security appliances (for example, the Defender). The Defender provides access for system administrators to perform configuration changes or troubleshoot a system failure. Endpoints contain multiple interfaces (for example, console port, Telnet or SSH sessions, FTP or SFTP sessions).

To access an endpoint interface, there are two types of connections between the Defender and the endpoint.

1. **Serial connection** - A physical connection between the Defender host port and a serial console port on the endpoint. The Defender 2-Port has two host ports and the Defender 4-Port has four host ports for connections to an endpoint console or serial ports. The host ports on the Defender are a DCE interface (Like a modem). For further details, refer to Section 4 of this guide as well as the *ASG Defender Administrator Guide*.
2. **Ethernet connection** - A physical connection via an IP Ethernet network. The Defender secures access to an Endpoint's administrative IP interface between the various interfaces of the appliance.

3.5.1 Set Network Parameters (SNP)

This section describes how to manually set the basic network parameters needed to use the ASG Defender. In some cases, ASG Guardian management software may administer the Defender.

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 Defender's AUX port.

To set network parameters:

1. At the system prompt type "SNP" and press <ENTER>. The Set Network Parameters screen displays as shown in Figure 3-6.

```
Ser5600G12345>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                192.168.0.1
      Mask                      255.255.255.0
External Interface              Auto Sensing
External Address                10.21.100.4
      Mask                      255.255.0.0
Default Gateway                 10.21.1.1
Nameserver
PPP Address                     1.1.1.1
PPP Peer Address                2.2.2.2
```

Figure 3-6: Set Network Parameters

2. Select menu item #1 "Network Initialization Params" and press <ENTER>.
3. Select 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. Enter the *External Address*, *Mask*, and *Gateway* pressing <ENTER> after each entry. This is the actual LAN address of the Defender.
6. Enter the PPP address. Use one of the following methods to obtain the address used to establish a PPP session upon dialing into the Defender.

For New Installations	<p>The PPP address is included within the installation script provided by the ART registration system.</p> <p>The output will look like this: RAS IP address: 10.28.x.x</p>
For Existing Installations	<p>At one of the S8xx0 media servers, execute the following command: Less /etc/opt/ecs/servers.conf</p> <p>The output will look like this: 10.1.1.37:10.1.1.38 Use the first IP address.</p>

7. Press <ENTER> through the rest of the parameters in the group.
Note: Use Ctrl+X to erase a line and Ctrl+A to abort a command.

3.5.2 Set Network Services

To set networking services:

1. At the system prompt type "SNS" and press <ENTER>. The Set Networking Services screen with the default values displays as shown in Figure 3-7.
2. For each of the menu prompts use the <SPACE BAR> to toggle to the desired selection and press <ENTER>. Figure 3-7 displays a typical network services configuration. Consult your network administration personnel to verify permissible services.

```
Ser5625123456>sns

--- Set Networking Services ---
Restore Factory Defaults ?      No

Telnet on Internal Port        Disable
Telnet on External Port        Disable
FTP    on Internal Port        Disable
FTP    on External Port        Disable
PPTP Server                    Disable
SSH                             Enable
IPSec                          Disable
Ping                           Device and subnet
```

Figure 3-7: Set Networking Services Screen

3.5.3 Add Avaya IP (AAIP)

The ASG Defender contains a special set of commands and action routines that enable you to configure Avaya IP-connected devices like the S8xx0 series.

To locate special commands:

1. At the system prompt type "N" and press <ENTER>. A list of "S8xx0 Parameters" for the S8xx0 displays.

Table 3-2 provides an overview of Avaya special commands.

Table 3-2: Avaya IP Commands

Command	Description
CONHOST	Connect to Avaya device.
AAIP	Add Avaya IP Device
XAIP	Delete an Avaya IP device.
CAIP	Change an Avaya IP device.
LAIP	List all Avaya IP devices.
AINIT	An action routine that initializes proxy rules. This is part of the Defender default configuration. No action is necessary.
ADDUMP	Download the table of Avaya IP devices.
ADCONFIG	Load the table of Avaya IP devices.

3.5.4 Administering an Avaya IP Device

By default, both CMaster and AMaster users can configure the Avaya IP Table. However, a CMaster user can issue the Block Avaya Administration (BAA) command to restrict an AMaster user from accessing certain parameters related to the customer's network.

To add an S8xx0 Avaya IP device:

1. At the system prompt type "AAIP" and press <ENTER>. The Add Avaya IP Device dialog begins as shown in Figure 3-8.
2. Type a unique alphanumeric device name and press <ENTER>.
3. Enter the actual IP address of the S8xx0 and press <ENTER>. 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 this information from the Expert Systems staff. The Defender will automatically translate the Avaya IP address into the actual IP address when Expert Systems connect using PPP.
5. Select the Terminal Connection Type (SSH or Telnet) and press <ENTER>.
6. Specify the ports that should be forwarded to the Avaya device and press <ENTER>. 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.

7. Enter any comments and press <ENTER>.
8. Add another device. Select Yes or NO and press <ENTER>.

```
Ser5625123456>aaip
--- Add Avaya IP Device ---
Device name                S8700
IP Address                 10.21.87.2
Avaya IP Address           10.29.0.16
Terminal Connection Type   SSH
Ports                     80,443,21,22,5022
Host Equipment Type        8700
Comments
Add another Device?        No

Reinitializing rules for Avaya devices...

12/05/05 11:46:58 B7EB {I} [T1:35] Add Avaya IP Device
Ser5625123456>
```

Figure 3-8: Administering an Avaya IP Device Screen

Note: After establishing a PPP session, the user may connect directly to Avaya IP devices, *except* on ports 23 and 5023. These ports are treated specially to prevent “telnet hopping.” Attempts to telnet directly to these ports will be redirected back to the ASG Defender login. Once authenticated into the Defender, use the “CONHOST” command to connect to the Avaya IP devices.

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

3.5.5 Set Alarming Configuration (INADS) Delivery

To enable alarm delivery from the S8xx0 devices to Avaya Expert Systems, a “Home Phone Number” parameter must be specified.

Note: Refer to the *ASG Defender Administrator Guide* for additional information on setting system parameters.

To specify a home phone number:

1. At the system prompt type "SSP 3" and press <ENTER>. The Action Routine Parameters dialog displays.
2. Enter the phone number for the Avaya Alarm Receiver. Ensure that 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

Note: Other international sites should contact their regional Avaya Support Team.

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

3. Press <ENTER> through the remaining parameters to save your settings.

3.5.6 Verify Connectivity of IP Devices

The CONHOST command is used to verify connectivity of IP devices.

Note: The CONHOST command can also be used to verify connectivity with serial devices; refer to “Verifying Connectivity of Serial Devices” on page 4-3.

To connect to an Avaya device using the CONHOST command:

1. At the system prompt type “conhost” and press <ENTER>. A list of IP and serial devices accessible from the Defender displays.
Note: If you know the device name, type “conhost devicename portnumber” and press <ENTER>.
2. Type the name of the device and press <ENTER>.
3. Type the number of the port: port 23/5023 (telnet) or port 22/5022 (SSH) and press <ENTER>.
Note: This step is for IP ports only. Figure 3-9 is an example of an SSH connection.
The Login prompt for the device displays.
4. Login to the device and press <ENTER>.
The following message displays: Are you sure you want to continue connecting (yes/no)?
5. Type “Yes” and press <ENTER>.
Authorization text and a password prompt display as shown in Figure 3-9.
6. Enter a password and press <ENTER>.
7. Enter your terminal type and press <ENTER>.
System messages and a user prompt for the device you just connected to display as shown in Figure 3-9.

```
Ser5625123456>conhost
--- Connect to Avaya device ---
Name          Comment
=====
S8500
S8700
SERIAL        Host Port 1
SERIAL        Host Port 2
HOST3         Host Port 3
HOST4         Host Port 4

Device name          S8500
Port (<Enter> for ssh default = 22 / telnet default = 23)
Login:username

Enter your terminal type (i.e., xterm, vt100, etc.) [vt100]=>

username@server1>
```

Figure 3-9: Connecting to an Avaya IP Device using the CONHOST Command

3.5.7 S8xx0 Automatic Login

The CONHOST command uses the credentials of the user that is passed in the conhost string.

To connect to an Avaya IP device using the CONHOST automatic login:

1. At the system prompt type “conhost userid@devicename portnumber” and press <ENTER>. A user prompt for the device you just connected to displays.

For example,

User Jane is an ASG Key user. Her user profile is in the S8xx0. The Defender will use Jane’s user ID and will emulate as an ASG authentication password to login to the S8xx0.

3.6 Setup ASG Defender with Avaya Serial Products

3.6.1 Configure Defender Host Ports

Table 4-1 specifies the ASG Defender host port settings required by the type of equipment it protects.

Table 3-3: ASG Defender Host Port Settings

Host Port Parameter	Definity G3r	Definity G3si	Intuity Audix RMB Conversant	Definity MAP D SAT	CMS	Octel 250/350 Aria	Octel 200/300 Serenade
Baud Rate (Modem Control Settings)	9600	9600	9600	9600	9600	9600	9600
Character Length/Parity	8/None	8/None	8/None	8/None	8/None	8/None	8/None
Alarm Filter	Definity	Definity	Intuity	None	CMS	None	None
Force CD/DSR High	DSR Only	DSR Only	DSR Only	Yes	Yes	Yes	Yes
Flow Control	None	None	None	None	None	None	Xon/Xoff

To set host port parameters:

1. At the system prompt type "SH" and press <ENTER>.
2. Select a host port number (for example, 2) and press <ENTER>. A screen similar to Figure 4-1 displays.

```

Ser5600G12345>sh
--- Set Host Port Params ---

Hosts:

1 = INTUITY-1      2 = INTUITY-2      3 = CMS-1      4 = CMS-2

Host Port Number          2
Restore Factory Defaults ?      No

-- Host 2:

Host Name                  INTUITY-2
Baud Rate Setting          9600
Character Length / Parity    8 / None
Alarm Filter                Intuity
Force CD/DSR High          DSR Only
Flow Control                None
Pass break on Ctl-B during CON?  Yes
Host Session Disconnect on Ctrl+?  A

-- Automatic Buffering --

Enable Automatic Buffering ?      No
Compress closed buffer files ?    No

Auto Switch: (Enter 0 to disable)

When CURRENT File exceeds 'n' KB  50
Every 'n' Hours                    24
- Synchronize at what hour (0-23)  0

-- Alarm Delivery --

Modem used for Alarm Delivery      First Avail.

08/30/05 09:05:46 B4C4 {I} [T1:72] Set Host Port Params
08/30/05 09:06:25 706F {I} [T1:72] Set Host Port Params - O.K.
Serxxxxxxx>

```

Figure 3-10: Setting Host Port Parameters

Refer to the *ASG Defender Administrator Guide* for additional information on host port parameters.

Note: When the Avaya GTS/COE group provisions a Defender, a configuration script is installed that automatically sets parameters for Definity and Intuity products installed by default on host port 1 and 2. Some customers may want to install other products on these ports, or manually configure other settings. **Configure any custom parameter settings only after the GTS/COE has completed the provisioning process.**

3.6.2 Modify the Avaya platform to interoperate with the ASG Defender

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
Definity	On the "Maintenance-Related System Parameters" screen: The INADS port must be set to "External" modem to enable the delivery of alarms via the ASG Defender. Miscellaneous INIT parameters should be set to: S12=24&W0
Intuity	The RMB board should be set for "pass-through" instead of modem connection.

3.6.3 Verify Connectivity of Serial Devices

The CONHOST command is used to verify connectivity of serial devices.

To connect to an Avaya device using the CONHOST command:

1. At the system prompt type "conhost" and press <ENTER>. A list of IP and serial devices accessible from the Defender displays.
Note: If you know the device name, type "conhost devicename" and press <ENTER>.
2. Type the name of the device and press <ENTER>. The Login prompt for the device displays.
3. Login to the device and press <ENTER>. Authorization text and a password prompt display.
4. Enter a password and press <ENTER>.

3.7 Register the ASG Defender with the Global Technical Services Group

To register the ASG Defender with GTS:

1. The Technician contacts the GTS registration team and informs them that he/she is installing an ASG Defender at their Customers location.
2. The Registration team adds the Solution Element in Maestro and downloads the Avaya user file.
3. The installer completes the registration in ART following Avaya's normal processes.

Appendix A: Defender to Avaya Equipment Cable and Port Requirements

Avaya Product	Device Port	Cable Type (see Note below)	ASG Defender Host Port #
Definity G3r	TN1648B System access maintenance board Modem port	"Y" Cable Material Code 700229958	Host 1
Definity G3si	DB25 (DCE)	Straight (Included with Defender)	Host 1
Prologix	Modem port on Octopus Cable	Straight	Host 1
Intuity Audix RMB Intuity Conversant	Intuity: DB9 connector on RMB board	Straight (Included with Defender)	Host 2
CMS	DB9 or DB25	Straight (Included with Defender)	Any host port not used by Definity or Intuity
Avaya IR UCS 1000	DB9 COM1	Straight (Included with Defender)	
Definity MapD	Check connector on octopus cable.	Straight (Use the 9-25 cable included w/ Defender if not already in use.)	
Definity SAT Terminal Port	SAT Terminal Note: Using this port is a customer option.	Null Terminal (Included with Defender)	
PG230	DB25	Straight (RJ45/DB9 to DB25 cable)	
PDS Platform HP 9000	DB9	Straight (RJ45/DB9 to DB9 cable)	
Octel 250/350 Series (Aria)	"Modem" port located on the front of the unit.	250: 9-pin to 9-pin Straight 350: 9-pin to 25-pin Straight	
Octel 200/300 Series (Serenade)	J1 Port	25-Pin Null Host Cable	

Appendix B: Cable and Connector Pinouts

B.1 AUX and Host Port Pinouts

The serial ports (AUX and Host) on the Defender are all RS232 DCE.

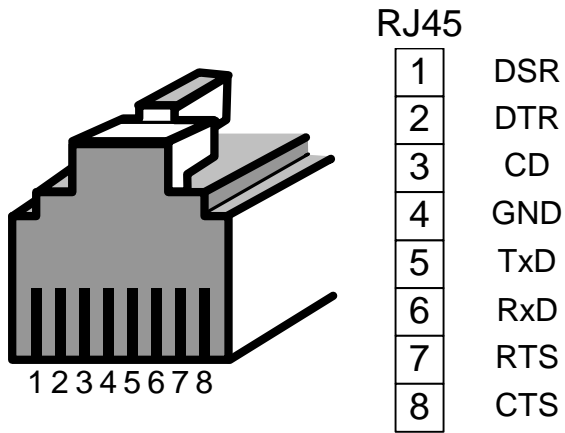


Figure B-1: RJ-45 Serial Pinout

B.2 Standard Serial Cables

RJ45 Host to DB9 (Straight)		
RJ45	DCE Signal	DB9
1	DSR	6
2	DTR	4
3	CD	1
4	GND	5
5	TxD	3
6	RxD	2
7	RTS	7
8	CTS	8

RJ45 to DB25 (Straight)		
RJ45	DCE Signal	DB25
1	DSR	6
2	DTR	20
3	CD	8
4	GND	7
5	TxD	2
6	RxD	3
7	RTS	4
8	CTS	5

RJ45 to DB9 (Null)		
RJ45	DCE Signal	DB9
1	DSR	
2	DTR	1
3	CD	4
4	GND	5
5	TxD	2
6	RxD	3
7	RTS	8
8	CTS	7

RJ45 to DB25 (Null)		
RJ45	DCE Signal	DB25
1	DSR	
2	DTR	8
3	CD	20
4	GND	7
5	TxD	3
6	RxD	2
7	RTS	5
8	CTS	4

DB9 Host to DB25 (Short)		
DB9	DCE Signal	DB25
1	CD	8
2	RxD	3
3	TxD	2
4	DTR	20
5	GND	7
6	DSR	6
7	RTS	4
8	CTS	5
9	RI	2

DB9 Host to DB9		
DB9	DCE Signal	DB25
1	CD	1
2	RxD	2
3	TxD	3
4	DTR	4
5	GND	5
6	DSR	6
7	RTS	7
8	CTS	8
9	RI	9

