



ASG Defender Release Notes

Version 1.0.3

**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 guide 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.

INTRODUCTION

This document contains the release notes for the ASG Defender. As each release becomes available, this document will be updated to reflect the changes.

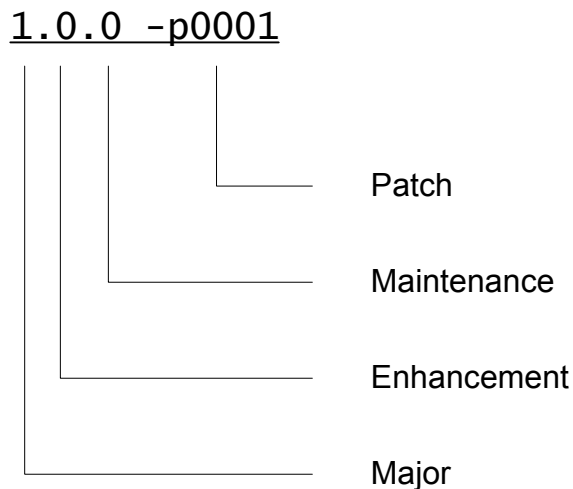
RELEASE TYPES

Avaya will generate software releases that fit into one of the following four descriptions.

1. **Patch:** This release provides an urgent fix for customers. The release is most frequently limited to one or a small number of fixes.
2. **Maintenance:** This release improves quality, reliability, and performance without adding any new functionality. All previous patch release fixes are included in this release.
3. **Enhancement:** This release significantly improves or provides additional functionality to the existing product. All previous patches and maintenance releases are included in this release.
4. **Major:** This release represents the initial or next generation product. All previous patches and maintenance releases are included in this release.

SOFTWARE VERSION NUMBER

The four release types are represented in the product version numbers as depicted below.



SUMMARY OF DEFENDER RELEASES

Release #	GA Date	Description	
1.0.3	04/15/2006	Release type:	Maintenance Release
		Which product:	ASG Defender (2- and 4-port)
		Who needs it:	All users of previous version 1.0.1 are recommended to upgrade to this version.
1.0.1	9/13/2005	Release type:	Major Release

DEFENDER – INSTALLATION AND UPGRADE NOTES

WHAT YOU NEED

Release notes (this document)
Patch/Upgrade binary file
Client PC system to transfer the file to the Defender

INSTALLATION

Consult the *ASG Defender Administrator Guide* for full installation details.

Quick instruction steps:

1. Login to the Defender with master level user access.
2. Transfer the binary file to Defender via ftp, X modem, or Z modem.
3. Run the command: upg <FILENAME>.
4. Select “Yes” after the “Are you sure?” question.

The Defender will perform the upgrade. It takes approximately two minutes to complete.

5. Confirm that the proper version was loaded by running the version command <ver>. This command will output the software version number.

MINIMUM SYSTEM REQUIREMENTS

System Processor:	NA
System Memory:	NA
Free Disk Space:	40 MB
Operating System:	NA
Networking:	NA

DEFENDER 1.0.3 – MAINTENANCE RELEASE

DEFENDER 1.0.3 – WHAT'S NEW?

Seventeen fixes are included in this release and five changes to code have been made to prevent problems. There are no new enhancements. Details included in the *Defender 1.0.3 - Fixed* section and *Defender 1.0.3 – Code Improvements* section.

DEFENDER 1.0.3 – VERSION COMPATIBILITY

Defender version 1.0.3 should only be applied to 2-port/4-port with versions 1.0.2 or lower.

DEFENDER 1.0.3 – FIXED

ID #	Description	
1048	Problem:	After transferring a file to the Defender via Zmodem or Xmodem, the erroneous file date of 04/07/2074 will be written. (Infrequent)
	Workaround:	Retransmit the file.
	Fix:	Operation is corrected.
1132	Problem:	Port forward rules are not removed from the DB after the <xpf> command.
	Workaround:	None.
	Fix:	Operation is corrected.
1088	Problem:	Files transferred to the Defender via Zmodem do not receive the READ file attribute. This causes subsequent file manipulation (such as FTP <get> command) to fail.
	Workaround:	Use Xmodem or FTP.
	Fix:	All files transferred to the Defender via Zmodem are automatically assigned READ permissions.
1112	Problem:	Using the Fast Meridian Filter on Host ports 1 and 2 causes host port 1 to lose access and alarming capability.
	Workaround:	Host port 1 can only be re-enabled by rebooting the system.
	Fix:	Fast Meridian Filtering can be used on two host ports simultaneously.
1117	Problem:	After performing an upgrade, the field "Site Name" in the Set System Parameter Table (SSP) displays the default system site name.
	Workaround:	Run SSP 1 and step through the table using the <enter> key. The original site name will return after this procedure. This can be verified by running SSP 1 again.
	Fix:	Operation is corrected.
1121	Problem:	If two near-simultaneous host port alarms invoke the SNMPTRAP action routine, then only trap is sent.
	Workaround:	None.
	Fix:	Operation is corrected.

1123	Problem:	After successfully setting up Defender SNMP Manager and sending traps, subsequent changes to the SNMP Manager settings do not take effect.
	Workaround:	All changes take effect at time of update.
	Fix:	Reboot system.
1061	Problem:	The Display Port Status command (<dps>) does not output real-time port status data.
	Workaround:	The command can only be repeated. No workaround for continual real-time status.
	Fix:	Operation is corrected.
1062	Problem:	For Defender 2-port units only, the Display Port Status command (<dps>) does not output real-time port status data.
	Workaround:	None.
	Fix:	RWI information has been removed from the output.
1074	Problem:	<u>Grammatical Error</u> : After running the upgrade command (<upg>), the message reads: "Enter the name of the file file ...". The word file is doubled.
	Workaround:	NA
	Fix:	The word "file" is deleted.
1087	Problem:	<u>Incorrect System Message</u> : When the Defender finishes sending a SNMP trap over IP, the message: "PPP Disconnected" displays.
	Workaround:	NA
	Fix:	The "PPP Disconnected" message has been removed.
1116	Problem:	When the Defender is used as a FTP client, using the <put> command generates the message "Permission Denied."
	Workaround:	Enable FTP in the <sns> menu.
	Fix:	Permission is not denied. The FTP disable/enable setting in the <sns> menu does not influence Defender FTP client sessions.
1119	Problem:	IPSEC tunnels loaded into a Defender via a config file do not successfully write to the DB.
	Workaround:	Manually configure IPSEC tunnels with the <aipsec> command.
	Fix:	Operation is corrected.
1141	Problem:	The SENDFTP action routine does not operate.
	Workaround:	Use FTP manually.
	Fix:	Operation is corrected.
1142	Problem:	Extraneous system data may appear in user sessions.
	Workaround:	Terminate and then restart the session.
	Fix:	Operation is corrected.
1144	Problem:	The enterprise OID of a Defender trap does not match the Defender MIB. This may cause an issue with certain NMS software such as HP Openview.
	Workaround:	Adjustments to trap-receiving software may workaround this problem.
	Fix:	Operation is corrected.

1114	Problem:	The Defender NTP client cannot connect with Linux/Unix NTP servers.
	Workaround:	None.
	Fix:	Operation is corrected.
1145	Problem:	Serial alarms can be unexpectedly truncated and/or the timestamp field can be truncated if the serial alarm exceeds forty characters.
	Workaround:	None.
	Fix:	Each serial alarm stream will be recorded for a period of 300ms before cutoff.
1148	Problem:	S8xxx alarms passing through the Defender lose the 10 th digit of the Product ID.
	Workaround:	None.
	Fix:	Operation is corrected.
1149	Problem:	Setup: [Connect2 ←PPP→ Defender ←IP→ Host server] Defender intercepts scp requests between Connect 2 and the Host server. Therefore, scp between Connect2 and host servers cannot be performed.
	Workaround:	Use FTP, Xmodem, or Zmodem, or dial into the host server directly.
	Fix:	A store and forward procedure is necessary to perform scp. After PPP dial-in, files need to be <scp> to the appliance followed by <scp> to the destination host.
1104	BIOS firmware has been updated to ensure successful initialization after a CMOS corruption. The BIOS version now displays in the <ver full> table.	
1136	Defender software has been updated to improve terminations of “ungraceful” session disconnections such as pulled phone lines.	
1146	<u>Upgrade robustness:</u> In the event that the Defender fails to upgrade three times or more during an upgrade, the system will restore back to its original version.	
1147	<u>Usability:</u> Whereas the UI uses the space bar to move forward through a list of parameters in any setup menu, the <backspace> key can now be used to cycle backward through the same list of parameters.	