



**ASG Guard II
Release Notes
Version 5.2
10/21/2005**

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



**2005 Avaya, Inc
All Rights Reserved
Printed in USA**

**September, 2005
Release 5.2**

Notice

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

Responsibility for Your System's Security

You and your System Manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The System Manager is also responsible for reading all installation, instruction, and system administration documents provided with this product to fully understand the features. Avaya is not responsible for any damages resulting out of or arising from the unauthorized use of your system.

Home Page

The home page for Avaya, Inc. is <http://www.avaya.com>.



ASG Guard II Release Notes 4

New Features 4

Enhancements 5

Bug Fixes 6

ASG Guard II Release Notes

This document describes the changes and new features that are available in the ASG Guard II v5.2.

NEW FEATURES

Support for SSH Proxy

Many Avaya platforms now support SSH access for secure communications. The ASG Guard II was enhanced to support end-to-end encryption for both in-band and out-of-band connections. The Guard II proxies SSH sessions via the CONT command to an endpoint device providing:

- A log entry identifying the user, endpoint, and start and end time of the session.
- Optionally, a recording of the session.

The CONT command was modified to not only support Telnet but also SSH connection to endpoints. The default connection type is configured through the AAIP (Add Avaya IP) or CAIP (Change Avaya IP) commands.

Automated Login

This feature was developed for automating connections through ASA and other terminal emulation clients.

This feature, called CONHOST, automates the user connection and authentication into Avaya communication devices. The CONHOST command launches an SSH or Telnet session and navigates through the endpoint login into an S8X00, Definity, or Intuity device.

Automated connection through CONHOST is accomplished using the following string format:

Format:

CONHOST [userid@devicename](#) port#

Example:

CONHOST [craft@S8700_Active](#) 5022

Customer Control of Avaya Access to Host Ports

Customers require a feature that controls Avaya access to serial host ports on the ASG Guard II. This feature is configured via the Block Avaya Access (BAA) command.

```
Ser6040630591>baa

--- Block/Unblock Avaya Admin. ---
Block Avaya Administration of Customer Users ? No
Block Avaya Master Use of AAIP CMD? No
Block Avaya Access to Host Ports 1,3:4 <-----NEW
Block Avaya Administration of Network Params ? No
```

To block Avaya access to specific ports, enter the BAA command and enter port numbers separated by a comma or port ranges separated by a colon(:). For example, 1,10:14 – this means block 1 and 10 through 14. The default setting for this field is blank, allowing Avaya access to all host ports.

ENHANCEMENTS

Support for Alarm Delivery and Access through External Modems

The ASG Guard II supports up to 4 external modems on a 16 or 28 host port device. The external modem feature was modified for this release to support secure access to and alarm delivery from Avaya devices .

All standard modem-access features are supported through the external modem. In addition, all standard modem messages are generated when connections are established through an external modem.

Support for Incoming SSH Over PPP for Avaya Tools

To better support SSH connections through Avaya's expert system connect tool, the PPP addressing structure was changed in the ASG Guard II. The IP address that the Guard II issues to the connection tool enables both secure Telnet and SSH sessions to the same IP address. The AVAYAPPP command was modified to support this IP structure.

Updates to Open SSH and Open SSL Code

The encryption software of the Guard II was updated with the latest software releases as follows:

Open SSH Version: 4.0p1
Open SSL Version: 0.9.7g

Store Keys/Passwords with 3DES

The ASG Guard II stored secret data (that is passwords and keys) with a single DES encryption. In release 5.2, keys and passwords are encrypted using 3DES. The following capabilities were added:

- Store keys/passwords in the system using 3DES
- Keys/passwords encrypted using 3DES in configuration files
- Capability to import older user tables that are encrypted with single DES.
- User command (SCK) to manage 128 bit-encrypting keys (Avaya and customer).

Modification to IP clients to support Binary Mode

Certain tools require the capability to download files from devices through an SSH session, which requires the SSH and Telnet clients to support Binary mode. The ASG Guard II was modified to support Binary Mode for both SSH and Telnet.



BUG FIXES

[980] Co processor inoperable.

Periodically the co-processor would fail and there was no capability to restore the connection. This bug fix enables the motherboard to restore the connection to the co-processor.

[981] Null Characters

Due to non-support of Binary mode for file transfers, the ASG Guard II was introducing spurious null characters into data streams when binary transfers were attempted. This issue was resolved through the Modification to support Binary Mode enhancement (see above).

[1005] XModem file transfer over SSH

Xmodem file transfer over SSH connections would periodically fail. This issue is resolved in this release using Teraterm client software.