GB - Flash

Firewall
APPLIANCE

Product Guide

powered by
GNAT Box
System Software

Global
Technology
Associates, Inc.

Copyright

Disclaimer

Neither GTA, nor its distributors and dealers, make any warranties or representations, either expressed or implied, as to the software and documentation, including without limitation, the condition of software and implied warranties of its merchantability or fitness for a particular purpose. GTA shall not be liable for any lost profits or for any direct, indirect, incidental, consequential or other damages suffered by licensee or others resulting from the use of the program or arising out of any breach of warranty. GTA further reserves the right to make changes to the specifications of the program and contents of the manual without obligation to notify any person or organization of such changes.

Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation for their use. GTA assumes no responsibility with regard to the performance or use of these products.

Every effort has been made to ensure that the information in this manual is accurate. GTA is not responsible for printing or clerical errors.

Trademarks

GNAT Box is a registered trademark of Global Technology Associates, Incorporated.
Netscape Navigator is a trademark of Netscape Communications Corporation.
Internet Explorer is a trademark of Microsoft Corporation.
All other products are trademarks of their respective companies.

Technical Support

GTA includes 30 days installation support from the day you receive the initial shipment. GTA's direct customers in the USA should email GTA via the contact information listed below. Other customers should contact their local GTA authorized reseller.

Contact Information

Global Technology Associates, Inc.
3505 Lake Lynda Drive, Suite 109
Orlando, FL 32817 USA

Tel: +1.407.380.0220
Fax: +1.407.380.6080
Web: http://www.gta.com
Email: info@gta.com

Support: support@gta.com

Document Information

GB-Flash Firewall Appliance Product Guide
with GNAT Box System Software Version 3.3.2 November 2002

Contents

1 Introduction

GNAT Box Basics

Since 1994, Global Technology Associates, Inc., has been designing and building Internet firewalls. In 1996, GTA developed the first truly affordable commercial-grade firewall, the GNAT Box®. Since then, ICSA-certified GNAT Box System Software has become the engine that drives all GTA Firewall Appliances.

GTA's Firewall Appliances, powered by GNAT Box System Software, currently include GB-Pro, GB-Flash, GB-1000 and RoBoX™. GTA's optional features include GNAT Box VPN, Surf Sentinel (content filtering), and H_2A (high availability).

Requirements

To use GNAT Box System Software, you need to know the following:

- An understanding of TCP/IP networking.
- Network IP addresses for all network interfaces used.
- Netmasks for each attached network.
- Default route for External Network.
- Services to allow inbound/outbound (if any).

To initially configure the GB-Flash using the Video Console interface, you must have a video card installed, and a monitor and keyboard connected.

To connect the GB-Flash to your network, you need at least two Ethernet cables, one for each required network; a crossover cable to connect the firewall directly to a host or router, or a straight-through cable to connect the firewall to a hub or switch.

Registration & Activation

The GB-Flash requires an activation code, serial number and hardware key block to be fully functional. They will only function when installed on the specific system. The activation code and the serial number are located on:

- Label of the product box.
- Registration card included inside the product box.
- Once registered, on the GTA website under Support.

To register, go to www.gta.com, click on Support, then on the GTA Support Center link. This takes you to the login screen. If you already have an account, enter your User ID and password. If you have not yet created an account, click New Account, enter profile information and choose a User ID and password. Once you have completed the form, click Add to save it.

Return to the login screen and enter the User ID and password you created. In the Make a Selection screen, click Support Center, then click on Product Registration in the next screen, the Account Home screen for your support information. In the form that appears, enter your serial number and activation (unlock) code, then click Submit. Your new product will now appear in the View Registered Products screen, accessible from the Account Home page.

Note

If you cannot retrieve your registration code, or a feature code does not appear under View Registered Products, email support with the product serial number and your Support Center User ID in the message subject.

In addition to qualifying you for installation support, your product registration will allow GTA to inform you about upgrades and special offers.

Copy Protection

Copying of GNAT Box System Software is allowed for backup purposes. However, to activate your system and any special features, you will need a serial number (pre-installed on the GB-Flash) and activation codes. Keep a copy of these codes; they will also be available online at the GTA Support Center after product registration.

The GB-Flash also requires a hardware key block. GTA's system is different from other key blocks because it is attached only to the firewall hardware, not to any client workstations. A key block provides freedom to upgrade or change system hardware by simply attaching the key block to the new equipment. See Installation, Chapter 2, for instructions on installing the hardware key block.

Activation Codes

All commercial GTA Firewalls–GB-Pro, GB-Flash, GB-100, GB-1000 and RoBoX–use activation codes to protect software. For firewall appliances, the required registration code is pre-installed. Codes are printed on packaging and available at www.gta.com in the GTA Support Center.

Feature Activation Codes

If you purchased additional features for your GTA Firewall, you will be provided with a feature activation code for each. The activation codes for new features must be entered in Features under the Basic Configuration menu. Your feature activation codes can be found under View Registered Products on the GTA Support site by selecting the GB-Flash by its serial number.

Installation Support

Installation ("up and running") support is available to registered users. If you have registered your product and need installation assistance during the first 30 days, contact the GTA Support team by email at support@gta.com.

Include in the email your product name, serial number, registration number any feature activation code numbers for your optional products, and a System Software or Hardware Configuration Report, if possible.

Installation support covers only the aspects of configuration related to installation and default setup of the firewall. For further assistance, contact the GTA Sales staff for information about GTA's support offerings.

Support Options

If you need support after installation and configuration to defaults, contact the GTA sales department to purchase a support contract. Contracts range from support by the incident to full coverage for a year.

Other avenues for assistance are available through the GNAT Box Mailing List and Forum, on the GTA website, found at www.gta.com, or through an authorized GTA Channel Partner.

Upgrades

Once registered, you can view available upgrades by going to View Registered Products in the GTA Support Center. If there is an upgrade available and you are on the latest version of GNAT Box System Software, e.g., 3.3.x, or have a current support contract, the Action column in the View Registered Products section will have a Free Upgrade link. If no update is available, the Action column will display "Up to date."

If you are not on the current version and do not have a current support contract, an upgrade for the latest patch release, e.g., 3.3.2, will display if one is available. If no patch is available, the Action column will display “Purchase Upgrade/Support.”

If an upgrade is available for your product, click the upgrade link.

When you return to the View Registered Products list, click the product’s serial number and see the Product Details section to obtain the new activation code. The Product Details section will also display your previous activation codes. Upgrades are also available in Support Center Downloads. Only downloads for your version will be shown.

Caution

Back up your configuration before upgrading!

Documentation

This Product Guide describes how to install the GB-Flash on your selection of hardware and set up the GNAT Box System Software in your network’s default configuration. The GNAT Box System Software User's Guide includes configuration functions, descriptions of GBAdmin and the Web interface, administrative tools and GNAT Box-specific terms.

Documentation Conventions

A few conventions are used in this guide to help you recognize specific elements of the text. If you are viewing this in a PDF, color variations are also used to emphasize notes, warnings and new sections.

Documentation Conventions	
Small Caps	Field names.
Bold Small Caps	Names of publications.
Bold Italics	Emphasis.
`Courier`	Screen text.
<brackets>	Names of keyboard keys, e.g., <Return>, <F12>.

Notes are indicated by an indented, italicized headline.

The Note body copy is further indented.

“How to” sections are indicated by an indented, bold headline.

The “How to” body copy is unbolded and closed with a rule line.

Additional Documentation

Documentation is available for GTA Firewall product owners. Product Guides show how to install and set up GTA Firewall products. Feature Guides describe GTA optional features. The GNAT Box System Software User's Guide includes advanced configuration functions, descriptions of GBAdmin and the Web interface, administrative tools and GNAT Box-specific terms.

Documentation Map

Topic	Document Name	Location
Installation	Product Guides	Shipped w/product*
System Setup	Product Guides	Shipped w/product*
GNAT Box Concepts	Concepts	www.gta.com
Troubleshooting	User's Guide or Product Guides	Shipped w/product, CD*
Configuration examples	–	www.gta.com
Sample reports	–	www.gta.com
Ports & Services	User's Guide	Shipped w/product, CD*
Drivers & NICs (Pro, Flash)	Product Guides	Shipped w/product*
GTA Firewalls	Product Guides	Shipped w/product*
Content Filtering	Surf Sentinel Feature Guide	Shipped w/product*
High Availability	H_2A Feature Guide	Shipped w/product*
VPN	GNAT Box VPN Feature Guide	Shipped w/product*
VPN Examples	GB-VPN to VPN Tech Docs	www.gta.com
GBAdmin interface	User's Guide	Shipped w/product, CD*
GBAdmin Help	GBAdmin Online Help	Shipped w/product, CD*
Web interface	User's Guide	Shipped w/product, CD*
Console interface	Console Interface Tech Doc	www.gta.com

* All documents for registered products can also be found on the www.gta.com website.

User Interfaces

GNAT Box System Software, GTA's operating system running on the GB-Flash, has three user interfaces: GBAdmin, the Web interface and the Console interface. For more information about the interfaces, see the GNAT Box System Software User's Guide and www.gta.com.

GBAdmin

GBAdmin is a Windows-based interface that can be operated without access to the Internet. The program has on-screen Help and uses standard Windows commands and conventions. It also requires a Windows-based computer or workstation and Internet Explorer, version 5.0 and up.

Web Interface

The Web interface can be used on any compatible browser, including Internet Explorer, Netscape Navigator, Mozilla and Opera, running on platforms such as Windows, Unix and Mac, with any caveats noted in the appropriate product guides and release notes.

Console

After setup, the Console interface is used for limited configuration changes and to reset the firewall to factory defaults. After initial configuration, you can select either the Video Console interface or the Serial Console interface.

The Video Console is accessed directly on the target system using a monitor and keyboard. The Serial Console is accessed from a terminal emulator installed on an administration workstation and attached through the system's serial port. For further Console interface instructions, see the **Console Interface User's Guide** at www.gta.com.

About GB-Flash

GB-Flash is a complete firewall running from a flash module installed in the user's Intel-based hardware. The GB-Flash contains Global Technology Associates' latest software technology. After installation on the target system, GB-Flash must be configured for local network requirements.

The Product Guide describes and explains how to install, set up and initially configure the GB-Flash. For more instructions on user interfaces and configuration options, see the GNAT Box® System Software User's Guide.

Features

- Stateful Packet Inspection
- Unlimited user license
- Built-in IPSec Manual Key Exchange VPN
- 128,000+ concurrent sessions

- ICSA-certified GNAT Box System Software
- Dynamic & static Network Address Translation (NAT)
* IP aliasing
- RIP support
- Stealth mode
- Remote logging
- Secure encrypted remote management
- Multimedia Application support (Real Audio, QuickTime Streaming)
- Secure Email Proxy (SMTP)
- ISDN TA/Async modem support

Software Specifications

- Max Concurrent Connections: 128,000+
- Remote Access Filters: 400
- Outbound Filters: 400
- Tunnels: 300
- Aliases: 300
- Static Routes: 300
- Static Maps: 300
- Time Groups: 100
- IP Pass Through Filters: 400
- VPN Security Associations: 300
- Objects: 300

CD-ROM Distribution

GB-Flash software is distributed on an ISO 9660-compliant CD-ROM. While a CD-ROM is not a required component of the GB-Flash, the user will need a CD-ROM drive in order to create a GNAT Box runtime floppy disk for reinstallation from the Installation CD-ROM. A DOS, Windows 98, 2000, NT or XP, Macintosh or Unix system may be used to create the runtime disk, as long as the system can read an ISO 9660 CD-ROM.

Options

- Mobile VPN Clients
- Surf Sentinel
- Multi-Interface Option
- Support Contract

Hardware

The GB-Flash is designed to operate efficiently on a broad spectrum of hardware, but the hardware you select will impact the GB-Flash's performance. This is especially true when the GB-Flash is used in an Intranet configuration with full network speeds on all interfaces. The best possible performance can be obtained by using a Pentium CPU with PCI based network cards. However, organizations with low speed (56Kb or less) Internet connections will find that 486 ISA based systems perform satisfactorily. Check www.gta.com for an up-to-date list of compatible NICs and drivers.

Network performance bottlenecks usually occur at the connection to the Internet when using DSL or T-1 class connectivity. A GB-Flash with 10 Mbps Ethernet cards easily provides enough throughput for network connectivity of up to T-1 speeds (1.5 Mbps). However, when the WAN connectivity is a T-3 or faster, GTA recommends that 100Mbps be used.

If you encounter problems, check your motherboard and IRQ assignments. Make sure any unused devices, such as IDE and SCSI controllers, sound cards and serial ports are disabled. Scan the hardware configuration report for error messages–often the cause of a problem is indicated in this report.

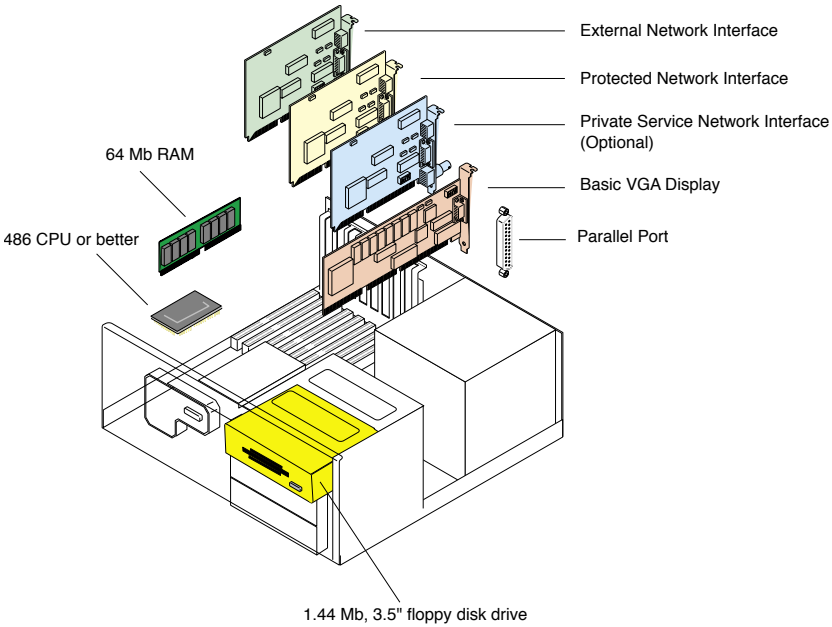
Note

Check www.gta.com for an up-to-date list of compatible NICs and drivers.

Hardware Requirements for GB-Flash

Qty	Description
1	Intel or compatible, 486 or better
1	64 MB RAM
1	1.44 Mbyte 3.5" disk drive
2	Supported network interface cards (minimum)
1	Basic VGA display adapter
1	Parallel printer port
1	Monitor (installation only)
1	Keyboard (installation only)
18	Additional NICs supported with Multi-interface option
1	Serial Port - COM 1-4 (1645x/1655x UARTs only)
1	Async modem for PPP connections or pager
1	ISDN TA with RS-232 interface for PPP connections

* Multi-interface option supports up to 20 total NICs.



Hardware Diagram

Note

GTA recommends only installing the required components in the system. Devices such as SCSI controllers, sound cards and hard disks remain unused and may complicate installation and compromise performance.

PPP Hardware

The GNAT Box System Software supports the use of a PPP network connection in place of a network interface card for the External Network interface. The PPP interface supports only a dial-up connection and a single remote system configuration.

- An external asynchronous modem. COM ports 1-4 are supported; only COM ports based on the 1645x/1655x UARTs are supported.
- An internal asynchronous modem. Only modems that use 1645x/1655x compliant UARTs are supported.
- An ISDN external modem/terminal adapter. COM ports 1-4 are supported; only COM ports based on the 1645x/1655x compliant UARTs are supported.
- NIC card for use with PPPoE (ADSL).

Serial Ports

Most serial ports will easily support any asynchronous modem or a single BRI 64KB ISDN connection. If both channels of a BRI line are used to achieve 128KB, throughput may be limited to 115KB, due to serial port limitations.

Modem/ISDN TA Configuration

GTA recommends configuring the modem or ISDN TA on another system before installing it on the GTA Firewall Appliance. Most modems allow the storage of a user configuration and the recall of this configuration using a specific command (e.g., ATZ). It is usually easiest to recall a configuration and set the modem to a known state with a few commands.

Note

The default configuration for most modems will generally work.

It's recommended to configure the modem to use a fixed DTE speed (the speed at which the computer talks to the modem). If the modem supports DTE speeds of 38,400 or 57,600, use one of these values to ensure the highest throughput. Configure your serial port to the highest possible speed when using an ISDN TA. Unless you wish to connect at a specific speed, set DCE (the speed at which the modem talks to a remote modem) to auto-negotiate.

Cable Modems and xDSL Configurations

Cable modems and xDSL configurations utilize a passive inter-connection device (cable modem, xDSL box) that is typically connected to an Ethernet card via a special network patch cable (crossover cable).

Memory Requirements

The GNAT Box System Software can operate with a memory size as small as 32 megabytes. However, you should consider certain factors when selecting a memory configuration for your GB-Flash. The table below lists the maximum concurrent sessions possible for a given memory configuration.

GB-Flash Memory and Concurrent Connections

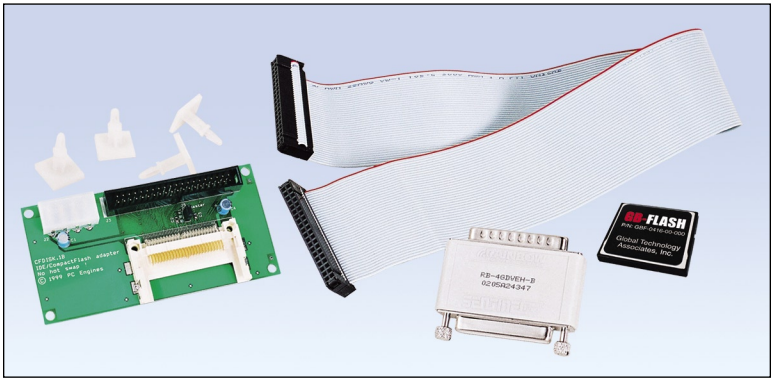
RAM	GB-Flash
32	13,312
40	19,456
64	32,765
128	128,000

* Generally, the more services that are being utilized (e.g., local Access Control Lists, Email Proxy), the more RAM is recommended for optimum performance.

2 Installation

GB-Flash Components

The GB-Flash Firewall Appliance comes with all the components pictured below: (clockwise) mounting posts, IDE cable, flash card, hardware key block and flash adapter board. This guide illustrates how to install these components on an example system; the target system illustrated is only one of the many configurations that can be used with the GB-Flash.



GB-Flash Components

Assemble Components

Assemble your components and target system. Do not plug in any part of the system; make sure that you are properly grounded to prevent static electricity discharge before opening the case.

Warning!!

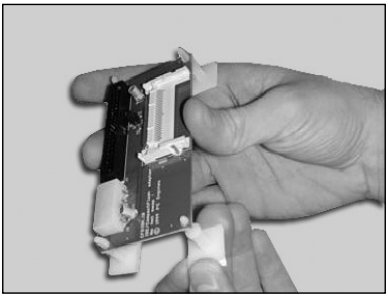
Improper grounding can damage your system or flash card, and may cause physical injury or death.

Verify Disk Drive (optional)

If you will be using the Video Console interface and a disk drive to produce your Recovery floppy disks, verify that the floppy disk drive is plugged in and has a functional power connection. Do not apply power yet.

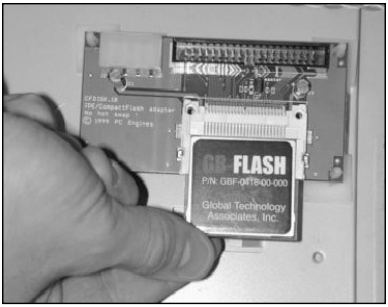
Assemble GB-Flash Module

Insert the four white nylon mounting posts into the mounting holes in the adapter board. (You can also mount the adapter board in a hard disk drive bay using 3.5” hard disk drive mounting hardware.)



Insert the mounting posts into the adapter board

Holding the flash card with the label up, slide the card into the slot on the adapter board, pinholes in, until firmly and evenly seated.



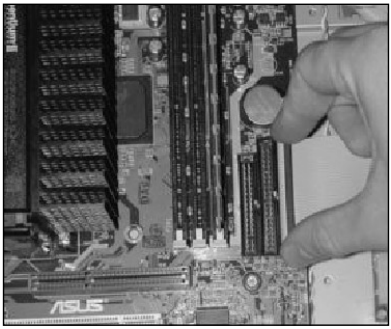
Insert the flash module into the adapter board

Install GB-Flash Module

Open the case of your target machine. (Please contact the case manufacturer if you have additional questions on how to complete this step.)

Locate IDE Ports

Locate the IDE ports on the motherboard, and remove anything that is plugged into them. The GB-Flash will not function properly with other components plugged into the IDE ports. (Refer to the motherboard's user guide if you cannot locate the IDE ports.)



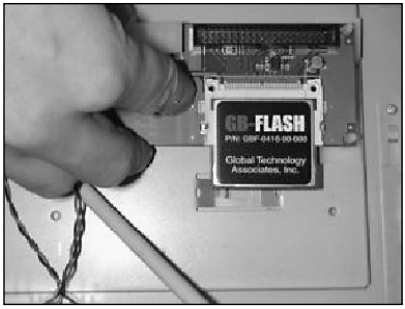
Locate your system's primary IDE port

Mount GB-Flash Module

Remove the protective covers on the bottom of the adapter board mounting posts to expose the adhesive. Mount the adapter board securely inside the system's case; find a place where the components fit easily and securely, and where the IDE cable can easily reach from the adapter board to the primary IDE port. **DO NOT** mount the adapter board onto or near other electronic components inside the case.

Caution

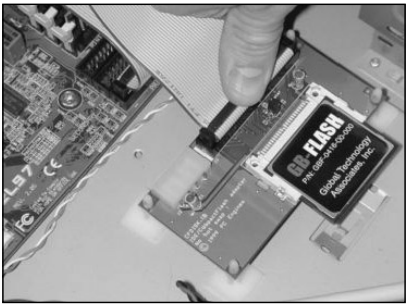
The GB-Flash module is NOT hot-swappable. Never insert or remove the flash module while the power is on. Doing so will damage the flash module, and electrical discharge could cause injury or death.



Mount the GB-Flash module inside the system case

Connect IDE Cable

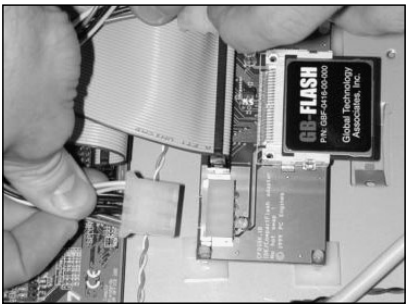
Insert one end of the IDE cable into the primary IDE port with the red-striped side of the cable lined up with pin #1 of the IDE port. Insert the other end of the IDE cable into the IDE port of the adapter board with the red-striped side of the IDE cable nearest to the 4-pin power port.



Attach the IDE cable to the flash adapter board

Connect Power Supply

Locate a 4-pin power connector on your system's power supply, and connect a power cable from it to the 4-pin power port of the adapter board.



Connect the power supply to the 4-pin power port on the adapter board

Close the system case and power on your newly installed GB-Flash system.

Detect IDE from System BIOS

Next, enter the system BIOS to detect the IDE settings. Typically, you can enter the BIOS by pressing <Delete> or <F1> **immediately** after power on.

Note

Steps vary depending on the manufacturer. Consult documentation from the motherboard manufacturer for specific instructions.

Once in the BIOS, load the Setup Defaults and/or the BIOS Defaults.

Locate and run IDE Auto-Detection. The GB-Flash Module should be auto-detected on the primary IDE port with the following values:

Size	15
Cylinders	15
Heads	32
Precomp	0
Landing Zone	247
Sectors	63
Mode	LBA

If these values are correct, select Save.

If the GB-Flash was not auto-detected, or the values are incorrect, find the manual setup and enter the values listed above.

Note

If you have an older system, e.g., Compaq PII 450 686T3 and Desk Pro EN, try setting the PIO mode to 0, then retry auto-detect.

If there is no manual setup, try using the auto-detected settings, and proceed to the next step.

Disable all other IDE devices and exit the BIOS. Your computer should continue the boot process and load the GB-Flash Setup Wizard.

If you still experience problems, contact GTA for installation support.

Hardware Key Block

After setting up the hardware but before initial configuration, install the hardware key block.

GTA's system is different from other key blocks because it is attached only to the GTA Firewall and not to any client workstations. The key block also provides freedom to upgrade or change system hardware: simply attach the hardware key block to the GB-Flash system hardware and boot the runtime disk.

The hardware key block must be installed in the parallel (printer) port. The side to be attached to the port is labeled COMPUTER, with arrows pointing in the direction of the computer. Screws are provided to connect the key block securely to the port. If the computer is close to a wall or other obstacle, you can attach an extension cable to the port, then attach the hardware key block to the cable. Use a straight-through, 25-pin, male-to-female cable.

If the Hardware Key Block is not recognized by your system, and you have checked that your serial number and activation code are both entered correctly, make sure that your system's parallel port is set to the values below.

Hardware Key Block Settings

Address (Hex Value)	IRQ
0x378	7
0x278	5
Mode	ERP, SPP or Both

Note

Without the key block, the software will operate in Demo mode, in which the system is operational for 180 minutes, decreasing by 30 minutes at each reboot.)

Utilities & Documentation

Prior to setting up the GB-Flash, install any utility software and documentation you would like to use on your workstation. If the workstation is running Windows 95, 98, NT, Me, XP or 2000, there is an automated installer on the CD-ROM that will install these files. If the workstation is running a non-Windows based OS or an older version of Windows, follow the instructions for your platform. These instructions are also available in the ReadMe in the directory on the CD-ROM for your OS.

Insert the CD-ROM into a CD-ROM drive; the installer should auto-start.

If the installer doesn't start automatically, open the "My Computer" icon on your desktop by double-clicking it. Find the GTA Firewall CD icon and open it. Double-click the "Install" icon, launching the installer application.

Options range from a complete install of all software, to copying just the GNAT Box System Software runtime image to your hard disk. A complete installation includes GNAT Box System Software, GBAdmin, the remote logging client, the database client, Acrobat PDF manuals and useful text files. At a minimum, select the GBAdmin program.

3 Set Up Default Configuration

Load the System

To load the GB-Flash system, apply power, and let the system boot up. (Your monitor and keyboard must be attached. You must have a video card installed in the GB-Flash system hardware.) The Video Console interface, the default interface on the GB-Flash, will start automatically.

There are three virtual modes on the Video Console: log messages, the main interface and statistics. View log messages by pressing <ALT><F1>. Press <ALT><F2> to switch to the main interface. These keys are always active. After initial setup, see firewall statistics by pressing <ALT><F3>. For more information, see the CONSOLE INTERFACE USER'S GUIDE, available on the installation CD and on the web at www.gta.com.

Video Console Interface Keystroke Guide

Function	Keystroke
Exit/Abort	<Esc>
Clear field	<F6>
Previous field	<F7>
Next field	<F8> or <Tab>
Delete/Backspace	<Del> or <Backspace>
Toggle choice list	<Space Bar>
Display choice list	<F2>
Toggle color	<F12>
Save	<F10>
Insert	<Insert Key>
Select a button	<Space Bar>

Once the system kernel is loaded, it will begin to probe for system hardware. To verify that the system has discovered and recognized your network cards, press <Alt><F1> to see the log messages. To scroll through the messages, engage the Scroll Lock key, and use either the <Page Up> and <Page Down> keys, or the up/down <Arrow> keys.

After the system has been loaded and configured, you can also view this using the Configuration Verification item on the Console or View Log Messages under the System Activity Menu using GBAdmin or the Web interface.

If your hardware was configured correctly and the system did not encounter any problems, the Setup Wizard should appear.

Selecting the Serial Console Interface

To use the Serial Console interface, provided as an option in GB-Flash, you must perform a “Re-Flash,” i.e., reinstall the system software using the “sio” runtime image and merge your customized configuration. This re-flash process is also used if the GB-Flash needs to be re-installed. See the Appendix for more instructions.

Using the Setup Wizard

GTA recommends using the GB-Flash Setup Wizard for easy firewall setup. There are a number of options in the GB-Flash setup: a configuration in which the External Network interface is PPP or PPPoE; a one in which one or both required network interfaces is DHCP; or a configuration in which both interfaces are static connections, neither PPP or DHCP. After step #4, select the option appropriate to your connection type.

1. GNAT Box Licensing Agreement

Move the cursor to “View License”; if you agree to the terms, select <Esc> to return to the previous display and select “Accept.” If you don’t accept the terms, select “Do Not Accept” to terminate the software installation.

2. GNAT Box Wizard

The next dialog box will prompt you to use the GNAT Box Wizard. Select “OK.” If you choose not to use the Wizard, select “Cancel.”

Note

Canceling will call up the “Network Information” screen, which must be completed to continue the boot process. See the **Console Interface User’s Guide** at www.gta.com for a complete reference.

Setup Wizard

3. Host Name

The next dialog box will prompt you for the Host Name of your GTA Firewall. The host name identifies your GTA Firewall system, but is not a fully-qualified domain name. Once you enter the name, select Next.

4. Contact Information

In the next dialog box, fill in the contact information and serial number for your GTA Firewall. The activation code and serial number are located on the product box, the registration card, and on the GTA website under Support after registration.

5a. PPP/PPPoE Runtime Image

The next dialog box will ask whether or not you wish to use PPP on the External interface. Select “No” if you will not be using PPP/PPPoE, and go to step 5b.

Otherwise, select “Yes” by toggling the field value and selecting Next, and go to page 21, PPP/PPPoE Configuration, step A. You must load the PPP runtime image to use PPP/PPPoE.

Use PPP?

5b. DHCP (No PPP/PPPoE)

The next dialog box offers to run DHCP on the network interface. If your system will not utilize DHCP on the selected interface, select “No,” and go to step 5c.

If your system will use DHCP on the selected interface, go to step 6. (Typically, cable modem and xDSL sites use DHCP.)

Run DHCP?

5c. IP Address (No DHCP)

If you do not choose to use DHCP on the interface, the dialogs in step 5c will prompt you for the IP address and subnet of the network interface.

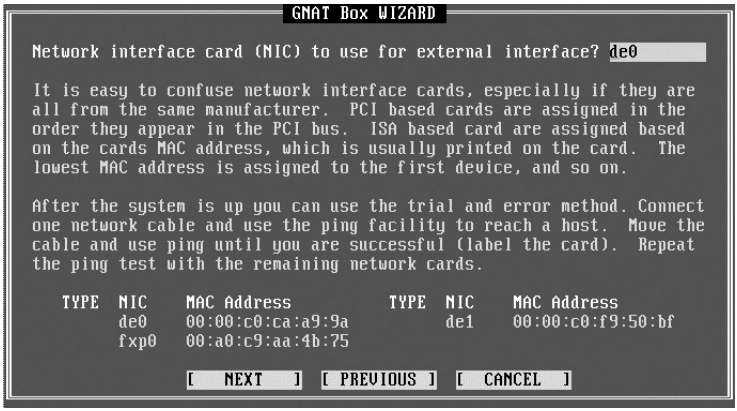
The IP address for the External Network interface should be a valid registered IP address if you will be connecting to the Internet.

6. Network Interface Card for the External, Protected or PSN

Next, select an available NIC (Network Interface Card) to assign to the interface. Use <F2> or the <space bar> to select from the device list. Each NIC detected on your system and its MAC address are listed at the bottom of the screen.

Note

All networks or sub-networks attached to a GTA Firewall interface must be on a logically different network from one another.



Select Network Interface Card

7. Protected Network Interface

The following set of dialogs assist you in selecting DHCP and NIC or assigning an IP address, subnet and NIC device for the Protected Network. (The Protected Network interface is required.) Use steps 5b, 5c, and 6. If you are not setting up a PSN at this time, go to step #9.

Note

Because GTA Firewalls perform NAT (Network Address Translation), the IP address and any network addresses behind the GTA Firewall (i.e., attached to, or on the Protected Network or PSN) can be unregistered.

8. Private Service Network Interface (Optional)

The following set of dialogs assist you in selecting DHCP and NIC or assigning an IP address, subnet and NIC device for the PSN. (The PSN interface is optional.) Use steps 5b, 5c, and 6. Once you have set up the PSN at this time, go to step #9.

Note

If you are setting up a new network, GTA recommends choosing network addresses described in RFC 1918. The Internet Assignment Numbers Authority (IANA) has specified network addresses in RFC 1918 that are designated exclusively for private networks.

IANA Private Networks

Qty	Network Type	Address Range
1	Class A	10.0.0.0 - 10.255.255.255
16	Class B	172.16.0.0 - 172.31.255.255
255	Class C	192.168.0.0 - 192.168.255.255

9. Gateway/Default Route on External Interface (No DHCP or PPP/PPPoE)

If your External Interface is not DHCP, complete this step.

Once the IP address, netmask, and device assignment have been made, you will be prompted for the default route for your GTA Firewall system. The Setup Wizard will have already determined the network portion of the IP address, so only the host portion needs to be entered.

10. Password

Next, assign a password to your GTA Firewall system (required). The dialog will provide data entry fields for password assignment. Initially, the User ID is set to “gnatbox”, however, it can be changed later in Admin Accounts under the Authorization menu.

Note

GTA recommends changing the default user ID and password. See the **GNAT Box System Software User's Guide** for instructions.

The summary screen displays all your configuration settings. If you need to make changes, use the “Previous” button to move back to the desired dialog and make corrections. You cannot make changes directly to the summary.

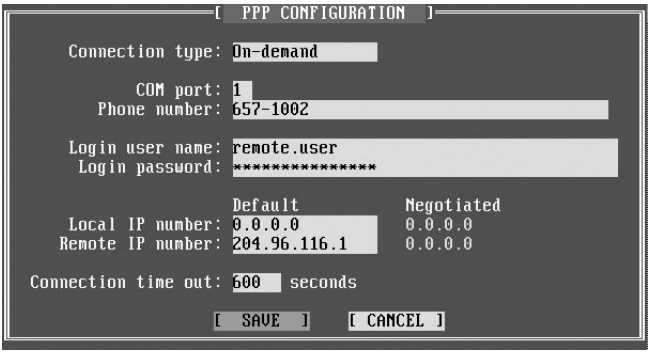
Once you are satisfied with your settings, select Save and allow the GTA Firewall to boot up into its fully operational mode. Initial configuration is complete. Go to the last section in this chapter, “Access the GB-Flash.”

PPP/PPPoE Configuration

As an alternative to the typical External Network configuration that uses a network interface card (NIC) and stand-alone router, a GTA Firewall can be configured to use serial PPP (Point-to-Point Protocol) or PPPoE (PPP over Ethernet, which uses a NIC connected to a DSL modem) for the External Network interface. The PPP/PPPoE interface can utilize internal and external async modems and external ISDN TAs.

To configure PPP/PPPoE, you must have already set up and installed your communications device according to the GB-Flash hardware installation instructions and the device manufacturer's guidelines.

The steps in this section, designated A-F, continue from step #5a of the instructions. Note that the selections in step B are different.



PPP Configuration

When you have finished the PPP/PPPoE portion of the setup, return to the previous section and complete steps #7 through #10.

Note

Using the Console interface, only the first (PPP0) of the five available PPP (Point-to-Point Protocol) and PPPoE (PPP over Ethernet) connections may be configured. Use the Web interface or GBAdmin to configure additional PPP/PPPoE connections. See the **GNAT Box System Software User's Guide** for more information.

A. Connection type

On-Demand: If the link is down, an on-demand connection will initiate and establish a connection with the remote site whenever a packet arrives on the Protected Network or PSN and is destined for the External Network. The link will stay established unless the time-out period expires.

On-Enabled: An on-enabled connection requires the administrator to manually enable the External Network interface, initiating a session and establishing a link with the remote site. The External Network interface may be enabled either from Admin -> Interfaces menu item on the Console interface or from the Administration -> Interfaces item on the Web interface. The link will stay established until manually disabled.

Dedicated: A dedicated connection establishes a link when the firewall boots up. The link will stay established until manually disabled, or the system is halted.

B. PPP/PPPoE

PPPoE Configuration

i. Select PPPoE if you are creating a connection over Ethernet.

ii. Select NIC to be used for the PPPoE connection.

iii. Leave the PROVIDER field blank unless you know the **exact** designation. An incorrect ISP name will cause the connection to fail.

PPP Configuration

i. Leave PPPoE unchecked (deselected) if you are using PPP.

ii. Select the COM port, internal modem card or serial interface, to be used for the PPP interface. COM ports 1-4 are allowed.

iii. Enter the telephone number of the remote site, The number should contain any special access codes or dialing directives required to call the remote site. Special characters used for pauses and secondary dial tones can be used. Consult your modem or ISDN TA manual for dialing codes.

C. User ID and Password for Connection

Enter the login user ID and password, then enter the user ID issued by the remote site for PPP access, and the associated password. The password is obscured in the data entry field.

D. Assign IP numbers

A PPP/PPPoE link uses two IP addresses, one local and one remote. GNAT Box System Software is capable of negotiating the addresses dynamically if the remote site supports dynamic address assignment, the default for ISPs and remote sites. Dedicated IP addresses are supported for either, or both, sides of the connection.

How to make dynamic and static IP Address assignments

Both local and remote sites use dynamic address assignment:

- Leave the LOCAL IP ADDRESS field set to 0.0.0.0, the default.
- In the REMOTE IP ADDRESS field, enter an IP address that may be assigned dynamically. It is not important that the IP number is actually

the one assigned, since this value will be negotiated. However, the PPP protocol requires that an IP address be used that resides on the remote network. A good choice for this number is the remote system's router IP address or DNS server IP address.

Both local and remote sites use static address assignment:

- In the LOCAL IP ADDRESS field, enter the dedicated IP address.
- In the REMOTE IP ADDRESS field, enter the dedicated IP address.

Local site uses static assignment, remote site uses dynamic:

- In the LOCAL IP ADDRESS field, enter the dedicated IP address.
- In the REMOTE IP ADDRESS field, enter an IP address that may be assigned dynamically. It is not important that the IP number is actually the one assigned, since this value will be negotiated. However, the PPP protocol requires that an IP address be used that resides on the remote network. A good choice for this number is the remote system's router IP address or DNS server IP address.

Local site uses dynamic assignment, remote site uses static:

- Leave the LOCAL IP ADDRESS field set to 0.0.0.0, the default.
- Enter the dedicated (static) Remote IP address.

E. Connection Time-out Value

Set the connection time-out value, the number of seconds of inactivity that the PPP link should wait before dropping a connection. A zero value indicates that no time out should be used.

F. Save, Continue with Step #7

Save your PPP configuration, select the Next button, and continue using the configuration instructions, starting with step #7 on page 22.

Access the GB-Flash

After completing the initial configuration in the Setup Wizard, your GTA Firewall should be active and functioning in default security mode, in which all internal users are allowed outbound, and no unsolicited connections are allowed inbound.

After testing connectivity, you should use the Web interface or GBAdmin to modify the system configuration to your local requirements. See the GNAT BOX SYSTEM SOFTWARE USER'S GUIDE for more information.

4 Troubleshooting Guidelines

GTA Support recommends the following guidelines as a starting point when troubleshooting network problems:

- Start with the simplest case of locally attached hosts.
- Use IP numbers, not names. Your real problem could be DNS.
- Work with one network segment at a time.
- Verify your system configuration with the Verification Configuration feature. The verification check is the best method of ensuring that your system is configured correctly. Correct all errors and warnings listed.
- Your first tests should be connectivity tests. Ping and Traceroute are very useful tools for testing connectivity.
- Make sure the network cabling is connected to the correct network interface. It is easy to confuse network interface ports. Some useful guidelines are:
    - In a GB-Flash, the port/NIC numbers, MAC addresses and logical names are listed on the Network Information screen and in the Configuration Report.
    - Use the trial and error method. Connect one network cable and use the ping facility to reach a host on the desired network. Move the cable and use ping until you are successful. Connect the next network cable and perform the test again with the two remaining network interface cards.
    - Generate a hardware report from one of the user interfaces. Check the report to ensure all your network devices have been recognized by the system at boot time.

Troubleshooting Q & A

1. Why can't *all* hosts behind the firewall reach the Internet?

This is usually a routing problem. The Traceroute facility can be very useful in debugging routing problems. Check for these problems:

- Are the hosts that can't reach the Internet on a different network subnet?
- Have you added a static route to the GTA Firewall to tell it which router is used to reach the problem network? Have you set the router's default route to be the GTA Firewall? Have you set the default route for hosts on the problem network to be the router?
- Is the wrong IP address assigned? All network interfaces on the GTA Firewall must be on different logical networks.
- Is the default route assigned incorrectly? The default route must always be on the same subnet as the network interface of the host (this is true for all hosts, not just the GTA Firewall). For a GB-Flash, the default route must be an IP address on the network which is attached to the External Network interface.

Exception

When using PPP or PPPoE, the default route is not necessarily on the same subnet. The route is assigned by your PPP provider.

2. Why can't *one* host behind the firewall reach the Internet?

This indicates that the default route is assigned incorrectly (or not at all) to hosts on the Protected or Private Service networks. All hosts protected by the GTA Firewall must use the IP address of the network interface for the respective network. Hosts that reside behind routers or other gateways on these networks generally use the IP address of the gateway or router.

3. Why can't I access the Web interface from the Protected Network?

The default Remote Access filter set is generated from the configuration parameters entered in the Network Information screen. It is possible that the Protected Network interface is on a different subnet from the remote host. Check the Remote Access filter for the Web interface; it may need to be adjusted.

4. Why do I get errors when GBAdmin starts up? Why is online help information not displayed?

GBAdmin requires Microsoft Internet Explorer 5.x or later installed on your workstation. Components from Internet Explorer are used to display the online help information.

For more Troubleshooting suggestions, see the GNAT Box System Software User's Guide and GTA's website at www.gta.com.

5. Why can't I see or ping the Protected Network interface?

You may have the wrong cable for your connection.

- For a direct connection (GTA Firewall to host or router) you need a crossover cable.
- For a connection to a hub or switch you need straight-through cables.

Note

To distinguish between a crossover cable and a straight-through cable, compare the connection ends. On a straight-through cable, the wire order matches; on a crossover cable, the first three of the four cables are in reverse order.

6. Why is my system booting up in demo mode instead of going to the Setup Wizard?

- Check your serial number and activation code.
- If both of these numbers are correct, it may mean that the Hardware Key Block is not being recognized by your system. Set your system's parallel port to the values below, and try rebooting your system.

Hardware Key Block Settings		
Address (hex value)	0x378	0x278
IRQ	7	5
Mode	ERP, SPP or Both	

Re-install

If you need to perform a complete re-install, or you would like to use the Serial Console interface, a set of disk images have been provided. These images are an installer disk image and three system software disk images.

How to Reinstall GB-Flash

Run the GB-Flash install program (e.g., gbflashv332.exe). If you want to use the Video Console interface, select the basic executable; if you want to use the Serial Console interface, select the sio version.

Make the re-install floppy disk set by selecting the gbMakeFloppies menu item from the workstation where you install the GB-Flash software.

Unix/Linux

Use the ‘dd’ command to create the recovery disks. The floppy disk device name will vary with each version of Unix/Linux, so use the appropriate raw floppy device for your Unix variant.

Macintosh OS9

The runtime disk images have been stored in a Stuffit archive, in the DiskDup+ format. Unstuff the archive by double-clicking the Mac OS9 .sit file. Launch DiskDup+ to create the runtime disk images.

Macintosh OSX

The runtime disk images have been stored in a WinZip archive. Unstuff the archive by double-clicking the Mac OSX .tar file; Mac OSX will create folder on the desktop. Double-click the folder to show the GNAT Box disk images .flp files.

Label the three disks:

- Installer Disk - GB Boot Recovery Installer Disk
- Disk Image 1 - GB-Flash Runtime Recovery Disk Image 1
- Disk Image 2 - GB-Flash Runtime Recovery Disk Image 2
- Disk Image 3 - GB-Flash Runtime Recovery Disk Image 3

Boot the GB-Flash using the Installer Disk.

If you are using the Video Console interface, the Console interface will open on the GB-Flash. If you are using the Serial Console interface, connected to a workstation through the serial port of the GB-Flash, use your terminal emulator to contact the firewall and continue the installation steps.

Once you accept the software license, the install wizard will walk you through the upgrade. You will be prompted to: save your configuration before installing; remove the Boot floppy; and select OK to begin install.

When prompted: “Do you want to restore your GNAT Box configuration?” select NO.

When prompted: “Do you want to preserve your old configuration?” select NO. (Answering YES will not reformat the flash module.)

When prompted: “Delete all existing configuration data?” select OK.

Insert Disk Image 1 when prompted and press the <Return> key. (Disk Image 1 processing may take a few minutes.)

When prompted: “Load next storage media” insert Disk Image 2. When prompted, enter “y” in the command line and press <Return>.

When prompted: “Load next storage media” insert Disk Image 3.

When prompted, enter “y” in the command line and press <Return>.

When installation is complete, you will be prompted to remove the last disk. Press <Return> to re-boot the GB-Flash. The system will reboot at this point and go into the standard GNAT Box system set up wizard for new installations.

After completing the wizard, you may enter your new activation code and perform any additional configuration tasks using GBAdmin or the Web interface. Restore your saved configuration data manually.

Appendix

Upgrading to GB-Flash from GB-Pro

This section is intended as a guide for those users upgrading from a GB-Pro Firewall System, version 2.1 and higher, to a GB-Flash Firewall Appliance. Those upgrading from GB-Pro 2.x and lower will need to re-enter all configuration information manually.

Note

You may want to print your configuration so you will have the network IP addresses and gateway (default route) IP address for setup.

To upgrade, you must have a viable GB-Pro configuration saved to floppy disk or to a hard disk drive. The upgrade will be similar to a normal GB-Flash initial installation.

Power up the GB-Flash. When the system completes the boot process, it will be unregistered and unconfigured. You will be prompted to use the GB-Flash Setup Wizard; select OK.

In the HOST NAME field, enter the name you have selected or use the default. Next, enter your contact information and the new serial number issued with your product. The correct serial number is required; your system will not be registered properly without it. In the next dialog, enter the registration code that came with your GB-Flash product.

Continue using the Setup Wizard, following the instructions in Chapter 3.

Note

For the upgrade, the Protected Network interface is particularly important; you will use the Protected interface to connect to the GB-Flash using GBAdmin or the Web interface, and transfer the GB-Pro configuration. You need not be concerned with the PSN at this time.

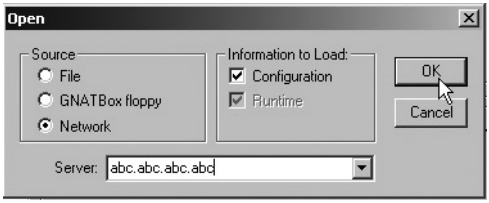
Once you have completed the Setup Wizard, the Protected Network interface should be able to access the GB-Flash.

Note

GTA recommends using GBAdmin to continue the upgrade.

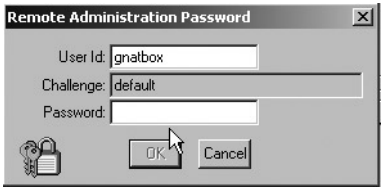
Upgrade Using GBAdmin

The GB-Flash software must be installed on your workstation. Locate your new version of GBAdmin. (In Windows, go to Start Menu -> Programs -> GTA -> GB-Flash 3.X.X -> GBAdmin.) In GBAdmin, click File -> Open, then Source -> Network. In the SOURCE field, enter the Protected Network interface IP address of the GB-Flash.



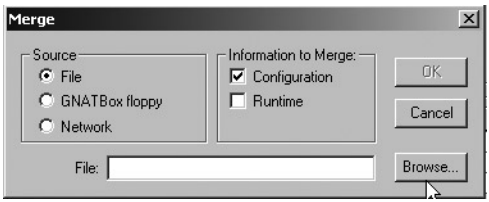
File -> Open -> Protected Network IP Address

GBAdmin will connect to the GB-Flash system and prompt you for the User ID and Password selected during installation. The GB-Flash system will load.



Login Dialog Box

To merge the old GB-Pro configuration onto the GB-Flash, click File -> Merge. A warning will display, asking if you wish to overwrite your current settings. Click "Yes." In the Merge dialog box, select File in the SOURCE field. In the INFORMATION TO MERGE field, select "Configuration" only. Do NOT check the Runtime checkbox.

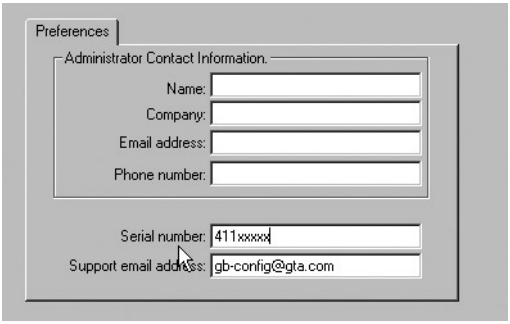


File -> Merge -> GB332_010101.GBcfg

Next, select Browse and find the directory where you saved the old GB-Pro configuration. Once you have selected that file, click “OK.”

In the password dialog box, enter the password used on your saved configuration. After entering it, press <return> to load the GB-Pro Configuration.

Go to Basic Configuration -> Preferences. Verify that the serial number for your new GB-Flash is entered. If you did not enter your serial number in the Setup Wizard, this field will contain the GB-Pro serial number. Enter your new system serial number. A GB-Flash upgrade number should begin with 41.

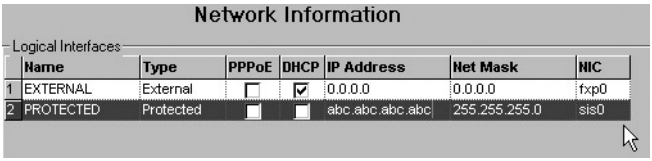


Verify Contact Information

Go to Basic Configuration -> Features. Verify that the system appears as registered, and that the 32 character activation code for your GB-Flash is displayed with a description. If the description is not correct, verify that the code is entered correctly, and the serial number is entered correctly in Preferences.

Registration and Feature Codes

Go to Basic Configuration -> Network Information. Verify that all your interfaces have been recognized and that they have the proper NICs selected.



	Name	Type	PPPoE	DHCP	IP Address	Net Mask	NIC
1	EXTERNAL	External	☐	☑	0.0.0.0	0.0.0.0	fxp0
2	PROTECTED	Protected	☐	☐	abc.abc.abc.abc	255.255.255.0	sis0

Network Information

Note

If your NIC card is not listed, then its possible that if you are upgrading from an older version in which that NIC was supported. Please contact support with any question on this matter. Additionally, if you are placing the config on a new system with different Network Interface Cards, you will need to re-select your cards.

Now, save the configuration to the firewall by clicking on the Save All button on the toolbar or by selecting File -> Save All. This will save the entire configuration and any changes you have made to the GB-Flash system.

Note

If you change the IP address you used in the Setup Wizard you will be disconnected. You will need to re-connect to the server on the new IP's.

Index