INTERNET SECURITY SYSTEMS ®

INTERNET|SECURITY|SYSTEMS®

proventia® network

Intrusion Prevention System

Getting Started Guide

GX3002 Appliance

IBM Internet Security Systems, Inc.
6303 Barfield Road
Atlanta, Georgia 30328-4233
United States
(404) 236-2600
http://www.iss.net

Contents

Contents

INTERNET | SECURITY | SYSTEMS®

Preface

Overview

Introduction   This guide is designed to help you connect and configure your Proventia Network IPS GX3002 appliance.

Scope   This guide includes basic information and required procedures for connecting the appliance and configuring basic settings.

Audience   This guide is intended for network security system administrators responsible for installing and configuring Proventia Network Intrusion Prevention System Appliances. A fundamental knowledge of network security policies and IP network configuration is helpful.

About Proventia Appliance Documentation

Introduction
This guide explains how to connect and configure the Proventia Network IPS GX3002 appliance. It also explains how to access the Proventia Manager to install appliance license files and apply initial updates.

Locating additional documentation
Additional documentation described in this topic is available on the ISS Web site at http://www.iss.net/support/documentation/.

Related publications
See the following for more information about the appliance:

Document	Contents
Proventia Network IPS G and GX Appliance User Guide	Provides overviews and procedures for creating and managing policies and responses, as well as maintaining appliance settings.
Proventia Intrusion Products Help	Procedures for creating and managing policies in Proventia Manager and the Proventia Network IPS Policy Editor in SiteProtector.
Proventia Network IPS Data Sheet	General information about previous Proventia Network IPS appliance features.
Proventia Network IPS Frequently Asked Questions	Frequently asked questions about the appliance and its functions.
Readme File	The most current information about product issues and updates, and how to contact Technical Support located at http://www.iss.net/download/.

Table 1: *Reference documentation*

INTERNET|SECURITY|SYSTEMS®

Conventions Used in this Guide

Introduction   This topic explains the typographic conventions used in this guide to make information in procedures and commands easier to recognize.

In procedures   The typographic conventions used in procedures are shown in the following table:

Convention	What it Indicates	Examples
Bold	An element on the graphical user interface.	Type the computer's address in the **IP Address** box. Select the **Print** check box. Click **OK**.
SMALL CAPS	A key on the keyboard.	Press ENTER. Press the PLUS SIGN (+).
Constant width	A file name, folder name, path name, or other information that you must type exactly as shown.	Save the User.txt file in the Addresses folder. Type IUSR__SMA in the **Username** box.
Constant width italic	A file name, folder name, path name, or other information that you must supply.	Type Version *number* in the **Identification information** box.
→	A sequence of commands from the taskbar or menu bar.	From the taskbar, select **Start→Run**. On the **File** menu, select **Utilities→Compare Documents.**

Table 2: *Typographic conventions for procedures*

**Command
conventions**

The typographic conventions used for command lines are shown in the following table:

Convention	What it Indicates	Examples
Constant width bold	Information to type in exactly as shown.	**md ISS**
Italic	Information that varies according to your circumstances.	**md** *your_folder_name*
[ ]	Optional information.	**dir** [*drive:*] [*path*] [*filename*] [**/P**] [**/W**] [**/D**]
|	Two mutually exclusive choices.	**verify** [**ON**|**OFF**]
{ }	A set of choices from which you must choose one.	**% chmod** {**u g o a**}=[**r**] [**w**] [**x**] *file*

Table 3: *Typographic conventions for commands*

INTERNET|SECURITY|SYSTEMS®

Getting Technical Support

Introduction   ISS provides technical support through its Web site and by email or telephone.

The ISS Web site   The Internet Security Systems (ISS) Resource Center Web site (http://www.iss.net/support/) provides direct access to frequently asked questions (FAQs), white papers, online user documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase (http://www.iss.net/support/knowledgebase/).

Support levels   ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24-7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Hours of support   The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 4: *Hours for technical support*

Contact information   The following table provides electronic support information and telephone numbers for technical support requests:

Regional Office	Electronic Support	Telephone Number
North America	Connect to the MYISS section of our Web site: www.iss.net	**Standard:** (1) (888) 447-4861 (toll free) (1) (404) 236-2700 **Select and Premium:** Refer to your Welcome Kit or call your Primary Designated Contact for this information.
Latin America	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Europe, Middle East, and Africa	support@iss.net	(44) (1753) 845105
Asia-Pacific, Australia, and the Philippines	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Japan	support@isskk.co.jp	Domestic: (81) (3) 5740-4065

Table 5: *Contact information for technical support*

INTERNET|SECURITY|SYSTEMS®

Chapter 1

Introducing the Proventia Network IPS GX3002 Appliance

Overview

Introduction   This chapter contains introductory information about deploying your Proventia Network IPS GX3002 appliance.

In this chapter   This chapter contains the following topics:

Topic	Page
Intrusion Prevention	12
Appliance Package Contents	14
About the GX3002 Appliance	15
Network Cabling Guidelines	18

Intrusion Prevention

Introduction   The Proventia Network Intrusion Prevention System (IPS) automatically
blocks malicious attacks while preserving network bandwidth and
availability. The Proventia Network IPS appliances are purpose-built,
Layer 2 network security appliances that you can deploy either at the
gateway or the network to block intrusion attempts, denial of service
(DoS) attacks, malicious code, backdoors, spyware, peer-to-peer
applications, and a growing list of threats without requiring extensive
network reconfiguration.
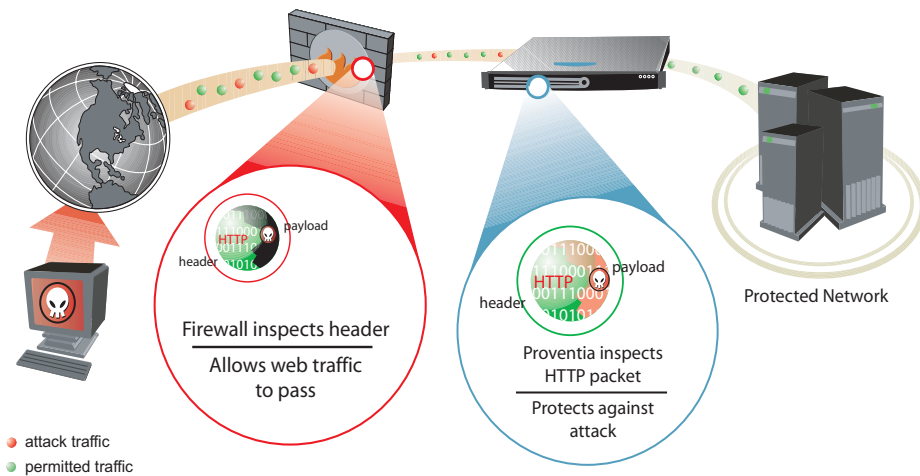
Figure 1: *Intrusion prevention overview*

Figure 1 displays how the Proventia Network IPS protects your network.
With flexible deployment options and out-of-the-box functionality, these
appliances ensure accurate, high-performance protection at both the
network perimeter and across internal networks and internal network
segments.

INTERNET|SECURITY|SYSTEMS®

About IPS monitoring modes

How you connect the appliance to the network depends on the mode in which you want to run the appliance. The inline appliances include the following adaptor modes:

Mode	Responses	Benefits
Inline protection	Block, Quarantine, Firewall	• Monitors network and actively blocks malicious traffic • Allows you to realize the full benefit of the IPS
Inline simulation	Block, Quarantine (Simulated)	• Monitors network without affecting traffic patterns • Helps you baseline and test your security policy
Passive monitoring	Block	• Replicates traditional IDS technology • Monitors traffic without sitting inline

Table 6: *Monitoring modes*

Appliance Package Contents

Introduction   Before you begin, you should verify that you have all of the package
contents necessary to install the appliance.

Verifying the   Verify the appliance package includes the following:
contents

✓	Item
❑	Proventia Network IPS GX3002 appliance
❑	Proventia serial console cable
❑	Ethernet crossover cable
❑	For each inline segment: • a pair of Ethernet cables, straight-through or crossover, depending on your network • a crossover adapter • additional Ethernet cables as needed **Note**: ISS provides one crossover adapter and two one-foot Ethernet cables per segment.
❑	Power cord
❑	Recovery CD pack
❑	Warranty statement
❑	Getting Started Guide

Table 7: *Materials for connecting appliance*

INTERNET|SECURITY|SYSTEMS®

About the GX3002 Appliance

Introduction   Before you connect the appliance to the network, familiarize yourself with the appliance's hardware features.

GX3002 front panel   Figure 2 displays the GX3002 front panel:
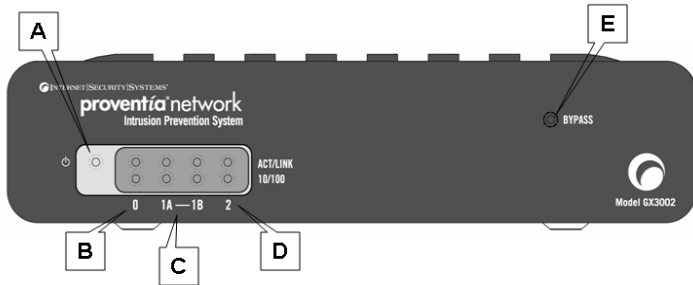
Figure 2: *GX3002 appliance front panel*

The front panel of the GX3002 appliance includes the following:

Label	Description
A	Power indicator.
B	The lights labeled 0 represent RSKill responses passing through the TCP Reset (RSKill) port. If you have configured the appliance for TCP Reset and the lights flash on, the appliance is in active TCP Reset mode. **Note**: Once you connect the appliance to the network through the TCP Reset port, you must configure the appliance to run TCP Reset. See "Configuring TCP Reset" on page 133 in the *Proventia Network IPS G and GX Appliance User Guide*.
C	Lights labeled 1A and 1B represent traffic passing across the protected ports. A green light indicates traffic passing at 100Mbps; no light indicates traffic passing at 10Mbps.
D	Lights labeled 2 represent the Management port, which the appliance uses to communicate with Proventia Manager and the Proventia SiteProtector central management system.

Table 8: *GX3002 front panel label descriptions*

Label	Description
E	When the Bypass light is on, the appliance is passing traffic successfully. If the light turns off, the appliance has gone into bypass mode, which means it has failed open and is no longer monitoring network traffic.

Table 8: *GX3002 front panel label descriptions*

GX3002 back panel   Figure 3 displays the GX3002 back panel:
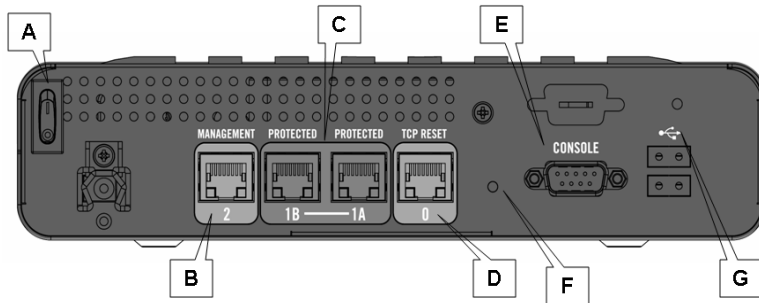
Figure 3: *GX3002 appliance back panel*

The back panel of the GX3002 appliance includes the following:

Label	Description
A	Power button.
B	The appliance uses the Management port to communicate with Proventia Manager and/or the Proventia SiteProtector central management system.
C	The Protected Ports work in either inline intrusion prevention (IPS mode) or passive intrusion detection (IDS mode). Inline intrusion prevention uses both ports in the pair; passive detection uses only the 1A port.

Table 9: *GX3002 back panel label descriptions*

INTERNET|SECURITY|SYSTEMS®

Label	Description
D	The TCP Reset port sends RSKill responses, after you configure the appliance for TCP Reset. For information about configuring TCP Reset, see the *Proventia Network IPS G and GX Appliance User Guide*.
E	The Console port enables terminal-based setup and recovery for the appliance.
F	The appliance reset button.
G	The USB ports are reserved for future use.

Table 9: *GX3002 back panel label descriptions*

Internal bypass   The GX3002 has built-in copper bypass hardware, which by default fails "open," allowing traffic to continue passing through the appliance without being monitored if the appliance fails or loses power.

Network Cabling Guidelines

Introduction

Before you connect the appliance to the network, consider the following guidelines to determine what cabling to use to connect the appliance to the network. Wherever you need a crossover connection, you may use your own Ethernet cable. ISS provides one crossover adapter and two one-foot Ethernet cables per segment. When the appliance is not running, its monitoring ports function as a crossover. The following scenarios work independently of the monitoring port you use.

General cabling guidelines

The following table lists some general cabling guidelines:

Use this Ethernet cable...	In these situations....
Crossover	Between the appliance and a workstation
	Between the appliance and a router
Straight-through	Between the appliance and a switch or hub

Table 10: *General cabling guidelines*

Switch or hub 1 to switch or hub 2

To deploy the appliance between two switches or hubs:

● use a straight-through Ethernet cable from Switch or Hub 1 to the appliance

● use a straight-through Ethernet cable from the appliance to Switch or Hub 2

INTERNET|SECURITY|SYSTEMS®
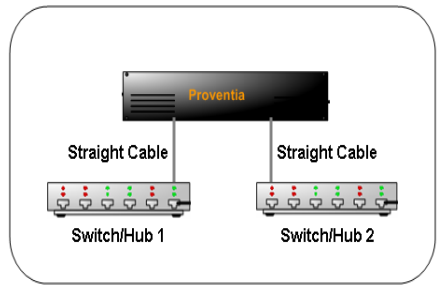
Workstation or server to router

To deploy the appliance between a workstation and a router:

- use an Ethernet crossover cable from the workstation to the appliance
- use an Ethernet crossover cable from the appliance to the router
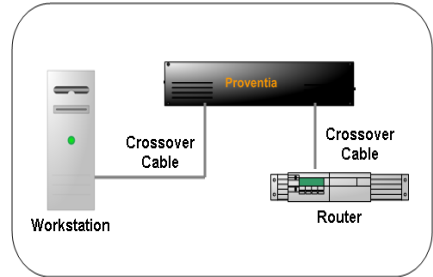
Workstation or server to switch or hub

To deploy the appliance between a workstation and a switch:

- use an Ethernet crossover cable from the workstation to the appliance
- use a straight-through Ethernet cable from the appliance to the switch
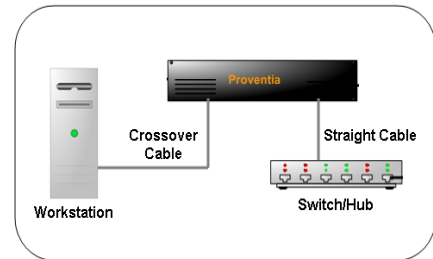
Router to switch or hub

To deploy the appliance between a router and a switch/hub:

- use an Ethernet crossover cable from the router to the appliance
- use a straight -through Ethernet cable from the appliance to the switch or hub
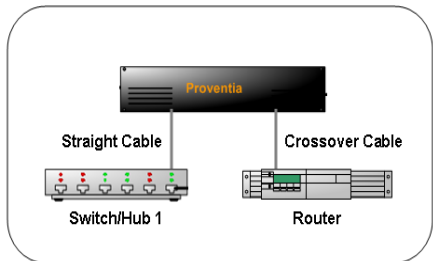
Router to router   To deploy the appliance between
two routers:

● use an Ethernet crossover
cable from Router 1 to the
appliance

● use an Ethernet crossover
cable from the appliance to
Router 2
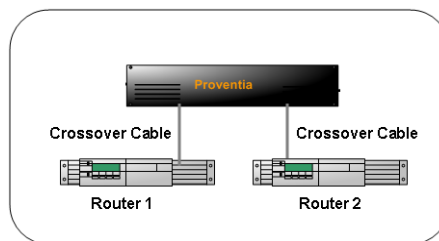
Chapter 2

Getting Started

Overview

Introduction   This chapter contains connection and configuration procedures for the GX3002 appliance. It also includes checklists to help you gather information to complete these tasks.

In this chapter   This chapter contains the following topics:

Getting Started

Setup process overview

Connecting and configuring the GX3002 appliance is an 8-step process:

Step	Description	Where to find the procedure
1	Connect the appliance cables to a computer and turn on the appliance.	"Connecting the Cables and Starting the Appliance" on page 23
2	Connect to the appliance through a serial console or remote connection.	"Connecting to the Appliance" on page 25
3	Gather required information.	"Required information checklist" on page 24
4	Log in to Proventia Setup and configure initial network settings.	"Completing the Initial Configuration" on page 26
5	Verify you have the following: • Internet Explorer version 6.0 or later • Java Runtime Environment (JRE) version 1.5. The application prompts you with an installation link if you do not have it installed.	
6	Open Internet Explorer and log in to Proventia Manager as username **admin** and the password you configured during Proventia Setup.	"Accessing Proventia Manager" on page 29
7	Collect license information and install license.	"Installing the License File" on page 33
8	Apply security and firmware updates.	"Applying Initial Updates" on page 35

Table 11: *Setup process*

Connecting the Cables and Starting the Appliance

Introduction

After you have determined where you plan to place the appliance in your network, you are ready to connect the appliance. You should install the correct network cabling and verify that traffic flows *before* you turn on the appliance.

Important: Keep your management and monitoring communication separate so that network traffic can pass uninterrupted through the appliance's network interface card (NIC).

Connecting the appliance to the network

To connect the appliance to the network:

1. Connect the power cord to the appliance.

2. Connect the **Management** port on the back panel to the network you will use to manage the appliance.

3. Connect the network cables to the **Protected** ports that correspond with the adapter mode (inline or passive) you plan to use for the appliance.

   Note: If you plan to run the appliance in passive mode, you should only connect Protected port 1A to the network.

4. If you want the appliance to send kill responses through the **TCP Reset** port while in inline protection or inline monitoring mode, connect the TCP Reset port to the network.

   Important: The appliance does not send kill responses for TCP events until you have configured the appliance for TCP Reset. See "Configuring TCP Reset" on page 130 in the *Proventia Network IPS G and GX Appliance User Guide*.

5. (Optional) Connect the serial **Console** cable to the appliance if you want to connect a computer directly to the appliance to complete the initial network configuration.

6. Verify that traffic is passing through the appliance.

7. Flip the power switch to the On position.

Required information checklist

Use the checklist in Table 12 to obtain the information you need to configure the IPS appliance.

✓	Setting	Description
☐	Appliance hostname	The unique computer name for your appliance **Example:** *myappliance*
	Your setting:	
☐	Appliance domain name	The domain suffix for the network **Example:** *mydomain.com*
	Your setting:	
☐	Appliance domain name server	This is the IP address of the server you are using to perform domain name lookups (DNS search path). (optional). **Example:** *10.0.0.1*
	Your setting:	
☐	Management Port IP Address	An IP address for the management network adapter.
	Your setting:	
☐	Management port subnet mask	The subnet mask value for the network that will connect to your management port.
	Your setting:	
☐	Management port default gateway (IP address)	This is the IP address for the management gateway.
	Your setting:	
☐	Adapter mode	The adapter (operation) mode to use for the appliance. The adapter mode you plan to use should correspond to the way you connected the network cables.
	Your setting:	

Table 12: *Checklist and worksheet for configuration information*

Connecting to the Appliance

Introduction   If you connected the appliance directly to a computer using the serial Console cable, you are ready to log on the appliance and begin configuring. See "Completing the Initial Configuration" on page 26.

If you want to configure the appliance from a remote computer, follow the procedure below, which explains how to connect to the appliance using Hyperterminal. You may use another terminal emulation program, such as PuTTY, to connect to the appliance, but those procedures are not outlined here. Follow the instructions listed in the documentation for the program you choose.

Procedure   To connect to the appliance remotely using Hyperterminal:

1. On your computer, select **Start→ Programs→ Accessories→ Communications.**

2. Select **Hyperterminal**.

3. Create a new connection using the following settings:

Setting	Value
Communications Port	Typically COM1 (depending on computer setup)
Emulation	VT100
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

4. Press ENTER to establish a connection.

   When the connection is established, the Proventia Setup Configuration Menu appears.

   Tip: If you are unable to establish a connection, ensure the appliance has power and that you have started the appliance.

Completing the Initial Configuration

Introduction   Proventia Setup is the program you use to configure initial appliance network settings.

Procedure   To complete the initial configuration for the appliance:

1. At the unconfigured login prompt, type the user name **admin**, and then press ENTER.

2. Type the default password **admin**.

3. Select **Start**, and then press ENTER.

4. Read the Software License Agreement, and then select **Accept** to continue.

5. Follow the on-screen instructions.

   The following table describes the required information. You can use the information you provided in the check list to complete many of these settings.

Information	Description
Change Password	• **Admin Password**—When you access the appliance, you must provide this password. This password can be the same as the root password. • **Root Password**—When you access the appliance from a command line, you must provide this password. • **Proventia Manager Password**—When you access Proventia Manager, you must provide this password. This password can be the same as the root password.
Network Configuration Information	• **IP Address**—The IP address of the management network adapter. • **Subnet Mask**—The subnet mask value for the network that connects to the management interface. • **Default Gateway**—The IP address for the management gateway.

INTERNET|SECURITY|SYSTEMS®

Information	Description
Host Configuration	The appliance uses domain names and DNS information to send email and SNMP responses. If you do not configure this information during setup, you must specify the IP address of the appliance's mail server each time you define an email or SNMP response. • **Hostname**—The computer name for the appliance. Example: myappliance. • **Domain Name**—The domain suffix (DNS search path) for the network. Example: mycompany.com. • **Primary Name Server**—The IP address for the DNS used to perform domain name lookups. Example: 10.0.0.1 • **Secondary Name Server**—The IP address for the secondary DNS used to perform domain name lookups.
Time Zone Configuration	These settings determine the time zone for the appliance.
Date/Time Configuration	You must set the date and time for the appliance as it appears in the management interface, so you can accurately track events as they occur on the network.
Agent Name Configuration	The Agent Name is the appliance name as it appears in the management interface. This name should correspond to a meaningful classification in the network scheme, such as the appliance's geographic location, business unit, or building address.

Information	Description
Port Link Configuration	Port link settings determine the appliance's performance mode, or how the appliance handles its connection to the network.
	You can select the speed (the rate at which traffic passes between the appliance and the network) and the duplex mode (which direction the information flows). Select link speeds and settings compatible with your particular network and in relation to the other devices that bracket the Proventia Network IPS appliance. If you are not sure about your network settings, select Auto to enable the appliance to negotiate the speed and duplex mode with the network automatically.
	Note: After the initial appliance configuration, you can only change port link speed and duplex settings for the inline monitoring and kill ports through Proventia Manager. For more information, see "Managing Network Adapter Cards" in the *Proventia Network IPS G and GX Appliance User Guide*.
Adapter Mode Configuration	The Adapter Mode determines how the appliance behaves within the network in order to protect it. Review "About IPS monitoring modes" on page 13 if you are not sure which mode to select.
	You can select different adapter modes for each port pair, but you must confirm that you have selected the correct adapter mode for the appliance's physical network connections. You may experience significant network implications if you have configured this setting incorrectly.

6. When you have entered all the information, the appliance applies the settings.

   When prompted, press ENTER to log off the appliance.

Accessing Proventia Manager

Introduction

Proventia Manager is the Web-based management interface for the appliance. Use Proventia Manager to perform the following tasks:

- monitor the status of the appliance
- configure and manage settings
- view quarantine table and apply changes
- review and manage appliance activities

Logging on to Proventia Manager

To log on to the Proventia Manager interface:

1. Start Internet Explorer 6.
2. Type https:// <appliance IP address>.
3. Log in using the user name admin and the Proventia Manager password.
4. If a message informs you that you do not have Java Runtime Environment (JRE) installed, install it, and then return to this procedure.
5. Select **Yes** to use the Getting Started procedures.

   Note: ISS recommends that you use the Getting Started procedures to help you customize the appliance settings. If this window does not appear, you can also access the Getting Started procedures from the Help.
6. Click **Launch Proventia Manager**.

Working with Proventia Manager

Introduction   When you open the Proventia Manager, the Home page provides an immediate snapshot of the current status of the appliance. This page includes the following navigation, information and reporting options:

- device name (the appliance domain name you configured during setup)
- protection status
- system status
- alerts for each module
- important messages

Viewing protection status   The protection status area describes the current status of the intrusion prevention component. Selecting a component name links you to the component status page.

The following status icons show you the current status of a component:

This icon...	Indicates...
◆	The component is active.
⊗	The component is stopped.
⊘	The component is in an unknown state. This status may require immediate attention.

Table 13: *Protection status icons*

INTERNET|SECURITY|SYSTEMS®

Viewing system status

On the Home page, the system status group box describes the current status of the system. The following table describes the data available in the System Status area:

Statistic	Description
Model Number	The model number of the appliance.
Base Version Number	The base version of the appliance software. **Note:** The base version is the software version shipped with the appliance, or the software version of the most recent firmware update.
Uptime	How long the appliance has been online, in the following format: `x days, x hours, x minutes`
Last Restart	The last time the appliance was restarted, in the following format: `yyyy-mm-dd hh:mm:ss` **Example:** `2004-05-04 16:24:37`
Last Firmware Update	The last time appliance firmware was updated, in the following format: `yyyy-mm-dd hh:mm:ss - version: x.x` **Example:** `2004-05-04 16:25:56 - version: 1.7`
Last Intrusion Prevention Update	The last time appliance security content was updated, in the following format: `yyyy-mm-dd hh:mm:ss - version: x.x` **Example:** `2004-01-25 12:34:36 - version: 1.7`
Last System Backup	The last time a system backup was created, in the following format: `yyyy-mm-dd hh:mm:ss` **Example:** `2004-05-04 15:49:01`
Backup Description	The backup type on the appliance: • Factory Default • Full System Backup

Table 14: *System Status statistics*

Viewing important messages
The Home page displays important messages about licensing and updates. If you have not configured the appliance to download updates automatically, these messages may appear with a link to the appropriate Proventia Manager page.

INTERNET|SECURITY|SYSTEMS®

Installing the License File

Introduction
Proventia Network IPS appliances require a properly configured license file. If you have not installed the appropriate license file, you cannot manage the appliance.

To purchase a license, contact your local sales representative.

Use the procedure below to install the license file, which is necessary to make your appliance run at full capability. You must save the license file to the appropriate location so that the Proventia Manager software can locate and acknowledge it.

Prerequisites
Before you install the license file, complete the following:

● register your customer license
● download the license from the ISS Registration Center

About the Licensing page
The Licensing page displays important information about the current status of the license file, including expiration dates. Additionally, this page allows you to access the License Information page, which includes information about how to acquire a current license.

Collecting license information
To collect your license information:

1. Contact your Sales Representative for your license registration number.

2. Register your customer license at the ISS License Registration center (https://www1.iss.net/cgi-bin/lrc).

3. Download the license key file from the ISS Registration Center to your computer.

   Note: Upload the license key file to a designated directory so that the appliance can download and install the latest updates automatically.

Installing the license file

To install the license file:

1. In Proventia Manager, select **System**→**Licensing**.

2. Click **Browse**.

3. Locate the license file that you downloaded.

4. Click **OK**.

5. Click **Upload**.

Applying Initial Updates

Introduction   Before you begin to create policies to manage your network security, you must ensure you have applied the latest updates to the appliance. The appliance retrieves updates from the ISS Download Center, accessible over the Internet.

For information about maintaining appliance updates, see Chapter 6, "Updating the Appliance," in the *Proventia Network IPS G and GX Appliance User Guide*.

Types of updates   You can install the following updates:

● **Firmware updates**. These updates include new program files, fixes or patches, enhancements, or online Help updates.

● **Intrusion prevention updates**. These updates contain the most recent security content provided by ISS's X-Force.

You can find updates on the Updates to Download page, and you can schedule automatic update downloads and installations from the Update Settings page.

Note: Some firmware updates require you to reboot the appliance. For more information about product issues and updates, see your appliance Readme.

Downloading updates   To download initial updates:

1. select **Updates→Available Downloads**.

2. If your appliance model requires it, the Export Administration window appears.

   Review the agreement, select **Yes**, and then click **Submit**.

3. The Updates to Download window appears and displays the following message if updates are available: "There are updates available. Click here to see details."

   Click the link in the message.

4. On the Updates to Download page, click **Download All Available Updates**.

Installing updates   To install updates:

1. In Proventia Manager, select **Updates→Available Installs**.

2. If your appliance model requires it, the Export Administration Regulation window appears.

   Review the agreement, select **Yes**, and then click **Submit**.

3. On the Available Installs page, select the updates you want to install, and then click **Install Updates**.

   Note: Some firmware updates require you to reboot the appliance. For detailed information about each firmware update, review the appliance Readme.

4. View the installation status in the Update History table on the Update Status page.

Chapter 3

Reinstalling the Appliance

Overview

Introduction   This chapter describes the process and procedures for reinstalling the GX3002 appliance.

Caution: Reinstalling the appliance firmware clears the appliance's current configuration settings and all data stored on the appliance.

In this chapter   This chapter contains the following topics:

Requirements

Introduction   The Recovery CD included in the appliance packaging contains the software that was installed on the appliance at the factory. You can reinstall the software from this CD on the appliance.

Important: Reinstalling the appliance means erasing all data from the system and returning it to its factory state. Only perform this procedure under the guidance of ISS technical support.

Results   This process does the following:

●   Overwrites software configuration changes you have made since you first installed the appliance.

●   Restores the original, default login credentials:

■   username = admin

■   password = admin

Supported network cards   The computer you use to reinstall appliance firmware must have one of the following network cards installed for you to complete the reinstallation successfully:

Important: ISS supports only the network cards listed.

Card	Brand Manufacturer
e1000	Intel PRO/1000
e100	Intel PRO/100
3c59x	3Com 3c590, 3c595, 3c905, 3c575
bcm5700	Broadcom 57xx Gigabit
sk98lin	SysKonnect and Marvell Gigabit
tulip	Digital/Intel 21x4x "Tulip"
eepro100	Intel PRO/100
8139too	RealTek 8139

Table 15: *Supported network cards*

INTERNET|SECURITY|SYSTEMS®

Card	Brand Manufacturer
ne2k-pci	NE2000-compatible PCI cards
pcnet32	AMD PCnet32, VMWare
sis900	SiS 900, 7016
via-rhine	Via Rhine VT86C100A, 6102, 6105
8139cp	RealTek 8139C+
epic100	SMC83c170, SMC83c175
xircom_cb	Xircom CardBus
3c574_cs	3Com 3c574
axnet_cs	Asix AX88190
nmclan_cs	AMD Am79C940
smc91c92_cs	SMC 91c92
xirc2ps_cs	Xircom CE2, CE IIps, RE-10, CEM28, CEM33, CEM56, CE3-100, CE3B, RE-100, REM10BT, REM56G-100
3c589_cs	3Com 3c589
fmvjl8x_cs	FMV J181, FMV J182, TDK LAK-CD021, ConTec C-NET (PC) C, Ungermann Access/CARD
pcnet_cs/NE2000 compatible cards	D-Link DE-650, Linksys PCMCIA, Accton EN2212, RPTI EP400, PreMax PE-200, IBM Credit Card Adapter, Novell NE4100, Kingston KNE-PCM/x, Allied Telesis LA-PCM, ASANTE FriendlyNet

Table 15: *Supported network cards*

Checklist

Introduction Before you reinstall the appliance firmware, ensure you complete the tasks listed in the following checklist.

Before you begin Before you begin, ensure you have gathered the proper materials and connected the appliance as specified in the following table:

| ✓	Description
❑	Choose a computer to access the appliance and reinstall the software. This computer is referred to as the *Pre-boot eXecution (PXE) server*. **Requirements:** • The BIOS settings on the computer must allow it to restart from a CD. For more information, see the computer's documentation. • Pentium II or compatible CPU • 64M RAM • IDE CD-ROM drive • COM1 serial port
❑	Locate the following items included with the appliance package: • *Proventia Network Intrusion Prevention System Recovery CD* • an Ethernet cross-over cable • a serial (null modem) cable **Important**: ISS does not support the use of other cables for this procedure.
❑	Create a backup of the current system in Proventia Manager. You can restore the system settings from this backup after you reinstall the appliance firmware. See "Appliance Management" in the *Proventia Network IPS G and GX Appliance User Guide* for more information.
❑	Record the following appliance settings for the management interface: • IP address, subnet mask, and default gateway • hostname, domain name, and DNS name server

Table 16: *Reinstallation checklist*

INTERNET|SECURITY|SYSTEMS

✓	Description
☐	Turn off the appliance, and then connect the computer (PXE server) directly to the appliance with the provided cables. See diagram below. **Connect the null modem cable to the devices as follows:** • On the computer (PXE server), use the port labeled COM1. • On the appliance, use the port labeled **Console**. **Connect the Ethernet cable to the devices as follows:** • On the computer (PXE server), use the Ethernet port. • On the appliance, use the left **Management** port labeled **1**. **Note:** Connecting to the computer (PXE server) to the appliance disables the appliance-Internet connection. When you finish the reinstall process, you must re-establish the Internet connection to retrieve appliance updates. **Important**: If you are running multiple PXE servers on the network, then you need to disconnect them prior to running the Proventia Network IPS reinstallation. You can verify that you are accessing the correct PXE server by the message displayed in Step 3.

Table 16: *Reinstallation checklist*

Diagram

The following diagram illustrates the proper computer-appliance connections for the reinstall process:

INTERNET|SECURITY|SYSTEMS
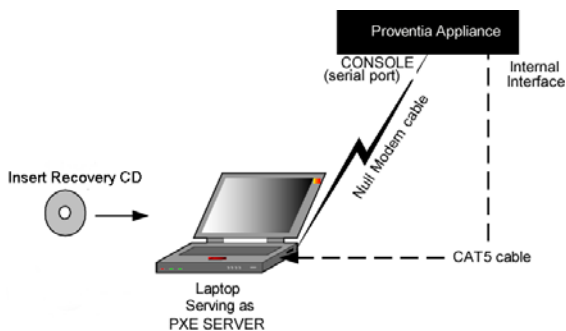
Reinstalling the Appliance

Introduction

Use the following procedure to reinstall the Proventia Network IPS firmware on your appliance.

Procedure

To reinstall the appliance:

1. Insert the *Proventia Network Intrusion Prevention System Recovery CD* into the CD-ROM drive of the PXE boot server, and then restart the PXE boot server.

    The PXE boot server displays the following messages:

    ```
    ***You may now boot your Proventia GXxxxx via the
    network***
    ***Starting Terminal Emulator***
    ***Press Control-G to Exit and Reboot***
    ```

    Note: The PXE boot server now acts as a terminal emulator for the appliance and displays the console output of the appliance.

2. Turn on the appliance.

    The PXE boot server displays boot process messages, and then displays the following prompt:

    ```
    Press L to boot from LAN, or press any other key to boot
    normally.
    ```

    Important: The installation process allows only five (5) seconds for you press L to boot from LAN. If you do not press L within this time period, the appliance boots as usual, and you must begin the reinstallation again.

3. Press the L key.

    The following message appears:

    ```
    Internet Security Systems
    Proventia GXxxxx Recovery Boot
    ```

    The PXE boot server displays status messages from the appliance, and then boots the installer over the network.

4. At the prompt, type **reinstall**, and then press ENTER.

The installer reloads the operating system.

Note: When the reinstallation is complete, the appliance automatically reboots. Let the appliance complete the boot process without interruption.

5. When the appliance has rebooted, the unconfigured.appliance login prompt appears.

You can log in with the default user and password of admin/admin and configure the appliance using the Configuration Menu.

INTERNET|SECURITY|SYSTEMS