IBM Proventia Network Intrusion Prevention System

G Appliance Getting Started Guide

IBM Internet Security Systems

IBM Global Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America.

Document part number: DOC-GSG-PNIPSG-001-A

November 14, 2007

Contents

Preface

Overview

Introduction

This guide is designed to help you connect and configure your Proventia Network Intrusion Prevention System (IPS) appliance.

Scope

This guide describes the appliance models (G100, G200, G1000 and G1200, G400, G400 (Rev A) and G2000) and explains the different ways to connect the appliances to your network. It also includes initial appliance setup procedures.

Additional documentation is located on the IBM ISS Web site at http://www.iss.net/support/documentation.

Audience

This guide is intended for network security system administrators responsible for installing and configuring IPS appliances. A fundamental knowledge of network security policies and IP network configuration is helpful.

Related publications

For the latest available appliance documentation, refer to the Help and the Readme files associated with each appliance release. Additional documents are available on the IBM ISS Web site at the following location: http://www.iss.net/support/documentation/

Additional documentation includes the following:

Document	Supports
Proventia Network IPS G and GX User Guide	All Proventia G appliances running release version 1.2 or later
Proventia G Next Generation Installation and Upgrade Procedures Guide	G100/G200/G1000/G1200 appliances running software versions prior to version 1.2 that need to be upgraded
Proventia G100/G200/G1000/ G1200 Appliance Quick Start Guide	Existing G100/G200/G1000/G1200 model appliances running software versions prior to version 1.2
SiteProtector Documentation	Any appliance managed through SiteProtector

Table 1: *Additional documentation*

Getting Technical Support

Introduction

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

The IBM ISS Web site

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

Support levels

IBM ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24x7 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 IBM 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 2: *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 3: *Contact information for technical support*

Chapter 1

Introducing the Proventia Network Intrusion Prevention System Appliance

Introduction

The Proventia Network Intrusion Prevention System (IPS) automatically blocks malicious attacks while preserving network bandwidth and availability. Proventia Network IPS appliances are 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.

In this chapter

This chapter contains the following topics:

Getting Started

Introduction

Verify that you have everything you need before you start setting up the appliance. This section lists package contents for both the appliance packaging and the rack mount kit, and includes information on bypass hardware.

Appliance package contents

The Proventia G appliance packaging includes the following:

- appliance
- power cord
- appliance recovery CD
- null modem serial cable
- warranty statement
- bezel cover with keys
- mouse/keyboard Y-cable
- crossover connectors and patch cables (copper only)
- rack mount kits and instructions

Rack mount kit materials

Table 4 describes the materials included in the rack mount kit for your appliance. Rack mount kit instructions are included in your appliance box and are also available online at http://www.iss.net/support/documentation.

This model kit...	Includes...
G400C, G400F, and G400CF	slide rail kit (option 1) mid-mount rack kit (option 2)
G2000C, G2000F, and G2000CF	tool-less slide rail kit

Table 4: *G Appliance rack mount kits*

Bypass hardware

The Proventia G400C, G400C (Rev A) and G2000C appliances have built-in copper bypass hardware, which by default fails "open," allowing traffic to continue passing through the appliance if the appliance fails or loses power. If you change the default setting to closed, the appliance will not allow traffic to pass in the event of a failure.

The G400F, G400CF, G400F (Rev A) G400CF (Rev A) and G2000F and G2000CF do not have built-in bypass hardware. You can purchase an optional fiber bypass unit and kit that provides bypass functionality. Contact Internet Security Systems for availability. See “Configuring the Appliance External Bypass Unit” on page 34 for more information.

Note: These models require the external bypass unit for the fiber ports only.

The G100/G200/G1000 and G1200 Front and Back Panels

Introduction

This topic identifies the front and back panels of a Proventia G100, G200, G1000, and G1200 appliance, along with descriptions for each item.

Front panel diagram and legend

The Proventia G100, G200, G1000, G1200 front panel is shown in Figure 1:

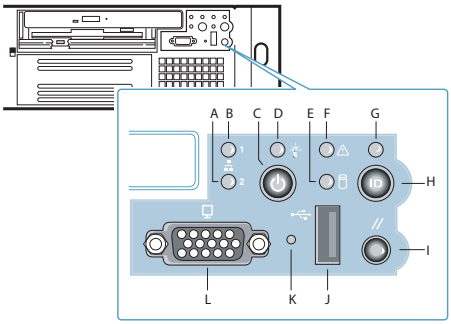


Figure 1: *G100/G200/G1000/G1200 appliance front panel*

The following table describes the elements pictured in Figure 1:

Label	Element
A	Management Interface (1) LED
B	RSKill Interface (2) LED
C	Power Button
D	Power LED
E	Hard Drive Activity LED
F	Fault LED
G	System ID LED
H	System ID Button
I	Reset Button

Table 5: *Elements on the front panel*

Label	Element
J	USB (unused)
K	Unused
L	Video

Table 5: *Elements on the front panel (Continued)*

Caution: You must operate this unit with the top cover installed to ensure proper cooling.

Back panel diagram (G100/G200)

The Proventia G100 /G200 (1U) back panel is shown in Figure 2:

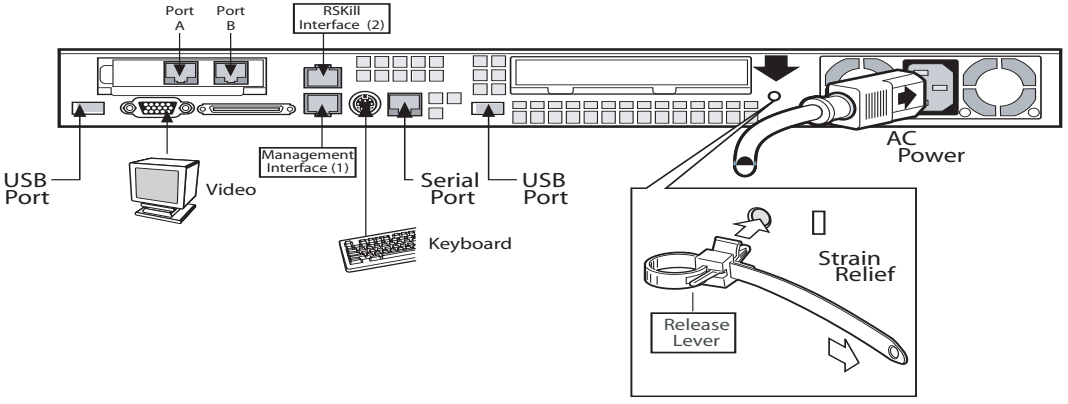


Figure 2: *G100/G200 appliance back panel*

Back panel diagram (G1000/G1200)

The network card is on the right side of the Proventia G1000 appliance. The Proventia G1200 appliance has eight ports. The Proventia G1200 offers AC or a DC power option. The Proventia G1000/G1200 (2U) back panel is shown in Figure 3.

Note: The AC power option is shown in Figure 3. The DC power information is shown in Figure 4 on page 15.

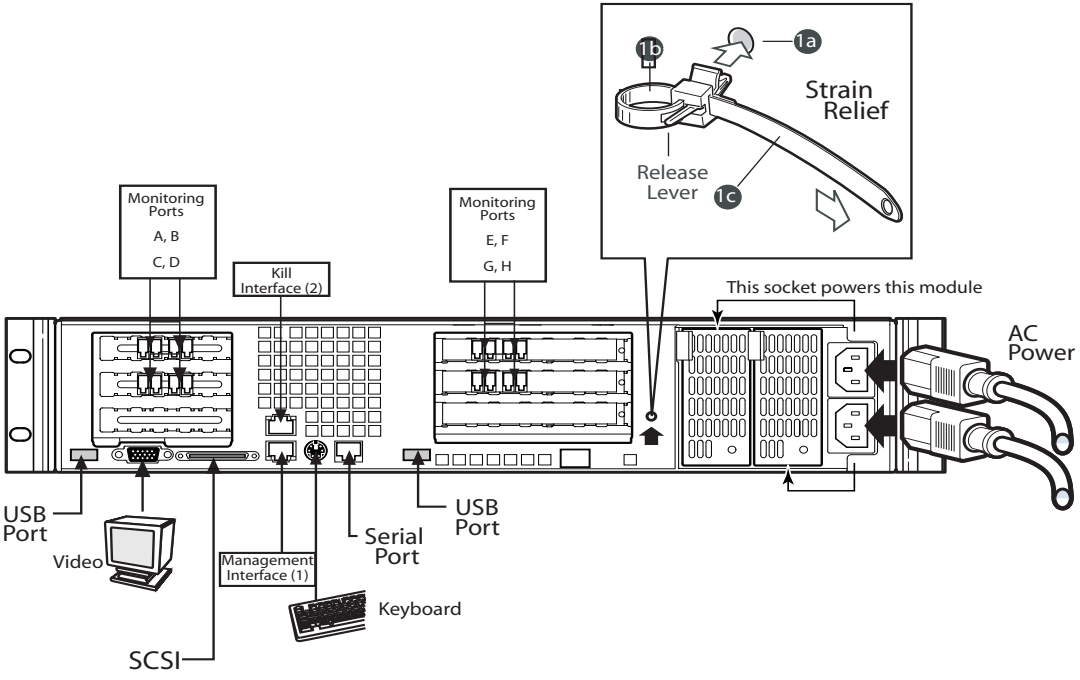


Figure 3: *G1000/G1200 appliance back panel*

DC power supply

The DC power supply used with the Proventia G1200 appliance uses a -48 to -60 VDC input switching power subsystem, which provides up to 470 Watts with -48 to -60 VDC input and with current and remote sense regulation. The power subsystem consists of one or two 470-Watt power supply modules. A system with two modules forms a redundant, hot-swappable (1+1) power subsystem.

Note: The DC power supply is only available for the Proventia G1200 appliance.

Back panel diagram (G1200)

The Proventia G1200 appliance has eight ports. DC power option is only offered on the Proventia G1200 appliance. The Proventia G1200 (2U) back panel is shown in Figure 4:

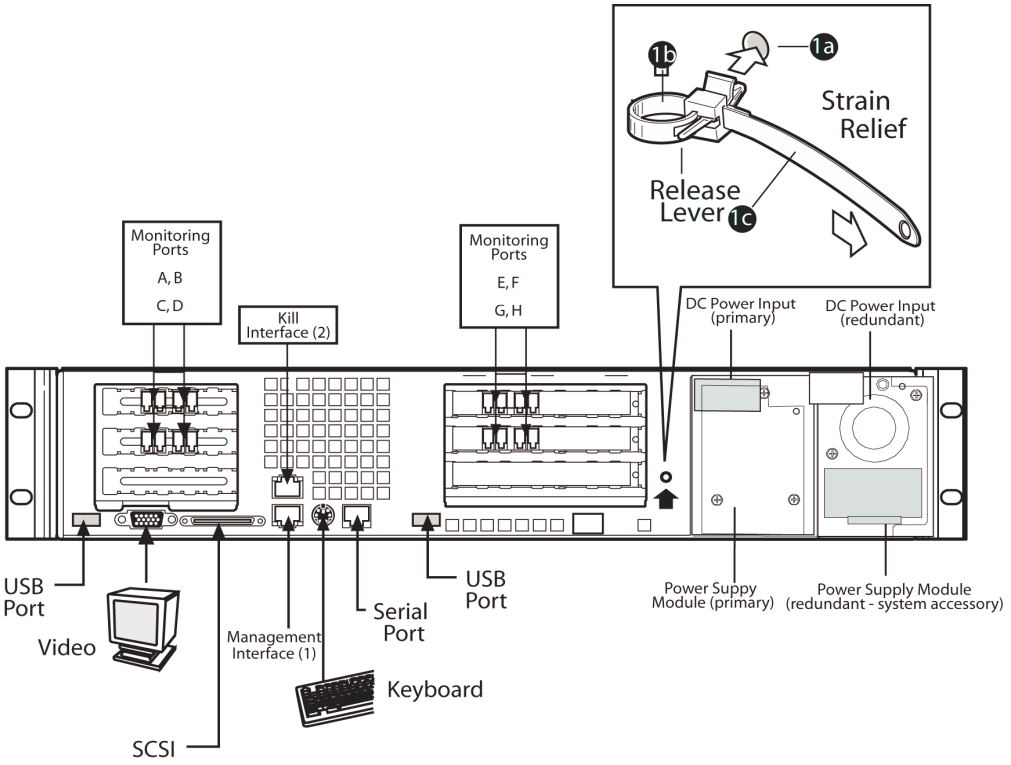


Figure 4: *G1200 appliance back panel with DC power option*

DC power supply features

The DC power supply includes the following features:

- 470-Watt output capability in full DC input voltage range
- power good indication LEDs
- predictive failure warning
- internal cooling fans with multi-speed capability

- remote sense of 3.3-Volt, 5-Volt, and 12-Volt DC outputs
- "DC_OK" circuitry for brown-out protection and recovery
- built-in load sharing capability
- built-in overloading protection capability
- onboard field replaceable unit (FRU) information
- I^2C interface for server management functions
- integral handle for insertion/extraction

Interface requirements for DC power

Table 6 identifies the interface requirements for DC power:

Interface	Description
DC Input	The DC power source may produce hazardous voltage levels exceeding -60 VDC and high energy levels above 240VA that may cause electric shock or burns. All DC input connections should be made only by a qualified service person to prevent injury. All wiring terminals connected to the DC input terminal block must be fully insulated with no exposed bare metal.
DC Output Connectors	The power subsystem DC power and control signals are connected to the server system by wire harnesses when the power supply modules are inserted into the power subsystem enclosure. The safety ground pin of the power supply module is the first pin to connect and the last to disconnect when the module is being inserted or removed from the power subsystem housing. In addition to the 5-V Standby, -12 V, +3.3 V, +5 V and +12 VDC outputs, the following signals and output pins are included: • +3.3 VDC remote sense • +5 VDC remote sense • +12 VDC remote sense • Remote sense return • Power Subsystem On (DC PWR enable) • Power Good

Table 6: *Interface requirements for DC power*

DC power supply module LED indicators

A single bi-color LED on the back of the system indicates the power supply status. Table 7 lists the conditions the LED can indicate:

Power Supply Condition	Power Supply LED
No DC power to all PSUs	OFF
No DC power to this PSU only	AMBER
DC present/Only Standby Outputs On	BLINK GREEN
Power supply DC outputs ON and OK	GREEN
Current limit	AMBER
Power supply failure (OTP, OCP, OVP, UV)	AMBER

Table 7: *DC power supply LED status conditions*

Note: S Failure, PS Presence, PS Predictive Fail, +12 V Mon, +5 V Mon, and the 5 V Standby rails failure are being monitored via an I2C interface chip.

DC input voltage specification

The power supply will operate within all specified limits over the input voltage range outlined in Table 8. The power supply will power-off if the DC input is less than -34 VDC.

Parameter	Minimum Tolerance	Nominal Rating	Maximum Tolerance	Maximum Input Current
Voltage	-38VDC	-48 to -60VDC	-75VDC	17.0 Amps

Table 8: *DC input voltage range*

DC output current specifications

The combined output power of all outputs will not exceed 450 W. The power supply meets both static and dynamic voltage regulation requirements for the minimum dynamic loading conditions. The power supply meets only the static load voltage regulation requirements for the minimum. Combined 3.3V/5V shall not exceed 0A.

Each output has a maximum and minimum current rating, as shown in Table 9.

Voltage	Current Rating
+3.3 VDC Output	20 Amp Max[1]
+5 VDC Output	26 Amp Max[1]
+12 V1DC Output	16 Amp Max[2]
+12 V2DC Output	12.0 Amp Max[2]
+12 V3DC Output	12.0 Amp Max[2]
-12 VDC Output	0.5 Amp Max
+5 VDC Standby	2.0 Amp Max
Output balancing	Total combined output power of all output shall not exceed 450 W.
DC Line Voltage	-48VDC to –60VDC
DC Input Current	17.0 Amp maximum

Table 9: *DC output voltage range*

Note: Combined 3.3V/5V shall not exceed 150W. 2. Maximum continuous load on the combined 12V output shall not exceed 25A. Peak load on the combined 12V output shall not exceed 30A for greater than 10 seconds.

The G400 and G2000 Front and Back Panels

Introduction

This topic identifies the front and back panels of the G400, G400 (Rev A) and G2000 appliances, along with descriptions for each item, including the external bypass unit.

Identifying the G400 (Rev A) appliance model

To determine the G400 (Rev A) appliance model, check the serial number and model label. It should say "Model G400 Rev: A."

Note: The G400 (Rev A) hardware port configurations are the same as the G2000 model. Refer to the appropriate diagram for your appliance model for information about ports and external bypass connectivity.

Front panel diagram and legend

The Proventia G400 and G2000 appliance front panel is shown in Figure 5:

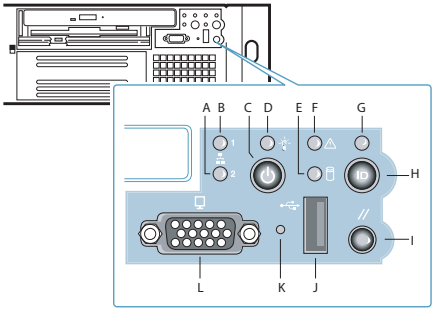


Figure 5: *G appliance front panel*

The following table describes the elements pictured in Figure 5:

Label	Element
A	Management Port LED
B	Kill Port LED
C	Power Button (press and hold to shutdown)
D	Power LED
E	Hard Drive Activity LED
F	Fault LED
G	System ID LED
H	System ID Button
I	Reset Button
J	USB (unused)
K	Unused
L	Video

Table 10: *Elements on the G400 and G2000 front panel*

⚠ **Caution:** You must operate this unit with the top cover installed to ensure proper cooling. A fault LED light generally does not indicate a problem with the appliance itself. The light can appear if the power cord is not plugged in properly.

G400F back panel diagram

Figure 6 illustrates the back of a G400F appliance. USB ports are labeled as they correspond to the monitoring ports for external bypass unit connectivity. For information on connecting the external bypass unit to this appliance, see “Configuring the Appliance External Bypass Unit” on page 34.

Important: Refer to the G2000 diagrams if you have a G400 (Rev A) appliance.

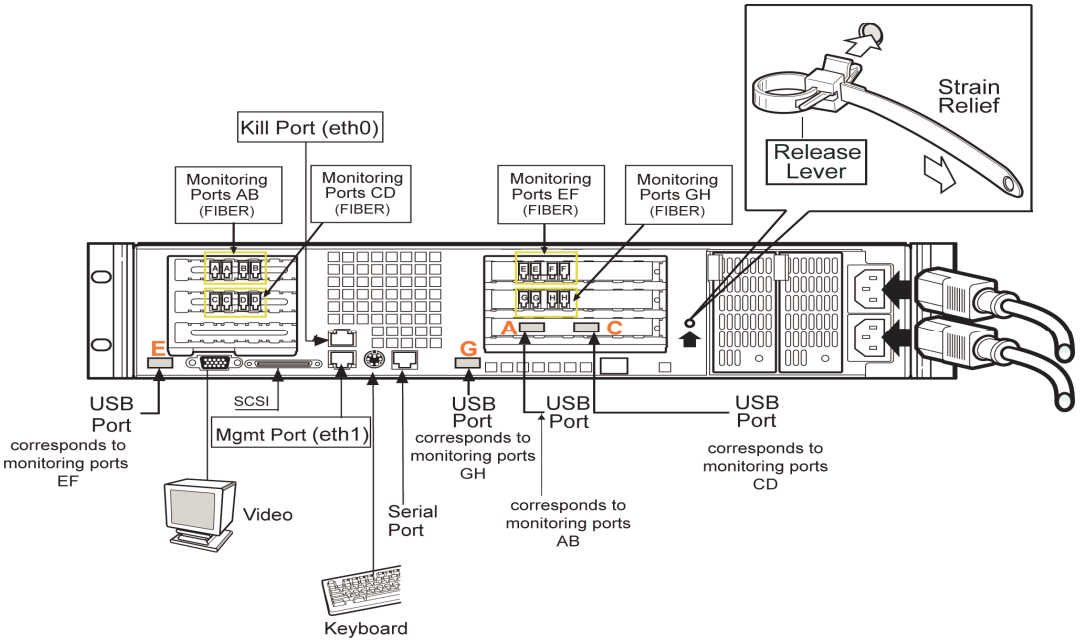


Figure 6: *G400F back panel diagram*

Note: An additional USB card with two more USB ports is added for additional G400 full fiber units (A and C).

G400CF back panel diagram

Figure 7 illustrates the back of the G400CF copper-fiber appliance. The USB ports are labeled as they correspond to the monitoring ports for external bypass connectivity. Other ports and connections are the same as the G400F back panel. Refer to Figure 6, "G400F back panel diagram" on page 21. For more information about external bypass connections, see "Configuring the Appliance External Bypass Unit" on page 34.

Important: Refer to the G2000 diagrams if you have a G400 (Rev A) appliance.

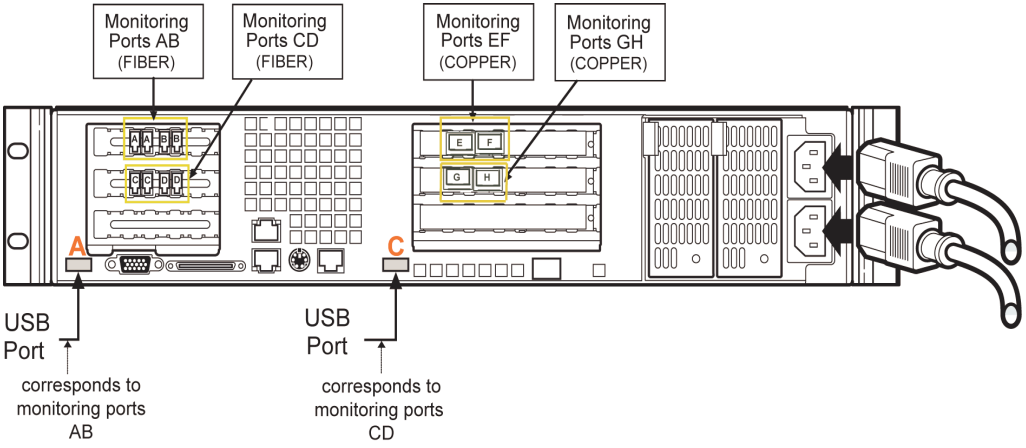


Figure 7: *G400CF back panel diagram*

G400F (Rev A) and G2000F back panel diagram

The following diagram describes the G400F (Rev A) or G2000F fiber appliance. USB ports are labeled as they correspond to the monitoring ports for external bypass unit connectivity. For information on connecting the external bypass unit to these appliances, see “Configuring the Appliance External Bypass Unit” on page 34.

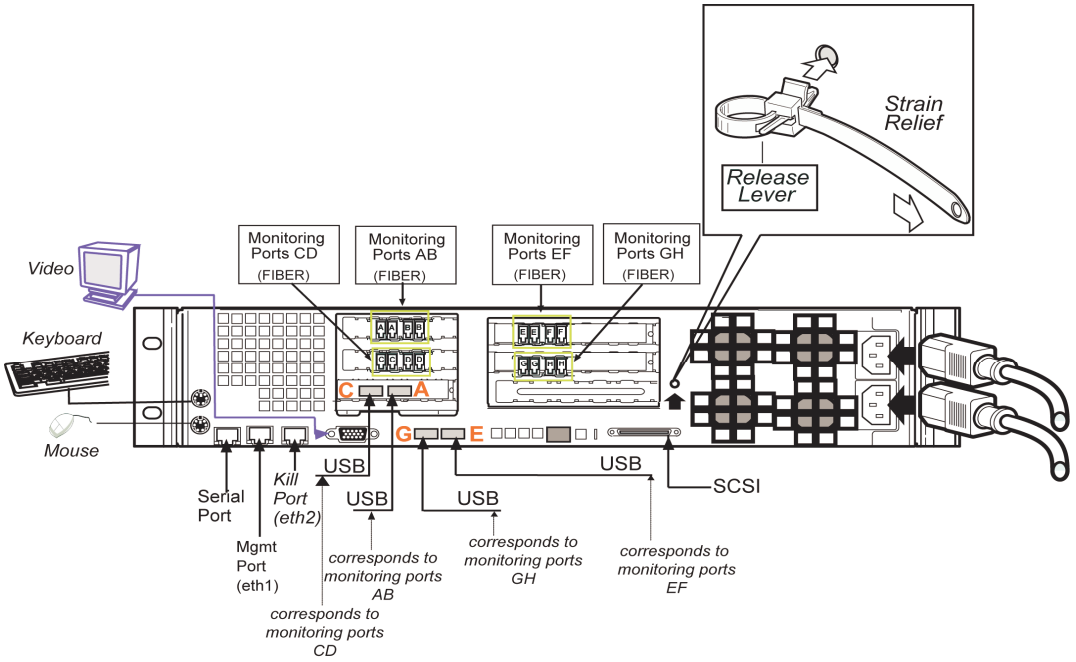


Figure 8: *G400F (rev A) or 2000F back panel diagram*

Note: An additional USB card with two more USB ports is added for additional G400 (Rev A) or G2000 full fiber units (C and A).

G400CF (Rev A) or 2000CF back panel diagram

Figure 9 shows the back of the G400CF (Rev A) or G2000CF copper-fiber appliance labeled for external bypass unit connectivity. USB ports are labeled as they correspond to the monitoring ports. For bypass unit connectivity information, see the "Configuring the Appliance External Bypass Unit" on page 34.

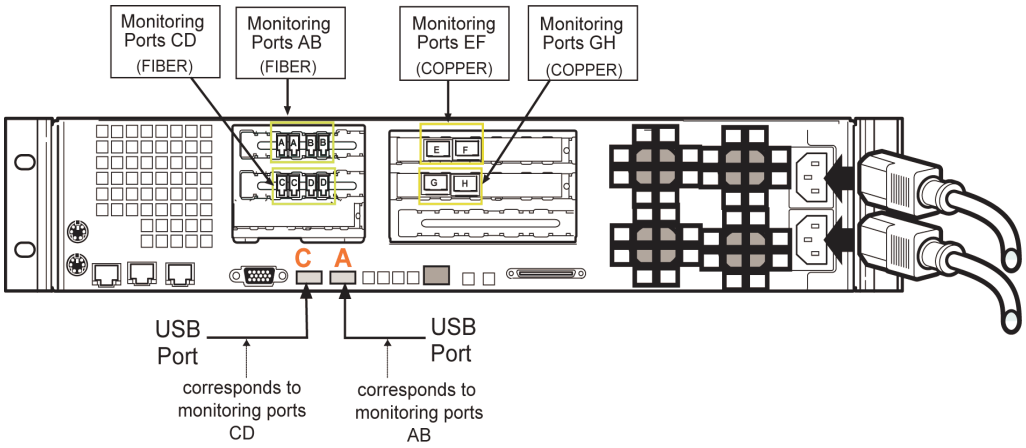


Figure 9: *G400CF (rev A) or 2000CF back panel diagram*

Network Cabling Guidelines

Introduction

The Proventia G400C, G400C (Rev A) and G2000C appliances have built-in copper bypass hardware, which by default fails "open," allowing traffic to continue passing through the appliance if the appliance fails or loses power. If you change the default setting to closed, the appliance will not allow traffic to pass in the event of a failure.

The G400F, G400CF, G400F (Rev A) G400CF (Rev A) and G2000F and G2000CF do not have built-in bypass hardware. You can purchase an optional fiber bypass unit and kit that provides bypass functionality. Contact Internet Security Systems for availability. See "Configuring the Appliance External Bypass Unit" on page 34 for more information.

Note: These models require the external bypass unit for the fiber ports only.

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

General cabling guidelines

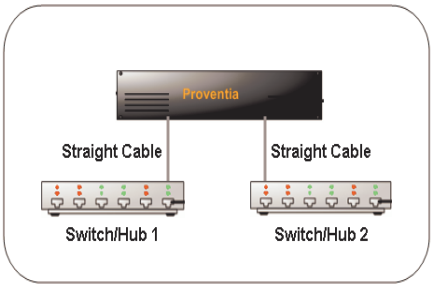
Where a crossover is needed, you may use your own CAT5 crossover cable or the provided one-foot cable and crossover coupler that comes with the appliance. When the appliance is not running, its monitoring ports function as a crossover. The following scenarios work independently of the monitoring port (A or B) you use.

Important: You should install the correct network cabling and verify that traffic flows *before* you turn on the appliance.

Switch or hub 1 to switch or hub 2

To deploy the appliance between two switches or hubs:

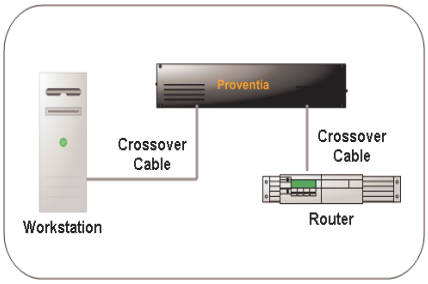
- use a straight-through Ethernet cable from Switch or Hub 1 to the appliance
- use a straight-through Ethernet cable from the appliance to Switch or Hub 2



Workstation or server to router

To deploy the appliance between a workstation and a router:

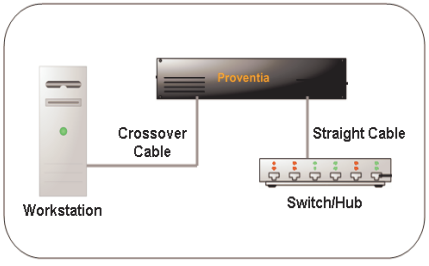
- use an Ethernet crossover cable from the workstation to the appliance
- use an Ethernet crossover cable from the appliance to the router



Workstation or server to switch or hub

To deploy the appliance between a workstation and a switch:

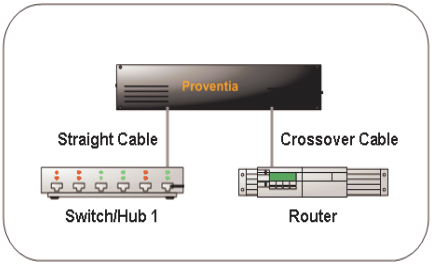
- use an Ethernet crossover cable from the workstation to the appliance
- use a straight-through Ethernet cable from the appliance to the switch



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

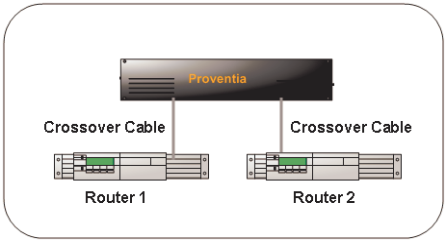


appliance to the switch or hub

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



High Availability Deployment

Appliances **cannot** be configured for high availability (HA) mode during the initial setup in the Proventia Setup Utility. Select one of the standard appliance modes during the initial setup, and then refer to High Availability Configuration topics in the *Proventia Network Intrusion Prevention System G/GX Appliance User Guide* or the Help for detailed procedures for enabling HA modes.

Chapter 2

Connecting and Configuring the Appliance

Overview

Introduction

This chapter describes how to configure a Proventia Network IPS G appliance. Use the "Configuration Checklist" on page 39 to gather the information you need to complete the configuration process.

In this chapter

This chapter contains the following topics:

Process Overview

Overview

This topic provides an overview of the steps required to set up a Proventia G appliance.

The setup process

The following table outlines the steps required to set up a Proventia G appliance:

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 32.
2	Start a terminal emulation session.	“Setting up terminal emulation” on page 33.
3	Gather required information.	“Configuration Checklist” on page 39.
4	Log in to the Proventia Setup Assistant as **admin/admin**.	“Completing the Initial Configuration” on page 42.
5	Configure initial network and appliance settings.	“Completing the Initial Configuration” on page 42.

Table 11: *Setup process*

Step	Description	Where to find the procedure
6	Contact your Sales Representative for your license registration number. Do the following: 1. Register your customer license at the IBM ISS License Registration center (https://www1.iss.net/cgi-bin/lrc). 2. Download the license key file from the IBM ISS Registration Center to your computer. **Note:** IBM ISS recommends that you upload the license key file to a designated directory so that the appliance can download and install the latest updates automatically. 3. Upload the license when you log in to Proventia Manager, when prompted.	"Acquiring the License File" on page 48.
7	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.	"Accessing Proventia Manager" on page 46.
8	Log in to Proventia Manager.	"Logging on to Proventia Manager" on page 46.
9	Install license.	"Acquiring the License File" on page 48
10	Apply updates.	"Applying Initial Updates" on page 50

Table 11: *Setup process (Continued)*

Connecting the Cables and Starting the Appliance

Introduction

This topic provides instructions for connecting cables and starting the appliance for the first time.

Important: Ensure that you keep your management and monitoring communication separate so that network traffic will be allowed to pass uninterrupted through the appliance's network interface card (NIC).

Connecting the power cord

The appliances have dual standard AC power connectors.

To connect the power cord(s):

1. Press the strain relief into the platform hole until it snaps into place.
2. Insert the power cord into the loop.

   Note: Leave some slack in the power cord between the strain relief and the power supply.
3. Pull the tab to secure the power cord in the loop.
4. Plug one end of the power cord into the back of the appliance.
5. Plug the other end of the power cord(s) into a standard AC power supply.

Connecting the network cables

To connect the network cables:

1. Connect the management port (eth1) on the back panel to the network you will use to manage it.
2. Connect the network cables to correspond with the adapter mode (inline or passive) you plan to use for the appliance.

   Note: Only connect the Kill port if you want the appliance to send kill responses through the Kill port while in monitoring mode.

   Reference: If you configure the appliance to operate in inline protection or inline simulation modes, see "Network Cabling Guidelines" on page 25.

Connecting to the appliance for first time setup

To connect to the appliance:

1. Ensure the appliance is on.
2. Connect the CAT5 cable from your management interface (eth1) to your hub or switch.
3. Plug one end of the null modem (serial) cable into the serial port on the back of the appliance (Figure 6 or Figure 8, depending on your appliance model).
4. Plug the other end of the serial cable into the serial port on your computer or laptop.
5. Use a terminal emulation program, such as Hyperterminal, to create a connection to the appliance.

Setting up terminal emulation

To set up terminal emulation and connect to the setup utility:

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.

   The unconfigured login prompt appears.
5. Proceed to “Completing the Initial Configuration” on page 42.

Configuring the Appliance External Bypass Unit

Introduction

The full fiber and copper-fiber hybrid model appliances—G400F, G400CF, G2000F, and G2000CF—use an external bypass unit. The external bypass unit monitors the appliance and ensures that network traffic continues to pass ("fails open") if the appliance fails or loses power.

Items you need

Table 12 outlines what you need to configure the external bypass unit:

Bypass Unit	Included Equipment (Appliance to bypass unit)	Other Required Cables (Bypass unit to network)
Single	• One USB cable • Two fiber cables (LC to LC connectors)	Two fiber cables (LC to whatever your network requires)
Double	• Two USB cables • Four fiber cables (LC to LC connectors)	Four fiber cables (LC to whatever your network requires)

Table 12: *Items needed to configure the bypass units*

Configuration diagram

Figure 10 illustrates bypass unit to appliance configuration.

Note: Internet Security Systems recommends that you place the bypass unit so that it faces the back of the rack. The front of the unit and the back of the appliance are now on the same side.

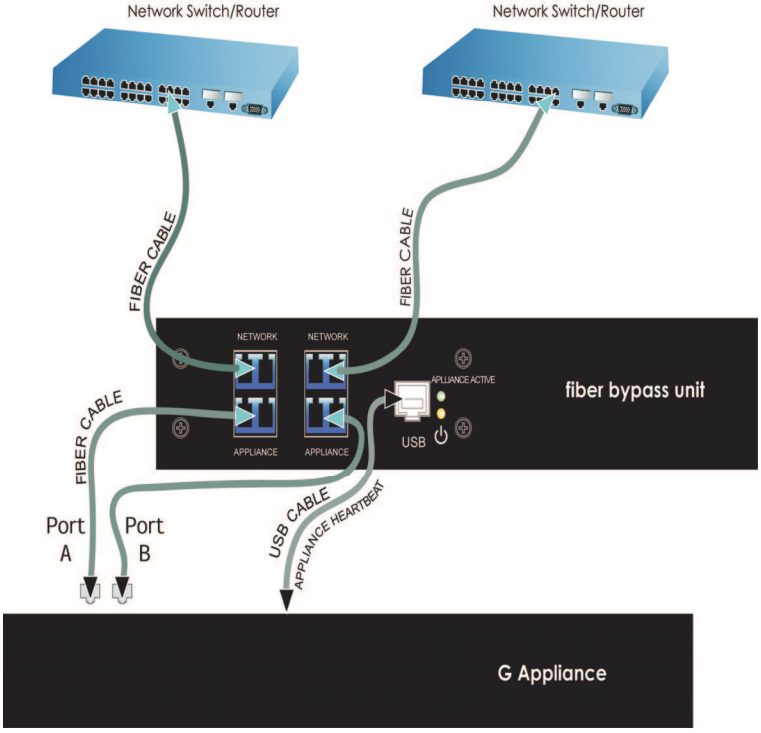


Figure 10: *Generic bypass unit to appliance configuration*

Before you connect the appliance

For each USB port to be correctly associated with the corresponding pair of monitoring ports, you must connect the USB cables before you turn on the appliance. If you connect or disconnect any USB cables while the appliance is on, you must restart the appliance.

Note: If you are unsure whether your appliance is full fiber or copper, refer to ports on the back of the appliance.

⚠ **Caution:** If you disconnect or change USB port connections, or replace interface cards after the appliance and bypass unit are initialized, the system may renumber the USB ports. IBM ISS recommends that you set up the connections as described in this topic. If you need to adjust your ports, you must turn off the appliance, and then reconfigure your port settings.

Connecting the cables

To connect the bypass unit to the appliance:

Important: The appliance MUST be OFF before you connect the appliance to the external bypass unit.

1. Connect the fiber cables from the network ports on the bypass unit to your network switch and routers.
2. Verify that traffic is flowing between the network and the appliance.

   Tip: If you can ping the appliance, traffic is flowing between the network and the appliance.
3. Connect the fiber cables (included with the appliance) from the ports on bypass unit to the corresponding ports on the back of the appliance.
4. Connect the USB cable from the USB port on the bypass unit to the correct USB port(s) on the back of the appliance.

Connecting the G400F and CF appliances

This topic describes how to connect an external bypass unit to the G400F and G400CF appliances. Refer to the back panel diagrams corresponding to your appliance model.

Important: If you have a G400 (Rev A) appliance, refer to the G2000 diagrams for connectivity information.

Port configurations for the G400F

Table 13 indicates USB and monitoring port configurations to connect the external bypass unit to a G400F fiber appliance.

This USB port driver...	Corresponds to monitoring port...
E	EF
G	GH
A	AB
C	CD

Table 13: *G400F USB port connections*

Port Configurations for the G400CF

Table 14 indicates USB and monitoring port configurations to connect an external bypass unit to a G400CF copper-fiber appliance.

This USB port driver...	Corresponds to this monitoring port...
A	AB
C	CD

Table 14: *G400CF copper-fiber USB port configuration*

Connecting the G400 (Rev A) or G2000 Appliances

Refer to your back panel diagrams for labels corresponding to the following tables.

Port configurations for the G400F (Rev A) or G2000F

Table 15 indicates the USB and monitoring port configurations for connecting a G400F (rev A) or G2000F fiber appliance to the external bypass unit.

This USB port driver...	Corresponds to this monitoring port...
C	CD
A	AB
G	GH
E	EF

Table 15: *G400F (rev A) or 2000F USB port connections*

Port configurations for the G400CF (Rev A) or G2000CF

Table 16 indicates the USB and monitoring port configurations for connecting a G2000CF copper-fiber appliance to the external bypass unit.

This USB port driver...	Corresponds to this monitoring port...
C	CD
A	AB

Table 16: *G400CF (rev A) or 2000CF (copper-fiber) USB port configuration*

Configuration Checklist

Required information checklist

Use the checklist in Table 17 to obtain the information you need to configure your Proventia G 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	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)	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 17: *Checklist and worksheet for configuration information*

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 18: *Monitoring modes*

High availability appliance modes

During setup, you can select one of the adapter modes described in Table 18. For the G400 or G2000, you can configure high availability (HA) through the Proventia Manager as part of your appliance management configuration. Table 19 lists the available HA modes.

Mode	Description
Normal mode	In Normal operation mode, the appliance cannot operate with another appliance in HA. Appliances can be configured to run in inline protection, inline simulation, and passive monitoring modes at the adapter level only.
HA Protection mode	In protection mode, both HA partner appliances monitor traffic inline and each report and block the attacks received on their inline ports. The appliances also monitor the traffic on each other's segments using mirror links—ready to take over reporting and protection in case of network failover.

Table 19: *HA appliance modes*

Mode	Description
HA Simulation mode	In HA simulation mode, both HA partner appliances monitor traffic inline but do not block any traffic. Instead they provide passive notification responses. The appliances also monitor the traffic on each other's segments using mirror links—ready to take over notification in case of network failover.

Table 19: *HA appliance modes (Continued)*

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.
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.

Information	Description
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.
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*.

Information	Description
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 40 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.

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

6. When you are prompted, press ENTER to log off the appliance.

Applying the settings and logging out

To apply your settings and exit:

1. On the Adapter Mode Configuration screen, press ENTER

   A progress bar appears while the appliance applies your settings.

   The log out screen appears, indicating that the configuration is complete.

2. Select **Logout**, and then press ENTER.

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: IBM 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**.

Chapter 3

Installing Licenses and Applying Updates

Overview

Introduction

This chapter describes how to obtain a license, install the license, and apply updates.

In this chapter

This chapter contains the following topics:

Acquiring 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.

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 IBM ISS License Registration center (https://www1.iss.net/cgi-bin/lrc).
3. Download the license key file from the IBM ISS Registration Center to your computer.

   Note: You must save the license file to the appropriate location so that the Proventia Manager software can locate and acknowledge it.

Location for the license key

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

Overview

The license file is necessary to make your appliance run at full capability. You must install the license before you can manage the appliance.

Prerequisites

Before you install the license file, you should have completed the following steps:

- register your customer license
- download the license from the IBM ISS Registration Center

Procedure

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 IBM 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 IBM ISS 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 4

Reinstalling the Appliance

Overview

Introduction

Reinstalling the appliance resets the appliance to its original factory settings. Under normal circumstances, you should never need to reinstall the appliance. Use the instructions in this chapter only if you have exhausted other options for correcting problems.

In this chapter

This chapter contains the following topics:

Understanding the Reinstallation Process

Introduction

Reinstalling the appliance erases all data from the system and returns it to its factory state.

Important: Perform this procedure only under the guidance of IBM ISS technical support.

Recovery CD

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.

Before you reinstall the appliance

Before you reinstall the appliance, complete the following tasks:

✓	Task Description
❑	Locate the *Proventia Network Intrusion Prevention System Recovery CD* included with the appliance package.
❑	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 20: *Before you reinstall the appliance*

Results of the reinstallation process

The reinstallation 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

Reinstalling the Appliance

Introduction

This topic describes the process for reinstalling the Proventia G Intrusion Prevention Appliances.

⚠ **Caution:** Reinstalling restores the appliance to its original configuration and removes any customized settings.

What you need

To reinstall a G appliance, you need the following:

- a computer to use as your configuration interface
- a *Proventia Network IPS G Appliance Recovery CD* (model-specific)
- the IP address, subnet mask, and default gateway of the appliance's management interface.

Reinstallation process task overview

To reinstall the appliance, follow the tasks in Table 21. See the complete procedure in "Procedure" on page 55:

Task	Description
1	Reinstall the appliance.
2	Log in and change the passwords.
3	Reconfigure the network interface and host.
4	Reconfigure the time and date.
5	Reconfigure the link speed, duplex and operational mode settings.
6	Apply your settings and logout.

Table 21: *Reinstallation process*

Important: After rebooting with the Recovery CD, the appliance reverts to the default login name and password, **admin/admin**.

Procedure

To reinstall the appliance:

1. If there is a bezel cover on the front of the appliance, remove it.
2. Connect a keyboard to the appliance or to the computer and monitor.

Reference: If using a computer, see "Setting up terminal emulation" on page 33.

3. Place your model-specific *Proventia Network IPS G Appliance Recovery CD* in the CD-ROM drive.
4. Restart the appliance.

   Tip: You can manually turn the power off and on if the appliance is not recognizing the CD .

   The appliance restarts.
5. At the **`boot:`** prompt, type `reinstall`, and then press ENTER.

   The appliance reloads the operating system, displays status messages, ejects the CD, and then reboots.

   Important: Promptly remove the CD prior to the appliance restarting.

   Wait for the appliance to completely finish the restart process.
6. At the unconfigured login prompt, enter the default username: **`admin`**
7. Enter the password, **`admin`**.

   The Proventia Setup screen appears.
8. Perform the configuration steps as described in "Completing the Initial Configuration" on page 42.

Index

p

r

s

t

u

w

Internet Security Systems, Inc., an IBM Company
Software License Agreement

BY INSTALLING, ACTIVATING, COPYING OR OTHERWISE USING THIS SOFTWARE PRODUCT, YOU AGREE TO ALL OF THE PROVISIONS OF THIS ISS SOFTWARE LICENSE AGREEMENT ("LICENSE"). EXCEPT AS MAY BE MODIFIED BY AN APPLICABLE LICENSE NOTIFICATION THAT ACCOMPANIES, PRECEDES, OR FOLLOWS THIS LICENSE, AND AS MAY FURTHER BE DEFINED IN THE USER DOCUMENTATION ACCOMPANYING THE SOFTWARE PRODUCT, YOUR RIGHTS AND OBLIGATIONS WITH RESPECT TO THE USE OF THIS SOFTWARE PRODUCT ARE AS SET FORTH BELOW. IF YOU ARE NOT WILLING TO BE BOUND BY THIS LICENSE, RETURN ALL COPIES OF THE SOFTWARE PRODUCT, INCLUDING ANY LICENSE KEYS, TO ISS WITHIN FIFTEEN (15) DAYS OF RECEIPT FOR A FULL REFUND OF ANY PAID LICENSE FEE. IF THE SOFTWARE PRODUCT WAS OBTAINED BY DOWNLOAD, YOU MAY CERTIFY DESTRUCTION OF ALL COPIES AND ANY LICENSE KEYS IN LIEU OF RETURN.

"ISS" is Internet Security Systems, Inc., an IBM Company.

"Software" is the following, including the original and all whole or partial copies: 1) machine-readable instructions and data, 2) components, 3) audio-visual content (such as images, text, recordings, or pictures), 4) related license materials, and 5) license use documents or keys, and documentation.

1. **License** - The Software is provided in object code and is licensed, not sold. Upon your payment of the applicable fees and ISS' delivery to you of the applicable license notification, Internet Security Systems, Inc., an IBM Company ("ISS") grants to you as the only end user ("Licensee") a nonexclusive and nontransferable, limited license for the accompanying Software, for use only on the specific network configuration, for the number and type of devices, and for the time period ("Term") that are specified in ISS' quotation and Licensee's purchase order, as accepted by ISS. If no Term is specified in the applicable ISS quotation or Licensee purchase order, the license shall be deemed perpetual. ISS limits use of Software based upon the number of nodes, users and/or the number and type of devices upon which it may be installed, used, gather data from, or report on, depending upon the specific Software licensed. A device includes any network addressable device connected to Licensee's network, including remotely, including but not limited to personal computers, workstations, servers, routers, hubs and printers. A device may also include ISS hardware (each an "Appliance") delivered with pre-installed Software and the license associated with such shall be a non-exclusive, nontransferable, perpetual (unless otherwise specified in the applicable ISS quotation or Licensee purchase order), limited license to use such pre-installed Software only in conjunction with the ISS hardware with which it is originally supplied. Except as provided in the immediately preceding sentence, Licensee may reproduce, install and use the Software on multiple devices, provided that the total number and type are authorized by ISS. Licensee may make a reasonable number of backup copies of the Software solely for archival and disaster recovery purposes.
   In connection with certain Software products, ISS licenses security content on a subscription basis for a Term. Content subscriptions are licensed pursuant to this License based upon the number of protected nodes or number of users. Security content is regularly updated and includes, but is not limited to, Internet content (URLs) and spam signatures that ISS classifies, security algorithms, checks, decodes, and ISS' related analysis of such information, all of which is owned and copyrighted by ISS and considered ISS confidential information and intellectual property. Security content may only be used in conjunction with the applicable Software in accordance with this License. The use or re-use of such content for commercial purposes is prohibited.
   Licensee's access to the security content is through an Internet update using the Software. In addition, unknown URLs may be automatically forwarded to ISS through the Software, analyzed, classified, entered into ISS' URL database and provided to Licensee as security content updates at regular intervals. ISS' URL database is located at an ISS facility or as a mirrored version on Licensee's premises. Any access by Licensee to the URL database that is not in conformance with this License is prohibited. Upon expiration of the security content subscription Term, unless Licensee renews such content subscription, Licensee shall implement appropriate system configuration modifications to terminate its use of the content subscription. Except for a perpetual license, upon expiration of the license Term, Licensee shall cease using the Software and certify return or destruction of it upon request.
2. **Migration Utilities** - For Software ISS markets or sells as a Migration Utility, the following shall apply. Provided Licensee holds a valid license to the Software to which the Migration Utility relates (the "Original Software"), ISS grants to Licensee as the only end user a nonexclusive and nontransferable, limited license to the Migration Utility and the related documentation ("Migration Utility") for use only in connection with Licensee's migration of the Original Software to the replacement software, as recommended by ISS in the related documentation. The Term of this License is for as long as Licensee holds a valid license to the applicable Original Software. Licensee may reproduce, install and use the Migration Utility on multiple devices in connection with its migration from the Original Software to the replacement software. Licensee shall implement appropriate safeguards and controls to prevent unlicensed use of the Migration Utility. Licensee may make a reasonable number of backup copies of the Migration Utility solely for archival and disaster recovery purposes.
3. **Third-Party Products** - Use of third party product(s) supplied hereunder, if any, will be subject solely to the manufacturer's terms and conditions that will be provided to Licensee upon delivery. ISS will pass any third party product warranties through to Licensee to the extent ISS is authorized to do so. If ISS supplies Licensee with Crystal Decisions Runtime Software, then the following additional terms apply:
   Licensee agrees not to alter, disassemble, decompile, translate, adapt or reverse-engineer the Runtime Software or the report file (.RPT) format, or to use, distribute or integrate the Runtime Software with any general-purpose report writing, data analysis or report delivery product or any other product that performs the same or similar functions as Crystal Decisions' product offerings;
   Licensee agrees not to use the Runtime Software to create for distribution a product that converts the report file (.RPT) format to an alternative report file format used by any general-purpose report writing, data analysis or report delivery product that is not the property of Crystal Decisions;
   Licensee agrees not to use the Runtime Software on a rental or timesharing basis or to operate a service bureau facility for the benefit of third-parties unless Licensee first acquires an Application Service Provider License from Crystal Decisions;
   CRYSTAL DECISIONS AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS, OR IMPLIED, INCLUDING WITHOUT LIMITATION THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. CRYSTAL DECISIONS AND ITS SUPPLIERS SHALL HAVE NO LIABILITY WHATSOEVER UNDER THIS AGREEMENT OR IN CONNECTION WITH THE RUNTIME SOFTWARE.
   In this Section 3 "Runtime Software" means the Crystal Reports software and associated documentation supplied by ISS and any updates, additional modules, or additional software provided by Crystal Decisions in connection therewith; it includes Crystal Decisions' Design Tools, Report Application Server and Runtime Software, but does not include any promotional software or other software products provided in the same package, which shall be governed by the online software license agreements included with such promotional software or software product.
4. **Beta License** - If ISS is providing Licensee with the Software, security content and related documentation, and/or an Appliance as a part of an alpha or beta test, the following terms of this Section 4 additionally apply and supersede any conflicting provisions herein or any other license agreement accompanying, contained or embedded in the subject prototype product or any associated documentation. ISS grants to Licensee a nonexclusive, nontransferable, limited license to use the ISS alpha/beta software program, security content, if any, Appliance and any related documentation furnished by ISS ("Beta Products") for Licensee's evaluation and comment (the "Beta License") during the Test Period. ISS' standard test cycle, which may be extended at ISS' discretion, extends for sixty (60) days, commencing on the date of delivery of the Beta Products (the "Test Period"). Upon expiration of the Test Period or termination of the Beta License,

Licensee shall, within thirty (30) days, return to ISS or destroy all copies of the beta Software, and shall furnish ISS written confirmation of such return or destruction upon request. If ISS provides Licensee a beta Appliance, Licensee agrees to discontinue use of and return such Appliance to ISS upon ISS' request and direction. If Licensee does not promptly comply with this request, ISS may, in its sole discretion, invoice Licensee in accordance with ISS' current policies.

Licensee will provide ISS information reasonably requested by ISS regarding Licensee's experiences with the installation and operation of the Beta Products. Licensee agrees that ISS shall have the right to use, in any manner and for any purpose, any information gained as a result of Licensee's use and evaluation of the Beta Products. Such information shall include but not be limited to changes, modifications and corrections to the Beta Products. Licensee grants to ISS a perpetual, royalty-free, non-exclusive, transferable, sublicensable right and license to use, copy, display, perform, make derivative works of and distribute any report, test result, suggestion or other item resulting from Licensee's evaluation of its installation and operation of the Beta Products.

LICENSEE AGREES NOT TO EXPORT BETA PRODUCTS DESIGNATED BY ISS IN ITS BETA PRODUCT DOCUMENTATION AS NOT YET CLASSIFIED FOR EXPORT TO ANY DESTINATION OTHER THAN THE U.S. AND THOSE COUNTRIES ELIGIBLE FOR EXPORT UNDER THE PROVISIONS OF 15 CFR § 740.17(A) (SUPPLEMENT 3), CURRENTLY CANADA, THE EUROPEAN UNION, AUSTRALIA, JAPAN, NEW ZEALAND, NORWAY, AND SWITZERLAND.

If Licensee is ever held or deemed to be the owner of any copyright rights in the Beta Products or any changes, modifications or corrections to the Beta Products, then Licensee hereby irrevocably assigns to ISS all such rights, title and interest and agrees to execute all documents necessary to implement and confirm the letter and intent of this Section. Licensee acknowledges and agrees that the Beta Products (including its existence, nature and specific features) constitute Confidential Information as defined in Section 18. Licensee further agrees to treat as Confidential Information all feedback, reports, test results, suggestions, and other items resulting from Licensee's evaluation and testing of the Beta Products as contemplated in this License. With regard to the Beta Products, ISS has no obligation to provide support, maintenance, upgrades, modifications, or new releases. However, ISS agrees to use commercially reasonable efforts to correct errors in the Beta Products and related documentation within a reasonable time, and will provide Licensee with any corrections it makes available to other evaluation participants. The documentation relating to the Beta Products may be in draft form and will, in many cases, be incomplete. Owing to the experimental nature of the Beta Products, Licensee is advised not to rely exclusively on the Beta Products for any reason. LICENSEE AGREES THAT THE BETA PRODUCTS AND RELATED DOCUMENTATION ARE BEING DELIVERED "AS IS" FOR TEST AND EVALUATION PURPOSES ONLY WITHOUT WARRANTIES OR INDEMNITIES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. LICENSEE ACKNOWLEDGES AND AGREES THAT THE BETA PRODUCT MAY CONTAIN DEFECTS, PRODUCE ERRONEOUS AND UNINTENDED RESULTS AND MAY AFFECT DATA NETWORK SERVICES AND OTHER MATERIALS OF LICENSEE. LICENSEE'S USE OF THE BETA PRODUCT IS AT THE SOLE RISK OF LICENSEE. IN NO EVENT WILL ISS BE LIABLE TO LICENSEE OR ANY OTHER PERSON FOR DAMAGES, DIRECT OR INDIRECT, OF ANY NATURE, OR EXPENSES INCURRED BY LICENSEE. LICENSEE'S SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE BETA PRODUCT LICENSE BY WRITTEN NOTICE TO ISS.

5. **Evaluation License** - If ISS is providing Licensee with the Software, security content and related documentation on an evaluation trial basis at no cost, such license Term is 30 days from installation, unless a longer period is agreed to in writing by ISS. ISS recommends using Software and security content for evaluation in a non-production, test environment. The following terms of this Section 5 additionally apply and supersede any conflicting provisions herein. Licensee agrees to remove or disable the Software and security content from the authorized platform and return the Software, security content and documentation to ISS upon expiration of the evaluation Term unless otherwise agreed by the parties in writing. ISS has no obligation to provide support, maintenance, upgrades, modifications, or new releases to the Software or security content under evaluation. LICENSEE AGREES THAT THE SOFTWARE, SECURITY CONTENT AND RELATED DOCUMENTATION ARE BEING DELIVERED "AS IS" FOR TEST AND EVALUATION PURPOSES ONLY WITHOUT WARRANTIES OR INDEMNITIES OF ANY KIND, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL ISS BE LIABLE TO LICENSEE OR ANY OTHER PERSON FOR DAMAGES, DIRECT OR INDIRECT, OF ANY NATURE, OR EXPENSES INCURRED BY LICENSEE. LICENSEE'S SOLE AND EXCLUSIVE REMEDY SHALL BE TO TERMINATE THE EVALUATION LICENSE BY WRITTEN NOTICE TO ISS.
6. **Covenants** - ISS reserves all intellectual property rights in the Software, security content and Beta Products. Licensee agrees: (i) the Software, security content and/or Beta Products is owned by ISS and/or its licensors, and is protected by copyright laws and international treaty provisions; (ii) to take all reasonable precautions to protect the Software, security content or Beta Product from unauthorized access, disclosure, copying or use; (iii) not to modify, adapt, translate, reverse engineer, decompile, disassemble, or otherwise attempt to discover the source code of the Software, security content or Beta Product; (iv) not to use ISS trade names or trademarks; (v) to reproduce all of ISS' and its licensors' copyright notices on any copies of the Software, security content or Beta Product; and (vi) not to transfer, lease, assign, sublicense, or distribute the Software, security content or Beta Product or make it available for timesharing, service bureau, managed services offering, or on-line use.
7. **Support and Maintenance** - Depending upon what maintenance programs Licensee has purchased, ISS will provide maintenance, during the period for which Licensee has paid the applicable maintenance fees, in accordance with its prevailing Maintenance and Support Policy that is available at http://documents.iss.net/maintenance_policy.pdf. Any supplemental Software code or related materials that ISS provides to Licensee as part of any support and maintenance service are to be considered part of the Software and are subject to the terms and conditions of this License, unless otherwise specified.
8. **Limited Warranty** - The commencement date of this limited warranty is the date on which ISS provides Licensee with access to the Software. For a period of ninety (90) days after the commencement date or for the Term (whichever is less), ISS warrants that the Software or security content will conform to material operational specifications described in its then current documentation. However, this limited warranty shall not apply unless (i) the Software or security content is installed, implemented, and operated in accordance with all written instructions and documentation supplied by ISS, (ii) Licensee notifies ISS in writing of any nonconformity within the warranty period, and (iii) Licensee has promptly and properly installed all corrections, new versions, and updates made available by ISS to Licensee. Furthermore, this limited warranty shall not apply to nonconformities arising from any of the following: (i) misuse of the Software or security content, (ii) modification of the Software or security content, (iii) failure by Licensee to utilize compatible computer and networking hardware and software, or (iv) interaction with software or firmware not provided by ISS. If Licensee timely notifies ISS in writing of any such nonconformity, then ISS shall repair or replace the Software or security content or, if ISS determines that repair or replacement is impractical, ISS may terminate the applicable licenses and refund the applicable license fees, as the sole and exclusive remedies of Licensee for such nonconformity. THIS WARRANTY GIVES LICENSEE SPECIFIC LEGAL RIGHTS, AND LICENSEE MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM JURISDICTION TO JURISDICTION. ISS DOES NOT WARRANT THAT THE SOFTWARE OR THE SECURITY CONTENT WILL MEET LICENSEE'S REQUIREMENTS, THAT THE OPERATION OF THE SOFTWARE OR SECURITY CONTENT WILL BE UNINTERRUPTED OR ERROR-FREE, OR THAT ALL SOFTWARE OR SECURITY CONTENT ERRORS WILL BE CORRECTED. LICENSEE UNDERSTANDS AND AGREES THAT THE SOFTWARE AND THE SECURITY CONTENT ARE NO GUARANTEE AGAINST UNSOLICITED E-MAILS, UNDESIRABLE INTERNET CONTENT, INTRUSIONS, VIRUSES, TROJAN HORSES, WORMS, TIME BOMBS, CANCELBOTS OR OTHER SIMILAR HARMFUL OR DELETERIOUS PROGRAMMING ROUTINES AFFECTING LICENSEE'S NETWORK, OR THAT ALL SECURITY THREATS AND VULNERABILITIES, UNSOLICITED E-MAILS OR UNDESIRABLE INTERNET CONTENT WILL BE DETECTED OR THAT THE PERFORMANCE OF THE SOFTWARE AND SECURITY CONTENT WILL RENDER LICENSEE'S SYSTEMS INVULNERABLE TO

SECURITY BREACHES. THE REMEDIES SET OUT IN THIS SECTION 8 ARE THE SOLE AND EXCLUSIVE REMEDIES FOR BREACH OF THIS LIMITED WARRANTY.

9. **Warranty Disclaimer** - EXCEPT FOR THE LIMITED WARRANTY PROVIDED ABOVE, THE SOFTWARE AND SECURITY CONTENT ARE EACH PROVIDED "AS IS" AND ISS HEREBY DISCLAIMS ALL WARRANTIES AND INDEMNITIES, BOTH EXPRESS AND IMPLIED, INCLUDING IMPLIED WARRANTIES RESPECTING MERCHANTABILITY, TITLE, NONINFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE. LICENSEE EXPRESSLY ACKNOWLEDGES THAT NO REPRESENTATIONS OTHER THAN THOSE CONTAINED IN THIS LICENSE HAVE BEEN MADE REGARDING THE GOODS OR SERVICES TO BE PROVIDED HEREUNDER, AND THAT LICENSEE HAS NOT RELIED ON ANY REPRESENTATION NOT EXPRESSLY SET OUT IN THIS LICENSE.
10. **Limitation of Liability** - Circumstances may arise where, because of a default on ISS' part or other liability, Licensee is entitled to recover damages from ISS. In each such instance, regardless of the basis on which Licensee may be entitled to claim damages from ISS, (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), ISS is liable for no more than 1) damages for bodily injury (including death) and damage to real property and tangible personal property and 2) the amount of any other actual direct damages up to the charges for the Software or security content that is the subject of the claim.
This limitation of liability also applies to ISS' licensors and suppliers. It is the maximum for which they and ISS are collectively responsible.
UNDER NO CIRCUMSTANCES IS ISS, ITS LICENSORS OR SUPPLIERS LIABLE FOR ANY OF THE FOLLOWING, EVEN IF INFORMED OF THEIR POSSIBILITY: LOSS OF, OR DAMAGE TO, DATA; SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES, OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES; OR LOST PROFITS, BUSINESS, REVENUE, GOODWILL, OR ANTICIPATED SAVINGS. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO LICENSEE.
11. **Termination** - Licensee may terminate this License at any time by notifying ISS in writing. All rights granted under this License will terminate immediately, without prior written notice from ISS, at the end of the Term of the License, if not perpetual. If Licensee fails to comply with any provisions of this License, ISS may immediately terminate this License if such default has not been cured within ten (10) days following written notice of default to Licensee. Upon termination or expiration of a license for Software, Licensee shall cease all use of such Software, including Software pre-installed on ISS hardware, and destroy all copies of the Software and associated documentation. Termination of this License shall not relieve Licensee of its obligation to pay all fees incurred prior to such termination and shall not limit either party from pursuing any other remedies available to it.
12. **General Provisions** - This License, together with the identification of the Software and/or security content, pricing and payment terms stated in the applicable ISS quotation and Licensee purchase order (if applicable) as accepted by ISS, constitute the entire agreement between the parties respecting its subject matter. Standard and other additional terms or conditions contained in any purchase order or similar document are hereby expressly rejected and shall have no force or effect. If Licensee has not already downloaded the Software, security content and documentation, then it is available for download at http://www.iss.net/download/. All ISS hardware with pre-installed Software and any other products not delivered by download are delivered f.o.b. origin. Both Licensee and ISS consent to the application of the laws of the State of New York to govern, interpret, and enforce all of Licensee's and ISS' rights, duties, and obligations arising from, or relating in any manner to, the subject matter of this License, without regard to conflict of law principles. The United Nations Convention on Contracts for the International Sale of Goods does not apply. Both Licensee and ISS irrevocably waive any right to a jury trial. If any part of this License is found void or unenforceable, it will not affect the validity of the balance of the License, which shall remain valid and enforceable according to its terms. This License may only be modified in writing signed by an authorized officer of ISS.
13. **Notice to United States Government End Users** - Licensee acknowledges that any Software and security content furnished under this License is commercial computer software and any documentation is commercial technical data developed at private expense and is provided with RESTRICTED RIGHTS. Any use, modification, reproduction, display, release, duplication or disclosure of this commercial computer software by the United States Government or its agencies is subject to the terms, conditions and restrictions of this License in accordance with the United States Federal Acquisition Regulations at 48 C.F.R. Section 12.212 and DFAR Subsection 227.7202-3 and Clause 252.227-7015 or applicable subsequent regulations. Contractor/manufacturer is Internet Security Systems, Inc., 6303 Barfield Road, Atlanta, GA 30328, USA.
14. **Export and Import Compliance** - Each party will comply with applicable import and export control laws and regulations, including those of the United States that prohibit or limit export for certain uses or to certain end users. Many ISS Software products include encryption and export outside of the United States or Canada is strictly controlled by U.S. laws and regulations. ISS makes its current export classification information available at http://www.iss.net/export. Please contact ISS' Sourcing and Fulfillment for export questions relating to the Software or security content (fulfillment@iss.net). Licensee understands that the foregoing obligations are U.S. legal requirements and agrees that they shall survive any term or termination of this License.
15. **Authority** - Because the Software is designed to test or monitor the security of computer network systems and may disclose or create problems in the operation of the systems tested, Licensee and the persons acting for Licensee represent and warrant that: (a) they are fully authorized by the Licensee and the owners of the computer network for which the Software is licensed to enter into this License and to obtain and operate the Software in order to test and monitor that computer network; (b) the Licensee and the owners of that computer network understand and accept the risks involved; and (c) the Licensee shall procure and use the Software in accordance with all applicable laws, regulations and rules.
16. **Disclaimers** - Licensee acknowledges that some of the Software and security content is designed to test the security of computer networks and may disclose or create problems in the operation of the systems tested. Licensee further acknowledges that neither the Software nor security content is fault tolerant or designed or intended for use in hazardous environments requiring fail-safe operation, including, but not limited to, aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which the failure of the Software and security content could lead to death or personal injury, or severe physical or property damage. ISS disclaims any implied warranty of fitness for High Risk Use. Licensee accepts the risk associated with the foregoing disclaimers and hereby waives all rights, remedies, and causes of action against ISS and releases ISS from all liabilities arising therefrom.
17. **Confidentiality** - "Confidential Information" means all information proprietary to a party or its suppliers that is marked as confidential. Each party acknowledges that during the term of this Agreement, it will be exposed to Confidential Information of the other party. The obligations of the party ("Receiving Party") which receives Confidential Information of the other party ("Disclosing Party") with respect to any particular portion of the Disclosing Party's Confidential Information shall not attach or shall terminate when any of the following occurs: (i) it was in the public domain or generally available to the public at the time of disclosure to the Receiving Party, (ii) it entered the public domain or became generally available to the public through no fault of the Receiving Party subsequent to the time of disclosure to the Receiving Party, (iii) it was or is furnished to the Receiving Party by a third party having the right to furnish it with no obligation of confidentiality to the Disclosing Party, or (iv) it was independently developed by the Receiving Party by individuals not having access to the Confidential Information of the Disclosing Party. The Receiving Party agrees not to disclose or use any Confidential Information of the Disclosing Party in violation of this License and to use Confidential Information of the Disclosing Party solely for the purposes of this License. Upon demand by the Disclosing Party and, in any event, upon expiration or termination of this License, the Receiving Party shall return to the Disclosing Party all copies of the Disclosing Party's Confidential Information in the Receiving Party's possession or control and destroy all derivatives and other vestiges of the Disclosing Party's Confidential Information obtained or created by the Disclosing Party. All Confidential Information of the Disclosing Party shall remain the exclusive property of the Disclosing Party, provided however that the Receiving Party may use in its business activities the ideas, concepts and know-how contained in the Disclosing Party's Confidential Information which are retained in the memories of the Receiving Party's employees who have had access to the Confidential Information under this License.

18. **Compliance** - From time to time, ISS may request Licensee to provide a certification that the Software and security content is being used in accordance with the terms of this License. If so requested, Licensee shall verify its compliance and deliver its certification within forty-five (45) days of the request. The certification shall state Licensee's compliance or non-compliance, including the extent of any non-compliance. ISS may also, at any time, upon thirty (30) days prior written notice, at its own expense appoint a nationally recognized software use auditor, to whom Licensee has no reasonable objection, to audit and examine use and records at Licensee offices during normal business hours, solely for the purpose of confirming that Licensee's use of the Software and security content is in compliance with the terms of this License. ISS will use commercially reasonable efforts to have such audit conducted in a manner such that it will not unreasonably interfere with the normal business operations of Licensee. If such audit should reveal that use of the Software or security content has been expanded beyond the scope of use and/or the number of authorized devices or Licensee certifies such non-compliance, ISS shall have the right to charge Licensee the applicable current list prices required to bring Licensee in compliance with its obligations hereunder with respect to its current use of the Software and security content. In addition to the foregoing, ISS may pursue any other rights and remedies it may have at law, in equity or under this License.
19. **Data Protection** - Licensee confirms that it is solely responsible for ensuring that any processing and security obligations comply with applicable data protection laws. Licensee contact information shall not be considered personal information processed on Licensee's behalf.
20. **Miscellaneous** - Except for any payment obligations, neither Licensee nor ISS is responsible for failure to fulfill any obligations due to causes beyond its control. This License will not create any right or cause of action for any third party, nor will ISS be responsible for any third party claims against Licensee except, as permitted by the Limitation of Liability section above, for bodily injury (including death) or damage to real or tangible personal property for which ISS is legally liable. Nothing in this License affects any statutory rights of consumers that cannot be waived or limited by contract. Licensee agrees to allow ISS to store and use Licensee's contact information, including names, phone numbers, and e-mail addresses, anywhere they do business. Such information will be processed and used in connection with our business relationship, and may be provided to contractors, Business Partners, and assignees of ISS for uses consistent with their collective business activities, including communicating with Licensee (for example, for processing orders, for promotions, and for market research). Neither Licensee nor ISS will bring a legal action under this License more than two years after the cause of action arose unless otherwise provided by local law without the possibility of contractual waiver or limitation.

Revised: February 14, 2007