IBM Proventia Network Intrusion Prevention System Getting Started for GX4000 Series Appliances

This document helps you do the following tasks:

- Connect the appliance
- Configure appliance settings
- Connect to Proventia® Manager
- Install the product license
- Update the appliance

After you finish these tasks:

- Use the applicable IBM® Proventia Network Intrusion Prevention System (IPS) Installation Guide to install specific firmware versions
- Use the applicable IBM Proventia Network Intrusion Prevention System (IPS) Appliance User Guide to
  - Set up appliance management
  - Configure your security policies, including specifying events and responses
  - Create firewall rules to protect your network
  - Track alerts
  - Monitor important system information

Reference Key
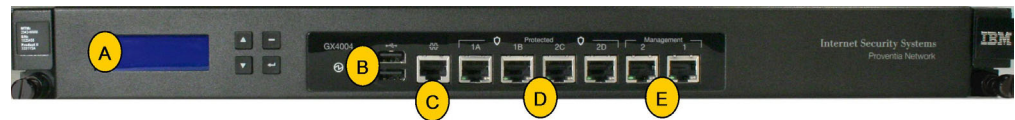
- **A**: **LCD Controller Module** - used for initial network configuration, restarting or shutting down the appliance, and obtaining IPS version information.
- **B**: **USB Ports**
- **C**: **Serial Console Port** - used for terminal-based setup and recovery.
- **D**: **Protected Ports**- used for either inline intrusion prevention (IPS mode) or passive intrusion detection (IDS mode). Inline prevention uses a pair of ports per segment. Passive detection uses a single port per segment.

  Note: Your port configuration may look slightly different depending on the number of ports.

- **E**: **Management Ports**

  Management Port 1 is used to communicate with Proventia Manager and SiteProtector Management

  Management Port 2 is used exclusively for sending TCP Reset responses

Requirements

- Power cable
- Proventia serial console cable (blue)
- Ethernet crossover cable (red)
- For each inline segment:.
  - A pair of Ethernet cables, straight-through or crossover, depending on your network type
  - A crossover adapter

  Note: IBM provides one crossover adapter and two one-foot Ethernet cables (green) per segment
- Additional Ethernet cables, as needed
- PC with Internet Explorer and Internet connection

Connect the appliance

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

Cable the appliance

Procedure

1. Connect the power cable(s) to the appliance. If your appliance has two power cords, you must connect both.
2. Connect Management port 1 to the network you will use to manage the appliance.

   Note: TCP Reset: Management port 2 is the RS Kill (TCP Reset) port. The appliance does not send TCP Reset responses until you configure TCP Reset.
3. (SFP-capable appliance only) Populate the protected ports with SFP modules as necessary. For each port pair, SFP modules must be the same media type; for example, if port 1A is copper (TX), then port 1B must also be copper (TX).
4. Connect the network cables to the protected ports. To run the appliance in passive mode, only connect the first protected port in the pair to the network.
5. Turn on the appliance.

Network information

Record the network information you need to configure the appliance.

Setting	Your network information
IP address	_____-_____-_____-_____
Subnet mask	_____-_____-_____-_____
Default gateway	_____-_____-_____-_____

Options for connecting to the network

Chose one of the options to connect the appliance to the network.

- "Connect to the network using the LCD panel" on page 3
- "Connect to the network using a serial console cable" on page 3

Connect to the network using the LCD panel

Procedure

1. Determine and record your IP address, subnet mask, and default gateway.

2. Press ◄┘ (Enter) on the LCD panel. The LCD displays a message asking if you want to set up the network.

3. Select **OK**, and then press ◄┘ (Enter).

4. Press ◄┘ (Enter) again on the LCD panel to display the IP address screen.

5. Press **UP** and **DOWN** to select a number, and then press ◄┘ (Enter) to move to the next field.

6. When you have completed all the fields, press ◄┘ (Enter).

7. Select **OK** to move forward, and then press ◄┘ (Enter) to confirm your selection.

8. Complete these steps again to provide the subnet mask and default gateway.

9. After you enter all your network information, a final conformation screen appears. Select **OK** to save all network information and enable the Management port, or select **Cancel** to return to the IBM ISS Proventia screen without saving any information.

10. After you confirm the settings, the appliance generates a temporary, case-sensitive password. Record this password; you must use it when you log on to the appliance.

11. Connect to the appliance using a secure network connection and the appliance's IP address to complete the initial configuration.

What to do next

Go to the next procedure in the getting started process, "Configure appliance settings" on page 4.

Connect to the network using a serial console cable

Procedure
1. Connect the serial console cable to the appliance and a computer to complete the initial configuration.
2. Connect to the appliance using Hyperterminal or another terminal emulation program. Follow the instructions listed in the documentation for the program you choose.
3. Use the following settings to connect.

Option	Description
Communication Port	Typically COM1
Emulation	VT100
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None

What to do next

Go to the next procedure in the getting started process, "Configure appliance settings."

Configure appliance settings

Procedure

1. Connect to the appliance using a secure network connection and the appliance's IP address to complete the initial configuration.
2. At the unconfigured login prompt, type `admin`, and then press **Enter**.
3. Do one of the following actions:

Option	Action
LCD panel	Type the case-sensitive password the Proventia Network IPS system generated for you and then press **Enter**.
Serial console cable	Type `admin` for the password and then press **Enter**.

4. Follow the on-screen instructions to provide the required information. The information needed depends upon the firmware version. See the applicable IBM Proventia Network IPS Installation Guide for more detailed information. Some of the required information includes:

Option	Description
Change Password	Change the admin, root, and Proventia Manager passwords that control access to each of these appliance areas.
Network Configuration Information	The IP address, subnet mask, and default gateway you entered through the LCD panel is displayed here. You can change this information as needed.
Host Configuration	Specify the host name and domain name for the appliance.
DNS Configuration	Specify how Proventia Network IPS uses DNS information to send e-mail and SNMP responses. If you do not configure this information during the setup process, you must specify the IP address of the mail server for Proventia Network IPS each time you define an e-mail or SNMP response.
	Select whether to let the DNS information be supplied by a DHCP server. If you do not enable the use of a DHCP-supplied DNS information, then supply the IP addresses for the DNS servers used to perform domain name lookups.
	You must also provide the DNS search path that should be used when performing DNS query searches.

Option	Description
Date/Time Configuration	Set the date and time as you want it to be displayed in the management interface.
Agent Name Configuration	Type the appliance name as it will be displayed in the management interface.
Port Link Configuration	Port link settings determine the appliance's performance mode, or how the appliance handles its connection to the network. Select link speeds and settings compatible with your network and in relation to the other devices that bracket the appliance. If you are not sure about your network settings, select **Auto** to let the appliance negotiate speed and duplex mode with the network.
Adapter Mode Configuration	The adapter mode determines how the appliance behaves within the network in order to protect it. • **Inline Protection Mode**: monitors the network and actively blocks malicious traffic. It includes the block, quarantine, and firewall responses. • **Inline Simulation Mode**: monitors the network without affecting traffic patterns to help you baseline and test your security policy. It includes simulated block and quarantine responses. • **Passive Monitoring Mode**: replicates traditional intrusion detection technology and monitors traffic without sitting inline. It includes the block response.

Connect to Proventia Manager

Proventia Manager is the Web-based management interface for the appliance. You use Proventia Manager to monitor the appliance status, to configure and manage settings, and to review and manage appliance activities.

Procedure

1. Start your web browser.
2. Type `https://<appliance IP address>` or type `https://<appliance host name>` if you are using a DNS server.
3. If needed, log in using the user name `admin` and the Proventia Manager password.

Install the product license

Proventia Network IPS requires a properly configured license file in order to 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.

About this task

Register your customer license and download the license from the IBM ISS Registration Center. Install the license using one of the following menu options. The option depend upon the firmware version.

- **System** > **Licensing**
- **Manage System Settings** > **Updates and Licensing** > **Administration**

Note: For more specific information on installing a product license and applying initial updates, see the applicable IBM Proventia Network IPS Installation Guide.

Apply initial updates

Ensure you have applied the latest updates to the appliance.

You can install the following update types:

- 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 the IBM Internet Security Systems X-Force research and development team.

Apply initial updates using one of the following menu options. The option depends upon the firmware version.

- **Updates** > **Available Downloads** and then **Updates** > **Available Installs**
- **Manage System Settings** > **Updates and Licensing** > **Administration**

Note: For more specific information on installing a product license and applying initial updates, see the applicable IBM Proventia Network IPS Installation Guide.

Next steps

Getting the latest documentation

You are now ready to configure advanced settings, including management, security, and firewall settings. Go to the applicable IBM Proventia Network IPS Appliance User Guide for more information. Find the latest documentation on the IBM ISS Product Documentation Web site at http://www.iss.net/support/documentation.

Customer Support

IBM Internet Security Systems offers a variety of contact options. To view these options, please visit http://www.iss.net/support/contact.html.

Copyright statement

(P) PN:51J2417

‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖

(2P) EC:L68216

‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖

(4L) Origin:SG

‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖‖

Printed in Singapore