IBM Security
Network Intrusion Prevention System

Network Intrusion Prevention System Installation Guide

Version 1 Release 4.5

Publication Date: August, 2012

Contents

Homologation statement - regulation notice

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks.

本製品は、電気通信事業者の通信回線への直接、またはそれに準ずる方法での接続を目的とするものではありません。

Safety, environmental, and electronic emissions notices

Safety notices may be printed throughout this guide. **DANGER** notices warn you of conditions or procedures that can result in death or severe personal injury. **CAUTION** notices warn you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous. **Attention** notices warn you of conditions or procedures that can cause damage to machines, equipment, or programs.

DANGER notices

DANGER

To prevent a possible shock from touching two surfaces with different protective ground (earth), use one hand, when possible, to connect or disconnect signal cables. (D001)

DANGER

Overloading a branch circuit is potentially a fire hazard and a shock hazard under certain conditions. To avoid these hazards, ensure that your system electrical requirements do not exceed branch circuit protection requirements. Refer to the information that is provided with your device or the power rating label for electrical specifications. (D002)

DANGER

If the receptacle has a metal shell, do not touch the shell until you have completed the voltage and grounding checks. Improper wiring or grounding could place dangerous voltage on the metal shell. If any of the conditions are not as described, STOP. Ensure the improper voltage or impedance conditions are corrected before proceeding. (D003)

DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on the metal parts of the system or the devices that attach to the system. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (D004)

DANGER

When working on or around the system, observe the following precautions:

Electrical voltage and current from power, telephone, and communication cables are hazardous. To avoid a shock hazard:

- **Connect power to this unit only with the IBM® ISS provided power cord. Do not use the IBM ISS provided power cord for any other product.**
- **Do not open or service any power supply assembly.**
- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **The product might be equipped with multiple power cords. To remove all hazardous voltages, disconnect all power cords.**
- **Connect all power cords to a properly wired and grounded electrical outlet. Ensure that the outlet supplies proper voltage and phase rotation according to the system rating plate.**
- **Connect any equipment that will be attached to this product to properly wired outlets.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following procedures when installing, moving, or opening covers on this product or attached devices.**

To disconnect:

1. **Turn off everything (unless instructed otherwise).**
2. **Remove the power cords from the outlets.**
3. **Remove the signal cables from the connectors.**
4. **Remove all cables from the devices.**

To connect:

1. **Turn off everything (unless instructed otherwise).**
2. **Attach all cables to the devices.**
3. **Attach the signal cables to the connectors.**
4. **Attach the power cords to the outlets.**
5. **Turn on the devices.**

(D005)

CAUTION notices

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at great than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

CAUTION:
The battery contains lithium. To avoid possible explosion, do not burn or charge the battery.

Do not:

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Exchange only with the IBM ISS-approved part. Recycle or discard the battery as instructed by local regulations. In the United States, IBM ISS has a process for the collection of this battery. For information, call 1-800-426-4333. Have the IBM ISS part number for the battery unit available when you call. (C003)

CAUTION:
For 19" rack mount products:

- **Do not install a unit in a rack where the internal rack ambient temperatures will exceed the manufacturer's recommended ambient temperature for all your rack-mounted devices.**
- **Do not install a unit in a rack where the air flow is compromised. Ensure that air flow is not blocked or reduced on any side, front, or back of a unit used for air flow through the unit.**
- **Consideration should be given to the connection of the equipment to the supply circuit so that overloading the circuits does not compromise the supply wiring or overcurrent protection. To provide the correct power connection to a rack, refer to the rating labels located on the equipment in the rack to determine the total power requirement of the supply circuit.**
- *(For sliding drawers)* **Do not pull or install any drawer or feature if the rack stabilizer brackets are not attached to the rack. Do not pull out more than one drawer at a time. The rack might become unstable if you pull out more than one drawer at a time.**
- *(For fixed drawers)* **This drawer is a fixed drawer and must not be moved for servicing unless specified by the manufacturer. Attempting to move the drawer partially or completely out of the rack might cause the rack to become unstable or cause the drawer to fall out of the rack.**

(R001 Part 2 of 2)

Product handling information

One of the following two safety notices may apply to this product. Please refer to the specific product specifications to determine the weight of the product to see which applies.

CAUTION:
This part or unit is heavy but has a weight smaller than 18 kg (39.7 lb). Use care when lifting, removing, or installing this part or unit. (C008)

CAUTION:
The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

Product safety labels

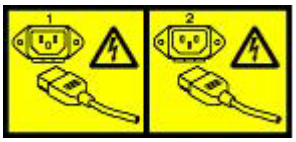
One or more of the following safety labels may apply to this product.

DANGER

Hazardous voltage, current, or energy levels are present inside any component that has this label attached. Do not open any cover or barrier that contains this label. (L001)

DANGER

Multiple power cords. The product might be equipped with multiple power cords. To remove all hazardous voltages, cdisconnect all power cords. (L003)



World trade safety information

Several countries require the safety information contained in product publications to be presented in their national languages. If this requirement applies to your country, a safety information booklet is included in the publications package shipped with the product. The booklet contains the safety information in your national language with references to the US English source. Before using a US English publication to install, operate, or service this IBM ISS product, you must first become familiar with the related safety information in the booklet. You should also refer to the booklet any time you do not clearly understand any safety information in the US English publications.

Laser safety information

The following laser safety notices apply to this product:

CAUTION:
This product may contain one or more of the following devices: CD-ROM drive, DVD-ROM drive, DVD-RAM drive, or laser module, which are Class 1 laser products. Note the following information:

- **Do not remove the covers. Removing the covers of the laser product could result in exposure to hazardous laser radiation. There are no serviceable parts inside the device.**
- **Use of the controls or adjustments or performance of procedures other than those specified herein might result in hazardous radiation exposure. (C026)**

CAUTION:
Data processing environments can contain equipment transmitting on system links with laser modules that operate at greater than Class 1 power levels. For this reason, never look into the end of an optical fiber cable or open receptacle. (C027)

Laser compliance

All lasers are certified in the U.S. to conform to the requirements of DHHS 21 CFR Subchapter J for class 1 laser products. Outside the U.S., they are certified to be in compliance with IEC 60825 as a class 1 laser product. Consult the label on each part for laser certification numbers and approval information.

Product recycling and disposal

This unit must be recycled or discarded according to applicable local and national regulations. IBM encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. IBM offers a variety of product return programs and services in several countries to assist equipment owners in recycling their IT products. Information on IBM ISS product recycling offerings can be found on IBM's Internet site at http:// www.ibm.com/ibm/environment/products/prp.shtml.

Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de programas y servicios de devolución de productos en varios países, a fin de ayudar a los propietarios de equipos a reciclar sus productos de TI. Se puede encontrar información sobre las ofertas de reciclado de productos de IBM en el sitio web de IBM http:// www.ibm.com/ibm/environment/products/prp.shtml.

Notice: This mark applies only to countries within the European Union (EU) and Norway.

Appliances are labeled in accordance with European Directive 2002/96/EC concerning waste electrical and electronic equipment (WEEE). The Directive determines the framework for the return and recycling of used appliances as applicable through the European Union. This label is applied to various products to indicate that the product is not to be thrown away, but rather reclaimed upon end of life per this Directive.

In accordance with the European WEEE Directive, electrical and electronic equipment (EEE) is to be collected separately and to be reused, recycled, or recovered at end of life. Users of EEE with the WEEE marking per Annex IV of the WEEE Directive, as shown above, must not dispose of end of life EEE as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and recovery of WEEE. Customer participation is important to minimize any potential effects of EEE on the environment and human health due to the potential presence of hazardous substances in EEE. For proper collection and treatment, contact your local IBM representative.

注意: このマークは EU 諸国およびノルウェーにおいてのみ適用されます。

この機器には、EU 諸国に対する廃電気電子機器指令 2002/96/EC(WEEE) のラベルが貼られています。この指令は、EU 諸国に適用する使用済み機器の回収とリサイクルの骨子を定めています。このラベルは、使用済みになった時に指令に従って適正な処理をする必要があることを知らせるために種々の製品に貼られています。

Remarque: Cette marque s'applique uniquement aux pays de l'Union Européenne et à la Norvège.

L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette précise que le produit sur lequel elle est apposée ne doit pas être jeté mais être récupéré en fin de vie.

Battery return program

This product contains a lithium battery. The battery must be recycled or disposed of properly. Recycling facilities may not be available in your area. For information on disposal of batteries outside the United States, go to http://www.ibm.com/ibm/environment/products/ batteryrecycle.shtm or contact your local waste disposal facility.

In the United States, IBM has established a return process for reuse, recycling, or proper disposal of used IBM sealed lead acid, nickel cadmium, nickel metal hydride, and other battery packs from IBM equipment. For information on proper disposal of these batteries, contact IBM at 1-800-426- 4333. Please have the IBM part number listed on the battery available prior to your call.

For Taiwan:

Please recycle batteries 廢電池請回收

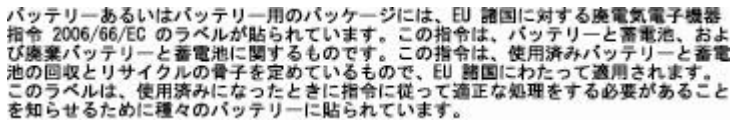
For the European Union:

Notice: This mark applies only to countries within the European Union (EU).

Batteries or packing for batteries are labeled in accordance with European Directive 2006/66/EC concerning batteries and accumulators and waste batteries and accumulators. The Directive determines the framework for the return and recycling of used batteries and accumulators as applicable throughout the European Union. This label is applied to various batteries to indicate that the battery is not to be thrown away, but rather reclaimed upon end of life per this Directive.

Les batteries ou emballages pour batteries sont étiquetés conformément aux directives européennes 2006/66/EC, norme relative aux batteries et accumulateurs en usage et aux batteries et accumulateurs usés. Les directives déterminent la marche à suivre en vigueur dans l'Union Européenne pour le retour et

le recyclage des batteries et accumulateurs usés. Cette étiquette est appliquée sur diverses batteries pour indiquer que la batterie ne doit pas être mise au rebut mais plutôt récupérée en fin de cycle de vie selon cette norme.


バッテリーあるいはバッテリー用のパッケージには、EU 諸国に対する廃電気電子機器指令 2006/66/EC のラベルが貼られています。この指令は、バッテリーと蓄電池、および廃棄バッテリーと蓄電池に関するものです。この指令は、使用済みバッテリーと蓄電池の回収とリサイクルの骨子を定めているもので、EU 諸国にわたって適用されます。このラベルは、使用済みになったときに指令に従って適正な処理をする必要があることを知らせるために種々のバッテリーに貼られています。

In accordance with the European Directive 2006/66/EC, batteries and accumulators are labeled to indicate that they are to be collected separately and recycled at end of life. The label on the battery may also include a symbol for the metal concerned in the battery (Pb for lead, Hg for the mercury, and Cd for cadmium). Users of batteries and accumulators must not dispose of batteries and accumulators as unsorted municipal waste, but use the collection framework available to customers for the return, recycling, and treatment of batteries and accumulators. Customer participation is important to minimize any potential effects of batteries and accumulators on the environment and human health due to potential presence of hazardous substances. For proper collection and treatment, contact your local IBM representative.

For California:

Perchlorate Material - special handling may apply. See http://www.dtsc.ca.gov/ hazardouswaste/ perchlorate.

The foregoing notice is provided in accordance with California Code of Regulations Title 22, Division 4.5, Chapter 33. Best Management Practices for Perchlorate Materials. This product, part, or both may include a lithium manganese dioxide battery which contains a perchlorate substance.

Electronic emissions notices

The following statements apply to this IBM product. The statement for other IBM products intended for use with this product will appear in their accompanying manuals.

Federal Communications Commission (FCC) Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. this equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions contained in the installation manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Note: Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors, by installation or use of this equipment other than xvi IBM Internet Security Systems as specified in the installation manual, or by any other unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

Note: This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Canadian Department of Communications Compliance Statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité aux normes du ministère des Communications du Canada

Cet appareil numérique de las classe A est conform à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/ EEC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM ISS cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM ISS option cards.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Warning:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

European Community contact:

IBM Technical Regulations
Pascalstr. 100, Stuttgart, Germany 70569
Telephone: 0049 (0) 711 785 1176
Fax: 0049 (0) 711 785 1283
e-mail: tjahn@de.ibm.com

EC Declaration of Conformity (In German)

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EUMitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem “Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)“. Dies ist die Umsetzung der EU-Richtlinie 89/336/EWG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 18. September 1998 (bzw. der EMC EG Richtlinie 89/336) für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EGKonformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die IBM Deutschland GmbH, 70548 Stuttgart.

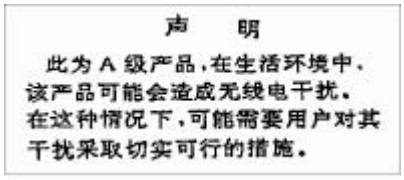
Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A

update: 2004/12/07

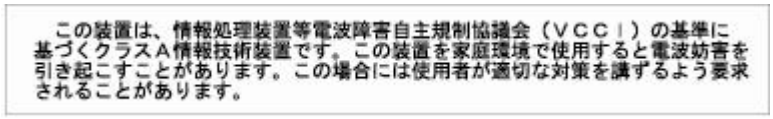
People's Republic of China Class A Compliance Statement:

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may need to perform practical actions.

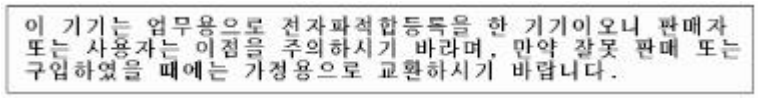


Japan Class A Compliance Statement:

This product is a Class A Information Technology Equipment and conforms to the standards set by the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). In a xviii IBM Internet Security Systems domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.



Korean Class A Compliance Statement:



About this publication

This section describes the scope and audience for this guide, identifies related publications, and provides contact information.

Scope

This publication describes how to install and configure Firmware version 4.1 (or newer) for Network IPS systems.

Intended audience

This publication is intended for network security system administrators who are responsible for installing and configuring Network IPS systems. Readers need to be familiar with network security policies and IP network configuration.

Related publications

See the following publications for more information:

Document	Description
IBM Security Network Intrusion Prevention System User Guide	A guide that explains the concepts and capabilities of the Network IPS system.
IBM Security Network Intrusion Prevention System Help	• Help for the IPS Local Management Interface (for local appliance management) • Help for the Proventia Network IPS Policy Editor (in SiteProtector)
Release Notes®	The most current information about product issues and updates, and how to contact Support located at http://www.iss.net/download/.

Support knowledge base

The IBM Support knowledge base is a valuable source of information. Visit the knowledge base at IBM Support knowledge base.

License agreement

For licensing information about IBM products, download the IBM Licensing Agreement from http://www.ibm.com/services/us/iss/html/contracts_landing.html.

Customer support

Before you contact IBM Security Solutions about a problem, see the IBM Support Home. This site provides the following information:

- Registration and eligibility requirements for receiving support
- Customer support telephone numbers for the country in which you are located
- Information you must gather before contacting customer support

Chapter 1. Installing Firmware version 4.1 (or newer)

This chapter provides important information about Firmware version 4.1 (or newer), explains how to back up the firmware on your current Network IPS system, and how to install Firmware version 4.1 (or newer) using a USB device/ISO image (IBM Security GX series systems) or an OVF file (IBM Security GV series systems).

Release-specific information

This topic provides information about supported Network IPS systems, supported versions of IBM SiteProtector, and the types of installation files available for Firmware version 4.1 (or newer).

Supported Network IPS systems

Firmware version 4.1 (or newer) supports the following IBM Security GX series systems:

GX4000 series
GX4000 series, V2
GX5000 series
GX5000 series, V2
GX6000 series

Firmware version 4.1 (or newer) supports the following IBM Security GV series systems:

GV200
GV1000

The correct firmware update path depends on the Network IPS system and the firmware version it is running.

Table 1. Network IPS systems and available update paths

Network IPS system	Current® version	Update path
G400 G2000	1.7	1.8
GX3000 series GX4000 series GX5000 series	1.7	1.8 + 4.1
GX6116	2.4	2.5 + 4.1
GX4000 series, V2 GX5000 series, V2 GX6116	3.2	3.2 + 4.1
GV200 GV1000	3.1	3.3 + 4.1 **Note:** IBM Security GV series systems running Firmware version 3.1 can move directly to version 3.3. (Updating to version 3.2 is not required.)

After you complete the update for Firmware version 4.1 (or newer), all currently supported Network IPS systems will be on the same firmware version and share the same update stream for future updates. This firmware release also removes limitations related to grouping similar systems into their own groups in SiteProtector. You can include a variety of Network IPS systems in the same SiteProtector group.

Because all supported Network IPS systems can run the same firmware version, you can now manage different systems in the same SiteProtector group because they all use the same policy versions.

Example: Before the Firmware version 4.1 (or newer) release, GX6116 systems could not be in a group with other Network IPS systems because of policy differences. This restriction no longer applies.

IBM Management SiteProtector™ system support

Check the release notes for the firmware version to determine the supported SiteProtector database service pack.

Types of installation files

You can download the USB image or the ISO image for IBM Security GX series systems, or download the Open Virtualization Format (OVF) file for IBM Security GV series systems from the IBM Download Center at http://www.iss.net/download/.

Compatibility

The following topic lists the web browsers and Java™ Runtime Environment (JRE) versions currently supported by the appliance.

Web browser compatibility

The following browser's are supported:

- Internet Explorer 8
- Internet Explore 9
- Firefox 13

Java Runtime Environment compatibility

JRE 1.6 and 1.7 are supported. Do one of the following actions when using JRE.

Important: JRE 1.7 works for only 32-bit Windows systems. It does not work with 64-bit Windows systems

- Clear the Java cache, often.
- Disable the Java console from keeping temporary files on the computer.
- Set the Java cache maximum space to zero.

Backing up a working version of your firmware

Use this procedure to create a backup copy of your current Network IPS firmware.

Procedure

1. Log on to the Network IPS system as `admin` using a local or a serial console.
2. From the Configuration Menu, select **Appliance Management**.
3. Select **Backup Current Configuration**.
4. Select **OK**. The Network IPS system saves configuration settings to a backup partition.

5. Copy the backup files to another location before you update your system with this firmware release.

What to do next

Upgrade your Network IPS system to Firmware version 4.1 (or newer).

Important: Installing Firmware version 4.1 (or newer) will re-image your Network IPS system. Make sure you have copied your files to another location before you install this firmware release.

Restoring firmware from a system backup

Use this procedure to restore your firmware from a backup copy using either SSH or a serial console connection for a remote installation.

About this task

If needed, you can use this procedure to revert the firmware on your Network IPS system to Firmware version 1.7 or Firmware version 2.5 after you have installed Firmware version 4.1 (or newer).

Procedure

1. Re-image your Network IPS system using the original CD ISO image for that release.
2. Set up your Network IPS system.
3. Copy your backup files onto the computer that is running the Network IPS system.
4. Log on to your Network IPS system as `admin`.
5. From the Configuration Menu, select **Appliance Management**.
6. Select **Restore Configuration From Backup** and then follow the prompts.

Restoring your Network IPS GX6000 system to factory defaults

Use this procedure to restore your Network IPS GX6000 series system to the factory defaults.

Procedure

1. Log on to the Network IPS system as `admin` using a local or serial console.
2. From the Configuration Menu, select **Appliance Management**.
3. Select **Restore to Factory Default (unconfigured)**.

Section A: Installation options for Network IPS systems

This section describes how to retrieve and install Firmware version 4.1 (or newer) on the specific operating system you are running on the computer that is connected to the Network IPS system.

Retrieving and installing firmware from an ISO image

You can download the ISO image for this firmware release from the IBM Download Center at http://www.iss.net/download/.

To install the ISO image for this firmware release, see the installation procedures for either the PXE boot server or the CD-ROM drive in Chapter 4, "Reinstalling the Network IPS firmware," on page 29 in this guide.

Retrieving and installing firmware using a USB device on a Windows OS

Use this procedure to retrieve and install the Network IPS firmware using a USB device on a Windows OS.

About this task

This procedure is not supported on the Proventia® GX3000 series, the Proventia GX4000 series (rev-A hardware), and the Proventia GX5000 (rev-A hardware with BIOS revisions before September 03 2009, version 6200I020).

If you are using one of the systems listed above, then you must use the ISO image to install Firmware version 4.1 (or newer). See the topic "Retrieving and installing firmware from an ISO image" on this page for more information.

Procedure

1. Retrieve the Network IPS firmware from the IBM Download Center at http://www.iss.net/download/.
2. Save the firmware to a secure host on your network.
3. Insert the USB device into a USB port on the same host and note where the operating system assigns the device.
4. Start an image writer program for Windows, such as Win32DiskImager.exe.

   Note: Depending on the program you use, you might need to change the extension of the firmware file. For example, you might need to rename the extension of the file from `.usbimg` to `.img`.
5. In the image writer program, write the firmware image to the USB device.
6. Connect the USB device to the Network IPS system. The system should be turned off.
7. Start the Network IPS system. You might need to type `b` for USB or you might need to go into the BIOS.
8. Type `reinstall`. This command installs the Network IPS firmware onto the system.

   Note: The Network IPS system restarts after the installation.

What to do next

Configure network settings for the IBM Security Network IPS system.

See Chapter 2, "Configuring network settings for the Network IPS system," on page 11 in this guide for network configuration procedures.

Retrieving and installing firmware using a USB device on a Linux OS

Use this procedure to retrieve and install the Network IPS firmware using a USB device on a Linux OS.

About this task

This procedure is not supported on the Proventia GX3000 series, the Proventia GX4000 series (rev-A hardware), and the Proventia GX5000 (rev-A hardware with BIOS revisions before September 03 2009, version 6200I020).

If you are using one of the systems listed above, then you must use the ISO image to install Firmware version 4.1 (or newer). See the topic "Retrieving and installing firmware from an ISO image" on page 5 in this guide for more information.

Procedure

1. Retrieve the Network IPS firmware from the IBM Download Center at http://www.iss.net/download/.
2. Save the firmware to a secure host on your network.
3. Insert the USB device into a USB port on the same host and note where the operating system assigns the device.
4. On the secure host, type `dd if=file.usbimage of=/dev/yourflashdevice` at the command line.

   Note: `/dev/yourflashdevice` is the **full** drive path, not a partition. **Example:** `/dev/sdb` (not `/dev/sdb1`)
5. Connect the USB device to the Network IPS system. The system should be turned off.
6. Start the Network IPS system. You might need to type `b` for USB or you might need to go into the BIOS.
7. Type `reinstall`. This command installs the Network IPS firmware onto the system.

   Note: The Network IPS system restarts after the installation.

What to do next

Configure network settings for the IBM Security Network IPS system.

See Chapter 2, "Configuring network settings for the Network IPS system," on page 11 in this guide for network configuration procedures.

Retrieving and installing firmware using a USB device on a Mac OS

Use this procedure to retrieve and install the Network IPS firmware using a USB device on a Mac OS.

About this task

This procedure is not supported on the Proventia GX3000 series, the Proventia GX4000 series (rev-A hardware), and the Proventia GX5000 (rev-A hardware with BIOS revisions before September 03 2009, version 6200I020).

If you are using one of the systems listed above, then you must use the ISO image to install Firmware version 4.1 (or newer). See the topic "Retrieving and installing firmware from an ISO image" on page 5 in this guide for more information.

Procedure

1. Retrieve the Network IPS firmware from the IBM Download Center at http://www.iss.net/download/.
2. Save the firmware to a secure host on your network.

3. On the secure host, open a Terminal Window.
4. Run the `diskutil list` command for a current list of devices.
5. Insert the USB device into a USB port on the secure host.
6. Run the `diskutil list` command again and determine which device node the system has assigned the USB device to.
7. Run the `sudo dd if=/path/to/downloaded.img of=/dev/rdiskN bs=1m` command.
8. Replace `/path/to/downloaded.img` with the path to the firmware file.

   Note: If you receive the error `dd: Invalid number '1m', you are using GNU dd`, then replace `bs=1m` with `bs=1M`.
9. Run the `diskutil eject /dev/diskN` command, and then remove your device after the command completes.
10. Connect the USB device to the Network IPS system. The system should be turned off.
11. Start the Network IPS system. You might need to type `b` for USB or you might need to go into the BIOS.
12. Type `reinstall`. This command installs the Network IPS firmware onto the system.

    Note: The Network IPS system restarts after the installation.

What to do next

Configure network settings for the IBM Security Network IPS system.

See Chapter 2, “Configuring network settings for the Network IPS system,” on page 11 in this guide for network configuration procedures.

Section B: Installation options for Network IPS GV series systems

This section describes how to import and install Firmware version 4.1 (or newer) using an Open Virtualization Format (OVF) file and how to install Firmware version 4.1 (or newer) using a VMX file.

Pre-configured settings

The following table lists the pre-configured settings that are imported with the OVF file for the GV series system.

Selection	Setting
Guest operating system	Linux
Version (guest operating system)	Other Linux 32-bit
Number of virtual processors	1
Memory	1024 MB
Number of NICs	4 Eth0: TCP Reset Port Eth1: Management Eth2: Protected A Eth3: Protected B
SCSI Adapter	BusLogic
Virtual disk size (storage)	8 GB, stored with the virtual machine
Virtual device node	SCSI (0:0)

Installing an OVF file for a Network IPS GV series system

Use this procedure to import and install the OVF file for the GV series system.

Before you begin

You must have a virtual environment with virtual switches already configured. If you do not, consult your VMware documentation.

Download the OVF file from the IBM Download Center at http://www.iss.net/download/.

About this task

The virtual software to use and the file type to install depends on the model of your GV series system.

Procedure

1. In VMware ESX or VMware ESXi, use the VMware vSphere Client, and navigate to **File** > **Deploy OVF Template** > **Import**. An importing wizard opens.
2. Click **Browse** to navigate to the OVF file on your network.
3. Complete the following sections of the importing wizard with the settings that are applicable to your network:

Option	Description
Name and Location	The name and location in your network of the GV series system.
Datastore	The data store in your network that stores the files for the GV series system.

Option	Description
Network Mapping	The networks in your virtual environment that map to the networks of the GV series system: Network adapter 1: TCP Reset Port Network adapter 2: Management Network adapter 3: Protected A Network adapter 4: Protected B **Important:** Map a different virtual network to each protected and managed port. If each port does not have its own virtual network, a loop might occur in the network and result in network failure.

After the wizard is finished, the system takes a few minutes to import the GV series system.

4. Click **Edit Virtual Machine Settings** in the VMware Infrastructure Client.
5. Click **Edit Settings**. A Virtual Machine Properties window opens.
6. For each network adapter, make sure you highlight the adapter and enable the **Connect at power on** check box.

What to do next

Configure network settings for the IBM Security Network IPS system.

See Chapter 2, "Configuring network settings for the Network IPS system," on page 11 in this guide for network configuration procedures.

Installing a VMX file for a Network IPS GV series system

Use this procedure to install the VMX file for the GV series system.

Before you begin

You must have a virtual environment. If you do not, consult your VMware documentation.

Download the VMX file from the IBM Download Center at http://www.iss.net/download/.

About this task

The virtual software to use and the file type to install depends on the model of your GV series system.

Procedure

1. In VMware Server, use the VMware Infrastructure Web Access and click **Add Virtual Machine to Inventory** in the Commands pane.
2. Select the VMX file for the GV series system and click **OK**. VMware Server adds the GV series system to the inventory.
3. In VMware Infrastructure Web Access, select the GV series system from the Inventory pane.
4. Review the network adapters in the Hardware pane. The network adapters should correspond to the following virtual networks:
   Network adapter 1: TCP Reset Port
   Network adapter 2: Management
   Network adapter 3: Protected A
   Network adapter 4: Protected B

   Tip: You can use the Virtual Network Editor from VMware to review and assign Network Interface Cards (NICs) to virtual networks.

5. If the virtual networks do not correspond to the network adapters listed earlier, configure the network adapters.
   a. Click the arrow next to the network adapter.
   b. Configure the options in the Network Adapter window to use these listed settings:

Option	Description
Device Status	Connected
Connect at power on	Enabled
Network Connection	Appropriate virtual network
MAC Address	Generated by the host

What to do next

Configure network settings for the IBM Security Network IPS system.

See Chapter 2, “Configuring network settings for the Network IPS system,” on page 11 in this guide for network configuration procedures.

Chapter 2. Configuring network settings for the Network IPS system

This chapter describes how to configure network settings for the Network IPS system after you have installed Firmware version 4.1 (or newer).

There are two network configuration methods available for Firmware version 4.1 (or newer):

- Zero configuration networking

  Zero configuration networking is a network configuration method that was introduced for Firmware version 4.1 (or newer). This method simplifies the initial setup of the Network IPS system because you use Bonjour, a zero configuration networking application from Apple, to discover the Network IPS system on the network and then use IPS Setup, a new Web-based configuration wizard, to configure network settings for the IPS system.
- LCD panel or serial console connection for IBM Security GX series systems or VMware console for IBM Security GV series systems

  If you do not want to use zero configuration networking to configure network settings, Firmware version 4.1 (or newer) still supports the traditional method of configuring network settings from the LCD panel (or using a serial console connection). Additionally, you can still use the setup program, IPS Setup, to complete the initial network configuration.

Section A: Using zero configuration networking

This section explains the concept of zero configuration networking as it applies to configuring network settings for the Network IPS system.

What is zero configuration networking?

Zero configuration networking allows you to automatically create a network of devices without having to manually configure a DHCP server, DNS services, or network settings for each device that you want to connect to that network.

For Firmware version 4.1 (or newer), you can use zero configuration networking applications to configure network settings for the Network IPS system.

How zero configuration networking works with the Network IPS system

Zero configuration networking is based on the following three elements:

- Automatic IP address selection for networked devices (which eliminates the need to configure a DHCP server)

  If the Network IPS system does not have an IP address assigned to it, then zero configuration networking uses link-local addressing to create an IP address in a range from 169.254.1.0 to 169.254.254.25. When an IP address is chosen, the link-local process sends out a query with that IP address onto the network to see if the IP address is already in use. If there is no response, the IP address is then assigned to the Network IPS system.
- Automatic domain name resolution and distribution of computer host names (which eliminates the need to configure a DNS server)

  Zero configuration networking implements multicast DNS (mDNS). mDNS allows the Network IPS system to select a domain name in the local namespace and then broadcast that name using a special multicast IP address, allowing other devices on the network to connect to it by name instead of by numbered IP address.

- Automatic location of network services through DNS service discovery (which eliminates the need for you to set up a directory server)

  Zero configuration networking enables the Network IPS system to use standard DNS queries to discover devices registered on the network that are broadcasting the services that they provide.

Zero configuration networking applications

You can use the following zero configuration networking applications with this release of the Network IPS system:

- Bonjour

  Bonjour is a zero configuration networking application from Apple that allows you to automatically create a network of devices in which hosts and services can connect to one another without requiring any user configuration. The services for each device are automatically registered on the network, and can be discovered by other devices on the network.

  If you are using a Windows computer connected to the Network IPS system, you must install the Bonjour plug-in for Windows. See the procedure for "Installing the Bonjour plug-in for Windows" in this guide.

  If you are using a Mac OS computer connected to the Network IPS system, there is no additional configuration needed because the Bonjour service discovery is already built into the Mac operating system.

- Avahi

  Avahi is an implementation of zero configuration networking that you use with Linux operating systems. Avahi is installed by default on most Linux systems and can run multicast DNS and DNS service discovery.

Installing the Bonjour plug-in for Windows

Use this procedure to install the Bonjour plug-in for Windows and then start IPS Setup, the Web Setup service that you use to automatically configure network settings for the Network IPS system.

Procedure

1. Install Firmware version 4.1 (or newer) on your Network IPS system from an ISO image or using an USB device. See Chapter 1, "Installing Firmware version 4.1 (or newer)," on page 1 in this guide for installation procedures.
2. Connect a Windows computer directly to the Network IPS system using an Ethernet crossover cable or connect a computer to the same network switch as the Network IPS system. The unconfigured system will initially obtain a DHCP-assigned IP address or link-local address (169.254.x.x). The range for the link-local address space is reserved from 169.254.0.0 - 169.254.255.255. However, 169.254.0.1 - 169.254.0.255 and 169.254.255.0 - 169.254.255.255 have been reserved for future use.
3. Download the Bonjour SDK for Windows Version 2.0, which includes Web browser plug-ins for Internet Explorer and Mozilla Firefox.
4. Install the plug-in on the Windows computer connected to the Network IPS system.
5. Open Internet Explorer and look for the Bonjour icon in the Internet Explorer toolbar. (If you do not see the Bonjour icon in the toolbar, you will need to reinstall Bonjour.)
6. Click on the Bonjour icon to display a window that lists the Bonjour services that are available on the network.
7. In the Bonjour menu, select the Network IPS system that you want to configure. The Network IPS name is displayed as "IBM Proventia GXmodel-LMI[serial number]" and offers a Web Setup service called IPS Setup.
8. Select the Web Setup service to start the IPS Setup wizard.

What to do next

Use IPS Setup to configure network settings for the Network IPS system.

Using the web version of IPS Setup to configure network settings

IPS Setup is a Web-based configuration wizard that you use to configure network settings for Network IPS.

Procedure

1. At the unconfigured login prompt, type the following login credentials, and then press **Enter**:
   - Username = admin
   - Password = admin
2. Follow the on screen instructions to complete the setup.

Option	Description
Welcome (including FIPS mode configuration)	Enable FIPS (Federal Information Processing Standards) mode. **Note:** Before you enable FIPS mode, see the *IBM Proventia Network IPS and SiteProtector FIPS Implementation Guide*. Enable FIPS mode only if you need FIPS compliancy. There is no advantage to enabling FIPS mode if you do not require FIPS compliance.
Service Agreement	Agree to the Software License Agreement and the Export Administration Regulations.
Upload License	Install the license file for the Network IPS system. **Important:** You will not be able to update the product without a valid license.
Root Password	Set the password that will be used to log directly into the Network IPS system (console) or to log in using SSH.
Network IPS Manager Password	Set the password that will be used to connect to IPS Local Management Interface, the web-based management interface for the Network IPS system.
Management Interface	Provide the following settings for the management interface: • **Host name:** The computer name for the Network IPS system. You can use up to 50 characters for a host name if there is no domain name, and up to 63 characters if you are using a fully-qualified domain name. **Example:** `myapplianceThe` period separating `hostname.domainname` is considered a character. **Example:** `mycompany.com` • **Agent name:** The name of the Network IPS system as it appears in the management interface. This name should correspond to a meaningful classification in the network scheme, such as a geographic location, business unit, or building address. • **mDNSResponder:** Select whether the Network IPS system will broadcast the network services that it provides. • **Configure IPv4 TCP/IP:** Select whether to use a DHCP-assigned IP address or use link-local addressing if a DHCP server is not available. • **Configure IPv6 TCP/IP:** Select whether to automatically assign the IPv6 address or to manually configure it. • **DNS Information:** Specify how 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 Network IPS each time you define an e-mail or an SNMP response.

Option	Description
Security Interfaces	Determine how Network IPS behaves in the network in order to protect it. Review the Proventia Network operating modes for a description of each mode and its behaviors. **Important:** (For Network IPS GV series systems only) When you select the adapter mode for the single port pair, confirm that you have selected the correct adapter mode for the network connections of the virtual system. You might experience significant network implications if you have configured this setting incorrectly. Select from the following modes: • **Inline Protection:** This mode monitors the network and actively blocks malicious traffic. It includes the block, quarantine, and firewall responses. **Note:** This is the default mode of the appliance. • **Passive Monitoring:** This mode replicates traditional intrusion detection technology and monitors traffic without sitting inline. It includes the block response. • **Inline Simulation:** This mode monitors the network without affecting traffic patterns to help you baseline and test your security policy. It includes simulated block and quarantine responses. Select the speed and duplex settings for your particular network. You can select **Auto** to allow Network IPS to determine the best choice for your network.
Date and Time	Set the date and the time for Network IPS as it appears in the management interface, so that you can accurately track events as they occur on the network. To synchronize the system time with a network time server, you must enable Network Time Protocol (NTP). Type the IP address or host name of the NTP server and select the NTP version. The appliance supports the use of NTP versions 1 through 4.
SiteProtector	Choose to register Network IPS with SiteProtector.
Updates	Install the latest security content available from IBM X-Force for Network IPS.
Completion	Review your configuration settings before they are applied.

3. After reviewing and pressing **Complete Setup**, the Network IPS system applies your settings.

What to do next

Access IPS Local Management Interface so that you can manage and monitor settings for your Network IPS system.

See the procedure "Accessing IPS Local Management Interface" on page 23 in this guide.

Using Bonjour from a Windows command line to discover services

If you are running the Network IPS system on Windows, you can use Bonjour to browse for services that are being broadcast on the local network.

DNS Service Discovery (DNS-SD) protocol

The DNS Service Discovery (DNS-SD) protocol can identify and discover devices on the network that have been enabled with the zero configuration standard. DNS-SD uses multicast DNS (mDNS). mDNS sends packets to every node on the network to resolve duplicate host names and to query the network for services.

From a Windows command-line, you can use the `dns-sd` command to browse for services that are being broadcast on the local network by mDNSResponder (a Bonjour system service that uses Multicast DNS Service Discovery for discovery of services on the local network).

Link-local address space

The range for the link-local address space is reserved from 169.254.0.0 - 169.254.255.255. However, 69.254.0.1 - 169.254.0.255 and 169.254.255.0 - 169.254.255.255 have been reserved for future use.

DNS queries that end in .local are sent to the address 224.0.0.251 (for IPv6: FF02::FB / FF02:0:0:0:0:0:0:FB) which is reserved for mDNS. Any packets that have been sent to these addresses are not forwarded beyond the local link or forwarded to the local link from outside the network. Any link-local multicast packet that is sent remains on the local link. Any link-local multicast packets that are received must originate from the local link.

Using the DNS-SD protocol to browse for services

Type `dns-sd -B _ssh._tcp` at the command line. You should see all SSH service broadcasts on the network.

Looking up the host name of a service

Type `dns-sd -L "<instance_name>" _ssh._tcp` at the command line, (where **"<instance name>"** is the name returned by the Browse command. For example: "IBM Proventia GX4002-SSH [30603041A0255]"

Important: Make sure you use quotation marks around the instance name.

Example of using SSH to access the Network IPS system using the .local host name returned by the Lookup command: `ssh root@unconfigured-gx4002-30603041A0255.local`

Browsing for a Web service instead of an SSH service

1. Type `dns-sd -B _http._tcp`, and then type `dns-sd -L "<instance_name>" _http._tcp`
2. In the Internet Explorer or Mozilla Firefox Location bar, type `https://<hostname>.local/`.

   Example: `https://unconfigured-gx4002-30603041A0255.local/`

Using Avahi command-line programs to discover services

If you are running the Network IPS system on Linux, you can use Avahi to browse for services that are being broadcast on the local network.

Before you begin: You must install the Avahi RPM package for the Linux operating system you are using before you can use the following command-line programs.

Using the avahi-browse command-line program /usr/bin/avahi-browse

avahi-browse is a command-line program that you can use to browse for all mDNS broadcasts on the network and to resolve the host name and IP address of the device performing the broadcasts.

avahi-browse command-line options: avahi-browse <options> <service type>

Use the following command-line options with the avahi-browse program:

Option	Description
`-d <domain>`	Specifies the domain in which you want to browse for services on. If you do not specify a domain, then all domains will be browsed. The Network IPS system broadcasts on the .local domain.
`--resolve`	Displays the host name and the IP address of the Network IPS system, including the service advertisement string. **Example:** "IBM Proventia GX4004--SSH"
`-t`	Terminates the avahi-browse program after dumping the current list of named services. The avahi-browse program no longer runs or listens for new broadcasts.
`-a`	Displays all service broadcasts on the network. You do not need to specify a **<service type>** with this command-line option.
`--no-db-lookup`	Instructs the avahi-browse program not to translate service types. **Example:** Translating `_ssh._tcp` to a friendlier name such as "SSH Remote Terminal" or translating `_http._tcp` to "Web Site"

Example of viewing the SSH broadcast for your Network IPS system

Type `avahi-browse -d local _ssh._tcp --resolve -t` at the command line.

(`-d` and `-t` are optional. If you use the `-a` command-line option instead of `_ssh._tcp`, you will see all broadcasts.) The `--resolve` command-line option provides the host name and IP address of the Network IPS system, so that you can SSH to that system using `ssh admin@<hostname>.local` or `ssh admin@<ip_address>`.

Example of viewing a Web site broadcast for your Network IPS system

1. Type `avahi-browse -d local _http._tcp --resolve -t` at a command line.
2. Open a Web browser. In the Location bar, type `https://<hostname>` or `https://<ip_address>` using the host name or IP address that was returned by the `--resolve` command-line option.

Using the avahi-discover-standalone command-line program /usr/bin/avahi-discover-standalone

The avahi-discover-standalone command-line program is an X Window program that displays all the discoverable services across all domains. You can only run this program from an X Window session.

This command-line program is the same as running `avahi-browse -a --resolve`. You can use the host name and IP address returned by this program to connect to a Network IPS system using SSH or a using a Web browser.

Section B: Using the LCD panel or serial console connection

This section explains how to use the LCD panel or a serial console connection to configure network settings for the Network IPS system.

Connecting cables and starting the Network IPS system

You should connect Network IPS to the network after you have determined where you want to place it on the network. You should install network cabling and verify that traffic flows before you turn on the Network IPS system.

Procedure

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

   Note: TCP Reset: Management Port 2 is the TCP Reset Port. The Network IPS system 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 Network IPS in passive mode, only connect the first protected port in the pair to the network.
5. Turn on Network IPS.

What to do next

Configure network settings for the Network IPS system. You can use the LCD panel or establish a serial console connection to the Network IPS system.

Initial setup from the LCD panel

You can perform this procedure on all IBM Security GX series systems, except for the GX3000. This procedure lets you set basic networking configurations from the LCD panel when serial access is not possible.

Procedure

1. Press the **Up** or the **Down** arrows on the LCD panel to scroll to the Set IP Address screen.
2. Press the **Up** and the **Down** arrows to select a number and then press the **Right** arrow to move to the next field.
3. When you have completed all the fields, press **Enter**.
4. Select **OK** to move forward and then press **Enter** to confirm your selection.
5. Repeat steps 1 through 6 again to provide the subnet mask and default gateway.
6. After you enter your network information, a final conformation screen appears. Select **OK** to save all network information and to enable the Management port, or select **Cancel** to return to the IBM Proventia screen without saving any information.
7. After you confirm your settings, Network IPS generates a temporary, case-sensitive password. Record this password; you must use it when you log in to the Network IPS system.
8. Connect to the Network IPS system using a secure network connection and the Network IPS IP address to complete the initial configuration.

What to do next

Use IPS Setup to complete the initial configuration of the Network IPS system.

See the procedure “Using the console version of IPS Setup to configure network settings” on page 19 in this guide.

Initial setup using a serial console connection

You can perform this procedure in conjunction with the procedure for configuring network settings from the LCD panel earlier in this section, or you can perform this procedure alone to perform a full setup of the Network IPS system.

Before you begin

If you are configuring IBM Security GV series systems, skip this procedure and go to the topic Using Proventia Setup to configure network settings in this guide.

Procedure

1. Connect the serial console cable to the Network IPS system and a computer to complete the initial configuration.
2. Connect to the Network IPS system 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 to the Network IPS system:

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

Use IPS Setup to complete the initial configuration of the Network IPS system.

See the procedure “Using the console version of IPS Setup to configure network settings” on page 19 in this guide.

Using the console version of IPS Setup to configure network settings

IPS Setup is a program you use to configure network settings for the Network IPS system.

Before you begin

If you are working with a GV series system, you must turn on the virtual machine and open a console in the applicable virtual platform in use in your network.

Procedure

1. Connect to the Network IPS system using a secure network connection and the IP address of the Network IPS system, if applicable.
2. At the unconfigured login prompt, type `admin`, and then press **Enter**.
3. Perform one of the following actions:

Option	Action
If you used the LCD panel to initially configure the IP address, subnet mask, and default gateway	Type the case-sensitive password the Network IPS system generated for you and then press **Enter**
If you did not use the LCD panel or you are configuring a GV series system	Type `admin` for the password and then press **Enter**
If you are re-configuring your Network IPS system	Type the appropriate password for the admin user

4. Follow the on screen instructions to complete the setup.

Option	Description
FIPS-140 level 2 Configuration	Enable FIPS (Federal Information Processing Standards) mode. **Note:** Before you enable FIPS mode, see the *IBM Proventia Network IPS and SiteProtector FIPS Implementation Guide*. Enable FIPS mode only if you need FIPS compliancy. There is no advantage to enabling FIPS mode if you do not require FIPS compliance.
Change Password	Set the admin, root, and IPS Manager passwords.
Network Configuration	Displays the IP address, subnet mask, and default gateway you entered through the LCD panel. You can change this information as needed. • **IPv4 Network Configuration** If you do not use a DHCP-supplied IPv4 address, you must provide the IPv4 address of the management network adapter, the subnet mask value for the network that is connected to the management interface, and the IPv4 address for the management gateway. • **IPv6 Network Configuration** Choose whether to automatically assign the IPv6 address or to manually configure it. If you do not use a static IPv6 address, you must provide the IPv6 address of the management network adapter, the decimal value that makes up the network portion of the address, and the IPv6 address for the management gateway.
Host Configuration	Specify the host name and the domain name for the Network IPS system. Network IPS uses domain names to send e-mail and SNMP responses. • **Host name:** The computer name for the Network IPS system. **Example:** `myappliance` • **Domain Name:** The domain suffix (DNS search path) for the network. **Example:** `mycompany.com`

Option	Description
DNS Configuration	Specify how 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 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. **Example:** `10.0.0.1` You must also provide the DNS search path that should be used when performing DNS query searches.
Time Zone Configuration	Set the time zone for the Network IPS system.
Configure NTP	Configure an NTP server to provide Coordinated Universal Time (UTC) for accuracy. Type the host name or IP address of the server and type the NTP version. The appliance supports the use of NTP versions 1, 2, 3, and 4.
Date/Time Configuration	Set the date and the time for Network IPS as it appears in the management interface, so that you can accurately track events as they occur on the network.
Agent Name Configuration	Provide the Network IPS name as it appears in the management interface. This name should correspond to a meaningful classification in the network scheme, such as a geographic location, business unit, or building address.
Security Interface Configuration	Determine how Network IPS behaves within the network in order to protect it. Review the Proventia Network operating modes for a description of each mode and its behaviors. **Important:** (For Proventia GV series systems only) When you select the adapter mode for the single port pair, confirm that you have selected the correct adapter mode for the network connections of the virtual system. You might experience significant network implications if you have configured this setting incorrectly. Select from the following modes: • **Inline Protection:** This mode monitors the network and actively blocks malicious traffic. It includes the block, quarantine, and firewall responses. • **Passive Monitoring:** This mode replicates traditional intrusion detection technology and monitors traffic without sitting inline. It includes the block response. • **Inline Simulation:** This mode monitors the network without affecting traffic patterns to help you baseline and test your security policy. It includes simulated block and quarantine responses.
Interface Link Configuration	Select the speed and duplex settings for your particular network. You can select **Auto** to allow Network IPS to determine the best choice for your network.
Configure SiteProtector Management	Select to register Network IPS with SiteProtector.
Configure mDNS Service Discovery	If you disable **mDNS Service Discovery**, Network IPS does not broadcast a local management Web interface or SSH. The firewall also rejects multicast packets to destination address 224.0.0.251.
Review Settings	Review your settings before they are applied. To skip the review, press **Finish** on any screen. **Note:** If you are configuring Network IPS with an SSH terminal, you might lose your connection when the system applies your settings. You can manually reconnect to Network IPS with a new SSH session.

5. Press **Enter** to log off.

What to do next

Access IPS Local Management Interface so that you can install the product license and apply initial updates to the Network IPS system.

See the procedure “Accessing IPS Local Management Interface” on page 23 in this guide.

Chapter 3. Installing licenses and applying updates

This chapter describes how to access IPS Local Management Interface, how to install a license file, and how to apply the latest updates for your Network IPS system.

Accessing IPS Local Management Interface

IPS Local Management Interface is the Web-based management interface for the Network IPS system.

About this task

Use IPS Local Management Interface to perform the following tasks:

- Monitor the status of the system
- Configure and manage settings
- View quarantine tables and apply changes
- Review and manage system 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 IPS Local Management Interface password.

Section A: Installing licenses

This section explains how to acquire and install a license file for the Network IPS system.

Important: The Network IPS system requires a properly configured license file to run. If you do not install the appropriate license file, you cannot manage the system. To purchase a license, contact your IBM representative.

Acquiring the license file

Use the Licensing page in IPS Local Management Interface to view information about the current status of the license file, including expiration dates. The Licensing page also allows you to access the License Information page, which includes information about how to acquire a current license.

Procedure

1. Contact your IBM representative to get a license registration number.
2. Register your customer license at the IBM License Registration Center. Go to https://www1.iss.net/cgi-bin/lrc and follow the instructions.
3. Download the license key file from the IBM Registration Center.

   Note: You must save the license file in the appropriate location so that the IPS Local Management Interface software can locate and acknowledge it.

What to do next

Upload the license key file to a designated directory so that the Network IPS system can download and install the latest updates automatically.

Viewing current license settings

Use the Administration page in IPS Local Management Interface to view current information about your license and to upload license keys for the Network IPS system.

Procedure

1. In IPS Local Management Interface, select **Manage System Settings** > **Updates and Licensing** > **Administration**.
2. Review information in the Usage license and Maintenance license areas. These areas list the status of each license and when they expire.
3. In the Update Tools area, use the **Upload license key** option to upload license files.

Section B: Applying initial firmware or IPS updates

This section explains how to apply the latest updates to the Network IPS system. The system retrieves updates from the IBM Download Center, which is accessible on the Internet.

Updating your Network IPS system

You can update your Network IPS system in two ways:

- Configure automatic updates
- Find, download, and install updates manually

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 X-Force.

You can find updates on the Administration page in IPS Local Management Interface, and you can schedule automatic update downloads and installations from the Update Settings page.

Note: Some firmware updates require you to restart the Network IPS system. For more information about product issues and updates, see the readme file for your Network IPS system available from the IBM Download Center at http://www.iss.net/download/.

Checking for updates

Use the Update Tools area in IPS Local Management Interface to check for possible updates so that you can upload them and then install them on your Network IPS system.

Procedure

1. In IPS Local Management Interface, select **Manage System Settings** > **Updates and Licensing** > **Administration**.
2. In the Update Tools section, click on the **Check for Updates** link.
3. If there are updates, click **Upload Update File** to browse for the update files found after running the Check for Updates process.

Installing available updates

You can install available updates for the intrusion prevention or the firmware on your Network IPS system.

Before you begin

Make sure you create a system backup before you install any firmware updates. This way you will have a system backup before each automatic firmware update installation.

1. In IPS Local Management Interface, select **Manage System Settings** > **Updates and Licensing** > **Update Settings**
2. Click the **Update Settings** tab.
3. In the Firmware Updates area, enable **Perform Full System Backup Before Installation**.
4. Complete any other appropriate information that appears on the Update Settings tab.

Procedure

1. In IPS Local Management Interface, select **Manage System Settings** > **Updates and Licensing** > **Administration**.
2. Click the appropriate tab: **Firmware** or **Intrusion Prevention**.

   Note: Some firmware updates require you to restart the Network IPS system. For more information about product issues and updates, see the readme file for your Network IPS system available from the IBM Download Center at http://www.iss.net/download/.
3. If updates are available, click **Install Update**.

Scheduling automatic updates

Use the Update Settings page in IPS Local Management Interface to configure the Network IPS system to automatically check for and install updates.

How to schedule an automatic update (example)

The following example explains how to configure the Network IPS system to automatically check for updates daily at 3:00 A.M., automatically perform a system backup at 5:00 A.M., and then install the available firmware updates.

The following table describes the process for scheduling an automatic update:

Stage	Description
1	At 3:00 AM, the Network IPS system checks the IBM Download Center for updates.
2	The Network IPS system downloads security and firmware updates.
3	The Network IPS system installs security updates immediately.
4	At 5:00 AM, the Network IPS system performs these actions: • Reboots, and then creates a system backup • Installs the firmware update, and then reboots if necessary

Automatic update settings in IPS Local Management Interface

The following table describes the settings you can use in IPS Local Management Interface to update the Network IPS system automatically:

Section	Setting	Description
Automatically Check for Updates	Check for updates daily or weekly	If you enable this option, select the **Day Of Week** and **Time Of Day** for the Network IPS system to check for updates. **Note:** Set the system to check for updates at least one (1) hour before installing scheduled updates to ensure that the system has downloaded all the necessary updates.
	Check for updates at given intervals	Checks for updates several times a day. Type a value in the **Interval (minutes)** box, or move the slider bar to select a value. The minimum interval is 60 minutes; the maximum is 1440.
Security Updates	Automatically Download	Automatically downloads security updates.
	Automatically Install	Automatically installs security updates.
Firmware Updates	Automatically Download	Automatically downloads firmware updates.
Firmware Updates - Install Options	Perform Full System Backup Before Installation	Enables the Network IPS system to reboot and perform a full system backup before it installs any updates. **Note:** Each time the system performs a backup, it overwrites the previous system backup.
	Do Not Install	Downloads firmware updates but does not install them.
	Automatically Install Updates	Automatically installs firmware updates. **Note:** When the Network IPS system automatically installs updates, it might be offline for several minutes.
Firmware Updates - When To Install	Delayed	Installs updates on the **Day Of Week** and **Time Of Day** you specify. **Note:** You must configure automatic installation to occur at least one (1) minute after the Network IPS system has completed downloading updates.
	Immediately	Installs updates as soon as they are downloaded. **Important:** Choosing immediately, might cause link losses, often.
	Schedule One Time Install	Installs one update instance at the **Date** and **Time** you specify.

Section	Setting	Description
Firmware Updates - Which Version To Install	All Available Updates	Installs all update versions, including the most recent one.
	Up To Specific Version	Installs all versions up to the **Version** number you specify.

Troubleshooting download problems after applying a firmware update

Follow these steps if you experience problems in IPS Local Management Interface after you have applied a firmware update to the Network IPS system.

Procedure

1. Close your Web browser.
2. Clear the Java cache.
3. Restart your Web browser.
4. Log on to IPS Local Management Interface.

What to do next

For more information about how to clear the Java cache, see your operating system documentation.

Chapter 4. Reinstalling the Network IPS firmware

This chapter describes how to reinstall the firmware for your Network IPS system.

Important: When you reinstall the Network IPS system, you are erasing all data from the system and returning it to its factory state. Perform these procedures under the guidance of IBM Technical Support.

Reinstalling the Network IPS firmware does the following things:

- Overwrites software configuration changes you have made since you first installed the Network IPS system.
- Restores the original, default login credentials:
  - Username = admin
  - Password = admin

Reinstalling firmware for a Network IPS GX series system older than firmware version 4.1

The Recovery CD, included in the package of legacy Network IPS systems, contains the software that was installed on the system at the factory. You can reinstall the firmware from this CD using a PXE boot server, or reinstall the firmware directly from a CD-ROM drive.

Note: If you need to restore your Network IPS system with Firmware version 4.1 (or newer), and not a prior firmware release, use any of the procedures explained in "Section A: Installation options for Network IPS systems" on page 5 in this guide.

Reinstalling the firmware using a PXE boot server

Use this procedure to reinstall the Network IPS firmware using a PXE boot server.

Procedure

1. Turn off the Network IPS system.
2. Insert the recovery CD into the CD-ROM drive of the PXE boot server, and then restart the PXE boot server.
3. If you are prompted to do so, type `bootserv` and press **Enter**. 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.
4. Turn on the Network IPS system. 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 to press `L` to boot from LAN. If you do not press `L` within this time period, the system boots as usual, and you must restart the system.
5. Press the `L` key. The following message appears:

`Internet Security Systems Proventia GXxxxx Recovery Boot`

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

6. At the prompt, type `reinstall`, and then press **Enter**. The installer reloads the operating system. When the reinstallation is complete, the Network IPS system automatically reboots. Let the system complete the boot process without interruption.

   Important: Do not turn off the Network IPS system or remove power from the system at any time during the installation process. Removing power can corrupt the installation process and permanently damage the Network IPS system, resulting in a situation whereby the system must be returned to the factory. If you want to turn off the system, wait until you see the unconfigured login prompt.
7. When the Network IPS system has rebooted, the `unconfigured.appliance` login prompt appears.

   You can log in with the default user and password of `admin/admin` and configure the system using IPS Setup, IPS Setup, or you can configure the system using the LCD panel on the front of the system.

Reinstalling the firmware using a USB CD-ROM drive

Use this procedure to reinstall the Network IPS firmware using a USB CD-ROM drive.

Procedure

1. Turn off the Network IPS system.
2. Connect a USB CD-ROM drive to the USB port on the Network IPS system.
3. Connect one end of the serial console cable to the console port of the Network IPS system and connect the other end to the serial port on another computer.
4. Establish a serial connection from the computer to the Network IPS system using a terminal emulation program. Use the following settings:
   - Port: The serial port you have used on the computer, typically COM1.
   - Emulation: VT100
   - Bits per second: 9600
   - Data Bits: 8
   - Parity: None
   - Stop Bits: 1
   - Flow Control: None
5. Restart the Network IPS system and insert the Recovery CD into the USB CD-ROM drive drive. The Network IPS system starts from the CD and displays the following message:

   ```
   CAUTION: Reinstalling from the recovery CD restores the appliance to its original
   configuration and removes any customized settings. The appliance also reverts to the default
   password.
   ```
6. Type `reinstall`, and press **Enter**. When the reinstallation process is complete, the Network IPS system automatically restarts.

   Important: Allow the system to complete the boot process without interruption. You might risk damaging the system if you do otherwise.

Reinstalling firmware for a Network IPS GV series system

Use this procedure to retrieve and reinstall the firmware for a GV series system.

Before you begin

- Create a backup of the current system in IPS Local Management Interface. You can restore the system settings from this backup after you reinstall the GV series system. See the procedure "Backing up a working version of your firmware" on page 2 in this guide.
- Record the following settings for the management interface:
  - IP address, subnet mask, and default gateway
  - Host name, domain name, and DNS server name

Procedure

1. Download or retrieve the file for the GV series system in the appropriate format.
2. Install the file. See Chapter 1, "Installing Firmware version 4.1 (or newer)," on page 1 in this guide for installation procedures.

What to do next

Log in with the default user name and password (`admin/admin`), and use the IPS Setup wizard or the IPS Setup program to configure network settings for the GV series system.

See Chapter 2, "Configuring network settings for the Network IPS system," on page 11 in this guide for network configuration methods.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Project Management
C55A/74KB
6303 Barfield Rd.,
Atlanta, GA 30328
U.S.A

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

Special characters

A

B

D

F

I

J

L

M

N

O

P

R

S

U

V

W

Z

Printed in USA