IBM Security

IBM Security Network Intrusion Prevention System and SiteProtector Management FIPS Implementation Guide

Copyright statement

Publication Date: August, 2012

Contents

About this publication

This guide is designed to help you implement FIPS mode for your IBM® Security Network Intrusion Prevention System (IPS) appliance and IBM Security SiteProtector™ System.

Important: about Federal Information Processing Standards 140 (FIPS 140) Validation

For specific information about IBM Security products that are FIPS certified, consult the IBM Security FIPS 140 Security Policy documents. Find these documents on the National Institute of Standards and Technology (NIST) web site, in the Module Validation Lists section: http://csrc.nist.gov/groups/STM/cmvp/index.html.

Scope

This guide lists considerations for enabling FIPS mode on your module, explains how to configure web browsers for FIPS-supported ciphering, describes how to enable FIPS mode, and explains some of the issues and solutions that might arise when using FIPS mode.

Additional documentation is located on the IBM Security Product Information Center at http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp.

Intended audience

This guide is intended for network security system administrators who are responsible for installing and configuring Network IPS and the SiteProtector System. This guide assumes that you are familiar with network security policies and IP network configuration.

About IBM Security product documentation

Related publications

See the IBM Security Product Information Center at http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp for related documentation concerning Network IPS appliances and the SiteProtector System.

Knowledgebase

Known problems are documented in the form of individual technotes in the IBM Support knowledge base. As problems are discovered and resolved, the IBM Support team updates the knowledge base. By searching the knowledge base, you can quickly find workarounds or solutions to problems.

Licensing agreement

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

Technical support contacts

IBM provides technical support to customers who are entitled to receive support. You can find information related to Customer Support hours of operation, phone numbers, and methods of contact on the IBM Customer Support page.

The IBM Customer Support site

The IBM Customer Support page at http://www.ibm.com/services/us/iss/support/ provides direct access to online user documentation, current version listings, detailed product literature, white papers, the Technical Support knowledge base, and contact information for Customer Support.

Chapter 1. Configuring web browsers and Java for FIPS-supported ciphering

This chapter lists the Internet browser settings and Java options for FIPS-supported ciphering. It describes how to enable transport layer security (TLS) as the cryptographic protocol for FIPS compliance.

"Configuring web browser settings" on page 2

"Configuring Java settings" on page 2

Configuring web browser settings

This topic lists the security protocol options to set in your Internet browser for FIPS-supported ciphering and the Network IPS appliance.

About this task

You must configure Java and your browser for FIPS-supported ciphering. If you do not, you cannot access the LMI.

Procedure

1. Open your browser.
2. Go to the advanced security protocols. Consult documentation for your specific browser to find the location of these settings.
3. Enable the browser security protocol option **Use TLS 1.0**.

Configuring Java settings

This topic explains how to configure Java for FIPS-supported ciphering and the Network IPS appliance.

About this task

You must configure Java and your browser for FIPS-supported ciphering. If you do not, you cannot access the LMI.

Procedure

1. Go to the **Java** settings on the host. These settings can often be found in the **Control Panel**.
2. Go to the **Security** options, which might be found in the **Advanced** section. If it is not in this section, consult Java documentation for the exact location.
3. Enable **Use TLS 1.0**.

Chapter 2. Implementing FIPS on Network IPS appliances

This chapter lists issues to consider before implementing FIPS mode, describes how to restore an appliance to factory defaults, and explains how to enable FIPS mode on your Network IPS appliance.

"FIPS considerations for Network IPS appliances" on page 4

"Restoring the Network IPS appliance to factory defaults" on page 4

"Enabling FIPS mode options" on page 5

FIPS considerations for Network IPS appliances

This topic lists important issues to consider before you enable FIPS mode on your Network IPS appliance.

Supported options

- Use firmware that you know to be FIPS certified for FIPS compliance.

  For specific information about IBM Security products that are FIPS certified, consult the IBM Security FIPS 140 Security Policy documents. Find these documents on the National Institute of Standards and Technology (NIST) web site, in the Module Validation Lists section: http://csrc.nist.gov/groups/STM/cmvp/index.html.
- You must enable FIPS mode during initial setup. You have no other options than to enable FIPS during initial setup.
- You must enable FIPS mode on a new installation of Network IPS or on an installation that you restored to factory default **(unconfigured)** settings.
- You can update the Security Content in the Protocol Analysis Module (PAM). However, other updates and patches might not be FIPS-compliant.
- You must use the cryptographic hash function SHA-1 in your symmetric key content in the NTP policy.
- You must use SHA-1 as the message digest algorithm and you must use DSA-SHA-1 as the encryption scheme in your autokey configurations in the NTP policy.

Options that are not supported

- It is not possible to migrate Network IPS policies after enabling FIPS mode.
- It is not possible to use the LCD (the display on the appliance) for initial setup. You must use one of the processes in "Enabling FIPS mode options" on page 5 for initial setup.
- Do not install Escalations Management Group (EMG) patches unless you know that they are FIPS certified.
- It is not possible to disable FIPS mode through IPS Local Management Interface. You must reimage the appliance and perform the initial setup without enabling FIPS mode.
- Do not select MD5 or DES when configuring SNMP responses because these options are not FIPS-compliant. If these options are chosen while in FIPS mode, the appliance does not execute the response and it creates an error message in the system log. The error message states that the response is invalid.
- Do not select Radius authentication when configuring remote authentication because the Radius protocol uses MD5 hashes. The use of MD5 hashes is not FIPS-compliant.
- Do not use MD5 hashes in the symmetric key content in the NTP policy.

Other considerations

- There is no advantage to enable FIPS mode if you do not need to be FIPS-compliant or if your firmware is not FIPS certified.
- If you manage FIPS enabled Network IPS appliances with the SiteProtector System, ensure SiteProtector is FIPS enabled, as well.
- Back up a working version of FIPS mode in case your Network IPS appliance enters a FIPS error state. See "Backing up a working FIPS mode version" on page 9.

Restoring the Network IPS appliance to factory defaults

This topic explains the option of restoring an appliance to factory defaults to enable FIPS mode. Use this option if an appliance is already in use and not in FIPS mode. If the appliance is new and has not been initially configured, this step is unnecessary.

Procedure

1. Log on to the appliance as `admin` by using a serial communication session or an SSH communication session.

   Note: See "Enabling FIPS mode by using a serial communication session" for possible settings.
2. From the Configuration Menu, select **Appliance Management**.
3. Select **Restore to Factory Default (unconfigured)**.

   Note: The **unconfigured** option is the only way to restore your appliance to enable FIPS mode. If you choose **configured**, you do not have the option to enable FIPS mode.

Enabling FIPS mode options

Use IPS Setup to enable FIPS mode on the Network IPS appliance if the appliance is new or has not been initially configured.

You can only enable FIPS mode during initial setup. If you decide to enable FIPS mode later, you must reinstall the Network IPS firmware or perform a restore to factory defaults (unconfigured).

If you need instructions on how to install firmware, see the applicable installation guide on the IBM Security Product Information Center, in the IBM Security Network Intrusion Prevention System (IPS) section, at http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp.

When enabled, IPS Local Management Interface displays the message `FIPS Mode: Enabled`.

Enabling FIPS mode by using a serial communication session

Use this option if the firmware is older than version 4.1.

Procedure

1. Connect to the appliance by using a serial console cable and a computer.
2. Connect to the appliance by using Hyperterminal or another terminal emulation program. Follow the instructions listed in the documentation for the program you choose.
3. Create connection by using the following settings.

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

4. Press **ENTER** to establish a connection. When the connection is established, you see the login screen.
5. At the unconfigured login prompt, log on to the appliance with the user name and password `admin/admin`.
6. Select **Start** and then press **ENTER**.
7. Enable **FIPS mode**.

   Note: When you enable FIPS mode, the appliance shuts down and restarts, immediately.

8. At the unconfigured login prompt, log on to the appliance with the user name and password `admin/admin`.
9. Follow the on-screen instructions to enable FIPS mode.

Enabling FIPS mode by using web-based set up

Use this option for firmware versions 4.1 and newer. However, if you want, you can use a serial communication session.

About this task

To perform this task, use zero configuration networking to access the web-based version of IPS Setup.

Note: For detailed information, see the Installation Guide, Chapter 2. "Configuring network settings for the Network IPS system," located on the IBM Security Product Information Center at http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp, in the IBM Security Network IPS section.

This task requires the Bonjour plug-in for Windows.

Procedure

1. Connect a Windows computer directly to the Network IPS system by using an Ethernet crossover cable or connect a computer to the same network switch as the Network IPS system. The unconfigured system initially obtains 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.
2. Download the Bonjour SDK for Windows Version 2.0, which includes web browser plug-ins for Internet Explorer and Mozilla Firefox.
3. Install the plug-in on the Windows computer connected to the Network IPS system.
4. Open the web browser and look for the Bonjour icon in the toolbar.

   Note: If you do not see the Bonjour icon in the toolbar, you must reinstall Bonjour.
5. Click the Bonjour icon to display a window that lists the Bonjour services that are available on the network.
6. From the Bonjour menu, select the Network IPS system you want to configure. The Network IPS name is displayed as "IBM Security <MODEL>-<SERVICE>[ID#]"
7. At the unconfigured login prompt, type the following login credentials, and then press Enter
   - User name = `admin`
   - Password = `admin`
8. In the Welcome section of IPS Setup, follow the instructions to enable FIPS mode.

Chapter 3. Network IPS and the FIPS error state

This chapter lists the actions the Network IPS appliance takes when in an error state, it lists symptoms of an error state, and it gives tips for troubleshooting. This chapter also explains how to back up a working version of FIPS mode, how to restore an earlier working version of FIPS mode, and how to recover from a FIPS error state.

FIPS error state and Network IPS appliance actions

When an appliance is in a FIPS error state, it takes the following actions:

- Shuts down SSH (Secure Shell protocol), web services, and IPS services
- Deletes cryptographic keys from appliance memory
- Unregisters with SiteProtector, if applicable
- Shuts down and restarts
- Runs in hardware bypass mode, if available

Symptoms

Notice the following symptoms when the Network IPS appliance enters an error state.

- You cannot use the SSH protocol to communicate with the appliance
- You cannot log on to the appliance LMI
- If you use SiteProtector to manage the appliance, SiteProtector reports that the appliance is unmanaged or inactive
- The appliance stops inspecting traffic
- The appliance passes all traffic

Confirming an error state

This topic explains how to confirm the Network IPS appliance is in a FIPS error state.

Procedure

1. Connect to the appliance by using the settings from “Enabling FIPS mode by using a serial communication session” on page 5.
2. At the unconfigured login prompt, log on to the appliance by using the `admin` credentials.
3. From the Configuration Menu, select **FIPS-140 Information**. This option states if the appliance is in an error state or not.

Troubleshooting a FIPS error state with the syslog

This topic lists several causes of a FIPS error state and explains how to view the syslog to research possible causes on the Network IPS appliance.

About this task

Many situations can cause a FIPS error state including the following options:

- Someone modifying a check-summed file on the appliance might trigger the FIPS error state. If the appliance is running firmware version 4.1 or older, restore the unmodified version of the check-summed file before restoring from backup to an earlier FIPS version or before using the **FIPS-140 Information** option.
- Someone installing an EMG patch that is not FIPS certified can cause an error state.
- Failure of boot time integrity checks can cause an error state.

Procedure

1. Connect to the appliance using information from“Enabling FIPS mode by using a serial communication session” on page 5.
2. At the unconfigured login prompt, log on to the appliance by using the `root` credentials.
3. Go to `/var/log/messages file` to view the syslog for possible causes of the FIPS error state.

Backup and restore options

Back up a working FIPS version so you can use it to recover from an error state. Another recovery option is to use the **FIPS-140 Information** > **Retry FIPS Mode** option, only if the appliance is running firmware version 4.1 or older. A last resort for recovering from an error state is to reimage the appliance.

If you need instructions on how to install firmware, see the applicable installation guide on the IBM Security Product Information Center, in the IBM Security Network Intrusion Prevention System (IPS) section, at http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp.

When you back up the firmware, the appliance saves a copy to the backup partition. However, some versions of Network IPS firmware when reinstalled, repartition the hard disk drives. To ensure that the backup copy is not lost, move the files off the appliance to a safe, convenient place on your network.

In order to restore from backup, ensure that the appliance firmware and the backup are the same firmware version.

Backing up a working FIPS mode version

Procedure

1. Log on to the appliance as `admin` by using a serial communication session or an SSH communication session.

   Note: See “Enabling FIPS mode by using a serial communication session” on page 5 for settings.
2. From the Configuration Menu, select **Appliance Management**.
3. Select **Backup Current Configuration**.
4. Select **OK**. The appliance might be offline for several minutes while it completes the restart.
5. As a best practice, when the appliance comes back online, copy files from `/restore/0/images` to a designated place off the appliance.

Restoring FIPS mode from backup

Procedure

1. Connect to the appliance using information from “Enabling FIPS mode by using a serial communication session” on page 5.

   Note: SSH, web services, and IPS services are shut down when the appliance is in the FIPS error state.
2. At the login prompt, log on to the appliance using the `admin` credentials.
3. From the Configuration Menu, select **Appliance Management**.
4. Select **Restore Configuration From Backup** and then follow the prompts.

   Note: The appliance might be offline for several minutes while it completes the restart.

Recovering from a FIPS error state by using the FIPS-140 Information option

About this task

This option is not available for Network IPS firmware versions 4.2 and newer.

Procedure

1. Connect to the appliance using information from “Enabling FIPS mode by using a serial communication session” on page 5.

   Note: SSH, web services, and IPS services are shut down when the appliance is in the FIPS error state.
2. At the login prompt, log on to the appliance using the `admin` credentials.
3. From the Configuration Menu, select **FIPS-140 Information**.
4. Select **Retry FIPS Mode**.
5. If you use SiteProtector to manage your Network IPS appliance, you must register with SiteProtector again. For detailed information about how to register with SiteProtector, see the Help or the User Guide located on the IBM Security Product Information Center, in the IBM Network Security Intrusion Prevention System (IPS) section, at http://publib.boulder.ibm.com/infocenter/sprotect/v2r8m0/index.jsp.

Chapter 4. SiteProtector FIPS Service

This chapter explains how to configure the SiteProtector FIPS Service in FIPS-approved mode.

Topics

About the SiteProtector FIPS Service

The SiteProtector FIPS Service enables the SiteProtector application to encrypt a management session to a managed FIPS-enabled agent.

About SiteProtector

SiteProtector is a centralized management system that unifies management and analysis for network, server, and desktop protection agents and small networks or appliances. SiteProtector is used as the central controlling point for IBM ISS appliances deployed on the network.

SiteProtector performs the following functions:

- Manages and monitors agents and SiteProtector subcomponents
- Enables an Administrator to view configuration data for a GX series appliance
- Displays audit and system data records
- Monitors the network connection between SiteProtector and the agents it is configured to monitor

How the SiteProtector FIPS Service works

The SiteProtector FIPS Service provides cryptographic services to the SiteProtector application.

The SiteProtector FIPS Service is a uniquely identifiable library that is linked into the SiteProtector application. All operations of the SiteProtector FIPS Service occur by way of calls from the SiteProtector application, but only when an operator has successfully authenticated to the host operating system.

The SiteProtector FIPS Service does not receive calls from untrusted services or daemons.

Supported roles, services, and authentication

The SiteProtector FIPS Service supports a Crypto Officer and a User role. It does not support a Maintenance role.

The Crypto Officer (a person) initializes and configures the SiteProtector FIPS Service. The User role (the SiteProtector application) can only access the SiteProtector FIPS Service.

Configuring the SiteProtector FIPS Service for FIPS-approved mode of operation in SiteProtector

With the SiteProtector FIPS Service, you can only use a SiteProtector system configured to manage FIPS-enabled agents. Follow these requirements while operating the SiteProtector FIPS Service.

SiteProtector FIPS Service installation requirements

SiteProtector FIPS Service Installer package

You should install the SiteProtector FIPS Service Installer over a new express install of SiteProtector Version 2.0 Service Pack 8.0. The SiteProtector Version 2.0 Service Pack 8.0 Express® Installer and SiteProtector FIPS Service Installer are available from the IBM Download Center.

OS requirements

The operating system (Windows Server 2003 R2 Standard, Version 5.2 SP2) you use must meet installation and configuration requirements specified in the Common Criteria Security Target for the operating system (http://www.commoncriteriaportal.org/files/epfiles/20080303_st_vid10184-st.pdf). The operating system should also be configured to lock an account after 5 failed authentication attempts.

SiteProtector Updates

Do not update any SiteProtector component unless that component is listed in this document. However, you can still update SiteProtector Database XPUs. To prevent the Update Server from automatically installing product updates, you must disable the **Automatically install updates** option in the XPU Settings policy for the Update Server.

Before you apply the SiteProtector FIPS Service Installer package, you will need to update the SiteProtector Database to Service Pack 8.2. Do not install beyond Service Pack 8.2.

To install the Service Packs one at a time:

1. Right-click on the SP Core, and then select **Properties**.
2. Click **Agent Properties**, and then click **Edit Agent Properties**.
3. Click the **X-Press and Product Update** tab, and then click the **Advanced** button.
4. Select the **Single (Apply updates one at a time)** option, and then click **OK**.

Security requirements for secure communication

To meet the cryptographic security requirements for secure communication, you must follow certain restrictions when you install and use SiteProtector.

The steps below will ensure that the SiteProtector FIPS Service implements required self-tests and uses only approved algorithms.

1. The Express Install package is the only package that is supported. Other install options are not valid. You cannot upgrade from a previous version of SiteProtector and then enable the SiteProtector FIPS Service. You must use the SiteProtector FIPS Service with a new SiteProtector 2.0 Service Pack 8 Express Install.
2. All SiteProtector components must be installed on a single hardware/OS platform. However, you can install and use the management console remotely.
3. The XPU Settings policy for the Update Server must be modified to disable the install of automatic product updates.
4. Do not install the optional Event Archiver package.

SiteProtector FIPS Service initialization requirements

In order to operate in FIPS-approved mode of operation, the Crypto Officer should verify that the software version of the SiteProtector FIPS Service is SiteProtector Version 2.0 Service Pack 8.0.

Additional rules for using the SiteProtector FIPS Service

All host system components that contain sensitive cryptographic data (main memory, system bus, disk storage) must be located in a secure environment.

The writable memory areas of the SiteProtector FIPS Service (data and stack segments) are accessible only by the SiteProtector application so that the module is in "single user" mode, meaning only the SiteProtector application has access to that instance of the module.

The operating system is responsible for multitasking operations so that other processes cannot access the address space of the process containing the module.

The User must configure and enforce the following initialization procedure in order to operate in FIPS-approved mode of operation:

- The end user of the operating system is responsible for zeroizing Critical Security Parameters (CSP) with wipe/secure delete procedures.

Appendix. 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)

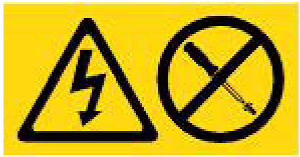
CAUTION:
The weight of this part or unit is between 18 and 32 kg (39.7 and 70.5 lb). It takes two persons to safely lift this part or unit. (C009)

Product safety labels

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

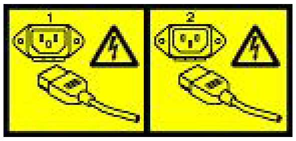
DANGER

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, disconnect 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)

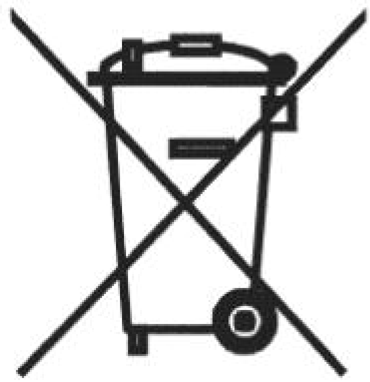
Laser compliance

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.

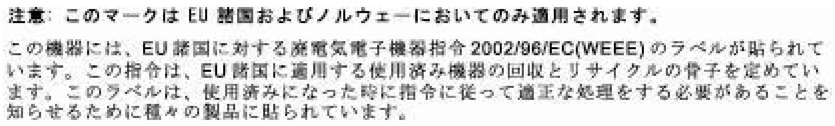
Esta unidad debe reciclarse o desecharse de acuerdo con lo establecido en la normativa nacional o local aplicable. IBM recomienda a los propietarios de equipos de tecnología de la información (TI) que reciclen responsablemente sus equipos cuando éstos ya no les sean útiles. IBM dispone de una serie de 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.

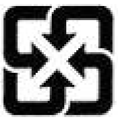
L'etiquette du système respecte la Directive européenne 2002/96/EC en matière de Déchets des Equipements Electriques et Electroniques (DEEE), qui détermine les dispositions de retour et de recyclage applicables aux systèmes utilisés à travers l'Union européenne. Conformément à la directive, ladite étiquette 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:



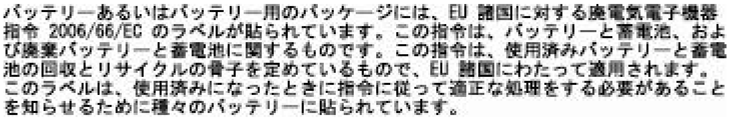
Please recycle batteries 廢電池請回收

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.

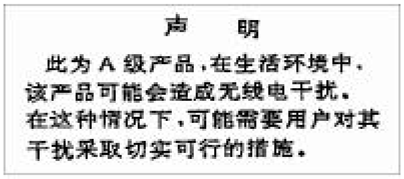
Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:

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.

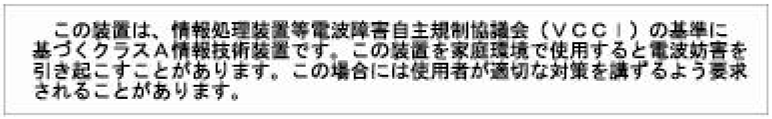


声　明

此为Ａ级产品，在生活环境中，
该产品可能会造成无线电干扰。
在这种情况下，可能需要用户对其
干扰采取切实可行的措施。

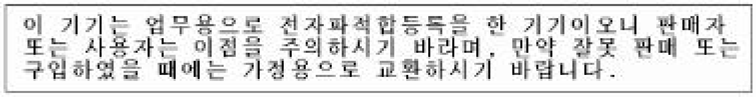
Japan Class A Compliance Statement:

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.



この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に
基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を
引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求
されることがあります。

Korean Class A Compliance Statement:



이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자
또는 사용자는 이점을 주의하시기 바라며, 만약 잘못 판매 또는
구입하였을 때에는 가정용으로 교환하시기 바랍니다.

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.

Other company, product, or service names may be trademarks or service marks of others.

Index

Printed in USA