IBM FlashSystem 810

User's Guide

IBM

Revision 3, 4/2014

IBM FlashSystem 810

User's Guide

Revision 3, 4/2014

Note

Before using this information and the product it supports, read the information in “Safety notices” on page v, “Notices” on page 23, the *IBM Systems Safety Notices* manual, G229-9054, and the *IBM Environmental Notices and User Guide*, Z125–5823.

This edition applies to IBM FlashSystem and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Safety notices

Safety notices may be printed throughout this guide:

- **DANGER** notices call attention to a situation that is potentially lethal or extremely hazardous to people.
- **CAUTION** notices call attention to a situation that is potentially hazardous to people because of some existing condition.
- **Attention** notices call attention to the possibility of damage to a program, device, system, or data.

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, safety information documentation is included in the publications package (such as in printed documentation, on DVD, or as part of the product) shipped with the product. The documentation contains the safety information in your national language with references to the U.S. English source. Before using a U.S. English publication to install, operate, or service this product, you must first become familiar with the related safety information documentation. You should also refer to the safety information documentation any time you do not clearly understand any safety information in the U.S. English publications.

Replacement or additional copies of safety information documentation can be obtained by calling the IBM Hotline at 1-800-300-8751.

German safety information

Das Produkt ist nicht für den Einsatz an Bildschirmarbeitsplätzen im Sinne § 2 der Bildschirmarbeitsverordnung geeignet.

Laser safety information

IBM® servers can use I/O cards or features that are fiber-optic based and that utilize lasers or LEDs.

Laser compliance

IBM servers may be installed inside or outside of an IT equipment rack.

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 provided power cord. Do not use the IBM 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)

DANGER

Observe the following precautions when working on or around your IT rack system:

- **Heavy equipment–personal injury or equipment damage might result if mishandled.**
- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.**
- **Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices.**

- **Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet when directed to disconnect power during servicing.**
- **Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.**
- **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.**

CAUTION

- **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 of 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 out 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)

CAUTION:
Removing components from the upper positions in the rack cabinet improves rack stability during relocation. Follow these general guidelines whenever you relocate a populated rack cabinet within a room or building:

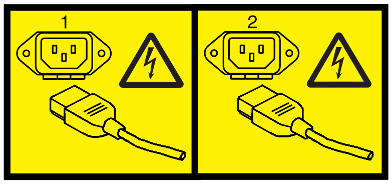
- **Reduce the weight of the rack cabinet by removing equipment starting at the top of the rack cabinet. When possible, restore the rack cabinet to the configuration of the rack cabinet as you received it. If this configuration is not known, you must observe the following precautions:**
  - **Remove all devices in the 32U position and above.**
  - **Ensure that the heaviest devices are installed in the bottom of the rack cabinet.**
  - **Ensure that there are no empty U-levels between devices installed in the rack cabinet below the 32U level.**
- **If the rack cabinet you are relocating is part of a suite of rack cabinets, detach the rack cabinet from the suite.**
- **Inspect the route that you plan to take to eliminate potential hazards.**
- **Verify that the route that you choose can support the weight of the loaded rack cabinet. Refer to the documentation that comes with your rack cabinet for the weight of a loaded rack cabinet.**
- **Verify that all door openings are at least 760 x 230 mm (30 x 80 in.).**
- **Ensure that all devices, shelves, drawers, doors, and cables are secure.**
- **Ensure that the four leveling pads are raised to their highest position.**
- **Ensure that there is no stabilizer bracket installed on the rack cabinet during movement.**
- **Do not use a ramp inclined at more than 10 degrees.**
- **When the rack cabinet is in the new location, complete the following steps:**
  - **Lower the four leveling pads.**
  - **Install stabilizer brackets on the rack cabinet.**
  - **If you removed any devices from the rack cabinet, repopulate the rack cabinet from the lowest position to the highest position.**
- **If a long-distance relocation is required, restore the rack cabinet to the configuration of the rack cabinet as you received it. Pack the rack cabinet in the original packaging material, or equivalent. Also lower the leveling pads to raise the casters off of the pallet and bolt the rack cabinet to the pallet.**

(R002)

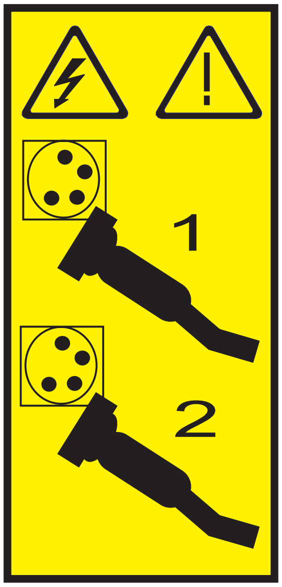
(L001)

(L002)

(L003)



or



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.

CAUTION:
This product might 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)

CAUTION:
This product contains a Class 1M laser. Do not view directly with optical instruments. (C028)

CAUTION:
Some laser products contain an embedded Class 3A or Class 3B laser diode. Note the following information: laser radiation when open. Do not stare into the beam, do not view directly with optical instruments, and avoid direct exposure to the beam. (C030)

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

Power and cabling information for NEBS (Network Equipment-Building System) GR-1089-CORE

The following comments apply to the IBM servers that have been designated as conforming to NEBS (Network Equipment-Building System) GR-1089-CORE:

The equipment is suitable for installation in the following:
- Network telecommunications facilities
- Locations where the NEC (National Electrical Code) applies

The intrabuilding ports of this equipment are suitable for connection to intrabuilding or unexposed wiring or cabling only. The intrabuilding ports of this equipment *must not* be metallically connected to the interfaces that connect to the OSP (outside plant) or its wiring. These interfaces are designed for use as intrabuilding interfaces only (Type 2 or Type 4 ports as described in GR-1089-CORE) and require isolation from the exposed OSP cabling. The addition of primary protectors is not sufficient protection to connect these interfaces metallically to OSP wiring.

Note: All Ethernet cables must be shielded and grounded at both ends.

The ac-powered system does not require the use of an external surge protection device (SPD).

The dc-powered system employs an isolated DC return (DC-I) design. The DC battery return terminal *shall not* be connected to the chassis or frame ground.

IBM FlashSystem 810 User's Guide

Learn about setting up, configuring, and managing the IBM FlashSystem™ 810.

Introduction

Use this information to learn about the IBM FlashSystem and its features.

System components

The IBM FlashSystem components include data storage capacity, controller slots, a front panel display for configuration, and Ethernet capacities.

The system components of the IBM FlashSystem 810 include the following features:
- Up to 10 TB of usable data storage capacity
- Two controller slots that can contain a mixture of dual-ported 8 Gb Fibre Channel (FC) or Quad Data Rate (QDR) InfiniBand controllers
- A front panel display for configuration and monitoring
- An Ethernet monitoring port

Power requirements

A fully configured IBM FlashSystem 810 requires approximately 250 watts of power.

The system includes two hot-swappable power modules that are auto-ranging (they accept either 110 V ac or 220 V ac).

Reliability functions

The storage system is designed to offer high reliability.

The storage system's standard functions include modular flash memory, fully redundant, hot-swappable power supplies, external alerts by using Simple Network Management Protocol (SNMP), and redundant data paths.

System management functions

Basic management operations, including manual shutdown and alerts, are available from the front panel screen.

Full monitoring and configuration capabilities are available over any browser by a password-protected Java™ applet, and through a command-line interface over Telnet or Secure Shell (SSH). The system is fully SNMP v2c-compatible and can provide notification of system events though email.

Reviewing your shipment

Reviewing your shipment is an important first step in ensuring an accurate order.

Unpacking

Refer to the packing list when you unpack your system.

Your system is supplied with a packing list. Ensure that you received all of the components listed.

1. Examine the external chassis for any damage that might have occurred during shipping.

2. Inspect the interface plate for any screws that might have loosened during shipping.
3. Inspect the front panel display for damage.
4. Report any meaningful damage.

Rack mounting

The storage system is provided with the slides and hardware that is needed to install it into a standard 19-inch rack, in a 1U space.

See the rack installation documentation that is supplied with the rack kit for details on installing the storage system in a rack.

DANGER

Observe the following precautions when working on or around your IT rack system:

- **Heavy equipment–personal injury or equipment damage might result if mishandled.**
- **Always lower the leveling pads on the rack cabinet.**
- **Always install stabilizer brackets on the rack cabinet.**
- **To avoid hazardous conditions due to uneven mechanical loading, always install the heaviest devices in the bottom of the rack cabinet. Always install servers and optional devices starting from the bottom of the rack cabinet.**
- **Rack-mounted devices are not to be used as shelves or work spaces. Do not place objects on top of rack-mounted devices.**
- **Each rack cabinet might have more than one power cord. Be sure to disconnect all power cords in the rack cabinet when directed to disconnect power during servicing.**
- **Connect all devices installed in a rack cabinet to power devices installed in the same rack cabinet. Do not plug a power cord from a device installed in one rack cabinet into a power device installed in a different rack cabinet.**
- **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.**

CAUTION

- **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 of 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 out 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)

System connections

You must install a host bus adapter or host channel adapter in the host system.

Installing a host bus adapter or host channel adapter in the host system

Host bus adapters (HBAs) provide an interface from the host system's PCI bus to Fibre Channel-attached devices. Host channel adapters (HCAs) provide an interface from the server's PCI bus to InfiniBand devices.

Ensure that the adapter that you select for use with the storage system provides a driver for the operating system version that you are using.

Note: In subsequent sections, the term HBA is used to represent HCA or HBA interchangeably.

Before you install the HBA, consult your server documentation to determine which one of its PCI slots is on the fastest and least congested PCI bus. Follow the instructions that are provided with the HBA to install the card and driver. Obtain the latest drivers and firmware for the HBA. Updated drivers might include new functions, improved performance, and minor bug fixes.

The speed of the server and network interface ultimately determine the storage system's capabilities. Some components that can affect the maximum performance of the storage system include FC or InfiniBand interfaces, host bus adapters, PCI buses, and server processor resources.

Fibre Channel interface bandwidth

Your storage system supports Fibre Channel (FC) communication speeds of 2 Gbps, 4 Gbps, or 8 Gbps.

Accounting for encoding and overhead, the maximum 8 Gbps transfer rate allows data to be transmitted to the system at a half duplex rate of approximately 800 MBps. Fibre Channel interfaces have separate read and write connections that allow a maximum data rate of twice the half-duplex rate. To sustain the maximum full duplex rate, the data usage pattern of the system must be 50% read and 50% write. This requirement is because of the individual half duplex limits. To find the maximum for other data usage patterns, use the following formula (given an 8 Gb HBA):

[(smaller usage percentage/larger percentage) × 800 MBps] + 800 MBps

For example, to calculate a data usage pattern with 66% reads and 33% writes,

[(33/66) × 800] + 800 = 1200 MBps

Many applications require storage bandwidth that exceeds what a single FC connection can provide. To accommodate this situation, up to 4 FC ports are available per system, each of which can supply the bandwidth described here. Using multiple FC connections requires one of the following solutions: multipathing software to a single logical unit, using software to stripe across multiple logical units, accessing multiple logical units concurrently, or connecting multiple servers to the storage system.

Host bus adapter settings

You can modify some host bus adapter (HBA) settings to increase performance.

For information specific to your HBA, consult the HBA documentation. Many settings are intended to increase the performance of slow storage devices and are not applicable to this high performance system.

In particular, it is always advisable to check the frame size. The amount of overhead for each Fibre Channel frame is fixed, so larger frames have lower overhead. Set the frame size to the maximum setting, generally 2048 bytes. For InfiniBand devices, also set the frame size to the maximum setting, generally 4096 bytes.

PCI bus selection and performance

High-bandwidth host bus adapter (HBA) traffic can quickly inundate slower PCI buses. When a PCI bus reaches its limit, you can do little to improve performance.

Many servers, however, provide different PCI buses with different speeds, and placing the HBA on a faster PCI bus can improve performance. When you install an 8 Gb, 2-port HBA in the server, allocate at least an entire PCI-X bus or a PCI Express (PCIe) slot.

Processor performance factors

At a certain point, processor performance can limit data transfer rates. Determine whether the server's processor resources are the limiting factor in performance while you benchmark the storage system as a raw physical device.

Otherwise, an improperly tuned file system or application can make the processor seem to be the limiting factor when it is not. Complete raw device testing after you set up any multipathing.

There are a few ways to decrease processor usage without increasing processor resources. Certain data usage patterns can be processor-intensive and fully use the processor. These usually involve small transfer sizes. When possible, increasing the average transfer size decreases processor usage and offers better performance.

Another way to decrease processor usage is by enabling interrupt coalescing. Interrupt coalescing is an HBA-dependent function that decreases processor usage at the expense of latency. This function delays the calling of the HBA transfer interrupt until several transfers are ready. However, in general, do not enable *interrupt coalescing* because the storage system performance benefits from low latency. For more information, see your HBA documentation.

Connecting the Fibre Channel or InfiniBand ports

Connect the Fibre Channel (FC) ports on the storage system to your server or to an FC switch. If your storage system has InfiniBand ports, connect them to an InfiniBand switch or host channel adapter (HCA) in your server.

The following figure shows the port layout for the storage system. Each controller has two FC ports: A and B, on the left and right respectively. The FC ports on the system can connect to Point-to-Point (N-Port), Arbitrated Loop (NL-port), or Switched Fabric (F-Port) topologies at 2 Gb, 4 Gb, or 8 Gb speeds.

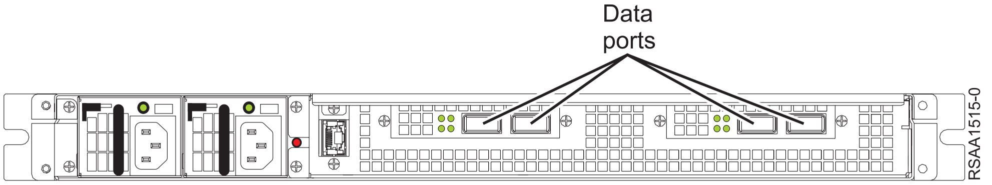


Figure 1. Fibre Channel or InfiniBand port locations

Although Figure 1 shows FC controller cards, an InfiniBand controller card can occupy either of the same slots as the FC controller cards. The InfiniBand controller card has two x4 InfiniBand ports: A and B, on the top and bottom respectively. The InfiniBand ports can connect to Quad Data Rate (QDR), Double Data Rate (DDR), or Single Data Rate (SDR) HCAs. This connection uses the Small Computer System Interface (SCSI) remote direct memory access (RDMA) Protocol (SRP).

- On an FC controller card, the FC port LED is green if the speed is set to 8 Gb. If the speed is set to 4 Gb, the LED for the FC port is amber.
- On an InfiniBand controller card, the port LED is green when the link is established.

Connecting the system to a management network

Your system includes a Gigabit Ethernet management controller port (MCP) connection for remote management over a network.

You use this connection to configure the system's storage and management functions.

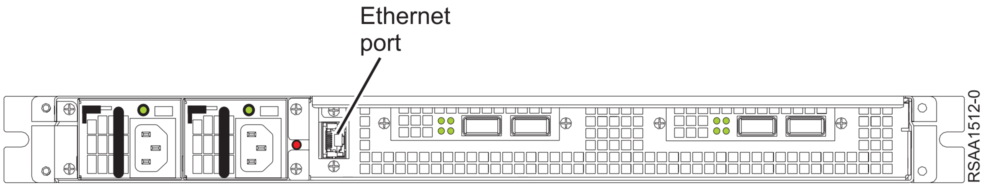


Figure 2. Ethernet management port location

Connect the Ethernet MCP to the network.

Connecting power to the system

Although the system operates when only one power supply is connected, this set up is not recommended.

Using the ac power cords that are provided, connect each power supply to a power source. As a best practice, connect each of the power cords to separate circuits.

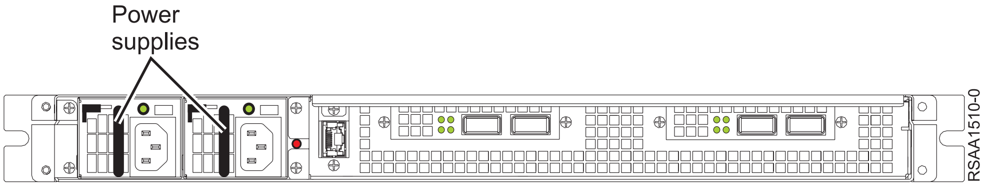


Figure 3. Power supplies

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 provided power cord. Do not use the IBM 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)

Getting started

There are several tasks that you can perform to set up your initial configuration.

To initially configure your new storage system, complete the following tasks:

- Use the front panel display to set up the network (see **** MISSING FILE ****).
- Set up the web management interface (see “Web interface basics” on page 12).
- Use the web interface to set the date and time (see “Setting the date and time by using the web interface” on page 13).
- Use the web interface to configure advanced network settings (see **** MISSING FILE ****.
- Use the web interface to configure security (see “Managing security with the web interface” on page 13).

System initialization

When ac power is connected, the storage system powers-up and the front panel display shows the power-on sequence.

When the system is fully ready, the front panel displays `Status: OK` and the system performance statistics, including the system bandwidth in Mbps and total input/output operations per second.

Front panel display overview

The front panel display provides a quick and easy way to view the status of the storage system.

The following figure shows the front panel display and selection buttons.

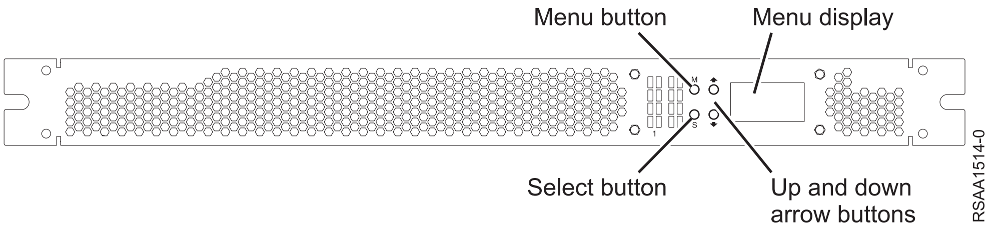


Figure 4. Front panel display and selection buttons

Use this display to complete the following tasks:

- Inspect the state of the system.
- Change the method of IP address assignment.
- Restart or shut down the system.

The following buttons are located to the left of the display and are used to make selections:

(M)enu
This button has two functions. On any of the status or performance displays, pressing this button starts the **Main Menu**. This button is also used as an escape function. When the menu system is open, pressing it returns to the prior screen.

(S)elect
When a menu item is displayed, pressing this button will either run that menu option or proceed to the next level in the menu.

↑
This button scrolls up through the menu. It is also used to cancel certain commands as indicated on the display. If the menu is not selected, this button is disabled.

↓
This button scrolls down through the menu. It is also used to confirm certain commands as indicated on the display. If the menu is not selected, this button is disabled.

To scan through the first level of options, press the Menu key.

- Selecting **System Info** displays status information.
- Selecting **System Status** displays messages. You can view the system informational, warning, or error messages. These messages are the same messages that scroll across the status screen.
- Selecting **Net Config** to configure the connection to your network. For more information, see **** MISSING FILE ****.
- Selecting **LED Config** gives you various options for controlling the LEDs to the left of the display.
- Selecting **Restart** restarts the storage system.
- Selecting **Poweroff** turns off the storage system. For more information, see “Powering off the system” on page 9.

Controlling system power with the front panel display

The storage system has functions that allow the administrator to safely power down the system.

Before you power down the system, unmount the drives from your operating system. Do not turn off the system by unplugging the power cords.

Powering off the system

You can use the front panel to shut down your storage system.

About this task

To shut down the storage system by using the front panel, complete the following steps:

Procedure

1. Use the arrow buttons to cycle through the top-level menu and select **Poweroff**, and then press the **Select** button.
2. Press the **Select** button to confirm the system shutdown.
3. The front panel display indicates that the system is powering down. When the system is ready, it automatically shuts off.

Results

To turn the system back on after manual shutdown, press the power button on the system back panel, to the right of the power supplies.

Restarting the system

You can restart the system manually by using the front panel.

About this task

To restart the system manually by using the front panel, complete the following steps:

Procedure

1. Use the arrow buttons to cycle through the top-level menu to select **Restart**. Use the **Select** button to select this menu item
2. When prompted, use the ↓ button to confirm. The front panel display indicates that the system is powering off. It automatically shuts off, then in approximately 9-seconds time, the system turns back on.

Automatic shutdown

The automatic shutdown function can prevent overheating and loss of power.

When the system senses a high system temperature, power out of range, or various other environmental conditions, the system automatically initiates the shutdown procedure.

Configuring the management controller port using the front panel display

The storage system supports system monitoring and configuration through the installed Ethernet management controller port (MCP).

About this task

You must provide the MCP with an IP address, a subnet mask, and a gateway address if used in your network. There are three possible IP address settings: Static IP, DHCP, or No Ethernet. The default factory setting is DHCP. For any questions that you have regarding IP assignment values, consult your network administrator.

To set up the network by using the front panel, complete the following steps:

Procedure

1. Use the arrow buttons to cycle through the top-level menu options until the display shows **Net Config**.
2. Use the **Select** button to choose this option and continue with the configuration. If your storage system has multiple management controllers installed, select the management controller you would like to configure.

Results

You can now use the arrow buttons to scroll through the following menu options:

Show Current
Displays the current IP configuration, host name, IP Config address, subnet mask, gateway address (if applicable), and hardware MAC address for the management controller port.

Eth0 Config
Configures the Eth0 Ethernet port.

Restart Net
Shuts down and restarts the Ethernet port by using the current IP assignment configuration.

Exit menu
Exits the network menu.

To continue setting up the Ethernet configuration select **Eth0 Config**, and then use the arrow buttons to cycle through the following IP configuration options:

Static Enables static IP addresses

DHCP
Sets the IP configuration to DHCP

None Disables Ethernet

Exit Returns to the Main Menu without changes

Consult your network administrator for the correct IP assignment type. Use the **Select** button to select the wanted method of IP assignment. If you choose the **Eth0 Config**, **DHCP** or **None** option, you must confirm the selection with the ↓ button.

Configuring a static IP address

If you configure the system with a static IP address, you must provide the IP address, subnet mask, and possibly a gateway address.

About this task

To configure the address, complete the following steps:

Procedure

1. After you choose the **Static IP** option, you are prompted to enter an address. Use the ↑ and ↓ buttons to move the cursor. Press Select to cycle through the numbers 0 through 9. You can cancel your current changes at anytime by pressing the **Menu** button and following the dialog.
2. After you finish entering the IP address, scroll the cursor off the end of the address. This action brings up the **Subnet Mask** screen.
3. Using the same procedure as entering the IP address, enter the subnet mask.

4. The final value that you must enter is the Ethernet gateway. If the system is on a private network and this value is not needed, enter `0.0.0.0` on the next screen and then press any key to dismiss this message. Otherwise, enter the gateway IP address.
5. After you enter all the necessary values, you can review them, apply, edit, or cancel your changes through the Review Configuration pane.
6. To apply your changes, select the **Apply new settings** option. The changes are then applied and the network is automatically restarted. The final pane displays the assigned IP address.

Results

Note: Because you established a static IP address rather than using DHCP, there is no automatic discovery of the network DNS server. To enter your network's DNS server information, you can use the web management interface. The DNS settings are configured using the Network node in the system tree.

Configuring DHCP

Your storage system is pre-configured to use DHCP as its IP address method. To configure your DHCP server, you must know the hardware MAC address of the storage system.

About this task

To obtain the MAC address and to configure your system to use DHCP, complete the following steps:

Procedure

1. From the **Net Config** submenu, select the **Show Current** option. This option displays the information for the management controller.
2. Use the ↓ button to scroll to the section that displays the information for the wanted Ethernet device. The MAC address is shown at the bottom and is displayed as six octets, such as `a2:78:90:f7:01:88`. Use this value to configure your DHCP server.
3. On the front panel display, choose **Eth0 Config** and select **DHCP**.
4. On the next pane, use the ↓ to confirm the setting. The system restarts automatically. The final screen displays the IP address that is assigned by the DHCP server.

Results

If the network fails to start, check the Ethernet connection and contact your system administrator. If the IP configuration was successfully saved, select the **Restart Net** option from the management controller menu instead of reselecting the same IP configuration.

Additional system management options

After you set up the basic system management options, you can use these additional functions. The functions include connecting by using Telnet and Secure Shell (SSH), monitoring your system with Simple Network Management Protocol (SNMP), and other advanced options.

Connecting by using Telnet and SSH

When you configure the Ethernet port on the storage system, you can remotely monitor the system by using a Telnet or SSH session.

Set your terminal settings to VT100 mode.

Connecting by using the web management interface

The storage system is equipped with a browser-enabled tool to facilitate system monitoring, management, and configuration.

This monitoring application is based on Java. A separate document, the *Web Interface Guide*, provides expanded information about this interface.

Monitoring by using SNMP

Your storage system supports the Simple Network Management Protocol (SNMP), which is the dominant network management protocol.

The industry accepts this protocol because of its relative simplicity. SNMP standards provide a framework for the definition of management information along with a protocol for the exchange of that information. The storage system is compatible with SNMP v2c.

The SNMP model contains *managers* and *agents*. A manager is a software module responsible for managing the configuration on behalf of the network management application users. Agents are devices, such as your storage system, which is responsible for maintaining local management information and delivering that information to a manager by SNMP. Both the manager and the agent can initiate management information exchanges.

Managers can access statistical information from the storage system through its management information base (MIB). For more information, see the SNMP Guide.

Web interface basics

Learn about the tasks you can complete by using the web interface.

Acquiring the system IP address

To use the web interface, you must connect to it over your network.

About this task

To acquire the IP address of the storage system by using the front panel display, complete the following steps:

Procedure

1. Press the **Menu** button to display the Main Menu pane. Use the arrow buttons to find the **System Info** option, and then press the **Select** button.
2. Use the ↓ button to scroll until you see the `Eth0 P` line and the lines below it.
3. Take note of the IP address.

Accessing the web interface

You can access the web interface from any web browser that supports Sun Java v1.5 or later.

About this task

To open the web interface, complete the following steps:

Procedure

1. Download the Sun Java plug-in for Microsoft Internet Explorer for Windows and for both Linux and Windows versions of Firefox. To obtain the latest Sun Java plug-in, go to http://www.java.com.
2. Using a standard web browser with the Sun Java plug-in, set the address to your IP address. The System Login pane is shown. The storage system is initially configured with a default admin user defined as User: admin and Password: password
3. Log in. The web interface opening pane is shown.
4. Expand or select the storage system icon in the system tree.

Setting the date and time by using the web interface

When you acquire the system, it is important to verify that the system date and time are correct.

About this task

If you must set the date and time, complete the following steps:

Procedure

1. From the web interface, select the **Management** node in the system tree.
2. Select the **Date/Time** node. The current date and time, and the length of the time the system has been running is shown.
3. If the date and time are incorrect, set them manually. Either use the right mouse button to click the **Date/Time** node and select **Date/time configuration**, or use the left-mouse to click the wrench icon in the button bar. Both methods start the **Date/Time** configuration wizard.
4. Follow the instructions in the wizard to configure the date and time, or specify a Network Time Protocol (NTP) server to supply this information automatically.

Configuring the management controller port by using the web interface

You can use the web interface to configure the settings for the management controller port (MCP).

About this task

To configure the settings by using the web interface, complete the following steps:

Procedure

1. From the web interface, select the **Management** tree under the system node.
2. Select **Network** to display the current network settings.
3. To modify the network configuration, right-click the **Network** node and click **Ethernet 0** to start the network configuration wizard.
4. After you edit the network settings, click **Finish**. The settings are saved and the system's network is restarted. Several system messages are displayed in the **Recent Event Log** panel of the web interface that confirm your settings.

Terawatch

The terawatch option can be used to manage multiple systems from a single web management interface.

The terawatch options that you can use follow.

- Use the **Add System** button to log in to more systems. Use this option to manage multiple storage systems at the same time.
- Use the **Discover** button to start a network broadcast that discovers other systems on the network.
  1. To set options for this action, select **Options** > **Preferences**. The Preferences pane is shown.
  2. Select the **Discovery** tab, and set the wanted options.

The web management interface also provides a way to view statistics, connect, or patch multiple systems simultaneously. These actions are available under the **Options** menu.

Managing security with the web interface

There are several settings that can help you manage security by using the web interface.

Default accounts

The storage system is initially configured with two types of user accounts: high-privileged user and low-privileged user.

High-privileged user
The high-privileged user is allowed to change configurations of the storage system. The default login settings follow:

- User: admin
- Password: password

Low-privileged user
The low-privileged user can view statistics, logs, and other information but cannot change any settings. The default login settings follow:

- User: user
- Password: password

Changing passwords

You can configure the security on the storage system to suit your needs. At a minimum, you must change the default high-privileged user password.

About this task

To change this password by using the web interface, complete the following steps:

Procedure

1. Expand the **Management** node under the system tree, and then select the **Users** node. The Change Password pane displays information about current user accounts in the Detailed Information pane.
2. To change the password to the high-privileged user account (the default value is admin), select this user and click **Password**.
3. In the Change User Password pane, type in the new password and confirm it. Click **Next** to confirm the change and then click **Finish**.

Adding users

You can add high-privileged users or low-privileged users with this function.

To add new users through the web interface, click the **Add** button in the **Users** pane to open the **Add User** pane.

- To add a high-privileged user, assign them to the admins group.
- To add a low-privileged user, assign them to the users group.

Lightweight Directory Access Protocol

The Lightweight Directory Access Protocol (LDAP) function provides central authentication of login credentials in addition to any local users.

Note: Users that are authenticated on the LDAP server are granted user-level permissions.

Before you use this function, you must first configure the LDAP settings to match the server.

To configure the LDAP settings, select the **User's** node under **Management** in the system tree. The configuration wizard includes the following settings:

Host This setting is the LDAP server. It must be resolvable without using LDAP. Multiple hosts might be specified, each separated by a space.

Base DN
This setting is the distinguished name (DN) of the search base.

Port (Optional) This setting is the port that is used to connect to the LDAP server. The default setting uses port 389 for TLS or no encryption, or port 636 for SSL encryption. If you use a different port, make sure to specify it in this field.

Bind DN

(Optional) This setting is the distinguished name that is used for binding to the LDAP server. If left in the default setting, the storage system tries to bind anonymously.

Bind Password

(Optional) This setting is the password that the LDAP server uses to authenticate the “Bind DN” when the storage system tries to bind.

Timeout

This setting is the timeout in seconds to wait for an LDAP search operation.

Bind Timeout

This setting is the timeout in seconds to wait for an LDAP bind operation.

Encryption

Choose which type of encryption to use for communication with the LDAP server.

Storage modes

Your storage system is configured with a specific storage mode.

Each mode is tailored to a use case for a high capacity solid-state disk.

Attention: You cannot switch between storage modes, as this is a destructive action and causes data loss.

Maximum capacity

Maximum capacity mode is the most flexible and is useful in an environment where the entire capacity of the unit is needed.

The maximum capacity storage mode is used to create logical units and assign access policies as needed. This mode is well-suited for deployments where the storage system is mirrored or preferred read mirrored with other storage. (In a preferred read mirror implementation, data is read from the storage with the lowest latency (the flashcards in the storage system).

Data acquisition

This specialized storage mode creates one logical unit and assigns access policies to all interface ports.

This data acquisition mode is used to present the entire storage space to all connected devices.

JBOF

The Just a Bunch of Flash (JBOF) storage mode automatically creates one logical unit for each flashcard present in the system.

The administrator can then assign access policies as needed. JBOF mode is useful in an environment where a host-based software RAID can be created to increase redundancy across the flashcards.

Active spare

The active spare storage mode automatically uses the last flashcard in the unit as a spare. This function provides another level of redundancy when a flashcard fails, in an environment where some of the storage capacity can be sacrificed for this additional data redundancy.

With the active spare storage mode, if a card experiences a recoverable failure (that is, a flash chip fails), the data is migrated off the failed card and onto a designated spare. The failed card is later replaced and the newly installed card becomes the new active spare storage mode. Note that the flashcards are not hot-swappable. In this storage mode, there are still a few components that are not protected by active spare storage mode, so there is a risk of an unrecoverable component failure. If a deployment requires no single point of failure, mirrored storage systems that use the maximum capacity storage mode is the preferred solution.

Attention: The failed card must be replaced immediately after the data replication is complete.

Creating logical units

The most common management activity on the storage system is logical unit creation.

About this task

Basic logical unit creation activities are covered here. For more detail, see the *Web Interface Guide*.

Important: For specific operating system and application optimizations for logical units, see the storage system *Integration Guide*.

To create a logical unit, complete the following steps:

Procedure

1. In the web interface system tree, right-click the **Logical Units** tree node and select **Create**. The logical unit creation wizard opens.
2. After you read the overview, click the **Next** button to set the logical unit parameters.
3. The parameters available for the logical unit follow.

   Name This setting is a user-defined name for the logical unit to make it easily identifiable.

   Number
   This setting is the logical unit number (LUN) that is presented to the host.

   Size This setting is the size of the logical unit.

   Device ID
   This setting is an OpenVMS specific identifier.

   Sector Size
   This setting is the sector size of the logical unit.

   Offset This setting sets the logical unit starting alignment to offset.

   Report corrected media errors to the SCSI host
   This setting controls whether any internal corrected errors are reported over the SCSI layer to the host. For most environments, enable this setting.

   Report uncorrected media errors to the SCSI host
   This setting controls whether any internal uncorrected errors are reported over the SCSI layer to the host. For most environments, enable this setting.

   Enable ACA Support
   This setting enables Auto Contingent Allegiance (ACA) support for the logical unit. Some host systems, such as systems that are running the AIX® operating system, require this setting to run multiple concurrent commands. After this option is changed, all interface ports that have access to the logical unit must be reset.
4. After you set the appropriate values, click **Next**. A final pane confirms the values. After you click **Finish**, the logical unit is created.

Results

For the logical unit to be used, you must define an access policy.

Logical unit access policies

You can use the web interface to create access lists for individual Fibre Channel or InfiniBand ports.

This access list allows the administrator to specify which ports are allowed to communicate with each logical unit.

New logical units are displayed with a warning state that notifies the administrator that a logical unit was created. The logical units are not presented to any hosts until an access policy is defined.

Adding an access policy to a logical unit

To make logical units accessible to connected servers, you must first link the logical unit to the storage system Fibre Channel or InfiniBand ports

About this task

To add an access policy to a new logical unit, complete the following steps:

Procedure

1. In the web interface system tree, click the logical unit node.
2. Click **Access** on the Logical Unit Overview pane to start the Access Policy wizard. The first step of the access policy wizard provides an overview of the process.
3. After you read the overview, click **Next** to continue to the Modify Access Policies pane.
4. The tree titled **Available** shows a tree of all controller ports in the system with each port's available access policies underneath. The tree titled **Assigned** shows the policies currently in use for each port in the system. If there are potential conflicts between policies that are assigned and policies that are available, the conflicting available policies are disabled in the **Available** tree. If the system detects a host server that is connected to the controller port for the access policy, the policy node's connector icon includes a plus sign.
   a. To add an Access Policy, select the wanted policy node from the **Available** tree. When it is highlighted, the **>>** button becomes enabled. Clicking this button moves the policy from the **Available** tree to the **Assigned** tree. When a new policy is added to the **Assigned** tree, its text color is green.
   b. To remove an Access Policy, select the wanted policy node from the **Assigned** tree and click the **<<** button. The policy is removed from the **Assigned** tree and added to the **Available** tree. When an in-use policy is deleted from the **Assigned** tree, its text color is red in the **Available** tree. Policy changes are not committed until the next step in the wizard.
5. When you finish making policy changes, click **Next** to continue to the modifications review page.
6. If policy modifications are only policy additions, click the **Confirm** check box and click **Finish** to exit the wizard and commit the policy changes. If there are policy removals, you are required to enter the admin login password to finish the wizard.

Logical unit masking

The logical unit (LU) masking feature assigns access policies to a LU on the storage system, thus restricting access to specific host servers through a controller port.

About this task

This feature is opposed to **Open Access** where the LU is accessible to all hosts connected to the port.

When the LU masking feature is installed, access to specific hosts can be created through the web management interface's Access Policy wizard. With LU masking available, the wizard shows the worldwide port names (WWPNs) of connected hosts in its **Available** policy tree. The wizard also supports the ability to create host ID aliases. You can use a host ID alias to associate a meaningful text name with a host's WWPN.

Procedure

1. In the web interface, select the logical unit in the system tree.
2. To run the Access Policy wizard, click the **Access** button on the **Logical Unit Overview** screen.
3. To create an alias, click the **New Alias** button underneath the **Available** policy tree. This action opens a dialog where you can enter the host's WWPN in the **Host ID** text box and the alias name in the **Alias** text box.
4. Click **Add** to finish and save the alias. The aliased host is listed in the Access Policies tree for each controller.
5. To remove or edit existing aliases, use the **Edit Alias** button on the Access Policy wizard.
6. The **Remove** button deletes the currently selected alias. To change an alias' name, select the alias in the table and click the **Re-alias** button to enable the **Alias** table cell for editing. When changes are complete, press the **Enter** key to leave edit mode and save the changes to the table. Click **OK** to exit the dialog.

Viewing the system logs with the web interface

You can view, configure, and clear system logs by using the web interface.

Accessing the system event log

The system event log is an important part of the web interface. This log tracks all events that occurred within the system, and is a valuable troubleshooting resource.

Accessing the system report

The system report contains information about the system configuration, firmware version, environment, and other information, including a copy of the system event log.

You must have a system report available before you contact Support.

To access the system report from the web interface, right-click the **Logs** item in the system tree and select **System Report**.

Configuring the mail service settings:

The mail service function provides system event email notifications and the ability to email the System Report directly for support purposes.

About this task

To configure the mail service settings, complete the following steps:

Procedure

1. In the web interface, select the **Management** node in the tree and click the **Mail** node. The Overview pane is shown.
2. Click the **Configure** button to open the configuration wizard. Use this wizard to enable available functions, select the SMTP server, and enter target email addresses. Any available mail service functions might be enabled by checking the box that corresponds to the function.
3. The SMTP server might be set manually or found automatically from DHCP by setting the server value to **Default**. You can specify up to five email targets to receive emails that are sent by the service.
4. To email the System Report, select the **Logs** node in the tree and click the **Email System Report** button in the toolbar.
5. Complete the **From** and **Comment** fields, and then click **OK** to send the System Report. This action takes a few seconds to complete while the report is generated. Click **Cancel** to close the dialog without sending a report.

Clearing the system event log

When a problem is diagnosed and solved, it is important to clear the errors from the log to provide visibility for any future issues.

To clear the system event log, right-click the **Logs** node in the system tree and select **Clear Event Log**. Alternatively, use the left mouse button to click **Clear Event Log** in the toolbar.

Statistic log

The statistics log option enables the storage system to save logs of system statistics such as system bandwidth and the maximum temperature of all system components.

Additionally, user-specified statistics can be added to the logged list.

In the web interface, the **History** node under **Statistics** shows the currently logged list.

Viewing statistics logs

You can view statistics logs for a specific time period and save the log to use later.

About this task

To view a statistics log, complete the following steps:

Procedure

1. Select between the **Day**, **Month**, or **Year** button to change the time period that is shown in the graph. The darker-colored line graph that is drawn for a statistic is an average line of periodic samples. The variance of these samples is represented by a lighter-shaded polygon of the same color.
2. Use the **Variance** check box to turn on or off the variance option.
3. Use the **Save** button to save the graph image as a JPEG or a CSV (comma-separated values) file.
4. To view one or multiple statistics history, select the statistic in the **Currently Logged Stats** table (press Ctrl + click to select multiple statistics), then click the **Save/View** action. This action opens a pane that displays a graph of the statistics daily history, showing the time in the x-axis and the statistics value in the y-axis.

Configuring logged statistics

You can add or remove system statistics to the logged history list.

About this task

The original list of logged statistics cannot be removed, but any user-added statistic can.

To configure the logged statistics, complete the following steps:

Procedure

1. To access the configuration wizard, select the **Configure** icon in the **Statistics Detailed Information** toolbar. The left side of the Modify Logged Statistics pane has two list boxes. The top box lists system components.
2. Select a component from the list to generate a list of its statistics in the lower box, similar to the statistics graph configuration dialog.
   - To add a statistic to the logged list, select a component and statistic pair and click the center **Add** button. The new statistic is shown at the bottom of the logged statistics list.
   - To remove a statistic, select it in the logged list and click the **Remove** button.

   A confirmation page is shown. Any added statistics are shown at the bottom of the list.

3. To complete the configuration wizard and save any changes, click the **Confirmation** check box and click **Finish**.

Upgrading the system software and firmware

You can upgrade your storage system software and firmware with a patch file by using the web interface.

About this task

To upgrade your storage system with a patch file, complete the following steps:

Procedure

1. From the web interface, select the **Management** node in the system tree. Highlight **Firmware** to view the current firmware version.
2. To update the firmware, either right-click the **Firmware** node and select **Firmware update**, or left-click **Update** in the toolbar.
3. In the patch file selector pane, either type in the path and file name of the patch, or click **Browse** to look for the file. After the file is selected, left-click **Next** and follow the instructions in the wizard. The wizard uploads the patch onto the system.
4. You must power-cycle the enclosure to apply and activate the new patch. To power-cycle the enclosure, complete the following steps:
   a. In the web interface, click the system IP address in the system tree to display the system panel.
   b. Click **Restart** or **Shutdown** to power-cycle the system and begin the patch process.
   c. Monitor progress in the Recent Event Log window on the lower half of the screen. The patch process requires 30 - 60 minutes to complete.

   An uploaded firmware patch can be canceled before the system is restarted. To cancel a patch, click **Cancel Patch** and confirm that you do not want to apply the currently uploaded patch.

   Attention: Patching the storage system is a delicate process. If the patch process is interrupted by power loss the system can become unusable. If your systems patch is interrupted, or hangs for some unforeseen reason longer than 1 hour, immediately contact Support. DO NOT DISCONNECT THE POWER CORDS to resolve the situation, unless recommended to do so by Support.

Saving and restoring the configuration

Use the save and restore configuration function to save the configuration of a storage system, including its logical units and users, and restore it later.

This function is beneficial if you have multiple storage systems and would like each one to have an identical configuration. That is, you can configure a system, save its configuration, and restore this configuration onto all other systems.

Attention: Restoring a configuration from a different system replaces the current configuration, which includes logical units. Data on the current logical units is not recoverable.

- To save a system's configuration, in the system tree, click **Management** > **Save Configuration**. You can then select a file to save the configuration. Remember the file name and location as it is needed to restore the configuration later.
- To restore a configuration, click the **Restore Configuration** in the system tree on the system you would like to apply the configuration to, and choose the previously saved configuration file.

Monitoring tasks

The storage system can record all configuration changes since the last power-cycle. This information can be valuable when you are diagnosing configuration problems.

The current tasks are on the **Task Monitor** tab next to the **Recent Event Log** at the bottom of the web interface pane.

Troubleshooting

The storage system is a complex device with many redundant functions to safeguard your data. When a component does fail, the system has many ways to inform you about what is happening inside the system.

Front panel display

The easiest way to detect an issue is to monitor the front panel display.

The normal display includes a line at the top that shows if the system is `Good`. If the system detects an error, the front panel display reports the error in a concise manner.

System event log

The system event log provides more detailed information about any problems.

For details on how to access the log, see “Accessing the system event log” on page 18.

All errors are permanently logged until the problem is resolved and the log is cleared. When a problem is diagnosed and solved, it is important to clear the errors from the log to provide visibility for any future issues. For details on clearing the log, see “Clearing the system event log” on page 19

System report

The system report provides a snapshot of all current configuration settings, statistics, and the event log.

For details on accessing the report by using the web interface, see “Accessing the system report” on page 18.

Reformatting uninitialized flashcards

If the storage system has been without power for more than one month, it is possible that the management GUI shows one or more flashcards as failed. The front panel may also show error messages such as Storage Offline.

Before you begin

This condition is NOT a failure. It is a characteristic of Enterprise Flash technologies that are used in the storage system. The remedy is to format the flash array. There is no immediate need to contact support if this condition is observed on first boot or if the storage system was powered off for more than one month. (You can verify the last power up date by selecting Logs in the GUI and verifying the date of the last entries.)

About this task

To log in to the command line interface and format the uninitialized flashcards, complete the following steps:

Procedure

1. From a telnet or Secure Shell (SSH) client, access the system by using the system IP address.
2. Log in using the default administrator username `admin` and the default password `password`, or your system's unique username and password.
3. At the command prompt, enter `#diag` to enter diagnostic mode.

4. To confirm the command, enter `YES`.
5. From the diagnostic menu, type `1`.
6. To confirm the command, enter `YES`.
7. From the Format Flashcard submenu, either enter `ALL` to format all flashcards, or select an individual flashcard by typing `flashcard-#`where `#` is the slot number of the new flashcard.
8. Enter `q` to exit diagnostic mode and return to the command prompt.
9. Enter `#storage` to confirm that all the flashcards are formatted.

Monitoring battery health

Internal sensors report on the battery voltage level. A monthly test ensures that the electrical current supplied from the batteries is sufficient to handle a sudden power loss.

When the internal sensors detect a problem, the errors are reported.

- If the battery voltage is out of specification or the monthly battery test fails, warnings are reported.
- If the batteries degrade and are unusable, errors are reported.

The batteries are redundant, so data is not at risk in the event of a single battery power failure. However, replacing the failed battery promptly is preferred.

To view the status of each battery, select the **Battery** node in the **Environmental** portion of the system tree.

For information about replacing a failed battery, see your system troubleshooting and service documentation.

Parts replacement information

For detailed information about replacing customer-serviceable components, see your system troubleshooting and service documentation.

Notices

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

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

The manufacturer 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 the manufacturer.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: THIS PUBLICATION IS PROVIDED "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. The manufacturer 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 websites not owned by the manufacturer are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this product and use of those websites is at your own risk.

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning products not produced by this manufacturer was obtained from the suppliers of those products, their published announcements or other publicly available sources. This manufacturer has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to products not produced by this manufacturer. Questions on the capabilities of products not produced by this manufacturer should be addressed to the suppliers of those products.

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

The manufacturer's prices shown are the manufacturer's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information in softcopy, the photographs and color illustrations may not appear.

The drawings and specifications contained herein shall not be reproduced in whole or in part without the written permission of the manufacturer.

The manufacturer has prepared this information for use with the specific machines indicated. The manufacturer makes no representations that it is suitable for any other purpose.

The manufacturer's computer systems contain mechanisms designed to reduce the possibility of undetected data corruption or loss. This risk, however, cannot be eliminated. Users who experience unplanned outages, system failures, power fluctuations or outages, or component failures must verify the accuracy of operations performed and data saved or transmitted by the system at or near the time of the outage or failure. In addition, users must establish procedures to ensure that there is independent data verification before relying on such data in sensitive or critical operations. Users should periodically check the manufacturer's support websites for updated information and fixes applicable to the system and related software.

Homologation statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact an IBM representative or reseller for any questions.

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 www.ibm.com/legal/copytrade.shtml.

INFINIBAND, InfiniBand Trade Association, and the INFINIBAND design marks are trademarks and/or service marks of the INFINIBAND Trade Association.

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

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

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Electronic emission notices

When attaching a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices supplied with the monitor.

Class A Notices

The following electronic emission statements apply to this product. The statements for other products that are intended for use with this product are included in their accompanying documentation.

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 instruction 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.

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 or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

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.

Industry Canada Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

European Community Compliance Statement

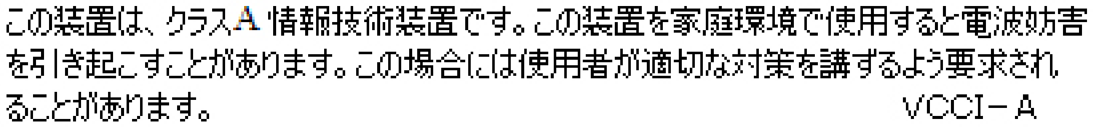
This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM 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 A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
email: lugi@de.ibm.com

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.

VCCI Statement - Japan

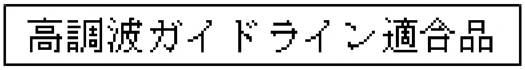


この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害
を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求され
ることがあります。 VCCI－A

The following is a summary of the VCCI Japanese statement in the box above:

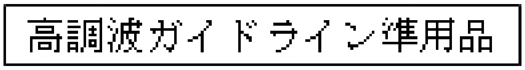
This is a Class A product based on the standard of the VCCI Council. If this equipment is used in a domestic environment, radio interference may occur, in which case, the user may be required to take corrective actions.

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline (products less than or equal to 20 A per phase)



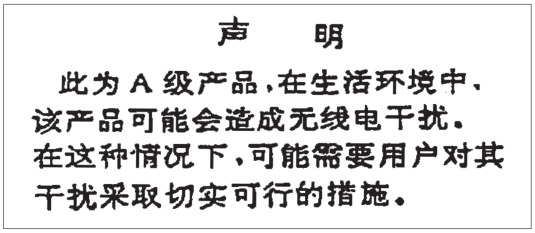
高調波ガイドライン適合品

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)



高調波ガイドライン準用品

Electromagnetic Interference (EMI) Statement - People's Republic of China

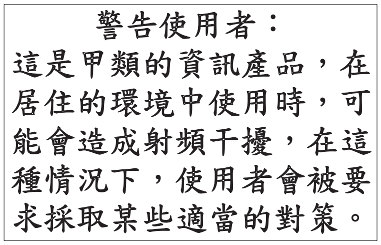


声 明

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。

Declaration: 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 action.

Electromagnetic Interference (EMI) Statement - Taiwan

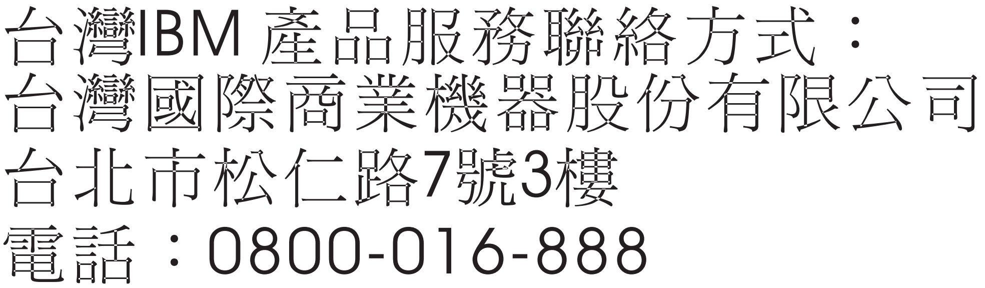


警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

The following is a summary of the EMI Taiwan statement above.

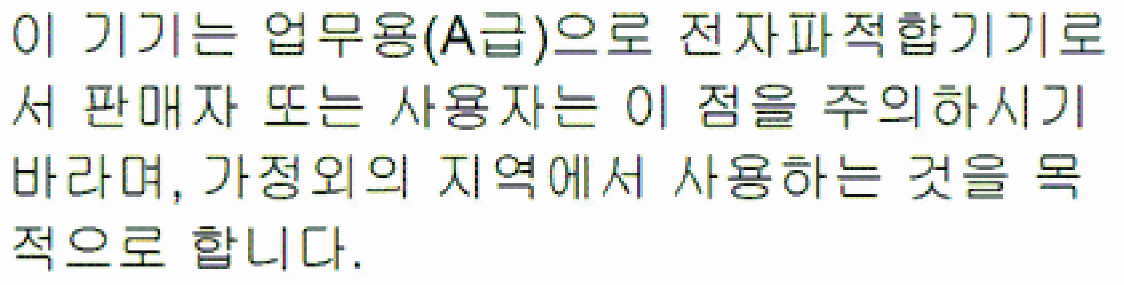
Warning: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user will be required to take adequate measures.

IBM Taiwan Contact Information:



台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea



이 기기는 업무용(A급)으로 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Germany Compliance Statement

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

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten 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 von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von 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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

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

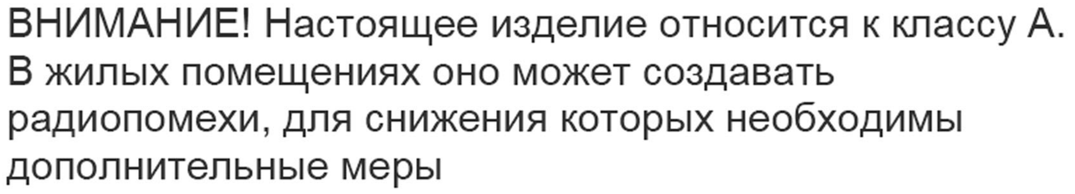
Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 7032 15 2941
email: lugi@de.ibm.com

Generelle Informationen:

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

Electromagnetic Interference (EMI) Statement - Russia



ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Class B Notices

The following Class B statements apply to features designated as electromagnetic compatibility (EMC) Class B in the feature installation information.

Federal Communications Commission (FCC) statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate this equipment.

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.

Industry Canada Compliance Statement

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

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

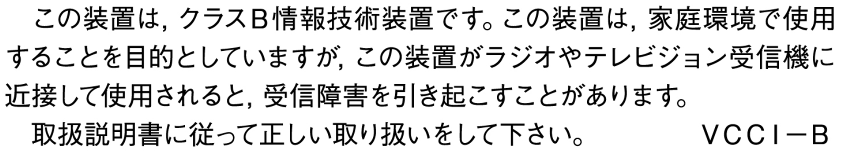
European Community Compliance Statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM 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 option cards.

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

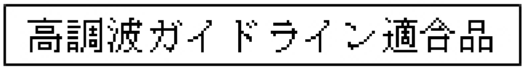
European Community contact:
IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Tele: +49 7032 15 2941
email: lugi@de.ibm.com

VCCI Statement - Japan



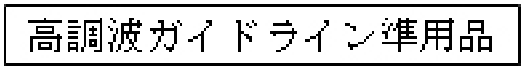
この装置は，クラスＢ情報技術装置です。この装置は，家庭環境で使用
することを目的としていますが，この装置がラジオやテレビジョン受信機に
近接して使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。　　ＶＣＣＩ－Ｂ

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline (products less than or equal to 20 A per phase)



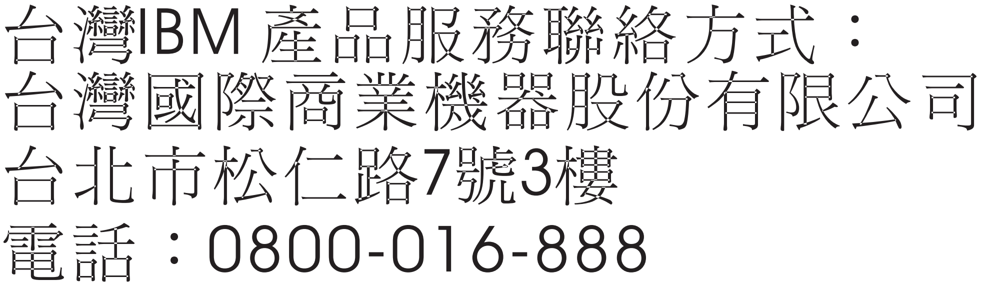
高調波ガイドライン適合品

Japanese Electronics and Information Technology Industries Association (JEITA) Confirmed Harmonics Guideline with Modifications (products greater than 20 A per phase)



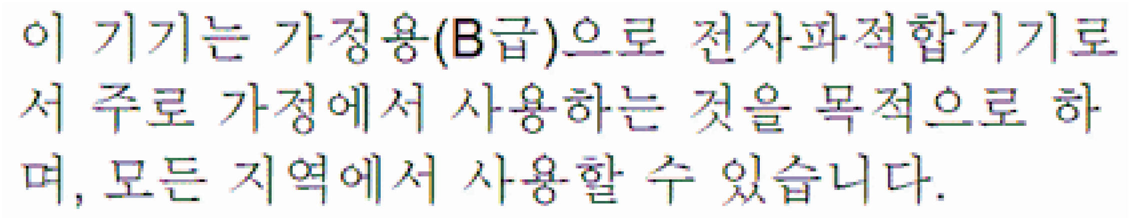
高調波ガイドライン準用品

IBM Taiwan Contact Information



台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Electromagnetic Interference (EMI) Statement - Korea



이 기기는 가정용(B급)으로 전자파적합기기로
서 주로 가정에서 사용하는 것을 목적으로 하
며, 모든 지역에서 사용할 수 있습니다.

Germany Compliance Statement

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

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse B 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 von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

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 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse B

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

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 7032 15 2941
email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse B.

Terms and conditions

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability: These terms and conditions are in addition to any terms of use for the IBM website.

Personal Use: You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative works of these publications, or any portion thereof, without the express consent of IBM.

Commercial Use: You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights: Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the Publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Printed in USA