Integrated Management Module II
User's Guide

Integrated Management Module II
User's Guide

First Edition (March 2012)

Contents

Tables

Chapter 1. Introduction

The Integrated Management Module II service processor (IMM2) is the second generation of the Integrated Management Module (IMM) service processor that consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board. As was the case with IMM, IMM2 offers several improvements over the combined functionality of the BMC and the Remote Supervisor Adapter II including these features:

- Choice of a dedicated or shared Ethernet connection for systems management.
- One IP address for both the Intelligent Platform Management Interface (IPMI) and the service processor interface. The feature does not apply to IBM BladeCenter blade servers.
- Embedded Dynamic System Analysis (DSA).
- Remote configuration with Advanced Settings Utility (ASU). The feature does not apply to IBM BladeCenter blade servers.
- Capability for applications and tools to access the IMM2 either in-band or out-of-band. Only the in-band IMM2 connection is supported on blade servers.
- Enhanced remote-presence capabilities. The feature does not apply to blade servers.

Note:

1. A dedicated systems-management network port is not available on IBM BladeCenter servers and some System x servers; for these servers only the *shared* setting is available.
2. For IBM BladeCenter blade servers the IBM BladeCenter advanced management module is the primary management module for systems-management functions and keyboard/video/mouse (KVM) multiplexing.

IBM System x® Server Firmware is IBM's implementation of Unified Extensible Firmware Interface (UEFI). It replaces BIOS in IBM System x servers and IBM BladeCenter blade servers. The basic input/output system (BIOS) was the standard firmware code that controlled basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard. IBM System x Server Firmware offers several features that BIOS does not, including UEFI 2.3 compliance, iSCSI compatibility, Active Energy Manager technology, and enhanced reliability and service capabilities. The Setup utility provides server information, server setup, customization compatibility, and establishes the boot device order.

Note:

1. IBM System x Server Firmware is often called server firmware, and occasionally called UEFI, in this document.
2. IBM System x Server Firmware is fully compatible with non-UEFI operating systems.
3. For more information about using IBM System x Server Firmware, see the documentation that came with your IBM server.

This document explains how to use the functions of the IMM2 in an IBM server. The IMM2 works with IBM System x Server Firmware to provide systems-management capability for System x and BladeCenter servers.

To check for firmware updates, complete the following steps.

Note: The first time you access the IBM Support Portal, you must choose the product category, product family, and model numbers for your storage subsystems. The next time you access the IBM Support Portal, the products you selected initially are preloaded by the website, and only the links for your products are displayed. To change or add to your product list, click the **Manage my product lists** link.

Changes are made periodically to the IBM website. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

1. Go to http://www.ibm.com/support/entry/portal.
2. Under **Choose your products**, select **Browse for a product** and expand **Hardware**.
3. Depending on your type of server, click **Systems** > **System x** or **Systems** > **BladeCenter**, and check the box for your server or servers.
4. Under **Choose your task**, click **Downloads**.
5. Under **See your results**, click **View your page**.
6. In the Flashes & alerts box, click the link for the applicable download or click **More results** to see additional links.

IMM2 features

With IMM2, Basic, Standard and Advanced levels of IMM2 functionality are offered. (See the documentation for your server for more about the level of IMM2 installed in your IBM server.) All levels provide the following:

- Around-the-clock remote access and management of your server
- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems

In addition, Standard and Advanced levels support Web-based management with standard web browsers.

The following tables list the features of each level.

IMM2 Features - Basic Level
IPMI 2.0 Interface
Thermal Monitoring
Fan Control
LED Management
Server Power/Reset Control
Sensor Monitoring
IPMI Platform Event Trap Alerting
IPMI Serial over LAN

IMM2 Features - Standard Level
All Features of IMM2 Basic Level
Web-based Management with Standard Web Browsers
SNMPv1 and SNMPv3 Interfaces
Telnet and ssh CLI
Scheduled Server Power/Reset Control
Human-Readable Event and Audit Logging
System Health Indication
Operating System Loader and Operating System Watchdogs
LDAP Authentication and Authorization
SNMP TRAP, E-mail, Syslog, and CIM Indication Alerting
NTP Clock Synchronization
Serial Console Redirection over telnet/ssh

IMM2 Features - Advanced Level
All Features of IMM2 Basic and Standard Levels
Remote Presence Java and ActivX Clients: • Remote Keyboard, Video, and Mouse Support • Remote Media • Remote Disk on Card
Failure Screen Capture for Operating System hangs

Note: Some features might not apply to IBM BladeCenter blade servers.

IMM2 feature improvements

The following table lists improvements made from IMM.

IMM2 improvements over IMM
Security (trusted service processor): • Secure boot • Signed updates • IMM2 Core Root for Trust Measurement • Trusted Platform Module
New Web GUI design consistent across IBM System x
Increased remote presence video resolution and color depth
ActiveX remote presence client
Ethernet-over-USB interface upgraded to USB 2.0
Syslog alerting
No IMM2 reset required after configuration changes

Upgrading IMM2

If your IBM server came with either Basic level or Standard level IMM2 firmware functionality, you might be able to upgrade IMM2 functionality. For more information about available upgrade levels and how to order, see Chapter 4, “Features on Demand,” on page 17

Using IMM2 with the BladeCenter advanced management module

The BladeCenter advanced management module is the standard systems-management interface for IBM BladeCenter products. Although the IMM2 is now included in some IBM BladeCenter blade servers, the advanced management module remains the management module for systems-management functions and keyboard, video, and mouse (KVM) multiplexing for BladeCenter products including the blade servers.

There is no external network access to the IMM2 on BladeCenter blade servers and the advanced management module must be used for remote management of blade servers. The IMM2 replaces the functionality of the BMC and the Concurrent Keyboard, Video and Mouse (cKVM) option card available in past blade server products.

Web browser and operating-system requirements

The IMM2 web interface requires the Java Plug-in 1.5 or later (for the remote presence feature) and one of the following web browsers:

- Microsoft Internet Explorer version 7.0 or later
- Mozilla Firefox version 3.5 or later

The following server operating systems have USB support, which is required for the remote presence feature:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux versions 4.0 and 5.0
- SUSE Linux version 10.0
- Novell NetWare 6.5

Notices used in this book

The following notices are used in the documentation:

- **Note:** These notices provide important tips, guidance, or advice.
- **Important:** These notices provide information or advice that might help you avoid inconvenient or problem situations.
- **Attention:** These notices indicate potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.

Chapter 2. Opening and using the IMM2 web interface

Important: This section does not apply to IBM BladeCenter and blade servers. Although the IMM2 is standard in some IBM BladeCenter products and IBM blade servers, the BladeCenter advanced management module is the primary management module for systems-management functions and keyboard/video/mouse (KVM) multiplexing for BladeCenter and blade servers.

The IMM2 combines service processor functions, a video controller, and remote presence function (when an optional virtual media key is installed) in a single chip. To access the IMM2 remotely by using the IMM2 web interface, you must first log in. This chapter describes the login procedures and the actions that you can perform from the IMM2 web interface.

Accessing the IMM2 web interface

The IMM2 supports static and Dynamic Host Configuration Protocol (DHCP) IPv4 addressing. The default static IPv4 address assigned to the IMM2 is 192.168.70.125. The IMM2 is initially configured to attempt to obtain an address from a DHCP server, and if it cannot, it uses the static IPv4 address.

The IMM2 also supports IPv6, but the IMM2 does not have a fixed static IPv6 IP address by default. For initial access to the IMM2 in an IPv6 environment, you can either use the IPv4 IP address or the IPv6 link-local address. The IMM2 generates a unique link-local IPv6 address, which is shown in the IMM2 web interface on the Network Interfaces page. The link-local IPv6 address has the same format as the following example.

```
fe80::21a:64ff:fee6:4d5
```

When you access the IMM2, the following IPv6 conditions are set as default:

- Automatic IPv6 address configuration is enabled.
- IPv6 static IP address configuration is disabled.
- DHCPv6 is enabled.
- Stateless auto-configuration is enabled.

The IMM2 provides the choice of using a dedicated systems-management network connection (if applicable) or one that is shared with the server. The default connection for rack-mounted and tower servers is to use the dedicated systems-management network connector.

Note: A dedicated systems-management network port might not be available on your server. If your hardware does not have a dedicated network port, the *shared* setting is the only IMM2 setting available.

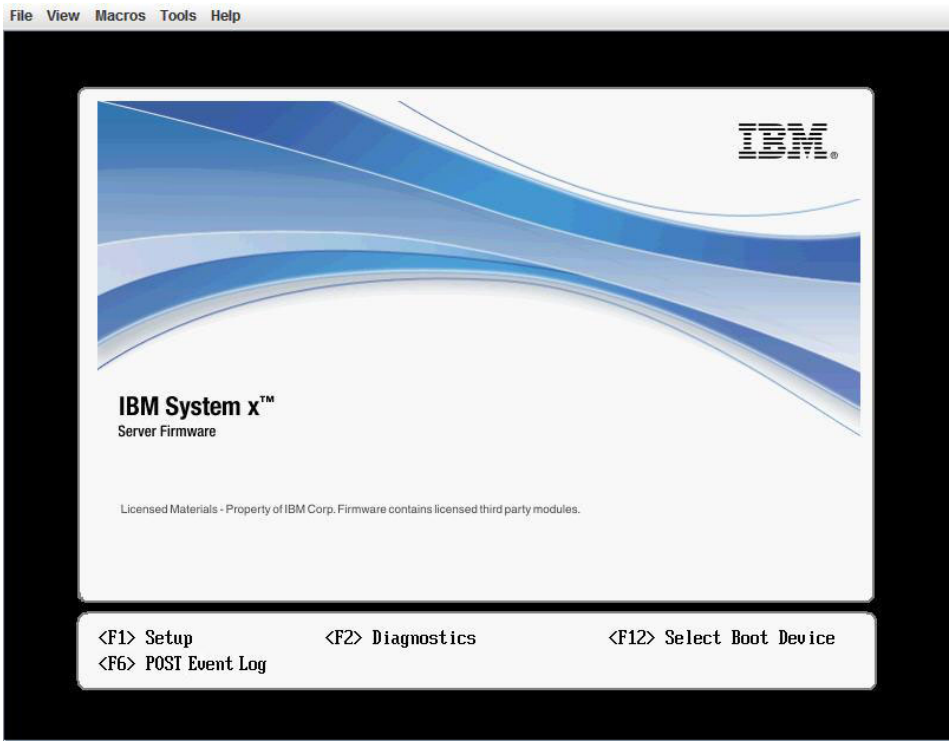
Setting up the IMM2 network connection through the IBM System x Server Firmware Setup utility

After you start the server, you can use the Setup utility to select an IMM2 network connection. The server with the IMM2 hardware must be connected to a Dynamic Host Configuration Protocol (DHCP) server, or the server network must be

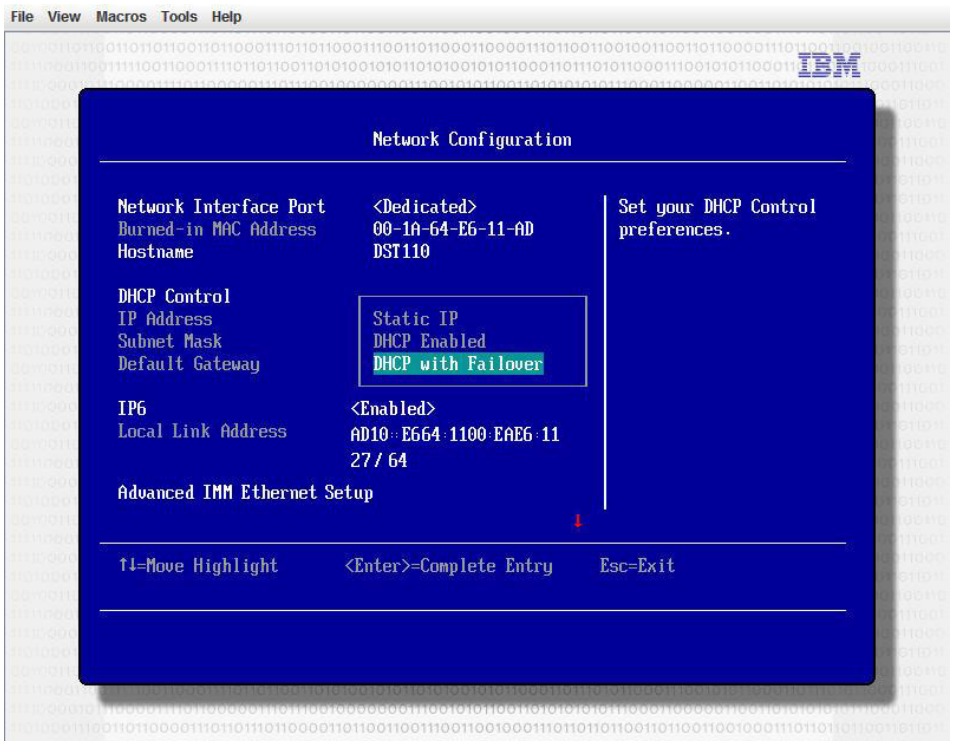
configured to use the IMM2 static IP address. To set up the IMM2 network connection through the Setup utility, complete the following steps:

1. Turn on the server. The IBM System x Server Firmware welcome screen is displayed.

   Note: Approximately 9 seconds after the server is connected to ac power, the power-control button becomes active.



2. When the prompt `<F1> Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to access the full Setup utility menu.
3. From the Setup utility main menu, select **System Settings**.
4. On the next screen, select **Integrated Management Module**.
5. On the next screen, select **Network Configuration**.
6. Highlight **DHCP Control**. There are three IMM2 network connection choices in the **DHCP Control** field:
   - Static IP
   - DHCP Enabled
   - DHCP with Failover (default)



7. Select one of the network connection choices.
8. If you choose to use a static IP address, you must specify the IP address, the subnet mask, and the default gateway.
9. You can also use the Setup utility to select a dedicated network connection (if your server has a dedicated network port) or a shared IMM2 network connection.

   Note:

   a. A dedicated systems-management network port might not be available on your server. If your hardware does not have a dedicated network port, the *shared* setting is the only IMM2 setting available. On the **Network Configuration** screen, select **Dedicated** (if applicable) or **Shared** in the **Network Interface Port** field.

   b. To find the locations of the Ethernet connectors on your server that are used by the IMM2, see the documentation that came with your server.
10. Scroll down and select **Save Network Settings**.
11. Exit from the Setup utility.

Note:

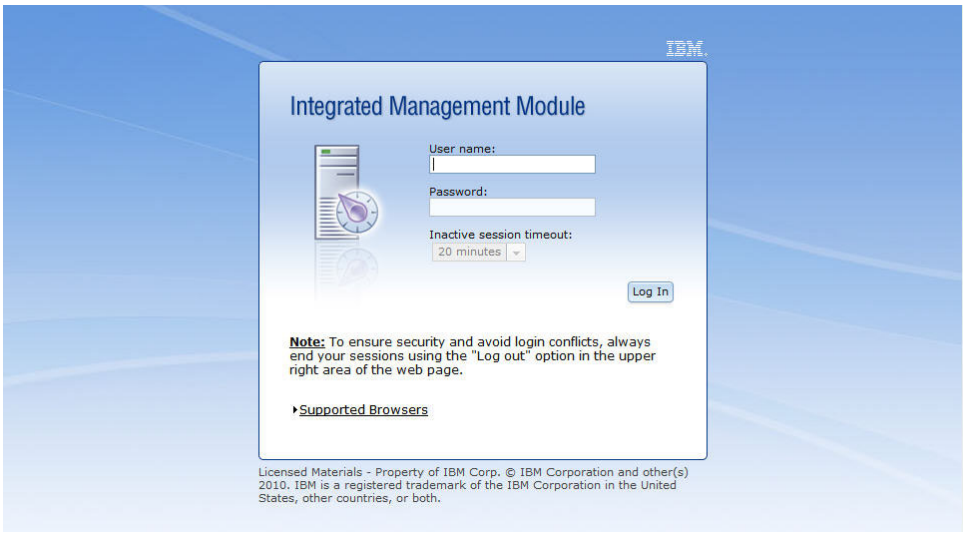
1. You must wait approximately 1 minute for changes to take effect before the server firmware is functional again.
2. You can also configure the IMM2 network connection through the IMM2 web interface or CLI. In the IMM2 web interface, network connections are configured on the **Network Protocol Properties** page (select **Network** from the **IMM Management** menu). In the IMM2 CLI, network connections are configured using several commands that depend on the configuration of your installation.

Logging in to the IMM2

Important: The IMM2 is set initially with a user name of USERID and password of PASSW0RD (with a zero, not the letter O). This default user setting has Supervisor access. Change this user name and password during your initial configuration for enhanced security.

To access the IMM2 through the IMM2 web interface, complete the following steps:

1. Open a web browser. In the address or URL field, type the IP address or host name of the IMM2 server to which you want to connect.



2. Type your user name and password in the IMM2 Login window. If you are using the IMM2 for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. Depending on how your system administrator configured the user ID, you might need to enter a new password.
3. Click **Log In** to start the session. The browser opens the System Status page, which gives you a quick view of the server status and the server health summary.

For descriptions of the actions that you can perform from the tabs at the top of the IMM2 web interface, see "IMM2 action descriptions."

IMM2 action descriptions

Navigate to activities you perform with the IMM at the top of the IMM window. The title bar identifies the user name that is logged in, allows you to configure **Settings** for the status screen refresh rate and a custom trespass message, and **Log out** of the IMM web interface. Beneath the title bar are tabs that allow you to access various IMM2 functions, as listed in Table 1.

Table 1. IMM2 actions

Tab	Selection	Description
System Status		The System Status page allows you to view system status, active system events, and hardware health information. It provides quick links to the System Information, Server Power Actions, and Remote Control functions of the Server Management tab, and allows you to view an image of the last operating-system-failure screen capture.
Events	Event Log	The Event Log page displays entries that are currently stored in the IMM event log. The log includes a text description of system events that are reported, including information about all remote access attempts and configuration changes. All events in the log are time stamped, using the IMM2 date and time settings. Some events also generate alerts, if they are configured to do so. You can sort and filter events in the event log and export them to a text file.
	Event Recipients	The Event Recipients page allows you to manage who will be notified of system events. It allows you to configure each recipient, and manage settings that apply to all event recipients. You can also generate a test event to verify notification feature operation.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
Service and Support	Download Service Data	The Download Service Data page creates a compressed file of information that can be used by IBM Support to assist you.
Server Management *(continued on next page)*	Server Firmware	The Server Firmware page displays firmware levels and allows you to update the IMM2 firmware, server firmware, and DSA firmware.
	Remote Control	The Remote Control page allows you to control the server at the operating system level. It provides access to both Remote Disk and Remote Console functionality. You can view and operate the server console from your computer, and you can mount one of your computer disk drives, such as the CD-ROM drive or the diskette drive, on the server. When you have mounted a disk, you can use it to restart the server and to update firmware on the server. The mounted disk appears as a USB disk drive that is attached to the server.
	Server Properties	The Server Properties page provides access to various properties, status, and settings for your server: • The General Settings tab displays information that identifies the system to operations and support personnel. • The LEDs tab displays the status of all system LEDs. It also allows you to change the state of the location LED. • The Hardware Information tab displays server vital product data (VPD). The IMM2 collects server information, server component information, and network hardware information. • The Environmentals tab displays voltage and temperature information for the server and its components. • The Hardware Activity tab displays a history of Field Replacable Unit (FRU) components that have been added to or removed from the system.
	Server Power Actions	The Server Power Actions page provides full remote power control over your server with power-on, power-off, and restart actions.
	Cooling Devices	The Cooling Devices page displays the current speed and status of cooling fans in the system. You can click on a device name to display active events for the cooling device.
	Power Modules	The Power Modules page displays the power modules in the system, along with their status and power ratings. You can click on a module name to display a events, additional hardware information, and errors for the power module.
	Disks	The Disks page displays the status of hard disk drives in the system. You can click on a drive name to display active events for the hard disk drive.
	Memory	The Memory page displays the memory modules available in the system, along with their status, type, and capacity. You can click on a module name to display a events and additional hardware information for the memory module. If you remove or replace DIMMs, the server needs to be powered on at least once after the removal or replacement to display the correct memory information.

Table 1. IMM2 actions (continued)

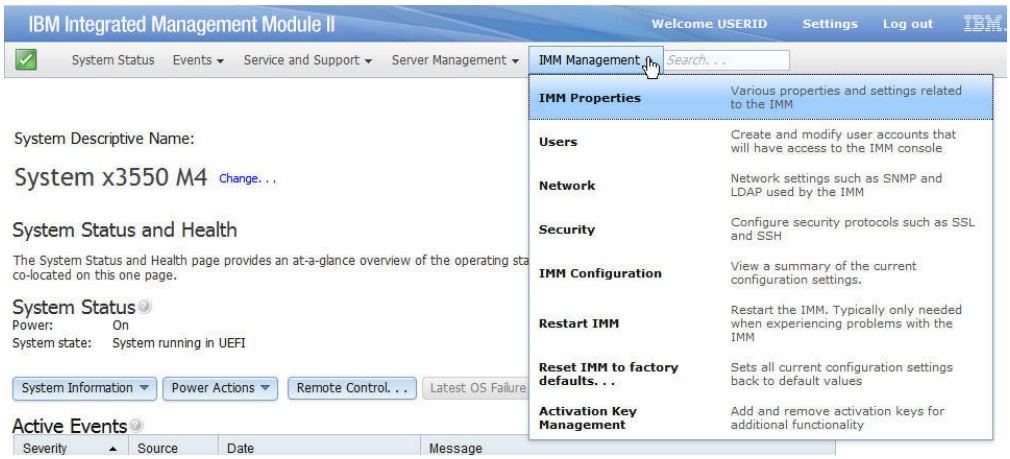
Tab	Selection	Description
Server Management *(continued)*	Processors	The CPUs page displays the microprocessors in the system, along with their status and rated speed. You can click on a microprocessor name to display events and additional hardware information for the microprocessor.
	Server Timeouts	The Server Timeouts page allows you to manage server start timeouts to detect and recover from server hang occurrences.
	PXE Network Boot	The PXE Network Boot page allows you to change the host server startup (boot) sequence for the next restart to attempt a Preboot Execution Environment (PXE)/Dynamic Host Configuration Protocol (DHCP) network startup. The host startup sequence will be altered only if the host is not under Privileged Access Protection (PAP).
	Latest OS Failure Screen	The Latest OS Failure Screen page displays a screen image, when available, of the most recent operating system failure on the server. For your IMM to capture operating system failure screens, the operating system watchdog must be enabled.
IMM Management *(continued on next page)*	IMM Properties	The IMM Properties page provides access to various properties, status, and settings for your IMM2: • The Firmware tab provides a link to the Server Firmware section of Server Management. • The IMM Date and Time Settings tab allows you to view and configure date and time settings for the IMM2. • The Serial Port tab configures the IMM2 serial port settings. These settings include the serial port baud rate used by the serial port redirection function and the key sequence to switch between the serial redirection and command-line interface (CLI) modes.
	Users	The Users page configures the IMM2 login profiles and global login settings, and view users that are currently logged in to the IMM2. Global login settings include enabling Lightweight Directory Access Protocol (LDAP) server authentication, setting the web inactivity timeout, and customizing the account security settings.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
IMM Management *(continued)*	Network	The Network Protocol Properties page provides access to networking properties, status, and settings for your IMM2: • The Ethernet tab manages how the IMM2 communicates using Ethernet. • The SNMP tab configures the SNMPv1 and SNMPv3 agents. • The DNS tab configures the DNS servers that the IMM2 interacts with. • The DDNS tab enables or disables and configures Dynamic DNS for the IMM2. • The SMTP tab configures SMTP server information used for alerts sent via email. • The LDAP tab configures user authentication for use with one or more LDAP servers. • The Telnet tab manages Telnet access to the IMM2. • The USB tab controls the USB interface used for in-band communication between the server and the IMM2. These settings do not affect the USB remote control functions (keyboard, mouse, and mass storage). • The Port Assignments tab allows you to change the port numbers used by some services on the IMM2.
	Security	The IMM Security page provides access to security properties, status, and settings for your IMM2: • The HTTPS Server tab allows you to enable or disable the HTTPS server and manage its certificates. • The CIM Over HTTPS tab allows you to enable or disable CIM over HTTPS and manage its certificates. • The LDAP Client tab allows you to enable or disable LDAP security and manage its certificates. • The SSH Server tab allows you to enable or disable the SSH server and manage its certificates.
	IMM Configuration	The IMM Configuration page displays a summary of the current IMM2 configuration settings. It also provides the following functions: • Backup the current IMM2 configuration • Restore a saved IMM2 configuration • Display backup and restoration status • Reset the configuration of the IMM2 to the factory defaults. • Access the IMM2 initial setup wizard
	Restart IMM	The Restart IMM page allows you to reset the IMM.
	Reset IMM to factory defaults...	The Reset IMM to factory defaults... page allows you to reset the configuration of the IMM2 to the factory defaults. **Attention:** When you click **Reset IMM to factory defaults...**, all of the modifications that you made to the IMM2 are lost.
	Activation Key Management	The Activation Key Management page allows you to manage activation keys for optional IMM2 or server Features on Demand (FoD) features.

Chapter 3. Configuring the IMM2

Use the selections in the **IMM Management** tab to configure the IMM2.



From the Integrated Management Module (IMM) Properties page, you can perform the following functions:

- Firmware tab: access server firmware information
- Date and Time tab:
  - Choose IMM2 time setting method: manual or NTP
  - Set the IMM2 date and time for manual setting method
  - Set NTP information for NTP setting method
  - Set IMM2 timezone information
- Serial port tab:
  - Configure the IMM2 serial port
  - Set IMM2 CLI key sequences

From the User Accounts page, you can perform the following functions:

- Manage IMM2 user accounts:
  - Create a user account
  - Click on a user name to edit properties for that user:
    - Edit user name
    - Set user password
    - Configure SNMPv3 settings for the user
    - Manage SSH public authentication keys for the user
  - Delete a user account
- Configure global user login settings:
  - Set user authentication method
  - Set web inactivity timeout
  - Configure user account security levels available for the IMM2
- View users that are currently connected to the IMM2

From the Network Protocol Properties page, you can perform the following functions:

- Configure Ethernet settings:
  - Ethernet settings:
    - Host name
    - IPv4 and IPv6 enablement and address settings
  - Advanced Ethernet settings:
    - Autonegotiation enablement
    - MAC address management
    - Setting the maximum transmission unit (MTU)
- Configure SNMP settings:
  - SNMPv1 enablement and configuration:
    - Set contact information
    - SNMP traps enablement and configuration
    - Community management
  - SNMPv3 enablement and configuration:
    - Set contact information
    - User account configuration
- Configure DNS settings:
  - Set DNS addressing preference (IPv4 or IPv6)
  - Additional DNS server addressing enablement and configuration
- Configure DDNS settings:
  - DDNS enablement
  - Select domain name source (custom or DHCP server)
    - Set custom domain name for custom, manually specified source
    - View DHCP server specified domain name
- Configure SMTP settings:
  - Set SMTP server IP address or host name
  - Set SMTP server port number
  - Test the SMTP connection
- Configure LDAP settings:
  - Set LDAP server configuration (DNS or pre-configured)
    - If DNS specified LDAP server configuration, set the search domain:
      - Extract search domain from login ID
      - Manually specified search domain and service name
      - Attempt to extract search domain from login ID then use manually specified search domain and service name
    - If using a pre-configured LDAP server:
      - Set the LDAP server host name or IP address
      - Set the LDAP server port number
  - Set LDAP server root distinguished name
  - Set UID search attribute
  - Select binding method (anonymous, with configured credentials, with login credentials)
    - For configured credentials, set client distinguished name and password
  - Enhanced role-based security for Active Directory Users enablement:
    - If disabled:

        - Set group filter
        - Set group search attribute
        - Set login permission attribute
      - If enabled, set the server target name
- Configure Telnet settings:
  - Telnet access enablement
  - Set maximum number of Telnet sessions
- Configure USB settings:
  - Ethernet over USB enablement
  - External Ethernet to Ethernet over USB port forwarding enablement and management
- Configure Port Assignments:
  - View open port numbers
  - Set port numbers used by IMM2 services:
    - HTTP
    - HTTPS
    - Telnet CLI
    - SSH CLI
    - SNMP agent
    - SNMP Traps
    - Remote Control
    - CIM over HTTPS
    - CIM over HTTP

From the IMM Security page, you can perform the following functions:

- HTTPS server enablement and certificate management
- CIM over HTTPS enablement and certificate management
- LDAP security selection and certificate management
- SSH server enablement and certificate management

From the Manage the IMM Configuration page, you can perform the following functions:

- View an IMM2 configuration summary
- Backup or restore the IMM2 configuration
- View backup or restore status
- Reset the IMM2 configuration to its factory default settings
- Access the IMM2 initial setup wizard

From the Restart IMM page, you can reset the IMM2.

From the Reset IMM to factory defaults... page, you can reset the IMM2 configuration to its factory default settings.

From the Activation Key Management page, you can manage activation keys for optional IMM2 and server Features on Demand (FoD) features. See Chapter 4, “Features on Demand,” on page 17 for information about managing FoD activation keys.

Chapter 4. Features on Demand

IMM2 Features on Demand (FoD) allows you to install and manage optional server and systems management features.

There are multiple levels of IMM2 firmware functionality and features available for your server. The level of IMM2 firmware features installed on your server vary based on hardware type. For information about the type of IMM2 hardware and features in your server, see the documentation that came with the server.

You can upgrade IMM2 functionality by purchasing and installing an FoD activation key. For additional detailed information about FoD, see the *Features on Demand User's Guide* at http://www.ibm.com/systems/x/fod/.

To order an FoD activation key, contact your IBM representative or business partner or go to http://www.ibm.com/systems/x/fod/.

Use the IMM2 web interface or the IMM2 CLI to manually install an FoD activation key that lets you use an optional feature you have purchased. Before activating a key:

- The FoD activation key must be on the system that you are using to login to the IMM2.
- You must have ordered the FoD option and received its authorization code via mail or email.

See "Installing an activation key" or "Removing an activation key" on page 19 for information about managing an FoD activation key using the IMM2 web interface. See "keycfg command" on page 41 for information about managing an FoD activation key using the IMM2 CLI.

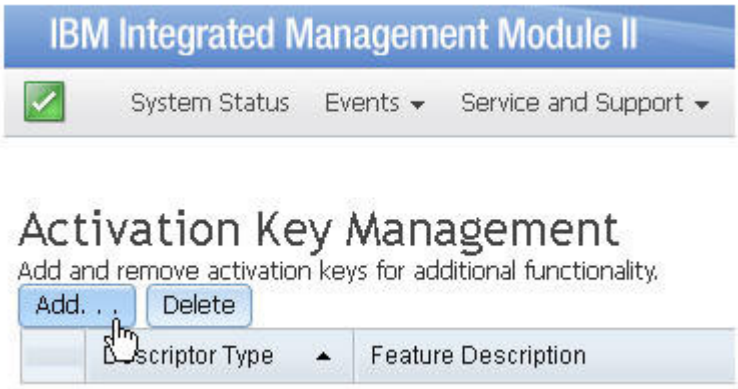
Installing an activation key

Install a Features on Demand (FoD) activation key to add an optional feature to your server.

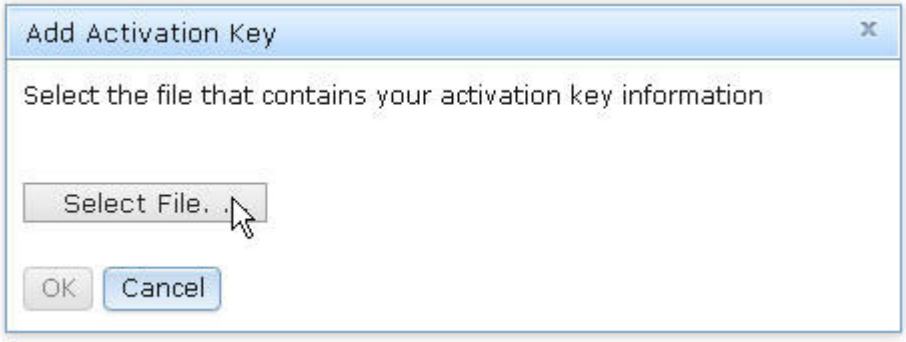
To install a FoD activation key, complete the following steps:

1. Log in to the IMM2. For more information, see "Logging in to the IMM2" on page 8.
2. From the IMM2 web interface, click on the **IMM Management** tab; then, click on **Activation Key Management**.

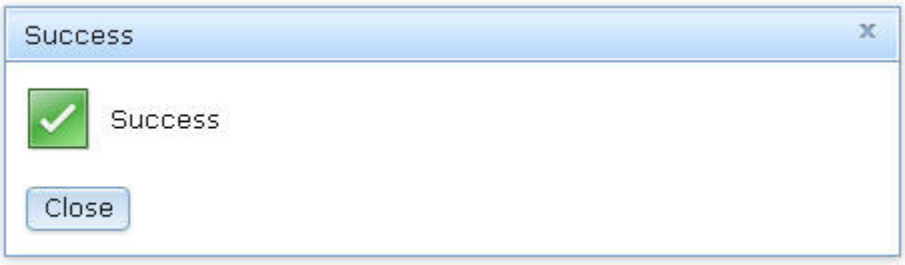
3. From the Activation Key Management page, click **Add...**.



4. In the Add Activation Key window, click **Select File...**; then, select the activation key file to add in the File Upload window and click **Open** to add the file or click **Cancel** to stop the installation. To finish adding the key, click **OK**, in the Add Activation Key window, or click **Cancel** to stop the installation.

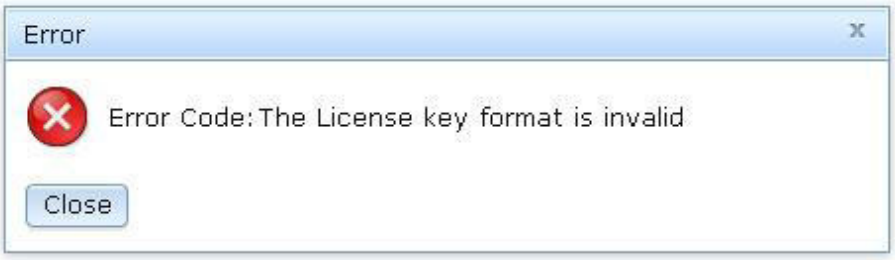


The Success window indicates that the activation key is installed.

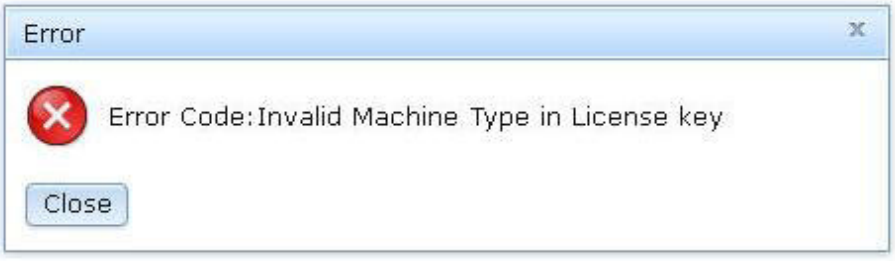


Note:

- If the activation key is not valid, you will see the following error window.

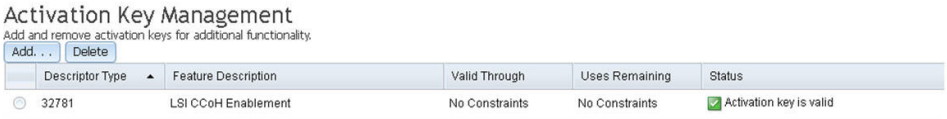


- If you are attempting to install the activation key on a machine type that does not support the FoD feature, you will see the following error window.



5. Click **OK**to close the Success window.

   The selected activation key is added to the server and appears in the Activation Key Management page.



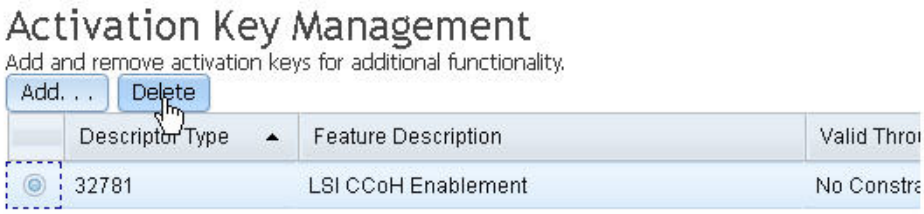
Removing an activation key

Remove a Features on Demand (FoD) activation key to delete an optional feature from your server.

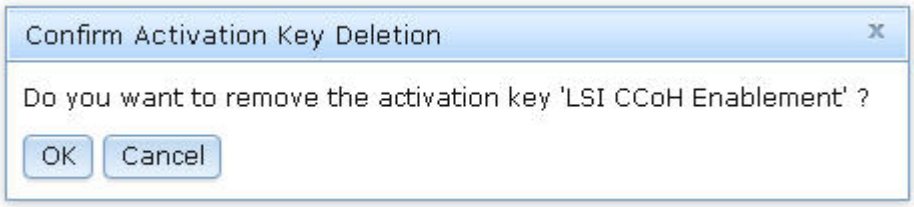
To remove a FoD activation key, complete the following steps:

1. Log in to the IMM2. For more information, see “Logging in to the IMM2” on page 8.
2. From the IMM2 web interface, click on the **IMM Management** tab; then, click on **Activation Key Management**.

3. From the Activation Key Management page, select the activation key to remove; then, click **Delete**.



4. In the Confirm Activation Key Deletion window, click **OK** to confirm activation key deletion or click **Cancel** to keep the key file.



The selected activation key is removed from the server and no longer appears in the Activation Key Management page.

Chapter 5. Command-line interface

Use the IMM2 command-line interface (CLI) to access the IMM2 without having to use the web interface. It provides a subset of the management functions that are provided by the web interface.

You can access the CLI through a Telnet or SSH session. You must be authenticated by the IMM2 before you can issue any CLI commands.

Managing the IMM2 with IPMI

The IMM2 comes with User ID 1 set initially to a user name of USERID and password of PASSW0RD (with a zero, not the letter O). This user has Supervisor access.

Important: Change this user name and password during your initial configuration for enhanced security.

The IMM2 also provides the following IPMI remote server management capabilities:

Command-line interfaces
The command-line interface provides direct access to server-management functions through the IPMI 2.0 protocol. You can use the IPMItool to issue commands to control server power, view server information, and identify the server. For more information about IPMItool, see "Using IPMItool."

Serial over LAN
To manage servers from a remote location, use the IPMItool to establish a Serial over LAN (SOL) connection. For more information about IPMItool, see "Using IPMItool."

Using IPMItool

IPMItool provides various tools that you can use to manage and configure an IPMI system. You can use IPMItool in-band or out-of-band to manage and configure the IMM2.

For more information about IPMItool, or to download IPMItool, go to http://sourceforge.net/.

Accessing the command line interface

To access the command line interface, start a Telnet or SSH session to the IMM2 IP address (see "Configuring serial-to-Telnet or SSH redirection" on page 22 for more information).

Logging in to the command-line session

To log in to the command line, complete the following steps:

1. Establish a connection with the IMM2.
2. At the user name prompt, type the user ID.
3. At the password prompt, type the password that you use to log in to the IMM2.

   You are logged in to the command line. The command-line prompt is `system>`. The command-line session continues until you type `exit` at the command line. Then you are logged off and the session is ended.

Configuring serial-to-Telnet or SSH redirection

Serial-to-Telnet or SSH redirection enables a system administrator to use the IMM2 as a serial terminal server. A server serial port can be accessed from a Telnet or SSH connection when serial redirection is enabled.

Notes:

1. The IMM2 allows a maximum of two open Telnet sessions. The Telnet sessions can access the serial ports independently so that multiple users can have a concurrent view of a redirected serial port.
2. The command-line interface **console 1** command is used to start a serial redirection session with the COM port.

Example session

```
telnet 192.168.70.125 (Press Enter.)
Connecting to 192.168.70.125...
username: USERID (Press Enter.)
password: ******** (Press Enter.)
system> console 1 (Press Enter.)
```

All traffic from COM2 is now routed to the Telnet session. All traffic from the Telnet or SSH session is routed to COM2.

```
ESC (
```

Type the exit key sequence to return to the command-line interface. In this example, press Esc and then type a left parenthesis. The CLI prompt displays to indicate return to the IMM2 CLI.

```
system>
```

Command syntax

Read the following guidelines before you use the commands:

- Each command has the following format:

  `command [arguments] [-options]`
- The command syntax is case sensitive.
- The command name is all lowercase.
- All arguments must immediately follow the command. The options immediately follow the arguments.
- Each option is always preceded by a hyphen (-). An option can be a short option (single letter) or a long option (multiple letters).
- If an option has an argument, the argument is mandatory, for example:

```
ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0
```

where **ifconfig** is the command, eth0 is an argument, and -i, -g, and -s are options. In this example, all three options have arguments.

- Brackets indicate that an argument or option is optional. Brackets are not part of the command that you type.

Features and limitations

The CLI has the following features and limitations:

- Multiple concurrent CLI sessions are allowed with different access methods (Telnet or SSH). At most, two Telnet command-line sessions can be active at any time.

  Note: The number of Telnet sessions is configurable; valid values are 0, 1, and 2. The value 0 means that the Telnet interface is disabled.
- One command is allowed per line (160-character limit, including spaces).
- There is no continuation character for long commands. The only editing function is the Backspace key to erase the character that you just typed.
- The Up Arrow and Down Arrow keys can be used to browse through the last eight commands. The **history** command displays a list of the last eight commands, which you can then use as a shortcut to execute a command, as in the following example:

```
MY IMM> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
MY IMM> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
MY IMM>
```

- In the command-line interface, the output buffer limit is 2 KB. There is no buffering. The output of an individual command cannot exceed 2048 characters. This limit does not apply in serial redirect mode (the data is buffered during serial redirect).
- The output of a command is displayed on the screen after the command has completed execution. This makes it impossible for commands to report real-time execution status. For example, in the verbose mode of the **flashing** command, the flashing progress is not shown in real time. It is shown after the command completes execution.
- Simple text messages are used to denote command execution status, as in the following example:

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```

- The command syntax is case sensitive.
- There must be at least one space between an option and its argument. For example, `ifconfig eth0 -i192.168.70.133` is incorrect syntax. The correct syntax is `ifconfig eth0 -i 192.168.70.133`.
- All commands have the `-h`, `-help`, and `?` options, which give syntax help. All of the following examples will give the same result:

```
system> power -h
system> power -help
system> power ?
```

- Some of the commands that are described in the following sections might not be available for your system configuration. To see a list of the commands that are supported by your configuration, use the help or ? option, as shown in the following examples:

```
system> help
system> ?
```

Alphabetical command listing

The complete list of all IMM2 CLI commands, in alphabetical order, is as follows:

Utility commands

The utility commands are as follows:

exit command

Use the **exit** command to log off and end the command-line interface session.

help command

Use the **help** command to display a list of all commands with a short description for each. You can also type **?** at the command prompt.

history command

Use the **history** command to display an indexed history list of the last eight commands that were issued. The indexes can then be used as shortcuts (preceded by !) to reissue commands from this history list.

Example:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Monitor commands

The monitor commands are as follows:

- "clearlog command"
- "fans command"
- "led command"
- "readlog command" on page 28
- "show command" on page 29
- "syshealth command" on page 29
- "temps command" on page 30
- "volts command" on page 30
- "vpd command" on page 31

clearlog command

Use the **clearlog** command to clear the event log of the IMM2. You must have the authority to clear event logs to use this command.

fans command

Use the **fans** command to display the speed for each of the server fans.

Example:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

led command

Use the **led** command to display and set LED states.

- Running the **led** command with no options displays the status of front panel LEDs.
- The **led -d** command option must be used with **led -identify on** command option.

The following table shows the arguments for the options.

Option	Description	Values
-l	Get status of all LEDs on system and its subcomponents	
-chklog	Turn off check log LED	Off
-identify	Change state of enclosure identify LED	Off, on, blink
-d	Turn on identification LED for specified time period	Time period (seconds)

Syntax:

```
led [options]
option:
  -l
  -chklog off
  -identify state
  -d time
```

Example:

```
system> led
Fault                Off
Identify             On            Blue
Chklog               Off
Power                Off

system> led -l
Label                Location                 State         Color
Battery              Planar                   Off
BMC Heartbeat        Planar                   Blink         Green
BRD                  Lightpath Card           Off
Channel A            Planar                   Off
Channel B            Planar                   Off
Channel C            Planar                   Off
Channel D            Planar                   Off
Channel E            Planar                   Off
Chklog               Front Panel              Off
CNFG                 Lightpath Card           Off
CPU                  Lightpath Card           Off
CPU 1                Planar                   Off
CPU 2                Planar                   Off
DASD                 Lightpath Card           Off
DIMM                 Lightpath Card           Off
DIMM 1               Planar                   Off
DIMM 10              Planar                   Off
DIMM 11              Planar                   Off
DIMM 12              Planar                   Off
DIMM 13              Planar                   Off
DIMM 14              Planar                   Off
DIMM 15              Planar                   Off
DIMM 16              Planar                   Off
DIMM 2               Planar                   Off
DIMM 3               Planar                   Off
DIMM 4               Planar                   Off
DIMM 5               Planar                   Off
DIMM 6               Planar                   Off
DIMM 7               Planar                   Off
DIMM 8               Planar                   Off
```

```
DIMM 9                Planar                  Off
FAN                   Lightpath Card          Off
FAN 1                 Planar                  Off
FAN 2                 Planar                  Off
FAN 3                 Planar                  Off
Fault                 Front Panel (+)         Off
Identify              Front Panel (+)         On            Blue
LINK                  Lightpath Card          Off
LOG                   Lightpath Card          Off
NMI                   Lightpath Card          Off
OVER SPEC             Lightpath Card          Off
PCI 1                 FRU                     Off
PCI 2                 FRU                     Off
PCI 3                 FRU                     Off
PCI 4                 FRU                     Off
Planar                Planar                  Off
Power                 Front Panel (+)         Off
PS                    Lightpath Card          Off
RAID                  Lightpath Card          Off
Riser 1               Planar                  Off
Riser 2               Planar                  Off
SAS ERR               FRU                     Off
SAS MISSING           Planar                  Off
SP                    Lightpath Card          Off
TEMP                  Lightpath Card          Off
VRM                   Lightpath Card          Off
system>
```

readlog command

Use the **readlog** command to display the IMM2 event log entries, five at a time. The entries are displayed from the most recent to the oldest.

readlog displays the first five entries in the event log, starting with the most recent, on its first execution, and then the next five for each subsequent call.

readlog -a displays all entries in the event log, starting with the most recent.

readlog -f resets the counter and displays the first 5 entries in the event log, starting with the most recent.

readlog -date *date* displays event log entries for the specified date, specified in mm/dd/yy format. It can be a pipe (|) separated list of dates.

readlog -sev *severity* displays event log entries for the specified severity level (E, W, I). It can be a pipe (|) separated list of severity levels.

readlog -i *ip_address* sets the IPv4 or IPv6 IP address of the TFTP or SFTP server where the event log is saved. The **-i** and **-l** command options are used together to specify the location.

readlog -l *filename* sets the file name of the event log file. The **-i** and **-l** command options are used together to specify the location.

readlog -pn *port_number* displays or sets the port number of the TFTP or SFTP server (default 69/22).

readlog -u *username* specifies the user name for the SFTP server.

readlog -pw *password* specifies the password for the SFTP server.

Syntax:

```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
```

```
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

Example:

```
system> readlog -f
1 I SERVPROC 12/18/03 10:18:58 Remote Login Successful.
Login ID:''USERID' CLI authenticated from 192.168.70.231 (Telnet).'
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.
Login ID: ''USERID' from web browser at IP@=192.168.70.231'
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

show command

Use the **show** command to display simple IMM settings.

- The **show** command displays values set using the **set** command.
- Settings are organized like a directory tree. Display the full tree using the **show -r** command option.
- Some of these settings, such as environment variables, are used by the command line interface.

The following table shows the arguments for the options.

Option	Description	Values
value	Path or setting value to display	
-r	Recursively display settings	

Syntax:

```
show [options]
option:
  value
  -r
```

syshealth command

Use the **syshealth** command to display a summary of the health of the server. The power state, system state, restart count, and IMM2 software status are displayed.

Example:

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

temps command

Use the **temps** command to display all the temperatures and temperature thresholds. The same set of temperatures are displayed as in the web interface.

Example:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
        WR      W      T     SS     HS
---------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
CPU2   58/14  72/22  80/27  85/29  90/32
DASD1  66/19  73/23  82/28  88/31  92/33
Amb    59/15  70/21  83/28  90/32  95/35
system>
```

Notes:

1. The output has the following column headings:
   - WR: warning reset
   - W: warning
   - T: temperature (current value)
   - SS: soft shutdown
   - HS: hard shutdown
2. All temperature values are in degrees Fahrenheit/Celsius.

volts command

Use the **volts** command to display all the voltages and voltage thresholds. The same set of voltages are displayed as in the web interface.

Example:

```
system> volts
      HSL   SSL   WL    WRL   V     WRH   WH   SSH    HSH
-----------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75  6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70  3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40 12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40 -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80 -2.70
VRM1                          3.45
VRM2                          5.45
system>
```

Note: The output has the following column headings:

- HSL: hard shutdown low
- SSL: soft shutdown low
- WL: warning low
- WRL: warning reset low
- V: voltage (current value)
- WRH: warning reset high
- WH: warning high
- SSH: soft shutdown high
- HSH: hard shutdown high

vpd command

Use the **vpd** command to display vital product data for the system (sys), IMM2 (imm), server BIOS (uefi), server Dynamic System Analysis Preboot (dsa), server firmware (fw), and server components (comp). The same information is displayed as in the web interface.

Syntax:

```
vpd [options]
option:
  -sys
  -imm
  -uefi
  -dsa
  -fw
  -comp
```

Example:

```
system> vpd -dsa
Type     Version      ReleaseDate
----     -------      -----------
dsa      D6YT19AUS    02/27/2009
system>
```

Server power and restart control commands

The server power and restart commands are as follows:

- "power command"
- "pxeboot command"
- "reset command" on page 32

power command

Use the **power** command to control the server power. To issue the **power** commands, you must have power and restart access authority.

power on turns on the server power.

power off turns off the server power. The **-s** option shuts down the operating system before the server is turned off.

power state displays the server power state (on or off) and the current state of the server.

power cycle turns off the server power and then turns on the power. The **-s** option shuts down the operating system before the server is turned off.

Syntax:

```
power on
power off [-s]
power state
power cycle [-s]
```

pxeboot command

Use the **pxeboot** command to display and set condition of the Preboot eXecution Environment.

Running **pxeboot** with no options, returns the current Preboot eXecution Environment setting. The following table shows the arguments for the options.

Option	Description	Values
-en	Sets Preboot eXecution Environment condition for next system restart	Enabled, disabled

Syntax:

```
pxeboot [options]
option:
  -en state
```

Example:

```
system> pxeboot
-en disabled
system>
```

reset command

Use the **reset** command to restart the server. To use this command, you must have power and restart access authority. The **-s** option shuts down the operating system before the server is restarted.

Syntax:

```
reset [option]
option:
-s
```

Serial redirect command

There is one serial redirect command: the "console command."

console command

Use the **console** command to start a serial redirect console session to the designated serial port of the IMM2.

Syntax:

```
console 1
```

Configuration commands

The configuration commands are as follows:

accseccfg command

Use the **accseccfg** command to display and configure account security settings.

Running the **accseccfg** command with no options displays all account security information. The following table shows the arguments for the options.

Option	Description	Values
-legacy	Sets account security to a predefined legacy set of defaults	
-high	Sets account security to a predefined high set of defaults	
-custom	Sets account security to user defined values	
-am	Sets user authentication method	Local, ldap, localldap, ldaplocal
-lp	Lockout period after maximum login failures (minutes)	0, 1, 2, 5, 10, 15, 20, 30, 60, 120, 180, or 240 minutes. The default value is 60 if "High Security" is enabled and 2 if "Legacy Security" is enabled. A value of zero disables this function.
-pe	Password expiration time period (days)	0 to 365 days
-pr	Password required	On, off
-pc	Password complexity rules	On, off
-pd	Password minimum number of different characters	0 to 19 characters
-pl	Password length	1 to 20 characters

Option	Description	Values
-ci	Minimum password change interval (hours)	0 to 240 hours
-lf	Maximum number of login failures	0 to 10
-chgdft	Change default password after first login	On, off
-chgnew	Change new user password after first login	On, off
-rc	Password reuse cycle	0 to 5
-wt	Web inactivity session timeout (minutes)	1, 5, 10, 15, 20, none, or user

Syntax:

```
accseccfg [options]
option:
  -legacy
  -high
  -custom
  -am authentication_method
  -lp lockout_period
  -pe time_period
  -pr state
  -pc state
  -pd number_characters
  -pl number_characters
  -ci minimum_interval
  -lf number_failures
  -chgdft state
  -chgnew state
  -rc reuse_cycle
  -wt timeout
```

Example:

```
system> accesscfg
-legacy
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgdft off
-chgnew off
-rc 0
-wt user
system>
```

alertcfg command

Use the **alertcfg** command to display and configure the IMM global remote alert parameters.

Running the **alertcfg** command with no options displays all global remote alert parameters. The following table shows the arguments for the options.

Option	Description	Values
-dr	Sets wait time between retries before the IMM resends an alert	0 to 4.0 minutes, in 0.5 minute increments
-da	Sets wait time before the IMM sends an alert to the next recipient in the list	0 to 4.0 minutes, in 0.5 minute increments
-rl	Sets the number of additional times that the IMM attempts to send an alert, if previous attempts were unsuccessful	0 to 8

Syntax:

```
alertcfg [options]
  options:
   -rl retry_limit
   -dr retry_delay
   -da agent_delay
```

Example:

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
system>
```

backup command

Use the **backup** command to create a backup file containing the current system security settings.

The following table shows the arguments for the options.

Option	Description	Values
-f	Backup file name	Valid file name
-pp	Password or pass-phrase used to encrypt passwords inside the backup file	Valid password or quote delimited pass-phrase
-ip	IP address of TFTP/SFTP server	Valid IP address
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	Username for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password

Option	Description	Values
-fd	Filename for XML description of backup CLI commands	Valid filename

Syntax:

```
backup [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -fd filename
```

Example:

```
system> backup –f imm-back.cli –pp xxxxxx –ip 192.168.70.200
ok
system>
```

dhcpinfo command

Use the **dhcpinfo** command to view the DHCP server-assigned IP configuration for eth0, if the interface is configured automatically by a DHCP server. You can use the **ifconfig** command to enable or disable DHCP.

Syntax:

```
dhcpinfo eth0
```

Example:

```
system> dhcpinfo eth0

-server : 192.168.70.29
-n     : IMM2A-00096B9E003A
-i     : 192.168.70.202
-g     : 192.168.70.29
-s     : 255.255.255.0
-d     : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6    : 0::0
-d6    : *
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>
```

The following table describes the output from the example.

Option	Description
-server	DHCP server that assigned the configuration
-n	Assigned host name
-i	Assigned IPv4 address
-g	Assigned gateway address

Option	Description
-s	Assigned subnet mask
-d	Assigned domain name
-dns1	Primary IPv4 DNS server IP address
-dns2	Secondary IPv4 DNS IP address
-dns3	Tertiary IPv4 DNS server IP address
-i6	IPv6 address
-d6	IPv6 domain name
-dns61	Primary IPv6 DNS server IP address
-dns62	Secondary IPv6 DNS IP address
-dns63	Tertiary IPv6 DNS server IP address

dns command

Use the **dns** command to view and set the DNS configuration of the IMM2.

Running the **dns** command with no options displays all DNS configuration information. The following table shows the arguments for the options.

Option	Description	Values
-state	DNS state	On, off
-ddns	DDNS state	Enabled, disabled
-i1	Primary IPv4 DNS server IP address	IP address in dotted decimal IP address format.
-i2	Secondary IPv4 DNS IP address	IP address in dotted decimal IP address format.
-i3	Tertiary IPv4 DNS server IP address	IP address in dotted decimal IP address format.
-i61	Primary IPv6 DNS server IP address	IP address in IPv6 format.
-i62	Secondary IPv6 DNS IP address	IP address in IPv6 format.
-i63	Tertiary IPv6 DNS server IP address	IP address in IPv6 format.
-p	IPv4/IPv6 priority	ipv4, ipv6

Syntax:

```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

Note: The following example shows an IMM2 configuration where DNS is enabled.

Example:

```
system> dns
-state  : enabled
-i1     : 192.168.70.202
-i2     : 192.168.70.208
-i3     : 192.168.70.212
-i61    : fe80::21a:64ff:fee6:4d5
-i62    : fe80::21a:64ff:fee6:4d6
-i63    : fe80::21a:64ff:fee6:4d7
-ddns   : enabled
-ddn    : ibm.com
-ddncur  : ibm.com
-dnsrc    : dhcp
-p     : ipv6

system>
```

The following table describes the output from the example.

Option	Description
-state	State of DNS (`on` or `off`)
-i1	Primary IPv4 DNS server IP address
-i2	Secondary IPv4 DNS IP address
-i3	Tertiary IPv4 DNS server IP address
-i61	Primary IPv6 DNS server IP address
-i62	Secondary IPv6 DNS IP address
-i63	Tertiary IPv6 DNS server IP address
-ddns	State of DDNS (`enabled` or `disabled`)
-dnsrc	Preferred DDNS domain name (`dhcp` or `manual`)
-ddn	Manually specified DDN
-ddncur	Current DDN (read only)
-p	Preferred DNS servers (`ipv4` or `ipv6`)

ethtousb command

Use the **ethtousb** command to display and configure Ethernet to Ethernet-over-USB port mapping.

The command allows you to map an external Ethernet port number to a different port number for Ethernet-over-USB.

Running the **ethtousb** command with no options displays Ethernet-over-USB information. The following table shows the arguments for the options.

Option	Description	Values
-en	Ethernet-over-USB state	Enabled, disabled

Option	Description	Values
-m*x*	Configure port mapping for index *x*	Port pair, separated by a colon (:), of the form *port1:port2*. Where: • The port index number, *x*, is specified as an integer from 1 to 10 in the command option. • *port1* of the port pair is the External Ethernet port number. • *port2* of the port pair is the Ethernet-over-USB port number.
-rm	Remove port mapping for specified index	1 through 10. Port map indexes are displayed using the **ethtousb** command with no options.

Syntax:

```
ethtousb [options]
option:
  -en state
  -mx port_pair
  -rm map_index
```

Example:

```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

ifconfig command

Use the **ifconfig** command to configure the Ethernet interface. Type `ifconfig eth0` to display the current Ethernet interface configuration. To change the Ethernet interface configuration, type the options, followed by the values. To change the interface configuration, you must have at least Adapter Networking and Security Configuration authority.

The following table shows the arguments for the options.

Option	Description	Values
-state	Interface state	disabled, enabled
-c	Configuration method	dhcp, static, dthens (dthens corresponds to the **try dhcp server, if it fails use static config** option on the web interface)
-i	Static IP address	Address in valid format
-g	Gateway address	Address in valid format
-s	Subnet mask	Address in valid format
-n	Host name	String of up to 63 characters. The string can include letters, digits, periods, underscores, and hyphens.

Option	Description	Values
-r	Data rate	10, 100, auto
-d	Duplex mode	full, half, auto
-m	MTU	Numeric between 60 and 1500
-l	LAA	MAC address format. Multicast addresses are not allowed (the first byte must be even).
-dn	Domain name	Domain name in valid format
-auto	Autonegotiation setting, which determines whether the Data rate and Duplex network settings are configurable	true, false
-nic	NIC access	Shared, dedicated
-address_table	Table of automatically-generated IPv6 addresses and their prefix lengths **Note:** The option is visible only if IPv6 and stateless auto-configuration are enabled.	This value is read-only and is not configurable
-ipv6	IPv6 state	disabled, enabled
-lla	Link-local address **Note:** The link-local address only appears if IPv6 is enabled.	The link-local address is determined by the IMM2. This value is read-only and is not configurable.
-ipv6static	Static IPv6 state	disabled, enabled
-i6	Static IP address	Static IP address for Ethernet channel 0 in IPv6 format
-p6	Address prefix length	Numeric between 1 and 128
-g6	Gateway or default route	IP address for the gateway or default route for Ethernet channel 0 in IPv6
-dhcp6	DHCPv6 state	disabled, enabled
-sa6	IPv6 stateless autoconfig state	disabled, enabled

Syntax:

```
ifconfig eth0 [options]
options:
  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
  -l locally_administered_MAC
  -dn domain_name
  -auto state
  -nic state
```

```
  -address_table
  -ipv6 state
  -ipv6static state
  -sa6 state
  -i6 static_ipv6_ip_address
  -g6 ipv6_gateway_address
  -p6 length
```

Example:

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM2.
system>
```

Note: The **-b** option in the ifconfig display is for the burned-in MAC address. The burned-in MAC address is read-only and is not configurable.

keycfg command

Use the **keycfg** command to display, add, or delete activation keys. These keys control access to optional IMM2 Features on Demand (FoD) features.

- When **keycfg** is run without any options, the list of installed activation keys is displayed. Key information displayed includes an index number for each activation key, the type of activation key, the date through which the key is valid, the number of uses remaining, the key status, and a key description.
- Add new activation keys through file transfer.
- Delete old keys by specifying the number of the key or the type of key. When deleting keys by type, only the first key of a given type is deleted.

The following table shows the arguments for the options.

Option	Description	Values
-add	Add activation key	Values for the -ip, -pn, -u, -pw, and -f command options.
-ip	IP address of TFTP server with activation key to add	Valid IP address for TFTP server.
-pn	Port number for TFTP/SFTP server with activation key to add	Valid port number for TFTP/SFTP server (default 69/22).
-u	User name for SFTP server with activation key to add	Valid user name for SFTP server.
-pw	Password for SFTP server with activation key to add	Valid password for SFTP server.

Option	Description	Values
-f	File name for activation key to add	Valid file name for activation key file.
-del	Delete activation key by index number	Valid activation key index number from **keycfg** listing.
-deltype	Delete activation key by key type	Valid key type value.

Syntax:

```
keycfg [options]
option:
  -add
     -ip ip_address
     -pn port_number
     -u username
     -pw password
     -f filename
  -del key_index
  -deltype key_type
```

Example:

```
system> keycfg
ID  Type  Valid         Uses  Status   Description
1   4     10/10/2010    5     "valid"  "IMM remote presence"
2   3     10/20/2010    2     "valid"  "IMM feature"
system>
```

ldap command

Use the **ldap** command to display and configure the LDAP protocol configuration parameters.

The following table shows the arguments for the options.

Option	Description	Values
-a	User authentication method	Local only, LDAP only, local first then LDAP, LDAP first then local
-b	Binding method	Anonymous, bind with ClientDN and password, user principal bind (UPN)
-c	Client distinguished name	String of up to 63 characters for *client_dn*
-d	Search domain	String of up to 31 characters for *search_domain*
-f	Group filter	String of up to 63 characters for *group_filter*
-g	Group search attribute	String of up to 63 characters for *group_search_attr*
-l	Login permission attribute	String of up to 63 characters for *string*
-m	Domain source	Extract search domain from login ID, use only configured search domain, try login first then configured value
-n	Service name	String of up to 15 characters for *service_name*
-p	Client password	String of up to 15 characters for *client_pw*

Option	Description	Values
-pc	Confirm client password	String of up to 15 characters for *confirm_pw* Command usage is: ldap -p *client_pw* -pc *confirm_pw* This option is required when you change the client password. It compares the *confirm_pw* argument with the *client_pw* argument, and the command will fail if they do not match.
-r	Root entry distinguished name (DN)	String of up to 63 characters for *root_dn*
s1ip	Server 1 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s2ip	Server 2 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s3ip	Server 3 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s4ip	Server 4 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s1pn	Server 1 port number	A numeric port number up to 5 digits for *port_number.*
s2pn	Server 2 port number	A numeric port number up to 5 digits for *port_number.*
s3pn	Server 3 port number	A numeric port number up to 5 digits for *port_number.*
s4pn	Server 4 port number	A numeric port number up to 5 digits for *port_number.*
-u	UID search attribute	String of up to 23 characters for *search_attrib*
-v	Get LDAP server address through DNS	Off, on
-ep	Password for backup and restore encryption	Valid password string
-h	Displays the command usage and options	

Syntax:

```
ldap [options]
options:
   -a loc|ldap|locId|Idloc
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -g group_search_attr
   -l string
   -m login|cfg|lthenc
   -n service_name
   -p client_pw
   -pc confirm_pw
   -r root_dn
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s4ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -s4pn port_number
```

```
-u search_attrib
-v off|on
-ep password
-h
```

ntp command

Use the **ntp** command to display and configure the Network Time Protocol (NTP).

The following table shows the arguments for the options.

Option	Description	Values
-en	Enables or disables the Network Time Protocol	Enabled, disabled
-i	Name or IP address of the Network Time Protocol server	The name of the NTP server to be used for clock synchronization.
-f	The frequency (in minutes) that the IMM2 clock is synchronized with the Network Time Protocol server	3 - 1440 minutes
-synch	Requests an immediate synchronization with the Network Time Protocol server	No values are used with this parameter.

Syntax:

```
ntp [options]
options:
-en state
-i  hostname
-f  frequency
-synch
```

Example:

```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

passwordcfg command

Use the **passwordcfg** command to display and configure the password parameters.

Option	Description
-legacy	Sets account security to a predefined legacy set of defaults
-high	Sets account security to a predefined high set of defaults
-exp	Maximum password age (0 - 365 days). Set to 0 for no expiration.
-cnt	Number of previous passwords that cannot be reused (0 - 5)
-nul	Allows accounts with no password (yes | no)
-h	Displays the command usage and options

Syntax:

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Example:

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

ports command

Use the **ports** command to display and configure IMM ports.

Running the **ports** command with no options displays information for all IMM ports. The following table shows the arguments for the options.

Option	Description	Values
-open	Display open ports	
-reset	Reset ports to default settings	
-httpp	HTTP port number	Default port number: 80
-httpsp	HTTPS port number	Default port number: 443
-telnetp	Telnet legacy CLI port number	Default port number: 23
-sshp	SSH legacy CLI port number	Default port number: 22
-snmpap	SNMP agent port number	Default port number: 161
-snmptp	SNMP traps port number	Default port number: 162
-rpp	Remote presence port number	Default port number: 3900
-cimhp	CIM over HTTP port number	Default port number: 5988
-cimhsp	CIM over HTTPS port number	Default port number: 5989

Syntax:

```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -telnetp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Example:

```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-telnetp 23
-cimhp 5988
-cimhsp 5989
system>
```

portcfg command

Use the **portcfg** command to configure the IMM for the serial redirection feature.

The IMM must be configured to match the server internal serial port settings. To change the serial port configuration, type the options, followed by the values. To change the serial port configuration, you must have at least Adapter Networking and Security Configuration authority.

Note: The server external serial port can only be used by the IMM for IPMI functionality. The command-line interface is not supported through the serial port. The **serred** and **cliauth** options that were present in the Remote Supervisor Adapter II command line interface are not supported.

Running the **portcfg** command with no options displays serial port configuration. The following table shows the arguments for the options.

Note: The number of data bits (8) is set in the hardware and cannot be changed.

Option	Description	Values
-b	Baud rate	9600, 19200, 38400, 57600, 115200
-p	Parity	None, odd, even
-s	Stop bits	1, 2
-climode	CLI mode	0, 1, 2 Where: • 0 = none: The command-line interface is disabled • 1 = cliems: The command-line interface is enabled with EMS-compatible keystroke sequences • 2 = cliuser: The command-line interface is enabled with user-defined keystroke sequences

Syntax:

```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

Example:

```
system> portcfg
-b       :    57600
-climode :    2 (CLI with user defined keystroke sequence)
-p  :    even
-s       :    1
system> portcfg -b 38400
ok
system>
```

restore command

Use the **restore** command to restore system settings from a backup file.

The following table shows the arguments for the options.

Option	Description	Values
-f	Backup file name	Valid file name
-pp	Password or pass-phrase used to encrypt passwords inside the backup file	Valid password or quote delimited pass-phrase
-ip	IP address of TFTP/SFTP server	Valid IP address
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	Username for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password

Syntax:

```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Example:

```
system> restore –f imm-back.cli –pp xxxxxx –ip 192.168.70.200
ok
system>
```

restoredefaults command

Use the **restoredefaults** command to restore all IMM settings to the factory default.

- There are no options for the **restoredefaults** command.
- You will be asked to confirm the command before it is processed.

Syntax:

```
restoredefaults
```

Example:

```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults...
```

set command

Use the **set** command to change IMM settings.

- Some IMM settings can be changed with a simple **set** command.
- Some of these settings, such as environment variables, are used by the command line interface.
- Use the **show** command to display values set using the **set** command.

The following table shows the arguments for the options.

Option	Description	Values
value	Set value for specified path or setting	Appropriate value for specified path or setting.

Syntax:

```
set [options]
option:
  value
```

smtp command

Use the **smtp** command to display and configure settings for the SMTP interface.

Running the **smtp** command with no options displays all SMTP interface information. The following table shows the arguments for the options.

Option	Description	Values
-s	SMTP server IP address or hostname	Valid IP address or hostname (63 character limit).
-pn	SMTP port number	Valid port number.

Syntax:

```
smtp [options]
option:
  -s ip_address_or_hostname
  -pn port_number
```

Example:

```
system> smtp
-s test.com
-pn 25
system>
```

snmp command

Use the **snmp** command to display and configure SNMP interface information.

Running the **snmp** command with no options displays all SNMP interface information. The following table shows the arguments for the options.

Option	Description	Values
-a	SNMPv1 agent	On, off **Note:** To enable the SNMPv1 agent, the following criteria must be met: • IMM contact specified using the -cn command option. • IMM location specified using the -l command option. • At least one SNMP community name specified using the one of the -c*x* command options. • At least one valid IP address is specified for each SNMP community using the one of the -c*xiy* command options.
-a3	SNMPv3 agent	On, off **Note:** To enable the SNMPv3 agent, the following criteria must be met: • IMM contact specified using the -cn command option. • IMM location specified using the -l command option.
-t	SNMP traps	On, off
-l	IMM location	String (limited to 47 characters). **Note:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear the IMM location by specifying no argument or by specifying an empty string as the argument, such as "".
-cn	IMM contact name	String (limited to 47 characters). **Note:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear the IMM contact name by specifying no argument or by specifying an empty string as the argument, such as "".

Option	Description	Values
-c*x*	SNMP community *x* name	String (limited to 15 characters). **Note:** • *x* is specified as 1, 2, or 3 in the command option to indicate the community number. • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear an SNMP community name by specifying no argument or by specifying an empty string as the argument, such as "".
-c*x*i*y*	SNMP community *x* IP address or hostname *y*	Valid IP address or hostname (limited to 63 characters). **Note:** • *x* is specified as 1, 2, or 3 in the command option to indicate the community number. • *y* is specified as 1, 2, or 3 in the command option to indicate the IP address or hostname number. • An IP address or hostname can only contain dots, underscores, minus signs, letters and digits. No embedded spaces or consecutive periods are allowed. • Clear an SNMP community IP address or hostname by specifying no argument.
-ca*x*	SNMPv3 community *x* access type	Get, set, trap **Note:** *x* is specified as 1, 2, or 3 in the command option to indicate the community number.

Syntax:

```
snmp [options]
option:
  -a state
  -a3 state
  -t state
  -l location
  -cn contact_name
  -c1 snmp_community_1_name
  -c2 snmp_community_2_name
  -c3 snmp_community_3_name
  -c1i1 community_1_ip_address_or_hostname_1
  -c1i2 community_1_ip_address_or_hostname_2
  -c1i3 community_1_ip_address_or_hostname_3
  -c2i1 community_2_ip_address_or_hostname_1
  -c2i2 community_2_ip_address_or_hostname_2
  -c2i3 community_2_ip_address_or_hostname_3
  -c3i1 community_3_ip_address_or_hostname_1
  -c3i2 community_3_ip_address_or_hostname_2
  -c3i3 community_3_ip_address_or_hostname_3
  -ca1 community_1_access_type
  -ca2 community_2_access_type
  -ca3 community_3_access_type
```

Example:

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l RTC,NC
```

```
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-ca1 set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>
```

snmpalerts command

Use the **snmpalerts** command to manage alerts sent via SNMP.

Running **snmpalerts** with no options displays all SNMP alert settings. The following table shows the arguments for the options.

Option	Description	Values
-status	SNMP alert status	On, off
-crt	Sets critical events that send alerts	All, none, custom:te | vo | po | di | fa | cp | me | in | re | ot Custom critical alert settings are specified using a pipe separated list of values of the form **snmpalerts -crt custom:te | vo**, where custom values are: • te: critical temperature threshold exceeded • vo: critical voltage threshold exceeded • po: critical power failure • di: hard disk drive failure • fa: fan failure • cp: microprocessor failure • me: memory failure • in: hardware incompatibility • re: power redundancy failure • ot: all other critical events
-crten	Send critical event alerts	Enabled, disabled

Option	Description	Values
-wrn	Sets warning events that send alerts	All, none, custom:rp | te | vo | po | fa | cp | me | ot Custom warning alert settings are specified using a pipe separated list of values of the form **snmpalerts -wrn custom:rp | te**, where custom values are: • rp: power redundancy warning • te: warning temperature threshold exceeded • vo: warning voltage threshold exceeded • po: warning power threshold exceeded • fa: non-critical fan event • cp: microprocessor in degraded state • me: memory warning • ot: all other warning events
-wrnen	Send warning event alerts	Enabled, disabled
-sys	Sets routine events that send alerts	All, none, custom:lo | tio | ot | po | bf | til | pf | el | ne Custom routine alert settings are specified using a pipe separated list of values of the form **snmpalerts -sys custom:lo | tio**, where custom values are: • lo: successful remote login • tio: operating system timeout • ot: all other informational and system events • po: system power on/off • bf: operating system boot failure • til: operating system loader watchdog timeout • pf: predicted failure (PFA) • el: event log 75% full • ne: network change
-sysen	Send routine event alerts	Enabled, disabled

Syntax:

```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

srcfg command

Use the **srcfg** command to configure the key sequence to end the serial redirection function. To change the serial redirect configuration, type the options, followed by the values. To change the serial redirect configuration, you must have at least Adapter Networking and Security Configuration authority.

Note: The IMM hardware does not provide for a serial port to serial port pass-through capability. Therefore the `-passthru` and `exitcliseq` options which are present in the Remote Supervisor Adapter II command line interface are not supported.

Running the **srcfg** command with no options displays the current serial redirection keystroke sequence. The following table shows the arguments for the `srcfg -exitcliseq` command option.

Option	Description	Values
-exitcliseq	Exit a command-line interface keystroke sequence	User-defined keystroke sequence to exit the CLI. **Note:** This sequence must have at least one character and at most 15 characters. The caret symbol (^) has a special meaning in this sequence. It denotes Ctrl for keystrokes that map to Ctrl sequences (for example, ^[for the escape key and ^M for carriage return). All occurrences of ^ are interpreted as part of a Ctrl sequence. Refer to an ASCII-to-key conversion table for a complete list of Ctrl sequences. The default value for this field is ^[(which is Esc followed by (.

Syntax:

```
srcfg [options]
options:
-exitcliseq exitcli_keyseq
```

Example:

```
system> srcfg
-exitcliseq ^[Q
system>
```

sshcfg command

Use the **sshcfg** command to display and configure SSH parameters.

Running the **sshcfg** command with no options displays all SSH parameters. The following table shows the arguments for the options.

Option	Description	Values
-cstatus	State of SSH CLI	Enabled, disabled
-hk gen	Generate SSH server private key	
-hk rsa	Display server RSA public key	

Syntax:

```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

Example:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

ssl command

Use the **ssl** command to display and configure the Secure Sockets Layer (SSL) parameters.

Note: Before you can enable an SSL client, a client certificate must be installed.

Running the **ssl** command with no options displays SSL parameters. The following table shows the arguments for the options.

Option	Description	Values
-ce	Enables or disables an SSL client	On, off
-se	Enables or disables an SSL server	On, off
-cime	Enables or disables CIM over HTTPS on the SSL server	On, off

Syntax:

```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

Parameters: The following parameters are presented in the option status display for the **ssl** command and are output only from the command-line interface:

Server secure transport enable
This status display is read-only and cannot be set directly.

Server Web/CMD key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL server CSR key status
This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client LDAP key status

This status display is read-only and cannot be set directly. Possible command line output values are as follows as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client CSR key status

This status display is read-only and cannot be set directly. Possible command line output values are as follows:

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

sslcfg command

Use the **sslcfg** command to display and configure SSL for the IMM and manage certificates.

Running the **sslcfg** command with no options displays all SSL configuration information. The following table shows the arguments for the options.

Option	Description	Values
-server	SSL server status	Enabled, disabled **Note:** The SSL server can be enabled only if a valid certificate is in place.
-client	SSL client status	Enabled, disabled **Note:** The SSL client can be enabled only if a valid server or client certificate is in place.
-cim	CIM over HTTPS status	Enabled, disabled **Note:** CIM over HTTPS can be enabled only if a valid server or client certificate is in place.
-cert	Generate self-signed certificate	Server, client, sysdir **Note:** • Values for the **-c**, **-sp**, **-cl**, **-on**, and **-hn** command options are required when generating a self-signed certificate. • Values for the **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, and **-dq** command options are optional when generating a self-signed certificate.
-csr	Generate CSR	Server, client, sysdir **Note:** • Values for the **-c**, **-sp**, **-cl**, **-on**, and **-hn** command options are required when generating a CSR. • Values for the **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd**, and **-un** command options are optional when generating a CSR.

Option	Description	Values
-i	IP address for TFTP/SFTP server	Valid IP address **Note:** An IP address for the TFTP or SFTP server must be specified when uploading a certificate, or downloading a certificate or CSR.
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22).
-u	User name for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password
-l	Certificate filename	Valid filename. **Note:** A filename is required when downloading or uploading a certificate or CSR. If no filename is specified for a download, the default name for the file is used and displayed.
-dnld	Download certificate file	This option takes no arguments, but must also specify values for the **-cert** or **-csr** command option (depending on the certificate type being downloaded), the **-i** command option, and **-l** (optional) command option.
-upld	Imports certificate file	This option takes no arguments, but must also specify values for the **-cert**, **-i**, and **-l** command options.
-tc*x*	Trusted certificate *x* for SSL client	Import, download, remove **Note:** The trusted certificate number, *x*, is specified as an integer from 1 to 3 in the command option.
-c	Country	Country code (2 letters) **Note:** Required when generating a self-signed certificate or CSR.
-sp	State or province	Quote-delimited string (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-cl	City or locality	Quote-delimited string (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-on	Organization name	Quote-delimited string (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-hn	IMM hostname	String (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-cp	Contact person	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-ea	Contact person email address	Valid email address (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-ou	Organizational unit	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-s	Surname	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.

Option	Description	Values
-gn	Given name	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-in	Initials	Quote-delimited string (maximum 20 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-dq	Domain name qualifier	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a self-signed certificate or CSR.
-cpwd	Challenge password	String (minimum 6 characters, maximum 30 characters) **Note:** Optional when generating a CSR.
-un	Unstructured name	Quote-delimited string (maximum 60 characters) **Note:** Optional when generating a CSR.

Syntax:

```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
  -i ip_address
  -pn port_number
  -u username
  -pw password
  -l filename
  -dnld
  -upld
  -tcx action
  -c country_code
  -sp state_or_province
  -cl city_or_locality
  -on organization_name
  -hn imm_hostname
  -cp contact_person
  -ea email_address
  -ou organizational_unit
  -s surname
  -gn given_name
  -in initials
  -dq dn_qualifier
  -cpwd challenge_password
  -un unstructured_name
```

Example:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
```

```
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
system>
```

telnetcfg command

Use the **telnetcfg** command to display and configure Telnet settings.

Running the **telnetcfg** command with no options displays Telnet state. The following table shows the arguments for the options.

Option	Description	Values
-en	Telnet state	Disabled, 1, 2 **Note:** If not disabled, Telnet is enabled for either one or two users.

Syntax:

```
telnetcfg [options]
option:
  -en state
```

Example:

```
system> telnetcfg
-en 1
system>
```

thermal command

Use the **thermal** command to display and configure the thermal mode policy of the host system.

Running the **thermal** command with no options displays the thermal mode policy. The following table shows the arguments for the options.

Option	Description	Values
-mode	Thermal mode selection	Normal, performance

Syntax:

```
thermal [options]
option:
  -mode thermal_mode
```

Example:

```
system> thermal
-mode normal
system>
```

timeouts command

Use the **timeouts** command to display the timeout values or change them. To display the timeouts, type `timeouts`. To change timeout values, type the options followed by the values. To change timeout values, you must have at least Adapter Configuration authority.

The following table shows the arguments for the timeout values. These values match the graduated scale pull-down options for server timeouts on the web interface.

Option	Timeout	Units	Values
-o	Operating system timeout	minutes	disabled, 2.5, 3, 3.5, 4
-l	Loader timeout	minutes	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120

Syntax:

```
timeouts [options]
options:
-o OS_watchdog_option
-l loader_watchdog_option
```

Example:

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
```

usbeth command

Use the **usbeth** command to enable or disable the in-band LAN over USB interface.

Syntax:

```
usbeth [options]
options:
-en <enabled|disabled>
```

Example:

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

users command

Use the **users** command to access all user accounts and their authority levels and to create new user accounts and modify existing accounts.

Running the **users** command with no options displays a list of users and some basic user information. The following table shows the arguments for the options.

Option	Description	Values
-user_index	User account index number	1 through 12, inclusive, or `all` for all users

Option	Description	Values
-n	User account name	Unique string containing only numbers, letters, periods, and underscores. Minimum of 4 characters and maximum of 16 characters.
-p	User account password	String that contains at least one alphabetic and one non-alphabetic character. Minimum of 6 characters and maximum of 20 characters. Null creates an account without a password that the user must set during their first login.
-a	User authority level	Super, ro, custom Where: • `super` (supervisor) • `ro` (read only) • `custom` is followed by a colon and list of values that are separated by a pipe (`|`), of the form `custom:am|rca`. These values can be used in any combination. `am` (user account management access) `rca` (remote console access) `rcvma` (remote console and virtual media access) `pr` (remote server power/restart access) `cel` (ability to clear event logs) `bc` (adapter configuration - basic) `nsc` (adapter configuration - network and security) `ac` (Adapter configuration - advanced)
-ep	Encryption password (for backup/restore)	Valid password
-clear	Erase specified user account	User account index number to erase must be specified, following the form: `users -clear -`*`user_index`*
-curr	Display users currently logged in	
-sauth	SNMPv3 authentication protocol	HMAC-MD5, HMAC-SHA, none
-spriv	SNMPv3 privacy protocol	CBC-DES, AES, none
-spw	SNMPv3 privacy password	Valid password
-sepw	SNMPv3 privacy password (encrypted)	Valid password
-sacc	SNMPv3 access type	Get, set
-strap	SNMPv3 trap hostname	Valid hostname

Option	Description	Values
-pk	Display SSH public key for user	User account index number. **Note:** • Each SSH key assigned to the user is displayed, along with an identifying key index number. • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk`. • All keys are in OpenSSH format.
-e	Display entire SSH key in OpenSSH format *(SSH public key option)*	This option takes no arguments and must be used exclusive of all other `users -pk` options. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -e`.
-remove	Remove SSH public key from user *(SSH public key option)*	Public key index number to remove must be given as a specific *-key_index* or `-all` for all keys assigned to the user. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -remove -1`.
-add	Add SSH public key for user *(SSH public key option)*	Quote-delimited key in OpenSSH format **Note:** • The `-add` option is used exclusive of all other `users -pk` command options. • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E+mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N50R6MbNcwlsx+mTEAvvcpJhug a70UNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="`
-upld	Upload an SSH public key *(SSH public key option)*	Requires the `-i` and `-l` options to specify key location. **Note:** • The `-upld` option is used exclusive of all other `users -pk` command options (except for `-i` and `-l`). • To replace a key with a new key, you must specify a *-key_index*. To add a key to the end of the list of current keys, do not specify a key index. • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`.

Option	Description	Values
-dnld	Download the specified SSH public key *(SSH public key option)*	Requires a *-key_index* to specify the key to download and the `-i` and `-l` options to specify the download location on another computer running a TFTP server. **Note:** • The `-dnld` option is used exclusive of all other `users -pk` command options (except for `-i`, `-l`, and *-key_index*). • When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
-i	IP address of TFTP/SFTP server for uploading or downloading a key file *(SSH public key option)*	Valid IP address **Note:** The `-i` option is required by the `users -pk -upld` and `users -pk -dnld` command options.
-pn	Port number of TFTP/SFTP server *(SSH public key option)*	Valid port number (default 69/22) **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-u	User name for SFTP server *(SSH public key option)*	Valid user name **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-pw	Password for SFTP server *(SSH public key option)*	Valid password **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-l	File name for uploading or downloading a key file via TFTP *(SSH public key option)*	Valid file name **Note:** The `-l` option is required by the `users -pk -upld` and `users -pk -dnld` command options.
-af	Accept connections from host *(SSH public key option)*	A comma-separated list of hostnames and IP addresses, limited to 511 characters. Valid characters include: alphanumeric, comma, asterisk, question mark, exclamation point, period, hyphen, colon and percent sign.
-cm	Comment *(SSH public key option)*	Quote-delimited string of up to 255 characters. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (*-userindex* option), of the form: `users -2 -pk -cm "This is my comment."`.

Syntax:

```
users [options]
 options:
   -user_index
   -n username
   -p password
   -a authority_level
   -ep encryption_password
   -clear
```

```
   -curr
   -sauth protocol
   -spriv protocol
   -spw password
   -sepw password
   -sacc state
   -strap hostname
users -pk [options]
 options:
   -e
   -remove index
   -add key
   -upld
   -dnld
   -i ip_address
   -pn port_number
   -u username
   -pw password
   -l filename
   -af list
   -cm comment
```

Example:

```
system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
4.  <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSW0RD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID  Read/Write
Password Expires: no expiration
2. test    Read/Write
Password Expires: no expiration
3. test2   Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest  custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>
```

IMM control commands

The IMM control commands are as follows:

- "info command" on page 68
- "resetsp command" on page 68

alertentries command

Use the **alertentries** command to manage alert recipients.

- **alertentries** with no options displays all alert entry settings.
- **alertentries -number -test** generates a test alert to the given recipient index number.
- **alertentries -number** (where number is 0-12) displays alert entry settings for the specified recipient index number or allows you to modify the alert settings for that recipient.

The following table shows the arguments for the options.

Option	Description	Values
-number	Alert recipient index number to display, add, modify, or delete	1 through 12
-status	Alert recipient status	On, off
-type	Alert type	Email, syslog
-log	Include event log in alert email	On, off
-n	Alert recipient name	String
-e	Alert recipient email address	Valid email address
-ip	Syslog IP address or hostname	Valid IP address or hostname
-pn	Syslog port number	Valid port number
-del	Delete specified recipient index number	
-test	Generate a test alert to specified recipient index number	
-crt	Sets critical events that send alerts	All, none, custom:te | vo | po | di | fa | cp | me | in | re | ot Custom critical alert settings are specified using a pipe separated list of values of the form **alertentries -crt custom:te | vo**, where custom values are: • te: critical temperature threshold exceeded • vo: critical voltage threshold exceeded • po: critical power failure • di: hard disk drive failure • fa: fan failure • cp: microprocessor failure • me: memory failure • in: hardware incompatibility • re: power redundancy failure • ot: all other critical events

Option	Description	Values
-crten	Send critical event alerts	Enabled, disabled
-wrn	Sets warning events that send alerts	All, none, custom:rp|te|vo|po|fa|cp|me|ot Custom warning alert settings are specified using a pipe separated list of values of the form **alertentries -wrn custom:rp|te**, where custom values are: • rp: power redundancy warning • te: warning temperature threshold exceeded • vo: warning voltage threshold exceeded • po: warning power threshold exceeded • fa: non-critical fan event • cp: microprocessor in degraded state • me: memory warning • ot: all other warning events
-wrnen	Send warning event alerts	Enabled, disabled
-sys	Sets routine events that send alerts	All, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Custom routine alert settings are specified using a pipe separated list of values of the form **alertentries -sys custom:lo|tio**, where custom values are: • lo: successful remote login • tio: operating system timeout • ot: all other informational and system events • po: system power on/off • bf: operating system boot failure • til: operating system loader watchdog timeout • pf: predicted failure (PFA) • el: event log 75% full • ne: network change
-sysen	Send routine event alerts	Enabled, disabled

Syntax:

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
      -wrn event_type
      -wrnen state
      -sys event_type
      -sysen state
```

Example:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

batch command

Use the **batch** command executes one or more CLI commands that are contained in a file.

- Comment lines in the batch file begin with a #.
- When running a batch file, commands that fail are returned along with a failure return code.
- Batch file commands that contain unrecognized command options might generate warnings.

The following table shows the arguments for the options.

Option	Description	Values
-f	Batch file name	Valid file name
-ip	IP address of TFTP/SFTP server	Valid IP address
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	Username for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password

Syntax:

```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Example:

```
system> batch –f sslcfg.cli –ip 192.168.70.200
1 : sslcfg –client –dnld –ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

clearcfg command

Use the **clearcfg** command to set the IMM2 configuration to its factory defaults. You must have at least Advanced Adapter Configuration authority to issue this command. After the configuration of the IMM2 is cleared, the IMM2 is restarted.

clock command

Use the **clock** command to display the current date and time according to the IMM2 clock and the GMT offset. You can set the date, time, GMT offset, and daylight saving time settings.

Note the following information:

- For a GMT offset of +2, -7, -6, -5, -4, or -3, special daylight saving time settings are required:
  - For +2, the daylight saving time options are as follows: off, ee (Eastern Europe), mik (Minsk), tky (Turkey), bei (Beirut), amm (Amman), jem (Jerusalem).
  - For -7, the daylight saving time settings are as follows: off, mtn (Mountain), maz (Mazatlan).
  - For -6, the daylight saving time settings are as follows: off, mex (Mexico), cna (Central North America).
  - For -5, the daylight saving time settings are as follows: off, cub (Cuba), ena (Eastern North America).
  - For -4, the daylight saving time settings are as follows: off, asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantic).
  - For -3, the daylight saving time settings are as follows: off, gtb (Godthab), moo (Montevideo), bre (Brazil - East).
- The year must be from 2000 to 2089, inclusive.
- The month, date, hours, minutes, and seconds can be single-digit values (for example, 9:50:25 instead of 09:50:25).
- GMT offset can be in the format of +2:00, +2, or 2 for positive offsets, and -5:00 or -5 for negative offsets.

Syntax:

```
clock [options]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

Example:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2011
ok
system> clock
12/31/2011 13:15:30 GMT-5:00 dst on
```

identify command

Use the **identify** command to turn the chassis identify LED on or off, or to have it flash. The -d option can be used with -s on to turn the LED on for only for the number of seconds specified with the -d parameter. The LED then turns off after the number of seconds elapses.

Syntax:

```
identify [options]
options:
-s on/off/blink
-d seconds
```

Example:

```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

info command

Use the **info** command to display and configure information about the IMM.

Running the **info** command with no options displays all IMM location and contact information. The following table shows the arguments for the options.

Option	Description	Values
-name	IMM name	String
-contact	Name of IMM contact person	String
-location	IMM location	String
-room	IMM room identifier	String
-rack	IMM rack identifier	String
-rup	Position of IMM in rack	String
-ruh	Rack unit height	Read only
-bbay	Blade bay location	Read only

Syntax:

```
info [options]
option:
  -name imm_name
  -contact contact_name
  -location  imm_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

resetsp command

Use the **resetsp** command to restart the IMM2 or IMM2. You must have at least Advanced Adapter Configuration authority to be able to issue this command.

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about IBM products, you will find a wide variety of sources available from IBM to assist you.

Use this information to obtain additional information about IBM and IBM products, determine what to do if you experience a problem with your IBM system or optional device, and determine whom to call for service, if it is necessary.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require IBM to perform warranty service on your IBM product, the IBM service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated firmware and operating-system device drivers for your IBM product. The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your IBM service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.ibm.com/servers/eserver/serverproven/compat/us/eserver.html to make sure that the hardware and software is supported by your IBM product.
- Go to http://www.ibm.com/systems/support/ to check for information to help you solve the problem.
- Gather the following information to provide to IBM Support. This data will help IBM Support quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (IBM 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/electronic/ to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to IBM Support quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that IBM provides in the online help or in the documentation that is provided with your IBM product. The documentation that comes with IBM systems also describes the diagnostic tests that you can perform. Most systems, operating systems, and programs come with documentation that contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your IBM system and preinstalled software, if any, or optional device is available in the documentation that comes with the product. That documentation can include printed documents, online documents, readme files, and help files.

See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. IBM maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://www.ibm.com/systems/support/ .

Getting help and information from the World Wide Web

Up-to-date information about IBM products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about IBM systems, optional devices, services, and support is available at http://www.ibm.com/systems/support/ . IBM System x information is at http://www.ibm.com/systems/bladecenter/ . IBM BladeCenter information is at http://www.ibm.com/systems/bladecenter/ . IBM IntelliStation information is at http://www.ibm.com/systems/bladecenter/ .

How to send DSA data to IBM

Use the IBM Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read http://www.ibm.com/de/support/ecurep/send_http.html .

You can use any of the following methods to send diagnostic data to IBM:

- **Standard upload:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:** http://www.ecurep.ibm.com/app/upload_hw/
- **Secure upload:** http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:** https://www.ecurep.ibm.com/app/upload_hw/

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your IBM products.

For more information about Support Line and other IBM services, see http://www.ibm.com/services/us/index.wss or see http://www.ibm.com/planetwide/ for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

You can receive hardware service through your IBM reseller or IBM Services.

To locate a reseller authorized by IBM to provide warranty service, go to http://www.ibm.com/partnerworld/ and click **Find Business Partners** on the right side of the page. For IBM support telephone numbers, see http://www.ibm.com/planetwide/ . In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

IBM Taiwan product service

Use this information to contact IBM Taiwan product service.

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

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Appendix B. 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 give 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.

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 websites 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 IBM product, and use of those websites 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.

Trademarks

IBM, the IBM logo, and ibm.com are 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 http://www.ibm.com/legal/copytrade.shtml .

Adobe and PostScript are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc., in the United States, other countries, or both and is used under license therefrom.

Intel, Intel Xeon, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

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

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

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

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

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1024 bytes, MB stands for 1,048,576 bytes, and GB stands for 1,073,741,824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1,000,000 bytes, and GB stands for 1,000,000,000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard disk drive bays with the largest currently supported drives that are available from IBM.

Maximum memory might require replacement of the standard memory with an optional memory module.

IBM makes no representation or warranties regarding non-IBM products and services that are ServerProven®, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. These products are offered and warranted solely by third parties.

IBM makes no representations or warranties with respect to non-IBM products. Support (if any) for the non-IBM products is provided by the third party, not IBM.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If IBM determines that the levels of particulates or gases in your environment have caused damage to the device, IBM may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 2. Limits for particulates and gases

Contaminant	Limits
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

1. ASHRAE 52.2-2008 - Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.
2. The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.
3. ANSI/ISA-71.04-1985. Environmental conditions for process measurement and control systems: Airborne contaminants. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Documentation format

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties when you use the PDF files and want to request a web-based format or accessible PDF document for a publication, direct your mail to the following address:

Information Development
IBM Corporation
205/A015

3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

In the request, be sure to include the publication part number and title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Telecommunication regulatory statement

This product is not intended to be connected directly or indirectly by any means whatsoever to interfaces of public telecommunications networks, nor is it intended to be used in a public services network.

Electronic emission notices

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

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 might cause undesired operation.

Industry Canada Class A emission 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.

Australia and New Zealand Class A statement

Attention: 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 Union EMC Directive conformance 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 nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 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.

Responsible manufacturer:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

European Community contact:

IBM Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
Email: tjahn@de.ibm.com

Germany Class A 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 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 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
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland
Technical Regulations, Department M456
IBM-Allee 1, 71137 Ehningen, Germany
Telephone: +49 7032 15-2937
Email: tjahn@de.ibm.com

Generelle Informationen:

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

Japan VCCI Class A statement

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

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). 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.

Korea Communications Commission (KCC) statement

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

This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

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

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

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。

Taiwan Class A compliance statement

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。

Index

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Part Number: 88Y7599

Printed in USA

(1P) P/N: 88Y7599