Integrated Management Module II
User's Guide

Integrated Management Module II
User's Guide

Fourth Edition (December 2013)

Contents

Tables

Chapter 1. Introduction

The Integrated Management Module II (IMM2) service processor 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 baseboard management controller (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 IBM BladeCenter blade servers.
- Enhanced remote-presence capabilities. The feature does not apply to IBM BladeCenter blade servers.

Notes:

- A dedicated systems-management network port is not available on IBM BladeCenter blade servers and some System x servers; for these servers only the *shared* setting is available.
- 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 the basic input/output system (BIOS) in IBM System x servers and IBM BladeCenter blade servers. The 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.

Notes:

- IBM System x Server Firmware is often called server firmware, and occasionally called UEFI, in this document.
- IBM System x Server Firmware is fully compatible with non-UEFI operating systems.
- 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, BladeCenter, and the IBM Flex System.

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 Basic, Standard, and Advanced Level features

With IMM2, Basic, Standard and Advanced levels of IMM2 functionality are offered. See the documentation for your server for more information 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.

Note: Some features might not apply to IBM BladeCenter bladeservers.

The following is a list of IMM2 basic level features:

IMM2 Basic Level features

The following is a list of IMM2 Basic Level features:

- 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 Standard Level features

The following is a list of IMM2 Standard Level features:

- All of the IMM2 Basic Level features
- 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 Advanced Level features

The following is a list of IMM2 Advanced Level features:

- All of the IMM2 Basic and Standard Level features
- 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

IMM2 feature improvements

The following is a list of IMM2 feature improvements over the 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 Basic level or Standard level IMM2 firmware functionality, you might be able to upgrade the IMM2 functionality in your server. For more information about available upgrade levels and how to order, see Chapter 7, “Features on Demand,” on page 145.

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 KVM multiplexing for IBM BladeCenter products including IBM blade servers.

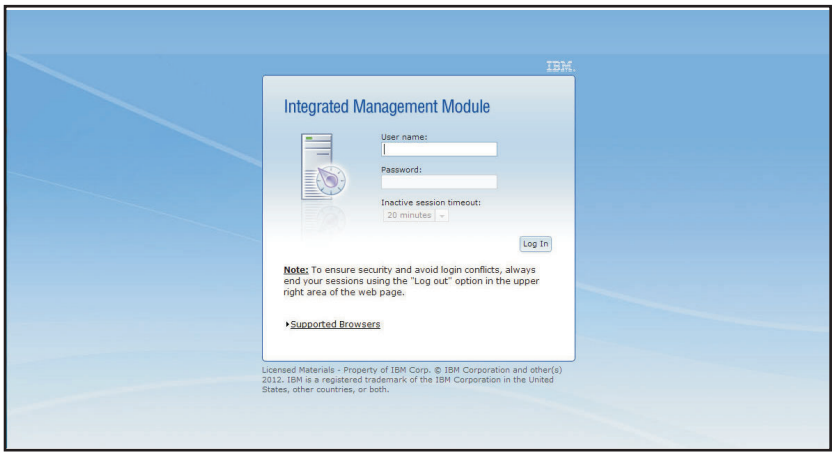
There is no external network access to the IMM2 on IBM BladeCenter blade servers and the advanced management module must be used for remote management of IBM BladeCenter blade servers. The IMM2 replaces the functionality of the BMC and the Concurrent Keyboard, Video and Mouse (cKVM) option card available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

Web browser and operating-system requirements

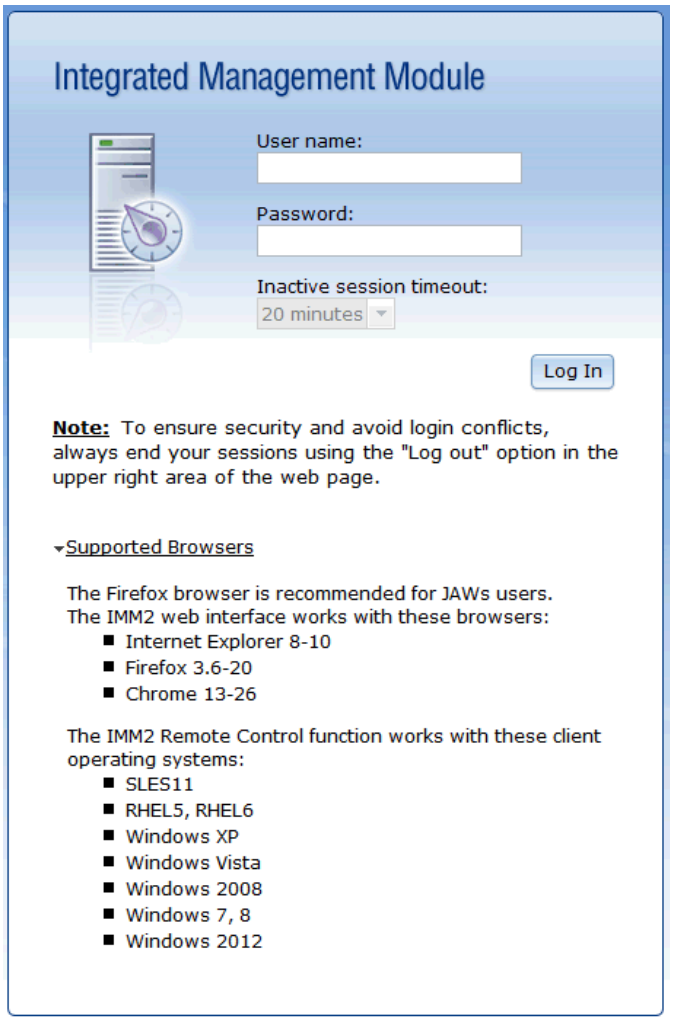
The IMM2 web interface requires the Java™ Plug-in 1.5 or later (for the remote presence feature) and one of the following web browsers:

- Microsoft Internet Explorer versions 8 through 10
- Mozilla Firefox versions 3.6 through 20
- Chrome versions 13 through 26

If you are using newer versions of Microsoft Internet Explorer, it is recommended that you use the Compatibility View in Internet Explorer to display the IMM2 web pages. The browsers listed above match those currently supported by the IMM2 firmware. The IMM2 firmware may be enhanced periodically to include support for other browsers. The following illustration displays the IMM2 login screen.



Depending upon the version of the firmware on the IMM2, web browser support can vary from the browsers listed in this section. To see the list of supported browsers for the firmware that is currently on the IMM2, click the **Supported Browsers** menu list from the IMM2 login page (as shown in the following illustration).



For increased security, only high strength ciphers are now supported when using https. When using https, the combination of your client operating system and browser must support one of the following cipher suites:

- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES256-SHA
- DHE-RSA-CAMELLIA256-SHA
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA
- DHE-RSA-SEED-SHA
- DHE-RSA-CAMELLIA128-SHA
- AES256-GCM-SHA384
- AES256-SHA256
- AES256-SHA
- AES128-GCM-SHA256
- AES128-SHA256
- AES128-SHA
- CAMELLIA256-SHA

- CAMELLIA128-SHA
- EDH-RSA-DES-CBC3-SHA
- DES-CBC3-SHA
- SEED-SHA
- RC4-SHA

The IMM2 Remote Control function works with the following client operating systems:

- SUSE Linux Enterprise Server 11 (SLES11)
- Red Hat Enterprise Linux Enterprise 5 (RHEL5)
- Red Hat Enterprise Linux Enterprise 6 (RHEL6)
- Microsoft Windows XP
- Microsoft Windows Vista
- Microsoft Windows 2008
- Microsoft Windows 7
- Microsoft Windows 8
- Microsoft Windows 2012

Your internet browser's cache stores information about web pages that you visit so that they will load more quickly in the future. After a flash update of the IMM2 firmware, your browser may continue to use information from its cache instead of retrieving it from the IMM2. After updating the IMM2 firmware it is recommended that you clear the browser cache to ensure that web pages served by the IMM2 are displayed correctly.

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 IBM blade servers. Although the IMM2 is standard in some IBM BladeCenter products and IBM blade servers, the IBM BladeCenter advanced management module is the primary management module for systems-management functions and keyboard/video/mouse (KVM) multiplexing for IBM BladeCenter products including IBM blade servers. Users who wish to configure the IMM2 settings on blade servers should use the Advanced Settings Utility (ASU) on the blade server to perform those actions.

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.

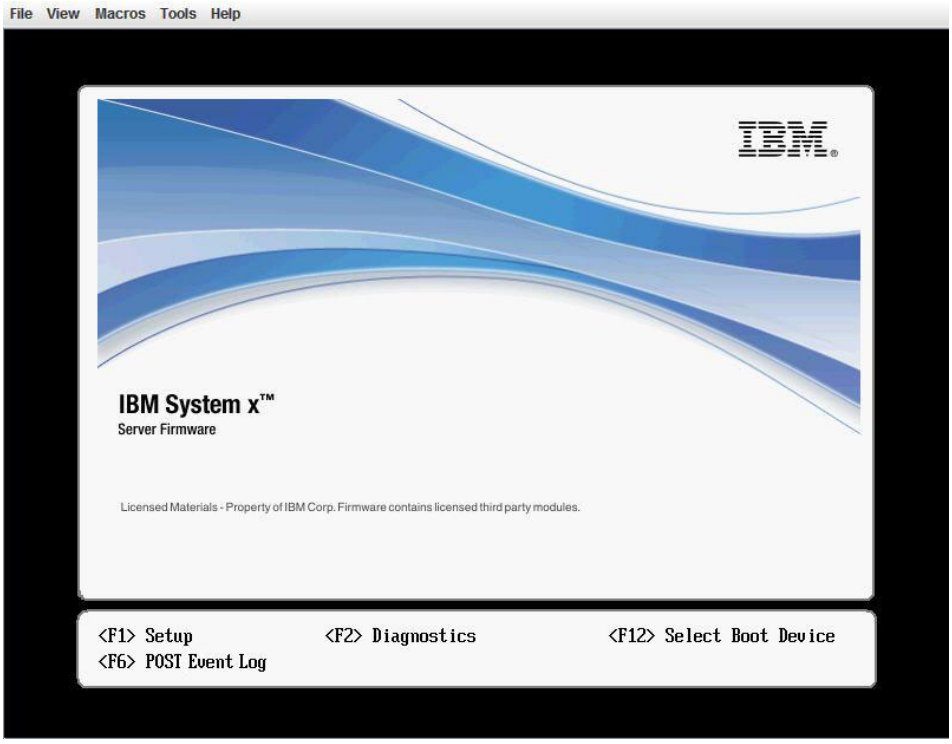
Setting up the IMM2 network connection through the IBM System x Server Firmware Setup utility

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 DHCP

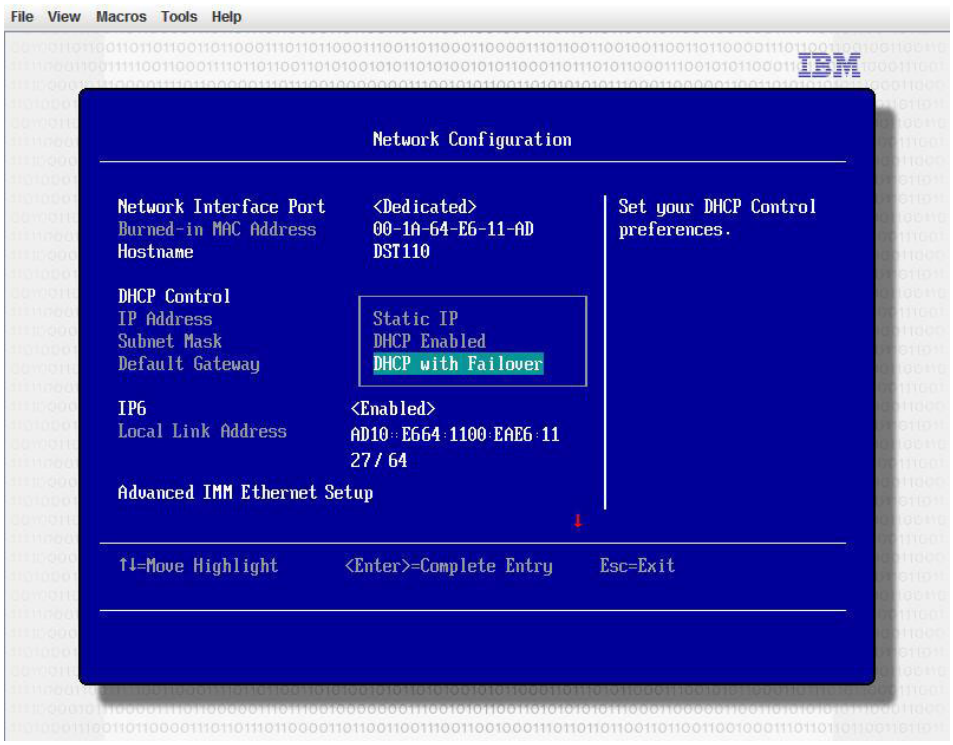
server, or the server network must be configured to use the IMM2 static IP address. To set up the IMM2 network connection through the Setup utility, complete the following steps:

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

   Note: Approximately 90 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.

   Notes:

   - 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.
   - 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.

Notes:

- You must wait approximately 1 minute for changes to take effect before the server firmware is functional again.
- You can also configure the IMM2 network connection through the IMM2 web interface or command-line interface (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.

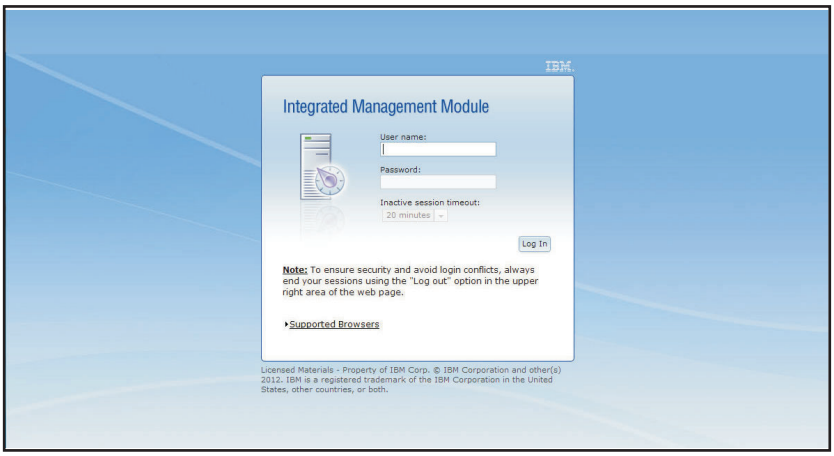
Logging in to the IMM2

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 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.

   The Login window is shown in the following illustration.

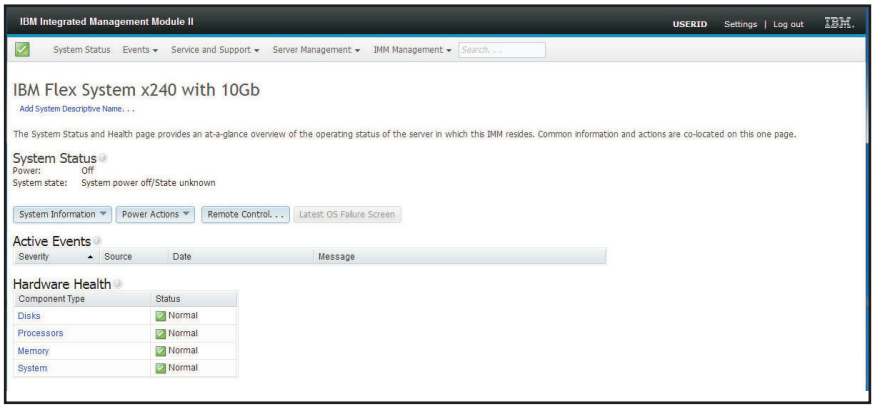


3. Click **Log In** to start the session. The browser opens the System Status page, as shown in the following illustration. This page gives you a quick view of the server status and the server health summary.

   Note: If you boot to the operating system while in the IMM2 GUI and the message "Booting OS or in unsupported OS" is displayed under **System Status → System State**, disable the Windows 2008 firewall or type the following command in the Windows 2008 console. This might also affect blue-screen capture features.

   ```
   netsh firewall set icmpsetting type=8 mode=ENABLE
   ```

   By default, the icmp packet is blocked by the Windows firewall. The IMM2 GUI will then change to "OS booted" status after you change the setting as indicated above in both the Web and CLI interfaces.



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 the top of the IMM2 window to perform activities with the IMM2. The title bar identifies the user name that is logged in. The title bar allows you to configure **Settings** for the status screen refresh rate and a custom trespass message, and **Log out** of the IMM2 web interface as shown in the following illustration. 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. See "System Status tab" on page 20 and "Viewing the system status" on page 103 for additional information.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
Events	Event Log	The Event Log page displays entries that are currently stored in the IMM2 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. See “Events tab” on page 26 and “Managing the event log” on page 131 for additional information.
	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. See “Event recipients” on page 28 and “Notification of system events” on page 132 for additional information.
Service and Support	Problems	The Problems page allows you to view current unresolved problems that are serviceable by the Support Center. You can also view the status of each problem as related to its resolution. See“Problems option” on page 31 for additional information.
	Settings	The Settings page configures your server to monitor and report service events. See “Settings option” on page 34 for additional information.
	Download Service Data	The Download Service Data page creates a compressed file of information that can be used by IBM Support to assist you. See “Download service data option” on page 37 and “Collecting service and support information” on page 137 for additional information.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
Server Management	Server Firmware	The Server Firmware page displays firmware levels and allows you to update the IMM2 firmware, server firmware, and DSA firmware. See "Server firmware" on page 38 and "Updating the server firmware" on page 125 for additional information.
	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. See "Remote control" on page 44 and "Remote presence and remote control functions" on page 113 for additional information.
	Server Properties	The Server Properties page provides access to various properties, status conditions, and settings for your server. The following options are available from the Server Properties page: • 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 Replaceable Unit (FRU) components that have been added to or removed from the system. See "Server properties" on page 49 for additional information.
	Cooling Devices	The Cooling Devices page displays the current speed and status of cooling fans in the server. See "Cooling devices" on page 53 for additional information.
	Power Modules	The Power Modules page displays power modules in the system with status and power ratings. See "Power modules" on page 54 for additional information.
	Server Power Actions	The Server Power Actions page provides full remote power control over your server with power-on, power-off, and restart actions. See "Server power actions" on page 53 and "Controlling the power status of the server" on page 112 for additional information.
	Disks	The Hard Disks page displays the status of hard disk drives in the server. You can click on a drive name to display active events for the hard disk drive. See "Disks" on page 55 for additional information.
	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 an event and additional hardware information for the memory module. If you remove or replace a dual inline memory module (DIMM), the server needs to be powered on at least once after the removal or replacement to display the correct memory information. See "Memory" on page 55 for additional 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 clock speed. You can click on a microprocessor name to display events and additional hardware information for the microprocessor. See "Processors" on page 57 for additional information.
	Server Timeouts	The Server Timeouts page allows you to manage server start timeouts to detect and recover from server hang occurrences. See "Server timeouts" on page 58 and "Setting server timeouts" on page 64 for additional information.
	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). See "PXE network boot" on page 58 and "Setting up PXE network boot" on page 124 for additional information.
	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 IMM2 to capture operating system failure screens, the operating system watchdog must be enabled. See "Latest OS failure screen" on page 58 and "Capturing the latest OS failure screen data" on page 139 for additional information.
	Power Management	The Server Power Management page allows you to manage power related policies and hardware and contains the history of the amount of power used by the server. See "Managing the server power" on page 140 for additional information.
IMM Management *(continued on next page)*	IMM Properties	The IMM Properties page provides access to various properties and settings for your IMM2. The following options are available from the IMM Properties page: • The Firmware tab provides a link to the Server Firmware section of Server Management. You can also enable automated promotion of the IMM2 backup firmware from this tab. • 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 CLI modes. See Chapter 4, "Configuring the IMM2," on page 61 for additional information.
	Users	The Users page configures the IMM2 login profiles and global login settings. You can also view user accounts 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. See "Configuring user accounts" on page 69 for additional information.

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. See "Configuring network protocols" on page 78 for additional information.
	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. See "Configuring security settings" on page 91 for additional information.
	IMM Configuration	The IMM Configuration page displays a summary of the current IMM2 configuration settings. See "Restoring and modifying your IMM configuration" on page 99 for additional information.
	Restart IMM	The Restart IMM page allows you to reset the IMM2. See "Restarting the IMM2" on page 99 for additional information.
	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. See "Resetting the IMM2 to the factory defaults" on page 101 for additional information. **Attention:** When you click **Reset IMM to factory defaults...**, all modifications that you have 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. See "Activation management key" on page 101 for additional information.

Chapter 3. IMM2 web user interface overview

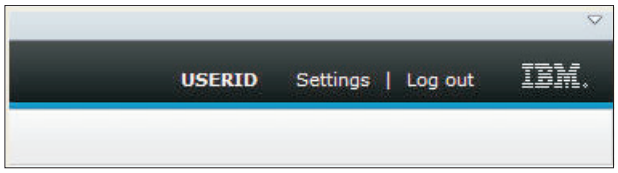
This chapter provides an overview of how to use the IMM2 web user interface features.

Important: This section does not apply to IBM BladeCenter and IBM blade servers. Although the IMM2 is standard in some IBM BladeCenter products and IBM blade servers, the IBM BladeCenter advanced management module is the primary management module for systems-management functions. Users who wish to configure the IMM2 settings on blade servers should use the Advanced Settings Utility (ASU) on the blade server to perform those actions.

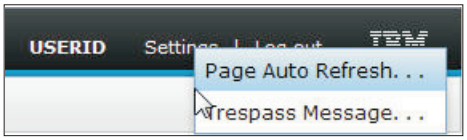
Web session settings

This section provides information about the settings for the web interface session main page.

The IMM2 main page displays menu selections in the upper right area of the web page. These menu items allow you to configure the web page refresh behavior and the message that is displayed to a user when the user enters their credentials to login. The following illustration shows the menu selections in the upper right area of the web page.

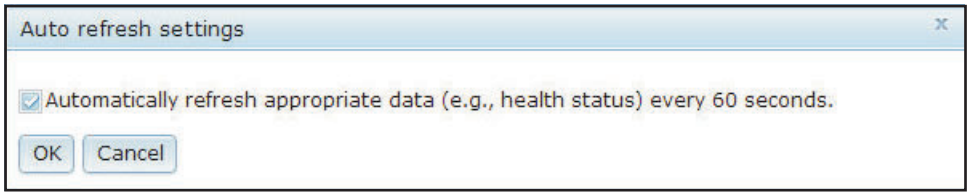


Click the **Settings** item and the following menu selections display:



Page auto refresh

Use the **Page Auto Refresh** option under the Settings menu item in the top upper right area of the web session page to set the page content to automatically refresh every 60 seconds. To set the page content to refresh every 60 seconds, select the **Automatically refresh appropriate data...** check box and press **OK**. To disable the automatic page refresh, deselect the check box and press **OK**. The following illustration shows the Auto refresh settings window.



Some IMM2 web pages are automatically refreshed, even if the automatic refresh check box is not selected. IMM2 web pages that are automatically refreshed are as follows:

- **System Status:**

  The system and power status is refreshed automatically every three seconds.
- **Server Power Actions:** (under the Server Management tab)**:**

  Power status is refreshed automatically every three seconds.
- **Remote Control:** (under the Server Management tab)**:**

  The Start remote control... buttons are automatically refreshed every second. The Session List table is refreshed once every 60 seconds.

Notes:

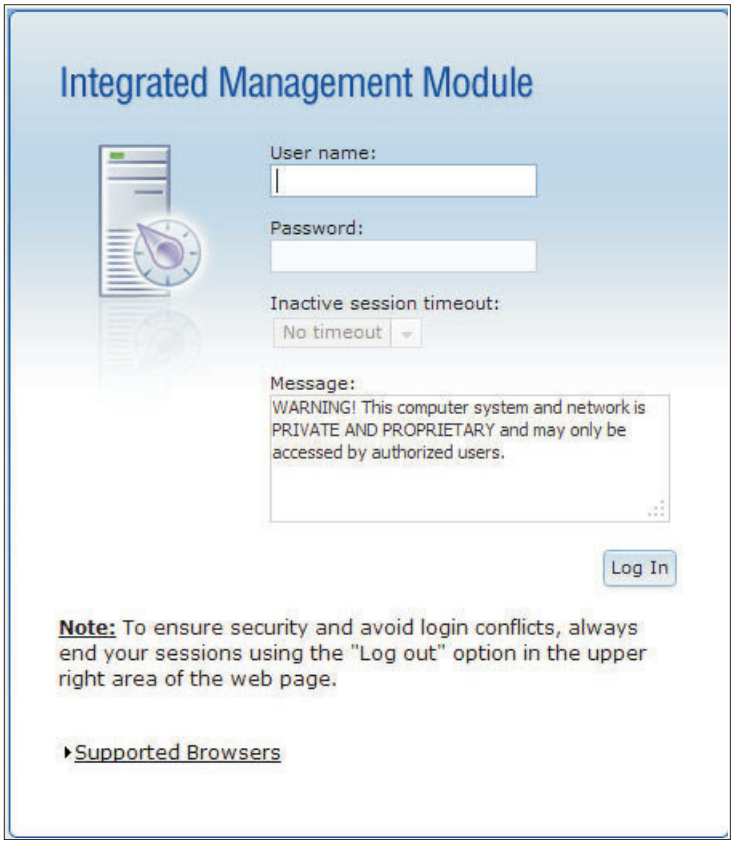
- If you navigate from your web browser to a web page that automatically refreshes, the inactivity timeout will not automatically end your web session.
- If you send a request to a Remote Control user using the Remote Control option page under Server Management, your web session will not timeout regardless of which web page you navigate to until a response is received from the Remote Control user, or until the Remote Control user times out. When the request from the Remote Control user completes processing, the inactivity timeout function will resume.

  Note: The preceding note applies to all web pages.
- The IMM2 firmware supports up to six simultaneous web sessions. To free up sessions for other users, log out of the web session when you are finished, rather than waiting on the inactivity timeout to automatically close your session. If you leave the browser while on an IMM2 web page that automatically refreshes, your web session will not automatically close due to inactivity.

Trespass message

Use the **Trespass Message** option under the Settings menu item in the top upper right area of the web session page to setup a message that you want displayed when a user logs in to the IMM2 server. The following screen displays when you select the Trespass Message option. Enter the message text that you want displayed to the user in the field provided and press **OK**.

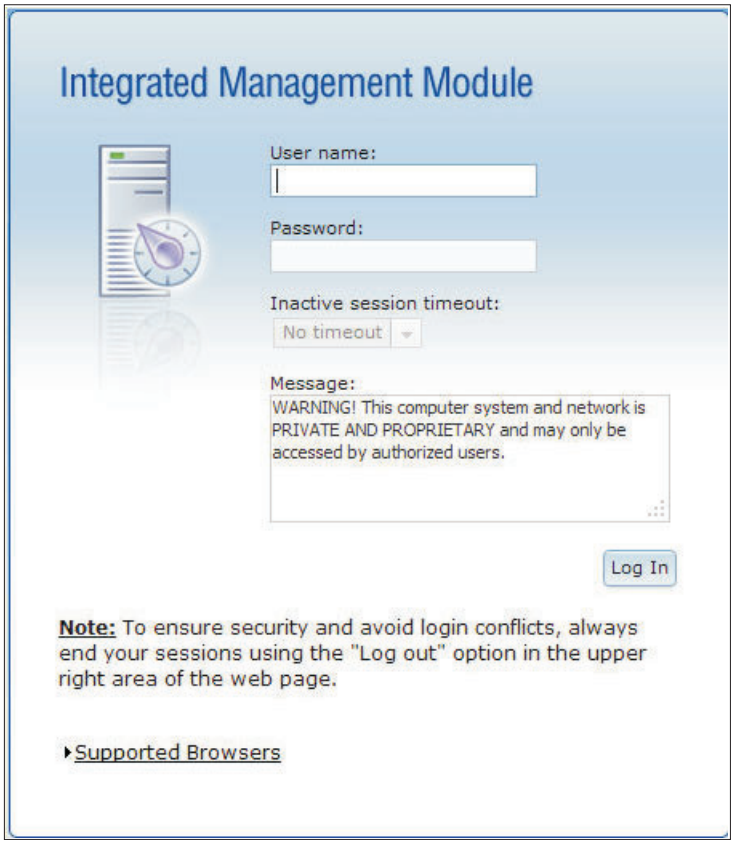
The message text will be displayed in the Message area of the IMM2 login page when a user logs in, as shown in the following illustration.



Log out

To ensure security, log out of the IMM2 web session when you are finished and manually close any other IMM2 web browser windows that you might have open.

To log out of the web session, click **Log out** in the top upper right area of the web page. The Login window will be shown.

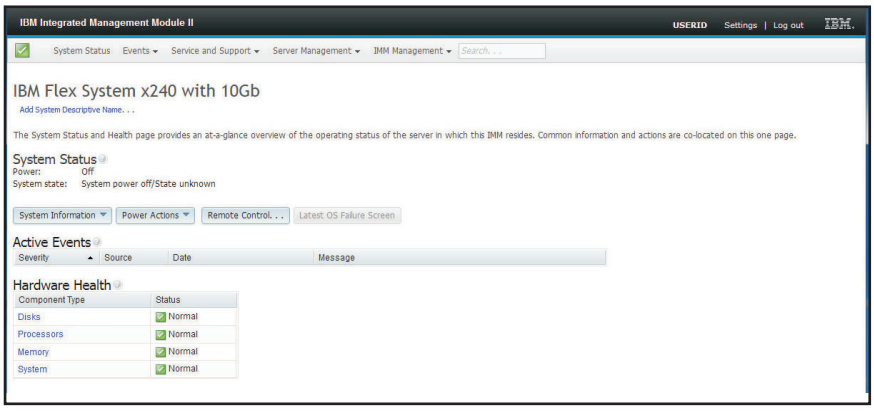


Note: The IMM2 firmware supports up to six simultaneous web sessions. To free up sessions for other users, log out of the web session when you are finished, rather than waiting on the inactivity timeout to automatically close your session. If you leave the browser while on an IMM2 web page that automatically refreshes, your web session will not automatically close due to inactivity.

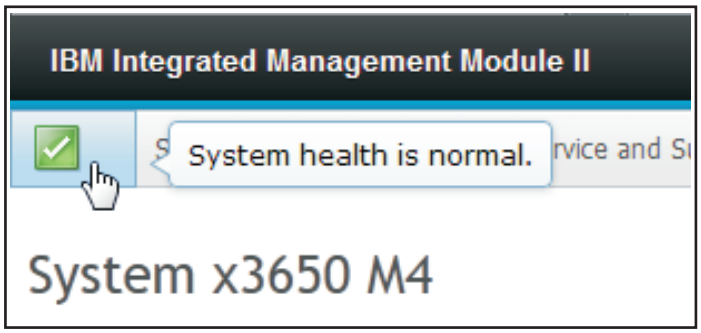
System Status tab

This section provides information for using the options under the System Status tab on the IMM2 web user interface.

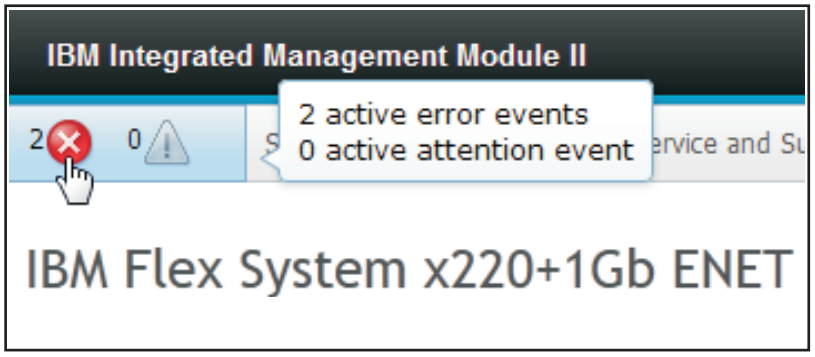
The System Status page is displayed after you log into the IMM2 web user interface or when you click the **System Status** tab. From the System Status page, you can view the system status, active system events, and hardware health information. The following window opens when you click the System Status tab or log into the IMM2 web interface.



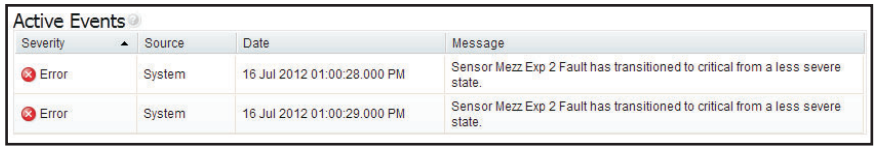
You can click on the green icon (with the check mark) in the upper left corner of the page to get a quick summary of the server health. A check mark indicates that the server is operating normally.



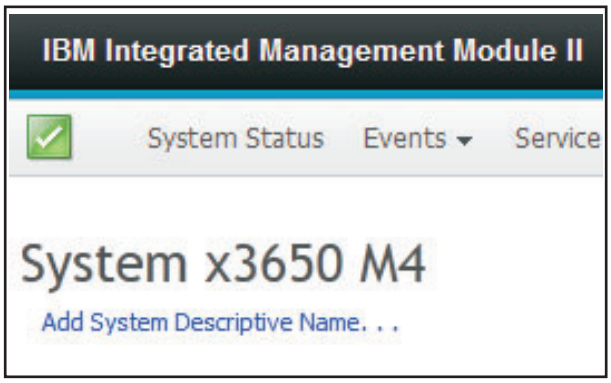
If a red circle or a yellow triangle icon is displayed, this indicates that an error or warning condition exists, as shown in the following illustration.



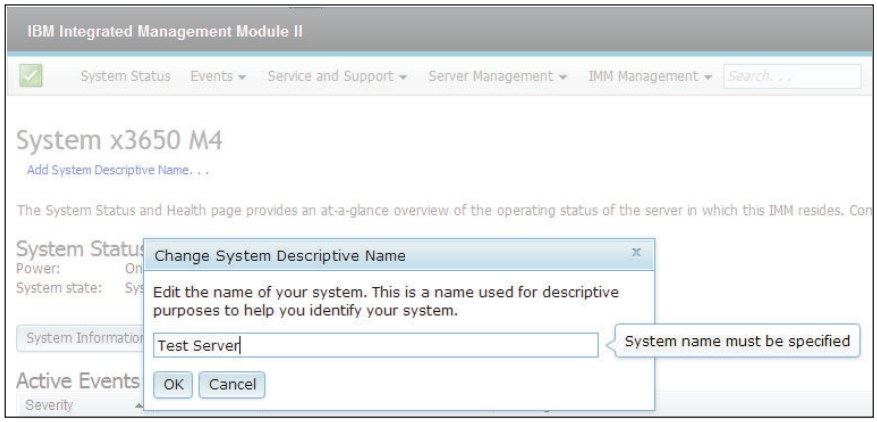
The red circle icon indicates that an error condition exists on the server. A yellow triangle icon indicates that a warning condition exists. When a red circle or a yellow triangle icon is displayed, the events associated with that condition are listed under the Active Events section on the System Status page, as shown in the following illustration.



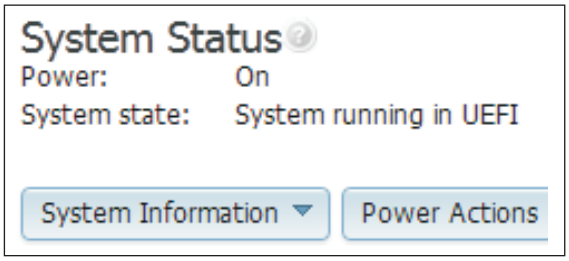
You can add a descriptive name to the IMM2 server to assist you in identifying one IMM2 server from another. To assign a descriptive name to the IMM2 server, click the **Add System Descriptive Name...** link located below the server product name.



When you click the **Add System Descriptive Name...** link, the following window opens for you to specify a name to associate with the IMM2 server. You can change the System Descriptive Name at any time.



The **System Status** section on the System Status page provides the server power state and operating state of the server. The status that is displayed is the server state at the time the System Status page is opened, (as shown in the following illustration).

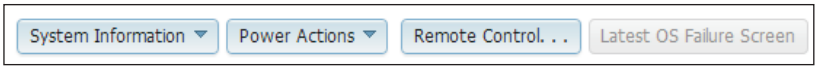


The server can be in one of the following states described in the following table:

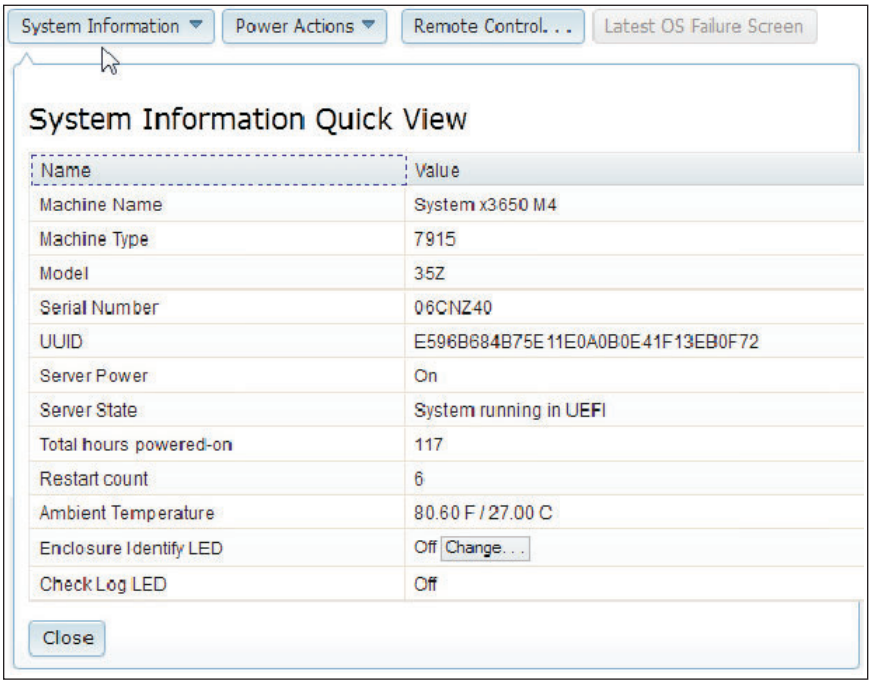
Table 2. Server power and operating states

Server state	**Description**
System power off/state unknown	The server is off.
System on/starting UEFI	The server is powered on, but UEFI is not running.
System running in UEFI	The server is powered on and UEFI is running.
System stopped in UEFI	The server is powered on; UEFI has detected a problem and has stopped running.
Booting OS or in unsupported OS	The server might be in this state for one of the following reasons: • The operating system loader has started but the operating system is not running yet. • The IMM2 Ethernet over USB interface is disabled. • The operating system does not have the drivers loaded that support the Ethernet over USB interface. • The operating system might be running a firewall; therefore, blocking communication to the IMM2.
OS booted	The server operating system is running.
Suspend to RAM	The server has been placed in standby or sleep state.

The System Status page also provide tabs for **System Information**, **Power Actions**, **Remote Control**, and **Latest OS Failure Screen**.



Click the **System Information** tab to view information about the server

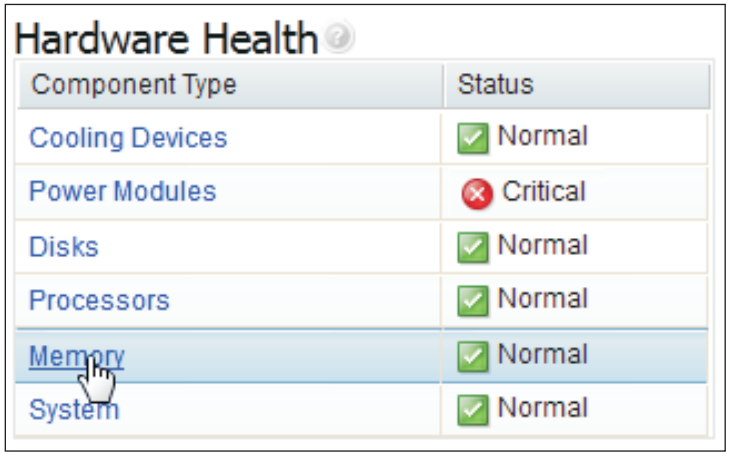


Click the **Power Actions** tab to view the actions that you can perform for full remote power control over the server with power-on, power-off, and restart actions. See "Controlling the power status of the server" on page 112 for details about how to remotely control the server power.

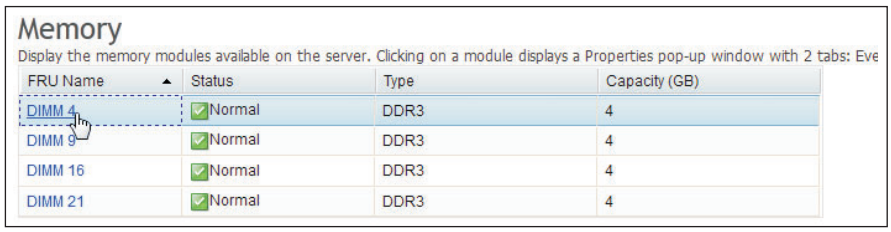
Click the **Remote Control** tab for information on how to control the server at the operating system level. See "Remote presence and remote control functions" on page 113 for details about the Remote Control function.

Click the **Latest OS Failure Screen** tab for information on how to capture the Latest OS Failure Screen data. See "Capturing the latest OS failure screen data" on page 139 for details about the Latest OS Failure Screen.

Under the **Hardware Health** section of the System Status page is a table with a list of the hardware components that are being monitored and their health status. The status displayed for a component might reflect the most critical state of the component in the Component Type column in the table. For example, a server might have several power modules installed and all of the power modules are operating normally except one. The status for the Power Modules components in the table will have a status of critical because of that *one* power module (as shown in the following illustration).

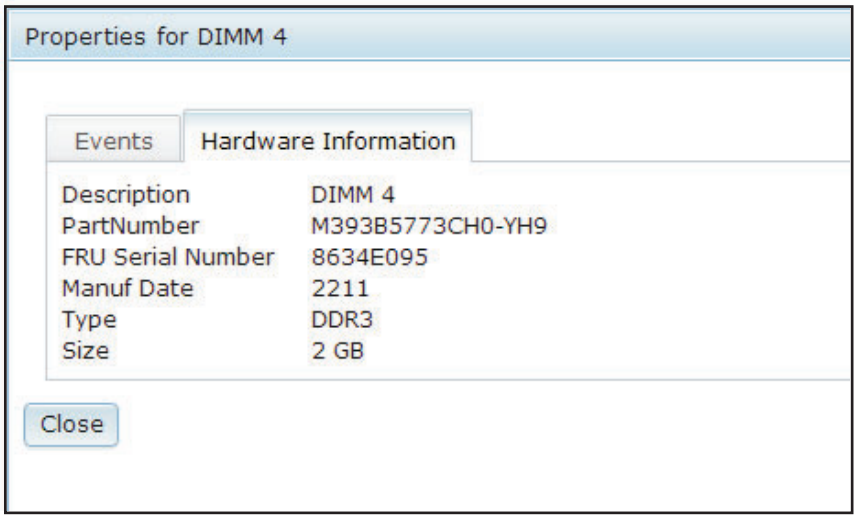


Each component type is a link that you can click to get more detailed information. When you click on a component type, a table listing the status for each of the individual components is displayed (as shown in the following illustration).



You can click on a component in the FRU Name column of the table to obtain additional information for that component. All active events for the component will be displayed.

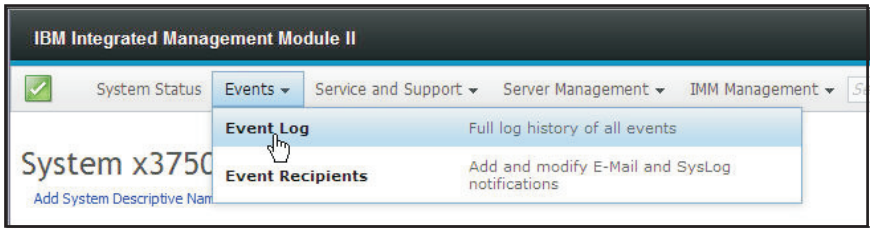
Click on the **Hardware Information** tab for detailed information about the component.



Events tab

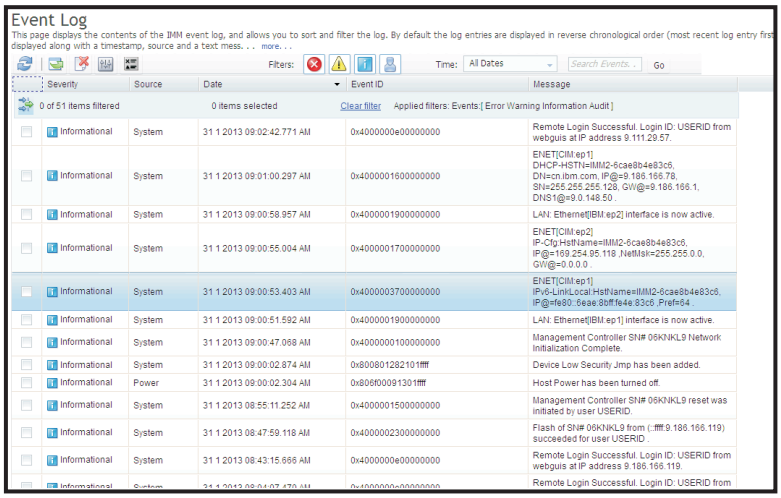
This section provides information for using the options under the Events tab on the IMM2 web user interface.

The options under the **Events** tab enables you to manage the Event Log history and manage Event Recipients for email and syslog notifications. The following illustration shows the options under the Events tab on the IMM2 web page.

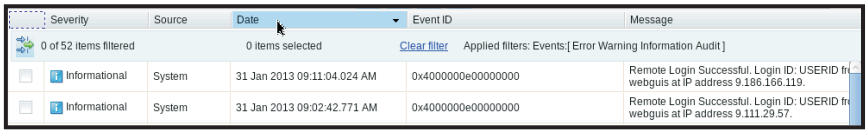


Event log

Select **Event Log** under the Events tab to display the Event Log page. The Event Log page shows the severity for the events that are reported by the IMM2, and 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 on the Event Recipients page. You can sort and filter events in the event log. The following is an illustration of the Event log page.

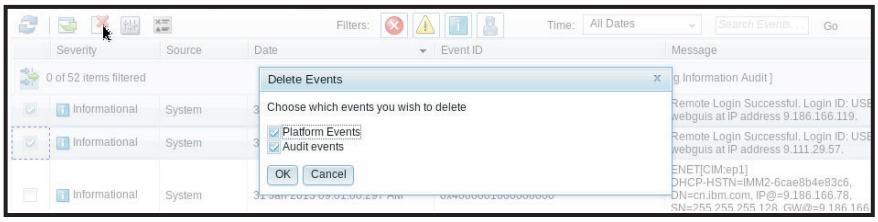


To sort and filter events in the event log, select the column heading (as shown in the following illustration).



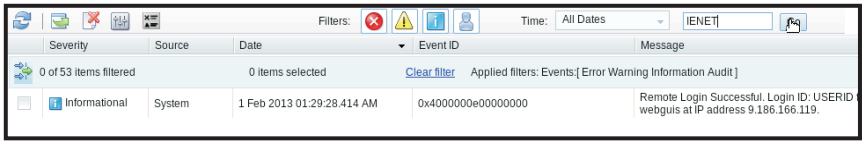
You can save all or save selected events in the event log to a file using the **Export** button. To select specific events, choose one or more events on the main Event Log page and left-click on the **Export** button (as shown in the following illustration).

Use the **Delete Events** button to choose the type of events you want to delete (as shown in the following illustration).

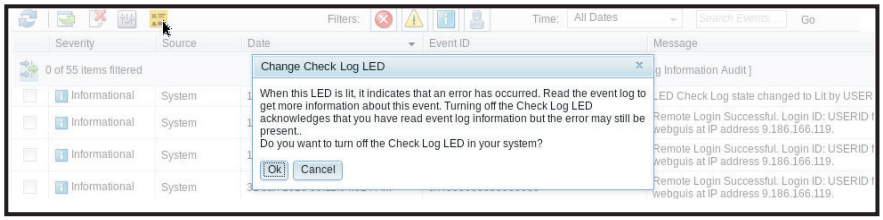


To select the type of event log entries that you want displayed, click the appropriate button (as shown in the following illustration).

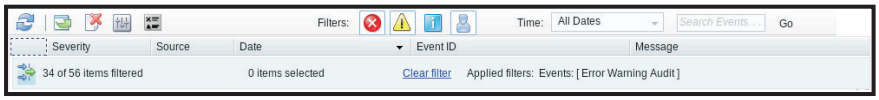
To search for specific types of events or keywords, type the type of event or keyword in the **Search Events** box; then, click **Go** (as shown in the following illustration).



To turn off the Check Log LED when the Check Log LED is on and the related Event Logs have been selected, click the **Check Log LED Status** button (as shown in the following illustration).

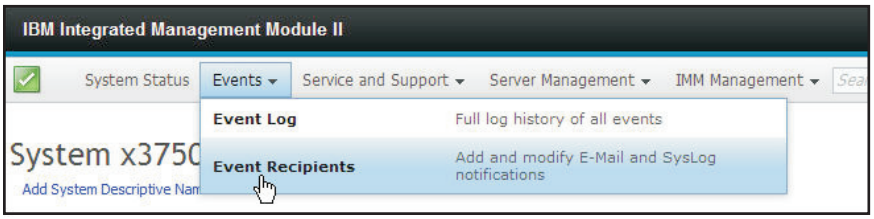


On the Event Log tool bar you can click any of the **Filter Events** buttons to select the events to be displayed. To clear the filter and show all types of events, click the **Clear Filter** link shown in the following illustration.



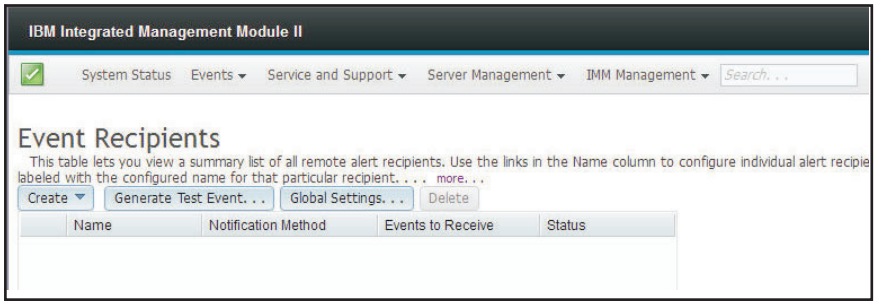
Event recipients

Use the **Events Recipients** option under the Events tab to add and modify email and syslog notifications.



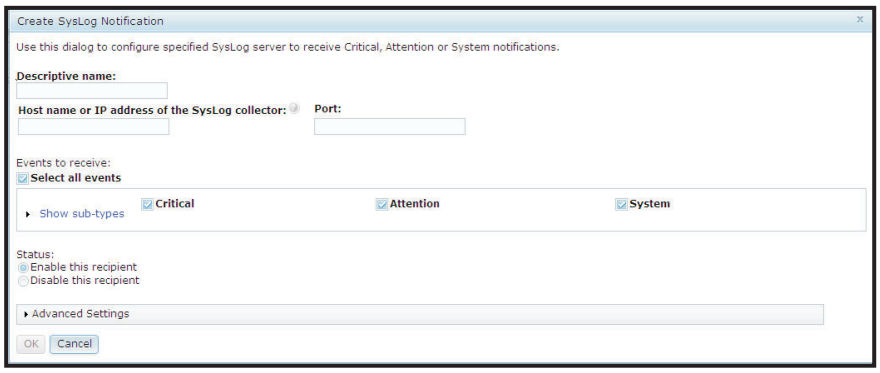
The Event Recipients option enables you to manage who will be notified of system events. You can configure each recipient, and manage settings that apply to all event recipients. You can also generate a test event to verify the notification feature.

Click the **Create** button to create email and syslog notifications. The following illustration shows the Event Recipients window.

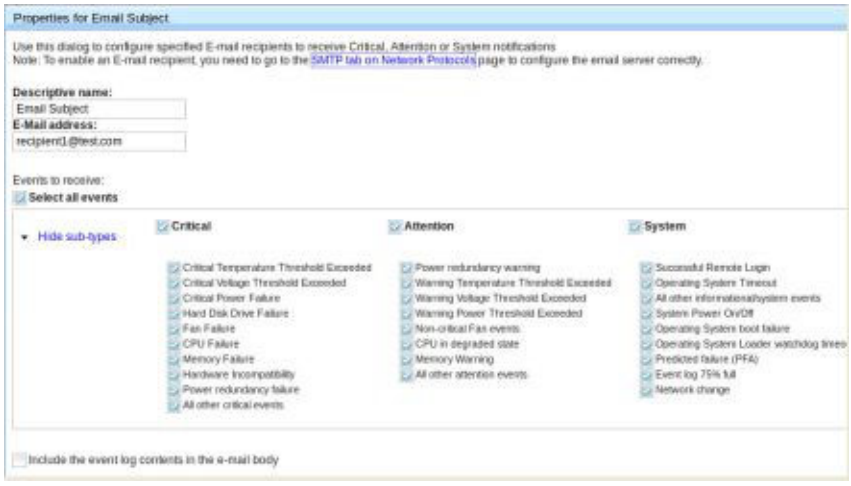


Select the **Create E-mail Notification** option to setup a target email address and choose the type of events for which you want to be notified. In addition, you can click **Advanced Settings** to select the starting index number. To include the event log in the email, select the **Include the event log contents in the e-mail body** check box. The following is an illustration of the Create E-mail Notification window.

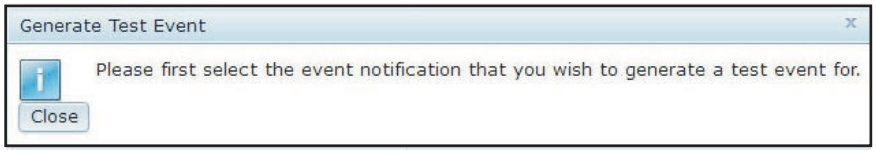
Select the **Create SysLog Notification** option to setup the Host name and IP Address for the SysLog collector and choose the type of events for which you want to be notified. In addition, you can click **Advanced Settings** to select the starting index number. You can also specify the port you want to use for this type of notification. The following is an illustration of the Create SysLog Notification window.



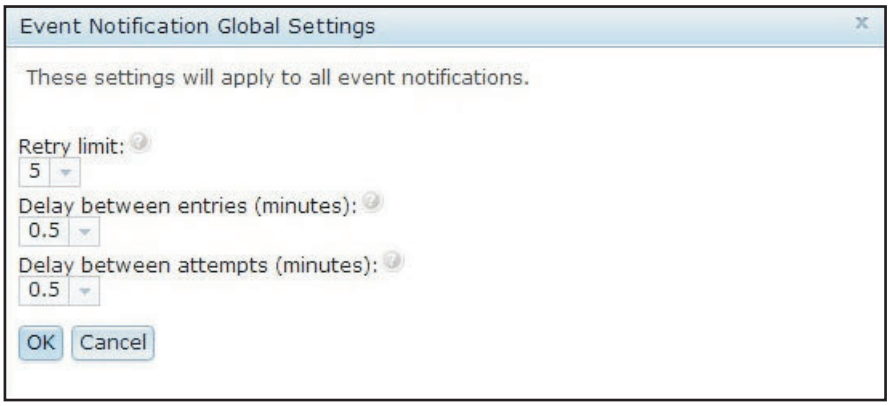
To configure an *existing* email notification or system notification target click the target name. The following is an illustration of the Properties for Email Subject window that is used to configure existing email notification and system notification targets.



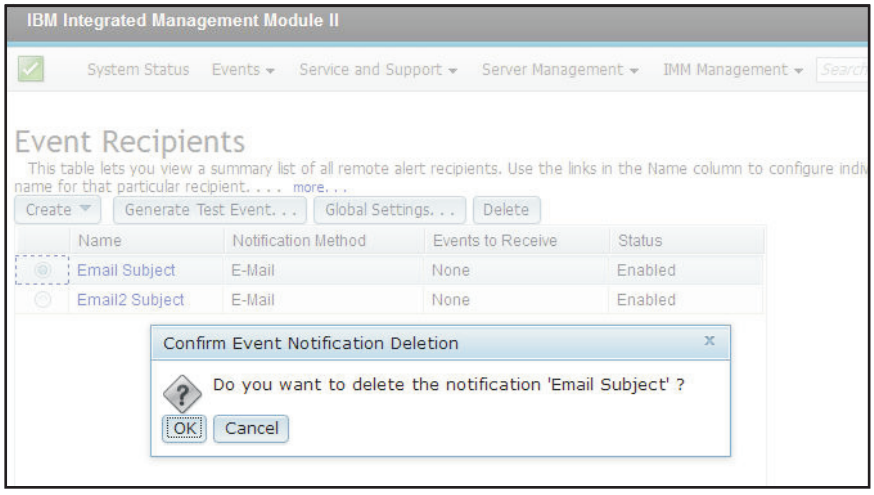
Select the **Generate Test Event** button to send a test email to a selected email target (as shown in the following illustration).



Select the **Global Settings** button to set a limit in which to retry the event notification, the delay (in minutes) between event notification entries, and the delay (in minutes) between attempts (as shown in the following illustration).

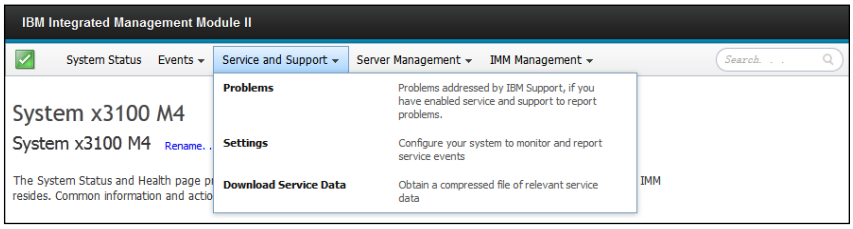


If you want to remove an email or syslog notification target, select the **Delete** button. The following window opens:



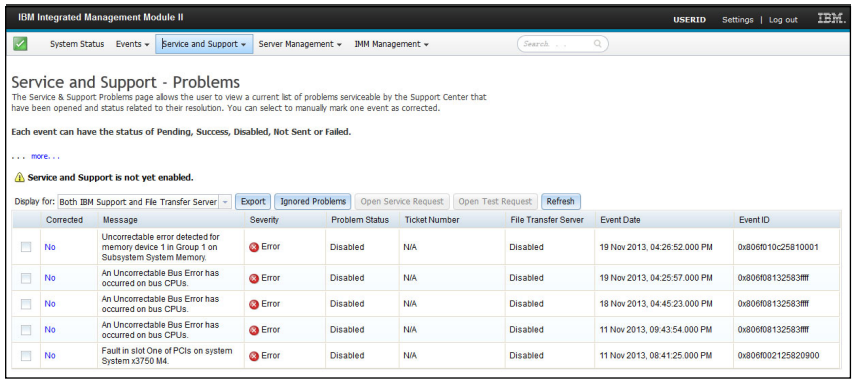
Service and support tab

This section provides information for using the options under the Service and Support tab on the IMM2 web user interface page (as shown in the following illustration).



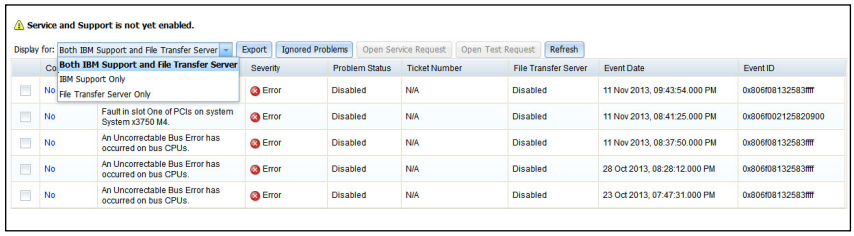
Problems option

Use the **Problems** option under the Service and Support tab to view a list of unresolved problems that are serviceable by the Support Center (as shown in the following illustration). You can view the status of each problem in the Problem Status column and manually flag an event as corrected in the Corrected column once the problem has been resolved. Events can have a Problem Status value of Pending, Success, Disable, Not Sent, or Failed.

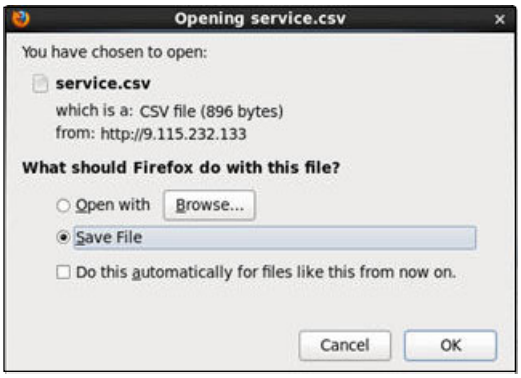


The **Display for:** field displays one of the following modes (as shown in the following illustration):

- Both IBM Support and File Transfer Server
- IBM Support Only
- File Transfer Server Only

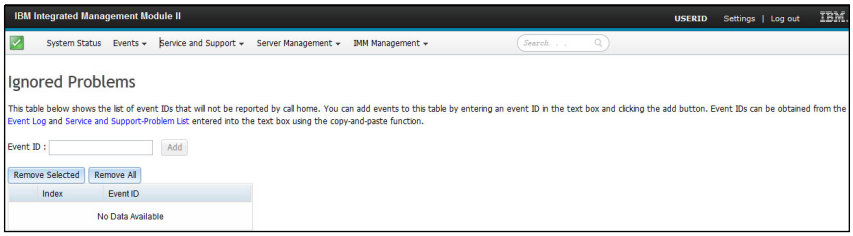


Click the **Export** tab to download a `service.csv` file. The following window is displayed.

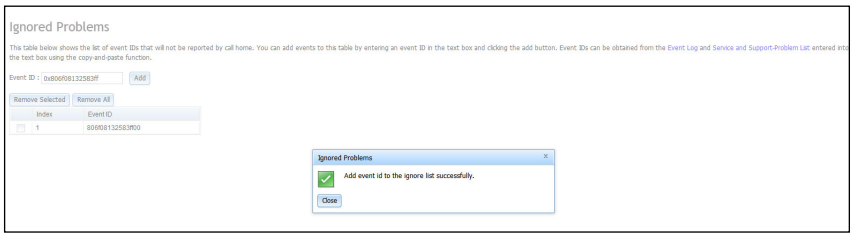


Click the **Ignore Problems** tab to display the list of event IDs that will not be reported by the *call home* feature. You can add event IDs to this list by entering an event ID in the **Event ID** field and clicking the **Add** button (as shown in the following illustration).

Note: Event IDs are obtained from the Event Log or from the Event ID column in the Service and Support Problem List. Add the event ID into the text box using the copy and paste function.



After entering a valid event ID and clicking the **Add** button, a confirmation window displays indicating the event ID is successfully added.

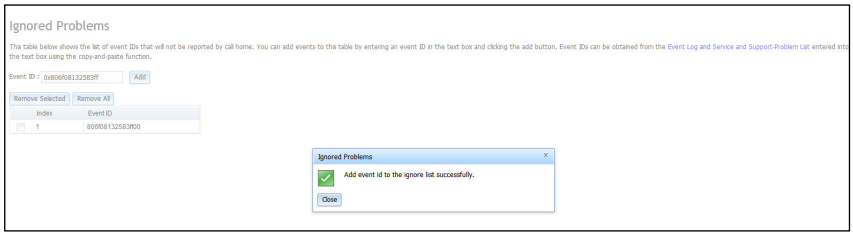


To remove an event ID from the Ignored Problems list, complete the following steps:

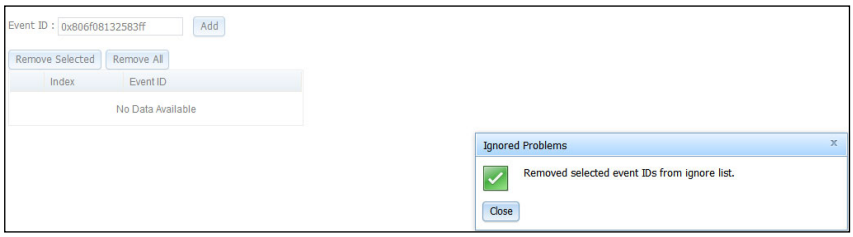
1. Select the **Index** check box of the event ID you want to remove.

   Note: To remove more than one event ID, select all applicable **Index** check boxes.

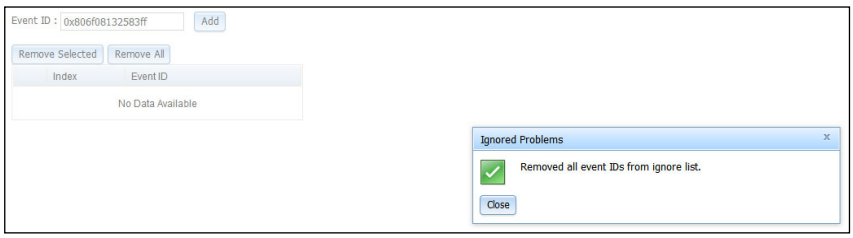
2. Click the **Remove Selected** button (as shown in the following illustration).



The selected event is deleted and a confirmation window is displayed.



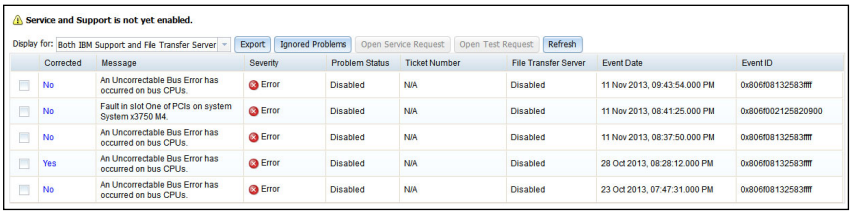
To remove all event IDs from the list, select the **Remove All** button. The following window is displayed.



Click the **Open Service Request** tab to manually open a service request by indicating the problem area and entering a text description of the issue.

Click the **Open Test Request** tab to generate a test *call home* (call IBM support) request to expedite the proper configuration of this feature or to test its proper operation.

Click the **Refresh** tab to update the list of problems with the current status (as shown in the following illustration).

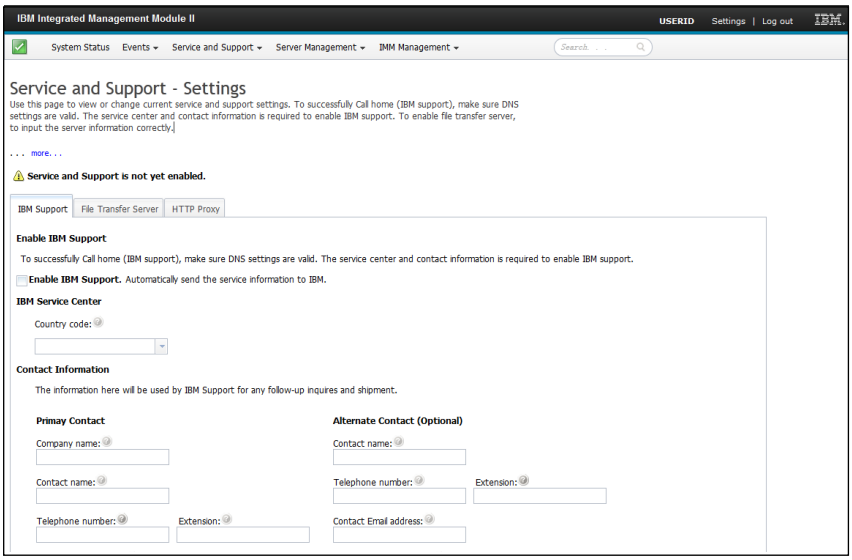


Settings option

Use the **Settings** option under the Service and Support tab to view, add, or change the service and support settings (as shown in the following illustration).

Notes:

- To successfully call home (call IBM support), make sure the Domain Name System (DNS) settings are valid.
- The service center and contact information are required to enable IBM support.
- To enable the file transfer server, the server information must be completed correctly.

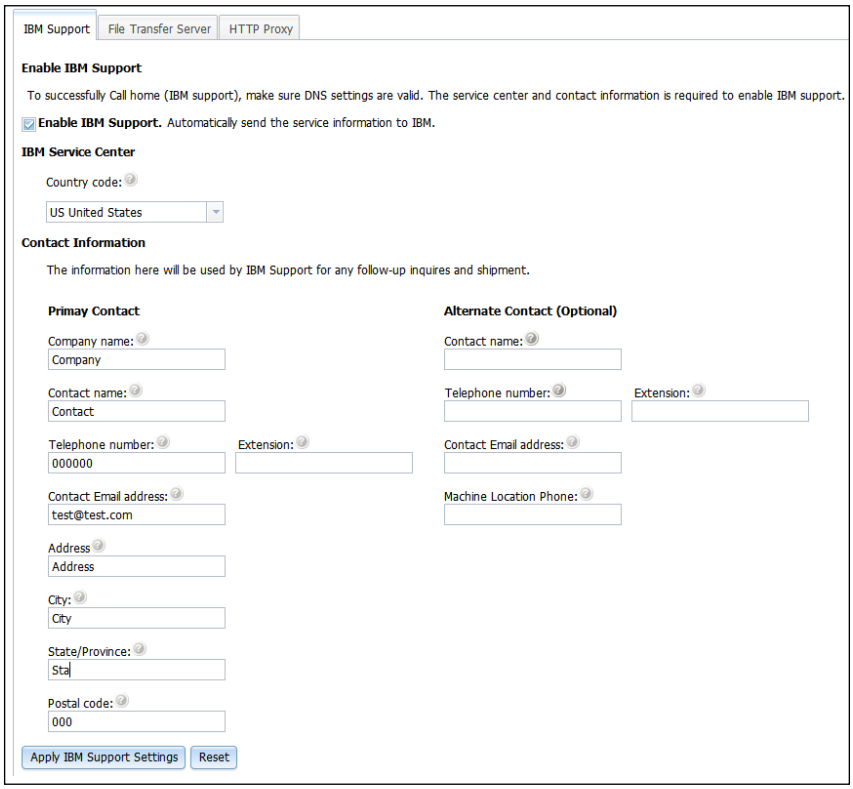


To allow the service processor to automatically send service information to IBM, complete the following steps (as shown in the following illustration):

1. Click the **IBM Support** tab.
2. Click the **Enable IBM Support** checkbox.
3. From the **IBM Service Center** list, select your IBM Service Center location.
4. Enter your **Primary Contact** information in the following fields:

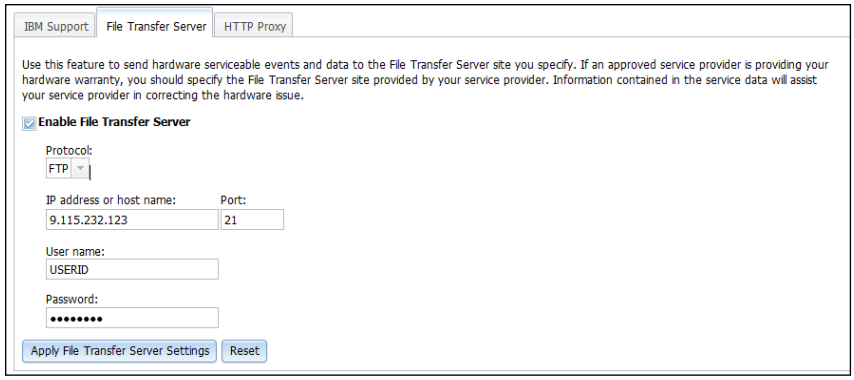
- Company name
- Contact name
- Telephone number
- Extension (if applicable)
- Contact Email address
- Address
- City
- State/Providence
- Postal code

5. Click the **Apply IBM Support Settings** button.



To allow the service processor to send hardware serviceable events and data to the specified File Transfer Server site, complete the following steps (as shown in the following illustration):

1. Click the **File Transfer Server** tab.
2. Check the **Enable File Transfer Server** checkbox.
3. Click the **Apply File Transfer Server Settings** button.

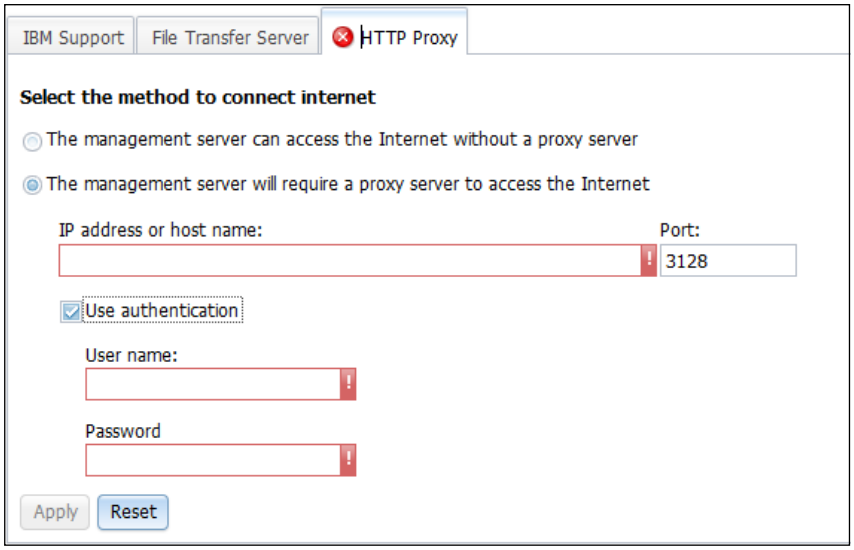


To establish the method used to connect to the internet, complete the following steps (as shown in the following illustration):

1. Click the **HTTP Proxy** tab.
2. Click one of the following methods to access the internet:
   - The management server can access the Internet without a proxy server
   - The management server will require a proxy server to access the Internet

3. If a proxy server is required to access the internet, complete the following steps (as shown in the following illustration); otherwise, continue to step 4 on page 37.
   a. In the **IP address or host name** field type the IP address or host name for the proxy server.
   b. In the **Port** field enter the port for the proxy server.

   Note: The **Use authentication** checkbox is an optional selection.

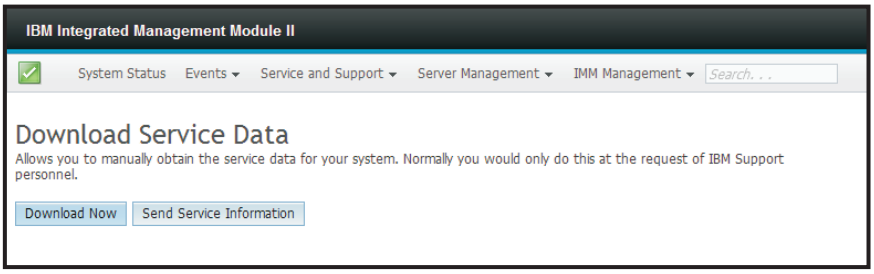


4. Click the **Apply** button.

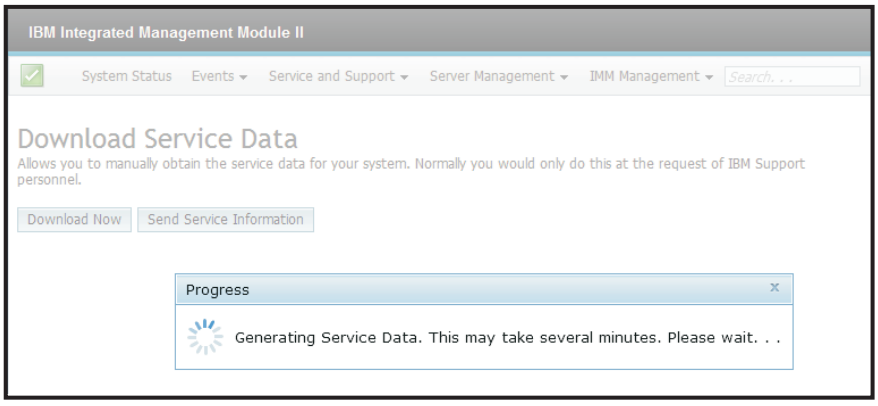
Download service data option

Use the **Download Service Data** option under the Service and Support tab to collect information and create a compressed file about the server. You can send this file to IBM Support to assist in problem determination.

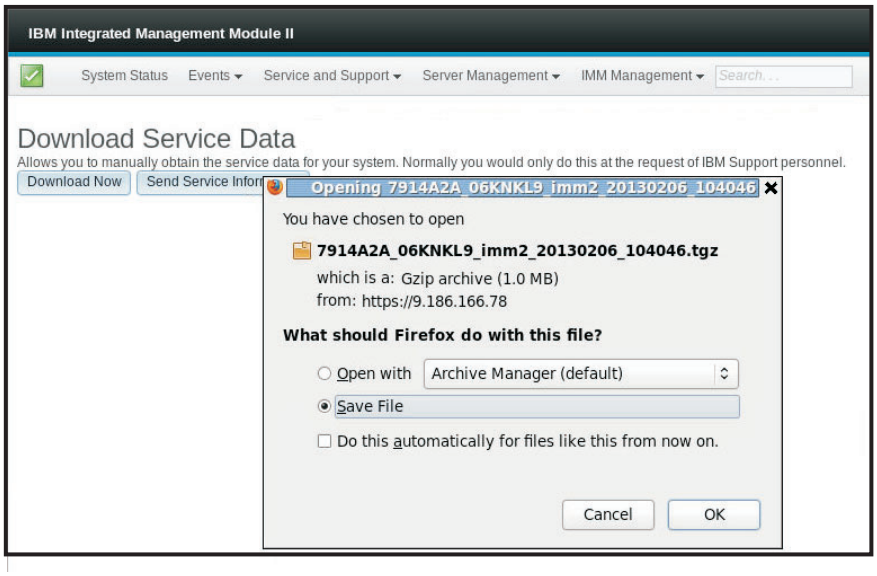
Click the **Download Now** button to download the service and support data (as shown in the following illustration).



The process for collecting the data starts. The process takes a few minutes to generate the service data that you can then save to a file. A progress window displays indicating that the data is being generated.



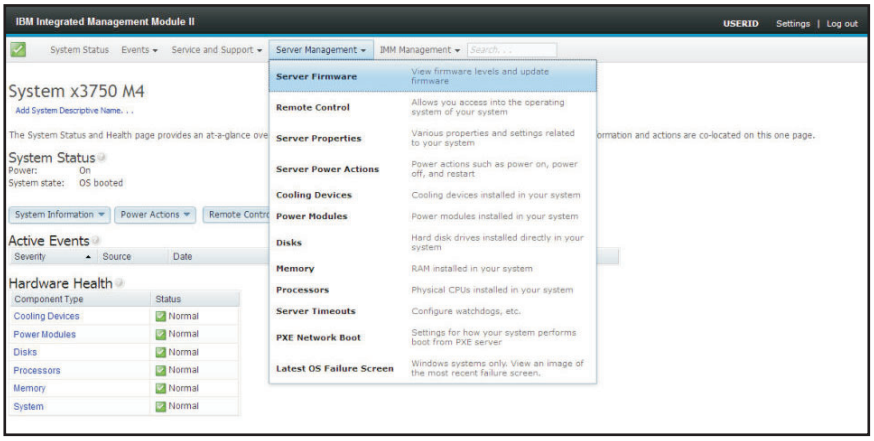
When the process is complete, the following window displays prompting you for the location in which to save the generated file.



Server management tab

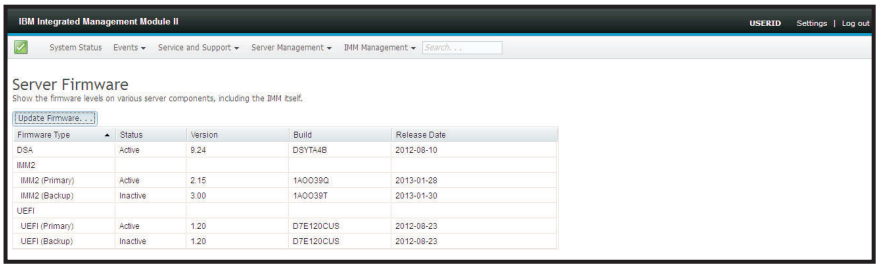
This section provides information about the options under the Server Management tab on the IMM2 web user interface home page.

The options under the Server Management tab enable you to view information about the server firmware status and control, remote control access, server properties status and control, server power actions, cooling devices, power modules, disks, memory, processors, server time-outs, PXE network boot, and latest OS failure screen (as shown in the following illustration).



Server firmware

Select the **Server Firmware** option under the Server Management tab to view the levels of firmware that are installed on the server and to apply firmware updates. The following illustration displays the server firmware levels and enables you to update the DSA, IMM2, and UEFI firmware.



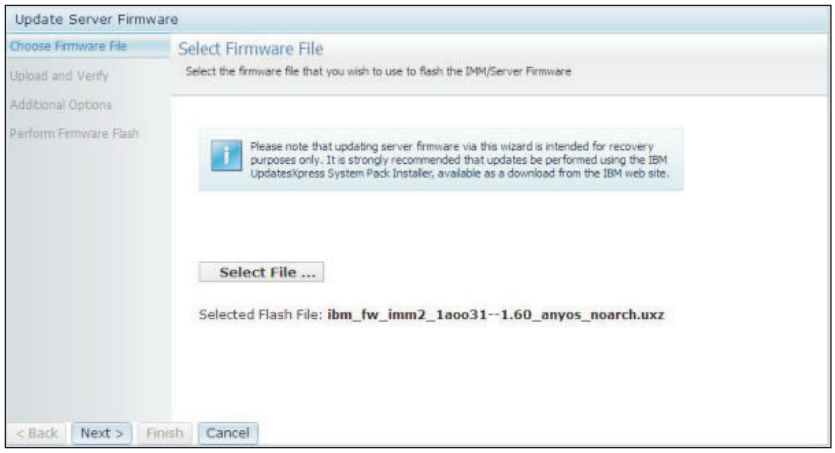
The current status and versions of firmware for the IMM2, UEFI, and DSA are displayed, including the primary and backup versions. There are three categories for the firmware status:

- **Active:** The firmware is active.
- **Inactive:** The firmware is not active.
- **Pending:** The firmware is waiting to become active.

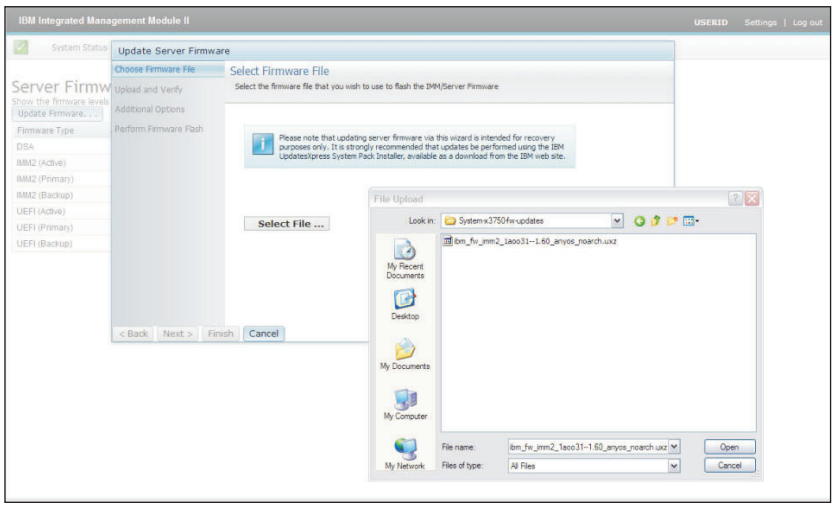
Attention: Installing the wrong firmware update might cause the server to malfunction. Before you install a firmware or device-driver update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware or device-driver version to the latest version.

To update the firmware, select the **Update Firmware...** button. The Update Server Firmware window displays (as shown in the following illustration). You can click **Cancel** and return to the previous Server Firmware window or click on the **Select File...** button to select the firmware file that you want to use to flash the server firmware.

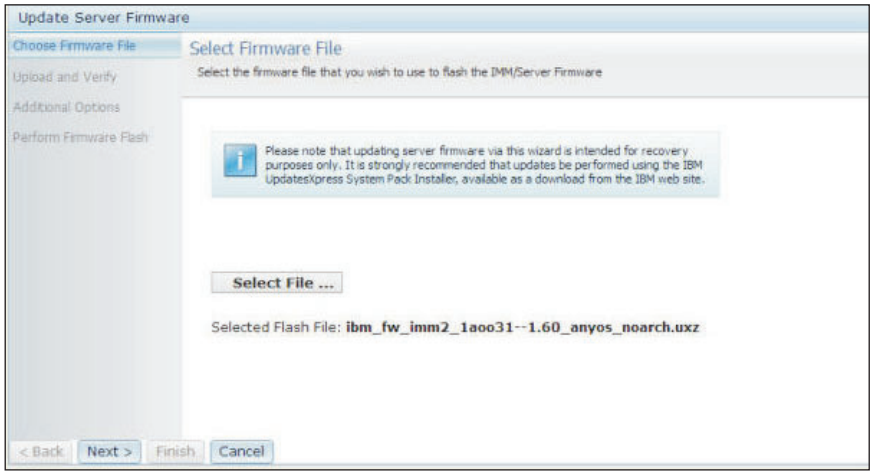
Note: Before you click on the **Select File...** button, read the warning displayed in the window prompt before you continue.



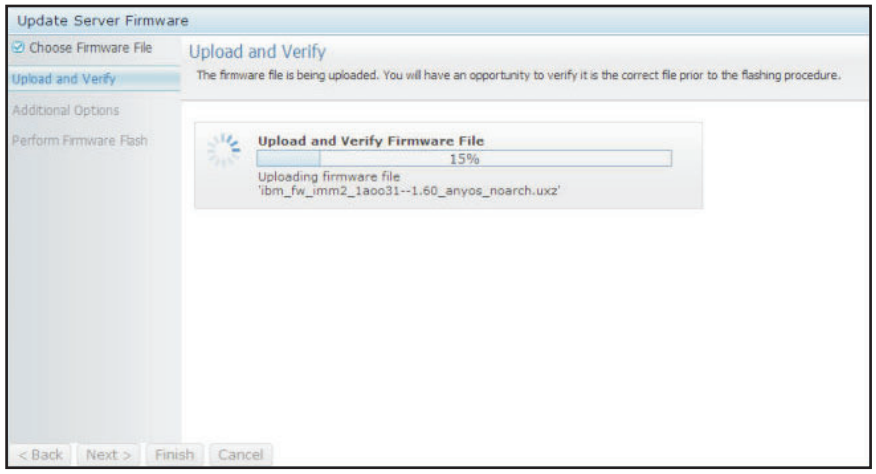
When you click the **Select File...** button, the File Upload window displays, which allows you to browse to the desired file.



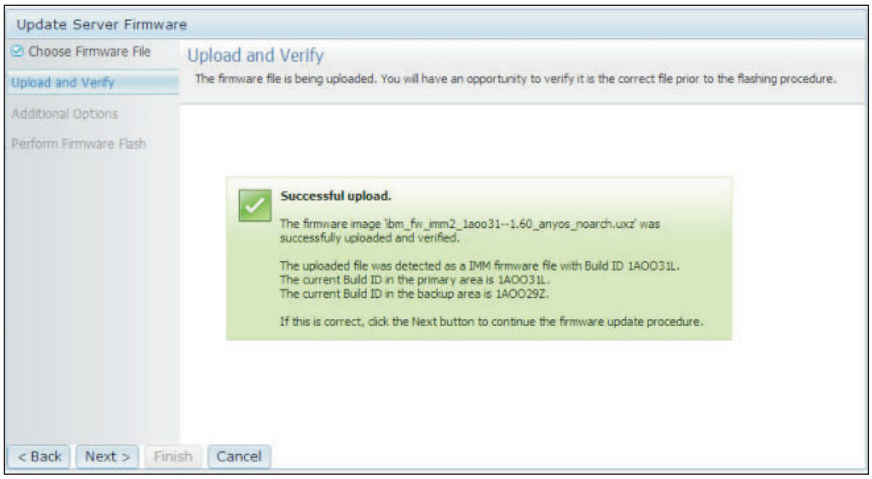
After you navigate to the file that you want to select, click the **Open** button, you are returned to the Update Server Firmware window with the selected file displayed (as shown in the following illustration).



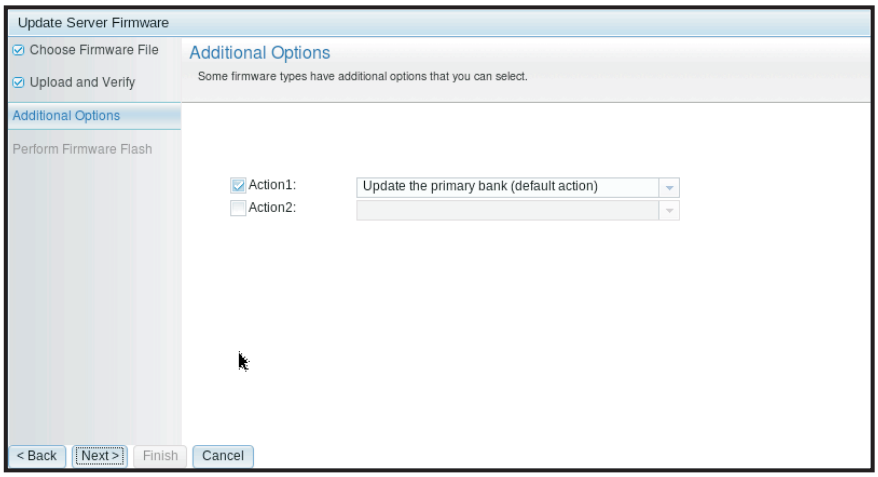
Click the **Next >** button to begin the upload and verify process on the selected file (as shown in the following illustration). A progress meter will be displayed as the file is being uploaded and verified.



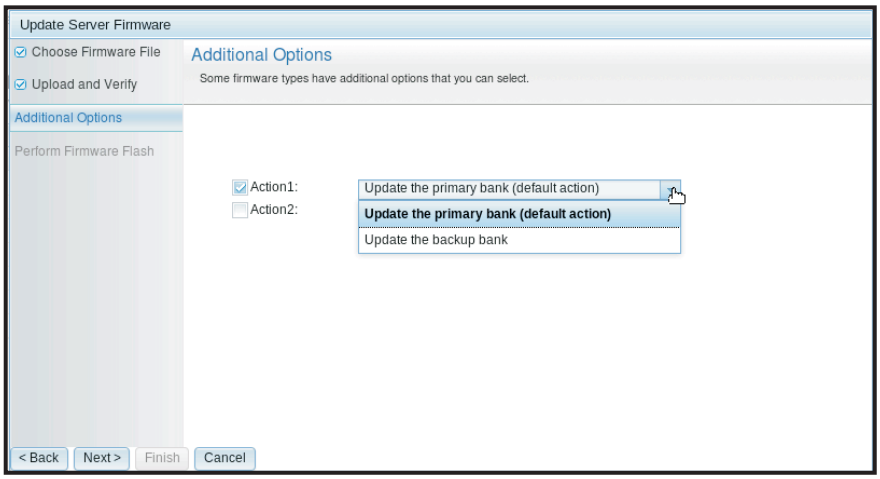
A status window opens (as shown in the following illustration) so you can verify that the file you selected to update is the correct file. The window will have information regarding the type of firmware file that is to be updated, such as DSA, IMM2, or UEFI. If the information is correct, click the **Next >** button. If you want to redo any of the selections, click the **< Back** button.



When you click the Next > button, a set of additional options are displayed as shown in the following illustration.



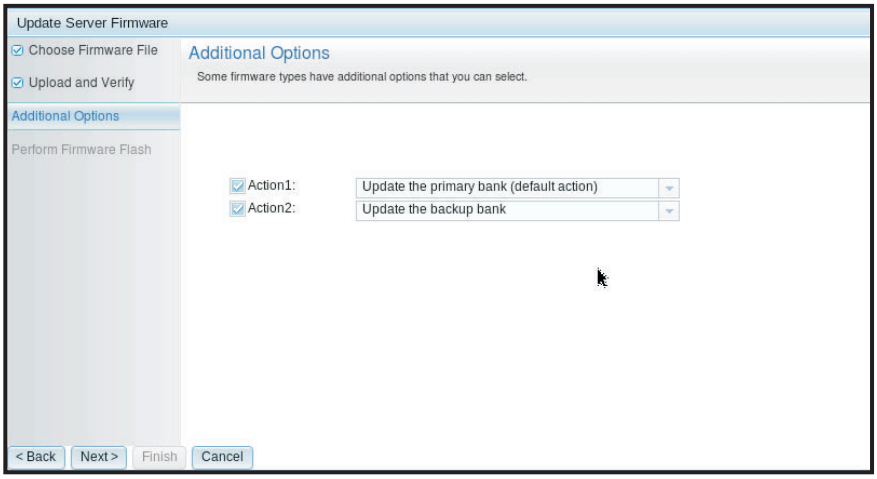
The drop-down menu beside **Action 1** (shown in the following illustration) gives you the choice to **Update the primary bank (default action)** or **Update the backup bank**.



After you select an action, you are returned to the previous window to allow additional actions by clicking the **Action 2** checkbox.

When the action is loaded, the selected action and a new **Action 2** drop-down menu are displayed (as shown in the following illustration).

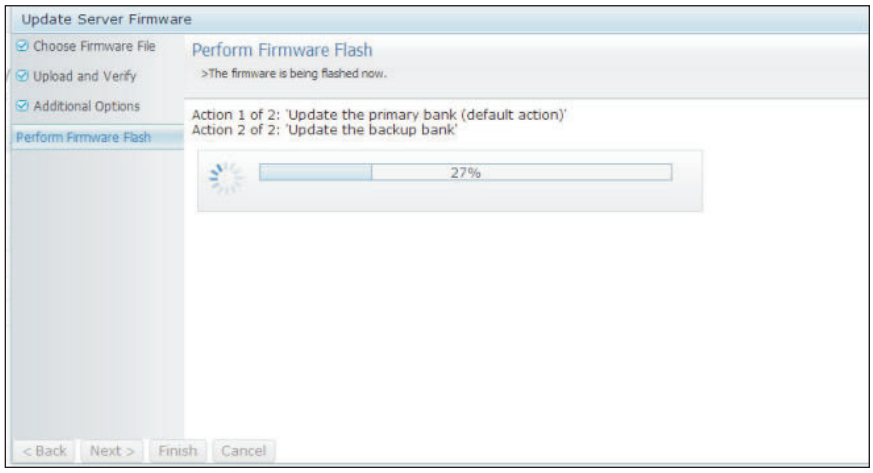
Note: To disable an action, click the checkbox beside the related action.



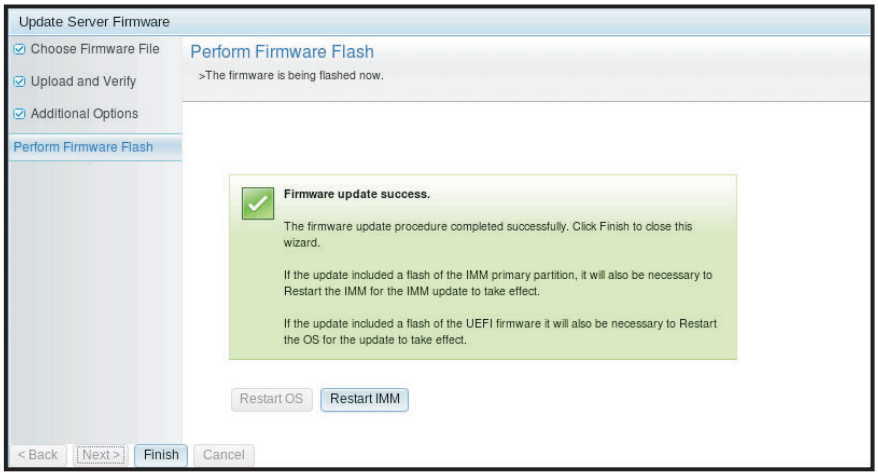
The previous screen shows that for Action 1, the primary bank is selected to be updated. You can also select to update the backup bank under Action 2 (as shown in the previous window). Both the primary bank and the backup bank will be updated at the same time when you click **Next >**.

Note: Action 1 must be different from Action 2.

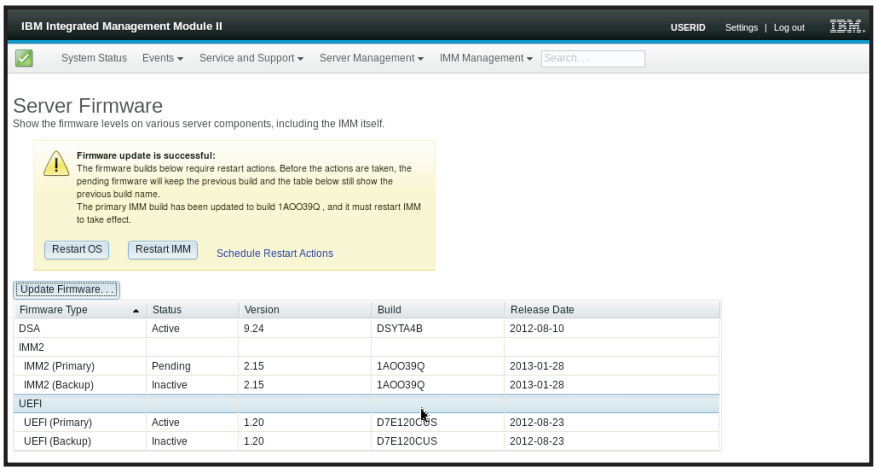
A progress meter is displayed that shows the progress of the firmware update (as shown in the following illustration).



When the firmware update is completed successfully, the following window opens. Select the related operation according to the displayed content to complete the update process.



If the primary firmware update did not complete, the following window opens.



Remote control

This section provides information about the remote control feature.

The ActiveX client and Java client are graphical remote consoles that allow you to remotely view the server video display and interact with it using the client keyboard and mouse.

Notes:

- The ActiveX client is only available with the Internet Explorer browser.
- To use the Java client, the Java Plug-in 1.5 or later release is required.
- The Java client is compatible with the IBM Java 6 SR9 FP2 or later release.

The remote control feature consist of two separate windows:

- **Video Viewer**

  The Video Viewer window uses a remote console for remote systems management. A remote console is an interactive graphical user interface (GUI) display of the server viewed on your computer. Your monitor displays exactly what is on the server console and you have keyboard and mouse control of the console.

Note: The video viewer is able to display only the video that is generated by the video controller on the system board. If a separate video controller adapter is installed and is used in place of the system's video controller, the IMM2 cannot display the video content from the added adapter on the remote video viewer.

- **Virtual Media Session**

  The Virtual Media Session window list all of the drives on the client that can be mapped as remote drives and allows you to map ISO and diskette image files as virtual drives. Each mapped drive can be marked as read-only. The CD, DVD drives, and ISO images are always read-only. The Virtual Media Session window is accessed from the Tools menu bar of the Video Viewer window.

  Notes:

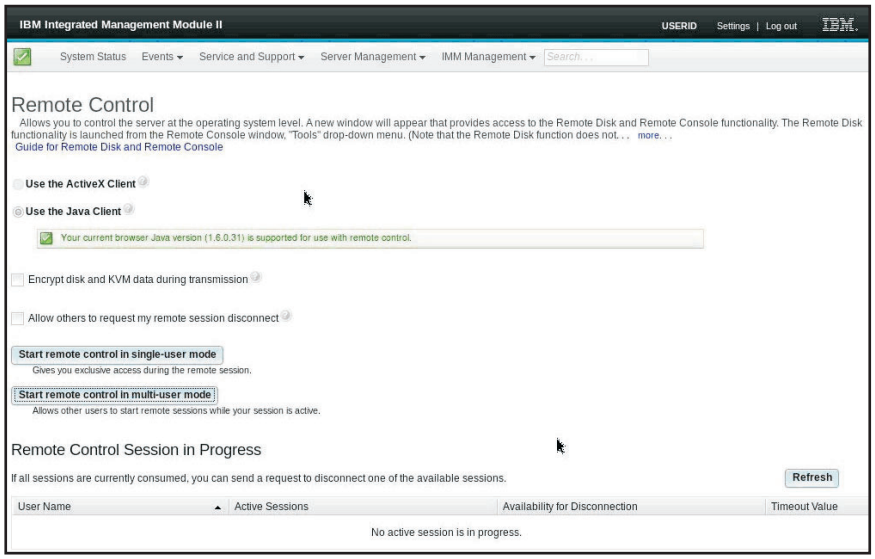
  – The Virtual Media Session can only be used by one remote control session client at a time.

  – If the ActiveX client is used, a parent window will open and that window must remain open until the remote session is complete.

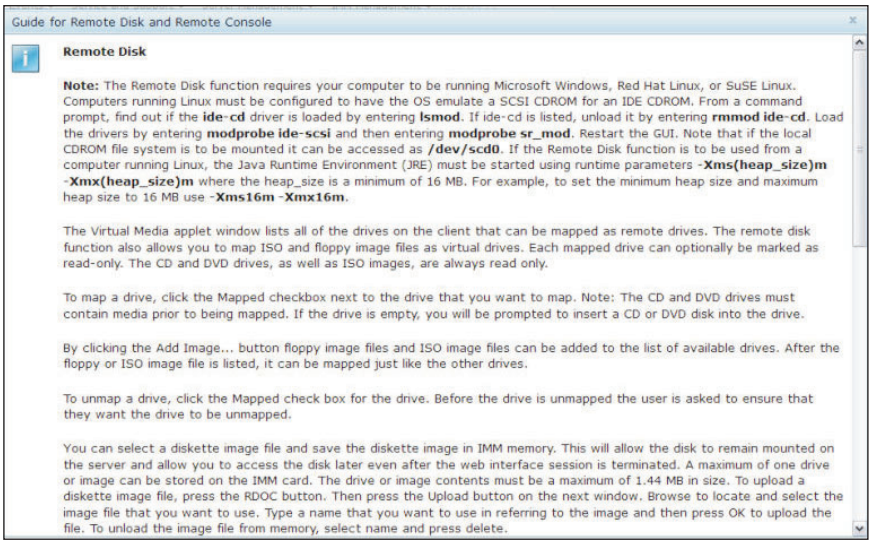
To remotely access a server console, complete the following steps:

1. Log in to the IMM2, (see “Logging in to the IMM2” on page 10 for additional information).
2. Access the Remote Control page by selecting one of the following menu choices:
   - Select the **Remote Control** option from the Server Management tab.
   - Click **Remote Control...** on the System Status page.

   The Remote Control page opens as shown in the following illustration.

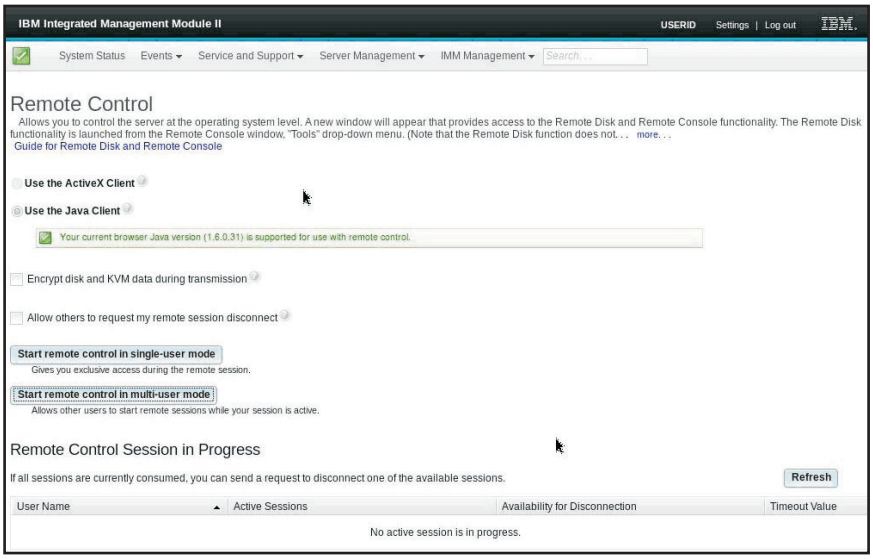


3. You can click the **Guide for Remote Disk and Remote Console** link to access additional information. The following illustration shows the Guide for Remote Disk and Remote Console window.



a. Click **Close** to exit from the Guide for Remote Disk and Remote Console window.

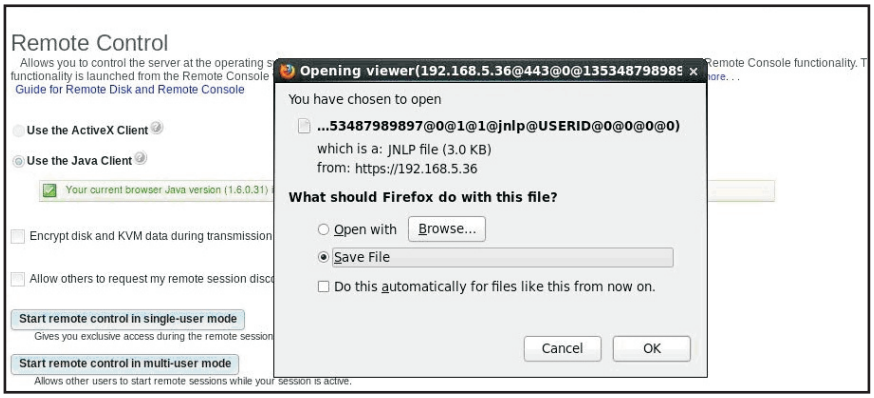
4. Select one of the following graphical remote console choices:
   - To use the Internet Explorer as your browser, select **Use the ActiveX Client**.
   - To use the Java client, select **Use the Java Client** as shown in the following illustration.



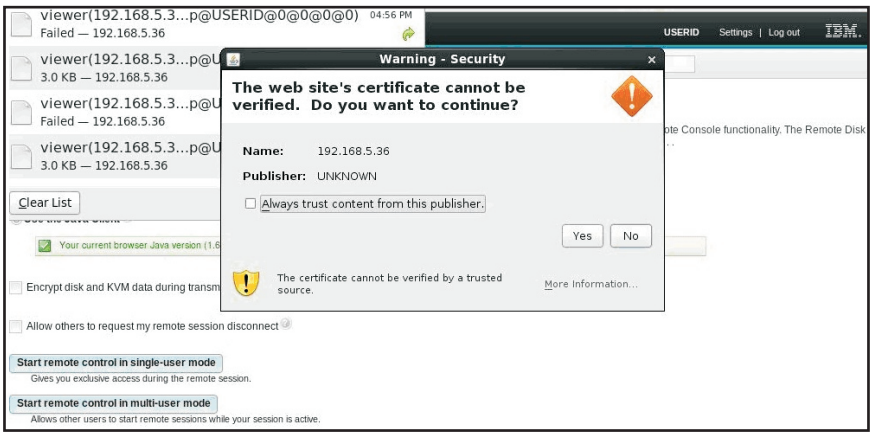
Notes:

- If you are not using the Internet Explorer browser, only the Java client can be selected.
- The ActiveX and Java clients have identical functionality.
- A status line will be displayed indicating whether your client is supported.

The following window opens. It shows the information that the browser (for example, the Firefox browser) will use to open the Viewer file.



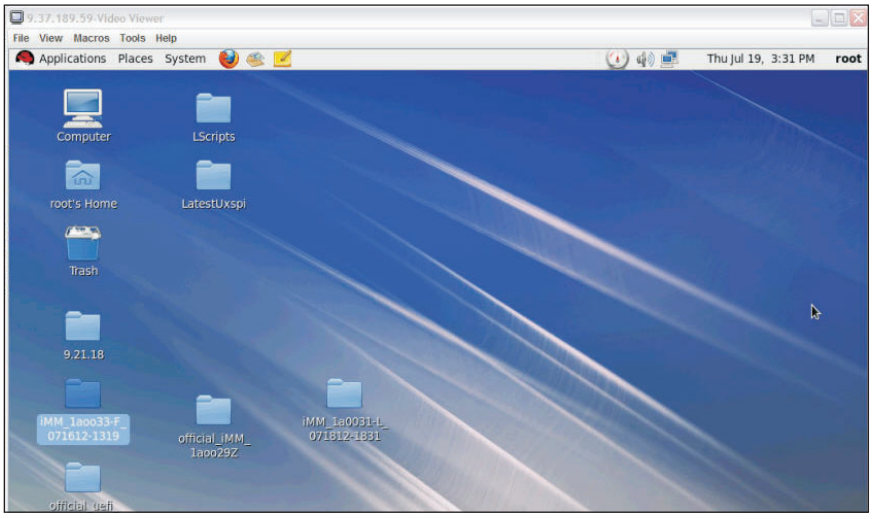
5. After the browser downloads and opens the Viewer file, a confirmation window opens with a warning about the website certificate verification (as shown in the following illustration). Click **Yes** to accept the certificate.



6. To control the server remotely, select one of the following menu choices:
   - To have exclusive remote access during your session, click **Start remote control in single User mode**.
   - To allow others to have remote console access during your session, click **Start remote control in multi user mode**.

     Note: If the **Encrypt disk and KVM data during transmission** checkbox is selected before the Video Viewer window is opened, the disk data is encrypted with ADES encryption during the session.

     The Video Viewer window opens as (shown in the following illustration). This window provides access to the Remote Console functionality.



7. Close the Video Viewer and the Virtual Media Session windows when you are finished using the Remote Control feature.

Notes:

- The Video Viewer will automatically close the Virtual Media Session window.
- Do *not* close the Virtual Media Session window if a remote disk is currently mapped. See "Remote disk" on page 123 for instructions about closing and unmapping a remote disk.
- If you have mouse or keyboard problems when you use the remote control functionality, see the help that is available from the Remote Control page in the web interface.
- If you use the remote console to change settings for the IMM2 in the Setup utility program, the server might restart the IMM2. You will lose the remote console and the login session. After a short delay you can log in to the IMM2 again with a new session, start the remote console again, and exit the Setup utility program.

Important: The IMM2 uses a Java applet or an ActiveX applet to perform the remote presence function. When the IMM2 is updated to the latest firmware level, the Java applet and the ActiveX applet are also updated to the latest level. By default, Java caches (stores locally) applets that were previously used. After a flash update of the IMM2 firmware, the Java applet that the server uses might not be at the latest level.

To correct this problem, turn off caching. The method used will vary based on the platform and Java version. The following steps are for Oracle Java 1.5 on Windows:

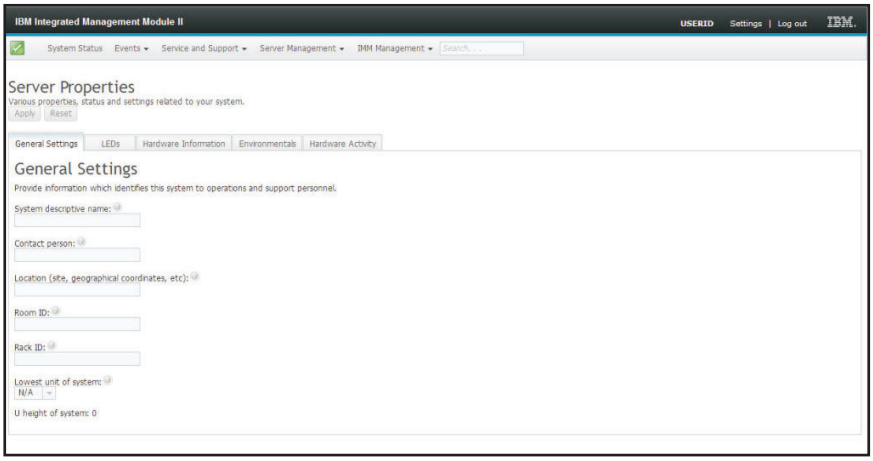
1. Click **Start → Settings → Control Panel**.
2. Double-click **Java Plug-in 1.5**. The Java Plug-in Control Panel window opens.
3. Click the **Cache** tab.
4. Choose one of the following options:
   - Clear the **Enable Caching** check box so that Java caching is always disabled.
   - Click **Clear Caching**. If you choose this option, you must click **Clear Caching** after each IMM2 firmware update.

For more information about updating IMM2 firmware, see "Updating the server firmware" on page 125.

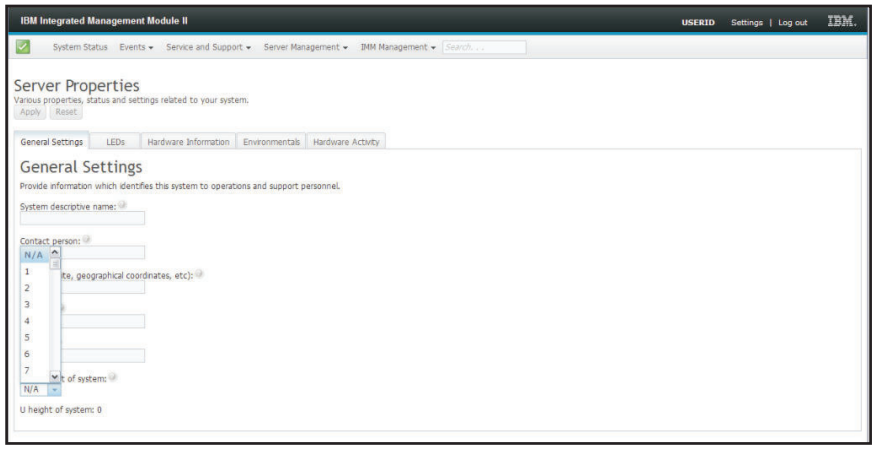
For more information about the remote control feature, see “Remote presence and remote control functions” on page 113.

Server properties

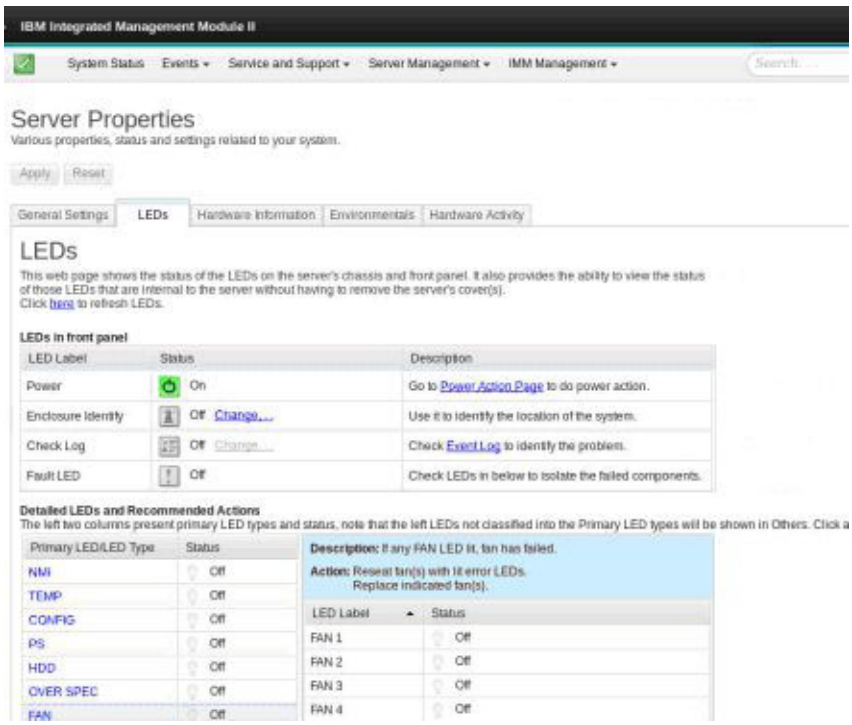
Select the **Server Properties** option under the Server Management tab to set various parameters to help identify the system. You can specify the **System descriptive name**, **Contact person**, **Location**, and additional information as shown in the following illustration. The information that you enter in these fields will take effect when you click **Apply**. To clear the information that was typed in the fields since the last time you applied changes, click **Reset**.



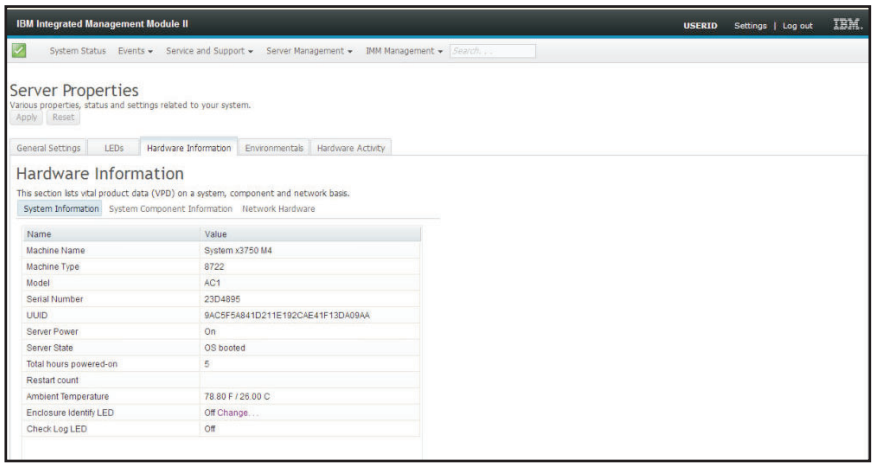
In the following illustration, you can specify the **Lowest unit of the system**. The **Lowest unit of the system** field requires a connection to the management module (for example the Advanced Management Module or Chassis Management Module).



To view the LEDs in the system, click the **LED** tab. The following window opens.

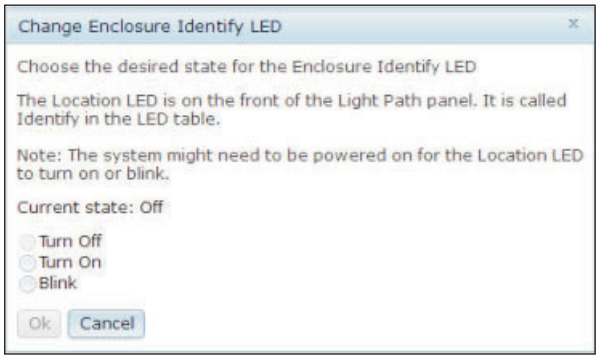


To view system information, system component information, and network hardware information, click the **Hardware Information** tab. Select the appropriate tab within the Hardware Information tab to view various Vital Product Data (VPD) information. The **System Information** tab provides information such as the machine name, serial number, and model. The following illustration shows the System Information window.

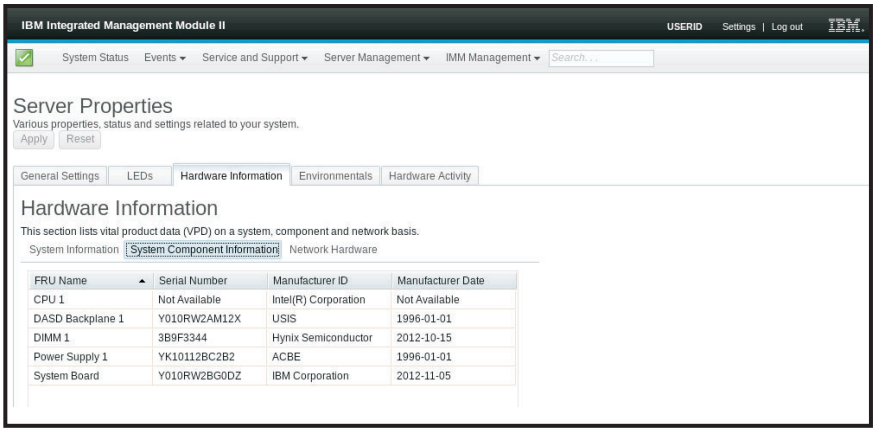


The status of the **Enclosure Identify LED** can be viewed and changed from System Information window. To change the **Enclosure Identify LED**, click the **Change..** link. The following window opens.

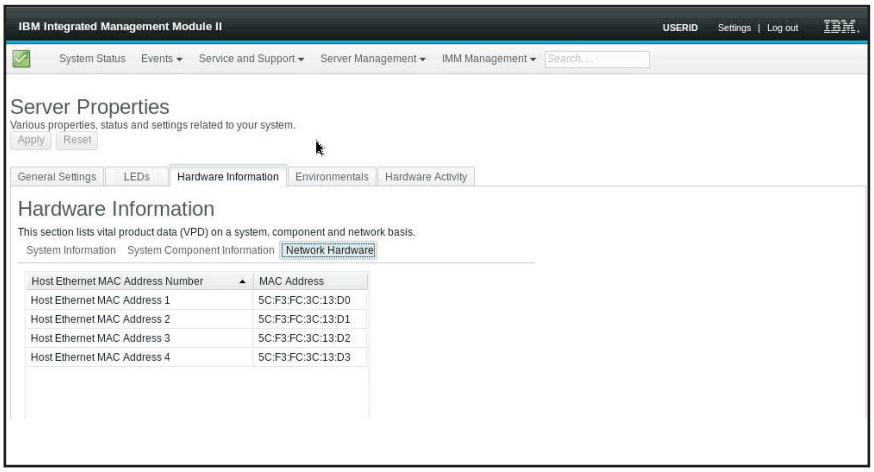
Note: The Enclosure Identity LED is on the front of the Light Path panel.



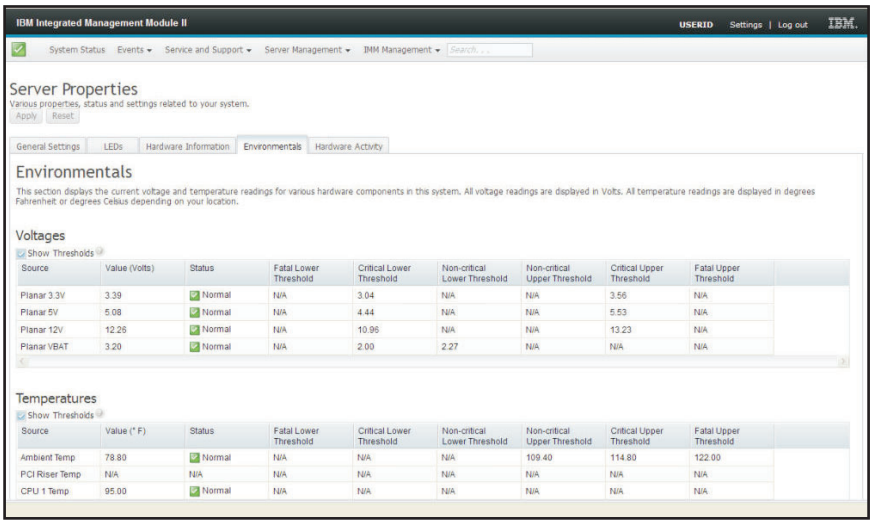
Select the **System Component Information** tab to view component information. Component information includes the FRU Name, Serial Number, and Manufacturer ID and Manufacturer Date. The following illustration shows the information that you will see when you click the **System Component Information** tab.



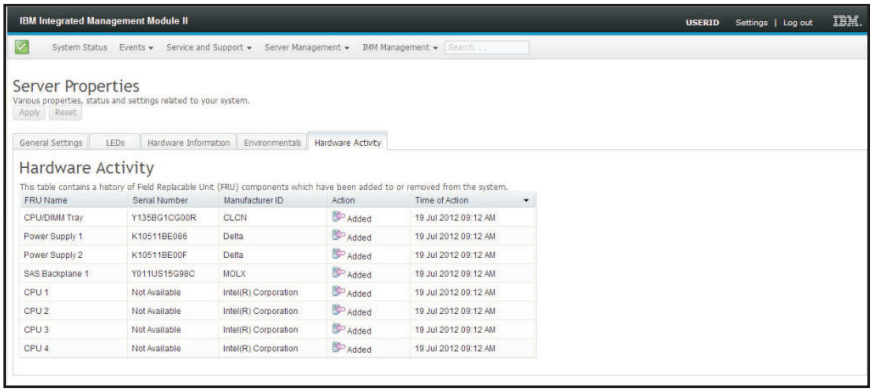
Select the **Network Hardware** tab to view the network hardware information. Network hardware information includes the Host Ethernet MAC Address Number and MAC Address. The following illustration shows the information that you will see when you click the **Network Hardware** tab.



Select the **Environmentals** tab on the Server Properties page to view the voltages and temperatures of the hardware components in the system. The following window opens. The **Status** column in the table shows normal activity or problem areas in the server.



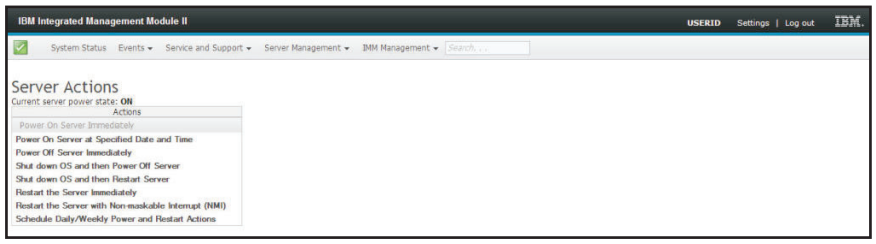
The **Hardware Activity** tab on the Server Properties page provides a history of the hardware that has been added or removed from the system. The following illustration shows the information that you will see when you click the **Hardware Activity** tab.



Server power actions

This section provides information about the Server Power Actions option under the Server Management tab on the IMM2 web interface home page.

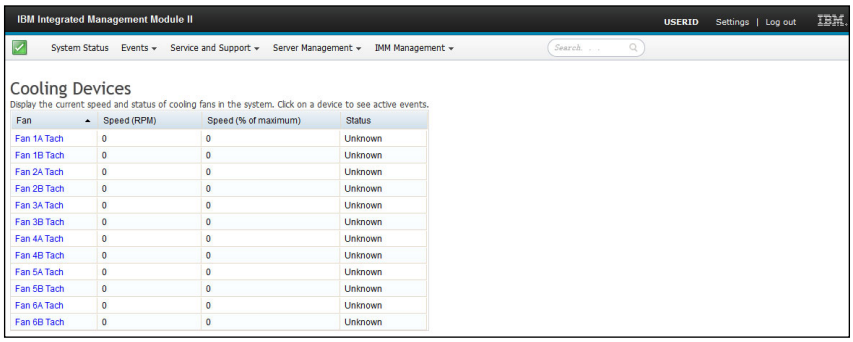
Select the **Server Power Actions** option under the Server Management tab to view a list of actions that you can use to control system power. The following illustration is an example of the Server Power Actions window.



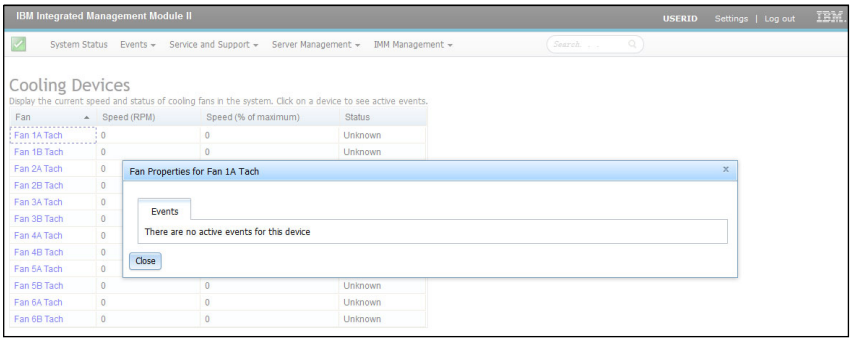
You can choose to power the server on immediately or at a scheduled time. You can also choose to shut down and restart the operating system. For more information about controlling the server power, see, “Controlling the power status of the server” on page 112.

Cooling devices

Select the **Cooling Devices** option under the Server Management tab to view the current speed and status of cooling fans in the server (as shown in the following illustration).

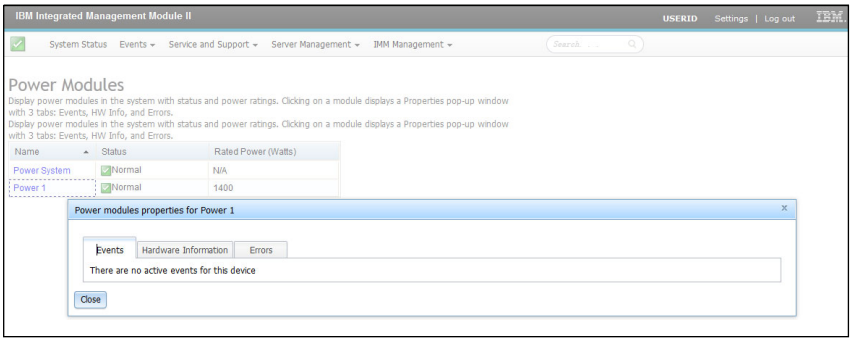


Click on a cooling device (Fan link) in the table to view any active events for the device (as shown in the following screen).

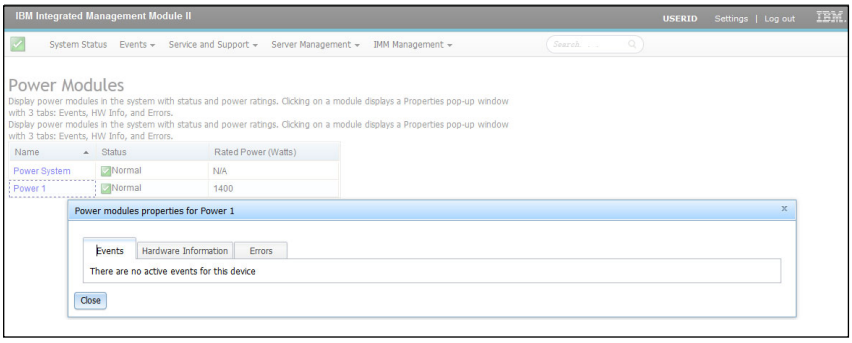


Power modules

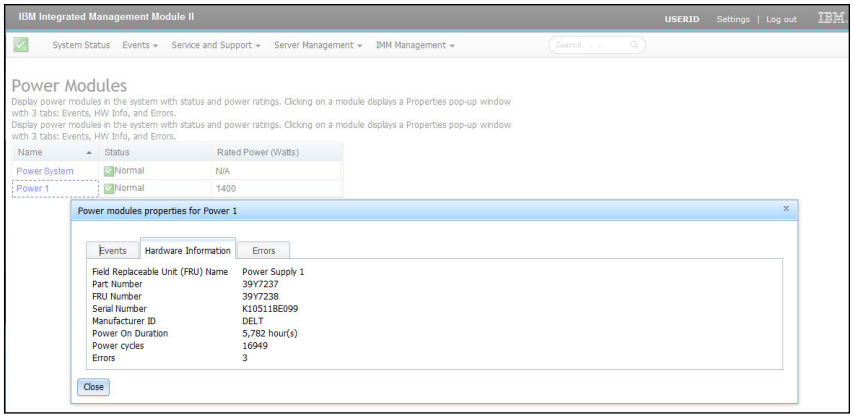
Select the **Power Modules** option under the Server Management tab to view the power modules in the system with status and power ratings. Click on a power link in the table to view active events, hardware information, and errors associated with the power module (as shown in the following illustration).



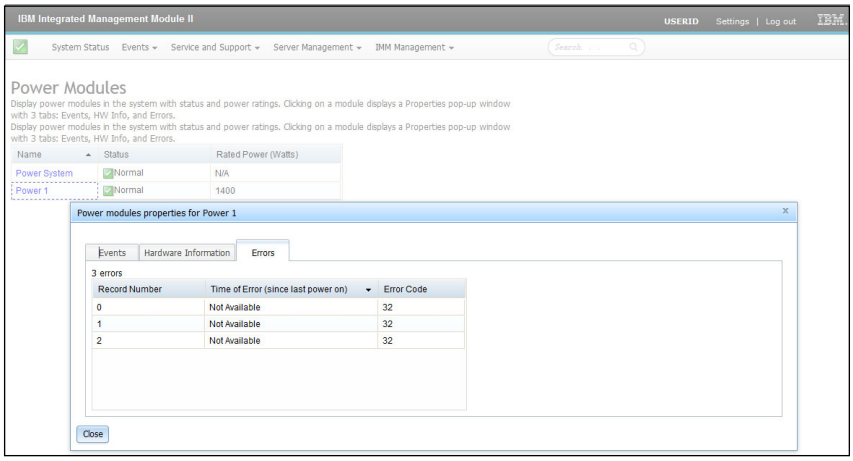
The Events tab displays active events, if any (as shown in the following screen).



Click the **Hardware Information** tab to view details about the component such as the FRU name and manufacturer ID (as shown in the following illustration).

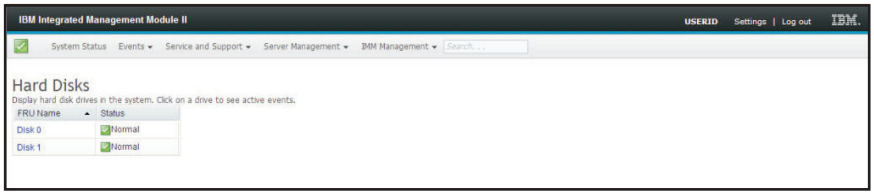


Click on the **Errors** tab to view detailed information about the errors of the Power Modules (as shown in the following illustration).



Disks

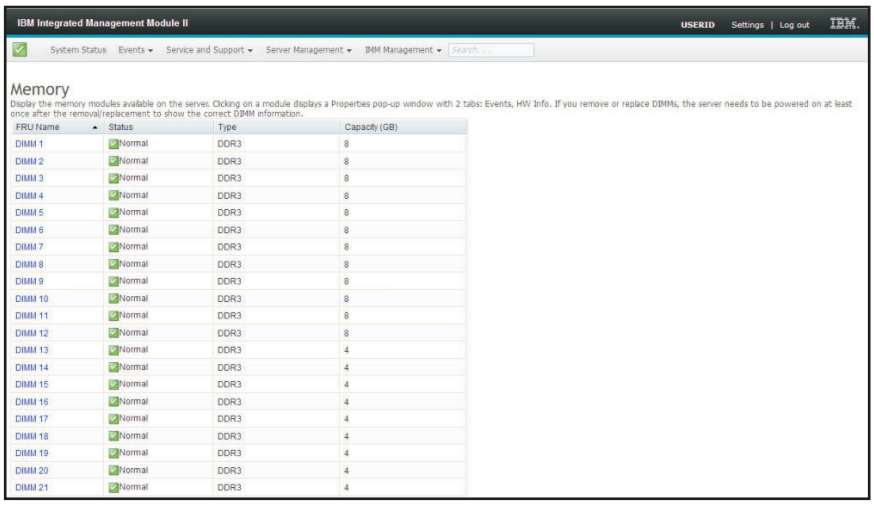
Select the **Disks** option under the Server Management tab to view the hard disk drives in the system (as shown in the following illustration). Click on a hard disk drive to view the events associated with the hard disk drive.



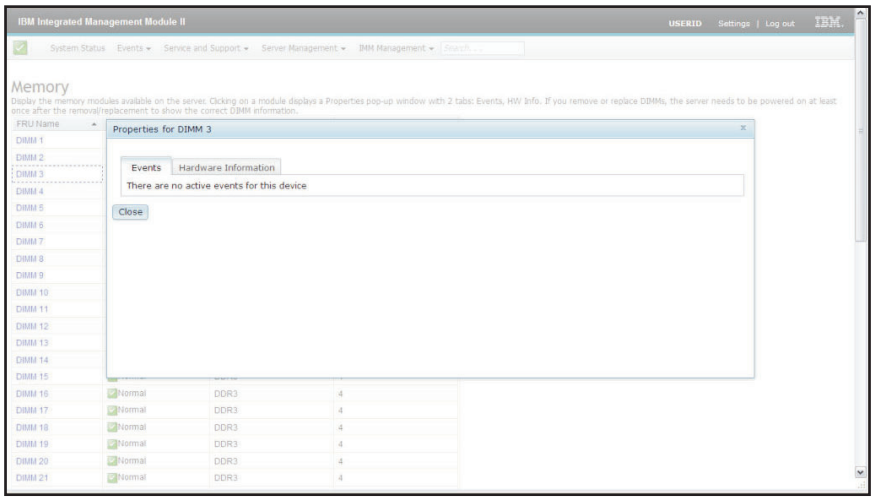
Memory

Select the **Memory** option under the Server Management tab to view information about the memory modules installed in the system. The following window opens. Each memory module is displayed in the table as a link that you can click to get more detailed information about the memory module. The table also displays the status of the DIMM, DIMM type, and DIMM capacity.

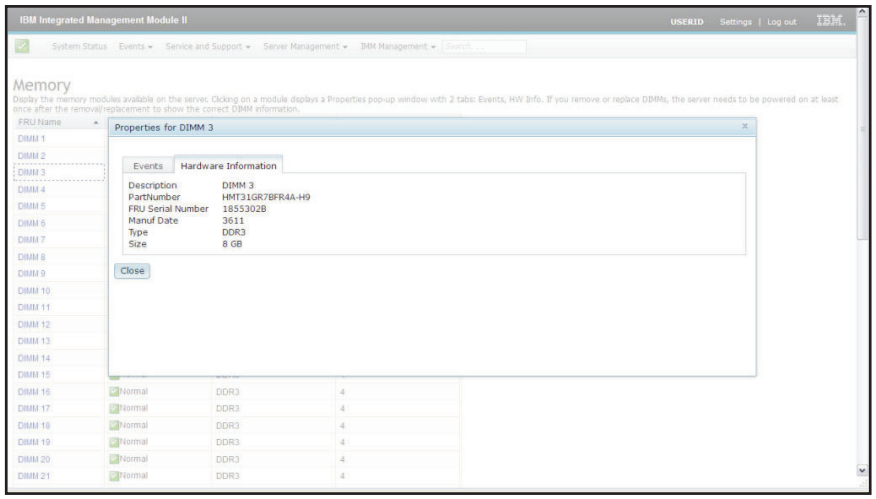
Note: If you remove or replace a DIMM, you must restart the system to view the updated DIMM information for the changes that you made to the system DIMMs.



Click on a **DIMM** link in the table to view any active events and more information about the component (as shown in the following screen).

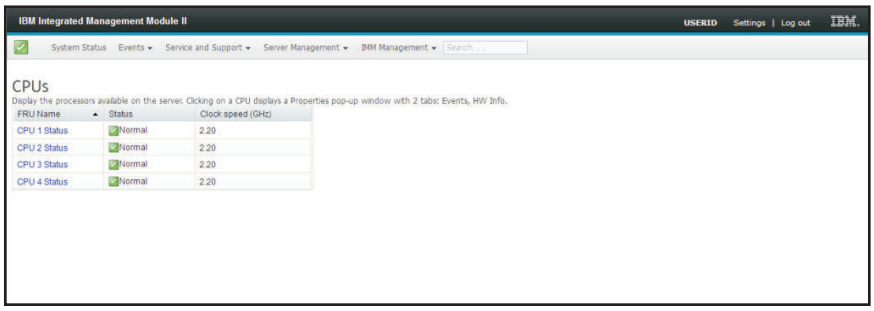


Click on the **Hardware Information** tab to view details about the component such as the description, part number, FRU serial number, manufacturing date (week/year), type (for example, DDR3), and size in gigabytes (as shown in the following illustration).

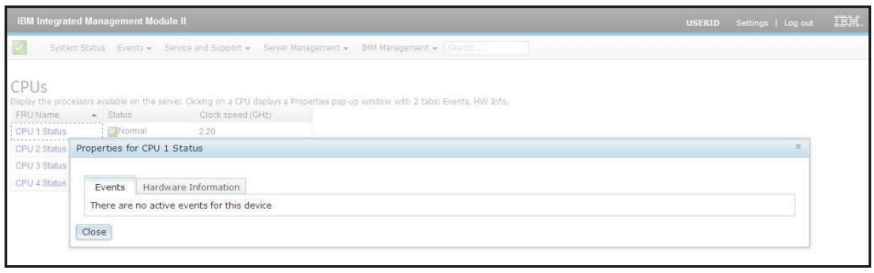


Processors

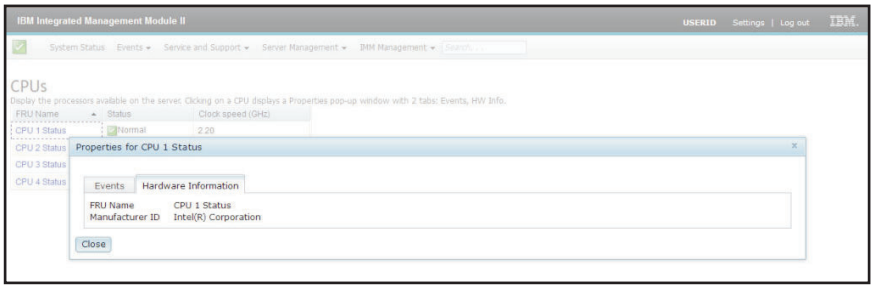
Select the **Processors** option under the Server Management tab to view information about the microprocessors that are installed in the system. The following window opens.



Click on a **CPU** link in the table to view any active events and more information about the component (as shown in the following illustration).



Click on the **Hardware Information** tab to view details about the component such as the FRU name and manufacturer ID (as shown in the following illustration).

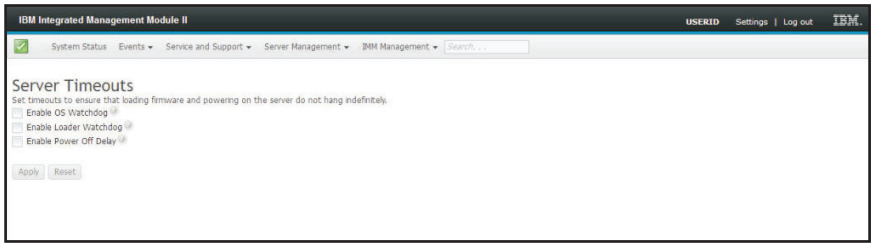


Server timeouts

Select the **Server Timeouts** option under the Server Management tab to set timeouts to ensure that during a firmware update and powering on the server, the server does not hang indefinitely. You can enable this function by setting the values for the options.

Note: Server timeouts require that the in-band USB interface or LAN over USB be enabled to use commands. For more information about configuring the USB interface, see "Configuring USB" on page 89.

The following illustration shows the Server Timeouts window.



For additional information about server timeouts, see "Setting server timeouts" on page 64.

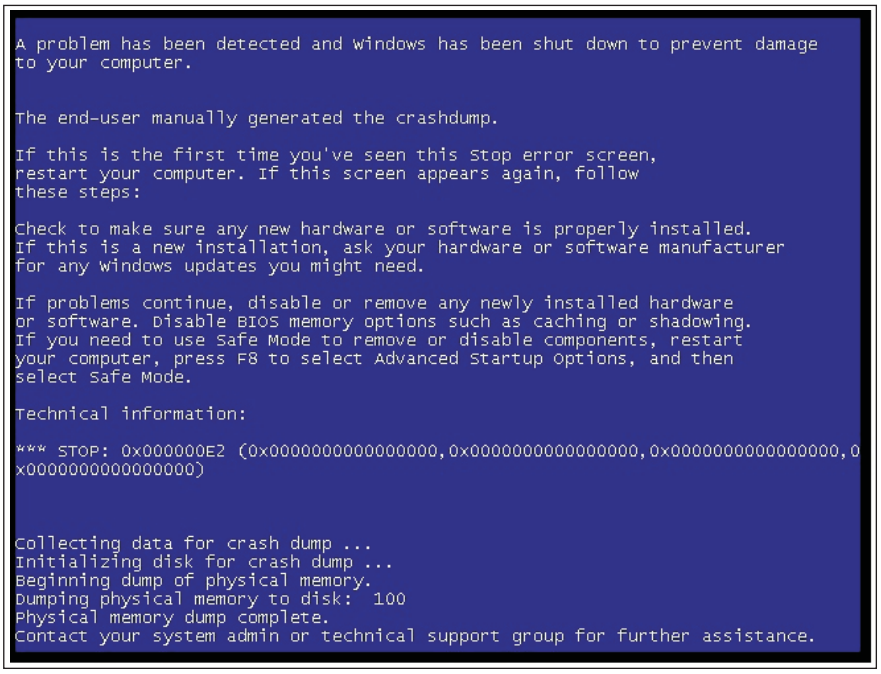
PXE network boot

Select the **PXE Network Boot** option under the Server Management tab to set up your server to attempt a PXE network boot at the next server restart. For more information about setting up a PXE network boot, see "Setting up PXE network boot" on page 124.

Latest OS failure screen

Select the **Latest OS Failure Screen** option under the Server Management tab to view or clear the most recent operating system failure screen data that has been saved by the IMM2. The IMM2 stores only the most recent error event information, overwriting earlier OS failure screen data when a new error event occurs.

The following illustration is an example of the OS Failure Screen.



For more information about the Latest OS Failure Screen option, see "Capturing the latest OS failure screen data" on page 139.

IMM Management tab

This section provides information about the options under the IMM Management tab on the IMM2 web user interface home page.

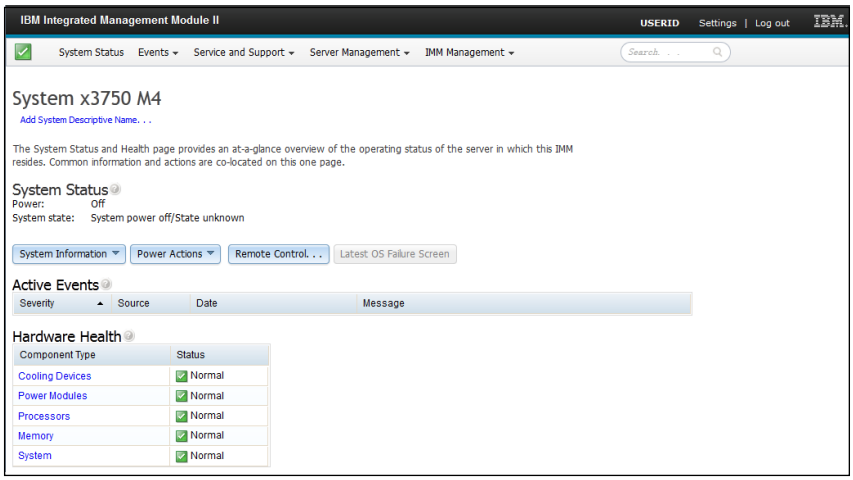
The options under the IMM Management tab enable you to view and modify the IMM2 setting. For the list of the options and details on how to use the options to configure the IMM2, see Chapter 4, "Configuring the IMM2," on page 61.

Chapter 4. Configuring the IMM2

The IMM Management tab contains options to configure the IMM2. Use the IMM Management tab to view and change IMM2 settings. The following options are listed under the IMM Management tab (as shown in the following illustration).

- IMM Properties
- Users
- Network
- Security
- IMM Configuration
- Restart IMM
- Reset IMM to factory defaults
- Activation Key Management

Note: In an IBM Flex System, some settings are managed by the IBM Flex System Chassis Management Module (CMM) and cannot be modified on the IMM2.



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

- Access the server firmware information
- Set the date and time:
  - 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
- Access the IMM2 serial port information:
  - Configure the IMM2 serial port
  - Set IMM2 command-line interface (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 Secure Shell (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
    - Set maximum transmission unit
    - Virtual LAN (VLAN) enablement
- Configure SNMP settings:
  - SNMPv1 enablement and configuration:
    - Set contact information
    - Community management
  - SNMPv3 enablement and configuration:
    - Set contact information
    - User account configuration
  - SNMP traps enablement and configuration
    - Configure the events alerted in the Traps tab
- 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 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 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.

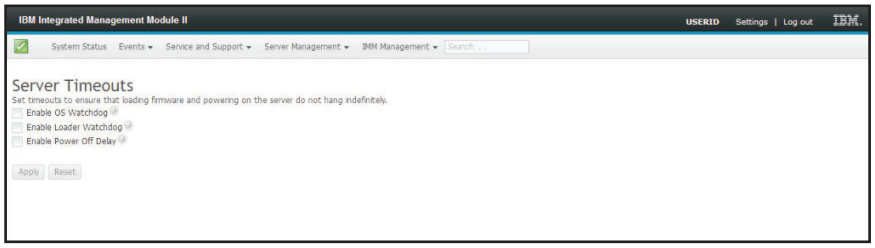
From the Reset IMM2 to factory defaults.. page, you can reset the IMM2 configuration to its factory default settings.

From the Activation Key Management page, you can manage activation keys for optional IMM2 and server Features on Demand (FoD). See Chapter 7, "Features on Demand," on page 145 for information about managing FoD activation keys.

Setting server timeouts

Use the Server Timeouts option to set timeouts to ensure that the server does not hang indefinitely during a firmware update or powering on the server. You can enable this function by setting the value for this option shown in the following illustration.

Note: Server timeouts require that the in-band USB interface or LAN over USB be enabled to use commands. For additional information about enabling and disabling the USB interface, see "Configuring USB" on page 89.



To set the server timeout values, complete the following steps:

1. Log in to the IMM2 where you want to set the server timeouts. (see "Logging in to the IMM2" on page 10).
2. Click **Server Management**; then, select **Server Timeouts**.

   You can set the IMM2 to respond automatically to the following events:

   - Halted operating system
   - Failure to load operating system
3. Enable the server timeouts that correspond to the events that you want the IMM2 to respond to automatically. See "Server timeout selections" for a description of each choice.
4. Click **Apply**.

   Note: There is a **Reset** button that you can use to clear all timeouts simultaneously.

Server timeout selections

Enable OS Watchdog

Use the **Enable OS Watchdog** field to specify the number of minutes between checks of the operating system by the IMM2. If the operating system fails to respond to one of these checks, the IMM2 generates an OS timeout alert and restarts the server. After the server is restarted, the OS watchdog is disabled until the operating system is shut down and the server is power cycled. To set the OS watchdog value, select **Enable OS Watchdog** and select a time interval from the menu. To turn off this watchdog, deselect **Enable OS Watchdog**. To capture operating-system-failure screens, you must enable the watchdog in the **Enable OS Watchdog** field.

Enable Loader Watchdog

Use the **Enable Loader Watchdog** field to specify the number of minutes that the IMM2 waits between the completion of POST and the starting of the operating system. If this interval is exceeded, the IMM2 generates a loader timeout alert and automatically restarts the server. After the server is restarted, the loader timeout is automatically disabled until the operating system is shut down and the server is power cycled (or until the operating system starts and the software is successfully loaded). To set the loader timeout value, select the time limit that the IMM2 waits for the operating-system startup to be completed. To turn off this watchdog, deselect **Enable Loader Watchdog** from the menu.

Enable Power Off Delay

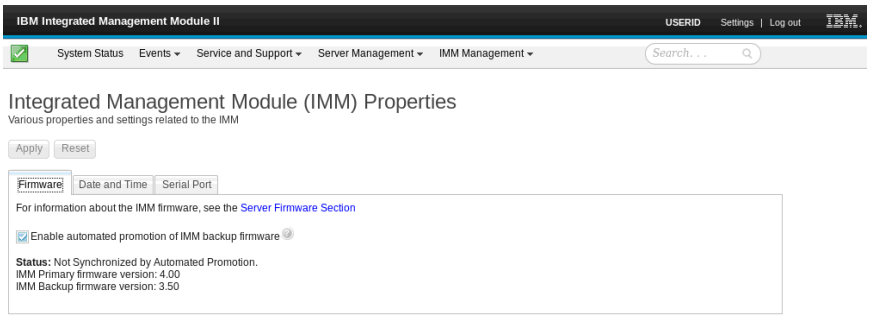
Use the **Enable Power Off Delay** field to specify the number of minutes that the IMM2 subsystem will wait for the operating system to shutdown before powering off the server. To set the power off delay timeout value, select the time limit that the IMM2 waits after the operating-system powers off. To turn off this watchdog, deselect **Enable Loader Watchdog** from the menu.

Changing the IMM2 firmware automated promotion settings

Select the **Firmware** tab to view or change the firmware automated promotion setting for the IMM2 backup firmware. If enabled, the Automated Promotion feature automatically copies the IMM2 firmware from the primary area into the backup area once the firmware in the primary area has run successfully for a period of time. This activity results in the primary and backup areas having the same firmware version. If you wish to keep different versions of the IMM2 firmware in the primary and backup areas, the **Enable automated promotion of IMM backup firmware** checkbox should not be checked.

The IMM2 firmware uses various metrics such as amount of run time and firmware activity to verify the stability of the firmware in the primary area before it is copied into the backup area. The minimum interval before the auto promotion takes place is two weeks; but, the actual interval might be longer depending upon the IMM2 activity that occurs during that interval.

The following illustration shows the Firmware tab with the **Enable automated promotion of IMM backup firmware** checkbox selected.



Setting the IMM2 date and time

Note: IMM2 Date and Time settings cannot be modified in an IBM Flex System.

Select the **Date and Time** tab to view or change the IMM2 date and time. The IMM2 uses its own real-time clock to time stamp all events that are logged in the event log. Alerts that are sent by email and Simple Network Management Protocol (SNMP) use the real-time clock setting to time stamp the alerts. The clock settings support Greenwich mean time (GMT) offsets and daylight saving time for added ease-of-use for administrators who are managing systems remotely over different time zones. You can remotely access the event log even if the server is turned off or disabled.

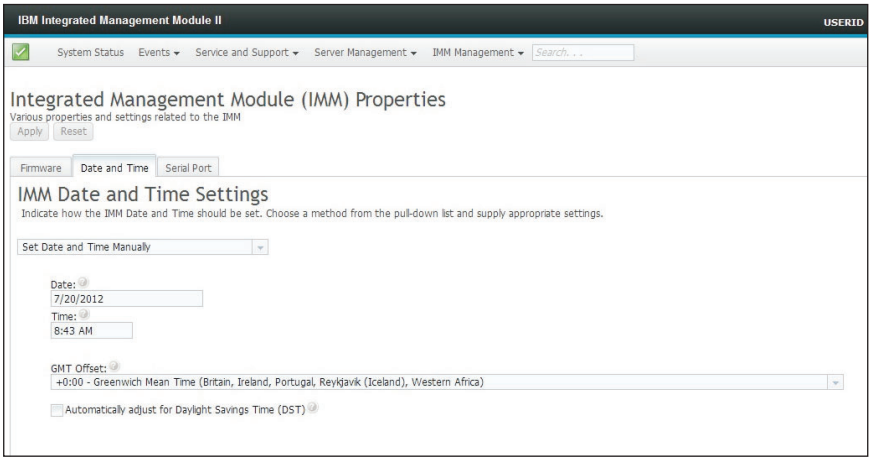
The IMM2 date and time setting affects only the IMM2 clock and not the server clock. The IMM2 real-time clock and the server clock are separate, independent clocks and can be set to different times.

Changing the time and date setting (manual mode)

Complete the following steps to manually change the time and date setting:

1. From the **Indicate how the IMM date and time should be set** menu list, click **Set Date and Time Manually**.
2. In the **Date** field, type the current month, day, and year.
3. In the **Time** field, type the numbers that correspond to the current hour and minutes.
   - The hour must be a number from 1- 12 as represented on a 12-hour clock.
   - The minutes must be numbers from 00 - 59.
   - Select **AM** or **PM**.
4. In the **GMT Offset** field, select the number that specifies the offset, in hours, from GMT. This number must correspond to the time zone where the server is located.
5. Select or clear the **Automatically adjust for Daylight Saving Time (DST)** check box to specify whether the IMM2 clock automatically adjusts when the local time changes between standard time and daylight saving time.

The following illustration shows the IMM Date and Time tab when setting the date and time manually.

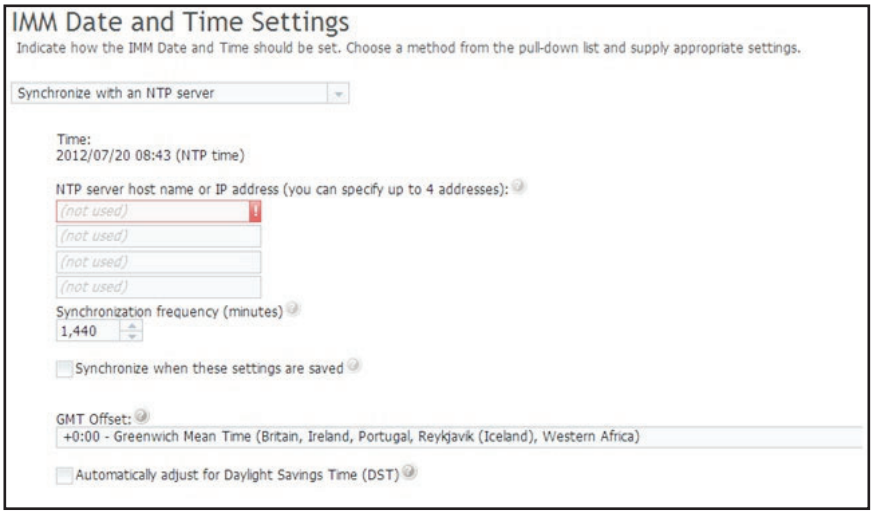


Changing the time and date settings (NTP server mode)

Complete the following steps to synchronize the IMM2 clock with the server clock:

1. From the **Indicate how the IMM date and time should be set** menu list, click **Synchronize with an NTP server**.
2. In the **NTP server host name or IP address** field, specify the name of the NTP server to be used for clock synchronization.
3. In the **Synchronization frequency (in minutes)** field, specify the approximate interval between synchronization requests. Enter a value between 3 - 1440 minutes.
4. Check the **Synchronize when these settings are saved** check box to request an immediate synchronization (when you click **Apply**), instead of waiting for the interval time to lapse.
5. In the **GMT Offset** field, select the number that specifies the offset, in hours, from GMT, corresponding to the time zone where the server is located.
6. Select or clear the **Automatically adjust for Daylight Saving Time (DST)** check box to specify whether the IMM2 clock automatically adjusts when the local time changes between standard time and daylight saving time.

The following illustration shows the IMM Date and Time tab when synchronizing with the server clock.



Configuring the serial port settings

Select the **Serial Port** tab to specify serial port redirection of the host. The IMM2 provides two serial ports that are used for serial redirection:

Serial port 1 (COM1)
Serial port 1 (COM1) on System x servers is used for Intelligent Platform Management Interface (IPMI) Serial over LAN (SOL). COM1 is configurable only through the IPMI interface.

Serial port 2 (COM2)
On blade servers, serial port 2 (COM2) is used for SOL. On System x rack servers and the IBM Flex System, COM2 is used for serial redirection through Telnet or SSH. COM2 is not configurable through the IPMI interface. On rack-mounted and tower servers, COM2 is an internal COM port with no external access.

Complete the following fields for serial port redirection:

Baud Rate
Specify the data-transfer rate of your serial port connection in this field. To set the baud rate, select the data-transfer rate, between 9600 and 115200, that corresponds to your serial port connection.

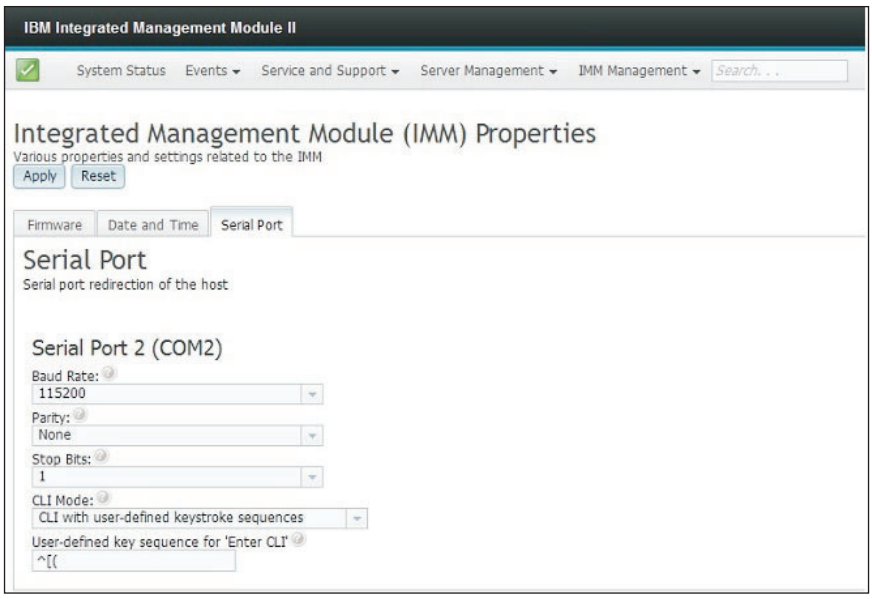
Parity Specify the parity bits of your serial port connection in this field. Available options are None, Odd, or Even.

Stop Bits
Specify the number of stop bits of your serial port connection in this field. Available options are 1 or 2.

CLI Mode
In this field, select **CLI with IMM2 compatible keystroke sequences** or select **CLI with user defined keystroke sequences** if you want to use your own key sequence. If you select **CLI with user defined keystroke sequences**, you must define the key sequence in the **User-defined key sequence for 'Enter CLI'** field.

After the serial redirection starts, it continues until you type the exit key sequence. When the exit key sequence is typed, serial redirection stops and you are returned to the command mode in the Telnet or SSH session. Use the **User-defined key sequence for 'Enter CLI'** field to specify the exit key sequence.

The following illustration shows the Serial Port tab.



Configuring user accounts

Select the **Users** option under the IMM Management tab to create and modify user accounts for the IMM2 and view group profiles. You will see the following informational message.

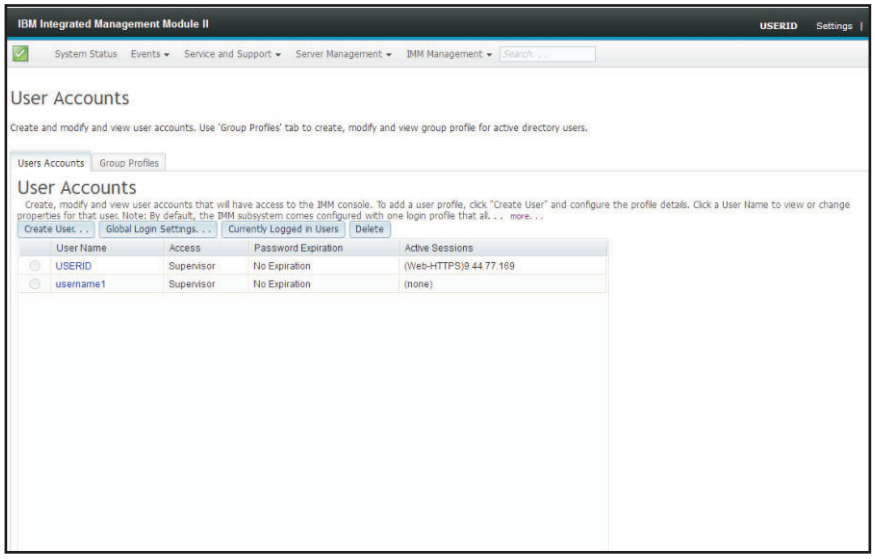
Note: In an IBM Flex System, IMM2 user accounts are managed by the CMM.

In an IBM Flex System, the user accounts that are configured in the IMM2 settings only authenticate access to the IMM2 using IPMI and SNMPv3 protocols. If a user has configured the CMM to centrally manage the IPMI and SNMPv3 user accounts on the IMM2, you will not be able to configure the accounts directly on the IMM2 itself. Access to other IMM2 interfaces such as the web and CLI is authenticated with the account credentials that reside on the LDAP server that the CMM has configured the IMM2 to use.

User accounts

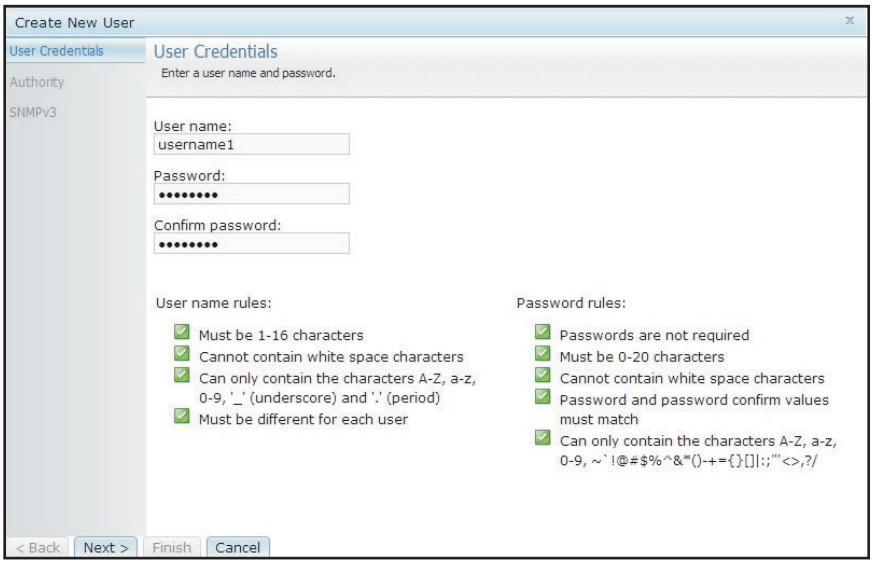
Select the **Users Accounts** tab to create, modify, and view user accounts as shown in the following illustration.

Note: The IMM2 subsystem comes with one login profile.



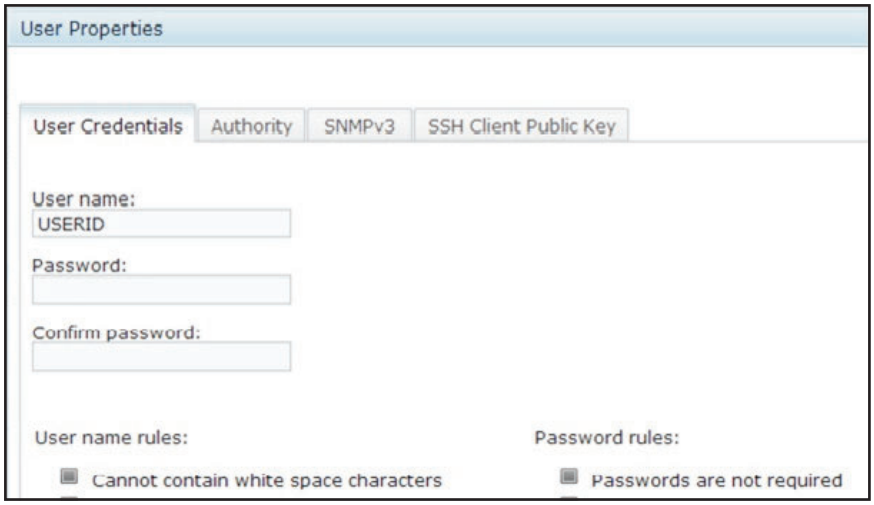
Create user

Click the **Create User...** tab to create a new user account. Complete the following fields: **User name**, **Password**, and **Confirm Password** (as shown in the following illustration).



User properties

Click the **User Properties** tab to modify existing user accounts (as shown in the following illustration).



User authority

Click the **Authority** tab to set the user authority level. The following user authority levels are available:

Supervisor
The Supervisor user authority level has no restrictions.

Read only
The Read only user authority level has read-only access and cannot perform actions such as file transfers, power and restart actions, or remote presence functions.

Custom
The Custom user authority level allows a more customized profile for user authority with settings for the actions that the user is allowed to perform.

Select one or more of the following Custom user authority levels:

User Account Management
A user can add, modify, or delete users, and change the global login settings.

Remote Console Access
A user can access the remote console.

Remote Console and Virtual Media Access
A user can access the remote console and the virtual media feature.

Remote Server Power/Restart Access
A user can perform power-on and restart functions for the remote server.

Ability to Clear Event Logs
A user can clear the event logs. Anyone can look at the event logs; but, this authority level is required to clear the logs.

Adapter Configuration - Basic
A user can modify configuration parameters on the Server Properties and Events pages.

Adapter Configuration - Networking & Security
A user can modify configuration parameters on the Security, Network, and Serial Port pages.

Adapter Configuration - Advanced
A user has no restrictions when configuring the IMM2. In addition, the user is said to have administrative access to the IMM2. Administrative access includes the following advanced functions: firmware updates, PXE network boot, restoring IMM2 factory defaults, modifying and restoring IMM2 settings from a configuration file, and restarting and resetting the IMM2.

When a user sets the authority level of an IMM2 login ID, the resulting IPMI privilege level of the corresponding IPMI User ID is set according to the following priorities:

- If a user sets the IMM2 login ID authority level to **Supervisor**, the IPMI privilege level is set to Administrator.
- If a user sets the IMM2 login ID authority level to **Read Only**, the IPMI privilege level is set to User.
- If a user sets the IMM2 login ID authority level to any of the following types of access, the IPMI privilege level is set to Administrator:
  - User Account Management Access
  - Remote Console Access
  - Remote Console and Remote Disk Access
  - Adapter Configuration - Networking & Security
  - Adapter Configuration - Advanced
- If a user sets the IMM2 login ID authority level to **Remote Server Power/Restart Access** or **Ability to Clear Event Logs**, the IPMI privilege level is set to Operator.
- If a user sets the IMM2 login ID authority level to **Adapter Configuration - Basic**, the IPMI privilege level is set to User.

SNMP access rights

Click the **SNMPv3** tab to set SNMP access for the account. The following user access options are available:

Authentication protocol
Specify either **HMAC-MD5** or **HMAC-SHA** as the authentication protocol. These are the algorithms used by the SNMPv3 security model for authentication. If the **Authentication Protocol** is not enabled, no authentication protocol will be used.

Privacy protocol
The data transfer between the SNMP client and the agent can be protected using encryption. The supported methods are **DES** and **AES**. Privacy protocol is valid only if the authentication protocol is set to either **HMAC-MD5** or **HMAC-SHA**.

Privacy password
Specify the encryption password in this field.

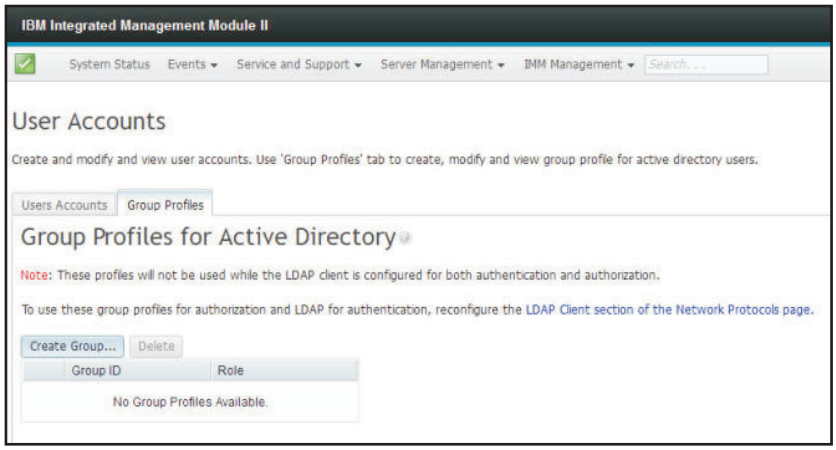
Confirm privacy password
Specify the encryption password again for confirmation.

Access type
Specify either **Get** or **Set** as the access type. SNMPv3 users with **Get** as the access type can perform only query operations. SNMPv3 users with **Set** as the access type, can perform query operations and modify settings (for example, setting the password for a user).

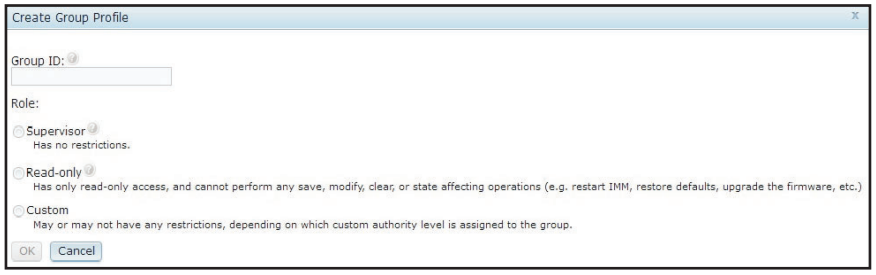
Hostname/IP address for traps
Specify the trap destination for the user. This can be an IP address or hostname. Using traps, the SNMP agent notifies the management station about events, (for example, when a processor temperature exceeds the limit).

Group profiles

Select the **Group Profiles** tab to create, modify, and view group profiles (as shown in the following illustration).

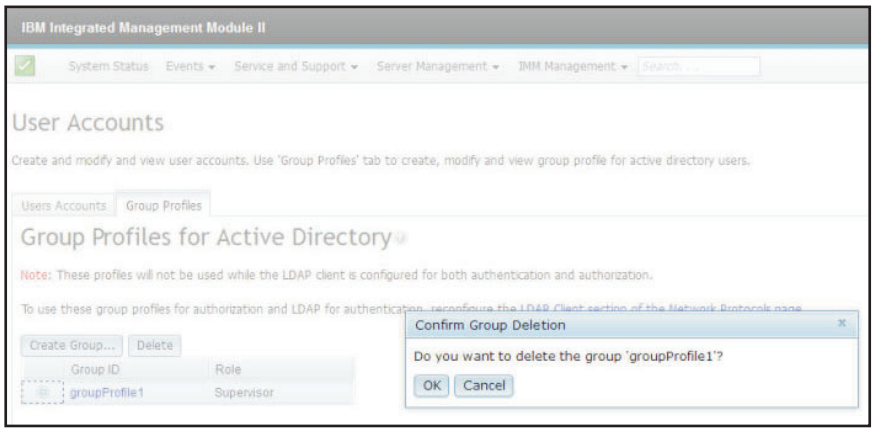


Click **Create Group** to create a new user group. The following illustration shows the Create Group Profile window.



Enter a **Group ID** and select the **Role**, (see "User authority" on page 71 for information about the user authority levels).

If you need to delete a group, click **Delete**. The following illustration shows the Confirm Group Deletion window.



Configuring global login settings

Use the Global login settings tab to configure login settings that apply to all users.

General settings

Click the **General** tab to select how user login attempts are authenticated and specify how long, in minutes, the IMM2 waits before it disconnects an inactive web session. In the **User authentication method** field, you can specify how users who are attempting to login should be authenticated. You can select one of the following authentication methods:

- **Local only:** Users are authenticated by a search of the local use account configured on the IMM2. If there is no match of the user ID and password, access is denied.
- **LDAP only:** The IMM2 attempts to authenticate the user using an LDAP server. Local user accounts on the IMM2 are *not* searched with this authentication method.
- **Local first, then LDAP:** Local authentication is attempted first. If local authentication fails; then, LDAP authentication is attempted.
- **LDAP first, then Local:** LDAP authentication is attempted first. If LDAP authentication fails; then, local authentication is attempted.

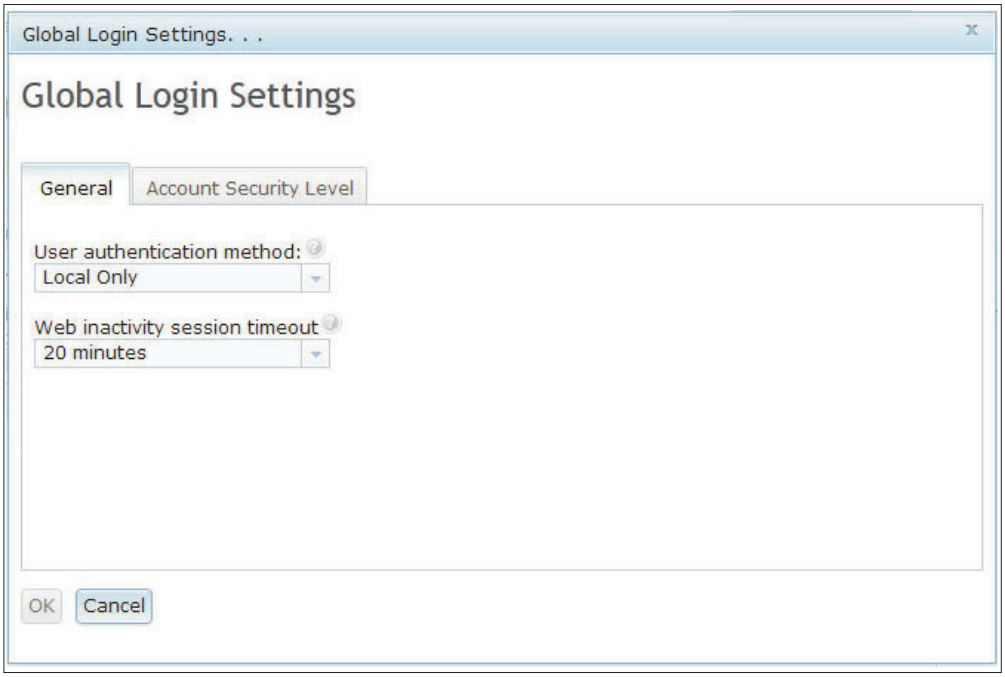
Notes:

- Only locally administered accounts are shared with the IPMI and SNMP interfaces. These interfaces do not support LDAP authentication.
- IPMI and SNMP users can login using the locally administered accounts when the **User authentication method** field is set to **LDAP only**.

In the **Web inactivity session timeout** field, you can specify how long, in minutes, the IMM2 waits before it disconnects an inactive web session. Select **No timeout** to disable this feature. Select **User picks timeout** to select the timeout period during the login process.

The inactivity timeout applies only to web pages that do *not* automatically refresh. If a web browser continuously request web page updates when a user navigates to a web page that automatically refreshes, the inactivity timeout will not automatically end the user's session. Users can choose whether or not to have the web page content automatically refreshed every 60 seconds. See "Page auto refresh" on page 17 for additional information describing the auto refresh setting.

The General tab is shown in the following illustration.



There are some IMM2 web pages that are automatically refreshed even if the automatic refresh setting is not selected. IMM2 web pages that are automatically refreshed are as follows:

- **System Status:** The system and power status will be refreshed automatically every three seconds.
- **Server Power Actions:** The power status will be refreshed automatically every three seconds.
- **Remote Control:** The Start remote control buttons will be refreshed automatically every second. The Session List table will be refreshed automatically once every minute.

The IMM2 firmware supports up to six simultaneous web sessions. To free up sessions for use by others, it is recommended that you log out of the web session when you are finished rather than relying on the inactivity timeout to automatically close your session.

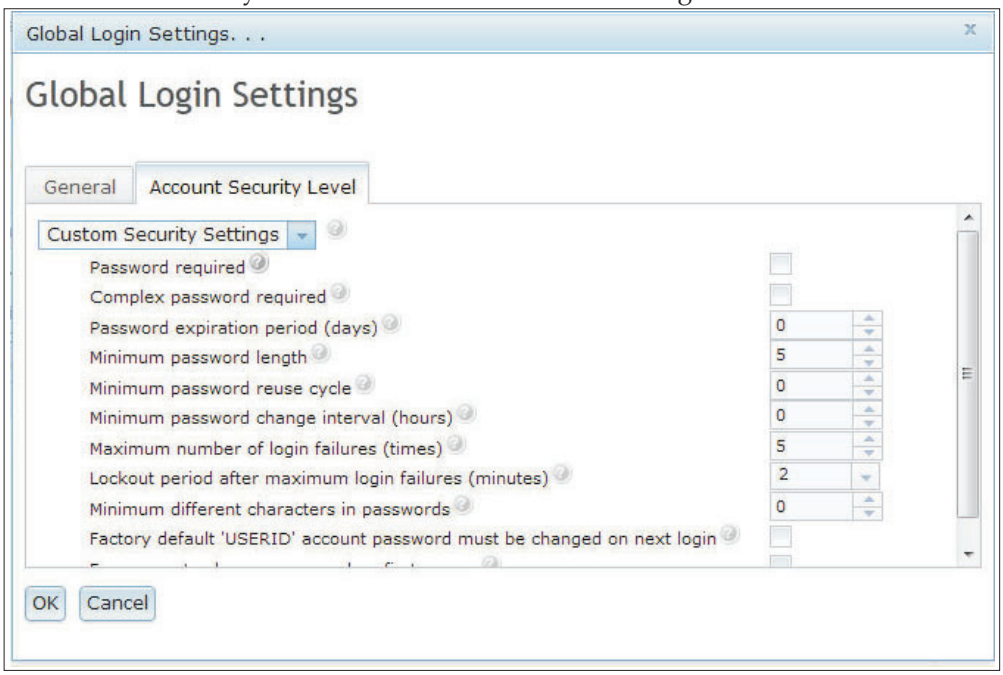
Note: If you leave the browser open on an IMM2 web page that automatically refreshes, your web session will not automatically close due to inactivity.

Account security policy settings

Click the **Account Security Level** tab to select the account security policy setting. There are three levels of account security policy settings:

- Legacy Security Settings
- High Security Settings
- Custom Security Settings

The Account Security Level tab is shown in the following illustration.



Select the account security policy setting from the Security Settings item list.

Notes:

- The Legacy Security Settings and High Security Settings predefine the policy setting values and cannot be changed.
- The Custom Security Settings allow users to customize the security policies as needed.

The following table shows the values for each level of the security settings.

Table 3. Security setting policy values

Policy setting/field	Legacy Security Settings	High Security Settings	Custom Security Settings
Password required	No	Yes	Yes or No
Complex password required	No	Yes	Yes or No
Password expiration period (days)	None	90	0 – 365
Minimum password length	None	8	5 – 20
Minimum password reuse cycle	None	5	0 – 5
Minimum password change interval (hours)	None	24	0 – 240
Maximum number of login failures (times)	5	5	0 – 10
Lockout period after maximum login failures (minutes)	2	60	0 – 240

Table 3. Security setting policy values (continued)

Policy setting/field	Legacy Security Settings	High Security Settings	Custom Security Settings
Minimum different characters in passwords	None	2	0 – 19
Factory default 'USERID' account password must be changed on next login	No	Yes	Yes or No
Force user to change password on first access	No	Yes	Yes or No

The following information is a description of the fields for the security settings.

Password required

This field indicates whether login IDs with no password are allowed to be created. If the **Password required** checkbox is selected, any existing login ID's with no password will be required to define a password the next time the user logs in.

Complex password required

If complex passwords are required the password must adhere to the following rules:

- Passwords must be a minimum of eight characters long.
- Passwords must contain at least three of the following four categories:
  - At least one lower case alpha character.
  - At least one upper case alpha character.
  - At least one numeric character.
  - At least one special character.
- Spaces or white space characters are not allowed.
- Passwords may have no more than three of the same character used consecutively (for example, aaa).
- Passwords must not be a repeat or reverse of the associated user ID.

If complex passwords are not required the password:

- Must be a minimum of five (or the number specified in the **Minimum password length** field) characters long.
- Cannot contain any spaces or white space characters.
- Must contain at least one numeric character.
- Can be blank (only if the **Password Required** check box is disabled).

Password expiration period (days)

This field contains the maximum password age that is permitted before the password must be changed. A value of 0 to 365 days are supported. The default value for this field is 0 (disabled).

Minimum password length

This field contains the minimum length of the password. 5 to 20 characters are supported for this field. If the **Complex password required** check box is checked; then, the minimum password length must be at least eight characters.

Minimum password reuse cycle
This field contains the number of previous passwords that cannot be reused. Up to five previous passwords can be compared. Select 0 to allow the reuse of all previous passwords. The default value for this field is 0 (disabled).

Minimum password change interval (hours)
This field contains how long a user must wait between password changes. A value of 0 to 240 hours are supported. The default value for this field is 0 (disabled).

Maximum number of login failures (times)
This field contains the number of failed login attempts that are allowed before the user is locked out for a period of time. A value of 0 to 10 is supported. The default value for this field is 0 (disabled).

Lockout period after maximum login failures (minutes)
This field specifies how long (in minutes), the IMM2 subsystem will disable remote login attempts from all users after detecting more than five sequential login failures from any user.

Minimum different characters in passwords
This field specifies the number of characters that must be different between the new password and the previous password. A value of 0 to 19 is supported.

Factory default 'USERID' account password must be changed on next login
A manufacturing option is provided to reset the default USERID profile after the first successful login. When this checkbox is enabled, the default password must be changed before the account can be used. The new password is subject to all active password enforcement rules.

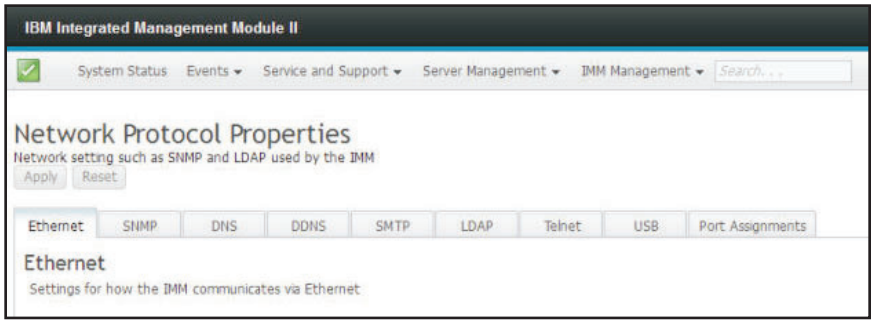
Force user to change password on first access
After setting up a new user with a default password, selection of this check box will force that user to change their password the first time the user logs in.

Configuring network protocols

Click the **Network** option under the IMM Management tab to view and set network settings.

Configuring the Ethernet settings

Click the **Ethernet** tab to view or modify IMM2 Ethernet settings (as shown in the following illustration).



To use an IPv4 Ethernet connection, complete the following steps:

1. Select the **IPv4** option; then, select the corresponding checkbox.

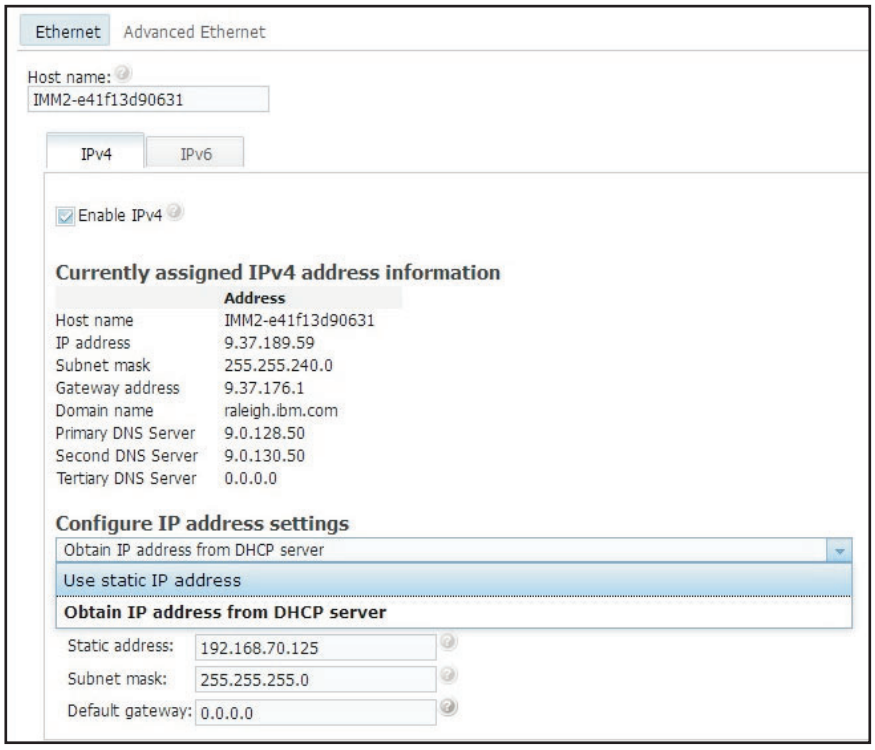
   Note: Disabling the Ethernet interface prevents access to the IMM2 from the external network.
2. From the **Configure IP address settings** list, select one of the following options:
   - Obtain an IP address from a DHCP server
   - Use static IP address
3. If you want the IMM2 to default to a static IP address if unable to contact a DHCP server, select the corresponding check box.
4. In the **Static address** field, type the IP address of the IMM2.

   Note: The IP address must contain four integers from 0 to 255 with no spaces and separated by periods.
5. In the **Subnet mask** field, type the subnet mask that is used by the IMM2.

   Note: The subnet mask must contain four integers from 0 to 255 with no spaces or consecutive periods and separated by periods. The default setting is 255.255.255.0.
6. In the **Default Gateway** field, type your network gateway router.

   Note: The gateway address must contain four integers from 0 to 255 with no spaces or consecutive periods and separated by periods.

The following illustration shows the Ethernet tab.



Configuring advanced Ethernet settings

Click the **Advanced Ethernet** tab to set additional Ethernet settings.

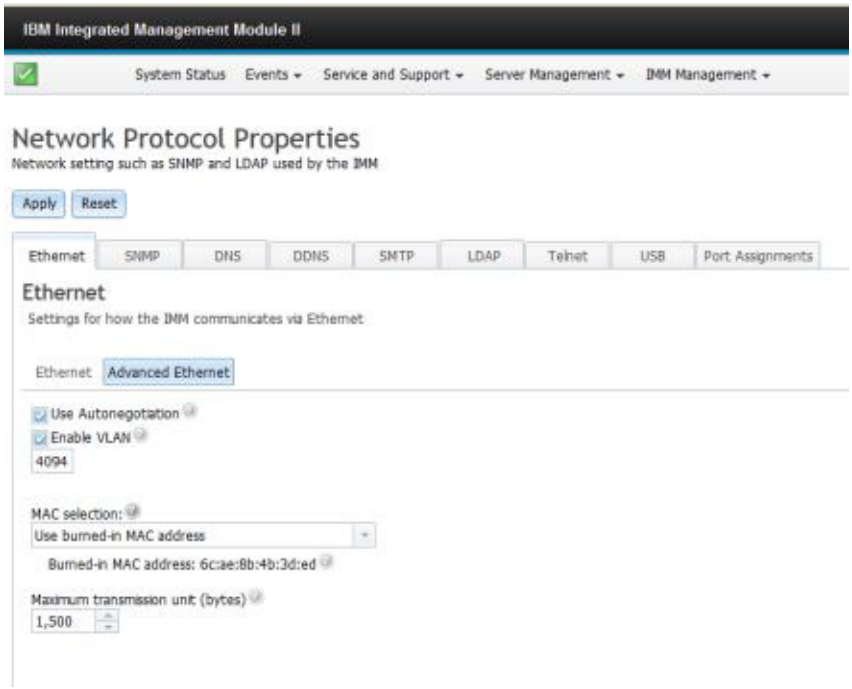
To enable Virtual LAN (VLAN) tagging select the **Enable VLAN** checkbox. When VLAN is enabled and a VLAN ID is configured, the IMM2 only accepts packets with the specified VLAN IDs. The VLAN IDs can be configured with numeric values between 1 and 4094.

From the **MAC selection** list choose one of the following selections:

- Used burned in MAC address
  - The Burned-in MAC address option is a unique physical address that is assigned to this IMM2 by the manufacturer. The address is a read-only field.
- Used locally administered MAC address
  - If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value from `000000000000` through `FFFFFFFFFFFF`. This value must be in the form *`xx:xx:xx:xx:xx:xx`* where *`X`* is a number from 0 to 9. The IMM2 does not support the use of a multicast address. The first byte of a multicast address is an odd number (the least significant bit is set to 1); therefore, the first byte must be an even number.

In the **Maximum transmission unit** field, specify the maximum transmission unit of a packet (in bytes) for your network interface. The maximum transmission unit range is from 60 to 1500. The default value for this field is 1500.

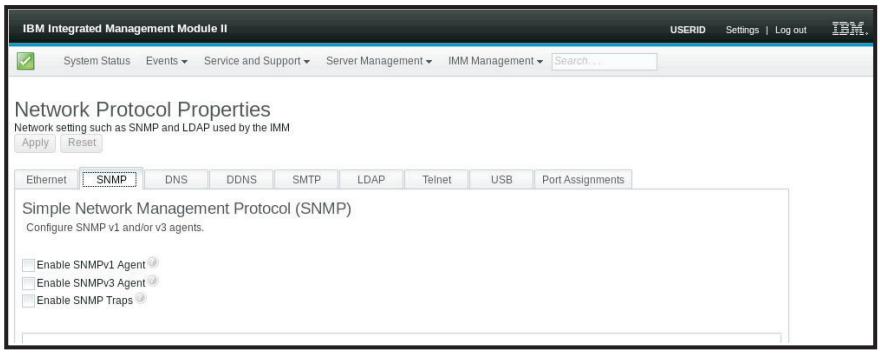
The following illustration shows the Advanced Ethernet tab and associated fields.



Configuring SNMP alert settings

Complete the following steps to configure the IMM2 SNMP setting.

1. Click the **SNMP** tab (as shown in the following illustration).



2. Check the corresponding checkbox to enable the SNMPv1 agent, the SNMPv3 agent or SNMP Traps.
3. If enabling the SNMPv1 agent, proceed to step 4. If enabling the SNMPv3 agent, proceed to step 5. If enabling the SNMP Traps, proceed to step 6
4. If enabling the SNMPv1 agent, complete the following fields:
   a. Click the **Contact** tab. In the **Contact person** field, enter the name of the contact person. In the **Location** field, enter the site (geographical coordinates).
   b. Click the **Communities** tab to set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community.

      Notes:

      - If an error message window appears, make the necessary adjustments to the fields that are listed in the error window; then, scroll to the top of the page and click **Apply** to save your corrected information.
      - You must configure at least one community to enable this SNMP agent.

      Complete the following fields:

      1) In the **Community Name** field, enter a name or authentication string to specify the community.
      2) In the **Access type** field, select an access type.
         - Select **Trap** to allow all hosts in the community to receive traps.
         - Select **Get** to allow all hosts in the community to receive traps and query management information base (MIB) objects.
         - Select **Set** to allow all hosts in the community to receive traps, query, and set MIB objects.

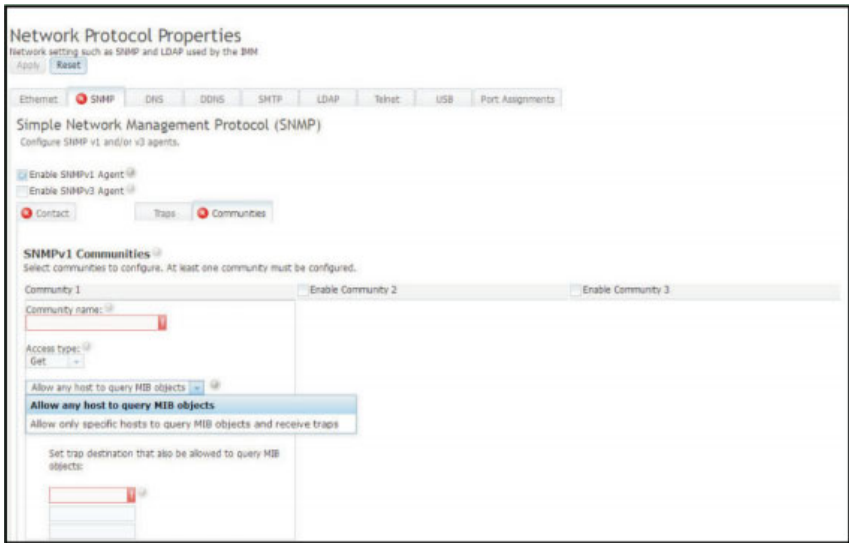
   c. In the **Host Name** or **IP Address** field, enter the host name or IP address of each community manager.
   d. Click **Apply** to apply the changes you have made.
5. If enabling the SNMPv3 agent, complete the following fields:
   a. Click the **Contact** tab. In the **Contact person** field, enter the name of the contact person. In the **Location** field, enter the site (geographical coordinates).
   b. Click the **Users** tab to show the list of local user accounts for the console.

      Note: This is the same list that is in the Users option. You must configure SNMPv3 for each user account that will need SNMPv3 access.

   c. Click **Apply** to apply the changes you have made.
6. If enabling the SNMP Traps, configure the events alerted in the **Traps** tab.

Note: When configuring SNMP, required fields that are not complete or have incorrect values are highlighted with a red X that can be used to guide you through completion of the required fields.

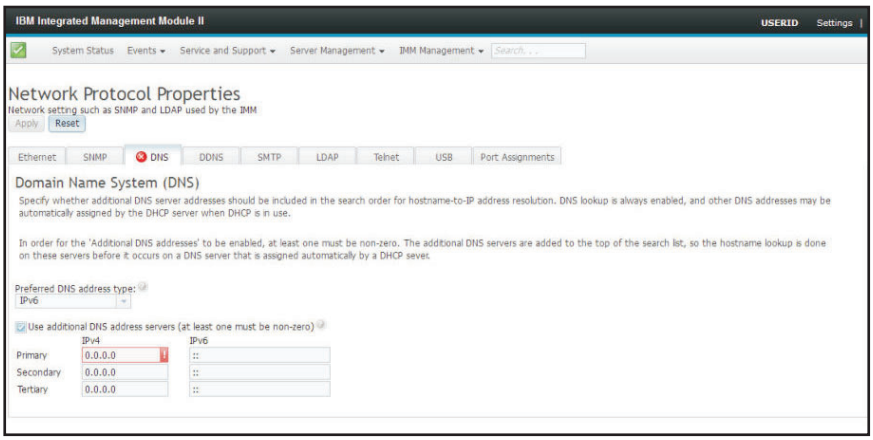
The following illustration shows the SNMP tab when configuring the SNMPv1 agent.



Configuring DNS

Note: In an IBM Flex System, DNS settings cannot be modified on the IMM2. DNS settings are managed by the CMM.

Click the **DNS** tab to view or modify IMM2 Domain Name System settings. If you click the **Use additional DNS address servers** checkbox, specify the IP addresses of up to three Domain Name System servers on your network. Each IP address must contain integers from 0 to 255, separated by periods (as shown in the following illustration).

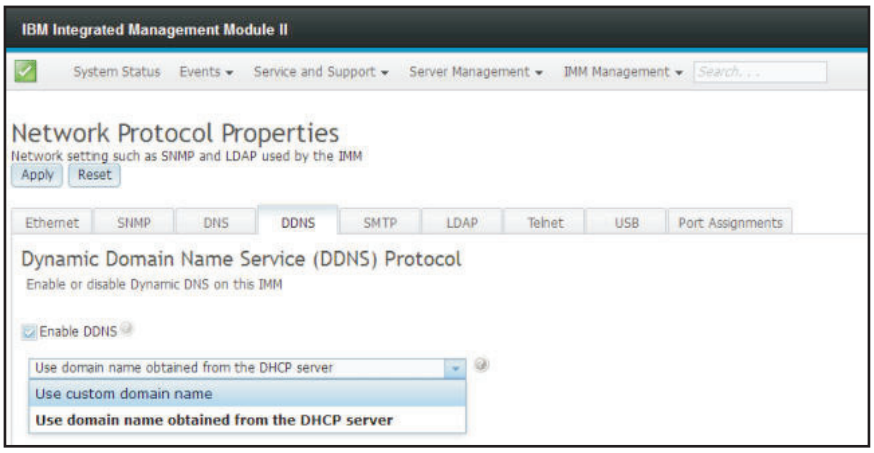


Configuring DDNS

Click the **DDNS** tab to view or modify IMM2 Dynamic Domain Name System settings. Click the **Enable DDNS** checkbox, to enable DDNS. When DDNS is

enabled, the IMM2 notifies a domain name server to change in real time, the active domain name server configuration of its configured hostnames, addresses or other information stored in the domain name server.

Choose an option from the item list to select how you want the domain name of the IMM2 to be selected, (as shown in the following illustration).



Configuring SMTP

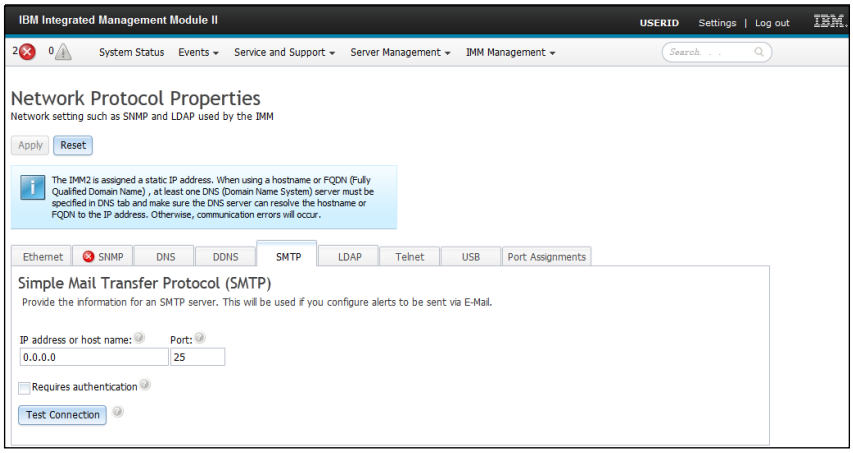
Click the **SMTP** tab to view or modify IMM2 SMTP settings. Complete the following fields to view or modify SMTP settings:

IP address or host name
Type the host name of the SMTP server. Use this field to specify the IP address or, if DNS is enabled and configured, the host name of the SMTP server.

Port Specify the port number for the SMTP server. The default value is 25.

Test connection
Click **Test Connection**, a test email is sent to verify your SMTP settings are correct.

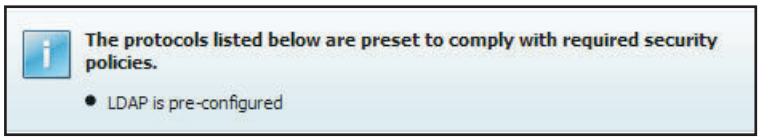
The following illustration shows the SMTP tab.



Configuring LDAP

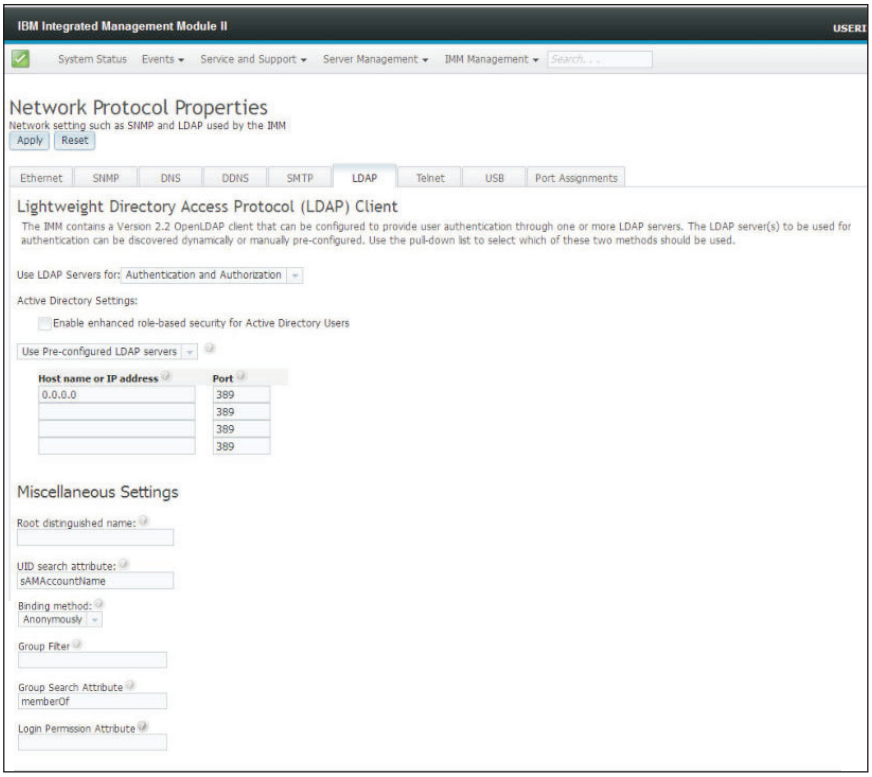
Click the **LDAP** tab to view or modify IMM2 LDAP Client settings.

Note: In an IBM Flex System, the IMM2 is set up to use the LDAP server running on the CMM. You will see an informational message that reminds you that the LDAP settings may not be changed, (as shown in the following illustration).



Using a LDAP server, the IMM2 can authenticate a user by querying or searching an LDAP directory on an LDAP server, instead of going through its local user database. The IMM2 can remotely authenticate any user's access through a central LDAP server. You can assign authority levels according to information that is found on the LDAP server. You can also use the LDAP server to assign users and IMM2s to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, an IMM2 can be associated with one or more groups, the user would pass group authentication only if the user belongs to at least one group that is associated with the IMM2.

The following illustration shows the LDAP tab.



To use a preconfigured LDAP server, complete the following fields:

LDAP server configuration item list

Select **Use Pre-Configured LDAP Server** from the item list. The port number for each server is optional. If this field is left blank, the default

value of 389 is used for nonsecured LDAP connections. For secured connections, the default value is 636. You must configure at least one LDAP server.

Root distinguished name

This is the distinguished name (DN) of the root entry of the directory tree on the LDAP server (for example, dn=mycompany,dc=com). This DN is used as the base object for all searches.

UID search attribute

When the binding method is set to **Anonymously** or **With Configured Credentials**, the initial bind to the LDAP server is followed by a search request that retrieves specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that represents the user IDs on that server. This attribute name is configured in this field. On Active Directory servers, the attribute name is usually **sAMAccountName**. On Novell eDirectory and OpenLDAP servers, the attribute name is **uid**. If this field is left blank, the default is **uid**.

Binding method

Before you can search or query the LDAP server you must send a bind request. This field controls how this initial bind to the LDAP server is performed. The following bind methods are available:

- Anonymously
  - Use this method to bind without a DN or password. This method is strongly discouraged because most servers are configured to not allow search requests on specific user records.
- With Configured Credentials
  - Use this method to bind with configured client DN and password.
- With Login Credentials
  - Use this method to bind with the credentials that are supplied during the login process. The user ID can be provided through a DN, a fully qualified domain name, or a user ID that matches the **UID Search Attribute** that is configured on the IMM2. If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in. If necessary, a second attempt to bind is made, this time with the DN that is retrieved from the user's LDAP record and the password that was entered during the login process. If this fails, the user is denied access. The second bind is performed only when the **Anonymous** or **With Configured Credentials** binding methods are used.

Group Filter

The **Group Filter** field is used for group authentication. Group authentication is attempted after the user's credentials are successfully verified. If group authentication fails, the user's attempt to log on is denied. When the group filter is configured, it is used to specify to which groups the service processor belongs. This means that the user must belong to at least one of the groups that are configured for group authentication to succeed. If the **Group Filter** field is left blank, group authentication automatically succeeds. If the group filter is configured, an attempt is made to match at least one group in the list to a group that the user belongs. If there is no match, the user fails authentication and is denied access. If there is at least one match, group authentication is successful.

The comparisons are case sensitive. The filter is limited to 511 characters and can consist of one or more group names. The colon (:) character must be used to delimit multiple group names. Leading and trailing spaces are ignored, but any other space is treated as part of the group name. A selection to allow or not allow the use of wildcards in the group name is provided. The filter can be a specific group name (for example, IMMWest), an asterisk (*) used as a wildcard that matches everything, or a wildcard with a prefix (for example, IMM*). The default filter is IMM*. If security policies in your installation prohibit the use of wildcards, you can choose to not allow the use of wildcards. The wildcard character (*) is then treated as a normal character instead of the wildcard. A group name can be specified as a full DN or using only the *cn* portion. For example, a group with a DN of cn=adminGroup,dc=mycompany,dc=com can be specified using the actual DN or with adminGroup.

In Active Directory environments only, nested group membership is supported. For example, if a user is a member of GroupA and GroupB, and GroupA is also a member of GroupC, the user is said to be a member of GroupC also. Nested searches stop if 128 groups have been searched. Groups in one level are searched before groups in a lower level. Loops are not detected.

Group Search Attribute

In an Active Directory or Novell eDirectory environment, the **Group Search Attribute** field specifies the attribute name that is used to identify the groups to which a user belongs. In an Active Directory environment, the attribute name is **memberOf**. In an eDirectory environment, the attribute name is **groupMembership**. In an OpenLDAP server environment, users are usually assigned to groups whose objectClass equals PosixGroup. In that context, this field specifies the attribute name that is used to identify the members of a particular PosixGroup. This attribute name is **memberUid**. If this field is left blank, the attribute name in the filter defaults to **memberOf**.

Login Permission Attribute

When a user is authenticated through an LDAP server successfully, the login permissions for the user must be retrieved. To retrieve the login permissions, the search filter that is sent to the server must specify the attribute name that is associated with login permissions. The **Login Permission Attribute** field specifies the attribute name. If this field is left blank, the user is assigned a default of read-only permissions, assuming that the user passes the user and group authentication.

The attribute value that is returned by the LDAP server searches for the keyword string IBMRBSPermissions=. This keyword string must be immediately followed by a bit string that is entered as 12 consecutive 0s or 1s. Each bit represents a set of functions. The bits are numbered according to their positions. The left-most bit is bit position 0, and the right-most bit is bit position 11. A value of 1 at a bit position enables the function that is associated with that bit position. A value of 0 at a bit position disables the function that is associated with that bit position.

The string IBMRBSPermissions=010000000000 is a valid example. The IBMRBSPermissions= keyword is used to allow it to be placed anywhere in this field. This enables the LDAP administrator to reuse an existing attribute; therefore, preventing an extension to the LDAP schema. This also enables the attribute to be used for its original purpose. You can add the keyword string anywhere in this field. The attribute that you use can allow

for a free-formatted string. When the attribute is retrieved successfully, the value that is returned by the LDAP server is interpreted according to the information in the following table.

Table 4. Permission bits

Bit position	Function	Explanation
0	Deny Always	A user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
1	Supervisor Access	A user is given administrator privileges. The user has read/write access to every function. If you set this bit, you do not have to individually set the other bits.
2	Read Only Access	A user has read-only access, and cannot perform any maintenance procedures (for example, restart, remote actions, or firmware updates) or make modifications (for example, the save, clear, or restore functions. Bit position 2 and all other bits are mutually exclusive, with bit position 2 having the lowest precedence. When any other bit is set, this bit will be ignored.
3	Networking and Security	A user can modify the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port configurations.
4	User Account Management	A user can add, modify, or delete users and change the Global Login Settings in the Login Profiles window.
5	Remote Console Access	A user can access the remote server console.
6	Remote Console and Remote Disk Access	A user can access the remote server console and the remote disk functions for the remote server.
7	Remote Server Power/Restart Access	A user can access the power on and restart functions for the remote server.
8	Basic Adapter Configuration	A user can modify configuration parameters in the System Settings and Alerts windows.
9	Ability to Clear Event Logs	A user can clear the event logs. **Note:** All users can view the event logs; but, the user is required to have this level of permission to clear the logs.

Table 4. Permission bits (continued)

Bit position	Function	Explanation
10	Advanced Adapter Configuration	A user has no restrictions when configuring the IMM2. In addition the user has administrative access to the IMM2. The user can perform the following advanced functions: firmware upgrades, PXE network boot, restore IMM2 factory defaults, modify and restore adapter configuration from a configuration file, and restart/reset the IMM2.
11	Reserved	This bit position is reserved for future use. If none of the bits are set, the user has read-only authority. Priority is given to login permissions that are retrieved directly from the user record. If the login permission attribute is not in the user's record, an attempt is made to retrieve the permissions from the groups to which the user belongs. This is performed as part of the group authentication phase. The user is assigned the inclusive OR of all the bits for all groups. The Read Only Access bit (position 2) is set only if all other bits are set to zero. If the Deny Always bit (position 0) is set for any of the groups, the user is refused access. The Deny Always bit (position 0) always has precedence over all other bits.

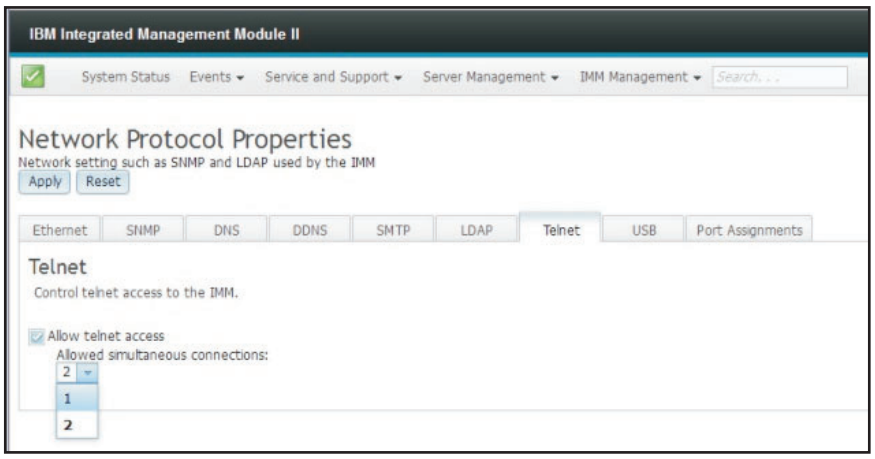
Configuring Telnet

Select the **Telnet** tab to view or modify IMM2 Telnet settings. Complete the following fields to view or modify Telnet settings:

Allow telnet access
Place a check-mark in the check box to choose whether or not you want the IMM2 to allow Telnet access.

Allowed simultaneous connections
Use the **Allowed simultaneous connections** list to choose the number of Telnet connections to allow at the same time.

The following illustration shows the Telnet tab.

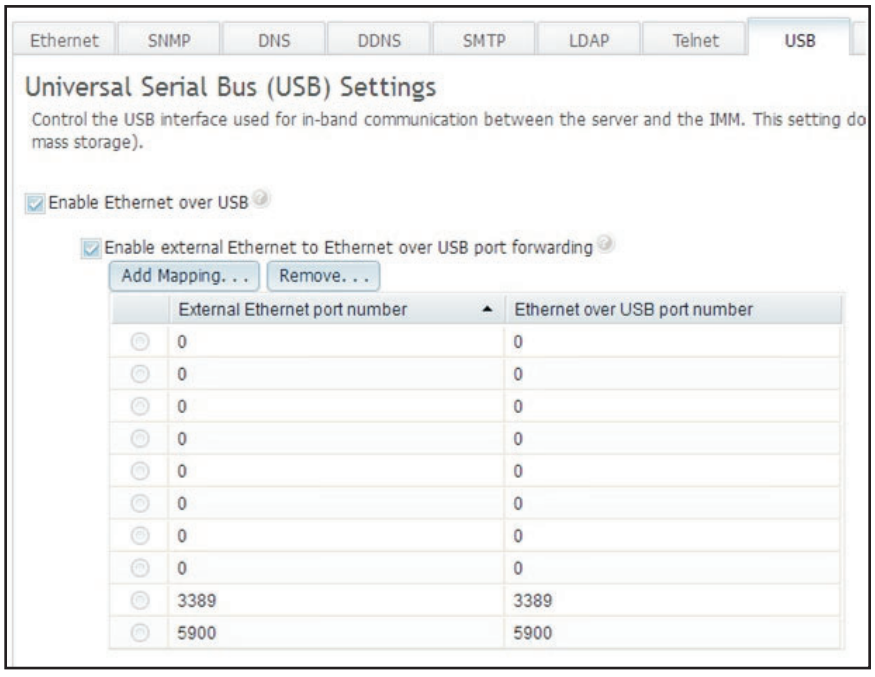


Configuring USB

Select the **USB** tab to view or modify IMM2 USB settings. The USB in-band interface, or LAN over USB, is used for in-band communications to the IMM2. Click the **Enable Ethernet over USB** check box to enable or disable the IMM2 Lan over USB interface.

Important: If you disable the USB in-band interface, you cannot perform an in-band update of the IMM2 firmware, server firmware, and DSA firmware using the Linux or Windows flash utilities. If the USB in-band interface is disabled, use the Firmware Server option under the Server Management tab to update the firmware. If you disable the USB in-band interface, also disable the watchdog timeouts to prevent the server from restarting unexpectedly.

The following illustration shows the USB tab.



Mapping of external Ethernet port numbers to Ethernet over USB port numbers is controlled by clicking the **Enable external Ethernet to Ethernet over USB port forwarding** check box and completing the mapping information for ports you wish to have forwarded.

Configuring port assignments

Select the **Port Assignments** tab to view or modify IMM2 port assignments. Complete the following fields to view or modify port assignments:

HTTP In this field specify the port number for the HTTP server of the IMM2. The default value is 80. Valid port number values are from 1 to 65535.

HTTPS
In this field specify the port number that is used for web interface HTTPS Secure Sockets Layer (SSL) traffic. The default value is 443. Valid port number values are from 1 to 65535.

Telnet CLI
In this field specify the port number for Legacy CLI to log in through the Telnet service. The default value is 23. Valid port number values are from 1 to 65535.

SSH Legacy CLI
In this field specify the port number that is configured for Legacy CLI to log in through the SSH protocol. The default value is 22.

SNMP Agent
In this field specify the port number for the SNMP agent that runs on the IMM2. The default value is 161. Valid port number values are from 1 to 65535.

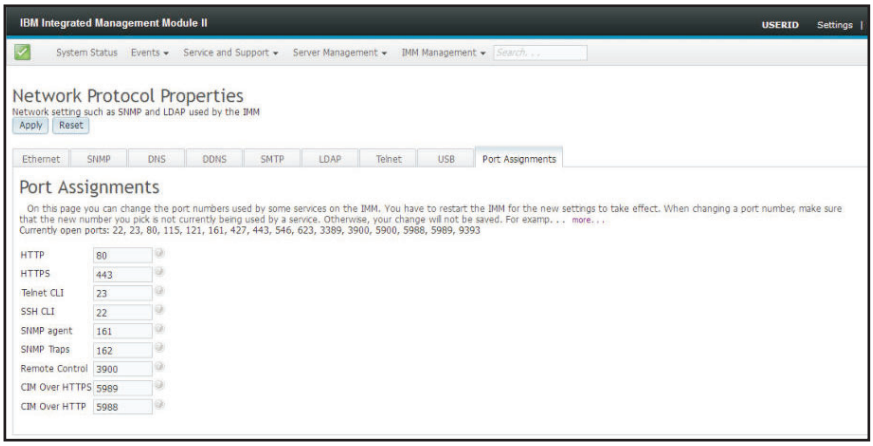
SNMP Traps
In this field specify the port number that is used for SNMP traps. The default value is 162. Valid port number values are from 1 to 65535.

Remote Control
In this field specify the port number that the remote control feature uses to view and interact with the server console. The default value is 3900 for rack-mounted and tower servers.

CIM over HTTP
In this field specify the port number for CIM over HTTP. The default value is 5988.

CIM over HTTPS
In this field specify the port number for CIM over HTTPS. The default value is 5989.

The following illustration shows the Port Assignments tab.



Configuring security settings

Click the **Security** option under the IMM Management tab (as shown in the following illustration) to access and configure security properties, status, and settings for your IMM2.

To apply any changes you have made, you must click the **Apply** button at the upper left of the IMM Security window. To reset any changes you have made, you must click the **Reset Values** button.

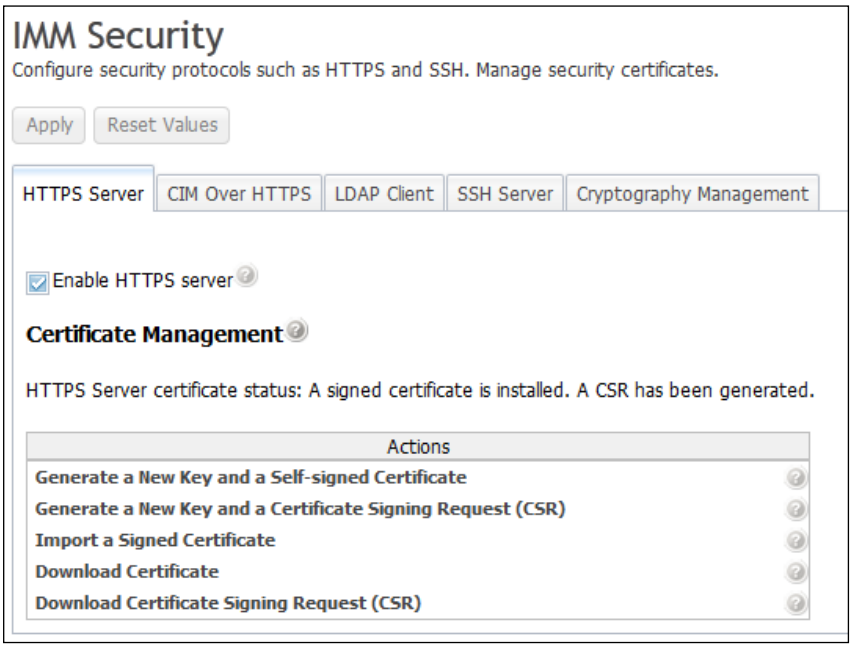
Configuring HTTPS protocol

Click the **HTTPS Server** tab to configure the IMM2 web interface to use the more secure HTTPS protocol rather than the default HTTP protocol.

Notes:

- Only one protocol can be enabled at a time.
- Enabling this option requires additional configuration of the SSL certificates.
- When you change protocols, you must restart the IMM2 web server.

For more information about SSL, see "SSL overview" on page 96. The following illustration shows the HTTPS Server tab.



Note: On some servers, the IMM2 security levels may be controlled by another management system. In such environments, you can disabled the above actions in the IMM2 web interface.

HTTPS certificate handling

Use the options in the Actions menu for HTTPS certificate handling. If an option is disabled, you might need to perform another action first to enable it. While working with HTTPS certificates, you should disable the HTTPS server. For more information about certificate handling, see "SSL certificate handling" on page 96.

Note: After you set up the certificate handling, you must restart the IMM2 for your changes to take effect.

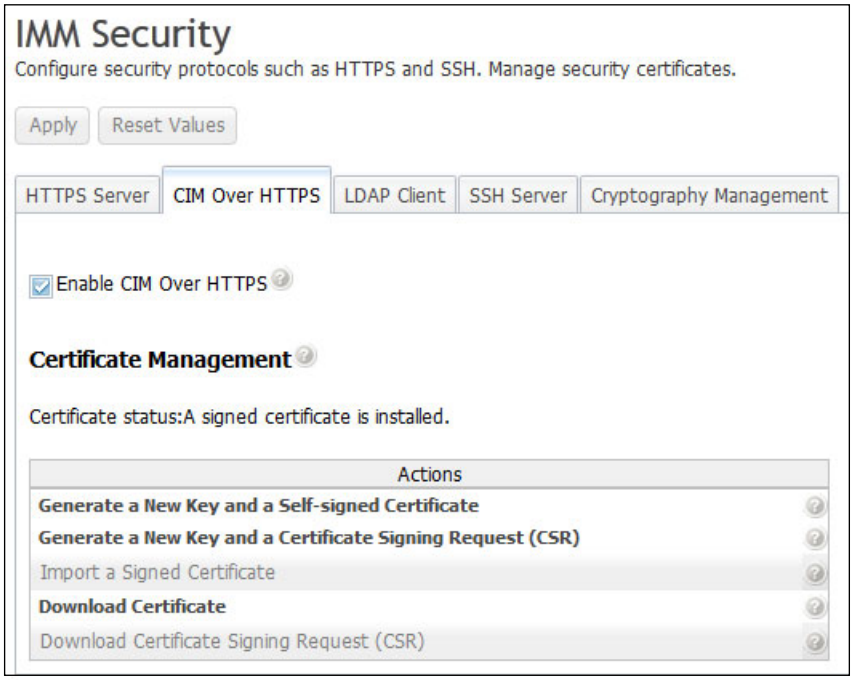
Configuring CIM over HTTPS protocol

Click the **CIM over HTTPS** tab to configure the IMM2 web interface to use the more secure CIM over HTTPS protocol, rather than the default CIM over HTTP protocol.

Notes:

- Only protocol may be enabled at a time.
- Enabling this option requires additional configuration of the SSL certificates.
- When you change protocols, you must restart the IMM2 web server.

For more information about SSL, see “SSL overview” on page 96. The following illustration shows the CIM over HTTPS tab.



CIM over HTTPS certificate handling

Use the options under the Actions menu for CIM over HTTPS certificate handling. If an option is disabled, you might need to perform another action first to enable it. For more information about certificate handling, see “SSL certificate handling” on page 96.

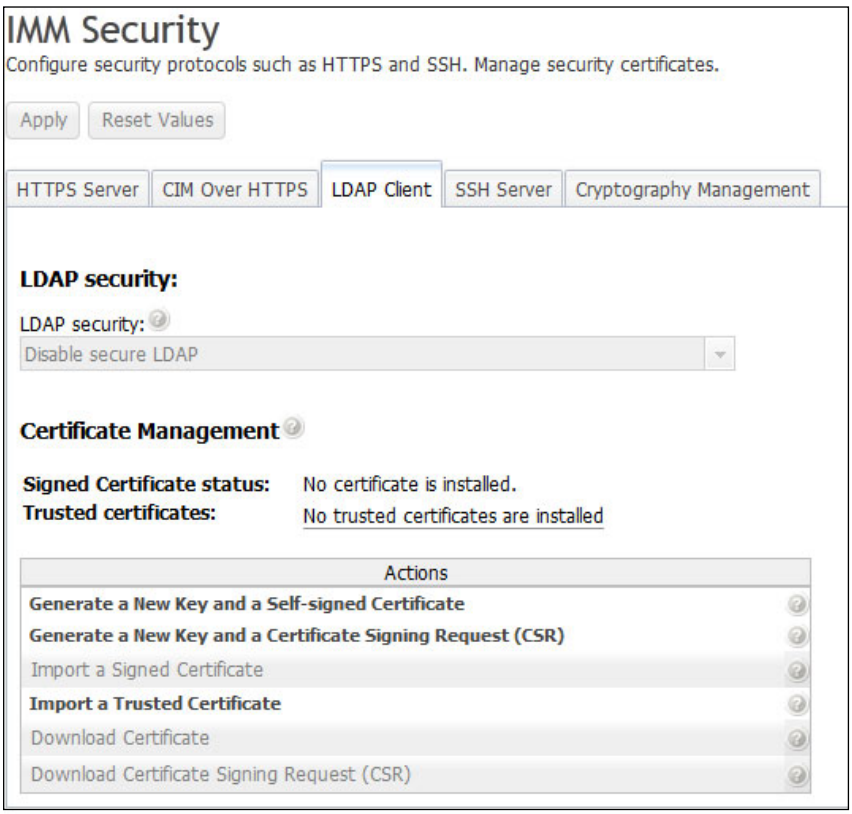
Note: After you set up the certificate handling, you must restart the IMM2 for your changes to take effect.

Configuring LDAP client protocol

Click the **LDAP Client** option to use the more secure LDAP over SSL protocol rather than the default LDAP protocol.

Note: Enabling this option requires additional configuration of the SSL certificates. For more information about SSL, see “SSL overview” on page 96.

The following illustration shows the LDAP Client tab.

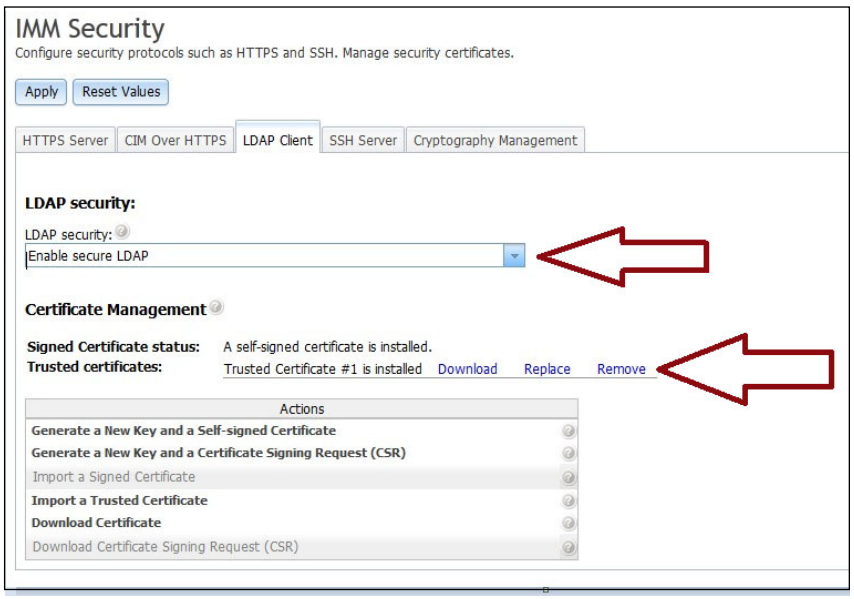


Secure LDAP client certificate handling

Use the options under the Actions menu for LDAP over SSL certificate handling. If an option is disabled, you might need to perform another action first to enable it. While manipulating HTTPS certificates, you should disable the HTTPS server. For more information about certificate handling, see “SSL certificate handling” on page 96. Once you have installed the Trusted Certificate, you can enable LDAP over SSL as shown in the following illustration.

Notes:

- Changes to your IMM2 will take effect immediately.
- Your LDAP server must support Secure Socket Layer 3 (SSL3) or Transport Layer security (TLS) to be compatible with the IMM2 secure LDAP client.



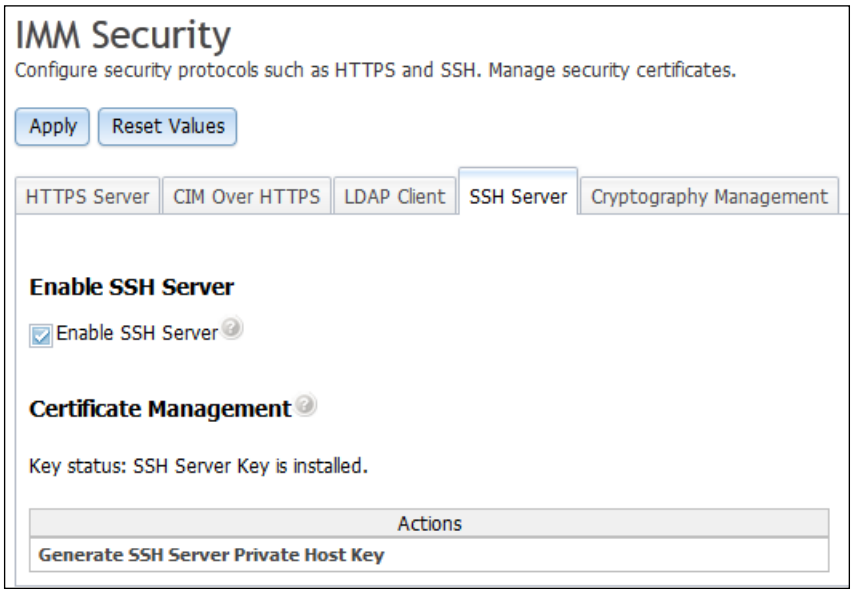
Configuring the Secure Shell server

Click the **SSH Server** tab to configure the IMM2 web interface to use the more secure SSH protocol, rather than the default Telnet protocol.

Note:

- No certificate management is required to use this option.
- The IMM2 will initially create a SSH Server key. If you wish to generate a new SSH Server key, click **Generate SSH Server Private Host Key** in the Actions menu.
- After you complete the action, you must restart the IMM2 for your changes to take effect.

The SSH Server tab is shown in the following illustration.



SSL overview

SSL is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that prevents eavesdropping, tampering, and message forgery. You can configure the IMM2 to use SSL support for different types of connections, such as secure web server (HTTPS), secure LDAP connection (LDAPS), CIM over HTTPS, and SSH server. You can view or change the SSL settings from the Security option under the IMM Management tab. You can also enable or disable SSL and manage the certificates that are required for SSL.

SSL certificate handling

You can use SSL with a self-signed certificate or with a certificate that is signed by a third-party certificate authority. Using a self-signed certificate is the simplest method for using SSL; but, it does create a small security risk. The risk arises because the SSL client has no way of validating the identity of the SSL server for the first connection that is attempted between the client and server. For example, it is possible that a third party might impersonate the IMM2 web server and intercept data that is flowing between the actual IMM2 web server and the user's web browser. If, at the time of the initial connection between the browser and the IMM2, the self-signed certificate is imported into the certificate store of the browser, all future communications will be secure for that browser (assuming that the initial connection was not compromised by an attack).

For more complete security, you can use a certificate that is signed by a certificate authority (CA). To obtain a signed certificate, click **Generate a New Key and a Certificate Signing Request (CSR)** in the Actions menu. You must then send the certificate-signing request (CSR) to a CA and make arrangements to obtain a final certificate. When the final certificate is received, it is imported into the IMM2 by clicking **Import a Signed Certificate** in the Actions menu.

The function of the CA is to verify the identity of the IMM2. A certificate contains digital signatures for the CA and the IMM2. If a well-known CA issues the certificate or if the certificate of the CA has already been imported into the web browser, the browser can validate the certificate and positively identify the IMM2 web server.

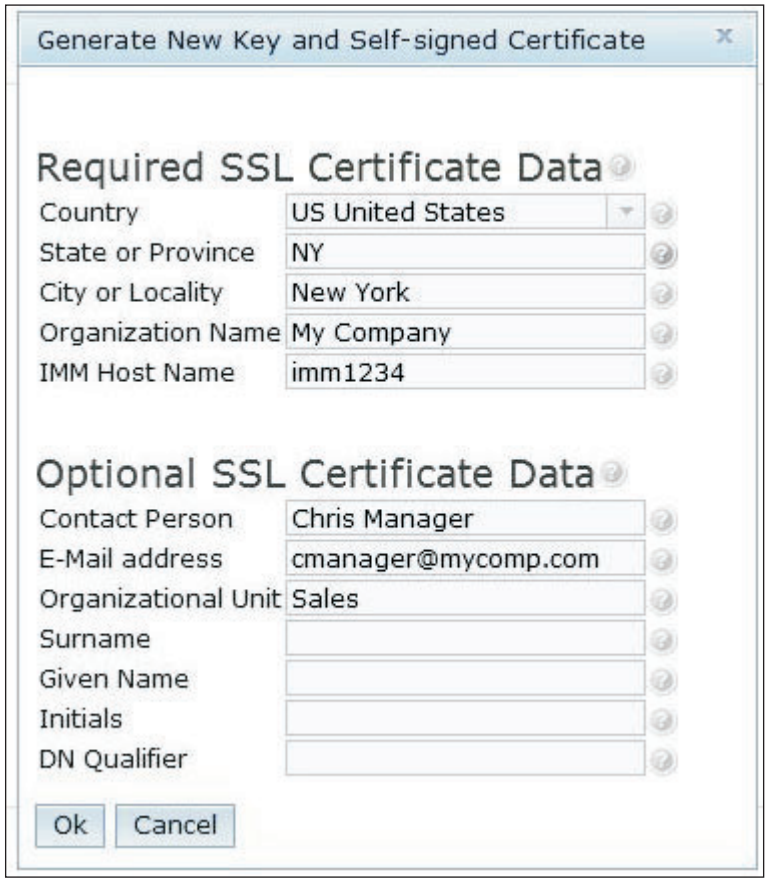
The IMM2 requires a certificate for use with HTTPS Server, CIM over HTTPS, and the secure LDAP client. In addition the secure LDAP client also requires one or more trusted certificates to be imported. The trusted certificate is used by the secure LDAP client to positively identify the LDAP server. The trusted certificate is the certificate of the CA that signed the certificate of the LDAP server. If the LDAP server uses self-signed certificates, the trusted certificate can be the certificate of the LDAP server itself. Additional trusted certificates must be imported if more than one LDAP server is used in your configuration.

SSL certificate management

When managing IMM2 certificates, you are presented with a list of actions or a subset of them, (as shown in the following illustration).

If a certificate is currently installed, you will be able to use the **Download Certificate** action in the Actions menu to download the currently installed certificate or CSR. Certificates that are grayed out are *not* currently installed. The secure LDAP client requires the user to import a trusted certificate. Click **Import a Trusted Certificate** in the Actions menu. After generation of a CSR, click **Import a Signed Certificate** in the Actions menu.

When performing one of the "Generate" actions, a Generate New Key and Self-signed Certificate window opens (as shown in the following illustration).



The Generate New Key and Self-signed Certificate window will prompt you to complete the required and optional fields. You *must* complete the required fields. Once you have entered your information, click **Ok** to complete the task. A Certificate Generated window opens (as shown in the following illustration).

Configuring cryptography management

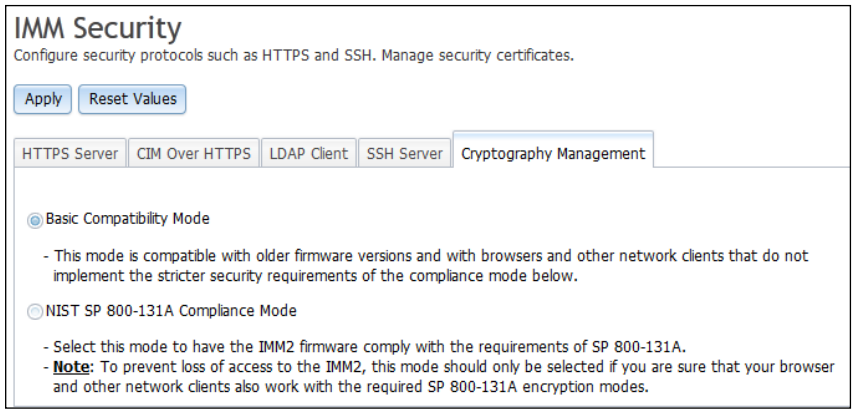
Click the **Cryptography Management** tab to configure the IMM2 firmware to comply with the requirements of SP 800-131A.

The **Cryptography Management** tab contains two choices:

- The Basic Compatibility Mode
- The NIST SP 800-131A Compliance Mode

The **Basic Compatibility Mode** is compatible with older firmware versions and with browsers and other network clients that do not use the NIST SP 800-131A Compliance Mode.

The Cryptography Management tab with the **Basic Compatibility Mode** selected is shown in the following illustration.

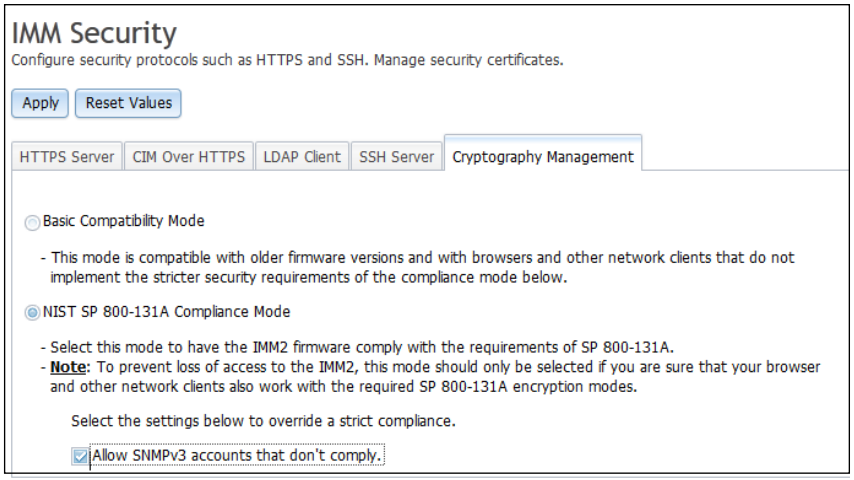


The **NIST SP 800-131A Compliance Mode** provides strict security requirements. When using the **NIST SP 800-131A Compliance Mode**, the IMM2 firmware will comply with the requirements of SP 800-131A.

Notes:

- To prevent loss of access to the IMM2, use the **NIST SP 800-131A Compliance Mode** only if you are sure that your browser and other network clients can work with the SP 800-131A encryption modes.
- When using the **NIST SP 800-131A Compliance Mode**, you can allow SNMPv3 accounts to disobey the restrictions set by the this mode.

The Cryptography Management tab with the **NIST SP 800-131A Compliance Mode** selected is shown in the following illustration.

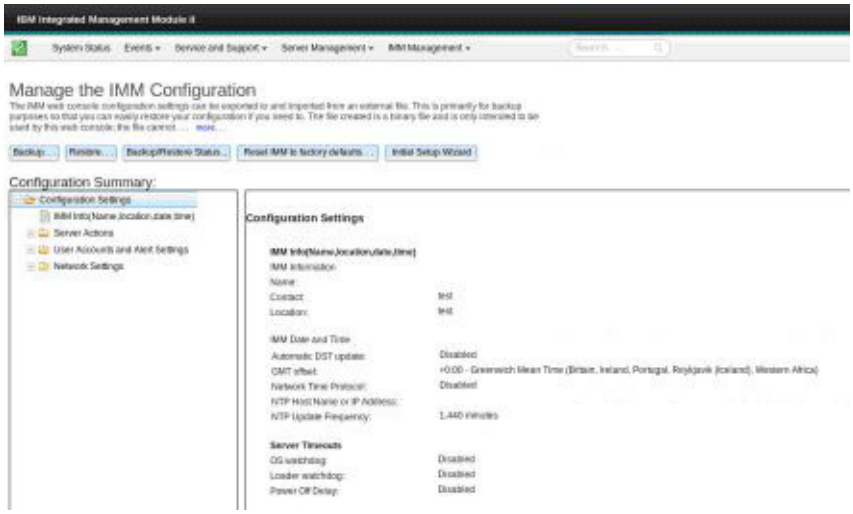


Restoring and modifying your IMM configuration

Select the **IMM Configuration** option from the IMM Management tab for the options to perform the following actions:

- 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

The following illustration shows the Manage the IMM Configuration window.



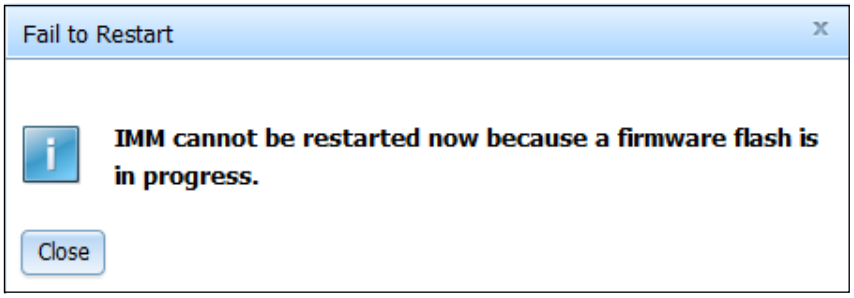
Restarting the IMM2

Select the **Restart IMM** option from the IMM Management tab to restart the IMM2.

Notes:

- Only persons with the Supervisor user authority level can perform this function.
- When Ethernet connections are temporarily dropped, you must log in to the IMM2 to access the IMM2 web interface.

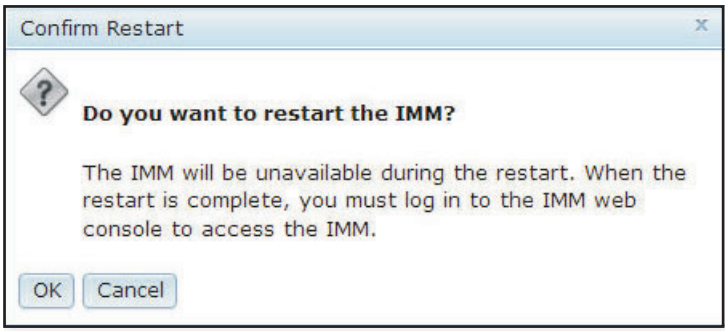
- When any other user is updating server firmware, Restart IMM cannot be performed (as shown in the following illustration).



To restart the IMM2 complete the following steps:

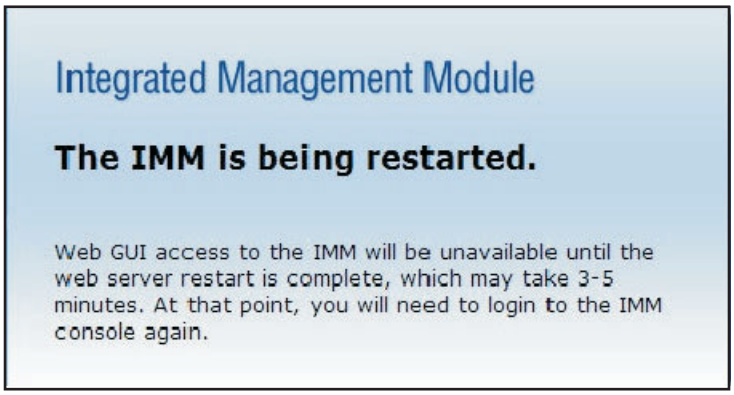
1. Log in to the IMM2. For more information, see "Logging in to the IMM2" on page 10.
2. Click the **IMM Management** tab; then, click **Restart IMM**.
3. Click the **OK** button on the Confirm Restart window. The IMM2 will be restarted.

   The following illustration shows the Confirm Restart window.



   When you restart the IMM2, your TCP/IP or modem connections are broken.

   The following illustration shows the notification window you will see when the IMM2 is being restarted.



4. Log in again to use the IMM2 web interface, (see "Logging in to the IMM2" on page 10 for instructions).

Resetting the IMM2 to the factory defaults

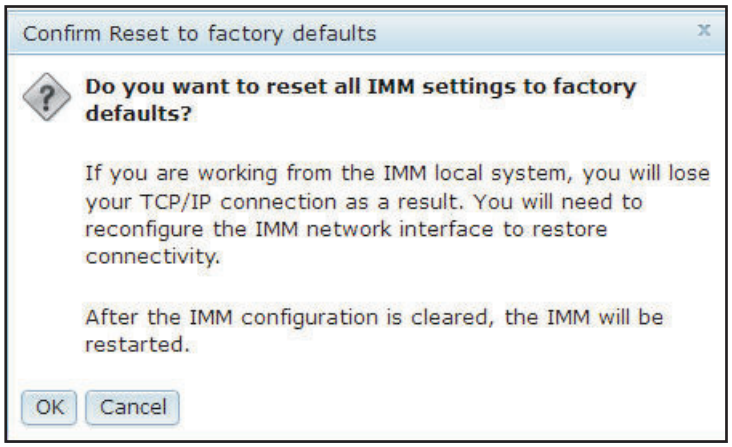
Select the **Reset IMM to factory defaults...** option from the IMM Management tab to restore the IMM2 to the factory default settings.

Notes:

- Only persons with the Supervisor user authority level can perform this function.
- When Ethernet connections are temporarily dropped, you must log in to the IMM2 to access the IMM2 web interface.
- When you use the Reset IMM to factory defaults option, you will lose all modifications that you have made to the IMM2.

To restore the IMM2 factory defaults, complete the following steps:

1. Log in to the IMM2. For more information, see "Logging in to the IMM2" on page 10.
2. Click the **IMM Management** tab; then, click **IMM Reset to factory defaults...**.
3. Click the **OK** button on the Confirm Reset to factory defaults window (as shown in the following illustration).



Note: After the IMM2 configuration is complete, the IMM2 will be restarted. If this is a local server, your TCP/IP connection will be broken and you must reconfigure the network interface to restore connectivity.

4. Log in again to the IMM2 to use the IMM2 web interface, (see "Logging in to the IMM2" on page 10 for instructions).
5. Reconfigure the network interface to restore connectivity.

Activation management key

Click the **Activation Key Management** option from the IMM Management tab to manage activation keys for optional IMM2 and server Features on Demand (FoD) features. See Chapter 7, "Features on Demand," on page 145 for information about managing FoD activation keys.

Chapter 5. Monitoring the server status

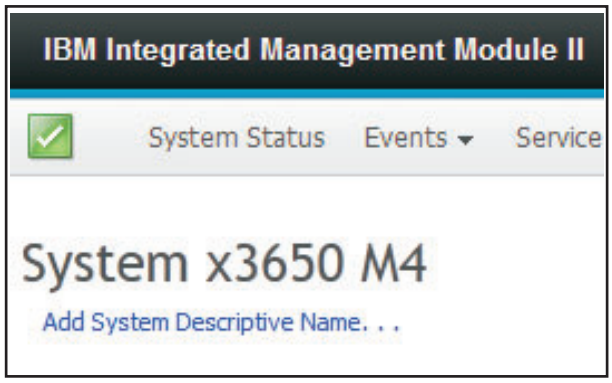
This chapter provides information about how to view and monitor the information for the server that you are accessing.

Viewing the system status

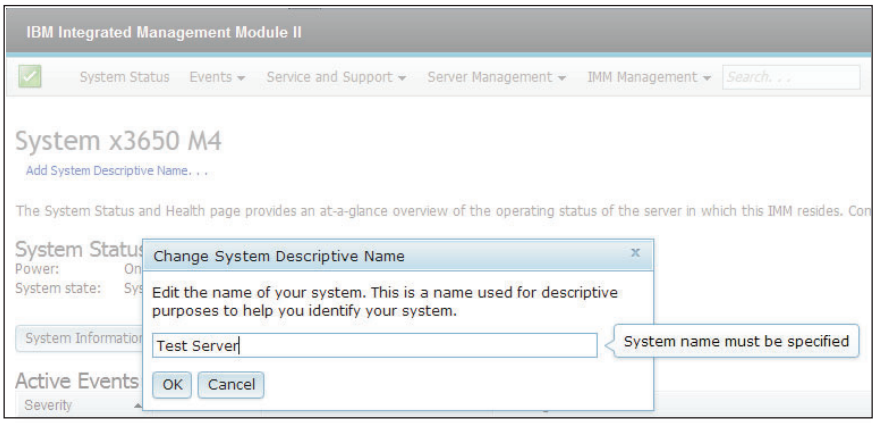
The System Status page provides an overview of the operating status of the IMM2 server. This page also displays the hardware health of the server and any active events occurring on the server.

Note: If you access another page from the System Status page, you can return to the System Status page by clicking **System Status** from the menu items at the top of the page.

You can add a descriptive name to the IMM2 to assist you in identifying one IMM2 from another. Click the **Add System Descriptive Name...** link located below the server product name to designate a name to associate with the IMM2, (as shown in the following illustration).



In the Change System Descriptive Name window, specify a name to associate with the IMM2 (as shown in the following illustration).

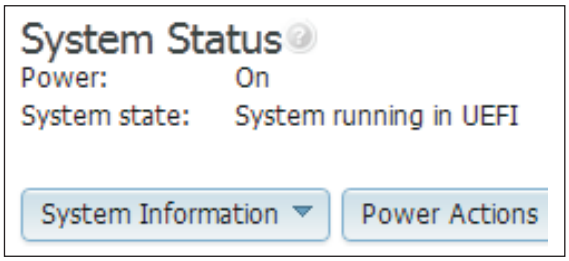


You can rename the System Descriptive Name by clicking the **Rename...** link that is located next to the System Descriptive Name.

The following illustration shows the Rename link.

The System Status page displays the server power state and operating state. The status displayed is the server state at the time the System Status page is opened.

The following illustration shows the **Power** and **System state** fields.



The server can be in one of the system states listed in the following table.

Table 5. System state descriptions

State	Description
System power off/State unknown	The server is powered off.
System on/starting UEFI	The server is powered on; but, UEFI is not running.
System running in UEFI	The server is powered on and UEFI is running.
System stopped in UEFI	The server is powered on; UEFI has detected a problem and has stopped running.

Table 5. System state descriptions (continued)

State	Description
Booting OS or in unsupported OS	The server might be in this state for one of the following reasons: • The operating system (OS) loader has started; but, the OS is not running • The IMM2 Ethernet over USB interface is disabled. • The OS does not have the drivers loaded that support the Ethernet over USB interface.
OS booted	The server OS is running.
Suspend to RAM	The server has been placed in standby or sleep state.

The following menu choices on the System Status page provide additional server information and actions that can be performed on the server.

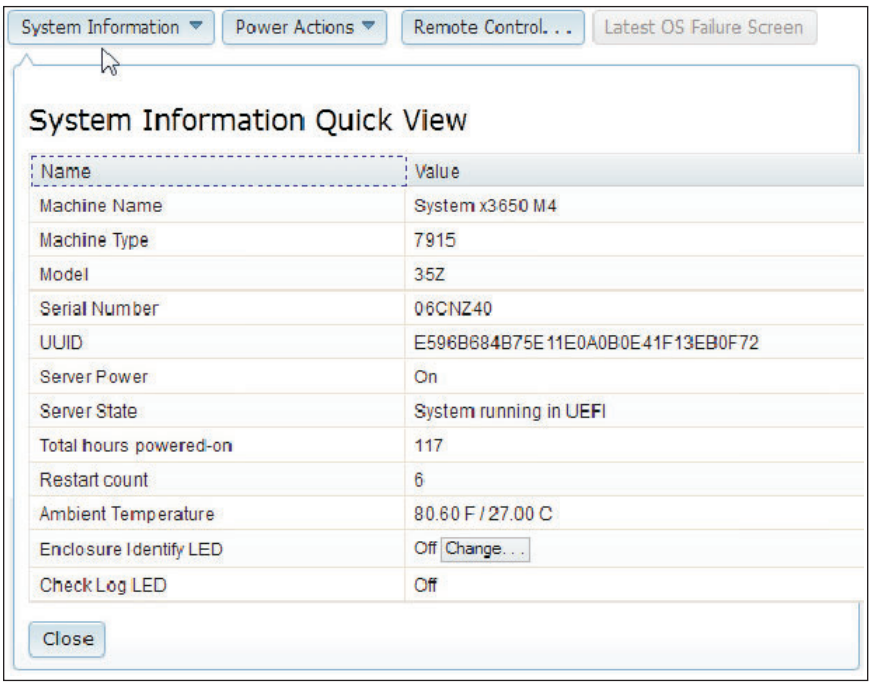
- System Information
- Power Actions
- Remote Control, (see "Remote presence and remote control functions" on page 113 for additional information).
- Latest OS Failure Screen, (see "Capturing the latest OS failure screen data" on page 139 for additional information).

Viewing the system information

The System Information menu provides a summary of common server information. Click the **System Information** tab on the System Status page to view the following information:

- Machine name
- Machine type
- Model
- Serial number
- Universally Unique Identifier (UUID)
- Server power
- Server state
- Total hours powered on
- Restart count
- Ambient temperature
- Enclosure identity LED
- Check log LED

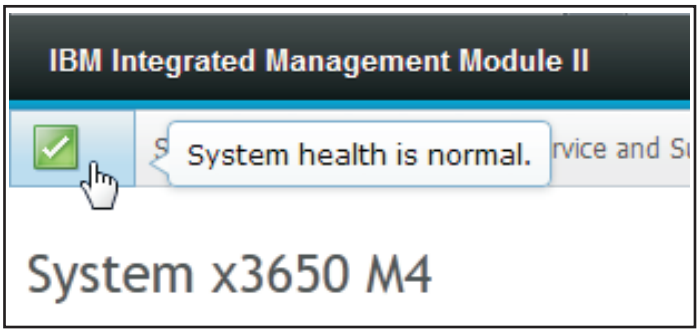
The following illustration shows the System Information window.



Viewing the server health

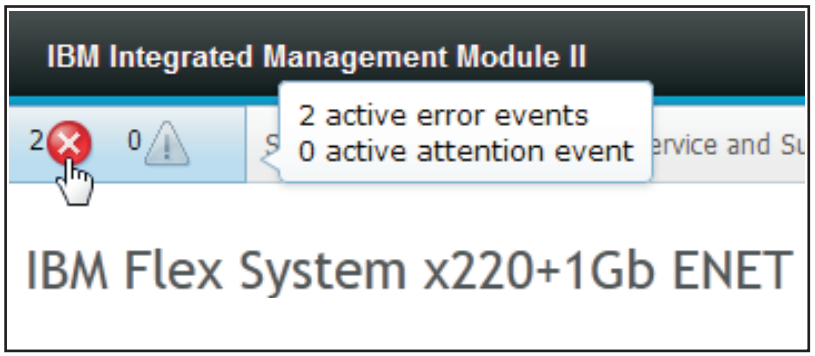
The server health is displayed under the title bar in the upper left corner of the System Status page and is designated by an icon. A green check mark indicates that the server hardware is operating normally. Move your cursor over the green checkmark to get a quick indication of the server health.

The following illustration is an example of a server in a normal mode of operation.



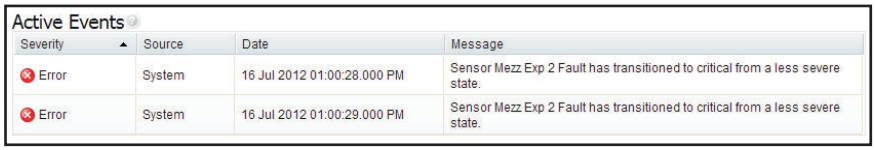
A yellow triangle icon indicates that a warning condition exists. A red circle icon indicates that an error condition exists.

The following illustration is an example of a server with active error events.



If a warning icon (yellow triangle) or error icon (red circle) is displayed, click the icon to display the corresponding events in the Active Events section of the System Status page.

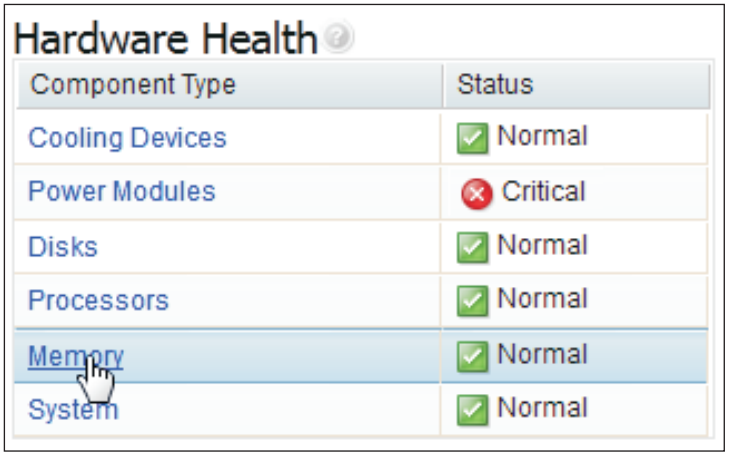
The following illustration is an example of the Active Events section with error conditions.



Viewing the hardware health

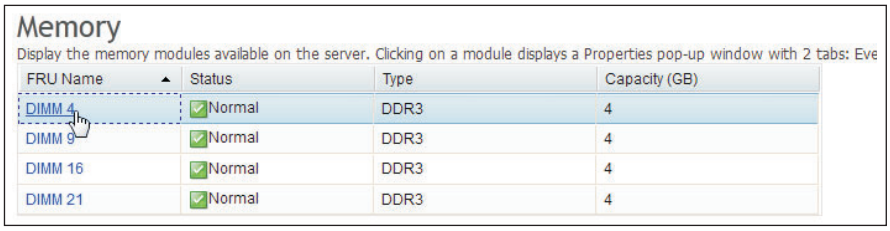
The Hardware Health section of the System Status page list the server hardware components and displays the health status of each component that is monitored by the IMM2. The health status displayed for a component might reflect the most critical state of all individual components for a component type. For example, a server might have several power modules installed and all of the power modules are operating normally except for one. The status for the Power Modules component will indicate critical because of the power module that is not operating normally.

The following illustration shows the Hardware Health section of the System Status page.



Each component type is displayed as a link that can be clicked to obtain more detailed information. When you select a Component Type to view, a table listing the status of all components for that Component Type is displayed.

The following illustration shows the components for the Memory Component Type.

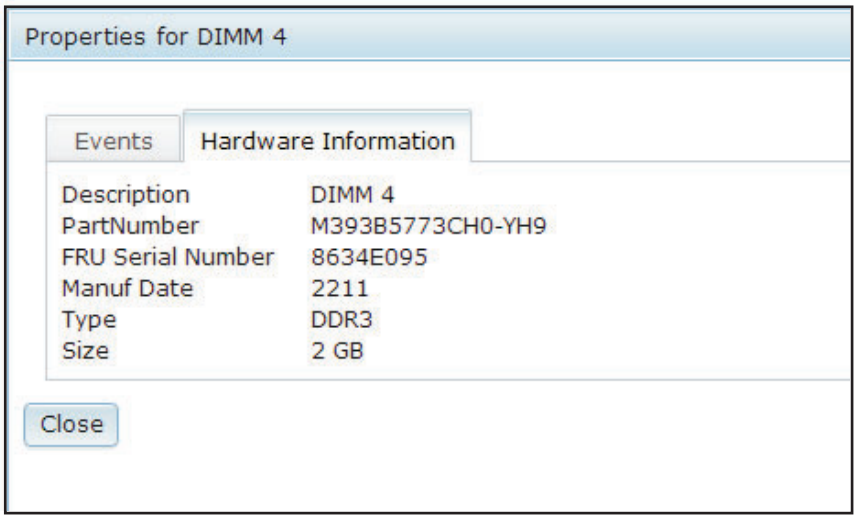


You can click on an individual Field Replaceable Unit (FRU) link in the table to obtain additional information for that component. All active events for the component are then displayed in the Events tab.

The following illustration shows the Events tab for DIMM 4.

If applicable, additional information for the component might be provided in the Hardware Information tab.

The following illustration shows the Hardware Information tab for DIMM 4.



Chapter 6. Performing IMM2 tasks

You can use the information in this section and Chapter 3, "IMM2 web user interface overview," on page 17 to perform the following tasks to control the IMM2.

From the System Status tab, you can perform the following tasks:

- View the server health
- View the server information, for example, the machine name and type, and serial number
- View server power and restart activity
- Remotely control the power status of the server
- Remotely access the server console
- Remotely attach a disk or disk image to the server
- View active events
- View the hardware health of the server components

Note: The System Status page is displayed after logging in to the IMM2. Common information and actions are colocated on this page.

From the Events tab, you can perform the following tasks:

- Manage event log history
- Manage event recipients for email notifications
- Manage event recipients for syslog notifications

From the Services and Support tab, you can perform the following task:

- Manually obtain the service data for your server

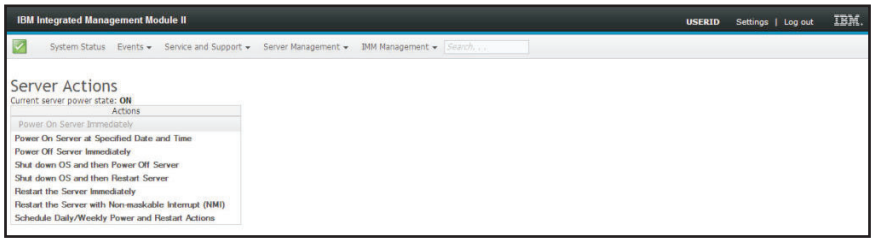
From the Server Management tab, you can select options to perform the following tasks:

- From the Server Firmware option, view and update the firmware levels of server components.
- From the Remote Control option, remotely view and interact with the server console:
  - Remotely control the power status of the server
  - Remotely access the server console
  - Remotely attach a CD drive, DVD drive, diskette drive, USB flash drive or disk image to the server
- From the Server Properties option, you can set parameters to assist in identifying the server.
- From the Server Power Actions option, you can perform such actions as power on, power off, and restart.
- From the Disks option, you can view hard disk drives and events associated with the hard disk drives installed in the server.
- From the Memory option, you can view information about the memory modules installed in the server.

- From the Processor option, you can view information about the microprocessors installed in the server.
- From the Server Timeouts option, you can set timeouts to ensure the server does not hang indefinitely during a firmware update or powering on of the server.
- From the PXE Network Boot option, you can set up attempts to preboot the server Execution Environment.
- From the Latest OS Failure Screen option, you can capture the OS failure screen data and store it.
- From the Power Management option, you can view system power usage and power supply capacity and set parameters for system power usage.

Controlling the power status of the server

The Power Actions option contains a list of actions that you can take to control the server power (as shown in the following illustration). You can choose to power the server on immediately or at a scheduled time. You can also choose to shut down and restart the operating system.



Complete the following steps to perform server power and restart actions:

1. Access the Power Actions menu by performing one of the following steps:
   - Click the **Power Actions** tab on the System Status page.
   - Click **Server Power Actions** from the Server Management tab.
2. Select the server action from the Actions menu list.

The following table contains a description of the power and restart actions that can be performed on the server.

Table 6. Power actions and descriptions

Power Action	Description
Power on server immediately	Select this action item to power on the server and boot the operating system.
Power on server at specified date and time	Select this action item to schedule the server to automatically power on at a specific date and time.
Power off server immediately	Select this action item to power off the server without shutting down the operating system.
Shut down operating system and then power off server [1]	Select this action item to shut down the operating system and power off the server.
Shut down operating system and then restart server [1]	Select this action item to reboot the operating system.

Table 6. Power actions and descriptions (continued)

Power Action	Description
Restart the server immediately	Select this action item to power cycle the server immediately without shutting down the operating system.
Restart the server with non-maskable interrupt (NMI)	Select this action item to force an NMI on a "hung "system. Selection of this action item allows the platform operating system to perform a memory dump that can be used for debug purposes of the system hang condition. The IMM2 firmware uses the auto reboot on the NMI setting from the UEFI F1 in the Setup menu to determine if a reboot after the NMI is needed.
Schedule daily/weekly power and restart actions	Select this action item to schedule daily and weekly power and restart actions for the server.
Enter Sleep Mode	When the platform operating system supports the S3 (Sleep Mode) function and the S3 function is enabled, this action item is displayed. When the operating system is on, select this action item to place the operating system into Sleep Mode.
Exit Sleep Mode	When the platform operating system supports the S3 (Sleep Mode) function and the S3 function is enabled, this action item is displayed. Select this action item to wake up the operating system from the Sleep Mode.
1. If the operating system is in the screen saver or locked mode when a "Shut Down" request is attempted, the IMM2 might not be able to initiate a normal shutdown. The IMM2 will perform a hard reset or shutdown after the power off delay interval expires while the operating system might still be running.	

Remote presence and remote control functions

You can use the IMM2 Remote Control feature or remote presence function in the IMM2 web interface to view and interact with the server console. You can assign to the server a CD or DVD drive, diskette drive, USB flash drive, or a disk image that is on your computer. The remote presence functionality is available with the IMM2 Premium features and is only available through the IMM2 web interface. You must log in to the IMM2 with a user ID that has Supervisor access to use any of the remote control features. For more information about upgrading from IMM2 Basic or IMM2 Standard to IMM2 Premium, see "Upgrading IMM2" on page 3. Refer to the documentation that came with your server for information about the level of IMM2 that is installed in your server.

Use the remote control features to do the following:

- Remotely view video with graphic resolution up to 1600 x 1200 at 75 Hz, regardless of the server state.
- Remotely access the server using the keyboard and mouse from a remote client.
- Map the CD or DVD drive, diskette drive, and USB flash drive on a remote client and map ISO and diskette image files as virtual drives that are available for use by the server.

- Upload a diskette image to the IMM2 memory and map it to the server as a virtual drive.

Notes:

- When the remote control feature is started in multi-user mode, the IMM2 supports up to six simultaneous sessions. The remote disk feature can be exercised by only one session at a time.
- The video viewer is able to display only the video that is generated by the video controller on the system board. If a separate video controller adapter is installed and is used in place of the system's video controller, the IMM2 cannot display the video content from the added adapter on the remote video viewer.

Updating your IMM2 firmware and Java or ActiveX applet

This section provides information about updating the firmware and Java and ActiveX applet.

Important: The IMM2 uses a Java applet or an ActiveX applet to perform the remote presence function. When the IMM2 is updated to the latest firmware level, the Java applet and the ActiveX applet are also updated to the latest level. By default, Java caches (stores locally) applets that were previously used. After a flash update of the IMM2 firmware, the Java applet that the server uses might not be at the latest level.

To correct this problem, turn off caching. The method used will vary based on the platform and Java version. The following steps are for Oracle Java 1.5 on Windows:

1. Click **Start → Settings → Control Panel**.
2. Double-click **Java Plug-in 1.5**. The Java Plug-in Control Panel window opens.
3. Click the **Cache** tab.
4. Choose one of the following options:
   - Clear the **Enable Caching** check box so that Java caching is always disabled.
   - Click **Clear Caching**. If you choose this option, you must click **Clear Caching** after each IMM2 firmware update.

For more information about updating IMM2 firmware, see “Updating the server firmware” on page 125.

Enabling the remote presence function

The IMM2 remote presence function is available only in IMM2 Premium. For more information about upgrading from IMM Standard to IMM Premium, see “Upgrading IMM2” on page 3.

After you have purchased and obtained the activation key for the IMM Premium upgrade install it, see “Installing an activation key” on page 145.

Remote control screen capture

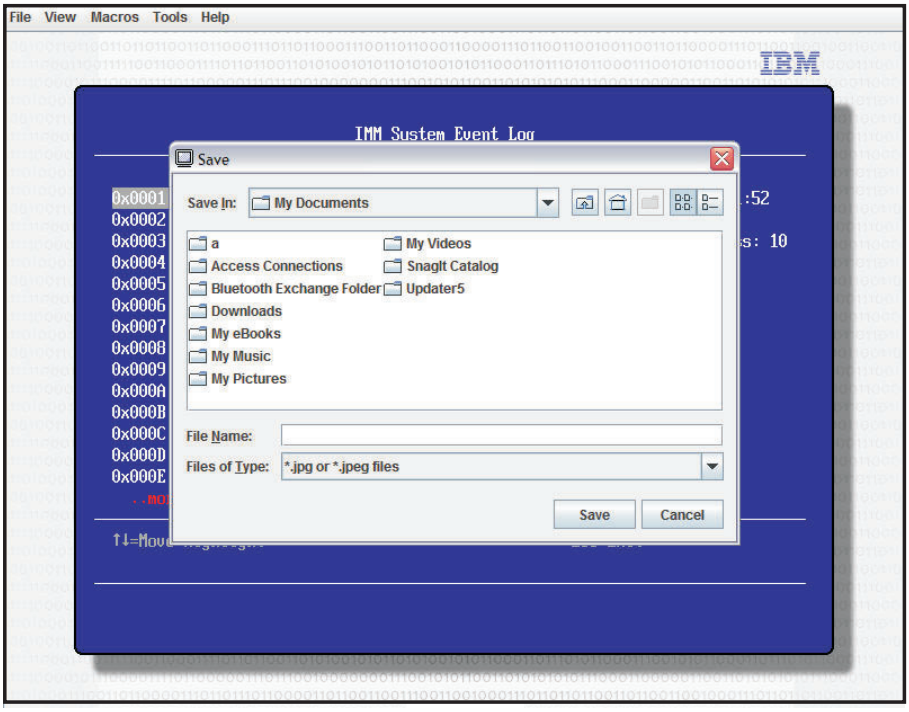
The screen capture feature in the Video Viewer window captures the video display contents of the server. To capture and save a screen image, complete the following steps:

1. In the Video Viewer window, click **File**.
2. Select **Capture to File** from the menu.

3. When you are prompted, enter a name for the image file and save it to the location that you choose on the local client.

   Note: The Java client saves the screen capture image as a JPG file type. The ActiveX client saves the screen capture image as a BMP file type.

   The following illustration shows the window where you specify the location for the image file and enter the name of the image file.



Remote control Video Viewer modes

To change the view of the Video Viewer window, click **View**. The following menu options are available:

Hide Status Bar
Hide the status bar that shows the state of the caps lock, num lock and scroll lock keys. This option is available only when the status bar is shown.

Show Status Bar
Show the status bar that displays the state of the caps lock, num lock and scroll lock keys. This option is available only when the status bar is hidden.

Refresh
The Video Viewer redraws the video display with the video data from the server.

Full Screen
The Video Viewer fills the client desktop with the video display. This option is available only when the Video Viewer is not in full screen mode.

Windowed
The Video Viewer switches out of full screen mode into windowed mode. This option is available only while the Video Viewer is in full screen mode.

Fit The Video Viewer resizes to completely display the target desktop without

an extra border or scroll bars. This requires that the client desktop be large enough to display the resized window.

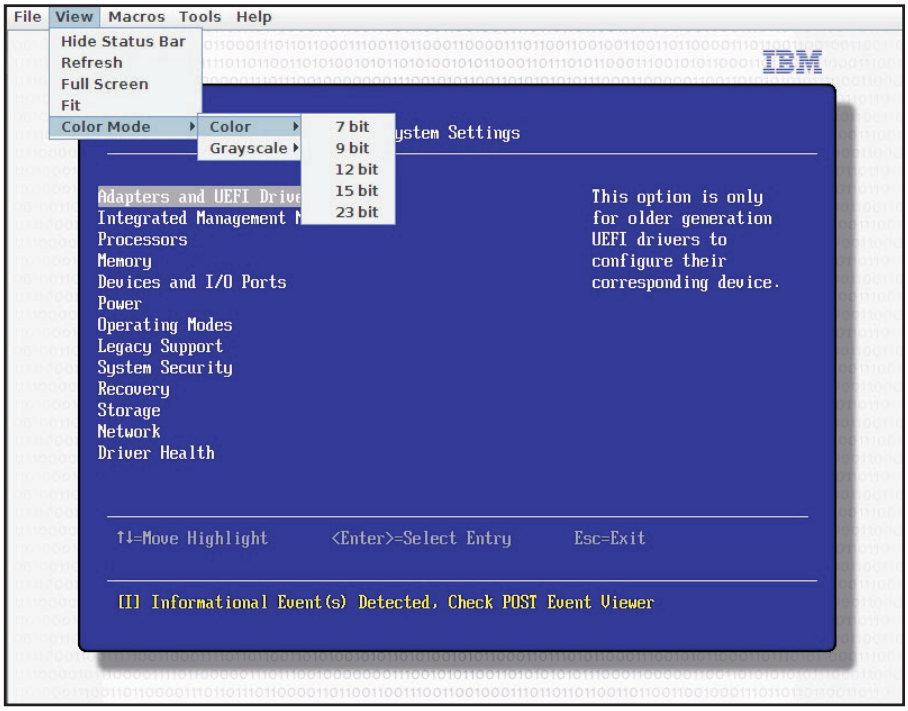
Remote control video color mode

If your connection to the remote server has limited bandwidth, you can reduce the bandwidth demand of the Video Viewer by adjusting the color settings in the Video Viewer window.

Note: The IMM2 has a menu item that allows for color depth adjustment to reduce the data that is transmitted in low-bandwidth situations. This menu item replaces the bandwidth slider used in the Remote Supervisor Adapter II interface.

To change the video color mode, complete the following steps:

1. In the Video Viewer window, click **View**.
2. Click **Color Mode**. Two color-mode options are available (as shown in the following illustration):
   - Color: 7, 9, 12, 15, and 23-bit
   - Grayscale: 16, 32, 64, and 128 shades



3. Select the Color or Grayscale setting.

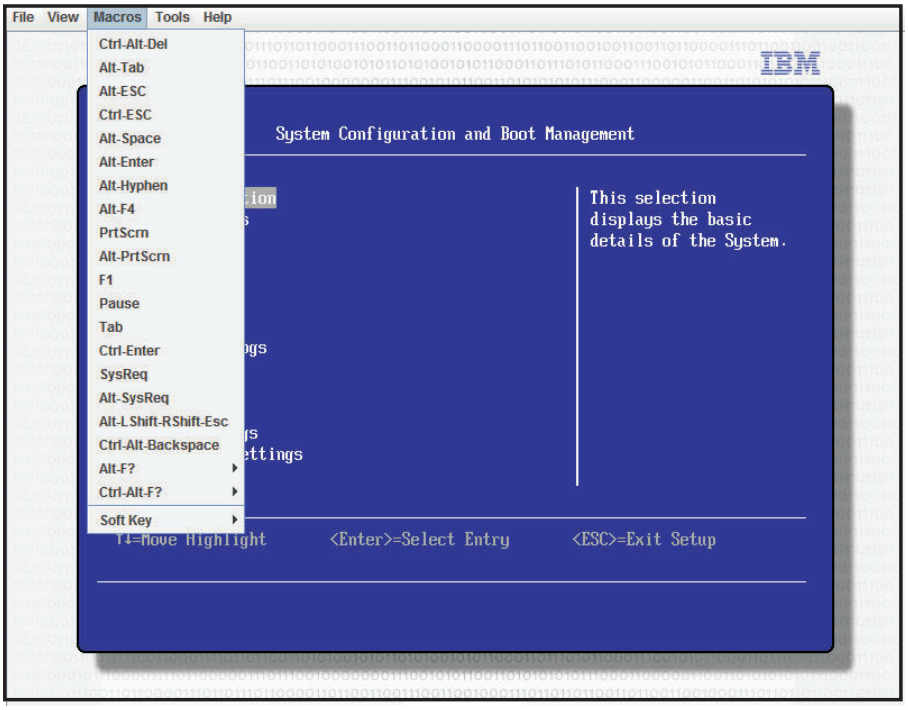
Remote control keyboard support

The operating system on the client server that you are using traps certain key combinations, such as Ctrl+Alt+Del in Microsoft Windows, instead of transmitting them to the server. Other keys, such as F1, might cause an action on your computer as well as on the server.

To use key combinations that affect the remote server, and not the local client, complete the following steps:

1. In the Video Viewer window, click **Macros**.

2. Select one of the predefined key combinations from the menu, or select **Soft Key** to choose or add a user-defined key combination (as shown in the following illustration).



Use the Video Viewer **Macros** menu item to create and edit customized buttons that can be used to send key strokes to the server.

To create and edit customized buttons, complete the following steps:

1. In the Video Viewer window, click **Macros**.
2. Select **Soft Key** and then select **Add**. A new window opens.
3. Click **New** to add a new key combination, or select a key combination and click **Delete** to remove an existing key combination.
4. If you are adding a new combination, type the key combination that you want to define in the window that opens after selecting **New**; then, click **OK**.
5. When you are finished defining or removing key combinations, click **OK**.

International keyboard support

The Video Viewer uses platform-specific native code to intercept key events to access the physical key information directly. The client detects the physical key events and passes them along to the server. The server detects the same physical keystrokes that the client experienced and supports all standard keyboard layouts with the only limitation that the target and client use the same keyboard layout. If a remote user has a different keyboard layout from the server, the user can switch the server layout while it is being accessed remotely and then switch back again.

Keyboard pass-through mode

The keyboard pass-through mode disables the handling of most special key combinations on the client so that they can be passed directly to the server. This provides an alternative to using the macros.

Some operating systems define certain keystrokes to be outside the control of an application, so the behavior of the pass-through mechanism operates independently of the server. For example, in a Linux X session, the Ctrl+Alt+F2 keystroke combination switches to Virtual Console 2. There is no mechanism to intercept this keystroke sequence and; therefore, no way for the client to pass these keystrokes directly to the target. The only option in this case is to use the keyboard macros defined for this purpose.

To enable or disable the keyboard pass-through mode, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Select **Session Options** from the menu.
3. When the Session Options window opens, click the **General** tab.
4. Select the **Pass all keystrokes to target** check box to enable or disable the keyboard pass-through mode.
5. Click **OK** to save the choice.

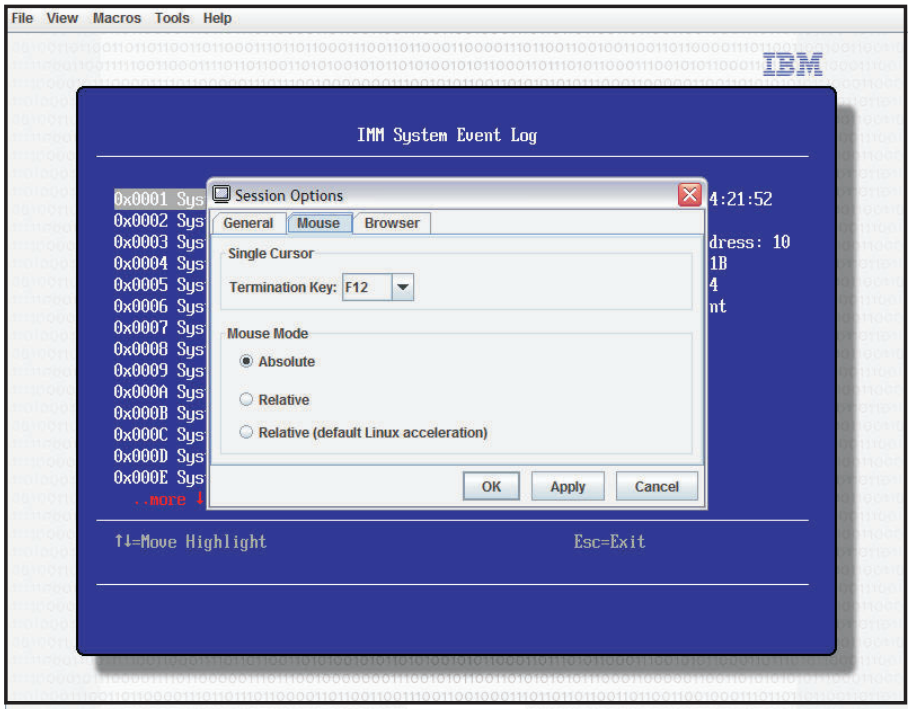
Remote control mouse support

The Video Viewer window offers several options for mouse control, including absolute mouse control, relative mouse control, and single cursor mode.

Absolute and relative mouse control

To access the absolute and relative options for controlling the mouse, complete the following steps:

1. In the Remote Control window, click **Tools**.
2. Select **Session Options** from the menu.
3. When the Session Options window opens, click the **Mouse** tab (as shown in the following illustration).



4. Select one of the following **Mouse Modes**:

Absolute
The client sends mouse location messages to the server that are always relative to the origin (upper left area) of the viewing area.

Relative
The client sends the mouse location as an offset from the previous location.

Relative (default Linux acceleration)
The client applies an acceleration factor to align the mouse better on Linux targets. The acceleration settings have been selected to maximize compatibility with Linux distributions.

Single cursor mode

Some operating systems do not align the local and remote cursors, which results in offsets between the local and remote mouse cursors. The single cursor mode hides the local client cursor while the mouse is within the Video Viewer window. When the single cursor mode is activated, you see only the remote cursor. To enable the single cursor mode, click **Tools > Single Cursor** from the Video Viewer window.

Note: When the Video Viewer is in the single cursor mode, you cannot use the mouse to switch to another window or click outside the KVM client window, because there is no local cursor.

To disable the single cursor mode, click the **Defined Termination** key. To view the defined termination key, or change the termination key, click **Tools > Session Options > Mouse**.

Remote power control

You can send server power and restart commands from the Video Viewer window without returning to the web browser. To control the server power with the Video Viewer, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Click **Power**. Select one of the following commands:

   On Turns on the server power.

   Off Turns off the server power.

   Reboot
   Restarts the server.

   Cycle Turns the server power off, then back on.

Viewing performance statistics

To view the Video Viewer performance statistics from the Video Viewer window, click **Tools**; then, click **Stats**. The following information is displayed:

Frame Rate
A running average of the number of frames, decoded per second by the client.

Bandwidth
A running average of the total number of kilobytes per second received by the client.

Compression
A running average of the bandwidth reduction due to video compression. This value is often displayed as 100.0%. It is rounded to the tenth of a percent.

Packet Rate
A running average of the number of video packets received per second.

Starting Remote Desktop Protocol

If the Windows-based Remote Desktop Protocol (RDP) client is installed, you can use a RDP client instead of the KVM client. The remote server must be configured to receive RDP connections.

Knock-knock feature description

When all possible remote control sessions are occupied (one session in the single-user mode option or six sessions in the multiuser mode option), another web user can send a disconnection request to the remote control user who has enabled the Knock-knock feature. This is only possible if the user that enabled the Knock-knock feature is not handling a disconnection request from other web user.

If the remote control user who has enabled the Knock-knock feature accepts the request or does not reply to the request within the timeout value, the remote control session will be terminated and will be reserved for the web user sending the request. If the web user sending the disconnection request does not launch a Java or ActiveX remote control session with the reserved remote control session within five minutes, the remote control session is no longer reserved for the web user.

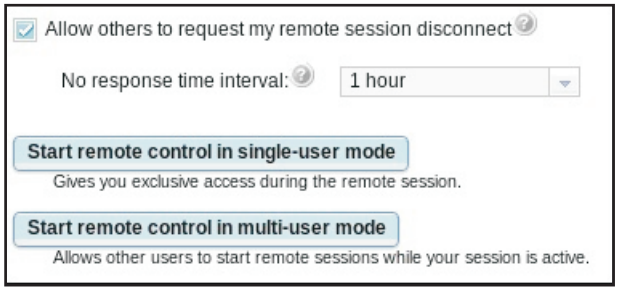
To enable the Knock-knock feature complete the following steps:

1. Access the Remote Control page by selecting one of the following menu choices:
   - Click **Remote Control** from the Server Management tab.
   - Click **Remote Control...** on the System Status page.
2. Click the **Allow others to request my remote session disconnect** checkbox.

   Note: There must exist one or more additional users selecting the **Allow others to request my remote session disconnect** checkbox when using the remote control feature.
3. Select a time interval from the **No response time interval** field.
4. Start the remote control session by selecting the user mode. Select one of the following modes:
   - Start remote control in single-user mode
   - Start remote control in multiuser mode

   Notes:
   - The IMM2 supports up to six simultaneous video sessions in the multiuser mode.
   - The Knock-knock feature is automatically enabled.

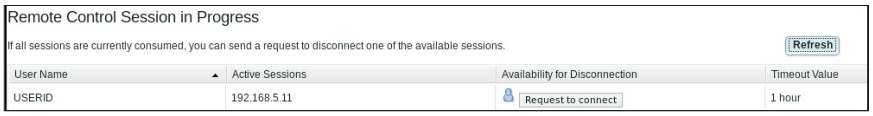
The following illustration shows the fields described in steps 2 through 4.



To request a remote session complete the following steps:

1. Click **Refresh** to display the Remote Control session that is in progress.

   The following illustration shows the Remote Control Session in Progress window.



   You will see one of the following responses in the **Availability for Disconnection** field:

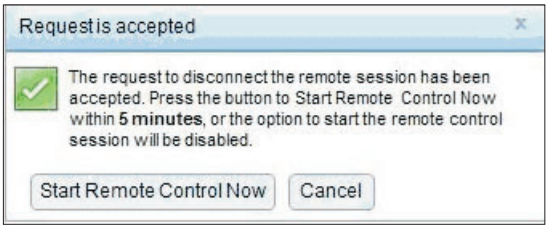
   - **Request to connect:** This text is displayed when the remote control user enables the Knock-knock feature and is not handling a disconnection request from another web user. The current web user has not sent a disconnection request to the remote control user.
   - **Waiting for response:** This text is displayed when the remote control user is handling the disconnection request from the current web user. The current web user can send a cancel request to the remote control user by clicking the **Cancel** button.
   - **Other request is pending:** This text is displayed for one of the following conditions:
     - The remote control user is handling the disconnection request from another web user.
     - The remote control user enabled the Knock-knock feature and the current web user is waiting for the response of the disconnection request from another remote control user.
   - **Not available:** This text is displayed under one of the following conditions:
     - All of the remote control sessions are not occupied. Whether the remote control user has or has not enabled the Knock-knock feature, has no effect on this condition.
     - All of the remote control sessions are occupied and the remote control user has not enable the Knock-knock feature.
     - This remote control connection is reserved for another user for five minutes.

2. Click **Request to connect** to send a disconnection request to the remote control user.

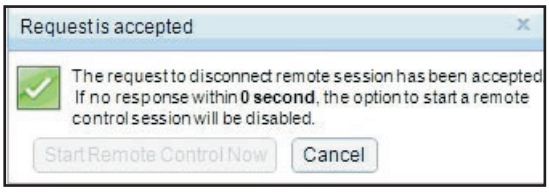
   The following illustration shows the window that is displayed when the request is successfully sent.

If the remote control user accepts the disconnect request, the web user must start the remote control session within five minutes. If the web user does not start the session within five minutes, the session will not be reserved.

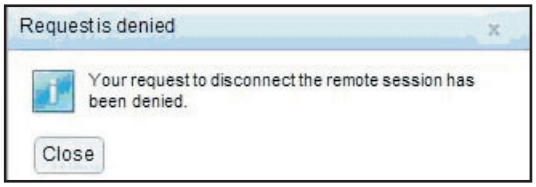
The following illustration shows the information that is displayed when the disconnect request is accepted and the request is in a reserved state.



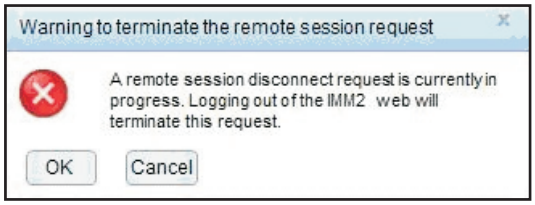
The following illustration shows the information that is displayed when the disconnect request is accepted and the request is in an unreserved state.



If the remote control user denies the disconnection request, the user submitting the disconnect request will receive information stating that the request is denied (as shown in the following illustration).

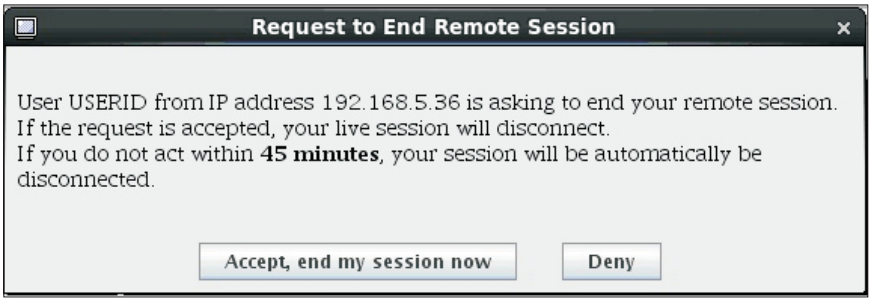


If the web user attempts to log out of the IMM2 before receiving a message about their request, the web user will receive a message (as shown in the following illustration).

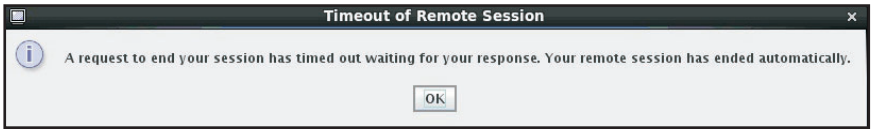


After the remote control user receives the request, the user must determine whether to release the remote session in the interval time selected before starting the remote control session. A Request to End Remote Session window is displayed to remind the remote control user of any time remaining.

The Request to End Remote Session window is shown in the following illustration.



If the remote control user selects **Accept, end my session now**, the remote viewer will automatically close. If the remote control user selects **Deny**, the remote control user will continue to keep the remote session. After the Request to End Remote Session is ended, the remote session will be released automatically and the following window opens.



Remote disk

From the Virtual Media Session window, you can assign to the server a CD or DVD drive, a diskette drive, USB flash drive that is on your computer, or you can specify a disk image on your computer for the server to use. You can use the drive for functions such as restarting (booting) the server, updating code, installing new software on the server, and installing or updating the operating system on the server. You can access the remote disk. Drives and disk images are displayed as USB drives on the server.

Notes:

- USB support is required for the remote disk functionality. The following server operating systems have USB support:
  - Microsoft Windows Server 2003: Web, Std, Ent, DC (SP2, R2, SBS)
  - Microsoft Windows Server 2008 SP2: Std, SBS, EBS
  - Microsoft Windows Server 2008 R2
  - SUSE Linux Enterprise Server V10 SP3: x86_64
  - SUSE Linux Enterprise Server V11: x86,_64
  - Red Hat Enterprise Linux Enterprise Servers V3.7: x86, x86_64
  - Red Hat Enterprise Linux Enterprise Servers V4.8: x86, x86_64
  - Red Hat Enterprise Linux Enterprise Servers V5.5: x86, x86_64
  - Red Hat Enterprise Linux Enterprise Servers V6.0: x86, x86_64
  - ESX 4.5: 4.0 U1
- The client server requires the Java 1.5 Plug-in or later.
- The client server must have an Intel Pentium III microprocessor or greater, operating at 700 MHz or faster, or equivalent.

Accessing the Remote Control

To begin a remote control session and access the remote disk, complete the following steps:

1. In the Video Viewer window click **Tools**.
2. Click **Launch Virtual Media**. The Video Viewer window opens.

Note: If the **Encrypt disk and KVM data during transmission** check box is selected before the Video Viewer window opens, the disk data is encrypted with ADES encryption.

The Virtual Media Session window is separate from the Video Viewer window. The Virtual Media Session window lists all of the drives on the client that can be mapped as remote drives. The Virtual Media Session window also allows you to map ISO and diskette image files as virtual drives. Each mapped drive can be marked as read-only. The CD and DVD drives and ISO images are always read-only.

Mapping and unmapping drives

To map a drive, select the **Select** check box next to the drive that you want to map.

Note: A CD or DVD drive must contain media before it is mapped. If the drive is empty, you are prompted to insert a CD or DVD into the drive.

Click the **Mount Selected** button to mount and map the selected drive or drives. If you click **Add Image**, diskette image files and ISO image files can be added to the list of available drives. After the diskette or ISO image file is listed in the Virtual Media Session window, it can be mapped just like the other drives. To unmap the drives, click the **Unmount All** button. Before the drives are unmapped, you must confirm that you want the drives to be unmapped.

Note: After you confirm that you want the drives to be unmapped, all of the drives are unmounted. You cannot unmount drives individually.

Once an image is added to the list and the **Map** checkbox is selected, (if the image is suitable for loading to IMM2 memory for the Remote Disk-on-Card (RDOC) feature) a window opens. This window gives you the option to transfer the image to the server. If you select **Yes**, enter a name for the image.

Note: Do not enter special characters such as an ampersand (&) or spaces in the name.

Uploading an image to IMM2 memory enables the disk to remain mounted on the server so that you can access the disk later, even after the IMM2 web interface session has ended. Multiple images can be stored on the IMM2; but, the total space used cannot exceed 50 Mb. To unload the image file from memory, select the name in the RDOC Setup window and click **Delete**.

Exiting Remote Control

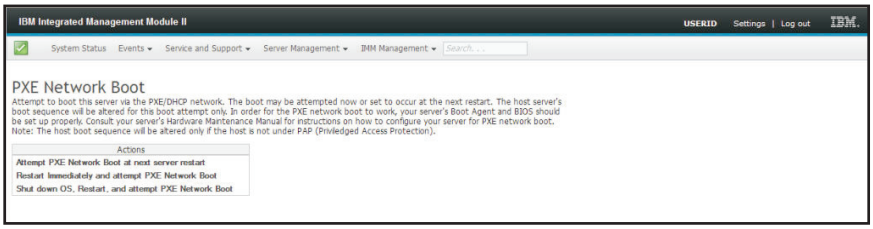
Close the Video Viewer and the Virtual Media Session windows when you have finished using the Remote Control feature.

Setting up PXE network boot

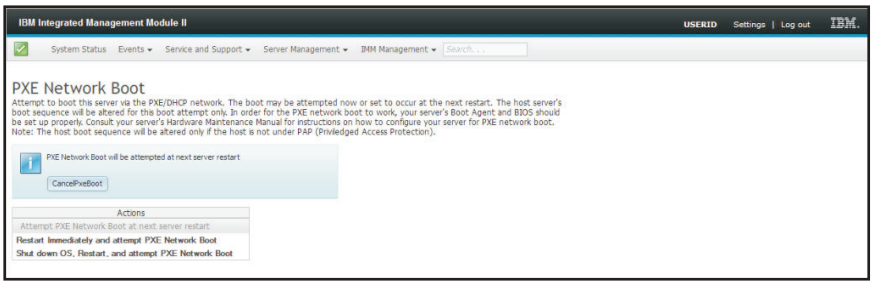
Use the PXE Network Boot option to set up attempts to preboot the server Execution Environment. Perform the following steps to set up your server to attempt a Preboot Execution Environment network boot at the next server restart.

1. Log in to the IMM2. For more information, see“Logging in to the IMM2” on page 10 for additional information.

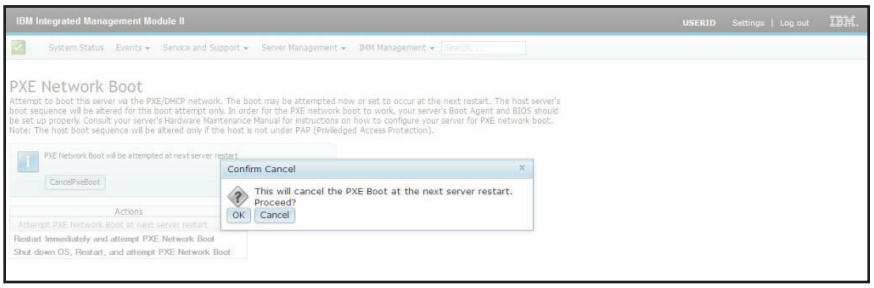
2. Click **Server Management**; then, select **PXE Network Boot**.
   The following window opens.



3. Select **Attempt PXE Network Boot at next server restart** from the Action options. The following window opens.



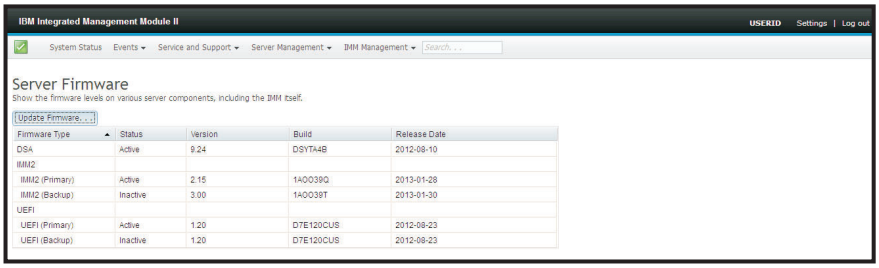
   If you wish to cancel the selection, click **CancelPxeBoot**. The following Confirm Cancel window opens.



Updating the server firmware

The Server Firmware option displays firmware levels and allows you to update the DSA, IMM2, and UEFI firmware. The current versions of the IMM2, UEFI, and DSA firmware are displayed. This includes the Active, Primary, and Backup versions.

The following illustration shows the Server Firmware page.



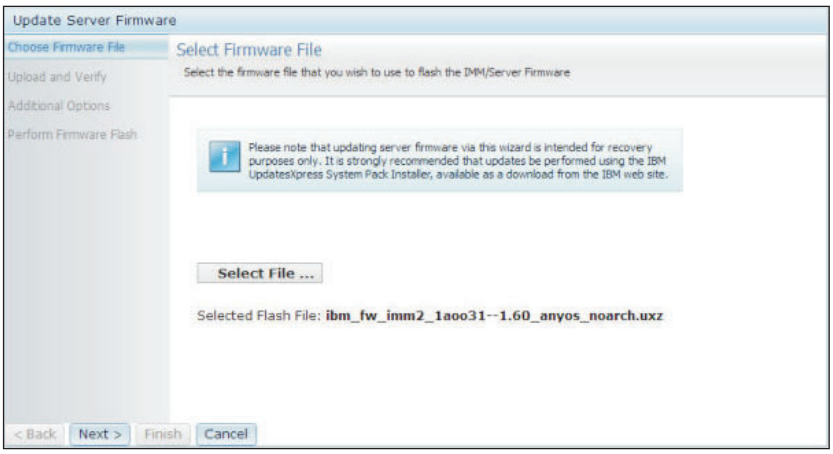
The current status and versions of firmware for the IMM2, UEFI, and DSA are displayed, including the primary and backup versions. There are three categories for the firmware status:

- **Active:** The firmware is active.
- **Inactive:** The firmware is not active.
- **Pending:** The firmware is waiting to become active.

Attention: Installing the wrong firmware update might cause the server to malfunction. Before you install a firmware or device-driver update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware or device-driver version to the latest version.

To update the server firmware complete the following steps:

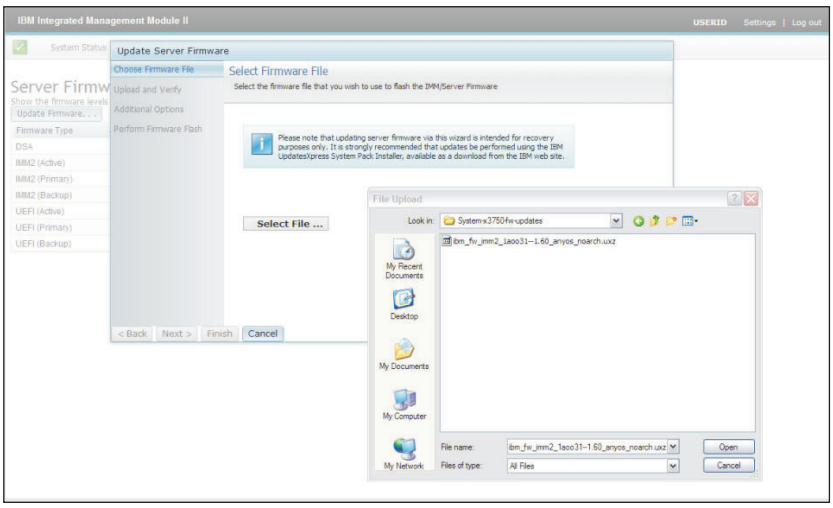
1. Click **Server Firmware** from the Server Management menu list.
2. Click **Update Firmware**. The Update Server Firmware window opens (as shown in the following illustration).



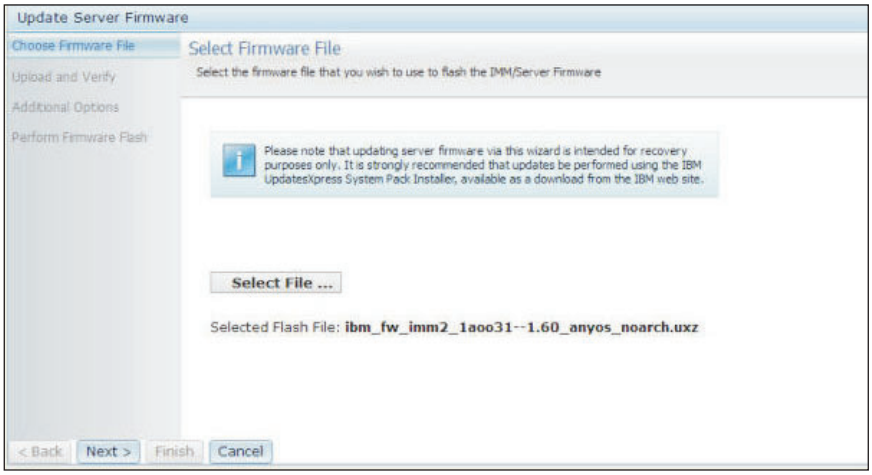
3. Read the warning notice *before* continuing with the next step.
4. Perform one of the following steps:
   - Click **Cancel** and return to the previous Server Firmware window.
   - Click **Select File...** to select the firmware file that you want to use to flash the server firmware.

     Note: All other options are grayed out when the Update Server Firmware window initially opens.

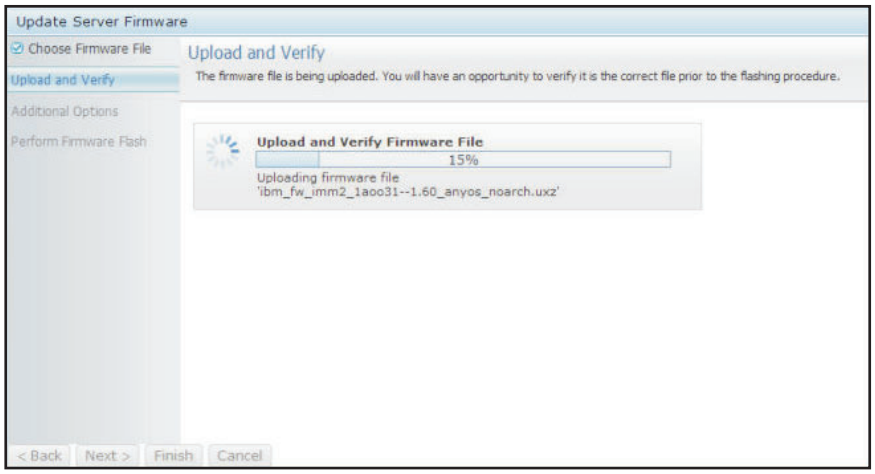
     When you click **Select File...**, a File Upload window opens (as shown in the following illustration). This window allows you to browse to the desired file.



5. Navigate to the file you want to select and click **Open**. You are returned to the Update Server Firmware window with the selected file displayed (as shown in the following illustration).

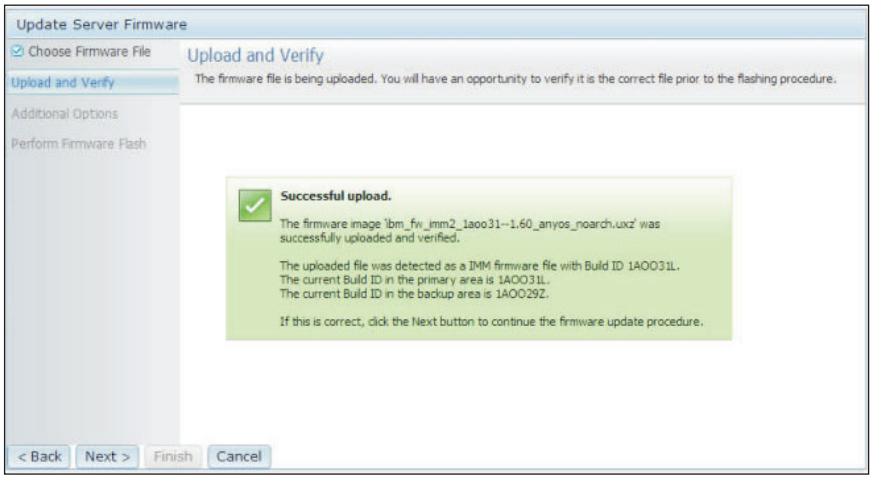


6. Click **Next >** to begin the upload and verify process on the selected file. A progress meter will be displayed as the file is being uploaded and verified (as shown in the following illustration).



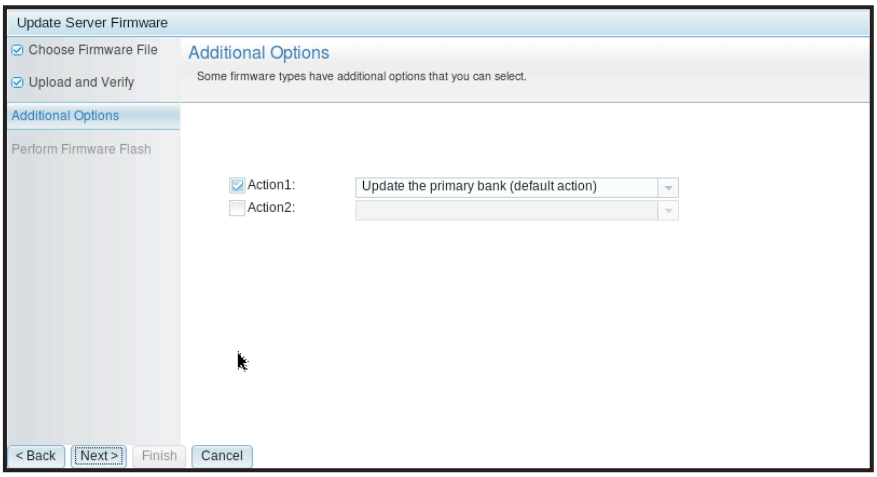
You can view this status window to verify that the file you selected to update is the correct file. The status window will have information regarding the type of firmware file that is to be updated such as DSA, IMM, or UEFI.

After the firmware file is uploaded and verified successfully, a Successful upload window opens (as shown in the following illustration).

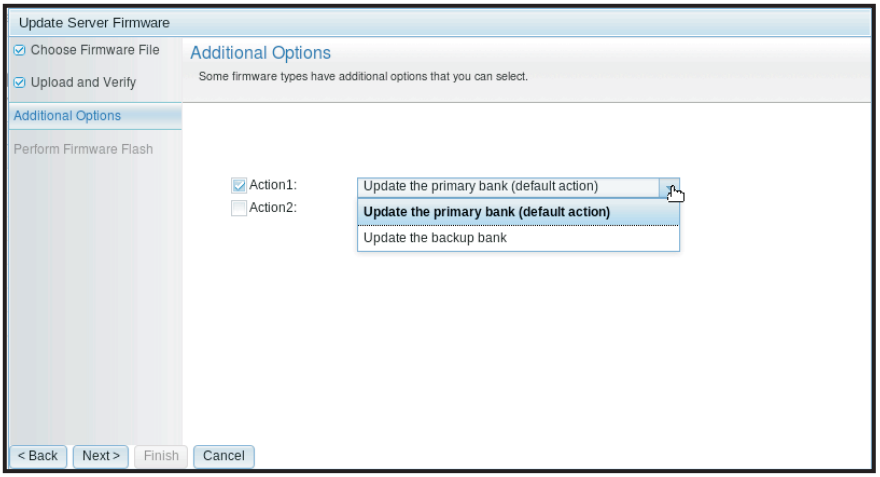


7. Click **Next >** if the information is correct. Click **< Back** if you want to redo any of the selections.

   If you click **Next >**, a set of additional options are displayed (as shown in the following illustration).



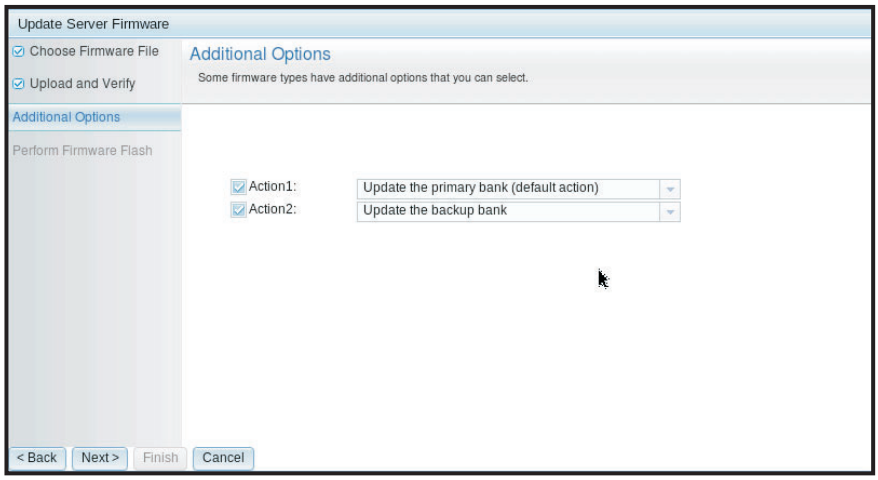
8. The drop-down menu beside the **Action 1** field gives you the choice to **Update the primary bank (default action)** or **Update the backup bank** (as shown in the following illustration).



After you select an action, you are returned to the previous screen with the requested additional action displayed.

After the selected action is loaded, that action and a new **Action 2** drop-down menu are displayed (as shown in the following illustration).

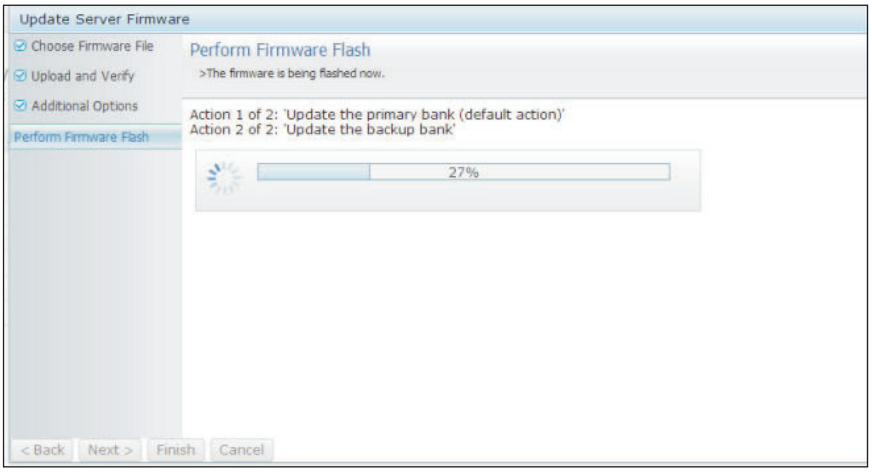
Note: To disable an action and start the additional option process again, click the checkbox beside the related action.



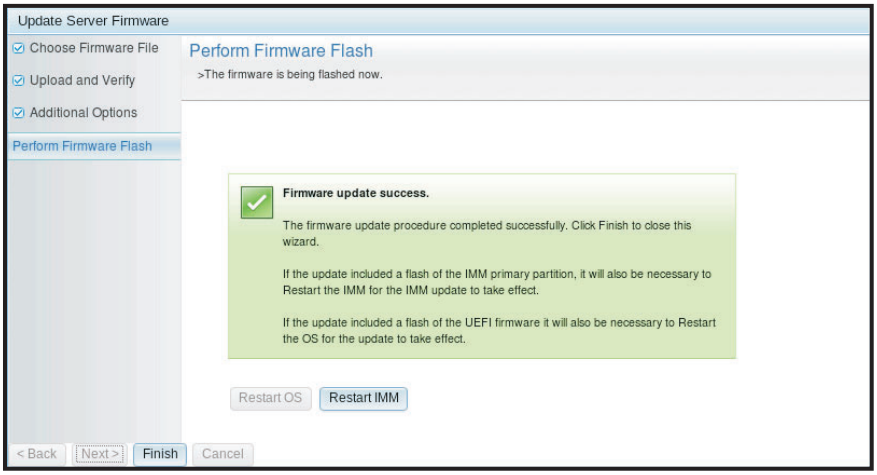
The previous screen shows that for Action 1, the primary bank is selected to be updated. You can also select to update the backup bank under Action 2 (as shown in the previous screen). Both the primary bank and the backup bank will be updated at the same time when you click **Next >**.

Note: Action 1 must be different from Action 2.

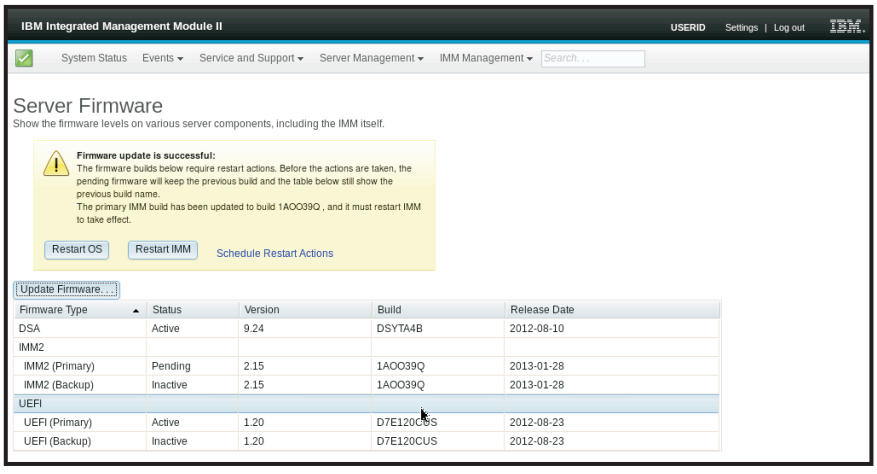
A progress meter shows the progress of the update for the primary and backup banks, (as shown in the following illustration).



When the firmware update is completed successfully, the following window opens. Select the related operation according to the displayed content to complete the update process.



If the primary firmware update did not complete, the following window opens when the Server Firmware screen is displayed.



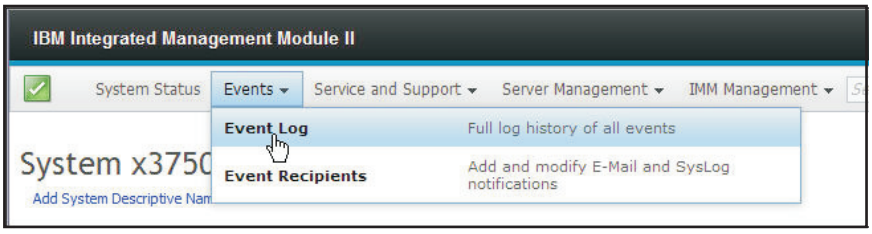
Managing system events

The Events menu enables you to manage the Event Log history and manage Event Recipients for email and syslog notifications.

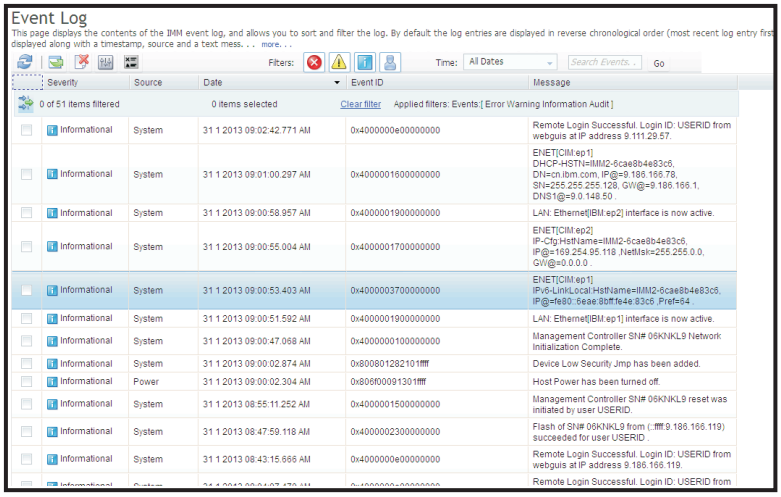
Managing the event log

Click the **Event Log** option to display the Event Log window. The Event Log window includes a description of the events that are reported by the IMM2 and 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 generate alerts, if they are configured to do so on the Event Recipients window. You can also sort and filter events in the event log. The capacity of the IMM2 logs can hold approximately 1024 event records and 1024 audit records. The actual number of records is dependent on the size of the each log's record content.

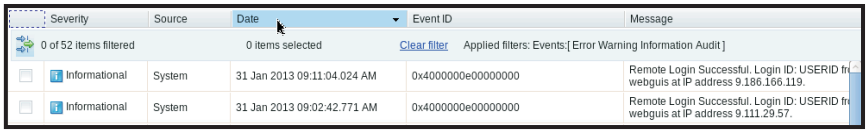
Click the **Event Log** option. The following window opens.



After selection of the Event Log option, the following window opens.



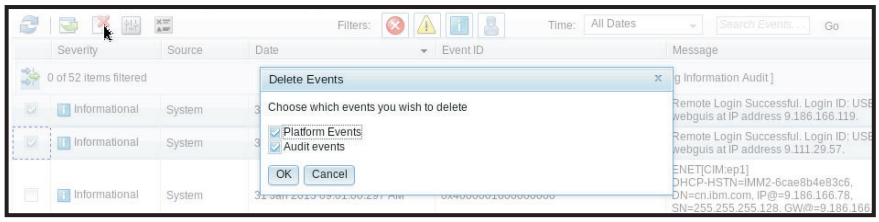
To sort and filter events in the event log, select the column heading (as shown in the following illustration).



You can save all or save selected events in the event log to a file using the **Export** button. To select specific events, choose one or more events on the main Event Log page and left-click on the **Export** button (as shown in the following illustration).

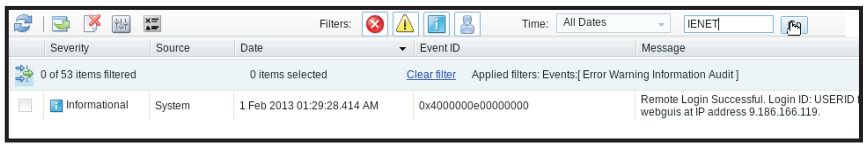
To choose which type of events you want to delete, click **Delete Events**. You must select the category of events you wish to delete.

The following illustration shows the Delete Events window.



To select the type of event log entries that you want to display, click the appropriate button (as shown in the following illustration).

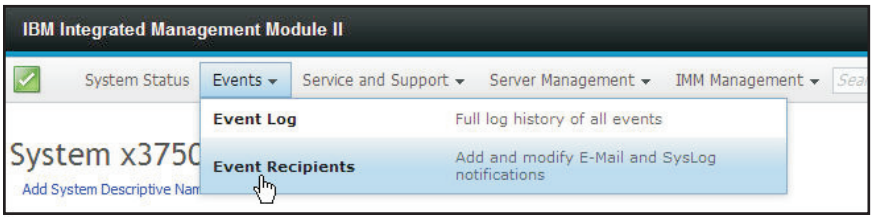
To search for specific types of events or keywords, type the type of event or keyword in the **Search Events** field and click **Go** (as shown in the following illustration).



Notification of system events

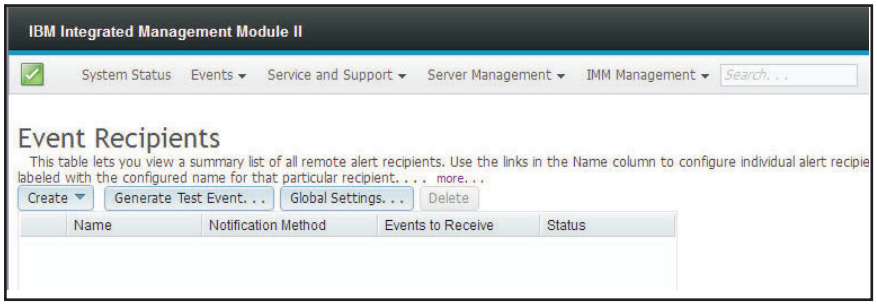
Select the **Event Recipients** option to add and modify email and syslog notifications.

The following illustration shows selection of the Event Recipients option.

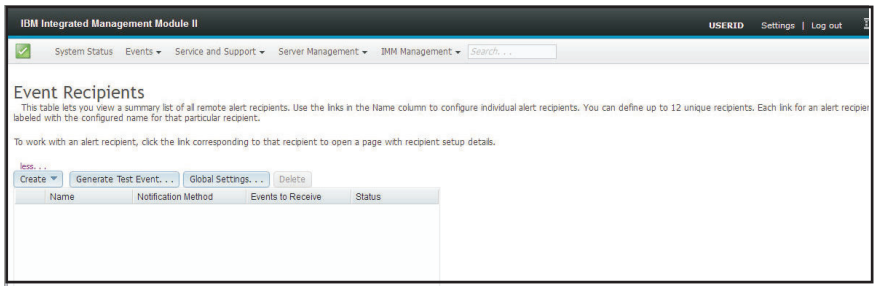


The Event Recipients option enables you to manage who will be notified of system events. You can configure each recipient and manage settings that apply to all Event Recipients. You can also generate a test event to verify notification feature operation.

The following illustration shows the Event Recipients page.



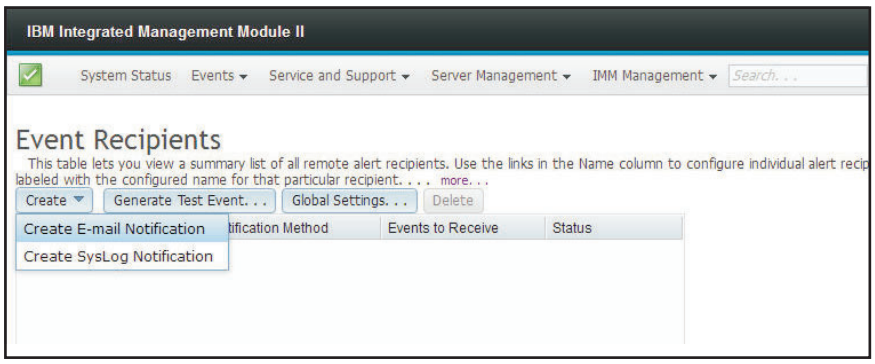
The following illustration shows additional information that is displayed when you click the **more** link on the Event Recipients page.



Creating email and syslog notifications

Select the **Create** tab to create email and syslog notifications.

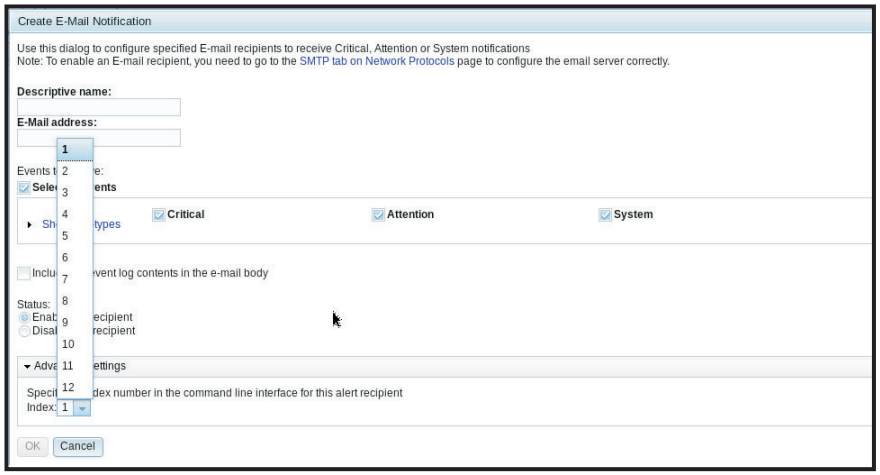
The following illustration shows the options available in the Create menu.



In the **Create E-mail Notification** option you can setup a target email address and choose the types of events for which you want to be notified. In addition you can click **Advanced Settings** to select the starting index number. To include the event log in the email, select the **Include the event log contents in the e-mail body** check box.

The following illustration shows the Create E-mail Notification screen.

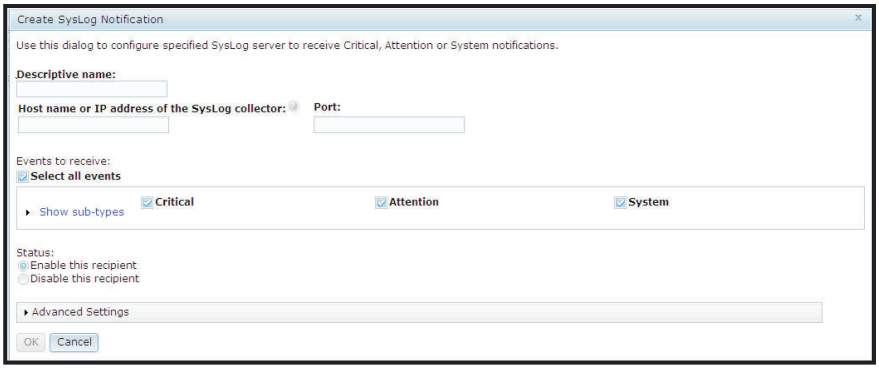
The following illustration shows the selections in the Advance Settings pane.



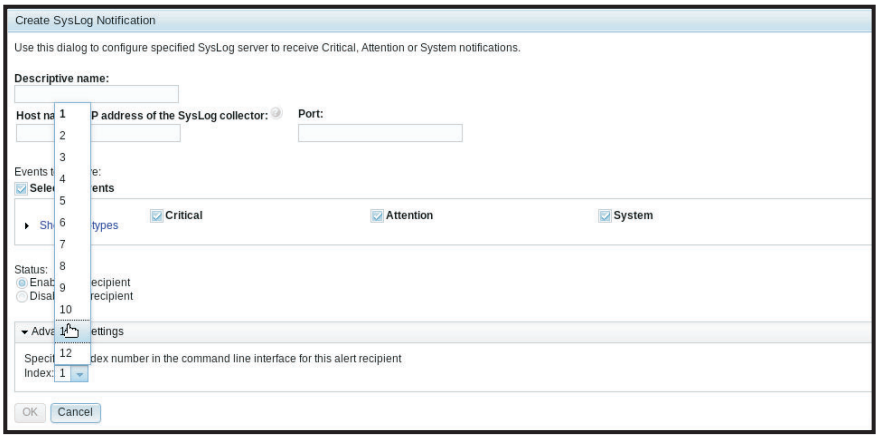
In the **Create Syslog Notification** option you can setup the host name and IP address of the syslog collector and choose the types of events for which you want

to be notified. You can click **Advanced Settings** to select the starting index number. You can also specify the port you want to use for this type of notification.

The following illustration shows the Create Syslog Notification screen.



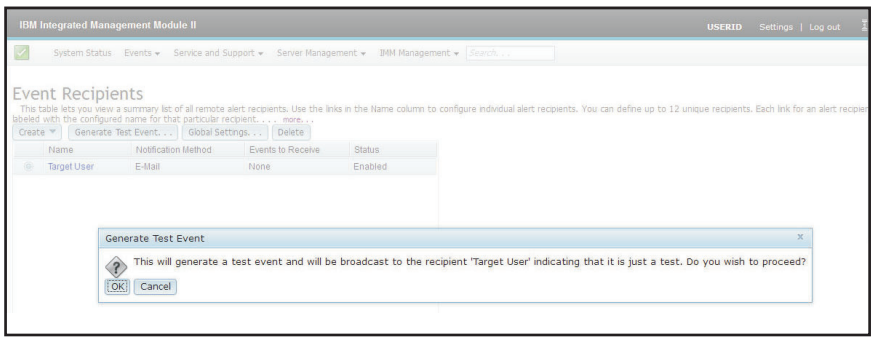
The following illustration shows the selections in the Advance Settings pane.



Generating test events

Use the **Generate Test Event...** tab to send a test email to a selected email target. After selection of the event notification, click **OK** to generate the test event. The test event is sent to the recipient with notification that this is a test.

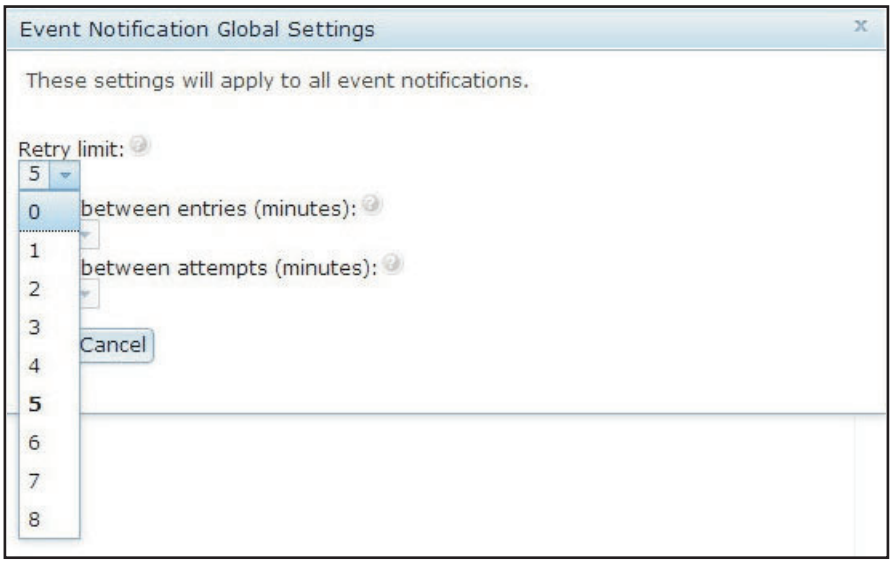
The following illustration shows the Generate Test Event window.



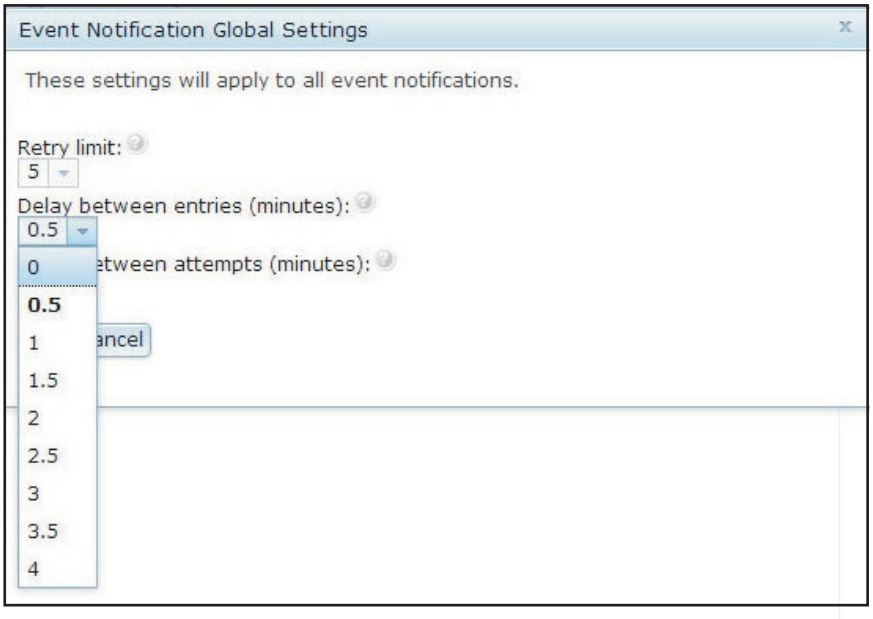
Setting limits to retry notifications

Use the **Global Settings...** tab to set a limit in which to retry the event notification, retry the delay between event notification entries (in minutes), and retry the delay between attempts (in minutes).

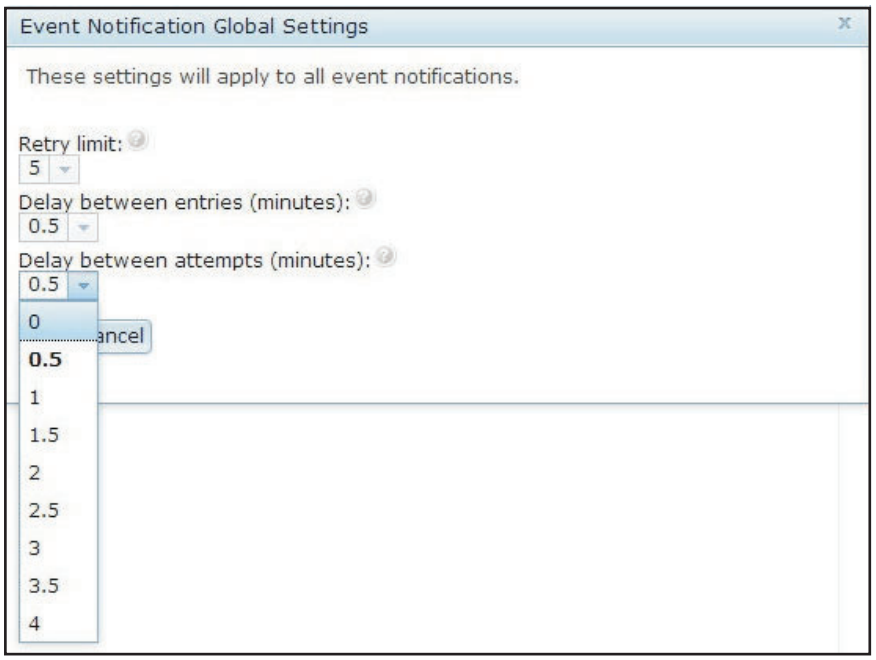
The following illustration shows the settings for the Retry limit option.



The following illustration shows the settings for the Delay between entries (minutes) option.



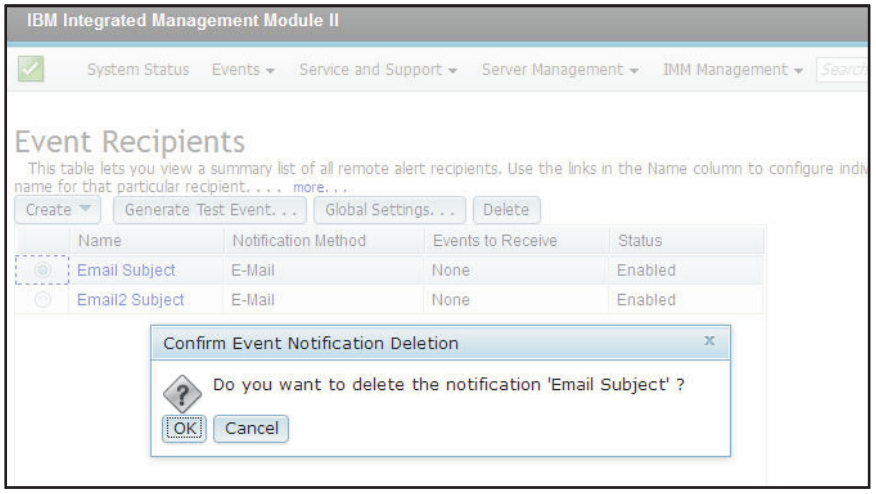
The following illustration shows the settings for the Delay between attempts (minutes) option.



Deleting email or syslog notifications

Use the **Delete** tab to remove an email or syslog notification target.

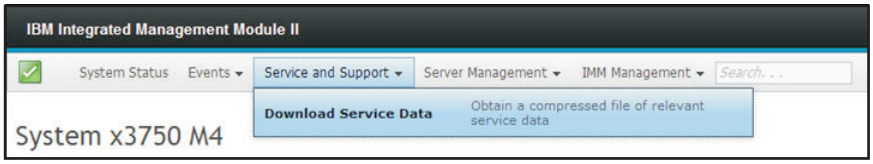
The following illustration shows the Confirm Event Notification Deletion window.



Collecting service and support information

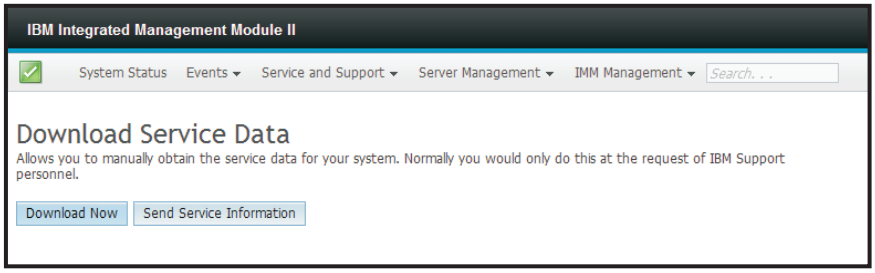
Click the **Download Service Data** option under the Service and Support menu to collect information about the server that can be used by IBM Support to assist you with your problem.

The following illustration shows the Service and Support menu.



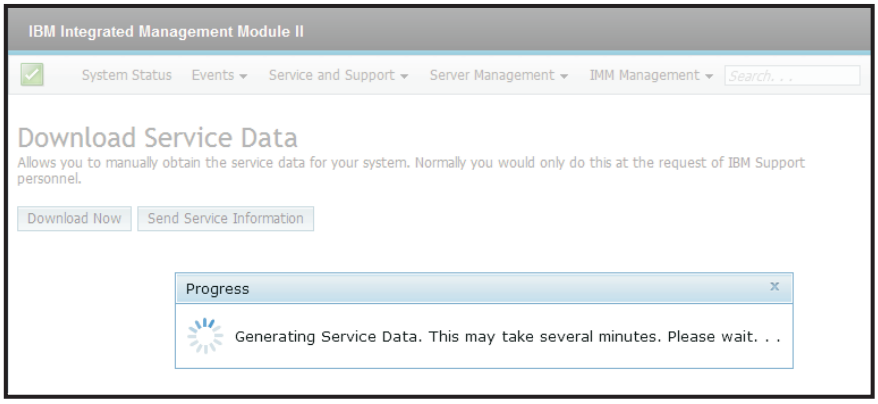
Click the **Download Now** button if you want to download the service and support data.

The following illustration shows the Download Service Data window.

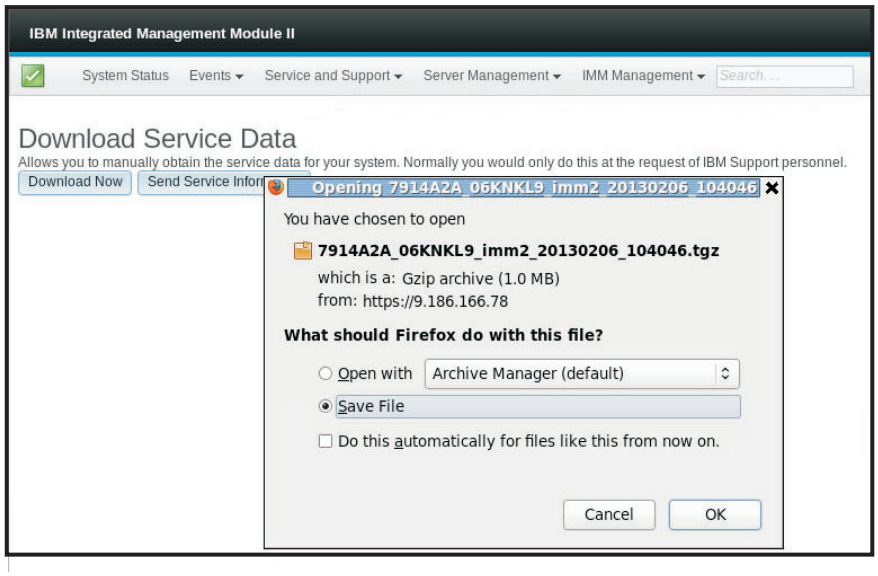


The process of collecting the service and support data starts. This process takes a few minutes to generate the service data that you can save to a file.

You will see the following Progress window while the Service data is being generated.



When the process is complete, you will be prompted to enter the location in which to save the file. Refer to the following illustration for an example.



Capturing the latest OS failure screen data

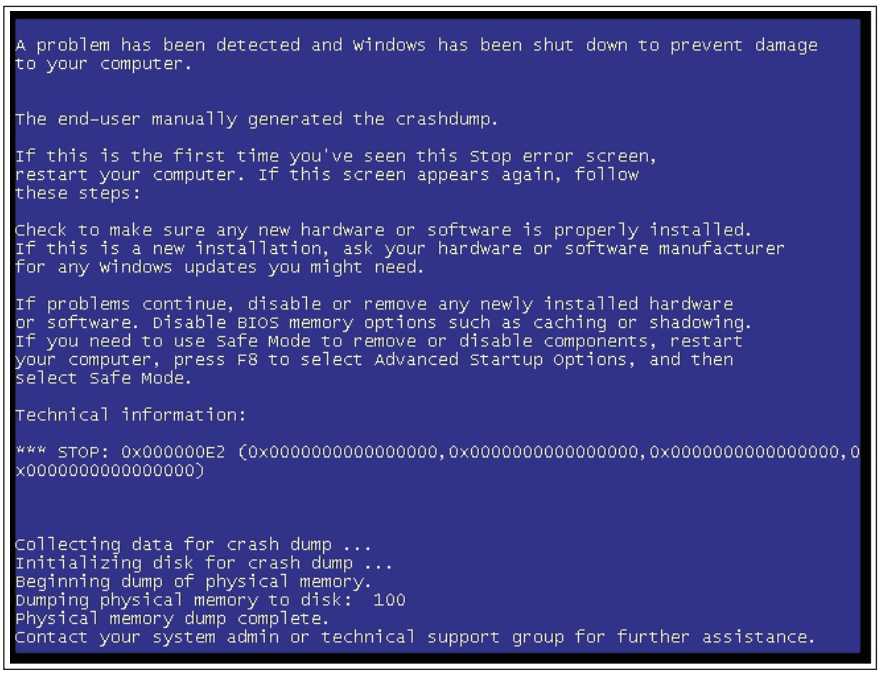
Use the Latest OS Failure Screen option to capture the operating system failure screen data and store the data. The IMM2 stores only the most recent error event information, overwriting earlier OS failure screen data when a new error event occurs. The OS Watchdog feature must be enabled to capture the OS failure screen. If an event occurs that causes the OS to stop running, the OS Watchdog feature is triggered The OS failure screen capture is available only with the IMM2 Advance Level functionality. See the documentation for your server for information about the level of IMM2 that is installed in your server.

To remotely display a OS Failure Screen image, select one of the following menu choices:

- **Latest OS Failure Screen** from the Server Management tab
- **Latest OS Failure Screen** tab on the System Status page

Note: If an OS Failure Screen has not been captured, the Latest OS Failure Screen tab on the System Status page will be grayed out and cannot be selected.

The following illustration shows the OS Failure Screen.

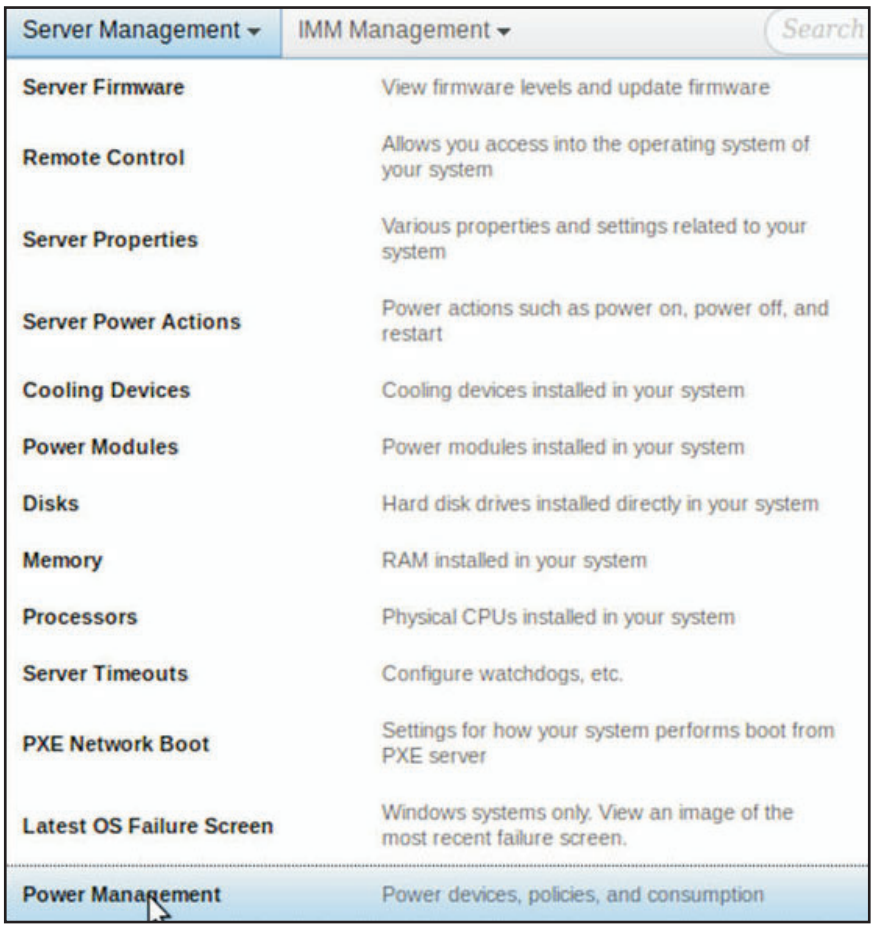


Managing the server power

Use the Power Management tab to perform the following tasks:

- Display information about installed power supplies.
- Control how the power supply "power" is managed.
- Control total system power.
- Display information about installed power supplies and current power supply capacity.
- Display the history of the amount of power used.

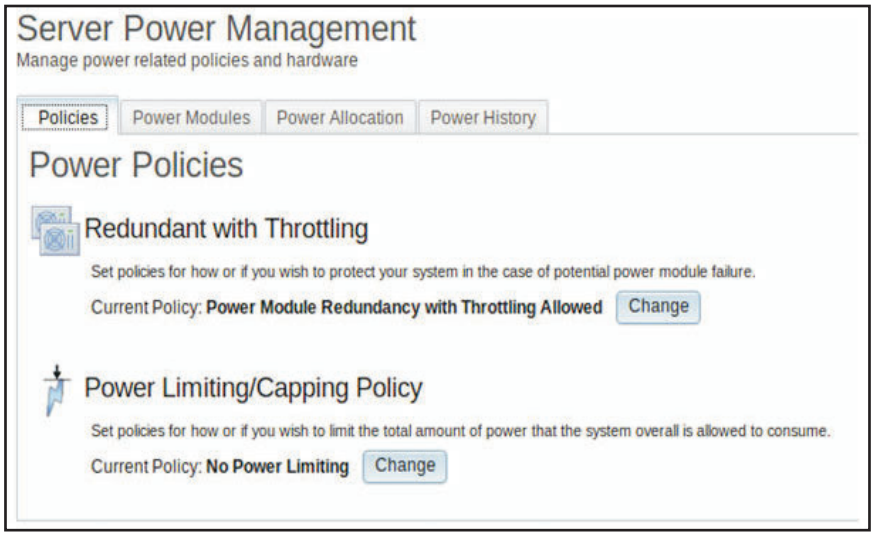
Select the **Power Management** option under the Server Management tab to view power management information and perform power management functions (as shown in the following illustration).



Controlling the power supply and total system power

Click the **Policies** tab to control how the power supply is managed and optionally control total system power with the Active Energy Manager by setting a capping policy (as shown in the following illustration).

Note: The **Policies** tab is not available in an IBM Flex System.



To select the policy you want to use to protect your server in the case of a potential power module failure, click the Current Policy **Change** button for the Redundant with Throttling option on the Power Policies window.

Note: By choosing a power policy you can trade off between redundancy and available power.

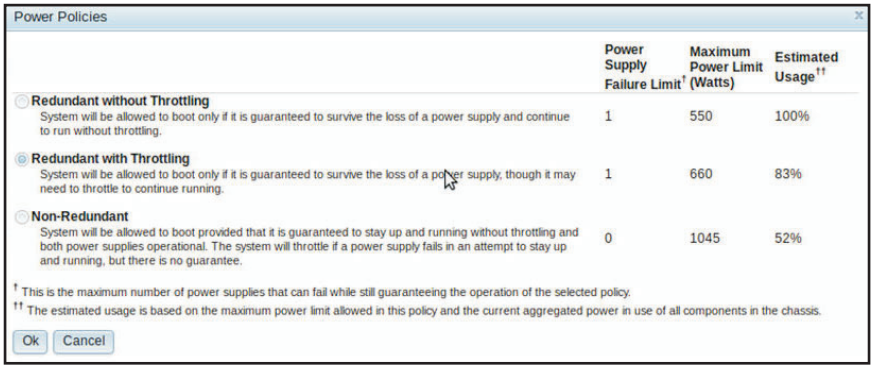
The power policy selections are as follows:

Redundant without Throttling
The server is allowed to boot if the server is guaranteed to survive the loss of a power supply and continue to run without throttling.

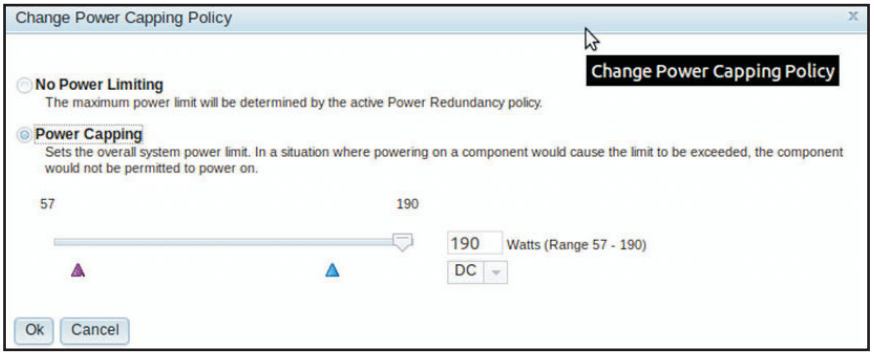
Redundant with Throttling
The server is allowed to boot if the server is guaranteed to survive the loss of a power supply, though the server may need to throttle to continue running.

Non-Redundant
The server is allowed to boot provided the server is guaranteed to continue running without throttling and both power supplies are operational. The server will throttle if a power supply fails in an attempt to remain running; but, there is no guarantee.

The following window opens when you select the **Change** button for the Redundant with Throttling option.



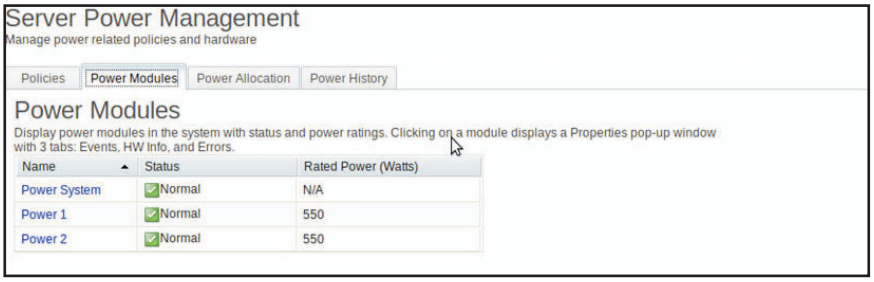
With Active Energy Manager you can limit the total amount of power that the server is allowed to use. To set a limit for server power usage, click the Current Policy **Change** button for the Power Limiting/Capping Policy option on the Power Policies window. The Change Power Capping Policy window opens (as shown in the following illustration).



Select the **Power Capping** button and move the slider mark to the desired wattage. The arrow on the right under the slider mark indicates the minimum setting that the Active Energy Manager can guarantee. The arrow on the left under the slider mark indicates the maximum system power usage over the past 24 hours. The two arrows provide guidance in setting a power cap limit.

Displaying currently installed power supplies

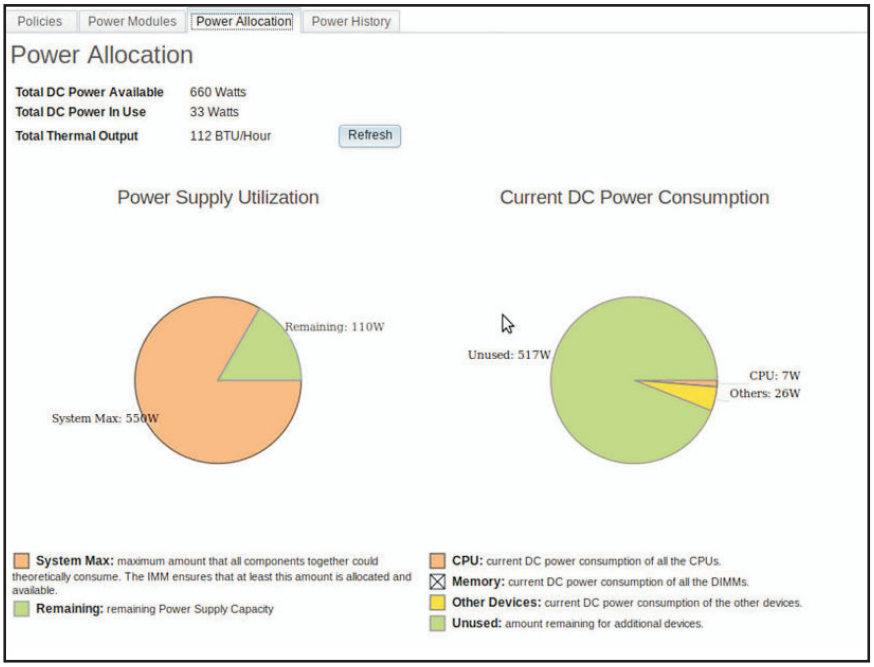
Click the **Power Modules** tab to display information about currently installed power supplies (as shown in the following illustration).



The name of each power module in the server is displayed along with the status and power rating of each power module. To display additional information for a power module, click on the name of a power module. A Properties window opens that contains three tabs: Events, HW Info and Errors for that specific power module.

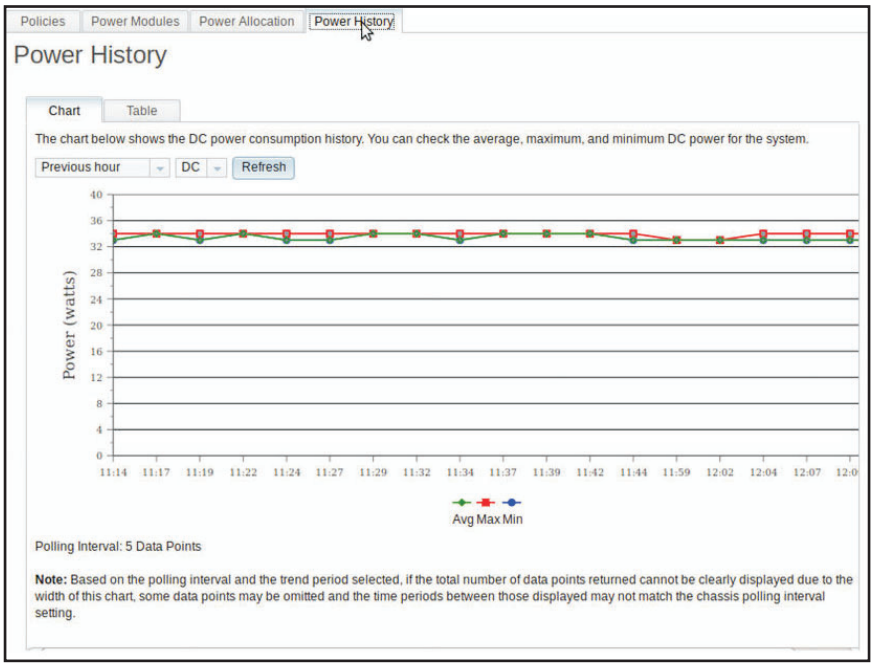
Displaying power supply capacity

Click the **Power Allocation** tab to display how much power supply capacity is being used and to display the current dc power consumption of the server (as shown in the following illustration).



Displaying the power history

Click the **Power History** tab to display how much power is being used by the system for a selected time period. From the **Chart** tab on the Power History page, you can select the time period and you also have the option to view ac or dc power. The average, minimum and maximum power usage is displayed (as shown in the following illustration).



Chapter 7. 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/.

Note: On servers with the IMM2 Basic level functionality, the IBM Integrated Management Module Standard Upgrade is required prior to installing the IBM Integrated Management Module Advanced Upgrade functionality.

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 command-line interface (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.

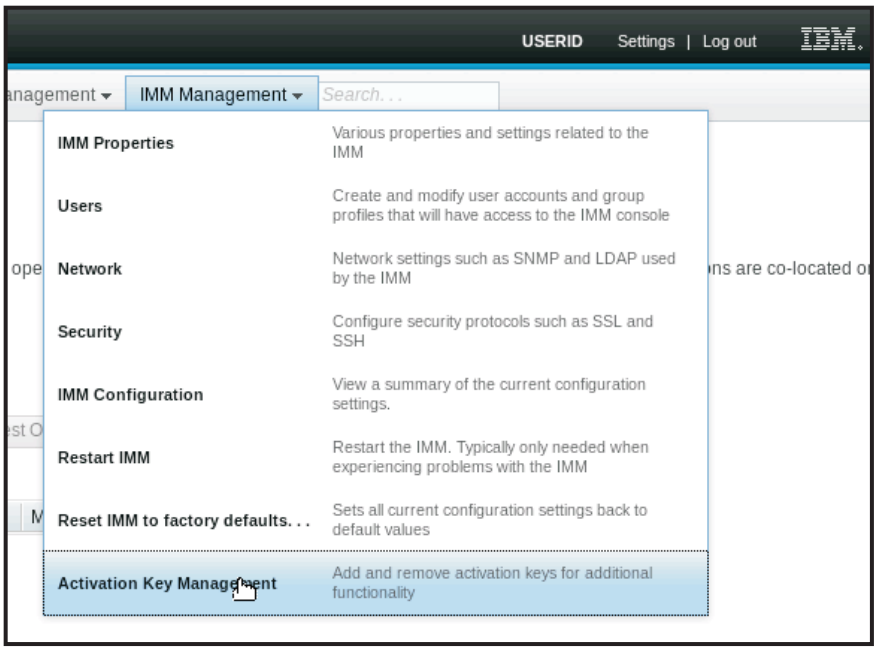
See "Installing an activation key," "Removing an activation key" on page 148 or "Exporting an activation key" on page 149 for information about managing an FoD activation key using the IMM2 web interface. See "keycfg command" on page 181 for information about managing an FoD activation key using the IMM2 CLI.

Installing an activation key

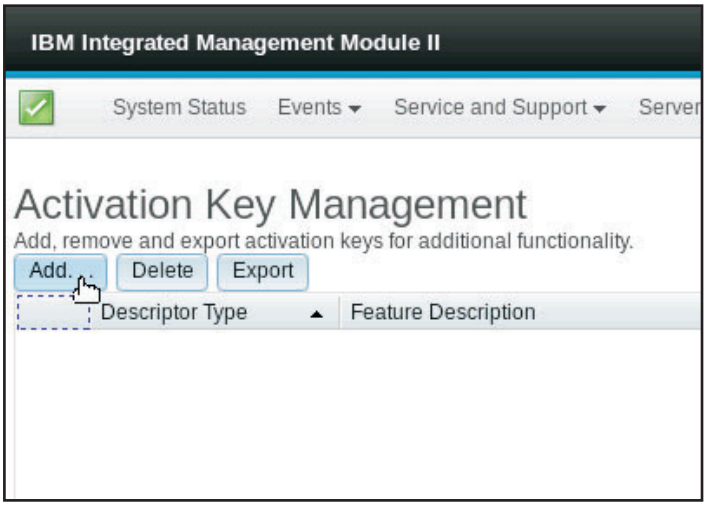
Install a FoD activation key to add an optional feature to your server.

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

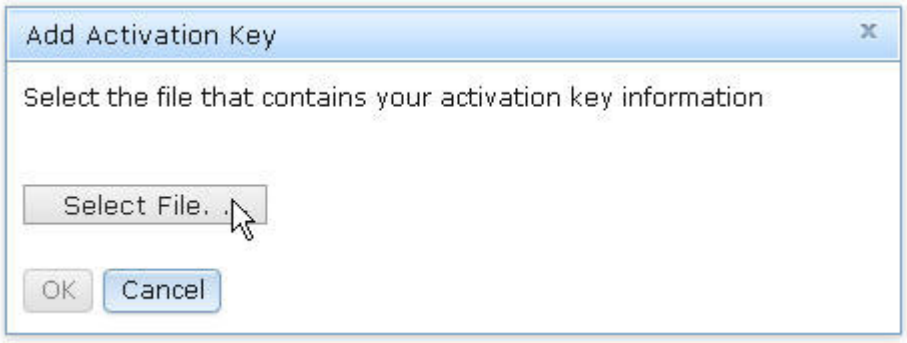
1. Log in to the IMM2. For more information, see "Logging in to the IMM2" on page 10.
2. From the IMM2 web interface, click on the **IMM Management** tab; then, click **Activation Key Management**.



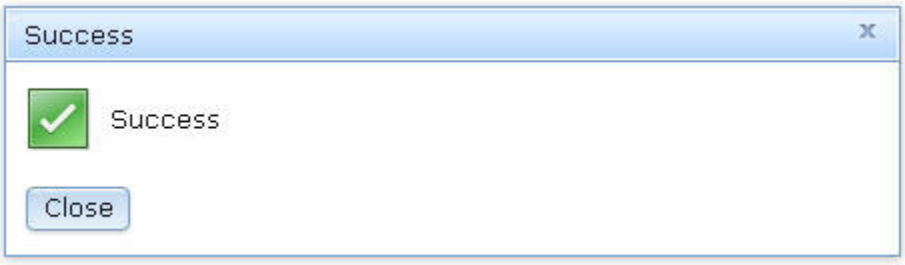
3. From the Activation Key Management page, click **Add...**.



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.



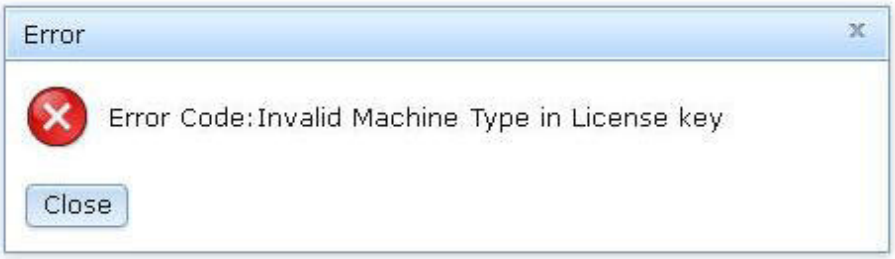
The Success window indicates that the activation key is installed.



Note:

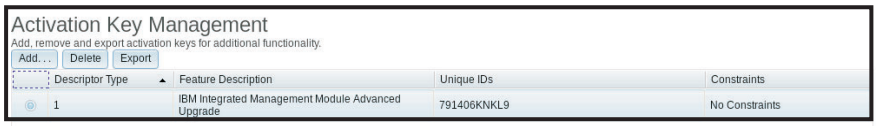
- If the activation key is not valid, you will see the following error window.

- 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.

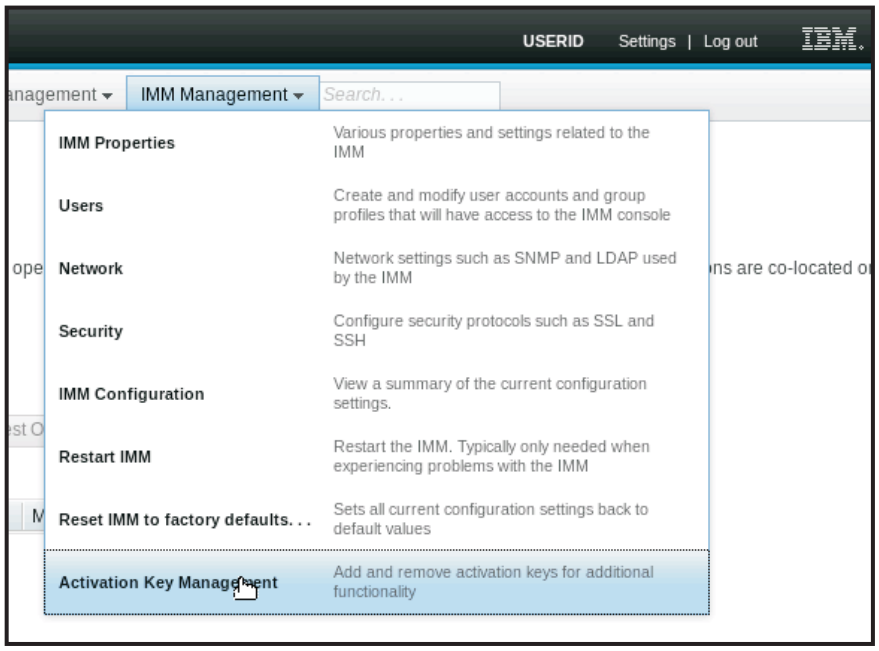


Removing an activation key

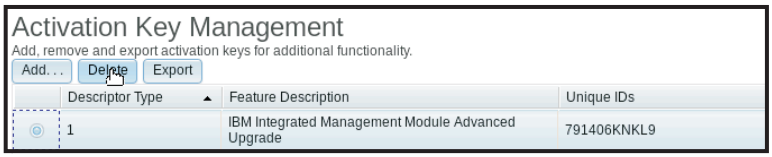
Remove a FoD activation key to delete an optional feature from your server.

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

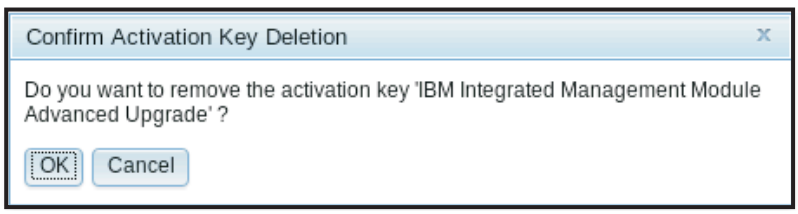
1. Log in to the IMM2. For more information, see "Logging in to the IMM2" on page 10.
2. From the IMM2 web interface, click on the **IMM Management** tab; then, click on **Activation Key Management**.



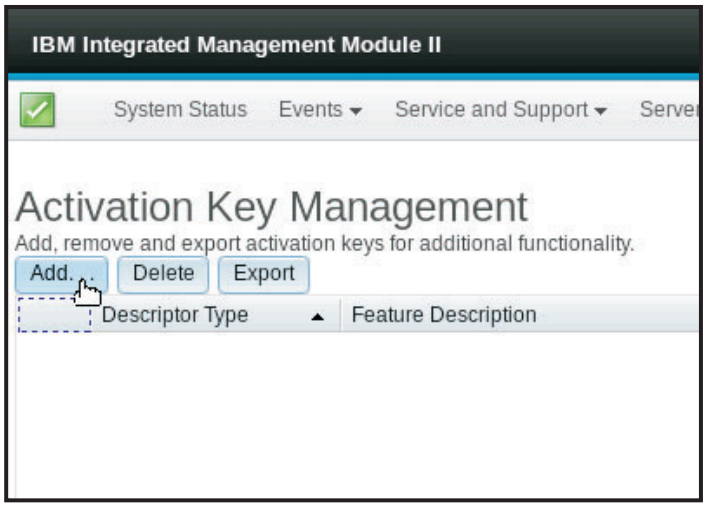
3. From the Activation Key Management page, select the activation key to remove; then, click **Delete**.



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.

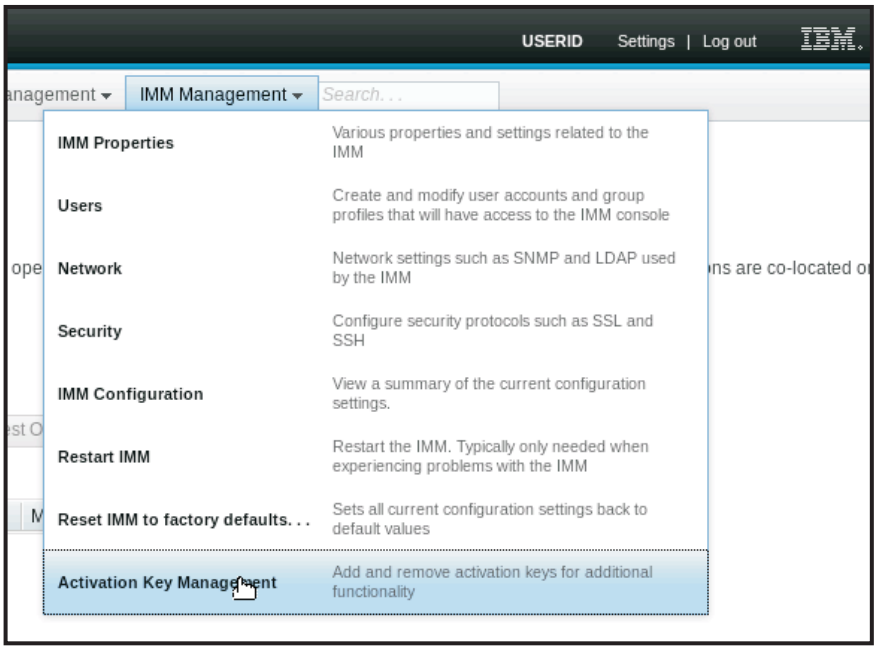


Exporting an activation key

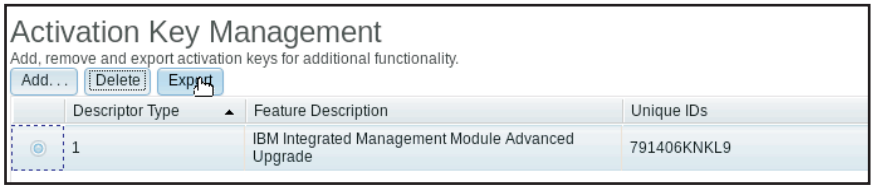
Export a FoD activation key to export an optional feature from your server.

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

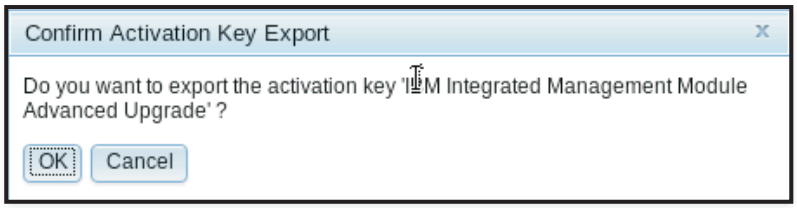
1. Log in to the IMM2. For more information, see "Logging in to the IMM2" on page 10.
2. From the IMM2 web interface, click on the **IMM Management** tab; then, click on **Activation Key Management**.



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



4. In the Confirm Activation Key Export window, click **OK** to confirm activation key exporting or click **Cancel** to cancel the key exporting request.



5. Select the directory to save the file. The selected activation key is exported from the server.

Chapter 8. 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.

In an IBM Flex System, a user can configured the IBM Flex System Chassis Management Module (CMM) to centrally manage the IMM2 Intelligent Platform Management Interface (IPMI) user accounts. In this circumstance you might not be able to access the IMM2 using IPMI until the CMM has configured the IPMI User IDs. The User ID credentials configured by the CMM might be different than the USERID/PASSW0RD combination described above.

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

Command-line interfaces
The CLI 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 CLI, start a Telnet or SSH session to the IMM2 IP address (see "Configuring serial-to-Telnet or SSH redirection" on page 152 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. 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 CLI **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 CLI. 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:

```
system > history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system > !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
system >
```

- In the CLI, 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> ?
```

- In an IBM Flex System, some settings are managed by the CMM and cannot be modified on the IMM2.

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 CLI 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

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>
```

ffdc command

Use the **ffdc** (first failure data capture) command to generate and transfer service data to IBM Support.

The following list consist of commands to be used with the **ffdc** command:

- **generate**, create a new service data file
- **status**, check status of service data file
- **copy**, copy existing service data
- **delete**, delete existing service data

The following table shows the arguments for the options.

Option	Description	Values
-t	Type number	1 (processor dump) and 4 (service data). The default value is 1.
-f [1]	Remote filename or sftp target directory.	For sftp, use full path or trailing / on directory name (~/ or /tmp/). The default value is the system generated name.
--ip [1]	Address of the tftp/sftp server	
-pn [1]	Port number of the tftp/sftp server	The default value is 69/22.
-u [1]	Username for the sftp server	
-pw [1]	Password for the sftp server	
1. Additional argurment for **generate** and **copy** commands		

Syntax:

```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Example:

```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
```

```
8737AC1_DSY0123_imm2_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_imm2_120926-105320.tgz
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>
```

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
```

Use the vpd command to display vital product data for different parts of the server.

Option	Description
-sys	Displays vital product data for the system
-imm	Displays vital product data for the IMM2 controller
-uefi	Displays vital product data for the BIOS
-dsa	Displays vital product data for the Diag
-fw	Displays vital product data for the system firmware
-comp	Displays vital product data for the system components

Example:

```
system> vpd -dsa
Type     Version      Build     ReleaseDate
----     -------      -----     ------
DSA      9,25         DSYTA5A   2012/07/31
system>
```

Server power and restart control commands

The server power and restart commands are as follows:

- "fuelg command"
- "power command" on page 163
- "pxeboot command" on page 166
- "reset command" on page 166

fuelg command

Use the **fuelg** command to display and configure server power management.

Use the **fuelg** command to display information about server power usage and configure server power management. This command also configures policies for power redundancy loss. The following table shows the arguments for the options.

Option	Description	Values
-pme	Enable or disable power management and capping on the server	on, off

Option	Description	Values
-pcapmode	Set the power capping mode for the server	ac, dc
-pcap	A numeric value that falls within the range of power capping values displayed when running the fuelg command, with no options, on the target.	numeric wattage value
If power supply redundancy is not supported the following option is supported:		
-pm	Set the policy mode for loss of redundant power	basic with throttling (default), redundant without throttling, redundant with throttling
If power supply redundancy is supported the following options are supported:		
-mpc	Set the maximum power consumption budget for the server	current configuration, all hot-plug components
-at	Allow throttling to keep the server within the power budget	on, off
-r	Allow power redundancy for the server	on, off
-nn	Value of N+N redundancy configuration	redundancy configuration value

Syntax:

```
fuelg [options]
option:
  -pme on|off
  -pcapmode dc|ac
  -pcap
  -pm bt|r|rt
  -mpc cc|ahp
  -at on|off
  -r on|off
  -nn
```

Example:

```
system> fuelg
-pme: on
system>
```

power command

Use the **power** command to control the server power. To issue **power** commands, you must have the Remote Server Power/Restart Access authority level.

The following table contains a subset of commands that can be used with the **power** command.

Table 7. Power commands

Command	Description	Value
power on	Use this command to turn on the server power.	on, off

Table 7. Power commands (continued)

Command	Description	Value
power off	Use this command to turn off the server power. **Note:** The **-s** option shuts down the operating system before the server is turned off.	on, off
power cycle	Use this command to turn off the server power and then turn on the server power. **Note:** The **-s** option shuts down the operating system before the server is turned off.	
power enterS3	Use this command to place the operating system into the S3 (sleep) mode. **Note:** This command is used only when the operating system is on. The S3 mode is not supported on all servers.	
power S3resume	Use this command to wake up the operating system from the S3 (sleep) mode. **Note:** This command is used only when the operating system is on. The S3 mode is not supported on all servers.	
power state	Use this command to display the server power state and the current state of the server.	on, off

The following table contains the options for the **power on**, **power off**, and **power cycle** commands.

Option	Description	Values
-s	Use this option to shut down the operating system before the server is turned off. **Note:** The **-s** option is implied when using the **-every** option for the **power off** and **power cycle** commands.	

Option	Description	Values
-every	Use this option with the **power on**, **power off**, and **power cycle** commands to control the server power. You can set up the dates, times, and frequency (daily or weekly) to power on, power off, or power cycle your server.	**Note:** The values for this option are presented on separate lines due to space limitations. Sun | Mon | Tue | Wed | Thu | Fri | Sat | Day | clear
-t	Use this option to specify the time in hours and minutes to power on the server, shut down the operating system, and power off or restart the server.	Use the following format: hh:mm
-rp	Use this option to specify the host power restore policy.	alwayson | alwaysoff | restore
-d	Use this option to specify the date to power on the sever. This is an additional option for the **power on** command. **Note:** The **-d** and **-every** options, cannot be used together on the same command.	Use the following format: mm/dd/yyyy
-clear	Use this option to clear the scheduled power on date. This is an additional option for the **power on** command.	

Syntax:

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

The following information are examples of the **power** command.

To shut down the operating system and power off the server every Sunday at 1:30, enter the following command:

```
power off -every Sun -t 01:30
```

To shut down the operating system and restart the server every day at 1:30, enter the following command:

```
power cycle -every Day -t 01:30
```

To power on the server every Monday at 1:30, enter the following command:

```
power on -every Mon -t 13:00
```

To power on the server on Dec 31 2013 at 11:30 PM, enter the following command:

```
power on -d 12/31/2013 -t 23:30
```

To clear a weekly power cycle, enter the following command:

```
power cycle -every clear
```

pxeboot command

Use the **pxeboot** command to display and set the 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 the Preboot eXecution Environment condition for the 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
-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> accseccfg
-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 IMM2 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 IMM2 resends an alert	0 to 4.0 minutes, in 0.5 minute increments
-da	Sets wait time before the IMM2 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 IMM2 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>
```

asu command

Advanced Settings Utility commands are used to set UEFI settings. The host system must be rebooted for any UEFI setting changes to take effect.

The following table contains a subset of commands that can be used with the **asu** command.

Table 8. ASU commands

Command	Description	Value
delete	Use this command to delete an instance or record of a setting. The setting must be an instance that allows deletion, for example, iSCSI.AttemptName.1.	*setting_instance*
help	Use this command to display help information for one or more settings.	*setting*
set	Use this command to change the value of a setting. Set the UEFI setting to the input value. **Notes:** • Set one or more setting/value pairs. • The setting can contain wildcards if it expands to a single setting. • The value must be enclosed in quotes if it contains spaces. • Ordered list values are separated by the equal symbol (=). For example, set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."	*setting value*
showgroups	Use this command to display the available setting groups. This command displays the names of known groups. Group names may vary depending on the installed devices.	*setting*
show	Use this command to display the current value of one or more settings.	*setting*

Table 8. ASU commands (continued)

Command	Description	Value
showvalues	Use this command to display all possible values for one or more settings. **Notes:** • This command will display information about the allowable values for the setting. • The minimum and maximum number of instances allowed for the setting is displayed. • The default value will be displayed if available. • The default value is enclosed with opening and closing angle brackets (< and >). • Text values show the minimum and maximum length and regular expression.	*setting*
Notes: • In the command syntax, *setting* is the name of a setting that you want to view or change, and *value* is the value that you are placing on the setting. • *Setting* can be more than one name, except when using the **set** command. • *Setting* can contain wildcards, for example an asterisk (*) or a question mark (?). • *Setting* can be a group, a setting name, or **all**.		

Examples of the syntax for the **asu** command are presented in the following list:

- To display all of the asu command options enter `asu --help`.
- To display verbose help for all commands enter `asu -v --help`.
- To display verbose help for one command enter `asu -v set --help`.
- To change a value enter `asu set setting value`.
- To display the current value enter `asu show setting`.
- To display settings in long batch format enter `asu show -l -b all`
- To display all possible values for a setting enter `asu showvalues setting`.

  Example **show values** command:

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```

The following table shows the arguments for the options.

Option	Description	Values
-b[1]	Display in batch format.	

Option	Description	Values
--help[3]	Display command usage and options. The --help option is placed before the command, for example **asu --help show**.	
--help[3]	Display help for the command. The --help option is placed after the command, for example, **asu show --help**.	
-l[1]	Long format setting name (include the configuration set).	
-m[1]	Mixed format setting name (use the configuration id).	
-v[2]	Verbose output.	
1. The -v option is used only between **asu** and the command. 2. The --help option can be used with any command.		

Syntax:

```
asu [options] command [cmdopts]
options:
   -v verbose output
   --help display main help
cmdopts:
   --help help for the command
```

Note: See individual commands for more command options.

Use the asu transaction commands to set multiple UEFI settings and create and execute batch mode commands. Use the **tropen** and **trset** commands to create a transaction file containing multiple settings to be applied. A transaction with a given id is opened using the **tropen** command. Settings are added to the set using the **trset** command. The completed transaction is committed using the **trcommit** command. When you are finished with the transaction, it can be deleted with the **trrm** command.

Note: The UEFI settings restore operation will create a transaction with an id using a random three digit number.

The following table contains transaction commands that can be used with the **asu** command.

Table 9. Transaction commands

Command	Description	Value
tropen *id*	This command creates a new transaction file containing several settings to be set.	*Id* is the identifying string, 1 - 3 alphanumeric characters.
trset *id*	This command adds one or more settings or value pairs to a transaction.	*Id* is the identifying string, 1 - 3 alphanumeric characters.

Table 9. Transaction commands (continued)

Command	Description	Value
trlist *id*	This command displays the contents of the transaction file first. This can be useful when the transaction file is created in the CLI shell.	*Id* is the identifying string, 1 - 3 alphanumeric characters.
trcommit *id*	This command commits and executes the contents of the transaction file. The results of the execution and any errors will be displayed.	*Id* is the identifying string, 1 - 3 alphanumeric characters.
trrm *id*	This command removes the transaction file after it has been committed.	*Id* is the identifying string, 1 - 3 alphanumeric characters.

Example of establishing multiple UEFI settings:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

autopromo command

Use the **autopromo** command to display and configure the setting for the automated promotion of IMM2 backup firmware. If enabled, the Automated Promotion feature automatically copies the IMM2 firmware from the primary area into the backup area once the firmware in the primary area has run successfully for a period of time.

Running the **autopromo** command with no options displays automated promotion parameters and status information. The following table shows the arguments for the option.

Option	Description	Values
-en	Enable or disable the automated promotion of the IMM2 backup firmware.	enabled, disabled

Syntax:

```
autopromo [options]
  options:
   -en enabled/disabled
```

Example:

```
system>autopromo -en enabled
ok
system>autopromo
-en: enabled
Status:  Not Synced
Primary bank version: 4.00
Backup bank version:  2.60
```

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
-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>
```

cryptomode command

Use the **cryptomode** command to display and configure the compliance mode with the exceptions for encryption. The following table shows the arguments for the options.

Option	Description	Values
-set	Select the compliance mode	basic, NIST
-esnmpv3	Allow or disallow SNMPv3 accounts to operate in a non-compliant manner with the NIST compliance mode	enable, disable

Option	Description	Values
-h	List the usage and options	

Syntax:

```
cryptomode [options]
  options:
   -set basic|nist
   -esnmpv3 enabled|disabled
   -h usage_options
```

Example:

```
system> cryptomode
Basic Compatibility
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
-s	Assigned subnet mask
-d	Assigned domain name
-dns1	Primary IPv4 DNS server IP address
-dns2	Secondary IPv4 DNS IP address

Option	Description
-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.

Note: In an IBM Flex System, DNS settings cannot be modified on the IMM2. DNS settings are managed by the CMM.

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>
```

gprofile command

Use the **gprofile** command to display and configure group profiles for the IMM2.

The following table shows the arguments for the options.

Option	Description	Values
-clear	Deletes a group	enabled, disabled
-n	The name of the group	String of up to 63 characters for *group_name*. The *group_name* must be unique.
-a	Role-based authority level	supervisor, operator, rbs <role list>: nsc | am | rca | rcvma | pr | bc | cel | ac Role list values are specified using a pipe separated list of values.
-h	Displays the command usage and options	

Syntax:

```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
```

```
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

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.
-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

Option	Description	Values
-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 value 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	enabled, disabled
-sa6	IPv6 stateless autoconfig state	enabled, disabled
-vlan	Enable or disable the VLAN tagging	enabled, disabled
-vlanid	Network packet identification tag for the IMM2	Numeric value between 1 and 4094

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
  -vlan state
  -vlanid VLAN ID
```

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.
-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
-aom	Authentication only mode	enabled, disabled
-b	Binding method	anonymous, bind with ClientDN and password, bind with Login Credential
-c	Client distinguished name	String of up to 127 characters for *client_dn*
-d	Search domain	String of up to 63 characters for *search_domain*
-f	Group filter	String of up to 127 characters for *group_filter*
-fn	Forest name	For active directory environments. String of up to 127 characters.
-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*
-p	Client password	String of up to 15 characters for *client_pw*
-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. The command will fail if the arguments do not match.
-r	Root entry distinguished name (DN)	String of up to 127 characters for *root_dn*
-rbs	Enhanced Role-Based Security for active directory users	enabled, disabled
-s1ip	Server 1 host name/IP address	String up to 127 characters or an IP address for *host name/ip_addr*
-s2ip	Server 2 host name/IP address	String up to 127 characters or an IP address for *host name/ip_addr*

Option	Description	Values
-s3ip	Server 3 host name/IP address	String up to 127 characters or an IP address for *host name/ip_addr*
-s4ip	Server 4 host name/IP address	String up to 127 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*
-t	Server target name	When the –rbs option is enabled, this field specifies a target name that can be associated with one or more roles on the Active Directory server through the Role-Based Security (RBS) Snap-In tool.
-u	UID search attribute	String of up to 63 characters for *search_attrib*
-v	Get LDAP server address through DNS	off, on
-h	Displays the command usage and options	

Syntax:

```
ldap [options]
options:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -r root_dn
   -rbs enable|disabled
   -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
   -t name
   -u search_attrib
   -v off/on
   -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[1]	Name or IP address of the Network Time Protocol server. This is the index number of the Network Time Protocol server.	The name of the NTP server to be used for clock synchronization. The range of the index number of the NTP server is from -i1 through -i4.
-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.
1. -i is the same as i1.		

Syntax:

```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-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 IMM2 ports.

Running the **ports** command with no options displays information for all IMM2 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 IMM2 for the serial redirection feature.

The IMM2 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 IMM2 for IPMI functionality. The CLI is not supported through the serial port. The **serred** and **cliauth** options that were present in the Remote Supervisor Adapter II CLI 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 CLI is disabled • 1 = cliems: The CLI is enabled with EMS-compatible keystroke sequences • 2 = cliuser: The CLI 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>
```

portcontrol command

Use the **portcontrol** command to turn a network service port on or off.

Currently this command only supports control of the port for the IPMI protocol. Type **portcontrol** to display the IPMI port state. To enable or disable the IPMI network port, type the **-ipmi** option followed by the **on** or **off** values.

Option	Description	Values
-ipmi	Enable or disable the ipmi-server 623 port	on, off
-h		

Syntax:

```
portcontrol [options]
 options:
   -ipmi on/off
   -h
```

Example:

```
system> portcontrol
-ipmi : on
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 IMM2 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 IMM2 settings.

- Some IMM2 settings can be changed with a simple **set** command.
- Some of these settings, such as environment variables, are used by the CLI.

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
-auth	SMTP authentication support	enabled, disabled
-authepw	SMTP authentication encrypted password	Valid password string
-authmd	SMTP authentication method	CRAM-MD5, LOGIN
-authn	SMTP authentication user name	String (limited to 256 characters)
-authpw	SMTP authentication password	String (limited to 256 characters)
-pn	SMTP port number	Valid port number.
-s	SMTP server IP address or hostname	Valid IP address or hostname (63 character limit)

Syntax:

```
smtp [options]
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -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: • IMM2 contact specified using the -cn command option. • IMM2 location specified using the -l command option. • At least one SNMP community name specified using one of the -c*x* command options. • At least one valid IP address is specified for each SNMP community using one of the -c*xiy* command options.

Option	Description	Values
-a3	SNMPv3 agent	on, off **Note:** To enable the SNMPv3 agent, the following criteria must be met: • IMM2 contact specified using the -cn command option. • IMM2 location specified using the -l command option.
-t	SNMP traps	on, off
-l	IMM2 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 IMM2 location by specifying no argument or by specifying an empty string as the argument, such as "".
-cn	IMM2 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 IMM2 contact name by specifying no argument or by specifying an empty string as the argument, such as "".
-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

Option	Description	Values
-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
-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 indicate the key sequence to enter the CLI from the serial redirection mode. 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 IMM2 hardware does not provide for a serial port to serial port pass-through capability. Therefore the `-passthru` and `entercliseq` options which are present in the Remote Supervisor Adapter II CLI 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 -entercliseq` command option.

Option	Description	Values
-entercliseq	Enter a CLI keystroke sequence	User-defined keystroke sequence to enter 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:
-entercliseq entercli_keyseq
```

Example:

```
system> srcfg
-entercliseq ^[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

Option	Description	Values
-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 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 CLI:

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 IMM2 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.

Option	Description	Values
-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.
-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). This option takes no arguments; but, must also specify values for 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 50 characters) **Note:** Required when generating a self-signed certificate or CSR.

Option	Description	Values
-on	Organization name	Quote-delimited string (maximum 60 characters) **Note:** Required when generating a self-signed certificate or CSR.
-hn	IMM2 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.
-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
 Trusted Certificate 4: Not available
system>
```

telnetcfg command

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

Running the **telnetcfg** command with no options displays the 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>
```

tls command

Use the **tls** command to set the minimum TLS level. The following table shows the arguments for the options.

Option	Description	Values
-min	Select the minimum TLS level	1.0, 1.1, or 1.2
-h	List the usage and options	

Syntax:

```
tls [options]
option:
  -min 1.0|1.1|1.2
```

Example:

```
system> tls
-min 1.0
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
-f	Power off delay	minutes	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-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
-o	Operating system timeout	minutes	disabled, 2.5, 3, 3.5, 4

Syntax:

```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-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. The **users** command is also used 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.
-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.

Option	Description	Values
-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
-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.

Option	Description	Values
-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`.
-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`.

Option	Description	Values
-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 or SFTP *(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>
```

IMM2 control commands

The IMM2 control commands are as follows:

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
-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 **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 to execute 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 IMM2.

Running the **info** command with no options displays all IMM2 location and contact information. The following table shows the arguments for the options.

Option	Description	Values
-name	IMM2 name	String
-contact	Name of IMM2 contact person	String
-location	IMM2 location	String
-room[1]	IMM2 room identifier	String
-rack[1]	IMM2 rack identifier	String
-rup[1]	Position of IMM2 in rack	String
-ruh	Rack unit height	Read only
-bbay	Blade bay location	Read only

1. Value is read only and cannot be reset if the IMM2 resides in an IBM Flex System.

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. You must have at least Advanced Adapter Configuration authority to be able to issue this command.

spreset command

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

Service advisor commands

The service advisor commands are as follows:

autoftp command

Use the **autoftp** command to display and configure the FTP/TFTP/SFTP server settings for the IMM2. The server will not send duplicate events if they are left unacknowledged in the activity log.

The following table shows the arguments for the options.

Option	Description	Values
-m	The automated problem reporting mode	ftp, sftp, tftp, disabled **Notes:** • For the **ftp** mode, all fields must be set. • For the **tftp** mode, only the **–i** and **–p** options are required.
-i	The FTP, SFTP, or TFTP server IP address or hostname for automated problem reporting	Valid IP address or hostname
-p	The FTP, SFTP, or TFTP transmission port for automated problem reporting	Valid port number (1 - 65535)
-u	The FTP, SFTP, or TFTP user name for automated problem reporting	Quote-delimited string up to 63 characters
-pw	FTP password for automated problem reporting	Quote-delimited string up to 63 characters

Syntax:

```
autoftp [options]
option:
  -m mode
  -i ip_address_or_hostname
  -p port_number
  -u user_name
  -pw password
```

chconfig command

Use the **chconfig** command to display and configure the Service Advisor settings.

Notes:

- The Service Advisor Terms and Conditions must be accepted, using the **chconfig -li** command option, before configuring any other parameters.
- All contact information fields, as well as the IBM Service Support Center field, are required before the IBM Support of Service Advisor can be enabled.
- All HTTP Proxy fields must be set, if an HTTP proxy is required.

The following table shows the arguments for the options.

Option	Description	Values
-li	View or accept the Service Advisor Terms and Conditions	view, accept
-sa	IBM Support status of the Service Advisor	enabled, disabled
-sc	Country code for the IBM Service Support Center	Two-character ISO country code
Service Advisor contact information options:		
-ce	Email address of primary contact person	Valid email address of the form `userid@hostname` (30 characters maximum)
-cn	Name of primary contact person	Quote-delimited string (30 characters maximum)
-co	Organization or company name of primary contact person	Quote-delimited string (30 characters maximum)
-cph	Phone number of primary contact person	Quote-delimited string (5 - 30 characters)
-cpx	Phone extension of primary contact person	Quote-delimited phone extension of the contact person (1 - 5 characters)
Alternate Service Advisor contact information options:		
-ae	Email address of alternate contact person	Valid email address of the form `userid@hostname` (30 characters maximum)
-an	Name of alternate contact person	Quote-delimited string (30 characters maximum)
-aph	Phone number of alternate contact person	Quote-delimited string (5 - 30 characters)
-apx	Phone extension of alternate contact person	Quote-delimited string (1 - 5 characters)
System location information option:		
-mp	Phone number for the machine location	Quote-delimited string (5 - 30 characters)
HTTP proxy settings options:		
-loc	HTTP proxy location	Fully qualified hostname or IP address for HTTP proxy (63 characters maximum)
-po	HTTP proxy port	Valid port number (1 - 65535)
-ps	HTTP proxy status	enabled, disabled
-pw	HTTP proxy password	Valid password, quote-delimited (15 characters maximum)
-u	HTTP proxy user name	Valid user name, quote-delimited (30 characters maximum)

Syntax:

```
chconfig [options]
option:
  -li view|accept
  -sa enable|disable
  -sc service_country_code
  -ce contact_email
  -cn contact_name
  -co company_name
  -cph contact_phone
  -cpx contact_extension_phone
  -an alternate_contact_name
  -ae alternate_contact_email
  -aph alternate_contact_phone
  -apx alternate_contact_extension_phone
  -mp machine_phone_number
  -loc hostname/ip_address
  -po proxy_port
  -ps proxy_status
  -pw proxy_pw
  -ccl machine_country_code
  -u proxy_user_name
```

chlog command

Use the **chlog** command to display Service Advisor activity log entries. The **chlog** command displays the last five entries from the call-home activity log that were generated by the server or the user. The most recent call home entry is shown first. The server will not send duplicate events if they are not acknowledged as corrected in the activity log.

The following table shows the arguments for the options.

Option	Description	Values
-index	Specify a call home entry by using the Index from the Activity Log	Event index number. The index numbers can be viewed using the **chlog** command.
-ack	Acknowledge or unacknowledged that a call home event has been corrected	yes, no **Note:** The ***-event_index*** command option specifies the event to acknowledge or unacknowledged.
-s	Displays the last five IBM Support entries from the call-home activity log	
-f	Displays the last five FTP/TFTP server entries from the call-home activity log	

Syntax:

```
chlog [options]
option:
  -index
  -ack state
  -s
  -f
```

chmanual command

Use the **chmanual** command to generate a manual call home request or a test call home event.

Note: Call home message recipients are configured using the **chconfig** command.

- The **chmanual -test** command generates a call home test message.
- The **chmanual -desc** command generates a manual call home message.

The following table shows the arguments for the options.

Option	Description	Values
-test	Generates a test message to call home recipients	
-desc	Sends user-generated message to call home recipients	Quote-delimited problem description string (100 characters maximum)

Syntax:

```
chmanual [options]
option:
  -test
  -desc message
```

events command

Note: The Service Advisor Terms and Conditions must be accepted first before using the **events** command.

Use the **events** command to view and edit the call home event configuration. Each type of event generated by the IMM2 has a unique event ID. You can prevent specific events from generating call home messages by adding them to the call home event *exclusion list*. The following table shows the arguments for the options.

Option	Description	Values
-add	Add a call home event into the call home *exclusion list*	Event ID of the form *0xhhhhhhhhhhhhhhhh*.
-rm	Remove a call home event from the call home *exclusion list*	Event ID of the form *0xhhhhhhhhhhhhhhhh* or all.

Syntax:

```
events -che [options]
option:
  -add event_id
  -rm event_id
```

sdemail command

Use the **sdemail** command to send service information using email. The **sdemail** command sends an email to the specified recipient with the IMM2 service log as an attachment.

The following table shows the arguments for the options.

Option	Description	Values
-to	Recipient's information *(required option)*	Recipient's email address: • Multiple addresses are separated with a comma (119 characters maximum), of the form: `userid1@hostname1,userid2@hostname2`. • The userid can be alphanumeric characters, '.', '-', or '_'; but, must begin and end with alphanumeric characters • The hostname can be alphanumeric characters, '.', '-', or '_'. It must contain two domain items. Every domain item should begin and end with alphanumeric characters. The last domain item should be 2 – 20 alphabetic characters
-subj	Email subject	Quote-delimited string (119 characters maximum)

Syntax:

```
sdemail [options]
option:
  -to recipient_info
  -subj subject
```

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 software, 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/systems/info/x86servers/serverproven/compat/us to make sure that the hardware and software is supported by your IBM product.
- Go to http://www.ibm.com/supportportal 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/entry/portal/Open_service_request 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/supportportal.

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/supportportal. IBM System x information is at http://www.ibm.com/systems/x. IBM BladeCenter information is at http://www.ibm.com/systems/bladecenter. IBM IntelliStation information is at http://www.ibm.com/systems/intellistation.

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 the terms of use at http://www.ibm.com/de/support/ecurep/terms.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

Creating a personalized support web page

You can create a personalized support web page by identifying IBM products that are of interest to you.

To create a personalized support web page, go to http://www.ibm.com/support/mynotifications. From this personalized page, you can subscribe to weekly email notifications about new technical documents, search for information and downloads, and access various administrative services.

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 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 **Business Partner Locator**. 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 http://www.ibm.com/legal/us/en/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.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. IBM is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

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 10. 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

Table 10. Limits for particulates and gases (continued)

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

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 Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@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 GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@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

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

Part Number: 00FH193

Printed in USA

(1P) P/N: 00FH193