Integrated Management Module II

User's Guide

Integrated Management Module II

User's Guide

Seventh Edition (December 2014)

Contents

Chapter 7. Features on Demand . . . 187

Chapter 8. Command-line interface 193

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 BladeCenter® blade servers.
- Embedded Dynamic System Analysis™ (DSA).
- Remote configuration with Advanced Settings Utility (ASU). The feature does not apply to 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 BladeCenter blade servers.
- Enhanced remote-presence capabilities. The feature does not apply to BladeCenter blade servers.

Notes:

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

System x Server Firmware is the implementation of Unified Extensible Firmware Interface (UEFI). It replaces the basic input/output system (BIOS) in System x servers and 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. 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:

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

This document explains how to use the functions of the IMM2 in a Lenovo® server. The IMM2 works with System x Server Firmware to provide systems-management capability for System x, BladeCenter, and a Flex System™.

To check for firmware updates, complete the following steps.

Note: The first time you access the Support Portal, you must choose the product category, product family, and model numbers for your storage subsystems. The next time you access the 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 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 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 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 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 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 187.

Using IMM2 with the BladeCenter advanced management module

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

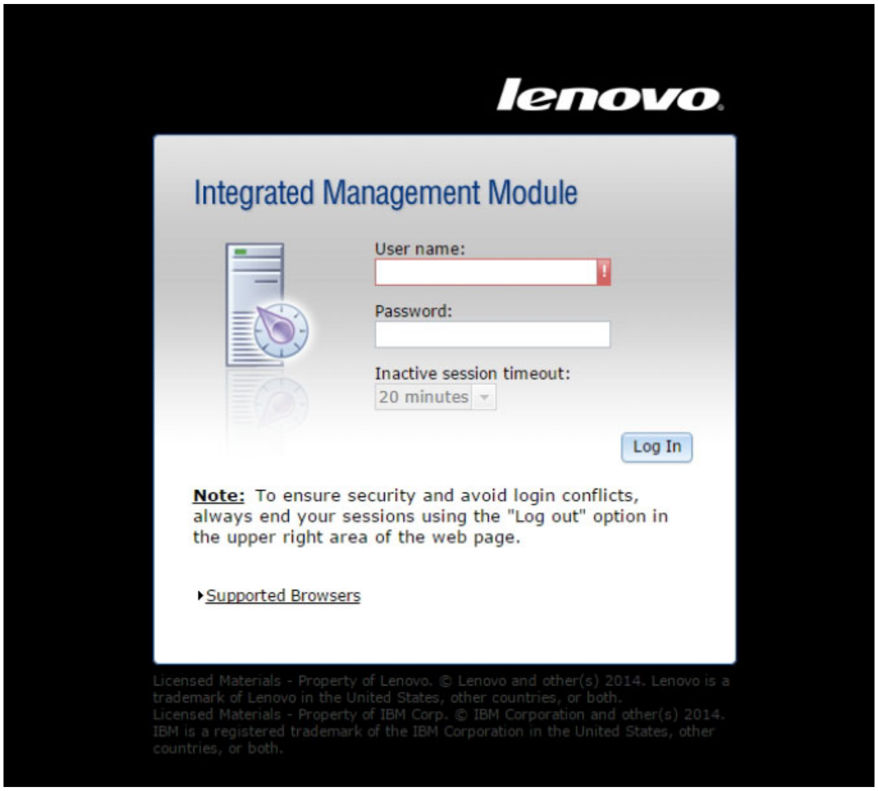
There is no external network access to the IMM2 on BladeCenter blade servers and the advanced management module must be used for remote management of BladeCenter blade servers. The IMM2 replaces the functionality of the BMC and the Concurrent Keyboard, Video and Mouse (cKVM) option card available in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

Web browser and operating-system requirements

The IMM2 web interface requires the Java Plug-in 1.7 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

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.

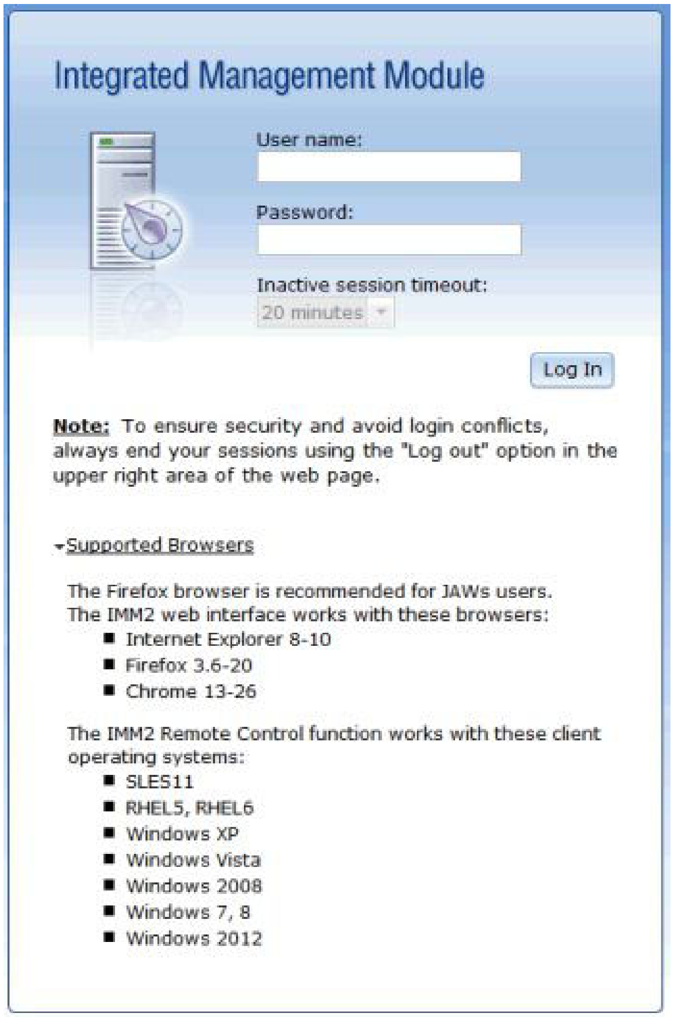


20 minutes

Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

Licensed Materials - Property of Lenovo. © Lenovo and other(s) 2014. Lenovo is a trademark of Lenovo in the United States, other countries, or both.
Licensed Materials - Property of IBM Corp. © IBM Corporation and other(s) 2014. IBM is a registered trademark of the IBM Corporation in the United States, other countries, or both.

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).



Inactive session timeout: 20 minutes

Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

Supported Browsers

The Firefox browser is recommended for JAWs users.
The IMM2 web interface works with these browsers:

- Internet Explorer 8-10
- Firefox 3.6-20
- Chrome 13-26

The IMM2 Remote Control function works with these client operating systems:

- SLES11
- RHEL5, RHEL6
- Windows XP
- Windows Vista
- Windows 2008
- Windows 7, 8
- Windows 2012

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

The *dedicated* systems-management network connection on some systems is provided through the Network Controller Sideband Interface (NCSI) instead of its own physical layer and is limited to the 10/100 speed of the sideband interface. For information and any limitations on the implementation of the management port on your system, see your system documentation.

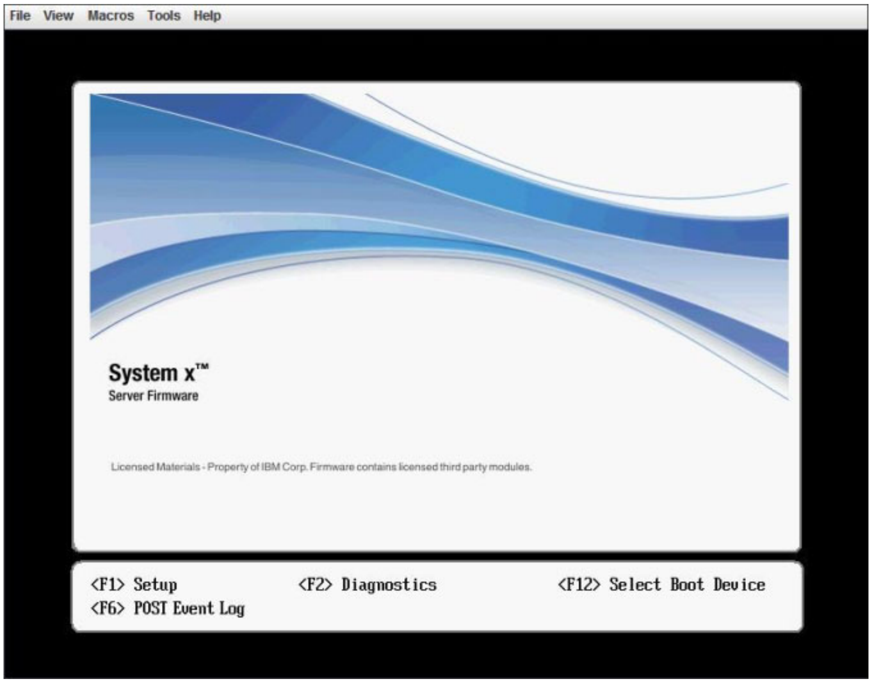
Note: A *dedicated* systems-management network port might not be available on your server. If your hardware does not have a *dedicated* network port, the *shared* setting is the only IMM2 setting available.

Setting up the IMM2 network connection through the 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:

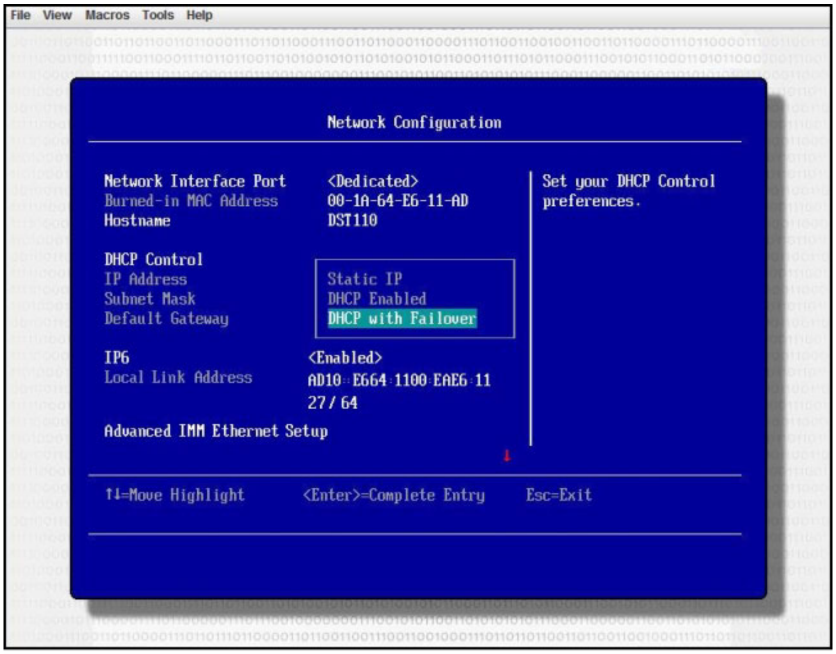
1. Turn on the server. The System x Server Firmware welcome screen is displayed.

   Note: Approximately 90 seconds after the server is connected to ac power, the power-control button becomes active.



Licensed Materials - Property of IBM Corp. Firmware contains licensed third party modules.

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)



```
                    Network Configuration

Network Interface Port    <Dedicated>            Set your DHCP Control
Burned-in MAC Address     00-1A-64-E6-11-AD      preferences.
Hostname                  DST110

DHCP Control
IP Address                Static IP
Subnet Mask               DHCP Enabled
Default Gateway           DHCP with Failover

IP6                      <Enabled>
Local Link Address       AD10::E664:1100:EAE6:11
                         27/64
Advanced IMM Ethernet Setup

↑↓=Move Highlight       <Enter>=Complete Entry     Esc=Exit
```

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

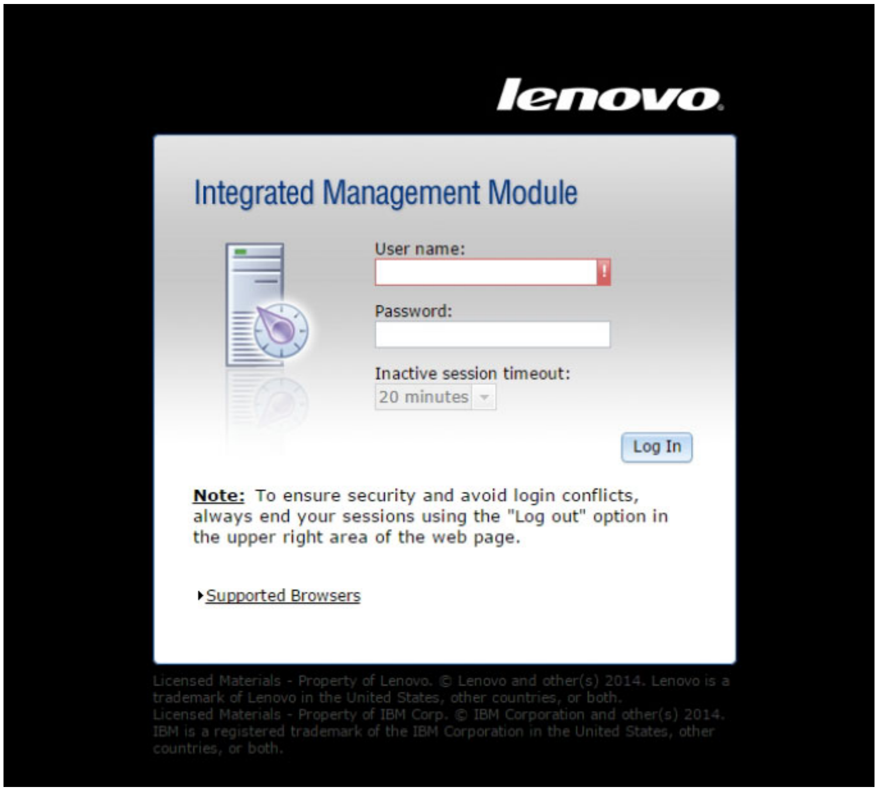
Important: The IMM2 is set initially with a user name of `USERID` and password of `PASSW0RD` (with a zero, not the letter O). This default user setting has Supervisor access. Change this user name and password during your initial configuration for enhanced security.

Note: In a Flex System, the IMM2 user accounts can be managed by a Flex System Chassis Management Module (CMM) and might be different than the USERID/PASSW0RD combination described above.

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.



Inactive session timeout: 20 minutes

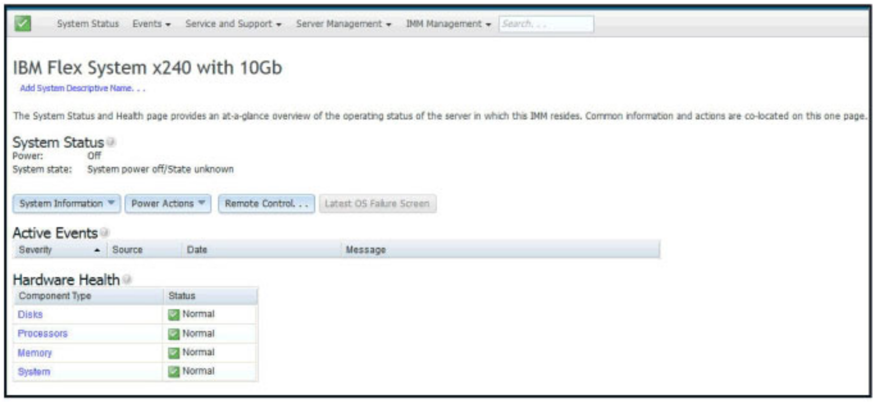
Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

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.



IBM Flex System x240 with 10Gb

The System Status and Health page provides an at-a-glance overview of the operating status of the server in which this IMM resides. Common information and actions are co-located on this one page.

System Status

Power: Off

System state: System power off/State unknown

Active Events

Severity	Source	Date	Message

Hardware Health

Component Type	Status
Disks	Normal
Processors	Normal
Memory	Normal
System	Normal

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.

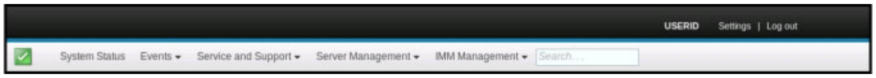


Table 1. IMM2 actions

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 115 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 149 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 151 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 Support to assist you. See "Download service data option" on page 38 and "Collecting service and support information" on page 156 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 39 and "Updating the server firmware" on page 144 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 45 and "Remote presence and remote control functions" on page 123 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.
	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 54 and "Controlling the power status of the server" on page 122 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 54 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 55 for additional information.
	Local Storage	The Local Storage page displays the physical structure and storage configuration of a storage device. See "Local storage" on page 56 and "Viewing and configuring the local storage configuration" on page 173 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 57 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 58 for additional information.
	Adapters	The Adapters page displays the hardware, firmware, and network adapter information for adapters installed in the server. See "Adapters" on page 59 and "Viewing the adapter information and configuration settings" on page 181 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 60 and "Setting server timeouts" on page 66 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 60 and "Setting up PXE network boot" on page 143 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 60 and "Capturing the latest OS failure screen data" on page 158 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 "Power management" on page 61 and "Managing the server power" on page 159 for additional information.
	Scalable Complex	The Scalable Complex page allows you to view and manage a scalable complex. See "Scalable complex" on page 61 and "Managing the scalable complex" on page 169 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 63 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 71 for additional information.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
IMM Management *(continued on next page)*	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 80 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. • The Cryptography Management tab allows you to configure the IMM2 firmware to comply with the requirements of SP 800-131A. • The Drive Access tab allows you to configure Security Key Lifecycle Manager (SKLM) encryption key settings. See “Configuring security settings” on page 94 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 110 for additional information.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
IMM Management *(continued)*	Restart IMM	The Restart IMM page allows you to reset the IMM2. See “Restarting the IMM2” on page 110 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 112 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 113 for additional information.

Chapter 3. IMM2 web user interface overview

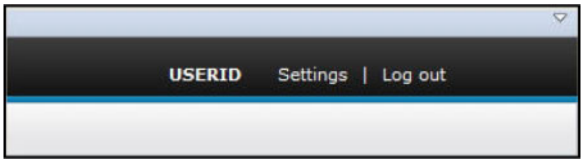
This chapter provides an overview of how to use the IMM2 web user interface features.

Important: This section does not apply to BladeCenter and blade servers. Although the IMM2 is standard in some BladeCenter products and blade servers, the 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 ASU on the blade server to perform those actions.

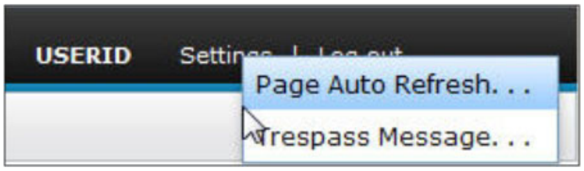
Web session settings

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.

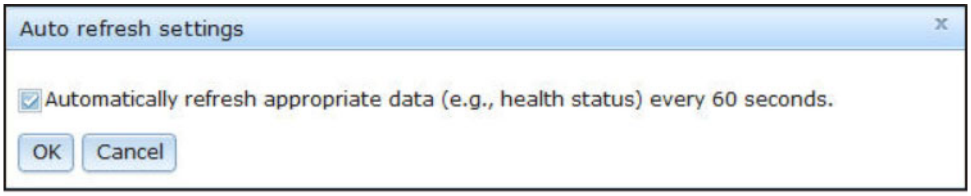


Click the **Settings** item and the following menu selections display:



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.



☑ Automatically refresh appropriate data (e.g., health status) every 60 seconds.

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.

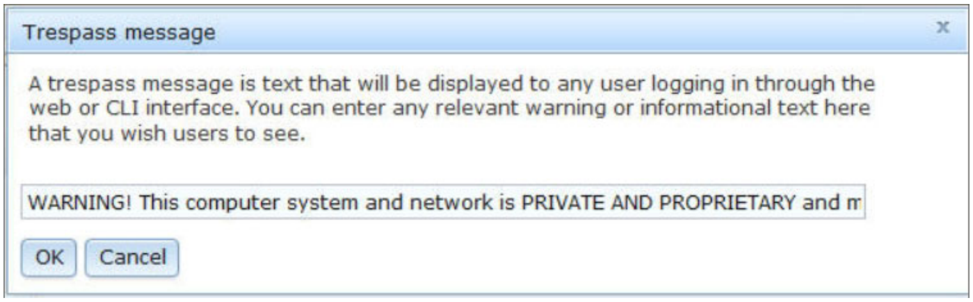
Notes:

- 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**.

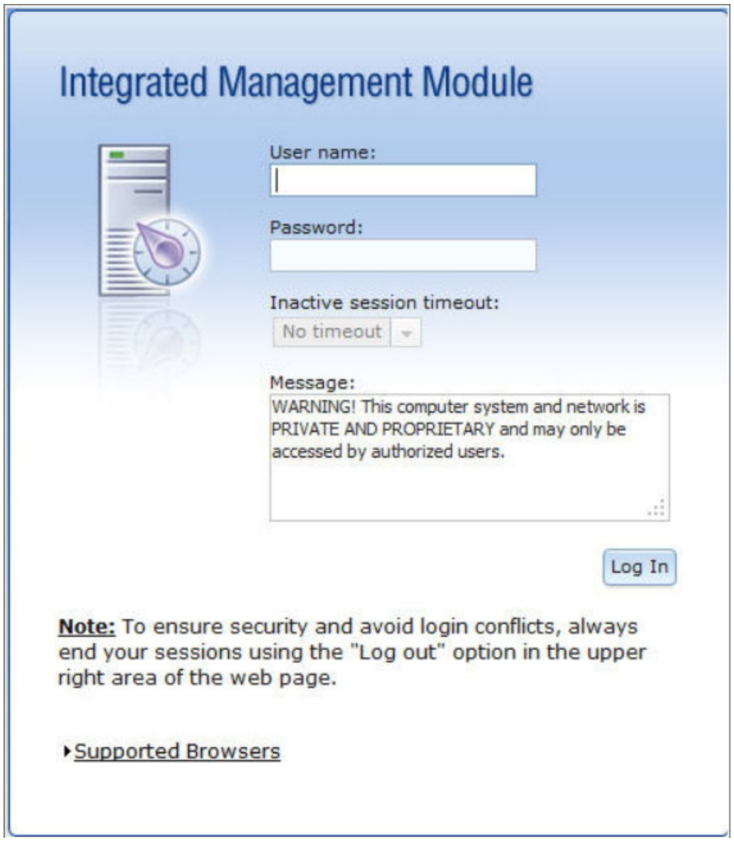


Trespass message

A trespass message is text that will be displayed to any user logging in through the web or CLI interface. You can enter any relevant warning or informational text here that you wish users to see.

WARNING! This computer system and network is PRIVATE AND PROPRIETARY and m

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.



Integrated Management Module

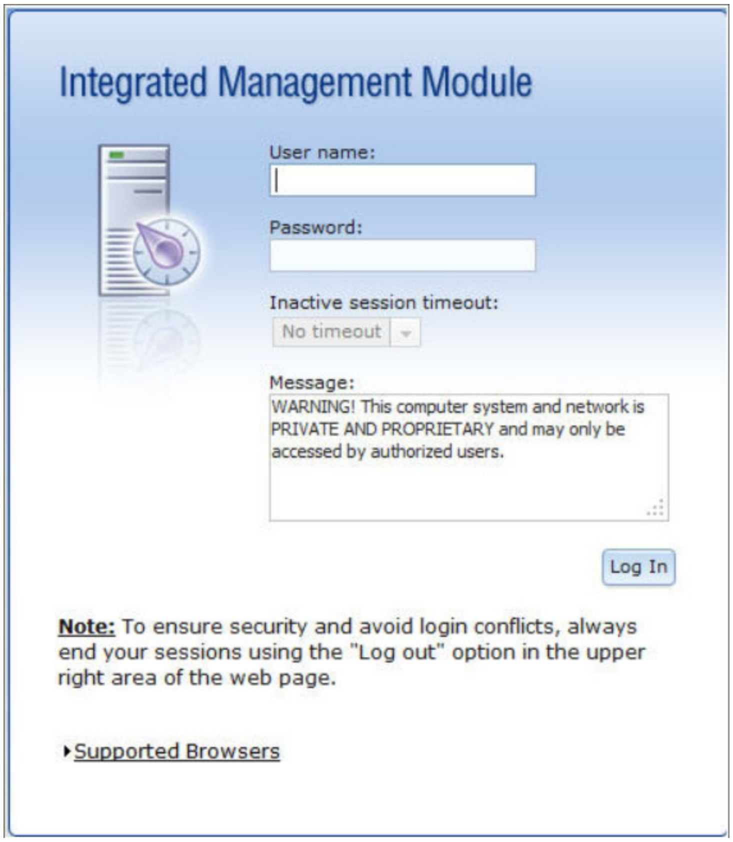
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.

Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

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.



Integrated Management Module

User name:

Password:

Inactive session timeout: No timeout

Message:
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.

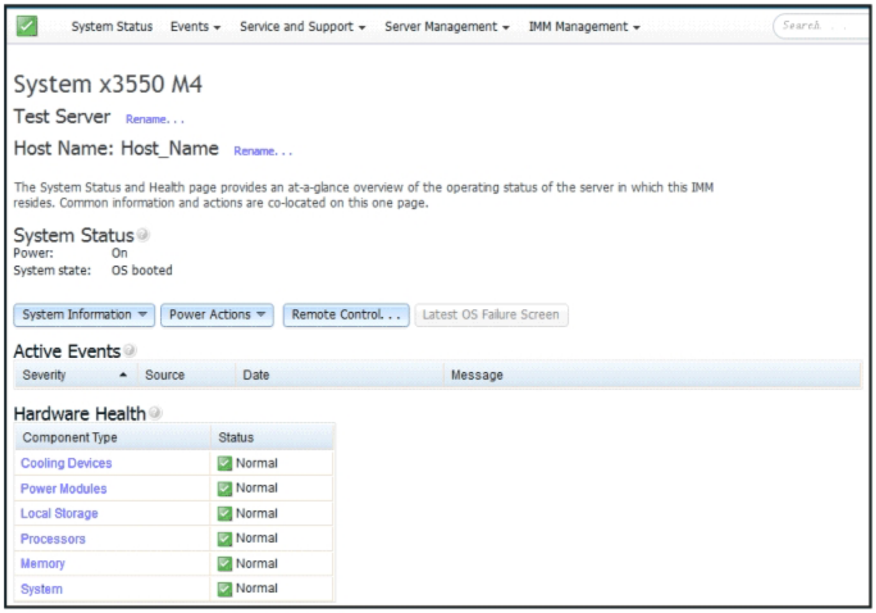
Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

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.



System x3550 M4

Test Server Rename...

Host Name: Host_Name Rename...

The System Status and Health page provides an at-a-glance overview of the operating status of the server in which this IMM resides. Common information and actions are co-located on this one page.

System Status

Power: On

System state: OS booted

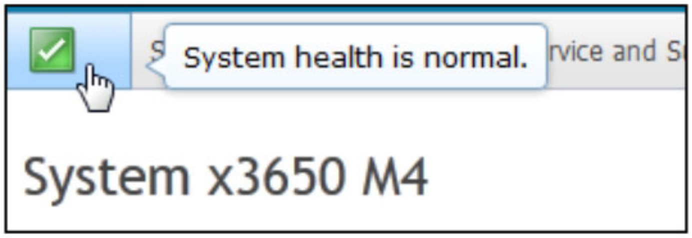
Active Events

Severity	Source	Date	Message

Hardware Health

Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✓ Normal
Local Storage	✓ Normal
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

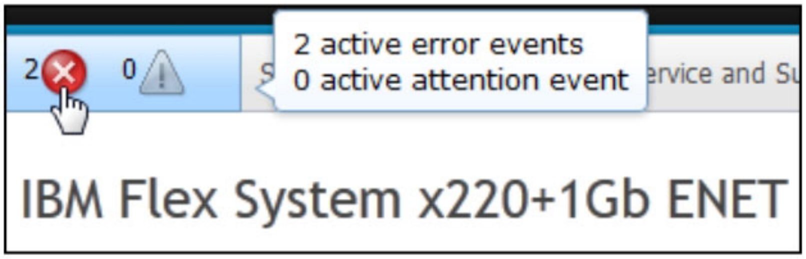
You can click on the green icon (with the check mark) in the upper left corner of the page to get a quick summary of the server health. A check mark indicates that the server is operating normally.



System health is normal.

System x3650 M4

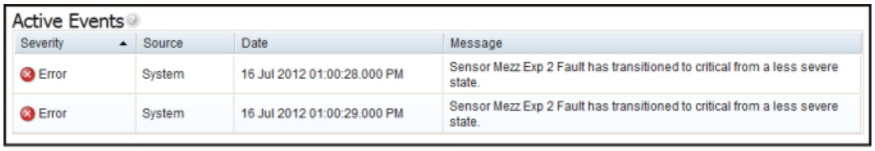
If a red circle or a yellow triangle icon is displayed, this indicates that an error or warning condition exists, as shown in the following illustration.



2 active error events
0 active attention event

IBM Flex System x220+1Gb ENET

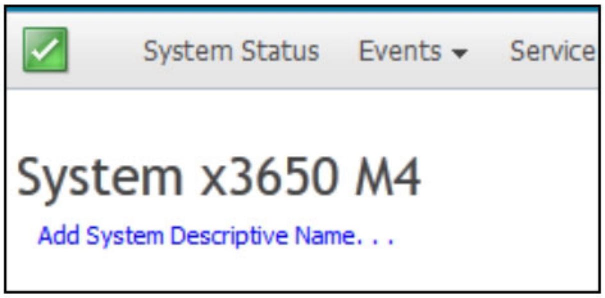
The red circle icon indicates that an error condition exists on the server. A yellow triangle icon indicates that a warning condition exists. When a red circle or a yellow triangle icon is displayed, the events associated with that condition are listed under the Active Events section on the System Status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



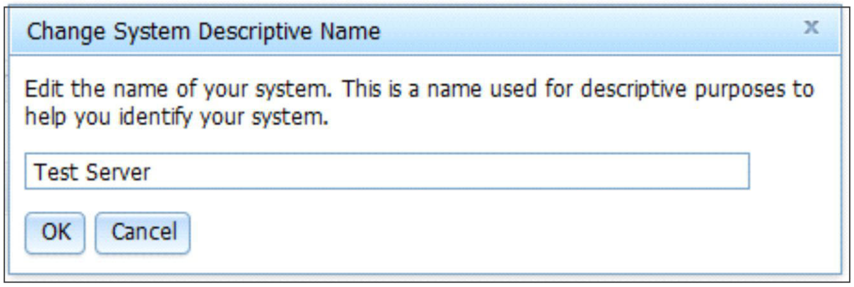
Active Events

Severity	Source	Date	Message
Error	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.
Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.

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.



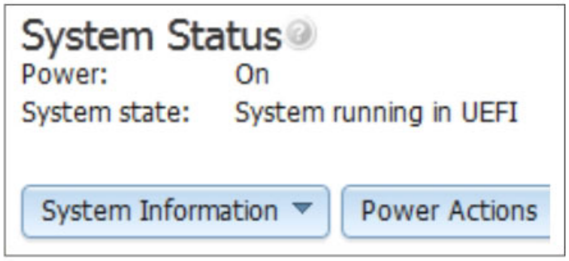
Change System Descriptive Name

Edit the name of your system. This is a name used for descriptive purposes to help you identify your system.

Test Server

If you click the **Rename...** link beside the Host Name, the Network Protocol Properties page opens. You can use the Network Protocol Properties page to configure the Host Name on the **Ethernet** tab. See “Configuring network protocols” on page 80 for additional information.

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).



System Status

Power: On

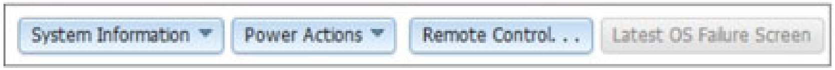
System state: System running in UEFI

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

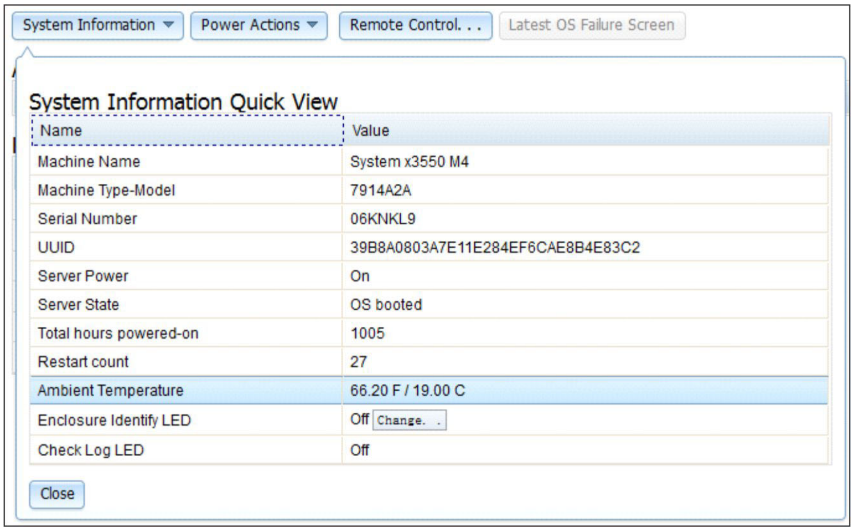
Table 2. Server power and operating states

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



System Information Quick View

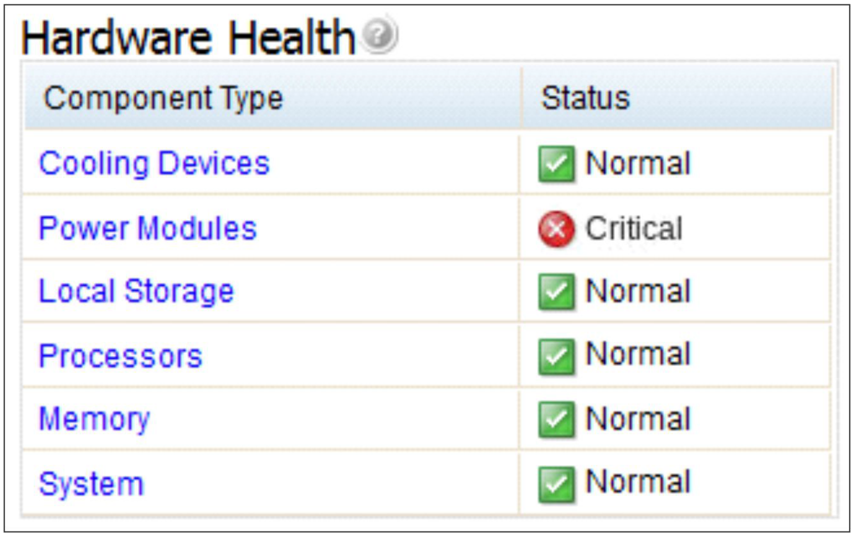
Name	Value
Machine Name	System x3550 M4
Machine Type-Model	7914A2A
Serial Number	06KNKL9
UUID	39B8A0803A7E11E284EF6CAE8B4E83C2
Server Power	On
Server State	OS booted
Total hours powered-on	1005
Restart count	27
Ambient Temperature	66.20 F / 19.00 C
Enclosure Identify LED	Off Change. .
Check Log LED	Off

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 122 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 123 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 158 for details about the Latest OS Failure Screen.

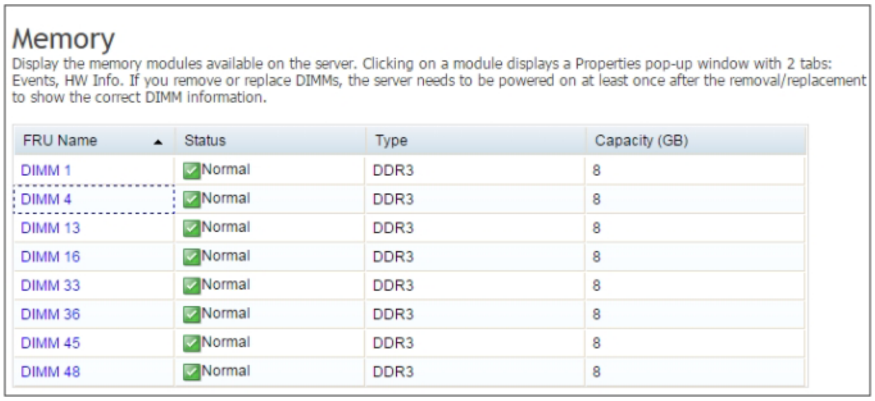
Under the **Hardware Health** section of the System Status page is a table with a list of the hardware components that are being monitored and their health status. The status displayed for a component might reflect the most critical state of the component in the Component Type column in the table. For 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).



Hardware Health

Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✗ Critical
Local Storage	✓ Normal
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

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).

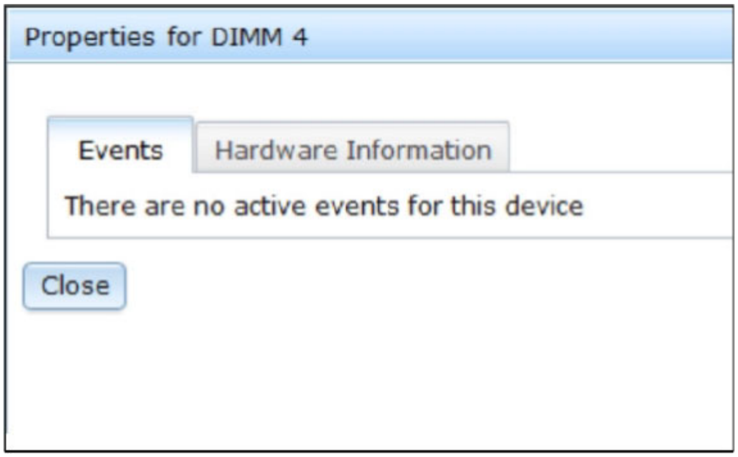


Memory

Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Events, HW Info. If you remove or replace DIMMs, the server needs to be powered on at least once after the removal/replacement to show the correct DIMM information.

FRU Name ▲	Status	Type	Capacity (GB)
DIMM 1	✓ Normal	DDR3	8
DIMM 4	✓ Normal	DDR3	8
DIMM 13	✓ Normal	DDR3	8
DIMM 16	✓ Normal	DDR3	8
DIMM 33	✓ Normal	DDR3	8
DIMM 36	✓ Normal	DDR3	8
DIMM 45	✓ Normal	DDR3	8
DIMM 48	✓ Normal	DDR3	8

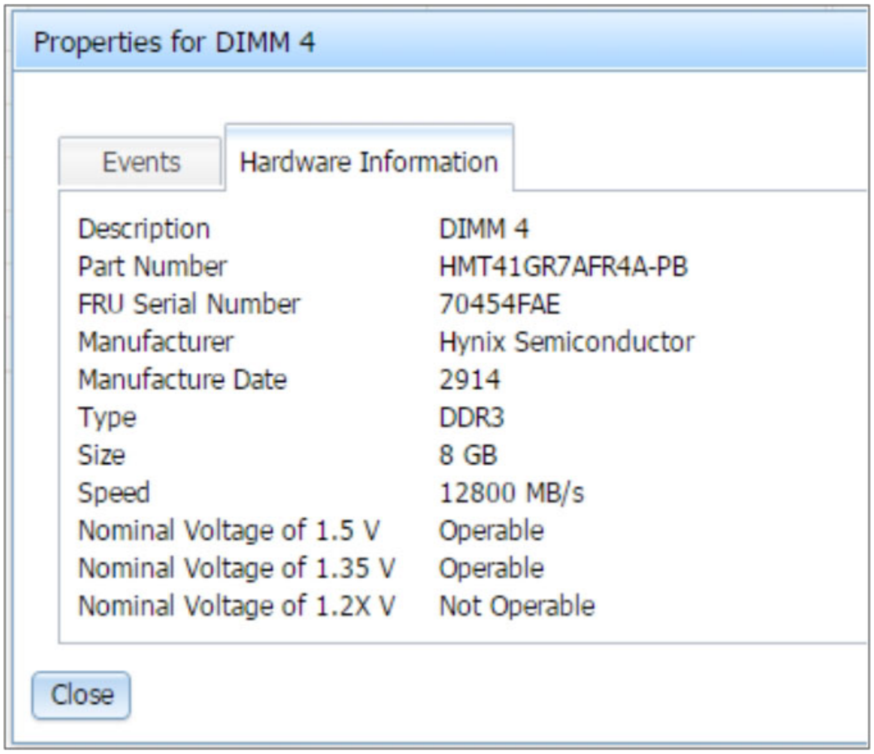
You can click on a component in the FRU Name column of the table to obtain additional information for that component. All active events for the component will be displayed.



Properties for DIMM 4

There are no active events for this device

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

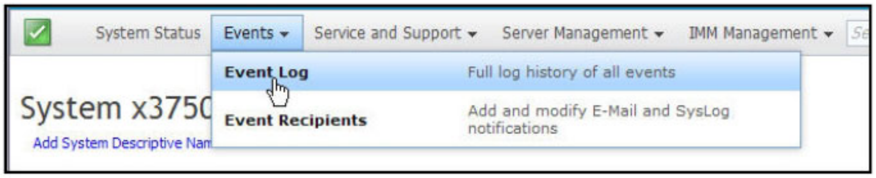


Description	DIMM 4
Part Number	HMT41GR7AFR4A-PB
FRU Serial Number	70454FAE
Manufacturer	Hynix Semiconductor
Manufacture Date	2914
Type	DDR3
Size	8 GB
Speed	12800 MB/s
Nominal Voltage of 1.5 V	Operable
Nominal Voltage of 1.35 V	Operable
Nominal Voltage of 1.2X V	Not Operable

Events tab

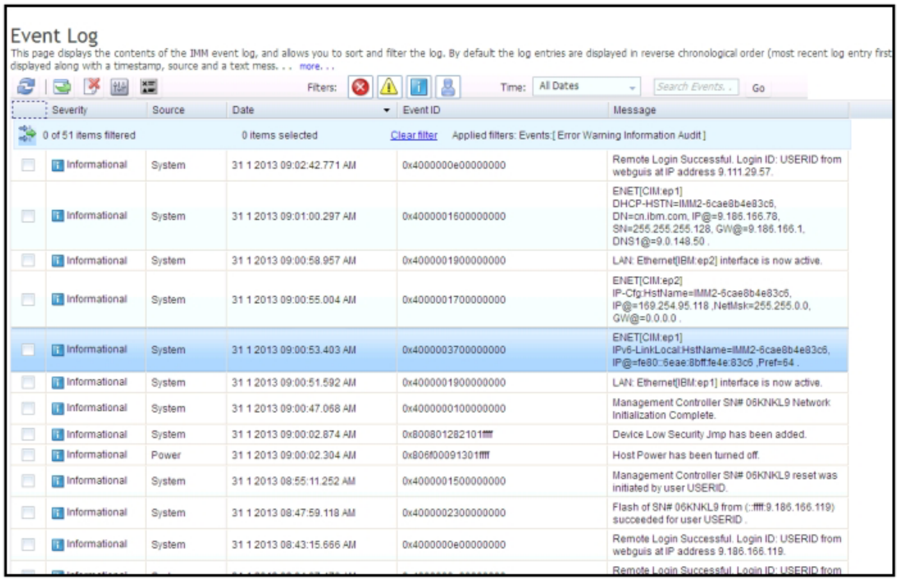
This section provides information for using the options under the **Events** tab on the IMM2 web user interface.

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.



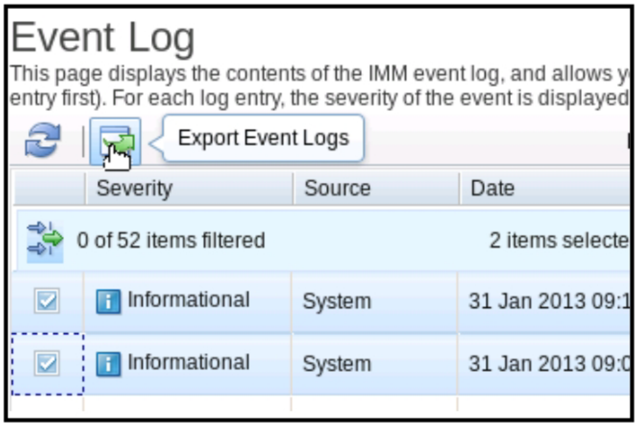
Event Log

This page displays the contents of the IMM event log, and allows you to sort and filter the log. By default the log entries are displayed in reverse chronological order (most recent log entry first displayed along with a timestamp, source and a text mess. . . more. . .

0 of 51 items filtered — 0 items selected — Clear filter — Applied filters: Events:[Error Warning Information Audit]

	Severity	Source	Date	Event ID	Message
□	Informational	System	31 1 2013 09:02:42.771 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.111.29.57.
□	Informational	System	31 1 2013 09:01:00.297 AM	0x4000001600000000	ENET[CIM:ep1] DHCP-HSTN=IMM2-6cae8b4e83c6, DN=cn.ibm.com, IP@=9.186.166.78, SN=255.255.255.128, GW@=9.186.166.1, DNS1@=9.0.148.50 .
□	Informational	System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet[IBM:ep2] interface is now active.
□	Informational	System	31 1 2013 09:00:55.004 AM	0x4000001700000000	ENET[CIM:ep2] IP-Cfg:HstName=IMM2-6cae8b4e83c6, IP@=169.254.95.118 ,NetMsk=255.255.0.0, GW@=0.0.0.0 .
□	Informational	System	31 1 2013 09:00:53.403 AM	0x4000003700000000	ENET[CIM:ep1] IPv6-LinkLocal:HstName=IMM2-6cae8b4e83c6, IP@=fe80::6eae:8bff:fe4e:83c6 ,Pref=64 .
□	Informational	System	31 1 2013 09:00:51.592 AM	0x4000001900000000	LAN: Ethernet[IBM:ep1] interface is now active.
□	Informational	System	31 1 2013 09:00:47.068 AM	0x4000000100000000	Management Controller SN# 06KNKL9 Network Initialization Complete.
□	Informational	System	31 1 2013 09:00:02.874 AM	0x800801282101ffff	Device Low Security Jmp has been added.
□	Informational	Power	31 1 2013 09:00:02.304 AM	0x806f00091301ffff	Host Power has been turned off.
□	Informational	System	31 1 2013 08:55:11.252 AM	0x4000001500000000	Management Controller SN# 06KNKL9 reset was initiated by user USERID.
□	Informational	System	31 1 2013 08:47:59.118 AM	0x4000002300000000	Flash of SN# 06KNKL9 from (::ffff:9.186.166.119) succeeded for user USERID .
□	Informational	System	31 1 2013 08:43:15.666 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.186.166.119.
					Remote Login Successful. Login ID: USERID from

To sort and filter events in the event log, select the column heading. 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).



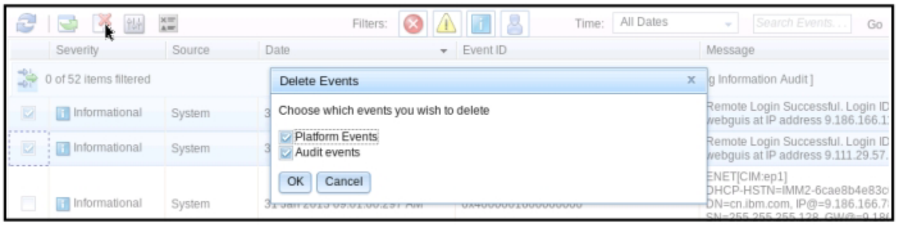
Event Log

This page displays the contents of the IMM event log, and allows y
entry first). For each log entry, the severity of the event is displayed

0 of 52 items filtered — 2 items selecte

	Severity	Source	Date
☑	Informational	System	31 Jan 2013 09:1
☑	Informational	System	31 Jan 2013 09:0

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



0 of 52 items filtered

Delete Events

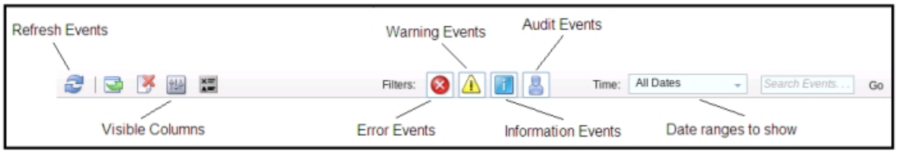
Choose which events you wish to delete

☑ Platform Events
☑ Audit events

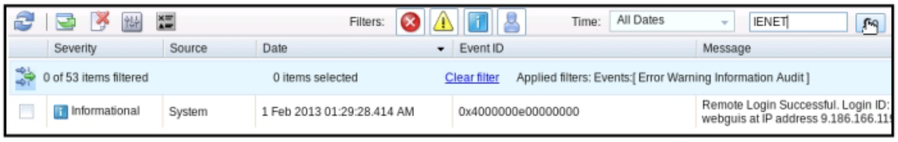
OK Cancel

Severity	Source	Message
Informational	System	Remote Login Successful. Login ID webguis at IP address 9.186.166.1
Informational	System	Remote Login Successful. Login ID webguis at IP address 9.111.29.57.
Informational	System	ENET[CIM:ep1] DHCP-HSTN=IMM2-6cae8b4e83c DN=cn.ibm.com, IP@=9.186.166.7 SN=255.255.255.128, GW@=0.18

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



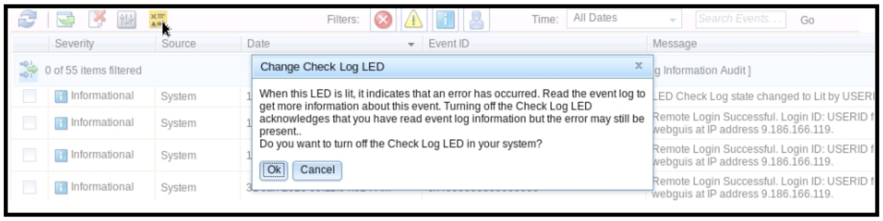
To search for specific types of events or keywords, type the type of event or keyword in the **Search Events** box; then, click **Go** (as shown in the following illustration).



0 of 53 items filtered   0 items selected   Clear filter   Applied filters: Events:[Error Warning Information Audit]

Severity	Source	Date	Event ID	Message
Informational	System	1 Feb 2013 01:29:28.414 AM	0x4000000e00000000	Remote Login Successful. Login ID: webguis at IP address 9.186.166.11

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).



0 of 55 items filtered

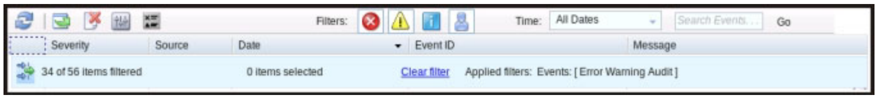
Change Check Log LED

When this LED is lit, it indicates that an error has occurred. Read the event log to get more information about this event. Turning off the Check Log LED acknowledges that you have read event log information but the error may still be present..
Do you want to turn off the Check Log LED in your system?

Ok Cancel

Severity	Source	Message
Informational	System	LED Check Log state changed to Lit by USERI
Informational	System	Remote Login Successful. Login ID: USERID f webguis at IP address 9.186.166.119.
Informational	System	Remote Login Successful. Login ID: USERID f webguis at IP address 9.186.166.119.
Informational	System	Remote Login Successful. Login ID: USERID f webguis at IP address 9.186.166.119.

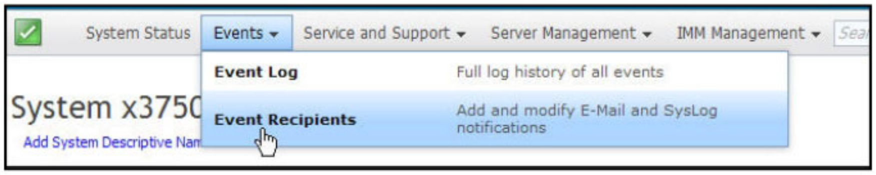
On the Event Log tool bar you can click any of the **Filter Events** buttons to select the events to be displayed. To clear the filter and show all types of events, click the **Clear Filter** link shown in the following illustration.



34 of 56 items filtered   0 items selected   Clear filter   Applied filters: Events: [Error Warning Audit]

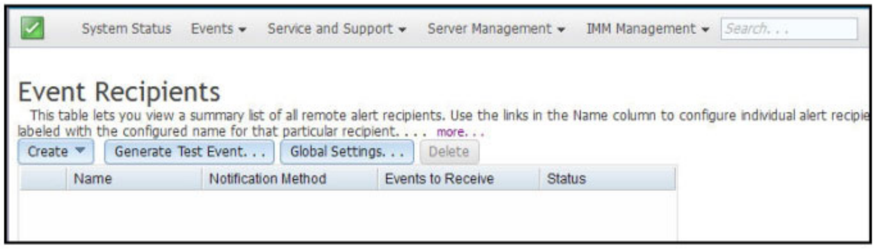
Event recipients

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.

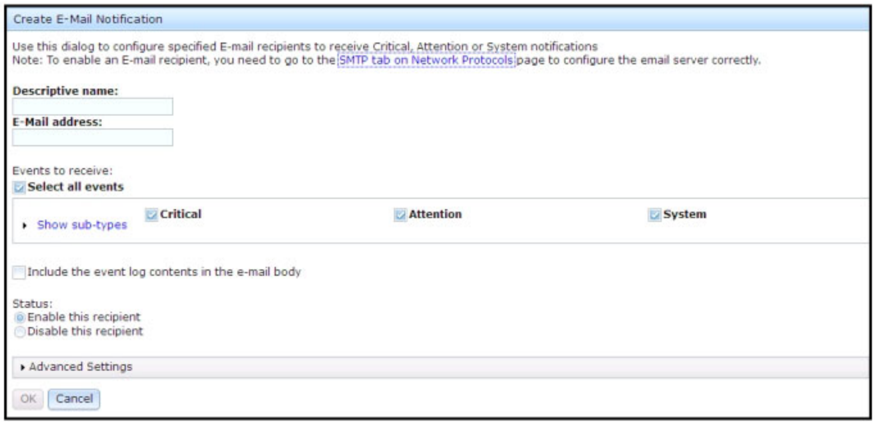


Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure individual alert recipie labeled with the configured name for that particular recipient. . . . more. . .

	Name	Notification Method	Events to Receive	Status

From the **Create** button 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.



Create E-Mail Notification

Use this dialog to configure specified E-mail recipients to receive Critical, Attention or System notifications
Note: To enable an E-mail recipient, you need to go to the SMTP tab on Network Protocols page to configure the email server correctly.

Descriptive name:

E-Mail address:

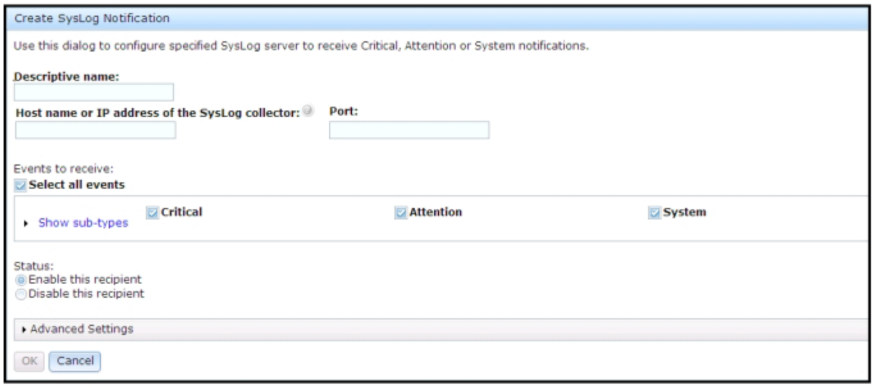
Events to receive:
☑ **Select all events**

☑ **Critical** ☑ **Attention** ☑ **System**

☐ Include the event log contents in the e-mail body

Status:
● Enable this recipient
○ Disable this recipient

From the **Create** button 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.



Create SysLog Notification

Use this dialog to configure specified SysLog server to receive Critical, Attention or System notifications.

Descriptive name:

Host name or IP address of the SysLog collector: **Port:**

Events to receive:

☑ **Select all events**

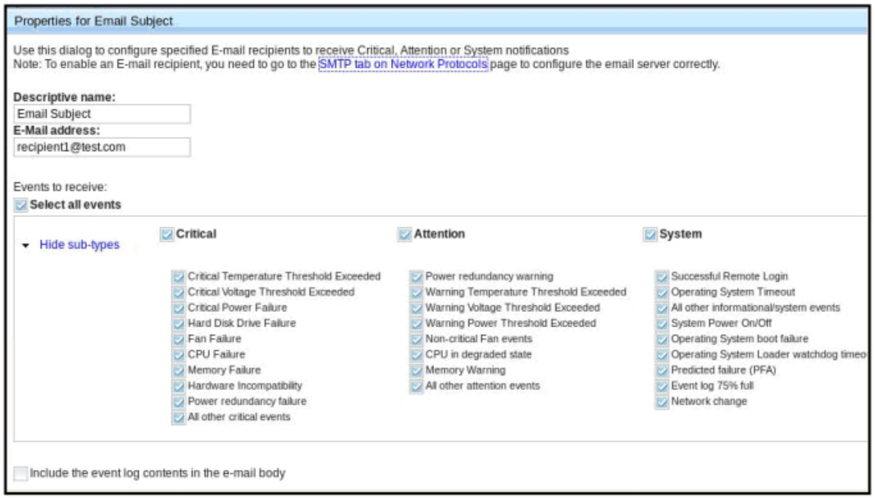
☑ **Critical** ☑ **Attention** ☑ **System**

Status:

● Enable this recipient

○ Disable this recipient

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.



Properties for Email Subject

Use this dialog to configure specified E-mail recipients to receive Critical, Attention or System notifications

Note: To enable an E-mail recipient, you need to go to the SMTP tab on Network Protocols page to configure the email server correctly.

Descriptive name: Email Subject

E-Mail address: recipient1@test.com

Events to receive:

☑ **Select all events**

☑ **Critical**

☑ Critical Temperature Threshold Exceeded
☑ Critical Voltage Threshold Exceeded
☑ Critical Power Failure
☑ Hard Disk Drive Failure
☑ Fan Failure
☑ CPU Failure
☑ Memory Failure
☑ Hardware Incompatibility
☑ Power redundancy failure
☑ All other critical events

☑ **Attention**

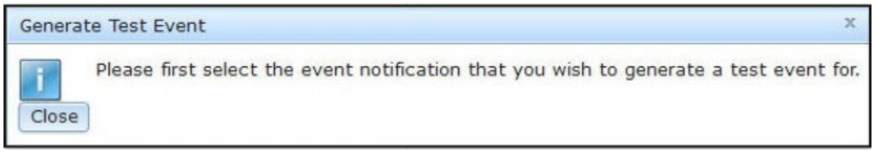
☑ Power redundancy warning
☑ Warning Temperature Threshold Exceeded
☑ Warning Voltage Threshold Exceeded
☑ Warning Power Threshold Exceeded
☑ Non-critical Fan events
☑ CPU in degraded state
☑ Memory Warning
☑ All other attention events

☑ **System**

☑ Successful Remote Login
☑ Operating System Timeout
☑ All other informational/system events
☑ System Power On/Off
☑ Operating System boot failure
☑ Operating System Loader watchdog timeo
☑ Predicted failure (PFA)
☑ Event log 75% full
☑ Network change

□ Include the event log contents in the e-mail body

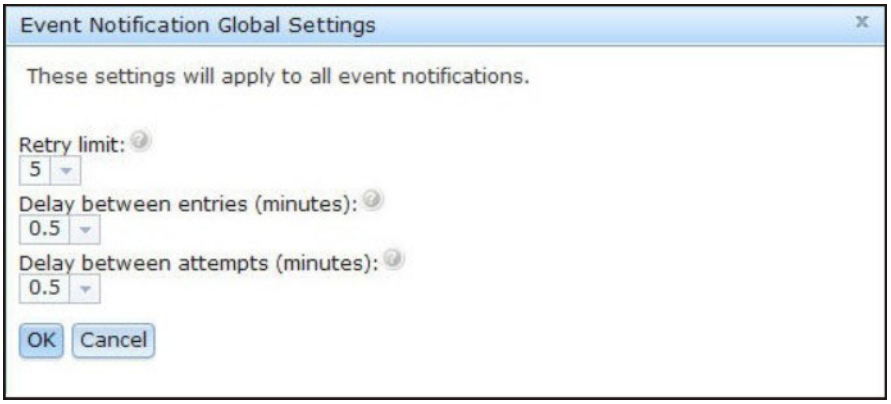
Select the **Generate Test Event** button to send a test email to a selected email target (as shown in the following illustration).



Generate Test Event

Please first select the event notification that you wish to generate a test event for.

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).


Event Notification Global Settings

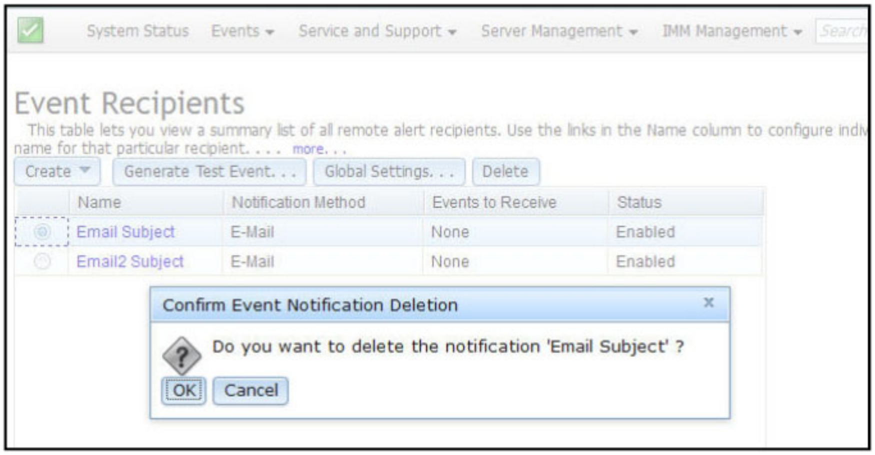
These settings will apply to all event notifications.

Retry limit: 5

Delay between entries (minutes): 0.5

Delay between attempts (minutes): 0.5

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



Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure indiv
name for that particular recipient. . . . more. . .

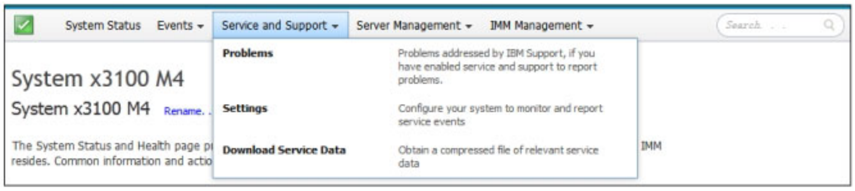
	Name	Notification Method	Events to Receive	Status
◉	Email Subject	E-Mail	None	Enabled
○	Email2 Subject	E-Mail	None	Enabled

Confirm Event Notification Deletion

Do you want to delete the notification 'Email Subject' ?

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).



System x3100 M4

System x3100 M4 Rename. .

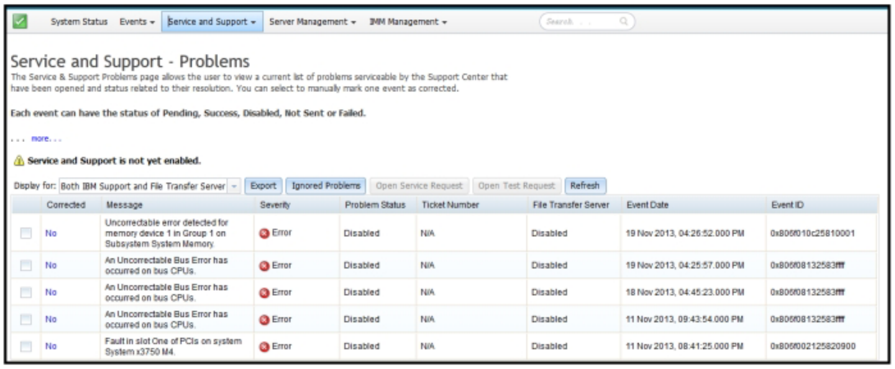
The System Status and Health page p
resides. Common information and actio

IMM

Problems	Problems addressed by IBM Support, if you have enabled service and support to report problems.
Settings	Configure your system to monitor and report service events
Download Service Data	Obtain a compressed file of relevant service data

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.



Service and Support - Problems

The Service & Support Problems page allows the user to view a current list of problems serviceable by the Support Center that have been opened and status related to their resolution. You can select to manually mark one event as corrected.

Each event can have the status of Pending, Success, Disabled, Not Sent or Failed.

. . . more. . .

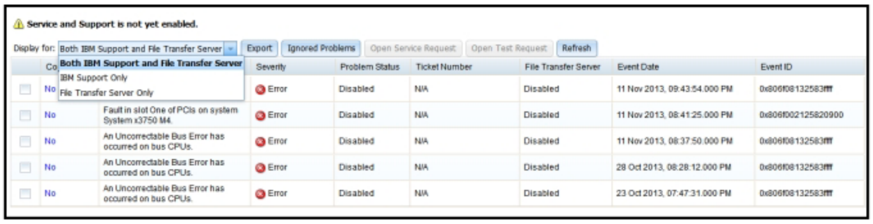
⚠ **Service and Support is not yet enabled.**

Display for: Both IBM Support and File Transfer Server

	Corrected	Message	Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
□	No	Uncorrectable error detected for memory device 1 in Group 1 on Subsystem System Memory	Error	Disabled	N/A	Disabled	19 Nov 2013, 04:26:52.000 PM	0x806f010c25810001
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	19 Nov 2013, 04:25:57.000 PM	0x806f08132583ffff
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	18 Nov 2013, 04:45:23.000 PM	0x806f08132583ffff
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 09:43:54.000 PM	0x806f08132583ffff
□	No	Fault in slot One of PCIs on system System x3750 M4.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:41:25.000 PM	0x806f002125820900

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

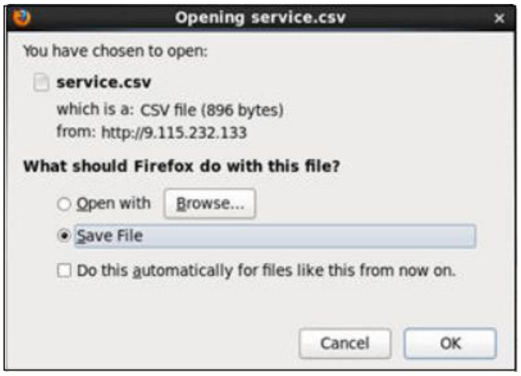
- Both IBM Support and File Transfer Server
- IBM Support Only
- File Transfer Server Only


⚠ **Service and Support is not yet enabled.**

Display for: Both IBM Support and File Transfer Server

	Co		Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
□	No		Error	Disabled	N/A	Disabled	11 Nov 2013, 09:43:54.000 PM	0x806f08132583ffff
□	No	Fault in slot One of PCIs on system System x3750 M4.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:41:25.000 PM	0x806f002125820900
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:37:50.000 PM	0x806f08132583ffff
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	28 Oct 2013, 08:28:12.000 PM	0x806f08132583ffff
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	23 Oct 2013, 07:47:31.000 PM	0x806f08132583ffff

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


Opening service.csv

You have chosen to open:

service.csv

which is a: CSV file (896 bytes)
from: http://9.115.232.133

What should Firefox do with this file?

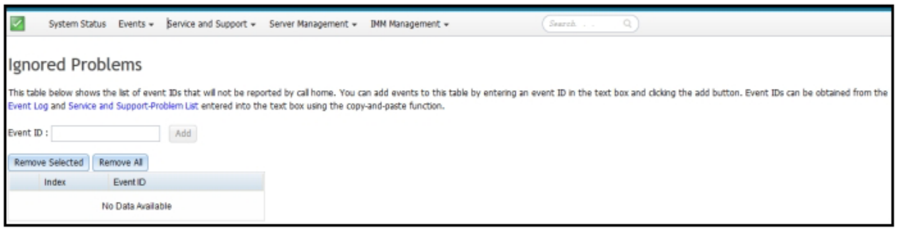
○ Open with

● Save File

□ Do this automatically for files like this from now on.

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.



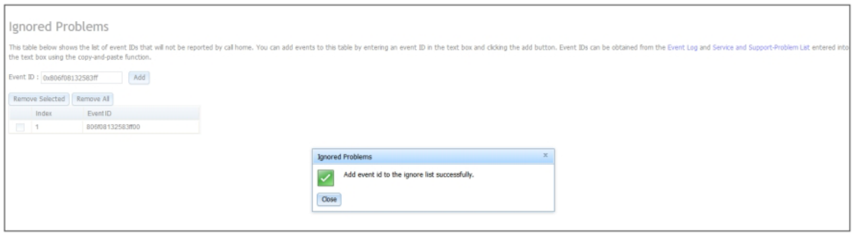
Ignored Problems

This table below shows the list of event IDs that will not be reported by call home. You can add events to this table by entering an event ID in the text box and clicking the add button. Event IDs can be obtained from the Event Log and Service and Support-Problem List entered into the text box using the copy-and-paste function.

Event ID :

No Data Available

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



Ignored Problems

This table below shows the list of event IDs that will not be reported by call home. You can add events to this table by entering an event ID in the text box and clicking the add button. Event IDs can be obtained from the Event Log and Service and Support-Problem List entered into the text box using the copy-and-paste function.

Event ID : 0x806f08132583ff

	Index	Event ID
□	1	806f08132583ff00

Ignored Problems

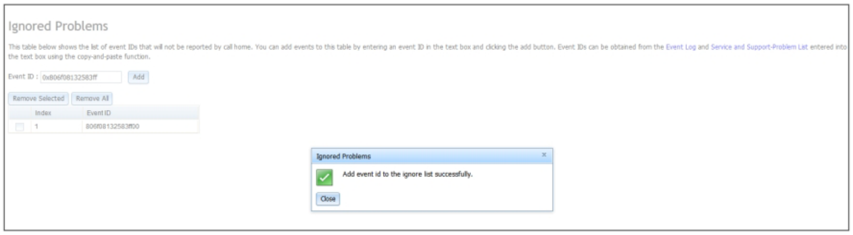
Add event id to the ignore list successfully.

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).

   Ignored Problems

   This table below shows the list of event IDs that will not be reported by call home. You can add events to this table by entering an event ID in the text box and clicking the add button. Event IDs can be obtained from the Event Log and Service and Support-Problem List entered into the text box using the copy-and-paste function.

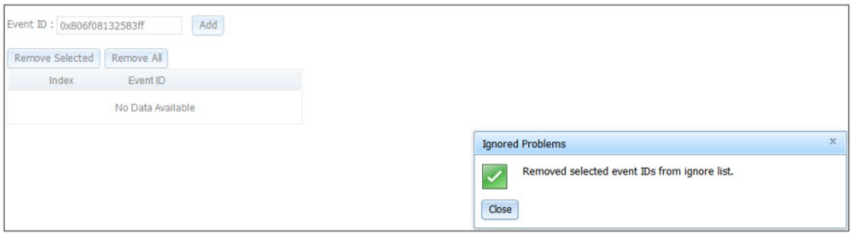
   Event ID : 0x806f08132583ff

	Index	Event ID
□	1	806f08132583ff00

   Ignored Problems

   Add event id to the ignore list successfully.

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

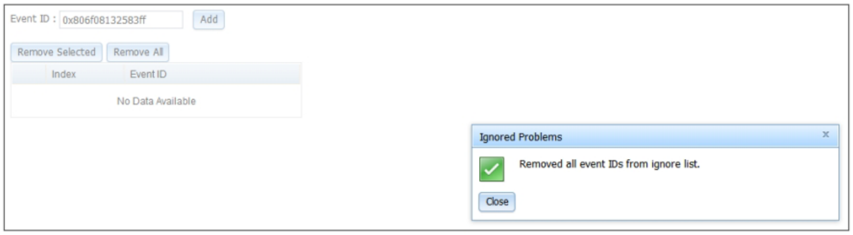
   Event ID : 0x806f08132583ff

   No Data Available

   Ignored Problems

   Removed selected event IDs from ignore list.

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

   Event ID : 0x806f08132583ff

   No Data Available

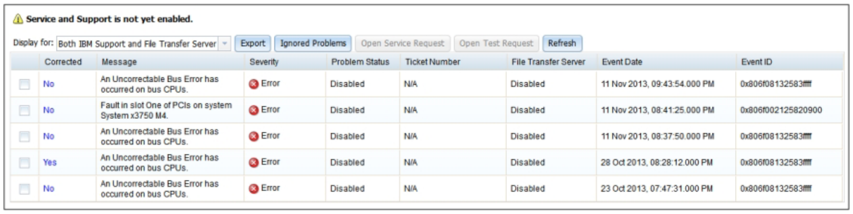
   Ignored Problems

   Removed all event IDs from ignore list.

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 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).



Service and Support is not yet enabled.

Display for: Both IBM Support and File Transfer Server

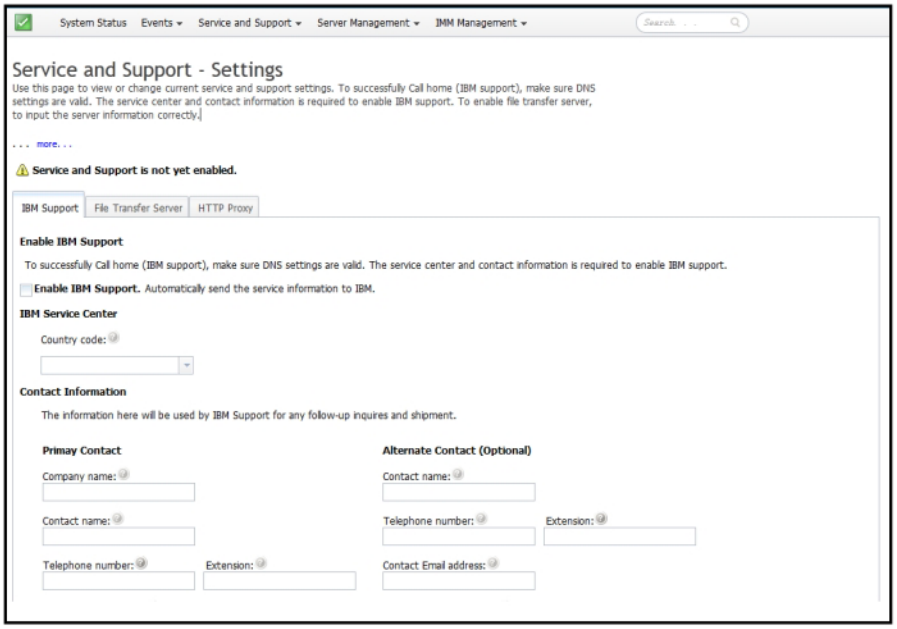
	Corrected	Message	Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 09:43:54.000 PM	0x806f08132583ffff
□	No	Fault in slot One of PCIs on system System x3750 M4.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:41:25.000 PM	0x806f002125820900
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	11 Nov 2013, 08:37:50.000 PM	0x806f08132583ffff
□	Yes	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	28 Oct 2013, 08:28:12.000 PM	0x806f08132583ffff
□	No	An Uncorrectable Bus Error has occurred on bus CPUs.	Error	Disabled	N/A	Disabled	23 Oct 2013, 07:47:31.000 PM	0x806f08132583ffff

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



Service and Support - Settings

Use this page to view or change current service and support settings. To successfully Call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support. To enable file transfer server, to input the server information correctly.

. . . more. . .

Service and Support is not yet enabled.

Enable IBM Support

To successfully Call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support.

□ Enable IBM Support. Automatically send the service information to IBM.

IBM Service Center

Country code:

Contact Information

The information here will be used by IBM Support for any follow-up inquires and shipment.

Primay Contact

Company name:

Contact name:

Telephone number: Extension:

Alternate Contact (Optional)

Contact name:

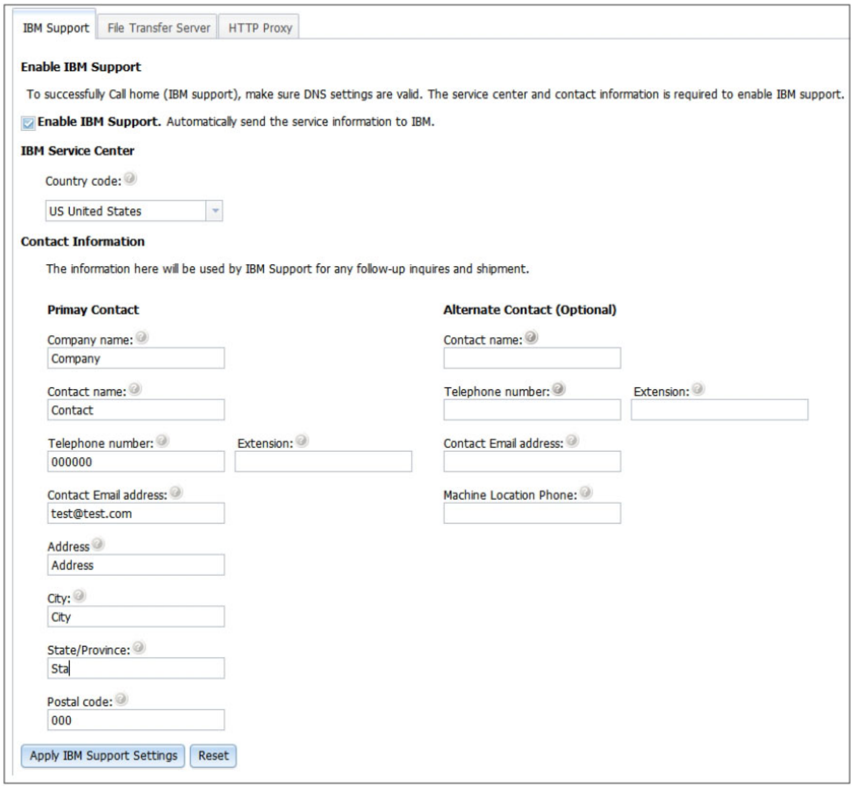
Telephone number: Extension:

Contact Email address:

To allow the service processor to automatically send service information, 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 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.



Enable IBM Support

To successfully Call home (IBM support), make sure DNS settings are valid. The service center and contact information is required to enable IBM support.

☑ **Enable IBM Support.** Automatically send the service information to IBM.

IBM Service Center

Country code: US United States

Contact Information

The information here will be used by IBM Support for any follow-up inquires and shipment.

Primay Contact

Company name: Company

Contact name: Contact

Telephone number: 000000

Extension:

Contact Email address: test@test.com

Address: Address

City: City

State/Province: Sta

Postal code: 000

Alternate Contact (Optional)

Contact name:

Telephone number:

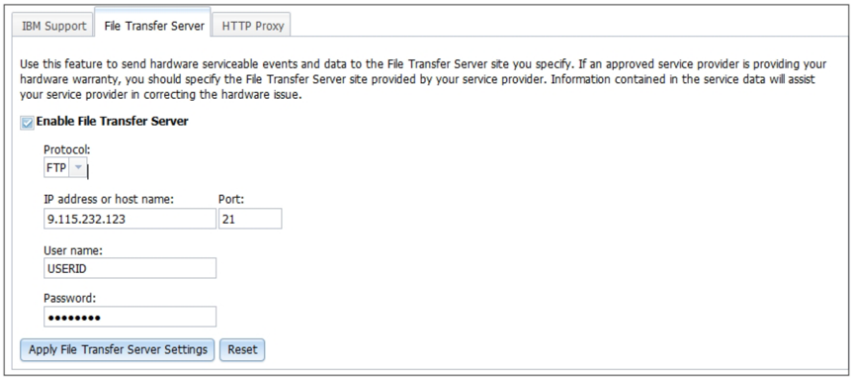
Extension:

Contact Email address:

Machine Location Phone:

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.



Use this feature to send hardware serviceable events and data to the File Transfer Server site you specify. If an approved service provider is providing your hardware warranty, you should specify the File Transfer Server site provided by your service provider. Information contained in the service data will assist your service provider in correcting the hardware issue.

☑ **Enable File Transfer Server**

Protocol: FTP

IP address or host name: 9.115.232.123

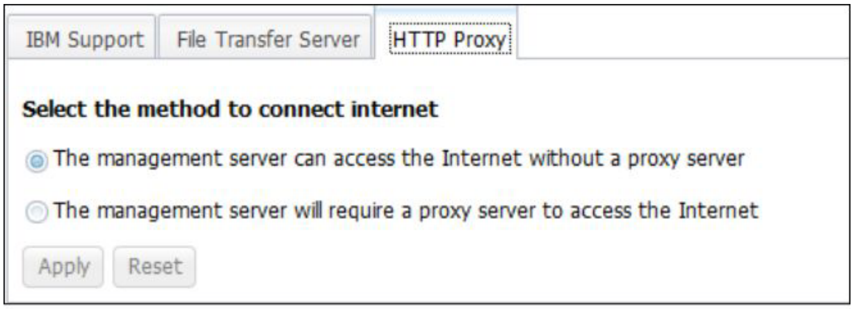
Port: 21

User name: USERID

Password: ••••••••

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



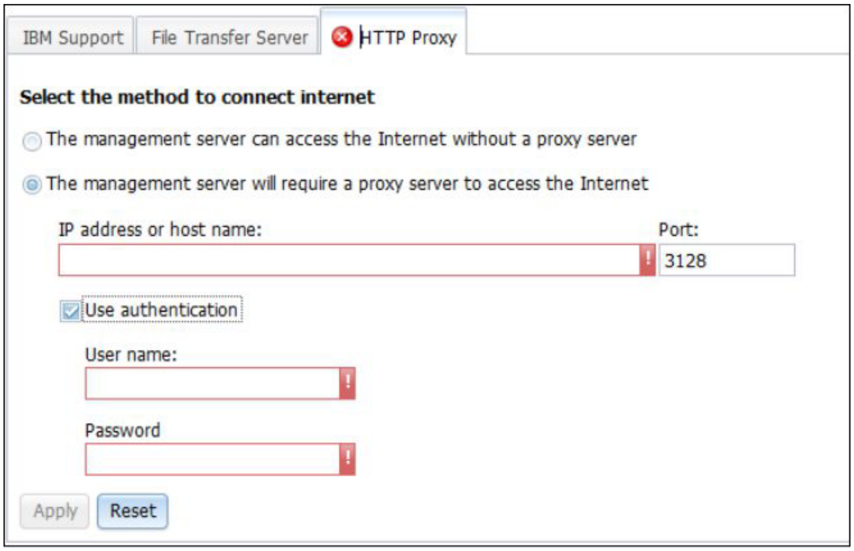
Select the method to connect internet

● 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.



Select the method to connect internet

○ The management server can access the Internet without a proxy server

● The management server will require a proxy server to access the Internet

IP address or host name:

Port: 3128

☑ Use authentication

User name:

Password

4. Click the **Apply** button.

Preparing firewalls and proxies

You must configure the firewalls and proxy server if you have firewalls in your network, or if the management server must use a proxy server to access the internet.

Complete the following steps to configure firewalls and proxies in your network:

1. Identify the ports that you will use in your systems-management environment and ensure that those ports are open before you start installation. For example, you must ensure that the listener ports are open.
2. Ensure that internet connections exist to the following internet addresses.

Note: IP addresses are subject to change, so ensure that you use DNS names whenever possible.

Table 3. Required internet connections

Host name	IP address	Port	Description
eccgw01.boulder.ibm.com	207.25.252.197	443	Electronic Customer Care (ECC) transaction gateway
eccgw02.rochester.ibm.com	129.42.160.51	443	ECC transaction gateway
www.ecurep.ibm.com	192.109.81.20	443	File upload for status reporting and problem reporting
www6.software.ibm.com	170.225.15.41	443	File upload for status reporting and problem reporting. Proxy to testcase.boulder.ibm.com
www-945.ibm.com	129.42.26.224	443	Problem reporting server v4
	129.42.34.224	443	Problem reporting server v4
	129.42.42.224	443	Problem reporting server v4

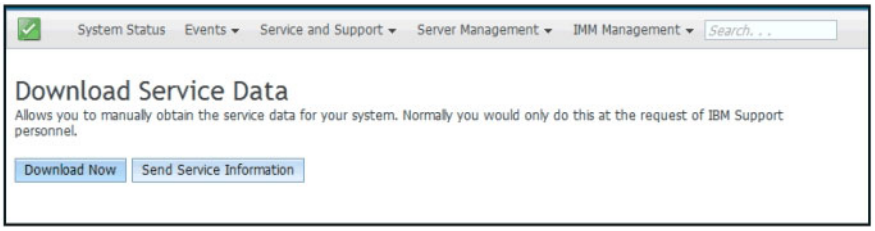
Table 3. Required internet connections (continued)

Host name	IP address	Port	Description
www.ibm.com	129.42.56.216	80, 443	Service provider file (CCF) download
	129.42.58.216	80, 443	Service provider file (CCF) download
	129.42.60.216	80, 443	Service provider file (CCF) download
www-03.ibm.com	204,146,30.17	80, 443	Service provider file (CCF) download

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 Support to assist in problem determination.

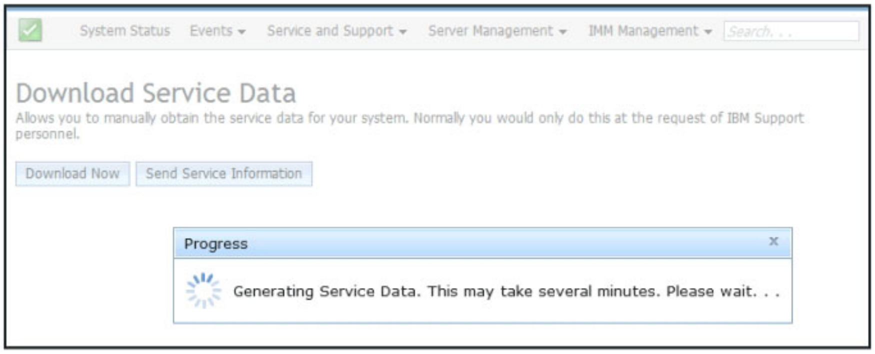
Click the **Download Now** button to download the service and support data (as shown in the following illustration).



Download Service Data

Allows you to manually obtain the service data for your system. Normally you would only do this at the request of IBM Support personnel.

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.



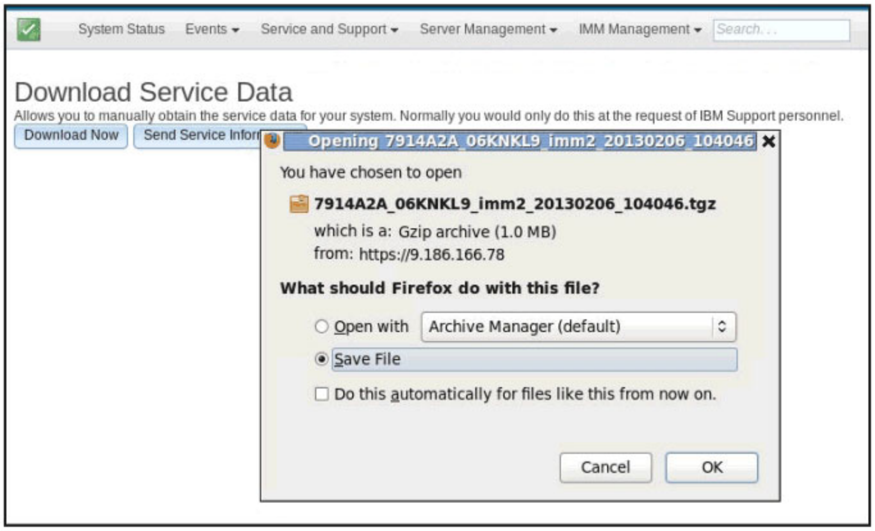
Download Service Data

Allows you to manually obtain the service data for your system. Normally you would only do this at the request of IBM Support personnel.

Progress

Generating Service Data. This may take several minutes. Please wait. . .

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



Download Service Data

Allows you to manually obtain the service data for your system. Normally you would only do this at the request of IBM Support personnel.

Opening 7914A2A_06KNKL9_imm2_20130206_104046

You have chosen to open

7914A2A_06KNKL9_imm2_20130206_104046.tgz

which is a: Gzip archive (1.0 MB)

from: https://9.186.166.78

What should Firefox do with this file?

○ Open with Archive Manager (default)

● Save File

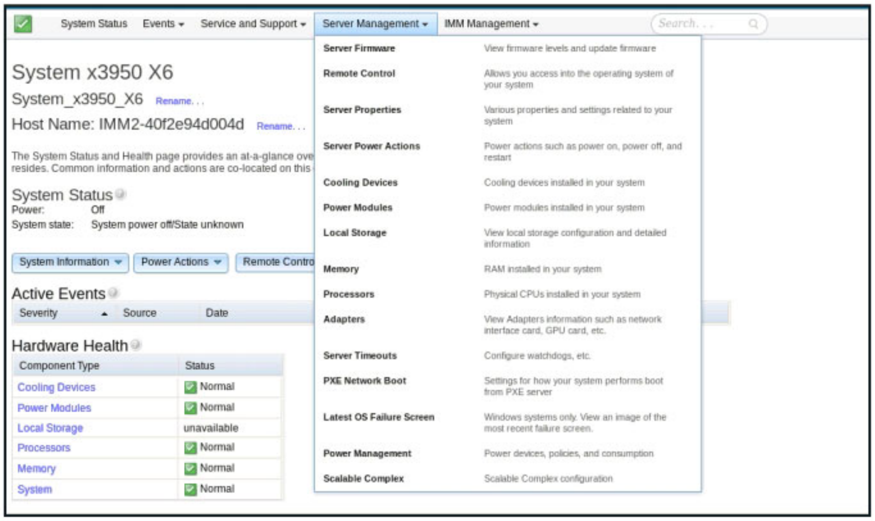
□ Do this automatically for files like this from now on.

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 or perform tasks associated with server firmware status and control, remote control access, server properties status and control, server power actions, cooling devices, power modules, local storage, memory, processors, adapters, server time-outs, PXE network boot, latest OS failure screen, power management, and scalable complex (as shown in the following illustration).

Important: Some options may not be available on your server's operating-system platform. Options that are displayed for the **Server Management** tab are contingent on the server's operating-system platform where the IMM2 is located and the adapters that are installed in the server.



Server Firmware	View firmware levels and update firmware
Remote Control	Allows you access into the operating system of your system
Server Properties	Various properties and settings related to your system
Server Power Actions	Power actions such as power on, power off, and restart
Cooling Devices	Cooling devices installed in your system
Power Modules	Power modules installed in your system
Local Storage	View local storage configuration and detailed information
Memory	RAM installed in your system
Processors	Physical CPUs installed in your system
Adapters	View Adapters information such as network interface card, GPU card, etc.
Server Timeouts	Configure watchdogs, etc.
PXE Network Boot	Settings for how your system performs boot from PXE server
Latest OS Failure Screen	Windows systems only. View an image of the most recent failure screen.
Power Management	Power devices, policies, and consumption
Scalable Complex	Scalable Complex configuration

System x3950 X6

System_x3950_X6

Host Name: IMM2-40f2e94d004d

The System Status and Health page provides an at-a-glance ove
resides. Common information and actions are co-located on this

System Status

Power: Off

System state: System power off/State unknown

Active Events

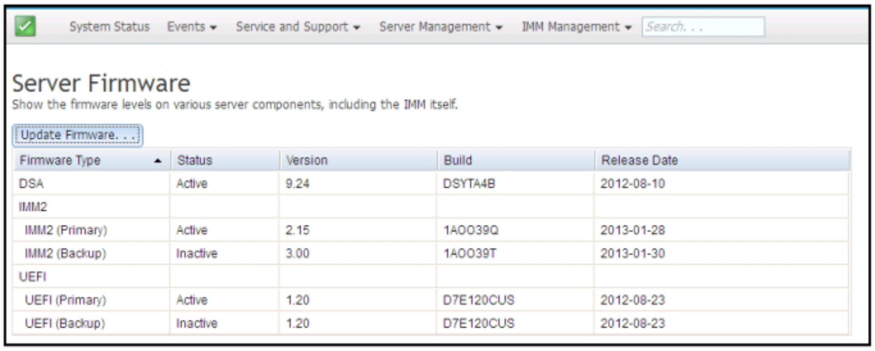
Hardware Health

Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✓ Normal
Local Storage	unavailable
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

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.



Server Firmware

Show the firmware levels on various server components, including the IMM itself.

Firmware Type ▲	Status	Version	Build	Release Date
DSA	Active	9.24	DSYTA4B	2012-08-10
IMM2				
IMM2 (Primary)	Active	2.15	1AOO39Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	1AOO39T	2013-01-30
UEFI				
UEFI (Primary)	Active	1.20	D7E120CUS	2012-08-23
UEFI (Backup)	Inactive	1.20	D7E120CUS	2012-08-23

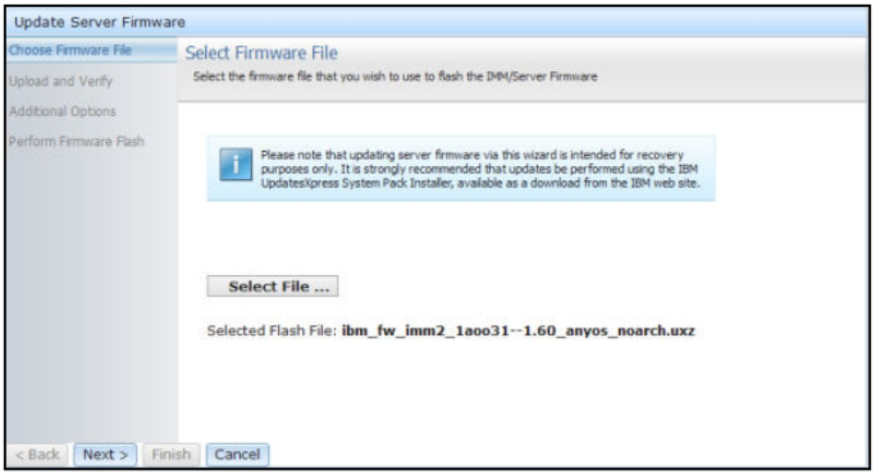
The current status and versions of firmware for the IMM2, UEFI, and DSA are displayed, including the primary and backup versions. There are three categories for the firmware status:

- **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.



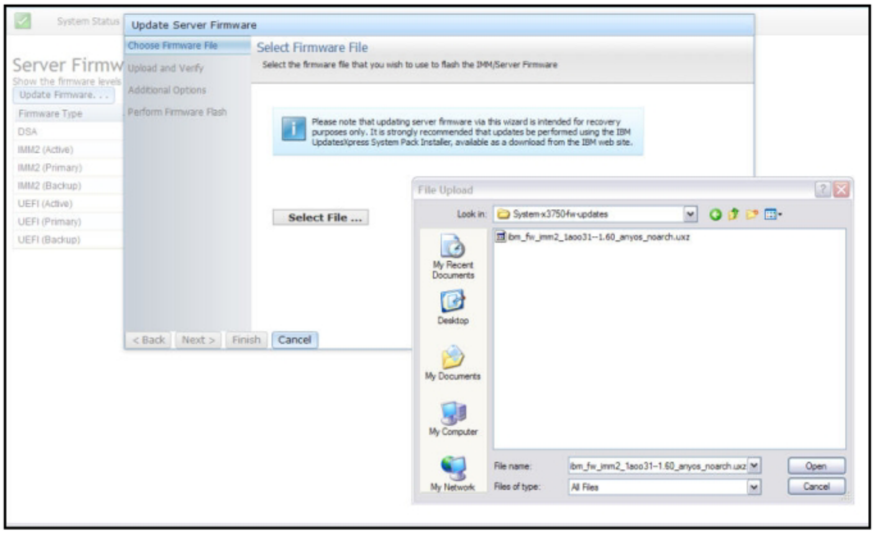
Select Firmware File

Select the firmware file that you wish to use to flash the IMM/Server Firmware

Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM UpdatesXpress System Pack Installer, available as a download from the IBM web site.

Selected Flash File: **ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz**

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



Select the firmware file that you wish to use to flash the IMM/Server Firmware

Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM UpdatesXpress System Pack Installer, available as a download from the IBM web site.

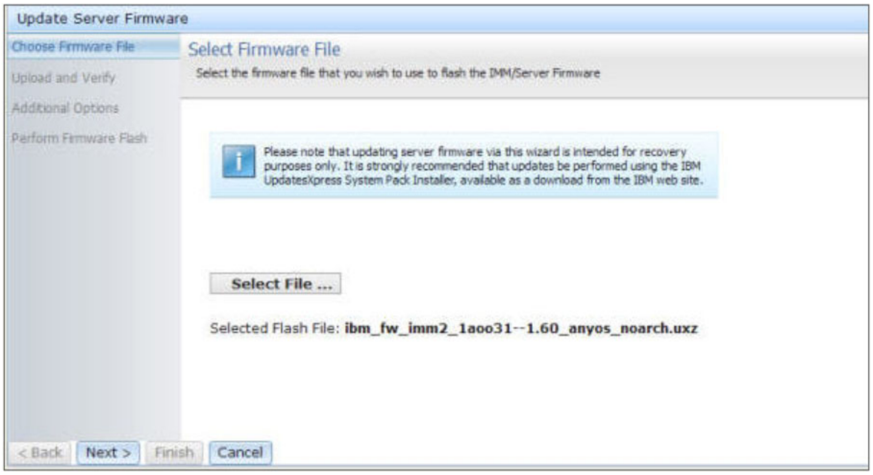
Look in: System-x3750fw-updates

ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz

File name: ibm_fw_imm2_1aoo31-1.60_anyos_noarch.uxz

Files of type: All Files

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).

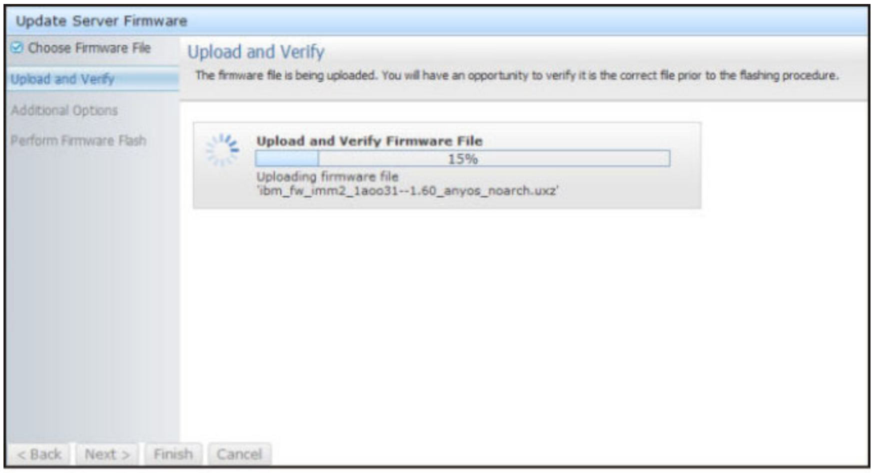


Select the firmware file that you wish to use to flash the IMM/Server Firmware

Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM UpdatesXpress System Pack Installer, available as a download from the IBM web site.

Selected Flash File: **ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz**

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.



Upload and Verify

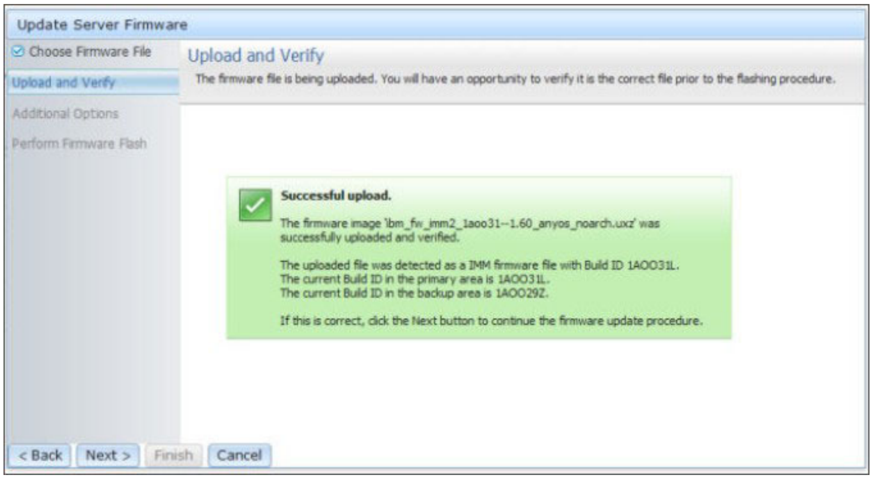
The firmware file is being uploaded. You will have an opportunity to verify it is the correct file prior to the flashing procedure.

Upload and Verify Firmware File

15%

Uploading firmware file
'ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz'

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.



Upload and Verify

The firmware file is being uploaded. You will have an opportunity to verify it is the correct file prior to the flashing procedure.

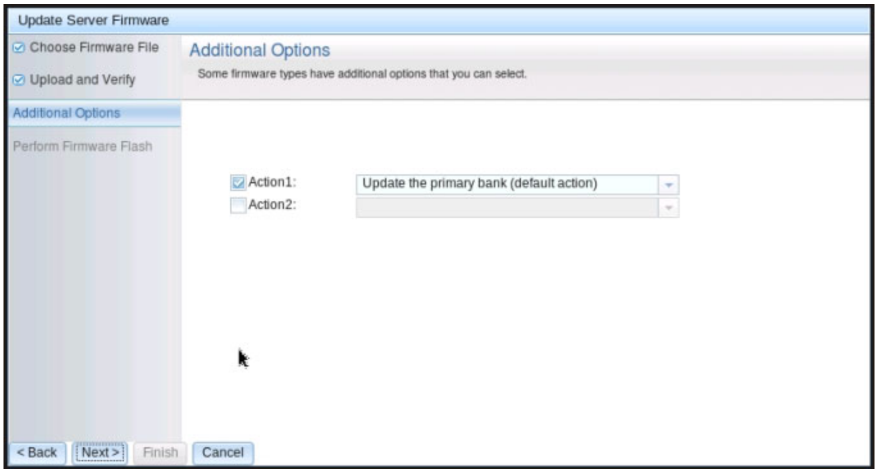
✓ **Successful upload.**

The firmware image 'ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz' was successfully uploaded and verified.

The uploaded file was detected as a IMM firmware file with Build ID 1AOO31L.
The current Build ID in the primary area is 1AOO31L.
The current Build ID in the backup area is 1AOO29Z.

If this is correct, click the Next button to continue the firmware update procedure.

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



Update Server Firmware

☑ Choose Firmware File

☑ Upload and Verify

Additional Options

Perform Firmware Flash

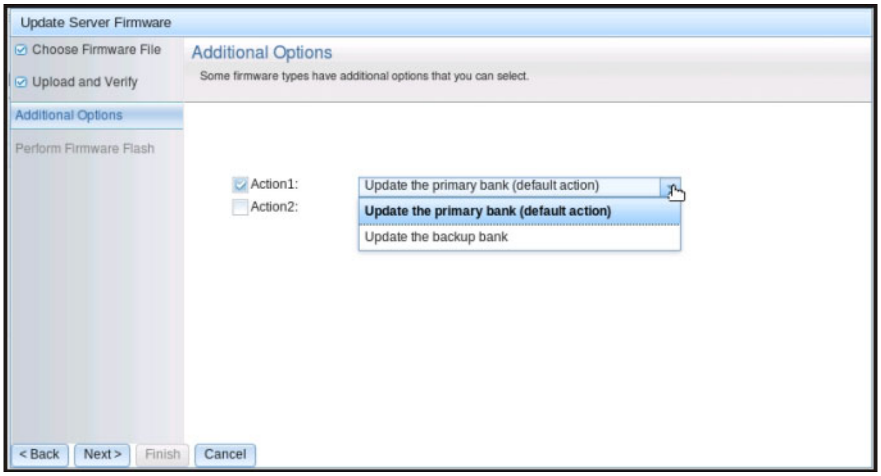
Additional Options

Some firmware types have additional options that you can select.

☑ Action1: Update the primary bank (default action)

□ Action2:

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**.



Update Server Firmware

☑ Choose Firmware File

☑ Upload and Verify

Additional Options

Perform Firmware Flash

Additional Options

Some firmware types have additional options that you can select.

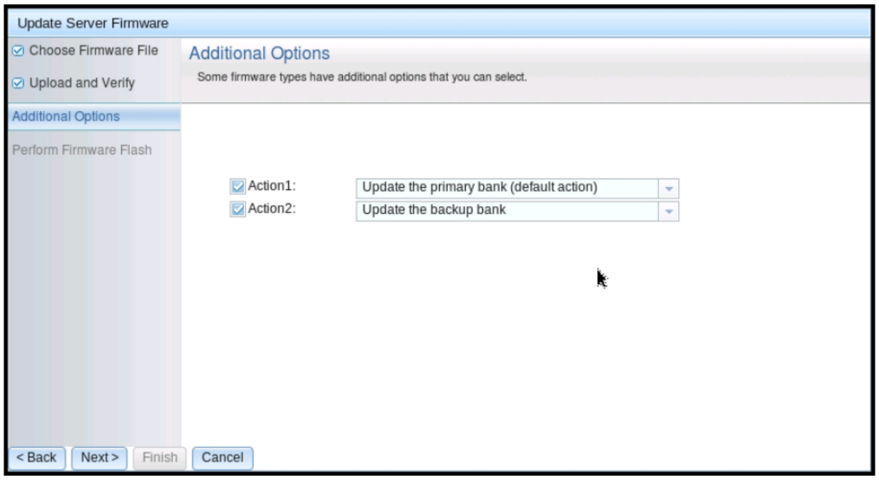
☑ Action1: Update the primary bank (default action)

□ Action2:

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.



Some firmware types have additional options that you can select.

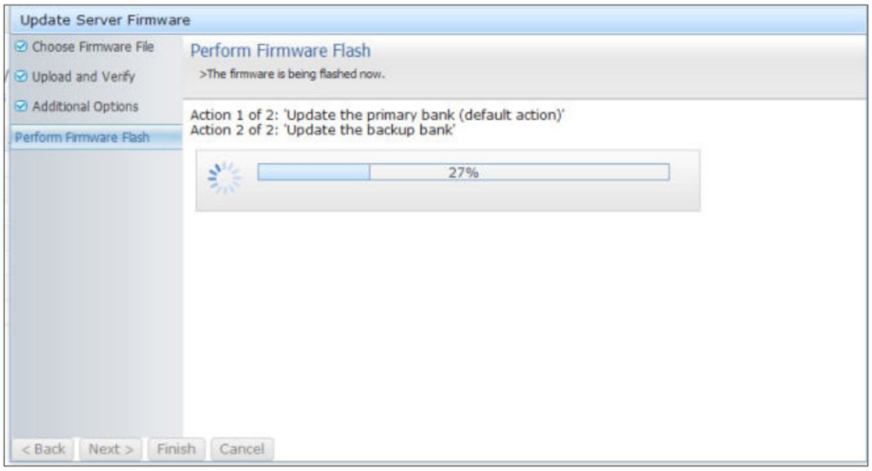
☑ Action1: Update the primary bank (default action)

☑ Action2: Update the backup bank

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.

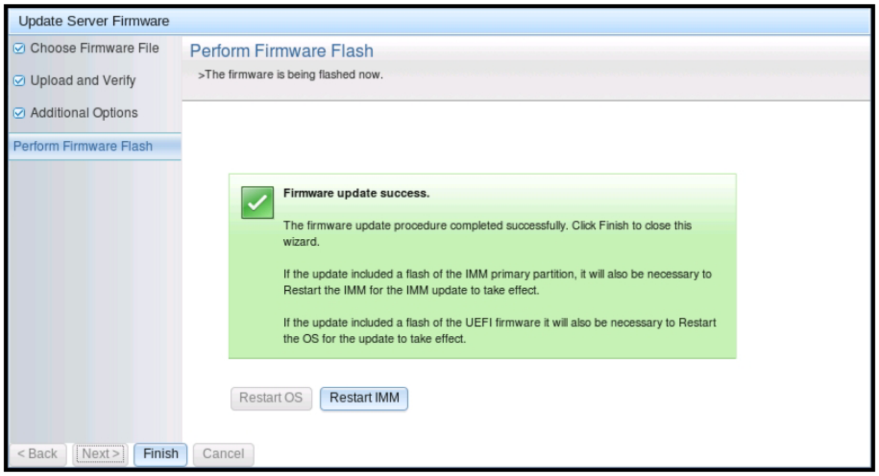
A progress meter is displayed that shows the progress of the firmware update (as shown in the following illustration).



>The firmware is being flashed now.

Action 1 of 2: 'Update the primary bank (default action)'
Action 2 of 2: 'Update the backup bank'

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.



Perform Firmware Flash

>The firmware is being flashed now.

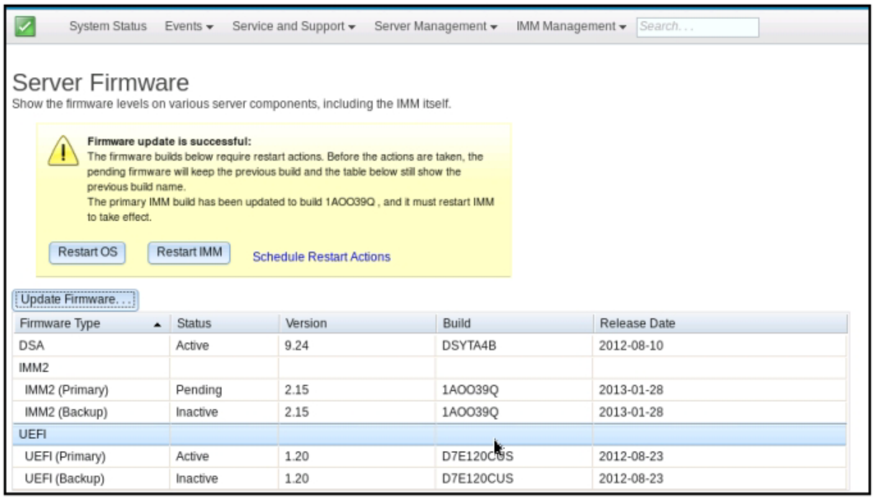
Firmware update success.

The firmware update procedure completed successfully. Click Finish to close this wizard.

If the update included a flash of the IMM primary partition, it will also be necessary to Restart the IMM for the IMM update to take effect.

If the update included a flash of the UEFI firmware it will also be necessary to Restart the OS for the update to take effect.

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



Server Firmware

Show the firmware levels on various server components, including the IMM itself.

Firmware update is successful:

The firmware builds below require restart actions. Before the actions are taken, the pending firmware will keep the previous build and the table below still show the previous build name.

The primary IMM build has been updated to build 1AOO39Q , and it must restart IMM to take effect.

Firmware Type ▲	Status	Version	Build	Release Date
DSA	Active	9.24	DSYTA4B	2012-08-10
IMM2				
IMM2 (Primary)	Pending	2.15	1AOO39Q	2013-01-28
IMM2 (Backup)	Inactive	2.15	1AOO39Q	2013-01-28
UEFI				
UEFI (Primary)	Active	1.20	D7E120CUS	2012-08-23
UEFI (Backup)	Inactive	1.20	D7E120CUS	2012-08-23

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. By using the Virtual Media option you can also mount client devices or images to the host operating system.

Notes:

- The ActiveX client is only available with the Internet Explorer browser.
- To use the Java client, the Java Plug-in 1.7 or later release is required.
- The Java client is compatible with the IBM Java 7 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 menu bar of the Video Viewer window.

  Notes:

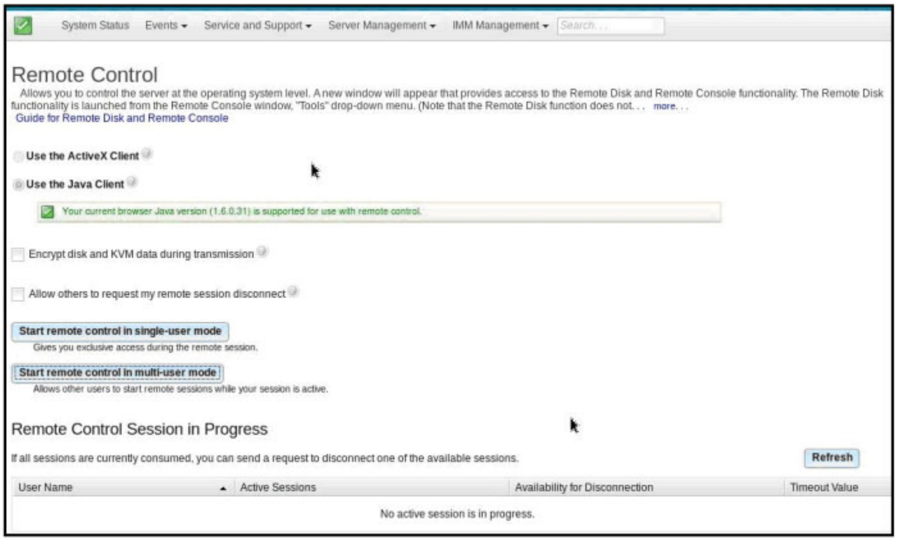
  – The Virtual Media Session can only be used by one remote control session client at a time.

  – 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.



Remote Control

Allows you to control the server at the operating system level. A new window will appear that provides access to the Remote Disk and Remote Console functionality. The Remote Disk functionality is launched from the Remote Console window, "Tools" drop-down menu. (Note that the Remote Disk function does not. . . more. . .

Guide for Remote Disk and Remote Console

○ Use the ActiveX Client

● Use the Java Client

Your current browser Java version (1.6.0.31) is supported for use with remote control.

□ Encrypt disk and KVM data during transmission

□ Allow others to request my remote session disconnect

Start remote control in single-user mode

Gives you exclusive access during the remote session.

Start remote control in multi-user mode

Allows other users to start remote sessions while your session is active.

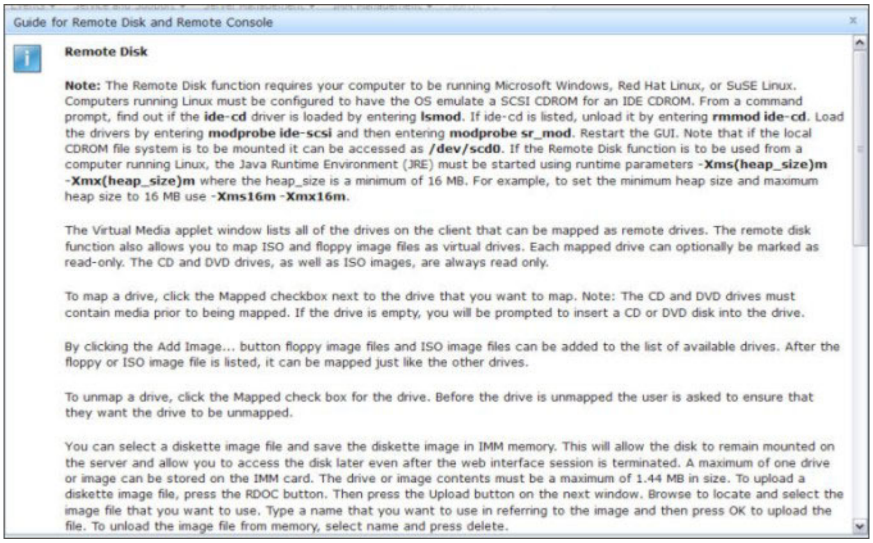
Remote Control Session in Progress

If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.

Refresh

User Name ▲	Active Sessions	Availability for Disconnection	Timeout Value
	No active session is in progress.		

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.



Remote Disk

Note: The Remote Disk function requires your computer to be running Microsoft Windows, Red Hat Linux, or SuSE Linux. Computers running Linux must be configured to have the OS emulate a SCSI CDROM for an IDE CDROM. From a command prompt, find out if the **ide-cd** driver is loaded by entering **lsmod**. If ide-cd is listed, unload it by entering **rmmod ide-cd**. Load the drivers by entering **modprobe ide-scsi** and then entering **modprobe sr_mod**. Restart the GUI. Note that if the local CDROM file system is to be mounted it can be accessed as **/dev/scd0**. If the Remote Disk function is to be used from a computer running Linux, the Java Runtime Environment (JRE) must be started using runtime parameters **-Xms(heap_size)m -Xmx(heap_size)m** where the heap_size is a minimum of 16 MB. For example, to set the minimum heap size and maximum heap size to 16 MB use **-Xms16m -Xmx16m**.

The Virtual Media applet window lists all of the drives on the client that can be mapped as remote drives. The remote disk function also allows you to map ISO and floppy image files as virtual drives. Each mapped drive can optionally be marked as read-only. The CD and DVD drives, as well as ISO images, are always read only.

To map a drive, click the Mapped checkbox next to the drive that you want to map. Note: The CD and DVD drives must contain media prior to being mapped. If the drive is empty, you will be prompted to insert a CD or DVD disk into the drive.

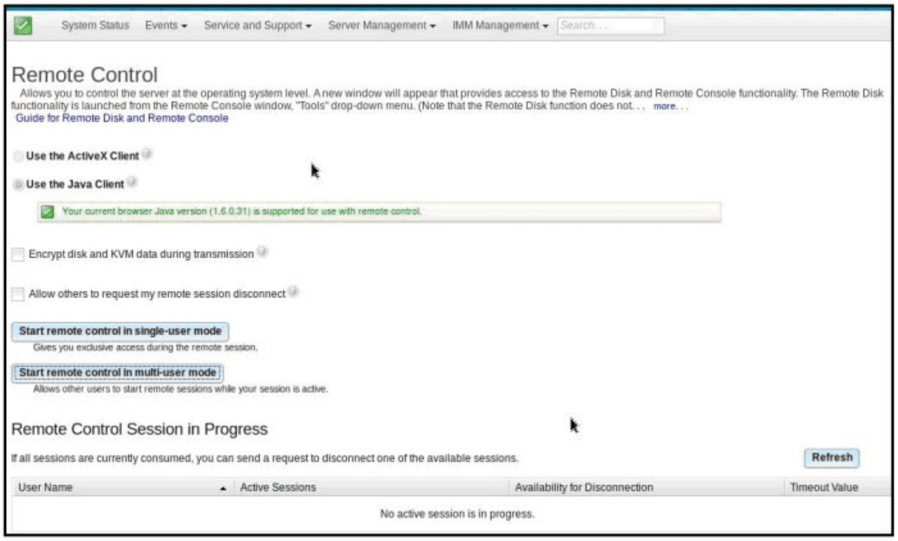
By clicking the Add Image... button floppy image files and ISO image files can be added to the list of available drives. After the floppy or ISO image file is listed, it can be mapped just like the other drives.

To unmap a drive, click the Mapped check box for the drive. Before the drive is unmapped the user is asked to ensure that they want the drive to be unmapped.

You can select a diskette image file and save the diskette image in IMM memory. This will allow the disk to remain mounted on the server and allow you to access the disk later even after the web interface session is terminated. A maximum of one drive or image can be stored on the IMM card. The drive or image contents must be a maximum of 1.44 MB in size. To upload a diskette image file, press the RDOC button. Then press the Upload button on the next window. Browse to locate and select the image file that you want to use. Type a name that you want to use in referring to the image and then press OK to upload the file. To unload the image file from memory, select name and press delete.

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.



Remote Control

Allows you to control the server at the operating system level. A new window will appear that provides access to the Remote Disk and Remote Console functionality. The Remote Disk functionality is launched from the Remote Console window, "Tools" drop-down menu. (Note that the Remote Disk function does not. . . more. . .

Guide for Remote Disk and Remote Console

○ Use the ActiveX Client

● Use the Java Client

Your current browser Java version (1.6.0.31) is supported for use with remote control.

□ Encrypt disk and KVM data during transmission

□ Allow others to request my remote session disconnect

Start remote control in single-user mode
Gives you exclusive access during the remote session.

Start remote control in multi-user mode
Allows other users to start remote sessions while your session is active.

Remote Control Session in Progress

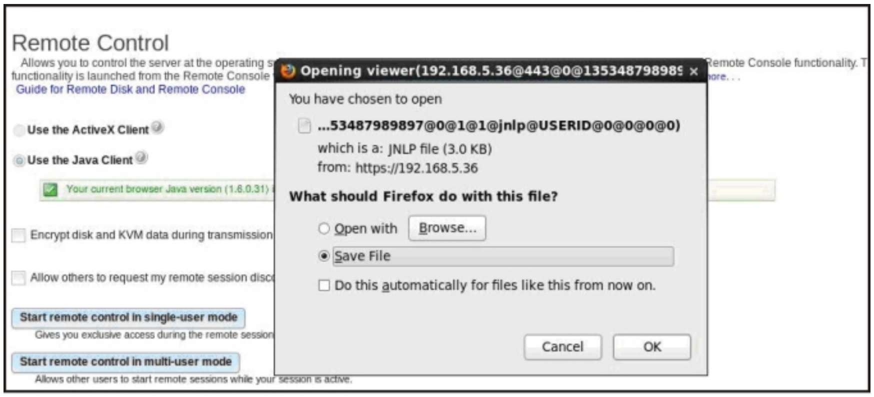
If all sessions are currently consumed, you can send a request to disconnect one of the available sessions. Refresh

User Name	Active Sessions	Availability for Disconnection	Timeout Value
No active session is in progress.			

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.



Remote Control

Allows you to control the server at the operating s

functionality is launched from the Remote Console

Guide for Remote Disk and Remote Console

Remote Console functionality. T

ore. . .

○ Use the ActiveX Client

● Use the Java Client

☑ Your current browser Java version (1.6.0.31)

□ Encrypt disk and KVM data during transmission

□ Allow others to request my remote session disc

Start remote control in single-user mode

Gives you exclusive access during the remote session

Start remote control in multi-user mode

Allows other users to start remote sessions while your session is active.

Opening viewer(192.168.5.36@443@0@13534879898

You have chosen to open

...53487989897@0@1@1@jnlp@USERID@0@0@0@0)

which is a: JNLP file (3.0 KB)

from: https://192.168.5.36

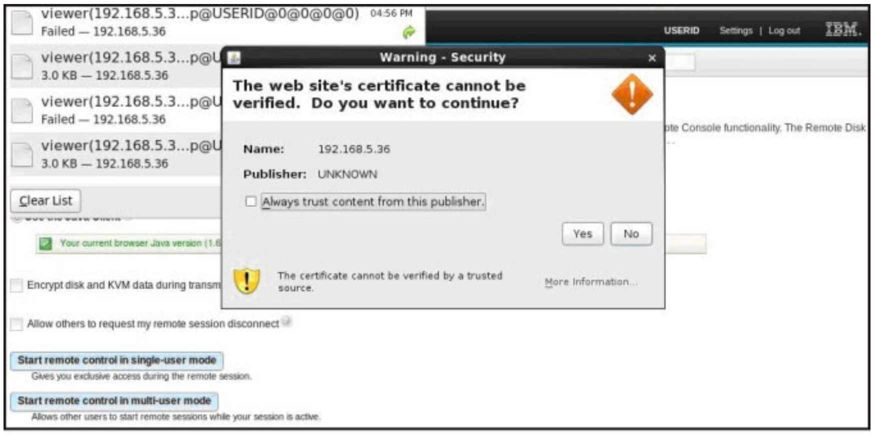
What should Firefox do with this file?

○ Open with Browse...

● Save File

□ Do this automatically for files like this from now on.

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.



viewer(192.168.5.3...p@USERID@0@0@0@0) 04:56 PM

Failed — 192.168.5.36

viewer(192.168.5.3...p@U

3.0 KB — 192.168.5.36

viewer(192.168.5.3...p@U

Failed — 192.168.5.36

viewer(192.168.5.3...p@U

3.0 KB — 192.168.5.36

ote Console functionality. The Remote Disk

☑ Your current browser Java version (1.6

□ Encrypt disk and KVM data during transm

□ Allow others to request my remote session disconnect

Start remote control in single-user mode

Gives you exclusive access during the remote session.

Start remote control in multi-user mode

Allows other users to start remote sessions while your session is active.

Warning - Security

The web site's certificate cannot be verified. Do you want to continue?

Name: 192.168.5.36

Publisher: UNKNOWN

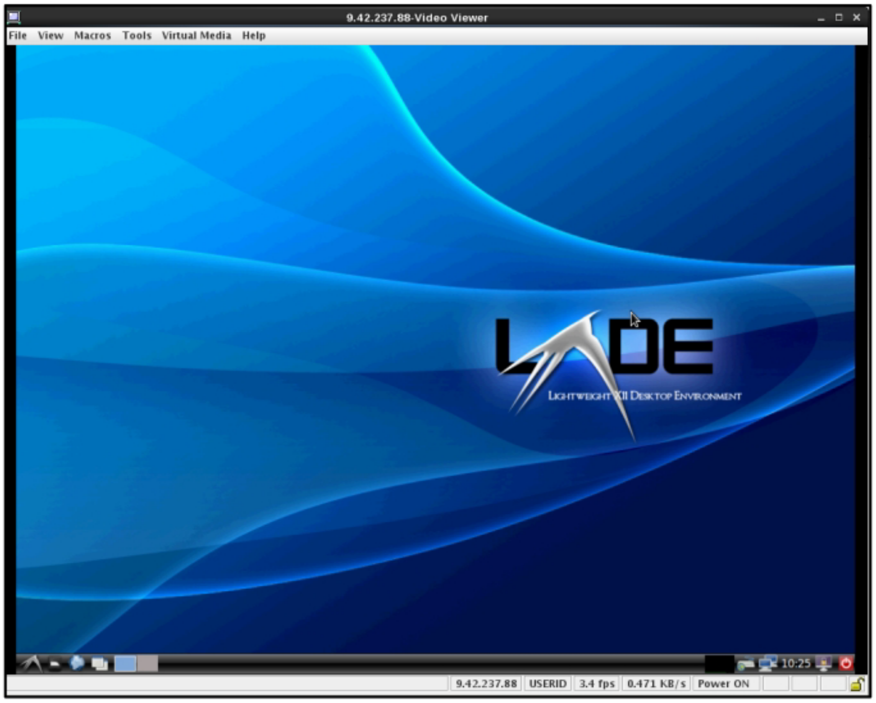
□ Always trust content from this publisher.

The certificate cannot be verified by a trusted source.

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 AES encryption during the session.

   The Video Viewer window opens as (shown in the following illustration). The Video Viewer window provides access to the Remote Console functionality and is comprised of a frame, menu bar, and the content area.


9.42.237.88-Video Viewer
File View Macros Tools Virtual Media Help
LXDE
Lightweight X11 Desktop Environment
10:25
9.42.237.88
USERID
3.4 fps
0.471 KB/s
Power ON

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

Notes:

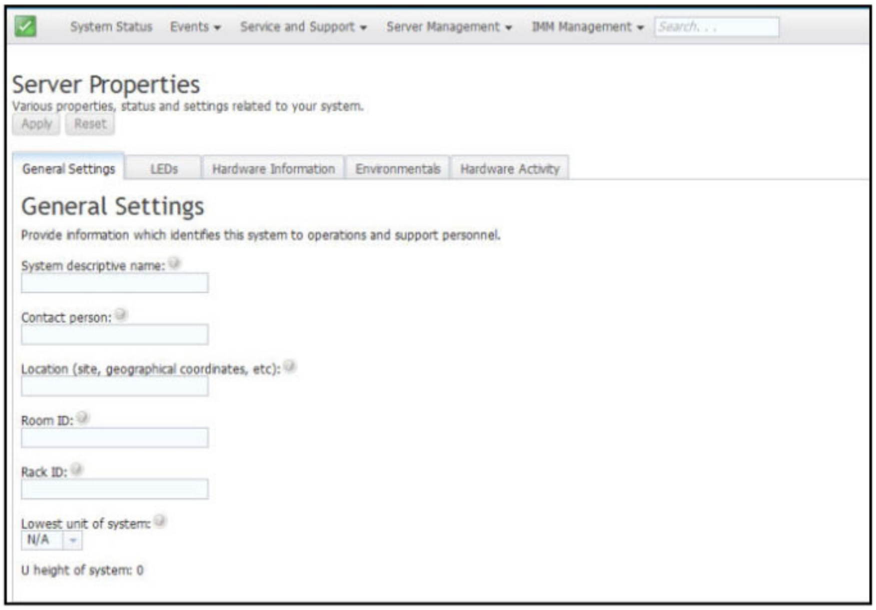
- The Video Viewer will automatically close the Virtual Media Session window.
- Do *not* close the Virtual Media Session window if a remote disk is currently mapped. See "Remote disk" on page 139 for instructions about closing and unmapping a remote disk.
- If you have mouse or keyboard problems when 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.

For more information about updating IMM2 firmware, see "Updating the server firmware" on page 144.

For more information about the remote control feature, see "Remote presence and remote control functions" on page 123.

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**.



Server Properties

Various properties, status and settings related to your system.

General Settings

Provide information which identifies this system to operations and support personnel.

System descriptive name:

Contact person:

Location (site, geographical coordinates, etc):

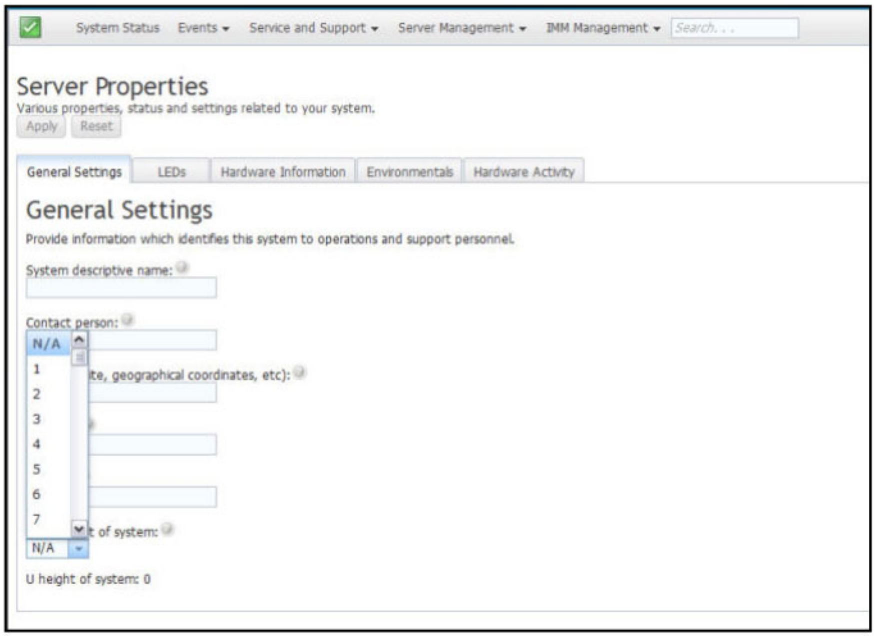
Room ID:

Rack ID:

Lowest unit of system: N/A

U height of system: 0

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 CMM).



Server Properties

Various properties, status and settings related to your system.

General Settings

Provide information which identifies this system to operations and support personnel.

System descriptive name:

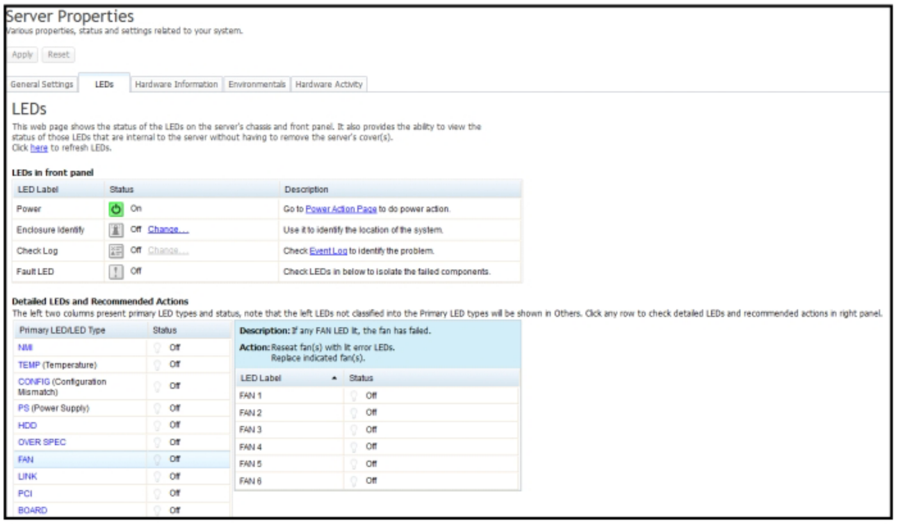
Contact person:

Location (site, geographical coordinates, etc):

Lowest unit of system: N/A

U height of system: 0

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



Server Properties

Various properties, status and settings related to your system.

LEDs

This web page shows the status of the LEDs on the server's chassis and front panel. It also provides the ability to view the status of those LEDs that are internal to the server without having to remove the server's cover(s).
Click here to refresh LEDs.

LEDs in front panel

LED Label	Status	Description
Power	On	Go to Power Action Page to do power action.
Enclosure Identify	Off Change...	Use it to identify the location of the system.
Check Log	Off Change...	Check Event Log to identify the problem.
Fault LED	Off	Check LEDs in below to isolate the failed components.

Detailed LEDs and Recommended Actions

The left two columns present primary LED types and status, note that the left LEDs not classified into the Primary LED types will be shown in Others. Click any row to check detailed LEDs and recommended actions in right panel.

Primary LED/LED Type	Status
NMI	Off
TEMP (Temperature)	Off
CONFIG (Configuration Mismatch)	Off
PS (Power Supply)	Off
HDD	Off
OVER SPEC	Off
FAN	Off
LINK	Off
PCI	Off
BOARD	Off

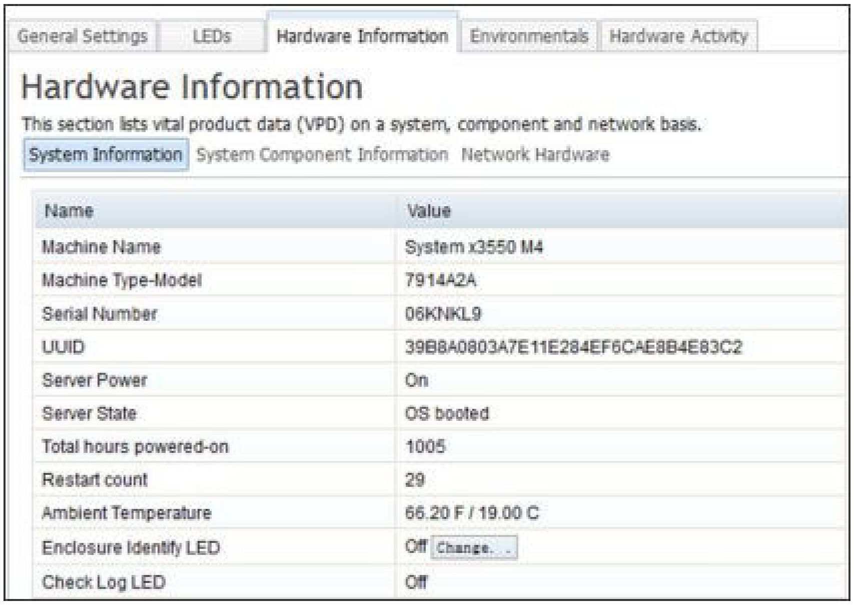
Description: If any FAN LED lit, the fan has failed.

Action: Reseat fan(s) with lit error LEDs.
Replace indicated fan(s).

LED Label ▲	Status
FAN 1	Off
FAN 2	Off
FAN 3	Off
FAN 4	Off
FAN 5	Off
FAN 6	Off

To view system information, system component information, and network hardware information, click the **Hardware Information** tab. You can also select the appropriate sub-tab within the **Hardware Information** tab to view various Vital Product Data (VPD) information.

The **System Information** sub-tab provides information such as the machine name, serial number, and model. The following illustration shows the System Information window.



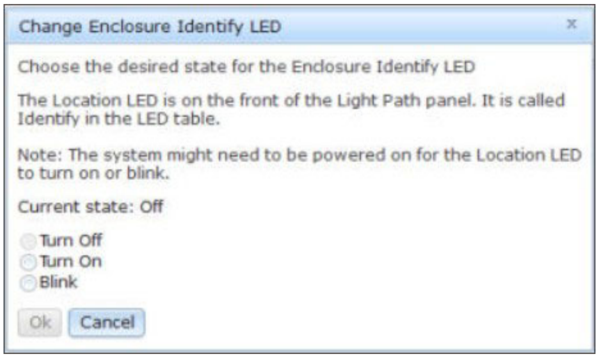
Hardware Information

This section lists vital product data (VPD) on a system, component and network basis.

Name	Value
Machine Name	System x3550 M4
Machine Type-Model	7914A2A
Serial Number	06KNKL9
UUID	39B8A0803A7E11E284EF6CAE8B4E83C2
Server Power	On
Server State	OS booted
Total hours powered-on	1005
Restart count	29
Ambient Temperature	66.20 F / 19.00 C
Enclosure Identify LED	Off Change...
Check Log LED	Off

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.



Change Enclosure Identify LED

Choose the desired state for the Enclosure Identify LED

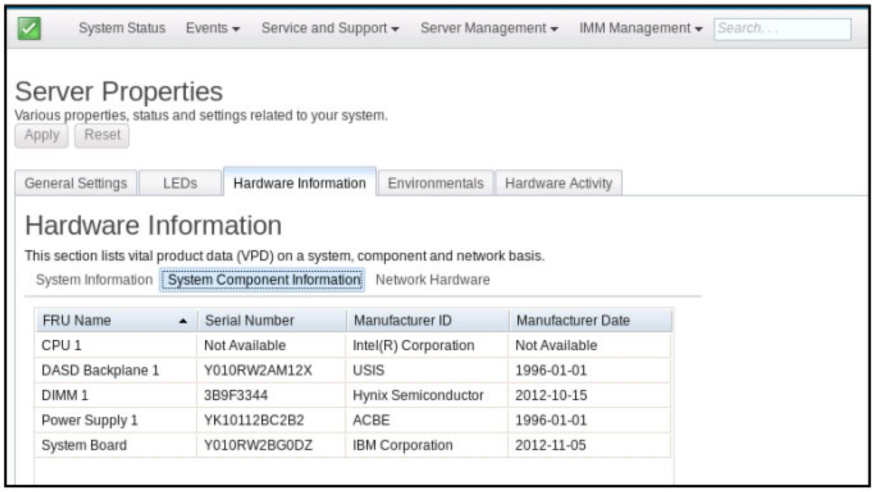
The Location LED is on the front of the Light Path panel. It is called Identify in the LED table.

Note: The system might need to be powered on for the Location LED to turn on or blink.

Current state: Off

○ Turn Off
○ Turn On
○ Blink

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



Server Properties

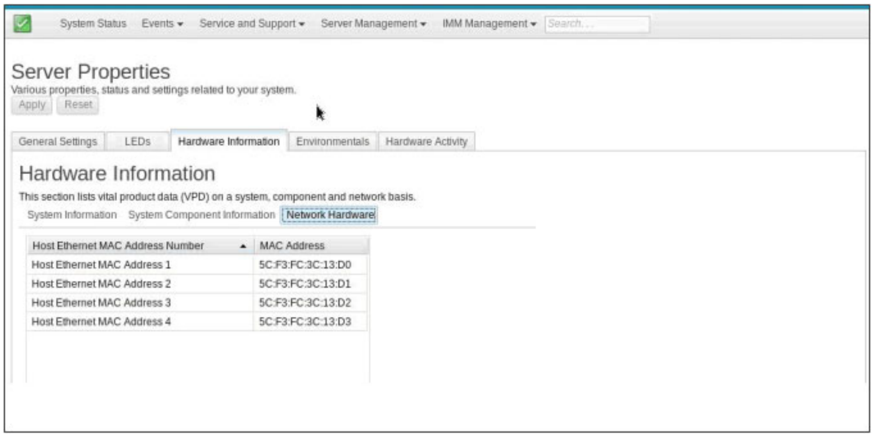
Various properties, status and settings related to your system.

Hardware Information

This section lists vital product data (VPD) on a system, component and network basis.

FRU Name	Serial Number	Manufacturer ID	Manufacturer Date
CPU 1	Not Available	Intel(R) Corporation	Not Available
DASD Backplane 1	Y010RW2AM12X	USIS	1996-01-01
DIMM 1	3B9F3344	Hynix Semiconductor	2012-10-15
Power Supply 1	YK10112BC2B2	ACBE	1996-01-01
System Board	Y010RW2BG0DZ	IBM Corporation	2012-11-05

Select the **Network Hardware** sub-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.



Server Properties

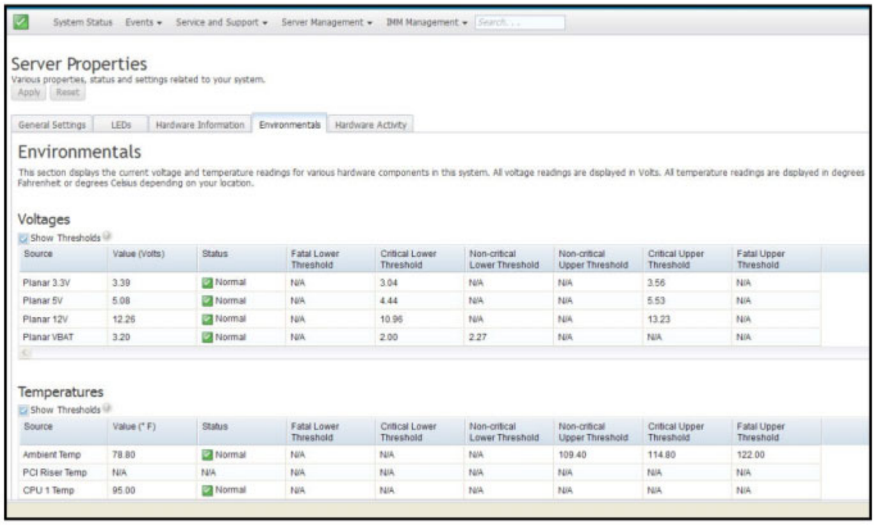
Various properties, status and settings related to your system.

Hardware Information

This section lists vital product data (VPD) on a system, component and network basis.

Host Ethernet MAC Address Number ▲	MAC Address
Host Ethernet MAC Address 1	5C:F3:FC:3C:13:D0
Host Ethernet MAC Address 2	5C:F3:FC:3C:13:D1
Host Ethernet MAC Address 3	5C:F3:FC:3C:13:D2
Host Ethernet MAC Address 4	5C:F3:FC:3C:13:D3

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.



Server Properties

Various properties, status and settings related to your system.

Environmentals

This section displays the current voltage and temperature readings for various hardware components in this system. All voltage readings are displayed in Volts. All temperature readings are displayed in degrees Fahrenheit or degrees Celsius depending on your location.

Voltages

☑ Show Thresholds

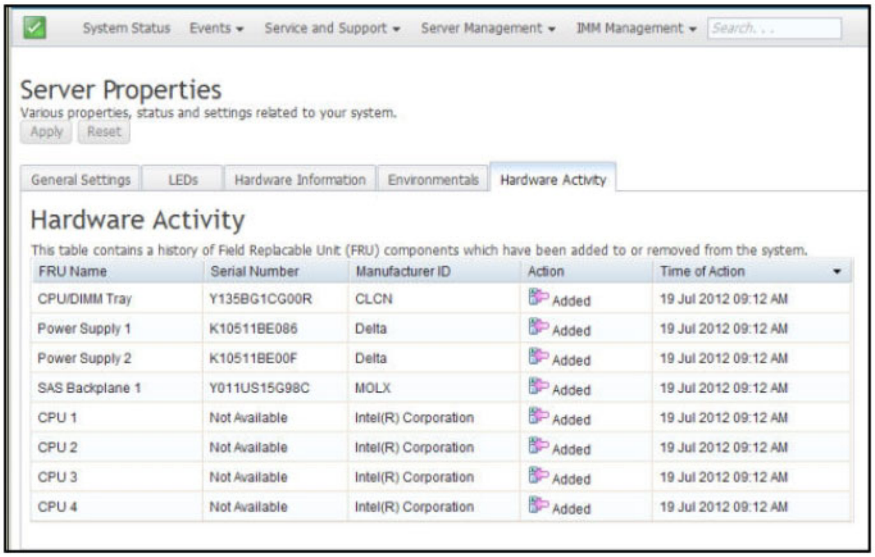
Source	Value (Volts)	Status	Fatal Lower Threshold	Critical Lower Threshold	Non-critical Lower Threshold	Non-critical Upper Threshold	Critical Upper Threshold	Fatal Upper Threshold
Planar 3.3V	3.39	✓ Normal	N/A	3.04	N/A	N/A	3.56	N/A
Planar 5V	5.08	✓ Normal	N/A	4.44	N/A	N/A	5.53	N/A
Planar 12V	12.26	✓ Normal	N/A	10.96	N/A	N/A	13.23	N/A
Planar VBAT	3.20	✓ Normal	N/A	2.00	2.27	N/A	N/A	N/A

Temperatures

☑ Show Thresholds

Source	Value (° F)	Status	Fatal Lower Threshold	Critical Lower Threshold	Non-critical Lower Threshold	Non-critical Upper Threshold	Critical Upper Threshold	Fatal Upper Threshold
Ambient Temp	78.80	✓ Normal	N/A	N/A	N/A	109.40	114.80	122.00
PCI Riser Temp	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CPU 1 Temp	95.00	✓ Normal	N/A	N/A	N/A	N/A	N/A	N/A

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 Properties

Various properties, status and settings related to your system.

Hardware Activity

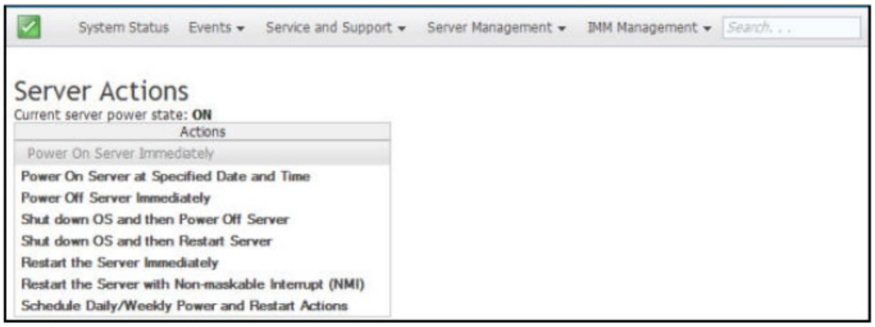
This table contains a history of Field Replacable Unit (FRU) components which have been added to or removed from the system.

FRU Name	Serial Number	Manufacturer ID	Action	Time of Action
CPU/DIMM Tray	Y135BG1CG00R	CLCN	Added	19 Jul 2012 09:12 AM
Power Supply 1	K10511BE086	Delta	Added	19 Jul 2012 09:12 AM
Power Supply 2	K10511BE00F	Delta	Added	19 Jul 2012 09:12 AM
SAS Backplane 1	Y011US15G98C	MOLX	Added	19 Jul 2012 09:12 AM
CPU 1	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 2	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 3	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM
CPU 4	Not Available	Intel(R) Corporation	Added	19 Jul 2012 09:12 AM

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.


System Status
Events
Service and Support
Server Management
IMM Management
Search. . .
Actions
Power On Server Immediately
Power On Server at Specified Date and Time
Power Off Server Immediately
Shut down OS and then Power Off Server
Shut down OS and then Restart Server
Restart the Server Immediately
Restart the Server with Non-maskable Interrupt (NMI)
Schedule Daily/Weekly Power and Restart Actions

Server Actions

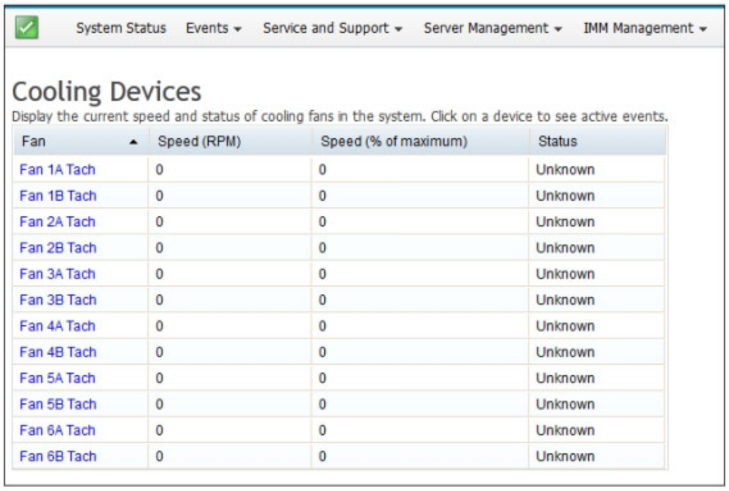
Current server power state: **ON**

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 122.

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).

Note: In a Flex System, cooling device settings are managed by a Flex System CMM and cannot be modified on the IMM2.

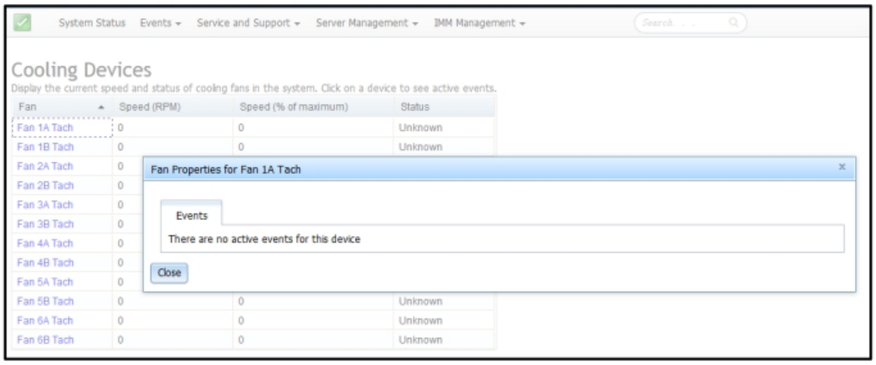


Cooling Devices

Display the current speed and status of cooling fans in the system. Click on a device to see active events.

Fan	Speed (RPM)	Speed (% of maximum)	Status
Fan 1A Tach	0	0	Unknown
Fan 1B Tach	0	0	Unknown
Fan 2A Tach	0	0	Unknown
Fan 2B Tach	0	0	Unknown
Fan 3A Tach	0	0	Unknown
Fan 3B Tach	0	0	Unknown
Fan 4A Tach	0	0	Unknown
Fan 4B Tach	0	0	Unknown
Fan 5A Tach	0	0	Unknown
Fan 5B Tach	0	0	Unknown
Fan 6A Tach	0	0	Unknown
Fan 6B Tach	0	0	Unknown

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



Cooling Devices

Display the current speed and status of cooling fans in the system. Click on a device to see active events.

Fan	Speed (RPM)	Speed (% of maximum)	Status
Fan 1A Tach	0	0	Unknown
Fan 1B Tach	0	0	Unknown
Fan 2A Tach	0		
Fan 2B Tach	0		
Fan 3A Tach	0		
Fan 3B Tach	0		
Fan 4A Tach	0		
Fan 4B Tach	0		
Fan 5A Tach	0		
Fan 5B Tach	0	0	Unknown
Fan 6A Tach	0	0	Unknown
Fan 6B Tach	0	0	Unknown

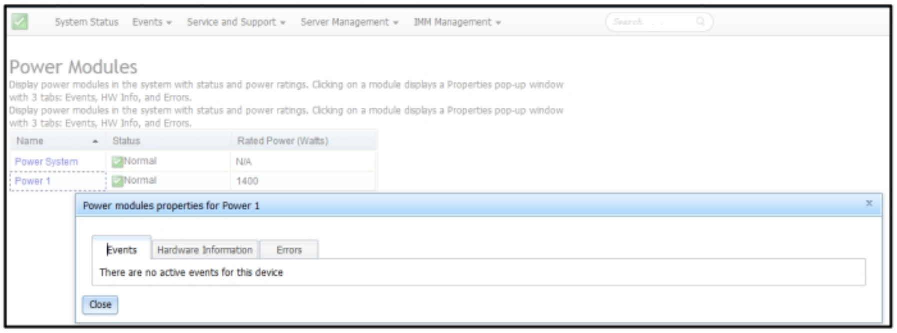
Fan Properties for Fan 1A Tach

There are no active events for this device

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).

Note: In a Flex System, power module settings are managed by a Flex System CMM and cannot be modified on the IMM2.



Power Modules

Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.

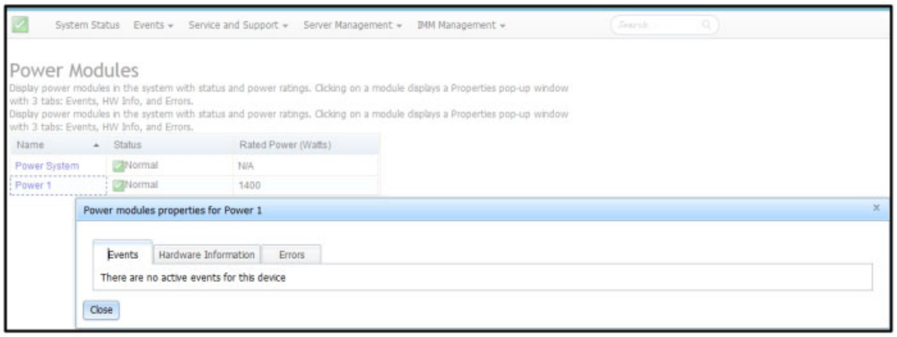
Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.

Name	Status	Rated Power (Watts)
Power System	✓ Normal	N/A
Power 1	✓ Normal	1400

Power modules properties for Power 1

There are no active events for this device

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



Power Modules

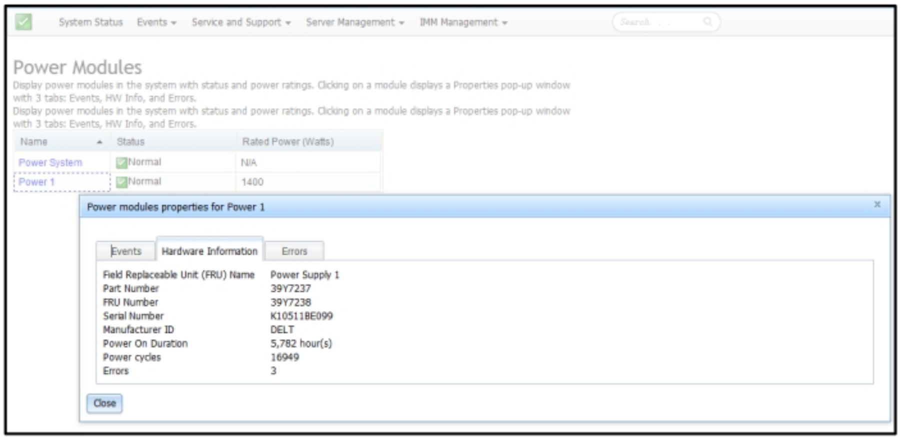
Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.
Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.

Name	Status	Rated Power (Watts)
Power System	✓ Normal	N/A
Power 1	✓ Normal	1400

Power modules properties for Power 1

There are no active events for this device

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).



Power Modules

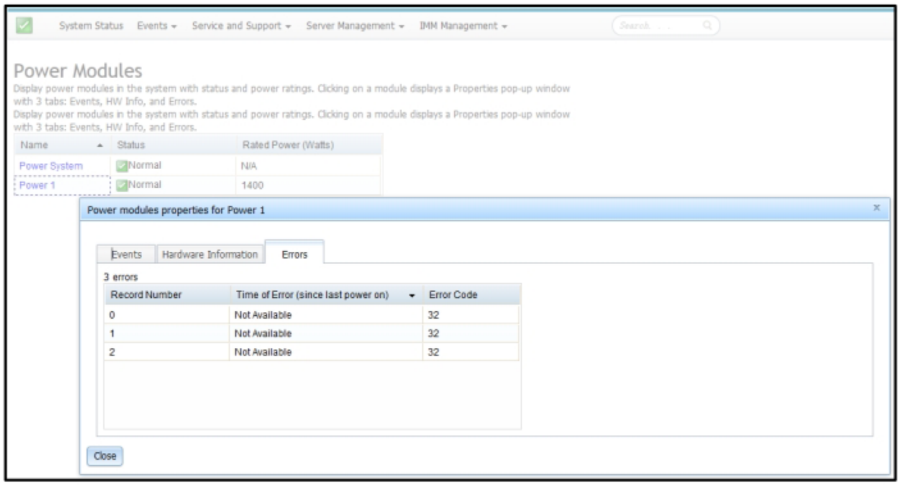
Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.
Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.

Name	Status	Rated Power (Watts)
Power System	✓ Normal	N/A
Power 1	✓ Normal	1400

Power modules properties for Power 1

Field Replaceable Unit (FRU) Name	Power Supply 1
Part Number	39Y7237
FRU Number	39Y7238
Serial Number	K10511BE099
Manufacturer ID	DELT
Power On Duration	5,782 hour(s)
Power cycles	16949
Errors	3

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



Power Modules

Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.
Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.

Name	Status	Rated Power (Watts)
Power System	✓ Normal	N/A
Power 1	✓ Normal	1400

Power modules properties for Power 1

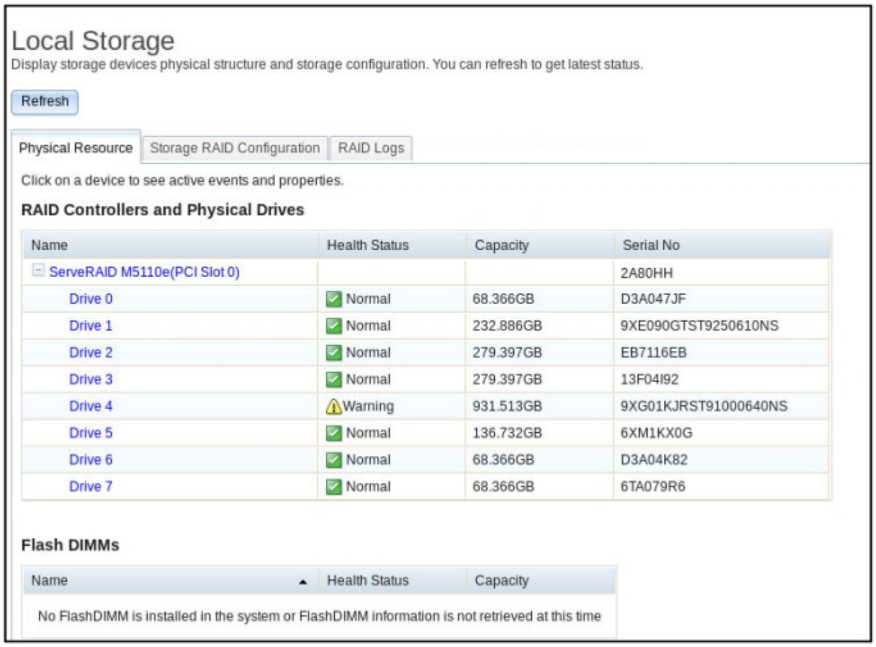
3 errors

Record Number	Time of Error (since last power on)	Error Code
0	Not Available	32
1	Not Available	32
2	Not Available	32

Local storage

Select the **Local Storage** option under the **Server Management** tab or the Local Storage link in the Hardware Health table on the System Status and Health page to view the local storage configuration information for the server. This option provides detailed information for the local storage devices in the server (as shown in the following illustration). You can view the physical or logical information for the local storage devices. Information is provided for supported RAID controllers and associated disks, storage pools, and volume information.

Note: If the operating-system platform does not support the **Local Storage** option, only the status of the disks and associated active events are displayed.



Local Storage

Display storage devices physical structure and storage configuration. You can refresh to get latest status.

Click on a device to see active events and properties.

RAID Controllers and Physical Drives

Name	Health Status	Capacity	Serial No
⊟ ServeRAID M5110e(PCI Slot 0)			2A80HH
Drive 0	✓ Normal	68.366GB	D3A047JF
Drive 1	✓ Normal	232.886GB	9XE090GTST9250610NS
Drive 2	✓ Normal	279.397GB	EB7116EB
Drive 3	✓ Normal	279.397GB	13F04I92
Drive 4	⚠ Warning	931.513GB	9XG01KJRST91000640NS
Drive 5	✓ Normal	136.732GB	6XM1KX0G
Drive 6	✓ Normal	68.366GB	D3A04K82
Drive 7	✓ Normal	68.366GB	6TA079R6

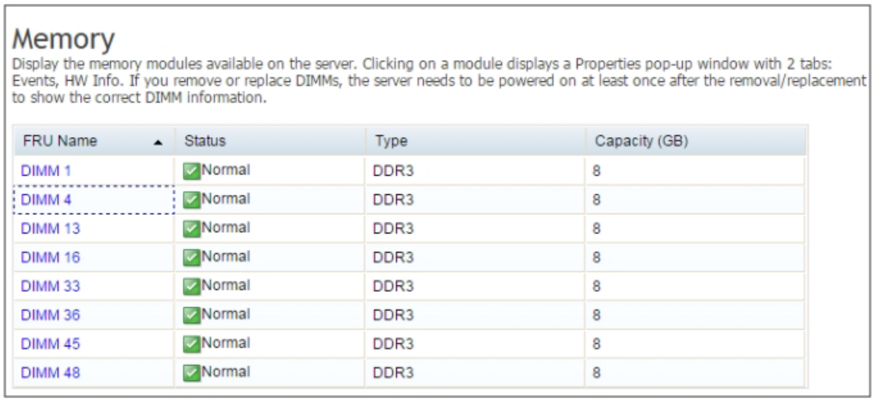
Flash DIMMs

Name ▲	Health Status	Capacity
No FlashDIMM is installed in the system or FlashDIMM information is not retrieved at this time		

Memory

Select the **Memory** option under the **Server Management** tab to view information about the memory modules installed in the system. A page similar to the following illustration is displayed. 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.

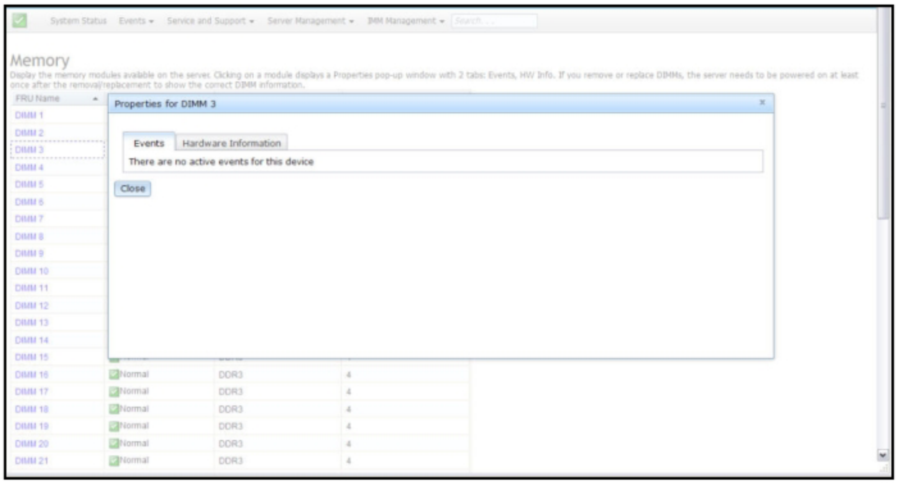


Memory

Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Events, HW Info. If you remove or replace DIMMs, the server needs to be powered on at least once after the removal/replacement to show the correct DIMM information.

FRU Name ▲	Status	Type	Capacity (GB)
DIMM 1	✓ Normal	DDR3	8
DIMM 4	✓ Normal	DDR3	8
DIMM 13	✓ Normal	DDR3	8
DIMM 16	✓ Normal	DDR3	8
DIMM 33	✓ Normal	DDR3	8
DIMM 36	✓ Normal	DDR3	8
DIMM 45	✓ Normal	DDR3	8
DIMM 48	✓ Normal	DDR3	8

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).



Memory

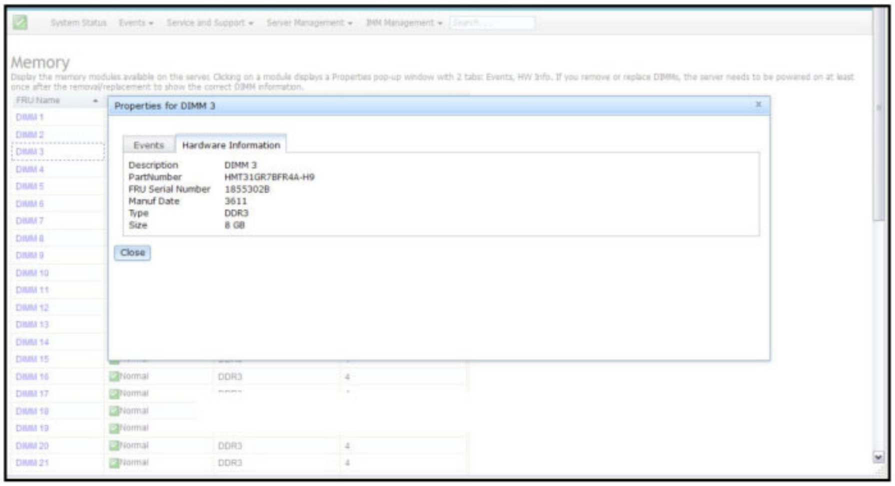
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Events, HW Info. If you remove or replace DIMMs, the server needs to be powered on at least once after the removal/replacement to show the correct DIMM information.

Properties for DIMM 3

There are no active events for this device

FRU Name			
DIMM 1			
DIMM 2			
DIMM 3			
DIMM 4			
DIMM 5			
DIMM 6			
DIMM 7			
DIMM 8			
DIMM 9			
DIMM 10			
DIMM 11			
DIMM 12			
DIMM 13			
DIMM 14			
DIMM 15			
DIMM 16	✓Normal	DDR3	4
DIMM 17	✓Normal	DDR3	4
DIMM 18	✓Normal	DDR3	4
DIMM 19	✓Normal	DDR3	4
DIMM 20	✓Normal	DDR3	4
DIMM 21	✓Normal	DDR3	4

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).



Memory

Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Events, HW Info. If you remove or replace DIMMs, the server needs to be powered on at least once after the removal/replacement to show the correct DIMM information.

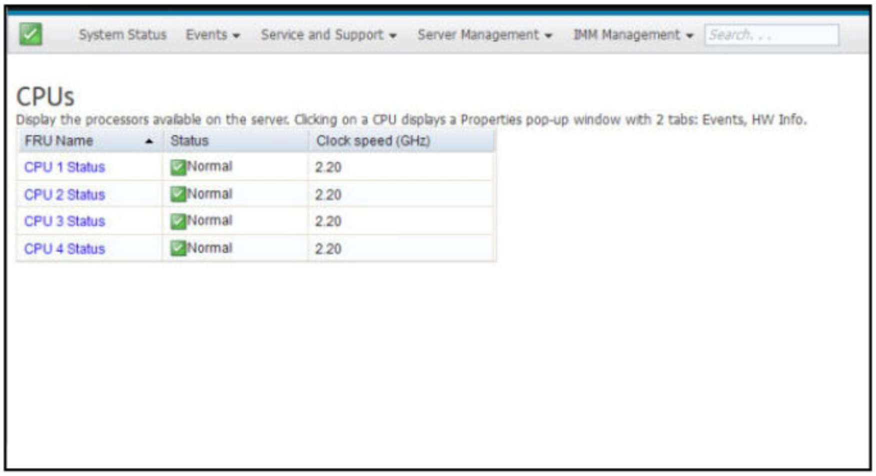
Properties for DIMM 3

Description	DIMM 3
PartNumber	HMT31GR7BFR4A-H9
FRU Serial Number	1855302B
Manuf Date	3611
Type	DDR3
Size	8 GB

FRU Name			
DIMM 1			
DIMM 2			
DIMM 3			
DIMM 4			
DIMM 5			
DIMM 6			
DIMM 7			
DIMM 8			
DIMM 9			
DIMM 10			
DIMM 11			
DIMM 12			
DIMM 13			
DIMM 14			
DIMM 15			
DIMM 16	✓Normal	DDR3	4
DIMM 17	✓Normal		
DIMM 18	✓Normal		
DIMM 19	✓Normal		
DIMM 20	✓Normal	DDR3	4
DIMM 21	✓Normal	DDR3	4

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.

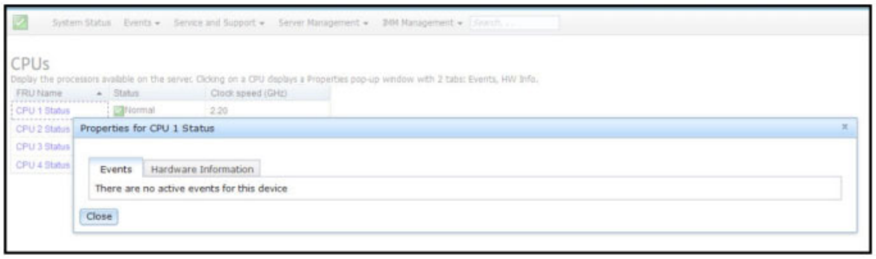


CPUs

Display the processors avaiable on the server. Clicking on a CPU displays a Properties pop-up window with 2 tabs: Events, HW Info.

FRU Name ▲	Status	Clock speed (GHz)
CPU 1 Status	✓Normal	2.20
CPU 2 Status	✓Normal	2.20
CPU 3 Status	✓Normal	2.20
CPU 4 Status	✓Normal	2.20

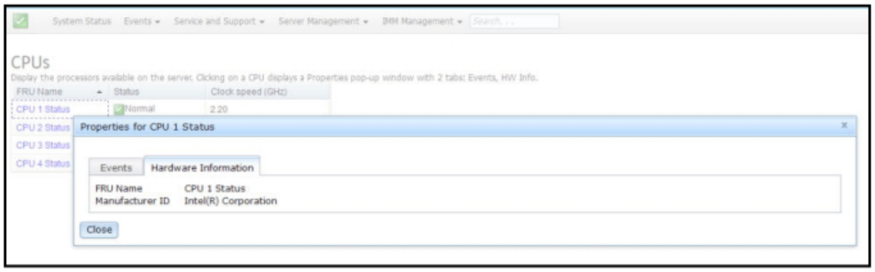
Click on a **CPU** link in the table to view any active events and more information about the component (as shown in the following illustration).



Properties for CPU 1 Status

There are no active events for this device

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).



Properties for CPU 1 Status

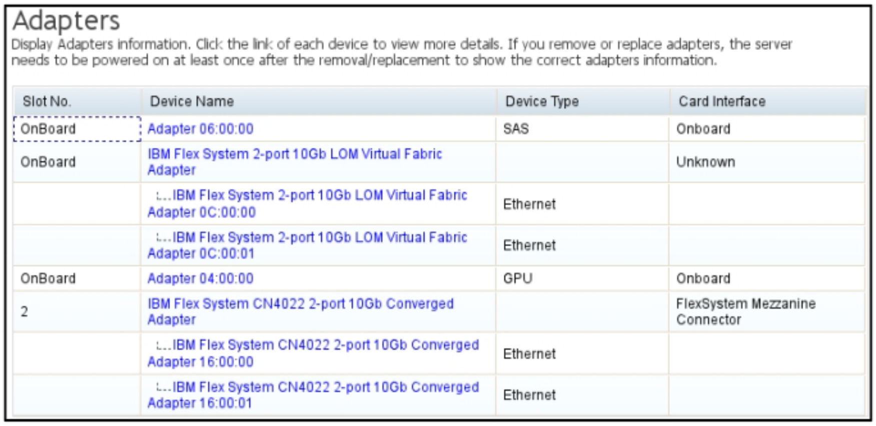
FRU Name	CPU 1 Status
Manufacturer ID	Intel(R) Corporation

Adapters

Select the **Adapters** option under the **Server Management** tab to view information about the PCIe adapters that are installed in the server. Each adapter and its function are listed with the card slot number, device type, and card interface information (as shown in the following illustration).

Notes:

- If the server does not support the Adapters option, this option is not visible.
- If you remove, replace, or configure any adapters, you must restart the server (at least once) to view the updated adapter information.



Adapters

Display Adapters information. Click the link of each device to view more details. If you remove or replace adapters, the server needs to be powered on at least once after the removal/replacement to show the correct adapters information.

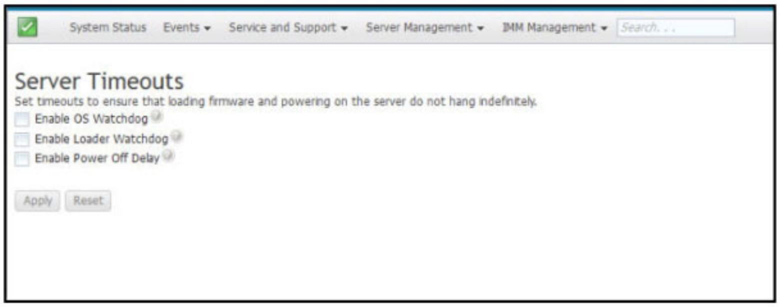
Slot No.	Device Name	Device Type	Card Interface
OnBoard	Adapter 06:00:00	SAS	Onboard
OnBoard	IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter		Unknown
	└...IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00	Ethernet	
	└...IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:01	Ethernet	
OnBoard	Adapter 04:00:00	GPU	Onboard
2	IBM Flex System CN4022 2-port 10Gb Converged Adapter		FlexSystem Mezzanine Connector
	└...IBM Flex System CN4022 2-port 10Gb Converged Adapter 16:00:00	Ethernet	
	└...IBM Flex System CN4022 2-port 10Gb Converged Adapter 16:00:01	Ethernet	

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 92.

The following illustration shows the Server Timeouts window.



Server Timeouts

Set timeouts to ensure that loading firmware and powering on the server do not hang indefinitely.

- □ Enable OS Watchdog
- □ Enable Loader Watchdog
- □ Enable Power Off Delay

For additional information about server timeouts, see "Setting server timeouts" on page 66.

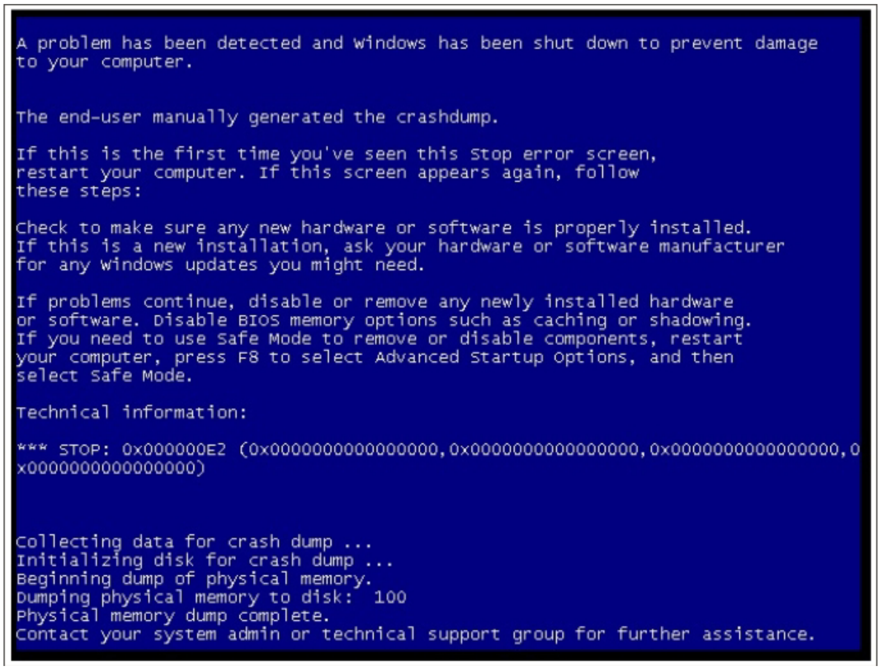
PXE network boot

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 143.

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.



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.


The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)



Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

For more information about the Latest OS Failure Screen option, see “Capturing the latest OS failure screen data” on page 158.

Power management

Select the **Power Management** option under the **Server Management** tab to view power management information and perform power management functions.

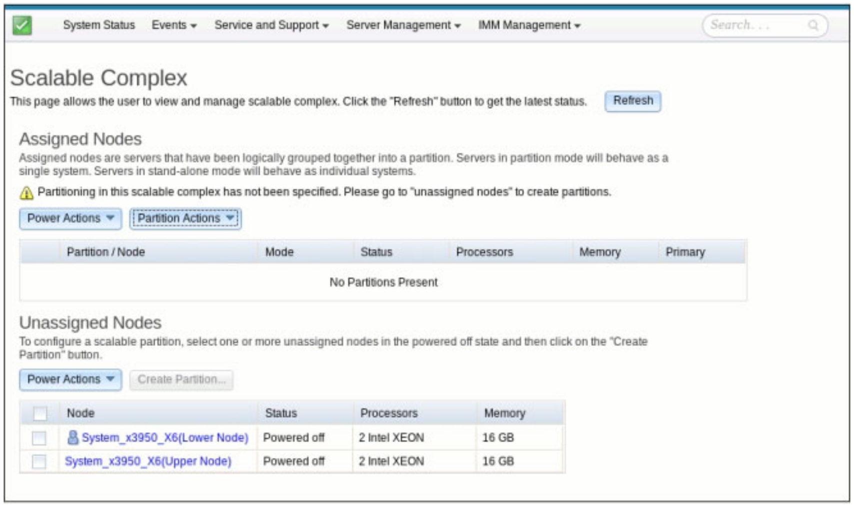
Use the **Power Management** option to perform the following tasks:

- 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.

For more information about the **Power Management** option, see “Managing the server power” on page 159.

Scalable complex

Select the **Scalable Complex** option under the **Server Management** tab to view and manage the current state of all available nodes (servers). A scalable complex allows nodes to be grouped into logical groups called partitions or separated into independent nodes. Nodes in a partition act as a single system and can share resources with each other. A node in a stand-alone (independent) mode operates as single (individual) node. For more information about the **Scalable Complex** option, see “Managing the scalable complex” on page 169. The following illustration shows the Scalable Complex window.



Scalable Complex

This page allows the user to view and manage scalable complex. Click the "Refresh" button to get the latest status.

Assigned Nodes

Assigned nodes are servers that have been logically grouped together into a partition. Servers in partition mode will behave as a single system. Servers in stand-alone mode will behave as individual systems.

⚠ Partitioning in this scalable complex has not been specified. Please go to "unassigned nodes" to create partitions.

	Partition / Node	Mode	Status	Processors	Memory	Primary
			No Partitions Present			

Unassigned Nodes

To configure a scalable partition, select one or more unassigned nodes in the powered off state and then click on the "Create Partition" button.

□	Node	Status	Processors	Memory
□	System_x3950_X6(Lower Node)	Powered off	2 Intel XEON	16 GB
□	System_x3950_X6(Upper Node)	Powered off	2 Intel XEON	16 GB

IMM Management tab

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

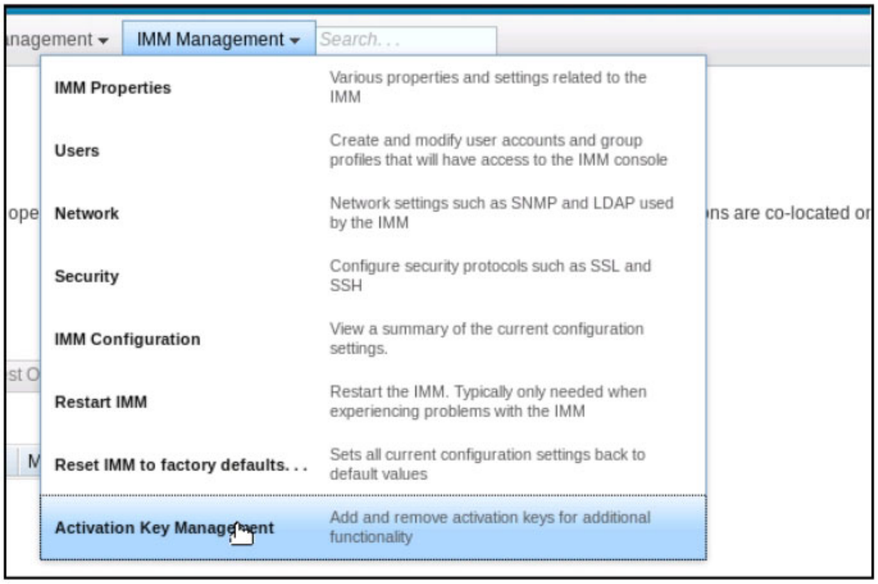
The options under the **IMM Management** tab enable you to view and modify the IMM2 setting. For the list of the options and details on how to use the options to configure the IMM2, see Chapter 4, “Configuring the IMM2,” on page 63.

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 a Flex System, some settings are managed by a Flex System CMM and cannot be modified on the IMM2.



IMM Properties Various properties and settings related to the IMM

Users Create and modify user accounts and group profiles that will have access to the IMM console

Network Network settings such as SNMP and LDAP used by the IMM

Security Configure security protocols such as SSL and SSH

IMM Configuration View a summary of the current configuration settings.

Restart IMM Restart the IMM. Typically only needed when experiencing problems with the IMM

Reset IMM to factory defaults. . . Sets all current configuration settings back to default values

Activation Key Management Add and remove activation keys for additional functionality

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 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
- Cryptography management
- Self Encrypting Drive (SED) encryption key 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.

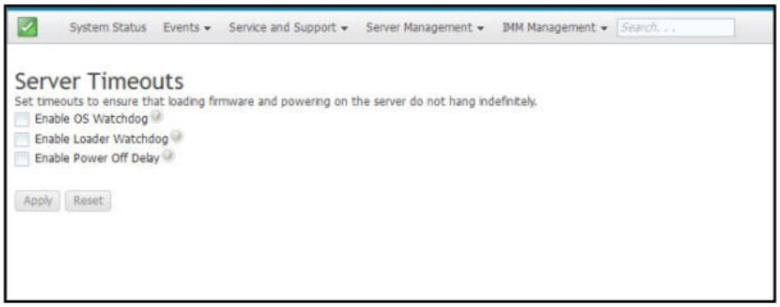
From the Reset IMM2 to factory defaults.. page, you can reset the IMM2 configuration to its factory default settings.

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 187 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 92.



Server Timeouts

Set timeouts to ensure that loading firmware and powering on the server do not hang indefinitely.

□ Enable OS Watchdog

□ Enable Loader Watchdog

□ Enable Power Off Delay

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.

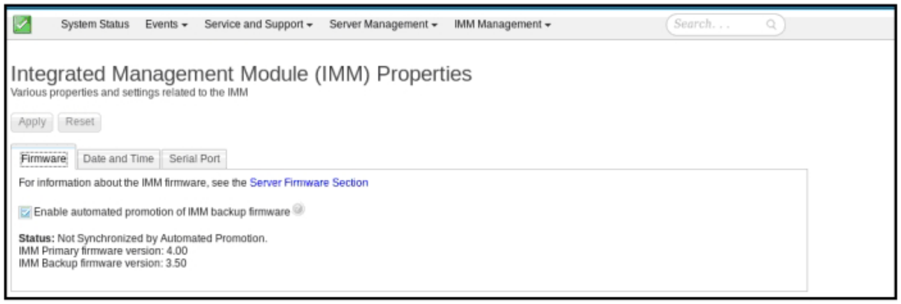
Enable Power Off Delay
Use the **Enable Power Off Delay** field to specify the number of minutes that the IMM2 subsystem will wait for the operating system to shutdown before powering off the server. To set the power off delay timeout value, select the time limit that the IMM2 waits after the operating-system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



Integrated Management Module (IMM) Properties

Various properties and settings related to the IMM

For information about the IMM firmware, see the Server Firmware Section

☑ Enable automated promotion of IMM backup firmware

Status: Not Synchronized by Automated Promotion.
IMM Primary firmware version: 4.00
IMM Backup firmware version: 3.50

Setting the IMM2 date and time

Note: IMM2 Date and Time settings cannot be modified in a 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.

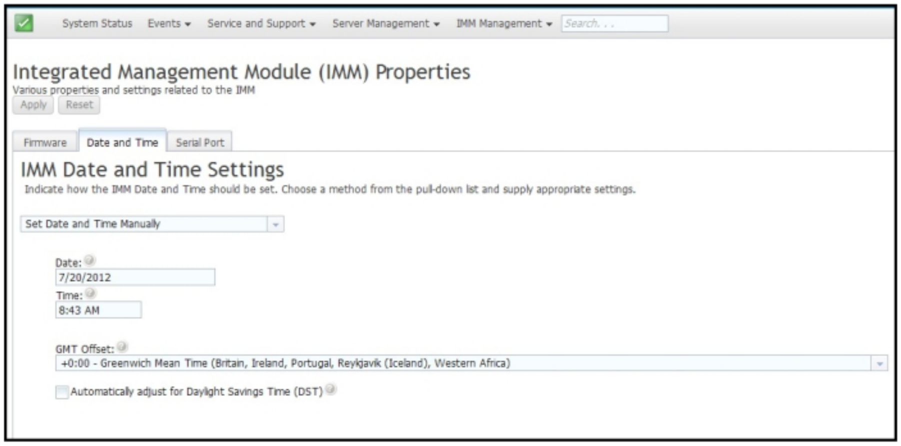
The IMM2 date and time setting affects only the IMM2 clock and not the server clock. The IMM2 real-time clock and the server clock are separate, independent clocks and can be set to different times.

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.



Integrated Management Module (IMM) Properties

Various properties and settings related to the IMM

IMM Date and Time Settings

Indicate how the IMM Date and Time should be set. Choose a method from the pull-down list and supply appropriate settings.

Set Date and Time Manually

Date: 7/20/2012

Time: 8:43 AM

GMT Offset: +0:00 - Greenwich Mean Time (Britain, Ireland, Portugal, Reykjavik (Iceland), Western Africa)

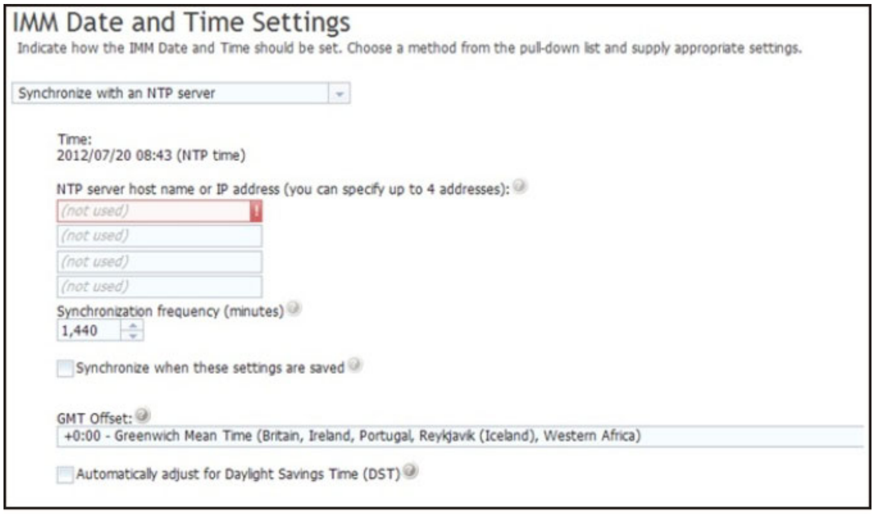
□ Automatically adjust for Daylight Savings Time (DST)

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.



IMM Date and Time Settings

Indicate how the IMM Date and Time should be set. Choose a method from the pull-down list and supply appropriate settings.

Synchronize with an NTP server

Time: 2012/07/20 08:43 (NTP time)

NTP server host name or IP address (you can specify up to 4 addresses):

(not used)

(not used)

(not used)

(not used)

Synchronization frequency (minutes): 1,440

□ Synchronize when these settings are saved

GMT Offset: +0:00 - Greenwich Mean Time (Britain, Ireland, Portugal, Reykjavik (Iceland), Western Africa)

□ Automatically adjust for Daylight Savings Time (DST)

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 on a 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.

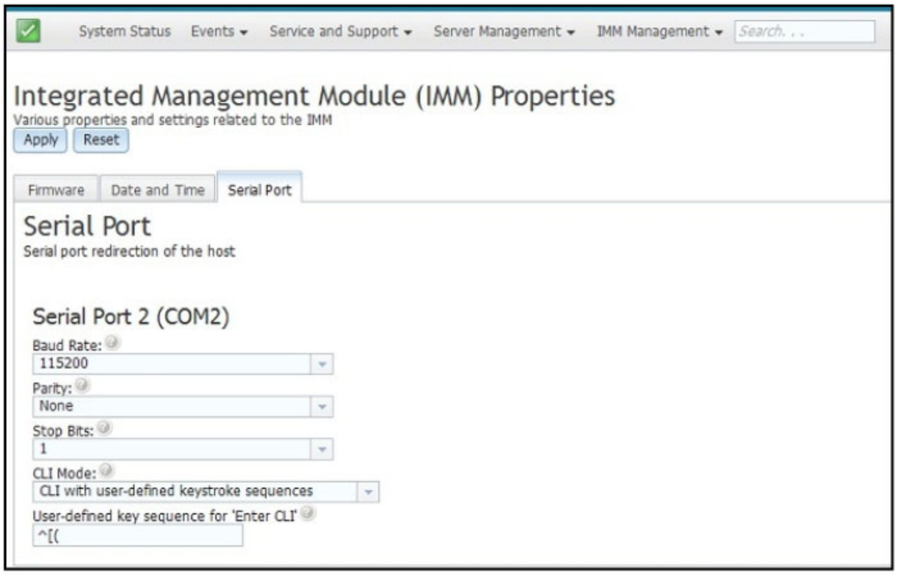
Parity
Specify the parity bits of your serial port connection in this field. Available options are None, Odd, or Even.

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.



Integrated Management Module (IMM) Properties

Various properties and settings related to the IMM

Serial Port

Serial port redirection of the host

Serial Port 2 (COM2)

Baud Rate: 115200

Parity: None

Stop Bits: 1

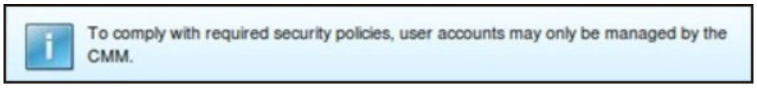
CLI Mode: CLI with user-defined keystroke sequences

User-defined key sequence for 'Enter CLI' ^[(

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 a Flex System, IMM2 user accounts are managed by the CMM.



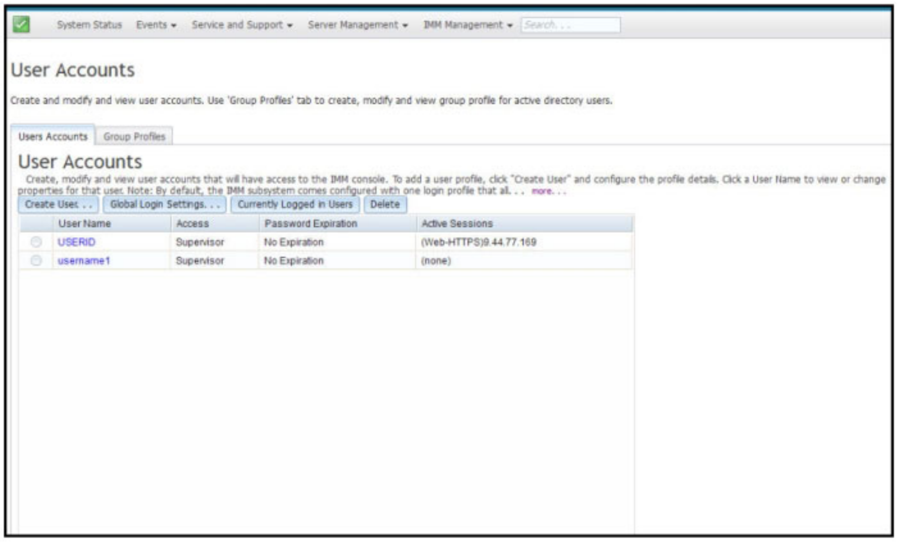
To comply with required security policies, user accounts may only be managed by the CMM.

In a 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.



User Accounts

Create and modify and view user accounts. Use 'Group Profiles' tab to create, modify and view group profile for active directory users.

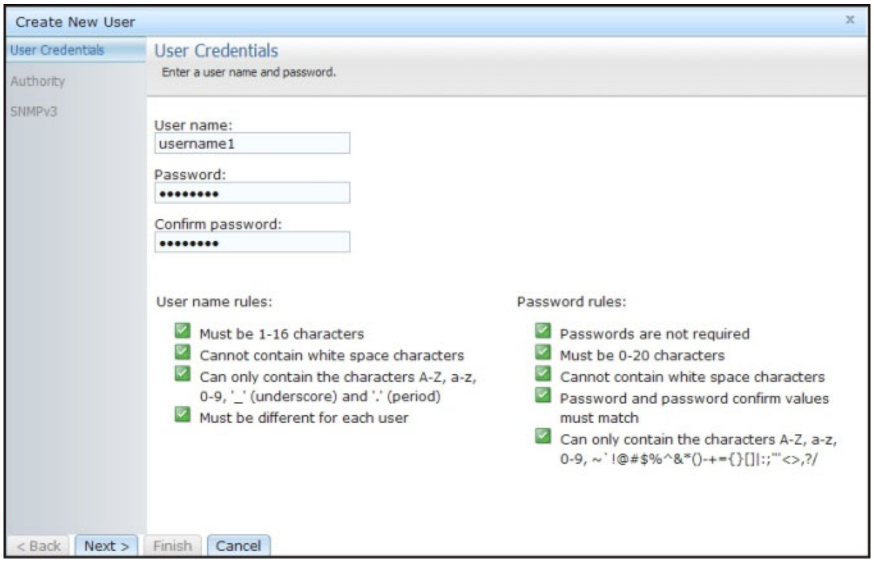
User Accounts

Create, modify and view user accounts that will have access to the IMM console. To add a user profile, click "Create User" and configure the profile details. Click a User Name to view or change properties for that user. Note: By default, the IMM subsystem comes configured with one login profile that all. . . more. . .

	User Name	Access	Password Expiration	Active Sessions
○	USERID	Supervisor	No Expiration	(Web-HTTPS)9.44.77.169
○	username1	Supervisor	No Expiration	(none)

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 Credentials

Enter a user name and password.

User name: username1

Password: ••••••••

Confirm password: ••••••••

User name rules:

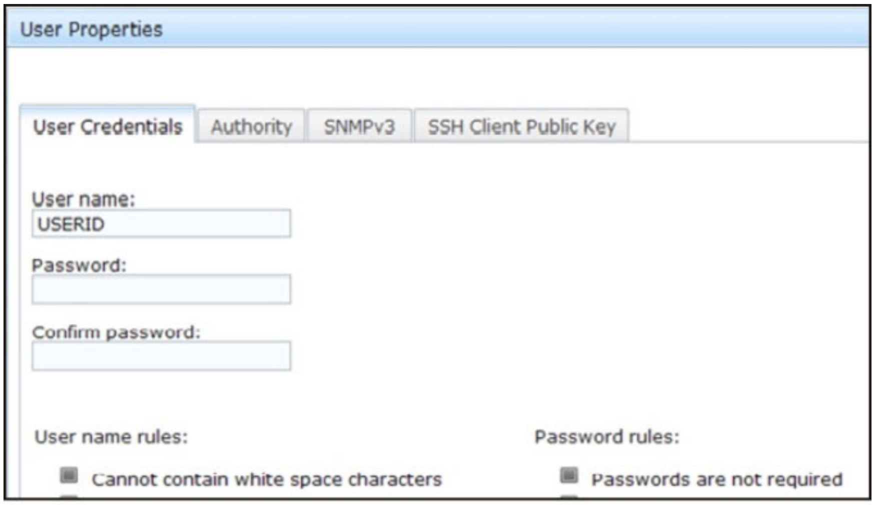
- ☑ Must be 1-16 characters
- ☑ Cannot contain white space characters
- ☑ Can only contain the characters A-Z, a-z, 0-9, '_' (underscore) and '.' (period)
- ☑ Must be different for each user

Password rules:

- ☑ Passwords are not required
- ☑ Must be 0-20 characters
- ☑ Cannot contain white space characters
- ☑ Password and password confirm values must match
- ☑ Can only contain the characters A-Z, a-z, 0-9, ~` !@#$%^&*()-+={}[]|:;"'<>,?/

User properties

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



User Properties

User name:
USERID

Password:

Confirm password:

User name rules:

■ Cannot contain white space characters

Password rules:

■ Passwords are not required

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.

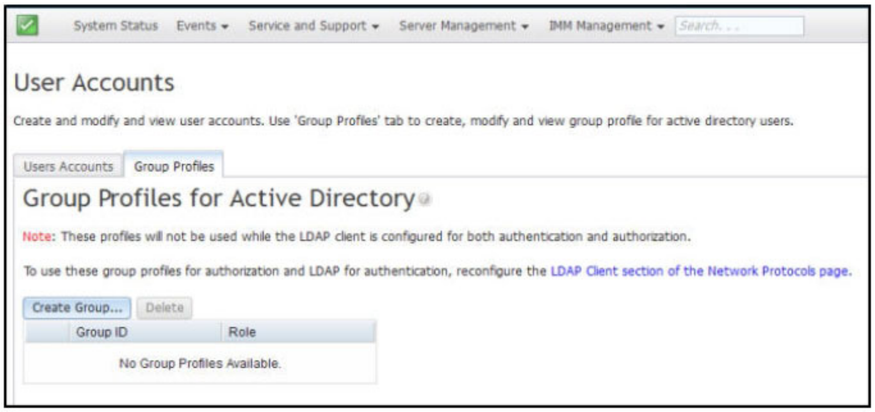
Confirm privacy password
Specify the encryption password again for confirmation.

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).



User Accounts

Create and modify and view user accounts. Use 'Group Profiles' tab to create, modify and view group profile for active directory users.

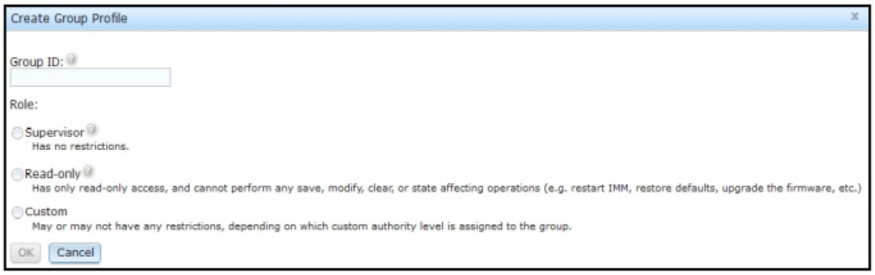
Group Profiles for Active Directory

Note: These profiles will not be used while the LDAP client is configured for both authentication and authorization.

To use these group profiles for authorization and LDAP for authentication, reconfigure the LDAP Client section of the Network Protocols page.

	Group ID	Role
	No Group Profiles Available.	

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


Create Group Profile

Group ID:

Role:

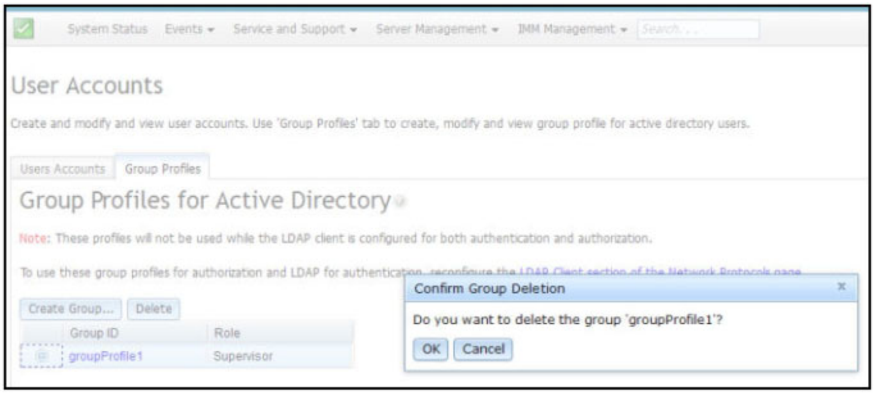
○ Supervisor
Has no restrictions.

○ Read-only
Has only read-only access, and cannot perform any save, modify, clear, or state affecting operations (e.g. restart IMM, restore defaults, upgrade the firmware, etc.)

○ Custom
May or may not have any restrictions, depending on which custom authority level is assigned to the group.

Enter a **Group ID** and select the **Role**, (see "User authority" on page 73 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.



User Accounts

Create and modify and view user accounts. Use 'Group Profiles' tab to create, modify and view group profile for active directory users.

Group Profiles for Active Directory

Note: These profiles will not be used while the LDAP client is configured for both authentication and authorization.

To use these group profiles for authorization and LDAP for authentication, reconfigure the LDAP Client section of the Network Protocols page.

	Group ID	Role
	groupProfile1	Supervisor

Confirm Group Deletion

Do you want to delete the group 'groupProfile1'?

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.

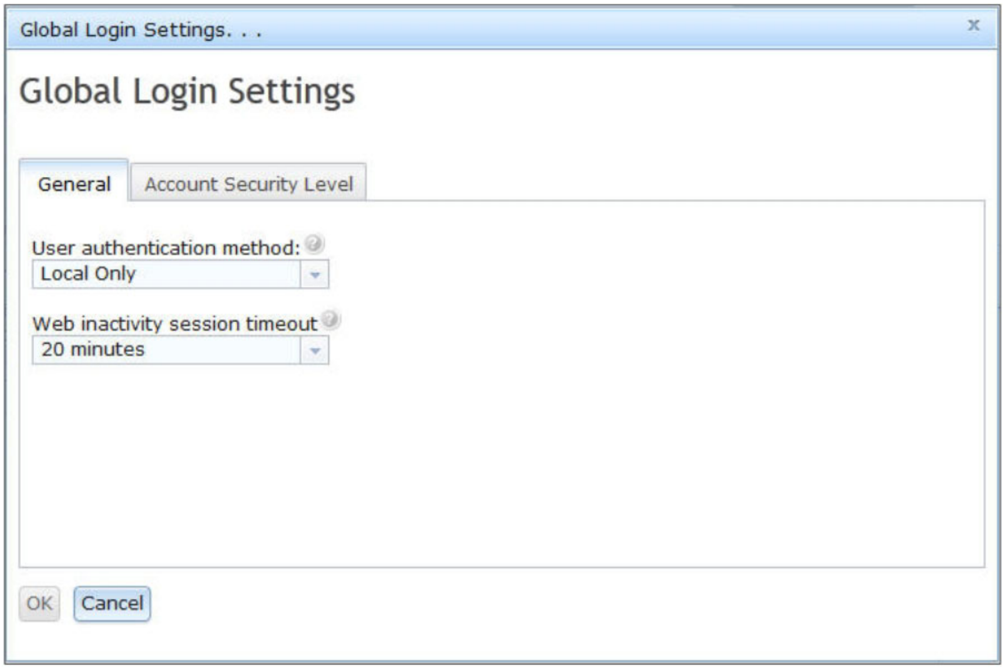
Notes:

- 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.



User authentication method: Local Only

Web inactivity session timeout 20 minutes

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.

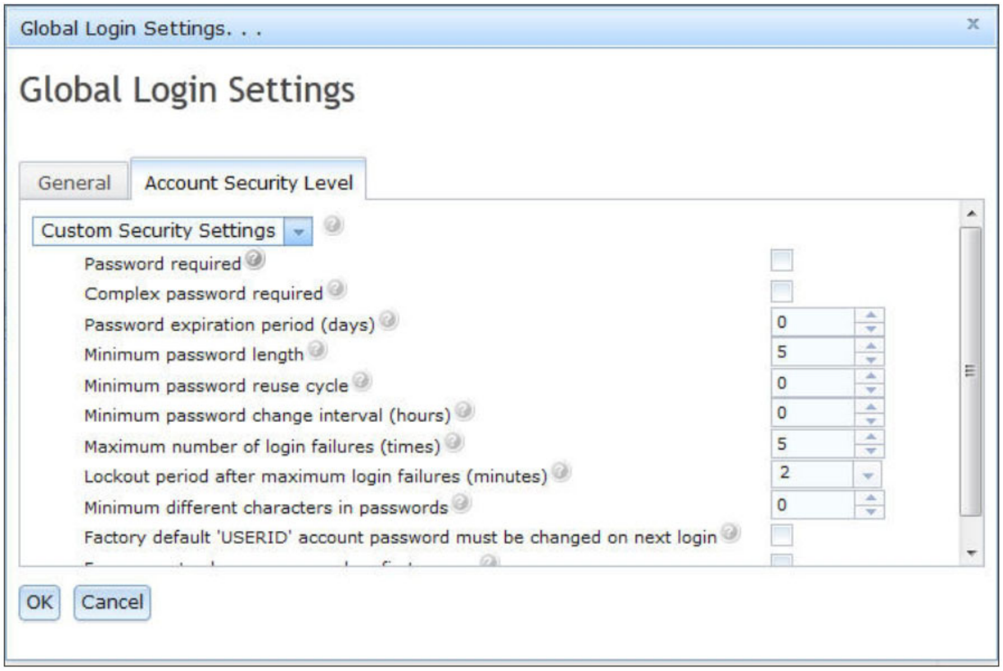
Note: If you leave the browser open on an IMM2 web page that automatically refreshes, your web session will not automatically close due to inactivity.

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.



Custom Security Settings

Password required □

Complex password required □

Password expiration period (days) 0

Minimum password length 5

Minimum password reuse cycle 0

Minimum password change interval (hours) 0

Maximum number of login failures (times) 5

Lockout period after maximum login failures (minutes) 2

Minimum different characters in passwords 0

Factory default 'USERID' account password must be changed on next login □

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 4. 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 4. 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.

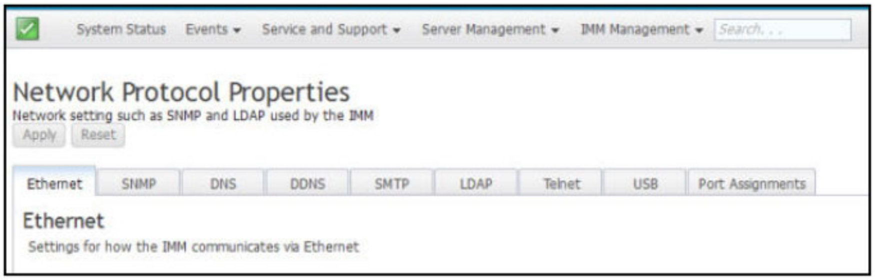
Force user to change password on first access
After setting up a new user with a default password, selection of this check box will force that user to change their password the first time the user logs in.

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).



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Ethernet

Settings for how the IMM communicates via Ethernet

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.

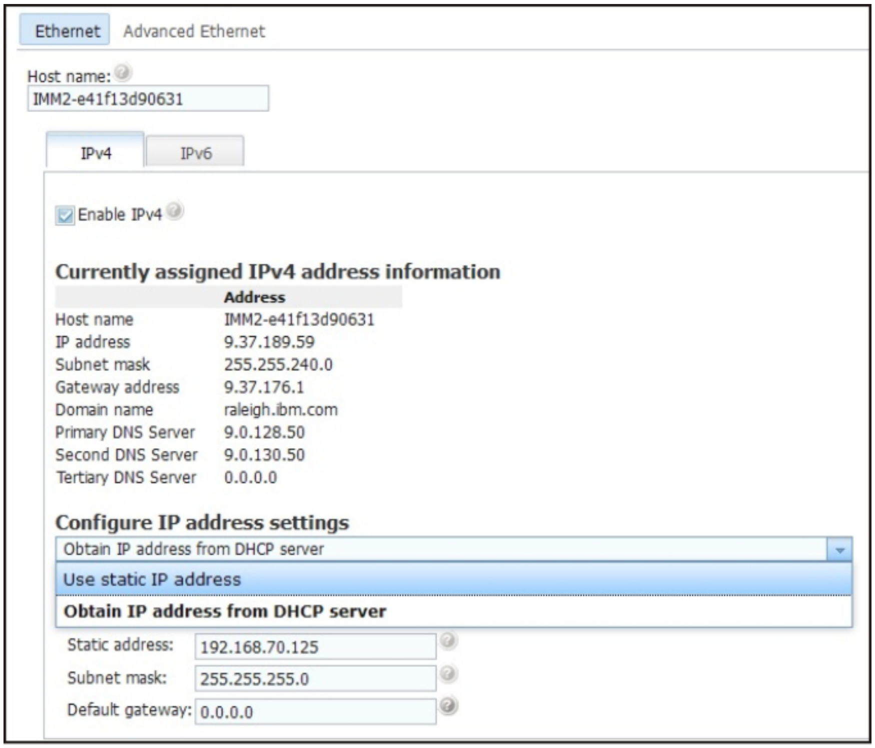
2. From the **Configure IP address settings** list, select one of the following options:
   - Obtain an IP address from a DHCP server
   - Use static IP address
3. If you want the IMM2 to default to a static IP address if unable to contact a DHCP server, select the corresponding check box.
4. In the **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.



Host name: IMM2-e41f13d90631

☑ Enable IPv4

Currently assigned IPv4 address information

	Address
Host name	IMM2-e41f13d90631
IP address	9.37.189.59
Subnet mask	255.255.240.0
Gateway address	9.37.176.1
Domain name	raleigh.ibm.com
Primary DNS Server	9.0.128.50
Second DNS Server	9.0.130.50
Tertiary DNS Server	0.0.0.0

Configure IP address settings

Obtain IP address from DHCP server

Use static IP address

Obtain IP address from DHCP server

Static address: 192.168.70.125

Subnet mask: 255.255.255.0

Default gateway: 0.0.0.0

Configuring advanced Ethernet settings

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

Note: In a Flex System, the VLAN settings are managed by a Flex System CMM and cannot be modified on the IMM2.

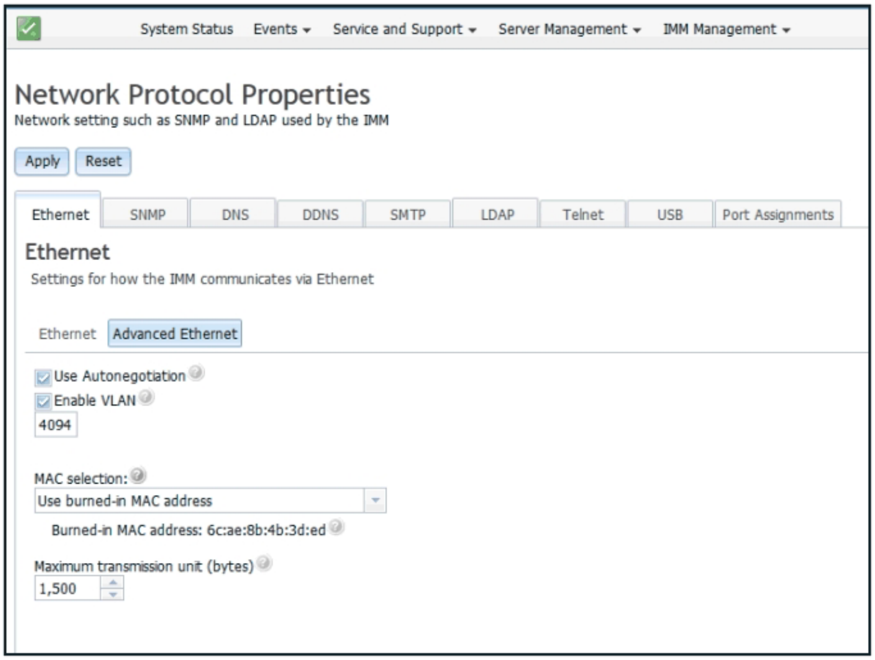
To enable Virtual LAN (VLAN) tagging select the **Enable VLAN** checkbox. When VLAN is enabled and a VLAN ID is configured, the IMM2 only accepts packets with the specified VLAN IDs. The VLAN IDs can be configured with numeric values between 1 and 4094.

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

- Use 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.
- Use 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.



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Ethernet

Settings for how the IMM communicates via Ethernet

☑ Use Autonegotiation

☑ Enable VLAN

4094

MAC selection: Use burned-in MAC address

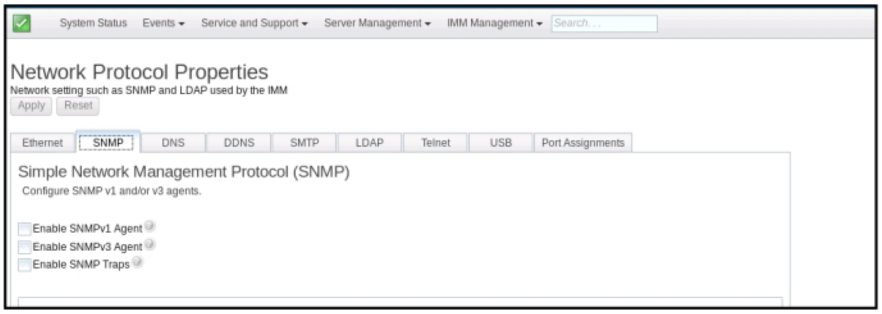
Burned-in MAC address: 6c:ae:8b:4b:3d:ed

Maximum transmission unit (bytes) 1,500

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).



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Simple Network Management Protocol (SNMP)

Configure SNMP v1 and/or v3 agents.

□ Enable SNMPv1 Agent

□ Enable SNMPv3 Agent

□ Enable SNMP Traps

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.

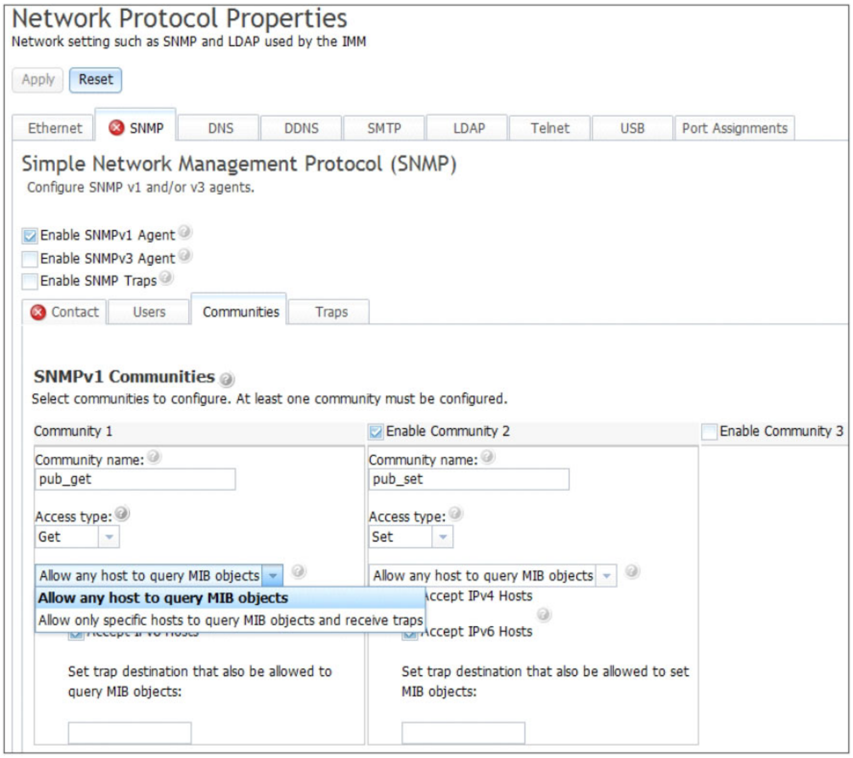
      Complete the following fields:

      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*. This *red X* can be used to guide you through completion of the required fields.

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



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Simple Network Management Protocol (SNMP)

Configure SNMP v1 and/or v3 agents.

☑ Enable SNMPv1 Agent

□ Enable SNMPv3 Agent

□ Enable SNMP Traps

SNMPv1 Communities

Select communities to configure. At least one community must be configured.

Community 1

Community name: pub_get

Access type: Get

Allow any host to query MIB objects

Allow any host to query MIB objects
Allow only specific hosts to query MIB objects and receive traps

Set trap destination that also be allowed to query MIB objects:

☑ Enable Community 2

Community name: pub_set

Access type: Set

Allow any host to query MIB objects

☑ Accept IPv4 Hosts

☑ Accept IPv6 Hosts

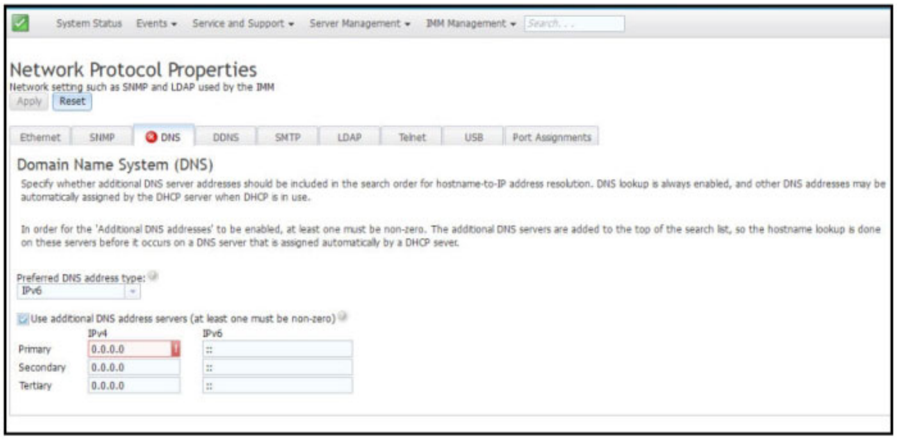
Set trap destination that also be allowed to set MIB objects:

□ Enable Community 3

Configuring DNS

Note: In a 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).



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Domain Name System (DNS)

Specify whether additional DNS server addresses should be included in the search order for hostname-to-IP address resolution. DNS lookup is always enabled, and other DNS addresses may be automatically assigned by the DHCP server when DHCP is in use.

In order for the 'Additional DNS addresses' to be enabled, at least one must be non-zero. The additional DNS servers are added to the top of the search list, so the hostname lookup is done on these servers before it occurs on a DNS server that is assigned automatically by a DHCP sever.

Preferred DNS address type: IPv6

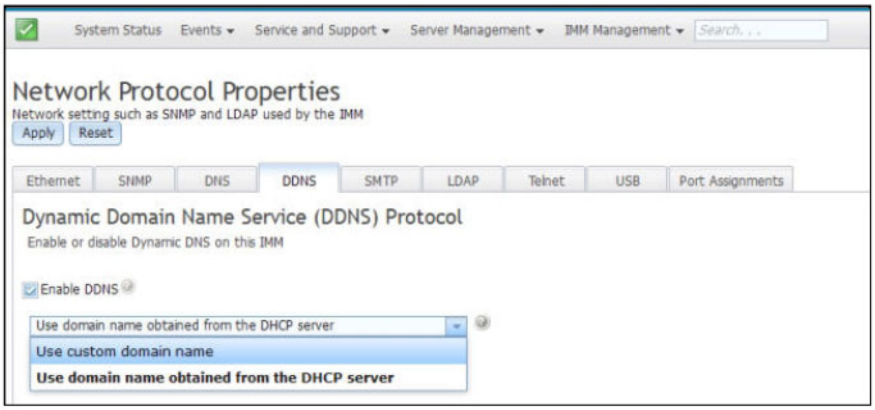
☑ Use additional DNS address servers (at least one must be non-zero)

	IPv4	IPv6
Primary	0.0.0.0	::
Secondary	0.0.0.0	::
Tertiary	0.0.0.0	::

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).



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Dynamic Domain Name Service (DDNS) Protocol

Enable or disable Dynamic DNS on this IMM

☑ Enable DDNS

Use domain name obtained from the DHCP server

Use custom domain name

Use domain name obtained from the DHCP server

Configuring SMTP

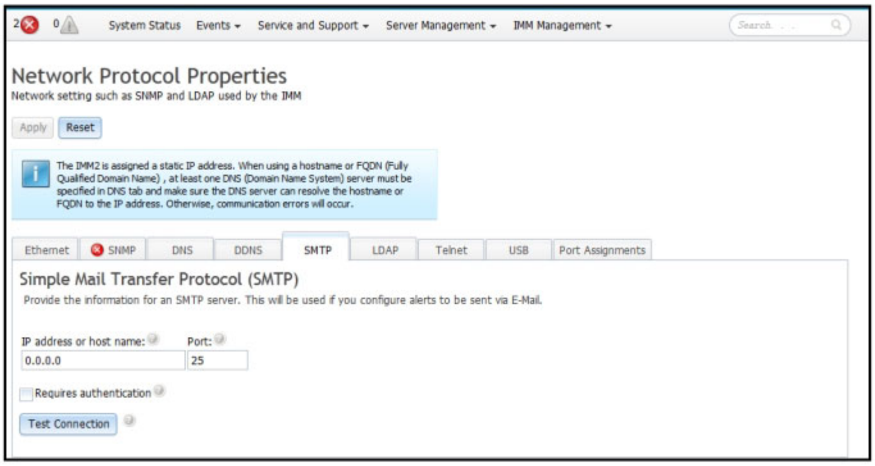
Click the **SMTP** tab to view or modify IMM2 SMTP settings. Complete the following fields to view or modify SMTP settings:

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.



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

The IMM2 is assigned a static IP address. When using a hostname or FQDN (Fully Qualified Domain Name) , at least one DNS (Domain Name System) server must be specified in DNS tab and make sure the DNS server can resolve the hostname or FQDN to the IP address. Otherwise, communication errors will occur.

Simple Mail Transfer Protocol (SMTP)

Provide the information for an SMTP server. This will be used if you configure alerts to be sent via E-Mail.

IP address or host name: 0.0.0.0

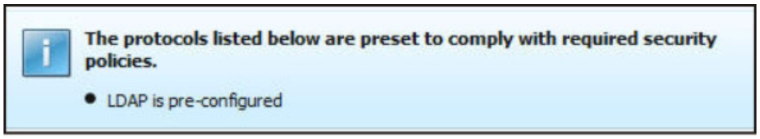
Port: 25

□ Requires authentication

Configuring LDAP

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

Note: In a 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).

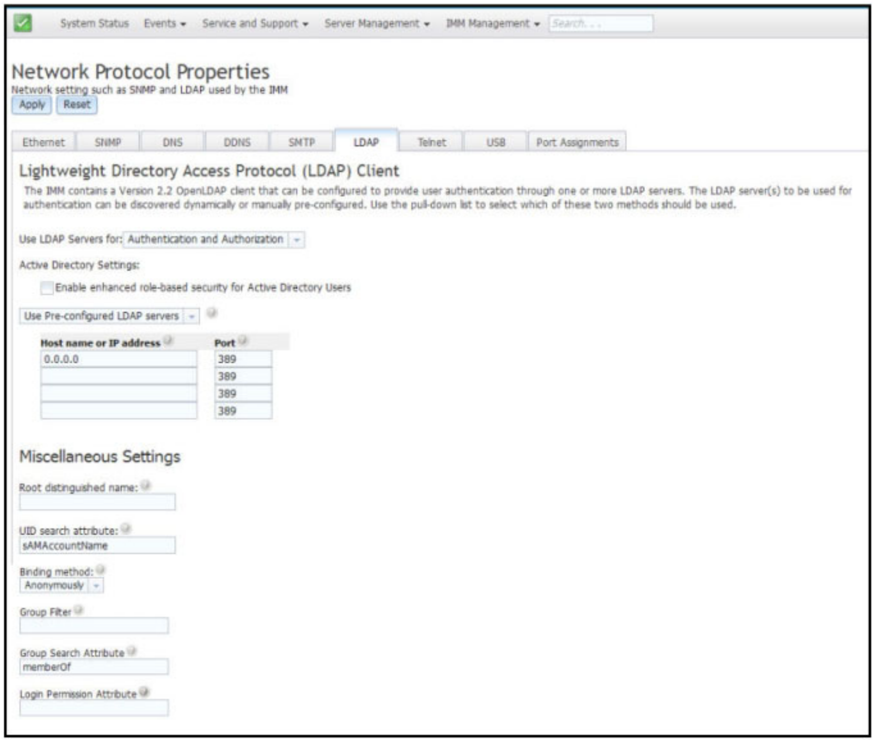


The protocols listed below are preset to comply with required security policies.

- LDAP is pre-configured

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 will 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.



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Lightweight Directory Access Protocol (LDAP) Client

The IMM contains a Version 2.2 OpenLDAP client that can be configured to provide user authentication through one or more LDAP servers. The LDAP server(s) to be used for authentication can be discovered dynamically or manually pre-configured. Use the pull-down list to select which of these two methods should be used.

Use LDAP Servers for: Authentication and Authorization

Active Directory Settings:

□ Enable enhanced role-based security for Active Directory Users

Use Pre-configured LDAP servers

Host name or IP address	Port
0.0.0.0	389
	389
	389
	389

Miscellaneous Settings

Root distinguished name:

UID search attribute: sAMAccountName

Binding method: Anonymously

Group Filter

Group Search Attribute memberOf

Login Permission Attribute

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 search requests.

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 the second attempt to bind 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 5. 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.

Table 5. Permission bits (continued)

Bit position	Function	Explanation
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, to clear the event logs the user is required to have this level of permission.
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.

Table 5. Permission bits (continued)

Bit position	Function	Explanation
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.

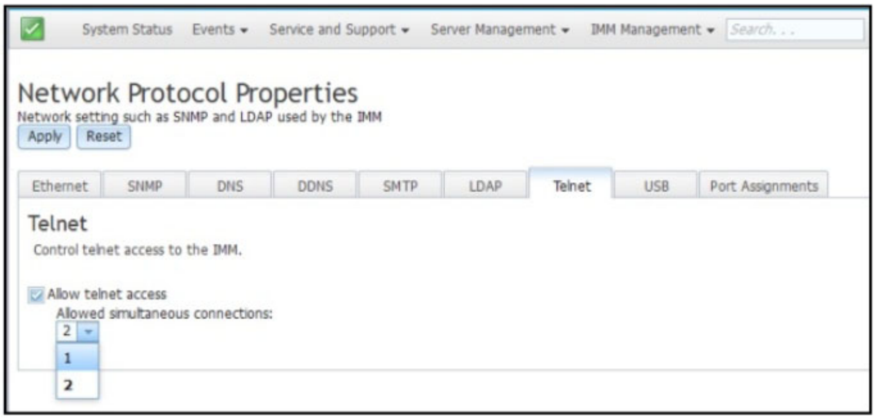
Configuring Telnet

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.



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Telnet

Control telnet access to the IMM.

☑ Allow telnet access

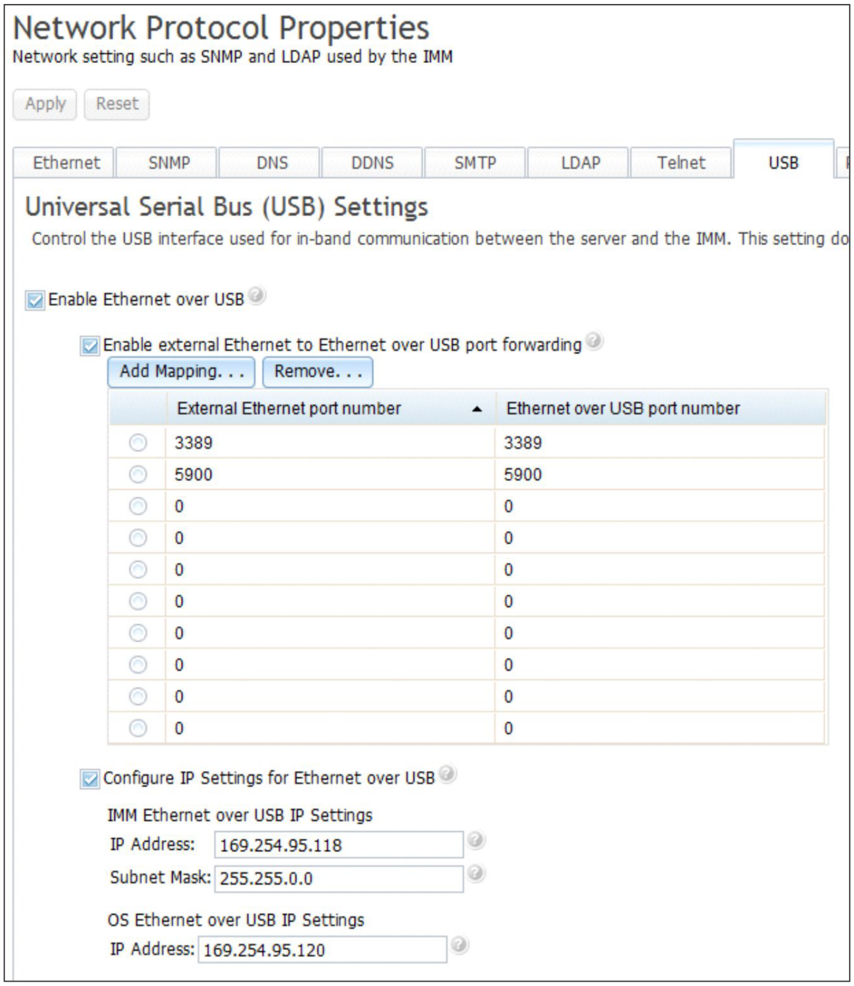
Allowed simultaneous connections: 2

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.



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Universal Serial Bus (USB) Settings

Control the USB interface used for in-band communication between the server and the IMM. This setting do

☑ Enable Ethernet over USB

☑ Enable external Ethernet to Ethernet over USB port forwarding

	External Ethernet port number ▲	Ethernet over USB port number
○	3389	3389
○	5900	5900
○	0	0
○	0	0
○	0	0
○	0	0
○	0	0
○	0	0
○	0	0
○	0	0

☑ Configure IP Settings for Ethernet over USB

IMM Ethernet over USB IP Settings

IP Address: 169.254.95.118

Subnet Mask: 255.255.0.0

OS Ethernet over USB IP Settings

IP Address: 169.254.95.120

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 that is configured 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.

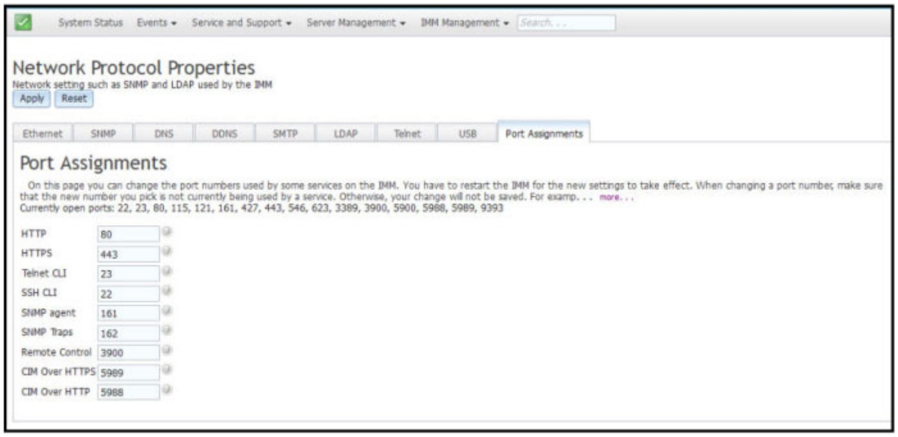
SNMP Traps
In this field specify the port number that is used for SNMP traps. The default value is 162. Valid port number values are from 1 to 65535.

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.



Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Port Assignments

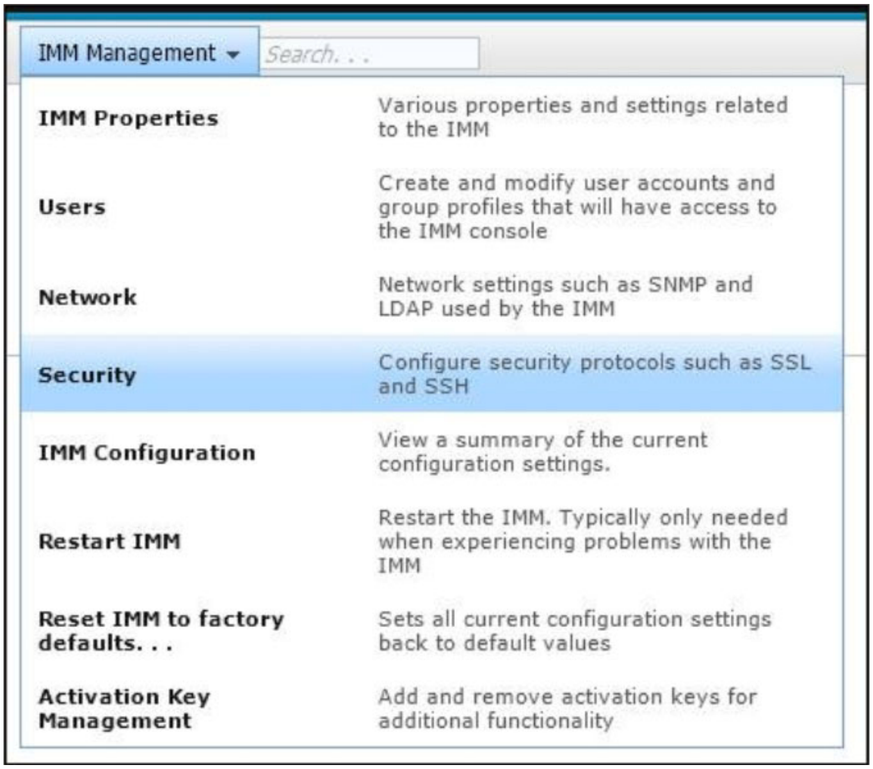
On this page you can change the port numbers used by some services on the IMM. You have to restart the IMM for the new settings to take effect. When changing a port number, make sure that the new number you pick is not currently being used by a service. Otherwise, your change will not be saved. For examp. . . more. . .
Currently open ports: 22, 23, 80, 115, 121, 161, 427, 443, 546, 623, 3389, 3900, 5900, 5988, 5989, 9393

HTTP	80
HTTPS	443
Telnet CLI	23
SSH CLI	22
SNMP agent	161
SNMP Traps	162
Remote Control	3900
CIM Over HTTPS	5989
CIM Over HTTP	5988

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.



IMM Management ▾ Search. . .

IMM Properties Various properties and settings related to the IMM

Users Create and modify user accounts and group profiles that will have access to the IMM console

Network Network settings such as SNMP and LDAP used by the IMM

Security Configure security protocols such as SSL and SSH

IMM Configuration View a summary of the current configuration settings.

Restart IMM Restart the IMM. Typically only needed when experiencing problems with the IMM

Reset IMM to factory defaults. . . Sets all current configuration settings back to default values

Activation Key Management Add and remove activation keys for additional functionality

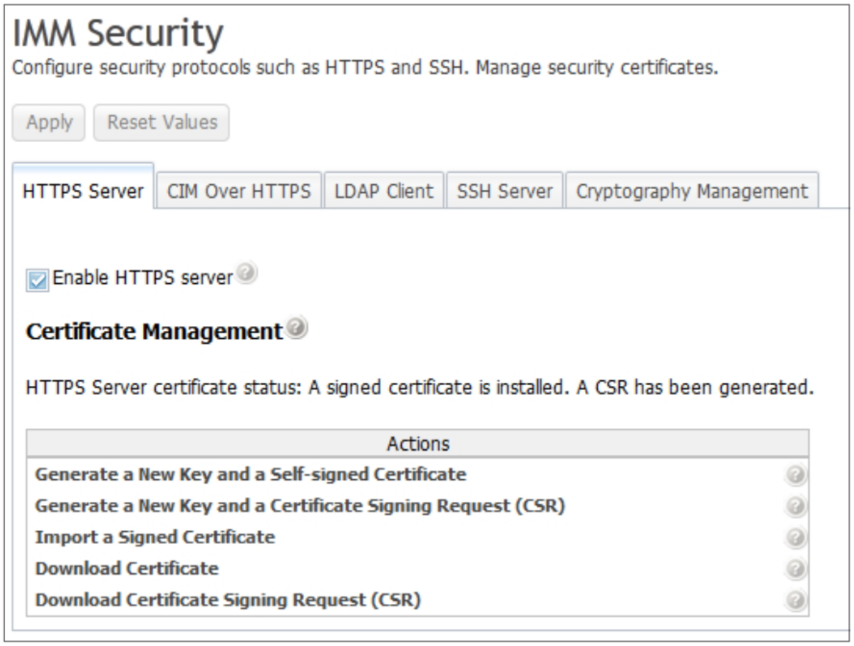
Configuring HTTPS protocol

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 99. The following illustration shows the **HTTPS Server** tab.



Configure security protocols such as HTTPS and SSH. Manage security certificates.

☑ Enable HTTPS server

Certificate Management

HTTPS Server certificate status: A signed certificate is installed. A CSR has been generated.

Actions
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Import a Signed Certificate
Download Certificate
Download Certificate Signing Request (CSR)

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 99.

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

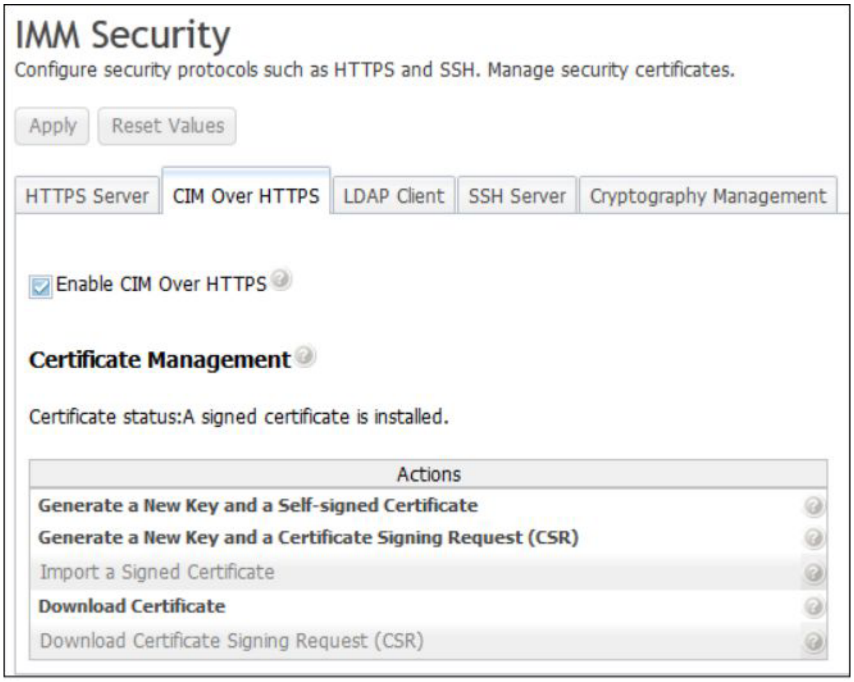
Configuring CIM over HTTPS protocol

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 99. The following illustration shows the **CIM over HTTPS** tab.


IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

☑ Enable CIM Over HTTPS

Certificate Management

Certificate status:A signed certificate is installed.

Actions
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Import a Signed Certificate
Download Certificate
Download Certificate Signing Request (CSR)

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 99.

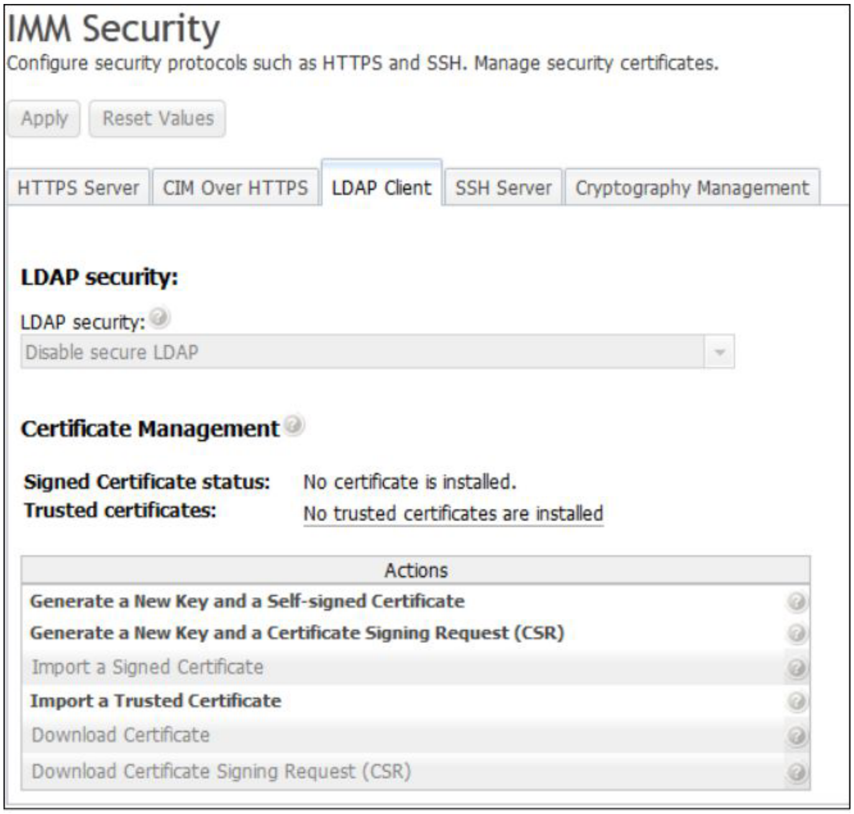
Note: After you set up the certificate handling, you must restart the IMM2 for your changes to take effect.

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 99.

The following illustration shows the LDAP Client tab.



IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

Apply
Reset Values
HTTPS Server
CIM Over HTTPS
LDAP Client
SSH Server
Cryptography Management

LDAP security:

LDAP security: Disable secure LDAP

Certificate Management

Signed Certificate status: No certificate is installed.

Trusted certificates: No trusted certificates are installed

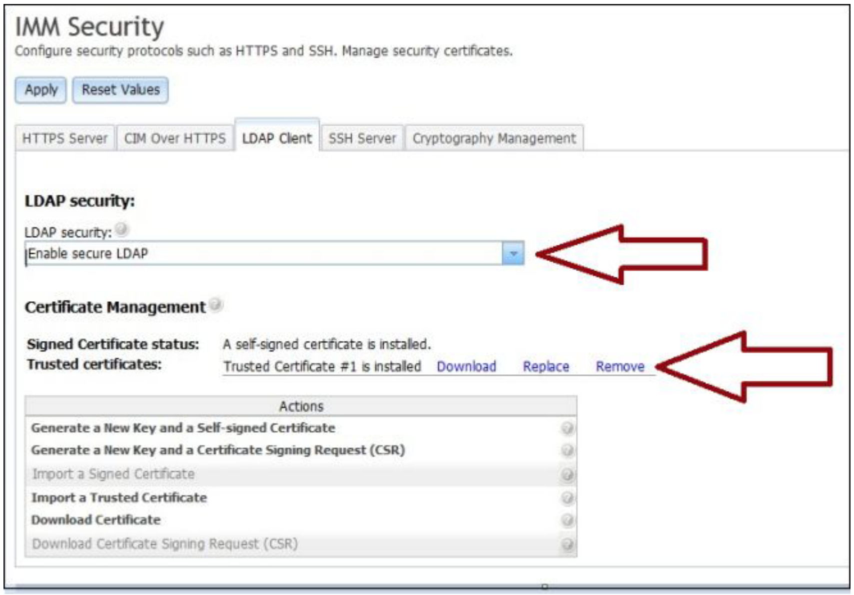
Actions
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Import a Signed Certificate
Import a Trusted Certificate
Download Certificate
Download Certificate Signing Request (CSR)

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 99. 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.



IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

LDAP security:

LDAP security: Enable secure LDAP

Certificate Management

Signed Certificate status: A self-signed certificate is installed.

Trusted certificates: Trusted Certificate #1 is installed Download Replace Remove

Actions
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Import a Signed Certificate
Import a Trusted Certificate
Download Certificate
Download Certificate Signing Request (CSR)

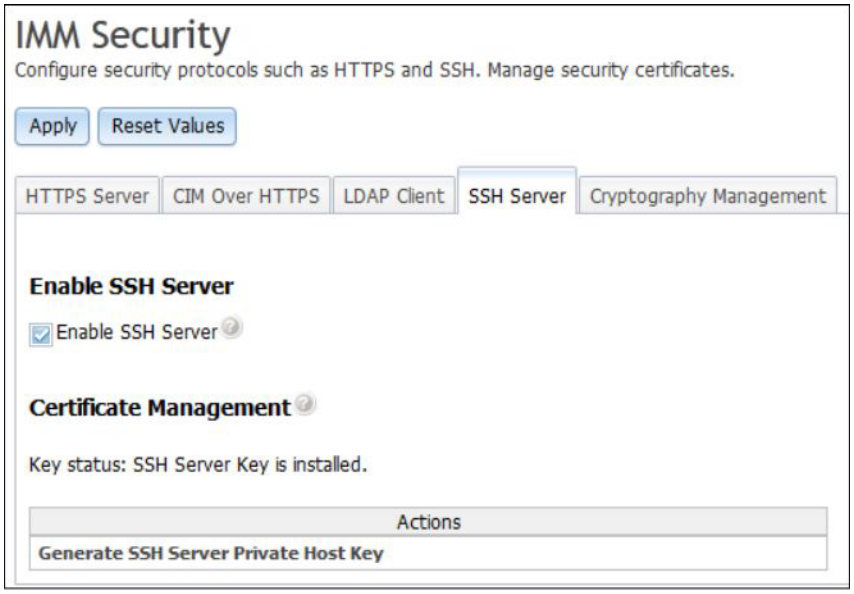
Configuring the Secure Shell server

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.



IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

Enable SSH Server

☑ Enable SSH Server

Certificate Management

Key status: SSH Server Key is installed.

Actions
Generate SSH Server Private Host Key

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).

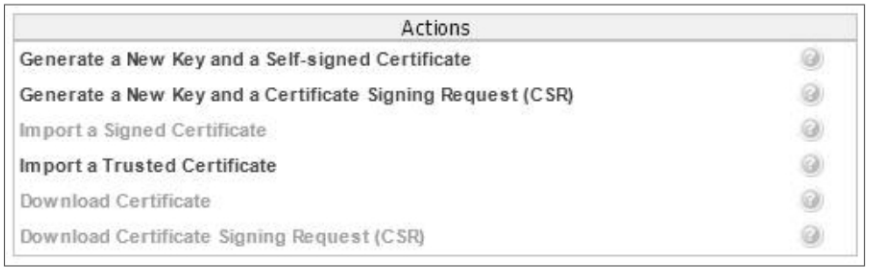
For more complete security, you can use a certificate that is signed by a certificate authority (CA). To obtain a signed certificate, click **Generate a New Key and a Certificate Signing Request (CSR)** in the Actions menu. You must then send the Certificate-Signing Request (CSR) to a CA and make arrangements 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.

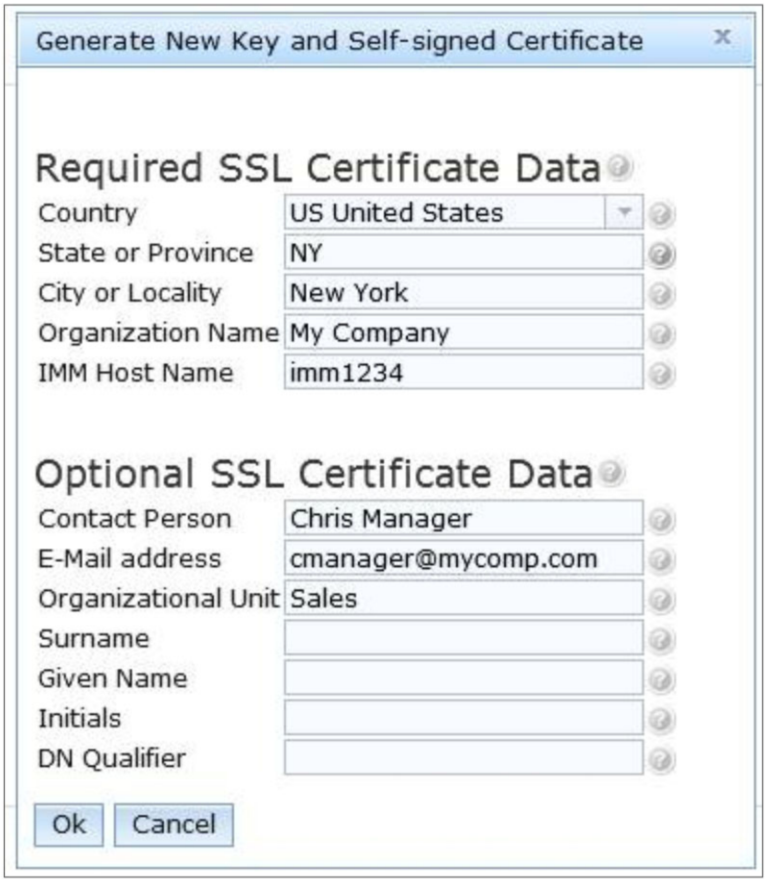
SSL certificate management

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


Actions
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Import a Signed Certificate
Import a Trusted Certificate
Download Certificate
Download Certificate Signing Request (CSR)

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).



Required SSL Certificate Data

Country	US United States
State or Province	NY
City or Locality	New York
Organization Name	My Company
IMM Host Name	imm1234

Optional SSL Certificate Data

Contact Person	Chris Manager
E-Mail address	cmanager@mycomp.com
Organizational Unit	Sales
Surname	
Given Name	
Initials	
DN Qualifier	

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).

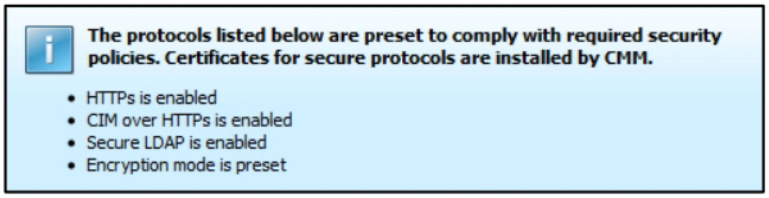
Certificate Generated

Compromised private keys

Private keys are used in client and server certificates to identify one end or both ends of communication transactions as well as to encrypt and decrypt the information that is being communicated. A private key is compromised when an *unauthorized* person obtains the private key or determines what the private key is that is used to encrypt and decrypt secret information. The compromised key can be used to decrypt encrypted data without the knowledge of the sender of the data.

If your private key is compromised and your certificate is signed by a certificate authority, notify your certificate authority and have your key placed on a Certificate Revocation list. This action will inform the appropriate audience that the private key is compromised and the public key has been revoked. You can subsequently generate a new key pair and obtain a new certificate for the public key.

If the certificates are installed and controlled by another management system, for example, a Flex System CMM refer to the documentation that came with your server for the procedures to remove, generate and install the certificates. The following illustration shows the warning message displayed when the certificates are installed and controlled by the CMM.


The protocols listed below are preset to comply with required security policies. Certificates for secure protocols are installed by CMM.

- HTTPs is enabled
- CIM over HTTPs is enabled
- Secure LDAP is enabled
- Encryption mode is preset

If the certificates are installed or controlled by the IMM2, refer to the following sections:

- See “Configuring the Secure Shell server” on page 98 for information about generating a replacement Secure Shell (SSH) Server Private Host Key
- See “Configuring LDAP” on page 86 for information abut removing and installing trusted certificates for the IMM2 LDAP client.
- See “SSL certificate handling” on page 99 for information about generating a replacement SSH Sever Private Host Key.

Private key states

A private key transitions through several states from the time that it is generated until the time it is destroyed. The following list includes an explanation of each state.

- Pre-activation state:
  - This state applies to a key when it has been generated; but, has not been authorized for use. This occurs when a CSR and private key are generated;

but, the corresponding signed certificate has not been imported. In this state the private key is considered to be in the *pre-activation* state. In this state the key is not used to encrypt or sign information.

- Active state:
  - This state occurs after a key is generated and the corresponding certificate is installed. In this state the key can be used to encrypt and sign information. All keys that have been used at least once and have not been destroyed are in an *active* state. This applies to the majority of keys in the server.
- Deactivated state:
  - This state applies to a key whose crypto-period has expired; but, the key has not been destroyed. The key is in the *deactivated* state until it is destroyed. The *deactivated* but not destroyed state does not apply to any keys on System x management devices and the CMM.
- Destroyed state:
  - This state applies to all keys that are no longer in use.
- Compromised/Destroyed compromised state:
  - A private key is in a *compromised* state when it is known by an unauthorized person. If a private key is thought to be compromised, it should be revoked by the certificate authority that issued the certificate associated with the key.
  - A key that is *active* (based on the description for the active state); but, revoked by the certificate authority is considered to be in a *compromised* state.
  - A key that is destroyed and also revoked by the certificate authority is considered to be in a *destroyed compromised* state.

Configuring cryptography management

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

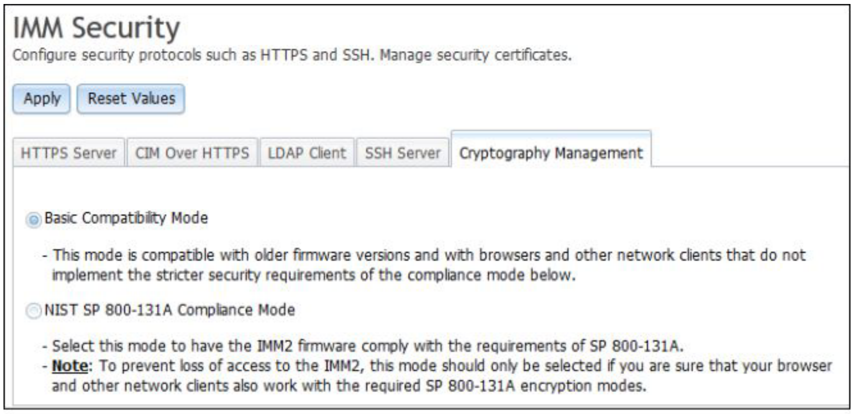
Important: Before you flash the IMM2 firmware back to an older version set the IMM2 Security option to use the Basic Compatibility Mode. This will prevent a possible loss of access to the IMM2.

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.


IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

● Basic Compatibility Mode

- This mode is compatible with older firmware versions and with browsers and other network clients that do not implement the stricter security requirements of the compliance mode below.

○ NIST SP 800-131A Compliance Mode

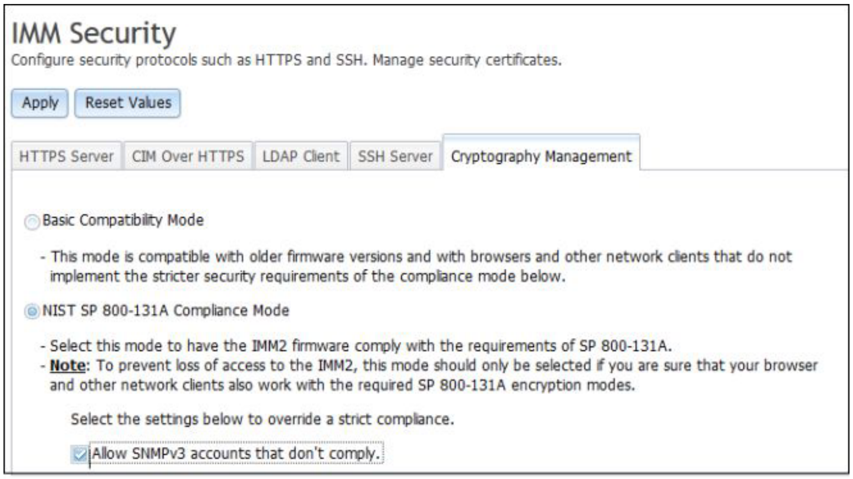
- Select this mode to have the IMM2 firmware comply with the requirements of SP 800-131A.
- **Note**: To prevent loss of access to the IMM2, this mode should only be selected if you are sure that your browser and other network clients also work with the required SP 800-131A encryption modes.

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.


IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

○ Basic Compatibility Mode

- This mode is compatible with older firmware versions and with browsers and other network clients that do not implement the stricter security requirements of the compliance mode below.

● NIST SP 800-131A Compliance Mode

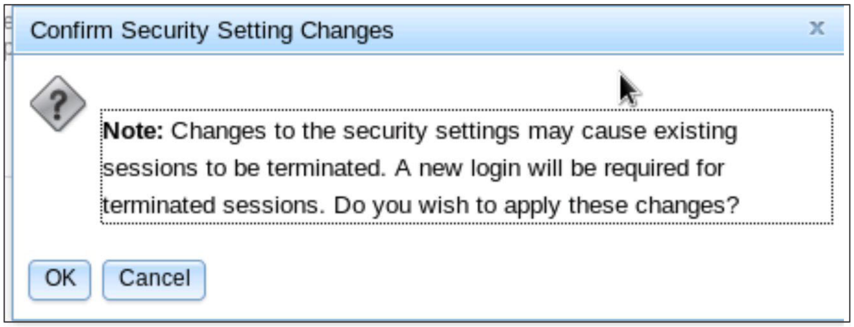
- Select this mode to have the IMM2 firmware comply with the requirements of SP 800-131A.
- **Note**: To prevent loss of access to the IMM2, this mode should only be selected if you are sure that your browser and other network clients also work with the required SP 800-131A encryption modes.

Select the settings below to override a strict compliance.

☑ Allow SNMPv3 accounts that don't comply.

To configure the cryptography mode for a stand-alone server, complete the following steps:

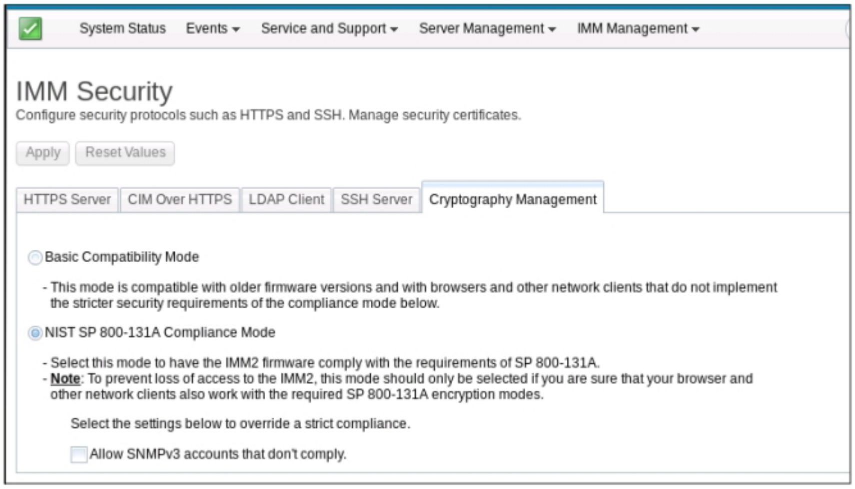
1. Log in to the IMM2.
2. Click the **Security** option under the **IMM Management** tab.
3. Click the **Cryptography Management** tab.
4. Select the cryptography mode on the Cryptography Management page; then, click the **Apply** button. You are asked for confirmation as shown in the following illustration.



Confirm Security Setting Changes

Note: Changes to the security settings may cause existing sessions to be terminated. A new login will be required for terminated sessions. Do you wish to apply these changes?

If the IMM2 has compatible certificates and SSH Keys, the Cryptography mode is set to the NIST-800-131A Compliance Mode as shown in the following illustration.



IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

○ Basic Compatibility Mode

- This mode is compatible with older firmware versions and with browsers and other network clients that do not implement the stricter security requirements of the compliance mode below.

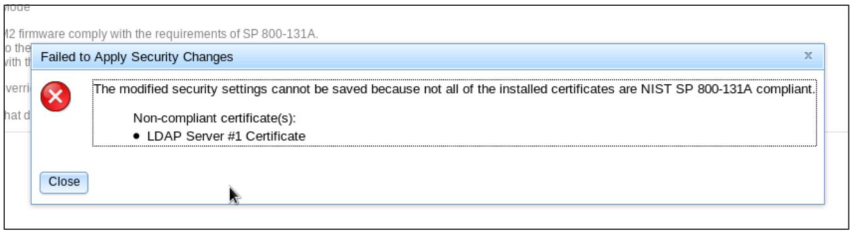
● NIST SP 800-131A Compliance Mode

- Select this mode to have the IMM2 firmware comply with the requirements of SP 800-131A.
- Note: To prevent loss of access to the IMM2, this mode should only be selected if you are sure that your browser and other network clients also work with the required SP 800-131A encryption modes.

Select the settings below to override a strict compliance.

□ Allow SNMPv3 accounts that don't comply.

If the installed certificates are not NIST-800-131A compliant the security settings cannot be changed as shown in the following illustration.



Failed to Apply Security Changes

The modified security settings cannot be saved because not all of the installed certificates are NIST SP 800-131A compliant.

Non-compliant certificate(s):

- LDAP Server #1 Certificate

Configuring the SKLM Feature on Demand option

The Security Key Lifecycle Manager (SKLM) is a software product for creating and managing security keys. The SKLM for System x Self Encrypting Drives (SED) - Features on Demand (FoD) option is a System x FoD option that enables centralized management of encryption keys. The encryption keys are used to gain access to data stored on SEDs in a System x server.

A centralized SKLM (key repository) server provides the encryption keys to unlock the SEDs in the System x server. The FoD option requires that a FoD Activation key be installed in the IMM2 FoD key repository. The Activation key for the FoD option is a unique identifier comprised of the machine type and serial number. To use the storage key/drive access functionality, the FoD key *System x TKLM Activation for Secure Drive Encryption (Type 32796 or 801C)* must be installed in the IMM2 FoD key repository. See Chapter 7, "Features on Demand," on page 187 for information pertaining to installing an activation key.

The SKLM FoD option is limited to System x IMM2-based servers. To increase security, the IMM2 can be placed in a separate management network. The IMM2 uses the network to retrieve encryption keys from the SKLM server; therefore, the SKLM server must be accessible to the IMM2 through this network. The IMM2 provides the communication channel between the SKLM server and the requesting System x server. The IMM2 firmware attempts to connect with each configured SKLM server, stopping when a successful connection is established.

The IMM2 establishes communication with the SKLM server if the following conditions are met:

- A valid FoD activation key is installed in the IMM2.
- One or more SKLM server hostname/IP addresses are configured in the IMM2.
- Two certificates (client and server) for communication with the SKLM server are installed in the IMM2.

Note: Configure at least two (a primary and a secondary) SKLM servers for your device. If the primary SLKM server does not respond to the connection attempt from the IMM2; connection attempts are initiated with the additional SKLM servers until a successful connection is established.

A Transport Layer Security (TLS) connection must be established between the IMM2 and the SKLM server. The IMM2 authenticates the SKLM server by comparing the *server* certificate submitted by the SKLM server, with the SKLM *server* certificate previously imported into the IMM2's trust store. The SLKM server authenticates each IMM2 that communicates with it and checks to verify that the IMM2 is permitted to access the SKLM server. This authentication is accomplished by comparing the *client* certificate that the IMM2 submits, with a list of trusted certificates that are stored on the SKLM server.

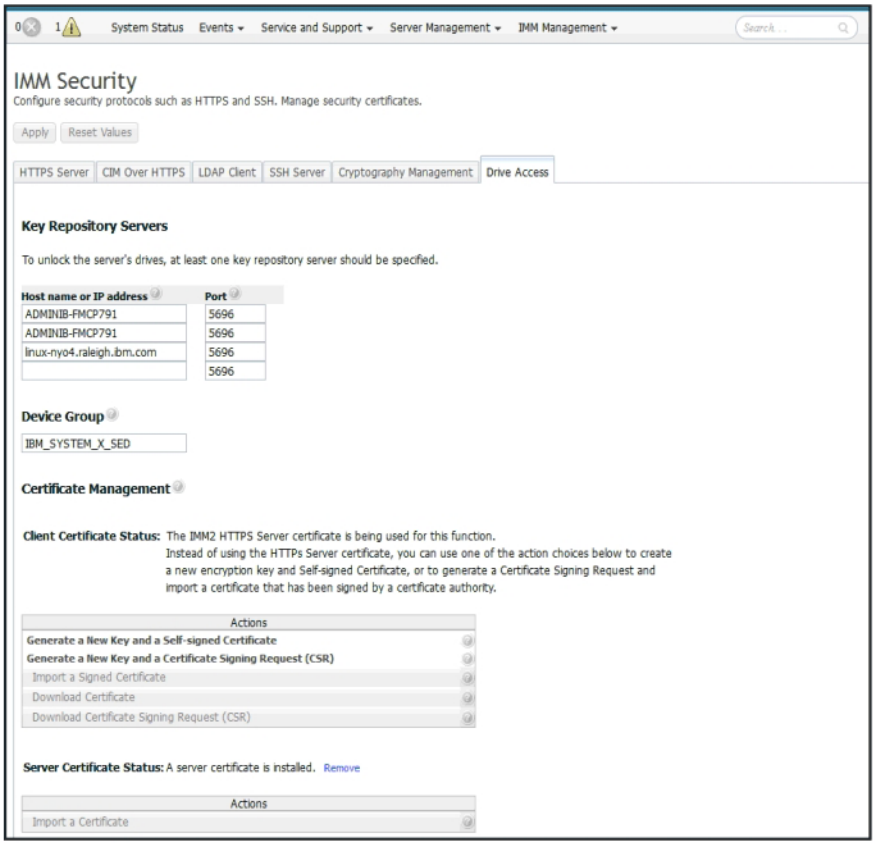
To configure SKLM settings for your server, complete the following steps:

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.
3. Click **Log In** to start the session.
4. Navigate to the top of the IMM2 window and locate the tabs below the title bar.
5. Click the **Security** option under the **IMM Management** tab.

6. Click the **Drive Access** tab on the IMM Security page.

The Drive Access page is displayed containing the following sections as shown in the next illustration:

- Key Repository Servers
- Device Group
- Certificate Management



IMM Security

Configure security protocols such as HTTPS and SSH. Manage security certificates.

Key Repository Servers

To unlock the server's drives, at least one key repository server should be specified.

Host name or IP address	Port
ADMINIB-FMCP791	5696
ADMINIB-FMCP791	5696
linux-nyo4.raleigh.ibm.com	5696
	5696

Device Group

IBM_SYSTEM_X_SED

Certificate Management

Client Certificate Status: The IMM2 HTTPS Server certificate is being used for this function. Instead of using the HTTPs Server certificate, you can use one of the action choices below to create a new encryption key and Self-signed Certificate, or to generate a Certificate Signing Request and import a certificate that has been signed by a certificate authority.

Actions
Generate a New Key and a Self-signed Certificate
Generate a New Key and a Certificate Signing Request (CSR)
Import a Signed Certificate
Download Certificate
Download Certificate Signing Request (CSR)

Server Certificate Status: A server certificate is installed. Remove

Actions
Import a Certificate

Notes:

- The **Drive Access** tab is not displayed if the SKLM FoD activation key is not installed in the IMM2.
- Additional information for the SKLM software product can be found at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=%2Fcom.ibm.sklm.doc_2.5%2Fwelcome.htm.
- The encryption key created by the SKLM server is associated with the System x server Universal Unique Identifier (UUID), machine type, and serial number. If the system board is replaced, the UUID, machine type, and serial number must be restored during the service procedure. The UUID, machine type, and serial number are necessary to obtain an existing key required for access to the SEDs. Information pertaining to restoring the UUID, machine type, and serial number can be found in the documentation for your server and by searching on the keywords *updating the Universal Unique Identifier* or searching on the keyword *UUID*.

Configuring the Key Repository Servers

The Key Repository Servers section of the Drive Access page consists of the following fields:

Host Name or IP address
Type the host name (if DNS is enabled and configured) or the IP address of the SLKM server in this field. Up to four servers can be added.

Port Type the port number for the SLKM server in this field. If this field is left blank, the default value of 5695 is used. Valid port number values are 1 to 65535.

Configuring the Device Group

The Device Group section of the Drive Access page contains the following field:

Device Group
A device group allows users to manage the keys for SEDs on multiple servers as a group. A device group with the same name must also be created on the SKLM server. The default value for this field is IBM_SYSTEM_X_SED.

Establishing Certificate Management

Client and server certificates are used to authenticate the communication between the SKLM server and the IMM2 located in the System x server. Client and server certificate management are discussed in this section.

Client Certificate Management: Client certificates are classified as one of the following:

- An IMM2 self-assigned certificate
- A certificate generated from an IMM2 CSR and signed (externally) by a third party CA.

A client certificate is required for communication with the SKLM server. The client certificate contains digital signatures for the CA and the IMM2.

Notes:

- Certificates must be preserved across firmware updates.
- If a client certificate is not created for communication with the SKLM server, the IMM2 HTTPS server certificate is used.
- The function of the CA is to verify the identity of the IMM2.

To create a client certificate locate the Client Certificate Status section on the Drive Access page. Under the Actions menu of the Client Certificate Status section, select one of the following items:

- Generate a New Key and a Self-Signed Certificate
- Generate a New Key and a Certificate Signing Request (CSR)

The **Generate a New Key and a Self-Signed Certificate** action item generates a new encryption key and a self-signed certificate. In the Generate New Key and Self-Signed Certificate window, type or select the information in the required fields and any optional fields that apply to your configuration, (see the following table). Click **Ok**, to generate your encryption key and certificate. A progress window displays while the self-signed certificate is being generated. A confirmation window is displayed when the certificate is successfully installed.

Note: The new encryption key and certificate replace any existing key and certificate.

Table 6. Generate a New Key and a Self-Signed Certificate

Field	Description
Country[1]	From the list item, select the country where the IMM2 physically resides.
State or Providence[1]	Type the state or providence where the IMM2 physically resides.
City or Locality[1]	Type the city or locality where the IMM2 physically resides.
Organization Name[1]	Type the company or organization name that owns the IMM2.
IMM2 Host Name[1]	Type the IMM2 host name that appears in the web address bar.
Contact Person	Type the name of the contact person that is responsible for the IMM2.
Email address	Type the email address of the contact person responsible for the IMM2.
Organization Unit	Type the unit within the company that owns the IMM2.
Surname	Type the surname of the person responsible for the IMM2. This field can contain a maximum of 60 characters.
Given Name	Type the given name of the person responsible for the IMM2. This field can contain a maximum of 60 characters.
Initials	Type the initials of the person responsible for the IMM2. This field can contain a maximum of 20 characters.
DN Qualifier	Type the Distinguished Name Qualifier for the IMM2. This field can contain a maximum of 60 characters.
1. This is a required field.	

After the client certificate has been generated you can download the certificate to storage on your IMM2 by selecting the **Download Certificate** action item.

The **Generate a New Key and a Certificate Signing Request (CSR)** action item generates a new encryption key and a CSR. In the Generate a New Key and a Certificate Signing Request window, type or select the information in the required fields and any optional fields that apply to your configuration, (see the following table). Click **Ok**, to generate your new encryption key and CSR.

A progress window displays while the CSR is being generated and a confirmation window is displayed upon successful completion. After generation of the CSR you must send the CSR to a CA for digital signing. Select the **Download Certificate Signing Request (CSR)** action item and click **Ok** to save the CSR to your server. You can then submit the CSR to your CA for signing.

Table 7. Generate a New Key and a Certificate Signing Request

Field	Description
Country[1]	From the list item, select the country where the IMM2 physically resides.
State or Providence[1]	Type the state or providence where the IMM2 physically resides.
City or Locality[1]	Type the city or locality where the IMM2 physically resides.
Organization Name[1]	Type the company or organization name that owns the IMM2.

Table 7. Generate a New Key and a Certificate Signing Request (continued)

Field	Description
IMM2 Host Name[1]	Type the IMM2 host name that appears in the web address bar.
Contact Person	Type the name of the contact person that is responsible for the IMM2.
Email address	Type the email address of the contact person responsible for the IMM2.
Organization Unit	Type the unit within the company that owns the IMM2.
Surname	Type the surname of the person responsible for the IMM2. This field can contain a maximum of 60 characters.
Given Name	Type the given name of the person responsible for the IMM2. This field can contain a maximum of 60 characters.
Initials	Type the initials of the person responsible for the IMM2. This field can contain a maximum of 20 characters.
DN Qualifier	Type the Distinguished Name Qualifier for the IMM2. This field can contain a maximum of 60 characters.
Challenge Password	Type the password to the CSR. This field can contain a maximum of 30 characters.
Unstructured Name	Type additional information, such as an unstructured name that is assigned to the IMM2. This field can contain a maximum of 60 characters.
1. This is a required field.	

The CSR is digitally signed by the CA using the user's certificate processing tool, such as the *OpenSSL* or *Certutil* command line tool. All client certificates that are signed using the user's certificate processing tool have the same *base* certificate. This *base* certificate must also be imported to the SKLM server so that all servers digitally signed by the user are accepted by the SKLM server.

After the certificate has been signed by the CA you must import it into the IMM2. Select the **Import a Signed Certificate** action item and select the file to upload as the client certificate; then, click the **Ok** button. A Progress window displays while the CA-signed certificate is being uploaded. A Certificate Upload window is displayed if the upload process is successful. A Certificate Upload Error window is displayed if the upload process is not successful.

Notes:

- For increased security use a certificate that is digitally signed by a CA.
- The certificate that is imported into the IMM2 must correspond to the CSR that was previously generated.

After a CA-signed certificate is imported into the IMM2, select the **Download Certificate** action item. When you select this action item, the CA-signed certificate is downloaded to storage on your IMM2.

Server Certificate Management: The server certificate is generated in the SLKM server and must be imported into the IMM2 before the secure drive access functionality will work. The server certificate that is exported from the SKLM server must be in the Distinguished Encoding Rules (DER) format. To import the certificate that authenticates the SKLM server to the IMM2, click **Import a Certificate** from the Server Certificate Status section of the Drive Access page. A progress indicator is displayed as the file is transferred to storage on the IMM2.

Note: Certificates must be preserved across firmware updates.

After the server certificate is successfully transferred to the IMM2, the Server Certificate Status area displays the following content: `A server certificate is installed`.

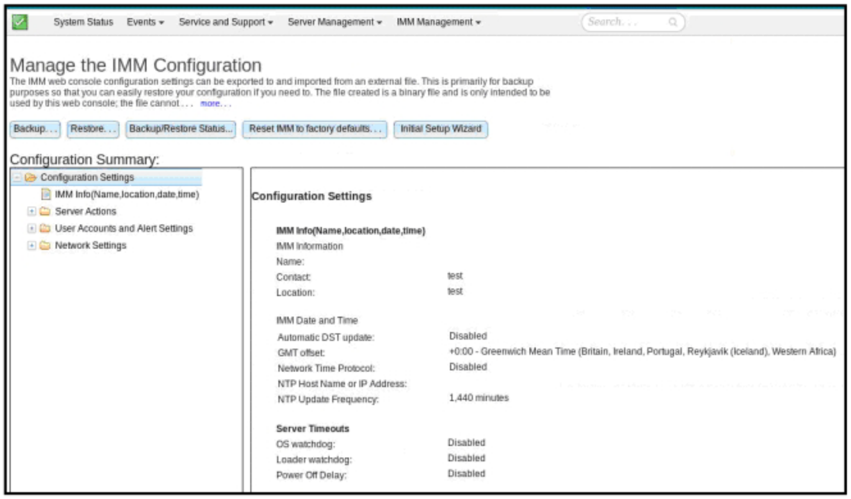
The **Remove** button is now available for the trusted certificate. If you want to remove a trusted certificate, click the corresponding **Remove** button.

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.



Manage the IMM Configuration

The IMM web console configuration settings can be exported to and imported from an external file. This is primarily for backup purposes so that you can easily restore your configuration if you need to. The file created is a binary file and is only intended to be used by this web console; the file cannot . . . more. . .

Configuration Settings

IMM Info(Name,location,date,time)

IMM Information

Name:	
Contact:	test
Location:	test

IMM Date and Time

Automatic DST update:	Disabled
GMT offset:	+0:00 - Greenwich Mean Time (Britain, Ireland, Portugal, Reykjavik (Iceland), Western Africa)
Network Time Protocol:	Disabled
NTP Host Name or IP Address:	
NTP Update Frequency:	1,440 minutes

Server Timeouts

OS watchdog:	Disabled
Loader watchdog:	Disabled
Power Off Delay:	Disabled

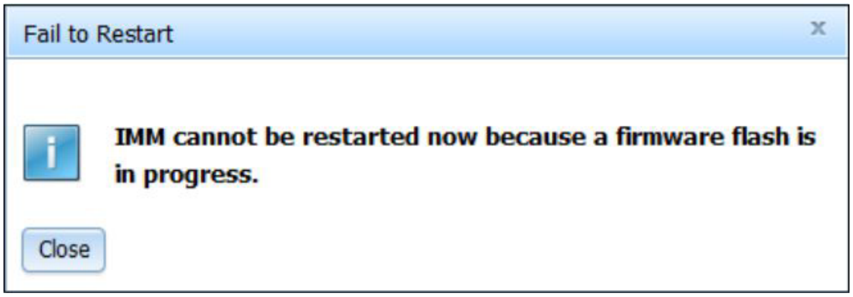
Restarting the IMM2

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).



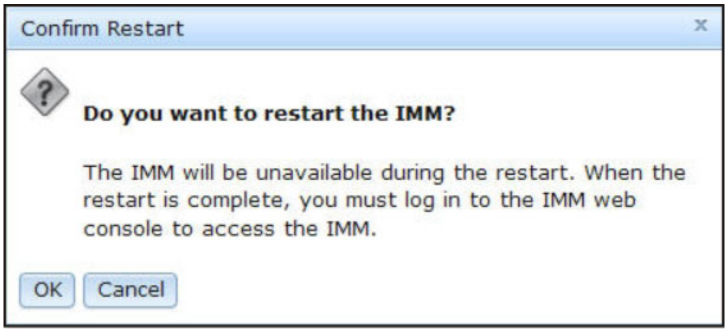
Fail to Restart

IMM cannot be restarted now because a firmware flash is in progress.

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.



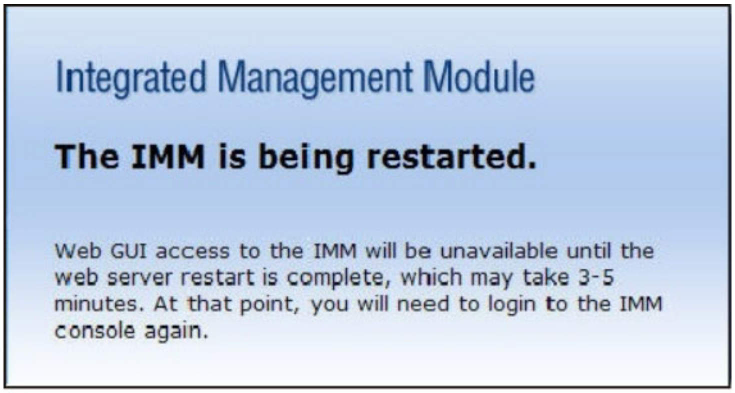
Confirm Restart

Do you want to restart the IMM?

The IMM will be unavailable during the restart. When the restart is complete, you must log in to the IMM web console to access the IMM.

   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.



Integrated Management Module

The IMM is being restarted.

Web GUI access to the IMM will be unavailable until the web server restart is complete, which may take 3-5 minutes. At that point, you will need to login to the IMM console again.

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.

The settings supported by the IMM2 and their default values can vary depending on the server the IMM2 resides in. The default values for the settings that are supported by the IMM2 can be determined by using the ASU. Use the **ASU showdefault** command to collect and report the default factory settings from the IMM2.

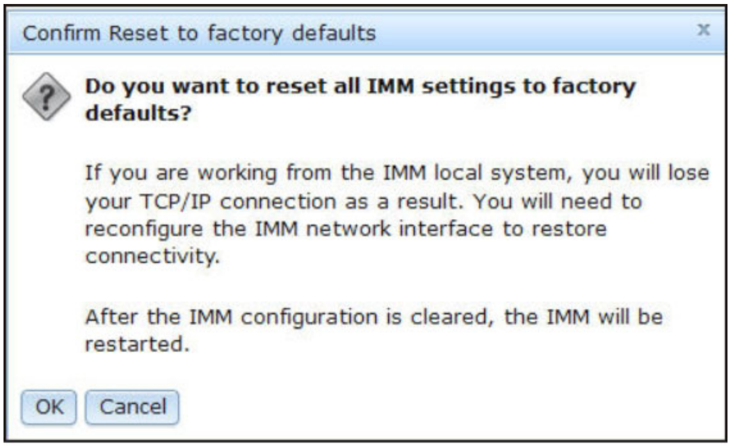
To display all of the IMM2 default settings, enter the following command:

```
asu showdefault IMM [-v] [-nx] [connect_options]
```

For additional information about the **ASU showdefault** command, see the chapter that describes the ASU commands in the *Advanced Settings Utility User's Guide*.

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).



Confirm Reset to factory defaults

Do you want to reset all IMM settings to factory defaults?

If you are working from the IMM 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.

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 Feature on Demand (FoD) features. See Chapter 7, “Features on Demand,” on page 187 for information about managing FoD activation keys.

Chapter 5. Monitoring the server status

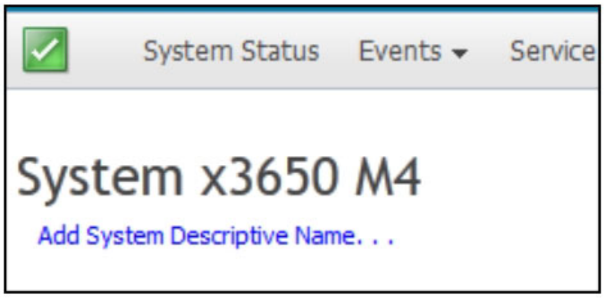
This chapter provides information about how to view and monitor the information for the server that you are accessing.

Viewing the system status

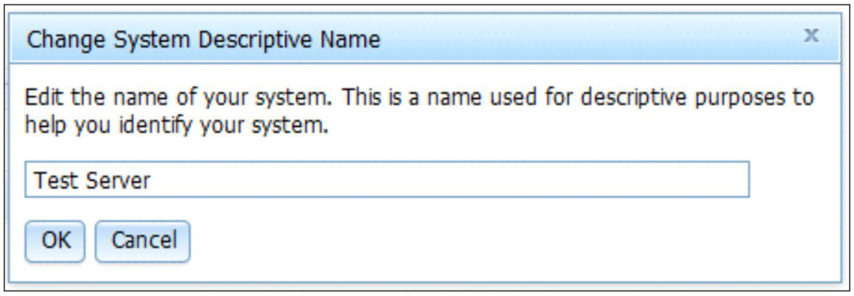
The System Status page provides an overview of the operating status of the IMM2 server. This page also displays the hardware health of the server and any active events occurring on the server.

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).

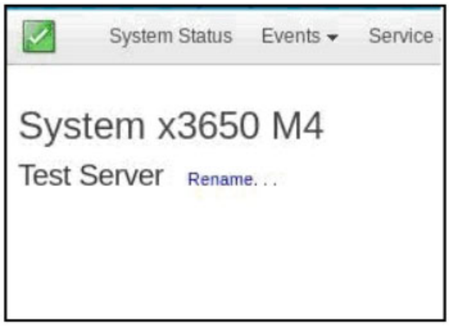


Edit the name of your system. This is a name used for descriptive purposes to help you identify your system.

Test Server

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.

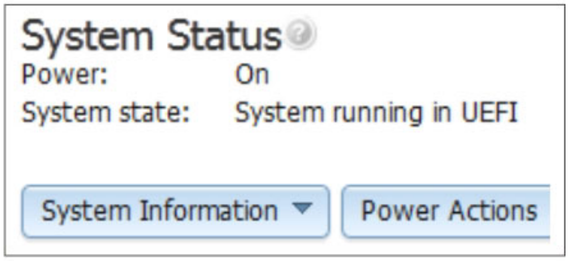


System x3650 M4

Test Server

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.



Power: On

System state: System running in UEFI

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

Table 8. 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.
Booting operating system or in unsupported operating system	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 • The IMM2 Ethernet over USB interface is disabled. • The operating system does not have the drivers loaded that support the Ethernet over USB interface.
operating system booted	The server operating system 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.

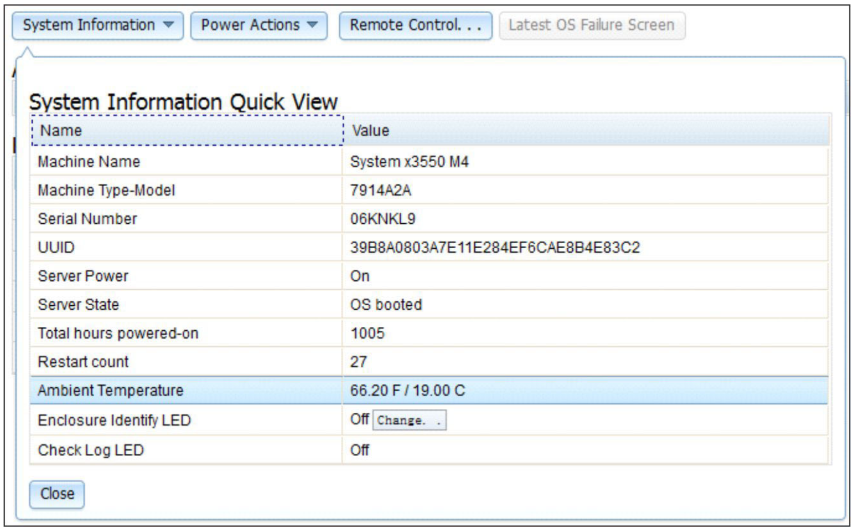
- System Information
- Power Actions
- Remote Control, (see "Remote presence and remote control functions" on page 123 for additional information).
- Latest OS Failure Screen, (see "Capturing the latest OS failure screen data" on page 158 for additional information).

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.



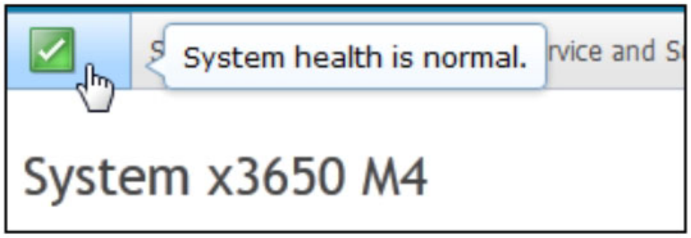
System Information Quick View

Name	Value
Machine Name	System x3550 M4
Machine Type-Model	7914A2A
Serial Number	06KNKL9
UUID	39B8A0803A7E11E284EF6CAE8B4E83C2
Server Power	On
Server State	OS booted
Total hours powered-on	1005
Restart count	27
Ambient Temperature	66.20 F / 19.00 C
Enclosure Identify LED	Off Change. .
Check Log LED	Off

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.

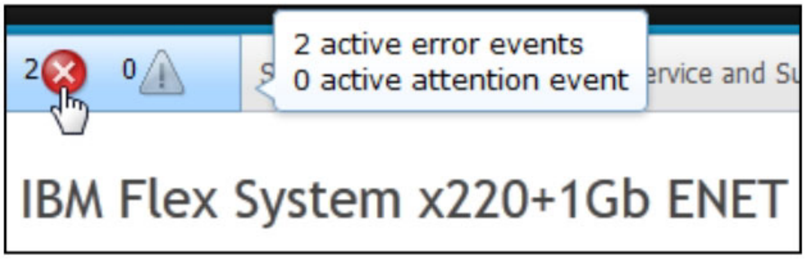


System health is normal.

System x3650 M4

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.

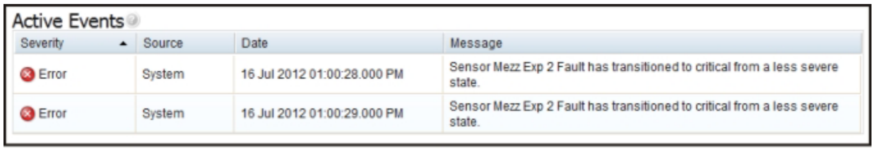


2 active error events
0 active attention event

IBM Flex System x220+1Gb ENET

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.



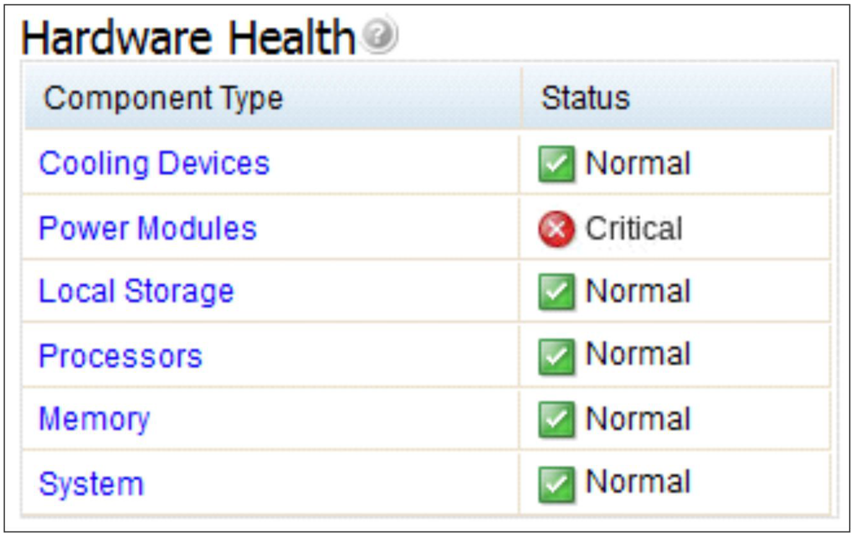
Active Events

Severity ▲	Source	Date	Message
✕ Error	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.
✕ Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.

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.

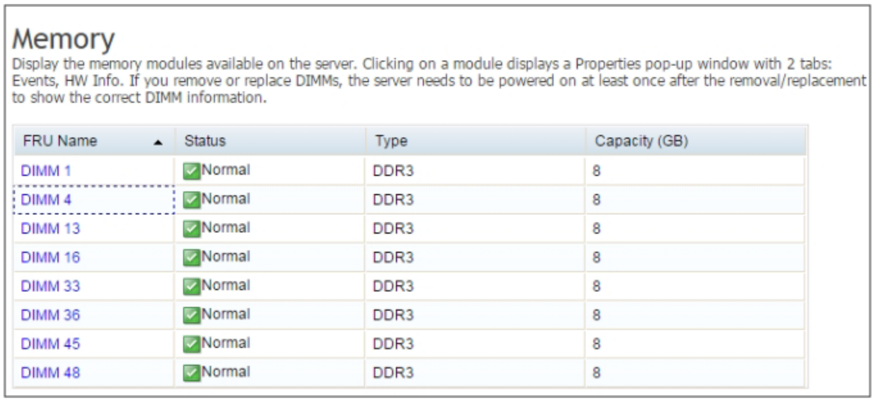


Hardware Health

Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✗ Critical
Local Storage	✓ Normal
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

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.



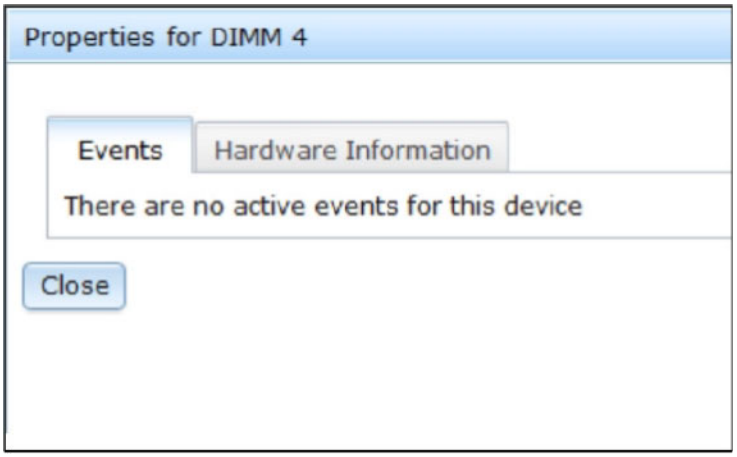
Memory

Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Events, HW Info. If you remove or replace DIMMs, the server needs to be powered on at least once after the removal/replacement to show the correct DIMM information.

FRU Name ▲	Status	Type	Capacity (GB)
DIMM 1	✓ Normal	DDR3	8
DIMM 4	✓ Normal	DDR3	8
DIMM 13	✓ Normal	DDR3	8
DIMM 16	✓ Normal	DDR3	8
DIMM 33	✓ Normal	DDR3	8
DIMM 36	✓ Normal	DDR3	8
DIMM 45	✓ Normal	DDR3	8
DIMM 48	✓ Normal	DDR3	8

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.

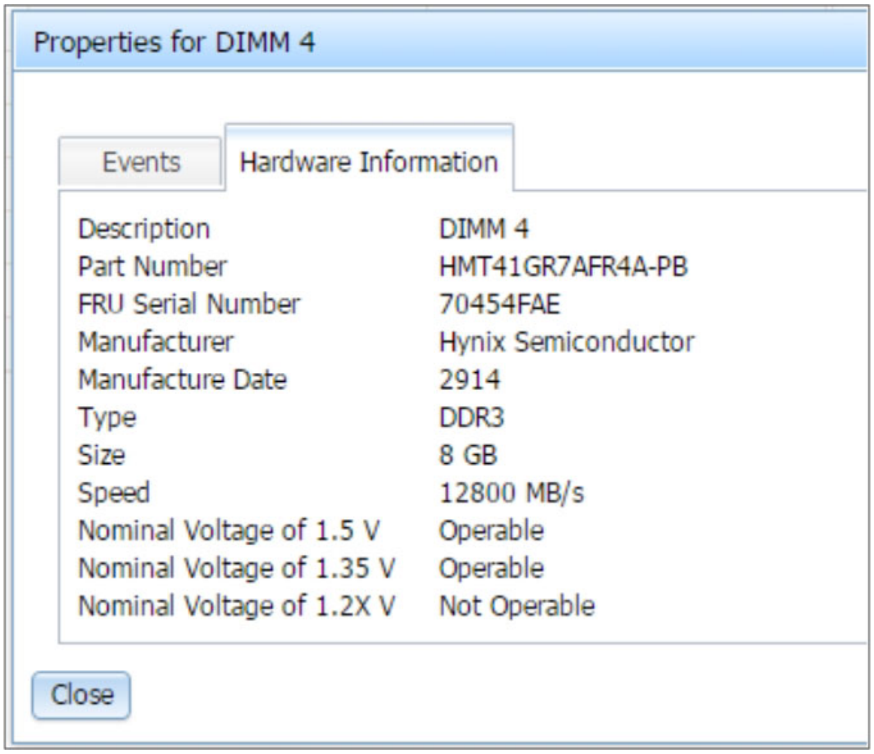


Properties for DIMM 4

There are no active events for this device

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.



Properties for DIMM 4

Description	DIMM 4
Part Number	HMT41GR7AFR4A-PB
FRU Serial Number	70454FAE
Manufacturer	Hynix Semiconductor
Manufacture Date	2914
Type	DDR3
Size	8 GB
Speed	12800 MB/s
Nominal Voltage of 1.5 V	Operable
Nominal Voltage of 1.35 V	Operable
Nominal Voltage of 1.2X V	Not Operable

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.

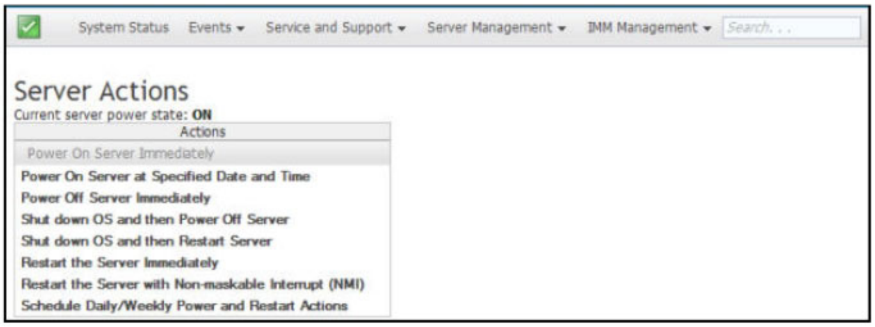
Important: Some options may not be available on your server's operating-system platform. Options that are displayed for the Server Management tab are contingent on the server's operating-system platform where the IMM2 is located and the adapters that are installed in the server.

- 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 Local Storage option, you can view the storage device's physical structure and storage configuration.
- 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 Adapters option, you can view information about the adapters that are 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.
- From the Scalable Complex option, you can view and manage the current state of all available nodes (servers).

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.


System Status
Events ▾
Service and Support ▾
Server Management ▾
IMM Management ▾
Search. . .

Server Actions

Current server power state: **ON**

Actions
Power On Server Immediately
Power On Server at Specified Date and Time
Power Off Server Immediately
Shut down OS and then Power Off Server
Shut down OS and then Restart Server
Restart the Server Immediately
Restart the Server with Non-maskable Interrupt (NMI)
Schedule Daily/Weekly Power and Restart Actions

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 9. 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.

Table 9. Power actions and descriptions (continued)

Power Action	Description
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.
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.
- If you have firewalls in your network, a network port must be opened to support the Remote Control feature. To view or change the network port number used by the Remote Control feature, see “Configuring port assignments” on page 92.

Updating your IMM2 firmware and Java or 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.

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 187.

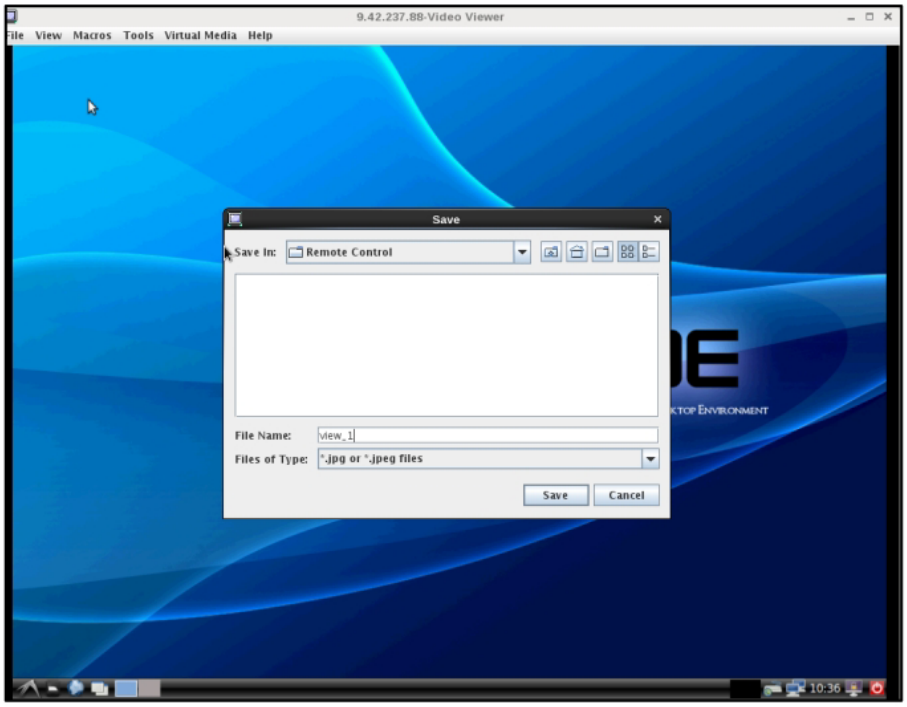
Remote control screen capture

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.



Save In: Remote Control

File Name: view_1

Files of Type: *.jpg or *.jpeg files

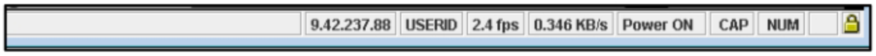
Remote control Video Viewer modes

To change the view of the Video Viewer window, click the **View** tab and the appropriate option.

The following menu options are available:

Status Bar
Click **View > Status Bar** to hide or display the status bar. The status bar displays the following items (as shown in the following illustration):

- The caps lock state
- The num lock state
- The system power state
- The IMM IP address
- The user id
- The update speed
- If Encryption of Disk and KVM data is selected

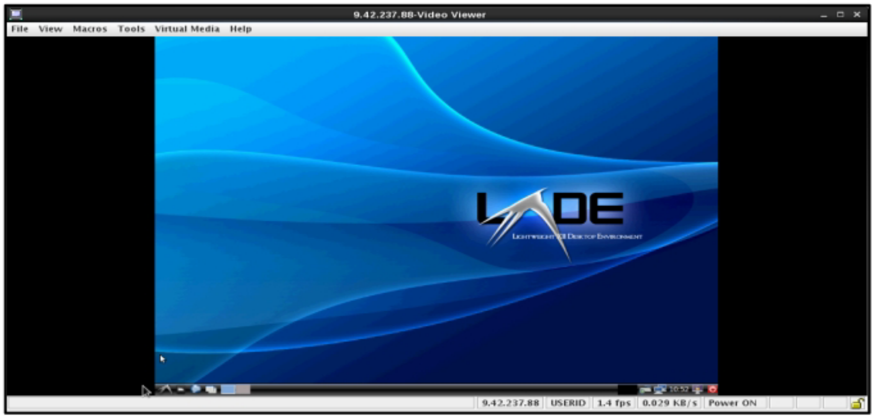


Refresh
Click **View > Refresh** to redraw the video display with the video data from the server.

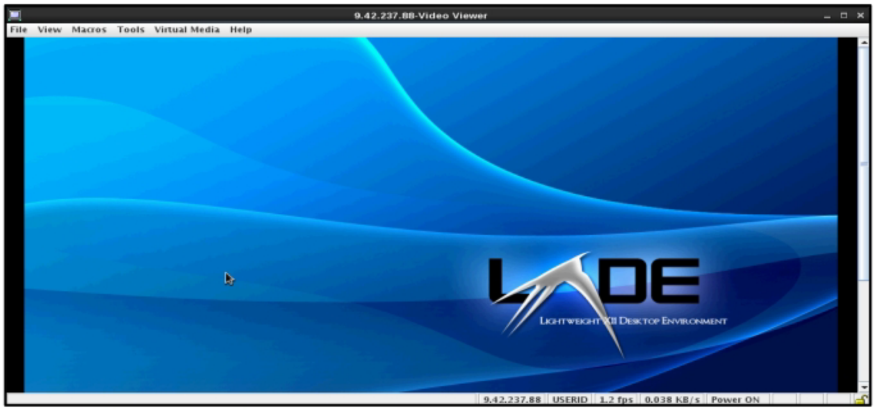
Video Scaling
Click **View > Video Scaling** to enable scaling for the video display. With Video Scaling *enabled*, the video image is sized so that the complete image is within the console window, (as shown in the following illustration).

Notes:

- If aspect ratio maintenance is in effect the display is sized so that the vertical (height) *or* horizontal (width) dimension completely fill the console window. If one dimension cannot fill the console window and still maintain the aspect ratio of the image; then, the area around the video image will be filled.
- If aspect ratio maintenance is not in effect; then, the image fills the console window in *both* (vertical and horizontal) dimensions.


9.42.237.88-Video Viewer
File View Macros Tools Virtual Media Help
LXDE
Lightweight X11 Desktop Environment
9.42.237.88 | USERID | 1.4 fps | 0.029 KB/s | Power ON

If video scaling is *not* enabled when the console window is re-sized the image will not be scaled. Scroll bars might be shown for access to parts of the video image not immediately viewable. If the console window size is larger than the video image the image is inset into the console window and surrounded by black bars, (as shown in the following illustration).


9.42.237.88-Video Viewer
File View Macros Tools Virtual Media Help
LXDE
Lightweight X11 Desktop Environment
9.42.237.88 | USERID | 1.2 fps | 0.038 KB/s | Power ON

Fit
Click **View > Fit** to completely display the target desktop *without* an extra border or scroll bars. This option requires that the client desktop is large enough to display the re-sized window.

Full Screen
Click **View > Full Screen** to fill the client desktop with the video display. When the Full Screen option is enabled, the Video Viewer menu becomes a floating menu.

Mini-Mode
Click **View > Mini-Mode** to display a *thumbnail* view of the host server display. This option provides no input for the keyboard or mouse and minimizes the Video Viewer window to the dimensions specified on the **Mini-Mode** tab of the Session Options window.

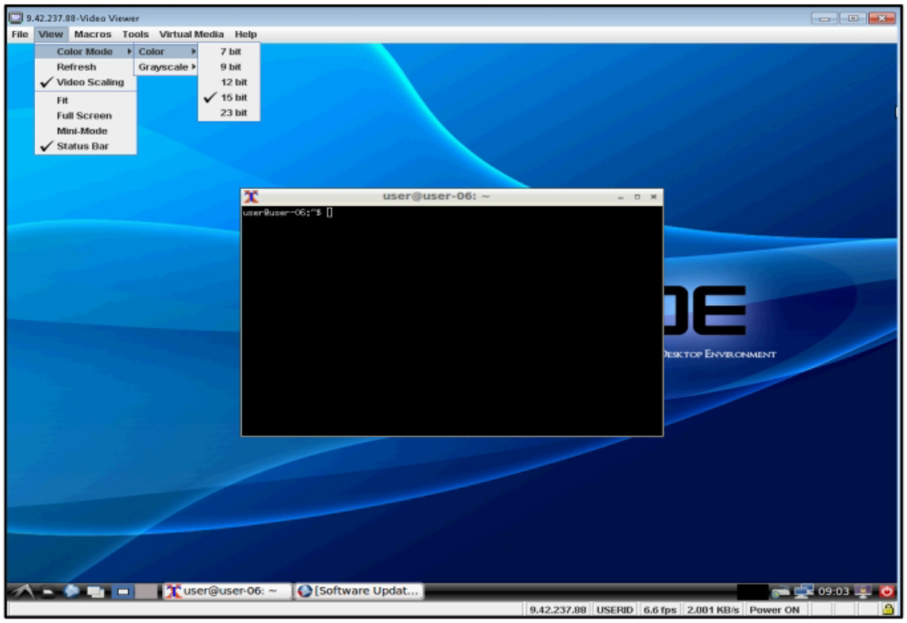
Remote control video color mode

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 the **View** tab and click the **Color Mode** option; then, select your color mode. Two color-mode choices are available, (as shown in the following illustration):
   - Color: 7, 9, 12, 15, and 23 bit
   - Grayscale: 16, 32, 64, and 128 shades



```
user@user-06:~$ []
```

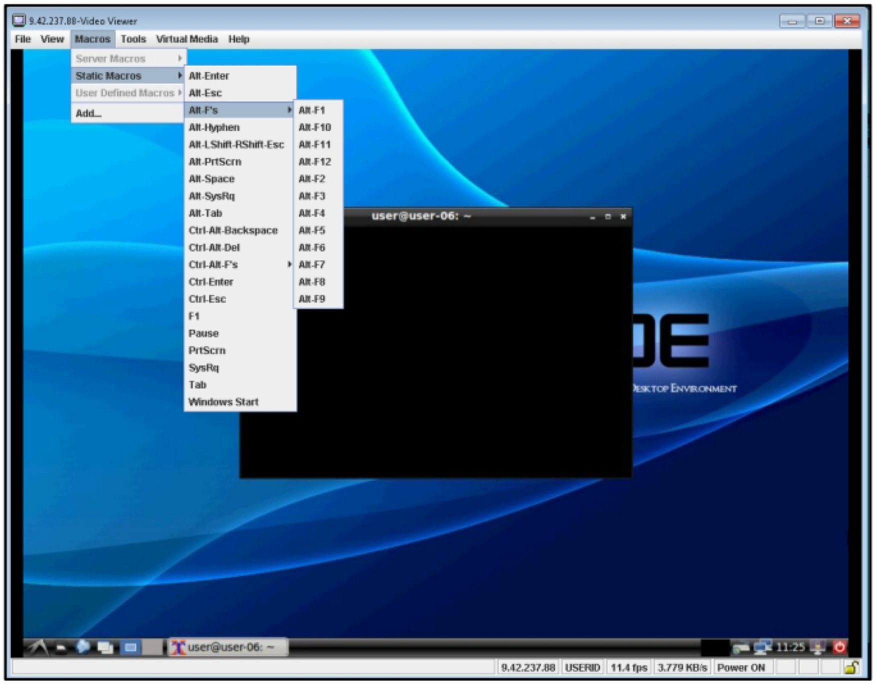
Remote control keyboard support

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. Macros provide a mechanism to send keystrokes to the operating system of the server that the user might; otherwise, not be able to send.

In the Video Viewer window under the **Macros** tab there are four options that are used to define and create macros, (as shown in the following illustration):

- Click **Macros > Server Macros** to use server defined macros. Server defined macros are downloaded from the IMM2.
  - A server defined macro can be associated with a hot-key.
  - The hot keys associated with server defined macros are F7 through F12 (with or without modifier keys Ctrl, Alt, and Shift).
- Click **Macros > Static Macros** to use predefined macros.

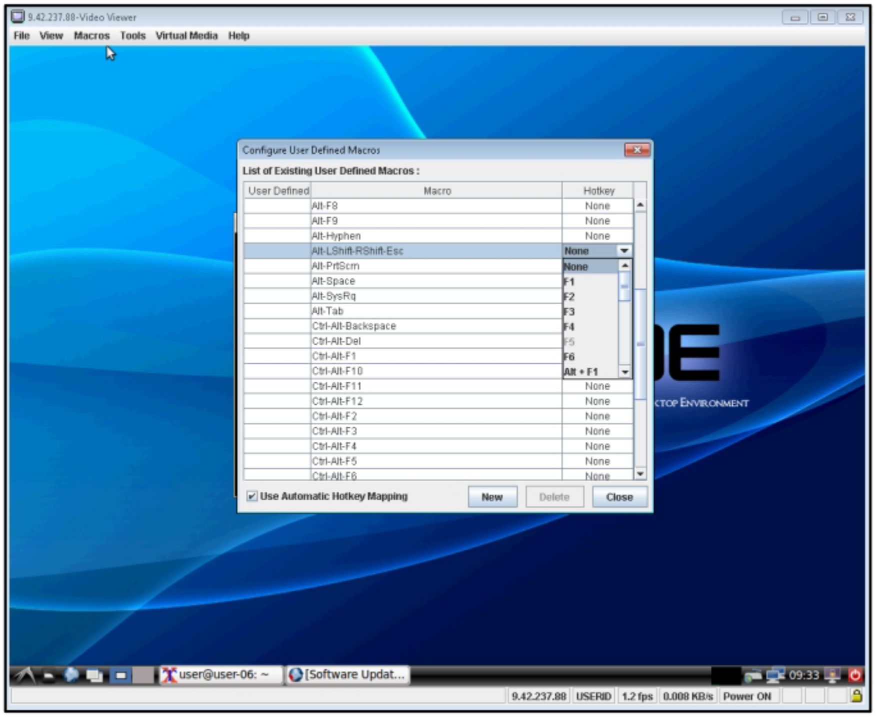
- Click **Macros > User Defined Macros** to create your custom macros.
  - The hot keys associated with user defined macros are F1 through F6 (with or without modifier keys Ctrl, Alt, and Shift).
- Click **Macros > Add** to assign hot keys and create user defined macros.



A hot key can be associated with a user defined macro or a server macro. A hot key is a special keystroke that when pressed instruct the operating system of the client server to perform the *associated* keyboard macro. The order of key entry direction and execution is as follows:

1. Highest priority
   - A hot key that is assigned to a macro. The macro assigned to the hot key is sent to the host server.
2. Keyboard pass-through
   - When keyboard pass-through is enabled, all keystrokes and key combinations (with the exception of the Ctrl+Alt+Del keystroke combination in Windows) and not assigned as a hot key to a macro are sent to the host server.
3. Non-keyboard pass-through
   - When keyboard pass-through is not enabled and if the entered key or key combination is not assigned as a hot key to a macro; then, the keystrokes are sent to the host server. The exception to this rule is if the keystrokes are *normally* routed to the client workstation operating system.

Assigning a hot key:
Click **Macros > Add** to assign a hot key. The Configure User Defined Macros window is displayed. This window contains a list of existing user defined macros, (as shown in the following illustration). Select the applicable macro and use the drop-down menu to associate the hot key to the macro.



List of Existing User Defined Macros :

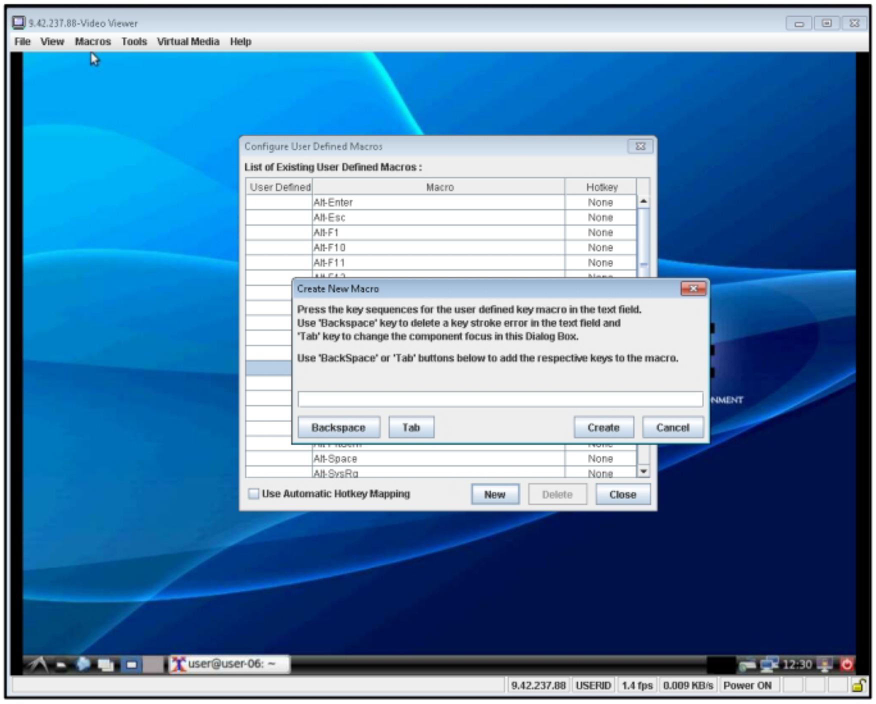
User Defined	Macro	Hotkey
	Alt-F8	None
	Alt-F9	None
	Alt-Hyphen	None
	Alt-LShift-RShift-Esc	None
	Alt-PrtScrn	
	Alt-Space	
	Alt-SysRq	
	Alt-Tab	
	Ctrl-Alt-Backspace	
	Ctrl-Alt-Del	
	Ctrl-Alt-F1	
	Ctrl-Alt-F10	
	Ctrl-Alt-F11	None
	Ctrl-Alt-F12	None
	Ctrl-Alt-F2	None
	Ctrl-Alt-F3	None
	Ctrl-Alt-F4	None
	Ctrl-Alt-F5	None
	Ctrl-Alt-F6	None

☑ Use Automatic Hotkey Mapping

New Delete Close

Located in the Configure User Defined Macros window is the **Use Automatic Hotkey Mapping** check box. When selected, this check box permits *automatic* reassignment of the hotkeys.

Creating a user defined macro:
To create a user defined macro, click the **Macros > Add** menu item. In the resulting Configure User Defined Macros window, click the **New** button. A Create New Macro window is displayed. Follow the instructions in the Create New Macro window to create your user defined macro, (as shown in the following illustration). The User Defined column indicates if the macro is created by the user. If a macro is created by the user and once that macro is selected the **Delete** button is enabled, allowing the macro to be deleted if desired.


9.42.237.88-Video Viewer
File
View
Macros
Tools
Virtual Media
Help
Configure User Defined Macros
List of Existing User Defined Macros :

User Defined	Macro	Hotkey
	Alt-Enter	None
	Alt-Esc	None
	Alt-F1	None
	Alt-F10	None
	Alt-F11	None
	Alt-Space	None
	Alt-SysRq	None

Press the key sequences for the user defined key macro in the text field.
Use 'Backspace' key to delete a key stroke error in the text field and
'Tab' key to change the component focus in this Dialog Box.

Use 'BackSpace' or 'Tab' buttons below to add the respective keys to the macro.

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 event and passes it along to the server. The server detects the same physical keystrokes that the client experiences. The server 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 the server layout back again.

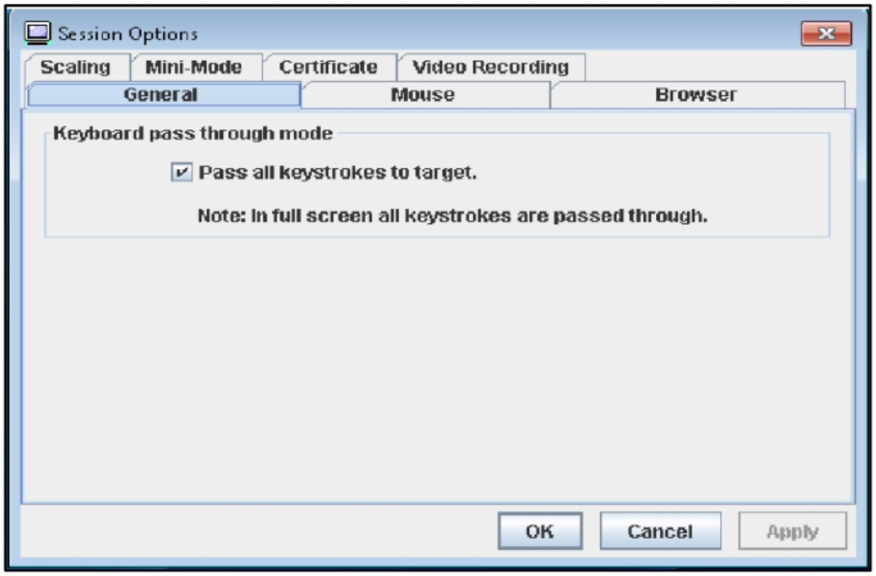
Keyboard pass-through mode

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. The keyboard pass-through mode 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 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 (as shown in the following illustration):

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 your choice.



Keyboard pass through mode

☑ Pass all keystrokes to target.

Note: In full screen all keystrokes are passed through.

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

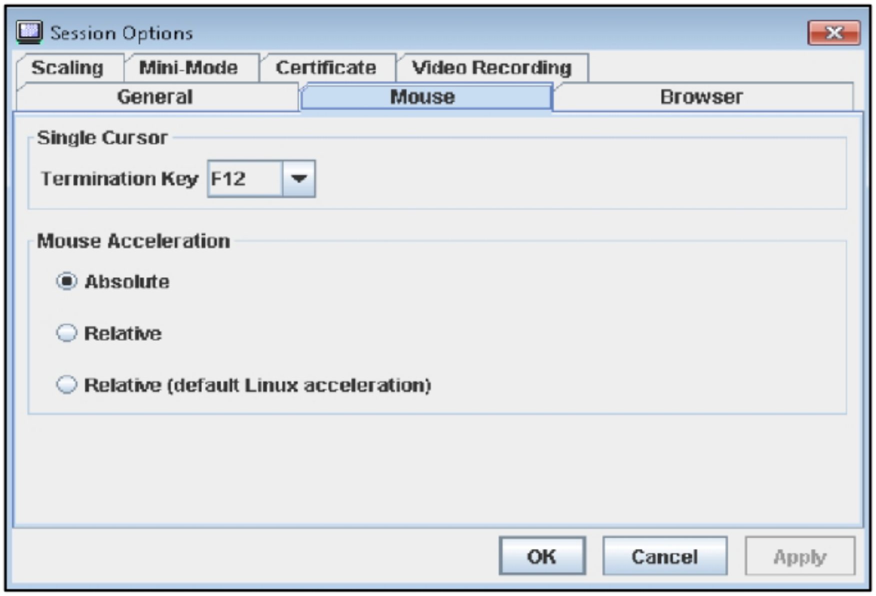
To access the absolute and relative options for controlling the mouse, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Select **Session Options** from the menu.
3. When the Session Options window opens, click the **Mouse** tab.
4. Select one of the following **Mouse Acceleration** modes (as shown in the following illustration):

   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
   The **Relative** mode is the default value for Linux applications. 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

Termination Key F12

Mouse Acceleration

● Absolute

○ Relative

○ Relative (default Linux acceleration)

Single cursor mode

Some operating systems do not align the local and remote cursors, which result 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 only see 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.

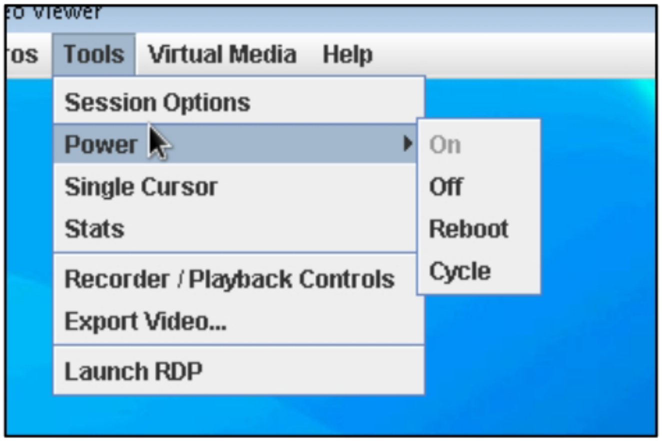
To view or change the **Termination Key** field, click **Video Viewer > Session Options > Mouse** and make your selection.

To disable the single cursor mode, click the **Termination Key**.

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 (as shown in the following illustration):
   - On
     - Turn on the server power
   - Off
     - Turn off the server power
   - Reboot
     - Restart the server
   - Cycle
     - Turn 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 (as shown in the next illustration):

Frame Rate
This field contains a running average of the number of frames, decoded per second by the client.

Bandwidth
This field contains a running average of the total number of kilobytes per second received by the client.

Compression
This field contains 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
This field contains a running average of the number of video packets received per second.

Target Drive
This field contains the type of device such as CD/DVD, Removable Disk, or Floppy Disk.

Mapped To
This field contains the local device or image file that the host server device is mapped to. If the appliance or service processor is indicating that a device is mapped; then, the **Mapped To** field is set to `Not Local`.

Duration
This field contains the elapsed time that the device has been mapped by the client in minutes and seconds.

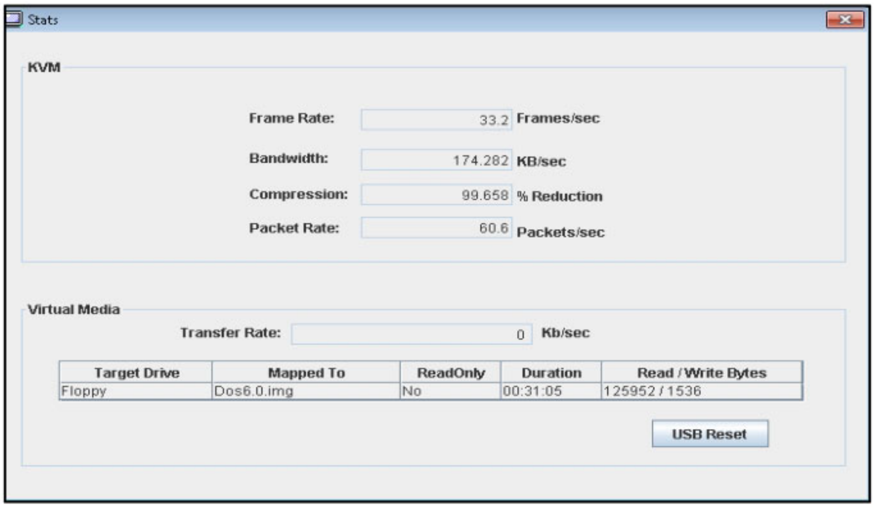
ReadOnly
This field indicates if the drive is read-only.

Read/Write Bytes
This field contains the number of bytes read and written to the drive.

Transfer Rate
This field contains the Megabytes (MB) per second data transfer rate of media between the client and the server.

USB Reset

If you select this button the USB bus on IMM2 is reset.



Frame Rate: 33.2 Frames/sec

Bandwidth: 174.282 KB/sec

Compression: 99.658 % Reduction

Packet Rate: 60.6 Packets/sec

Transfer Rate: 0 Kb/sec

Target Drive	Mapped To	ReadOnly	Duration	Read / Write Bytes
Floppy	Dos6.0.img	No	00:31:05	125952 / 1536

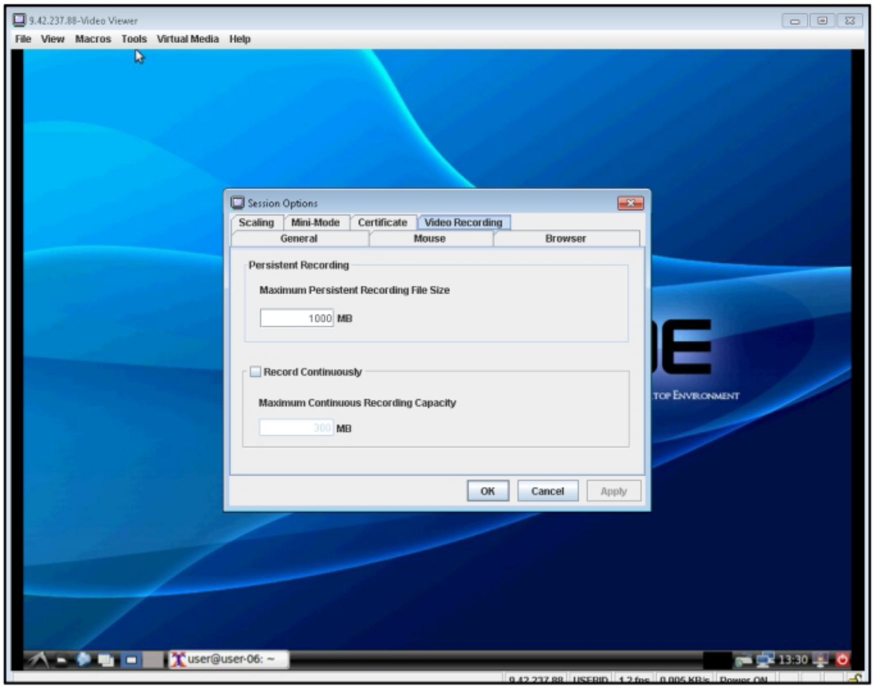
Starting Remote Desktop Protocol

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. Click **Tools > Launch RDP** from the Video Viewer window to launch the RDP client.

Video Recording

The client contains a built-in video recorder and player. The live recorder can operate the entire length of time a session is in progress. The live recorder can continuously store video in blocks of 30 seconds up to a maximum retained video of 30 minutes. If the maximum retained video limit is exceeded the earliest blocks of video are released. To initiate video recording, complete the following steps:

1. In the Video Viewer window click **Tools > Session Options**.
2. In the Session Options window click the **Video Recording** tab to choose one of the following recording preferences, (as shown in the following illustration).
   - Enter the maximum file size for persistent recordings in the **Maximum Persistent Recording File Size** field.
   - Click the **Record Continuously** check box if continuous recording is in effect; then, enter the maximum space taken by the continuous recording buffer in the **Maximum Continuous Recording Capacity** field.
3. Click **OK** to save your selection.



Persistent Recording

Maximum Persistent Recording File Size

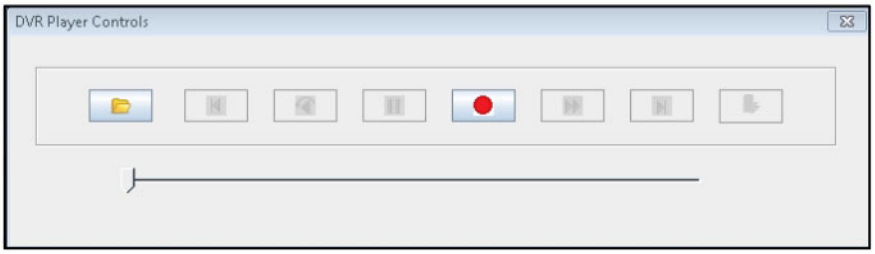
1000 MB

□ Record Continuously

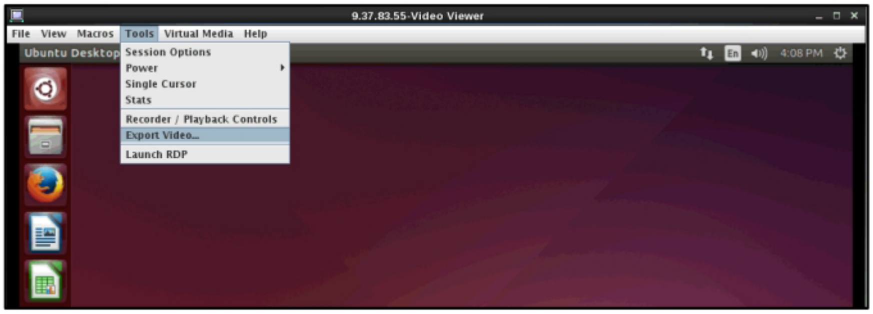
Maximum Continuous Recording Capacity

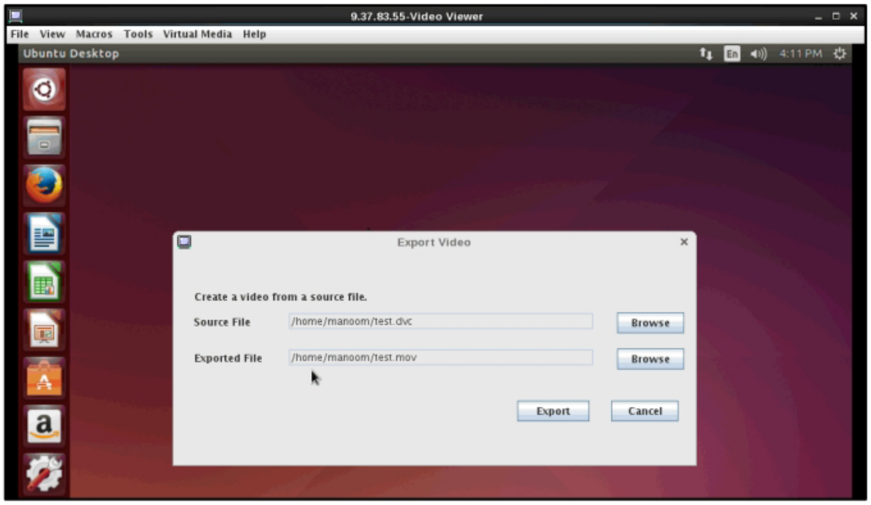
300 MB

From the Video Viewer window, click **Tools > Recorder/Playback Controls** to playback the video and operate the recording controls. The DVR Player Controls window is displayed, (as shown in the following illustration).



From the Video Viewer window click **Tools > Export Video** to transform recorded video to a standard type of format that can be played back with commercial products such as Windows Media or Quicktime Player, (as shown as the following illustrations).





Create a video from a source file.

Source File: /home/manoom/test.dvc

Exported File: /home/manoom/test.mov

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.

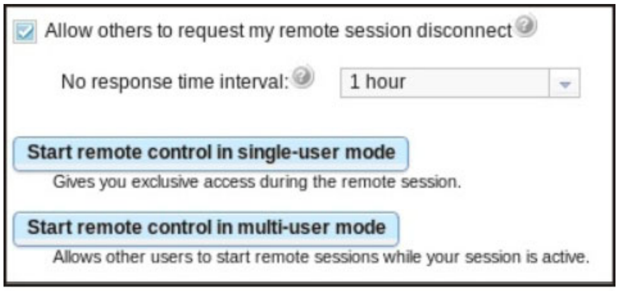
To enable the Knock-knock feature complete the following steps:

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 step 2 on page 136 through step 4 on page 136.



☑ Allow others to request my remote session disconnect

No response time interval: 1 hour

Start remote control in single-user mode

Gives you exclusive access during the remote session.

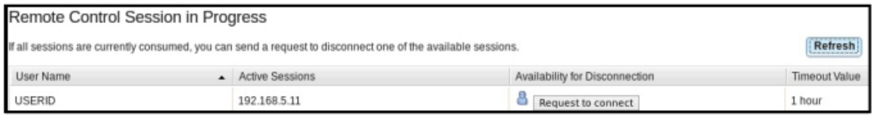
Start remote control in multi-user mode

Allows other users to start remote sessions while your session is active.

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.

   Remote Control Session in Progress

   If all sessions are currently consumed, you can send a request to disconnect one of the available sessions.

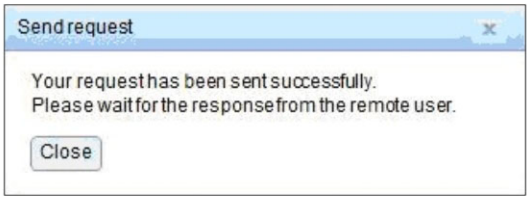
User Name ▲	Active Sessions	Availability for Disconnection	Timeout Value
USERID	192.168.5.11	Request to connect	1 hour

   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.

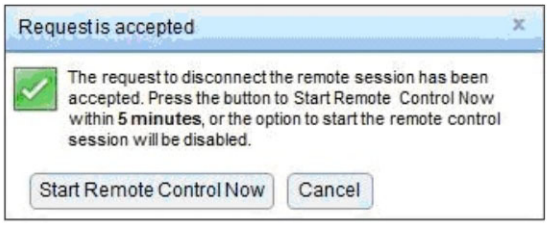
   The following illustration shows the window that is displayed when the request is successfully sent.



Your request has been sent successfully.
Please wait for the response from the remote user.

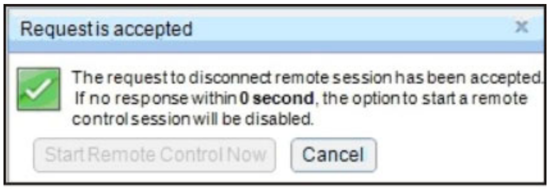
If the remote control user accepts the disconnect request, the web user must start the remote control session within five minutes. If the web user does not start the session within five minutes, the session will not be reserved.

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



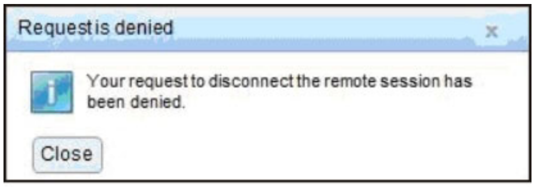
The request to disconnect the remote session has been accepted. Press the button to Start Remote Control Now within **5 minutes**, or the option to start the remote control session will be disabled.

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



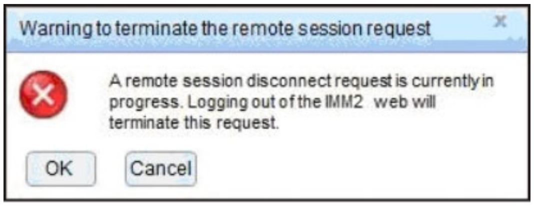
The request to disconnect remote session has been accepted. If no response within **0 second**, the option to start a remote control session will be disabled.

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).



Your request to disconnect the remote session has been denied.

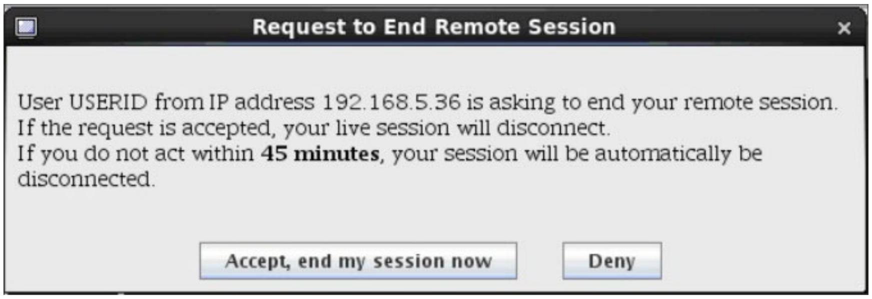
If the web user attempts to log out of the IMM2 before receiving a message about their request, the web user will receive a message (as shown in the following illustration).



A remote session disconnect request is currently in progress. Logging out of the IMM2 web will terminate this request.

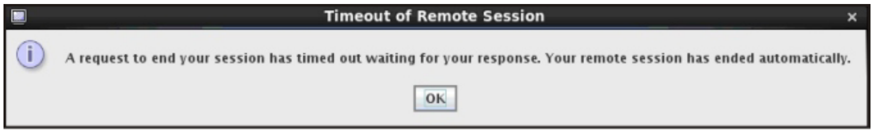
After the remote control user receives the request, the user must determine whether to release the remote session in the interval time selected before starting the remote control session. A Request to End Remote Session window is displayed to remind the remote control user of any time remaining.

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



User USERID from IP address 192.168.5.36 is asking to end your remote session.
If the request is accepted, your live session will disconnect.
If you do not act within **45 minutes**, your session will be automatically be disconnected.

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.



A request to end your session has timed out waiting for your response. Your remote session has ended automatically.

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 1.7 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

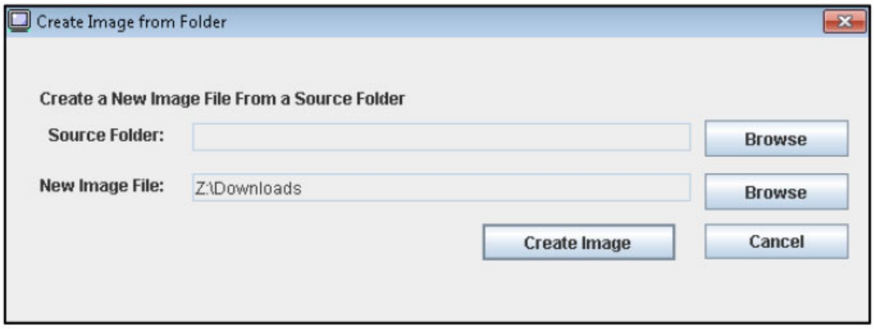
To begin a remote control session and access the remote disk, complete the following steps:

1. From the Video Viewer window click the **Virtual Media** tab.
2. Click **Activate**.
3. Click **Select Devices to Mount**.

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 AES encryption.

Creating an image file: To create a new image file from a specified source folder, complete the following steps:
1. Click the **Create Image** option under the **Virtual Media** tab in the Video Viewer window. The Create Image from Folder window is displayed.
2. Click the **Browse** button associated with the **Source Folder** field to select the specific source folder.
3. Click the **Browse** button associated with the **New Image File** field to select the image file to use.
4. Click the **Create Image** button.

The Create Image from Folder window is shown in the following illustration.



Create Image from Folder

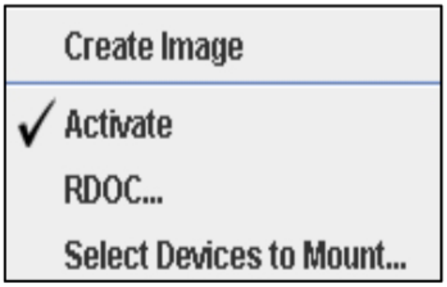
Create a New Image File From a Source Folder

Source Folder:

New Image File: Z:\Downloads

The new image file is ready for mounting to the host operating system.

The Virtual Media session must be activated for you to mount a drive or image file to the host operating system, (as shown in the following illustration).



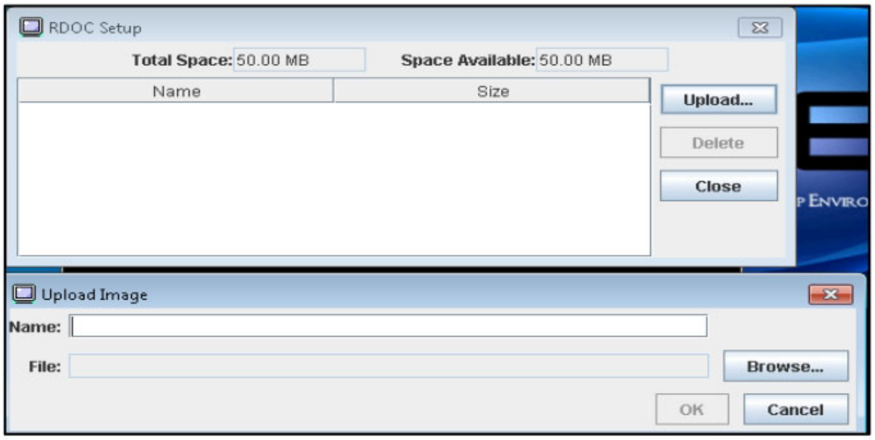
Uploading an image file: To upload an image file to the host operating system, complete the following steps:
1. Click the **RDOC** option under the **Virtual Media** tab in the Video Viewer window. The RDOC Setup window is displayed.
2. Click the **Upload** button in the RDOC Setup window.
3. Click the **Browse** button to locate the image file that you want to use.

4. Enter a name for the image file in the **Name** field in the Upload Image window.
5. Click **OK** to save your selection.

Notes:

- The image file will remain on the server after a reboot of the host operating system.
- The maximum size of the image file cannot exceed 50 MB.
- To remove (unload) the image file from memory, click the **Delete** button.

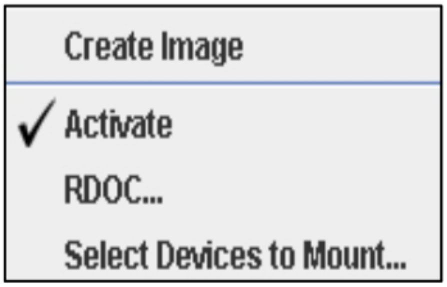
The RDOC Setup and Upload Image windows are shown in the following illustration.



Total Space: 50.00 MB

Space Available: 50.00 MB

Selecting devices to mount: The Virtual Media session must be activated for you to mount a drive or image file to the host operating system, (as shown in the following illustration).



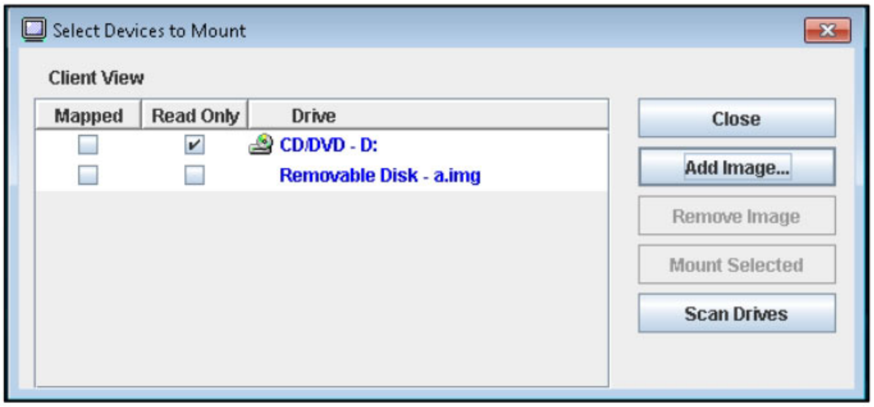
To select the devices to mount, complete the following steps:

1. Click the **Select Devices to Mount** option under the **Virtual Media** tab in the Video Viewer window. The Select Devices to Mount window is displayed, (as shown in the following illustration).
2. Click the check box of the device or devices that you want to mount or map.
3. Click the **Mount Selected** button.

The Select Devices to Mount window contains a list of the current local devices that are available for mounting. This window contains the following fields and buttons:

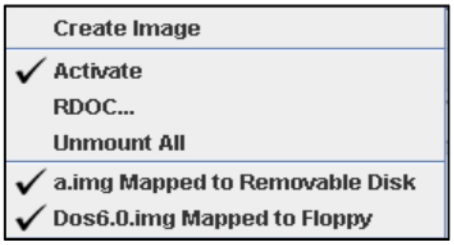
- The **Mapped** field contains the check box that allows you to select the devices to mount or map.

- The **Read Only** field contains the check box that allows you to select the mapped or mounted devices that will be *read-only* on the host server.
- The **Drive** field contains the device path on the local machine.
- Click the **Close** button to close the Select Devices to Mount window and return to the Video Viewer page.
- Click the **Add Image** button to browse for the diskette image and ISO image file in your local file system that you want to add to the list of devices.
- Click the **Remove Image** button to remove an image that has been added to the list of devices.
- Click the **Mount Selected** button to mount or map all devices that are checked for mounting or mapping in the **Mapped** field.
- Click the **Scan Drives** button to refresh the list of local devices.



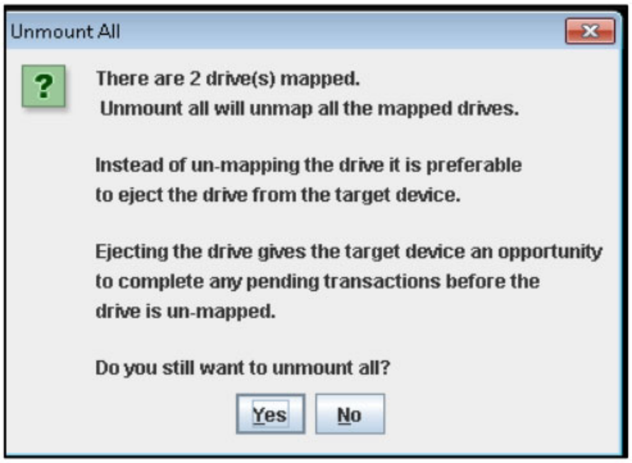
Mapped	Read Only	Drive
□	☑	CD/DVD - D:
□	□	Removable Disk - a.img

Selecting devices to unmount: After the devices are mounted the **Select Devices to Mount** option in the Virtual Media tab, is changed to **Unmount All**, (as shown in the following illustration).


Create Image
✓ Activate
RDOC...
Unmount All
✓ a.img Mapped to Removable Disk
✓ Dos6.0.img Mapped to Floppy

Click the **Unmount All** option to unmount the host server devices. After selecting the **Unmount All** option you are presented with an Unmount All confirmation window, (as shown in the following illustration). If you accept, *all* host server devices on the server are unmounted.

Note: You cannot unmount drives individually.



There are 2 drive(s) mapped.
Unmount all will unmap all the mapped drives.

Instead of un-mapping the drive it is preferable to eject the drive from the target device.

Ejecting the drive gives the target device an opportunity to complete any pending transactions before the drive is un-mapped.

Do you still want to unmount all?

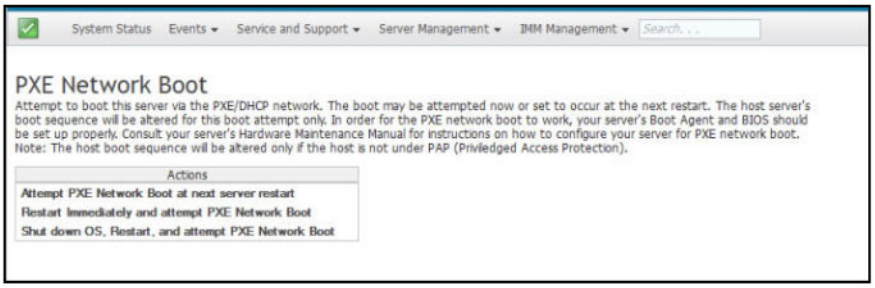
Exiting Remote Control:
To exit your remote control session close the Video Viewer and the Virtual Media Session windows.

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**.

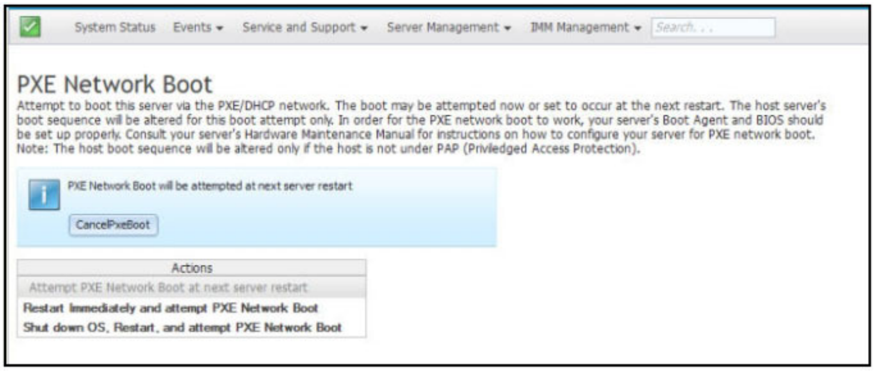
   The following window opens.


System Status
Events ▾
Service and Support ▾
Server Management ▾
IMM Management ▾
Search. . .
Actions
Attempt PXE Network Boot at next server restart
Restart Immediately and attempt PXE Network Boot
Shut down OS, Restart, and attempt PXE Network Boot

PXE Network Boot

Attempt to boot this server via the PXE/DHCP network. The boot may be attempted now or set to occur at the next restart. The host server's boot sequence will be altered for this boot attempt only. In order for the PXE network boot to work, your server's Boot Agent and BIOS should be set up properly. Consult your server's Hardware Maintenance Manual for instructions on how to configure your server for PXE network boot. Note: The host boot sequence will be altered only if the host is not under PAP (Priviedged Access Protection).

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

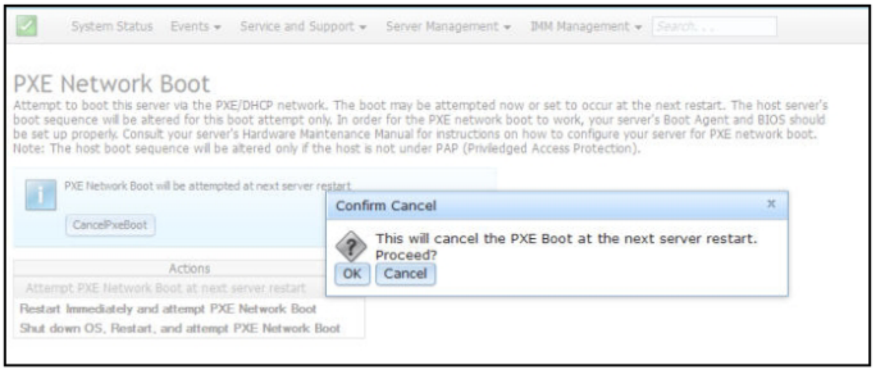

System Status
Events ▾
Service and Support ▾
Server Management ▾
IMM Management ▾
Search. . .
CancelPxeBoot
Actions
Attempt PXE Network Boot at next server restart
Restart Immediately and attempt PXE Network Boot
Shut down OS, Restart, and attempt PXE Network Boot

PXE Network Boot

Attempt to boot this server via the PXE/DHCP network. The boot may be attempted now or set to occur at the next restart. The host server's boot sequence will be altered for this boot attempt only. In order for the PXE network boot to work, your server's Boot Agent and BIOS should be set up properly. Consult your server's Hardware Maintenance Manual for instructions on how to configure your server for PXE network boot. Note: The host boot sequence will be altered only if the host is not under PAP (Priviedged Access Protection).

PXE Network Boot will be attempted at next server restart

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



PXE Network Boot

Attempt to boot this server via the PXE/DHCP network. The boot may be attempted now or set to occur at the next restart. The host server's boot sequence will be altered for this boot attempt only. In order for the PXE network boot to work, your server's Boot Agent and BIOS should be set up properly. Consult your server's Hardware Maintenance Manual for instructions on how to configure your server for PXE network boot. Note: The host boot sequence will be altered only if the host is not under PAP (Priviledged Access Protection).

PXE Network Boot will be attempted at next server restart.

Confirm Cancel

This will cancel the PXE Boot at the next server restart. Proceed?

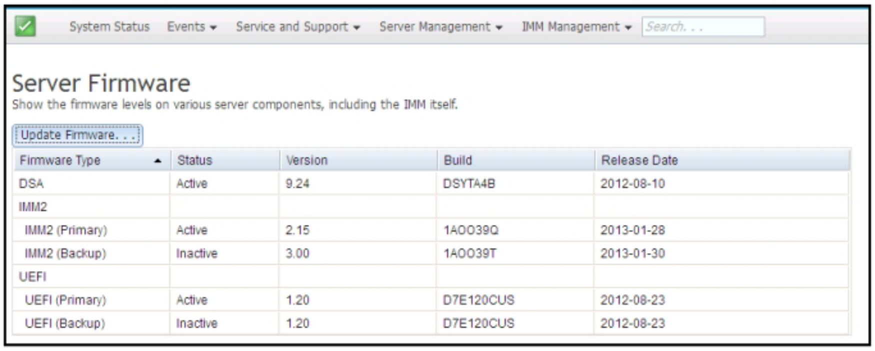
Actions

Attempt PXE Network Boot at next server restart
Restart Immediately and attempt PXE Network Boot
Shut down OS, Restart, and attempt PXE Network Boot

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.



Server Firmware

Show the firmware levels on various server components, including the IMM itself.

Firmware Type	Status	Version	Build	Release Date
DSA	Active	9.24	DSYTA4B	2012-08-10
IMM2				
IMM2 (Primary)	Active	2.15	1AOO39Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	1AOO39T	2013-01-30
UEFI				
UEFI (Primary)	Active	1.20	D7E120CUS	2012-08-23
UEFI (Backup)	Inactive	1.20	D7E120CUS	2012-08-23

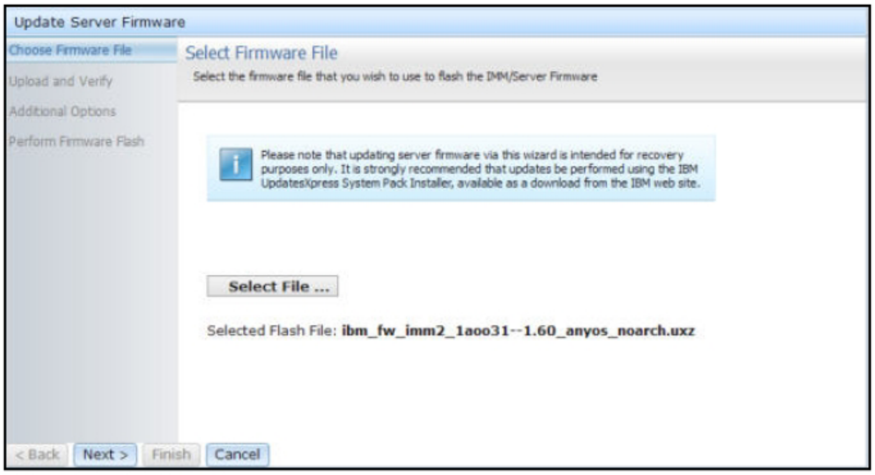
The current status and versions of firmware for the IMM2, UEFI, and DSA are displayed, including the primary and backup versions. There are three categories for the firmware status:

- **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).



Select the firmware file that you wish to use to flash the IMM/Server Firmware

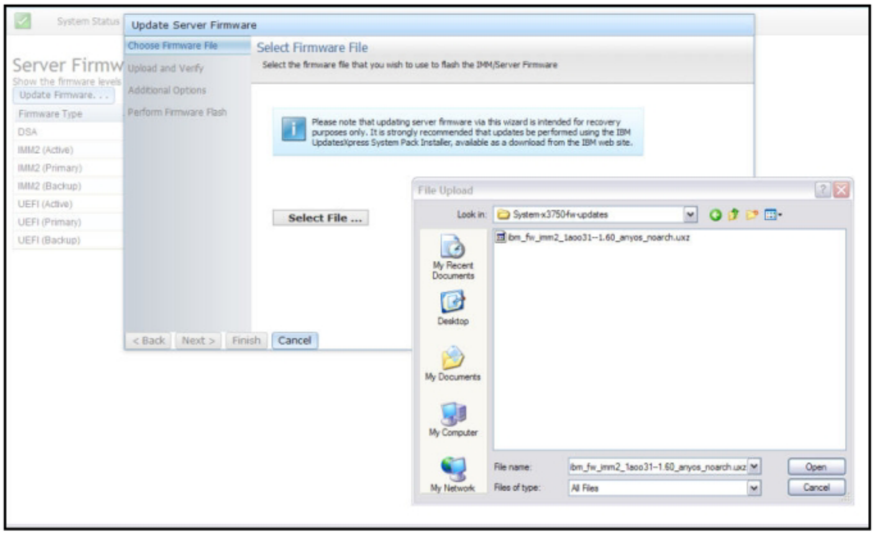
Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM UpdatesXpress System Pack Installer, available as a download from the IBM web site.

Selected Flash File: **ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz**

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.



Select the firmware file that you wish to use to flash the IMM/Server Firmware

Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM UpdatesXpress System Pack Installer, available as a download from the IBM web site.

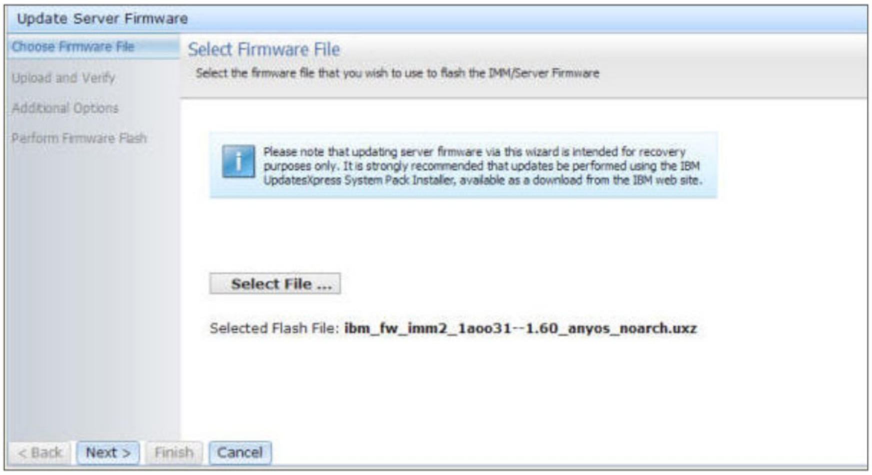
Look in: System-x3750fw-updates

ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz

File name: ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz

Files of type: All Files

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).



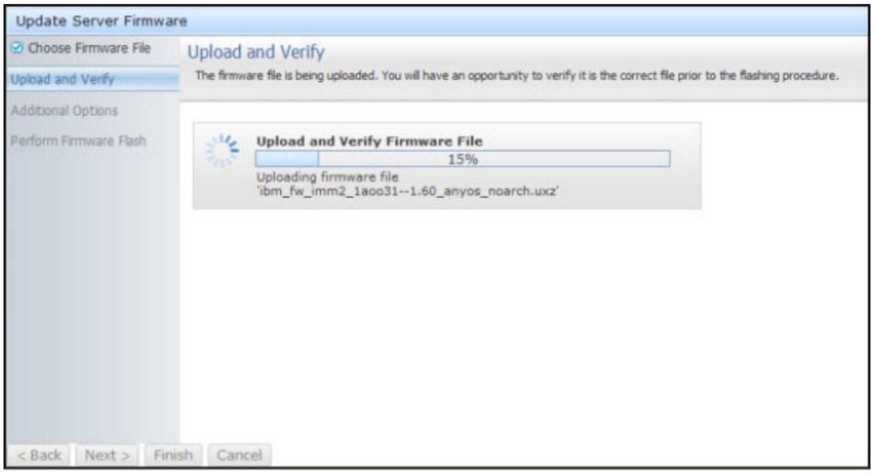
Select Firmware File

Select the firmware file that you wish to use to flash the IMM/Server Firmware

Please note that updating server firmware via this wizard is intended for recovery purposes only. It is strongly recommended that updates be performed using the IBM UpdatesXpress System Pack Installer, available as a download from the IBM web site.

Selected Flash File: **ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz**

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).



Upload and Verify

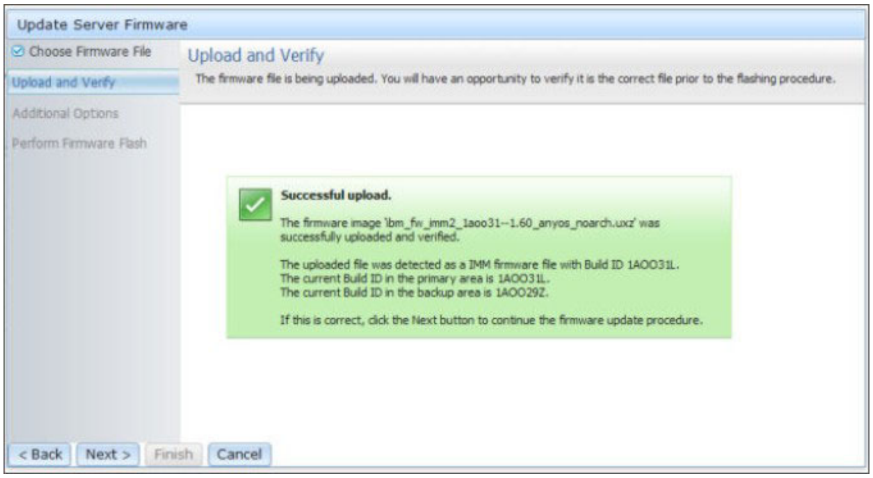
The firmware file is being uploaded. You will have an opportunity to verify it is the correct file prior to the flashing procedure.

Upload and Verify Firmware File

Uploading firmware file 'ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz'

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).



Upload and Verify

The firmware file is being uploaded. You will have an opportunity to verify it is the correct file prior to the flashing procedure.

Successful upload.

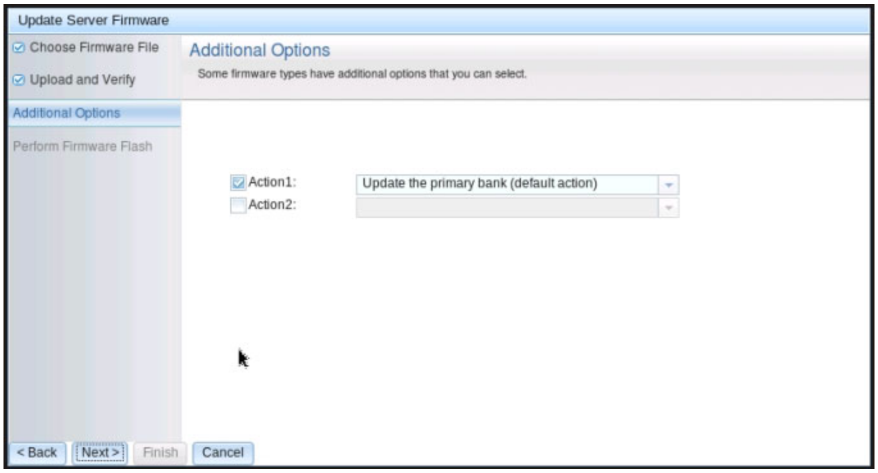
The firmware image 'ibm_fw_imm2_1aoo31--1.60_anyos_noarch.uxz' was successfully uploaded and verified.

The uploaded file was detected as a IMM firmware file with Build ID 1AOO31L.
The current Build ID in the primary area is 1AOO31L.
The current Build ID in the backup area is 1AOO29Z.

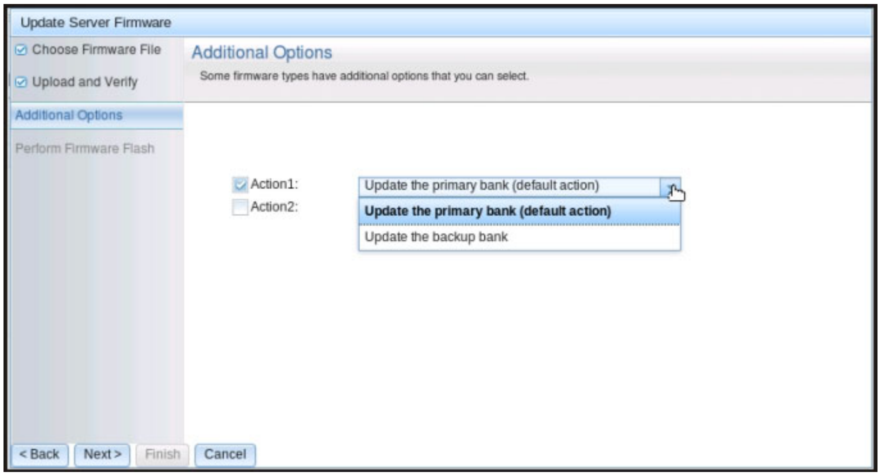
If this is correct, click the Next button to continue the firmware update procedure.

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).

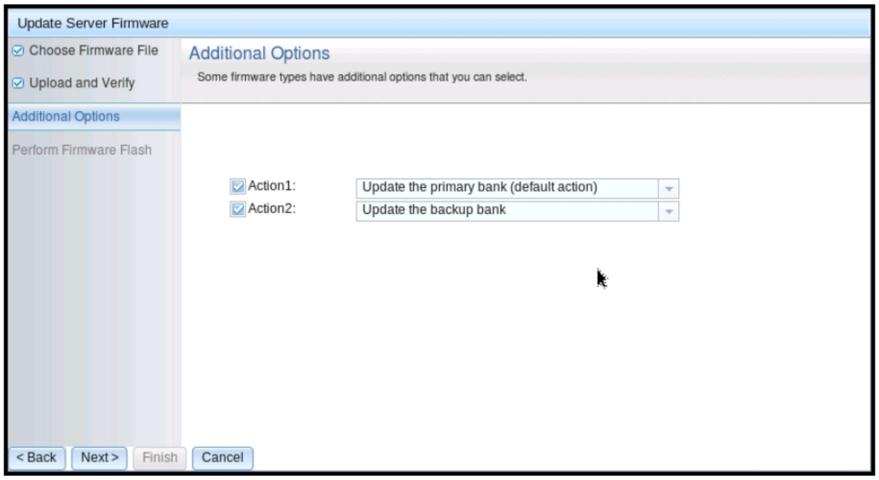
8. The drop-down menu beside the **Action 1** field gives you the choice to **Update the primary bank (default action)** or **Update the backup bank** (as shown in the following illustration).

   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.



Additional Options

Some firmware types have additional options that you can select.

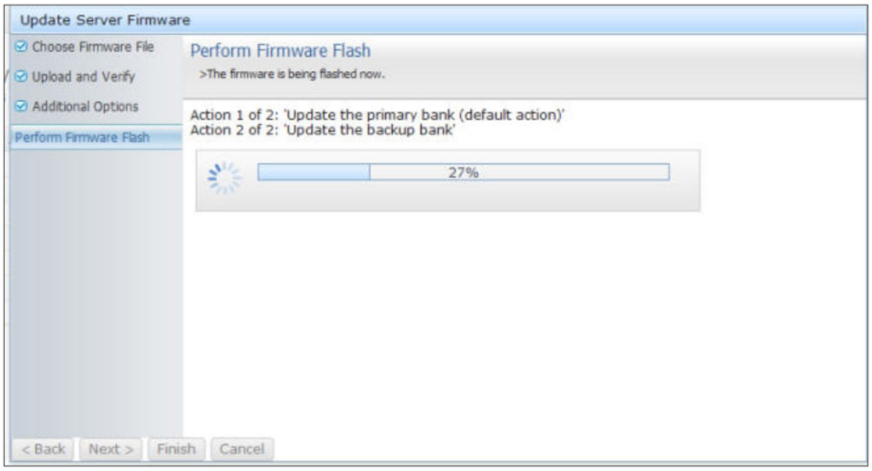
☑ Action1: Update the primary bank (default action)

☑ Action2: Update the backup bank

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).

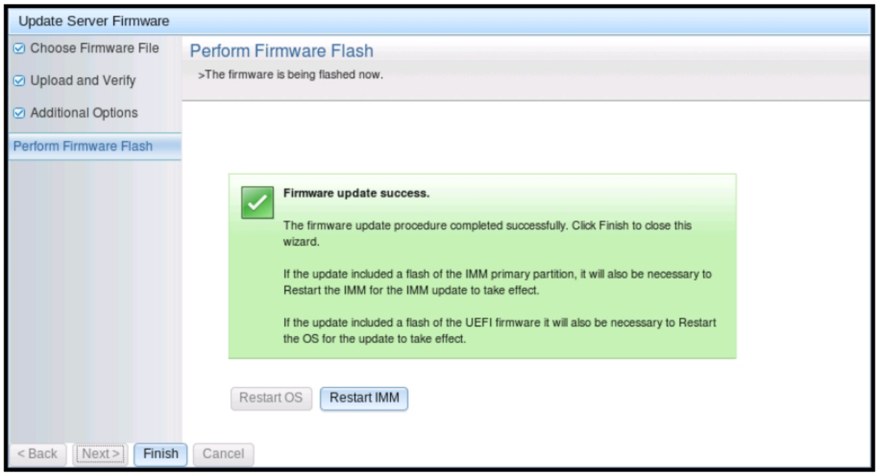


Perform Firmware Flash

>The firmware is being flashed now.

Action 1 of 2: 'Update the primary bank (default action)'
Action 2 of 2: 'Update the backup bank'

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.



Perform Firmware Flash

>The firmware is being flashed now.

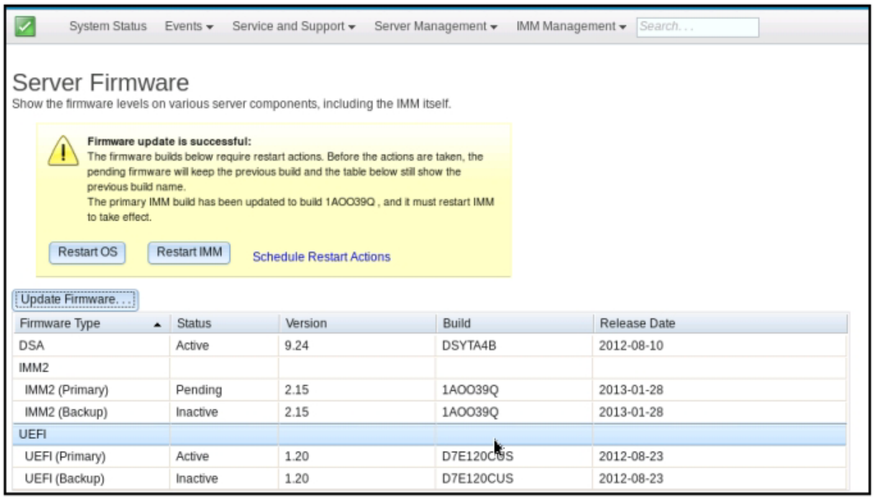
Firmware update success.

The firmware update procedure completed successfully. Click Finish to close this wizard.

If the update included a flash of the IMM primary partition, it will also be necessary to Restart the IMM for the IMM update to take effect.

If the update included a flash of the UEFI firmware it will also be necessary to Restart the OS for the update to take effect.

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



Server Firmware

Show the firmware levels on various server components, including the IMM itself.

Firmware update is successful:
The firmware builds below require restart actions. Before the actions are taken, the pending firmware will keep the previous build and the table below still show the previous build name.
The primary IMM build has been updated to build 1AOO39Q , and it must restart IMM to take effect.

Firmware Type ▲	Status	Version	Build	Release Date
DSA	Active	9.24	DSYTA4B	2012-08-10
IMM2				
IMM2 (Primary)	Pending	2.15	1AOO39Q	2013-01-28
IMM2 (Backup)	Inactive	2.15	1AOO39Q	2013-01-28
UEFI				
UEFI (Primary)	Active	1.20	D7E120CUS	2012-08-23
UEFI (Backup)	Inactive	1.20	D7E120CUS	2012-08-23

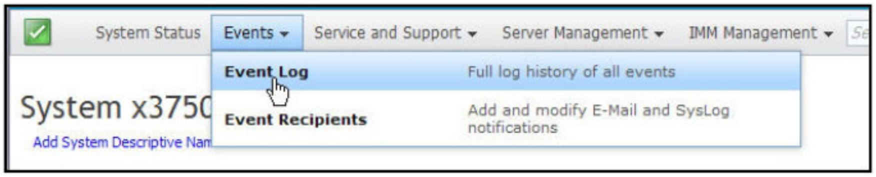
Managing system events

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

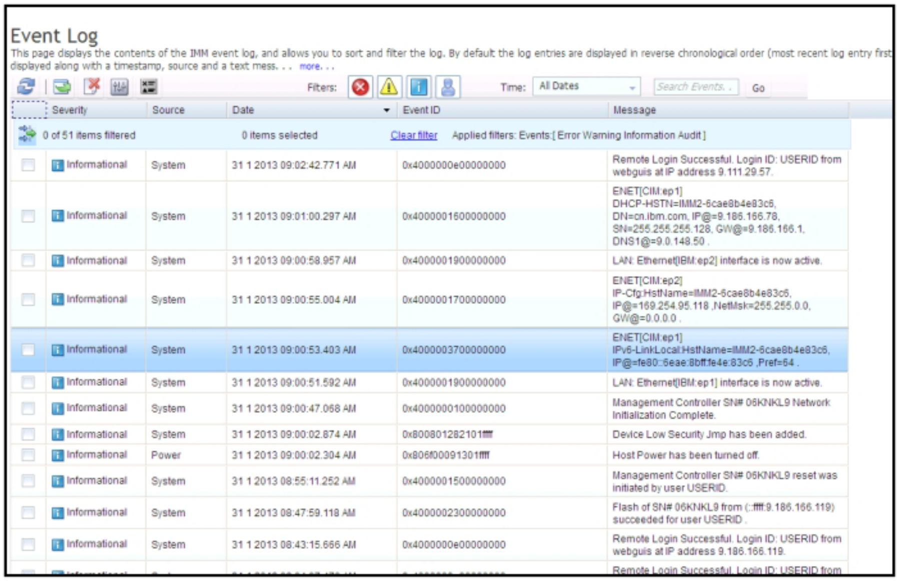
Managing the event log

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 Event Log window opens.

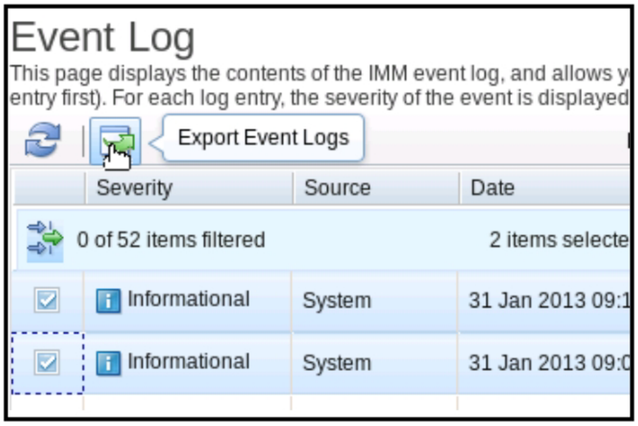

Event Log

This page displays the contents of the IMM event log, and allows you to sort and filter the log. By default the log entries are displayed in reverse chronological order (most recent log entry first displayed along with a timestamp, source and a text mess. . . more. . .

0 of 51 items filtered 0 items selected Clear filter Applied filters: Events:[Error Warning Information Audit]

	Severity	Source	Date	Event ID	Message
□	Informational	System	31 1 2013 09:02:42.771 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.111.29.57.
□	Informational	System	31 1 2013 09:01:00.297 AM	0x4000001600000000	ENET[CIM:ep1] DHCP-HSTN=IMM2-6cae8b4e83c6, DN=cn.ibm.com, IP@=9.186.166.78, SN=255.255.255.128, GW@=9.186.166.1, DNS1@=9.0.148.50 .
□	Informational	System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet[IBM:ep2] interface is now active.
□	Informational	System	31 1 2013 09:00:55.004 AM	0x4000001700000000	ENET[CIM:ep2] IP-Cfg:HstName=IMM2-6cae8b4e83c6, IP@=169.254.95.118 ,NetMsk=255.255.0.0, GW@=0.0.0.0 .
□	Informational	System	31 1 2013 09:00:53.403 AM	0x4000003700000000	ENET[CIM:ep1] IPv6-LinkLocal:HstName=IMM2-6cae8b4e83c6, IP@=fe80::6eae:8bff:fe4e:83c6 ,Pref=64 .
□	Informational	System	31 1 2013 09:00:51.592 AM	0x4000001900000000	LAN: Ethernet[IBM:ep1] interface is now active.
□	Informational	System	31 1 2013 09:00:47.068 AM	0x4000000100000000	Management Controller SN# 06KNKL9 Network Initialization Complete.
□	Informational	System	31 1 2013 09:00:02.874 AM	0x800801282101ffff	Device Low Security Jmp has been added.
□	Informational	Power	31 1 2013 09:00:02.304 AM	0x806f00091301ffff	Host Power has been turned off.
□	Informational	System	31 1 2013 08:55:11.252 AM	0x4000001500000000	Management Controller SN# 06KNKL9 reset was initiated by user USERID.
□	Informational	System	31 1 2013 08:47:59.118 AM	0x4000002300000000	Flash of SN# 06KNKL9 from (::ffff:9.186.166.119) succeeded for user USERID .
□	Informational	System	31 1 2013 08:43:15.666 AM	0x4000000e00000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.186.166.119.
					Remote Login Successful. Login ID: USERID from

To sort and filter events in the event log, select the column heading. 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).


Event Log

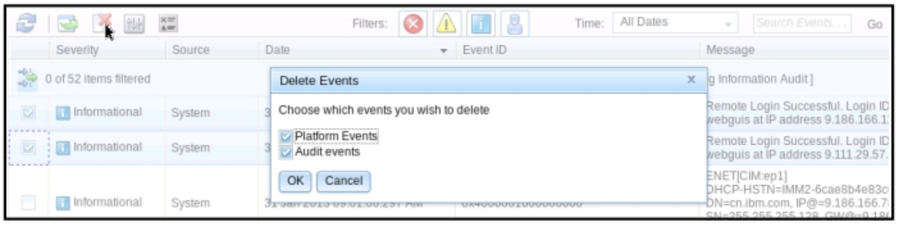
This page displays the contents of the IMM event log, and allows y entry first). For each log entry, the severity of the event is displayed

0 of 52 items filtered 2 items selecte

	Severity	Source	Date
☑	Informational	System	31 Jan 2013 09:1
☑	Informational	System	31 Jan 2013 09:0

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.



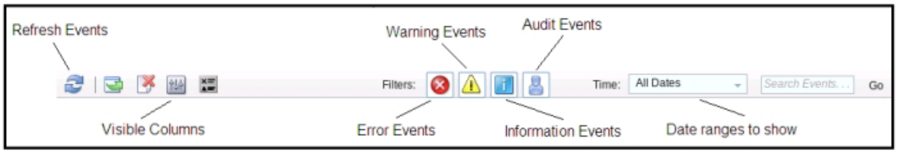
Delete Events

Choose which events you wish to delete

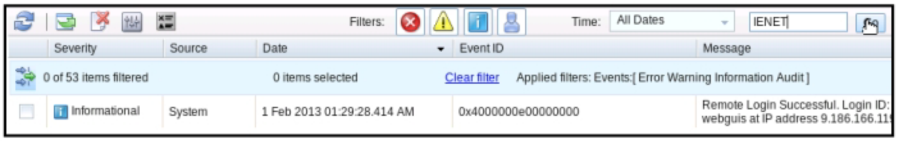
☑ Platform Events
☑ Audit events

OK Cancel

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).

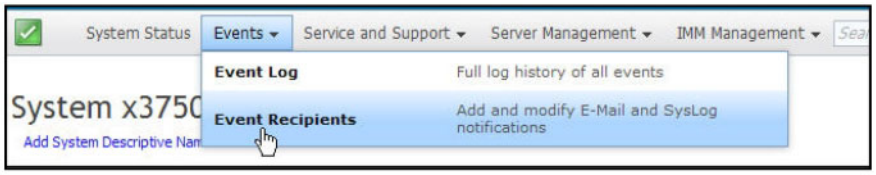


	Severity	Source	Date	Event ID	Message
	0 of 53 items filtered		0 items selected	Clear filter	Applied filters: Events:[Error Warning Information Audit]
□	Informational	System	1 Feb 2013 01:29:28.414 AM	0x4000000e00000000	Remote Login Successful. Login ID: webguis at IP address 9.186.166.11

Notification of system events

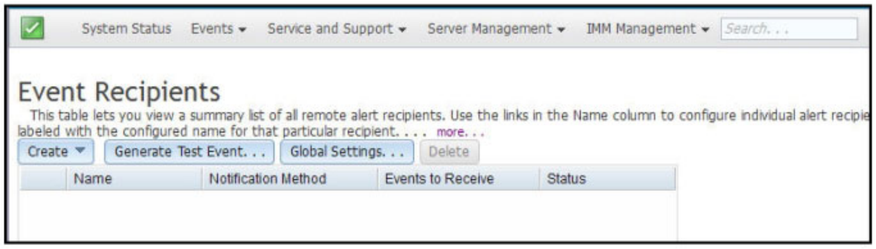
Select the **Event Recipients** option to add and modify email and syslog notifications.

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.

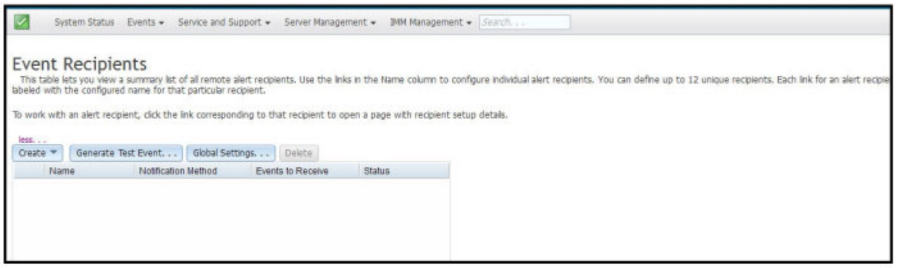


Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure individual alert recipie labeled with the configured name for that particular recipient. . . . more. . .

Name	Notification Method	Events to Receive	Status

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



Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure individual alert recipients. You can define up to 12 unique recipients. Each link for an alert recipie labeled with the configured name for that particular recipient.

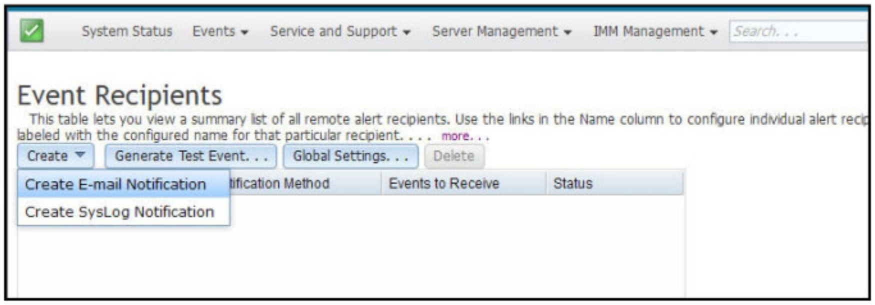
To work with an alert recipient, click the link corresponding to that recipient to open a page with recipient setup details.

Name	Notification Method	Events to Receive	Status

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.

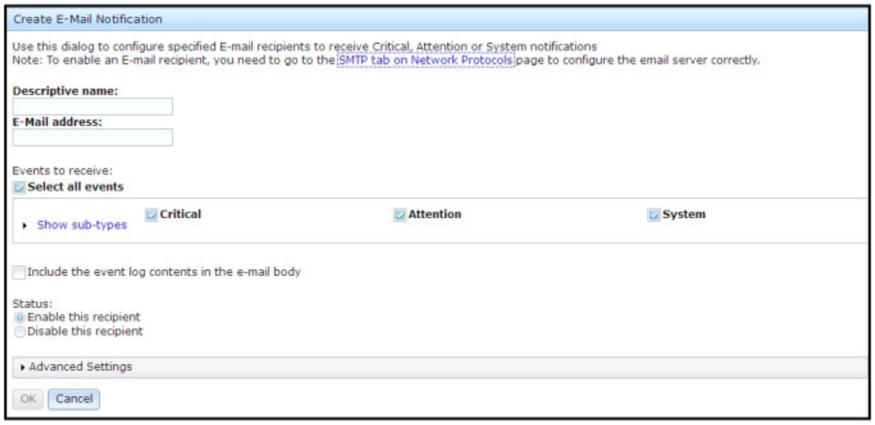


Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure individual alert recip labeled with the configured name for that particular recipient. . . . more. . .

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.


Create E-Mail Notification

Use this dialog to configure specified E-mail recipients to receive Critical, Attention or System notifications
Note: To enable an E-mail recipient, you need to go to the SMTP tab on Network Protocols page to configure the email server correctly.

Descriptive name:

E-Mail address:

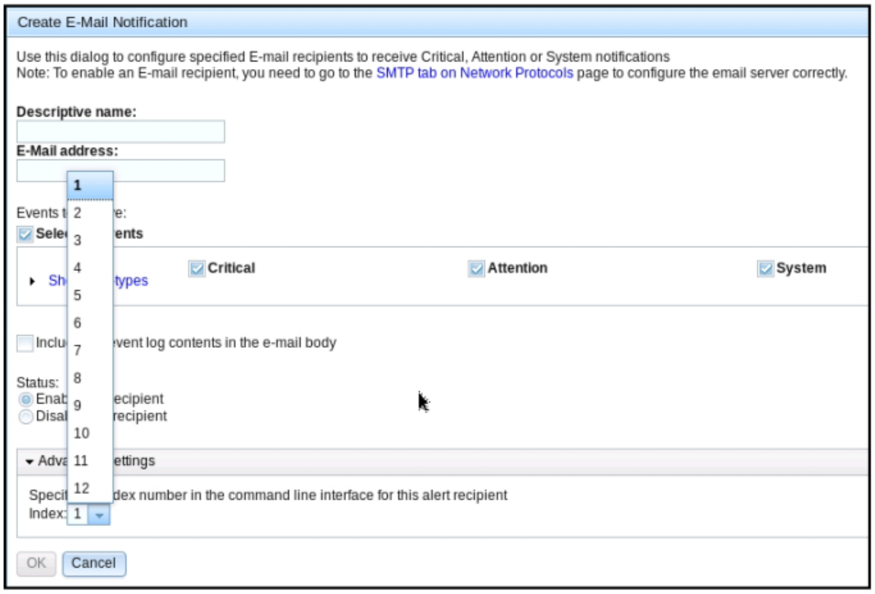
Events to receive:
☑ **Select all events**

☑ **Critical** ☑ **Attention** ☑ **System**

□ Include the event log contents in the e-mail body

Status:
● Enable this recipient
○ Disable this recipient

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



Create E-Mail Notification

Use this dialog to configure specified E-mail recipients to receive Critical, Attention or System notifications
Note: To enable an E-mail recipient, you need to go to the SMTP tab on Network Protocols page to configure the email server correctly.

Descriptive name:

E-Mail address:

Events t e:
☑ Sele ents

▸ Sh types ☑ Critical ☑ Attention ☑ System

□ Inclu vent log contents in the e-mail body

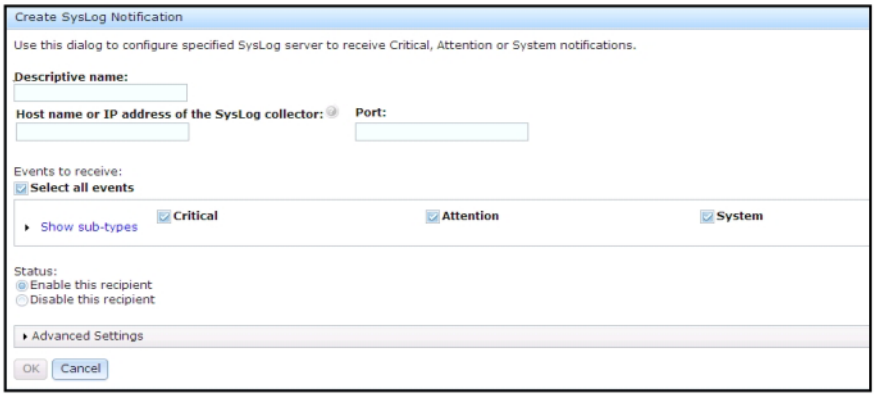
Status:
● Enab ecipient
○ Disal recipient

▾ Adva ettings

Speci dex number in the command line interface for this alert recipient
Index: 1

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.



Create SysLog Notification

Use this dialog to configure specified SysLog server to receive Critical, Attention or System notifications.

Descriptive name:

Host name or IP address of the SysLog collector: Port:

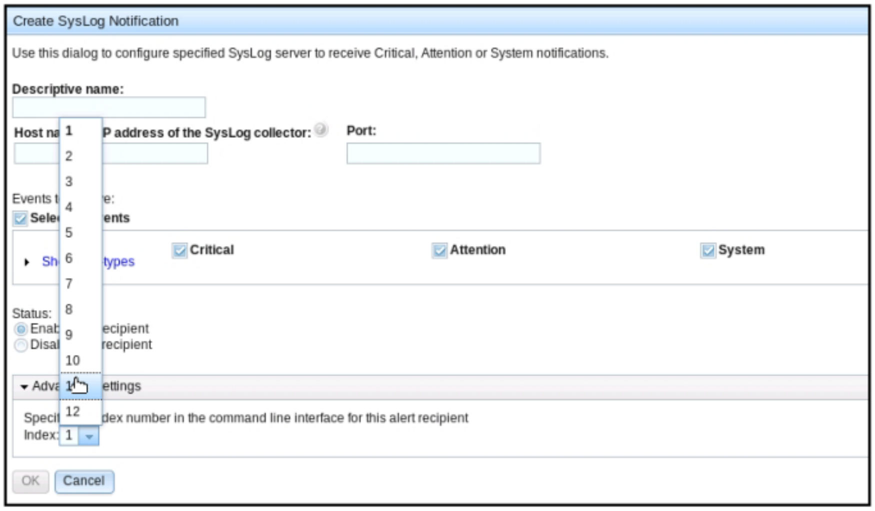
Events to receive:
☑ Select all events

▸ Show sub-types ☑ Critical ☑ Attention ☑ System

Status:
● Enable this recipient
○ Disable this recipient

▸ Advanced Settings

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



Create SysLog Notification

Use this dialog to configure specified SysLog server to receive Critical, Attention or System notifications.

Descriptive name:

Host na P address of the SysLog collector: Port:

Events t e:

☑ Sele ents

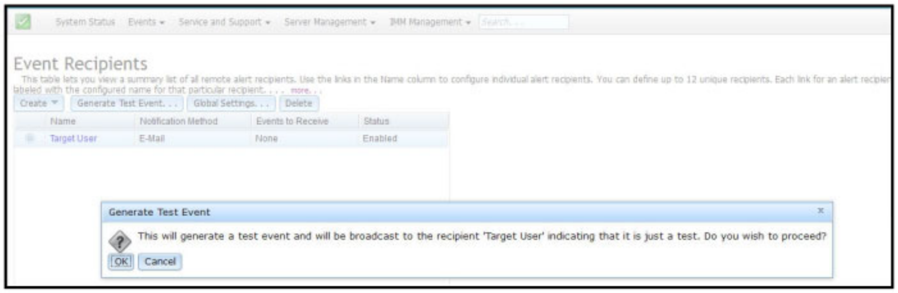
Status:
● Enab ecipient
○ Disal recipient

Speci dex number in the command line interface for this alert recipient
Index: 1

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.



Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure individual alert recipients. You can define up to 12 unique recipients. Each link for an alert recipie labeled with the configured name for that particular recipient. . . . more. . .

	Name	Notification Method	Events to Receive	Status
○	Target User	E-Mail	None	Enabled

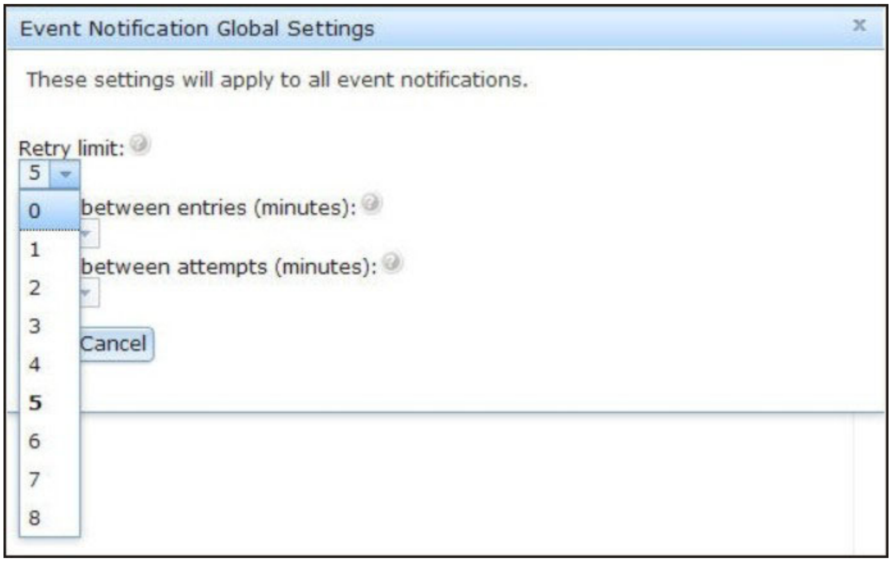
Generate Test Event

This will generate a test event and will be broadcast to the recipient 'Target User' indicating that it is just a test. Do you wish to proceed?

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.

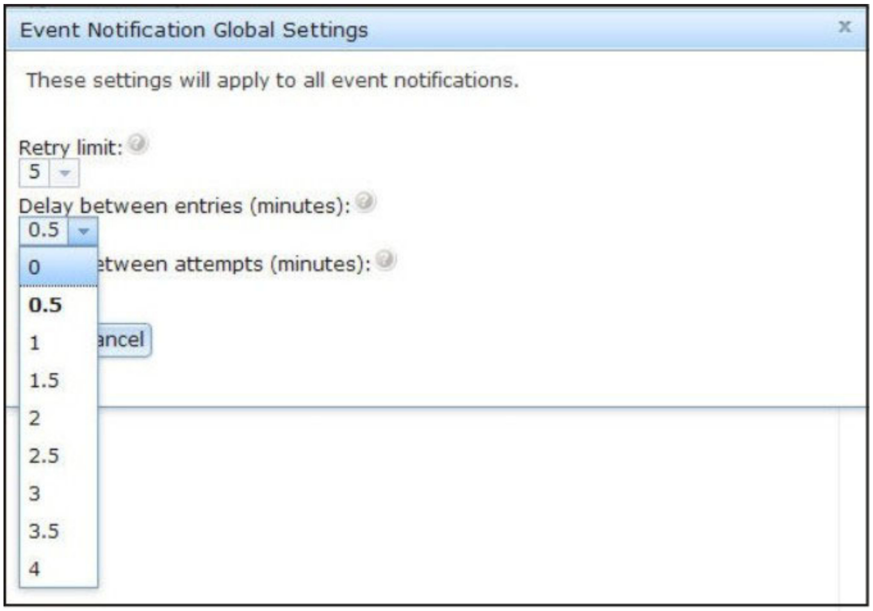


Event Notification Global Settings

These settings will apply to all event notifications.

Retry limit: 5

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



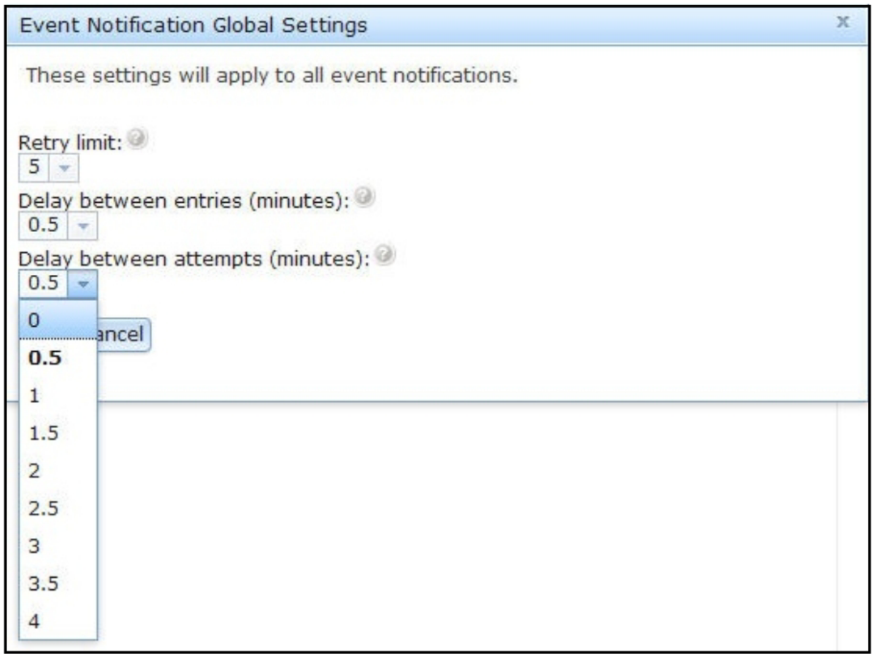
Event Notification Global Settings

These settings will apply to all event notifications.

Retry limit: 5

Delay between entries (minutes): 0.5

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


Event Notification Global Settings

These settings will apply to all event notifications.

Retry limit: 5

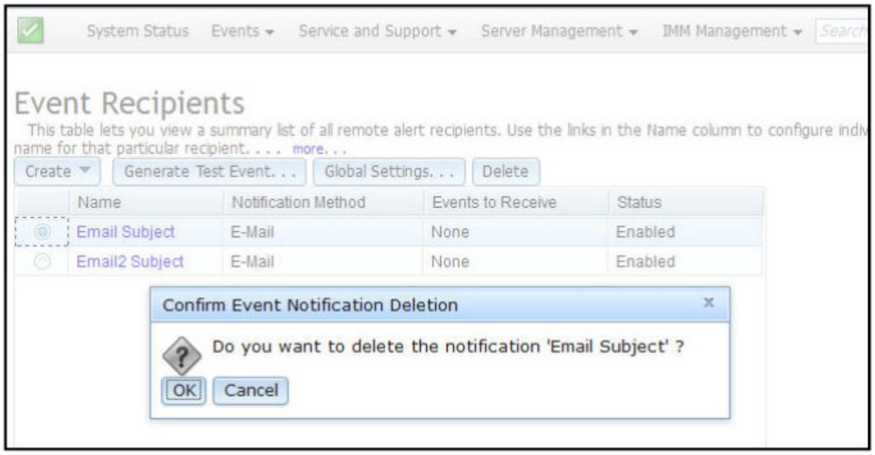
Delay between entries (minutes): 0.5

Delay between attempts (minutes): 0.5

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.



Event Recipients

This table lets you view a summary list of all remote alert recipients. Use the links in the Name column to configure indiv name for that particular recipient. . . . more. . .

	Name	Notification Method	Events to Receive	Status
◉	Email Subject	E-Mail	None	Enabled
○	Email2 Subject	E-Mail	None	Enabled

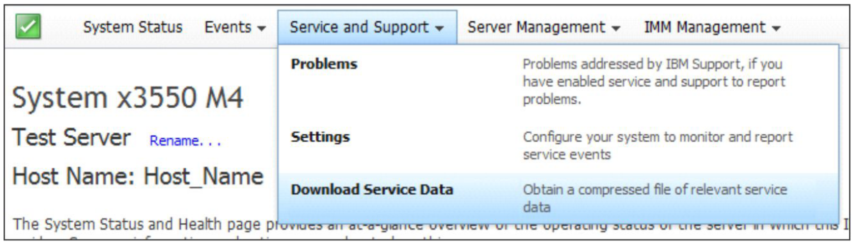
Confirm Event Notification Deletion

Do you want to delete the notification 'Email Subject' ?

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 Support to assist you with your problem.

The following illustration shows the Service and Support menu.



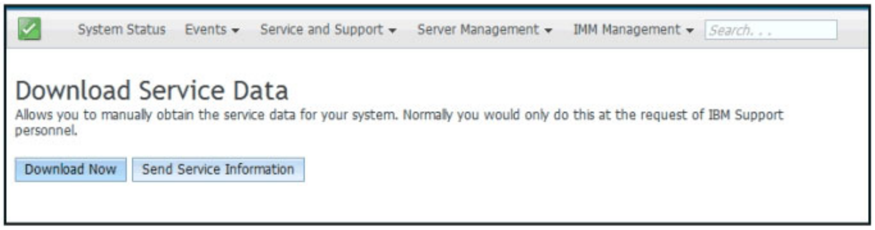
Problems Problems addressed by IBM Support, if you have enabled service and support to report problems.

Settings Configure your system to monitor and report service events

Download Service Data Obtain a compressed file of relevant service data

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

The following illustration shows the Download Service Data window.

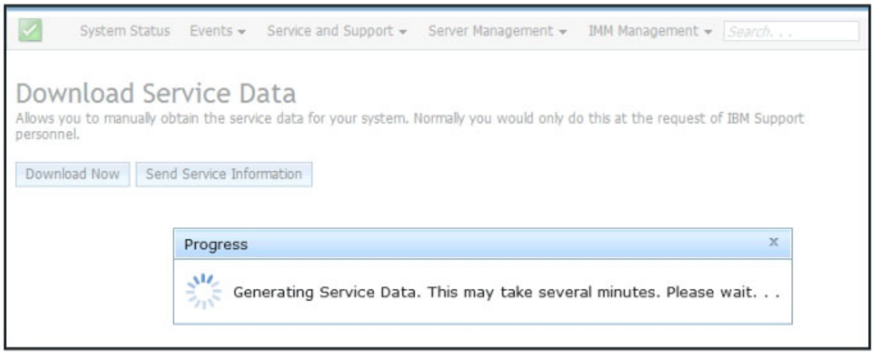


Download Service Data

Allows you to manually obtain the service data for your system. Normally you would only do this at the request of IBM Support personnel.

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.

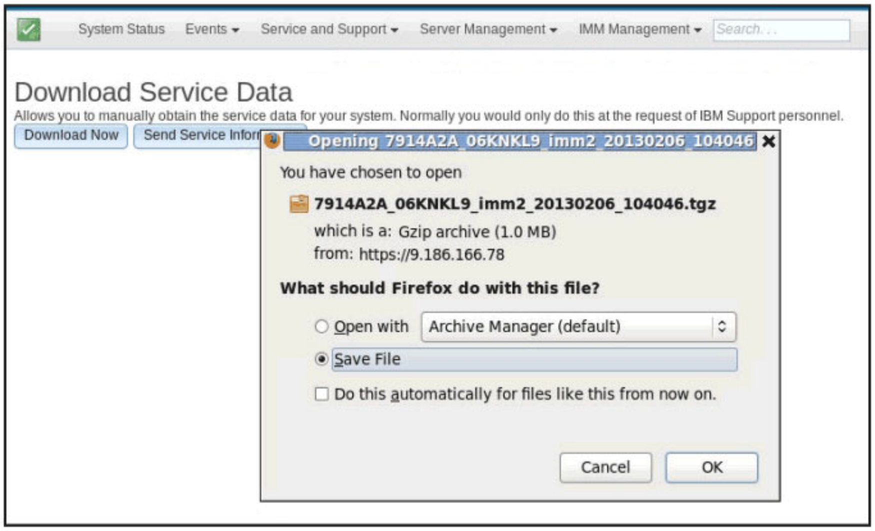


Download Service Data

Allows you to manually obtain the service data for your system. Normally you would only do this at the request of IBM Support personnel.

Generating Service Data. This may take several minutes. Please wait. . .

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.



Download Service Data

Allows you to manually obtain the service data for your system. Normally you would only do this at the request of IBM Support personnel.

Opening 7914A2A_06KNKL9_imm2_20130206_104046

You have chosen to open

7914A2A_06KNKL9_imm2_20130206_104046.tgz

which is a: Gzip archive (1.0 MB)

from: https://9.186.166.78

What should Firefox do with this file?

○ Open with Archive Manager (default)

● Save File

☐ Do this automatically for files like this from now on.

Capturing the latest OS failure screen data

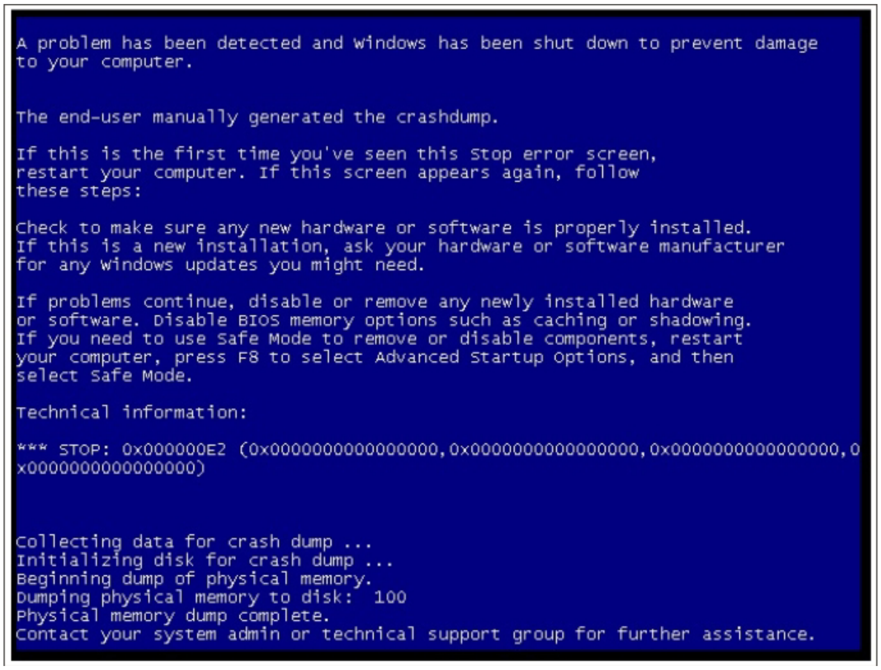
Use the **Latest OS Failure Screen** option to capture the operating system failure screen data and store the data. The IMM2 stores only the most recent error event information, overwriting earlier OS failure screen data when a new error event occurs. The OS Watchdog feature must be enabled to capture 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.



```
A problem has been detected and Windows has been shut down to prevent damage
to your computer.


The end-user manually generated the crashdump.

If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any Windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)



Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk:  100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

Managing the server power

Select the **Power Management** option under the **Server Management** tab to view power management information and perform power management functions.

Note: In a Flex System, the CMM controls chassis cooling and power; therefore, the Cooling Devices and Power Modules options do not appear in the **Server Management** tab.

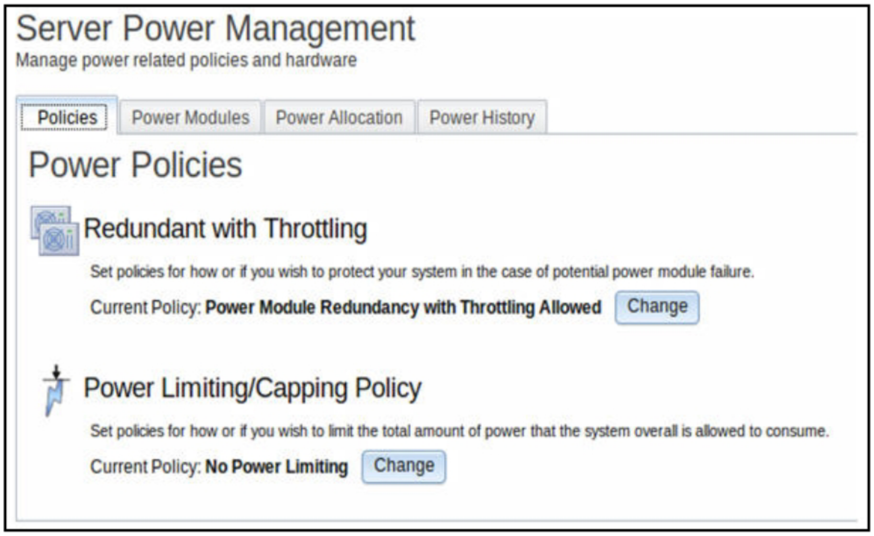
Controlling the power supply and total system power

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.

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

Configuring up to two power supplies

The following illustration shows the **Policies** tab for servers that support up to two power supplies.



Server Power Management

Manage power related policies and hardware

Power Policies

Redundant with Throttling

Set policies for how or if you wish to protect your system in the case of potential power module failure.

Current Policy: **Power Module Redundancy with Throttling Allowed**

Power Limiting/Capping Policy

Set policies for how or if you wish to limit the total amount of power that the system overall is allowed to consume.

Current Policy: **No Power Limiting**

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.

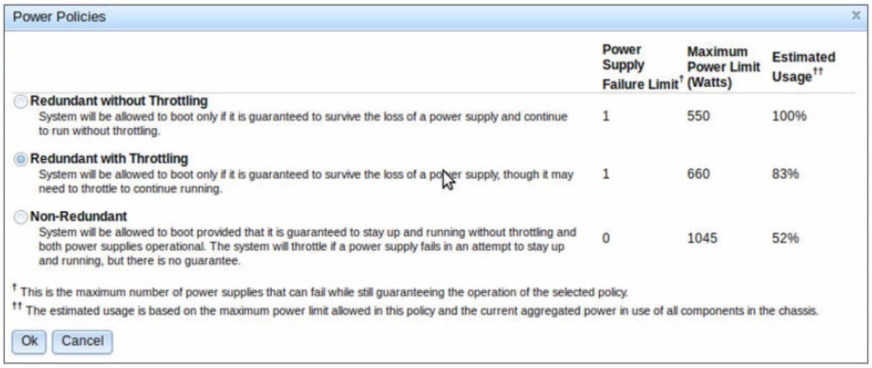
Available fields on the Power Polices page are as follows:

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.



Power Policies

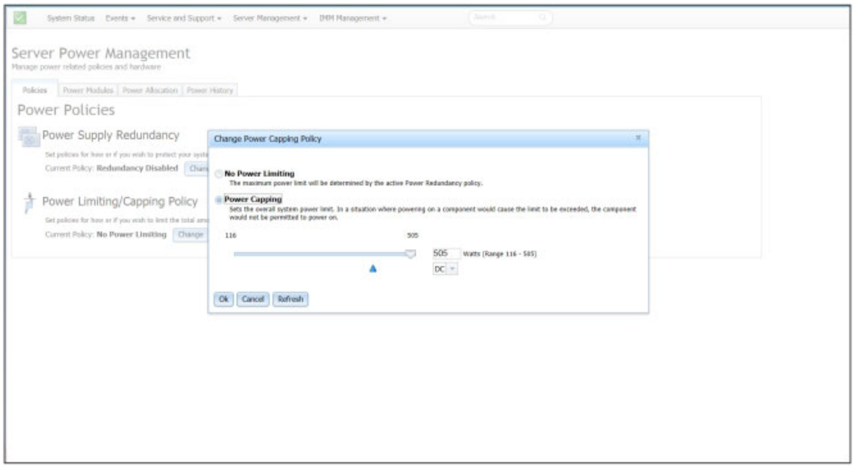
	Power Supply Failure Limit†	Maximum Power Limit (Watts)	Estimated Usage††
○ **Redundant without Throttling** System will be allowed to boot only if it is guaranteed to survive the loss of a power supply and continue to run without throttling.	1	550	100%
● **Redundant with Throttling** System will be allowed to boot only if it is guaranteed to survive the loss of a power supply, though it may need to throttle to continue running.	1	660	83%
○ **Non-Redundant** System will be allowed to boot provided that it is guaranteed to stay up and running without throttling and both power supplies operational. The system will throttle if a power supply fails in an attempt to stay up and running, but there is no guarantee.	0	1045	52%

† This is the maximum number of power supplies that can fail while still guaranteeing the operation of the selected policy.

†† The estimated usage is based on the maximum power limit allowed in this policy and the current aggregated power in use of all components in the chassis.

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.

On the Change Power Capping Policy window, click the **Power Capping** button and move the *slider mark* to the desired wattage to set the overall server power limit, (as shown in the following illustration). The arrow provides guidance in setting a power cap limit.



Server Power Management

Manage power related policies and hardware

Power Policies

Power Supply Redundancy

Set policies for how or if you wish to protect your syste

Current Policy: **Redundancy Disabled**

Power Limiting/Capping Policy

Set policies for how or if you wish to limit the total am

Current Policy: **No Power Limiting**

Change Power Capping Policy

○ **No Power Limiting**

The maximum power limit will be determined by the active Power Redundancy policy.

● **Power Capping**

Sets the overall system power limit. In a situation where powering on a component would cause the limit to be exceeded, the component would not be permitted to power on.

116 505

505 Watts (Range 116 - 505)

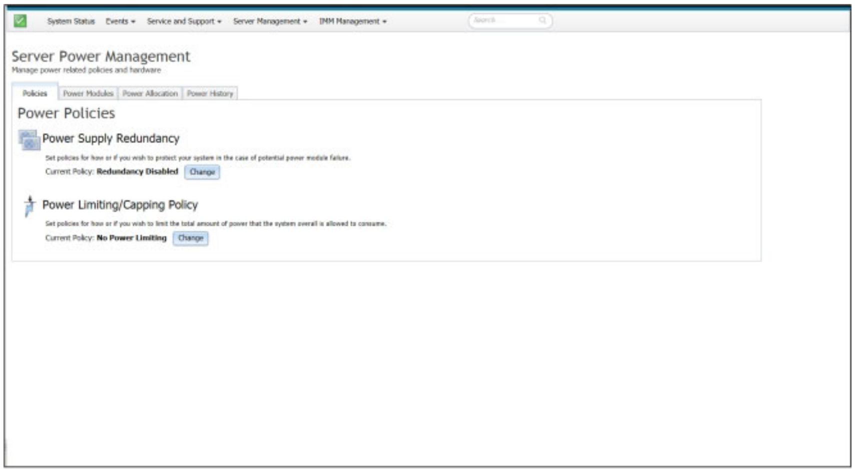
DC

Configuring up to four power supplies

If the server supports up to four power supplies you can configure the server to provide *power-feed* redundancy. With *power-feed* redundancy one or two power supplies are plugged into one power feed and one or two additional power supplies are plugged into another power feed. If one power feed fails, the power supply (supplies) on the other power feed will prevent failure of the server.

Note: For power-feed redundancy to function properly, the power supplies in bays 1 and 3 must be plugged into one power feed. The power supplies in bays 2 and 4 must be plugged into another power feed.

The following illustration shows the **Policies** tab for servers that support up to four power supplies.



Server Power Management

Manage power related policies and hardware

Power Policies

Power Supply Redundancy

Set policies for how or if you wish to protect your system in the case of potential power module failure.

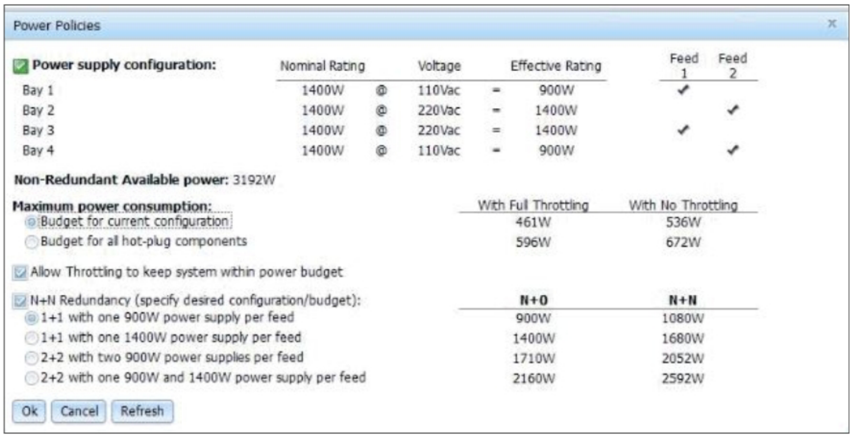
Current Policy: **Redundancy Disabled**

Power Limiting/Capping Policy

Set policies for how or if you wish to limit the total amount of power that the system overall is allowed to consume.

Current Policy: **No Power Limiting**

To select the policy you want to use to protect the server in the case of a potential power module failure, click the Current Policy **Change** button for the Power Supply Redundancy option on the Power Policies window. You will see a window similar to the following illustration. By choosing a power policy you can trade off between redundancy and available power.



Power Policies

☑ **Power supply configuration:**

	Nominal Rating		Voltage		Effective Rating	Feed 1	Feed 2
Bay 1	1400W	@	110Vac	=	900W	✓	
Bay 2	1400W	@	220Vac	=	1400W		✓
Bay 3	1400W	@	220Vac	=	1400W	✓	
Bay 4	1400W	@	110Vac	=	900W		✓

Non-Redundant Available power: 3192W

Maximum power consumption:	With Full Throttling	With No Throttling
● Budget for current configuration	461W	536W
○ Budget for all hot-plug components	596W	672W

☑ Allow Throttling to keep system within power budget

☑ N+N Redundancy (specify desired configuration/budget):	N+0	N+N
● 1+1 with one 900W power supply per feed	900W	1080W
○ 1+1 with one 1400W power supply per feed	1400W	1680W
○ 2+2 with two 900W power supplies per feed	1710W	2052W
○ 2+2 with one 900W and 1400W power supply per feed	2160W	2592W

Available fields on the Power Polices page are as follows:

Power supply configuration

This field is a read-only section that displays the power supplies in each bay and associated information for each power supply.

Non-Redundant Available power

When the server is running in a non-redundant mode of operation, this field displays the available non-redundant power. All of the power from all power supplies is assumed to be available in the non-redundant mode of operation.

Maximum power consumption

This field displays the maximum amount of power the server is capable of consuming, regardless of the power supplies installed. You can choose the configuration you want to budget for by selecting one of the following:

- Budget for current configuration
- Budget for all hot-plug components

Allow Throttling to keep system within power budget

Click this checkbox to permit throttling. Microprocessor throttling is a process that efficiently saves server energy and power; therefore, keeping the server within the power budget.

Note: Throttling during normal operation might impair performance of the server.

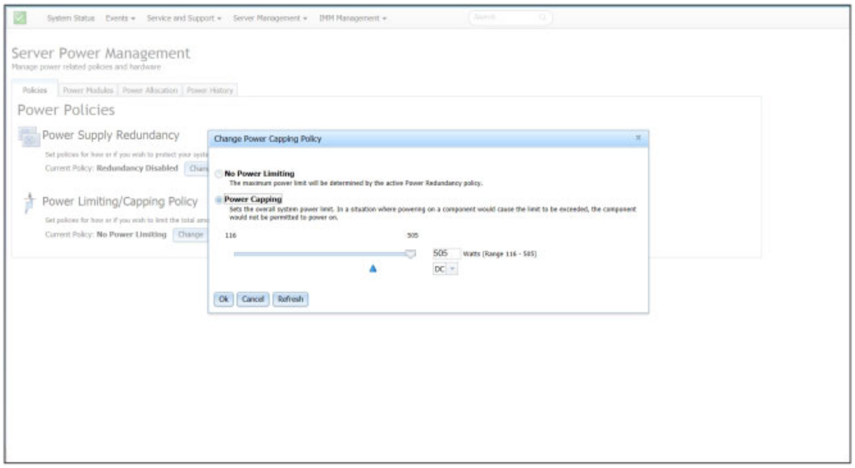
N+N Redundancy (specify desired configuration/budget)

Click this checkbox if you want the server to run in the redundancy mode of operation. When you click this checkbox, you are presented with additional redundancy configurations to choose from to achieve your desired configuration or power budget.

Note: If this checkbox is not selected, the server will run without redundancy.

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.

On the Change Power Capping Policy window, click the **Power Capping** button and move the *slider mark* to the desired wattage to set the overall server power limit, (as shown in the following illustration). The arrow provides guidance in setting a power cap limit.



Server Power Management

Manage power related policies and hardware

Power Policies

Power Supply Redundancy

Set policies for how or if you wish to protect your syste

Current Policy: **Redundancy Disabled** Chan

Power Limiting/Capping Policy

Set policies for how or if you wish to limit the total amo

Current Policy: **No Power Limiting** Change

Change Power Capping Policy

○ **No Power Limiting**

The maximum power limit will be determined by the active Power Redundancy policy.

● **Power Capping**

Sets the overall system power limit. In a situation where powering on a component would cause the limit to be exceeded, the component would not be permitted to power on.

116 505

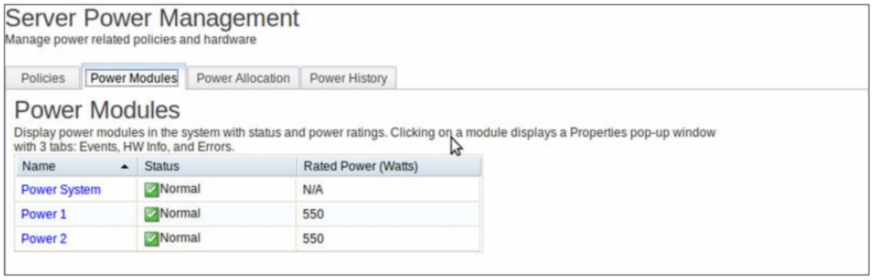
505 Watts (Range 116 - 585)

DC

Displaying currently installed power supplies

Click the **Power Modules** tab to display information about the currently installed power supplies. The name of each power module installed 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.

The following illustration shows the **Power Modules** tab for servers that can support up to two power supplies.



Server Power Management

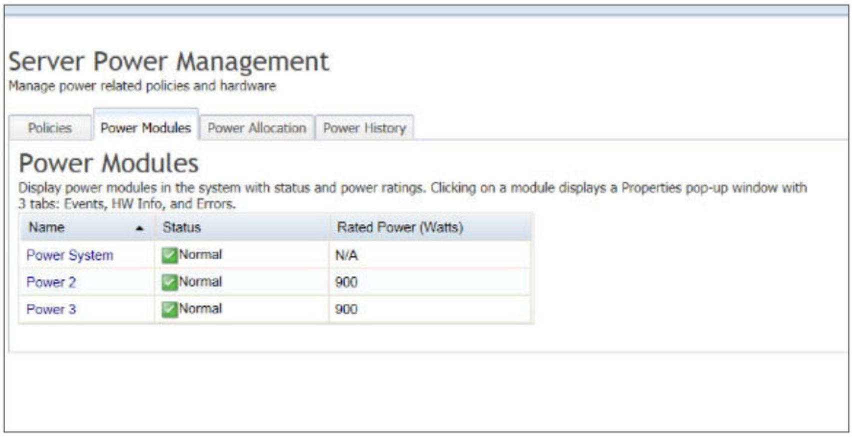
Manage power related policies and hardware

Power Modules

Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.

Name ▲	Status	Rated Power (Watts)
Power System	✓Normal	N/A
Power 1	✓Normal	550
Power 2	✓Normal	550

The following illustration shows the **Power Modules** tab for servers that can support up to four power supplies.



Server Power Management

Manage power related policies and hardware

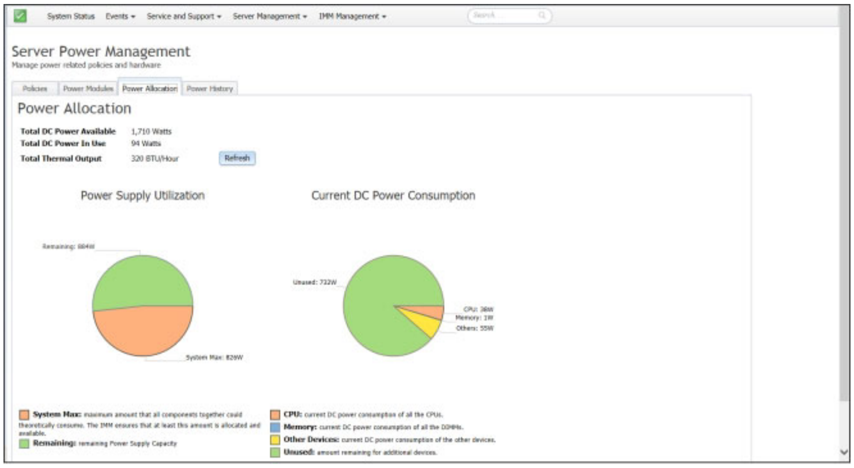
Power Modules

Display power modules in the system with status and power ratings. Clicking on a module displays a Properties pop-up window with 3 tabs: Events, HW Info, and Errors.

Name ▲	Status	Rated Power (Watts)
Power System	✓ Normal	N/A
Power 2	✓ Normal	900
Power 3	✓ Normal	900

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).



Server Power Management

Manage power related policies and hardware

Power Allocation

Total DC Power Available	1,710 Watts
Total DC Power In Use	94 Watts
Total Thermal Output	320 BTU/Hour

🟧 **System Max:** maximum amount that all components together could theoretically consume. The IMM ensures that at least this amount is allocated and available.

🟩 **Remaining:** remaining Power Supply Capacity

🟧 **CPU:** current DC power consumption of all the CPUs.

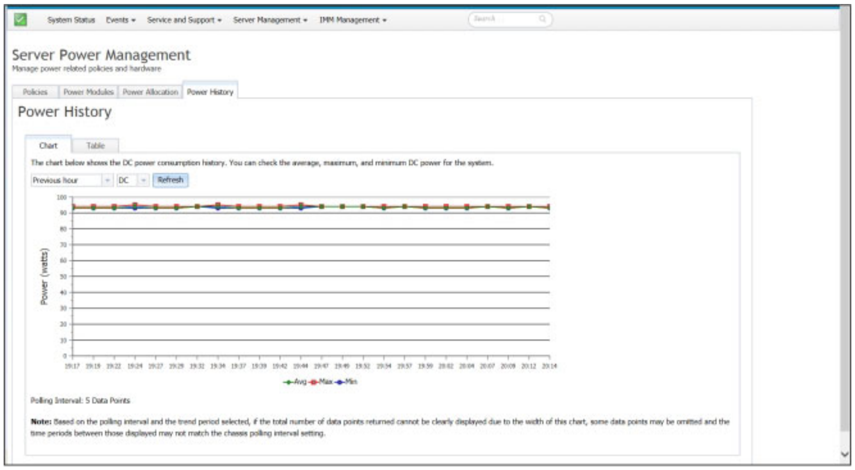
🟦 **Memory:** current DC power consumption of all the DIMMs.

🟨 **Other Devices:** current DC power consumption of the other devices.

🟩 **Unused:** amount remaining for additional devices.

Displaying the power history

Click the **Power History** tab to display how much power is being used by the server 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).



Server Power Management

Manage power related policies and hardware

Power History

The chart below shows the DC power consumption history. You can check the average, maximum, and minimum DC power for the system.

Previous hour ▾ DC ▾ Refresh

Polling Interval: 5 Data Points

Note: Based on the polling interval and the trend period selected, if the total number of data points returned cannot be clearly displayed due to the width of this chart, some data points may be omitted and the time periods between those displayed may not match the chassis polling interval setting.

Displaying the power performance

Click the **Performance** tab to display the power performance information for the server. The **Performance** tab might not be available on all systems. The **Chart** and **Table** tabs show the compute utilization history and power performance for the following components:

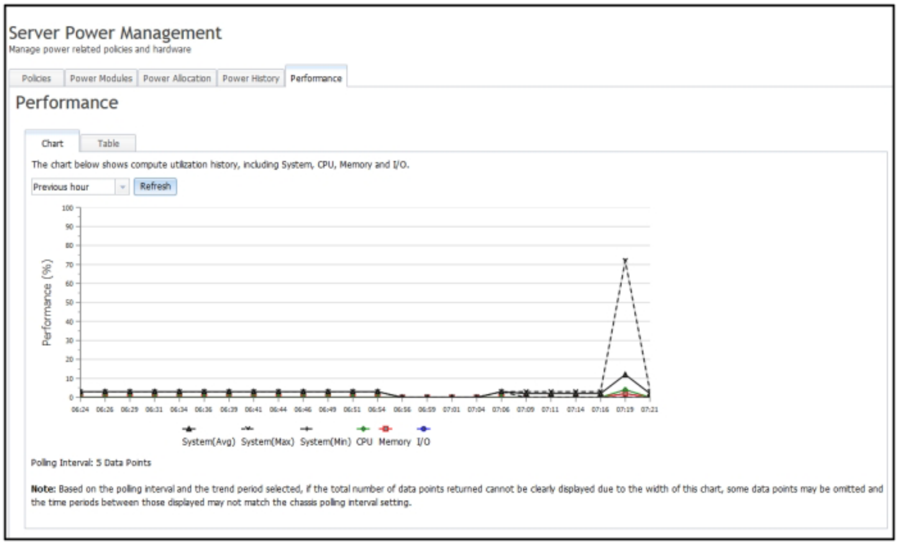
- System
- Microprocessor
- Memory
- I/O

On the **Chart** tab select the **Previous hour** list to select the period of time to be displayed. Optional choices are the following:

- 1 hour
- 6 hours
- 12 hours
- 24 hours

Click the **Refresh** button to refresh the information simultaneously in the **Chart** and **Table** tabs. In the following illustration (for the **Chart** tab), the selected time is displayed horizontally (X-axis) and the performance (percentage) is displayed vertically (Y-axis) for the following performance indicators:

- System (Avg)
- System (Max)
- System (Min)
- Microprocessor
- Memory
- I/O



Server Power Management

Manage power related policies and hardware

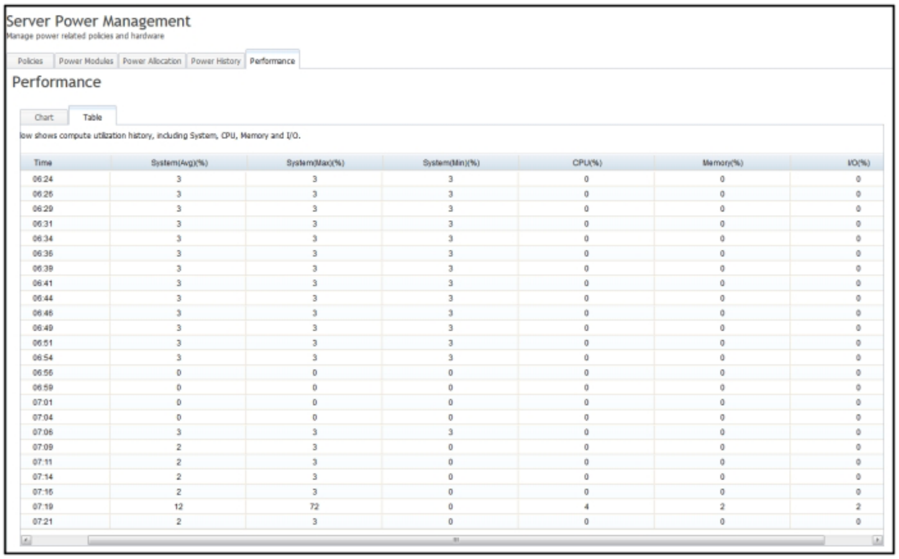
Performance

The chart below shows compute utilization history, including System, CPU, Memory and I/O.

Polling Interval: 5 Data Points

Note: Based on the polling interval and the trend period selected, if the total number of data points returned cannot be clearly displayed due to the width of this chart, some data points may be omitted and the time periods between those displayed may not match the chassis polling interval setting.

The **Table** tab displays the same performance indicators and information in a different format, as shown in the following illustration.



Server Power Management

Manage power related policies and hardware

Performance

low shows compute utilization history, including System, CPU, Memory and I/O.

Time	System(Avg)(%)	System(Max)(%)	System(Min)(%)	CPU(%)	Memory(%)	I/O(%)
06:24	3	3	3	0	0	0
06:26	3	3	3	0	0	0
06:29	3	3	3	0	0	0
06:31	3	3	3	0	0	0
06:34	3	3	3	0	0	0
06:36	3	3	3	0	0	0
06:39	3	3	3	0	0	0
06:41	3	3	3	0	0	0
06:44	3	3	3	0	0	0
06:46	3	3	3	0	0	0
06:49	3	3	3	0	0	0
06:51	3	3	3	0	0	0
06:54	3	3	3	0	0	0
06:56	0	0	0	0	0	0
06:59	0	0	0	0	0	0
07:01	0	0	0	0	0	0
07:04	0	0	0	0	0	0
07:06	3	3	3	0	0	0
07:09	2	3	0	0	0	0
07:11	2	3	0	0	0	0
07:14	2	3	0	0	0	0
07:16	2	3	0	0	0	0
07:19	12	72	0	4	2	2
07:21	2	3	0	0	0	0

Managing and monitoring power consumption with IPMI commands

This topic describes how the Intel Intelligent Power Node Manager and the Data Center Manageability Interface (DCMI) can be used to provide power and thermal monitoring and policy-based power management for a server using Intelligent Platform Management Interface (IPMI) power management commands.

For servers using Intel Node Manager SPS 3.0, IMM2 users can use IPMI power management commands provided by Intel's Management Engine (ME) to control Node Manager features and monitor server power consumption. Server power management can also be accomplished using DCMI power management commands. Example Node Manager and DCMI power management commands are provided in this topic.

Managing the server power using Node Manager commands

The Intel Node Manager firmware does not have an external interface; therefore, the Node Manager commands must first be received by the IMM2 and then sent to the Intel Node Manager. The IMM2 functions as a relay and a transport device for the IPMI commands using standard IPMI bridging.

Note: Changing Node manager policies using Node Manager IPMI commands might create conflicts with the IMM2 power management functionality. By default, bridging of the Node Manager commands is disabled to prevent any conflict.

For users who want to manage the server power using the Node Manager instead of the IMM2, an OEM IPMI command consisting of (network function: *0x3A*) and (command: *0xC7*) is available for use.

To enable native Node Manager IPMI commands type:

```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x01
```

To disable native Node Manager IPMI commands type:

```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x00
```

The following information are examples of Node Manager power management commands.

Notes:

- By specifying IPMI *channel 0* and a target address of *0x2c*, you can use the IPMITOOL to send commands to the Intel Node Manager for processing. A request message is used to initiate an action and a response message is returned to the requester.
- Commands are displayed in the following format due to space limitations.

Power monitoring using the Get Global System Power Statistics, (command code 0xC8):

Request:

```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2E
0xC8 0x57 0x01 0x00 0x01 0x00 0x00
```

Response:

57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Power capping using the Set Intel Node Manager Policy, (command code 0xC1):

Request:

```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e
0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00
0x00 0x1e 0x00
```

Response:

57 01 00

Power savings using the Set Intel Node Manager Policy, (command code 0xC1):

Request:

```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e
0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00
0x00 0x1e 0x00
```

Get device ID function using the Get Intel Management Engine Device ID:

Request:

```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x06
```

```
0x01
```
Response:
50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

For additional Intel Node Manager commands, see the latest release of the *Intel Intelligent Power Node Manager External Interface Specification Using IPMI* at https://businessportal.intel.com.

Managing the server power using DCMI commands

The DCMI provides monitoring and control functions that can be exposed through standard management software interfaces. Server power management functions can also be accomplished using DCMI commands.

The following information are examples of commonly used DCMI power management functions and commands. A request message is used to initiate an action and a response message is returned to the requester.

Note: Commands are displayed in the following formats due to space limitations.

Get Power Reading:
Request:
```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x02 0xdc 0x01
0x00 0x00
```
Response:
```
dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40
```

Set Power Limit:
Request:
```
ipmitool -H <$IMM_IP> -U <USERID> -P PASSWORD raw 0x2c 0x04 0xdc 0x00 0x00
0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03
```
Response:
```
dc
```

Get Power Cap:
Request:
```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x03 0xdc 0x00
0x00
```
Response:
```
dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00
```

Activate the Power Limit:
Request:
```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x01
0x00 0x00
```
Response:
```
dc
```

Deactivate the Power Limit: function:
Request:
```
ipmitool -H <$IMM_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x00
0x00 0x00
```
Response:
```
dc
```

Note: On some servers the Exception Actions for the **Set Power Limit** command might not be supported. For example, the *Hard Power Off system and log events to SEL* parameter might not be supported.

For the complete list of commands that are supported by the DCMI specification, see the latest release of the *Data Center Manageability Interface Specification* at http://www.intel.com/content/www/us/en/data-center/dcmi/data-center-manageability-interface.html.

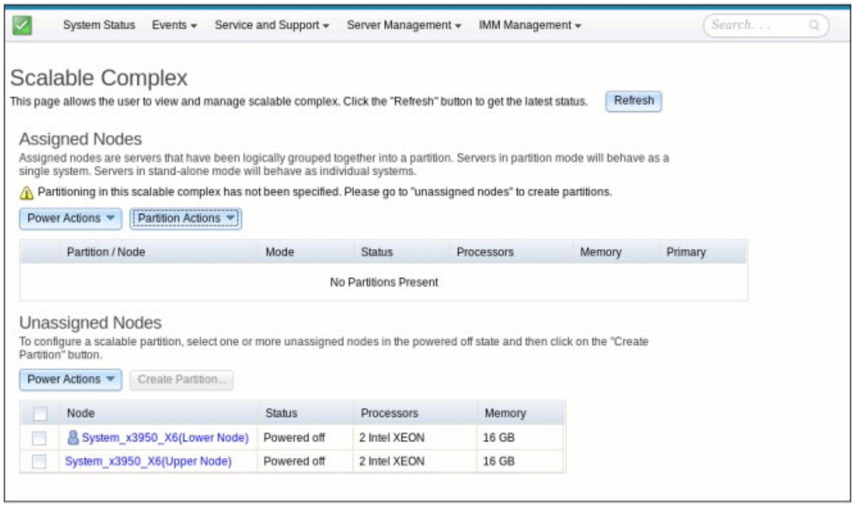
Managing the scalable complex

Note: In this section the words *nodes* and *servers* are used interchangeably.

Use the **Scalable Complex** option to view and manage the current state of all available nodes (servers). A scalable complex allows nodes to be subdivided into separate partitions or independent nodes. Assigned nodes are servers that are logically grouped together into a partition. Servers in a partition act as a *single* system and can share resources with each other. The nodes in a partition can also be separated into stand-alone (independent) nodes. A node in the stand-alone mode performs as an *individual* system. Select the **Scalable Complex** option under the **Server Management** tab to configure the server. The Scalable Complex page consist of the Assigned Nodes and Unassigned Nodes sections. You can click the **Refresh** button to get the latest status information for the nodes.

The following illustration has no assigned nodes. In this illustration the nodes perform as individual servers. Without any nodes being assigned the only available functionality is to remotely control the server power or create a partition from the Assigned Nodes section. You can control the server power by selecting the **Power Actions** tab, see "Controlling the power status of the server" on page 122 for additional information.

Note: All power to the server must be turned off to add or remove a partition.



Scalable Complex

This page allows the user to view and manage scalable complex. Click the "Refresh" button to get the latest status.

Assigned Nodes

Assigned nodes are servers that have been logically grouped together into a partition. Servers in partition mode will behave as a single system. Servers in stand-alone mode will behave as individual systems.

⚠ Partitioning in this scalable complex has not been specified. Please go to "unassigned nodes" to create partitions.

	Partition / Node	Mode	Status	Processors	Memory	Primary
	No Partitions Present					

Unassigned Nodes

To configure a scalable partition, select one or more unassigned nodes in the powered off state and then click on the "Create Partition" button.

□	Node	Status	Processors	Memory
□	System_x3950_X6(Lower Node)	Powered off	2 Intel XEON	16 GB
□	System_x3950_X6(Upper Node)	Powered off	2 Intel XEON	16 GB

Creating a partition

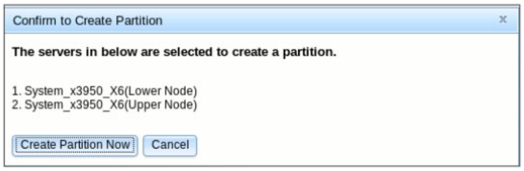
In the Unassigned nodes section of the Scalable Complex page, select the checkbox that corresponds to the nodes that you want to add to your partition.

Notes:

- To add a partition all power to the server must be turned off.
- The **Create Partition** button is grayed out until a node is selected.
- If you select the Node check box, all nodes are automatically included and marked as checked.
- Firmware versions of the nodes within the scalable complex must be the same.

A Confirm to Create Partition window opens consisting of the nodes previously selected, (as shown in the following illustration). Click the **Create Partition Now** button to create the partition. You will receive a confirmation message indicating the partition is successfully created. Click the **Refresh** button to see the new partition status if the page does not automatically refresh. Once the partition is created the status of all partitions and any unassigned nodes is displayed. Power to the server can be turned on or off using the **Power Actions** button and the partition can be removed or the mode of operation for the partition can be changed using the **Partition Actions** button.

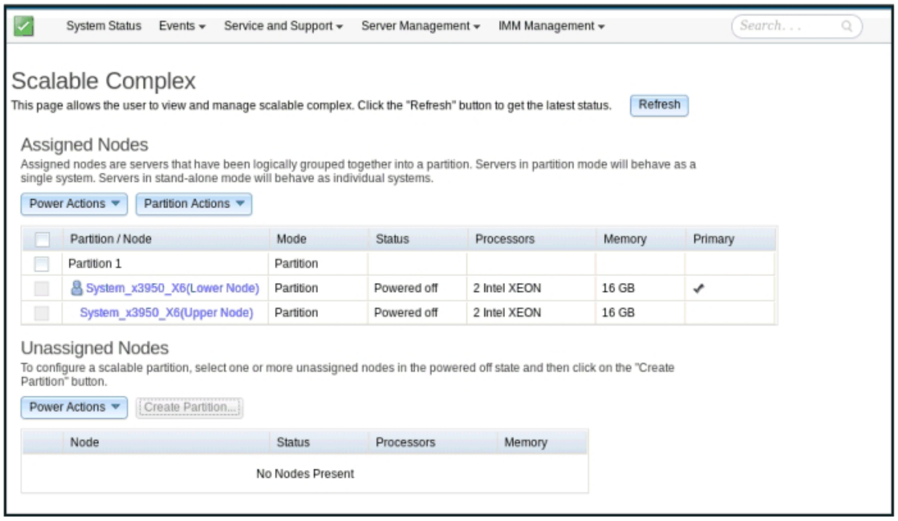
Note: Nodes in the partition mode of operation perform as one single system sharing resources.



The servers in below are selected to create a partition.

1. System_x3950_X6(Lower Node)
2. System_x3950_X6(Upper Node)

After the partition is created you will see a window similar to the following illustration displaying the status of all partitions and unassigned nodes.



Scalable Complex

This page allows the user to view and manage scalable complex. Click the "Refresh" button to get the latest status.

Assigned Nodes

Assigned nodes are servers that have been logically grouped together into a partition. Servers in partition mode will behave as a single system. Servers in stand-alone mode will behave as individual systems.

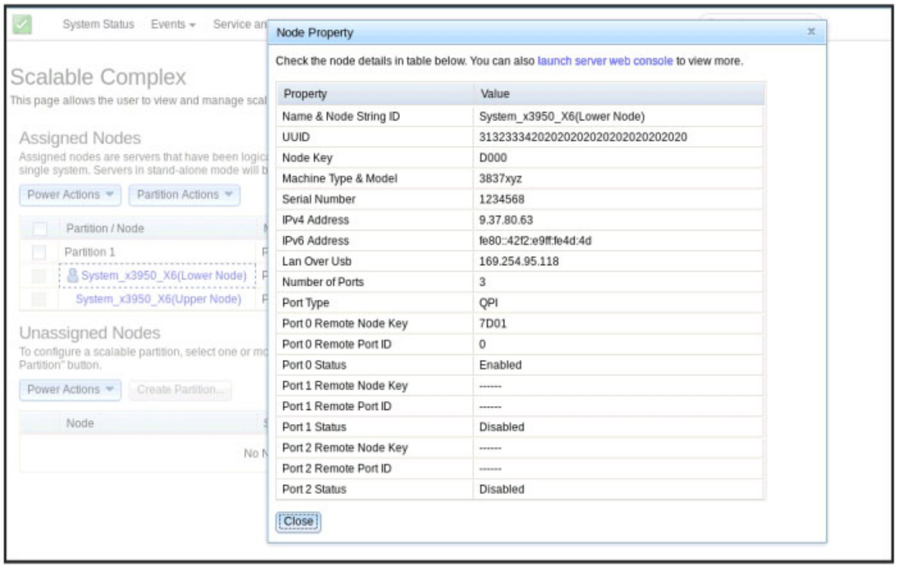
□	Partition / Node	Mode	Status	Processors	Memory	Primary
□	Partition 1	Partition				
□	System_x3950_X6(Lower Node)	Partition	Powered off	2 Intel XEON	16 GB	✓
□	System_x3950_X6(Upper Node)	Partition	Powered off	2 Intel XEON	16 GB	

Unassigned Nodes

To configure a scalable partition, select one or more unassigned nodes in the powered off state and then click on the "Create Partition" button.

	Node	Status	Processors	Memory
	No Nodes Present			

The details for a node are accessed by clicking on an individual node in the partition. The Node Property window is displayed (as shown in the following illustration).



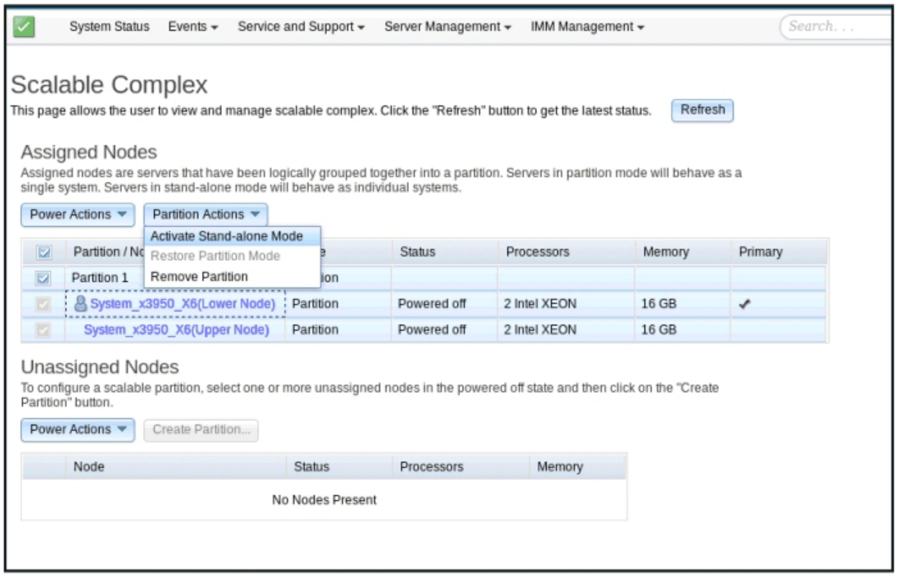
Node Property

Check the node details in table below. You can also launch server web console to view more.

Property	Value
Name & Node String ID	System_x3950_X6(Lower Node)
UUID	31323334202020202020202020202020
Node Key	D000
Machine Type & Model	3837xyz
Serial Number	1234568
IPv4 Address	9.37.80.63
IPv6 Address	fe80::42f2:e9ff:fe4d:4d
Lan Over Usb	169.254.95.118
Number of Ports	3
Port Type	QPI
Port 0 Remote Node Key	7D01
Port 0 Remote Port ID	0
Port 0 Status	Enabled
Port 1 Remote Node Key	------
Port 1 Remote Port ID	------
Port 1 Status	Disabled
Port 2 Remote Node Key	------
Port 2 Remote Port ID	------
Port 2 Status	Disabled

Changing a partition mode

Click the **Partition Actions** tab on the Scalable Complex page to change the mode of operation for the partition or to remove the partition (as shown in the following illustration).



Scalable Complex

This page allows the user to view and manage scalable complex. Click the "Refresh" button to get the latest status.

Assigned Nodes

Assigned nodes are servers that have been logically grouped together into a partition. Servers in partition mode will behave as a single system. Servers in stand-alone mode will behave as individual systems.

☑	Partition / Nc	e	Status	Processors	Memory	Primary
☑	Partition 1	ion				
☑	System_x3950_X6(Lower Node)	Partition	Powered off	2 Intel XEON	16 GB	✓
☑	System_x3950_X6(Upper Node)	Partition	Powered off	2 Intel XEON	16 GB	

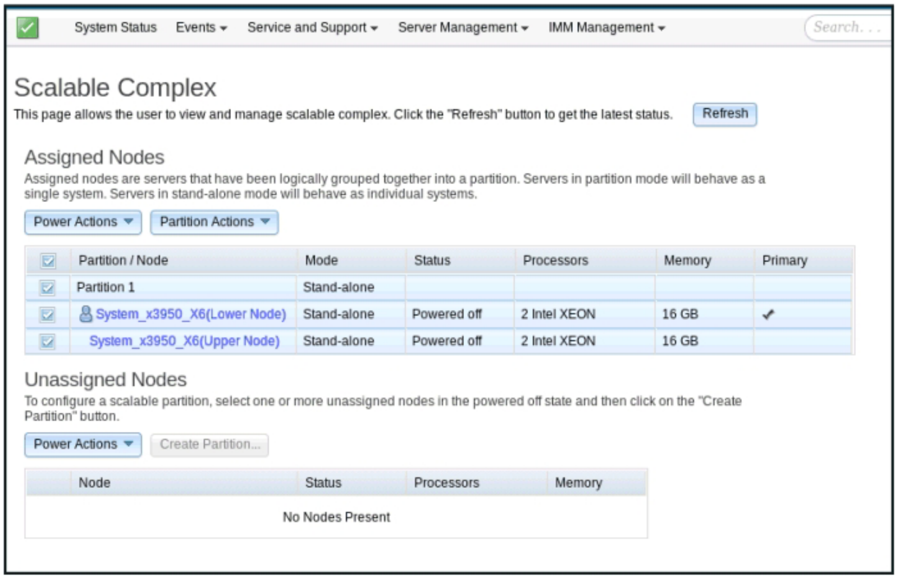
Unassigned Nodes

To configure a scalable partition, select one or more unassigned nodes in the powered off state and then click on the "Create Partition" button.

Node	Status	Processors	Memory
No Nodes Present			

Click **Activate Stand-alone Mode** to allow each node to act independently of one another. Click **Restore Partition Mode** to switch between the partition and stand-alone modes. Click **Remove Partition** to remove the partition.

The following illustration shows the nodes in the stand-alone mode of operation.



Scalable Complex

This page allows the user to view and manage scalable complex. Click the "Refresh" button to get the latest status.

Assigned Nodes

Assigned nodes are servers that have been logically grouped together into a partition. Servers in partition mode will behave as a single system. Servers in stand-alone mode will behave as individual systems.

☑	Partition / Node	Mode	Status	Processors	Memory	Primary
☑	Partition 1	Stand-alone				
☑	System_x3950_X6(Lower Node)	Stand-alone	Powered off	2 Intel XEON	16 GB	✓
☑	System_x3950_X6(Upper Node)	Stand-alone	Powered off	2 Intel XEON	16 GB	

Unassigned Nodes

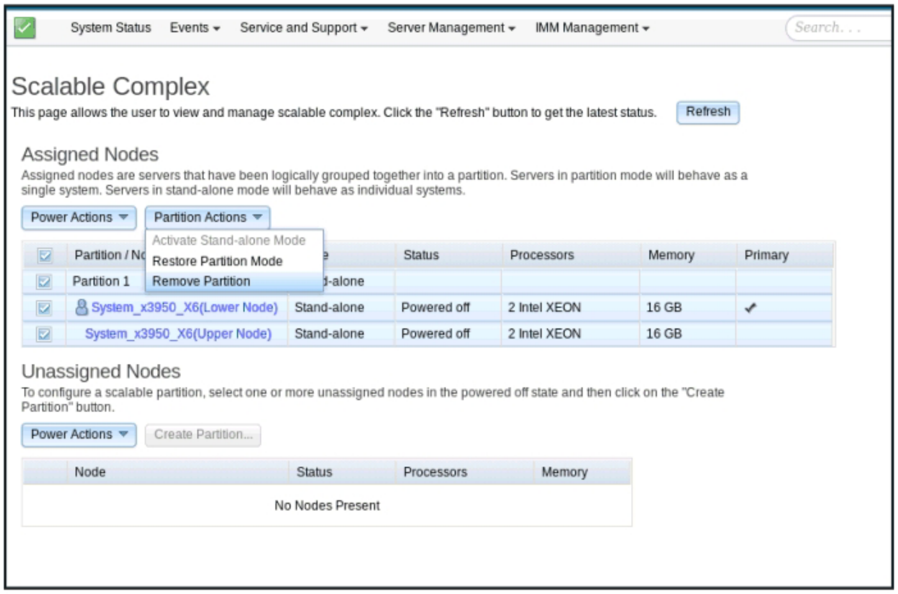
To configure a scalable partition, select one or more unassigned nodes in the powered off state and then click on the "Create Partition" button.

Node	Status	Processors	Memory
No Nodes Present			

Deleting a partition mode

Select the **Remove Partition** tab to delete a partition (as shown in the following illustration).

Note: To remove a partition the power to the node must be turned off.



Scalable Complex

This page allows the user to view and manage scalable complex. Click the "Refresh" button to get the latest status.

Assigned Nodes

Assigned nodes are servers that have been logically grouped together into a partition. Servers in partition mode will behave as a single system. Servers in stand-alone mode will behave as individual systems.

☑	Partition / No	e	Status	Processors	Memory	Primary
☑	Partition 1	l-alone				
☑	System_x3950_X6(Lower Node)	Stand-alone	Powered off	2 Intel XEON	16 GB	✓
☑	System_x3950_X6(Upper Node)	Stand-alone	Powered off	2 Intel XEON	16 GB	

Unassigned Nodes

To configure a scalable partition, select one or more unassigned nodes in the powered off state and then click on the "Create Partition" button.

Node	Status	Processors	Memory
No Nodes Present			

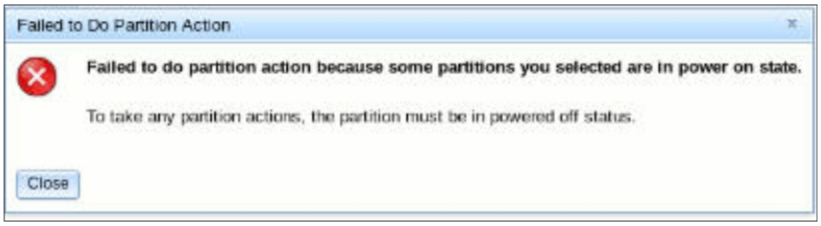
Partition errors

Error conditions can occur when working with partitions. If an error condition exists, the IMM2 will return an event code to the event logs. Two error conditions are described in the following table and displayed in the next two illustrations.

Table 10. Partition error conditions

Error	Description	Action
Failed to do partition action.	Some partitions that are selected are in the power on state.	Power off the partition.
Failed to group partition.	There is a mismatch of the firmware versions between the nodes within the complex.	Update the IMM2 firmware version for all of the nodes to the same firmware version.

The following illustration is the response received if attempting to perform any type of partition action and the nodes in that partition are powered on. To correct this problem power down all nodes in the partition.

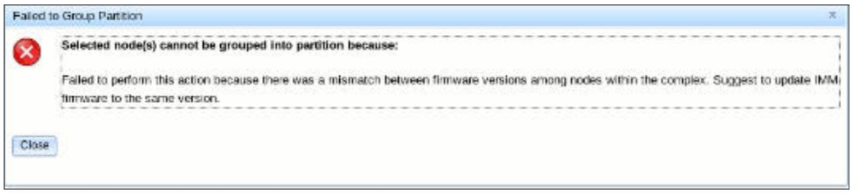


Failed to Do Partition Action

Failed to do partition action because some partitions you selected are in power on state.

To take any partition actions, the partition must be in powered off status.

The following illustration is the response received if there is a mismatch between the firmware versions among the nodes. To correct this problem ensure all nodes contain the same IMM2 firmware version.



Failed to Group Partition

Selected node(s) cannot be grouped into partition because:

Failed to perform this action because there was a mismatch between firmware versions among nodes within the complex. Suggest to update IMM firmware to the same version.

Viewing and configuring the local storage configuration

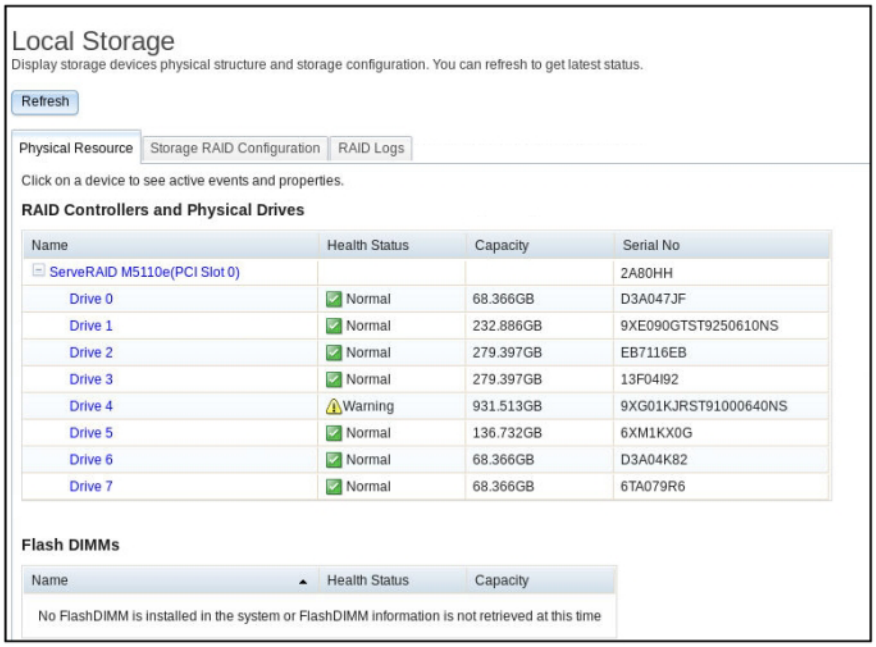
Click the **Local Storage** option under the **Server Management** tab or the Local Storage link in the Hardware Health table on the System Status and Health page to view the storage status and configure storage information for the server. This option provides the local storage status, configuration, and detailed information for the server.

Note: If the server does not support the **Local Storage** option, only the status of the disks and associated active events are displayed.

Viewing the physical resource information

On the Local Storage page click the **Physical Resource** tab to display the physical resource summary of the server (as shown in the following illustration). The summary includes the supported RAID controller and associated drive information. To obtain the latest status information click the **Refresh** button.

Note: On the Physical Resource page, the supported RAID controllers and associated physical drives are displayed. For physical drives that do not have an associated RAID controller, `None-manageable drives to IMM` is displayed in the **Name** field.



Local Storage

Display storage devices physical structure and storage configuration. You can refresh to get latest status.

Click on a device to see active events and properties.

RAID Controllers and Physical Drives

Name	Health Status	Capacity	Serial No
⊟ ServeRAID M5110e(PCI Slot 0)			2A80HH
Drive 0	✓ Normal	68.366GB	D3A047JF
Drive 1	✓ Normal	232.886GB	9XE090GTST9250610NS
Drive 2	✓ Normal	279.397GB	EB7116EB
Drive 3	✓ Normal	279.397GB	13F04I92
Drive 4	⚠ Warning	931.513GB	9XG01KJRST91000640NS
Drive 5	✓ Normal	136.732GB	6XM1KX0G
Drive 6	✓ Normal	68.366GB	D3A04K82
Drive 7	✓ Normal	68.366GB	6TA079R6

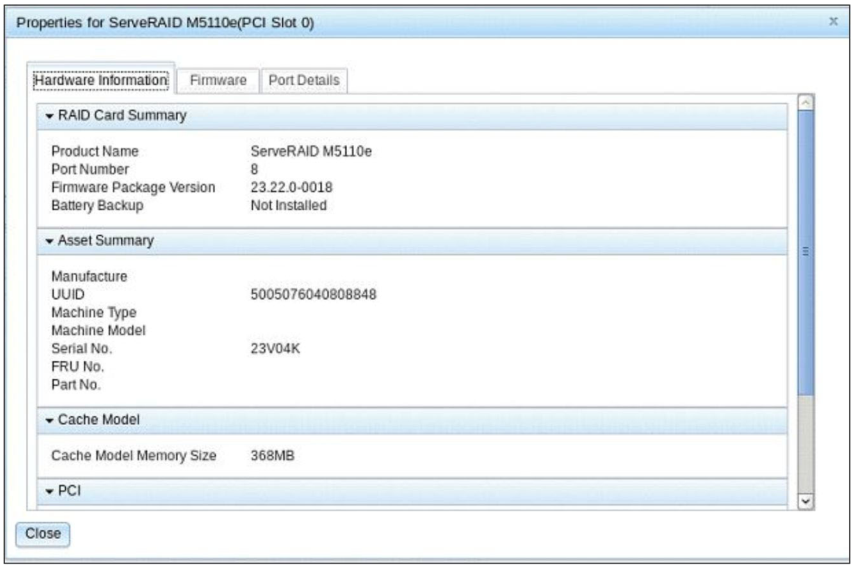
Flash DIMMs

Name ▲	Health Status	Capacity
No FlashDIMM is installed in the system or FlashDIMM information is not retrieved at this time		

Click the link of the supported RAID controller to view the controller's active events, hardware, firmware, and port information.

The **Hardware Information** tab, contains the following information (as shown in the following illustration):

- RAID card summary
- Asset summary
- Cache model
- PCI
- Battery backup (if a battery backup has been installed)


Properties for ServeRAID M5110e(PCI Slot 0)

▾ RAID Card Summary

Product Name	ServeRAID M5110e
Port Number	8
Firmware Package Version	23.22.0-0018
Battery Backup	Not Installed

▾ Asset Summary

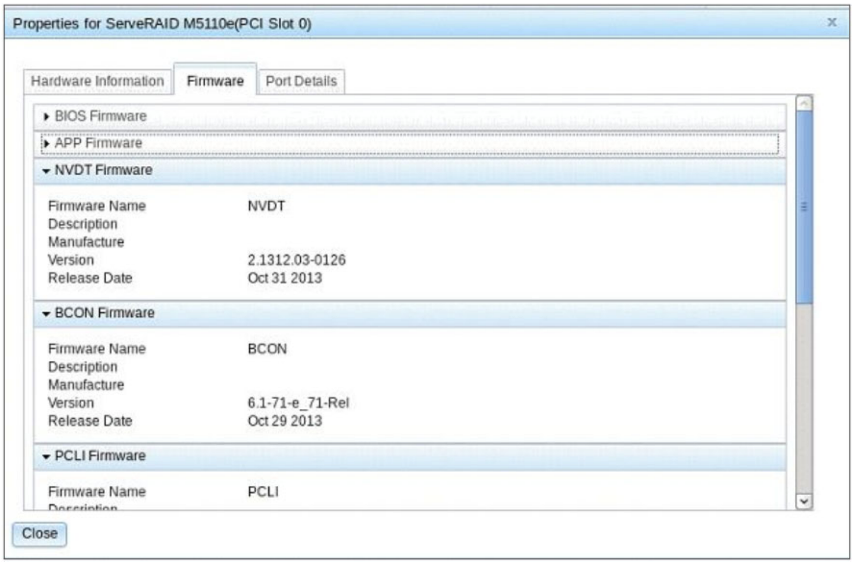
Manufacture	
UUID	5005076040808848
Machine Type	
Machine Model	
Serial No.	23V04K
FRU No.	
Part No.	

▾ Cache Model

Cache Model Memory Size	368MB

▾ PCI

The **Firmware** tab contains detailed firmware information for the RAID controller (as shown in the following illustration).


Properties for ServeRAID M5110e(PCI Slot 0)

▸ BIOS Firmware

▸ APP Firmware

▾ NVDT Firmware

Firmware Name	NVDT
Description	
Manufacture	
Version	2.1312.03-0126
Release Date	Oct 31 2013

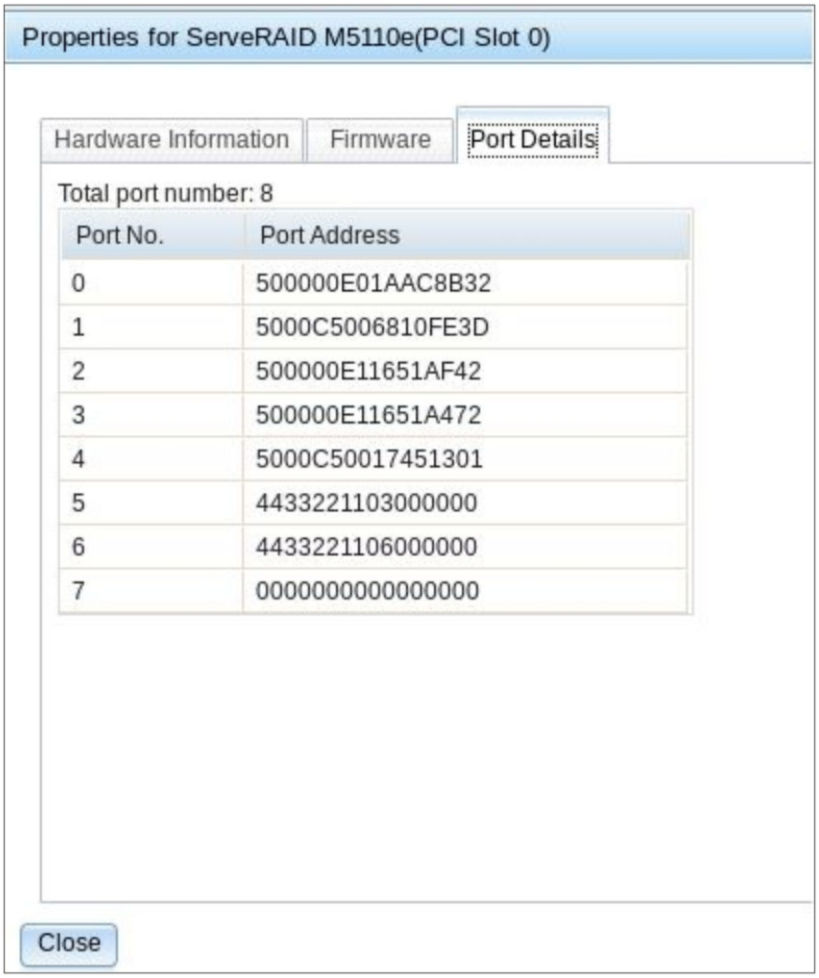
▾ BCON Firmware

Firmware Name	BCON
Description	
Manufacture	
Version	6.1-71-e_71-Rel
Release Date	Oct 29 2013

▾ PCLI Firmware

Firmware Name	PCLI
Description	

The **Port Details** tab contains the port number and port address information for the RAID controller (as shown in the following illustration).



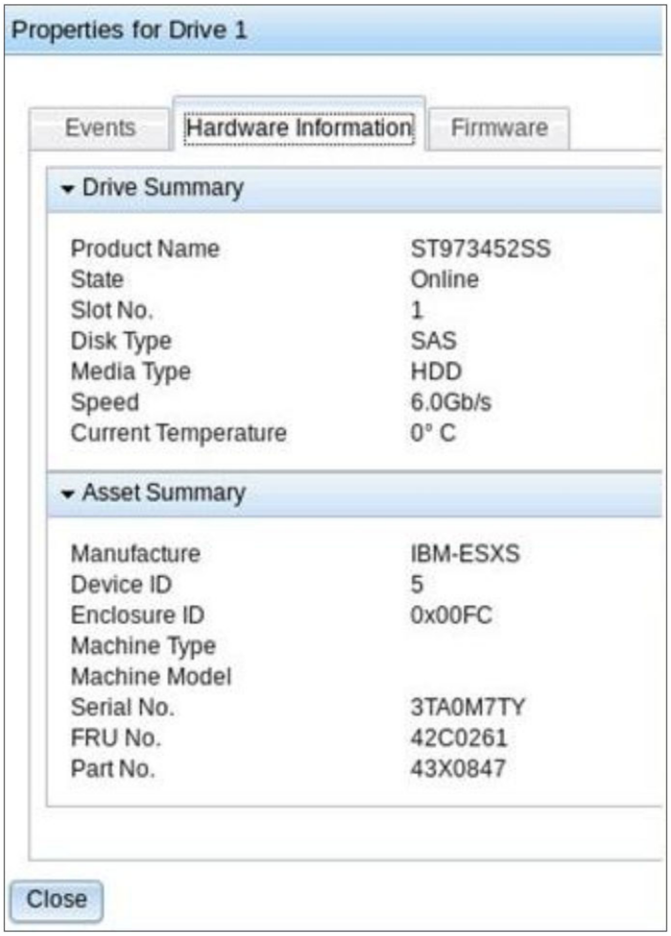
Total port number: 8

Port No.	Port Address
0	500000E01AAC8B32
1	5000C5006810FE3D
2	500000E11651AF42
3	500000E11651A472
4	5000C50017451301
5	4433221103000000
6	4433221106000000
7	0000000000000000

Click the link of the associated drive for the RAID controller. The Properties page for the drive opens. Click the **Events**, **Hardware Information**, or **Firmware** tab to view additional information about the drive.

Note: If the drive is displayed as `Non-manageable drives to IMM` on the Physical Resource page, only the associated active events are displayed.

The following two illustrations display the Hardware Information and Firmware pages for the drive associated with the RAID controller.

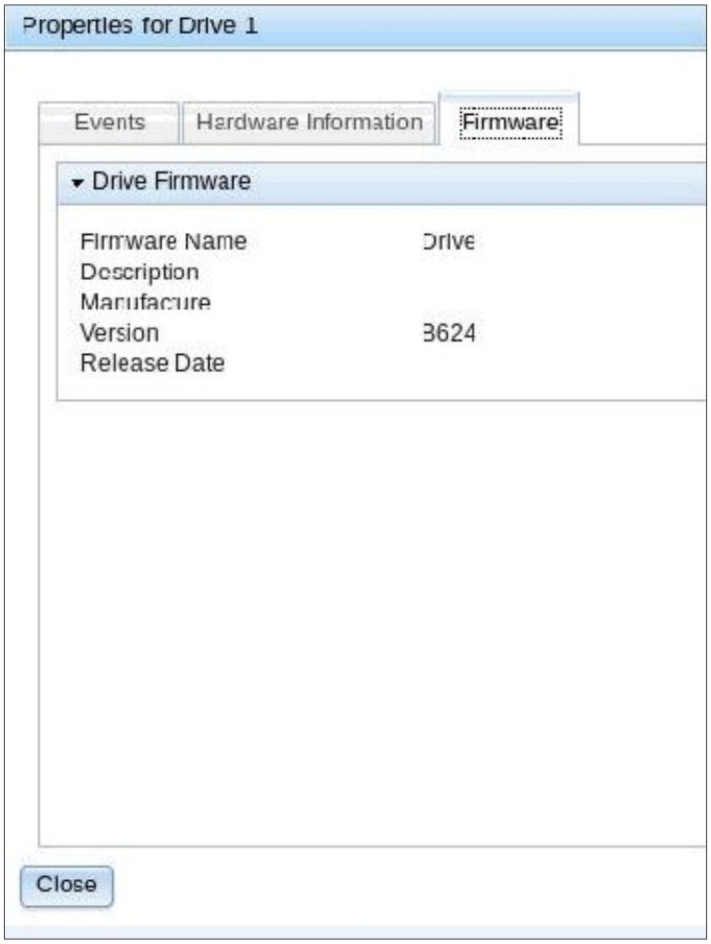


Drive Summary

Product Name	ST973452SS
State	Online
Slot No.	1
Disk Type	SAS
Media Type	HDD
Speed	6.0Gb/s
Current Temperature	0° C

Asset Summary

Manufacture	IBM-ESXS
Device ID	5
Enclosure ID	0x00FC
Machine Type	
Machine Model	
Serial No.	3TA0M7TY
FRU No.	42C0261
Part No.	43X0847



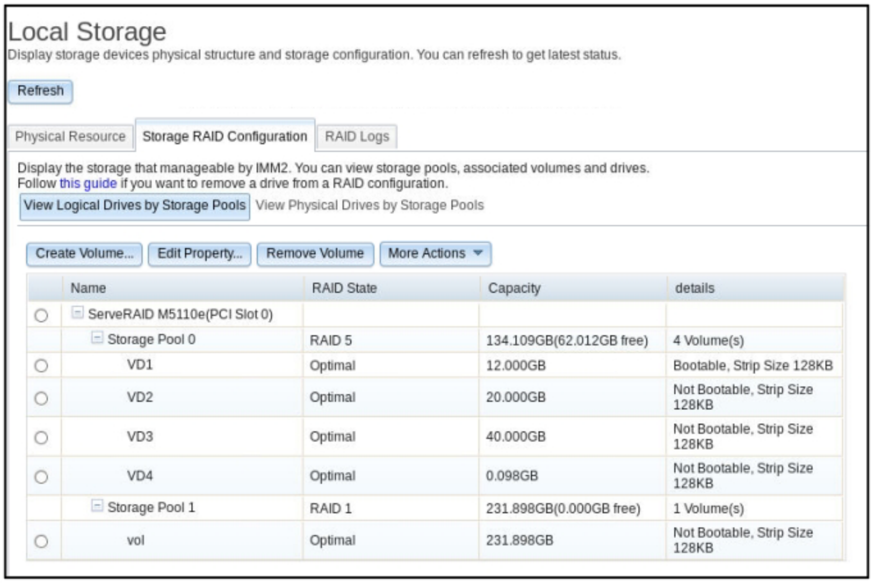
Drive Firmware

Firmware Name Drive
Description
Manufacture
Version B624
Release Date

Displaying and configuring the storage RAID configuration information

On the Local Storage page click the **Storage Raid Configuration** tab to display and configure (if supported by the platform), the storage that is managed by the IMM2. You can view and configure storage pools, associated volumes and drives for the RAID controller. To obtain the latest status information click the **Refresh** button.

The **View Logical Drives by Storage Pools** tab displays and configures (if supported by the platform) the logical drives on the RAID controller (as shown in the following illustration). The logical drives are sorted by storage pools and controllers. Detailed information about the volume such as the volume strip size and bootable information is displayed.



Local Storage

Display storage devices physical structure and storage configuration. You can refresh to get latest status.

Refresh
Physical Resource
Storage RAID Configuration
RAID Logs

Display the storage that manageable by IMM2. You can view storage pools, associated volumes and drives.
Follow this guide if you want to remove a drive from a RAID configuration.

View Logical Drives by Storage Pools
View Physical Drives by Storage Pools
Create Volume...
Edit Property...
Remove Volume
More Actions

	Name	RAID State	Capacity	details
○	⊟ ServeRAID M5110e(PCI Slot 0)			
	⊟ Storage Pool 0	RAID 5	134.109GB(62.012GB free)	4 Volume(s)
○	VD1	Optimal	12.000GB	Bootable, Strip Size 128KB
○	VD2	Optimal	20.000GB	Not Bootable, Strip Size 128KB
○	VD3	Optimal	40.000GB	Not Bootable, Strip Size 128KB
○	VD4	Optimal	0.098GB	Not Bootable, Strip Size 128KB
	⊟ Storage Pool 1	RAID 1	231.898GB(0.000GB free)	1 Volume(s)
○	vol	Optimal	231.898GB	Not Bootable, Strip Size 128KB

On the **View Logical Drives by Storage Pools** tab, the following sub-tabs are displayed:

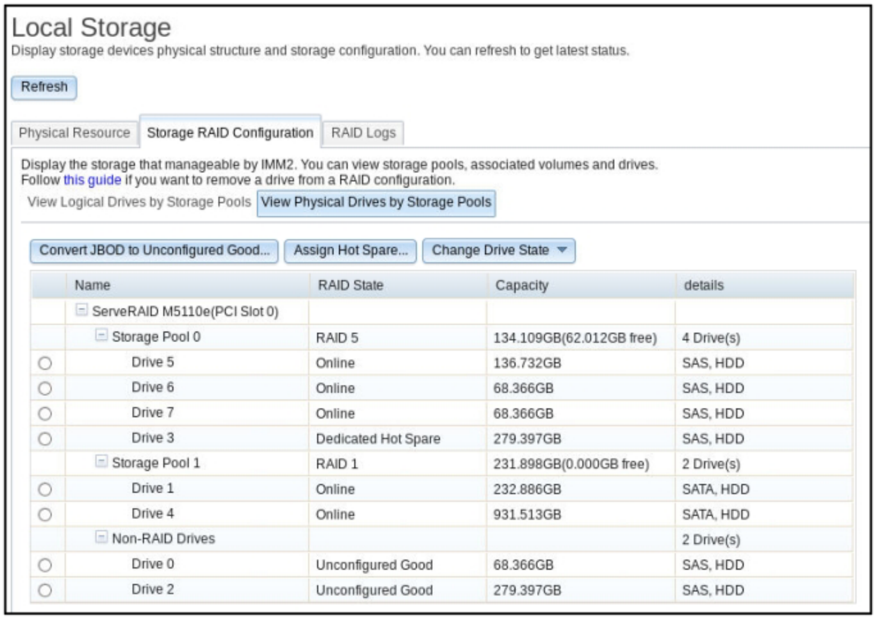
Create Volume
Select this tab to create one logical drive or multiple logical drives on one controller or on one existing storage pool.

Edit Property
Select this tab to edit the properties of the selected logical drive.

Remove Volume
Select this tab to delete the selected logical drive.

More Actions
Select this tab to detect, import, and clear the foreign or local configuration on the selected controller.

To view and configure (if supported by the platform), the physical drives and associated storage pools click the **View Physical drives by Storage Pools** tab (as shown in the following illustration). The capacity and RAID level of the storage pool are displayed. The RAID state of the drive, the number of drives in the storage pool, along with the interface and one drive type are also displayed.


Refresh
Physical Resource
Storage RAID Configuration
RAID Logs
View Logical Drives by Storage Pools
View Physical Drives by Storage Pools
Convert JBOD to Unconfigured Good...
Assign Hot Spare...
Change Drive State

Local Storage

Display storage devices physical structure and storage configuration. You can refresh to get latest status.

Display the storage that manageable by IMM2. You can view storage pools, associated volumes and drives.
Follow this guide if you want to remove a drive from a RAID configuration.

	Name	RAID State	Capacity	details
	⊟ ServeRAID M5110e(PCI Slot 0)			
	⊟ Storage Pool 0	RAID 5	134.109GB(62.012GB free)	4 Drive(s)
○	Drive 5	Online	136.732GB	SAS, HDD
○	Drive 6	Online	68.366GB	SAS, HDD
○	Drive 7	Online	68.366GB	SAS, HDD
○	Drive 3	Dedicated Hot Spare	279.397GB	SAS, HDD
	⊟ Storage Pool 1	RAID 1	231.898GB(0.000GB free)	2 Drive(s)
○	Drive 1	Online	232.886GB	SATA, HDD
○	Drive 4	Online	931.513GB	SATA, HDD
	⊟ Non-RAID Drives			2 Drive(s)
○	Drive 0	Unconfigured Good	68.366GB	SAS, HDD
○	Drive 2	Unconfigured Good	279.397GB	SAS, HDD

On the **View Physical drives by Storage Pools** tab, the following sub-tabs are displayed:

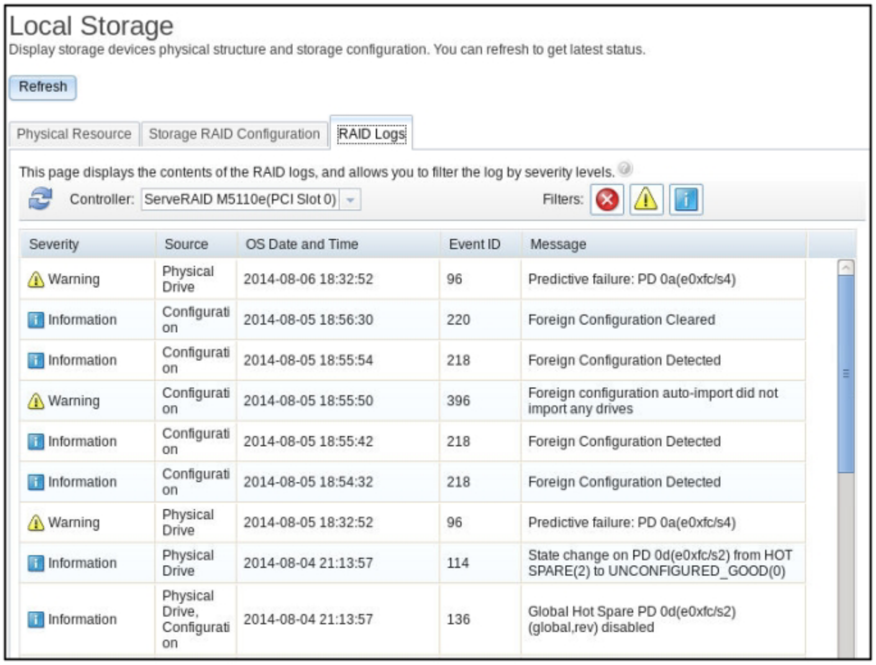
Convert JBOD to Unconfigured Good...
Select this tab to convert the just a bunch of disks (JBOD) drive to an unconfigured good state.

Assign Hot Spare
Select this tab to assign the selected drive as a global hot spare or to one or multiple storage pools as a dedicated hot spare.

Change Drive State
Select this tab to change the state of the selected drive to another state.

Displaying the RAID log information

On the Local Storage page click the **RAID Logs** tab to display the contents of the RAID logs. You can view the severity, source, operating system date and time, event identification, and message for the RAID logs as displayed in the following illustration. To obtain the latest status information click the **Refresh** button.



Local Storage

Display storage devices physical structure and storage configuration. You can refresh to get latest status.

This page displays the contents of the RAID logs, and allows you to filter the log by severity levels.

Controller: ServeRAID M5110e(PCI Slot 0)

Filters: ⊗ ⚠ ℹ

Severity	Source	OS Date and Time	Event ID	Message
⚠ Warning	Physical Drive	2014-08-06 18:32:52	96	Predictive failure: PD 0a(e0xfc/s4)
ℹ Information	Configuration	2014-08-05 18:56:30	220	Foreign Configuration Cleared
ℹ Information	Configuration	2014-08-05 18:55:54	218	Foreign Configuration Detected
⚠ Warning	Configuration	2014-08-05 18:55:50	396	Foreign configuration auto-import did not import any drives
ℹ Information	Configuration	2014-08-05 18:55:42	218	Foreign Configuration Detected
ℹ Information	Configuration	2014-08-05 18:54:32	218	Foreign Configuration Detected
⚠ Warning	Physical Drive	2014-08-05 18:32:52	96	Predictive failure: PD 0a(e0xfc/s4)
ℹ Information	Physical Drive	2014-08-04 21:13:57	114	State change on PD 0d(e0xfc/s2) from HOT SPARE(2) to UNCONFIGURED_GOOD(0)
ℹ Information	Physical Drive, Configuration	2014-08-04 21:13:57	136	Global Hot Spare PD 0d(e0xfc/s2) (global,rev) disabled

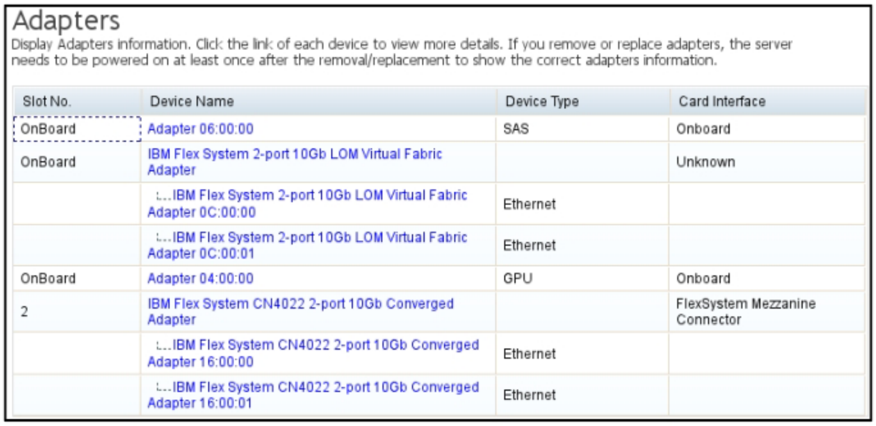
Viewing the adapter information and configuration settings

Click the **Adapters** option under the **Server Management** tab to view information about the PCIe adapters installed in the server.

Notes:

- If the server does support the **Adapters** option and you remove, replace, or configure any adapters, you must restart the server (at least once) to view the updated adapter information.
- If the server does not support the **Adapters** option, this option is not available on the **Server Management** tab.

Click an adapter or functional link on the Adapters page to view details about the component (as shown in the following illustration).

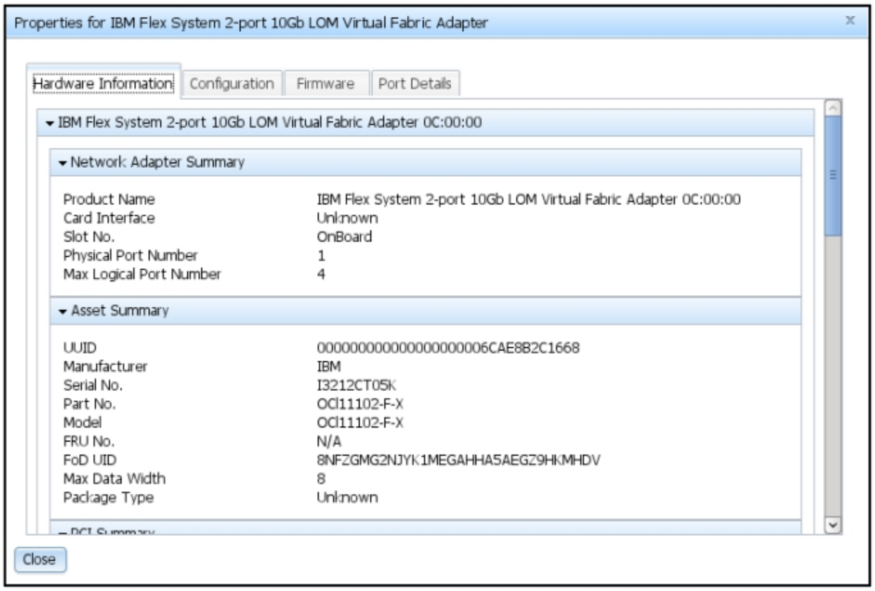


Adapters

Display Adapters information. Click the link of each device to view more details. If you remove or replace adapters, the server needs to be powered on at least once after the removal/replacement to show the correct adapters information.

Slot No.	Device Name	Device Type	Card Interface
OnBoard	Adapter 06:00:00	SAS	Onboard
OnBoard	IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter		Unknown
	└...IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00	Ethernet	
	└...IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:01	Ethernet	
OnBoard	Adapter 04:00:00	GPU	Onboard
2	IBM Flex System CN4022 2-port 10Gb Converged Adapter		FlexSystem Mezzanine Connector
	└...IBM Flex System CN4022 2-port 10Gb Converged Adapter 16:00:00	Ethernet	
	└...IBM Flex System CN4022 2-port 10Gb Converged Adapter 16:00:01	Ethernet	

From the Properties page the hardware, configuration, and firmware information, along with the port details for the component can be viewed (as shown in the following illustration).


Properties for IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter
Hardware Information
Configuration
Firmware
Port Details
Close

IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00

Network Adapter Summary

Product Name	IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00
Card Interface	Unknown
Slot No.	OnBoard
Physical Port Number	1
Max Logical Port Number	4

Asset Summary

UUID	000000000000000000006CAE8B2C1668
Manufacturer	IBM
Serial No.	I3212CT05K
Part No.	OCl11102-F-X
Model	OCl11102-F-X
FRU No.	N/A
FoD UID	8NFZGMG2NJYK1MEGAHHA5AEGZ9HKMHDV
Max Data Width	8
Package Type	Unknown

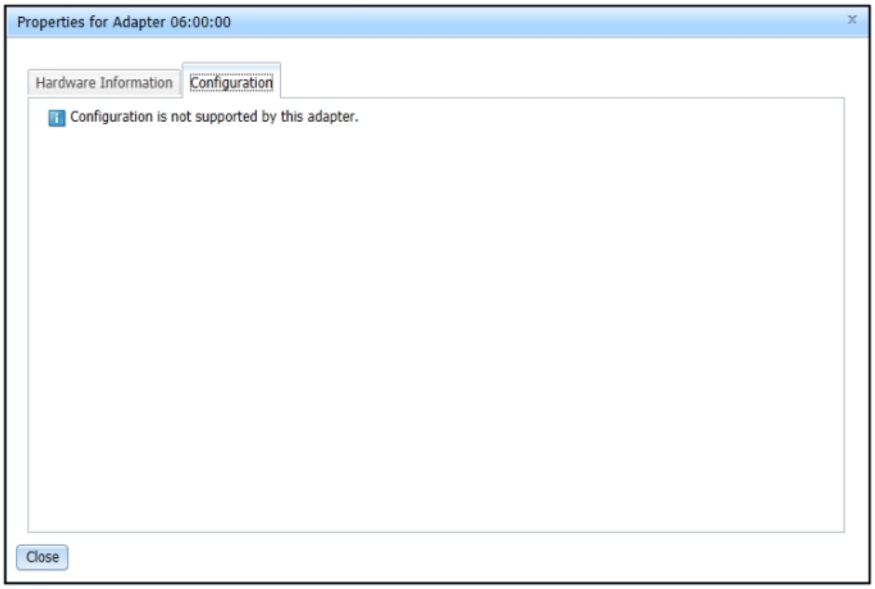
PCI Summary

For adapters using older firmware or for adapters that do not support out-of-band inventory, only part of the hardware information can be displayed. Firmware, port, and chipset information cannot be retrieved. Some information might display as `N/A` or `Unknown` if the information is not applicable to the adapter or if the adapter is supported by older hardware or a previous firmware version.

Configuring the adapter information

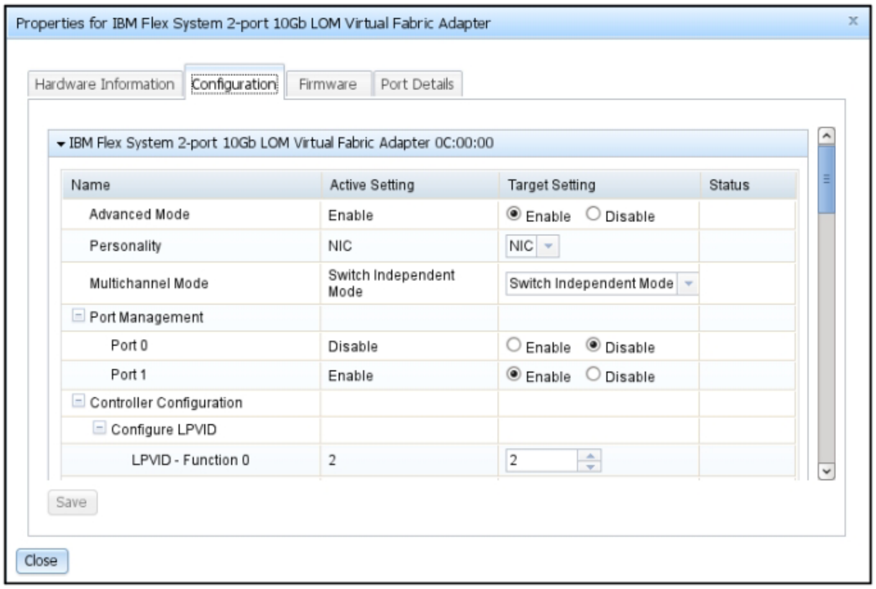
On the Properties for Adapter page click the **Configuration** tab to display and change the configuration information for the adapter.

Note: The **Configuration** tab is only visible when the user authority level is set to **Supervisor** or **Adapter Configuration - Advanced**.
If an adapter does not support the configuration functionality (for example, a SAS or graphic processing unit (GPU) adapter), the following window is displayed.



Configuration is not supported by this adapter.

If an adapter does support the configuration functionality, all changeable settings are listed, (as shown in the following illustration).



Properties for IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter

Hardware Information | Configuration | Firmware | Port Details

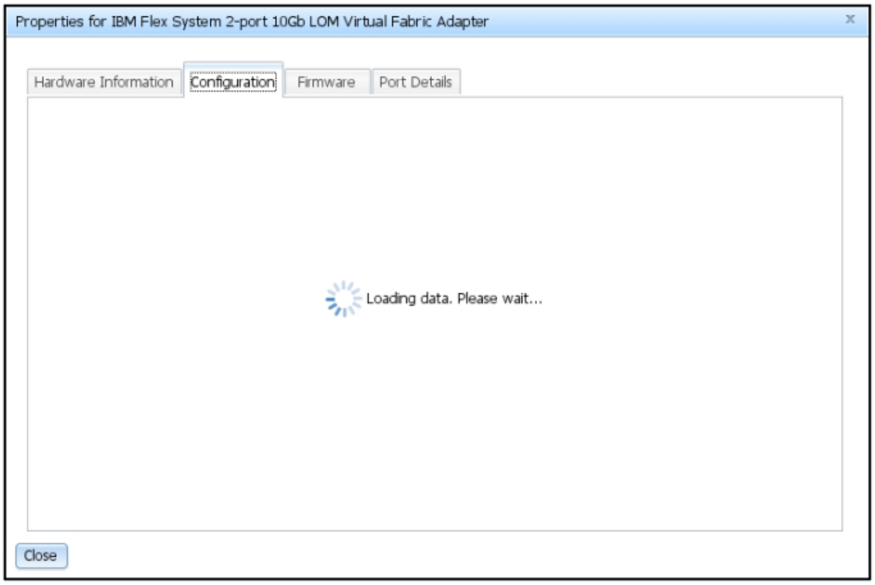
▾ IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00

Name	Active Setting	Target Setting	Status
Advanced Mode	Enable	● Enable ○ Disable	
Personality	NIC	NIC ▾	
Multichannel Mode	Switch Independent Mode	Switch Independent Mode ▾	
⊟ Port Management			
Port 0	Disable	○ Enable ● Disable	
Port 1	Enable	● Enable ○ Disable	
⊟ Controller Configuration			
⊟ Configure LPVID			
LPVID - Function 0	2	2	

Save

Close

It takes several moments for the IMM2 to load the adapter information into the window. When you click the **Configuration** tab and if the settings are not completely loaded, you will see the following message `Loading data, Please wait` (as shown in the following illustration).



Properties for IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter

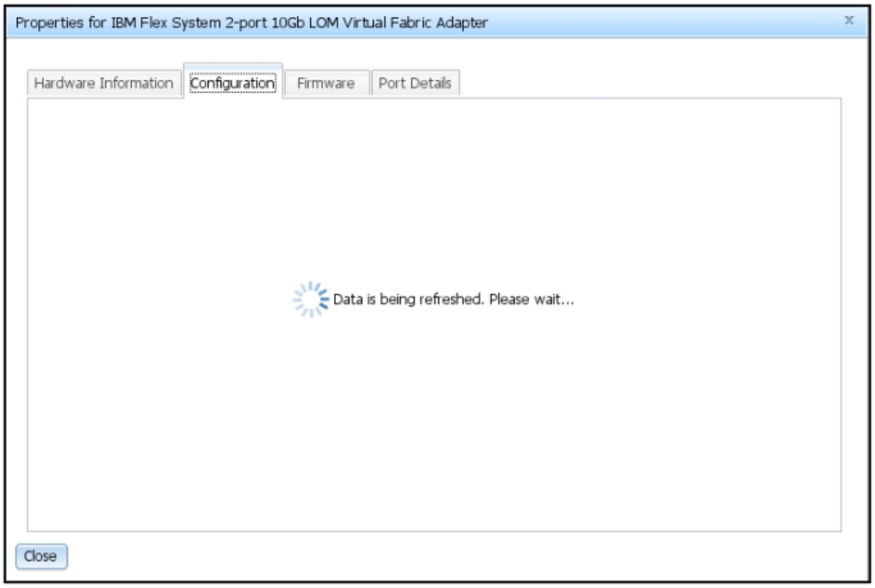
Hardware Information | Configuration | Firmware | Port Details

Loading data. Please wait...

Close

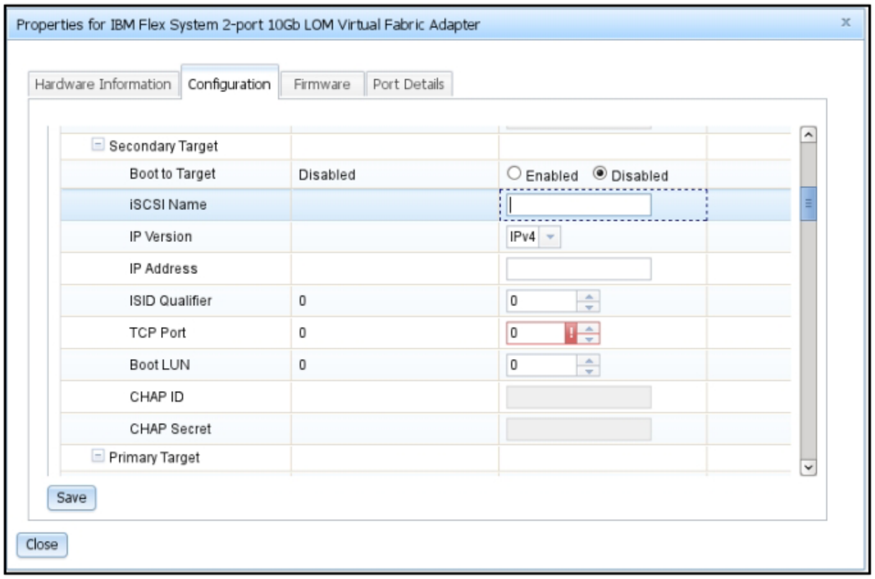
Note: Microsoft Internet Explorer 8 is not efficient in running certain JavaScript files. Using Microsoft Internet Explorer 8 may cause the IMM2 web interface to *automatically* navigate to the IMM2 login page, due to a timeout condition. To avoid this timeout condition and *automatic* navigation, it is recommended to upgrade Microsoft Internet Explorer to a newer version or to release server overloads.

It takes approximately one minute for the IMM2 to refresh the configuration data during a server restart. You might see the following message, `Data is being refreshed. Please wait` (as shown in the following illustration).


Properties for IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter

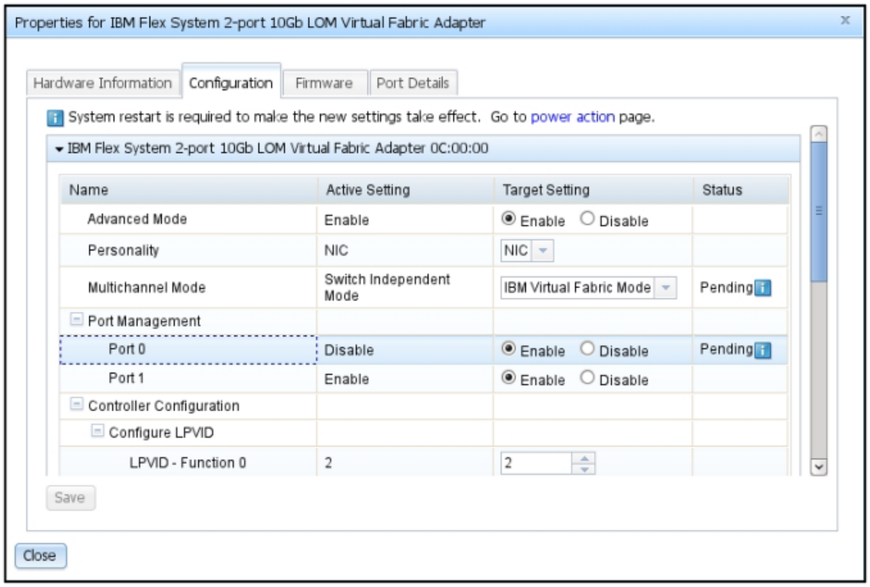
Data is being refreshed. Please wait...

After all of the adapter information is loaded into the window, you can change and save your settings. Some basic checking is performed by the IMM2 on changed values. For example, attempting to input text or adding a number that is out of range for a numeric field is not permitted. A warning symbol is displayed if the changed value is not a valid value (as shown in the following illustration). Invalid values cannot be saved.


Properties for IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter

⊟ Secondary Target		
Boot to Target	Disabled	○ Enabled ● Disabled
iSCSI Name		
IP Version		IPv4
IP Address		
ISID Qualifier	0	0
TCP Port	0	0 !
Boot LUN	0	0
CHAP ID		
CHAP Secret		
⊟ Primary Target		

After the **Save** button is clicked, all valid settings (settings without warning symbols) are saved. A restart of the server is required for the new values to become active (as shown in the following illustration).



Properties for IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter

System restart is required to make the new settings take effect. Go to power action page.

IBM Flex System 2-port 10Gb LOM Virtual Fabric Adapter 0C:00:00

Name	Active Setting	Target Setting	Status
Advanced Mode	Enable	● Enable ○ Disable	
Personality	NIC	NIC	
Multichannel Mode	Switch Independent Mode	IBM Virtual Fabric Mode	Pending
Port Management			
Port 0	Disable	● Enable ○ Disable	Pending
Port 1	Enable	● Enable ○ Disable	
Controller Configuration			
Configure LPVID			
LPVID - Function 0	2	2	

You should be familiar with adapter settings in the UEFI Setup before attempting to modify adapters using the IMM2 web interface. Unlike the UEFI, the IMM2 does *not* perform a comprehensive check for all settings. Some settings might be invalid with no warning indication displayed. After applying and saving a setting without error, performing a restart of the server; then, reopening the properties page you may notice the setting is not changed to the new value. Settings in this category can temporarily be saved; but, eventually will be discarded by the adapter.

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 Integrated Management Module Standard Upgrade is required prior to installing the Integrated Management Module Advanced Upgrade functionality.

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

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

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

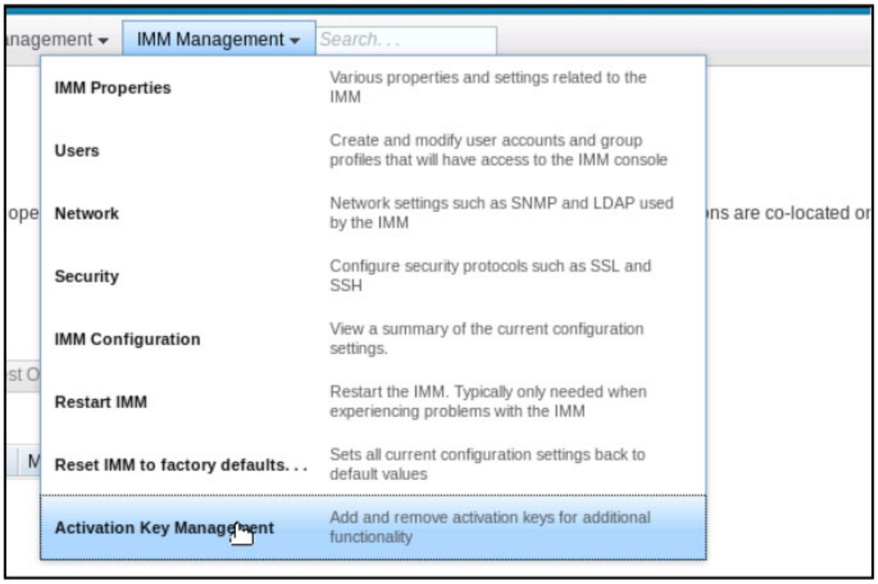
See “Installing an activation key,” “Removing an activation key” on page 189 or “Exporting an activation key” on page 191 for information about managing an FoD activation key using the IMM2 web interface. See “keycfg command” on page 225 for information about managing an FoD activation key using the 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**.



IMM Properties Various properties and settings related to the IMM

Users Create and modify user accounts and group profiles that will have access to the IMM console

Network Network settings such as SNMP and LDAP used by the IMM

Security Configure security protocols such as SSL and SSH

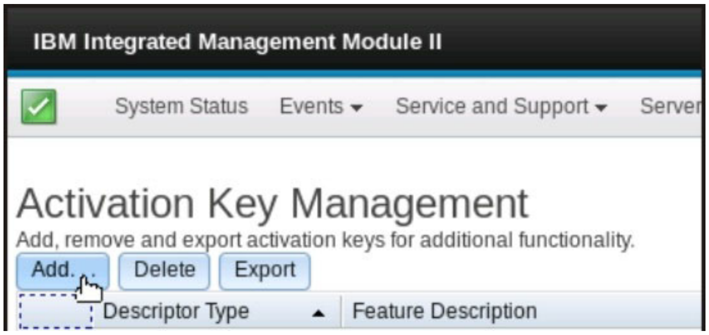
IMM Configuration View a summary of the current configuration settings.

Restart IMM Restart the IMM. Typically only needed when experiencing problems with the IMM

Reset IMM to factory defaults. . . Sets all current configuration settings back to default values

Activation Key Management Add and remove activation keys for additional functionality

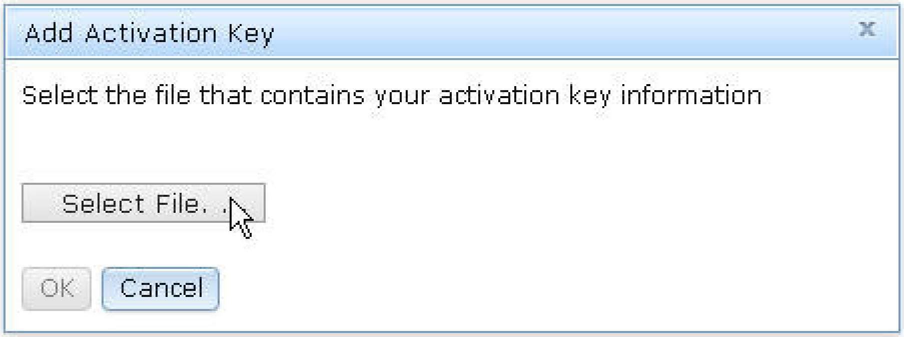
3. From the Activation Key Management page, click **Add...**.



Activation Key Management

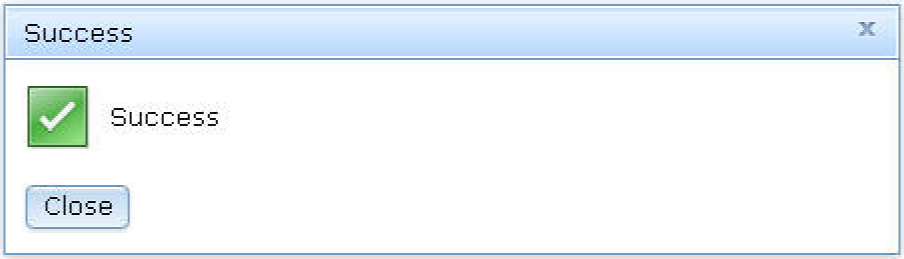
Add, remove and export activation keys for additional functionality.

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.



Select the file that contains your activation key information

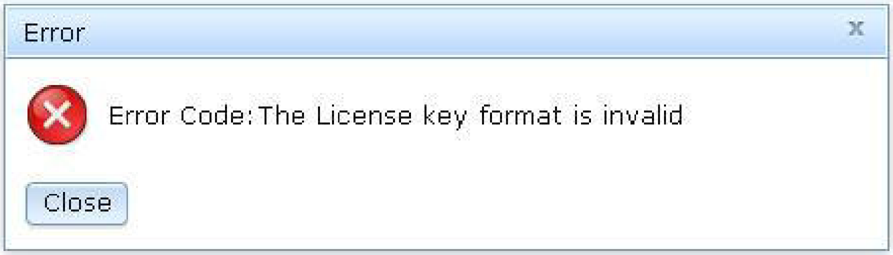
The Success window indicates that the activation key is installed.



Success

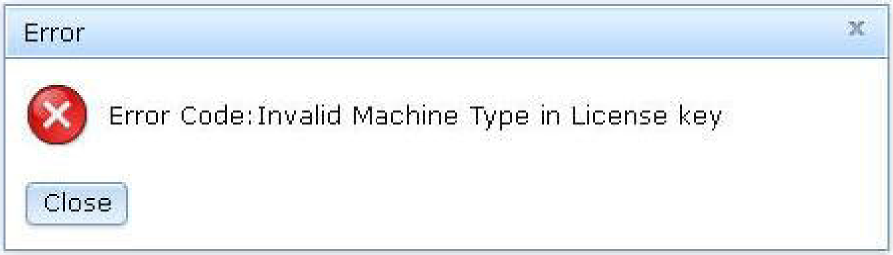
Note:

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



Error Code:The License key format is invalid

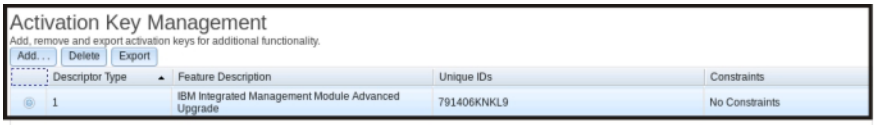
- If you are attempting to install the activation key on a machine type that does not support the FoD feature, you will see the following error window.



Error Code:Invalid Machine Type in License key

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.



Activation Key Management

Add, remove and export activation keys for additional functionality.

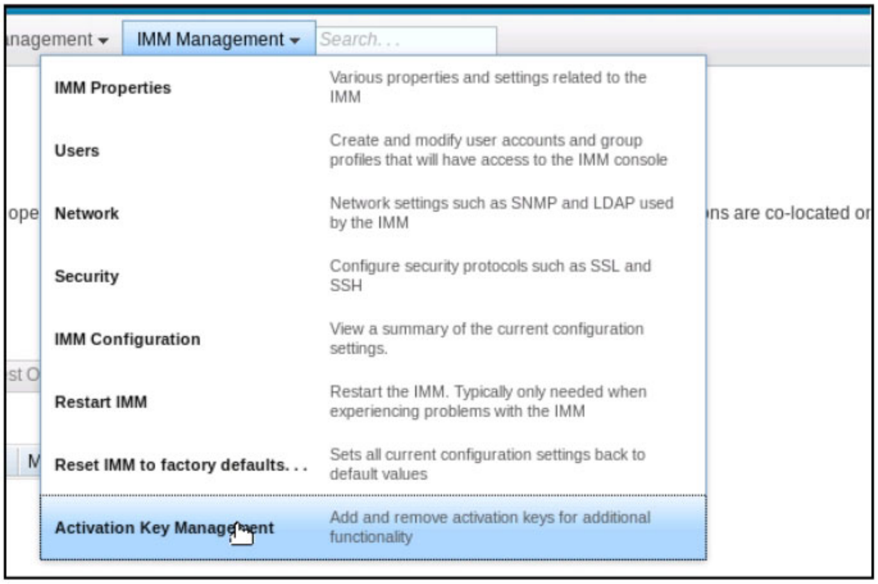
	Descriptor Type	Feature Description	Unique IDs	Constraints
○	1	IBM Integrated Management Module Advanced Upgrade	791406KNKL9	No Constraints

Removing an activation key

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

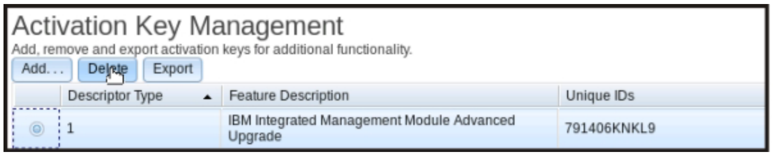
To remove a FoD activation key, complete the following steps:

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**.



IMM Properties	Various properties and settings related to the IMM
Users	Create and modify user accounts and group profiles that will have access to the IMM console
Network	Network settings such as SNMP and LDAP used by the IMM
Security	Configure security protocols such as SSL and SSH
IMM Configuration	View a summary of the current configuration settings.
Restart IMM	Restart the IMM. Typically only needed when experiencing problems with the IMM
Reset IMM to factory defaults. . .	Sets all current configuration settings back to default values
Activation Key Management	Add and remove activation keys for additional functionality

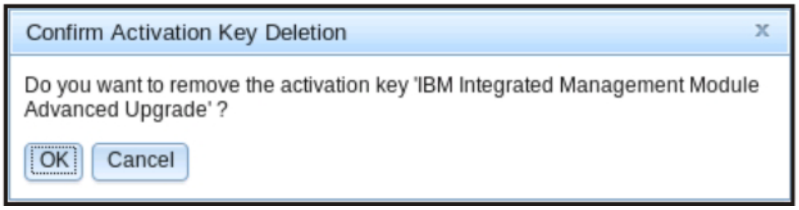
3. From the Activation Key Management page, select the activation key to remove; then, click **Delete**.


Activation Key Management

Add, remove and export activation keys for additional functionality.

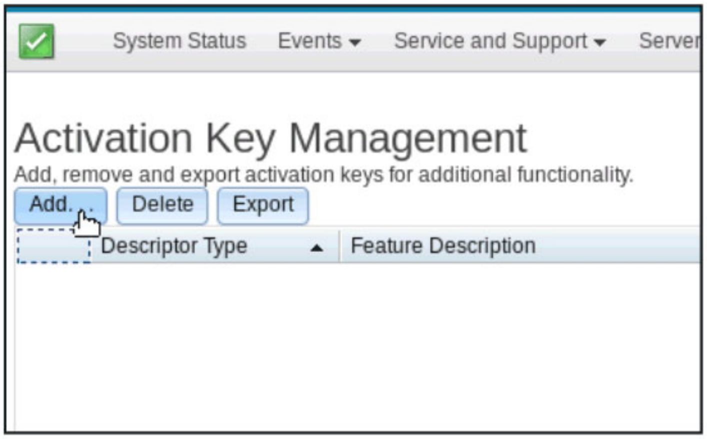
	Descriptor Type ▲	Feature Description	Unique IDs
○	1	IBM Integrated Management Module Advanced Upgrade	791406KNKL9

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


Confirm Activation Key Deletion

Do you want to remove the activation key 'IBM Integrated Management Module Advanced Upgrade' ?

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



Activation Key Management

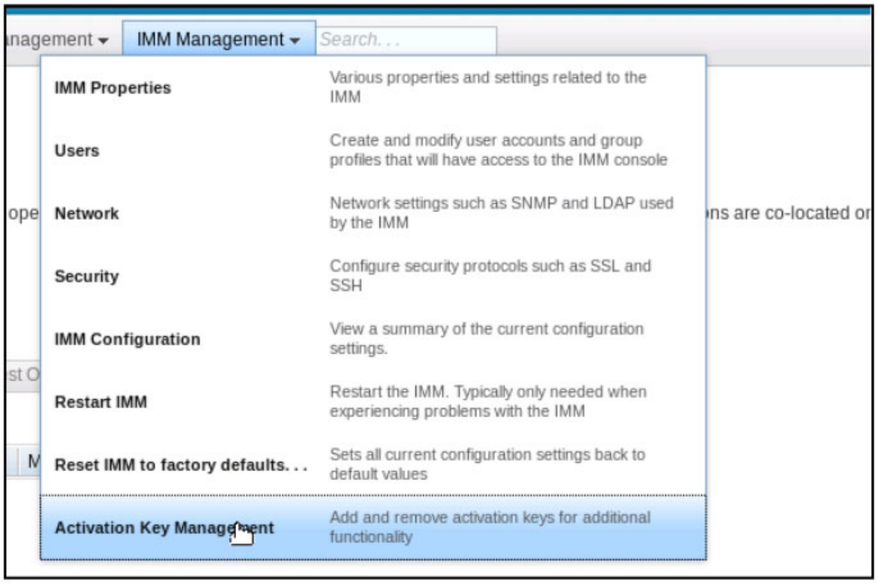
Add, remove and export activation keys for additional functionality.

Exporting an activation key

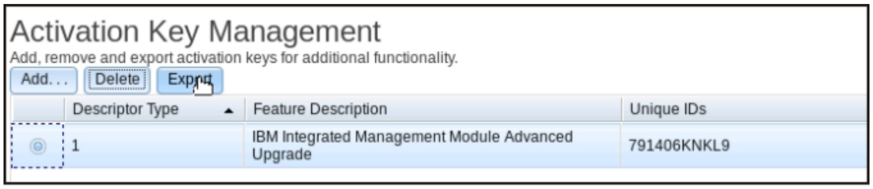
Export a FoD activation key to export an optional feature from your server.

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**.


nagement
IMM Management
Search. . .
IMM Properties
Various properties and settings related to the IMM
Users
Create and modify user accounts and group profiles that will have access to the IMM console
Network
Network settings such as SNMP and LDAP used by the IMM
Security
Configure security protocols such as SSL and SSH
IMM Configuration
View a summary of the current configuration settings.
Restart IMM
Restart the IMM. Typically only needed when experiencing problems with the IMM
Reset IMM to factory defaults. . .
Sets all current configuration settings back to default values
Activation Key Management
Add and remove activation keys for additional functionality
ope
ns are co-located or
st O
M

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

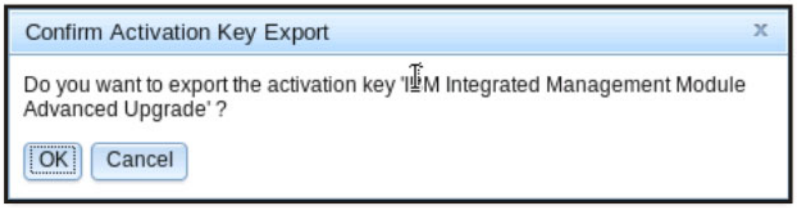


Activation Key Management

Add, remove and export activation keys for additional functionality.

	Descriptor Type	Feature Description	Unique IDs
◉	1	IBM Integrated Management Module Advanced Upgrade	791406KNKL9

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



Confirm Activation Key Export

Do you want to export the activation key 'IBM Integrated Management Module Advanced Upgrade' ?

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 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 a Flex System, a user can configure a Flex System 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 the IPMI until the CMM has configured the IPMI User IDs.

Note: The User ID credentials configured by the CMM might be different than the USERID/PASSW0RD combination described above. If no IPMI User IDs have been configured by the CMM, the network port associated with the IPMI protocol will be closed.

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 the 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 the IPMItool, see "Using IPMItool."

Using IPMItool

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

For more information about the IPMItool, or to download the 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" 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 a 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:

- "accseccfg command" on page 211
- "alertcfg command" on page 213
- "alertentries command" on page 283
- "asu command" on page 214
- "autoftp command" on page 288
- "autopromo command" on page 216
- "backup command" on page 217
- "batch command" on page 285
- "chconfig command" on page 289
- "chlog command" on page 290
- "chmanual command" on page 291
- "clearcfg command" on page 286
- "clearlog command" on page 200
- "clock command" on page 286
- "console command" on page 210
- "cryptomode command" on page 218
- "dhcpinfo command" on page 219
- "dns command" on page 220
- "ethtousb command" on page 221
- "events command" on page 291
- "exit command" on page 198
- "fans command" on page 200
- "ffdc command" on page 201

- “fuelg command” on page 206
- “gprofile command” on page 222
- “help command” on page 198
- “history command” on page 198
- “identify command” on page 287
- “ifconfig command” on page 223
- “info command” on page 287
- “keycfg command” on page 225
- “ldap command” on page 226
- “led command” on page 202
- “ntp command” on page 228
- “passwordcfg command” on page 229
- “ports command” on page 229
- “portcfg command” on page 230
- “portcontrol command” on page 231
- “power command” on page 207
- “pxeboot command” on page 209
- “readlog command” on page 203
- “reset command” on page 210
- “resetsp command” on page 288
- “restore command” on page 232
- “restoredefaults command” on page 233
- “scale command” on page 233
- “sdemail command” on page 292
- “sdraid command” on page 242
- “set command” on page 254
- “smtp command” on page 254
- “snmp command” on page 255
- “snmpalerts command” on page 257
- “spreset command” on page 288
- “srcfg command” on page 258
- “sshcfg command” on page 259
- “ssl command” on page 259
- “sslcfg command” on page 260
- “storage command” on page 264
- “storekeycfg command” on page 274
- “syshealth command” on page 204
- “telnetcfg command” on page 276
- “temps command” on page 205
- “thermal command” on page 277
- “timeouts command” on page 277
- “tls command” on page 276
- “usbeth command” on page 278
- “users command” on page 278
- “volts command” on page 205

- “vpd command” on page 206

Utility commands

The utility commands are as follows:

- “exit command”
- “help command”
- “history command”

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” on page 200
- “fans command” on page 200
- “ffdc command” on page 201
- “led command” on page 202
- “readlog command” on page 203
- “storage command” on page 264
- “syshealth command” on page 204
- “temps command” on page 205
- “volts command” on page 205

- “vpd command” on page 206

adapter command

Use the **adapter** command to display PCIe adapter inventory information. PCIe adapters managed by the IMM2 include: Ethernet, Fibre Channel, InfiniBand, and graphic processing units (GPU).

The following table shows the arguments for the options.

Option	Description	Values
-list	List all PCIe adapters in the server	
-show *target_id*	Show the detailed information for the target PCIe adapter	*target_id* *[info|firmware|ports|chips]* Where: • *info*: display the hardware information for the adapter • *firmware*: display all firmware information for the adapter • *ports*: display all Ethernet port information for the adapter • *chips*: display all GPU chip information for the adapter
-h	Display the command usage and options	

Syntax:

```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

Examples:

```
system> adapter
–list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
```

```
system> adapter
–show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
```

```
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

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 first failure data capture (**ffdc**) command to generate and transfer service data to 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 argument 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 or active events of the server. The power state, system state, restart count, and IMM2 software status are displayed.

Syntax:

```
syshealth [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
```

Example:

```
system> syshealth summary
Power    On
State    OS booted
```

```
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

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 [argument]
argument:
sys
imm
uefi
dsa
fw
comp
```

Example:

```
system> vpd dsa
Type     Status      Version      Build     ReleaseDate
----     -------      -----     ------
DSA      Active      9.36         DSYTAE2   2013/01/18
system>
```

Server power and restart control commands

The server power and restart commands are as follows:

- "fuelg command"
- "power command" on page 207
- "pxeboot command" on page 209
- "reset command" on page 210

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
-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

Option	Description	Values
The following option might not be available on all systems:		
-perf	Display the current compute utilization, including system, microprocessor, and I/O.	percentage
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.

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

Command	Description	Value
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 rp	Use this option to specify the host power restore policy.	alwayson|alwaysoff|restore
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.	
-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
-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

Option	Description	Values
-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:

```
system> 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:

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

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

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

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

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

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

```
system> 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 following table shows the arguments for the options.

Option	Description	Values
-s	Shut down the operating system before the server is reset.	
-d	Delay performing the reset for the given number of seconds.	0 - 120
-nmi	Generate a non-maskable interrupt (NMI)) on the server.	

Syntax:

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

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.

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*
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*

Command	Description	Value
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.	
--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.

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.
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[1]
-esnmpv3	Allow or disallow SNMPv3 accounts to operate in a non-compliant manner with the NIST compliance mode	enable, disable
-h	List the usage and options	
1. If the compliance mode is set to NIST the TLS level must be set to 1.2.		

Syntax:

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

Examples:

To set the cryptomode to basic, type the following command:

```
system> cryptomode
-set basic
ok
system> cryptomode
Mode                Exceptions
Basic Compatibility
system>
```

To set the cryptomode to NIST Strict, type following command:

```
system> cryptomode
-set NIST
ok
```

```
system> cryptomode
Mode                Exceptions
NIST SP 800-131A
system>
```

To set the cryptomode to NIST Strict and allow SNMP in the compatible mode, type following command:

```
system> cryptomode
-set NIST -esnmpv3 enabled
ok
system> cryptomode
Mode                Exceptions
NIST SP 800-131A    allow SNMPv3 accounts
system>
```

If there are certificates or key strengths that are not compatible with the NIST mode; the command fails and an error message is generated. The compliance mode is not changed See the following example:

```
system> cryptomode
-set NIST
LDAP Server 1 certificate invalid
fail
system>
```

dhcpinfo command

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

Syntax:

```
dhcpinfo eth0
```

Example:

```
system> dhcpinfo eth0

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

The following table describes the output from the example.

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

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

dns command

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

Note: In a 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
-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	Delete 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	Display 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.

Note: In a Flex System, the VLAN settings are managed by a Flex System CMM and cannot be modified on the IMM2.

The following table shows the arguments for the options.

Option	Description	Values
-b	Burned-in MAC Address (read-only and not configurable)	
-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

Option	Description	Values
-nic	NIC access. This option determines which network port will be used by the IMM2.	shared, dedicated, shared_option_1[1]
-failover[2]	Failover mode	none, shared, shared_option_1
-nssync[3]	Network setting synchronization	enabled, disabled
-address_table	Table of automatically-generated IPv6 addresses and their prefix lengths **Note:** The option is visible only if IPv6 and stateless auto-configuration are enabled.	This value is read-only and is not configurable.
-ipv6	IPv6 state	disabled, enabled
-lla	Link-local address **Note:** The link-local address only appears if IPv6 is enabled.	The link-local address is determined by the IMM2. This value is read-only and is not configurable.
-ipv6static	Static IPv6 state	disabled, enabled
-i6	Static IP address	Static IP address for Ethernet channel 0 in IPv6 format.
-p6	Address prefix length	Numeric 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.

Notes:
1. The shared_option_1 value is available on servers that have an optional mezzanine network card installed. This mezzanine network card can be used by the IMM2.
2. If the IMM2 is configured to use the dedicated management network port, the -failover option will direct the IMM2 to switch to the shared network port if the dedicated port is disconnected.
3. If the failover mode is enabled, the -nssync option directs the IMM2 to use the same network settings that are used on the dedicated management network port for the shared network port.

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
  -b burned_in_MAC_address
  -dn domain_name
  -auto state
  -nic state
  -failover mode
  -nssync state
  -address_table
  -lla ipv6_link_local_addr
  -dhcp6 state
  -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>
```

keycfg command

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

- When the **keycfg** command 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

Option	Description	Values
-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"
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM System x TKLM
                                                    Activation for Secure
                                                    Drive Encryption"
system>
```

Note: The **Description** field for ID number 3 is displayed on separate lines due to space limitations.

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

Option	Description	Values
-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.
-ep	Encrypted password	Backup/restore password (internal use only)
-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*
-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

Option	Description	Values
-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
   -ep encrypted_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...
```

scale command

Use the **scale** command to set and display the partition control and configuration settings for multiple nodes (servers) in a scalable complex.

- Entering the **scale** command with no options displays all scalable information of the complex that the node belongs to.
- All nodes in a scalable complex must use the same firmware version.

The following information shows the arguments for the options.

Option	Description
-auto	Automatically create a partition spanning across all nodes of the scalable complex.
-auto *Node_Key*	Create a partition spanning across all nodes of the scalable complex. If the current system supports selection of a primary node; then, the node with the specified Node Key is chosen as the primary node of the partition being created. The Node Key is a unique identifier for the node.
-create *<Node1_Key> <Node2_Key>*$_1$	Create a partition spanning across only the specified nodes of the scalable complex. If the current system supports selection of a primary node; then, the node with the first Node Key in this list is chosen as the primary node of the partition being created. The Node Key list is a space separated list of all the node keys for the nodes in the partition.

Option	Description
-create *_with_physical_node_id <PhysNodeId1> <PhysNodeId2>*[1]	Create a partition spanning across only the specified nodes of the scalable complex. If the current system supports selection of a primary node; then, the node with the first Physical Node Id in the list is chosen as the primary node of the partition being created. The Physical Node Id list is a space-separated list of all the physical node IDs for the nodes in the partition.
-delete *-partid <id>|-node <Node_Key>*[1]	Delete a specific partition in the scalable complex. **Note:** The partition must be powered off to delete it. Delete a partition by providing one of the following identifiers: • The partition ID of a partition in the scalable complex. • The node key of a node in the partition in the scalable complex.
-delete	Delete all partitions in the scalable complex. **Note:** The partitions must be powered off to delete them.
-mode *[stand-alone|partition] [-partid <id>|-node <Node_Key>]*[1]	Set the mode for a specific partition in the scalable complex to stand-alone or partition. When you select the stand-alone mode, the nodes in the partition boot individually. When you select the partition mode, all nodes in the partition boot together. To set the partition mode, you can provide one of the following identifiers: • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex.
-start *-partid <id>|-node <Node_Key>*[1]	Power on a node or all of the nodes in a partition in the scalable complex. To power on the nodes in a partition, you can provide one of the following identifiers: • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. When the partition ID is provided as an argument and the nodes in the partition are in the partition mode, this option powers on all nodes within the partition. When a node key is provided as an argument and the node is in the partition mode, this option powers on all nodes within the partition to which the node key belongs. When a node key is provided as an argument and the node is in the stand-alone mode, this option powers on only the node to which the node key belongs.

Option	Description
-reset *-partid <id>* | *-node <Node_Key>*[1]	Hard reset a node or all of the nodes in a partition in the scalable complex. To hard reset the nodes in a partition, you can provide one of the following identifiers: • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. When the partition ID is provided as an argument and the nodes in the partition are in the partition mode, this option will hard reset all nodes within the partition. When a node key is provided as an argument and the node is in the partition mode, this option will hard reset all nodes within the partition to which the node key belongs. When a node key is provided as an argument and the node is in the stand-alone mode, this option will hard reset only the node to which the node key belongs.
-stop *-partid <id>* | *-node <Node_Key>*[1]	Power off a node or all of the nodes in a partition in the scalable complex. To power off the nodes in a partition, you can provide one of the following identifiers: • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. When the partition ID is provided as an argument and the nodes in the partition are in the partition mode, this option powers off all nodes within the partition. When a node key is provided as an argument and the node is in the partition mode, this option powers off all nodes within the partition to which the node key belongs. When a node key is provided as an argument and the node is in the stand-alone mode, this option powers off only the node to which the node key belongs.

Option	Description
-poweron *-partid <id>* | *-node <Node_Key>*[1]	Powers on a node or all of the nodes in a partition in the scalable complex. To power on the nodes in a partition, you can provide one of the following identifiers: • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. When the partition ID is provided as an argument and the nodes in the partition are in the partition mode, this option powers on all nodes within the partition. When a node key is provided as an argument and the node is in the partition mode, this option powers on all nodes within the partition to which the node key belongs. When a node key is provided as an argument and the node is in the stand-alone mode, this option powers on only the node to which the node key belongs.
-poweroff *-partid <id>* | *-node <Node_Key>*[1]	Power off a node or all of the nodes in a partition in the scalable complex. To power-off the nodes in a partition, you can provide one of the following identifiers: • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. When the partition ID is provided as an argument and the nodes in the partition are in the partition mode, this option powers off all nodes within the partition. When a node key is provided as an argument and the node is in the partition mode, this option powers off all nodes within the partition to which the node key belongs. When a node key is provided as an argument and the node is in the stand-alone mode, this option powers off only the node to which the node key belongs.

Option	Description
-powercycle *-partid <id>*|*-node <Node_Key>*[1]	Power cycle a node or all of the nodes in a partition in the scalable complex. To power cycle the nodes in a partition, you can provide one of the following identifiers: • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. When the partition ID is provided as an argument and the nodes in the partition are in the partition mode, this option will power cycle all nodes within the partition. When a node key is provided as an argument and the node is in the partition mode, this option will power cycle all nodes within the partition to which the node key belongs. When a node key is provided as an argument and the node is in the stand-alone mode, this option will power cycle only the node to which the node key belongs.
-partid *id*	This option is used to display information about the partition in the scalable complex.
-node *Node_Key*	This option is used to display information about a node in the scalable complex.
-smp	This option is used to display scalability hardware information.
-h or -help	This option is used to display usage information about the scale command.
Note: 1. Option is displayed on multiple lines due to space limitations.	

Syntax:

```
scale
```

Example:

```
system> scale
SMP Hardware =2-node SMP

Complex Signature       =COMD
Complex ID              =0x4062
Complex Partition Count =1
Complex Node Count      =2
    Node[0] UUID =575D2D11717411E382996CAE8B7037F0
    Node[0] Serial Number =23ZBVC8
    Node[0] Node Key =0x6F00
    Node[0] Machine Type & Model =7903AC1
    Node[0] Slot ID =3-4
    Node[0] Logical ID =0x00
    Node[0] Partition ID =0x01
    Node[0] Partition Node Count =0x02
    Node[0] Partition Flags =0x1F
    Node[0] String ID =23ZBVC8[3-4]
    Node[0] Port[0] Remote Node Key =0x3F01
    Node[0] Port[0] Remote Port Number =0x00
    Node[0] Port[0] Status =Enabled
    Node[0] Port[0] Type =QPI
    Node[0] Port[1] Remote Node Key =0xFFFF
    Node[0] Port[1] Remote Port Number =0xFF
    Node[0] Port[1] Status =Disabled
    Node[0] Port[1] Type =QPI
    Node[0] Port[2] Remote Node Key =0xFFFF
    Node[0] Port[2] Remote Port Number =0xFF
    Node[0] Port[2] Status =Disabled
    Node[0] Port[2] Type =QPI
    Node[1] UUID =DEDB90B5722111E3BADB6CAE8B703620
    Node[1] Serial Number =23ZBVF0
    Node[1] Node Key =0x3F01
    Node[1] Machine Type & Model =7903AC1
    Node[1] Slot ID =5-6
    Node[1] Logical ID =0x01
    Node[1] Partition ID =0x01
    Node[1] Partition Node Count =0x02
    Node[1] Partition Flags =0x1F
    Node[1] String ID =23ZBVF0[5-6]
    Node[1] Port[0] Remote Node Key =0x6F00
    Node[1] Port[0] Remote Port Number =0x00
    Node[1] Port[0] Status =Enabled
    Node[1] Port[0] Type =QPI
    Node[1] Port[1] Remote Node Key =0xFFFF
    Node[1] Port[1] Remote Port Number =0xFF
    Node[1] Port[1] Status =Disabled
    Node[1] Port[1] Type =QPI
    Node[1] Port[2] Remote Node Key =0xFFFF
    Node[1] Port[2] Remote Port Number =0xFF
    Node[1] Port[2] Status =Disabled
    Node[1] Port[2] Type =QPI
system>
```

Syntax:

```
scale [options]
options:
  -auto node_key
```

Example:

```
system> scale
–auto 0x2f00
system>
```

```
system> scale
–auto
system>
```

Syntax:

```
scale [options]
options:
  -create node1_key node2_key
```

Example:

```
system> scale
–create 0x2f00 0x8f01
system>
```

Syntax:

```
scale [options]
options:
  -create _with_physical_node_id
```

Example:

```
system> scale
-create_with_physical_node_id <PhysNodeId1 PhysNodeId2>
system>
```

Syntax:

```
scale [options]
options:
  -delete
```

Examples:

```
system> scale
–delete –node 0x2f00
system>
```

```
system> scale
–delete –partid 1
system>
```

Syntax:

```
scale [options]
options:
  -mode
```

Examples:

```
system> scale
–mode standalone –partid 1
system>
```

```
system> scale
–mode partition –partid 1
system>
```

```
system> scale
–mode standalone –node 0x2f00
system>
```

```
system> scale
–mode partition –node 0x2f00
system>
```

Syntax:

```
scale [options]
option:
  -start
```

Examples:

```
system> scale
–start –partid 1
system>
```

```
system> scale
–start –node 0x2f00
system>
```

Syntax:

```
scale [options]
option:
  -reset
```

Examples:

```
system> scale
–reset –partid 1
system>
```

```
system> scale
–reset –node 0x2f00
system>
```

Syntax:

```
scale [options]
option:
  -stop
```

Examples:

```
system> scale
–stop –partid 1
system>
```

```
system> scale
–stop –node 0x2f00
system>
```

Syntax:

```
scale [options]
option:
  -poweron
```

Examples:

```
system> scale
–poweron –partid 1
system>
```

```
system> scale
–poweron –node 0x2f00
system>
```

Syntax:

```
scale [options]
option:
  -poweroff
```

Examples:

```
system> scale
–poweroff –partid 1
system>
```

```
system> scale
–poweroff –node 0x2f00
system>
```

Syntax:

```
scale [options]
option:
  -powercycle
```

Examples:

```
system> scale
–powercycle –partid 1
system>
```

```
system> scale
–powercycle –node 0x2f00
system>
```

Syntax:

```
scale [options]
option:
  -partid
```

Example:

```
system> scale
-partid 1
Partition Id 1
    Node count = 2
    Complex id = 0x3360

    Node Logical id =0x00
      Node UUID = BA DF CC 0C DC A7 4E D6 96 44 D9 24 49 10 29 C3
      Node serial number = BOGUS04
      Node key =0x2F00
      Node machine type = 7903AC1
      Node partition id =0x01
      Node partition count =0x02
      Node partition flags =0x1F
      Node string id = []
         Node port[0] remote node key =0x0001
         Node port[0] remote node number =0x00
         Node port[0] port status =0x01
         Node port[0] port type =0x00
         Node port[1] remote node key =0x00FF
         Node port[1] remote node number =0xFF
         Node port[1] port status =0x00
         Node port[1] port type =0x00
         Node port[2] remote node key =0x00FF
         Node port[2] remote node number =0xFF
         Node port[2] port status =0x00
         Node port[2] port type =0x00

    Node Logical id =0x01
      Node UUID = BA D4 FF 2D F7 49 45 36 A9 E5 4E 77 6C 41 8B A0
      Node serial number = BOGUS05
      Node key =0x8F01
      Node machine type = 7903AC1
      Node partition id =0x01
      Node partition count =0x02
      Node partition flags =0x1F
      Node string id = []
        Node port[0] remote node key =0x0000
        Node port[0] remote node number =0x00
        Node port[0] port status =0x01
        Node port[0] port type =0x00
        Node port[1] remote node key =0x00FF
        Node port[1] remote node number =0xFF
        Node port[1] port status =0x00
        Node port[1] port type =0x00
        Node port[2] remote node key =0x00FF
        Node port[2] remote node number =0xFF
        Node port[2] port status =0x00
        Node port[2] port type =0x00
system>
```

Syntax:

```
scale [options]
option:
  -node
```

Example:

```
system> scale
-node 0x2f00
Node Logical id =0x00
        Node UUID = BA DF CC 0C DC A7 4E D6 96 44 D9 24 49 10 29 C3
        Node serial number = BOGUS04
        Node key =0x2F00
        Node machine type = 7903AC1
        Node partition id =0x01
        Node partition count =0x02
        Node partition flags =0x1F
        Node string id = []
            Node port[0] remote node key =0x0001
            Node port[0] remote node number =0x00
            Node port[0] port status =0x01
            Node port[0] port type =0x00
            Node port[1] remote node key =0x00FF
            Node port[1] remote node number =0xFF
            Node port[1] port status =0x00
            Node port[1] port type =0x00
            Node port[2] remote node key =0x00FF
            Node port[2] remote node number =0xFF
            Node port[2] port status =0x00
            Node port[2] port type =0x00
system>
```

Syntax:

```
scale [options]
option:
  -smp
```

Example:

```
system> scale
–smp –partid 1
SMP Hardware =2-node SMP
system>
```

Syntax:

```
scale [options]
option:
  -help
```

Examples:

```
system> scale
–h
system>
```

```
system> scale
–help
system>
```

sdraid command

Use the **sdraid** command to configure and control the optional SD Media RAID Adapter for System x. The SD Media Adapter consist of dual secure digital (SD) card slots that can support up to two removable SD cards. The SD Media Adapter also features a RAID controller capable of supporting RAID level 1.

Important:

For IMM firmware levels less than TCOO08F:

- Use of the -driveLun *0* option where *immOnly* drives exist might result in undesirable consequences and should not be used. If *immOnly* drives exist use the -driveName option in place of the -driveLun option.
- The IMM CLI displays a logical unit number value of *0* for all *immOnly* drives.
- The -driveLun option can safely be used for logical unit number values that are greater than or equal to *1*.

For IMM firmware levels TCOO08F or higher:

- The -driveLun option can safely be used for all displayed numerical logical unit number values.
- The IMM displays a value of `NA` for the logical unit number of *immOnly* drives.
- *immOnly* drives should be targeted by the -driveName option.

The following table shows the arguments for the options.

Option	Description	Values
-version	This option is used to display the firmware version installed in the adapter.	
-reset	This option is used to reset the adapter.	
-getMode	This option is used to check the current mode of operation of the adapter firmware. This option also displays the state of the related RAID services.	
-setMode	This option is used to configure the mode of operation of the adapter firmware. This option also displays the state of the related RAID services.	Operational, Configuration
-initializeConfig	This option is used to clear the existing configuration of the SD card and re-initialize the SD card's configuration to the default value.	
-migrateConfig	This option is used to specify the source SD card that maintains the metadata information (global configuration). This option is also used to set the RAID configuration information.	1, 2
-SDCard	This option is used to display the properties of an installed SD card.	1, 2
-getFreeSpaceInfo	This option is used to display the free space information in the SD cards.	
-driveLun	This option is used to display the summary information of a drive configured on the adapter.	0 - 15
-driveName	This option is used to display the summary information of a drive configured on the adapter.	Null-terminated name string (maximum of 15 characters).
-driveList	This option is used to display the summary information of all drives configured on the adapter.	
-create	This option is used to create a new drive.	

Option	Description	Values
-delete	This option is used to delete an existing drive. This option can be used with parameters -driveLun or -driveName.	
-modify	This option is used to modify the properties of an existing drive.	
-getOwner	This option is used to get information about the current ownership of a specific drive. This option can be used with parameters -driveLun and -driveName.	
-setOwner	This option is used to set the current ownership of the drive to the IMM2 or the server. This option can be used with parameters -driveLun or -driveName.	
-help	This option is used to display command usage and option information.	

Syntax:

```
sdraid [options]
options:
-version
-reset
-getMode
-setMode mode of operation
-initializeConfig
-migrateConfig PrimaryCard number
-SDCard card number
-getFreeSpaceInfo
-driveLun drive number
-driveName drive name
-driveList
-create
-delete
-modify
-getOwner
-setOwner
-help
```

The following sections provide example usage of each option.

Option -version

This option displays the firmware version (level) installed in the adapter.

Example:

```
system> sdraid -version
Firmware Version = 1.3.2.166
ok
system>
```

Option -reset

Use this option to reset the adapter.

Examples:

```
system> sdraid -reset
Note that this operation will disconnect all of the disks assigned to the
system/OS and halt any file operations currently in progress via the IMM.
Make sure that the system is not currently booted from this device and that
all partition provisioning operations have been completed before continuing.

To perform the reset, issue command: "sdraid -reset -now".
ok
system>
```

```
system> sdraid -reset -now
Reset complete
ok
system>
```

Option -getMode

This option is used to check the current mode of operation of the adapter firmware.

Examples:

```
system> sdraid -getMode
SD Media have mismatched RAID Configuration. To preserve data integrity
IMM will remain in Configuration mode until this is manually resolved.
ok
system>
```

```
system> sdraid -getMode
The adapter mode is Configuration.
ok
system>
```

```
system> sdraid -getMode
The adapter mode is Operational.
ok
system>
```

Option -setMode

This option is used to configure the mode of operation of the adapter firmware.

Examples:

```
system> sdraid -setMode Configuration
Note that this operation will disconnect all of the disks assigned to the
system/OS and halt any file operations currently in progress via the IMM.
Make sure that the system is not currently booted from this device and that
all partition provisioning operations have been completed before continuing.

To perform the mode change, issue command: "sdraid -setMode Configuration -now".
ok
system>
```

```
system> sdraid -setMode Configuration -now
The controller mode is Configuration.
ok
system>
```

```
system> sdraid -setMode Operational -now
The controller mode is Operational.
ok
system>
```

Option -initializeConfig

This option is used to initialize the SD Media cards.

Note: The **sdraid –initializeConfig -now** command can only be run if the adapter is in the *Configuration* mode of operation. This command will fail if the adapter is in the *Operational* mode of operation.

Examples:

```
system> sdraid -initializeConfig
Note that this operation will destroy all existing disks on this adapter
on both SD Media cards.

To perform the initialization, issue command: "sdraid -initializeConfig -now"
ok
system>
```

```
system> sdraid –initializeConfig -now
Global RAID configuration has been set.
ok
system>
```

Option -migrateConfig

This option is used to specify the primary SD card and set the RAID configuration.

Note: The **sdraid –migrateConfig -primaryCard** ***number*** **-now** command can only be run if the adapter is in the *Configuration* mode of operation. This command will fail if the adapter is in the *Operational* mode of operation.

Mandatory parameter	Explanation	Values
-primaryCard	The primary card is the source SD card that maintains the metadata.	1, 2

Examples:

```
system> sdraid -migrateConfig -primaryCard 1
Any existing data on card (SDCard2) will be lost during this operation.
After this operation, any RAID data on SDCard1 will be synchronized to SDCard2
automatically.

To perform the operation, issue command: "sdraid -migrateConfig -primaryCard
1|2 -now".
ok
system>
```

```
system> sdraid -migrateConfig -primaryCard 1 -now
Global RAID configuration has been set.
ok
system>
```

```
system> sdraid -migrateConfig -primaryCard 1 -now
Unable to set RAID configuration. (SetRaidConf[4A] Cannot configure when
RAID operation is started).
ok
system>
```

Option -SDCard

This option is used to display information for the specified SD card.

Mandatory parameter	Explanation	Values
-SDCard	The SD card number.	1, 2

Output	Explanation	Values
Status	The state of the SD card.	Status values are as follows: • Healthy - the SD card has good metadata • Unhealthy - the SD card is bad • Uninitialized - no metadata is present • Mismatch - the metadata on the two SD cards does not match • Rebuilding - a drive synchronization is currently in progress
FRU number	The value as read from the SD card.	Alphanumeric value
Serial number	The value as read from the SD card.	Alphanumeric value
Manufacturer	The SD card manufacturer name.	SD card manufacturer names are as follows: • SanDisk • Micron • unknown
Is primary	Indicate if this SD card is the primary host for the RAID drives.	true, false
Capacity	The size of the SD card in Megabytes (MB).	Numeric value
Largest available space	The size of the maximum drive in MB that can be created on the SD card.	Numeric value
Drive count	The number of drives that are configured on the SD card.	1 - 8
Drive *n* name	The volume name for drive *n*.	Null-terminated name string up to 15 characters for the name of the drive.

Example:

```
system> sdraid -SDCard 1
SDCard
   Status                  = Healthy
   FRU Number              = 00SE32G
   Serial Number           = bd5ff15
   Manufacturer            = SanDisk
   Is Primary              = true
   Capacity                = 30436 Mbytes
   Largest Available Space = 30436 Mbytes
   DriveCount              = 2
   Drive 1 Name            = MDRIVE_1
   Drive 2 Name            = MDRIVE_2
ok
system>
```

Option -getFreeSpaceinfo

This option is used to display information pertaining to the free blocks (space) available in the SD cards.

Output	Explanation	Values
Free block region *n*	The index number of the free region from the list of free block regions for the two SD cards.	where *n* is a numeric value
SDCard	The SD card that the region is located on.	1, 2
Start address	The start address for the free block region.	Numeric value
Region size	This is the free block region size.	Region size values are as follows: • SanDisk • Micron • unknown

Example:

```
system> sdraid -getFreeSpaceInfo
Free Block Region [1]
   SDCard        = 1
   Start Address = 4259840
   Region Size   = 28356 MBytes
Free Block Region [2]
   SDCard        = 2
   Start Address = 0
   Region Size   = 1060 MBytes
Free Block Region [3]
   SDCard        = 2
   Start Address = 6430720
   Region Size   = 27296 MBytes
system>
```

Option -driveLun

This option is used to display the properties of a drive that is configured on the SD card.

Mandatory parameter	Explanation	Values
-driveLun	The logical unit number of the drive.	0 - 15

Output	Explanation	Values
Drive name	The name of the drive.	Null-terminated name string up to 15 characters for the name of the drive.
Target	The target where the drive is located.	SDCard1, SDCard2, mirror
LUN	The logical unit number of the drive.	0 - 15
Size *n*	The size of the drive in MB.	where *n* is the number of MB
Status	The status of the drive.	Ok, Fail, Degraded, Optimal
Owner	The current owner of the drive.	imm, immOnly, system, systemOnly

Output	Explanation	Values
Read only	Flag to indicate if the drive is write-protected.	true, false
Removable	Flag to indicate if the drive can be a removable USB drive for the server.	true, false

Example:

```
system> sdraid -driveLun 1
Drive Name                = PAIR_B_02
   Target                 = mirror
   LUN                    = 1
   Size                   = 1040 MBytes
   Mode                   = RAID
   Status                 = Optimal
   Owner                  = system
   System Options
     Read Only            = false
     Removable            = true
ok
system>
```

Option -driveName

This option is used to display the properties of a drive that is configured on the SD Media RAID adapter.

Note: The output and restrictions are the same as that for option -driveLun.

Mandatory parameter	Explanation	Values
-driveName	The volume name for the drive.	Null-terminated name string up to 15 characters for the name of the drive.

Example:

```
system> sdraid -driveName PAIR_B_02
Drive Name                = PAIR_B_02
   Target                 = mirror
   LUN                    = 1
   Size                   = 1040 MBytes
   Mode                   = RAID
   Status                 = Optimal
   Owner                  = system
   System Options
      Read Only           = false
      Removable           = true
ok
system>
```

Option -driveList

This option is used to display information for all of the drives configured on the SD Media RAID adapter.

Output	Explanation	Values
Index	The index number of the drive on the SD card.	1 - 8
LUN	The logical unit number of the drive.	0 - 15

Output	**Explanation**	**Values**
Drive name	The name of the drive.	Null-terminated name string up to 15 characters for the name of the drive.
Type	The type of drive.	RAID, non-RAID
Size *n*	The size of the drive in MB.	where *n* is the number of MB
Owner	The current owner of the drive.	imm, immOnly, system, systemOnly
Access	Flag to indicate if the drive is write-protected.	RW, RO
Removable	Flag to indicate if the drive can be a removable USB drive for the server.	yes, no

Example:

```
system> sdraid -driveList
SDCard 1
Index  LUN  Name             Type      Size(MB)   Owner      Access  Removable
  1      2  DRIVE_03         RAID        2048     system       RW        no
  2      1  DRIVE_02         non-RAID    1024     system       RW        no

SDCard 2
Index  LUN  Name             Type      Size(MB)   Owner      Access  Removable
  1      2  DRIVE_03         RAID        2048     system       RW        no
  2      0  DRIVE_01         non-RAID    1024     imm          RW        no
ok
system>
```

Option -create

This option is used to create a new drive.

Note: The **sdraid –create** command can only be run if the adapter is in the *Configuration* mode of operation. This command will fail if the adapter is in the *Operational* mode of operation.

Mandatory parameter	**Explanation**	**Values**
-driveName	The name of the drive.	Null-terminated name string up to 15 characters for the name of the drive.
-sizeMB *n*	The size of the drive in MB.	where *n* is the number of MB
-target	The card location for the drive. This is used to specify if the drive is to be created as mirrored on both SD cards or as a non-raid drive on one of the specified SD cards.	SDCard1, SDCard2, mirror
-removable	The drive is mapped to a fixed LUN.	0, 1
-owner	The owner of the drive.	imm, immOnly, system, systemOnly
-systemReadOnly	Flag to indicate if the drive is read-only when it is owned by the system.	0, 1

Optional parameter	Explanation	Values
-LUN	The LUN number assigned to the drive that is being created, LUN 0 is the bootable drive as seen by the server.	0

Examples:

```
system> sdraid -create -driveName DRIVE_01 -sizeMB 1024  -target SDCard2
-removable 0 -owner imm -systemReadOnly 0 -LUN 0
successfully created a drive.
Successfully set drive owner to imm
ok
system>
```

```
system> sdraid -create -driveName DRIVE_02 -sizeMB 1024 -target SDCard1
-removable 0 -owner system -systemReadOnly 0
successfully created a drive.
Successfully set drive owner to system
ok
system>
```

Option -delete

This option is used to delete an existing drive and can be used with parameters -driveLun or-driveName.

Note: The **sdraid –delete -driveLun** command can only be run if the adapter is in the *Configuration* mode of operation. This command will fail if the adapter is in the *Operational* mode of operation.

Mandatory parameter	Explanation	Values
-driveName	The volume name for the drive.	Null-terminated name string up to 15 characters for the name of the drive.
-driveLun	The logical unit number for the drive.	0 - 15

Examples:

```
system> sdraid -delete –driveName DRIVE_03
successfully deleted drive DRIVE_03
ok
system>
```

```
system> sdraid -delete -driveLun 2
successfully deleted drive DRIVE_03
ok
system>
```

```
system> sdraid -delete -driveLun 2
The controller is presently not in Configuration mode.
This command option can only be used in Configuration mode.
ok
system>
```

Option -modify

This option is used to modify the properties of an existing drive. This option can be used with parameters -driveLun or-driveName.

Note: The **sdraid –modify -driveLun -owner system** command can only be run if the adapter is in the *Configuration* mode of operation. This command will fail if the adapter is in the *Operational* mode of operation.

Mandatory parameter	Explanation	Values
-driveName or -driveLun	The volume name or the logical unit number of the drive.	Null-terminated name string up to 15 characters for the name of the drive.

Optional parameter	Explanation	Values
-systemReadOnly	Flag to indicate if the drive is read-only when it is owned by the system.	0, 1
-removable	The drive is mapped to a fixed logical unit number.	0, 1
-owner	The owner of the drive.	imm, immOnly, system, systemOnly

Examples:

```
system> sdraid -modify -driveLun 0 -removable 1
successfully configured drive DRIVE_03
ok
system>
```

```
system> sdraid -modify -driveLun 0 -owner imm
successfully configured drive DRIVE_03
Successfully set drive owner to imm
ok
system>
```

```
system> sdraid -modify -driveLun 0 -owner system
The controller is presently not in Configuration mode.
This command option can only be used in Configuration mode.
ok
system>
```

Option -getOwner

This option is used to display information about the current ownership of a specific drive. This option can be used with parameters -driveLun or -driveName.

Mandatory parameter	Explanation	Values
-driveLun	The logical unit number of the drive.	0 - 15
-driveName	The volume name of the drive.	Null-terminated name string up to 15 characters for the name of the drive.

Examples:

```
system> sdraid -getOwner -driveLun 1
Current owner of drive DRIVE_02 is system
ok
system>
```

```
system> sdraid -getOwner -driveName DRIVE_01
Current owner of drive DRIVE_01 is imm
ok
system>
```

Option -setOwner

This option is used to set the ownership of a specific drive to the IMM2 or the system. This option can be used with parameters -driveLun or -driveName.

Mandatory parameter	Explanation	Values
-driveLun	The logical unit number of the drive.	0 - 15
-driveName	The volume name of the drive.	Null-terminated name string up to 15 characters for the name of the drive.

Examples:

```
system> sdraid -setOwner imm  -driveLun 2
Successfully set drive owner to imm
ok
system>
```

```
system> sdraid -setOwner system -driveName DRIVE_01
Successfully set drive owner to system
ok
system>
```

Option -help

This option is used to display the command usage and options.

Examples:

```
system> sdraid –h
```

```
system> sdraid -help
```

Using the sdraid command without an option

Using the **sdraid** command with no options displays all relevant information for the SD RAID adapter. The following information is displayed for the installed adapter:

- Firmware version
- Global RAID configuration settings
- RAID device information

Example:

```
system> sdraid
SD Media Adapter for System x
   Hardware Revision     = 3.0
   Firmware Version      = 1.3.2.166
   Serial Number         =
   FRU Number            = 00AN748
Mode                    = Operational
SDCard1
   Status                = Healthy
   Capacity              = 30436 MBytes
   FRU Number            = 00SE32G
SDCard2
   Status                = Healthy
   Capacity              = 30436 MBytes
   FRU Number            = 00SE32G
system>
```

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*x*i*y* command options.
-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 "".

Option	Description	Values
-c*x*i*y*	SNMP community *x* IP address or hostname *y*	Valid IP address or hostname (limited to 63 characters). **Note:** • *x* is specified as 1, 2, or 3 in the command option to indicate the community number. • *y* is specified as 1, 2, or 3 in the command option to indicate the IP address or hostname number. • An IP address or hostname can only contain dots, underscores, minus signs, letters and digits. No embedded spaces or consecutive periods are allowed. • Clear an SNMP community IP address or hostname by specifying no argument.
-ca*x*	SNMPv3 community *x* access type	get, set, trap **Note:** *x* is specified as 1, 2, or 3 in the command option to indicate the community number.

Syntax:

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

Example:

```
system> snmp
-a Enabled
-a3 Enabled
-t Enabled
-l RTC,NC
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-ca1 set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
```

```
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>
```

snmpalerts command

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

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

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

Option	Description	Values
-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
-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:

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 **sslcfg** command is used to generate a new encryption key and self-signed certificate or certificate signing request (CSR). The following table shows the arguments for the options.

Option	Description	Values
-server	SSL server status	enabled, disabled **Note:** The SSL server can be enabled only if a valid certificate is in place.
-client	SSL client status	enabled, disabled **Note:** The SSL client can be enabled only if a valid server or client certificate is in place.
-cim	CIM over HTTPS status	enabled, disabled **Note:** CIM over HTTPS can be enabled only if a valid server or client certificate is in place.
-cert	Generate self-signed certificate	server, client, sysdir, storekey **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 a CSR	server, client, sysdir, storekey **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.

Option	Description	Values
-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.
-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
-tc x 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
```

Examples:

```
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
```

Client certificate examples:

- To generate a CSR for a storage key, enter the following command:

  ```
  system> sslcfg
  -csr storekey -c US -sp NC -cl rtp -on IBM -hn IMM2-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

The above example is displayed on multiple lines due to space limitations.

- To download a certificate from the IMM2 to another server, enter the following command:

  ```
  system> sslcfg
  -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```

- To upload the certificate processed by the Certificate Authority (CA), enter the following command:

  ```
  system> sslcfg
  -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```

- To generate a self-signed certificate, enter the following command:

```
system> sslcfg
-cert storekey -c US -sp NC -cl rtp -on IBM -hn IMM2-5cf3fc6e0c9d
-cp Contact -ea "" -ou "
ok
```

  The above example is displayed on multiple lines due to space limitations.

SKLM Server certificate example:

- To import the SKLM server certificate, enter the following command:

```
system> storekeycfg
-add -ip 192.168.70.200 -f tklm-server.der
ok
```

storage command

Use the **storage** command to display and configure (if supported by the platform) information about the server's storage devices that are managed by the IMM2.

The following table shows the arguments for the options.

Option	Description	Values
-list	List the storage targets managed by the IMM2.	*controllers* | *pools* | *volumes* | *drives* Where *target* is: • *controllers*: list the supported RAID controllers[1] • *pools*: list the storage pools associated with the RAID controller[1] • *volumes*: list the storage volumes associated with the RAID controller[1] • *drives*: list the storage drives associated with the RAID controller[1]
-list -target *target_id*	List the storage *targets* managed by the IMM2 according to the *target_id*.	*pools* | *volumes* | *drives ctrl[x]* | *pool[x]* Where *target* and *target_id* are: • *pools ctrl[x]*: list the storage pools associated with the RAID controller, based on the target_id[1] • *volumes ctrl[x]* | *pool[x]*: list the storage volumes associated with the RAID controller, based on the target_id[1] • *drives ctrl[x]* | *pool[x]*: list the storage drives associated with the RAID controller, based on the target_id[1]
-list flashdimms	List the Flash DIMMs managed by the IMM2.	

Option	Description	Values
-list devices	Display the status of all disks and Flash DIMMS managed by the IMM2.	
-show *target_id*	Display information for the selected target that is managed by the IMM2.	Where *target_id* is: *ctrl[x]* | *vol[x]* | *disk[x]* | *pool[x]* | *flashdimm[x]*[3]
-show *target_id* info	Display detailed information for the selected target that is managed by the IMM2.	Where *target_id* is: *ctrl[x]* | *vol[x]* | *disk[x]* | *pool[x]* | *flashdimm[x]*[3]
-show *target_id firmware* [3]	Display the firmware information for the selected target that is managed by the IMM2.	Where *target_id* is: *ctrl[x]* | *disk[x]* | *flashdimm[x]*[2]
-showlog *target_id* *<m:n* | *all>*[3]	Display the event logs of the selected target that is managed by the IMM2.	Where *target_id* is: *ctrl[x]*[4] *m:n* | *all* Where *m:n* is one to the maximum number of event logs Where *all* are all of the event logs
-config ctrl -scanforgn -target *target_id*[3]	Detect the foreign RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config ctrl -imptforgn -target *target_id*[3]	Import the foreign RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config ctrl -clrforgn -target *target_id*[3]	Clear the foreign RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config ctrl -clrcfg -target *target_id*[3]	Clear the RAID configuration.	Where *target_id* is: *ctrl[x]*[5]
-config drv -mkoffline -target *target_id*[3]	Change the drive state from online to offline.	Where *target_id* is: *disk[x]*[5]
-config drv -mkonline -target *target_id*[3]	Change the drive state from offline to online.	Where *target_id* is: *disk[x]*[5]
-config drv -mkmissing -target *target_id*[3]	Mark the offline drive as an unconfigured good drive.	Where *target_id* is: *disk[x]*[5]
-config drv -prprm -target *target_id*[3]	Prepare an unconfigured good drive for removal.	Where *target_id* is: *disk[x]*[5]
-config drv -undoprprm -target *target_id*[3]	Cancel the prepare an unconfigured good drive for removal operation.	Where *target_id* is: *disk[x]*[5]
-config drv -mkbad -target *target_id*[3]	Change the unconfigured good drive to a unconfigured bad drive.	Where *target_id* is: *disk[x]*[5]

Option	Description	Values
-config drv -mkgood -target *target_id*[3]	Change an unconfigured bad drive to a unconfigured good drive. or Convert the just a bunch of disks (JBOD) drive to an unconfigured good drive.	Where *target_id* is: *disk[x]*[5]
-config drv -addhsp -*[dedicated pools]* -target *target_id*[3]	Assign the selected drive as a hot spare to one controller or to existing storage pools.	Where *target_id* is: *disk[x]*[5]
-config drv -rmhsp -target *target_id*[3]	Remove the hot spare.	Where *target_id* is: *disk[x]*[5]
-config vol -remove -target *target_id*[3]	Remove one volume.	Where *target_id* is: *vol[x]*[5]

Option	Description	Values
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target *target_id*[3]	Modify the properties of one volume.	• [-N *volume_name*] is the name of the volume • [-w <*0*|*1*|*2*>] is the cache write policy: – Type *0* for the Write Through policy – Type *1* for the Write Back policy – Type *2* for the Write With Battery Backup Unit (BBU) policy • [-r <*0*|*1*|*2*>] is the cache read policy: – Type *0* for the No Read Ahead policy – Type *1* for the Read Ahead Policy – Type *2* for the Adaptive Read Ahead policy • [-i <*0*|*1*>] is the cache I/O policy: – Type *0* for the Direct I/O policy – Type *1* for the Cached I/O policy • [-a <*0*|*2*|*3*>] is the access policy: – Type *0* for the Read Write policy – Type *2* for the Read Only policy – Type *3* for the Blocked policy • [-d <*0*|*1*|*2*>] is the disk cache policy: – Type *0* if the policy is unchanged – Type *1* to enable the policy[6] – Type *2* to disable the policy • [-b <*0*|*1*>] is the background initialization: – Type *0* to enable initialization – Type *1* to disable initialization • *-target_id* is *vol[x]*[5]

<table>
<tr><th>Option</th><th>Description</th><th>Values</th></tr>
<tr><td>-config vol -add <[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3][7]</td><td>Create one volume for a new storage pool when the target is a controller.
or
Create one volume with an existing storage pool when the target is a storage pool.</td><td>• [-R <i>&lt;0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0</i>&gt;] This option defines the RAID level and is only used with a new storage pool
• [-D disk <i>[id11]:disk[id12]:..disk[id21]:disk[id22]:..</i>] This option defines the drive group (including spans) and is only used with a new storage pool
• [-H disk <i>[id1]:disk[id2]:..</i>] This option defines the hot spare group and is only used with a new storage pool
• [-1 hole] This option defines the index number of the free hole space for an existing storage pool
• [-N <i>volume_name</i>] is the name of the volume
• [-w &lt;<i>0|1|2</i>&gt;] is the cache write policy:
– Type <i>0</i> for the Write Through policy
– Type <i>1</i> for the Write Back policy
– Type <i>2</i> for the Write With Battery Backup Unit (BBU) policy
• [-r &lt;<i>0|1|2</i>&gt;] is the cache read policy :
– Type <i>0</i> for the No Read Ahead policy
– Type <i>1</i> for the Read Ahead policy
– Type <i>2</i> for the Adaptive Read Ahead policy</td></tr>
</table>

Option	Description	Values
-config vol -add [-i] [-a] [-d] [-f] [-S] [-P] -target *target_id*[3]	Create one volume for a new storage pool when the target is a controller. or Create one volume with an existing storage pool when the target is a storage pool.	• [-i <*0*|*1*>] is the cache I/O policy: – Type *0* for the Direct I/O policy – Type *1* for the Cached I/O policy • [-a <*0*|*2*|*3*>] is the access policy: – Type *0* for the Read Write policy – Type *2* for the Read Only policy – Type *3* for the Blocked policy • [-d <*0*|*1*|*2*>] is the disk cache policy: – Type *0* if the policy remains unchanged – Type *1* to enable the policy[6] – Type *2* to disable the policy • [-f <*0/1/2*>] is the type of initialization: – Type *0* for no initialization – Type *1* for quick initialization – Type *2* for full initialization • [-S *volume_size*] is the size of the new volume in MB • [-P *strip_size*] is the volume strip size for example, 128K or 1M • -target *target_id* is: – *ctrl[x]* (new storage pool[5]) – *pool[x]* (existing storage pool)[5]
-config vol -getfreecap [-R] [-D disk] [-H disk] -target *target_id*[3]	Get the free capacity amount of the drive group.	• [-R <*0*|*1*|*5*|*1E*|*6*|*10*|*50*|*60*|*00*|*1ERLQ0*|*1E0RLQ0*>] This option defines the RAID level and is only used with a new storage pool • [-D disk *[id11]:[id12]:.. [id21]:[id22]:..*] This option defines the drive group (including spans) and is only used with a new storage pool • [-H disk *[id1]:[id2]:..*] This option defines the hot spare group and is only used with a new storage pool • -target *target_id* is: – *ctrl[x]*[5]

Option	Description	Values
-help	Display the command usage and options	
Notes: 1. This command is only supported on servers where the IMM2 can access the RAID controller. 2. Firmware information is displayed only for associated controllers, disks, and Flash DIMMs. Firmware information for associated pools and volumes are not displayed. 3. Information is displayed on multiple lines due to space limitations. 4. This command is only supported on servers that support RAID logs. 5. This command is only supported on servers that support RAID configurations. 6. The *Enable* value does not support RAID level 1 configurations. 7. A partial list of available options are listed here. The remaining options for the **storage -config vol -add** command are listed in the following row.		

Syntax:

```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]} firmware
  -showlog ctrl[x] m:n|all
  -h help
```

Examples:

```
system> storage
-config ctrl -clrcfg -target ctrl[0]
ok
system>
```

```
system> storage
-config ctrl -clrforgn -target ctrl[0]
ok
system>
```

```
system> storage
-config ctrl -imptforgn -target ctrl[0]
ok
system>
```

```
system> storage
-config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
```

```
system> storage
-config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
```

```
system> storage
-config drv -addhsp -target disk[0-0]
ok
system>
system> storage
-config drv -mkbad -target disk[0-0]
ok
system>

system> storage
-config drv -mkgood -target disk[0-0]
ok
system>

system> storage
-config drv -mkmissing -target disk[0-0]
ok
system>

system> storage
-config drv -mkoffline -target disk[0-0]
ok
system>

system> storage
-config drv -mkonline -target disk[0-0]
ok
system>

system> storage
-config drv -prprm -target disk[0-0]
ok
system>

system> storage
-config drv -rmhsp -target disk[0-0]
ok
system>

system> storage
-config drv -undoprprm -target disk[0-0]
ok
system>

system> storage
-config vol -add -1 1 -target pool[0-1]
ok
system>

system> storage
-config vol -add -R 1 -D disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>

system> storage
-config vol -getfreecap -R 1 -D disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>

system> storage
-config vol -remove -target vol[0-1]
ok
system>

system> storage
-config vol -set -N LD_volume -w 0 -target vol[0-0]
ok
system>

system> storage
-list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage
-list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
```

```
system> storage
-list flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
```

```
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
```

```
system> storage
-list volumes
system>storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
```

```
system> storage
-list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
```

```
system> storage
-list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
```

```
system> storage
-list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
```

```
system> storage
-list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
```

```
system> storage
-list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
```

```
system> storage
-show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
```

```
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
```

```
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0]  Storage Pool 0
pool[0-1]  Storage Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
```

```
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
```

```
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
```

```
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
```

```
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
```

```
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
```

```
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
```

```
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
```

```
system> storage
-show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

storekeycfg command

Use the **storekeycfg** command to configure the hostname or IP address and network port for a SKLM server. You can configure up to four SKLM server targets. The **storekeycfg** command is also used to install and remove the certificates that are used by the IMM2 for authentication to the SKLM server.

The following table shows the arguments for the options.

Option	Description	Values
-add	Add the activation key	Values are -ip, -pn, -u, -pw, and -f command options
-ip	Host name or IP address for the TFTP/SFTP server	Valid host name or IP address for TFTP/SFTP server
-pn	Port number of the TFTP or SFTP server	Valid port number for TFTP/SFTP server (default value is 69/22)
-u	User name for SFTP server	Valid user name for SFTP server
-pw	Password for SFTP server	Valid password for SFTP server
-f	File name for activation key	Valid file name for activation key file name
-del	Use this command to delete the activation key by index number	Valid activation key index number from keycfg listing
-dgrp	Add the device group	Device group name
-sxip	Add the host name or IP address for the SKLM server	Valid host name or IP address for SKLM server. Numeric value of 1, 2, 3, or 4.
-sxpn	Add the port number of the SKLM server	Valid port number for SKLM server. Numeric value of 1, 2, 3, or 4.
-testx	Test the configuration and connection to the SKLM server	Numeric value of 1, 2, 3, or 4
-h	Display the command usage and options	

Syntax:

```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

Examples:

To import the SKLM server certificate, enter the following command:

```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

To configure the SKLM server address and port number, enter the following command:

```
system> storekeycfg
-slip 192.168.70.249
system> ok
```

To set the device group name, enter the following command:

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

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, 1.2 [1]
-h	List the usage and options	
Note: 1. When the cryptography mode is set to the NIST-800-131A Compliance mode, the TLS version must be set to 1.2.		

Syntax:

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

Examples:

To get the usage for the tls command, issue the following command:

```
system> tls
-h
system>
```

To obtain the current tls version, issue the following command:

```
system> tls
-min 1.0
system>
```

To change the current tls version to 1.2, issue the following command:

```
system> tls
-min 1.2
ok
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, minimal, efficiency, custom
-table	Vendor, device identification (ID) and alternate thermal table	

Syntax:

```
thermal [options]
option:
  -mode thermal_mode
  -table vendorID_device table_number
```

Example:

```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
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

Option	Timeout	Units	Values
-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.

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

Option	Description	Values
-pk	Display SSH public key for user	User account index number. **Notes:** • Each SSH key assigned to the user is displayed, along with an identifying key index number. • When using the SSH public key options, the `-pk` option must be used after the user index (`-`*`userindex`* option), of the form: `users -2 -pk`. • All keys are in OpenSSH format.
-e	Display entire SSH key in OpenSSH format *(SSH public key option)*	This option takes no arguments and must be used exclusive of all other `users -pk` options. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (`-`*`userindex`* option), of the form: `users -2 -pk -e`.
-remove	Remove SSH public key from user *(SSH public key option)*	Public key index number to remove must be given as a specific `-`*`key_index`* or `-all` for all keys assigned to the user. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (`-`*`userindex`* option), of the form: `users -2 -pk -remove -1`.

-add	Add SSH public key for user
	(SSH public key option)
		Quote-delimited key in OpenSSH format
		Notes:
		• 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. **Notes:** • The `-upld` option is used exclusive of all other `users -pk` command options (except for `-i` and `-l`). • To replace a key with a new key, you must specify a `-`*`key_index`*. To add a key to the end of the list of current keys, do not specify a key index. • When using the SSH public key options, the `-pk` option must be used after the user index (`-`*`userindex`* option), of the form: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`.

Option	Description	Values
-dnld	Download the specified SSH public key *(SSH public key option)*	Requires a `-key_index` to specify the key to download and the `-i` and `-l` options to specify the download location on another computer running a TFTP server. **Notes:** • The `-dnld` option is used exclusive of all other `users -pk` command options (except for `-i`, `-l`, and `-key_index`). • When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
-i	IP address of TFTP/SFTP server for uploading or downloading a key file *(SSH public key option)*	Valid IP address **Note:** The `-i` option is required by the `users -pk -upld` and `users -pk -dnld` command options.
-pn	Port number of TFTP/SFTP server *(SSH public key option)*	Valid port number (default 69/22) **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-u	User name for SFTP server *(SSH public key option)*	Valid user name **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-pw	Password for SFTP server *(SSH public key option)*	Valid password **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
-l	File name for uploading or downloading a key file via TFTP 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” on page 283
- “batch command” on page 285
- “clearcfg command” on page 286
- “clock command” on page 286
- “identify command” on page 287

- “info command” on page 287
- “resetsp command” on page 288
- “spreset command” on page 288

alertentries command

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

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

The following table shows the arguments for the options.

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

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

Syntax:

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

Example:

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

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

batch command

Use the **batch** command 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 the **-s on** option to turn the LED on for only the number of seconds specified with the **-d** option. The LED 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 a 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 issue this command.

spreset command

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

Service advisor commands

The service advisor commands are as follows:

- "autoftp command"
- "chconfig command" on page 289
- "chlog command" on page 290
- "chmanual command" on page 291
- "events command" on page 291
- "sdemail command" on page 292

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 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	Support status of the Service Advisor	enabled, disabled
-sc	Country code for the 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

Option	Description	Values
-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 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 Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the System x, Flex System, and NeXtScale System products.

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 warranty service for your Lenovo product, the 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 Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your 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 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 the service technician. This data will help the service technician 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 (Lenovo 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 the service technicians. The 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 Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs 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 Lenovo system and preinstalled software, if any, or optional device is available in the product documentation. 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. Lenovo 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 Lenovo products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support is available at http://www.ibm.com/supportportal. The most current version of the product documentation is available in the following product-specific Information Centers:

Flex System products:
http://publib.boulder.ibm.com/infocenter/flexsys/information/index.jsp

System x products:
http://www.ibm.com/systems/x

NeXtScale System products:

How to send DSA data

You can use the 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:

- **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 Lenovo 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 Lenovo 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

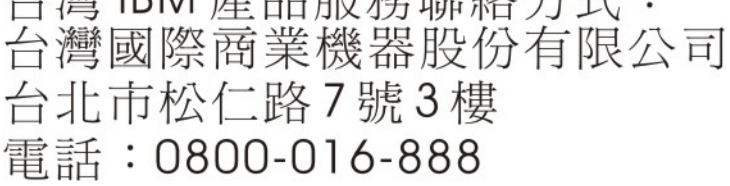
IBM is Lenovo's preferred service provider for the System x, Flex System and NeXtScale System products.

You can receive hardware service through your Lenovo reseller or from IBM. To locate a reseller authorized by Lenovo 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.

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

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo 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:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO 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 jurisdictions 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. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

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

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

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

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and x Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

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

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 1 024 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 Lenovo.

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. Lenovo 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.

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

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

Recycling information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to:
.

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 Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo 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 11. 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 11. 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.	

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 a Lenovo 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. Lenovo 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. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

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

Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

Germany Class A statement

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

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 (früher 89/336/EWG) 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 Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmittein Dieses Produkt entspricht dem „Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln“ EMVG (früher „Gesetz über die elektromagnetische Verträglichkeit von Geräten“). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007

(früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse A.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

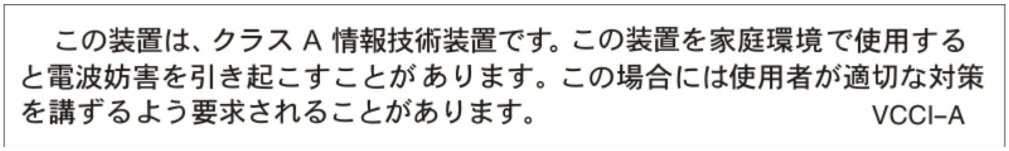
Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4: **Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.**

Nach der EN 55022: „Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen und dafür aufzukommen.“

Nach dem EMVG: „Geräte dürfen an Orten, für die sie nicht ausreichend entstört sind, nur mit besonderer Genehmigung des Bundesministers für Post und Telekommunikation oder des Bundesamtes für Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Störungen zu erwarten sind.“ (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbüchern angegeben, zu installieren und zu betreiben.

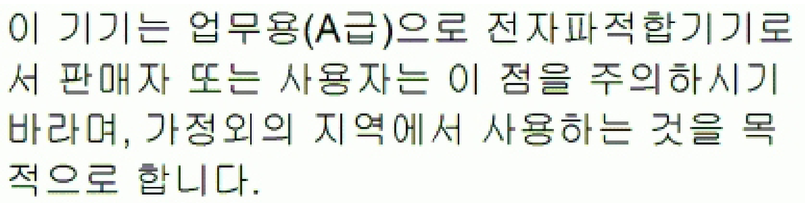
Japan VCCI Class A statement



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.

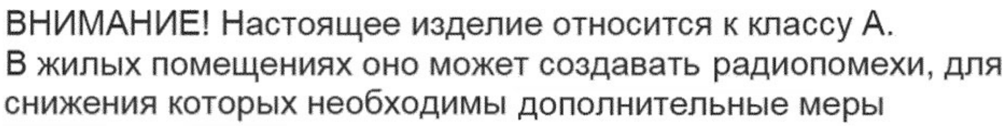
Korea Communications Commission (KCC) statement



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

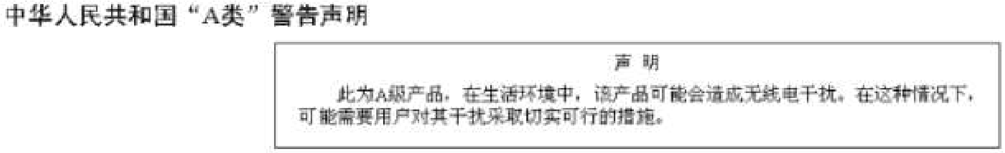
This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

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

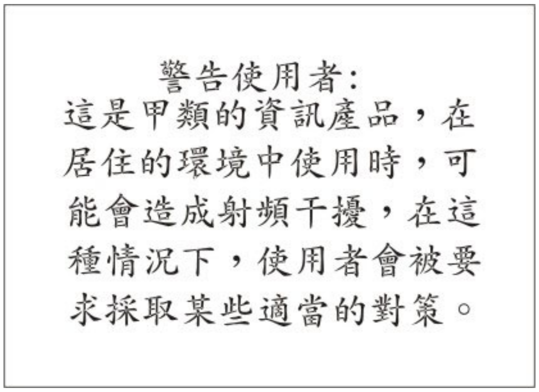


中华人民共和国“A类”警告声明

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

Part Number: 00FH740

Printed in USA

(1P) P/N: 00FH740