



Integrated Management Module II User's Guide



Note: Before using this information, read the general information in [Appendix B “Notices”](#) on page 323.

Twenty second (May 2019)

© Copyright Lenovo 2012, 2019.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant to a General Services Administration “GSA” contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925

Contents

Contents i

Chapter 1. Introduction 1

IMM2 Basic, Standard, and Advanced Level features	2
IMM2 Basic Level features	2
IMM2 Standard Level features	2
IMM2 Advanced Level features	3
IMM2 feature improvements	3
Upgrading IMM2	3
Using IMM2 with the BladeCenter advanced management module.	4
Web browser and operating-system requirements	4
Notices used in this book	7

Chapter 2. Opening and using the IMM2 web interface 9

Accessing the IMM2 web interface	9
Setting up the IMM2 network connection through the System x Server Firmware Setup utility	10
Logging in to the IMM2	11
IMM2 action descriptions	13

Chapter 3. IMM2 web user interface overview 19

Web session settings	19
Page auto refresh	19
Trespass message	20
Log out	21
System Status tab	22
Events tab	28
Event log	28
Event recipients	30
Service and Support tab	33
Problems option	33
Settings option	36
Preparing firewalls and proxies	40
Download service data option	41
Server Management tab	42
Server firmware	43
Remote control	48
Server properties	56
Server power actions	60
Cooling devices	61
Power modules	62
Local storage	63

Memory	66
Processors	68
Adapters	69
Server timeouts	69
PXE network boot	70
Latest OS failure screen	70
Power management	71
Scalable complex	71
IMM Management tab	71

Chapter 4. Configuring the IMM2 . . . 73

Setting server timeouts	76
Changing the IMM2 firmware automated promotion settings	78
Setting the IMM2 date and time	78
Configuring the serial port settings	80
Configuring user accounts	81
User accounts	81
Group profiles	85
Configuring global login settings	86
General settings	86
Account security policy settings	87
Configuring network protocols	90
Configuring the Ethernet settings	90
Configuring SNMP alert settings	93
Configuring DNS	95
Configuring DDNS	95
Configuring SMTP	96
Configuring LDAP	96
Configuring Telnet	100
Configuring USB	101
Setting Ethernet over USB for SUSE Linux Enterprise 12 or higher versions.	102
Configuring IPMI	103
Configuring port assignments	104
Configuring access control	105
Configuring security settings	106
Configuring HTTPS protocol	107
Configuring CIM over HTTPS protocol	108
Configuring LDAP client protocol	109
Configuring the Secure Shell server	111
SSL overview	112
SSL certificate handling	112
SSL certificate management	112
Compromised private keys	114
Configuring cryptography management	115

Configuring the SKLM Feature on Demand option	117
Restoring and modifying your IMM configuration	123
Restarting the IMM2	123
Resetting the IMM2 to the factory defaults	124
Activation management key	125

Chapter 5. Monitoring the server status.127

Viewing the system status.	127
Viewing the system information	129
Viewing the server health	130
Viewing the hardware health	131

Chapter 6. Performing IMM2 tasks135

Controlling the power status of the server.	136
Remote presence and remote control functions	137
Updating your IMM2 firmware and Java or ActiveX applet	138
Enabling the remote presence function	138
Remote control screen capture	138
Remote control Video Viewer modes.	139
Remote control video color mode	141
Remote control keyboard support	141
Remote control mouse support	145
Remote power control	146
Viewing performance statistics	147
Starting Remote Desktop Protocol	148
Video Recording.	148
Knock-knock feature description	150
Remote disk	153
Setting up PXE network boot	157
Updating the server firmware	158
Managing system events	163
Managing the event log	163
Notification of system events.	165
Collecting service and support information	170
Capturing the latest OS failure screen data	172
Managing the server power	173
Controlling the power supply and total system power	173
Displaying currently installed power supplies	177
Displaying power supply capacity	178
Displaying the power history	178
Displaying the power performance	179
Managing and monitoring power consumption with IPMI commands	180
Managing the scalable complex	182
Creating a partition.	183

Changing a partition mode.	184
Deleting a partition mode	185
Partition errors	186
Viewing and configuring the local storage configuration	187
Viewing the physical resource information.	187
Displaying and configuring the storage RAID configuration information	191
Displaying the RAID log information	193
Displaying information and configuring the SD Media RAID adapter for System x	194
Viewing the adapter information and configuration settings	200
Configuring the adapter information	201

Chapter 7. Features on Demand . . .205

Installing an activation key.	205
Removing an activation key	208
Exporting an activation key	209

Chapter 8. Command-line interface211

Managing the IMM2 with IPMI	211
Using IPMITool	211
Accessing the command-line interface.	211
Logging in to the command-line session	212
Configuring serial-to-Telnet or SSH redirection	212
Command syntax	212
Features and limitations	213
Alphabetical command listing	214
Utility commands	216
exit command.	216
help command	216
history command	216
Monitor commands	217
adapter command	217
clearlog command	219
fans command	220
ffdc command	220
led command	221
readlog command	223
syshealth command	224
temps command	225
volts command	225
vpd command	226
Server power and restart control commands	226
fuelg command	226
power command	228
pxeboot command.	230
reset command	230
Serial redirect command	231

console command	231
Configuration commands	231
accseccfg command	232
alertcfg command	234
asu command	235
autopromo command	238
backup command	239
cryptomode command	239
dhcinfo command	241
dns command	242
ethtousb command	243
gprofile command	244
ifconfig command	245
keycfg command	247
ldap command	248
ntp command	250
passwordcfg command	251
ports command	252
portcfg command	253
portcontrol command	254
restore command	255
restoredefaults command	255
scale command	256
sdraid command	265
services command	277
set command	278
smtp command	278
snmp command	279
snmpalerts command	282
srcfg command	283
sshcfg command	284
ssl command	285
sslcfg command	286
storage command	289
storekeycfg command	299
telnetcfg command	300
tls command	301
thermal command	302
timeouts command	302
usbeth command	303
users command	303
IMM2 control commands	307
alertentries command	308
batch command	310
clearcfg command	311
clock command	311
identify command	312
info command	312
resetsp command	313
spreset command	313

Service advisor commands	313
autoftp command	313
chconfig command	314
chlog command	316
chmanual command	317
events command	317
sdemail command	318

Appendix A. Getting help and technical assistance **319**

Before you call	319
Using the documentation	320
Getting help and information from the World Wide Web	320
How to send DSA data	320
Creating a personalized support web page	320
Software service and support	320
Hardware service and support	321
Taiwan product service	321

Appendix B. Notices **323**

Trademarks	324
Important notes	324
Recycling information	325
Particulate contamination	325
Telecommunication regulatory statement	326
Electronic emission notices	326
Federal Communications Commission (FCC) statement	326
Industry Canada Class A emission compliance statement	326
Avis de conformité à la réglementation d'Industrie Canada	327
Australia and New Zealand Class A statement	327
European Union EMC Directive conformance statement	327
Germany Class A statement	327
Japan VCCI Class A statement	328
Japanese statement of compliance for products less than or equal to 20 A per phase for JEITA harmonics guideline	328
Japan Electronics and Information Technology Industries Association (JEITA) statement	328
Korea Communications Commission (KCC) statement	328
Russia Electromagnetic Interference (EMI) Class A statement	329
People's Republic of China Class A electronic emission statement	329
Taiwan Class A compliance statement	329

Index **331**

Chapter 1. Introduction

The Integrated Management Module II (IMM2) service processor is the second generation of the Integrated Management Module (IMM) service processor.

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.lenovo.com/support>.
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

Use the information in this topic to understand the Basic, Standard, and Advanced levels of IMM2 functionality.

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

Use the information in this topic for a list of the Basic Level IMM2 features.

The following is a list of IMM2 Basic Level features:

- IPMI 2.0 RMCP+ 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

Use the information in this topic for a list of the Standard Level IMM2 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

Use the information in this topic for a list of the Advanced Level IMM2 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

Use the information in this topic for a list of IMM2 feature improvements over the IMM.

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

Use this information to understand the firmware upgrade functionality for the 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 205](#).

Using IMM2 with the BladeCenter advanced management module

Use the information in this topic to understand how the IMM2 is used 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.

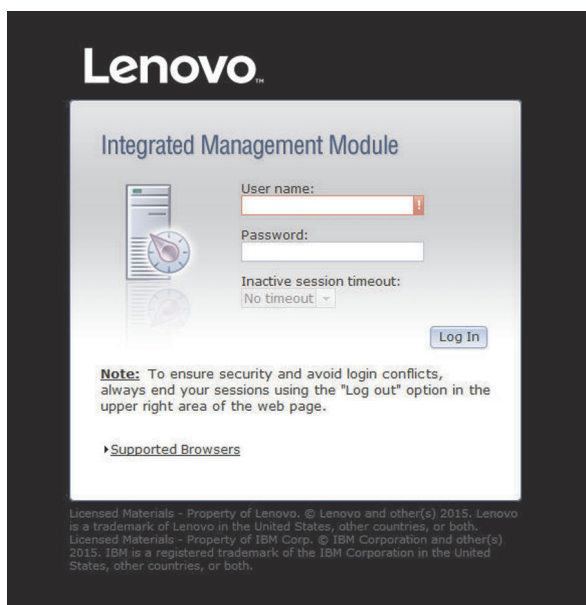
Web browser and operating-system requirements

Use the information in this topic to view the list of supported browsers, cipher suites and operating systems for your server.

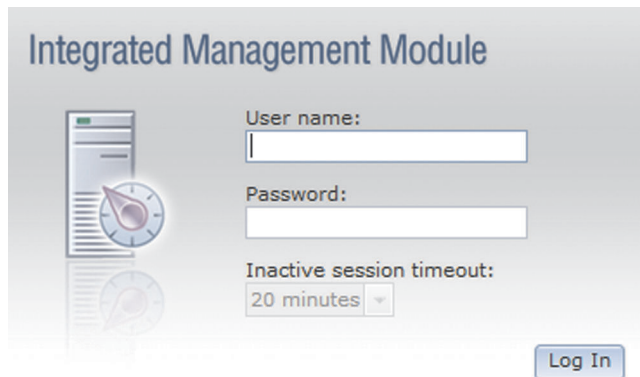
The IMM2 web interface supports the following web browsers:

- Internet Explorer versions 8 through 11
- Firefox versions 3.6 through 29
- Chrome versions 13 through 35

The browsers listed above match those currently supported by the IMM2 firmware. The IMM2 firmware may be enhanced periodically to include support for other browsers. The following illustration displays the IMM2 login screen.



Depending upon the version of the firmware in 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).



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 8-11
- Firefox 3.6-29
- Chrome 13-35

NOTE: If a browser version is not listed as supported, it may still work, especially on browsers with rapid release cycles (e.g. Chrome, Firefox).

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

- SLES11, SLES12
- RHEL5, RHEL6, RHEL7
- Windows XP
- Windows Vista
- Windows 2008
- Windows 7, 8, 10
- Windows 2012
- OS X v10.7
- OS X v10.8

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-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- AES256-GCM-SHA384
- AES256-SHA256
- AES128-GCM-SHA256
- AES128-SHA256

In addition to the above list of ciphers, the ciphers listed below are supported when the IMM2 is configured to use the Basic Compatibility cryptography mode:

- DHE-DSS-AES128-GCM-SHA256
- DHE-DSS-AES128-SHA256
- DHE-DSS-AES256-GCM-SHA384
- DHE-DSS-AES256-SHA256
- ECDH-ECDSA-AES128-GCM-SHA256
- ECDH-ECDSA-AES128-SHA256
- ECDH-ECDSA-AES256-GCM-SHA384
- ECDH-ECDSA-AES256-SHA384
- ECDH-RSA-AES128-GCM-SHA256
- ECDH-RSA-AES128-SHA256
- ECDH-RSA-AES256-GCM-SHA384
- ECDH-RSA-AES256-SHA384
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-ECDSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384

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 10
- Microsoft Windows 2012
- OS X v10.7
- OS X v10.8

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

Use this information to understand the notices that are used in this document.

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

This topic describes the login procedures and the actions that you can perform from 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 information in this topic explains how to access 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

Use the information in this topic to set up an 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:

Step 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.



Step 2. When the prompt <F1> Set up 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.

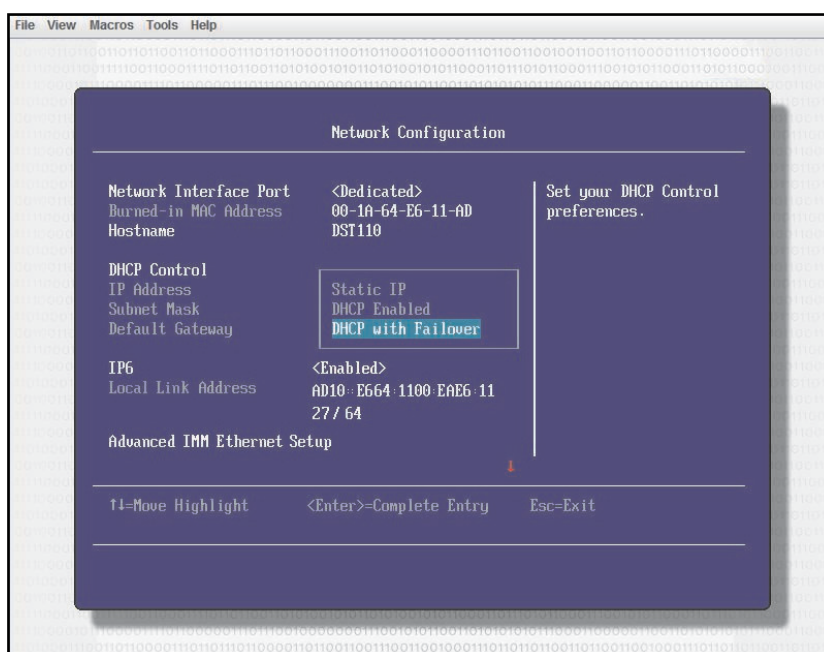
Step 3. From the Setup utility main menu, select **System Settings**.

Step 4. On the next screen, select **Integrated Management Module**.

Step 5. On the next screen, select **Network Configuration**.

Step 6. Highlight **DHCP Control**. There are three IMM2 network connection choices in the **DHCP Control** field:

- Static IP
- DHCP Enabled
- DHCP with Failover (default)



Step 7. Select one of the network connection choices.

Step 8. If you choose to use a static IP address, you must specify the IP address, the subnet mask, and the default gateway.

Step 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.

Step 10. Scroll down and select **Save Network Settings**.

Step 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

Use the information in this topic to access the IMM2 through the IMM2 web interface.

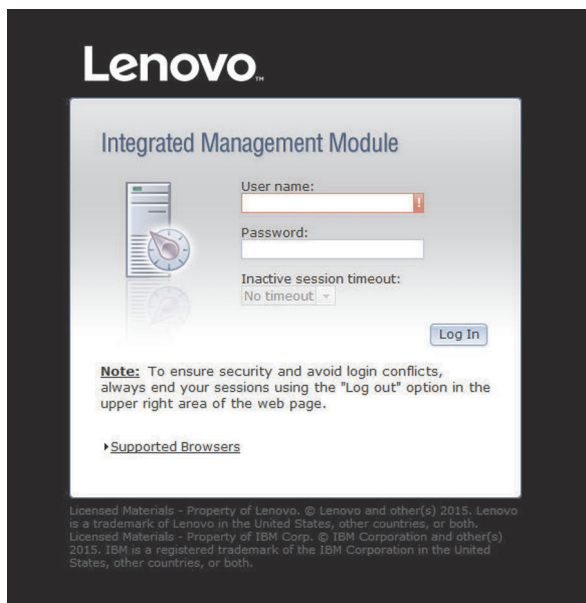
Important: The IMM2 is set initially with a user name of USERID and password of PASSWORD (with a zero, not the letter O). This default user setting has Supervisor access. Change this user name and password during your initial configuration for enhanced security.

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/PASSWORD combination described above.

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

- Step 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.
- Step 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.



- Step 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.

Notes: 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**, you can do either of the following:

For Windows 2008

- Disable the Windows 2008 firewall.
- 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
```

For Windows 2010

- Disable the Windows 2010 firewall.

- Type the following command in the Windows 2010 console. This might also affect blue-screen capture features.

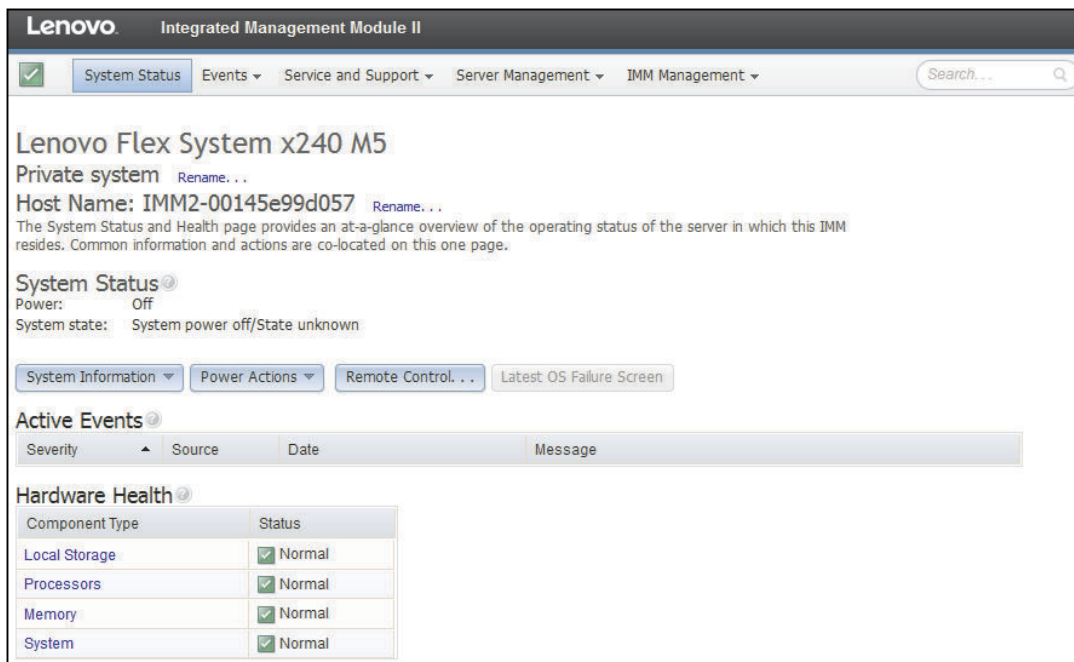
```
netsh advfirewall firewall set icmpsetting type=8 mode=ENABLE
```

For Windows 2012

- Disable the Windows 2012 firewall.
- Type the following command in the Windows 2012 console. This might also affect blue-screen capture features.

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

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



For descriptions of the actions that you can perform from the tabs at the top of the IMM2 web interface, see [“IMM2 action descriptions” on page 13](#). Then, go to [Chapter 4 “Configuring the IMM2” on page 73](#).

IMM2 action descriptions

Use the information in this topic to understand and access various IMM2 functions.

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 “IMM2 actions” on page 14](#).

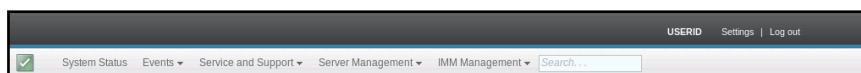


Table 1. IMM2 actions

Three column table containing descriptions of the actions that you can perform from the tabs at the top of the IMM2 web interface.

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 22 and “Viewing the system status” on page 127 for additional information.
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 28 and “Managing the event log” on page 163 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 30 and “Notification of system events” on page 165 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 33 for additional information.
	Settings	The Settings page configures your server to monitor and report service events. See “Settings option” on page 36 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 41 and “Collecting service and support information” on page 170 for additional information.
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 43 and “Updating the server firmware” on page 158 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 48 and “Remote presence and remote control functions” on page 137 for additional information.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
	Server Properties	<p>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:</p> <ul style="list-style-type: none"> • 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 56 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 60 and “Controlling the power status of the server” on page 136 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 61 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 62 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 63 and “Viewing and configuring the local storage configuration” on page 187 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 66 for additional information.
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 68 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 69 and “Viewing the adapter information and configuration settings” on page 200 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 69 and “Setting server timeouts” on page 76 for additional information.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
	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 70 and “Setting up PXE network boot” on page 157 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 70 and “Capturing the latest OS failure screen data” on page 172 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 71 and “Managing the server power” on page 173 for additional information.
	Scalable Complex	The Scalable Complex page allows you to view and manage a scalable complex. See “Scalable complex” on page 71 and “Managing the scalable complex” on page 182 for additional information.
IMM Management (continued on next page)	IMM Properties	<p>The IMM Properties page provides access to various properties and settings for your IMM2. The following options are available from the IMM Properties page:</p> <ul style="list-style-type: none"> • 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. <p>See Chapter 4 “Configuring the IMM2” on page 73 for additional information.</p>
	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 81 for additional information.

Table 1. IMM2 actions (continued)

Tab	Selection	Description
IMM Management (continued on next page)	Network	<p>The Network Protocol Properties page provides access to networking properties, status, and settings for your IMM2:</p> <ul style="list-style-type: none"> • 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 IPMI tab enables or disables IPMI access to IMM2. • The Port Assignments tab allows you to change the port numbers used by some services on the IMM2. • The Access Control tab allows you to configure blacklist for IP/MAC address and time duration to deny accessing IMM2. <p>See “Configuring network protocols” on page 90 for additional information.</p>
	Security	<p>The IMM Security page provides access to security properties, status, and settings for your IMM2:</p> <ul style="list-style-type: none"> • 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. <p>See “Configuring security settings” on page 106 for additional information.</p>
	IMM Configuration	<p>The IMM Configuration page displays a summary of the current IMM2 configuration settings. See “Restoring and modifying your IMM configuration” on page 123 for additional information.</p>
IMM Management (continued)	Restart IMM	<p>The Restart IMM page allows you to reset the IMM2. See “Restarting the IMM2” on page 123 for additional information.</p>
	Reset IMM to factory defaults...	<p>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 124 for additional information.</p> <p>Attention: When you click Reset IMM to factory defaults..., all modifications that you have made to the IMM2 are lost.</p>

Table 1. IMM2 actions (continued)

Tab	Selection	Description
	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 125 for additional information.

Chapter 3. IMM2 web user interface overview

Use the information in this topic to understand how to use the IMM2 web user interface features.

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

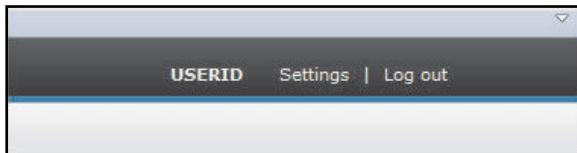
Important: This section does not apply to BladeCenter and blade servers. Although the IMM2 is standard in some BladeCenter products and blade servers, the BladeCenter advanced management module is the primary management module for systems-management functions. Users who wish to configure the IMM2 settings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

Web session settings

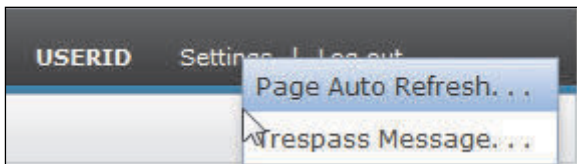
Use the information in this topic to understand the settings for the web interface session main page.

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.



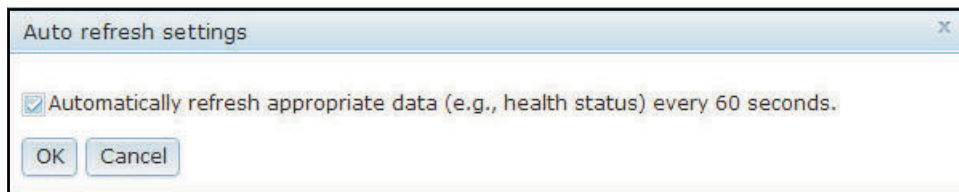
Click the **Settings** item and the following menu selections display:



Page auto refresh

To set the page content to automatically refresh use the information in this topic.

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



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

- **System Status:**

The system and power status is refreshed automatically every three seconds.

- **Server Power Actions:** (under the Server Management tab). Power status is refreshed automatically every three seconds.
- **Remote Control:** (under the Server Management tab). The Start remote control... buttons are automatically refreshed every second. The Session List table is refreshed once every 60 seconds.

Notes:

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

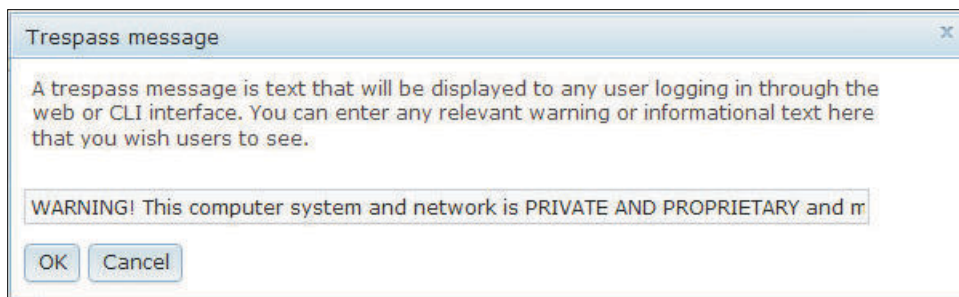
Note: The preceding note applies to all web pages.

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

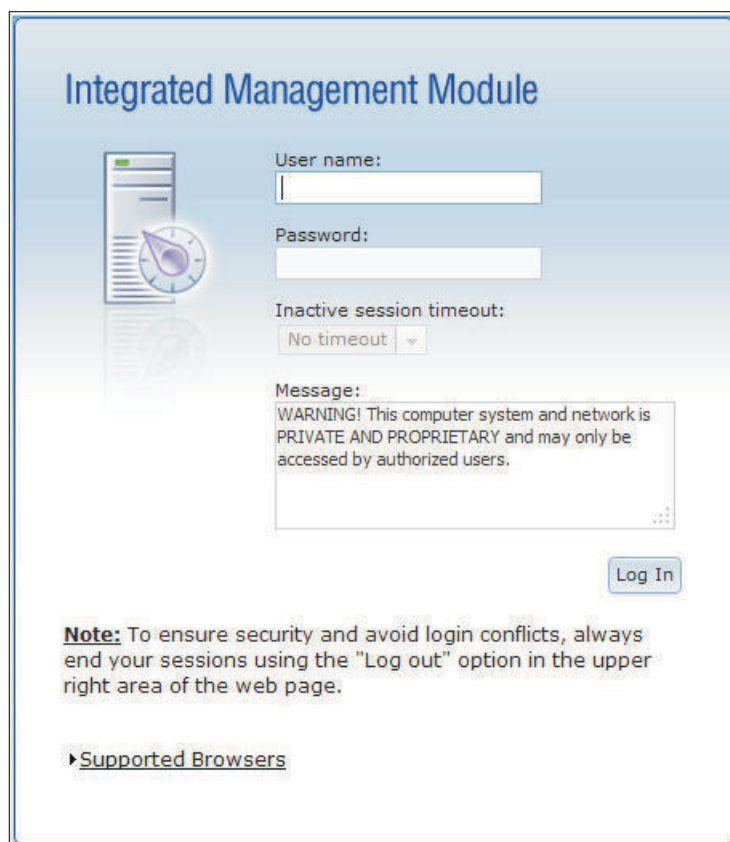
Trespass message

To create the message displayed when a user logs in to the IMM2 server use the information in this topic.

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



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



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.

Log In

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.

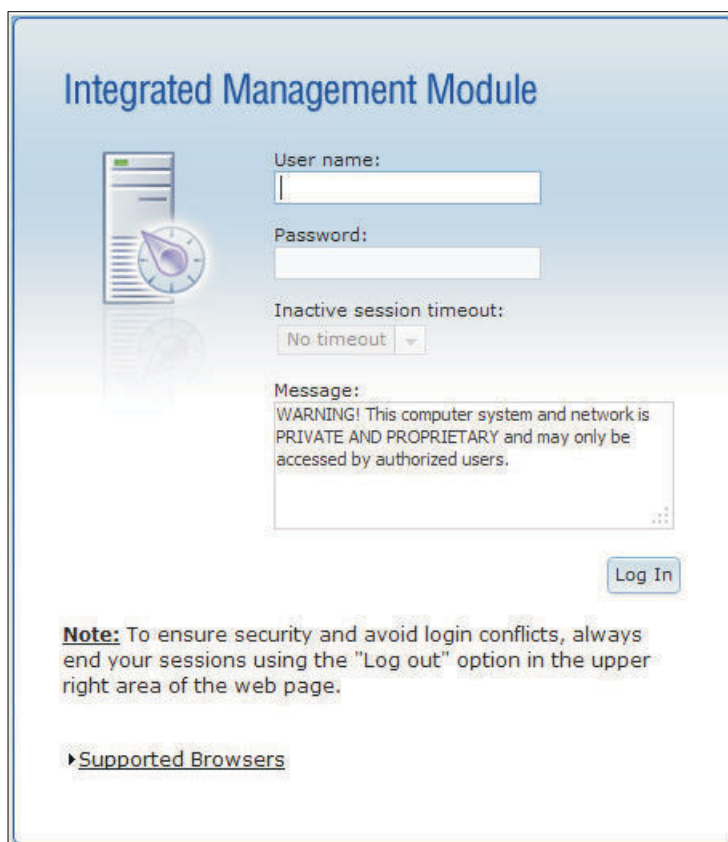
► [Supported Browsers](#)

Log out

To log out of the web session use the information in this topic.

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.

Log In

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](#)

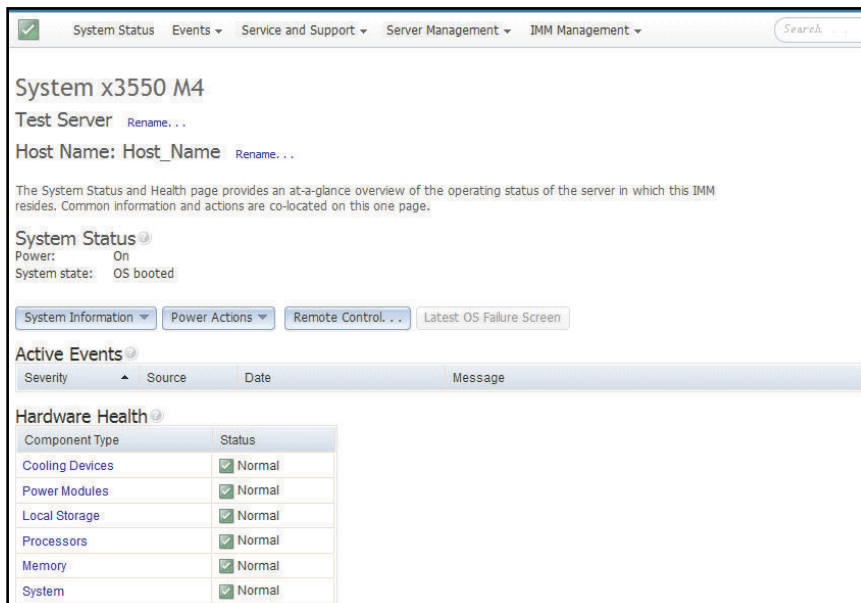
Note: The IMM2 firmware supports up to six simultaneous web sessions. To free up sessions for other users, log out of the web session when you are finished, rather than waiting on the inactivity timeout to automatically close your session. If you leave the browser while on an IMM2 web page that automatically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

System Status tab

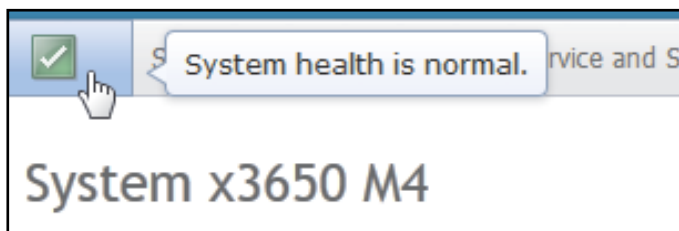
Use the information in this topic to understand the options under the **System Status** tab.

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

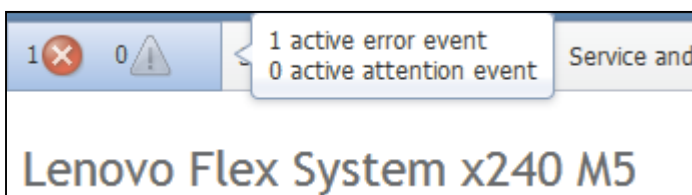
The System Status page is displayed after you log into the IMM2 web user interface or when you click the **System Status** tab. From the System Status page, you can view the system status, active system events, and hardware health information. The following window opens when you click the **System Status**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



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



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

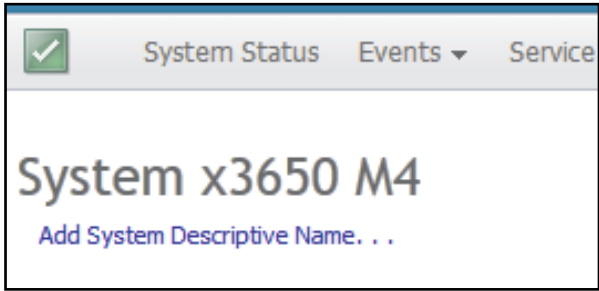


The red circle icon indicates that an error condition exists on the server. A yellow triangle icon indicates that a warning condition exists. When a red circle or a yellow triangle icon is displayed, the events associated with that condition are listed under the Active Events section on the System Status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

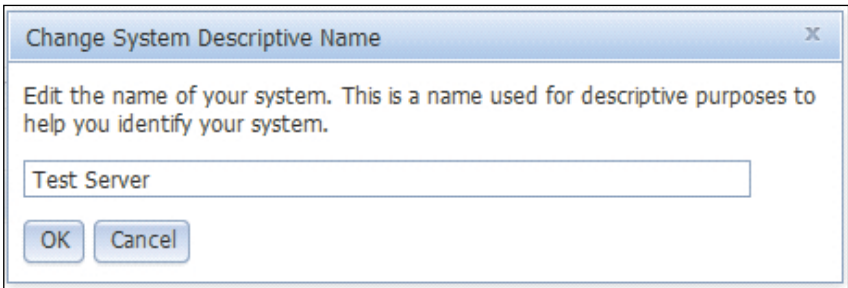
Active Events

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.

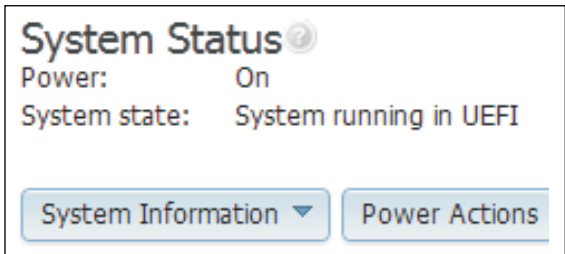


When you click the **Add System Descriptive Name...** link, the following window opens for you to specify a name to associate with the IMM2 server. You can change the System Descriptive Name at any time.



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 90](#) 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).



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

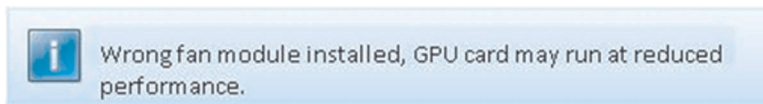
Table 2. Server power and operating states

Two column table with headers documenting the server operating states.

Table 2. Server power and operating states (continued)

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	<p>The server might be in this state for one of the following reasons:</p> <ul style="list-style-type: none"> • 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.
System Running in Setup	The server is powered on and UEFI has booted into F1 setup menu

The System Status page will display a message when an error or warning condition occurs, as seen in the following illustration.



In this example, when the GPU card is installed without a correct fan installed, the system status page will show one of the following warning messages to warn you that the GPU card may not be able to run at 100% functionality.

- “Wrong fan module installed, GPU card may run at reduced performance.”
- “Unknown fan module status”

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
Power Actions
Remote Control. . .
Latest OS Failure Screen

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

Close

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 136](#) 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 137](#) 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 172](#) 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.

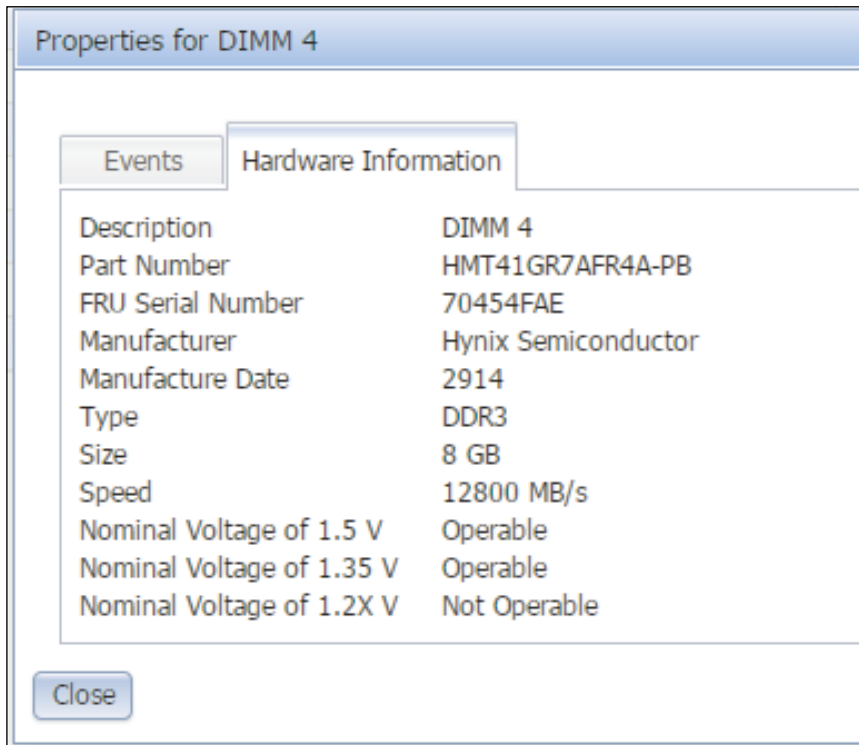
Properties for DIMM 4

Events Hardware Information

There are no active events for this device

Close

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

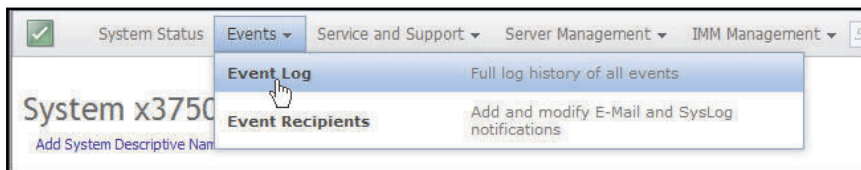


Events tab

To manage the Event Log history and Event Recipients for email and syslog notifications use the information in this topic.

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

The options under the **Events** tab enable 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

The Event log includes information about the severity of the events that are reported by the IMM2, and information about all remote access attempts and configuration changes.

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. A sequence number can be displayed to assist in determining the order of events when more than one event has the same time stamp.

Note: Some sequence numbers are used by internal BMC processes, so it is normal that there may be gaps in the sequence numbers when the events are sorted by sequence number.

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...)

Filters: [X] [Warning] [Info] [User] Time: All Dates Search Events... Go

Severity	Source	Date	Event ID	Message
0 of 51 items filtered	0 items selected	Clear filter Applied filters: Events [Error Warning Information Audit]		
Informational	System	31 1 2013 09:02:42.771 AM	0x400000e000000000	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[CM.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@=9.0.1.148.50.
Informational	System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet[BM.ep2] interface is now active.
Informational	System	31 1 2013 09:00:55.004 AM	0x4000001700000000	ENET[CM.ep2] IP-Cfg HstName=IMM2-6cae8b4e83c6, IP@=169.254.95.118, NetMask=255.255.0.0, GW@=0.0.0.0.
Informational	System	31 1 2013 09:00:53.403 AM	0x4000003700000000	ENET[CM.ep1] IPv6-LinkLocal HstName=IMM2-6cae8b4e83c6, IP@=fe80::6eae8b4e83c6, Pref=64.
Informational	System	31 1 2013 09:00:51.592 AM	0x4000001900000000	LAN: Ethernet[BM.ep1] interface is now active.
Informational	System	31 1 2013 09:00:47.068 AM	0x4000001900000000	Management Controller SN# 06KNKL9 Network Initialization Complete.
Informational	System	31 1 2013 09:00:02.874 AM	0x800801282101fff	Device Low Security Jmp has been added.
Informational	Power	31 1 2013 09:00:02.304 AM	0x805f00091301fff	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 (SN# 9.186.166.119) succeeded for user USERID.
Informational	System	31 1 2013 08:43:15.666 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.186.166.119.
Informational	System	31 1 2013 08:43:15.666 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.111.29.57.

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 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...)

Export Event Logs

Severity	Source	Date
0 of 52 items filtered	2 items selected	
<input checked="" type="checkbox"/> Informational	System	31 Jan 2013 09:02:42.771 AM
<input checked="" type="checkbox"/> Informational	System	31 Jan 2013 09:01:00.297 AM

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

Delete Events

Choose which events you wish to delete

☒ Platform Events
☒ Audit events

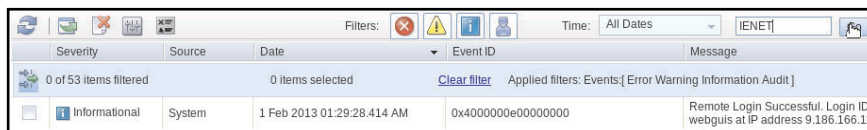
OK Cancel

Severity	Source	Date	Event ID	Message
0 of 52 items filtered				g Information Audit]
Informational	System	31 Jan 2013 09:02:42.771 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.186.166.119.
Informational	System	31 Jan 2013 09:01:00.297 AM	0x4000001600000000	Remote Login Successful. Login ID: USERID from webguis at IP address 9.111.29.57.
Informational	System	31 Jan 2013 09:00:58.957 AM	0x4000001900000000	ENET[CM.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@=9.0.1.148.50.

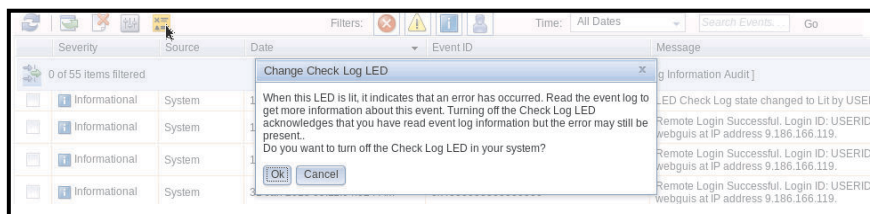
To select the type of event log entries that you want displayed, click the appropriate button (as shown in the following illustration).



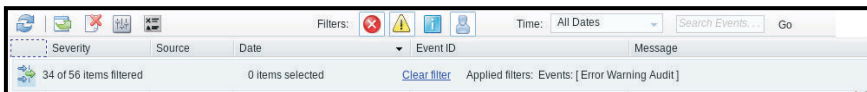
To search for specific types of events or keywords, type the type of event or keyword in the **Search Events** box; then, click **Go** (as shown in the following illustration).



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



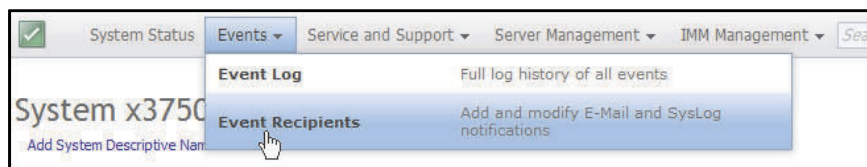
On the Event Log tool bar you can click any of the **Filter Events** buttons to select the events to be displayed. To clear the filter and show all types of events, click the **Clear Filter** link shown in the following illustration.



Event recipients

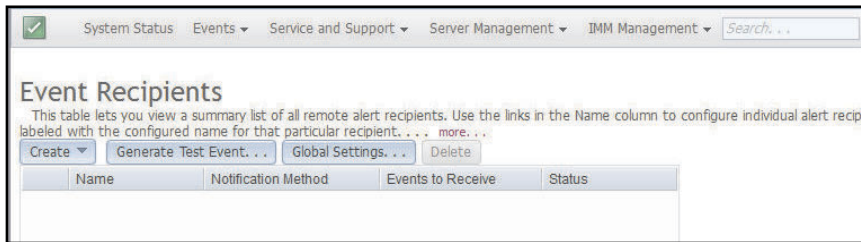
To add and modify email and syslog notifications, use the information in this topic.

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.



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.

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.

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:

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

<input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> Attention	<input checked="" type="checkbox"/> System
<input checked="" type="checkbox"/> Critical Temperature Threshold Exceeded	<input checked="" type="checkbox"/> Power redundancy warning	<input checked="" type="checkbox"/> Successful Remote Login
<input checked="" type="checkbox"/> Critical Voltage Threshold Exceeded	<input checked="" type="checkbox"/> Warning Temperature Threshold Exceeded	<input checked="" type="checkbox"/> Operating System Timeout
<input checked="" type="checkbox"/> Critical Power Failure	<input checked="" type="checkbox"/> Warning Voltage Threshold Exceeded	<input checked="" type="checkbox"/> All other informational/system events
<input checked="" type="checkbox"/> Hard Disk Drive Failure	<input checked="" type="checkbox"/> Warning Power Threshold Exceeded	<input checked="" type="checkbox"/> System Power On/Off
<input checked="" type="checkbox"/> Fan Failure	<input checked="" type="checkbox"/> Non-critical Fan events	<input checked="" type="checkbox"/> Operating System boot failure
<input checked="" type="checkbox"/> CPU Failure	<input checked="" type="checkbox"/> CPU in degraded state	<input checked="" type="checkbox"/> Operating System loader watchdog timed
<input checked="" type="checkbox"/> Memory Failure	<input checked="" type="checkbox"/> Memory Warning	<input checked="" type="checkbox"/> Predicted failure (PFA)
<input checked="" type="checkbox"/> Hardware Incompatibility	<input checked="" type="checkbox"/> All other attention events	<input checked="" type="checkbox"/> Event log 75% full
<input checked="" type="checkbox"/> Power redundancy failure		<input checked="" type="checkbox"/> Network change
<input checked="" type="checkbox"/> All other critical events		

☐ 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

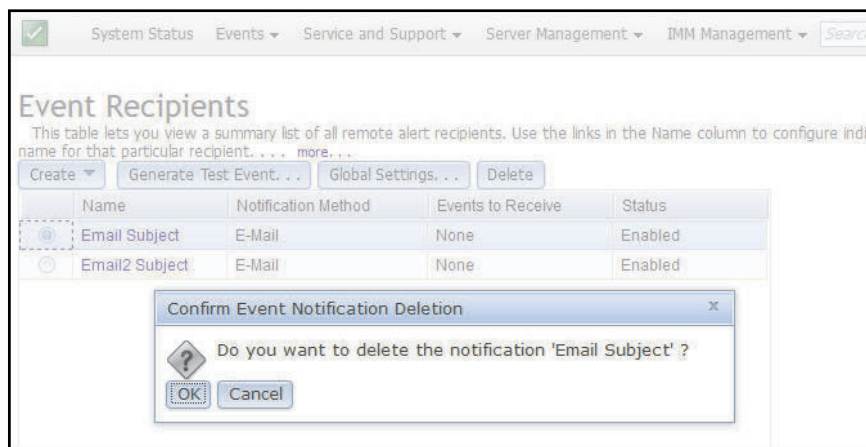
These settings will apply to all event notifications.

Retry limit:

Delay between entries (minutes):

Delay between attempts (minutes):

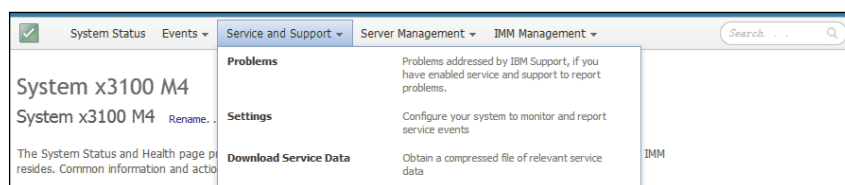
If you want to remove an email or syslog notification target, select the **Delete** button. The following window opens:



Service and Support tab

Use the information in this topic to understand and use the Problems, Settings and Download Service Data options.

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



Problems option

To view unresolved problems that are serviceable by the Support Center use the information in this topic.

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.

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

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 Support Center and File Transfer Server Export Ignored Problems Open Service Request Open Test Request Refresh

Corrected	Message	Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
<input type="checkbox"/> No	The connector Front Video has encountered a configuration error.	Error	Disabled	N/A	Disabled	25 Feb 2016, 02:38:54.000 AM	0x806f011b0701fff
<input type="checkbox"/> No	The Drive 2 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	29 Jan 2016, 06:08:39.000 AM	0x806f010d0402fff
<input type="checkbox"/> No	The Drive 1 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	29 Jan 2016, 06:08:31.000 AM	0x806f010d0401fff
<input type="checkbox"/> No	The Drive 3 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	22 Jan 2016, 05:42:04.000 AM	0x806f010d0403fff
<input type="checkbox"/> No	The Drive 4 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	22 Jan 2016, 05:20:27.000 AM	0x806f010d0404fff

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

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

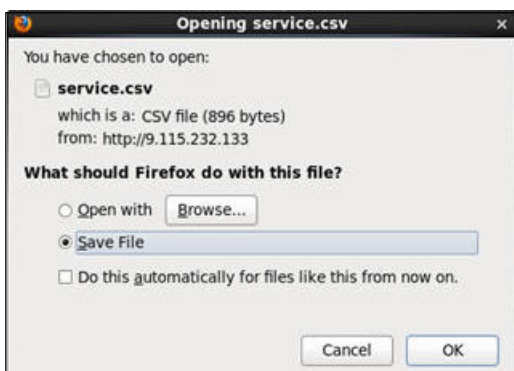
Service and Support is not yet enabled.

Display for: Both Support Center and File Transfer Server Export Ignored Problems Open Service Request Open Test Request Refresh

Both Support Center and File Transfer Server
Support Center Only
File Transfer Server Only

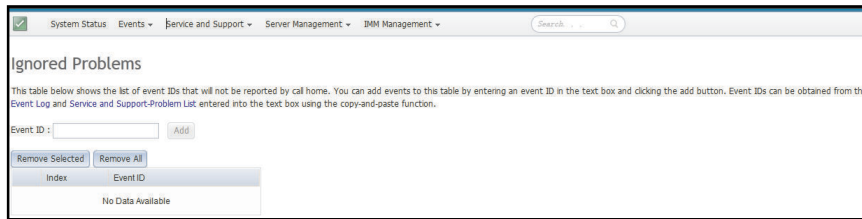
Corrected	Message	Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
<input type="checkbox"/> No	The Drive 1 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	29 Jan 2016, 06:08:39.000 AM	0x806f010d0402fff
<input type="checkbox"/> No	The Drive 3 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	29 Jan 2016, 06:08:31.000 AM	0x806f010d0401fff
<input type="checkbox"/> No	The Drive 3 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	22 Jan 2016, 05:42:04.000 AM	0x806f010d0403fff
<input type="checkbox"/> No	The Drive 4 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	22 Jan 2016, 05:20:27.000 AM	0x806f010d0404fff
<input type="checkbox"/> No	The Drive 4 has been disabled due to a detected fault.	Error	Disabled	N/A	Disabled	22 Jan 2016, 05:19:38.000 AM	0x806f010d0404fff

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

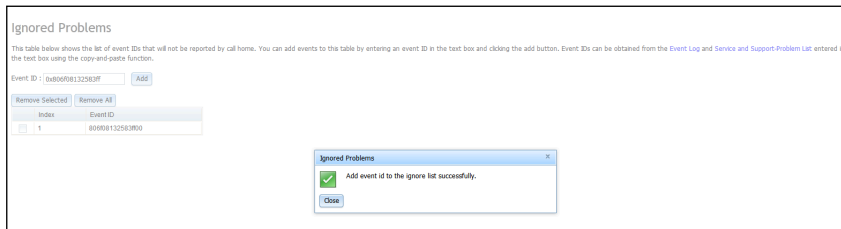


Click the **Ignore Problems** tab to display the list of event IDs that will not be reported by the *call home* feature. You can add event IDs to this list by entering an event ID in the **Event ID** field and clicking the **Add** button (as shown in the following illustration).

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



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

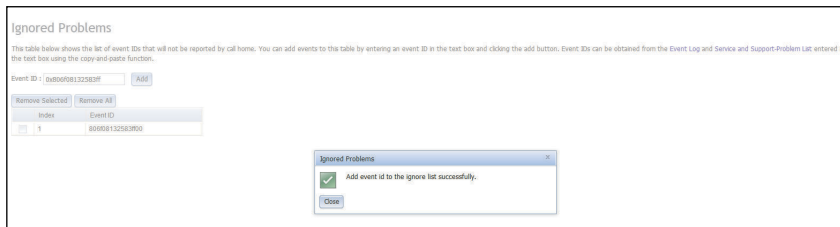


To remove an event ID from the Ignored Problems list, complete the following steps:

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

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

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



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



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



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

Click the **Open Test Request** tab to generate a test *call home* (call 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 Support Center and File Transfer Server								
Export Ignored Problems Open Service Request Open Test Request Refresh								
	Corrected	Message	Severity	Problem Status	Ticket Number	File Transfer Server	Event Date	Event ID
<input type="checkbox"/>	No	An Uncorrectable Bus Error has occurred on bus CPUs.	⚠ Error	Disabled	N/A	Disabled	11 Nov 2013, 09:43:54.000 PM	0x806f08132583fff
<input type="checkbox"/>	No	Fault in slot One of PCI's on system System x3750 M4.	⚠ Error	Disabled	N/A	Disabled	11 Nov 2013, 08:41:25.000 PM	0x806f002125820900
<input type="checkbox"/>	No	An Uncorrectable Bus Error has occurred on bus CPUs.	⚠ Error	Disabled	N/A	Disabled	11 Nov 2013, 08:37:50.000 PM	0x806f08132583fff
<input type="checkbox"/>	Yes	An Uncorrectable Bus Error has occurred on bus CPUs.	⚠ Error	Disabled	N/A	Disabled	28 Oct 2013, 08:28:12.000 PM	0x806f08132583fff
<input type="checkbox"/>	No	An Uncorrectable Bus Error has occurred on bus CPUs.	⚠ Error	Disabled	N/A	Disabled	23 Oct 2013, 07:47:31.000 PM	0x806f08132583fff

Settings option

To view, add, or change the service and support settings use the information in this topic.

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 (support center), make sure DNS settings are valid. The service center and contact information is required to enable support. To enable file transfer server, to input the server information correctly... more...

Service and Support is not yet enabled.

Support | File Transfer Server | HTTP Proxy

Enable Support Center

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

☐ **Enable Support Center.** Automatically send the service information to the support center.

Service Center

Country code:

Contact Information

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

Primary Contact	Alternate Contact (Optional)
Company name: <input type="text"/>	Contact name: <input type="text"/>
Contact name: <input type="text"/>	Telephone number: <input type="text"/> Extension: <input type="text"/>
Telephone number: <input type="text"/> Extension: <input type="text"/>	Contact Email address: <input type="text"/>
Contact Email address: <input type="text"/>	Machine Location Phone: <input type="text"/>
Address: <input type="text"/>	
City: <input type="text"/>	
State/Province: <input type="text"/>	
Postal code: <input type="text"/>	

Apply Support Center Settings | Reset

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

1. Click the **Support** tab.
2. Click the **Enable Support Center** checkbox.
3. From the **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/Province
 - Postal code
5. Click the **Apply Support Center Settings** button.

Support
File Transfer Server
HTTP Proxy

Enable Support Center

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

☒ **Enable Support Center.** Automatically send the service information to the support center.

Service Center

Country code:

US United States

Contact Information

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

Primary Contact

Company name:

Company

Contact name:

Contact

Telephone number:

000p00

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:

Apply Support Center Settings
Reset

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.

Support | **File Transfer Server** | HTTP Proxy

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. [less...](#)

☒ **Enable File Transfer Server**

Protocol:
FTP

IP address or host name: 9.115.232.123 Port: 21

User name:
USERID

Password:
••••••••

Apply File Transfer Server Settings Reset

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

Support | File Transfer Server | **HTTP Proxy**

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

Apply Reset

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.
 - a. In the **IP address or host name** field type the IP address or host name for the proxy server.
 - b. In the **Port** field enter the port for the proxy server.

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

4. Click the **Apply** button.

Preparing firewalls and proxies

To configure firewalls and proxies in your network use the information in this topic.

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

Four column table containing required internet connections used to configure firewalls and proxies.

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	80, 443	File upload for status reporting and problem reporting
www6.software.ibm.com	170.225.15.41	80, 443	File upload for status reporting and problem reporting. Proxy to testcase.boulder.ibm.com
www-945.ibm.com	129.42.26.224	80, 443	Problem reporting server v4
	129.42.42.224	80, 443	Problem reporting server v4
	129.42.50.224	80, 443	Problem reporting server v4

Table 3. Required internet connections (continued)

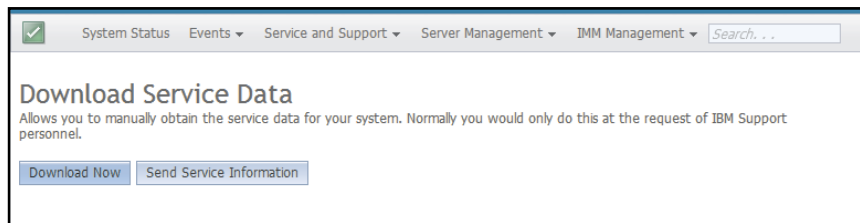
Host name	IP address	Port	Description
www.ibm.com	129.42.56.216	80, 443	Service provider file (CCF) download
	129.42.58.216	80, 443	Service provider file (CCF) download
	129.42.60.216	80, 443	Service provider file (CCF) download
www-03.ibm.com	204,146,30.17	80, 443	Service provider file (CCF) download

Download service data option

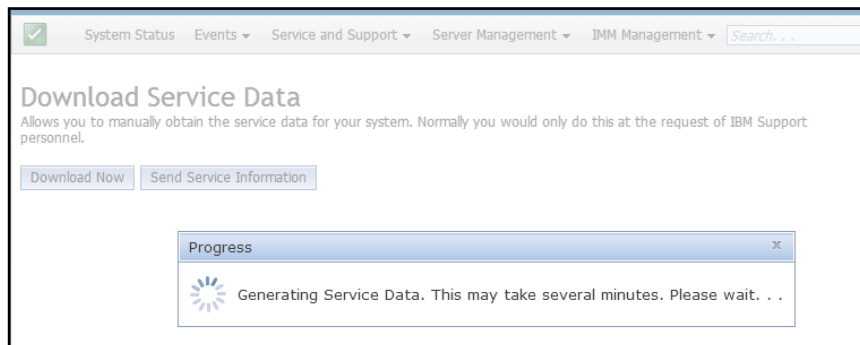
To download service and support data and create a compressed file about the server use this option.

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.

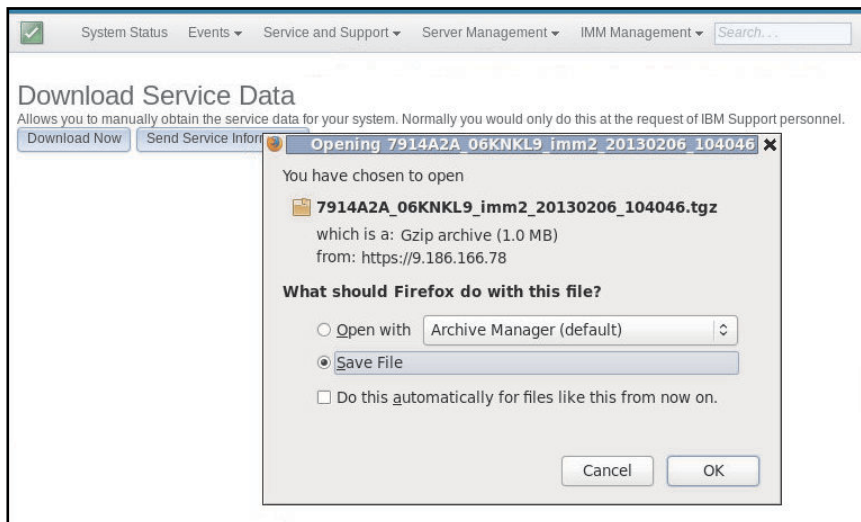
Click the **Download Now** button to download the service and support data (as shown in the following illustration).



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



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



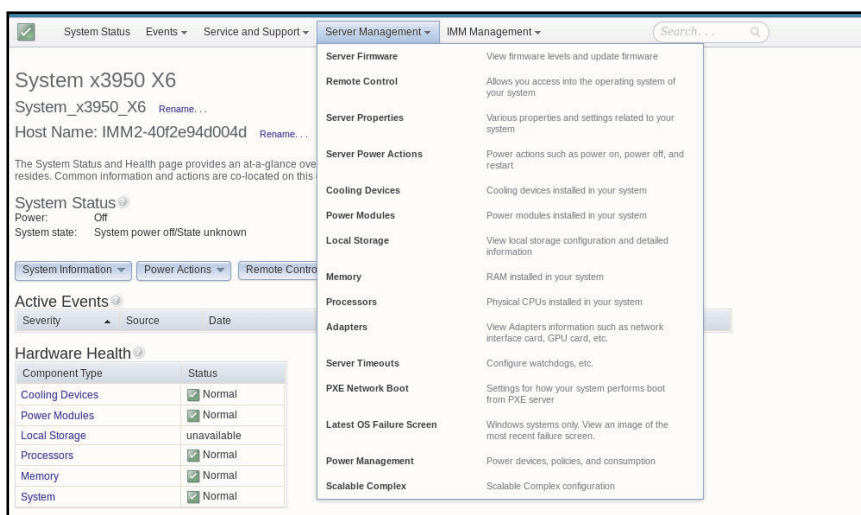
Server Management tab

To understand the options under the **Server Management** tab use the information in this topic.

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).

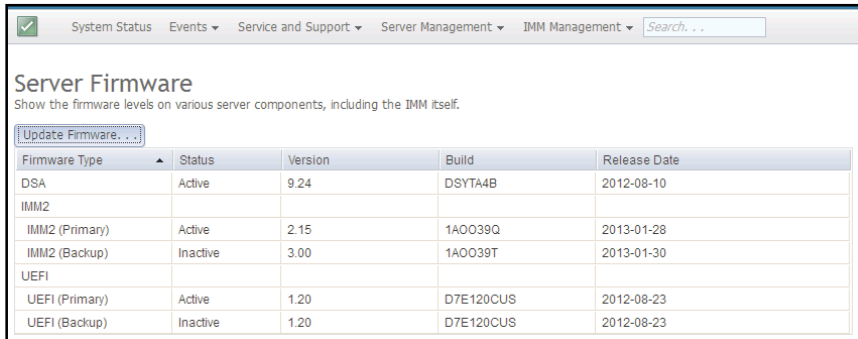
Important: Some options may not be available on your server's operating-system platform. Options that are displayed for the **Server Management** tab are contingent on the server's operating-system platform where the IMM2 is located and the adapters that are installed in the server.



Server firmware

To view the firmware levels and apply firmware updates use the information in this topic.

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



The screenshot shows the 'Server Firmware' section of a management console. It includes a navigation bar with tabs like 'System Status', 'Events', 'Service and Support', 'Server Management', and 'IMM Management'. Below the navigation bar, there's a title 'Server Firmware' and a description 'Show the firmware levels on various server components, including the IMM itself.' A button 'Update Firmware...' is visible. The main content is a table with columns: Firmware Type, Status, Version, Build, and Release Date. The table lists firmware for DSA, IMM2 (Primary and Backup), and UEFI (Primary and Backup).

Firmware Type	Status	Version	Build	Release Date
DSA	Active	9.24	DSYTA4B	2012-08-10
IMM2				
IMM2 (Primary)	Active	2.15	1A0O39Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	1A0O39T	2013-01-30
UEFI				
UEFI (Primary)	Active	1.20	D7E120CUS	2012-08-23
UEFI (Backup)	Inactive	1.20	D7E120CUS	2012-08-23

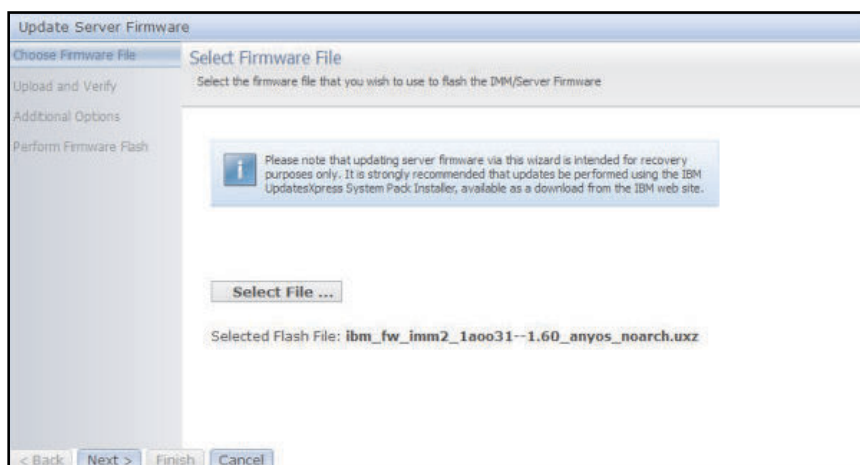
The current status and versions of firmware for the IMM2, UEFI, and DSA are displayed, including the primary and backup versions. There are three categories for the firmware status:

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

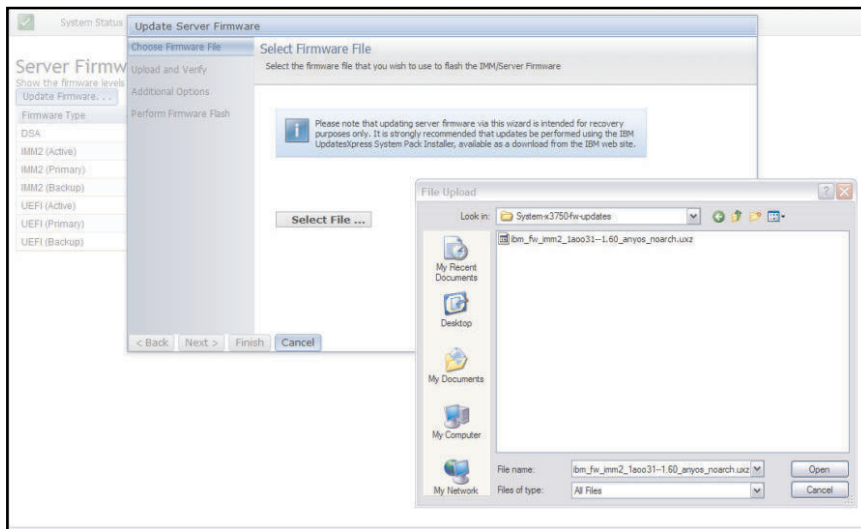
Attention: Installing the wrong firmware update might cause the server to malfunction. Before you install a firmware or device-driver update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure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

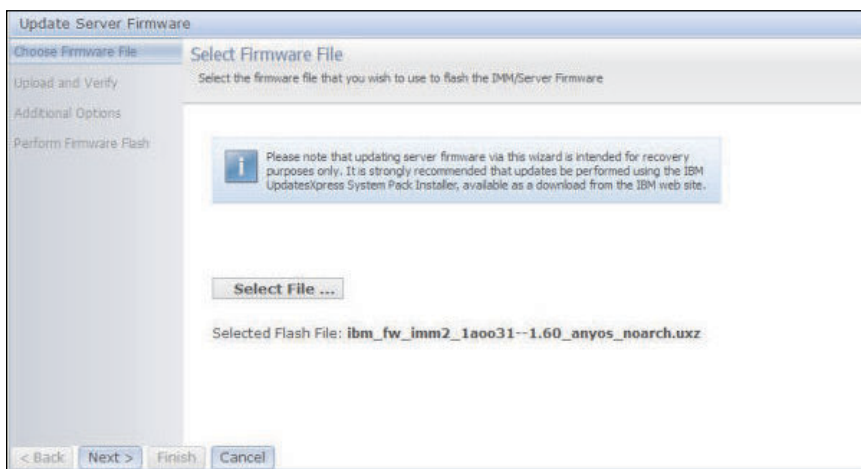
Note: Before you click on the **Select File...** button, read the warning displayed in the window prompt before you continue.



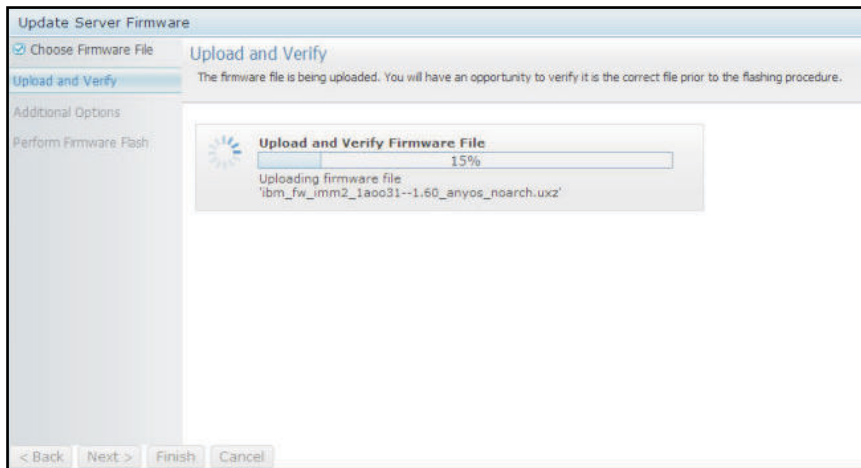
When you click the **Select File...** button, the File Upload window displays, which allows you to browse to the desired file.



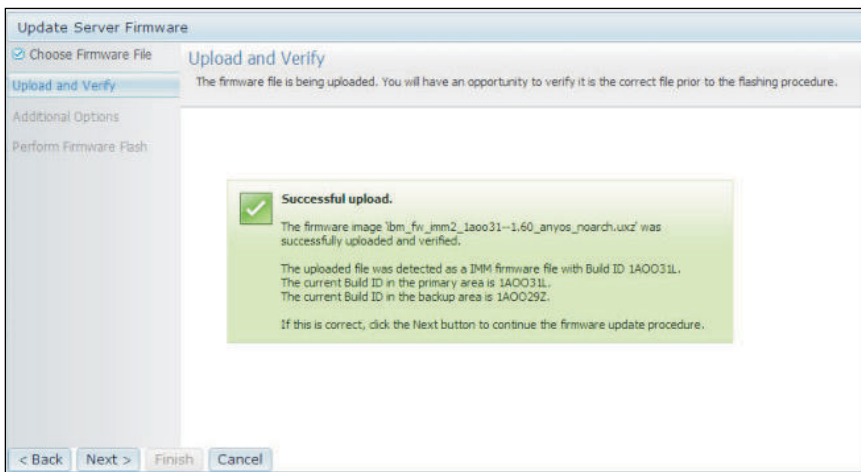
After you navigate to the file that you want to select, click the **Open** button, you are returned to the Update Server Firmware window with the selected file displayed (as shown in the following illustration).



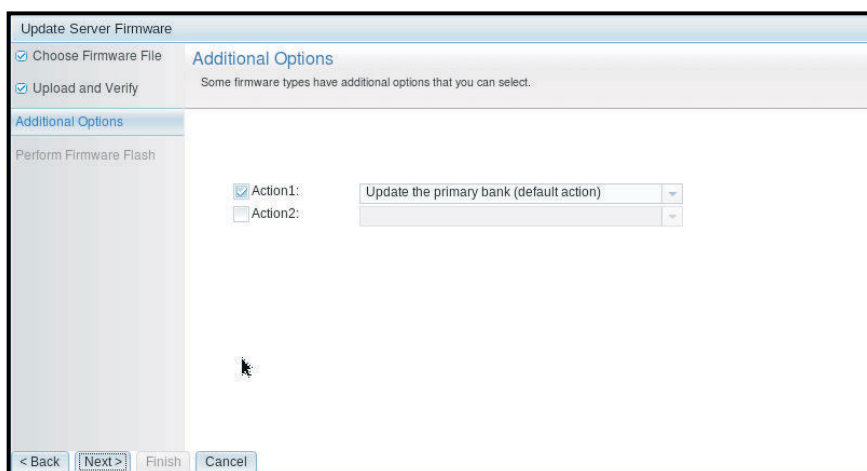
Click the **Next >** button to begin the upload and verify process on the selected file (as shown in the following illustration). A progress meter will be displayed as the file is being uploaded and verified.



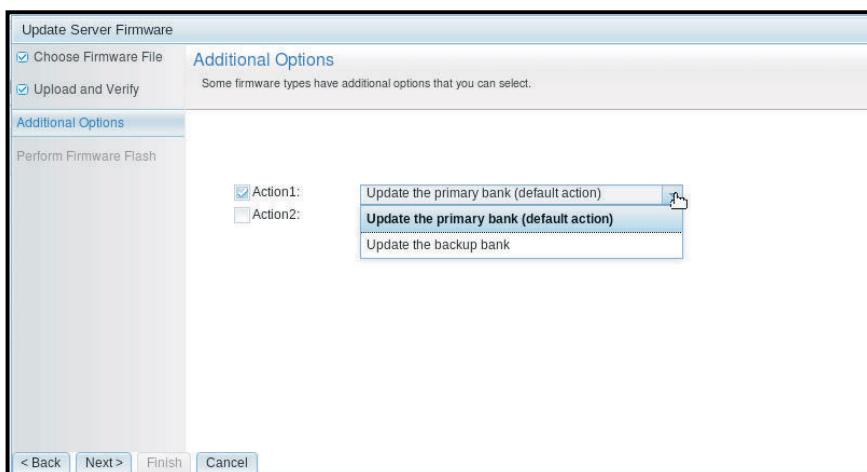
A status window opens (as shown in the following illustration) so you can verify that the file you selected to update is the correct file. The window will have information regarding the type of firmware file that is to be updated, such as DSA, IMM2, or UEFI. If the information is correct, click the **Next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



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



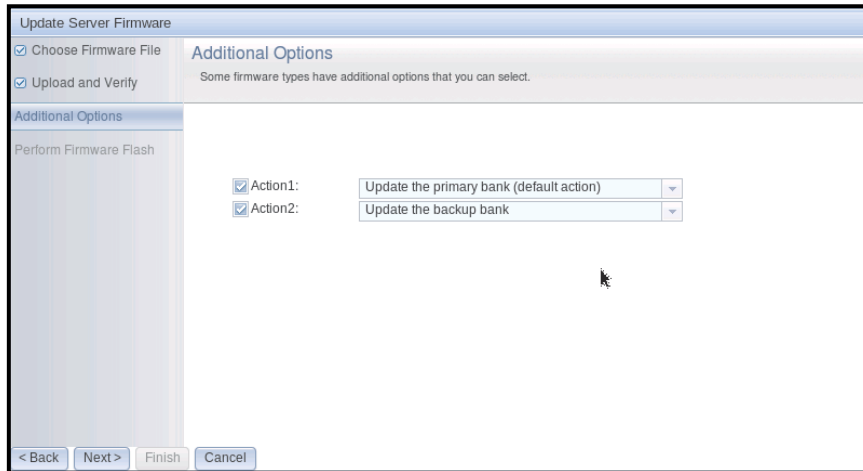
The drop-down menu beside **Action 1** (shown in the following illustration) gives you the choice to **Update the primary bank (default action)** or **Update the backup bank**.



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

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

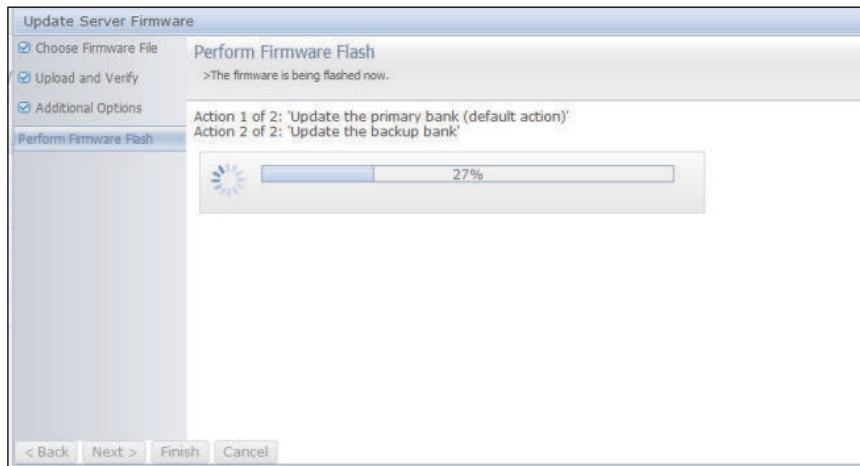
Note: To disable an action, click the checkbox beside the related action.



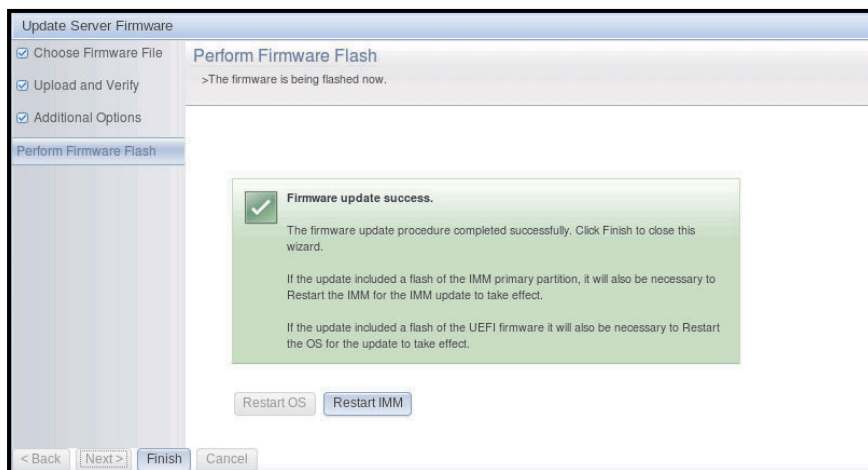
The previous screen shows that for Action 1, the primary bank is selected to be updated. You can also select to update the backup bank under Action 2 (as shown in the previous window). Both the primary bank and the backup bank will be updated at the same time when you click **Next >**.

Note: Action 1 must be different from Action 2.

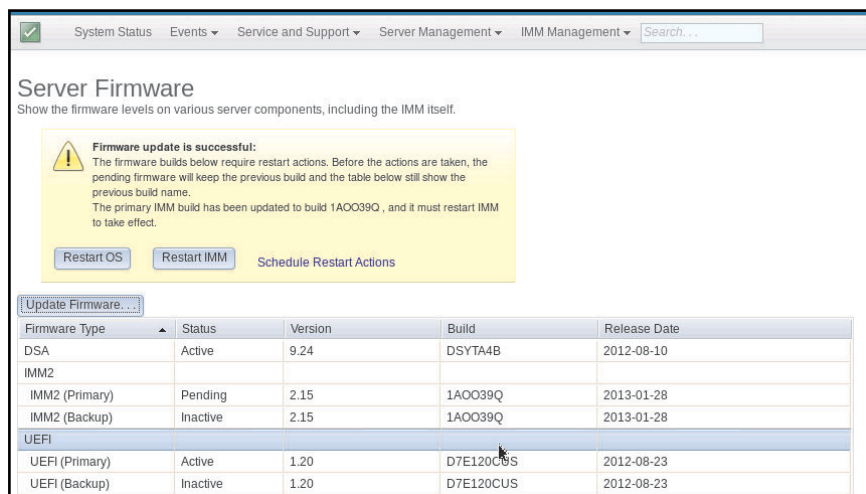
A progress meter is displayed that shows the progress of the firmware update (as shown in the following illustration).



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



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



Remote control

To understand and use the remote control feature refer to the information in this topic.

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.
- The Java client requires a minimum JAVA release level.
 - IMM2 firmware 1.00 through 1.51: JAVA 1.7 or newer is required.
 - IMM2 firmware 1.60 through 3.20: JAVA 1.8 or newer is required.
 - IMM2 firmware 3.50 through current firmware: JAVA 1.8 is required but the firmware does not prohibit operation with other JAVA versions.

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 11](#) 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 Virtual Media and Remote Console functionality. The Virtual Media functionality is launched from the Remote Console window, “Virtual Media” menu. (Note that the Virtual Media function does... more...)

[Guide for Virtual Media and Remote Console](#)

☐ Use the ActiveX Client

☒ Use the Java Client **Note:** In order to use the Remote Control java functions, Java Runtime Environment 1.8 or newer is required.

☒ Use the browser client

☒ Encrypt disk and KVM data during transmission

☒ 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.

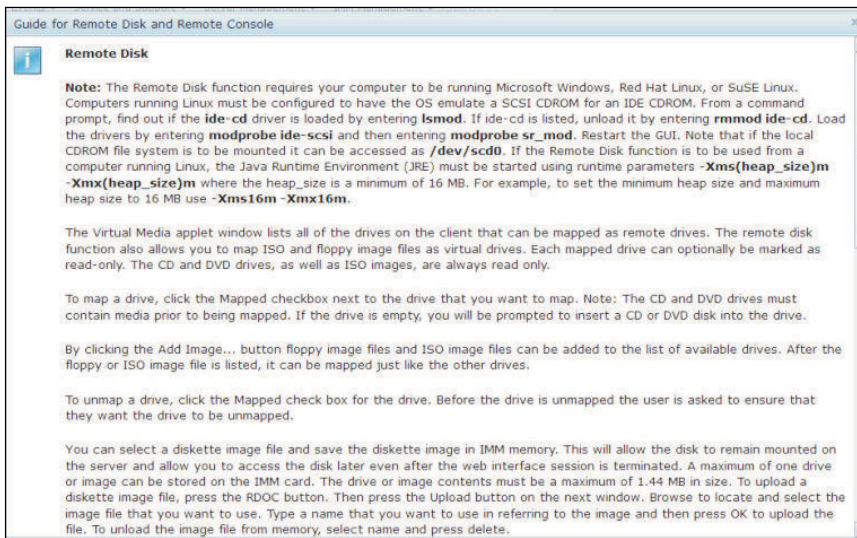
Start remote control in multi-user mode
Allows other users to start remote sessions while your session is active.

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.



- 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 Virtual Media and Remote Console functionality. The Virtual Media functionality is launched from the Remote Console window, "Virtual Media" menu. (Note that the Virtual Media function does... more...
[Guide for Virtual Media and Remote Console](#)

- ☐ Use the ActiveX Client
☐ Use the Java Client **Note:** In order to use the Remote Control java functions, Java Runtime Environment 1.8 or newer is required.
☒ Use the browser client

☒ Encrypt disk and KVM data during transmission

☒ 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.

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 system level. A new window will appear that provides access to the Virtual Media and Remote Console functionality. The Virtual Media functionality is launched from the Remote Console window, "Virtual Media" menu. (Note that the Virtual Media function does. . . [more. . .](#))
[Guide for Virtual Media and Remote Console](#)

☐ Use the ActiveX Client

☒ Use the Java Client **Note:** In order to use the Remote Control java functions, Java Runtime Environment 1.8 or newer is required.

☐ Use the browser client

☒ Encrypt disk and KVM data during transmission

☒ Allow others to request my remote session disconnect

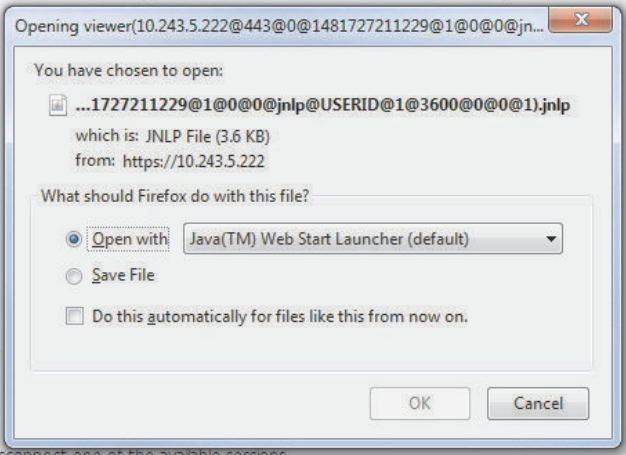
No response time interval: 1 hour

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

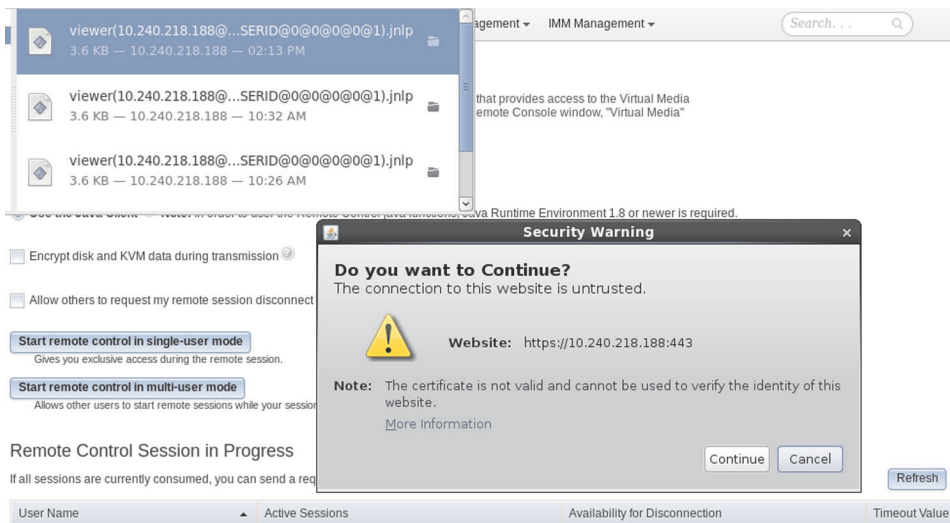
Start remote control in multi-user mode
Allows other users to start remote sessions while your session is active.

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
No active session is in progress.		



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 **Continue** to accept the certificate.

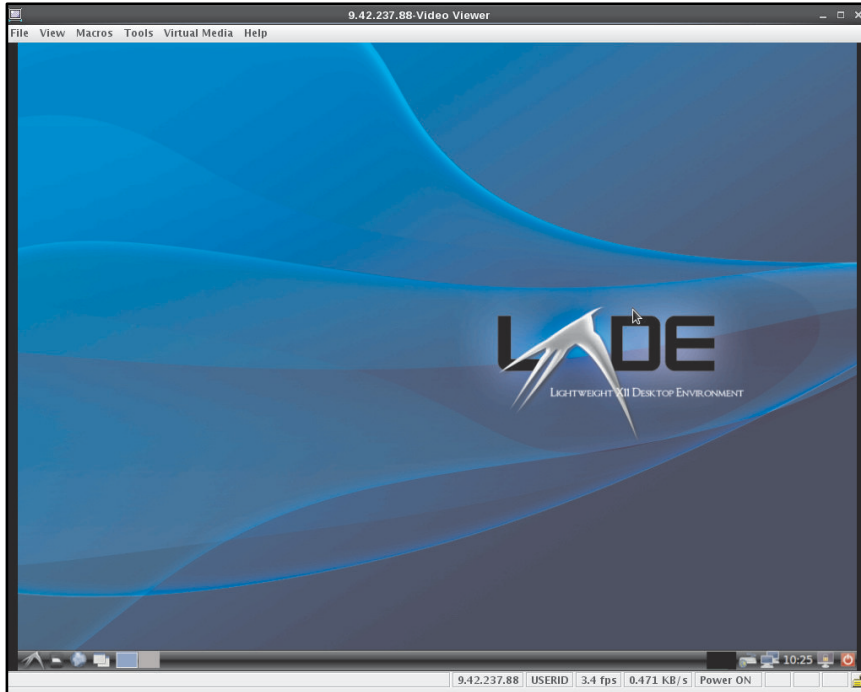


The screenshot shows the IMM Management web interface with a list of viewer sessions. A Security Warning dialog box is open, asking 'Do you want to Continue?' because the connection to the website is untrusted. The website is https://10.240.218.188:443. The dialog box also includes a 'Note' that the certificate is not valid and cannot be used to verify the identity of the website, and a 'More Information' link. The 'Continue' button is highlighted.

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.



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 153](#) 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.

HTML5 web browser support

To launch the web browser with HTML5 support, select **Use the browser client**.

- 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.

Remote Control

Allows you to control the server at the operating system level. A new window will appear that provides access to the Virtual Media and Remote Console functionality. The Virtual Media functionality is launched from the Remote Console window, "Virtual Media" menu. (Note that the Virtual Media function does. . . [more. . .](#)
[Guide for Virtual Media and Remote Console](#)

☐ Use the ActiveX Client

☐ Use the Java Client **Note:** In order to use the Remote Control java functions, Java Runtime Environment 1.8 or newer is required.

☒ Use the browser client

☐ Encrypt disk and KVM data during transmission

☒ Allow others to request my remote session disconnect

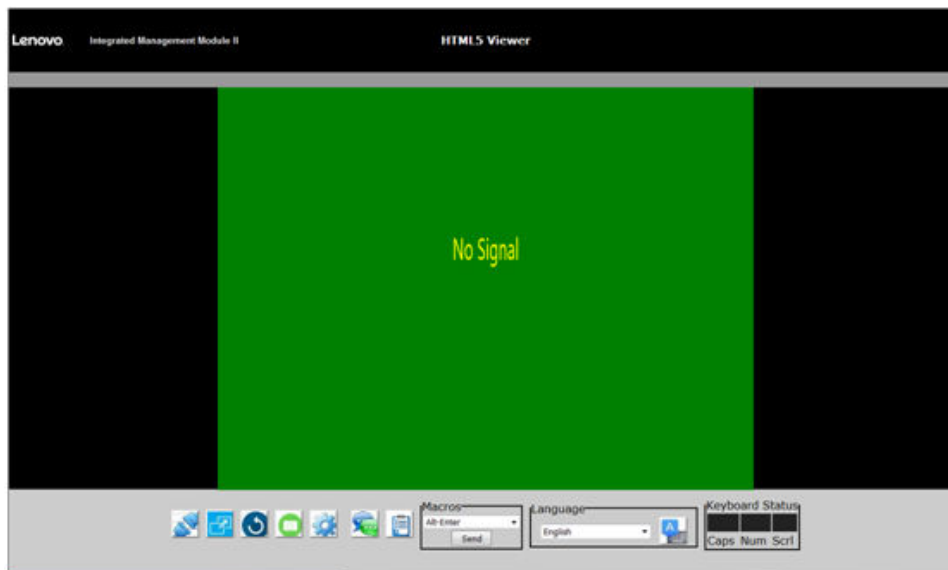
No response time interval: 1 hour

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.

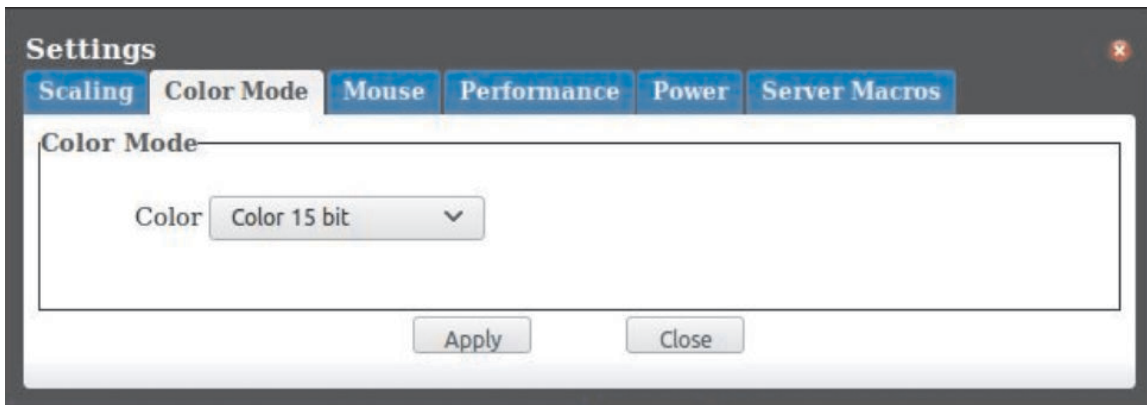
A HTML5 remote presence viewer will open (shown in the following illustration). The Video Viewer window provides access to the Remote Console functionality and is of some settings that you can configure.

Note: Most browsers block pop-up windows by default. If this occurs, disable the blocking function to launch the HTML5 remote presence viewer.

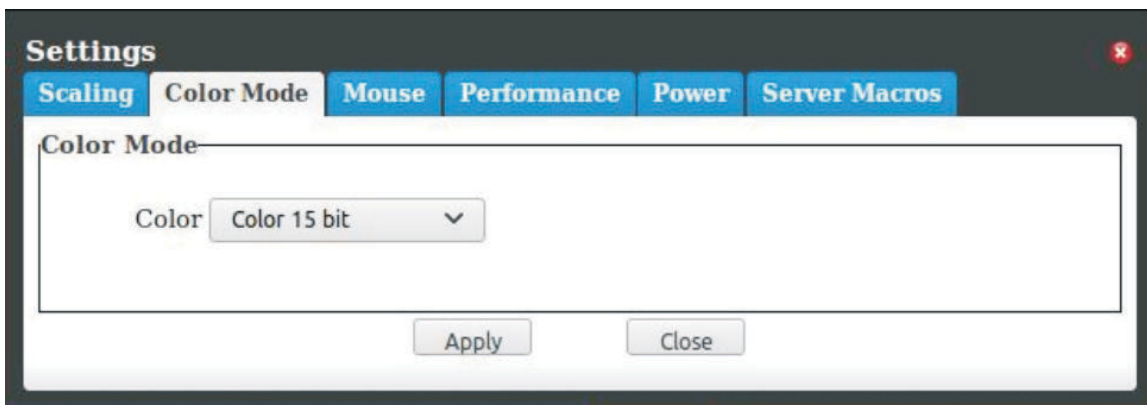


Below is a brief description of the icons displayed at the bottom in the remote presence viewer window starting from the left to the right:

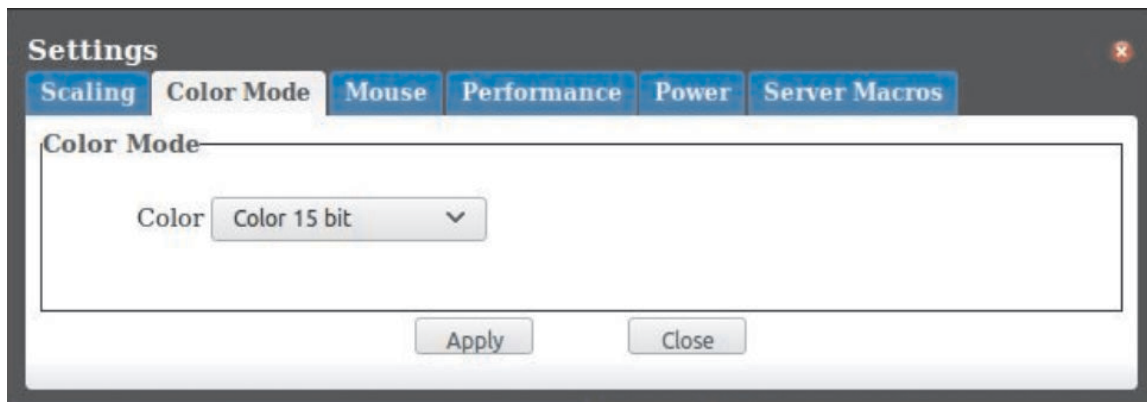
- **Disconnect:** Closes the remote presence viewer.
- **Refresh View:** Refreshes the content currently being displayed.
- **Screenshot Capture:** Saves the current screen view into a PNG file.
- **Settings**
 - **Scaling:** Select whether or not to maintain aspect ratio.



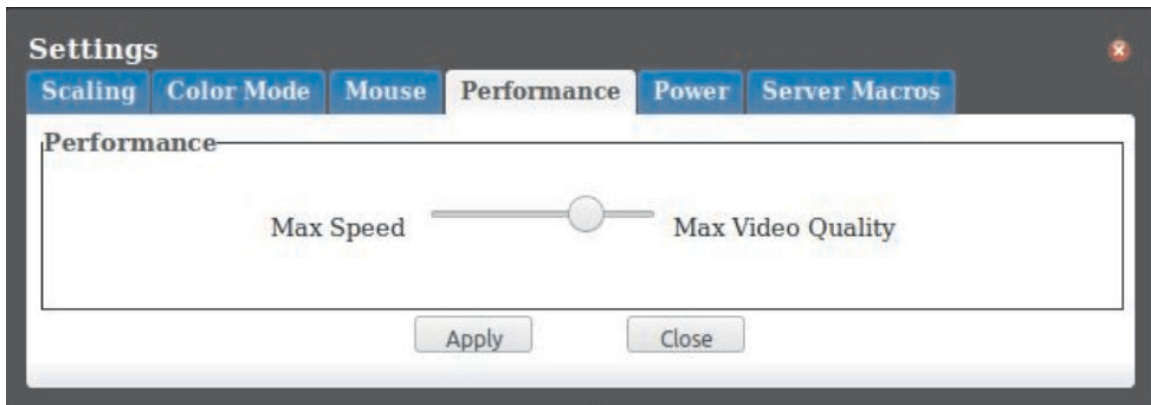
- **Color Mode:** Select the preferred color mode.



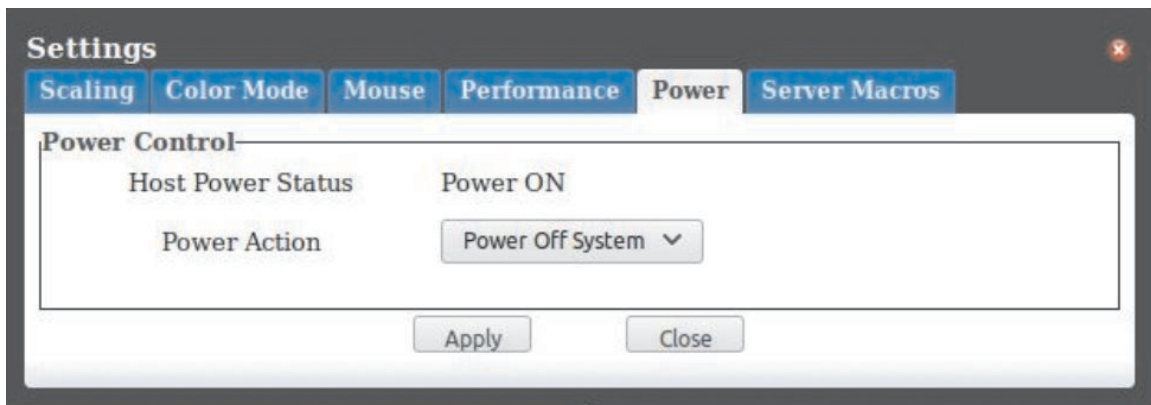
- **Mouse:** Select the preferred mouse acceleration setting.



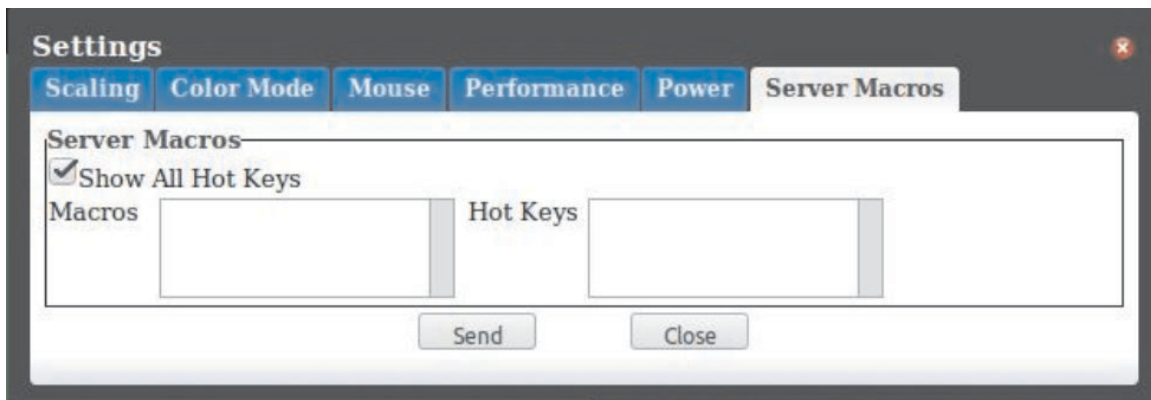
- **Performance:** Select the preferred performance and video quality.



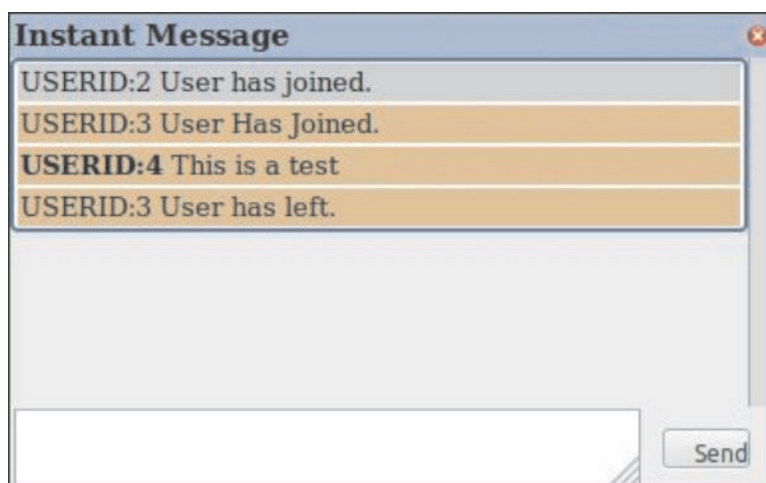
- **Power Option:** Select the preferred power-related settings.



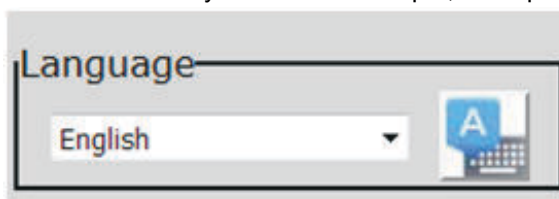
- **Server Macros:** Displays hot key macros assignments.



- **Chat instant message box:** Send messages between users that currently have a session opened to the same IMM2 management controller.



- **Remote video settings:** Displays the video inventory.
- **Language:** Selects the language for the virtual keyboard. For example, to display the English language



virtual keyboard, select **English**

; then, click the Virtual



Keyboard icon



Note: Remember to always first select the language before clicking the Virtual Keyboard icon. Otherwise, the intended language of the virtual keyboard may not be displayed.

For more information about the remote control feature, see [“Remote presence and remote control functions” on page 137](#).

Server properties

To set parameters to identify the system refer to the information in this topic.

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**.

The screenshot shows the 'Server Properties' page with the 'General Settings' tab selected. The page title is 'Server Properties' with a subtitle 'Various properties, status and settings related to your system.' Below the title are 'Apply' and 'Reset' buttons. The 'General Settings' section contains the following fields:

- System descriptive name:** A text input field.
- Contact person:** A text input field.
- Location (site, geographical coordinates, etc):** A text input field.
- Room ID:** A text input field.
- Rack ID:** A text input field.
- Lowest unit of system:** A dropdown menu currently showing 'N/A'.
- U height of system:** A text input field showing '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).

This screenshot shows the same 'Server Properties' page, but the 'Lowest unit of system' dropdown menu is expanded. The dropdown list contains the following items:

- N/A
- 1
- 2
- 3
- 4
- 5
- 6
- 7

The 'N/A' option is currently selected. The other fields remain the same as in the previous screenshot.

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.

Apply | Reset

General Settings | **LEDs** | Hardware Information | Environmentals | Hardware Activity

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	Description: If any FAN LED is, the fan has failed. Action: Reset fan(s) with it error LEDs. Replace indicated fan(s).
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	

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.

General Settings | LEDs | **Hardware Information** | Environmentals | Hardware Activity

Hardware Information

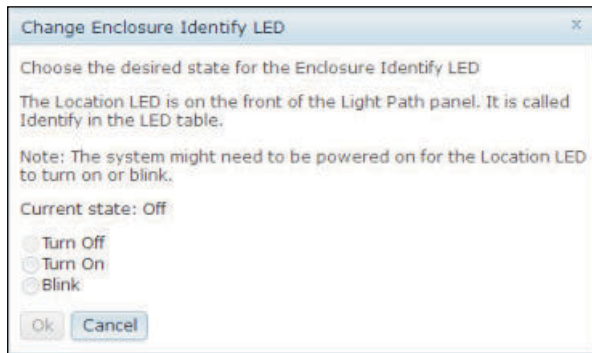
This section lists vital product data (VPD) on a system, component and network basis.

System Information | System Component Information | Network Hardware

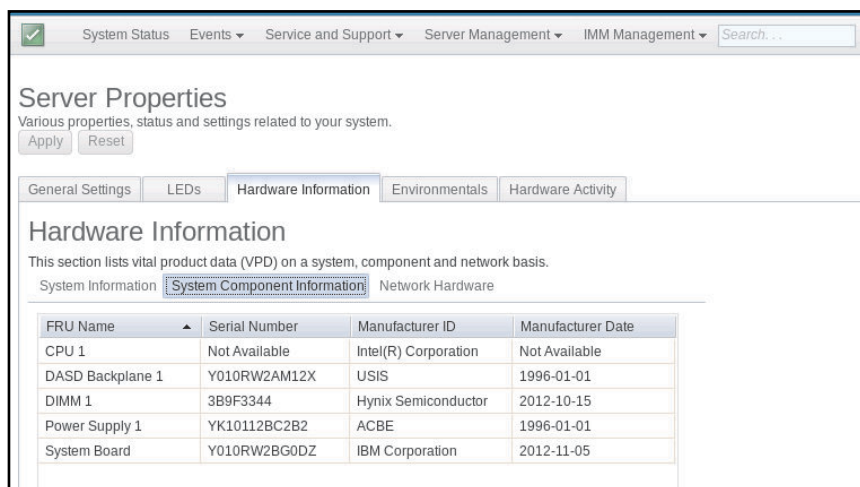
Name	Value
Machine Name	System x3550 M4
Machine Type-Model	7914A2A
Serial Number	06KNKL9
UUID	39B8A0803A7E11E284EF6CAE8B4E83C2
Server Power	On
Server State	OS booted
Total hours powered-on	1005
Restart count	29
Ambient Temperature	66.20 F / 19.00 C
Enclosure Identify LED	Off Change..
Check Log LED	Off

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.

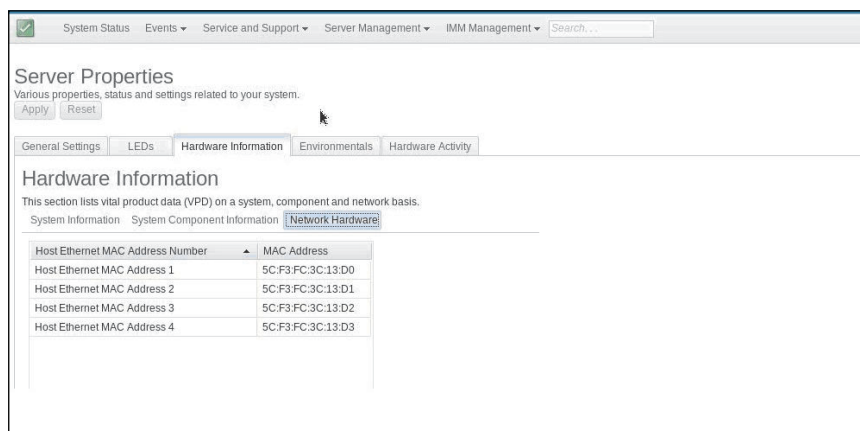
Note: The Enclosure Identity LED is on the front of the Light Path panel.



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.



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.



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. Some sensor values will show "N/A" if the sensors are not supported by the system. CPU temperature monitoring cannot be detected by unsupported systems.

Server Properties
Various properties, status and settings related to your system.
Apply Reset

General Settings LEDs Hardware Information **Environmentals** Hardware Activity

Environmental
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	3.29	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.
Apply Reset

General Settings LEDs Hardware Information Environmentals **Hardware Activity**

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

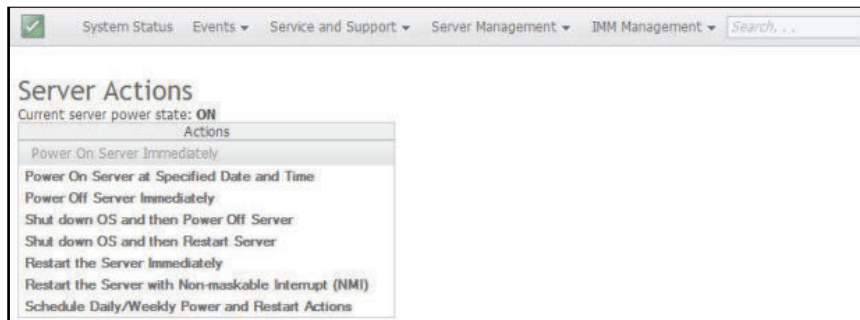
FRU Name	Serial Number	Manufacturer ID	Action	Time of Action
CPU/DIMM Tray	Y135BG1CG00R	CLCN	Added	19 Jul 2012 09:12 AM
Power Supply 1	K10511BE086	Delta	Added	19 Jul 2012 09:12 AM
Power Supply 2	K10511BE00F	Delta	Added	19 Jul 2012 09:12 AM
SAS Backplane 1	Y011US15G98C	MOLX	Added	19 Jul 2012 09:12 AM
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

To control the system power refer to the information in this topic.

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

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



You can choose to power the server on immediately or at a scheduled time. You can also choose to shut down and restart the operating system. For more information about controlling the server power, see, [“Controlling the power status of the server” on page 136](#).

Cooling devices

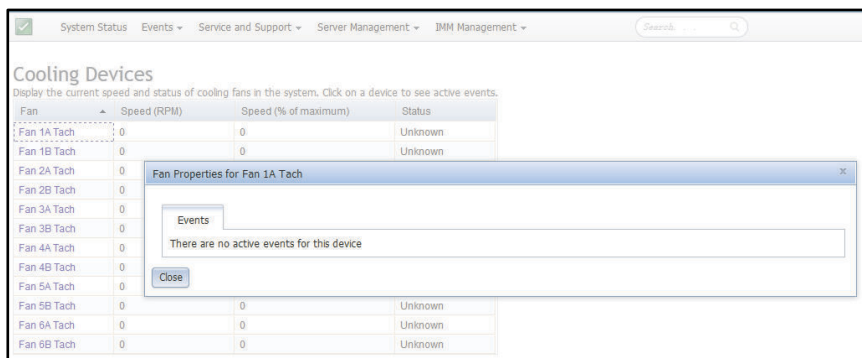
This topic describes how to view the status of the cooling fans in the server.

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.

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).

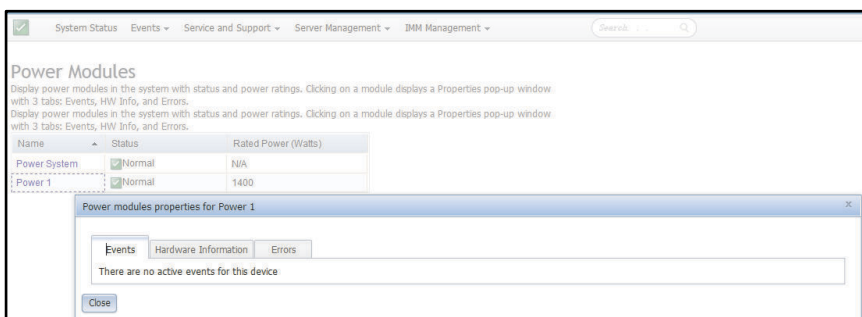


Power modules

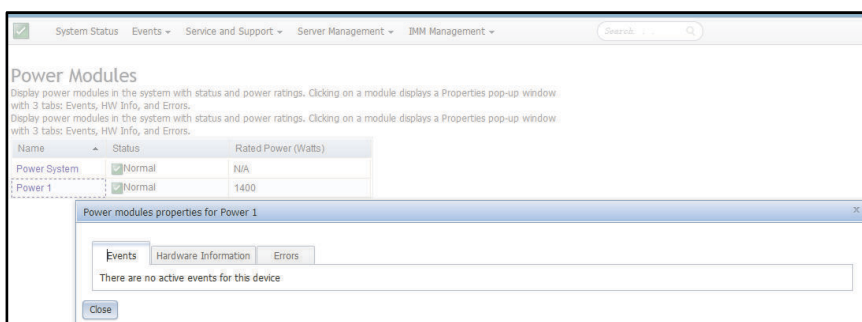
Use the information in this topic to view the power modules in the system.

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).

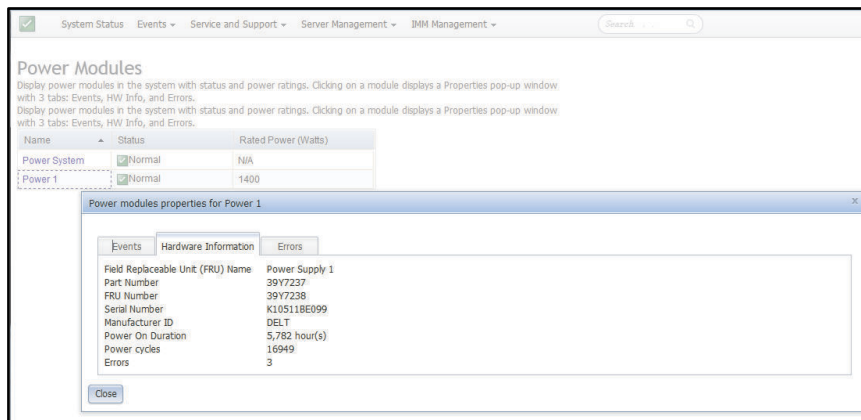
Note: In a Flex System, power module settings are managed by a Flex System CMM and cannot be modified on the IMM2.



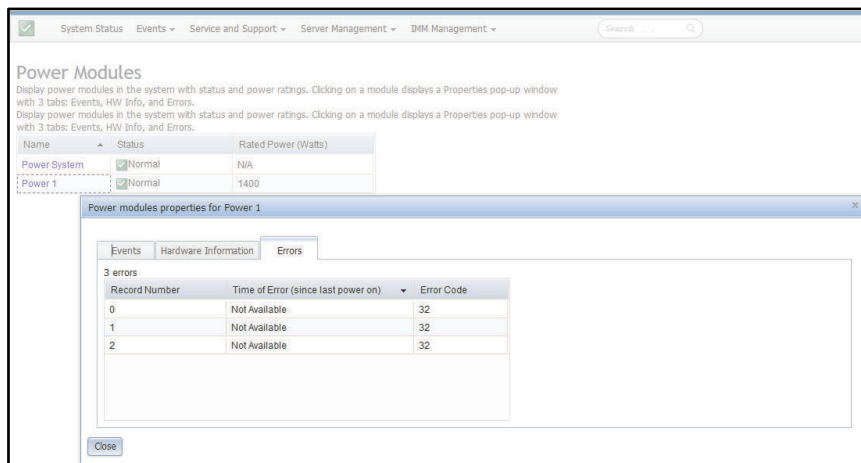
The **Events** tab displays active events, if any (as shown in the following screen).



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



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



Local storage

To understand how to view the local storage information use the information in this topic.

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.

[Refresh](#)

Physical Resource **Storage RAID Configuration** RAID Logs

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		

For System x server products that can display storage RAID, please refer to the below table.

Notes:

1. Please refer to the Installation and Service Guide of each server product regarding the slot limitation.
2. Remember to update the IMM firmware to the latest version. Older versions may not be able to display the storage RAID.

Model name	RAID cards that support displaying storage RAID
System x3100 M5 Type 5457	<ul style="list-style-type: none"> • M5110
System x3300 M4 Type 7382	<ul style="list-style-type: none"> • M5110
System x3500 M4 Type 7383	<ul style="list-style-type: none"> • M5110 • M5210
System x3530 M4 Type 7160	<ul style="list-style-type: none"> • M5110
System x3550 M4 Type 7914	<ul style="list-style-type: none"> • M5110 • M5210
System x3630 M4 Type 7158	<ul style="list-style-type: none"> • M5110
System x3650 M4 Type 7915	<ul style="list-style-type: none"> • M5110 • M5210 • M1215

Model name	RAID cards that support displaying storage RAID
System x3650 M4 HD Type 5460	<ul style="list-style-type: none"> • M5210 • M5210e • M1215
System x3650 M4 BD Type 5466	<ul style="list-style-type: none"> • M5110

For System x server products that can display and configure storage RAID, please refer to the below table.

Notes:

1. Please refer to the Installation and Service Guide of each server product regarding the slot limitation.
2. Remember to update the IMM firmware to the latest version. Older versions may not be able to display the storage RAID.

Model name	RAID cards that support displaying and configuring storage RAID
System x3500 M5 Type 5464	<ul style="list-style-type: none"> • M5210 • M1215 • M5225
System x3550 M5 Type 5463	<ul style="list-style-type: none"> • M5210 • M1215 • M5225
System x3650 M5 Type 5462	<ul style="list-style-type: none"> • M5210 • M1215 • M5225
System x3750 M4 Type 8752	<ul style="list-style-type: none"> • M5225 • M5210 • M1215 • M5210e • M5120
System x3750 M4 Type 8753	<ul style="list-style-type: none"> • M5210 • M1215 • M5210e • M5120

Model name	RAID cards that support displaying and configuring storage RAID
System x3850 X6 and x3950 X6 Type 6241	<ul style="list-style-type: none"> • M5225 • M5210 • M5120
System x3850 X6 and x3950 X6 Type 3837	<ul style="list-style-type: none"> • M5225 • M5210 • M5120

For Flex server products that can display and configure storage RAID, please refer to the below table.

Notes:

1. Please refer to the Installation and Service Guide of each server product regarding the slot limitation.
2. Remember to update the IMM firmware to the latest version. Older versions may not be able to display the storage RAID.

Model name	RAID cards that support displaying and configuring storage RAID
Flex System x240 M5	<ul style="list-style-type: none"> • M5115 • M1210e • M5215
IBM Flex System x240	<ul style="list-style-type: none"> • M5115 • Storage Enclosure Node
Flex System x880	<ul style="list-style-type: none"> • M5115 • M1210e

For NeXtScale server products that can display and configure storage RAID, please refer to the below table.

Notes:

1. Please refer to the Installation and Service Guide of each server product regarding the slot limitation.
2. Remember to update the IMM firmware to the latest version. Older versions may not be able to display the storage RAID.

Model name	RAID cards that support displaying and configuring storage RAID
NeXtScale nx360 M5	<ul style="list-style-type: none"> • M5210 • M1215

Memory

To view information about the memory modules use the information in this topic.

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.

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](#)

[DIMM 17](#)

[DIMM 18](#)

[DIMM 19](#)

[DIMM 20](#)

[DIMM 21](#)

Properties for DIMM 3

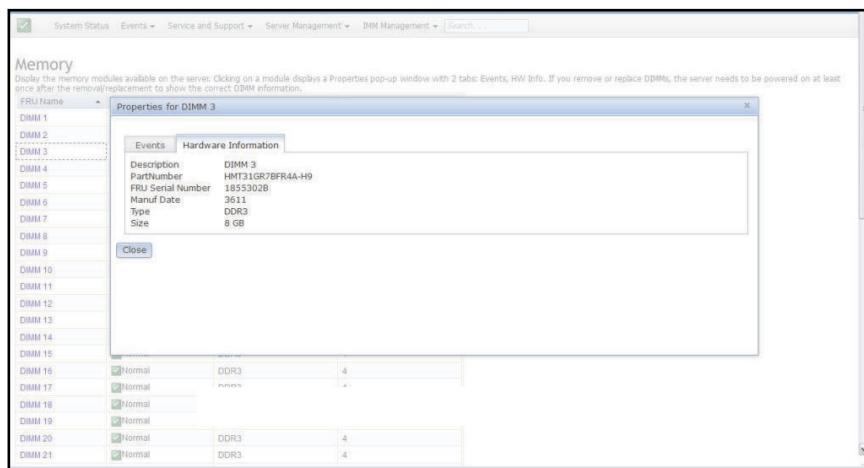
Events Hardware Information

There are no active events for this device.

Close

✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8
✓ Normal	DDR3	8

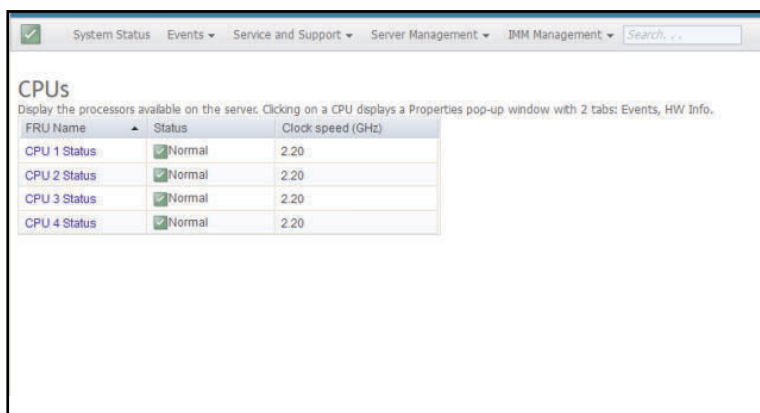
Click on the **Hardware Information** tab to view details about the component such as the description, part number, FRU serial number, manufacturing date (week/year), type (for example, DDR3), and size in gigabytes (as shown in the following illustration).



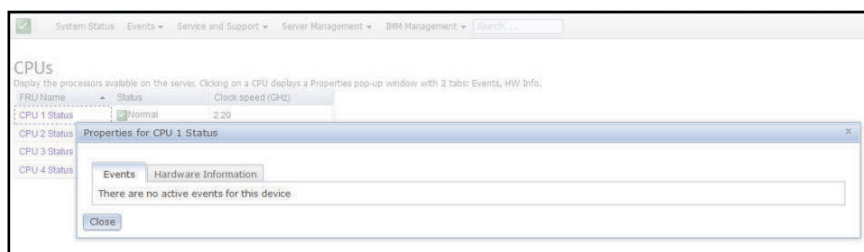
Processors

To view information about the microprocessors installed in the server use the information in this topic.

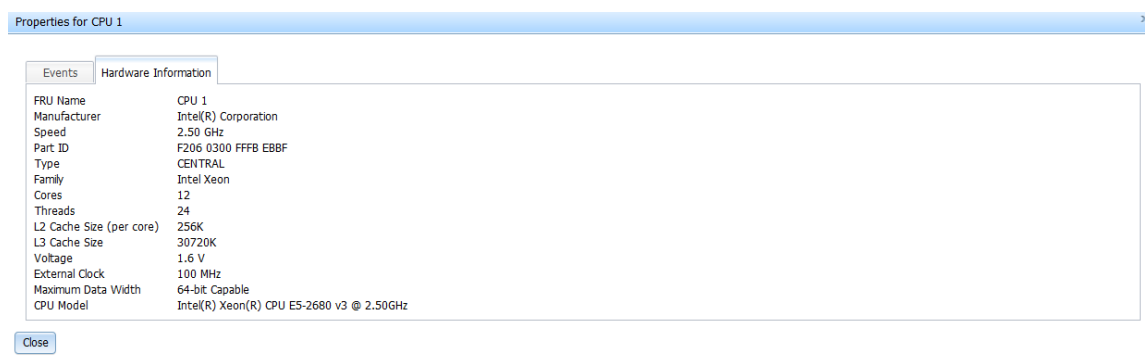
Select the **Processors** option under the **Server Management** tab to view information about the microprocessors that are installed in the system. The following window opens.



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



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



Adapters

To view information about the PCIe adapters installed in the server use the information in this topic.

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	

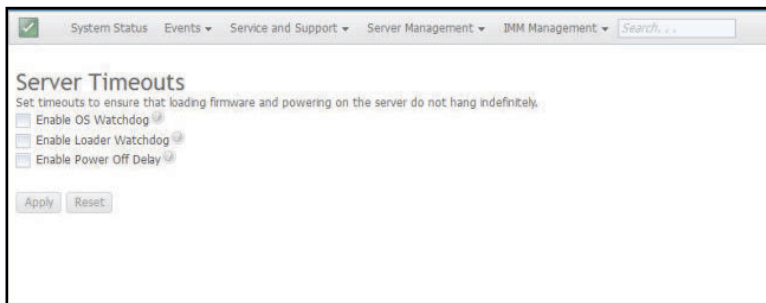
Server timeouts

To set timeouts for the server use the information in this topic.

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 101](#).

The following illustration shows the Server Timeouts window.



For additional information about server timeouts, see [“Setting server timeouts” on page 76](#).

PXE network boot

This topic contains information about the PXE Network Boot option.

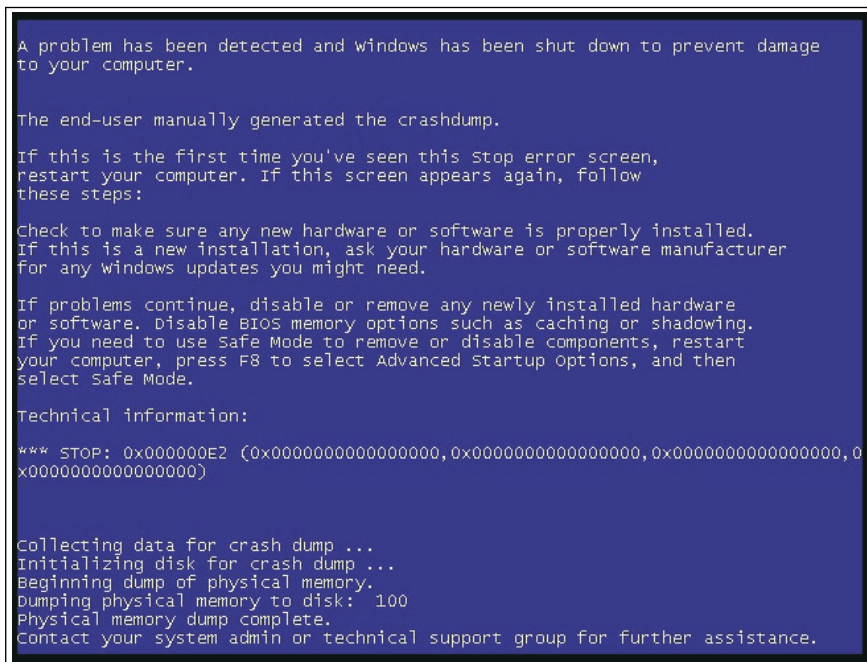
Select the **PXE Network Boot** option under the **Server Management** tab to set up your server to attempt a PXE network boot at the next server restart. For more information about setting up a PXE network boot, see [“Setting up PXE network boot” on page 157](#).

Latest OS failure screen

This topic contains information to help you understand the operating system failure screen data.

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

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



For more information about the Latest OS Failure Screen option, see [“Capturing the latest OS failure screen data” on page 172](#).

Power management

To perform power management functions and view power management information use the information in this topic.

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:

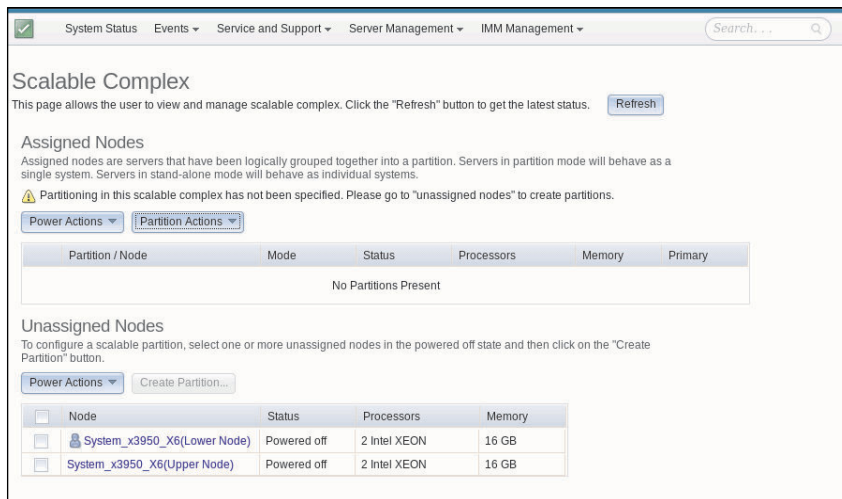
- Display information about installed power supplies.
- Control how the power supply "power" is managed.
- Control total system power.
- Display information about installed power supplies and current power supply capacity.
- Display the history of the amount of power used.

For more information about the **Power Management** option, see [“Managing the server power” on page 173](#).

Scalable complex

To understand a scalable complex refer to the information in this topic.

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 182](#). The following illustration shows the Scalable Complex window.



IMM Management tab

This topic contains information about the options under the **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 73](#).

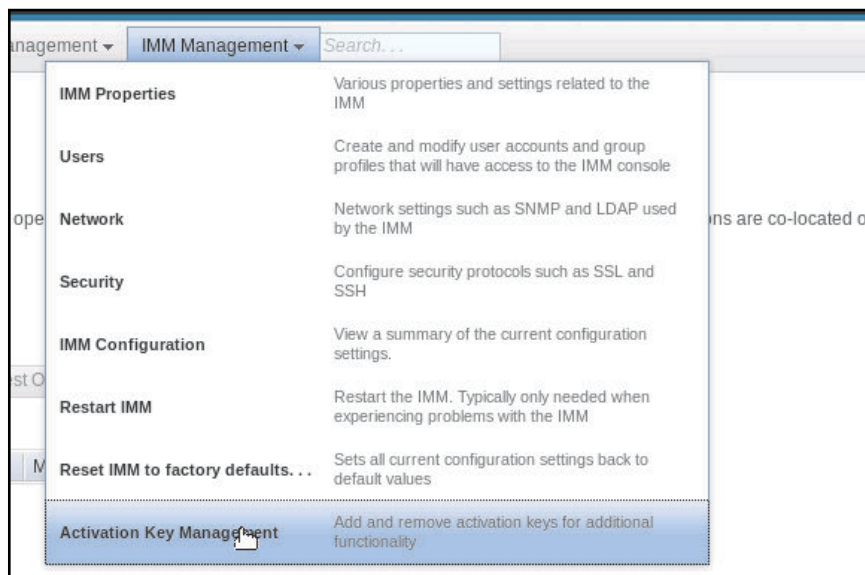
Chapter 4. Configuring the IMM2

Use the information in this section to understand the options available for IMM2 configuration.

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.



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 IPMI settings:
 - IPMI access enablement
- 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
- Configure Access Control:
 - Blocked IP address list enablement and configuration
 - Blocked MAC address list enablement and configuration
 - Restricted access interval enablement and configuration

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.

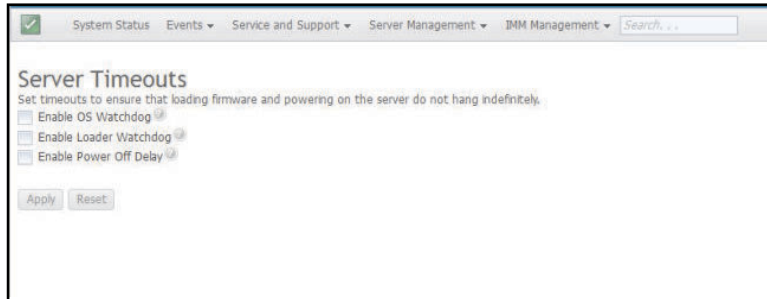
From the Activation Key Management page, you can manage activation keys for optional IMM2 and server Features on Demand (FoD). See [Chapter 7 “Features on Demand” on page 205](#) for information about managing FoD activation keys.

Setting server timeouts

Use the information in this topic to select a server timeout value.

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 101](#).



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 11](#)).
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.

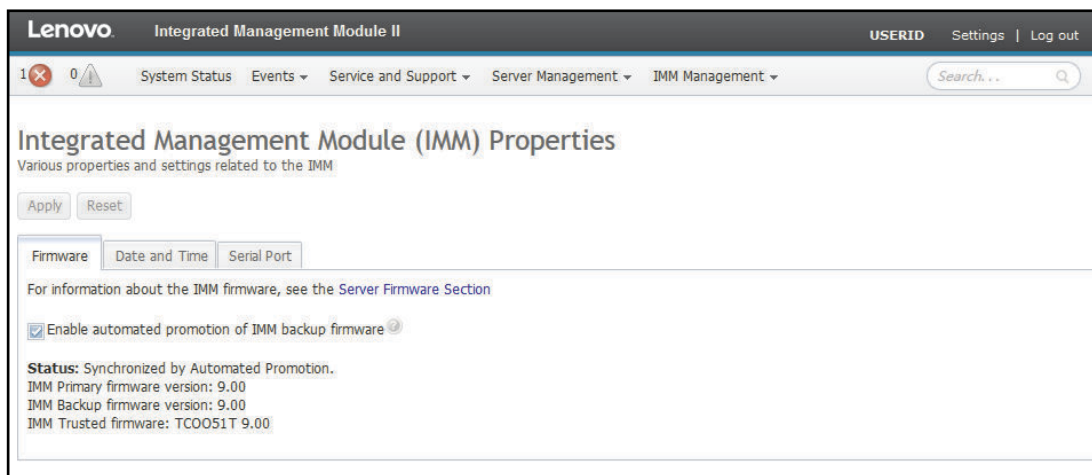
Changing the IMM2 firmware automated promotion settings

Use the information in this topic to understand and enable the automated promotion of IMM2 backup firmware.

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

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

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



Setting the IMM2 date and time

Use the information in this topic to understand IMM2 date and time settings. Instructions are provided to manually change the IMM2 date and time and to synchronize the IMM2 clock with the server clock.

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.

The screenshot shows the 'Integrated Management Module (IMM) Properties' window. The 'Date and Time' tab is selected. Under 'IMM Date and Time Settings', the 'Set Date and Time Manually' option is chosen from a dropdown. The 'Date' field is set to 7/20/2012, the 'Time' field is set to 8:43 AM, and the 'GMT Offset' dropdown is set to +0:00 - Greenwich Mean Time (Britain, Ireland, Portugal, Reykjavik (Iceland), Western Africa). The 'Automatically adjust for Daylight Savings Time (DST)' checkbox is unchecked.

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.

The screenshot shows the 'IMM Date and Time Settings' page. At the top, it says 'Indicate how the IMM Date and Time should be set. Choose a method from the pull-down list and supply appropriate settings.' Below this is a dropdown menu set to 'Synchronize with an NTP server'. The 'Time' is displayed as '2012/07/20 08:43 (NTP time)'. There are four input fields for 'NTP server host name or IP address (you can specify up to 4 addresses):', all containing '(not used)'. Below these is a 'Synchronization frequency (minutes)' spinner set to '1,440'. A checkbox 'Synchronize when these settings are saved' is checked. The 'GMT Offset' is set to '+0:00 - Greenwich Mean Time (Britain, Ireland, Portugal, Reykjavik (Iceland), Western Africa)'. At the bottom, a checkbox 'Automatically adjust for Daylight Savings Time (DST)' is also checked.

Configuring the serial port settings

Use the information in this topic to understand and specify serial port redirection 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

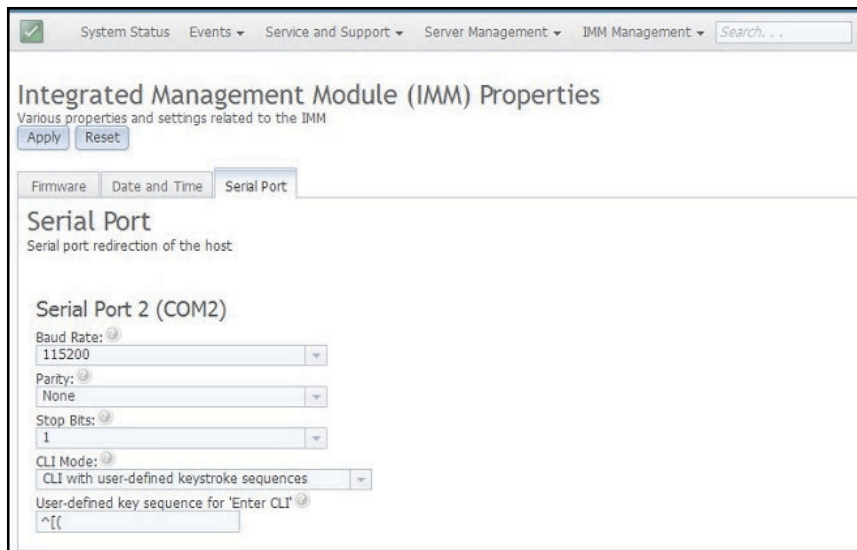
Specify the number of stop bits of your serial port connection in this field. Available options are 1 or 2.

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.



Configuring user accounts

Use the information in this topic to understand how user accounts are managed.

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.



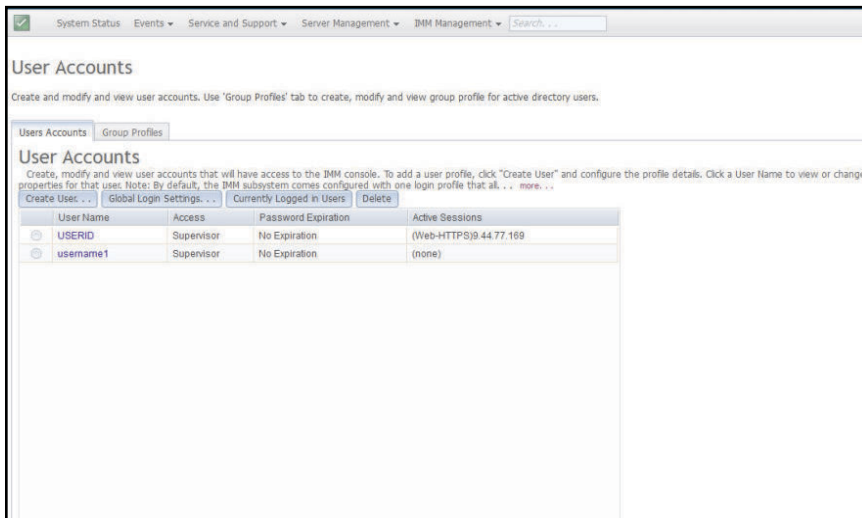
In a Flex System, the user accounts that are configured in the IMM2 settings only authenticate access to the IMM2 using IPMI and SNMPv3 protocols. If a user has configured the CMM to centrally manage the IPMI and SNMPv3 user accounts on the IMM2, you will not be able to configure the accounts directly 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

Use the information in this topic to create, modify, and view user accounts that have access to the IMM2 console.

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

Note: The IMM2 subsystem comes with one login profile.



Create user

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

User properties

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

The screenshot shows a 'User Properties' window with four tabs: 'User Credentials', 'Authority', 'SNMPv3', and 'SSH Client Public Key'. The 'User Credentials' tab is active. It features three input fields: 'User name:' containing 'USERID', 'Password:', and 'Confirm password:'. At the bottom, there are two checkboxes: 'User name rules:' with the text 'Cannot contain white space characters' and 'Password rules:' with the text '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 **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. **MD5** authentication is no longer an option due to security problem

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 **HMAC-SHA**. **Auth/NoPriv** is not an option

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).

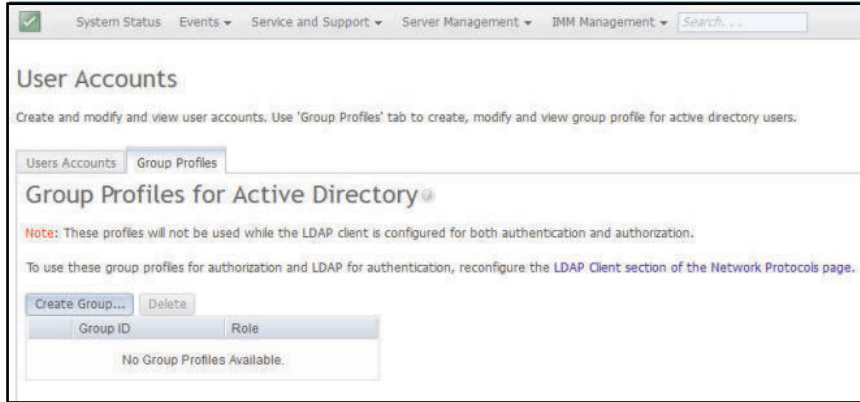
Hostname/IP address for traps

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).

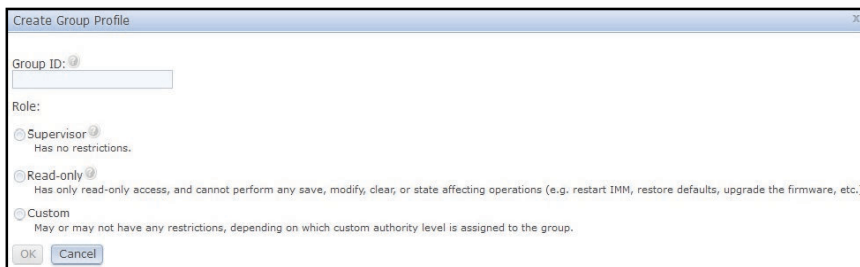
Group profiles

Use the information in this topic to establish, change, and view a group profile for active directory users.

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

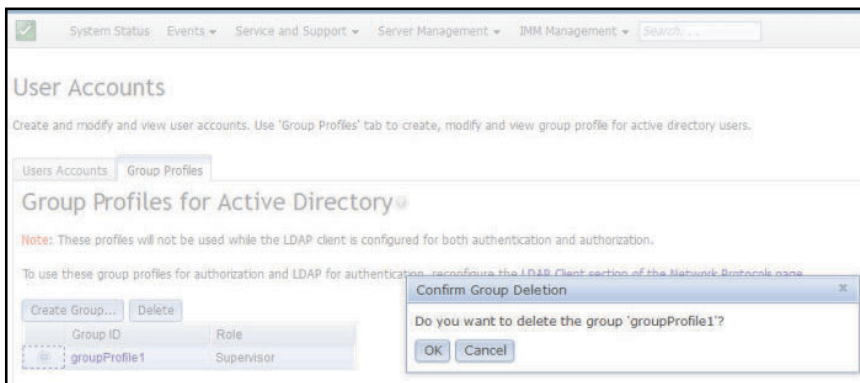


Click **Create Group** to create a new user group. The following illustration shows the Create Group Profile window.



Enter a **Group ID** and select the **Role**, (see [“User authority” on page 83](#) for information about the user authority levels).

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



Configuring global login settings

Use the information in this topic to establish user login settings.

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

General settings

Use the information in this topic to understand login attempt authentication and how to specify the wait time before disconnection of an inactive session.

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 user 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.

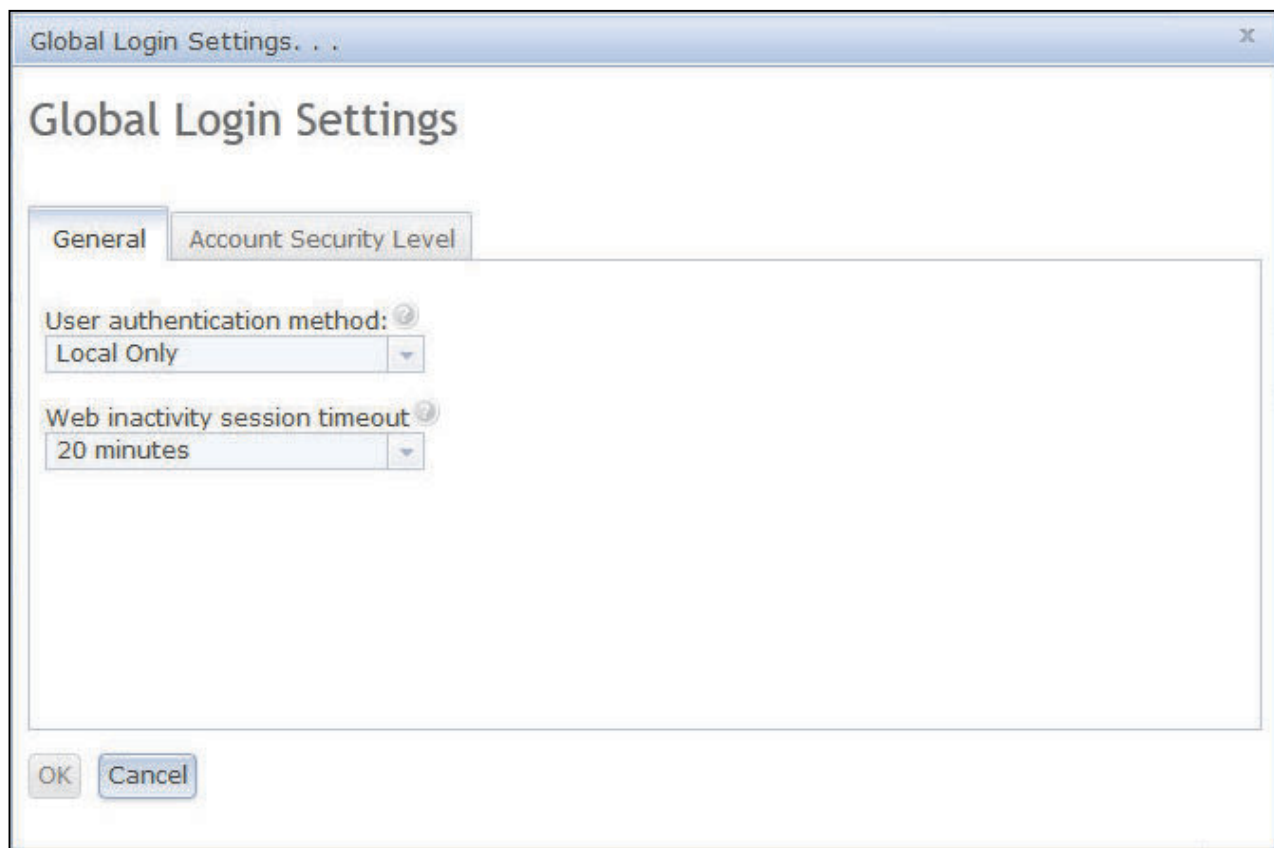
Notes:

- 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 users session. Users can choose whether or not to have the web page content automatically refreshed every 60 seconds. See [“Page auto refresh” on page 19](#) for additional information describing the auto refresh setting.

The **General** tab is shown in the following illustration.



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

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

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

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

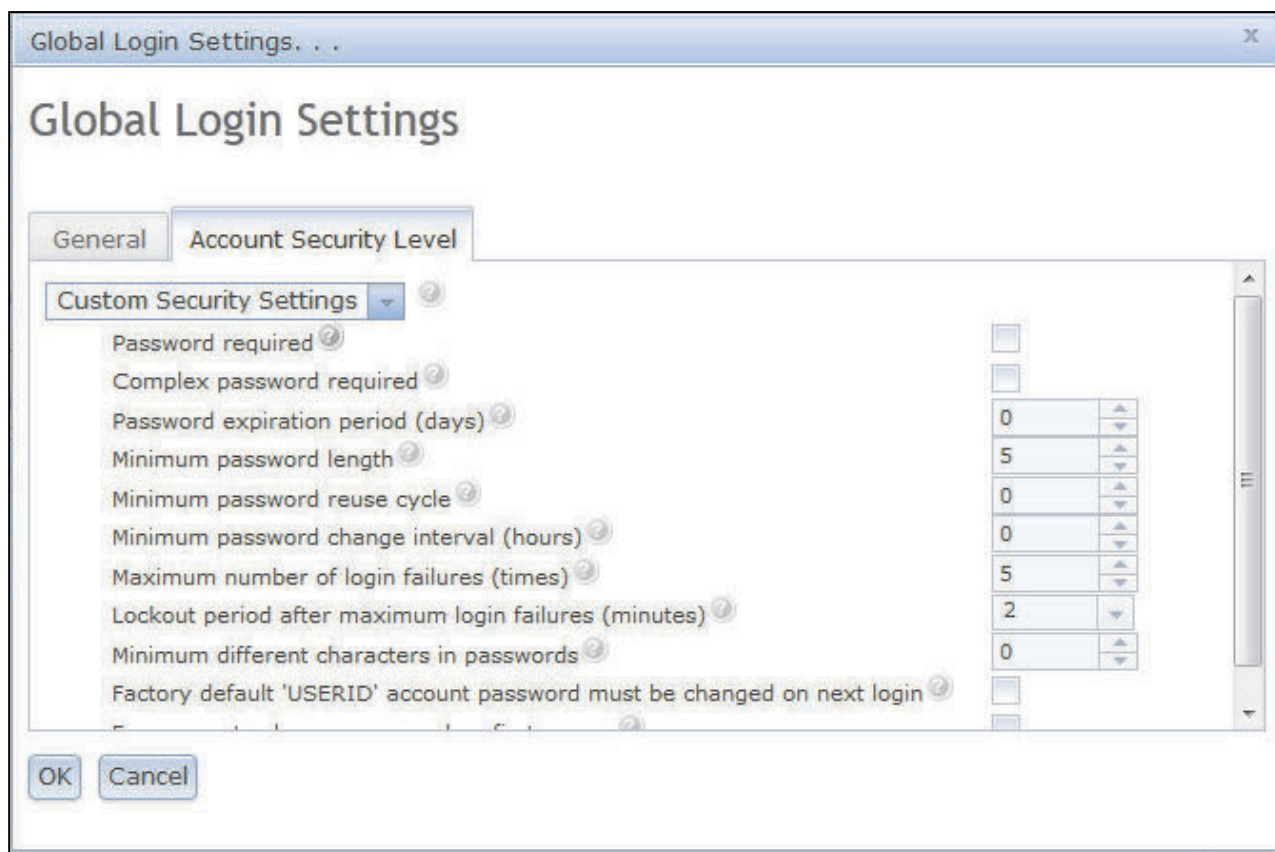
Account security policy settings

Use this information to understand and select the account security policy setting for your server.

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

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

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



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

Notes:

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

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

Table 4. Security setting policy values

Four column table containing the values for each level of the security settings.

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

Table 4. Security setting policy values (continued)

Policy setting/field	Legacy Security Settings	High Security Settings	Custom Security Settings
Maximum number of login failures (times)	5	5	0 10
Lockout period after maximum login failures (minutes)	2	60	0 240
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

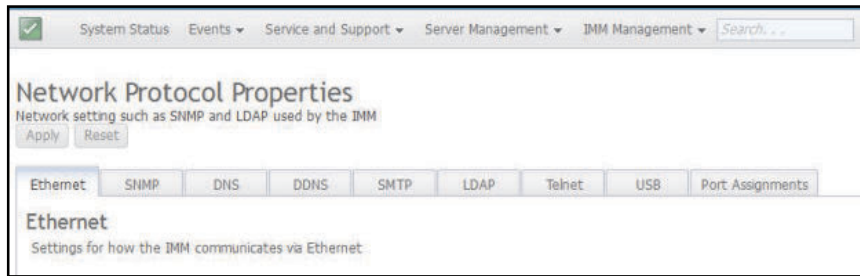
Use the information in this topic to view or establish network settings for the IMM2.

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

Configuring the Ethernet settings

Use the information in this topic to view or change how the IMM2 communicates by way of an Ethernet connection.

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



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

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

Note: Disabling the Ethernet interface prevents access to the IMM2 from the external network.

2. From the **Configure IP address settings** list, select one of the following options:

- Obtain an IP address from a DHCP server
- Use static IP address

3. If you want the IMM2 to default to a static IP address if unable to contact a DHCP server, select the corresponding check box.

4. In the **Static address** field, type the IP address of the IMM2.

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

5. In the **Subnet mask** field, type the subnet mask that is used by the IMM2.

Note: The subnet mask must contain four integers from 0 to 255 with no spaces or consecutive periods and separated by periods. The default setting is 255.255.255.0.

6. In the **Default Gateway** field, type your network gateway router.

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

The following illustration shows the **Ethernet** tab.

Ethernet Advanced Ethernet

Host name: IMM2-e41f13d90631

IPv4 IPv6

☒ 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 FFFFFFFF. 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.

The screenshot shows the 'Network Protocol Properties' window with the 'Ethernet' tab selected. The window title is 'Network Protocol Properties' with a subtitle 'Network setting such as SNMP and LDAP used by the IMM'. There are 'Apply' and 'Reset' buttons at the top. Below the tabs, the 'Ethernet' section is active, showing 'Settings for how the IMM communicates via Ethernet'. Under 'Ethernet', the 'Advanced Ethernet' sub-tab is selected. The configuration includes:

- ☒ Use Autonegotiation
- ☒ Enable VLAN, with a value of 4094.
- MAC selection: 'Use burned-in MAC address' (selected from a dropdown). Below it, the 'Burned-in MAC address' is 6c:ae:8b:4b:3d:ed.
- Maximum transmission unit (bytes): 1,500.

Configuring SNMP alert settings

Use the information in this topic to configure SNMP agents.

Complete the following steps to configure the IMM2 SNMP setting.

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

The screenshot shows the 'Network Protocol Properties' window with the 'SNMP' tab selected. The window title is 'Network Protocol Properties' with a subtitle 'Network setting such as SNMP and LDAP used by the IMM'. There are 'Apply' and 'Reset' buttons at the top. Below the tabs, the 'Simple Network Management Protocol (SNMP)' section is active, showing 'Configure SNMP v1 and/or v3 agents'. The configuration includes:

- ☐ 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.

The screenshot shows the 'Network Protocol Properties' window for the 'SNMP' tab. The 'Simple Network Management Protocol (SNMP)' section is active, showing options to 'Enable SNMPv1 Agent', 'Enable SNMPv3 Agent', and 'Enable SNMP Traps'. The 'Communities' tab is selected, displaying the 'SNMPv1 Communities' section. It instructs the user to 'Select communities to configure. At least one community must be configured.' There are three community configuration blocks. Community 1 is configured with 'Community name: pub_get', 'Access type: Get', and 'Allow any host to query MIB objects'. Community 2 is configured with 'Community name: pub_set', 'Access type: Set', and 'Allow any host to query MIB objects'. Community 3 is not configured. The 'Traps' tab is also visible, showing options to 'Accept IPv4 Hosts' and 'Accept IPv6 Hosts'.

Configuring DNS

Use the information in this topic to view or change IMM2 Domain Name System (DNS) settings.

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 DNS 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).

The screenshot shows the 'Network Protocol Properties' window with the 'DNS' tab selected. The window title bar includes 'System Status', 'Events', 'Service and Support', 'Server Management', and 'IMM Management'. Below the title bar, there's a search bar and a 'Reset' button. The 'DNS' tab is active, showing 'Domain Name System (DNS)' settings. A description states: '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.' Below this, a note explains that additional DNS servers are added to the top of the search list. The 'Preferred DNS address type' is set to 'IPv6'. The 'Use additional DNS address servers (at least one must be non-zero)' checkbox is checked. Below this, there are input fields for 'IPv4' and 'IPv6' addresses, each with 'Primary', 'Secondary', and 'Tertiary' rows. The IPv4 fields contain '0.0.0.0' and the IPv6 fields contain '::'.

Configuring DDNS

Use the information in this topic to enable or disable Dynamic Domain Name System (DDNS) protocol on the IMM2.

Click the **DDNS** tab to view or modify IMM2 DDNS 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).

The screenshot shows the 'Network Protocol Properties' window with the 'DDNS' tab selected. The window title bar is the same as the previous screenshot. Below the title bar, there's a search bar and a 'Reset' button. The 'DDNS' tab is active, showing 'Dynamic Domain Name Service (DDNS) Protocol' settings. A description states: 'Enable or disable Dynamic DNS on this IMM'. The 'Enable DDNS' checkbox is checked. Below this, there's a dropdown menu with three options: 'Use domain name obtained from the DHCP server', 'Use custom domain name', and 'Use domain name obtained from the DHCP server'. The first option is selected.

Configuring SMTP

Use the content in this topic to enter the information for a SMTP server.

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

IP address or host name

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

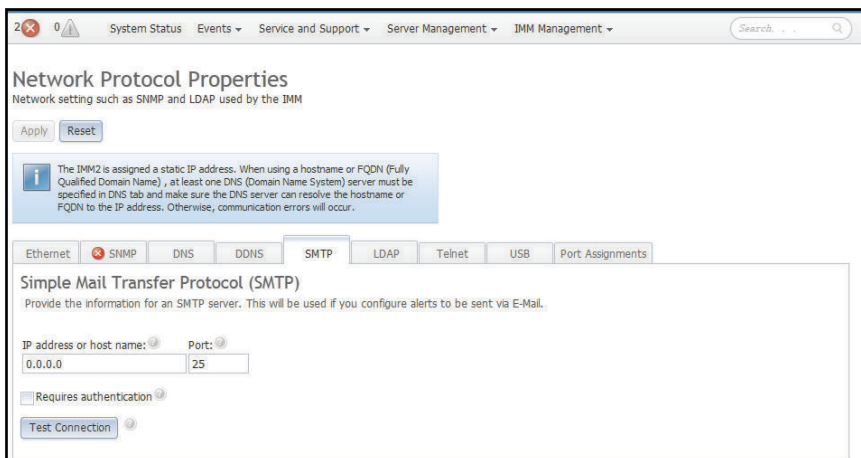
Port

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

Test connection

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

The following illustration shows the **SMTP** tab.



Configuring LDAP

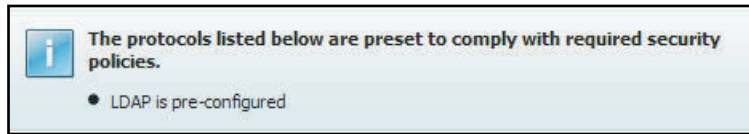
Use the information in this topic to view or change IMM2 LDAP settings.

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

Notes:

- The IMM2 LDAP implementation supports the following LDAP servers:
 - Microsoft Active Directory
 - Novell eDirectory Server
 - Open LDAP 2.1
- The IMM2 LDAP support includes:
 - Support for LDAP protocol version 3 (RFC-2251)
 - Support for the standard LDAP client APIs (RFC-1823)
 - Support for the standard LDAP search filter syntax (RFC-2254)
 - Support for Lightweight Directory Access Protocol (v3) Extension for Transport Layer Security (RFC-2830)

- 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).



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.

System Status Events Service and Support Server Management IMM Management Search

Network Protocol Properties

Network setting such as SNMP and LDAP used by the IMM

Apply Reset

Ethernet SNMP DNS DDNS SMTP **LDAP** Telnet USB Port Assignments

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 attributes:

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

Three column table containing bit position explanations.

Bit position	Function	Explanation
0	Deny Always	A user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
1	Supervisor Access	A user is given administrator privileges. The user has read/write access to every function. If you set this bit, you do not have to individually set the other bits.
2	Read Only Access	A user has read-only access, and cannot perform any maintenance procedures (for example, restart, remote actions, or firmware updates) or make modifications (for example, the save, clear, or restore functions. Bit position 2 and all other bits are mutually exclusive, with bit position 2 having the lowest precedence. When any other bit is set, this bit will be ignored.
3	Networking and Security	A user can modify the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port configurations.
4	User Account Management	A user can add, modify, or delete users and change the Global Login Settings in the Login Profiles window.

Table 5. Permission bits (continued)

Bit position	Function	Explanation
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.
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

Use the information in this topic to control telnet access to the IMM2.

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

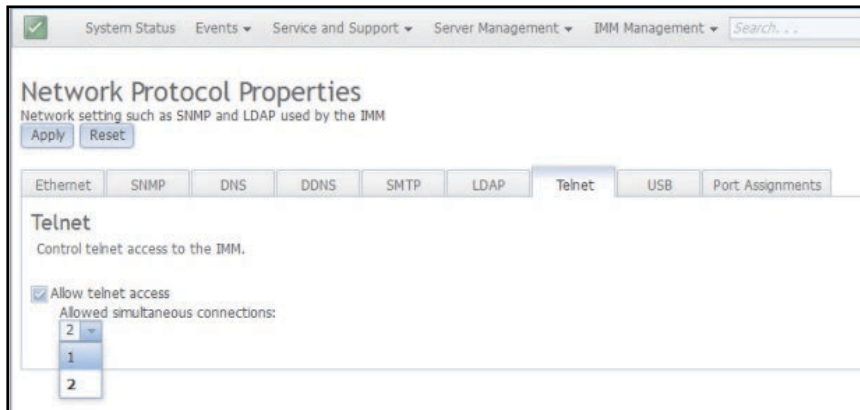
Allow telnet access

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

Allowed simultaneous connections

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

The following illustration shows the **Telnet** tab.



Configuring USB

Use the information in this topic to control the USB interface used for in-band communication between the server and the IMM2.

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

Apply Reset

Ethernet SNMP DNS DDNS SMTP LDAP Telnet **USB**

Universal Serial Bus (USB) Settings

Control the USB interface used for in-band communication between the server and the IMM. This setting does not affect the USB interface used for out-of-band communication.

☒ Enable Ethernet over USB

☒ Enable external Ethernet to Ethernet over USB port forwarding

Add Mapping... Remove...

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
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.

Setting Ethernet over USB for SUSE Linux Enterprise 12 or higher versions

Use the information in this topic to understand how to set Ethernet over USB for SUSE Linux Enterprise 12 or higher.

- Step 1. Set the static IP address for USB0 in the OS. Set the IP address manually in the following preferred range.
- 10.0.0.0 - 10.255.255.255
 - 172.16.0.0 - 172.31.255.255
 - 192.168.0.0 - 192.168.255.255
- Step 2. Change the network script (/etc/sysconfig/network/ifcfg-usb0) as follows:

```
BOOTPROTO='static'
```

```
ONBOOT='yes'
```

```
BROADCAST=''
```



```
ETHTOOL_OPTIONS=""
```

```
IPADDR='172.16.10.10/16'
```

```
MTU=""
```

```
NAME='usb0'
```

```
NETMASK='255.255.0.0'
```

```
NETWORK=""
```

```
REMOTE_IPADDR=""
```

```
STARTMODE='auto'
```

```
USERCONTROL='no'
```

Note: As an example, 172.16.10.10 is set as the static IP address. Bring down the interface once and bring it back up using ifup and ifdown.

```
linux-akn6:~ # ifdown usb0
```

```
usb0 device-ready
```

```
linux-akn6:~ # ifup usb0
```

```
usb0 up
```

- Step 3. Change the IP address for IMM in IMM management>>Network >> USB. Configure the IP settings for Ethernet over USB with an IP address in range with the IP address set on the OS level. The IP address set as 172.16.10.20 is for reference only. Keep the subnet mask the same. After completing the following step, it is observed the IMM can be accessed via in-band communication.

Note: For setting up Ethernet over USB for USB1 in a multi-node system, follow the steps mentioned above for USB0.

Configuring IPMI

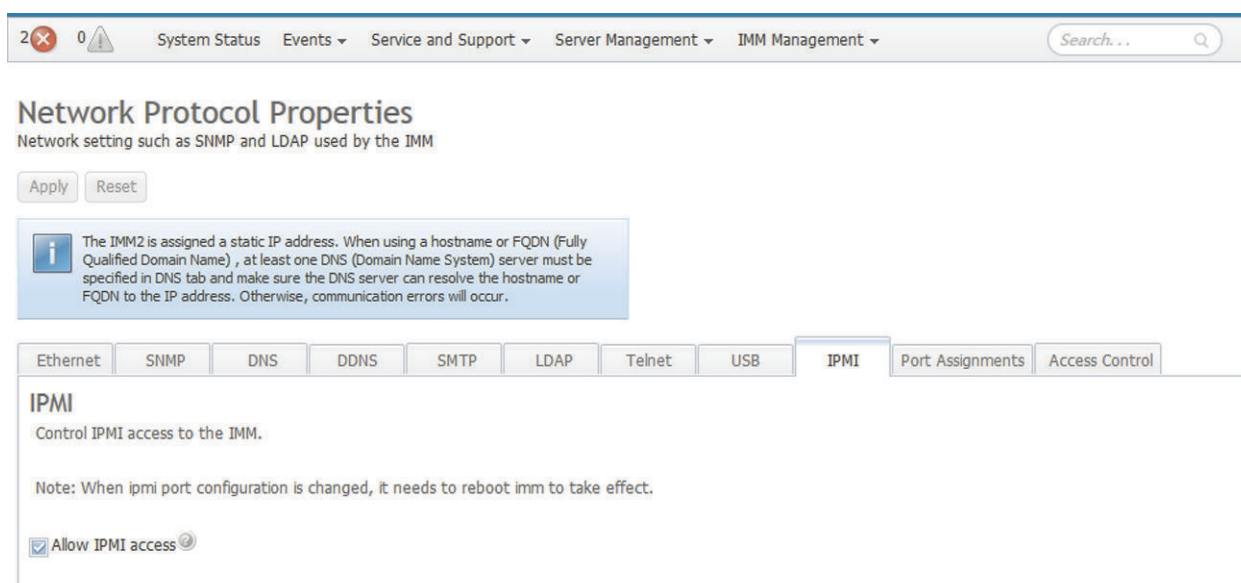
Use the information in this topic to control IPMI access to the IMM2.

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

Allow IPMI access

Tick the checkbox if you would like the IMM2 to allow IPMI access.

The following illustration shows the **IPMI** tab.



Configuring port assignments

Use the information in this topic to view or change the port numbers used by some services on the IMM2.

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 network ports might be used by the IMM2 and are *not* user-configurable:

File Transfer Protocol (FTP)

The port numbers are 20 and 21.

Trivial File Transfer Protocol (TFTP)

The port number is 69.

SSH File Transfer Protocol (SFTP)

The port number is 115.

Note: IMM.SFTPPortControl=open is required for OneCLI in-band updates.

Network Time Protocol (NTP)

The port number is 123.

Service Location Protocol (SLP)

The port number is 427.

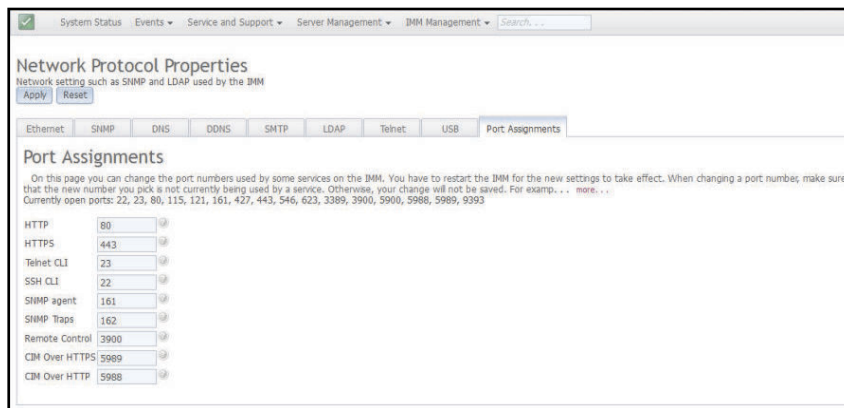
Remote Management Control Protocol (RMCP)

The port number is 623.

Web Services for Management (WS-Management)

The port numbers are 5985 (WS-Management over HTTP) and 5986 (WS-Management over HTTPS).

The following illustration shows the **Port Assignments** tab.



Configuring access control

Use the information in this topic to view or change IMM2 access control settings.

Click the **Access Control** tab to view or modify IMM2 access control settings.

To use access control, complete the following fields:

List of Blocked IP address

If the checkbox of “Blacklist of IP Addresses” is ticked, one textbox will be shown. Users could enter no more than three IPv4 addresses or ranges which are not allowed to access this IMM. And users must use comma to split them. The formats of IPv4 addresses and ranges are:

1. The single IPv4 address. For example: 192.168.1.1
2. The supernet IPv4 address. For example: 192.168.1.0/24
3. The IPv4 range. For example: 192.168.1.1-192.168.1.5

List of Blocked MAC address

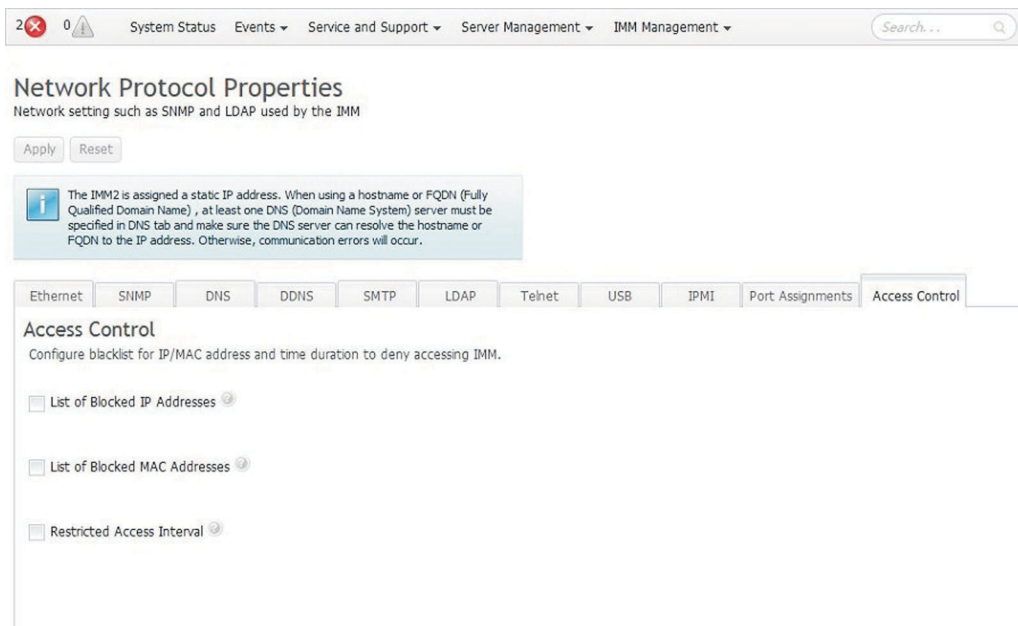
If the checkbox of “Blacklist of MAC Addresses” is checked, one textbox will be shown. Users could enter no more than three MAC addresses which are not allowed to access this IMM. And users must use comma to split them. The format of MAC addresses is the single MAC address. For example: 11:22:33:44:55:66.

Restricted Access (one time)

You can schedule a one-time time interval during which the XClarity Controller cannot be accessed. For the time interval that you specify:

- The beginning date and time must be later than the current XCC time.
- The ending date and time must be later than the beginning date and time.

The following illustration shows the **Access Control** tab.



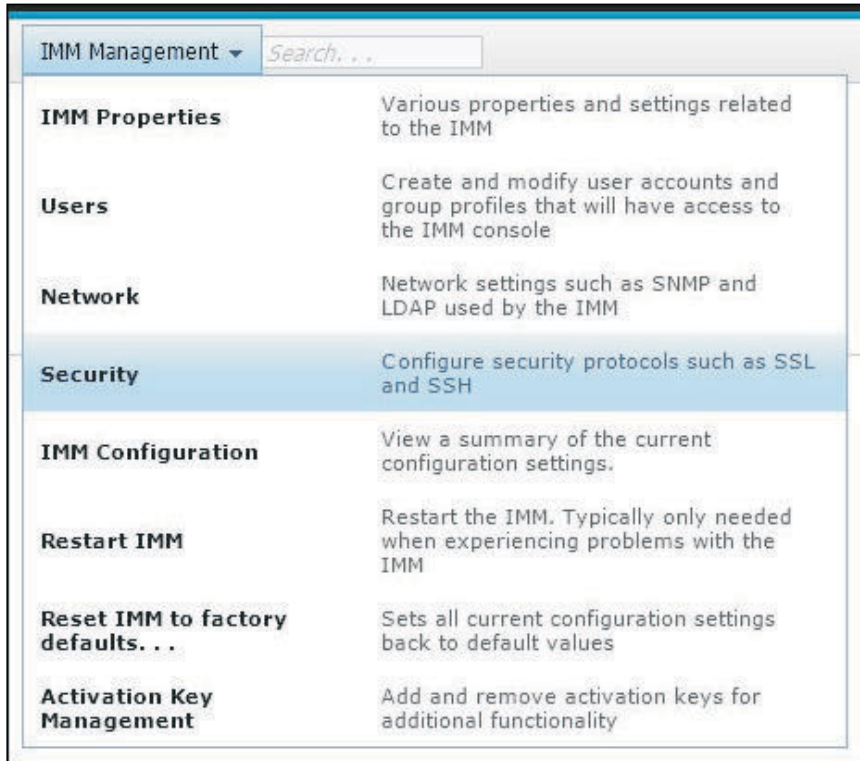
Configuring security settings

Use the information in this topic to configure security protocols.

Note: For enhanced security, the IMM2 firmware has been changed to use TLS version 1.2 as the minimum acceptable level. The firmware will continue to use the current minimum TLS version setting until the IMM2 is reset to factory defaults. You can configure the IMM2 to use other TLS versions if needed by your browser or management applications, but the minimum setting is version 1.2 by default. For more information, see [“tls command” on page 301](#).

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

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



Configuring HTTPS protocol

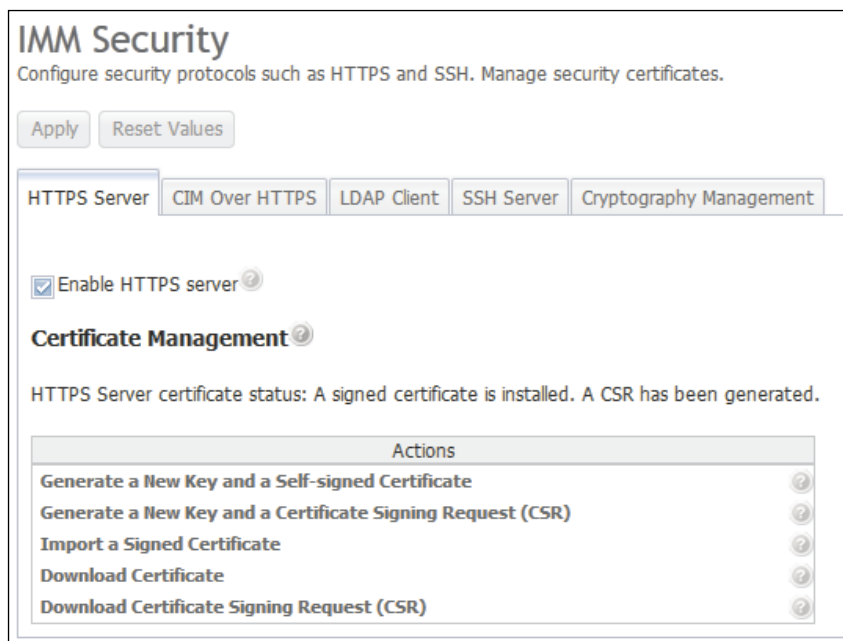
Use the information in this topic to understand and enable the HTTPS security protocol.

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 112](#). The following illustration shows the **HTTPS Server** tab.



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

HTTPS certificate handling

Use the options in the Actions menu for HTTPS certificate handling. If an option is disabled, you might need to perform another action first to enable it. While working with HTTPS certificates, you should disable the HTTPS server. For more information about certificate handling, see [“SSL certificate handling” on page 112](#).

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

Configuring CIM over HTTPS protocol

Use the information in this topic to understand and enable the CIM over HTTPS security 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 112](#). The following illustration shows the **CIM over HTTPS** 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

☒ 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 112](#).

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

Configuring LDAP client protocol

Use the information in this topic to understand and enable the LDAP over SSL security protocol.

Click the **LDAP Client** tab 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 112](#).

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

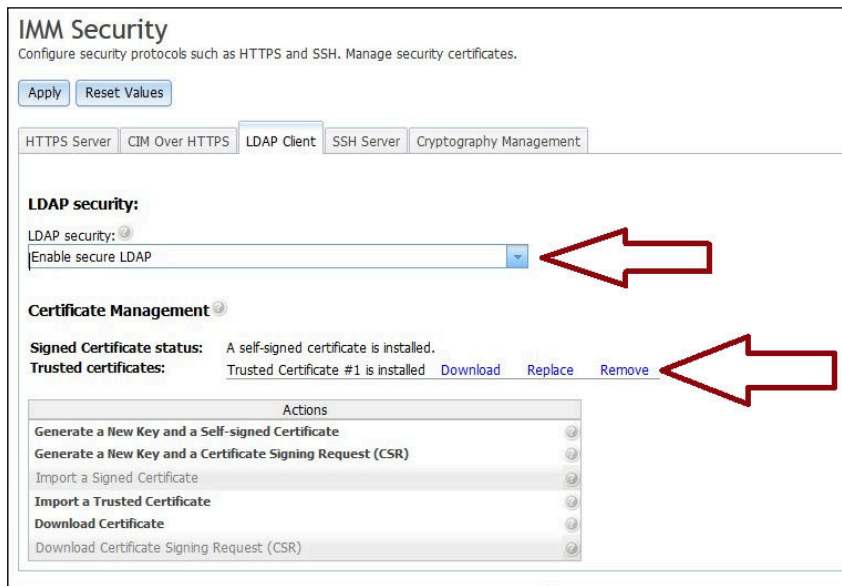
Actions	
Generate a New Key and a Self-signed Certificate	?
Generate a New Key and a Certificate Signing Request (CSR)	?
Import a Signed Certificate	?
Import a Trusted Certificate	?
Download Certificate	?
Download Certificate Signing Request (CSR)	?

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 112](#). Once you have installed the Trusted Certificate, you can enable LDAP over SSL as shown in the following illustration.

Notes:

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



Configuring the Secure Shell server

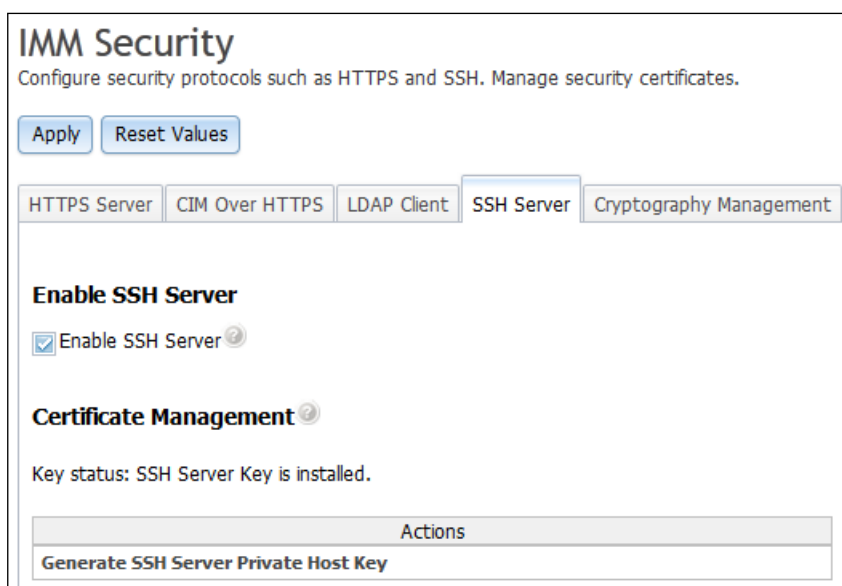
Use the information in this topic to understand and enable the SSH security protocol.

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

Notes:

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

The **SSH Server** tab is shown in the following illustration.



SSL overview

This topic is an overview of the SSL security protocol.

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

This topic provides information about the administration of certificates that can be used with the SSL security protocol.

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 users 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

This topic provides information about some of the actions that can be selected for certificate management with the SSL security protocol.

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

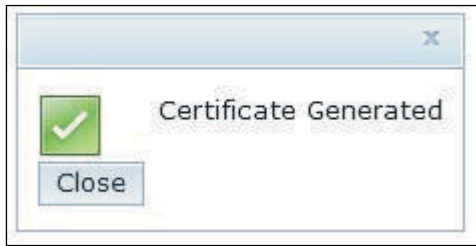


If a certificate is currently installed, you will be able to use the **Download Certificate** action in the Actions menu to download the currently installed certificate or CSR. Certificates that are grayed out are *not* currently installed. The secure LDAP client requires the user to import a trusted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

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

 A screenshot of a dialog box titled 'Generate New Key and Self-signed Certificate'. The dialog box is divided into two sections: 'Required SSL Certificate Data' and 'Optional SSL Certificate Data'. The 'Required' section contains five fields: 'Country' (a dropdown menu showing 'US United States'), 'State or Province' (text box with 'NY'), 'City or Locality' (text box with 'New York'), 'Organization Name' (text box with 'My Company'), and 'IMM Host Name' (text box with 'imm1234'). The 'Optional' section contains seven fields: 'Contact Person' (text box with 'Chris Manager'), 'E-Mail address' (text box with 'cmanager@mycomp.com'), 'Organizational Unit' (text box with 'Sales'), 'Surname' (empty text box), 'Given Name' (empty text box), 'Initials' (empty text box), and 'DN Qualifier' (empty text box). Each field has a help icon to its right. At the bottom of the dialog box are 'Ok' and 'Cancel' buttons.

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).



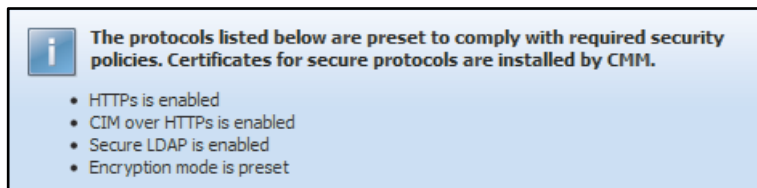
Compromised private keys

Use this topic to understand what a compromised private key is and what actions to take if your private key is comprised.

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.



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

- See [“Configuring the Secure Shell server” on page 111](#) for information about generating a replacement Secure Shell (SSH) Server Private Host Key
- See [“Configuring LDAP” on page 96](#) for information about removing and installing trusted certificates for the IMM2 LDAP client.
- See [“SSL certificate handling” on page 112](#) for information about generating a replacement SSH Server Private Host Key.

Private key states

Use this topic to understand the various transition states of a private key.

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

Use this topic to understand the purpose of cryptography management and how to configure the cryptography mode for the IMM2 firmware.

The purpose of any cryptography is to ensure the confidentiality, authenticity and integrity of data. These goals are achieved with the use of cryptography keys. Cryptography is a method of storing and transmitting data in a particular form so that only those for whom the data is intended can read and process it.

Click the **Cryptography Management** tab to configure the cryptography mode for the IMM2 firmware.

Important: Before you flash the IMM2 firmware back to an older firmware 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:

- Basic Compatibility Mode
- 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.

Apply Reset Values

HTTPS Server CIM Over HTTPS LDAP Client SSH Server **Cryptography Management**

☒ 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 a stronger level of encryption protection than the **Basic Compatibility Mode**. 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 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.

Apply Reset Values

HTTPS Server CIM Over HTTPS LDAP Client SSH Server **Cryptography Management**

☐ 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

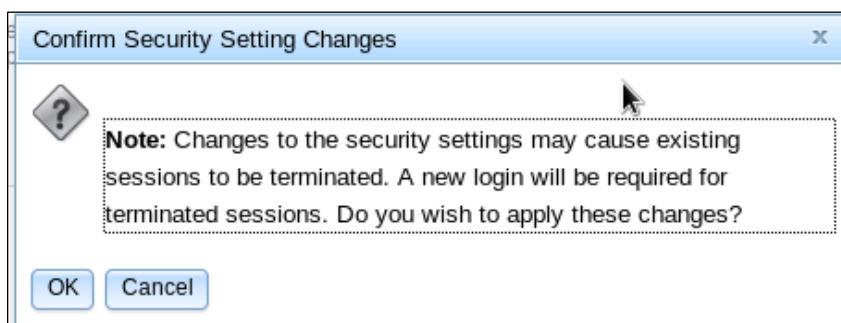
- Select this mode to have the IMM2 firmware comply with the requirements of SP 800-131A.
- **Note:** To prevent loss of access to the IMM2, this mode should only be selected if you are sure that your browser and other network clients also work with the required SP 800-131A encryption modes.

Select the settings below to override a strict compliance.

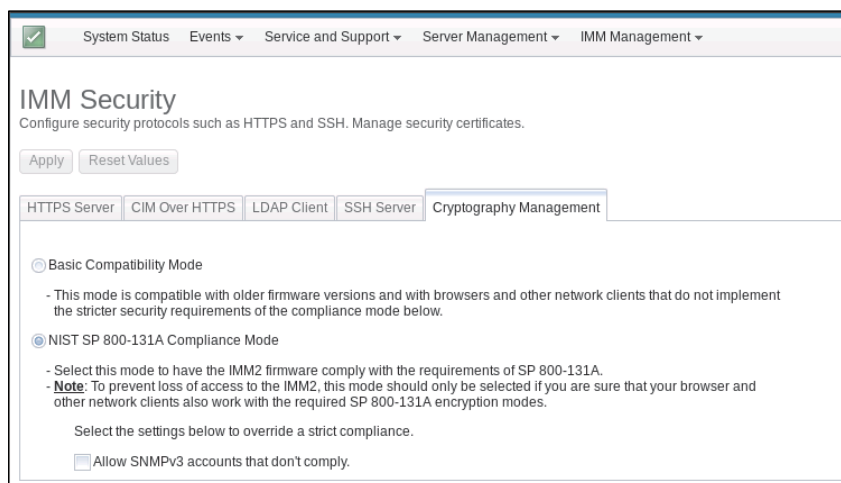
☒ Allow SNMPv3 accounts that don't comply.

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

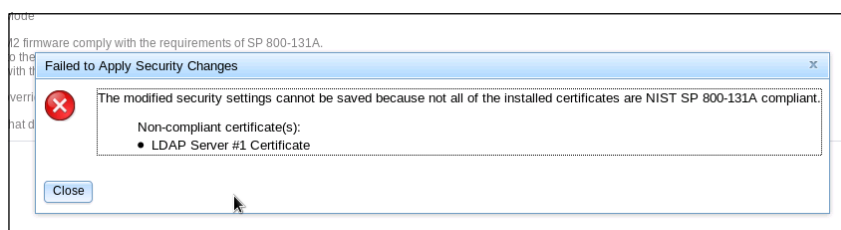
1. Log in to the IMM2.
2. Click the **Security** option under the **IMM Management** tab.
3. Click the **Cryptography Management** tab.
4. Select the cryptography mode on the Cryptography Management page; then, click the **Apply** button. You are asked for confirmation as shown in the following illustration.



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.



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



Configuring the SKLM Feature on Demand option

This topic provides information about the Security Key Lifecycle Manager (SKLM) software product that is used for creating and managing security keys.

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 205](#) 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 SKLM 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 SKLM 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.

Apply Reset Values

HTTPS Server CIM Over HTTPS LDAP Client SSH Server Cryptography Management **Drive Access**

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.skml.doc_2.5%2Fwelcome.html.
- 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

Use the information in this topic to create the hostname or IP address and associated port information for the SKLM server.

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

This topic contains information about the Device Group section of the IMM Security page.

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

This topic provides information about client and server 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

This topic provides information about 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

Two column table with headers documenting the required and optional fields for the Generate a new key and a self-signed certificate action. The bottom row spans across both columns.

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

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

Two column table with headers documenting the required and optional fields for the Generate a new key and certificate signing request action. The bottom row spans across both columns.

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

This topic provides information about server certificate management.

The server certificate is generated in the SKLM 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.

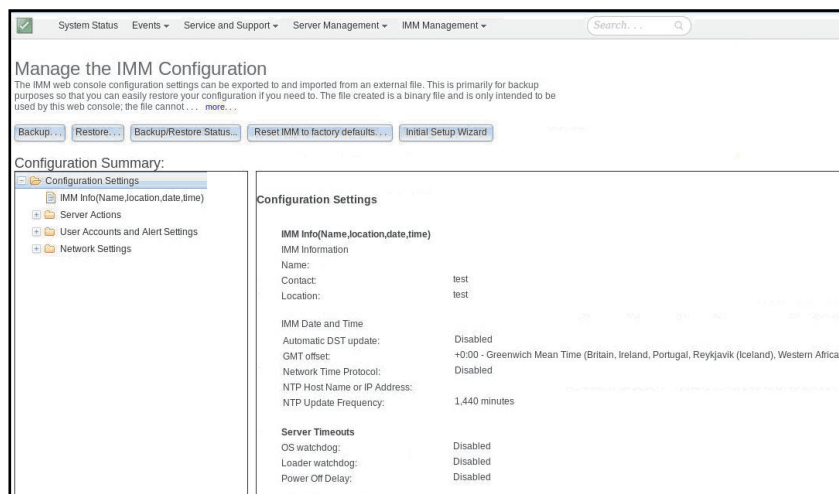
Restoring and modifying your IMM configuration

The information in this topic describes how to restore or modify your IMM2 configuration.

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

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

The following illustration shows the Manage the IMM Configuration window.



Restarting the IMM2

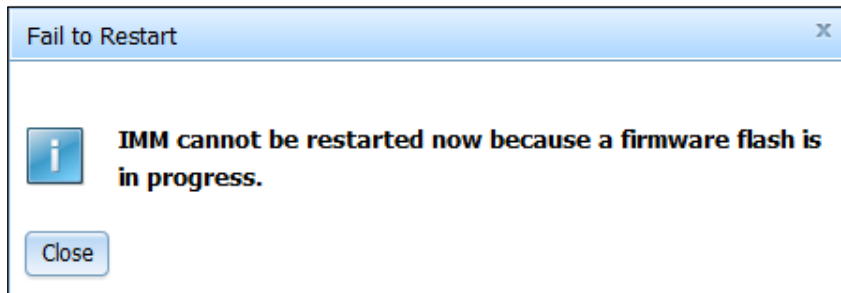
The information in this topic explains how to restart your IMM2.

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

Notes:

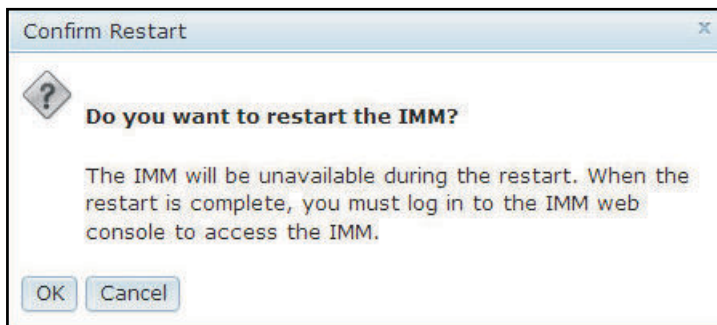
- Only persons with the Supervisor user authority level can perform this function.
- When Ethernet connections are temporarily dropped, you must log in to the IMM2 to access the IMM2 web interface.

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



To restart the IMM2 complete the following steps:

1. Log in to the IMM2. For more information, see [“Logging in to the IMM2” on page 11](#).
2. Click the **IMM Management** tab; then, click **Restart IMM**.
3. Click the **OK** button on the Confirm Restart window. The IMM2 will be restarted. The following illustration shows the Confirm Restart window.



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

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



4. Log in again to use the IMM2 web interface, (see [“Logging in to the IMM2” on page 11](#) for instructions).

Resetting the IMM2 to the factory defaults

This topic provides information about resetting the IMM2 to the factory default settings.

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.

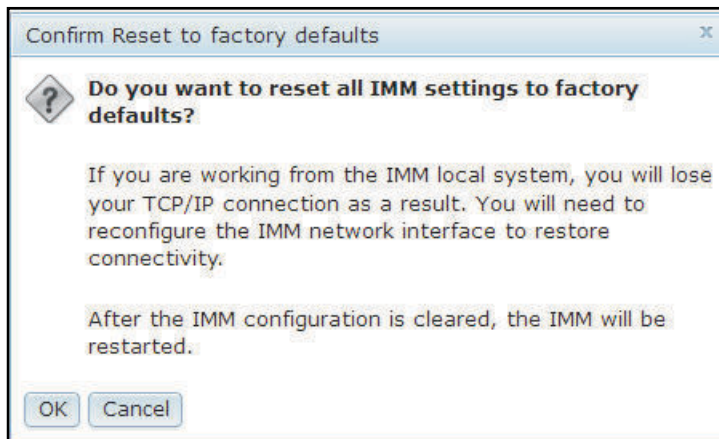
The settings supported by the IMM2 and their default values can vary depending on the server the IMM2 resides in. The default values for the settings that are supported by the IMM2 can be determined by using the ASU. Use the **ASU showdefault** command to collect and report the default factory settings 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 11](#).
2. Click the **IMM Management** tab; then, click **IMM Reset to factory defaults...**
3. Click the **OK** button on the Confirm Reset to factory defaults window (as shown in the following illustration).



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

4. Log in again to the IMM2 to use the IMM2 web interface, (see [“Logging in to the IMM2” on page 11](#) for instructions).
5. Reconfigure the network interface to restore connectivity.

Activation management key

This topic provides information about managing activation keys for optional IMM2 and server Feature on Demand (FoD) features.

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 205](#) for information about managing FoD activation keys.

Chapter 5. Monitoring the server status

Use the information in this topic to understand how to view and monitor information for the server that you are accessing.

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

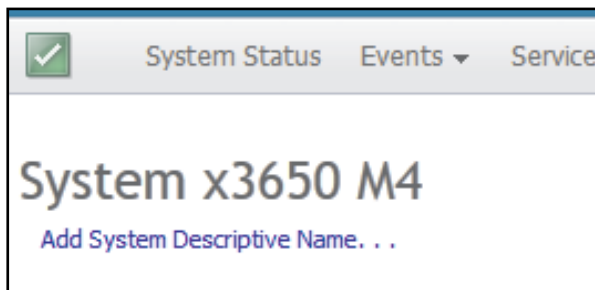
Viewing the system status

Use the information in this topic to understand the menu selections and choices on the System Status page.

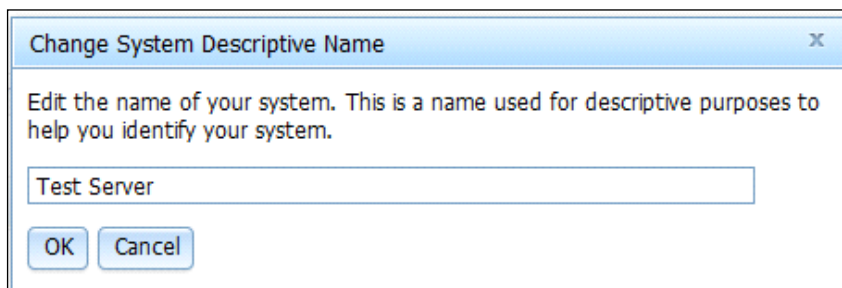
The System Status page provides an overview of the operating status of the IMM2 server. This page also displays the hardware health of the server and any active events occurring on the server.

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

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

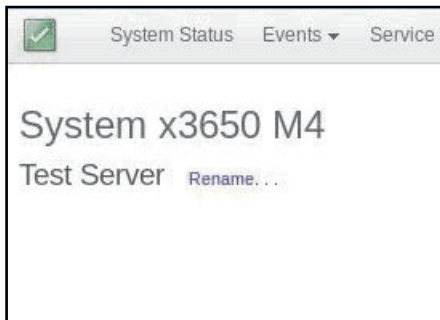


In the Change System Descriptive Name window, specify a name to associate with the IMM2 (as shown in the following illustration).



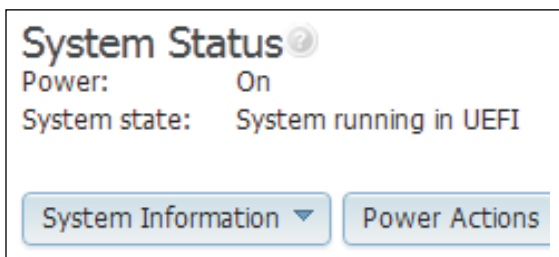
You can rename the System Descriptive Name by clicking the **Rename...** link that is located next to the System Descriptive Name.

The following illustration shows the Rename link.



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

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



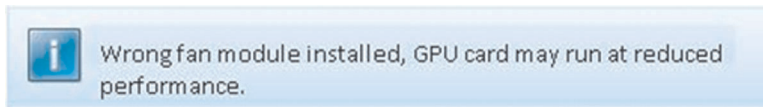
The server can be in one of the system states listed in the following table.

Table 8. System state descriptions

Two column table with headers documenting the system states of the server.

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.
Bootting operating system or in unsupported operating system	The server might be in this state for one of the following reasons: <ul style="list-style-type: none"> 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.
System Running in Setup	The server is powered on and UEFI has booted into F1 setup menu

The System Status page will display a message when an error or warning condition occurs, as seen in the following illustration.



In this example, when the GPU card is installed without a correct fan installed, the system status page will show one of the following warning messages to warn you that the GPU card may not be able to run at 100% functionality.

- “Wrong fan module installed, GPU card may run at reduced performance.”
- “Unknown fan module status”

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 137](#) for additional information).
- Latest OS Failure Screen, (see [“Capturing the latest OS failure screen data” on page 172](#) for additional information).

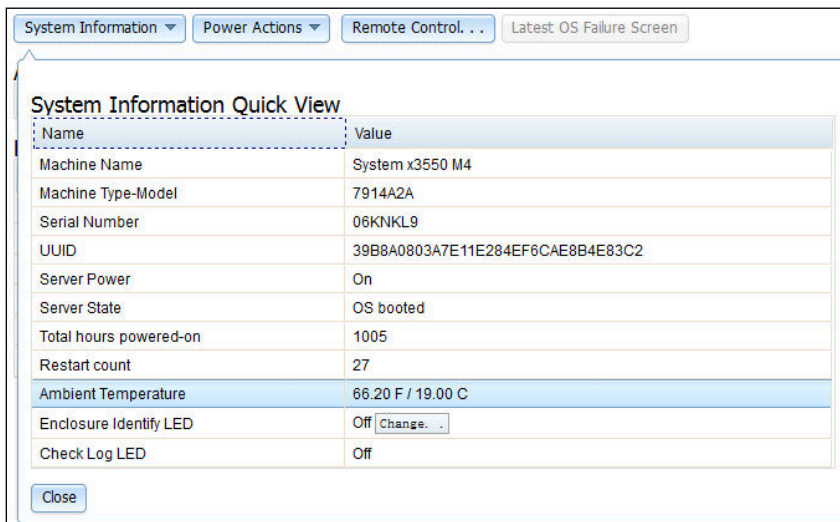
Viewing the system information

This topic explains how to obtain a summary of common server information.

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

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

The following illustration shows the System Information window.

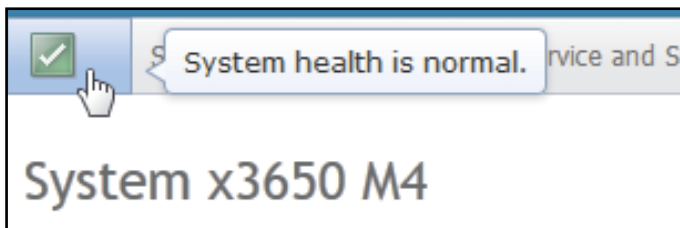


Viewing the server health

Use the information in this topic to understand how to interpret server health icon indicators and what to do if a warning or error condition exist.

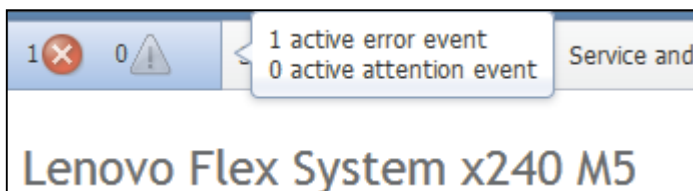
The server health is displayed under the title bar in the upper left corner of the System Status page and is designated by an icon. A green check mark indicates that the server hardware is operating normally. Move your cursor over the green checkmark to get a quick indication of the server health.

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






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

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



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

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








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

Use the information in this topic to understand the content displayed in the Hardware Health section of the System Status page.

The Hardware Health section of the System Status page lists 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.



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

Events

Hardware Information

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

Close

Chapter 6. Performing IMM2 tasks

This topic lists the tasks that can be performed to control the IMM2.

You can use the information in this section and [Chapter 3 “IMM2 web user interface overview” on page 19](#) 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.

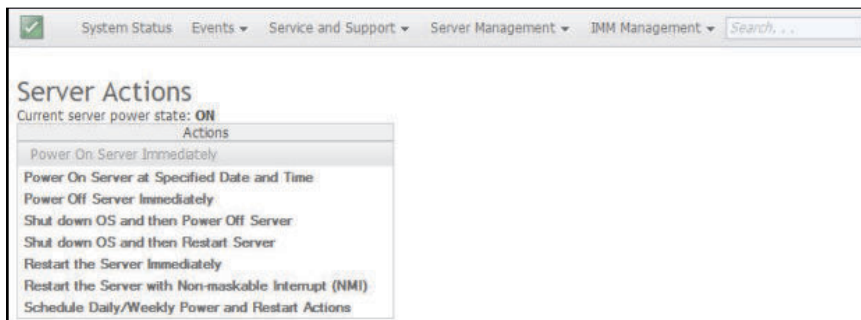
- From the Server Firmware option, view and update the firmware levels of server components.
- From the Remote Control option, remotely view and interact with the server console:
 - Remotely control the power status of the server
 - Remotely access the server console
 - Remotely attach a CD drive, DVD 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

Use the information in this topic to understand how to control the power state and perform various power actions for the server.

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



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

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

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

Table 9. Power actions and descriptions

Two column table containing descriptions of the server power and restart actions.

Power Action	Description
Power on server immediately	Select this action item to power on the server and boot the operating system.
Power on server at specified date and time	Select this action item to schedule the server to automatically power on at a specific date and time.

Table 9. Power actions and descriptions (continued)

Power Action	Description
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

Use the information in this topic to understand how to remotely view and interact with the server console.

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 104](#).

Updating your IMM2 firmware and Java or ActiveX applet

This topic contains an Important notice about IMM2 firmware and the 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

This topic provides information about the availability of 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 205](#).

Remote control screen capture

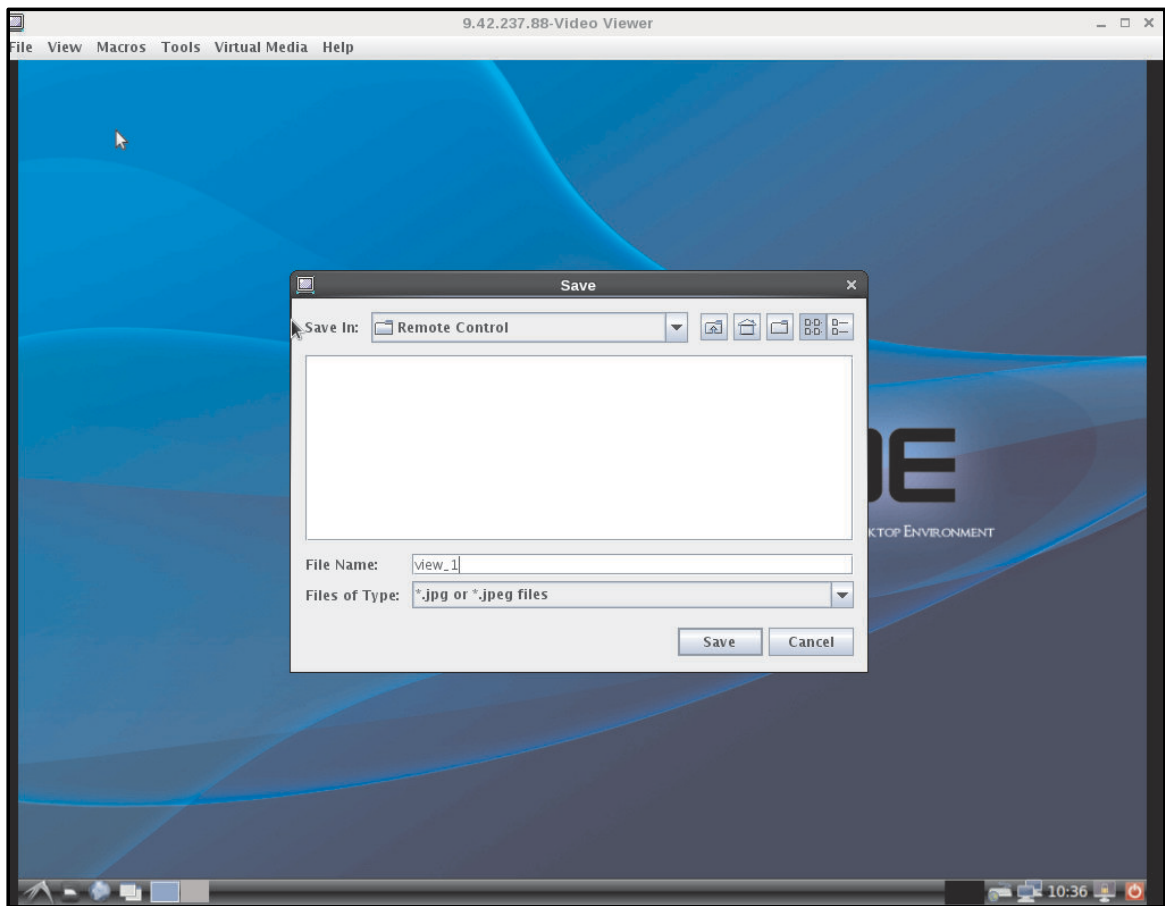
Use the information in this topic to understand how to use the remote control screen capture feature.

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:

- Step 1. In the Video Viewer window, click **File**.
- Step 2. Select **Capture to File** from the menu.
- Step 3. When you are prompted, enter a name for the image file and save it to the location that you choose on the local client.

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

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



Remote control Video Viewer modes

Use the information in this topic to use the 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

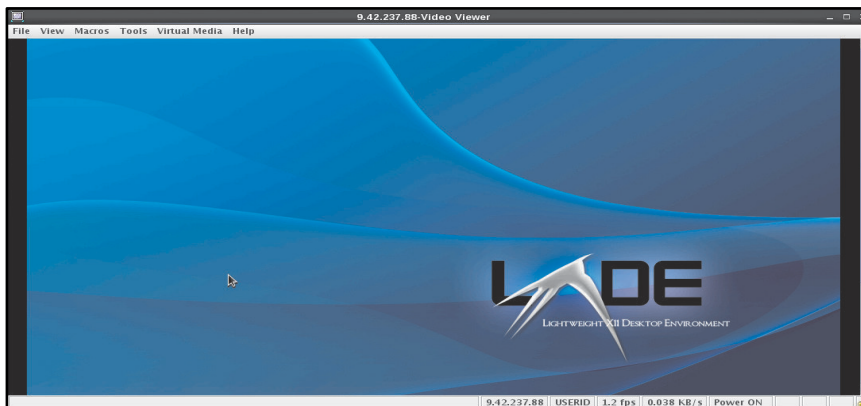
Click **View > Video Scaling** to enable scaling for the video display. With Video Scaling *enabled*, the video image is sized so that the complete image is within the console window, (as shown in the following illustration).

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.



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).



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

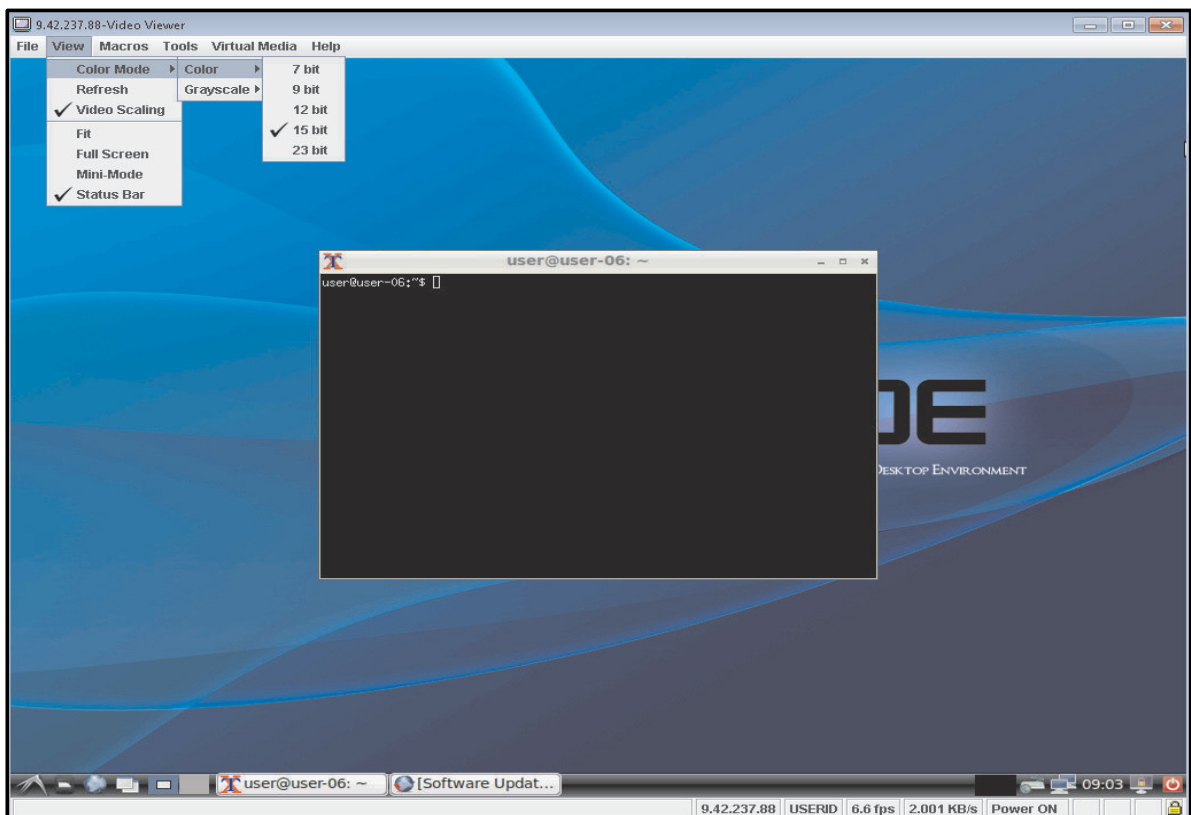
Use the information if your connection to the remote server has limited bandwidth and you wish to reduce the bandwidth demand.

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



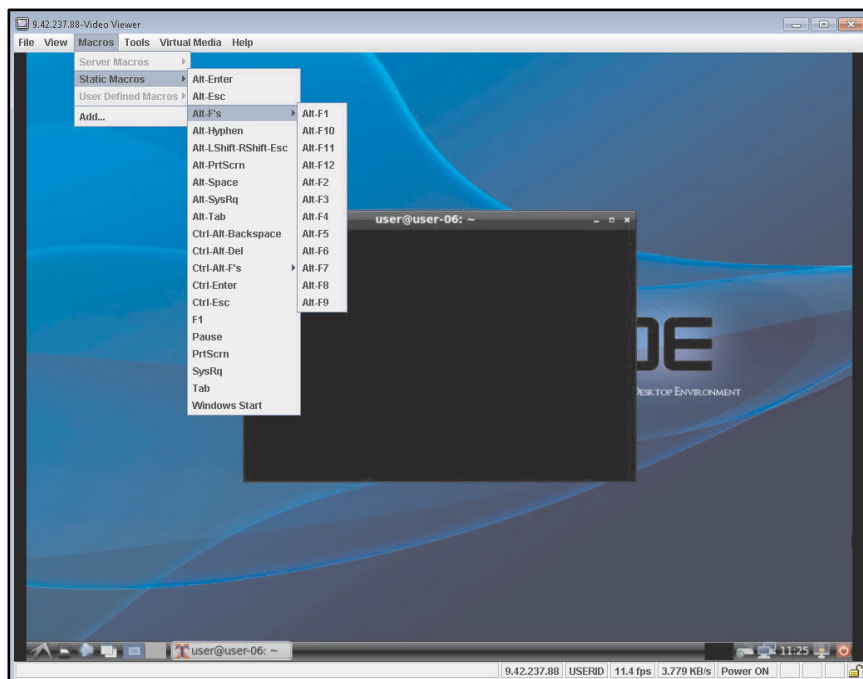
Remote control keyboard support

Use this information to create macros that can provide 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).
 - The Advanced Setting Utility (ASU) can be used to configure the server macros. For example,
 - To associate the key sequence “4FT” with the left Alt key + F1 combination, use the following command: `asu64.exe set IMM.ServerMacro.1 “[Alt(Left)+F1]+4+F+T”`
 - To remove the key sequence, use the following command: `asu64.exe loaddefault IMM.ServerMacro.1.`
- 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.

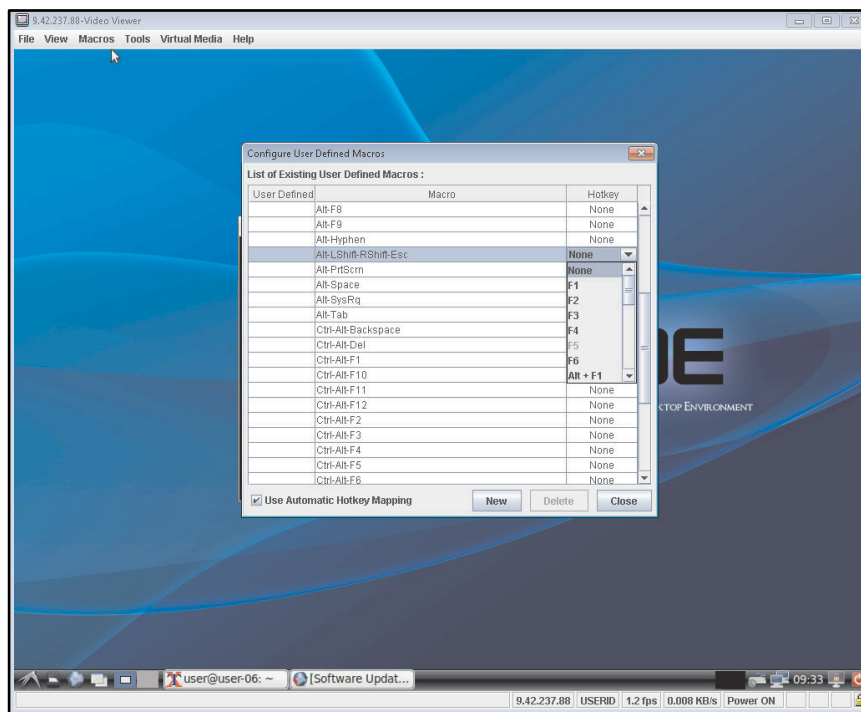
2. Keyboard pass-through

- 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

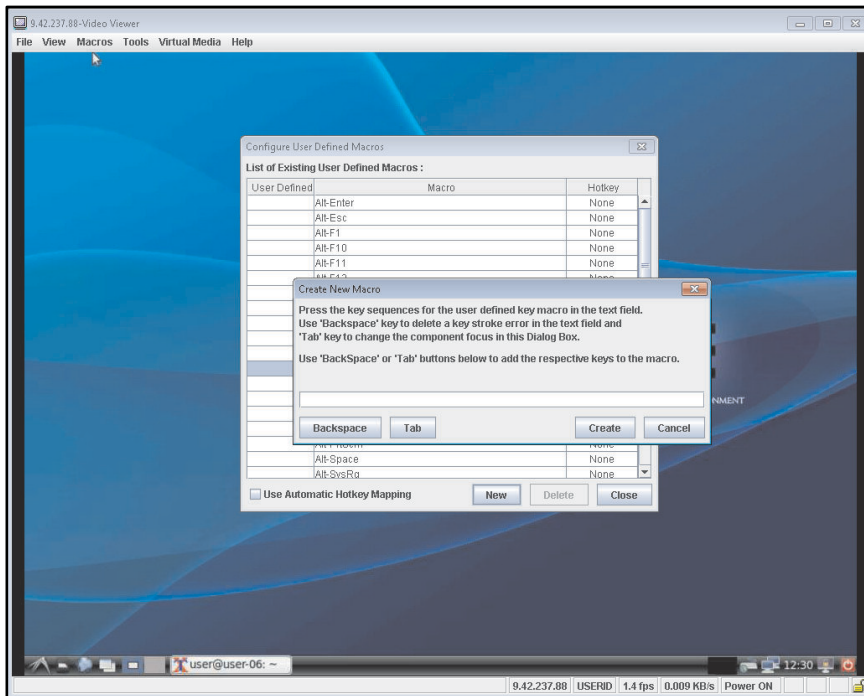
- When keyboard pass-through is not enabled and if the entered key or key combination is not assigned as a hot key to a macro; then, the keystrokes are sent to the host server. The exception to this rule is if the keystrokes are *normally* routed to the client workstation operating system.

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.



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.



International keyboard support

This topic describes how international keyboard support is managed.

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

This topic describes how keyboard pass-through is managed.

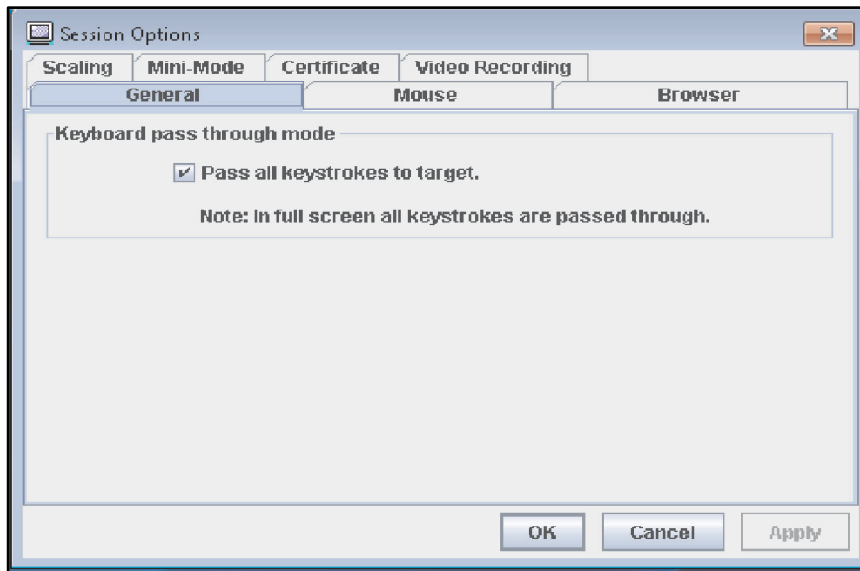
The keyboard pass-through mode disables the handling of most special key combinations on the client so that they can be passed directly to the server. The keyboard pass-through mode provides an alternative to using the macros.

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.



Remote control mouse support

Use this information to understand the options for remote mouse control.

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

Use this information to access the absolute and relative options for controlling the mouse.

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

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

Absolute

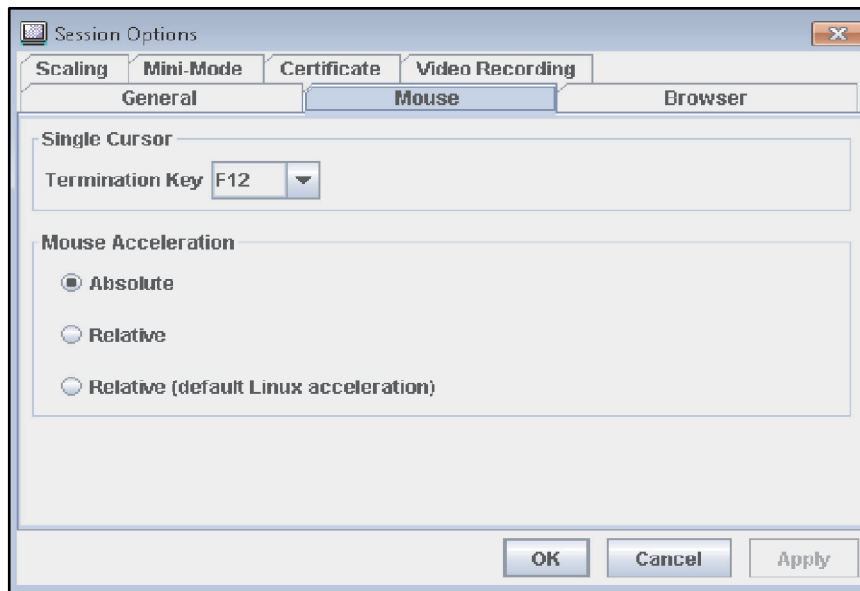
The client sends mouse location messages to the server that are always relative to the origin (upper left area) of the viewing area.

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 mode

This topic provides information about the single cursor mouse mode of operation.

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

This topic explains how to send server power and restart commands from the Video Viewer window.

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:

- Step 1. In the Video Viewer window, click **Tools**.
- Step 2. Click **Power**. Select one of the following commands (as shown in the following illustration):
 - Power On Server Immediately
 - Select this action item to power on the server.
 - Shut down OS and then Power Off Server
 - Select this action item to shut down the operating system and power off the server.
 - Restart the Server Immediately
 - Select this action item to power cycle the server immediately without first shutting down the operating system.

- Shut down OS and then Restart Server
 - Select this action item to shut down the operating system and power cycle the server.

Viewing performance statistics

This topic explains how to view Video Viewer performance statistics and understand the information displayed in the Stats window.

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

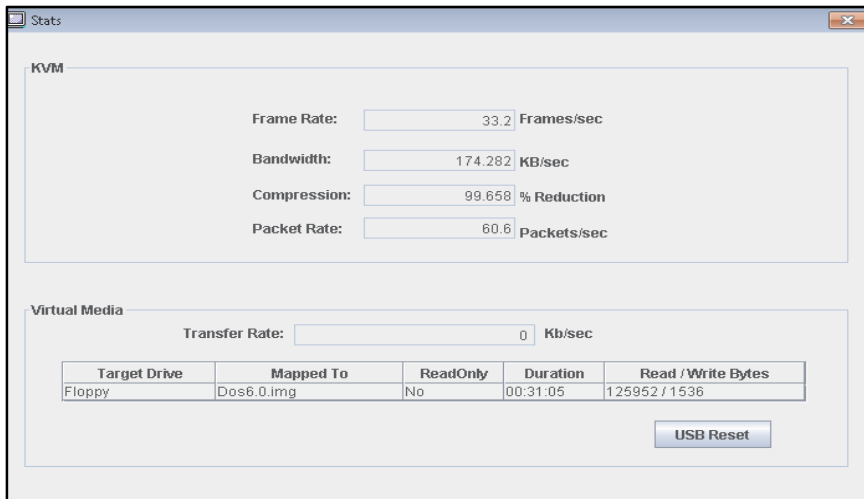
This field contains the number of bytes read and written to the drive.

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.



Starting Remote Desktop Protocol

Use the information in this topic to launch the remote desktop protocol client.

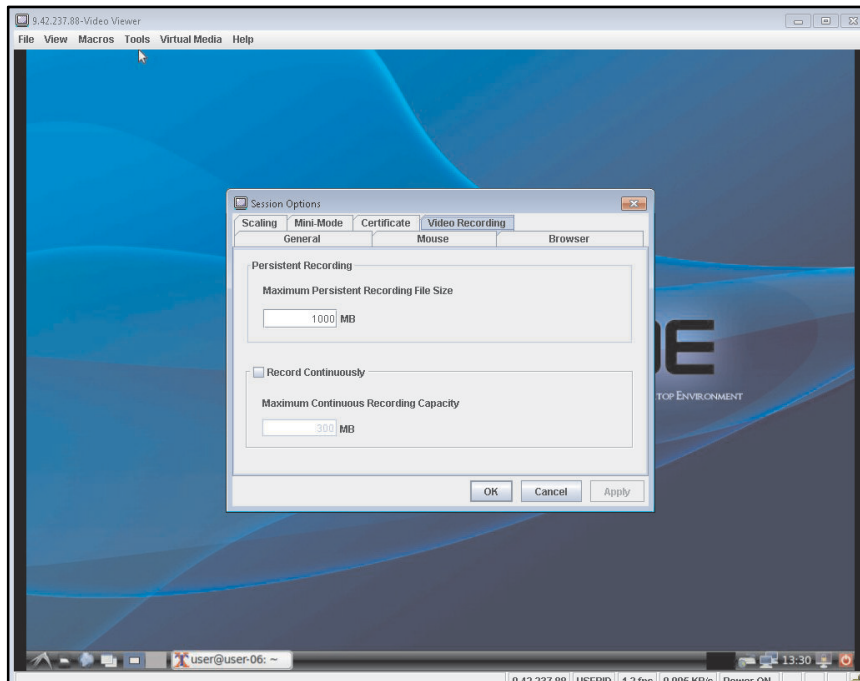
If the Windows-based Remote Desktop Protocol (RDP) client is installed, you can use a RDP client instead of the KVM client. The remote server must be configured to receive RDP connections. Click **Tools > Launch RDP** from the Video Viewer window to launch the RDP client.

Video Recording

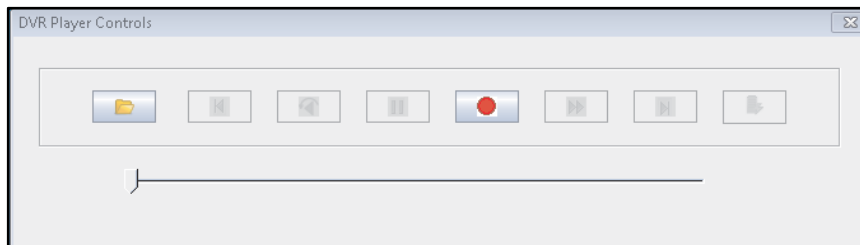
Use the information in this topic to select the video recording preference.

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:

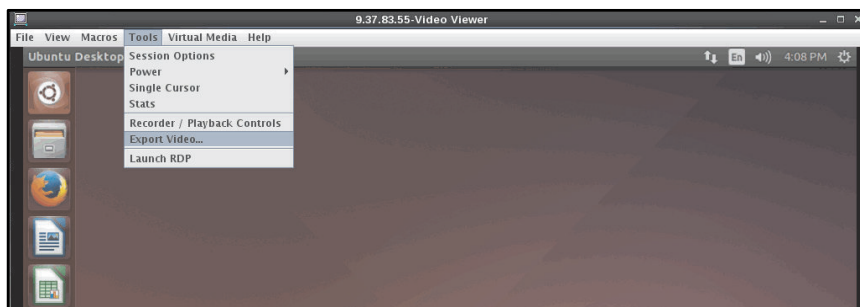
1. In the Video Viewer window click **Tools > Session Options**.
2. In the Session Options window click the **Video Recording** tab to choose one of the following recording preferences, (as shown in the following illustration).
 - Enter the maximum file size for persistent recordings in the **Maximum 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.

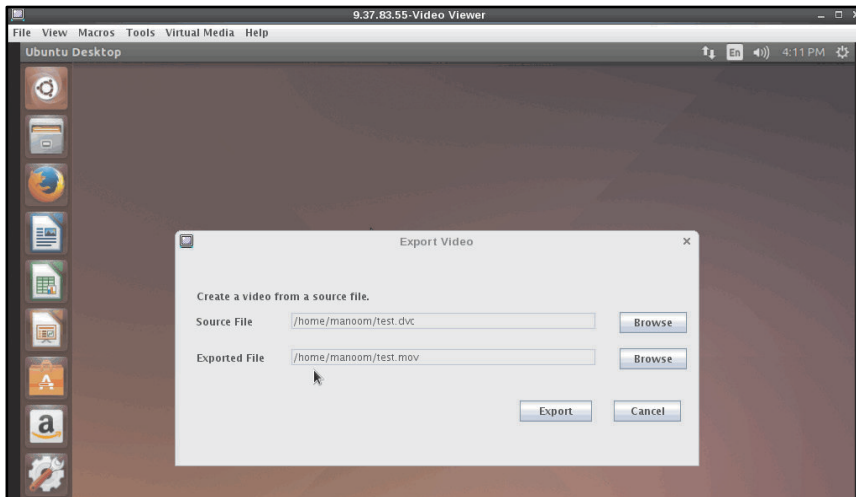


From the Video Viewer window, click **Tools > Recorder/Playback Controls** to playback the video and operate the recording controls. The DVR Player Controls window is displayed, (as shown in the following illustration).



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).





Knock-knock feature description

Use this information when you want to send a disconnection request to the remote control user who has enabled the Knock-knock feature.

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

Note:

- 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 through step 4.

To request a remote session complete the following steps:

1. Click **Refresh** to display the Remote Control session that is in progress. The following illustration shows the Remote Control Session in Progress window.

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:

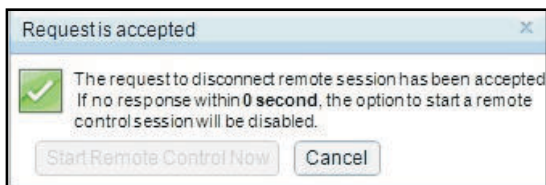
- **Request to connect:** This text is displayed when the remote control user enables the Knock-knock feature and is not handling a disconnection request from another web user. The current web user has not sent a disconnection request to the remote control user.
 - **Waiting for response:** This text 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.

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

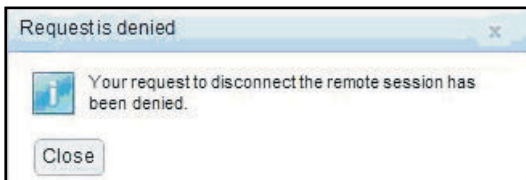
The following illustration shows the information that is displayed when the disconnect request is accepted and the request is in a reserved state.



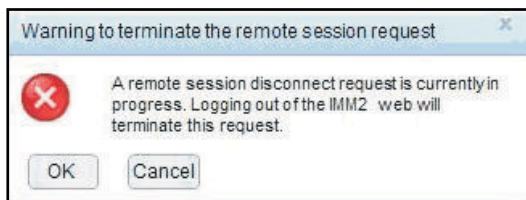
The following illustration shows the information that is displayed when the disconnect request is accepted and the request is in an unreserved state.



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

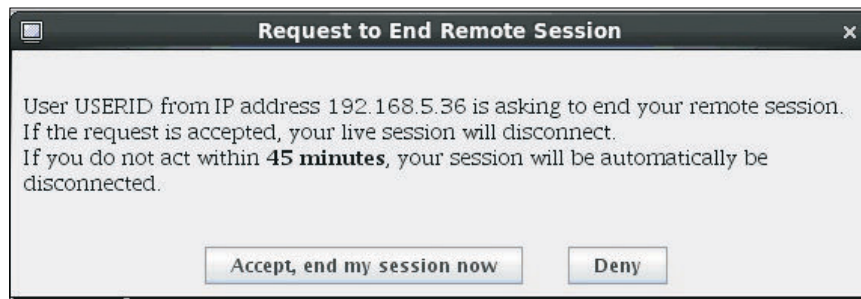


If the web user attempts to log out of the IMM2 before receiving a message about their request, the web user will receive a message (as shown in the following illustration).

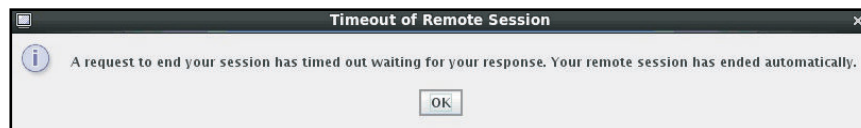


After the remote control user receives the request, the user must determine whether to release the remote session in the interval time selected before starting the remote control session. A Request to End Remote Session window is displayed to remind the remote control user of any time remaining.

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



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



Remote disk

Use the information in this topic to understand remote disk functionality.

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.

Note:

- 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 must have an Intel Pentium III microprocessor or greater, operating at 700 MHz or faster, or equivalent.

Accessing the Remote Control

Use this information to start a remote control session.

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

- Step 1. From the Video Viewer window click the **Virtual Media** tab.
- Step 2. Click **Activate**.
- Step 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.

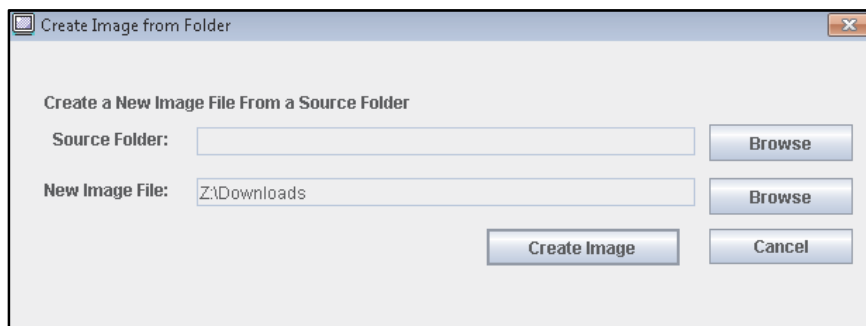
Creating an image file

To create a new image file use the information in this topic.

To create a new image file from a specified source folder, complete the following steps:

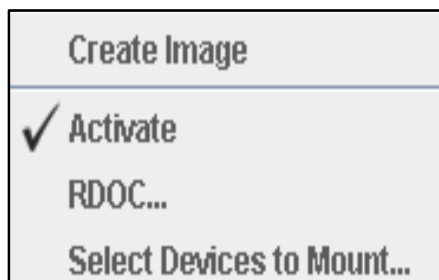
1. Click the **Create Image** option under the **Virtual Media** tab in the Video Viewer window. The Create Image from Folder window is displayed.
2. Click the **Browse** button associated with the **Source Folder** field to select the specific source folder.
3. Click the **Browse** button associated 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.



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 use the information in this topic.

To upload an image file to the host operating system, complete the following steps:

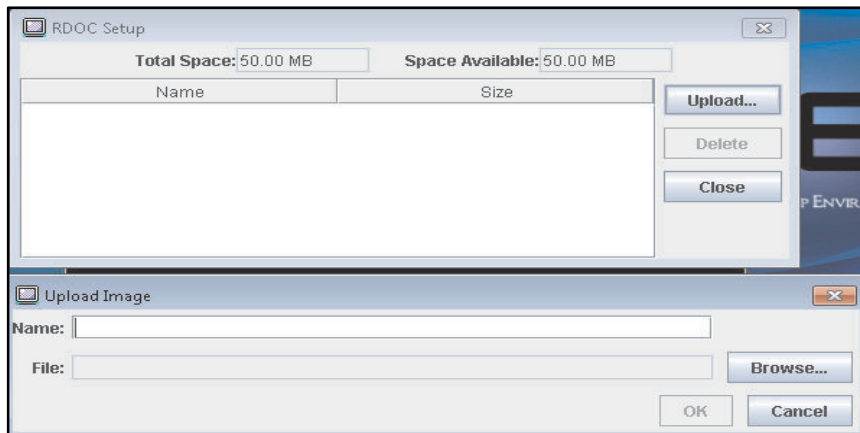
1. Click the **RDOC** option under the **Virtual Media** tab in the Video Viewer window. The RDOC Setup window is displayed.

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.



Selecting devices to mount

To select the devices to mount to the host operating system use the information in this topic.

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).

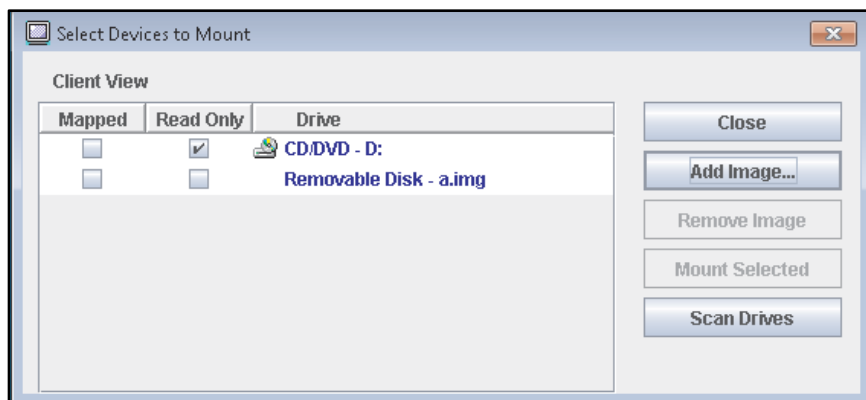


To select the devices to mount, complete the following steps:

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:

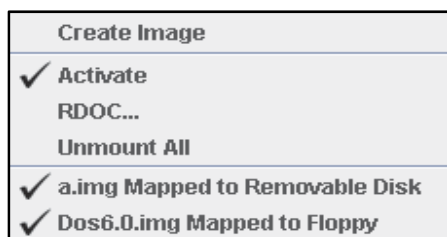
- The **Mapped** field contains the check box that allows you to select the devices to mount or map.
- The **Read Only** field contains the check box that allows you to select the mapped or mounted devices that will be *read-only* on the host server.
- The **Drive** field contains the device path on 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.



Selecting devices to unmount

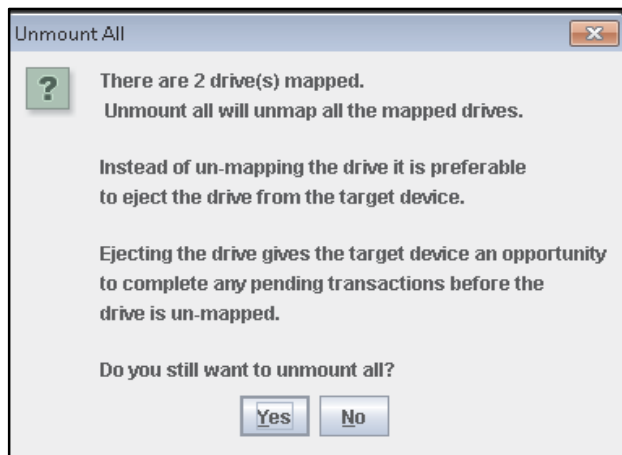
To unmount the host server devices use the information in this topic.

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).



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.



Exiting Remote Control

This topic explains how to end your remote control session.

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

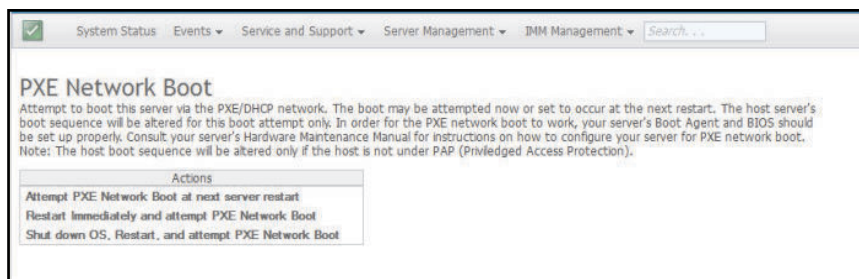
Setting up PXE network boot

To set up your server to attempt a Preboot Execution Environment network boot, use the information in this topic.

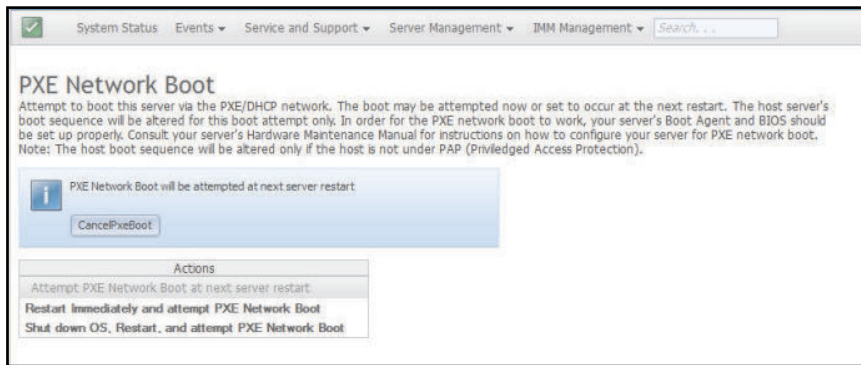
Use the **PXE Network Boot** option to set up an attempt to preboot the server Execution Environment.

Perform the following steps to set up your server to attempt a Preboot Execution Environment network boot at the next server restart.

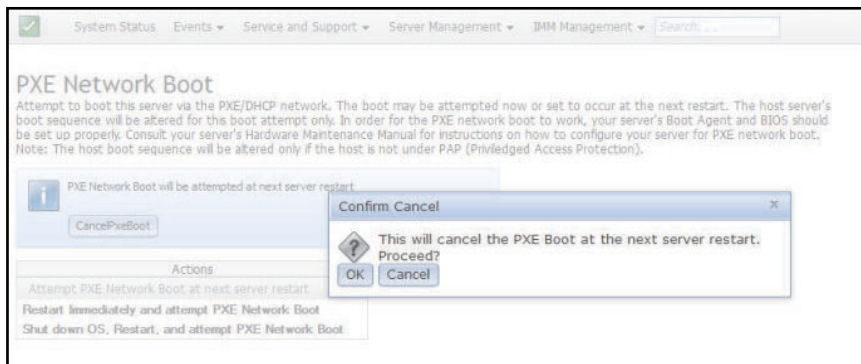
1. Log in to the IMM2. For more information, see [“Logging in to the IMM2” on page 11](#) for additional information.
2. Click **Server Management**; then, select **PXE Network Boot**. The following window opens.



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



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



Updating the server firmware

To update the server firmware use the information in this topic.

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 window.

Server Firmware				
Show the firmware levels on various server components, including the IMM itself.				
Update Firmware...				
Firmware Type	Status	Version	Build	Release Date
DSA	Active	9.24	DSYT44B	2012-08-10
IMM2				
IMM2 (Primary)	Active	2.15	1A0039Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	1A0039T	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:

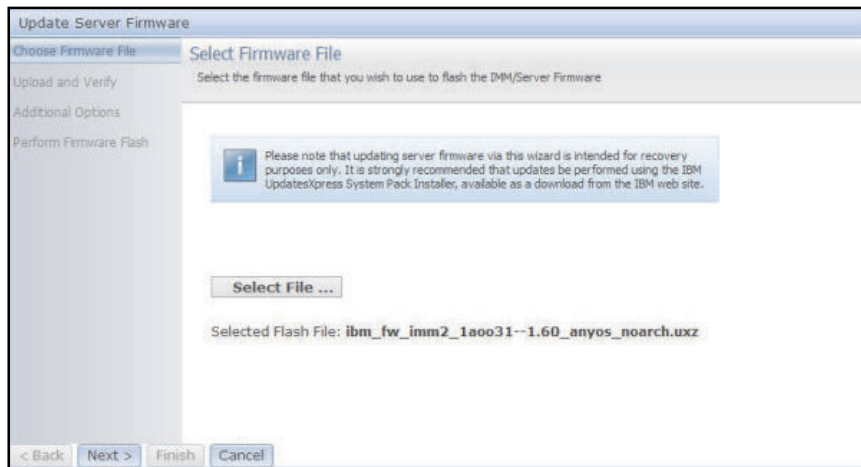
- **Active:** The firmware is active.
- **Inactive:** The firmware is not active.

- **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:

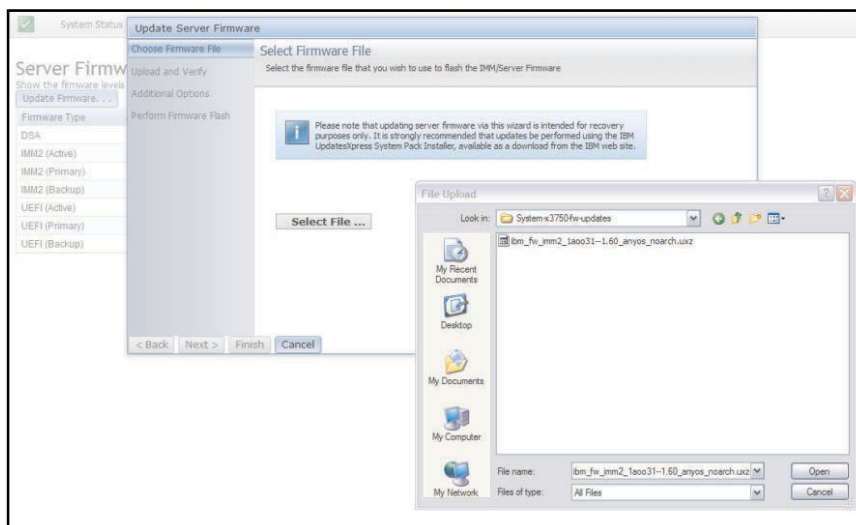
1. Click **Server Firmware** from the Server Management menu list.
2. Click **Update Firmware**. The Update Server Firmware window opens (as shown in the following illustration).



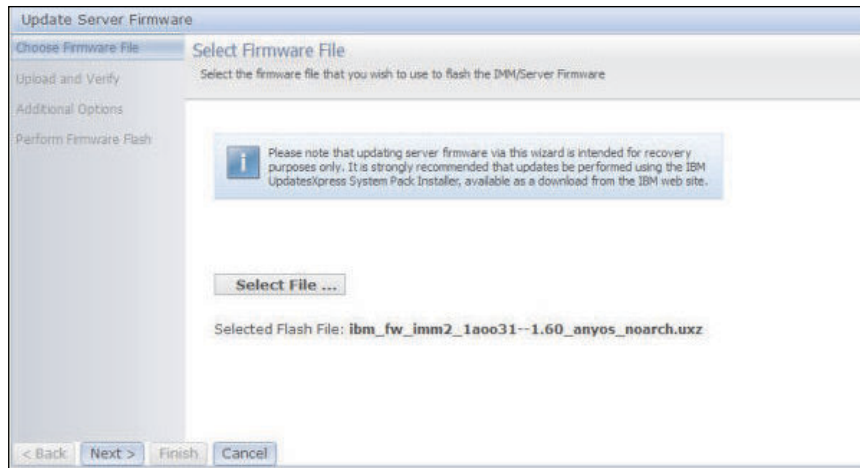
3. Read the warning notice *before* continuing with the next step.
4. Perform one of the following steps:
 - Click **Cancel** and return to the previous Server Firmware window.
 - Click **Select File...** to select the firmware file that you want to use to flash the server firmware.

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

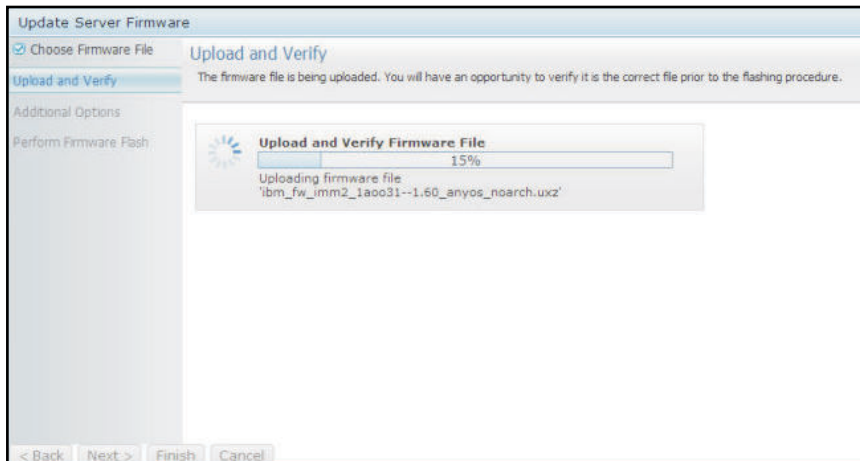
When you click **Select File...**, a File Upload window opens (as shown in the following illustration). This window allows you to browse to the desired file.



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

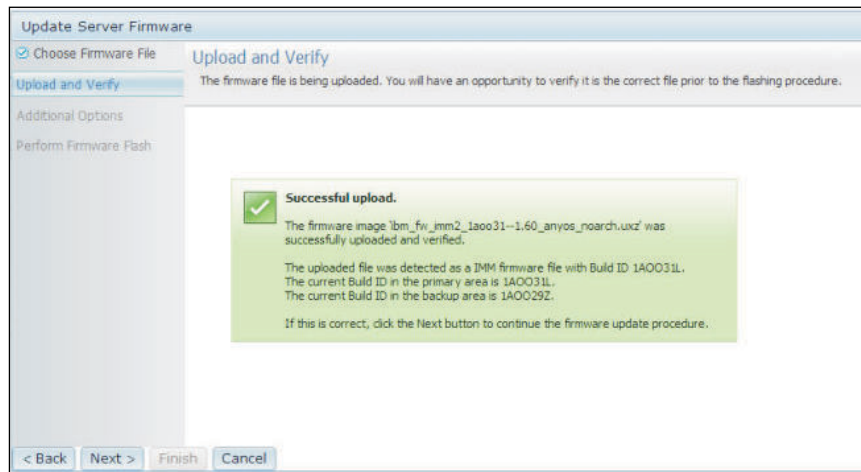


6. Click **Next >** to begin the upload and verify process on the selected file. A progress meter will be displayed as the file is being uploaded and verified (as shown in the following illustration).

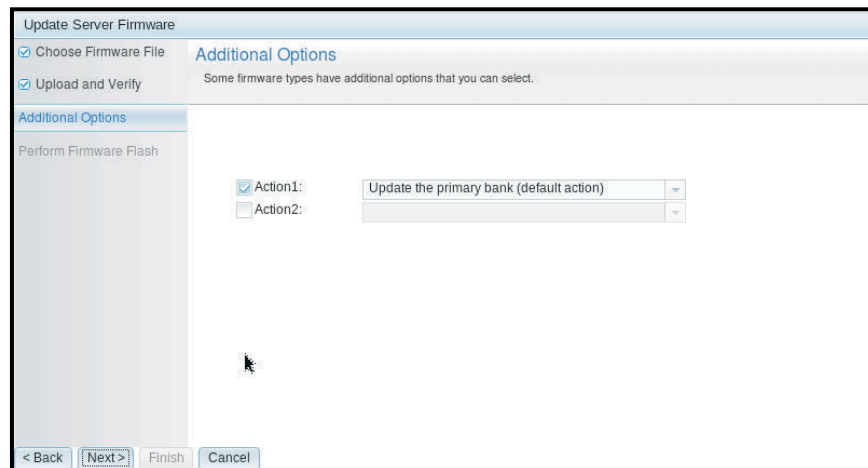


You can view this status window to verify that the file you selected to update is the correct file. The status window will have information regarding the type of firmware file that is to be updated such as DSA, IMM, or UEFI.

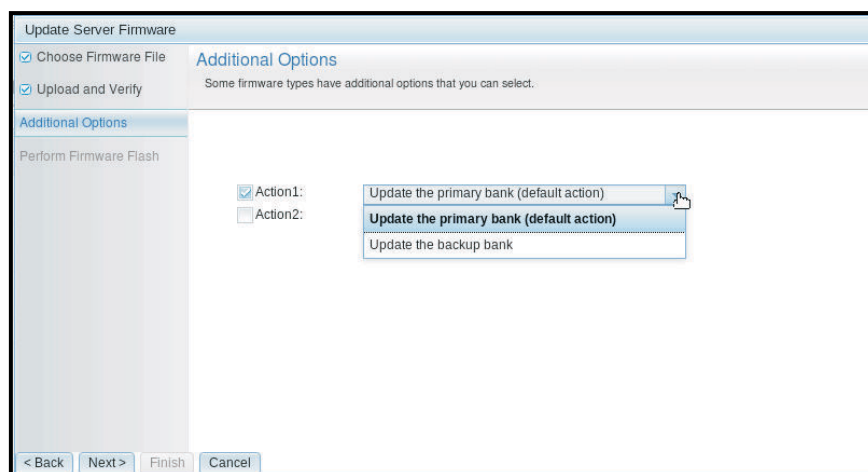
After the firmware file is uploaded and verified successfully, a Successful upload window opens (as shown in the following illustration).



- 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).



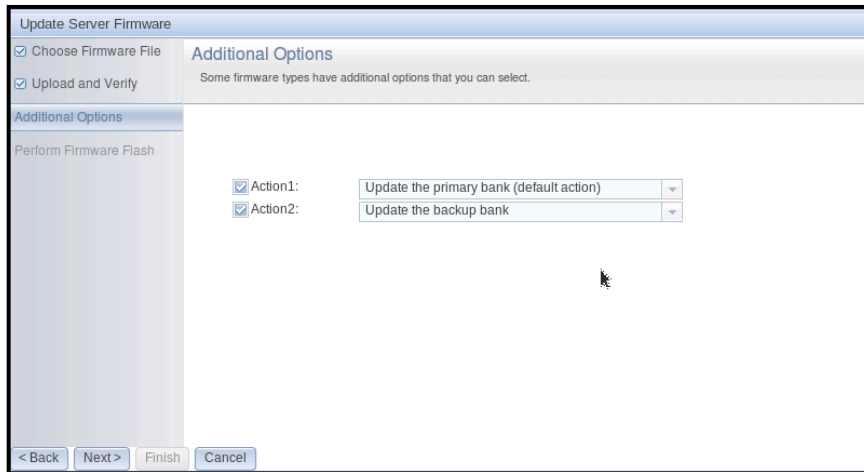
- The drop-down menu beside the **Action 1** field gives you the choice to **Update the primary bank (default action)** or **Update the backup bank** (as shown in the following illustration).



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

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

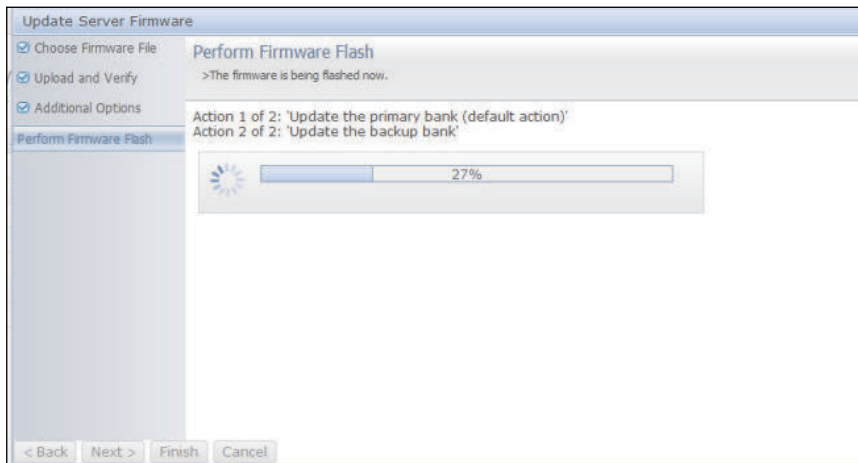
Note: To disable an action and start the additional option process again, click the checkbox beside the related action.



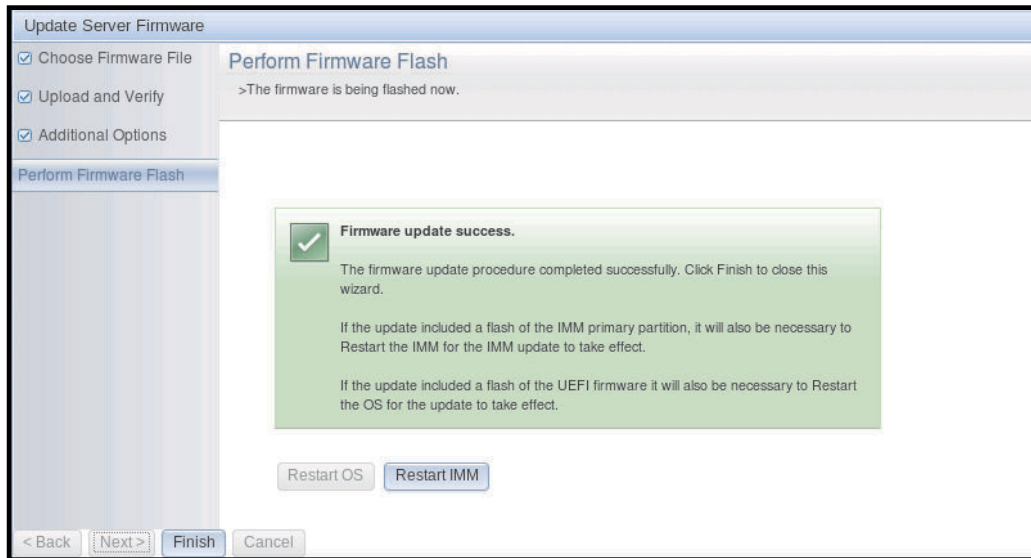
The previous screen shows that for Action 1, the primary bank is selected to be updated. You can also select to update the backup bank under Action 2 (as shown in the previous screen). Both the primary bank and the backup bank will be updated at the same time when you click **Next >**.

Note: Action 1 must be different from Action 2.

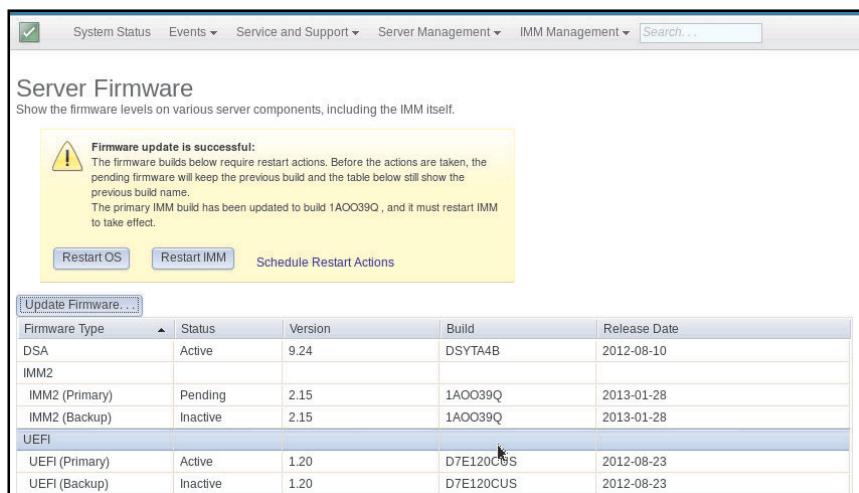
A progress meter shows the progress of the update for the primary and backup banks, (as shown in the following illustration).



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



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



Managing system events

This topic contains information to manage the Event Log history and Event Recipients for email and syslog notifications.

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

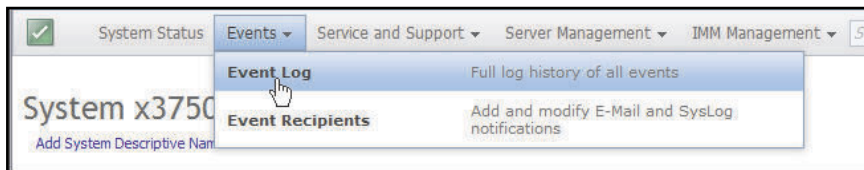
Managing the event log

Use this information to get a description of the events that are reported by the IMM2 and information about all remote access attempts and configuration changes.

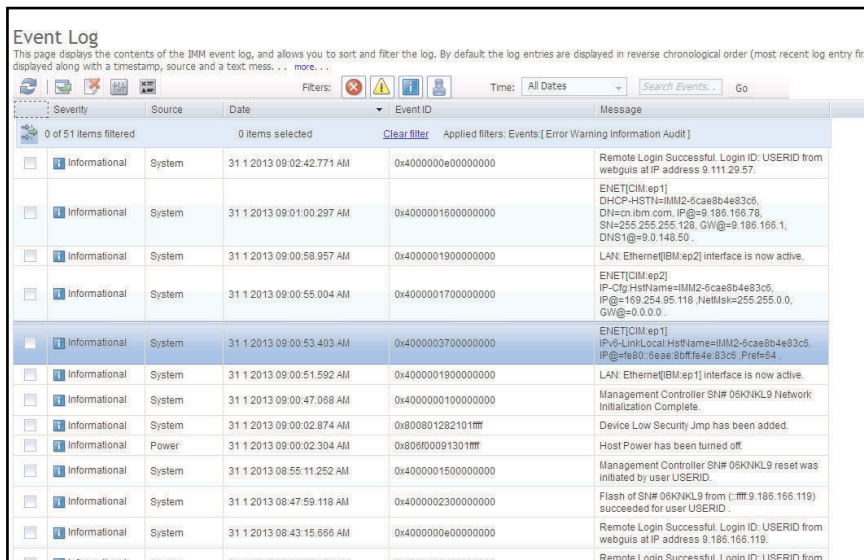
Click the **Event Log** option to display the Event Log window. The Event Log window includes a description of the events that are reported by the IMM2 and information about all remote access attempts and configuration changes. All events in the log are time stamped using the IMM2 date and time settings. 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.

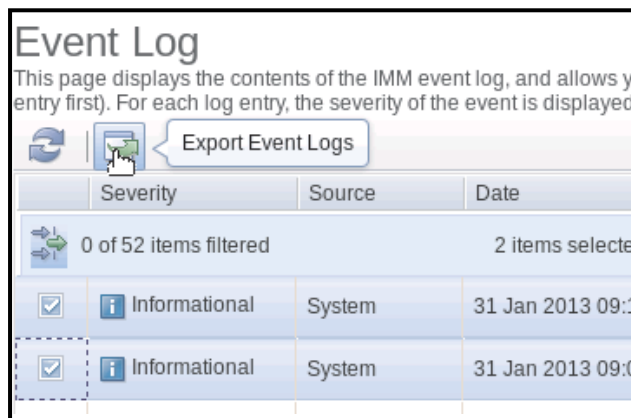
Click the **Event Log** option. The following window opens.



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

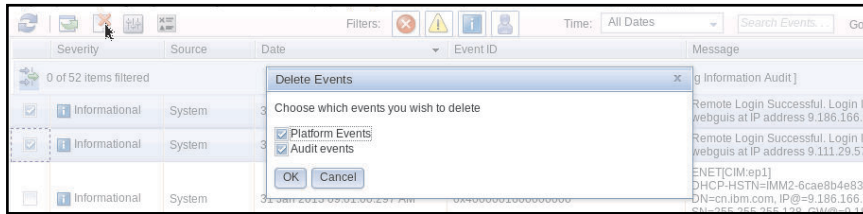


To sort and filter events in the event log, select the column heading. You can save all or save selected events in the event log to a file using the **Export** button. To select specific events, choose one or more events on the main Event Log page and left-click on the **Export** button (as shown in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



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

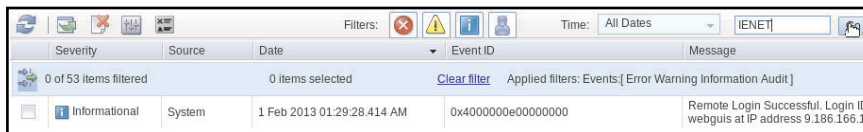
The following illustration shows the Delete Events window.



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



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

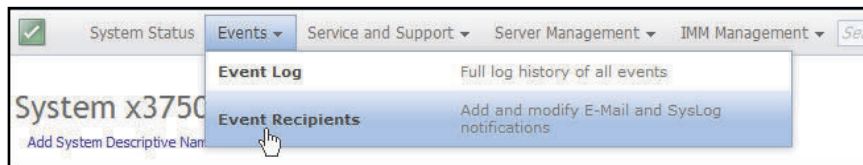


Notification of system events

To add and modify email and syslog notifications use the information in this topic.

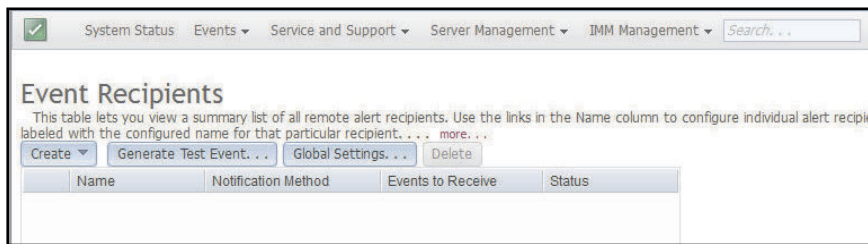
Select the **Event Recipients** option to add and modify email and syslog notifications.

The following illustration shows selection of the **Event Recipients** option.

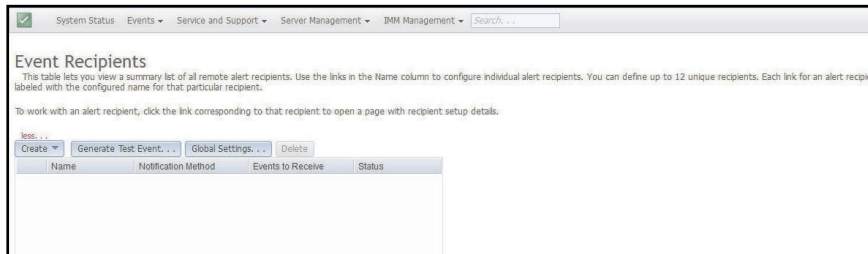


The **Event Recipients** option enables you to manage who will be notified of system events. You can configure each recipient and manage settings that apply to all Event Recipients. You can also generate a test event to verify notification feature operation.

The following illustration shows the Event Recipients page.



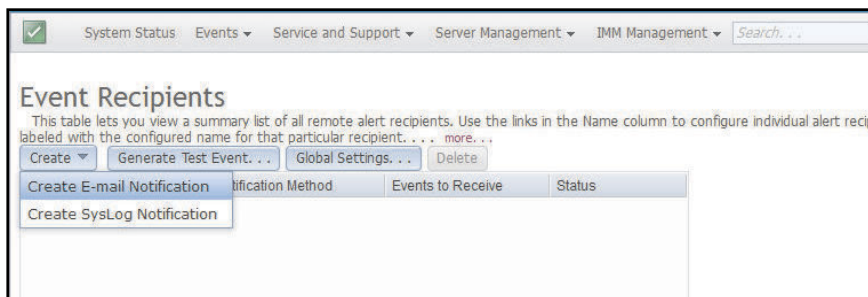
The following illustration shows additional information that is displayed when you click the **more** link on the Event Recipients page.



Creating email and syslog notifications

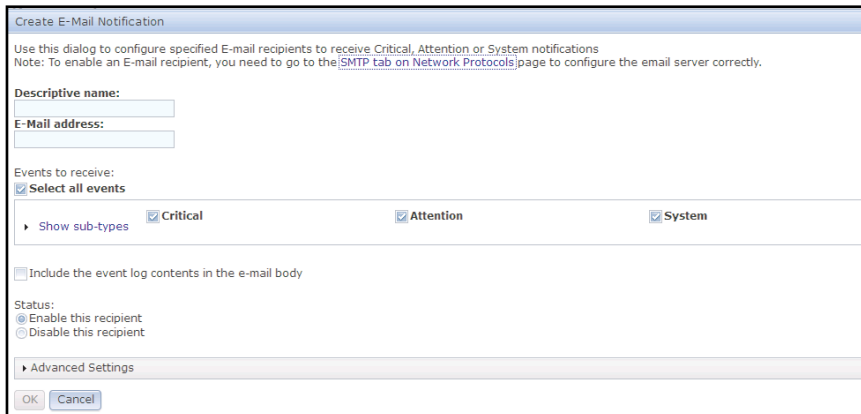
Select the **Create** tab to create email and syslog notifications.

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



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

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



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

► Show sub-types ☒ Critical ☒ Attention ☒ System

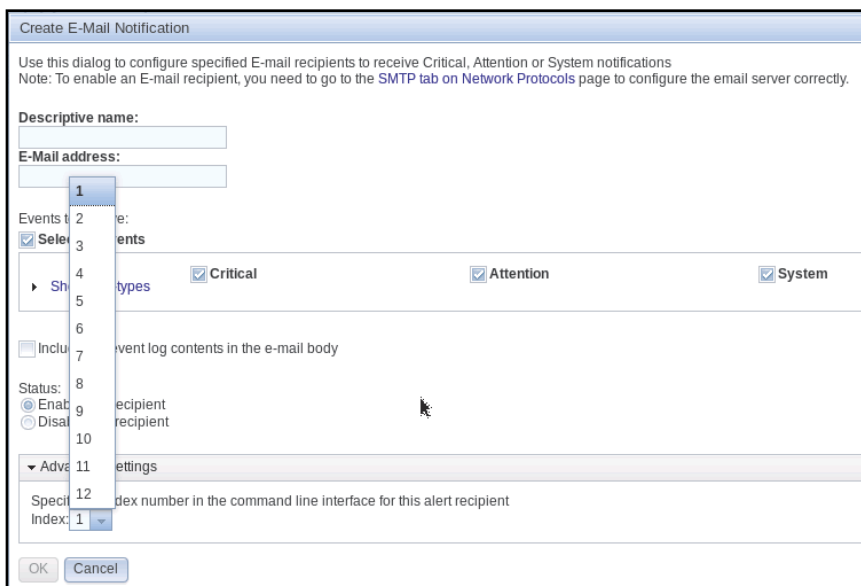
☐ Include the event log contents in the e-mail body

Status:
☒ Enable this recipient
☐ Disable this recipient

► Advanced Settings

OK Cancel

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 to receive:
☒ Select all events

► Show sub-types ☒ Critical ☒ Attention ☒ System

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

Status:
☒ Enable this recipient
☐ Disable this recipient

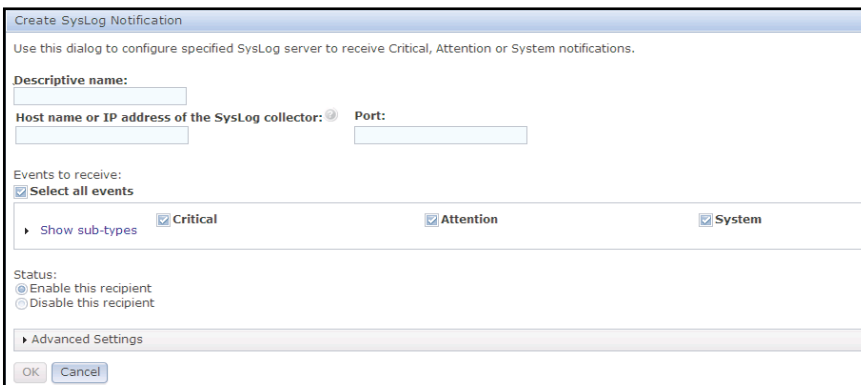
▼ Advanced Settings

Specify index number in the command line interface for this alert recipient
 Index: 1

OK Cancel

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

OK Cancel

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 name: Address of the SysLog collector: Port:

Events to receive: ☒ System

Status: ☒ Enabled ☐ Disabled

Specify index number in the command line interface for this alert recipient:

OK Cancel

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 recipient is 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

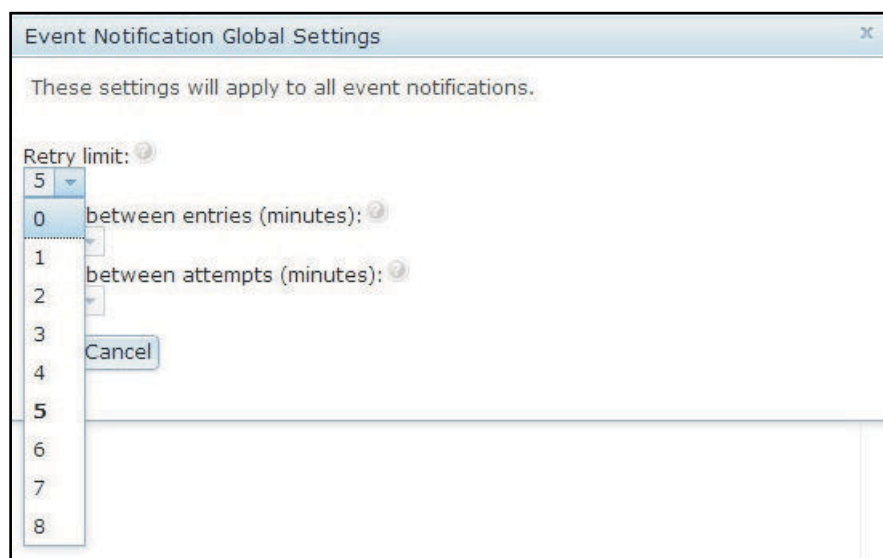
This will generate a test event and will be broadcast to the recipient 'Target User' indicating that it is just a test. Do you wish to proceed?

OK Cancel

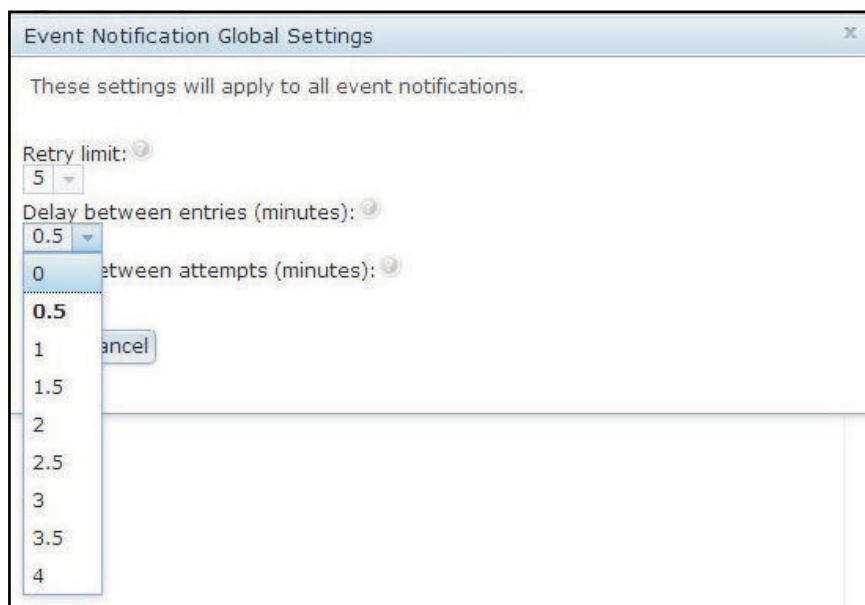
Setting limits to retry notifications

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

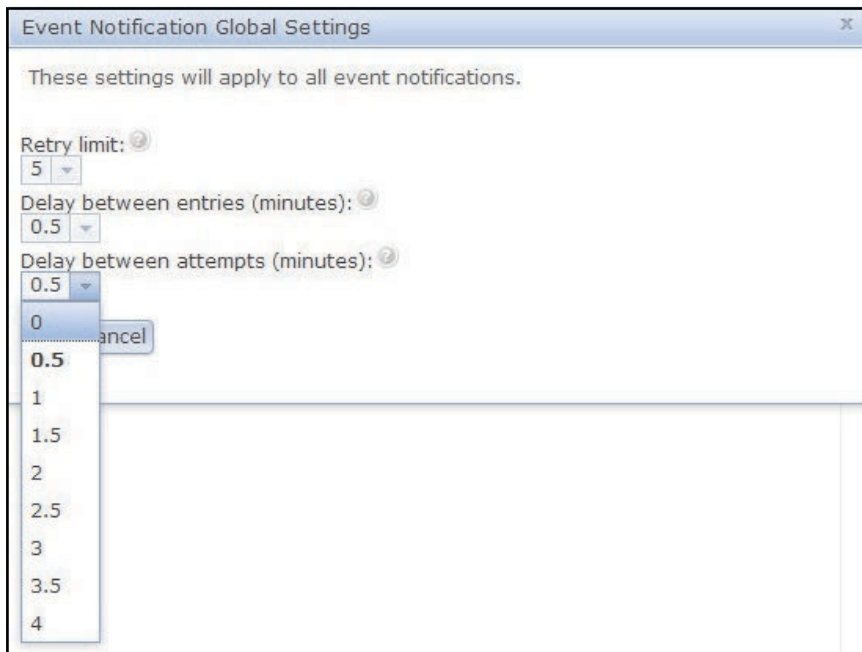
The following illustration shows the settings for the Retry limit option.



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



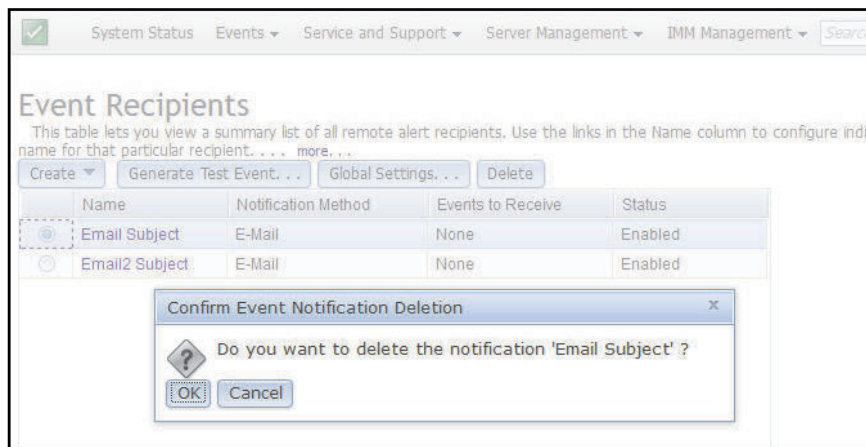
The following illustration shows the settings for the Delay between attempts (minutes) option.



Deleting email or syslog notifications

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

The following illustration shows the Confirm Event Notification Deletion window.

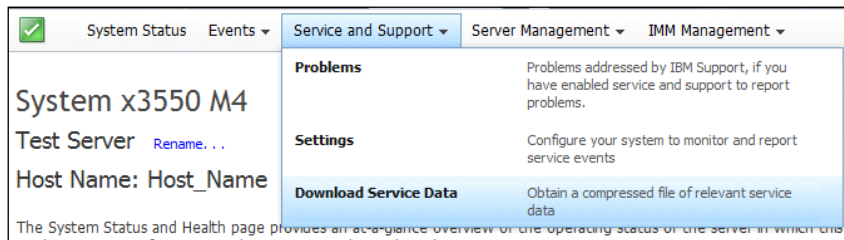


Collecting service and support information

Use the information in this topic to collect information about your server.

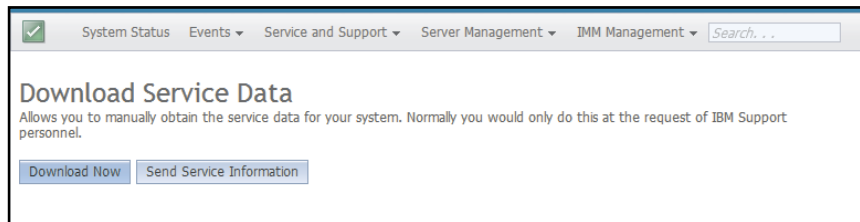
Click the **Download Service Data** option under the Service and Support menu to collect information about the server that can be used by Support to assist you with your problem.

The following illustration shows the Service and Support menu.



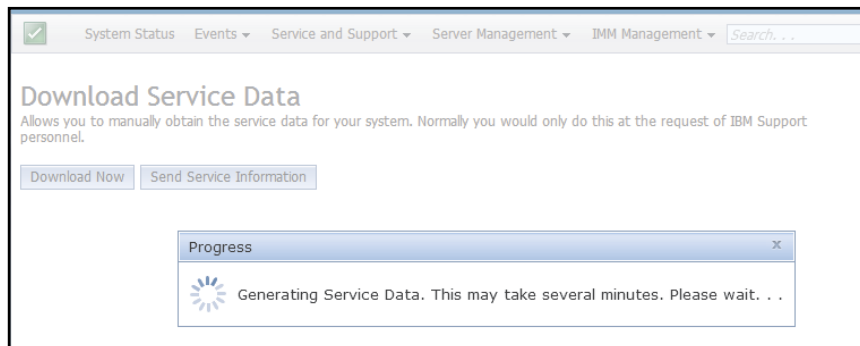
Click the **Download Now** button if you want to download the service and support data.

The following illustration shows the Download Service Data window.

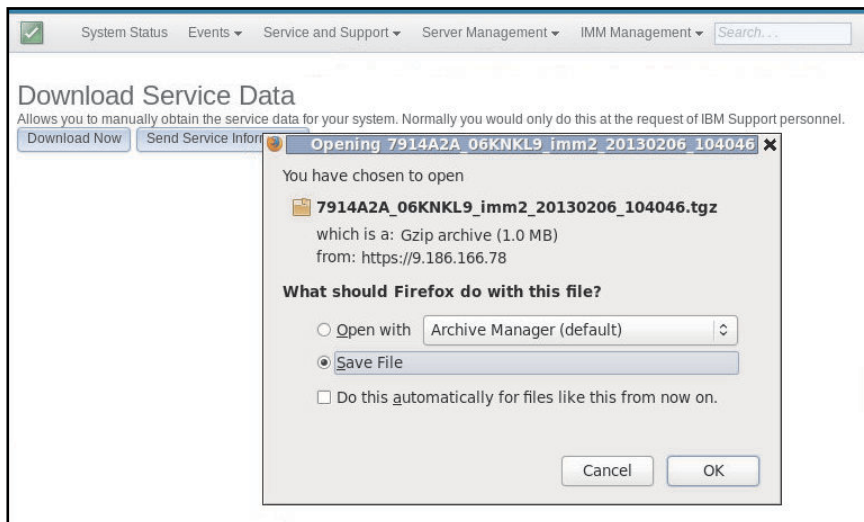


The process of collecting the service and support data starts. This process takes a few minutes to generate the service data that you can save to a file.

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



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



Capturing the latest OS failure screen data

Use the information in this topic to capture the operating system failure screen data and store the 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

To view power management information and perform power management functions, use the information in this topic.

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

To control how the power supply is managed use the information in this topic.

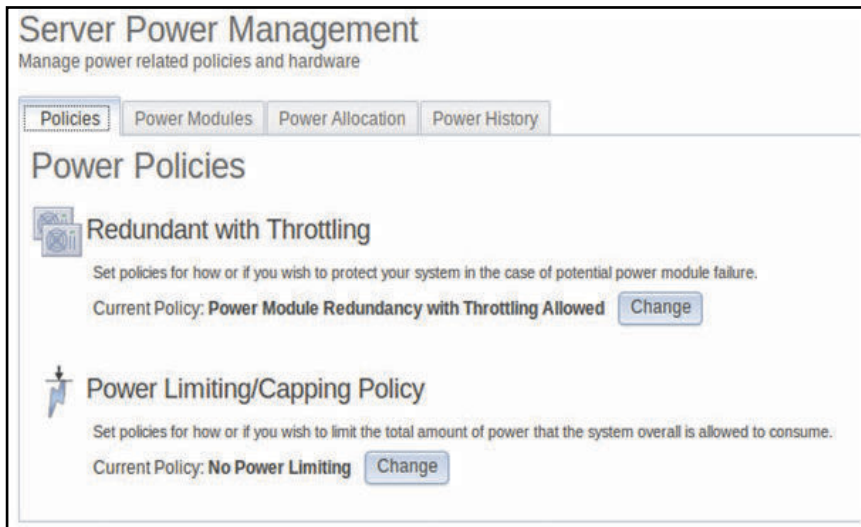
Click the **Policies** tab to control how the power supply is managed and optionally control total system power with the Active Energy Manager by setting a capping policy.

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

Configuring up to two power supplies

Use the information in this topic to configure up to two power supplies for your server.

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



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 Policies 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.

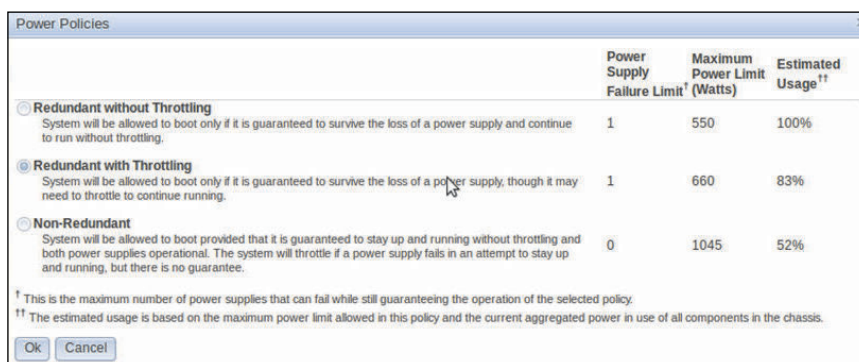
Redundant with Throttling

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

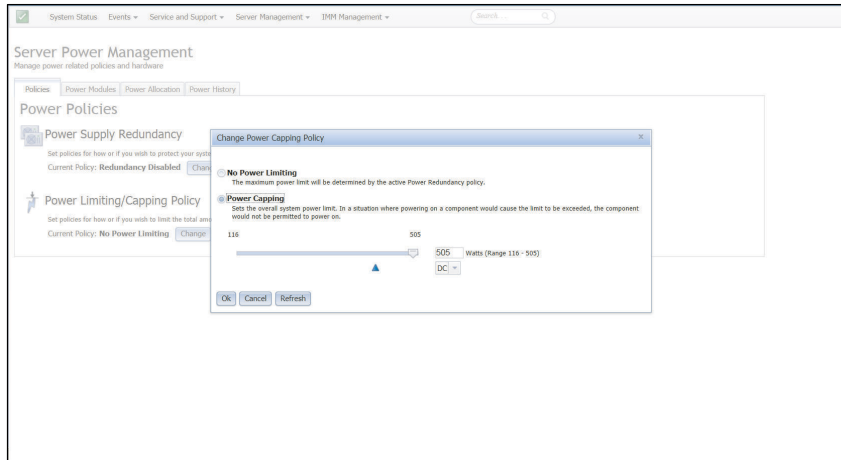
The server is allowed to boot provided the server is guaranteed to continue running without throttling and both power supplies are operational. The server will throttle if a power supply fails in an attempt to remain running; but, there is no guarantee.

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



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.



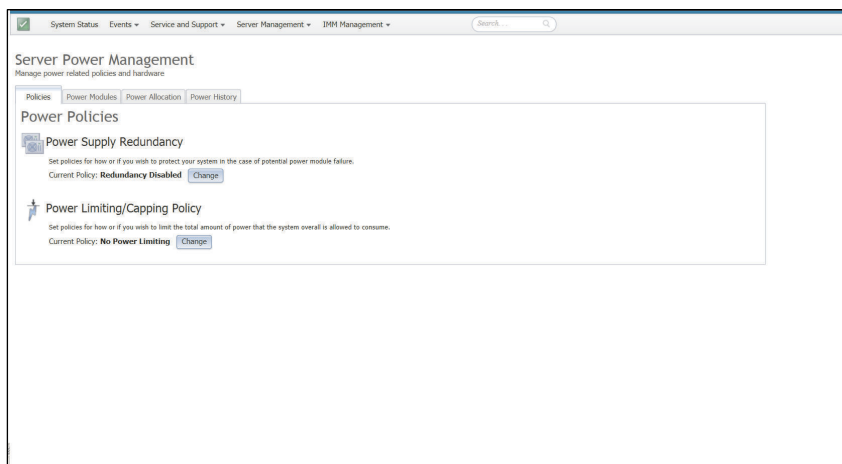
Configuring up to four power supplies

Use the information in this topic to configure up to four power supplies for your server.

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.



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.

The screenshot shows the 'Power Policies' window with the following sections:

- Power supply configuration:** A table with columns: Nominal Rating, Voltage, Effective Rating, Feed 1, and Feed 2.

	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:**
 - ☒ Budget for current configuration:

	With Full Throttling	With No Throttling
	461W	536W
 - ☐ Budget for all hot-plug components:

	With Full Throttling	With No Throttling
	596W	672W
- ☒ Allow Throttling to keep system within power budget
- ☒ N+N Redundancy (specify desired configuration/budget):

	N+0	N+N
<input checked="" type="radio"/> 1+1 with one 900W power supply per feed	900W	1080W
<input type="radio"/> 1+1 with one 1400W power supply per feed	1400W	1680W
<input type="radio"/> 2+2 with two 900W power supplies per feed	1710W	2052W
<input type="radio"/> 2+2 with one 900W and 1400W power supply per feed	2160W	2592W

Buttons: Ok, Cancel, Refresh

Available fields on the Power Policies 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.

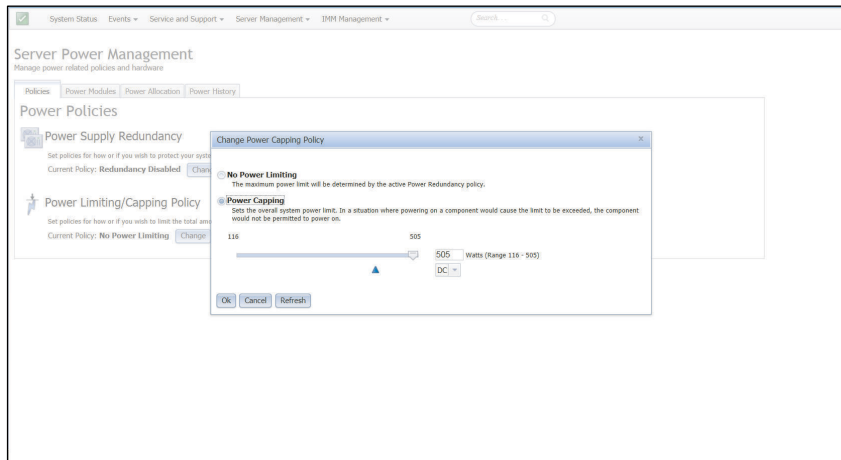
N+N Redundancy (specify desired configuration/budget)

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.

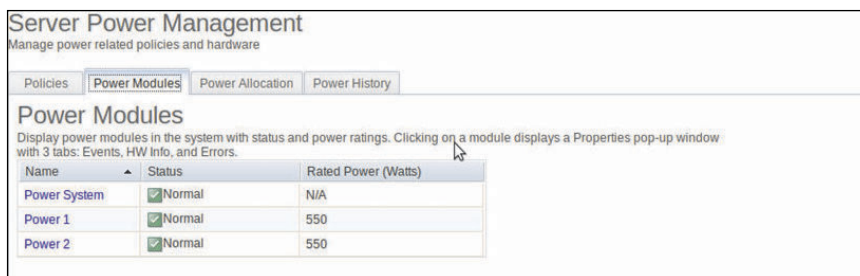


Displaying currently installed power supplies

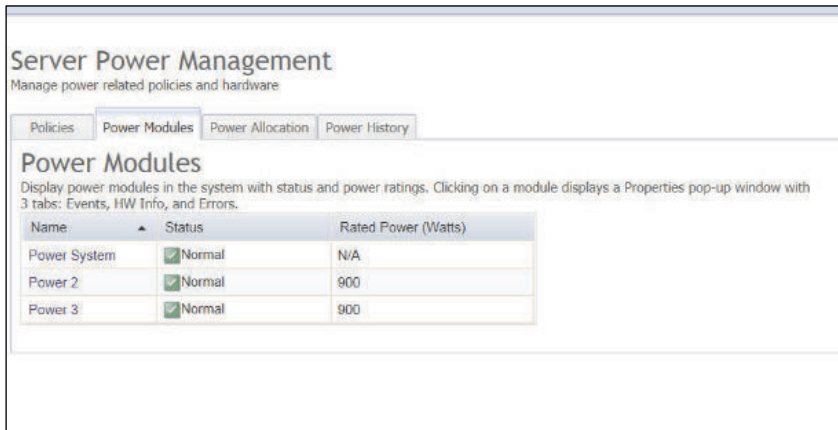
Use the information in this topic to display information about currently installed power supplies.

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.



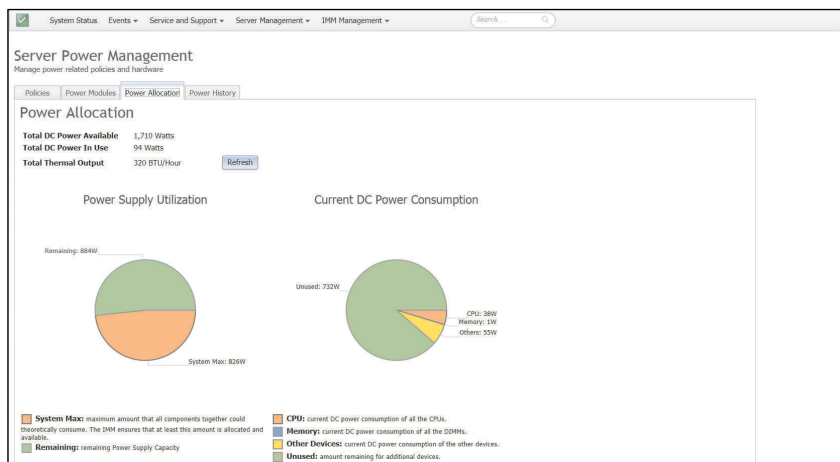
The following illustration shows the **Power Modules** tab for servers that can support up to four power supplies.



Displaying power supply capacity

Use the information in this topic to display the power consumption of the server.

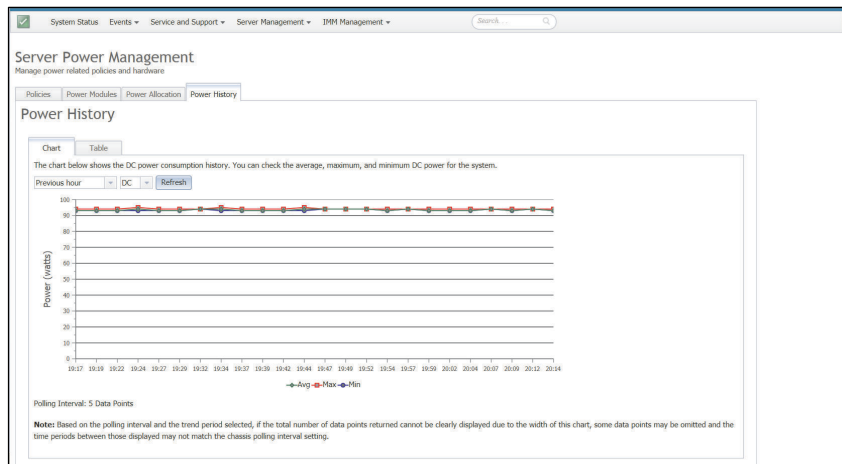
Click the **Power Allocation** tab to display how much power supply capacity is being used and to display the current dc power consumption of the server (as shown in the following illustration).



Displaying the power history

Use the information in this topic to display how much power is being used by the server for a selected time period

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).



Displaying the power performance

Use the information in this topic to display the power performance of the server.

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:

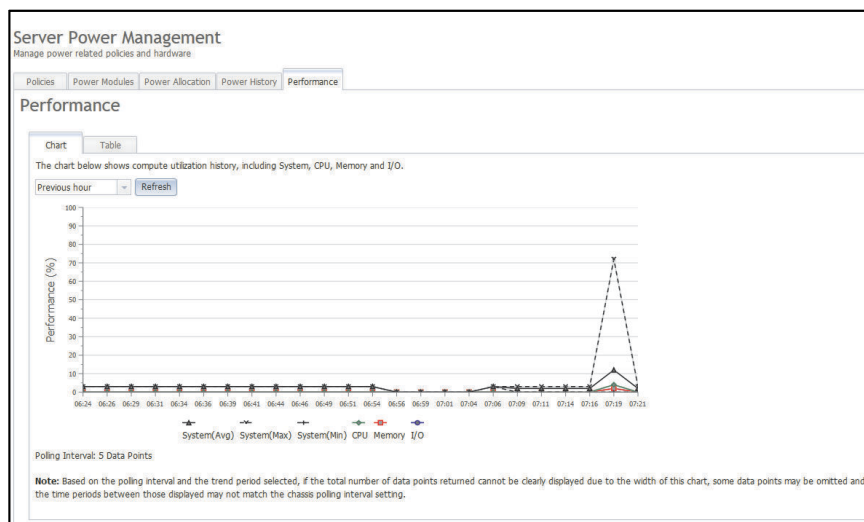
- System
- Microprocessor
- Memory
- I/O

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



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.

Policies Power Modules Power Allocation Power History Performance

Performance

Chart Table

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

Use the information in this topic to manage and monitor power consumption using 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

Use the information in this topic to manage the server power using the Node Manager.

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

Use the information in this topic to manage 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 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

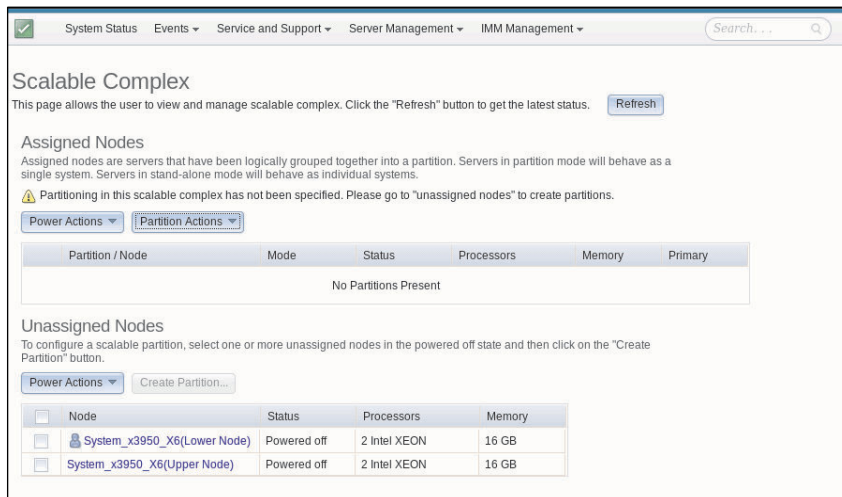
Use the information in this topic to configure a scalable complex that is used to view and manage the current state of all available servers.

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 consists 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 136 for additional information.

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



Creating a partition

Use the information in this topic to create a scalable complex partition.

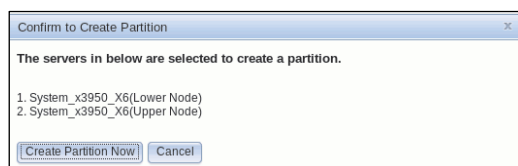
In the Unassigned nodes section of the Scalable Complex page, select the checkbox that corresponds to the nodes that you want to add to your partition.

Notes:

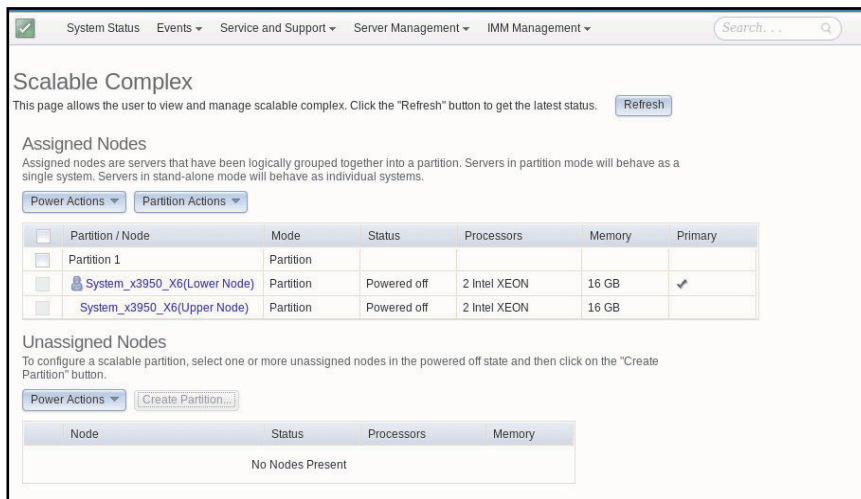
- To add a partition all power to the server must be turned off.
- The **Create Partition** button is grayed out until a node is selected.
- If you select the Node check box, all nodes are automatically included and marked as checked.
- Firmware versions of the nodes within the scalable complex must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

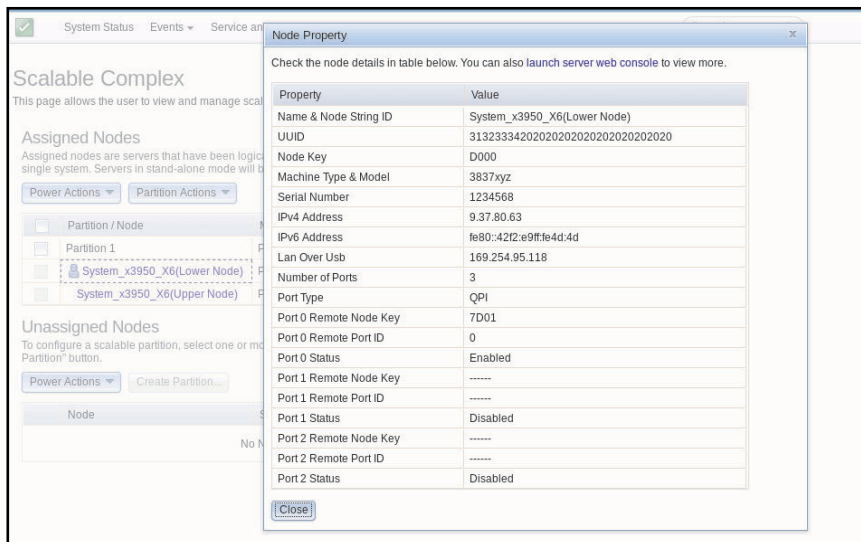
Note: Nodes in the partition mode of operation perform as one single system sharing resources.



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



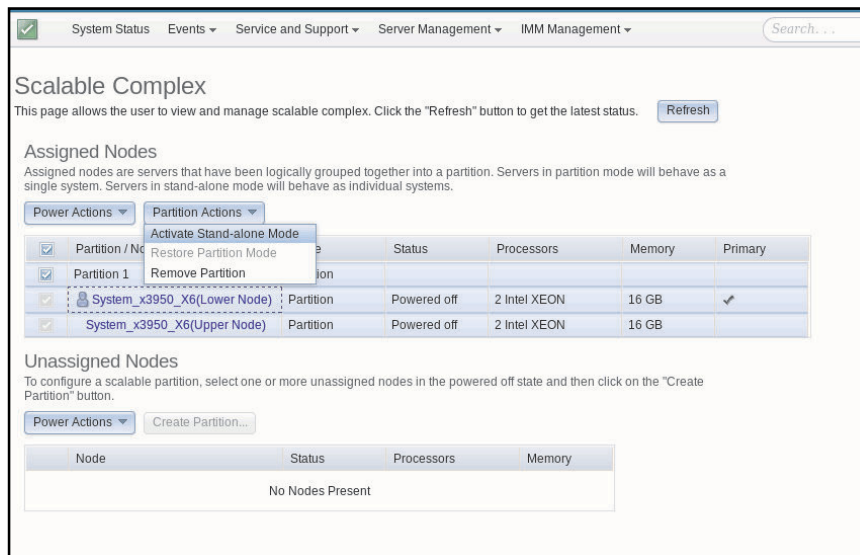
The details for a node are accessed by clicking on an individual node in the partition. The Node Property window is displayed (as shown in the following illustration).



Changing a partition mode

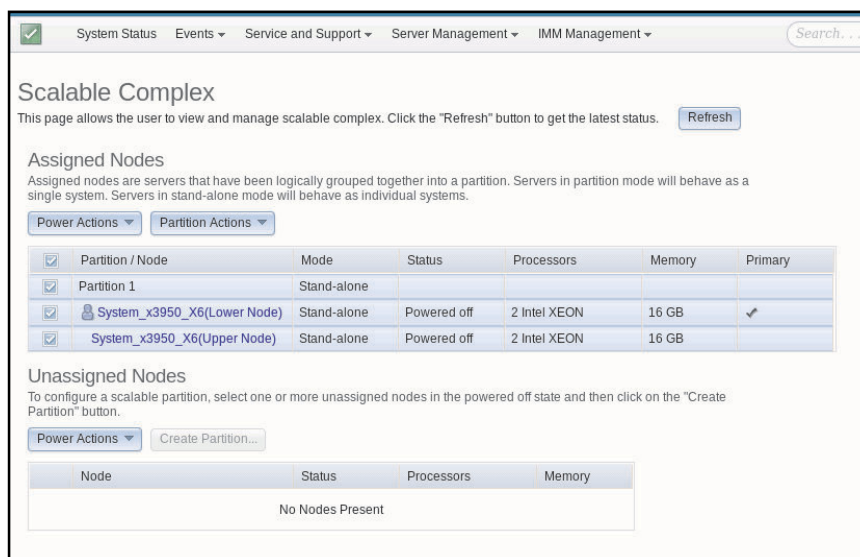
Use the information in this topic to change a scalable complex partition.

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).



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.

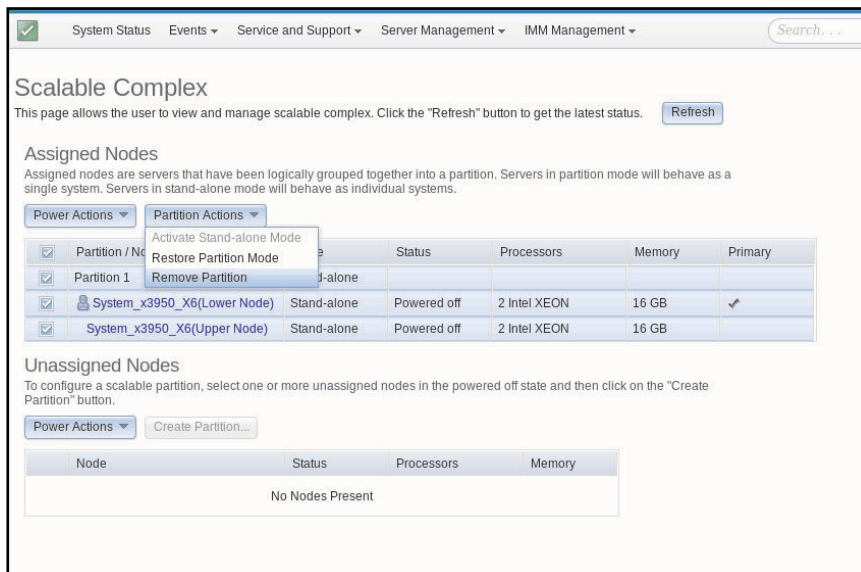


Deleting a partition mode

Use the information in this topic to delete a scalable complex partition.

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.



Partition errors

This topic provides example error messages that can occur when working with partitions.

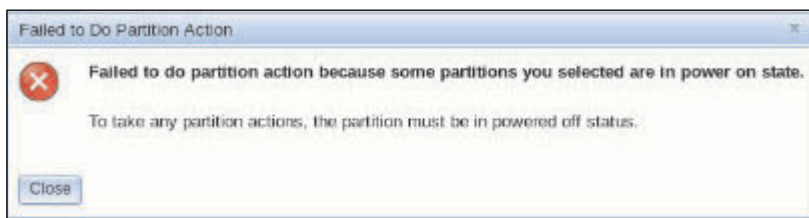
Error conditions can occur when working with partitions. If an error condition exists, the IMM2 will return an event code to the event logs. Two error conditions are described in the following table and displayed in the next two illustrations.

Table 10. Partition error conditions

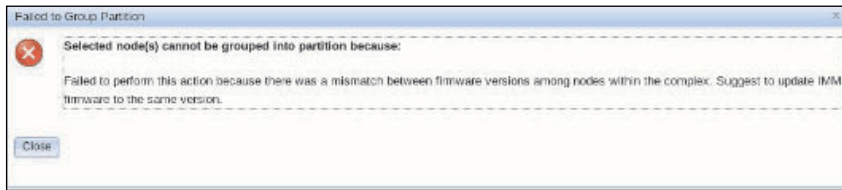
Three column table with two rows describing partition error messages and the action to take to resolve the error condition.

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.



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.



Viewing and configuring the local storage configuration

Use the information in this topic to view the storage status and configure storage information for the server.

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

Use the information in this topic to display the physical structure and storage configuration for the storage devices in the server.

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.

[Refresh](#)

Physical Resource [Storage RAID Configuration](#) [RAID Logs](#)

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

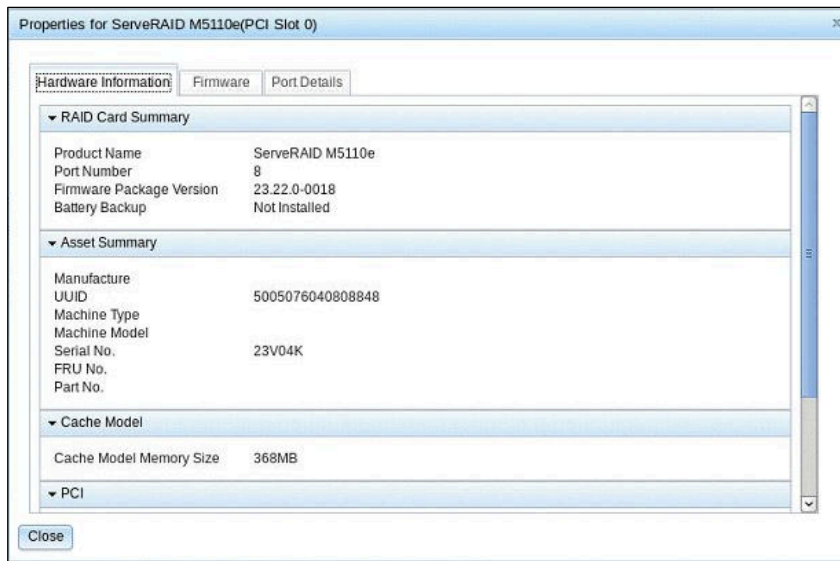
Flash DIMMs

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

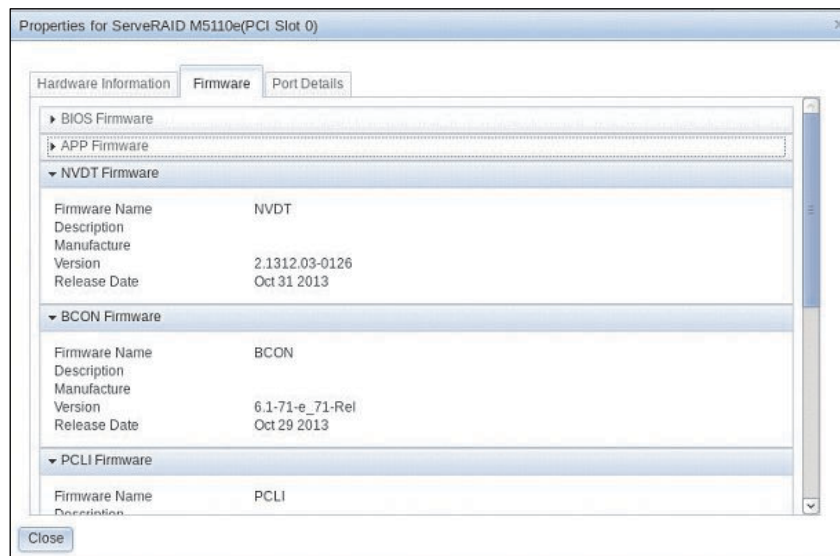
Click the link of the supported RAID controller to view the controller's active events, hardware, firmware, and port information.

The **Hardware Information** tab, contains the following information (as shown in the following illustration):

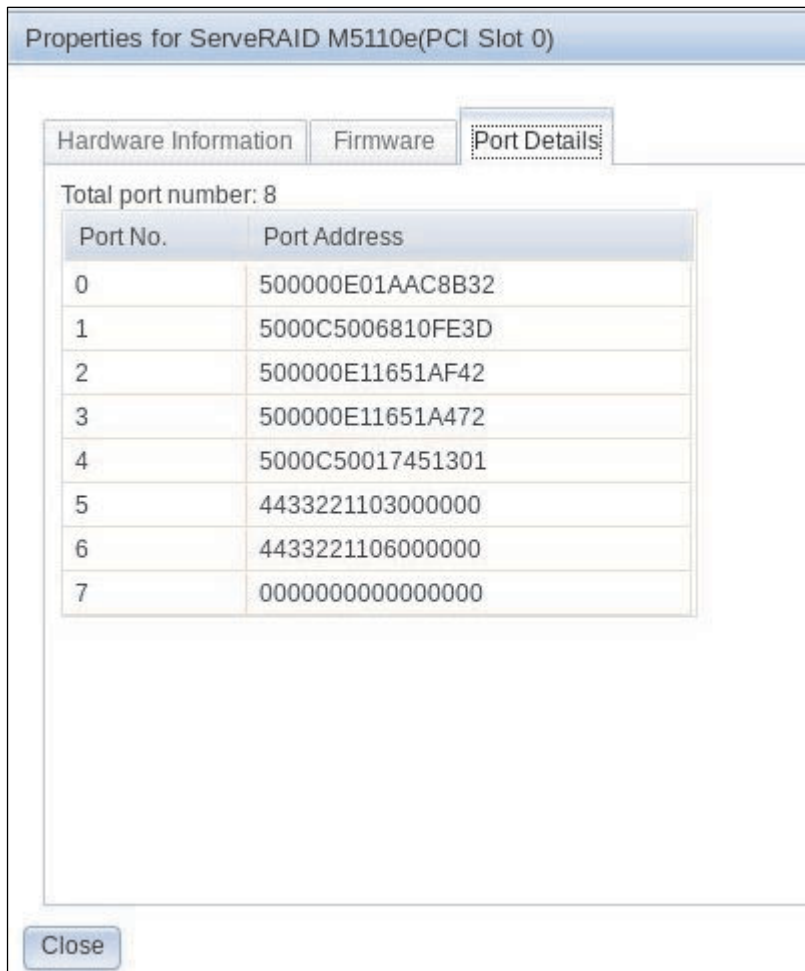
- RAID card summary
- Asset summary
- Cache model
- PCI
- Battery backup (if a battery backup has been installed)



The **Firmware** tab contains detailed firmware information for the RAID controller (as shown in the following illustration).



The **Port Details** tab contains the port number and port address information for the RAID controller (as shown in the following illustration).



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.

Properties for Drive 1

Events

Hardware Information

Firmware

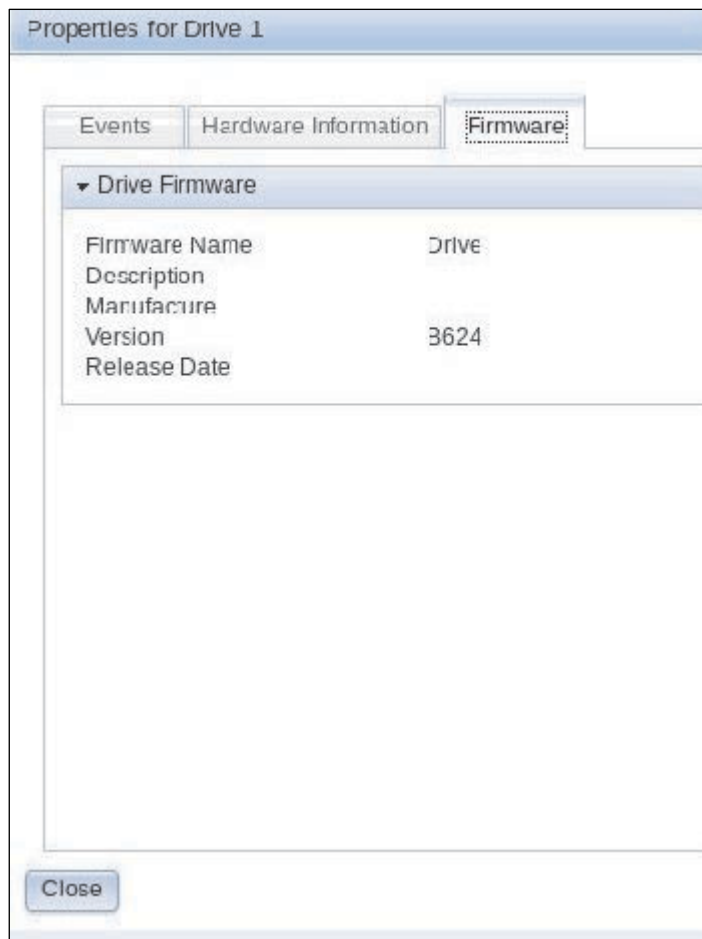
▼ Drive Summary

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

Close

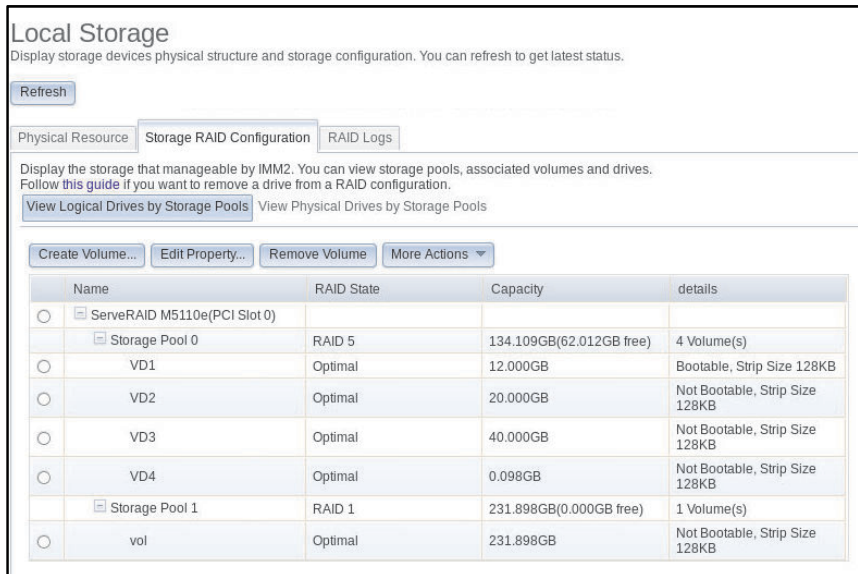


Displaying and configuring the storage RAID configuration information

Use the information in this topic to view and configure storage pools, associated volumes and drives for the RAID controller.

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.



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.

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](#)**

[Convert JBOD to Unconfigured Good...](#) [Assign Hot Spare...](#) [Change Drive State ▾](#)

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

Use the information in this topic to view the contents of the RAID logs.




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.

[Refresh](#)

Physical Resource Storage RAID Configuration **RAID Logs**

This page displays the contents of the RAID logs, and allows you to filter the log by severity levels.

Controller: Filters:   

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)
 Information	Configuration	2014-08-05 18:56:30	220	Foreign Configuration Cleared
 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
 Information	Configuration	2014-08-05 18:55:42	218	Foreign Configuration Detected
 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)
 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)
 Information	Physical Drive, Configuration	2014-08-04 21:13:57	136	Global Hot Spare PD 0d(e0xfc/s2) (global,rev) disabled

Displaying information and configuring the SD Media RAID adapter for System x

Use the information in this topic to view information and configure the SD Media RAID adapter.

The SD Media RAID Adapter for System x is an option that can be added to some server machine types. 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.

If this option is installed in the server, the SD controller and card(s) are displayed on the **Physical Resource** tab of the Local Storage web page (as shown in the following illustration).

Local Storage

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

[Refresh](#)

Physical Resource Storage RAID Configuration SD Configuration RAID Logs

Click on a device to see properties.

RAID Controllers and Physical Drives

Name	Health Status	Capacity	Serial Number
<input type="checkbox"/> Controller1ProductName (PCI Slot No.)			
Drive 1	<input checked="" type="checkbox"/> Normal	30.000GB	D3A047JF
Drive 2	<input checked="" type="checkbox"/> Normal	20.000GB	D3A04K82
Drive 4	<input checked="" type="checkbox"/> Normal	30.000GB	D3A04Z93
<input type="checkbox"/> Non-manageable drives to IMM			
Drive 5	<input checked="" type="checkbox"/> Normal	30.000GB	D3A04U47
Drive 6	<input checked="" type="checkbox"/> Normal	30.000GB	D3A03A32

SD Cards

Name	Health Status	Capacity	Serial Number
<input type="checkbox"/> SD Card Controller1			
SD card 1	<input checked="" type="checkbox"/> Healthy	30.000GB	9XE090GTST9250610NS
SD card 2	<input type="checkbox"/> Unhealthy	20.000GB	9XG01KJRST9100640NS

Click the link for the SD card controller or click the SD card to view its properties (as shown in the following two illustrations).

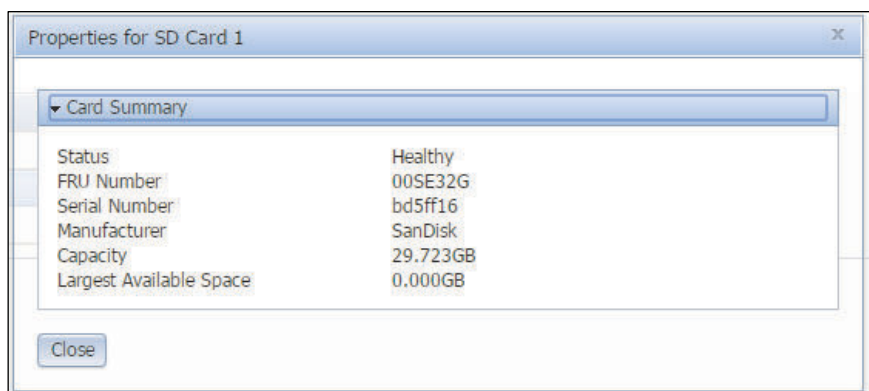
Properties for SD Card Controller 1

▼ Controller Summary

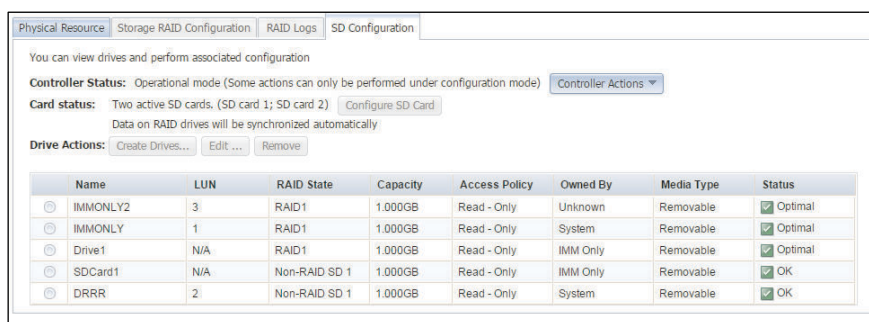
Product Name	SD Media Adapter for System x
Hardware Revision	3.0
Firmware Version	1.3.2.171
Serial Number	
FRU No	00AN748
Mode	Operational mode

[Close](#)

The **Largest Available Space** field on the Properties for SD Card page indicate the remaining capacity that is available to create a RAID drive. To create a RAID drive using two SD cards, the maximum storage space that can be configured is the *lower* value of the two cards **Largest Available Space** properties.



The SD card controller, the SD card, and drive information can be viewed and configured on the **SD Configuration** tab of the Local Storage page (as shown in the following illustration).



The remaining sections in this topic provide descriptive information for the fields on the SD Configuration page.

The **Controller Status** field determines what type of drive operations can be performed. There are four types of controller status modes:

- Configuration
 - In this mode there is no active file operation being run and you can execute any operation available on this page.
- Operational
 - File operations are actively running and you can only execute a very *basic* edit of drive operation. All other drive actions are greyed out.
 - Partitions cannot be created or deleted while the controller is in the Operational mode.
 - The IMM2 can claim ownership of a system partition, format the partition, save or load contents, and return ownership to the system.
 - When in this mode, the drive owner can only be changed to **System** if the system is powered on.
- Unmanaged
 - This mode occurs when the SD card controller has recently been updated or reset and needs to be re-activated.
- Unknown
 - In this mode you *cannot* perform any drive operation.
 - This mode will rarely occur. When the system has a problem reading data from the SD card controller, check that the hardware option is properly seated; otherwise, contact Support for assistance.

Notes:

- The controller status can only be manually toggled between the **Configuration** and **Operational** status modes.
- The **Unmanaged** and **Unknown** status modes might occur; but, the feature will usually be in the **Configuration** or **Operational** status mode.

The status of a drive on a SD card can be in one of the following states:

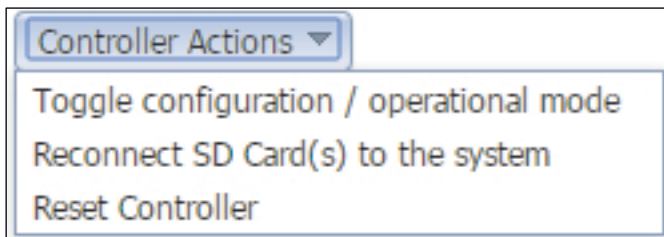
- Optimal
 - This state only applies to RAID drives. This state implies that both SD cards are in a healthy state and drive operations are functioning as expected.
- Degraded
 - This state only applies to RAID drives and indicates that one of the two SD cards for the drive is currently failing.

Note: The **Physical Resource** tab shows the health status of the SD cards.

- Ok
 - This state only applies to Non-RAID drives and indicates that the drive on the SD card is operating as expected.
- Failed
 - This state implies that all SD cards associated with the drive have failed.

Note: The **Physical Resource** tab displays the health status of the SD cards.

From the **Controller Actions** menu you can perform the following controller actions (as shown in the following illustration).



- Toggle between the **Configuration** and **Operational** status modes.
 - This action item allows you to swap between the two modes to configure drives or perform file operations.
- Reconnect SD Card(s) to the system
 - Execute a hardware disconnect or reconnect sequence between the SD Media Adapter and the system chipset.
 - Can be used in cases where the IMM2 is performing operations on one or more disks that it has ownership of and you want the device and any new logical unit number (LUN), to be completely rediscovered by the server.
- Reset Controller
 - When the SD card controller firmware is updated to a new level, this controller action must be manually run.

The **Card Status** field displays the presence of the connected SD Cards. Click the **Configure SD Card** button to open the following window.

You can select one SD card to view the drive information, set it as primary card, or format the card

SD Card 1 Set as Primary Card Initialize the SD Card(s)

Health: **Healthy** State: **Active**

Drive list in SD card: 1

Name	LUN	RAID State	Capacity	Status
IMMONLY2	3	RAID1	1.000GB	Optimal
IMMONLY	1	RAID1	1.000GB	Optimal
Drive1	0	RAID1	1.000GB	Optimal
SDCard1	0	Non-RAID SD 1	1.000GB	OK
DRRR	2	Non-RAID SD 1	1.000GB	OK

You can select a specific SD Card to view the drive information and run the **Set as Primary Card** or **Initialize the SD Card(s)** actions:

- Set as Primary Card
 - The selected SD card is configured as the Primary card. From this point all RAID configured drives are mirrored from this drive. If you select a new Primary card, all data on the secondary card is lost. RAID data is automatically synced between the two cards after this action.
- Initialize the SD Card(s)
 - This action clears all data on both SD cards.

From the **Drive Actions** field you can perform the following actions:

- Create drives
- Edit
- Remove

Click the **Create Drives...** button to create a new drive. You can only create drives while the SD card controller is in Configuration mode. The fields in the Create New drive window are shown in the following illustration.

Drive Name:

RAID State:

Owned By:

Media Type:

Access Policy:

Set as LUN 0: ☐

Define the Drive capacity by:

☒ Using fixed capacity.

Apply Cancel

Drive name

Must be a unique string value and follow a proper string format; otherwise, the following error message will prevent you from continuing.

Please enter a drive name with only 15 valid letters, numbers, or _

Media type

Removable
Non-Removable

Raid state

Non-RAID SD1: This creates a drive on SD Card1 and is independent of SD Card2.

Non-RAID SD2: This creates a drive on SD Card2 and is independent of SD Card1.

RAID1: This creates a mirrored drive using both SD Cards. The Primary card is selected in the Configure SD Card window on the SD Configuration page.

Note: The SD Cards only support RAID drives of type RAID1 (mirrored mode).

Access Policy

Read - Only
Read - Write

Owned By

IMM: The drive can be controlled and mounted by the IMM2. The server is not aware of this drive.

System: The drive cannot be mounted by the IMM2, but the IMM2 still controls drive metadata. The drive can be mounted by the server.

IMM Only: The drive can be controlled and mounted by the IMM2. The server sees a LUN for the drive; but, the drive responds with Not Ready, so the operating system sees a LUN size of 0. The operating system continues to test the drive every second until it becomes accessible. This value is used when transferring ownership of a single drive between the server and the IMM2 without forcing a physical disconnect of all the drives at the same time.

System Only: The drive cannot be mounted by the IMM2. The IMM2 control of the drive metadata cannot be regained until the server power is turned off. The drive can be mounted by the server.

Set as LUN 0

This field will set the drive to be discovered by UEFI as the generic Hypervisor boot target and will override the current LUN 0 drive.

Note: Drives with owners of *IMM Only* are not assigned a LUN number and cannot be set as LUN 0.

Using fixed capacity

This field produces an error if a capacity value is entered that exceeds the largest available free space; thus, preventing the user from creating a drive. Refresh the SD Configuration page to update the **Largest Available Space**.

Click the **Edit...** button to change certain drive properties (as shown in the following illustration).

Notes:

- In order to edit a drive, a drive must be selected.
- Not all drive properties on the Create Drives page can be changed.

	Name	LUN	RAID State	Capacity	Access Policy	Owned By	Media Type	Status
⊕	IMMONLY2	3	RAID1	1,000GB	Read - Only	System	Removable	Optimal
⊖	IMMONLY	1	RAID1	1,000GB	Read - Only	IMM	Removable	Optimal

The settings that can be configured or viewed in the **Configuration** or **Operational** status modes are shown in the following two illustrations.

Note: The System Power might occasionally be displayed as *on* even if the system power is off. The current state of the system power is shown on the System Status page.

Controller status: Configuration mode System Power: On

Drive Properties

Drive Name: IMMONLY2 Media Type: Removable

Owned By: System Access Policy: Read - Only

RAID State: RAID1

Capacity: 1.000GB

Apply Cancel

Controller status: Operational mode System Power: On

Drive Properties

Drive Name: IMMONLY2 Media Type: Removable

Owned By: System Access Policy: Read - Only

RAID State: RAID1

Capacity: 1.000GB

Apply Cancel

Click the **Remove** button to clear an entire drive and return its allocated storage space back to the SD card (as shown in the following illustration).

Note: A drive must be selected; otherwise, the button is greyed out.

Local Storage

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

Refresh

Physical Resource Storage RAID Configuration **SD Configuration** RAID Logs

You can view Drives and perform associated configuration.

Controller status: Operational mode (Some actions can only be performed under configuration mode.) Controller Actions ▾

Card status: Two active SD cards: (SD card 1; SD card 2) Configure SD Card

Data on RAID drives will be synchronized automatically.

Drive actions: Create Drives ... Edit ... Remove

	Name	LUN	RAID State	Capacity	Access Policy	Owned By	Media Type
<input type="radio"/>	Drive 1	0	RAID 1	100.000GB	Read - Only	IMM	Non- Removable
<input checked="" type="radio"/>	Drive 2	1	RAID 1	30.000GB	Read - Only	IMM	Removable
<input type="radio"/>	Drive 3	2	Non-RAID SD 1	20.000GB	Read - Write	System	Removable
<input type="radio"/>	Drive 4	6	Non-RAID SD 2	30.000GB	Read - Write	IMM only	Removable
<input type="radio"/>	Drive 5	4	RAID 1	30.000GB	Read - Write	System only	Removable

Viewing the adapter information and configuration settings

Use the information in this topic to view information about the PCIe adapters installed in the server.

Click the **Adapters** option under the **Server Management** tab to view information about the PCIe adapters installed in the server.

- 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.

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	

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

▼ 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	000000000000000000000006CAE8B2C1668
Manufacturer	IBM
Serial No.	I3212CT05K
Part No.	0C111102-F-X
Model	0C111102-F-X
FRU No.	N/A
FoD UID	8NFZGMG2NJYK1MEGAHH45AEGZ9HKMHDV
Max Data Width	8
Package Type	Unknown

▼ PCI Summary

Close

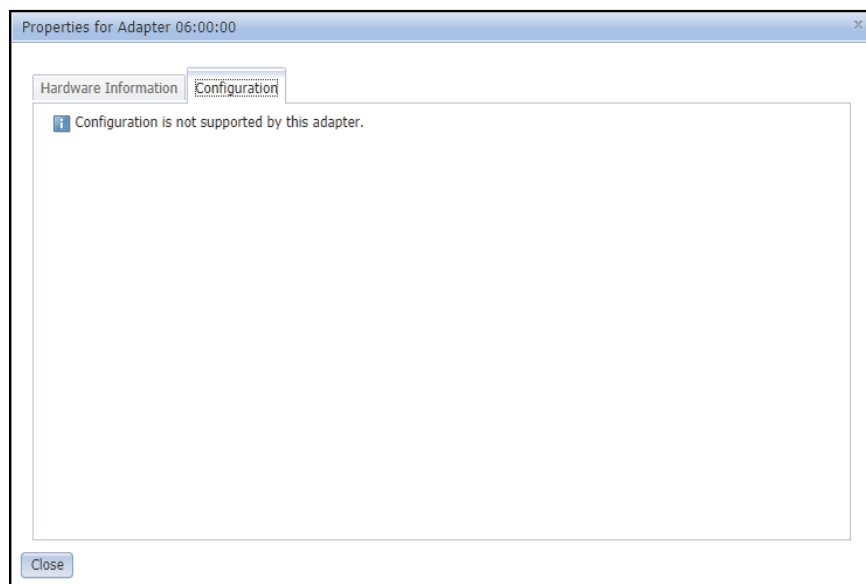
Configuring the adapter information

Chapter 6. Performing IMM2 tasks **201**

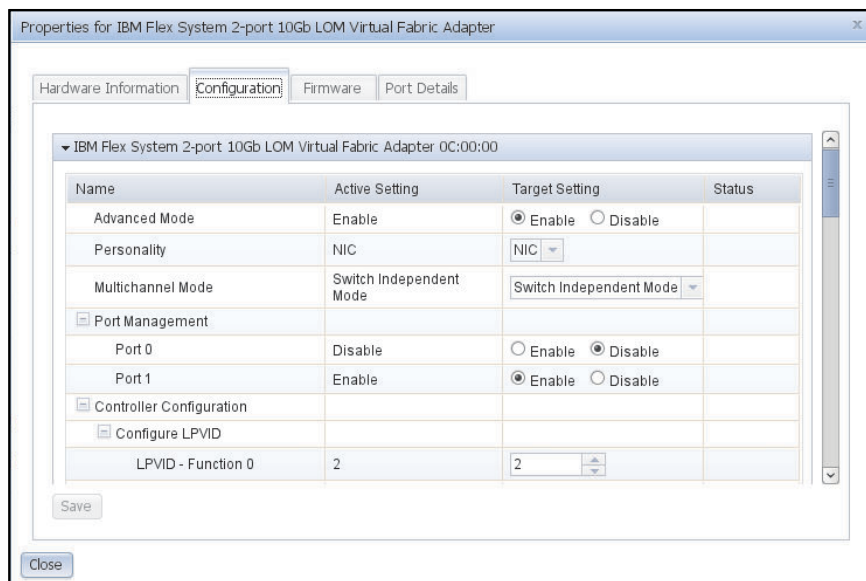
On the Properties for Adapter page click the **Configuration** tab to display and change the configuration information for the adapter.

Note: The **Configuration** tab is only visible when the user authority level is set to **Supervisor** or **Adapter Configuration - Advanced**.

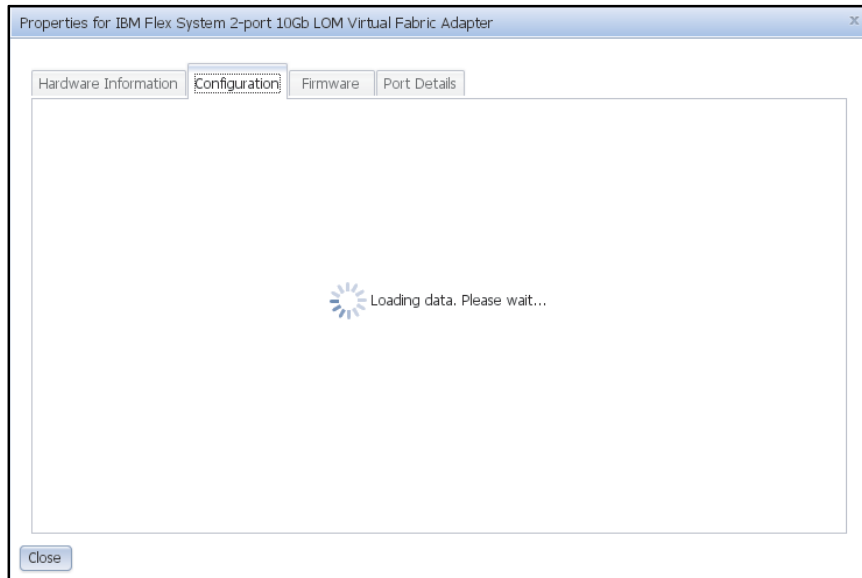
If an adapter does not support the configuration functionality (for example, a SAS or graphic processing unit (GPU) adapter), the following window is displayed.



If an adapter does support the configuration functionality, all changeable settings are listed, (as shown in the following illustration).

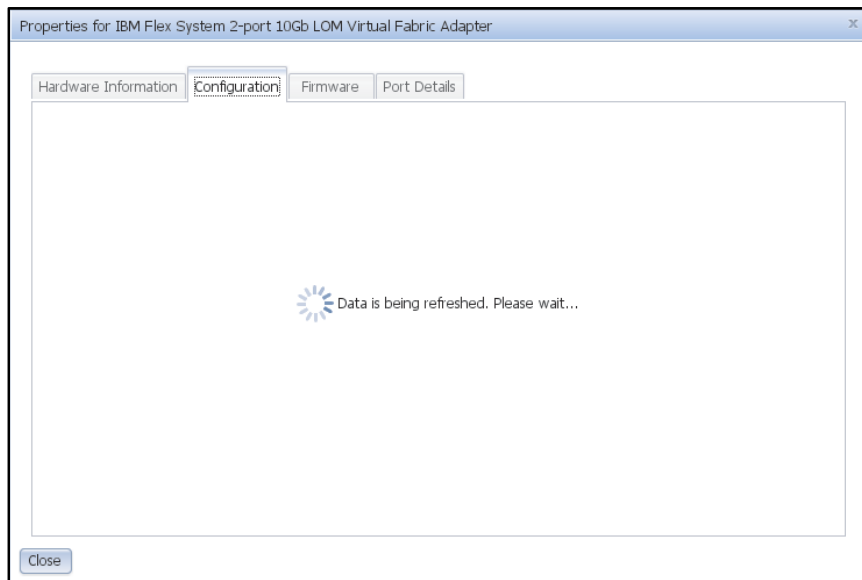


It takes several moments for the IMM2 to load the adapter information into the window. When you click the **Configuration** tab and if the settings are not completely loaded, you will see the following message Loading data, Please wait (as shown in the following illustration).



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).



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

Hardware Information Configuration Firmware Port Details

Secondary Target

Boot to Target	Disabled	<input type="radio"/> Enabled <input checked="" type="radio"/> 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

Save

Close

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

Hardware Information Configuration Firmware Port Details

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	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Personality	NIC	NIC	
Multichannel Mode	Switch Independent Mode	IBM Virtual Fabric Mode	Pending
Port Management			
Port 0	Disable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Pending
Port 1	Enable	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Controller Configuration			
Configure LPVID			
LPVID - Function 0	2	2	

Save

Close

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 Users Guide* at <https://lenovopress.com/redp4895-using-lenovo-features-on-demand>.

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 <https://lenovopress.com/redp4895-using-lenovo-features-on-demand>.

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.

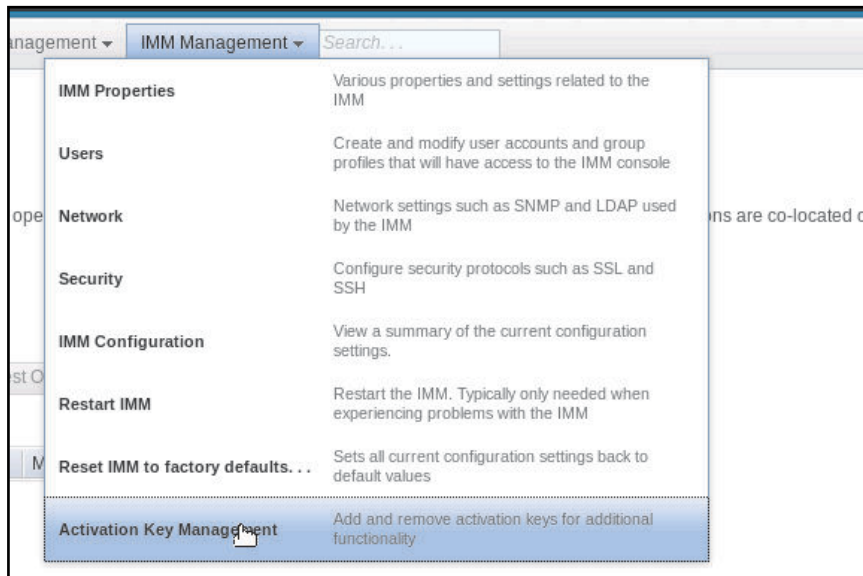
See “[Installing an activation key](#)” on page 205, “[Removing an activation key](#)” on page 208 or “[Exporting an activation key](#)” on page 209 for information about managing an FoD activation key using the IMM2 web interface. See “[keycfg command](#)” on page 247 for information about managing an FoD activation key using the IMM2 CLI.

Installing an activation key

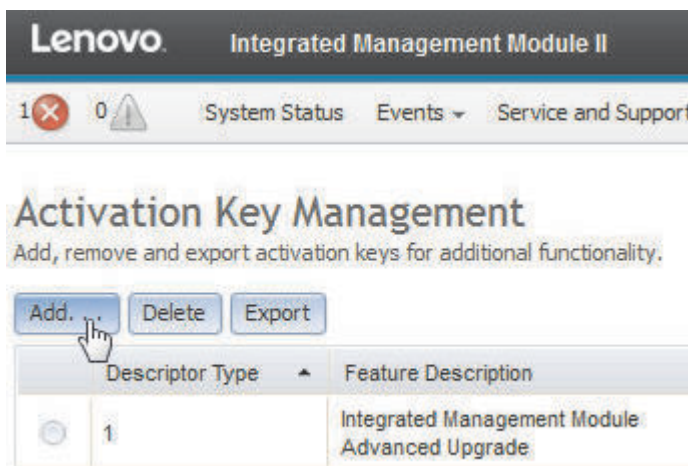
Use the information in this topic to add an optional feature to your server.

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

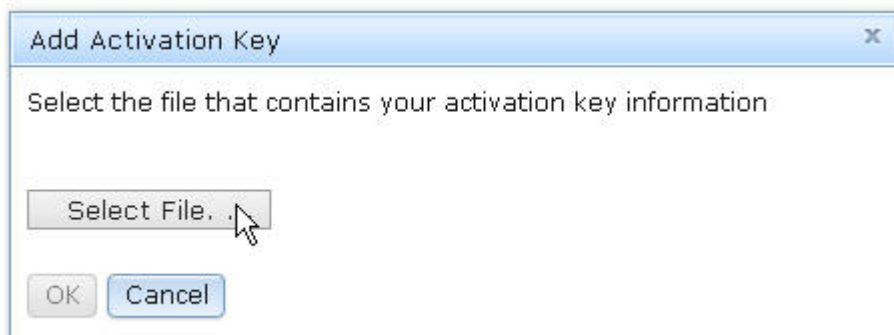
- Step 1. Log in to the IMM2. For more information, see “[Logging in to the IMM2](#)” on page 11.
- Step 2. From the IMM2 web interface, click on the **IMM Management** tab; then, click **Activation Key Management**.



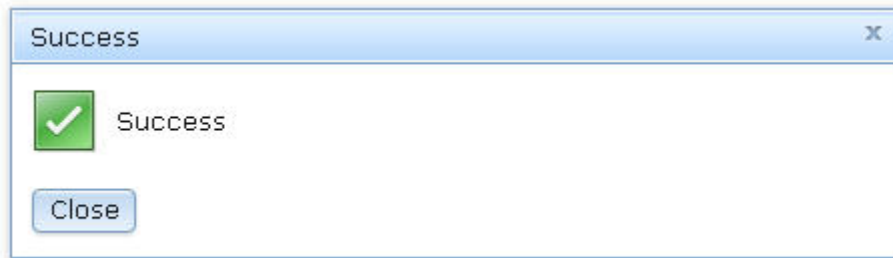
Step 3. From the Activation Key Management page, click **Add....**



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

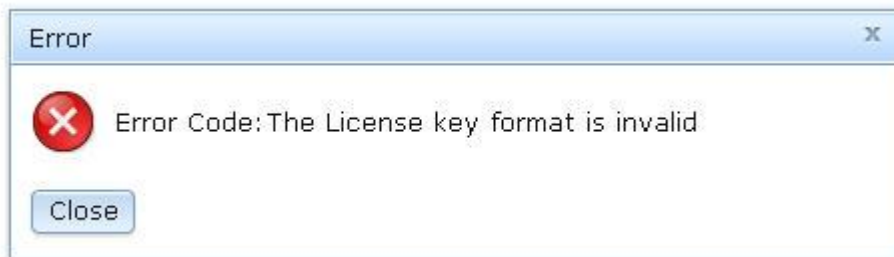


The Success window indicates that the activation key is installed.

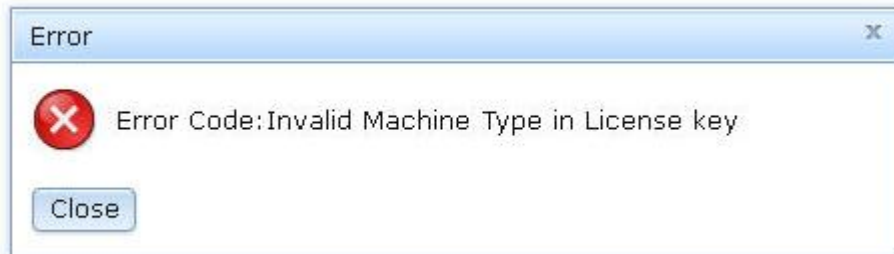


Notes:

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



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



Step 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.

Support | **File Transfer Server** | HTTP Proxy

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. [less...](#)

☒ **Enable File Transfer Server**

Protocol:
FTP

IP address or host name: 9.115.232.123 Port: 21

User name: USERID

Password: ••••••••

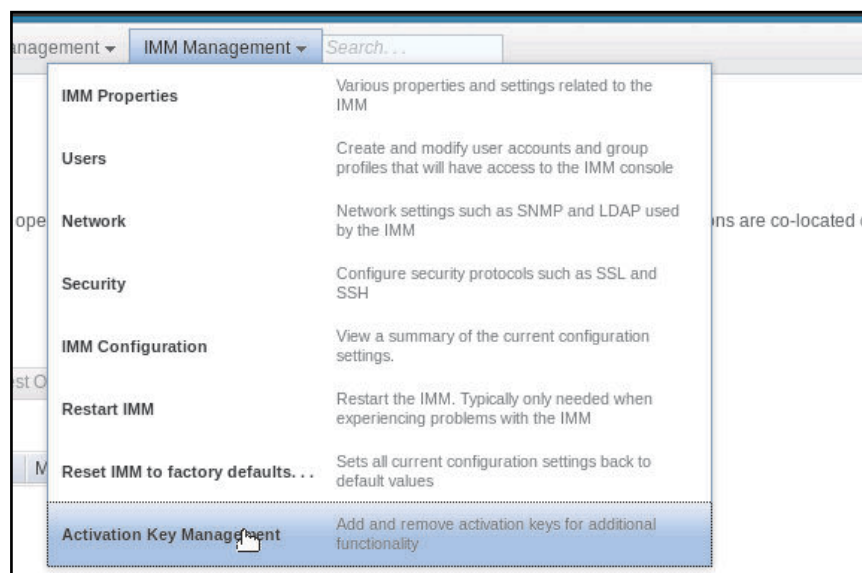
Apply File Transfer Server Settings Reset

Removing an activation key

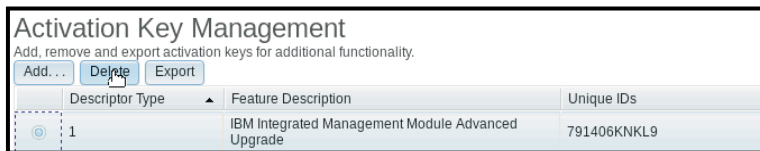
Use the information in this topic to delete an optional feature from your server.

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

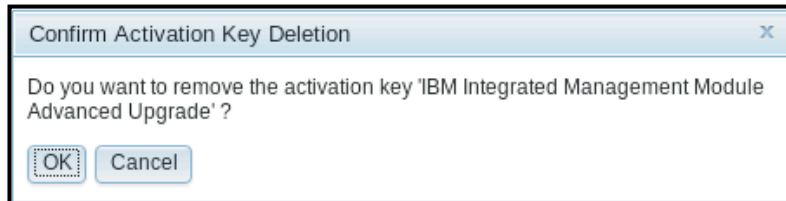
- Step 1. Log in to the IMM2. For more information, see [“Logging in to the IMM2” on page 11](#).
- Step 2. From the IMM2 web interface, click on the **IMM Management** tab; then, click on **Activation Key Management**.



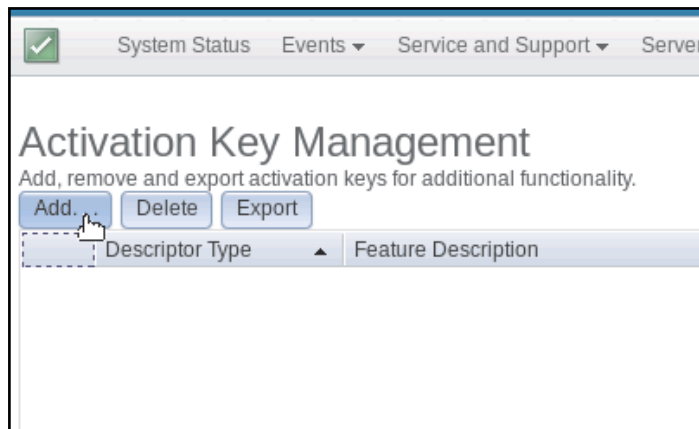
- Step 3. From the Activation Key Management page, select the activation key to remove; then, click **Delete**.



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



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

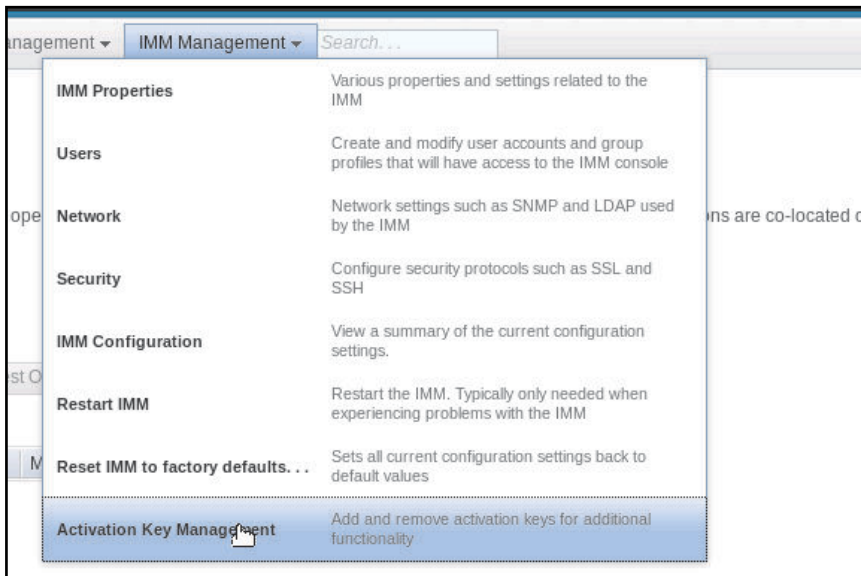


Exporting an activation key

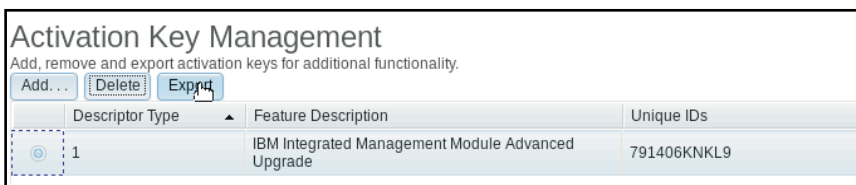
Use the information in this topic to export an optional feature from your server.

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

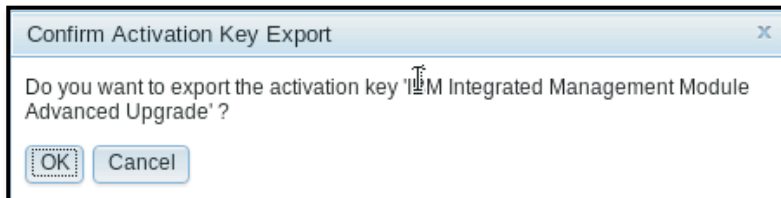
- Step 1. Log in to the IMM2. For more information, see [“Logging in to the IMM2” on page 11](#).
- Step 2. From the IMM2 web interface, click on the **IMM Management** tab; then, click on **Activation Key Management**.



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



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



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

Chapter 8. Command-line interface

Use the information in this topic to enter commands that manage and monitor the IMM2 without having to use the IMM2 web interface.

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

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

Managing the IMM2 with IPMI

Use the information in this topic to manage the IMM2 using the Intelligent Platform Management Interface (IPMI).

The IMM2 comes with User ID 1 set initially to a user name of USERID and password of PASSWORD (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 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/PASSWORD 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” on page 211](#).

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” on page 211](#).

Using IPMITool

Use the information in this topic to access information about the 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 <https://sourceforge.net/projects/ipmitool/>.

Accessing the command-line interface

Use the information in this topic to access the CLI.

To access the CLI, start a Telnet or SSH session to the IMM2 IP address (see [“Configuring serial-to-Telnet or SSH redirection” on page 212](#) for more information).

Logging in to the command-line session

Use the information in this topic to log in to the command line session.

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

- Step 1. Establish a connection with the IMM2.
- Step 2. At the user name prompt, type the user ID.
- Step 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

This topic provides information about using the IMM2 as a serial terminal server.

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

Review the guidelines in this topic to understand how to enter commands in the CLI.

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

This topic contains information about CLI 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

This topic contains a list of CLI commands in alphabetic order. Links are provided to topics for each command. Each command topic provides information about the command, its function, syntax, and usage.

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

- [“accseccfg command” on page 232](#)
- [“alertcfg command” on page 234](#)
- [“alertentries command” on page 308](#)
- [“asu command” on page 235](#)
- [“autoftp command” on page 313](#)
- [“autopromo command” on page 238](#)
- [“backup command” on page 239](#)
- [“batch command” on page 310](#)
- [“chconfig command” on page 314](#)
- [“chlog command” on page 316](#)
- [“chmanual command” on page 317](#)
- [“clearcfg command” on page 311](#)
- [“clearlog command” on page 219](#)
- [“clock command” on page 311](#)
- [“console command” on page 231](#)
- [“cryptomode command” on page 239](#)

- “dhcpcinfo command” on page 241
- “dns command” on page 242
- “ethtousb command” on page 243
- “events command” on page 317
- “exit command” on page 216
- “fans command” on page 220
- “ffdc command” on page 220
- “fuelg command” on page 226
- “gprofile command” on page 244
- “help command” on page 216
- “history command” on page 216
- “identify command” on page 312
- “ifconfig command” on page 245
- “info command” on page 312
- “keycfg command” on page 247
- “ldap command” on page 248
- “led command” on page 221
- “ntp command” on page 250
- “passwordcfg command” on page 251
- “ports command” on page 252
- “portcfg command” on page 253
- “portcontrol command” on page 254
- “power command” on page 228
- “pxeboot command” on page 230
- “readlog command” on page 223
- “reset command” on page 230
- “resetsp command” on page 313
- “restore command” on page 255
- “restoredefaults command” on page 255
- “scale command” on page 256
- “sdemail command” on page 318
- “sdraid command” on page 265
- “set command” on page 278
- “smtp command” on page 278
- “snmp command” on page 279
- “snmpalerts command” on page 282
- “spreset command” on page 313
- “srcfg command” on page 283
- “sshcfcg command” on page 284
- “ssl command” on page 285
- “sslcfcg command” on page 286

- [“storage command” on page 289](#)
- [“storekeycfg command” on page 299](#)
- [“syshealth command” on page 224](#)
- [“telnetcfg command” on page 300](#)
- [“temps command” on page 225](#)
- [“thermal command” on page 302](#)
- [“timeouts command” on page 302](#)
- [“tls command” on page 301](#)
- [“usbeth command” on page 303](#)
- [“users command” on page 303](#)
- [“volts command” on page 225](#)
- [“vpd command” on page 226](#)

Utility commands

This topic provides an alphabetic list of utility CLI commands.

The utility commands are as follows:

- [“exit command” on page 216](#)
- [“help command” on page 216](#)
- [“history command” on page 216](#)

exit command

Use this command to log off the CLI session,

Use the **exit** command to log off and end the CLI session.

help command

This command displays a list of all commands.

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

This command provides a list of previously issued commands.

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

This topic provides an alphabetic list of monitor CLI commands.

The monitor commands are as follows:

- [“adapter command” on page 217](#)
- [“clearlog command” on page 219](#)
- [“fans command” on page 220](#)
- [“ffdc command” on page 220](#)
- [“led command” on page 221](#)
- [“readlog command” on page 223](#)
- [“storage command” on page 289](#)
- [“syshealth command” on page 224](#)
- [“temps command” on page 225](#)
- [“volts command” on page 225](#)
- [“vpd command” on page 226](#)

adapter command

This command is used to display PCIe adapter inventory information.

All servers do not support the **adapter** command. If the **adapter** command is not supported, the server responds with the following message when the command is issued:

Your platform does not support this command.

If you remove, replace, or configure any adapters, you must restart the server (at least once) to view the updated adapter information.

The following table shows the arguments for the options.

Table 11. adapter command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 11. adapter command (continued)

Option	Description	Values
-list	List all PCIe adapters in the server	
-show <i>target_id</i>	Show the detailed information for the target PCIe adapter	<i>target_id</i> [<i>info</i>] <i>firmware</i> <i>ports</i> <i>chips</i> Where: <ul style="list-style-type: none"> <i>info</i>: display the hardware information for the adapter <i>firmware</i>: display all firmware information for the adapter <i>ports</i>: display all Ethernet port information for the adapter <i>chips</i>: 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

This command is used to clear the IMM2 event log.

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.

Note: This command is intended only for support personnel use.

The following table shows the arguments for the options.

Table 12. clearlog command

The following table is a one-row two column table consisting of the option and option descriptions.

Option	Description
-t <all platform audit>	Event type, choose which type of event to clear. If not specified, all event types will be selected.

Event type descriptions

- **all**: All event type, including platform event and audit event.
- **platform**: Platform event type.
- **audit**: Audit event type.

Example:

```
system> clearlog
All event log cleared successfully
system> clearlog -t all
All event log cleared successfully
system> clearlog -t platform
Platform event log cleared successfully
system> clearlog -t audit
Audit event log cleared successfully
```

fans command

This command is used to display the velocity of the server fans.

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

This command is used to generate a new service data file.

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.

Table 13. *ffdc* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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	

Table 13. *ffdc* command (continued)

Option	Description	Values
-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 this command to display and set LED states.

The **led** command displays and sets the server LED states.

- Running the **led** command with no options displays the status of the 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.

Table 14. *led command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-l	Get the status of all system and system subcomponent LEDs	
-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

This command displays the IMM2 event logs.

Use the **readlog** command to display the IMM2 event log entries. Five event logs are displayed 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

This command provides a summary of the health or active events.

Use the **syshealth** command to display a summary of the health or active events of the server. The power state, system state, hardware state (includes fan, power supply, storage, processor, memory), restart count, and IMM2 software status are displayed.

Syntax:

syshealth [argument]

argument:

- summary -display the system health summary
- activeevents -display active events
- cooling - display cooling devices health status
- power - display power modules health status
- storage - display local storage health status
- processors - display processors health status
- memory - display memory health status

Example:

```
system> syshealth summary
Power    On
State    OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

temps command

This command displays all temperature and temperature threshold information.

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	N/A	N/A	80/27	N/A	N/A
CPU2	N/A	N/A	80/27	N/A	N/A
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 (Positive-going Threshold Hysteresis value)
 - W: warning (Upper non-critical Threshold)
 - T: temperature (Current value)
 - SS: soft shutdown (Upper critical Threshold)
 - HS: hard shutdown (Upper non-recoverable Threshold)
2. All temperature values are in degrees Fahrenheit/Celsius.
3. N/A represents not applicable.

volts command

Use this command to display the server voltage information.

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
```

	i	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 (Lower non-recoverable Threshold)
- SSL: soft shutdown low (Lower critical Threshold)

WL: warning low (Lower non-critical Threshold)
WRL: warning reset low (Negative-going Threshold Hysteresis value)
V: voltage (current value)
WRH: warning reset high (Positive-going Threshold Hysteresis value)
WH: warning high (Upper non-critical Threshold)
SSH: soft shutdown high (Upper critical Threshold)
HSH: hard shutdown high (Upper non-recoverable Threshold)

vpd command

This command displays configuration and informational data (vital product data) associated with the hardware and software of the server.

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), server components (comp) and PCIe devices (pcie). The same information is displayed as in the web interface.

Syntax:

```
vpd [argument]
argument:
sys
imm
uefi
dsa
fw
comp
pcie
```

Example:

```
system> vpd dsa
Type      Status      Version      Build      ReleaseDate
-----
DSA       Active       9.36         DSYTAE2    2013/01/18
system>
```

Server power and restart control commands

This topic provides an alphabetic list of power and restart CLI commands.

The server power and restart commands are as follows:

- [“fuelg command” on page 226](#)
- [“power command” on page 228](#)
- [“pxeboot command” on page 230](#)
- [“reset command” on page 230](#)

fuelg command

This command displays information about the server power.

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.

Table 15. *fuelg* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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 <i>fuelg</i> command, with no options, on the target.	numeric wattage value
-pc	Display current power consumption	ac,dc
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
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
- perf
- pc *ac|dc*
- pm *bt|r|rt*
- mpc *cc|ahp*
- at *on|off*
- r *on|off*
- nn

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

power command

This command describes how to control the server power.

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

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

Table 16. power command

The following table is a multi-row three column table consisting of the power commands, command descriptions, and associated values for the commands.

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.	
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 enterS3 parameter is not supported on all servers.	
power rp	Use this option to specify the host power restore policy.	alwayson alwayssoff 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 S3resume parameter 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.

Table 17. power command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 17. *power* command (continued)

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
-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

This command displays and sets 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.

Table 18. *pxeboot command*

The following table is a single-row three column table consisting of the option, option description, and associated values for the option.

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

This command describes how to reset the server.

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.

Table 19. *reset command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 19. *reset command (continued)*

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

This topic contains the serial redirect command.

There is one serial redirect command: the [“console command” on page 231](#).

console command

This command is used to start a serial redirect console session.

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

Syntax:

`console 1`

Configuration commands

This topic provides an alphabetic list of configuration CLI commands.

The configuration commands are as follows:

- [“accseccfg command” on page 232](#)
- [“alertcfg command” on page 234](#)
- [“asu command” on page 235](#)
- [“autopromo command” on page 238](#)
- [“backup command” on page 239](#)
- [“cryptomode command” on page 239](#)
- [“dhcpinfo command” on page 241](#)
- [“dns command” on page 242](#)
- [“ethtousb command” on page 243](#)
- [“gprofile command” on page 244](#)

- “ifconfig command” on page 245
- “keycfg command” on page 247
- “ldap command” on page 248
- “ntp command” on page 250
- “passwordcfg command” on page 251
- “ports command” on page 252
- “portcfg command” on page 253
- “portcontrol command” on page 254
- “restore command” on page 255
- “restoredefaults command” on page 255
- “sdraid command” on page 265
- “set command” on page 278
- “smtp command” on page 278
- “snmp command” on page 279
- “snmpalerts command” on page 282
- “srcfg command” on page 283
- “sshcfg command” on page 284
- “ssl command” on page 285
- “sslcfg command” on page 286
- “storage command” on page 289
- “storekeycfg command” on page 299
- “telnetcfg command” on page 300
- “thermal command” on page 302
- “timeouts command” on page 302
- “tls command” on page 301
- “usbeth command” on page 303
- “users command” on page 303

accseccfg command

Use this 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.

Table 20. accseccfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 20. *accseccfg* command (continued)

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 this 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.

Table 21. *alertcfg* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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

This command is used to set UEFI settings.

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

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

Table 22. asu command

The following table is a multi-row three column table consisting of a subset of commands that can be used in conjunction with the **asu** command. Descriptive information and associated values for the commands are provided.

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.	<i>setting_instance</i>
help	Use this command to display help information for one or more settings.	<i>setting</i>
set	Use this command to change the value of a setting. Set the UEFI setting to the input value. Notes: <ul style="list-style-type: none">• 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."	<i>setting value</i>
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.	<i>setting</i>
show	Use this command to display the current value of one or more settings.	<i>setting</i>

Table 22. *asu* command (continued)

Command	Description	Value
showvalues	<p>Use this command to display all possible values for one or more settings.</p> <p>Notes:</p> <ul style="list-style-type: none"> • 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. 	<i>setting</i>
<p>Notes:</p> <ul style="list-style-type: none"> • In the command syntax, <i>setting</i> is the name of a setting that you want to view or change, and <i>value</i> is the value that you are placing on the setting. • <i>Setting</i> can be more than one name, except when using the set command. • <i>Setting</i> can contain wildcards, for example an asterisk (*) or a question mark (?). • <i>Setting</i> 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.

Table 23. *asu* options

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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 .	

Table 23. *asu options (continued)*

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

Syntax:

asu [*options*] **command** [*cmdopts*]

options:

-v *verbose output*
 --help *display main help*

cmdopts:

--help *help for the command*

Note: See individual commands for more command options.

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

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

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

Table 24. *asu transaction commands*

The following table is a multi-row three column table consisting of the transactions commands, the command descriptions, and associated values for the commands.

Command	Description	Value
tropen <i>id</i>	This command creates a new transaction file containing several settings to be set.	<i>id</i> is the identifying string, 1 - 3 alphanumeric characters.
trset <i>id</i>	This command adds one or more settings or value pairs to a transaction.	<i>id</i> is the identifying string, 1 - 3 alphanumeric characters.
trlist <i>id</i>	This command displays the contents of the transaction file first. This can be useful when the transaction file is created in the CLI shell.	<i>id</i> is the identifying string, 1 - 3 alphanumeric characters.

Table 24. asu transaction commands (continued)

Command	Description	Value
trcommit <i>id</i>	This command commits and executes the contents of the transaction file. The results of the execution and any errors will be displayed.	<i>Id</i> is the identifying string, 1 - 3 alphanumeric characters.
trrm <i>id</i>	This command removes the transaction file after it has been committed.	<i>Id</i> 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

This command is used to display and configure settings for the automated promotion of backup firmware.

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.

Table 25. autopromo command

The following table is a single-row three column table consisting of the option, option description, and associated values 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 this command to create a backup file containing the current system security settings.

The following table shows the arguments for the options.

Table 26. *backup command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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*

username

-pw *password*
-fd *filename*

Example:

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

```
ok
```

```
system>
```

cryptomode command

Use this command to display and configure the compliance mode with the exceptions for encryption.

The following table shows the arguments for the options.

Table 27. *cryptomode command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 27. *cryptomode* command (continued)

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 <i>NIST</i> , 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>
```

dhcpcinfo command

Use this command to view the DHCP server-assigned IP configuration for eth0.

Use the **dhcpcinfo** 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:

```
dhcpcinfo eth0
```

Example:

```
system> dhcpcinfo eth0
```

```
*s192.168.70.29
*nIMM2A-00096B9E003A
*i192.168.70.202
*g192.168.70.29
*s255.255.255.0
*dlinux-sp.raleigh.ibm.com
*d192.168.70.29
*d0.0.0.0
*d0.0.0.0
*i0::0
*d6
*d0s61
*d0s62
*d0s63
```

```
system>
```

The following table describes the output from the example.

Table 28. *dhcpcinfo* command

The following table is a multi-row two column table describing the options that are used in the previous example.

Option	Description
-server	DHCP server that assigned the configuration
-n	Assigned host name
-i	Assigned IPv4 address
-g	Assigned gateway address
-s	Assigned subnet mask
-d	Assigned domain name
-dns1	Primary IPv4 DNS server IP address
-dns2	Secondary IPv4 DNS IP address
-dns3	Tertiary IPv4 DNS server IP address
-i6	IPv6 address
-d6	IPv6 domain name
-dns61	Primary IPv6 DNS server IP address

Table 28. *dhcpcinfo* command (continued)

Option	Description
-dns62	Secondary IPv6 DNS IP address
-dns63	Tertiary IPv6 DNS server IP address

dns command

Use this 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.

Table 29. *dns* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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.

```
system> dns
+ sstabled
+ i192.168.70.202
+ i292.168.70.208
+ i392.168.70.212
+ i680::21a:64ff:fee6:4d5
+ i680::21a:64ff:fee6:4d6
+ i680::21a:64ff:fee6:4d7
+ dwnabled
+ didm.com
+ didmcom
+ dnlsep
-p ipv6
```

The following table describes the options used in the previous example.

Table 30. *dns* command output

The following table is a multi-row two column table describing the options used in the previous 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)
-dnsrsc	Preferred DDNS domain name (dhcp or manual)
-ddn	Manually specified DDN
-ddncur	Current DDN (read only)
-p	Preferred DNS servers (ip v4 or ip v6)

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.

Table 31. `ethtousb` command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 31. *ethtousb* command (continued)

Option	Description	Values
-en	Ethernet-over-USB state	enabled, disabled
-mx	Configure port mapping for index <i>x</i>	Port pair, separated by a colon (:), of the form <i>port1:port2</i> Where: <ul style="list-style-type: none"> The port index number, <i>x</i>, is specified as an integer from 1 to 10 in the command option. <i>port1</i> of the port pair is the External Ethernet port number. <i>port2</i> 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 this command to display and configure group profiles for the IMM2.

The following table shows the arguments for the options.

Table 32. *gprofile* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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 <i>group_name</i> . The <i>group_name</i> must be unique.
-a	Role-based authority level	supervisor, operator, rbs <role list>: nsc am rca rcvma pr bc cell 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 this 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.

Table 33. *ifconfig* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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).

Table 33. ifconfig command (continued)

Option	Description	Values
-dn	Domain name	Domain name in valid format.
-auto	Autonegotiation setting, which determines whether the Data rate and Duplex network settings are configurable	true, false
-nic	NIC access. 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: <ol style="list-style-type: none"> 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 this command to display, add, or delete activation keys.

Activation keys control access to optional IMM2 Features on Demand (FoD) features.

Notes:

- 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.

Table 34. *keycfg* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-add	Add activation key	Values for the -ip, -pn, -u, -pw, and -f command options
-ip	IP address of TFTP server with activation key to add	Valid IP address for TFTP server
-pn	Port number for TFTP/SFTP server with activation key to add	Valid port number for TFTP/SFTP server (default 69/22)
-u	User name for SFTP server with activation key to add	Valid user name for SFTP server
-pw	Password for SFTP server with activation key to add	Valid password for SFTP server
-f	File name for activation key to add	Valid file name for activation key file
-del	Delete activation key by index number	Valid activation key index number from keycfg listing
-deltype	Delete activation key by key type	Valid key type value

Syntax:

keycfg [*options*]

option:

-add

-ip *ip_address*

port_number

username

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 this command to display and configure the LDAP protocol configuration parameters.

The following table shows the arguments for the options.

Table 35. *Idap command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-a	User authentication method	local only, LDAP only, local first then LDAP, LDAP first then local
-aom	Authentication only mode	enabled, disabled
-b	Binding method	anonymous, bind with ClientDN and password, bind with Login Credential
-c	Client distinguished name	String of up to 127 characters for <i>client_dn</i>
-d	Search domain	String of up to 63 characters for <i>search_domain</i>
-f	Group filter	String of up to 127 characters for <i>group_filter</i>
-fn	Forest name	For active directory environments. String of up to 127 characters.
-g	Group search attribute	String of up to 63 characters for <i>group_search_attr</i>
-l	Login permission attribute	String of up to 63 characters for <i>string</i>
-p	Client password	String of up to 15 characters for <i>client_pw</i>
-pc	Confirm client password	String of up to 15 characters for <i>confirm_pw</i> Command usage is: <code>Idap -p <i>client_pw</i> -pc <i>confirm_pw</i></code> This option is required when you change the client password. It compares the <i>confirm_pw</i> argument with the <i>client_pw</i> 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 <i>root_dn</i>
-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 <i>host name/ip_addr</i>
-s2ip	Server 2 host name/IP address	String up to 127 characters or an IP address for <i>host name/ip_addr</i>
-s3ip	Server 3 host name/IP address	String up to 127 characters or an IP address for <i>host name/ip_addr</i>
-s4ip	Server 4 host name/IP address	String up to 127 characters or an IP address for <i>host name/ip_addr</i>
-s1pn	Server 1 port number	A numeric port number up to 5 digits for <i>port_number</i>
-s2pn	Server 2 port number	A numeric port number up to 5 digits for <i>port_number</i>
-s3pn	Server 3 port number	A numeric port number up to 5 digits for <i>port_number</i>
-s4pn	Server 4 port number	A numeric port number up to 5 digits for <i>port_number</i>
-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.

Table 35. *ldap command (continued)*

Option	Description	Values
-u	UID search attribute	String of up to 63 characters for <i>search_attr</i>
-v	Get LDAP server address through DNS	off, on
-h	Displays the command usage and options	

Syntax:

ldap [*options*]

options:

- a *loc|ldap|ocld|dloc*
- 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_attr*
- v *off|on*
- h

ntp command

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

The following table shows the arguments for the options.

Table 36. *ntp command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 36. *ntp command (continued)*

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 this command to display and configure the password parameters.

The following table contains descriptive text for the options supported by this command.

Table 37. *passwordcfg command*

The following table is a multi-row two column table consisting of the options and associated descriptions for this command.

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 this 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.

Table 38. *ports* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-open	Display open ports	
-reset	Reset ports to default settings	
-http	HTTP port number	Default port number: 80
-https	HTTPS port number	Default port number: 443
-telnet	Telnet legacy CLI port number	Default port number: 23
-ssh	SSH legacy CLI port number	Default port number: 22
-snmp	SNMP agent port number	Default port number: 161
-snmptrap	SNMP traps port number	Default port number: 162
-rpp	Remote presence port number	Default port number: 3900
-cimhttp	CIM over HTTP port number	Default port number: 5988
-cimhttps	CIM over HTTPS port number	Default port number: 5989

Syntax:

ports [*options*]

option:

- open
- reset
- http *port_number*
- https *port_number*
- telnet *port_number*
- ssh *port_number*
- snmp *port_number*
- snmp *port_number*
- rpp *port_number*
- cimhp *port_number*
- cimhsp *port_number*

Example:

```
system> ports
-http 80
-https 443
-rpp 3900
-snmp 161
-snmp 162
-ssh 22
-telnet 23
-cimhp 5988
-cimhsp 5989
system>
```

portcfg command

Use this 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 **cliath** 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.

Table 39. portcfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-b	Baud rate	9600, 19200, 38400, 57600, 115200
-p	Parity	none, odd, even

Table 39. *portcfg* command (continued)

Option	Description	Values
-s	Stop bits	1, 2
-climode	CLI mode	0, 1, 2 Where: <ul style="list-style-type: none"> 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 this 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.

Table 40. *portcontrol* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

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 this command to restore system settings from a backup file.

The following table shows the arguments for the options.

Table 41. *restore command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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
username
  -pw password
```

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

restoredefaults command

Use this 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 this 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.

Table 42. *scale command*

The following table is a multi-row two column table consisting of the options for this command and associated descriptions.

Option	Description
-auto	Automatically create a partition spanning across all nodes of the scalable complex.
-auto <i>Node_Key</i>	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 < <i>Node1_Key</i> > < <i>Node2_Key</i> > 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.
-create <i>_with_physical_node_id</i> < <i>PhysNodeId1</i> > < <i>PhysNodeId2</i> > 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.

Table 42. *scale* command (continued)

Option	Description
<code>-delete -partid <id> -node <Node_Key>¹</code>	<p>Delete a specific partition in the scalable complex.</p> <p>Note: The partition must be powered off to delete it.</p> <p>Delete a partition by providing one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of a partition in the scalable complex. • The node key of a node in the partition in the scalable complex.
<code>-delete</code>	<p>Delete all partitions in the scalable complex.</p> <p>Note: The partitions must be powered off to delete them.</p>
<code>-mode [stand-alone partition][-partid <id> -node <Node_Key>]¹</code>	<p>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.</p> <p>To set the partition mode, you can provide one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex.
<code>-start -partid <id> -node <Node_Key>¹</code>	<p>Power on a node or all of the nodes in a partition in the scalable complex.</p> <p>To power on the nodes in a partition, you can provide one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. <p>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.</p> <p>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.</p> <p>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.</p>

Table 42. *scale* command (continued)

Option	Description
<code>-reset -partid <id> -node <Node_Key>¹</code>	<p>Hard reset a node or all of the nodes in a partition in the scalable complex.</p> <p>To hard reset the nodes in a partition, you can provide one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. <p>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.</p> <p>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.</p> <p>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.</p>
<code>-stop -partid <id> -node <Node_Key>¹</code>	<p>Power off a node or all of the nodes in a partition in the scalable complex.</p> <p>To power off the nodes in a partition, you can provide one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. <p>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.</p> <p>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.</p> <p>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.</p>

Table 42. *scale* command (continued)

Option	Description
<code>-poweron -partid <id> -node <Node_Key>¹</code>	<p>Powers on a node or all of the nodes in a partition in the scalable complex.</p> <p>To power on the nodes in a partition, you can provide one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. <p>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.</p> <p>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.</p> <p>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.</p>
<code>-poweroff -partid <id> -node <Node_Key>¹</code>	<p>Power off a node or all of the nodes in a partition in the scalable complex.</p> <p>To power-off the nodes in a partition, you can provide one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. <p>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.</p> <p>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.</p> <p>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.</p>

Table 42. *scale* command (continued)

Option	Description
<code>-powercycle -partid <id> -node <Node_Key>¹</code>	<p>Power cycle a node or all of the nodes in a partition in the scalable complex.</p> <p>To power cycle the nodes in a partition, you can provide one of the following identifiers:</p> <ul style="list-style-type: none"> • The partition ID of the partition in the scalable complex. • The node key of a node in the partition in the scalable complex. <p>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.</p> <p>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.</p> <p>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.</p>
<code>-partid id</code>	This option is used to display information about the partition in the scalable complex.
<code>-node Node_Key</code>	This option is used to display information about a node in the scalable complex.
<code>-smp</code>	This option is used to display scalability hardware information.
<code>-h</code> or <code>-help</code>	This option is used to display usage information about the <i>scale</i> command.
Notes: 1. Option is displayed on multiple lines due to space limitations.	

Syntax:
scale

Example:
`system> scale`
 SMP Hardware =2-node SMP

```
Complex Signature      =CMD
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 =DEDB90B572211E3BADB6CAE8B703620
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_keynode2_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 this 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.

Table 43. *sdr raid command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
<code>-version</code>	This option is used to display the firmware version installed in the adapter.	
<code>-reset</code>	This option is used to reset the adapter.	
<code>-getMode</code>	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.	
<code>-setMode</code>	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
<code>-initializeConfig</code>	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.	
<code>-migrateConfig</code>	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
<code>-SDCard</code>	This option is used to display the properties of an installed SD card.	1, 2
<code>-getFreeSpaceInfo</code>	This option is used to display the free space information in the SD cards.	
<code>-driveLun</code>	This option is used to display the summary information of a drive configured on the adapter.	0 - 15
<code>-driveName</code>	This option is used to display the summary information of a drive configured on the adapter.	Null-terminated name string (maximum of 15 characters).
<code>-driveList</code>	This option is used to display the summary information of all drives configured on the adapter.	
<code>-create</code>	This option is used to create a new drive.	
<code>-delete</code>	This option is used to delete an existing drive. This option can be used with parameters <code>-driveLun</code> or <code>-driveName</code> .	
<code>-modify</code>	This option is used to modify the properties of an existing drive.	

Table 43. *sdraid* command (continued)

Option	Description	Values
-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.

Table 44. -migrateConfig option

The following table is a single-row three column table listing the mandatory parameter for this option. A parameter explanation and associated values for the parameter are provided.

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.

Table 45. -SDCard option

The following table is a single-row three column table listing the mandatory parameter for this option. A parameter explanation and associated values for the parameter are provided.

Table 45. -SDCard option (continued)

Mandatory parameter	Explanation	Values
-SDCard	The SD card number.	1, 2

Table 46. -SDCard option output

The following table is a multi-row three column table describing the information that is generated when using this option. Output descriptions and associated values are provided.

Output	Explanation	Values
Status	The state of the SD card.	Status values are as follows: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 <i>n</i> name	The volume name for drive <i>n</i> .	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.

Table 47. -getFreeSpaceinfo output option

The following table is a multi-row three column table describing the information that is generated when using this option. Output descriptions and associated values are provided.

Output	Explanation	Values
Free block region <i>n</i>	The index number of the free region from the list of free block regions for the two SD cards.	where <i>n</i> 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: <ul style="list-style-type: none"> • 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.

Table 48. -driveLun option

The following table is a single-row three column table listing the mandatory parameter for this option. A parameter explanation and associated values for the parameter are provided.

Mandatory parameter	Explanation	Values
-driveLun	The logical unit number of the drive.	0 - 15

Table 49. -driveLun output option

The following table is a multi-row three column table describing the information that is generated when using this option. Output descriptions and associated values are provided.

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 <i>n</i>	The size of the drive in MB.	where <i>n</i> 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
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.

Table 50. -driveName option

The following table is a single-row three column table listing the mandatory parameter for this option. A parameter explanation and associated values for the parameter are provided.

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.

Table 51. -driveList option

The following table is a multi-row three column table describing the information that is generated when using this option. Output descriptions and associated values are provided.

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
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 <i>n</i>	The size of the drive in MB.	where <i>n</i> 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.

Table 52. *-create option*

The following table is a multi-row three column table listing the mandatory parameters for this option. A parameter explanation and associated values for the parameter are provided.

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 <i>n</i>	The size of the drive in MB.	where <i>n</i> 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

Table 53. *-create option (optional parameter)*

The following table is a single-row three column table listing the optional parameter for this option. A parameter explanation and associated value for the parameter are provided.

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.

Table 54. -delete option

The following table is a multi-row three column table listing the mandatory parameters for this option. A parameter explanation and associated values for the parameter are provided.

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.

Table 55. -modify option

The following table is a single-row three column table listing the mandatory parameter for this option. A parameter explanation and associated values for the parameter are provided.

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.

Table 56. -modify option (optional parameters)

The following table is a multi-row three column table listing the optional parameters for this option. A parameter explanation and associated values for the parameter are provided.

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.

Table 57. -getOwner option

The following table is a multi-row three column table listing the mandatory parameters for this option. A parameter explanation and associated values for the parameter are provided.

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.

Table 58. -setOwner option

The following table is a multi-row three column table listing the mandatory parameters for this option. A parameter explanation and associated values for the parameter are provided.

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>
```

services command

This command is used to display and configure services enablement.

The Redfish service is enabled by default. Redfish service setting doesn't support the backup/restore, and need to be rebooted to take effect.

Table 59. services command

The following table is a single-row three column table consisting of the option, option description, and associated values for the option.

Table 59. *services* command (continued)

Option	Description	Values
-redfish	Enable/disable Redfish service	enabled, disabled

Example:

```
system> services
-redfish : disabled
system> services -redfish enabled
This feature requires the IMM2 to be rebooted.
system> services -redfish disabled
This feature is not supported on this system
```

set command

Use this command to change some 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.

Table 60. *set* command

The following table is a single-row three column table consisting of the command description and associated information.

Option	Description	Values
<i>value</i>	Set value for specified path or setting	Appropriate value for specified path or setting.

Syntax:

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

smtp command

Use this 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.

Table 61. *smtp* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-auth	SMTP authentication support	enabled, disabled
-authpwd	SMTP authentication encrypted password	Valid password string

Table 61. *smtp* command (continued)

Option	Description	Values
-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*
- authpw *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 this 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.

Table 62. *snmp* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 62. snmp command (continued)

Option	Description	Values
-a	SNMPv1 agent	on, off Notes: To enable the SNMPv1 agent, the following criteria must be met: <ul style="list-style-type: none"> • 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 -cx command options. • At least one valid IP address is specified for each SNMP community using one of the -xiy command options.
-a3	SNMPv3 agent	on, off Notes: To enable the SNMPv3 agent, the following criteria must be met: <ul style="list-style-type: none"> • 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). Notes: <ul style="list-style-type: none"> • 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). Notes: <ul style="list-style-type: none"> • 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 "".
-cx	SNMP community x name	String (limited to 15 characters). Notes: <ul style="list-style-type: none"> • 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 "".

Table 62. snmp command (continued)

Option	Description	Values
-cxiy	SNMP community x IP address or hostname y	Valid IP address or hostname (limited to 63 characters). Notes: <ul style="list-style-type: none"> 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.
-cax	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 this command to manage alerts sent via the SNMP.

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

Table 63. *snmpalerts command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-status	SNMP alert status	on, off
-crt	Sets critical events that send alerts	<p>all, none, custom:te vo po di fa cp me in re ot</p> <p>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:</p> <ul style="list-style-type: none"> 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

Table 63. *snmpalerts* command (continued)

Option	Description	Values
-wrn	Sets warning events that send alerts	all, none, custom:rp te vo po fa cp me ot Custom warning alert settings are specified using a pipe separated list of values of the form snmpalerts -wrn custom:rp te , where custom values are: <ul style="list-style-type: none"> rp: power redundancy warning te: warning temperature threshold exceeded vo: warning voltage threshold exceeded po: warning power threshold exceeded fa: non-critical fan event cp: microprocessor in degraded state me: memory warning ot: all other warning events
-wrnen	Send warning event alerts	enabled, disabled
-sys	Sets routine events that send alerts	all, none, custom:lo tio ot po bf til pf el ne Custom routine alert settings are specified using a pipe separated list of values of the form snmpalerts -sys custom:lo tio , where custom values are: <ul style="list-style-type: none"> 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 this 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 `entercli` 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 -entercli` command option.

Table 64. *srcfg* command

The following table is a single-row three column table consisting of the option, option description, and value information for the option.

Option	Description	Values
-entercli	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:

`-entercli entercli_keyseq`

Example:

`system> srcfg`

`-entercli ^[Q`

`system>`

sshcfg command

Use this 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.

Table 65. *sshcfg* command

This following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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 this command to display and configure the SSL parameters.

To 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.

Table 66. *ssl* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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 this command to display and configure the 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.

Table 67. *sslcfg* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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.

Table 67. *sslcfg* command (continued)

Option	Description	Values
-cert	Generate self-signed certificate	server, client, sysdir, storekey Notes: <ul style="list-style-type: none"> 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 Notes: <ul style="list-style-type: none"> 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.
-csrform	The format of the CSR will be exported in (der, pem)	
-rm	Remove the certificate (server,client,cim, storekey)	
-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.
-tcx	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.

Table 67. sslcfg command (continued)

Option	Description	Values
-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*
- csrform *The format of the CSR will be exported in (der, pem)*
- rm *Remove the certificate (server, client, cim, storekey)*
- i *ip_address*

port *number*

username

- pw *password*
- l *filename*
- dnld
- upld
- tc *xaction*
- 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 this 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.

Table 68. *storage command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-list	List the storage targets managed by the IMM2.	<i>controllers pools volumes drives</i> Where <i>target</i> is: <ul style="list-style-type: none"> • <i>controllers</i>: list the supported RAID controllers¹ • <i>pools</i>: list the storage pools associated with the RAID controller¹ • <i>volumes</i>: list the storage volumes associated with the RAID controller¹ • <i>drives</i>: list the storage drives associated with the RAID controller¹
-list -target <i>target_id</i>	List the storage <i>targets</i> managed by the IMM2 according to the <i>target_id</i> .	<i>pools volumes drives ctrl[x] pool[x]</i> Where <i>target</i> and <i>target_id</i> are: <ul style="list-style-type: none"> • <i>pools ctrl[x]</i>: list the storage pools associated with the RAID controller, based on the <i>target_id</i>¹ • <i>volumes ctrl[x] pool[x]</i>: list the storage volumes associated with the RAID controller, based on the <i>target_id</i>¹ • <i>drives ctrl[x] pool[x]</i>: list the storage drives associated with the RAID controller, based on the <i>target_id</i>¹
-list flashdimms	List the Flash DIMMs managed by the IMM2.	
-list devices	Display the status of all disks and Flash DIMMS managed by the IMM2.	
-show <i>target_id</i>	Display information for the selected target that is managed by the IMM2.	Where <i>target_id</i> is: <i>ctrl[x] vol[x] disk[x] pool[x]</i> <i> flashdimm[x]</i> 3
-show <i>target_id</i> info	Display detailed information for the selected target that is managed by the IMM2.	Where <i>target_id</i> is: <i>ctrl[x] vol[x] disk[x] pool[x]</i> <i> flashdimm[x]</i> 3
-show <i>target_id</i> firmware ³	Display the firmware information for the selected target that is managed by the IMM2.	Where <i>target_id</i> is: <i>ctrl[x] disk[x] flashdimm[x]</i> ²

Table 68. storage command (continued)

Option	Description	Values
-showlog <i>target_id</i> < <i>m:n</i> <i>all</i> > ³	Display the event logs of the selected target that is managed by the IMM2.	Where <i>target_id</i> is: <i>ctrl</i> [<i>x</i>] ⁴ <i>m:n</i> <i>all</i> Where <i>m:n</i> is one to the maximum number of event logs Where <i>all</i> are all of the event logs
-evtfwd on	Enable RAID event forwarding feature.	
-evtfwd off	Disable RAID event forwarding feature.	
-evtfwd status	Show RAID event forwarding status.	The status info: feature: on/off warning: asserted //show this line if feature is on and warning is asserted error: asserted //show this line if feature is on and error is asserted
-evtfwd deassert all	De-assert all forwarded RAID events.	Including warning RAID events and error RAID events.
-evtfwd deassert warning	De-assert warning RAID events.	
-evtfwd deassert error	De-assert error RAID events.	
-config ctrl -scanforgn -target <i>target_id</i> ³	Detect the foreign RAID configuration.	Where <i>target_id</i> is: <i>ctrl</i> [<i>x</i>] ⁵
-config ctrl -imptforgn -target <i>target_id</i> ³	Import the foreign RAID configuration.	Where <i>target_id</i> is: <i>ctrl</i> [<i>x</i>] ⁵
-config ctrl -clrforngn -target <i>target_id</i> ³	Clear the foreign RAID configuration.	Where <i>target_id</i> is: <i>ctrl</i> [<i>x</i>] ⁵
-config ctrl -clrcfg -target <i>target_id</i> ³	Clear the RAID configuration.	Where <i>target_id</i> is: <i>ctrl</i> [<i>x</i>] ⁵
-config drv -mkoffline -target <i>target_id</i> ³	Change the drive state from online to offline.	Where <i>target_id</i> is: <i>disk</i> [<i>x</i>] ⁵
-config drv -mkonline -target <i>target_id</i> ³	Change the drive state from offline to online.	Where <i>target_id</i> is: <i>disk</i> [<i>x</i>] ⁵
-config drv -mkmissing -target <i>target_id</i> ³	Mark the offline drive as an unconfigured good drive.	Where <i>target_id</i> is: <i>disk</i> [<i>x</i>] ⁵
-config drv -prprm -target <i>target_id</i> ³	Prepare an unconfigured good drive for removal.	Where <i>target_id</i> is: <i>disk</i> [<i>x</i>] ⁵
-config drv -undoprprm -target <i>target_id</i> ³	Cancel the prepare an unconfigured good drive for removal operation.	Where <i>target_id</i> is: <i>disk</i> [<i>x</i>] ⁵
-config drv -mkbad -target <i>target_id</i> ³	Change the unconfigured good drive to a unconfigured bad drive.	Where <i>target_id</i> is: <i>disk</i> [<i>x</i>] ⁵

Table 68. storage command (continued)

Option	Description	Values
-config drv -mkgood -target <i>target_id</i> 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 <i>target_id</i> is: <i>disk[x]</i> ⁵
-config drv -addhsp -[<i>dedicated pools</i>] -target <i>target_id</i> ³	Assign the selected drive as a hot spare to one controller or to existing storage pools.	Where <i>target_id</i> is: <i>disk[x]</i> ⁵
-config drv -rmhsp -target <i>target_id</i> ³	Remove the hot spare.	Where <i>target_id</i> is: <i>disk[x]</i> ⁵
-config vol -remove -target <i>target_id</i> ³	Remove one volume.	Where <i>target_id</i> is: <i>vol[x]</i> ⁵
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target <i>target_id</i> ³	Modify the properties of one volume.	<ul style="list-style-type: none"> • [-N <i>volume_name</i>] is the name of the volume • [-w <0 1 2>] is the cache write policy: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – Type 0 for the Direct I/O policy – Type 1 for the Cached I/O policy • [-a <0 2 3>] is the access policy: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – Type 0 if the policy is unchanged – Type 1 to enable the policy⁶ – Type 2 to disable the policy • [-b <0 1>] is the background initialization: <ul style="list-style-type: none"> – Type 0 to enable initialization – Type 1 to disable initialization • -<i>target_id</i> is <i>vol[x]</i>⁵

Table 68. storage command (continued)

Option	Description	Values
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r] ³⁷	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.	<ul style="list-style-type: none"> • [-R <0 1 5 1E 6 10 50 60 00 1E RLQ0 1E0RLQ0>] This option defines the RAID level and is only used with a new storage pool • [-D disk [id11]:disk[id12]:...disk[id21]:disk[id22]:...] This option defines the drive group (including spans) and is only used with a new storage pool • [-H disk [id1]:disk[id2]:...] 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 volume_name] is the name of the volume • [-w <0 1 2>] is the cache write policy: <ul style="list-style-type: none"> – 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 : <ul style="list-style-type: none"> – Type 0 for the No Read Ahead policy – Type 1 for the Read Ahead policy – Type 2 for the Adaptive Read Ahead policy
-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.	<ul style="list-style-type: none"> • [-i <0 1>] is the cache I/O policy: <ul style="list-style-type: none"> – Type 0 for the Direct I/O policy – Type 1 for the Cached I/O policy • [-a <0 2 3>] is the access policy: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – Type 0 if the policy remains unchanged – Type 1 to enable the policy⁶ – Type 2 to disable the policy • [-f <0 1 2>] is the type of initialization: <ul style="list-style-type: none"> – 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

Table 68. storage command (continued)

Option	Description	Values
		<ul style="list-style-type: none"> [-P <i>strip_size</i>] is the volume strip size for example, 128K or 1M -target <i>target_id</i> is: <ul style="list-style-type: none"> <i>ctrl[x]</i> (new storage pool⁵) <i>pool[x]</i> (existing storage pool)⁵
-config vol -getfreecap[-R] [-D disk] [-H disk] -target <i>target_id</i> ³	Get the free capacity amount of the drive group.	<ul style="list-style-type: none"> [-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 <i>[id11]:[id12]:...[id21]:[id22]:...</i>] This option defines the drive group (including spans) and is only used with a new storage pool [-H disk <i>[id1]:[id2]:...</i>] This option defines the hot spare group and is only used with a new storage pool -target <i>target_id</i> is: <ul style="list-style-type: none"> <i>ctrl[x]</i>⁵
-help	Display the command usage and options	
Notes: <ol style="list-style-type: none"> This command is only supported on servers where the IMM2 can access the RAID controller. Firmware information is displayed only for associated controllers, disks, and Flash DIMMs. Firmware information for associated pools and volumes are not displayed. Information is displayed on multiple lines due to space limitations. This command is only supported on servers that support RAID logs. This command is only supported on servers that support RAID configurations. The <i>Enable</i> value does not support RAID level 1 configurations. 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. The -evtfwd command only applies to RAID logs. 		

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
-evtfwd <on|off|deassert|status>Configure warning/error RAID events forwarding as warning/error IMM events
-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
Manufacture: 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
Storage Pool 0
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: HDD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclosure 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 this 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.

Table 69. storekeycfg command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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.
-sxp	Add the port number of the SKLM server	Valid port number for SKLM server. Numeric value of 1, 2, 3, or 4.

Table 69. *storekeycfg* command (continued)

Option	Description	Values
-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*
- sxiip *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 tkml-server.der
system> ok
```

To configure the SKLM server address and port number, enter the following command:

```
system> storekeycfg
-s1ip 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 this 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.

Table 70. *telnetcfg* command

The following table is a single-row three column table consisting of the option, option description, and associated values for the option.

Table 70. *telnetcfg* command (continued)

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 this command to set the minimum TLS level.

The following table shows the arguments for the options.

Table 71. *tls* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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	
Notes:		
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 this 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.

Table 72. *thermal command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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_devicetable_number
```

Example:

```
system> thermal
```

```
-mode normal
```

```
-table 80860126 1 10DE0DFA 3
```

```
system>
```

timeouts command

Use this command to display or change the timeout values.

- 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.

Table 73. *timeouts command*

The following table is a multi-row four column table consisting of the options, option descriptions, and associated values for the options.

Table 73. *timeouts* command (continued)

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

Syntax:

`timeouts [options]`

options:

-f *power_off_delay_watchdog_option*

-o *OS_watchdog_option*

-l *loader_watchdog_option*

Example:

```
system> timeouts
```

```
-o disabled
```

```
-l 3.5
```

```
system> timeouts -o 2.5
```

```
ok
```

```
system> timeouts
```

```
-o 2.5
```

```
-l 3.5
```

usbeth command

Use this 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 this 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.

Table 74. *users* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 74. *users* command (continued)

Option	Description	Values
-user_index	User account index number	1 through 12, inclusive, or all for all users.
-n	User account name	Unique string containing only numbers, letters, periods, and underscores. Minimum of 4 characters and maximum of 16 characters.
-p	User account password	String that contains at least one alphabetic and one non-alphabetic character. Minimum of 6 characters and maximum of 20 characters. Null creates an account without a password that the user must set during their first login.
-a	User authority level	super, ro, custom Where: <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> 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-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

Table 74. *users* command (continued)

Option	Description	Values
-pk	Display SSH public key for user	User account index number. Notes: <ul style="list-style-type: none"> 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 (-<i>userindex</i> 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 (- <i>userindex</i> 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_ <i>index</i> 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 (- <i>userindex</i> 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: <ul style="list-style-type: none"> 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 (-<i>userindex</i> option), of the form: users -2 -pk -add "AAAAB3Nzc1yc2EAAAABIWAAA QEA vfnTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wLZnuC4aD HMA1UmnMyLOCiIaNOy400ICEKcQjKEhrYymtAoVtfKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SA tMu cUsTkYjLXcqex10Qz4+N50R6MbNcwl s x+mTEAvvc pJhug a70UNPGhLJML6k7jeJiQ8Xd2p Xb0ZQ=="
-upld	Upload an SSH public key (SSH public key option)	Requires the -i and -l options to specify key location. Notes: <ul style="list-style-type: none"> 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_<i>index</i>. 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 (-<i>userindex</i> option), of the form: users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key.

Table 74. users command (continued)

Option	Description	Values
-dnld	Download the specified SSH public key (SSH public key option)	Requires a <i>-key_index</i> to specify the key to download and the <i>-i</i> and <i>-l</i> options to specify the download location on another computer running a TFTP server. Notes: <ul style="list-style-type: none"> The <i>-dnld</i> option is used exclusive of all other users <i>-pk</i> command options (except for <i>-i</i>, <i>-l</i>, and <i>-key_index</i>). When using the SSH public key options, the <i>-pk</i> option must be used after the user index (<i>-userindex</i> 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>-i</i> option is required by the users <i>-pk -upld</i> and users <i>-pk -dnld</i> 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 <i>-pk -upld</i> and users <i>-pk -dnld</i> command options.
-u	User name for SFTP server (SSH public key option)	Valid user name Note: An optional parameter for the users <i>-pk -upld</i> and users <i>-pk -dnld</i> command options.
-pw	Password for SFTP server (SSH public key option)	Valid password Note: An optional parameter for the users <i>-pk -upld</i> and users <i>-pk -dnld</i> 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 <i>-l</i> option is required by the users <i>-pk -upld</i> and users <i>-pk -dnld</i> 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 <i>-pk</i> option must be used after the user index (<i>-userindex</i> 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. jacobyackenovici custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSWORD -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. jacobyackenovici 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

This topic provides an alphabetic list of IMM2 control CLI commands.

The IMM2 control commands are as follows:

- [“alertentries command” on page 308](#)
- [“batch command” on page 310](#)
- [“clearcfg command” on page 311](#)
- [“clock command” on page 311](#)

- [“identify command” on page 312](#)
- [“info command” on page 312](#)
- [“resetsp command” on page 313](#)
- [“spreset command” on page 313](#)

alertentries command

Use this command to manage alert recipients.

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

The following table shows the arguments for the options.

Table 75. *alertentries command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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	

Table 75. *alertentries* command (continued)

Option	Description	Values
-crt	Sets critical events that send alerts	all, none, custom:te vo po di fa cp me in re ot Custom critical alert settings are specified using a pipe separated list of values of the form alertentries -crt custom:te vo , where custom values are: <ul style="list-style-type: none"> 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 alertentries -wrn custom:rp te , where custom values are: <ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 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 this 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.

Table 76. *batch command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 76. *batch* command (continued)

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*

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 this 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 this 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 this 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 this 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.

Table 77. *info* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-name	IMM2 name	String
-contact	Name of IMM2 contact person	String

Table 77. info command (continued)

Option	Description	Values
-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
-imm_location
-room room_id
-rack rack_id
-rup unit_position
-ruh unit_height
-bbay blade_bay
```

resetsp command

Use this command to restart the IMM2.

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

sreset command

Use this command to restart the IMM2.

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

Service advisor commands

This topic provides an alphabetic list of service advisor CLI commands.

The service advisor commands are as follows:

- [“autoftp command” on page 313](#)
- [“chconfig command” on page 314](#)
- [“chlog command” on page 316](#)
- [“chmanual command” on page 317](#)
- [“events command” on page 317](#)
- [“sdemail command” on page 318](#)

autoftp command

Use this 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.

Table 78. *autoftp command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-m	The automated problem reporting mode	ftp, sftp, tftp, disabled Notes: <ul style="list-style-type: none"> 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 this command to display and configure the Service Advisor settings.

- 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 **Service Support Center** field (using chconfig -sc command option), 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.

Table 79. *chconfig command*

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Table 79. *chconfig* command (continued)

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
-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 this 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.

Table 80. *chconfig* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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 this 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.

Table 81. *chmanual* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values 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

Use this command to view and edit the call home event configuration.

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

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.

Table 82. *events* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-add	Add a call home event into the call home <i>exclusion list</i>	Event ID of the form <i>0xhhhhhhhhhhhhhhhh</i> .
-rm	Remove a call home event from the call home <i>exclusion list</i>	Event ID of the form <i>0xhhhhhhhhhhhhhhhh</i> 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.

Table 83. *sdemail* command

The following table is a multi-row three column table consisting of the options, option descriptions, and associated values for the options.

Option	Description	Values
-to	Recipient's information (<i>required option</i>)	Recipient's email address: <ul style="list-style-type: none">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.lenovo.com/serverproven/> to make sure that the hardware and software is supported by your product.
- Go to <http://www.lenovo.com/support> 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 Lenovo 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.lenovo.com/support>.

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.lenovo.com/support>. The most current version of the product documentation is available in the following product-specific Information Centers:

Flex System products: <http://pic.dhe.ibm.com/infocenter/flexsys/information/index.jsp>

System x products: <http://shop.lenovo.com/us/en/systems/>

NeXtScale System products: <http://pic.dhe.ibm.com/infocenter/nxtscale/documentation/index.jsp>

How to send DSA data

You can use the Enhanced Customer Data Repository to send diagnostic data to Lenovo.

Before you send diagnostic data to Lenovo, 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 the 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 product service for Taiwan.

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, System x and For Those Who Do are trademarks or registered trademarks of Lenovo in the United States, other countries, or both.

A current list of Lenovo trademarks is available on the web at: <http://www.lenovo.com/legal/copytrade.html>.

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in the United States and/or other countries.

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

Fusion-io is a registered trademark of Fusion-io, in the United States.

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

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

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

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

SAP HANA is a trademark of SAP Corporation in the United States, other countries, or both.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates.

Other product and service names might be trademarks of Lenovo or other companies.

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: <http://www.lenovo.com/recycling>.

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 84. Limits for particulates and gases

Limits for particulates and gases

Table 84. Limits for particulates and gases (continued)

Contaminant	Limits
Particulate	<ul style="list-style-type: none"> The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2¹. 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	<ul style="list-style-type: none"> Copper: Class G1 as per ANSI/ISA 71.04-1985³ Silver: Corrosion rate of less than 300 Å in 30 days
<p>¹ ASHRAE 52.2-2008 - <i>Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size</i>. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.</p> <p>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.</p> <p>³ ANSI/ISA-71.04-1985. <i>Environmental conditions for process measurement and control systems: Airborne contaminants</i>. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.</p>	

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 Betriebsmitteln 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.

Japanese statement of compliance for products less than or equal to 20 A per phase for JEITA harmonics guideline

日本の定格電流が 20A/相 以下の機器に対する高調波電流規制
高調波電流規格 JIS C 61000-3-2 適合品

Japan Electronics and Information Technology Industries Association (JEITA) statement

高調波ガイドライン準用品

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

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

A

- absolute mouse control 145
- access
 - remote control 153
 - Telnet 75, 300
- access control
 - settings 105
- accsecfg command 232
- action descriptions
 - IMM2 13
- actions
 - partitions 184
- activate stand-alone
 - partition 184
- activation key
 - export 209
 - install 205, 247
 - manage 76, 247
 - remove 208, 247
- Active Directory Users
 - LDAP 75, 303
- active energy manager
 - policies tab 173, 175
 - power management 173, 175
 - power management option 173
- ActiveX applet
 - updating 138
- adapter command 217
- adapter configuration
 - server management tab 200
- adapters option
 - server management 200–201
 - Server Management tab 69
- advanced Ethernet
 - settings 90
- advanced level features 3
- advanced management module 1, 4, 9
- Advanced Settings Utility (ASU) 1
- alertcfg command 234
- alertentries command 308
- alphabetical command list 214
- assigned nodes
 - scalable complex 182
- assistance, getting 319
- asu command 235
- Australia Class A statement 327
- autoftp command 313
- autonegotiation
 - set 74, 245
- autopromo command 238

B

- backup command 239
- backup configuration
 - IMM2 76
- backup status view
 - IMM2 76
- baseboard management controller (BMC) 1
- basic level features 2
- batch command 310
- binding method
 - LDAP server 75, 248
- BIOS (basic input/output system) 1
- blade servers 1, 4, 9
- BladeCenter 1, 4, 9
- blue screen capture 138

- browser requirements 4

C

- CA-signed
 - certificate 120
- Canada Class A electronic emission statement 326
- capacity
 - power supply 178
- centralized management
 - encryption keys 117
- certificate classifications
 - CA-signed 120
 - self-assigned 120
- certificate handling
 - CIM over HTTPS 108
 - secure LDAP client 109
- certificate management
 - CIM over HTTPS 76, 285–286
 - client 120
 - Drive Access 299
 - HTTPS server 76, 285–286
 - LDAP 76, 285–286
 - server 122
 - SSH server 76, 284
- certificate signing request
 - IMM2 120
- change partition mode
 - scalable complex 184
- chart tab
 - performance tab
 - power management option 179
 - power history tab 178
 - power management option 178
- chconfig command 314
- China Class A electronic emission statement 329
- chlog command 316
- chmanual command 317
- CIM over HTTP port
 - set 76, 252
- CIM over HTTPS
 - certificate management 76, 285–286
 - security 76, 285–286
- CIM over HTTPS port
 - set 76, 252
- Class A electronic emission notice 326
- clearcfg command 311
- clearlog command 219
- CLI key sequence
 - set 73, 253
- client
 - certificate management 120
- client certificate management
 - CA-signed 120
 - self-assigned 120
- client distinguished name
 - LDAP server 75, 248
- clock command 311
- collecting service and support data 170
- command-line interface (CLI)
 - accessing 211
 - command syntax 212
 - description 211
 - features and limitations 213
 - logging in 212
- commands
 - accsecfg 232

- adapter 217
- alertcfg 234
- alertentries 308
- asu 235
- autoftp 313
- autopromo 238
- backup 239
- batch 310
- chconfig 314
- chlog 316
- chmanual 317
- clearcfg 311
- clearlog 219
- clock 311
- console 231
- cryptomode 239
- dhcpinfo 241
- dns 242
- ethtousb 243
- events 317
- exit 216
- fans 220
- ffdc 220
- fuelg 226
- gprofile 244
- help 216
- history 216
- identify 312
- ifconfig 245
- info 312
- keycfg 247
- ldap 248
- led 221
- ntp 250
- passwordcfg 251
- portcfg 253
- portcontrol 254
- ports 252
- power 228
- pxeboot 230
- readlog 223
- reset 230
- resetsp 313
- restore 255
- restoredefaults 255
- scale 256
- sdemail 318
- sdraid 265
- services 277
- set 278
- smtp 278
- snmp 279
- snmpalerts 282
- sreset 313
- srcfg 283
- sshcfg 284
- ssl 285
- sslcfg 286
- storage 289
- storekeycfg 299
- syshealth 224
- telnetcfg 300
- temps 225
- thermal 302
- timeouts 302
- TLS 301
- usbeth 303
- users 303
- volts 225
- vpd 226
- commands, alphabetical list 214
- commands, types of
 - configuration 231
 - IMM2 control 307
 - monitor 217
 - serial redirect 231
 - server power and restart 226
 - service advisor 313
 - utility 216
- compromised private keys
 - security 114
- configuration backup
 - IMM2 76
- configuration commands 231
- configuration restore
 - IMM2 76, 255
- configuration summary, viewing 13
- configuration tab
 - properties page 201
- configuration view
 - IMM2 76
- configure
 - access control 105
 - CIM over HTTPS protocol 108
 - cryptography management 115
 - DDNS 75, 242
 - DDNS settings 95
 - DNS 74, 242
 - DNS settings 95
 - Ethernet 74, 245
 - Ethernet over USB 75, 243
 - Ethernet settings 90
 - HTTPS protocol 107
 - IMM2 76
 - IPMI 75, 103
 - IPMI access 75
 - IPv4 74, 245
 - IPv6 74, 245
 - LDAP 75, 248
 - LDAP client protocol 109
 - LDAP server 75, 248
 - LDAP settings 96
 - network protocols 90
 - network service port 254
 - port assignments 104
 - ports 75, 252
 - security 76
 - security settings 106
 - serial port 73, 80, 253
 - SKLM device group 120
 - SKLM key repository servers 119
 - SMTP 75, 278
 - SMTP settings 96
 - SNMP alert settings 93
 - SNMPv1 74, 279
 - SNMPv1 traps 74, 279
 - SNMPv3 user accounts 74, 303
 - ssh server 111
 - Telnet 300
 - Telnet settings 75, 100
 - up to four power supplies 175
 - up to two power supplies 173
 - USB 75, 243
 - USB settings 101
 - user account security levels 74, 232
- configuring
 - global login settings 86
 - serial-to-SSH redirection 212
 - serial-to-Telnet redirection 212
- configuring the IMM2
 - options to configure the IMM2 73
- console command 231
- contamination, particulate and gaseous 325
- controlling the power status
 - of the server 136
- cooling devices option
 - under Server Management tab 61
- create
 - disk image 154

- email notification 165
- syslog notification 165
- user account 74, 303
- create a partition
 - scalable complex 183
- creating a personalized support web page 320
- cryptomode command 239
- custom support web page 320

D

- date
 - set 73, 311
- date and time, IMM2
 - setting 78
- dcmi
 - functions and commands 181
 - power management 181
- DDNS
 - configure 75, 242
 - custom domain name 75, 242
 - DHCP server specified domain name 75, 242
 - domain name source 75, 242
 - manage 75, 242
- default configuration
 - IMM 255
 - IMM2 76
- default static IP address 10
- delete
 - email notification 165
 - syslog notification 165
 - user 74, 303
- delete group
 - enable, disable 244
- delete partition
 - scalable complex 185
- description
 - partition error 186
- device group
 - drive access page 120
- devices
 - map 155
 - mount 155
 - unmount 156
- dhcpinfo command 241
- disk image
 - create 154
 - upload 154
 - Virtual Media Session 154–156
- disk, remote 153
- distinguished name, client
 - LDAP server 75, 248
- distinguished name, root
 - LDAP server 75, 248
- DNS
 - configure 74, 242
 - IPv4 addressing 74, 242
 - IPv6 addressing 74, 242
 - LDAP server 75, 248
 - server addressing 74, 242
- dns command 242
- documentation
 - using 320
- domain name source
 - DDNS 75, 242
- domain name, custom
 - DDNS 75, 242
- domain name, DHCP server specified
 - DDNS 75, 242
- download service data
 - option, overview 41
 - services and support tab 33
- Drive Access

- certificate management 299
- security 299
- drive access page
 - configure 119
 - device group 120
 - SKLM certificate management 120, 122
 - SKLM key repository servers 119
- Drive Access tab
 - security option 117, 119–120, 122
- DSA, sending data 320

E

- electronic emission Class A notice 326
- email recipients
 - setting up 30
- encryption keys
 - centralized management 117
- enhanced role-based security
 - LDAP 75, 303
- Ethernet
 - configure 74, 245
- Ethernet over USB
 - configure 75, 243
 - port forwarding 75, 243
 - SUSE Linux Enterprise 12 or higher 102
- ethtousb command 243
- European Union EMC Directive conformance statement 327
- event
 - log 163
- event id
 - problem list 33
- event log 28
 - manage 163
- event notification 30
- event recipient 30
- event recipients
 - manage 163
- event tab
 - log 28
- events
 - recipients 165
- events command 317
- events menu 163
- events tab
 - overview 28
- exit command 216
- exiting
 - remote control 157
 - Video Viewer 157
 - Virtual Media Session 157
- export
 - activation key 209
- export feature
 - Features on Demand 209
 - FoD 209

F

- fans command 220
- FCC Class A notice 326
- feature
 - knock knock 150
- features of IMM2 2
- Features on Demand 205
 - export feature 209
 - install feature 205, 247
 - manage 76, 247
 - remove feature 208, 247
- ffdc command 220
- firewalls and proxies
 - IBM Systems Director 40

- firmware
 - view server 73, 226
- firmware automated promotion, IMM2
 - setting 78
- firmware, server
 - updating 158
- FoD 205
 - export feature 209
 - install feature 205, 247
 - manage 76, 247
 - remove feature 208, 247
- four power supplies
 - configure 175
- fuelg command 226
- functions and commands
 - dcmi 181
 - node manager 180

G

- gaseous contamination 325
- Germany Class A statement 327
- global login
 - settings 86
- global login settings
 - account security level tab 87
 - general tab 86
- gprofile command 244
- group filter
 - LDAP 75, 248
- group profile
 - management 85
- group search attribute
 - LDAP 75, 248

H

- hardware health 131
- hardware service and support telephone numbers 321
- help
 - from the World Wide Web 320
 - from World Wide Web 320
 - sending diagnostic data 320
 - sources of 319
- help command 216
- history command 216
- host name
 - LDAP server 75, 248
 - set 74, 245
 - SMTP server 75, 278
- host server startup sequence, changing 13
- HTTP port
 - set 76, 252
- HTTPS port
 - set 76, 252
- HTTPS server
 - certificate management 76, 285–286
 - security 76, 285–286

I

- IBM Systems Director
 - firewalls and proxies 40
 - system management tool 40
- identify command 312
- ifconfig command 245
- image
 - remote disk 155–156
- IMM
 - configure 76

- default configuration 255
- reset 313
- reset configuration 255
- restart 313
- restore configuration 255
- sreset 313
- IMM management
 - activation management key 125
 - configure network protocol 90
 - configuring user accounts 81
 - IMM configuration
 - restore and modify IMM configuration 123
 - IMM properties
 - serial port settings 80
 - restart IMM2 123
 - security settings 106
 - user
 - accounts 81
 - group profiles 85
- IMM management tab 71
- IMM2
 - action descriptions 13
 - activation management key 125
 - backup configuration 76
 - backup status view 76
 - certificate signing request 120
 - configuration backup 76
 - configuration options 73
 - configuration restore 76, 255
 - configuration view 76
 - default configuration 76
 - description 1
 - features 2
 - IMM2 advanced level 2
 - IMM2 basic level 2
 - IMM2 Premium, upgrading to 3
 - IMM2 standard level 2
 - IMM2 Standard, upgrading from 3
 - improvements over IMM 3
 - ipmi bridging 180
 - network connection 10
 - new functions 1
 - reset 76, 124
 - reset configuration 76
 - restart 76, 123
 - restore configuration 76
 - restore status view 76
 - serial redirection 212
 - setup wizard 76
 - view backup status 76
 - view configuration 76
 - view restore status 76
 - web interface 9
 - web user interface overview 19
- IMM2 control commands 307
- IMM2 features
 - advanced level 3
 - basic level 2
- IMM2 featuresstandard level features
 - standard level 2
- IMM2 management
 - IMM properties
 - date and time 78
 - firmware automated promotion 78
 - reset IMM2 124
- IMM2 Premium, upgrading to 3
- IMM2 Standard, upgrading from 3
- IMM2 tasks 135
- IMM2 web session
 - logging out 21
- IMM2 web user interface
 - events tab
 - options overview 28
 - overview 19
 - service and support tab

- options overview 33
- system status tab
 - overview 22
- important notices 324
- info command 312
- information center 320
- install
 - activation key 205, 247
- install feature
 - Features on Demand 205, 247
 - FoD 205, 247
- installed power supplies
 - power modules tab 177
- international keyboard support in remote control 144
- IP address
 - configuring 9
 - IPv4 9
 - IPv6 9
 - LDAP server 75, 248
 - SMTP server 75, 278
- IP address, default static 10
- IPMI
 - configure 75, 103
 - remote server management 211
- IPMI access
 - configure 75
- ipmi bridging
 - power management 180
 - through IMM2 180
- ipmi commands
 - power consumption 180
- IPMITool 211
- IPv4
 - configure 74, 245
- IPv4 addressing
 - DNS 74, 242
- IPv6 9
 - configure 74, 245
- IPv6 addressing
 - DNS 74, 242

J

- Japan Class A electronic emission statement 328
- Japan Electronics and Information Technology Industries Association statement 328
- Japanese statement of compliance for products less than or equal to 20 A per phase for JEITA harmonics guideline 328
- Java 4, 153
- Java applet
 - updating 138
- JEITA statement 328

K

- keyboard pass-through mode in remote control 144
- keyboard support in remote control 141
- keycfg command 247
- knock knock feature
 - enable 150
 - request remote session 150
 - user mode
 - multi 150
 - single 150
- Korea Class A electronic emission statement 328

L

- latest OS failure screen option
 - under Server Management tab 70

LDAP

- Active Directory Users 75, 303
- certificate management 76, 285–286
- configure 75, 248
- enhanced role-based security 75, 303
- group filter 75, 248
- group search attribute 75, 248
- login permission attribute 75, 248
- role-based security, enhanced 75, 303
- security 76, 285–286
- server target name 75, 248
- ldap command 248
- LDAP server
 - binding method 75, 248
 - client distinguished name 75, 248
 - configure 75, 248
 - DNS 75, 248
 - host name 75, 248
 - IP address 75, 248
 - password 75, 248
 - port number 75, 248
 - pre-configured 75, 248
 - root distinguished name 75, 248
 - search domain 75, 248
 - UID search attribute 75, 248
- LDAP server port
 - set 75, 248
- led command 221
- local storage configuration
 - RAID logs 193
 - SD Media RAID 194
 - server management tab 187, 191, 193–194
- local storage option
 - server management 187, 191, 193–194
 - Server Management tab 63
- logging in to the IMM2 11
- logging out of the IMM2 session 21
- logical
 - storage pools 187
- logical drives
 - storage pools 191
- login permission attribute
 - LDAP 75, 248

M

- MAC address
 - manage 74, 245
- manage
 - activation key 76, 247
 - DDNS 75, 242
 - Features on Demand 76, 247
 - FoD 76, 247
 - MAC address 74, 245
 - SNMPv1 communities 74, 279
 - user 74, 303
- management
 - SKLM certificate 120, 122
- managing power
 - using IPMI commands 180
- maximum sessions
 - Telnet 75, 300
- maximum transmission unit
 - set 74, 245
- memory option
 - under Server Management tab 66
- minimum, levels
 - TLS 301
- monitor commands 217
- monitoring power
 - using IPMI commands 180
- monitoring the server status 127
- mount and map

- devices 155
- mouse control
 - absolute 145
 - relative 145
 - relative with default Linux acceleration 145
- mouse support in remote control 145
- MTU
 - set 74, 245

N

- network connection 10
 - default static IP address 10
 - IP address, default static 10
 - static IP address, default 10
- network protocol properties
 - access control 105
 - DDNS 95
 - DNS 95
 - Ethernet settings 90
 - IPMI 103
 - LDAP 96
 - port assignments 104
 - SMTP 96
 - SNMP alert settings 93
 - Telnet 100
 - USB 101
- network service port
 - configure 254
- New Zealand Class A statement 327
- node manager
 - functions and commands 180
- notes, important 324
- notices 323
 - electronic emission 326
 - FCC, Class A 326
- notices and statements 7
- ntp command 250

O

- online publications
 - documentation update information 1
 - error code information 1
 - firmware update information 1
- operating-system requirements 4
- operating-system screen capture 138
- option
 - SKLM 117
- options on the
 - IMM management tab 71
 - server management tab 42
- OS failure screen data
 - capture 172
- overview
 - download service data 41
 - ssl 112

P

- page auto refresh option 19
- particulate contamination 325
- partition
 - actions 184
 - activate stand-alone
 - remove, restore 184
- partition error
 - description 186
 - scalable complex 186
- partitions

- scalable complex 182–183
- password
 - LDAP server 75, 248
 - user 74, 303
- passwordcfg command 251
- People's Republic of China Class A electronic emission statement 329
- performing
 - IMM2 tasks 135
- physical
 - storage pools 187
- physical drives
 - storage pools 187
- port assignments
 - configure 104
 - settings 104
- port forwarding
 - Ethernet over USB 75, 243
- port number
 - LDAP server 75, 248
 - SMTP server 75, 278
- port numbers
 - set 76, 252
- portcfg command 253
- portcontrol command 254
- ports
 - configure 75, 252
 - set numbers 76, 252
 - view open 75, 252
- ports command 252
- power
 - managing using IPMI commands 180
 - monitoring using IPMI commands 180
- power actions 136
 - scalable complex 182
- power allocation tab
 - power management option 178
- power command 228
- power consumption
 - ipmi commands 180
- power management
 - active energy manager 173, 175
 - dcmi 181
 - ipmi bridging 180
 - policies tab 173, 175
 - under Server Management tab 71
- power management option
 - active energy manager 173
 - chart tab 178
 - performance tab
 - chart tab 179
 - policies tab 173
 - power allocation tab 178
 - power history tab 178
 - power modules tab 177
 - Server Management tab 173
- power modules option
 - under Server Management tab 62
- power modules tab
 - installed power supplies 177
 - power management option 177
- power supply
 - capacity 178
- pre-configured
 - LDAP server 75, 248
- private key states
 - active 114
 - comprised/destroyed comprised 114
 - deactive 114
 - destroyed 114
 - pre-activation 114
 - security 114
- private keys
 - security 114
- problem list

- event id 33
- problems
 - services and support tab 33
- problems, option
 - services and support 33
- processors option
 - under Server Management tab 68
- product service, Taiwan 321
- properties page
 - configuration tab 201
- PXE Boot Agent 13
- PXE network boot
 - setting up 157
- PXE network boot option
 - under Server Management tab 70
- pxeboot command 230

R

- RAID logs
 - local storage configuration 193
- readlog command 223
- relative mouse control 145
- relative mouse control for Linux (default Linux acceleration) 145
- remote access 2
- remote boot 153
- remote control
 - absolute mouse control 145
 - accessing 153
 - exiting 157
 - international keyboard support 144
 - keyboard pass-through mode 144
 - keyboard support 141
 - mouse support 145
 - performance statistics 147
 - power and restart commands 146
 - relative mouse control 145
 - relative mouse control for Linux (default Linux acceleration) 145
 - screen capture 138
 - single cursor mode 146
 - video viewer 137
 - Video Viewer 139, 141
 - virtual media session 137
 - Virtual Media Session 153
- remote control feature 48, 137
- remote control mouse support 145
- Remote Control port
 - set 76, 252
- remote control, windows
 - video viewer 48
 - virtual media session 48
- Remote Desktop Protocol (RDP)
 - launching 148
- remote disk 153
 - image 154–156
- Remote Disk On Chip
 - upload image 154
 - Virtual Media Session 154
- remote power control 146
- remote presence functionality 137
 - enabling 138
- Remote Supervisor Adapter II 1
- remove
 - activation key 208, 247
- remove feature
 - Features on Demand 208, 247
 - FoD 208, 247
- remove, partition mode
 - scalable complex 185
- remove, restore
 - partition 184

- requirements
 - operating system 4
 - web browser 4
- reset
 - IMM 313
 - IMM2 76
- reset command 230
- reset configuration
 - IMM 255
 - IMM2 76
- resetsp command 313
- restart
 - IMM 313
 - IMM2 76
- restore command 255
- restore configuration
 - IMM2 76, 255
- restore status view
 - IMM2 76
- restoredefaults command 255
- role-based levels
 - operator 244
 - rbs 244
 - supervisor 244
- role-based security, enhanced
 - LDAP 75, 303
- root distinguished name
 - LDAP server 75, 248
- Russia Class A electronic emission statement 329

S

- scalable complex
 - change partition mode 184
 - create a partition 183
 - delete partition 185
 - managing 182
 - partition error 186
 - partitions 183
 - remove, partition mode 185
 - separate nodes 182
 - server management tab 71
 - viewing 182
- scale command 256
- SD Media RAID
 - local storage configuration 194
- sdemail command 318
- sdraid command 265
- search domain
 - LDAP server 75, 248
- security
 - CIM over HTTPS 76, 285–286
 - CIM over HTTPS protocol 108
 - compromised private keys 114
 - configure 76
 - cryptography management 115
 - Drive Access 299
 - HTTPS protocol 107
 - HTTPS server 76, 285–286
 - LDAP 76, 285–286
 - LDAP client 109
 - private key states 114
 - private keys 114
 - ssh server 111
 - SSH server 76, 284
 - ssl certificate handling 112
 - SSL certificate management 112
 - ssl overview 112
- security option
 - Drive Access tab 117, 119, 122
- Security option
 - Drive Access tab 120
- self-assigned

- certificate 120
- sending diagnostic data 320
- Serial over LAN 211
- serial port
 - configuration 80
 - configure 73, 253
- serial redirect command 231
- serial-to-SSH redirection 212
- serial-to-Telnet redirection 212
- server
 - certificate management 122
 - server addressing
 - DNS 74, 242
 - server firmware
 - updating 158
 - server firmware option
 - under the Server Management tab 43
 - server health 130
 - server management
 - adapters option 200–201
 - local storage option 187, 191, 193–194
 - OS failure screen data 172
 - PXE network boot 157
 - server firmware 158
 - server timeouts, setting 76
- Server Management
 - latest OS failure screen option 70
 - memory option 66
 - power management 71
 - power modules option 62
 - processors option 68
 - PXE network boot option 70
 - server cooling devices option 61
 - server firmware option 43
 - server power actions option 60
 - server properties option 56
 - server timeouts option 69
- server management tab 42
 - adapter configuration 200
 - local storage configuration 187, 191, 193–194
 - scalable complex 71
- Server Management tab
 - adapters option 69
 - local storage option 63
 - power management option 173
- server power
 - controlling 136
- server power actions option
 - under Server Management tab 60
- server power and restart
 - commands 226
- server properties
 - environmentals tab 56
 - general settings tab 56
 - hardware activity tab 56
 - hardware information tab
 - network hardware tab 56
 - system component information tab 56
 - system information tab 56
 - LED tab 56
- server properties option
 - under Server Management tab 56
- server status
 - monitoring 127
- server target name
 - LDAP 75, 248
- server timeout
 - selections 76
- server timeouts option
 - under Server Management tab 69
- service advisor commands 313
- service and support
 - before you call 319
 - hardware 321
 - software 320

- service and support data
 - collecting 170
 - downloading 170
- service and support tab
 - overview 33
- services and support
 - option, problems 33
 - option, settings 36
- services and support tab
 - download service data 33
 - problems 33
 - settings 33
- services command 277
- sessions, maximum
 - Telnet 75, 300
- set
 - autonegotiation 74, 245
 - CIM over HTTP port 76, 252
 - CIM over HTTPS port 76, 252
 - CLI key sequence 73, 253
 - date 73, 311
 - host name 74, 245
 - HTTP port 76, 252
 - HTTPS port 76, 252
 - LDAP server port 75, 248
 - maximum transmission unit 74, 245
 - MTU 74, 245
 - Remote Control port 76, 252
 - SNMP agent port 76, 252
 - SNMP Traps port 76, 252
 - SNMPv1 contact 74, 279
 - SNMPv3 contact 74, 279
 - SSH CLI port 76, 252
 - Telnet CLI port 76, 252
 - time 73, 311
 - user authentication method 74, 232
 - VLAN enablement 74
 - web inactivity timeout 74, 232
- set command 278
- set port numbers 76, 252
- setting
 - IMM2 firmware automated promotion 78
 - the IMM2 date and time 78
- setting server timeouts 76
- setting up
 - alert recipients 30
- settings
 - access control 105
 - advanced 90
 - CIM over HTTPS 108
 - cryptography management 115
 - DDNS 95
 - DNS 95
 - Ethernet 90
 - for the web session 19
 - global login 86
 - account security level tab 87
 - general tab 86
 - HTTPS 107
 - LDAP 96
 - LDAP client protocol 109
 - port assignments 104
 - security 106
 - services and support tab 33
 - SMTP 96
 - SNMP alert 93
 - ssh server 111
 - Telnet 100
 - USB 101
- settings, option
 - services and support 36
- setup wizard
 - IMM2 76
- single cursor mode 146
- SKLM

- key repository servers 119
- option 117
- SKLM certificate
 - management 120, 122
- SKLM certificate management
 - drive access page 120, 122
- SKLM device group
 - configuration 120
- SKLM key repository servers
 - configure 119
 - drive access page 119
- SMTP
 - configure 75, 278
 - server host name 75, 278
 - server IP address 75, 278
 - server port number 75, 278
 - test 75
- smtp command 278
- SNMP agent port
 - set 76, 252
- snmp command 279
- SNMP Traps port
 - set 76, 252
- snmpalerts command 282
- SNMPv1
 - configure 74, 279
- SNMPv1 communities
 - manage 74, 279
- SNMPv1 contact
 - set 74, 279
- SNMPv1 traps
 - configure 74, 279
- SNMPv3 contact
 - set 74, 279
- SNMPv3 settings
 - user 74, 303
- SNMPv3 user accounts
 - configure 74, 303
- software service and support telephone numbers 320
- spreset command 313
- srcfg command 283
- SSH CLI port
 - set 76, 252
- SSH keys
 - user 74, 303
- SSH server
 - certificate management 76, 284
 - security 76, 284
- sshcfg command 284
- SSL
 - certificate handling 112
 - certificate management 112
- ssl command 285
- sslcfg command 286
- startup sequence, changing 13
- static IP address, default 10
- storage command 289
 - storage devices 289
- storage devices
 - storage command 289
- storage pools
 - logical
 - physical 187
 - logical drives 191
 - physical drives 187
- storekeycfg command 299
- support web page, custom 320
- syshealth command 224
- system event
 - notification 165
 - retry notification 165
- system event notification 30
- system information 129
- system status 127
- system status page, overview 22

- system status tab
 - overview 22
- System x Server Firmware
 - description 1
 - Setup utility 10
- Systems Director, IBM
 - systems management tool 40
- systems management tool
 - IBM Systems Director 40

T

- tab
 - video recording 148
- Taiwan Class A electronic emission statement 329
- Taiwan product service 321
- target name, server
 - LDAP 75, 248
- telecommunication regulatory statement 326
- telephone numbers 320–321
- Telnet
 - access 75, 300
 - configure 300
 - maximum sessions 75, 300
- Telnet CLI port
 - set 76, 252
- Telnet settings
 - configure 75
- telnetcfg command 300
- temps command 225
- test
 - SMTP 75
- test events
 - generate 165
- the system information
 - viewing 129
- thermal command 302
- time
 - set 73, 311
- timeouts command 302
- TLS
 - minimum level 301
- TLS command 301
- tools
 - IPMITool 211
- trademarks 324
- trespass message option 20
- two power supplies
 - configure 173

U

- UID search attribute
 - LDAP server 75, 248
- unassigned nodes
 - scalable complex 182
- United States FCC Class A notice 326
- unmount
 - devices 156
- updating
 - the ActiveX applet 138
 - the Java applet 138
- updating firmware 138
- upload image
 - Remote Disk On Chip 154
- USB
 - configure 75, 243
- usbeth command 303
- user
 - delete 74, 303
 - manage 74, 303
 - password 74, 303

- SNMPv3 settings 74, 303
- SSH keys 74, 303
- user account
 - create 74, 303
 - group profile 85
 - management 81
- user account security levels
 - configure 74, 232
- user accounts
 - configuring 81
- user authentication method
 - set 74, 232
- users
 - view current 74, 303
- users command 303
- using
 - ActiveX client 48
 - Java client 48
 - remote control feature 137
 - remote presence function 137
- utility commands 216

V

- video color mode in remote control 141
- video recording
 - launch 148
 - tab 148
- video viewer 148
- Video Viewer
 - absolute mouse control 145
 - exiting 157
 - international keyboard support 144
 - keyboard pass-through mode 144
 - mouse support 145
 - performance statistics 147
 - power and restart commands 146
 - relative mouse control 145
 - relative mouse control for Linux (default Linux acceleration) 145
 - screen capture 138
 - single cursor mode 146
 - video color mode 141

- view modes 139
- view backup status
 - IMM 76
- view configuration
 - IMM2 76
- view current
 - users 74, 303
- view firmware information
 - server 73, 226
- view modes in remote control 139
- view open ports 75, 252
- view restore status
 - IMM2 76
- viewing
 - the hardware health 131
 - the server health 130
 - the system status 127
- viewing and managing
 - scalable complex partitions 182
- Virtual Light Path 13
- Virtual Media Session
 - disk image 154–156
 - exiting 157
 - launch 153
 - remote disk 153
 - Remote Disk On Chip 154
- VLAN enablement
 - set 74
- volts command 225
- vpd command 226

W

- Web browser requirements 4
- web inactivity timeout
 - set 74, 232
- web interface
 - logging in to web interface 11
- web interface, opening and using 9
- web session settings 19
- working with
 - events in the event log 28

Lenovo™

Part Number: 00YJ305

Printed in China

(1P) P/N: 00YJ305

