Integrated Management Module I
User's Guide

Integrated Management Module I
User's Guide

Sixth Edition (May 2013)

Contents

Tables

Chapter 1. Introduction

The integrated management module (IMM) consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities in a single chip on the server system board. The IMM replaces the baseboard management controller (BMC) and Remote Supervisor Adapter II in IBM® System x servers.

Before the IMM was used in IBM servers, the baseboard management controller (BMC) and basic input/output system (BIOS) were the standard systems-management hardware and firmware. System x servers used BMC service processors to manage the interface between systems-management software and platform hardware. The Remote Supervisor Adapter II and Remote Supervisor Adapter II Slimline were optional controllers for out-of-band server management.

Important: Although the IMM is standard in some IBM BladeCenter products and IBM blade servers, the BladeCenter advanced management module remains the primary management module for systems-management functions and keyboard/video/mouse (KVM) multiplexing for BladeCenter and blade servers. The contents that are related to IMM Web Interface and the Command-line Interface do not apply to IBM BladeCenter and blade servers. Users who wish to configure the IMM settings on blade servers should use the Advanced Settings Utility (ASU) on the blade server to perform those actions.

The IMM offers several improvements over the combined functionality of the BMC and the Remote Supervisor Adapter II:

- Choice of dedicated or shared Ethernet connection. The dedicated Ethernet connection is not available on blade servers or some System x servers.

  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 IMM setting available.
- One IP address for both the Intelligent Platform Management Interface (IPMI) and the service processor interface. The feature does not apply to blade servers.
- Embedded Dynamic System Analysis (DSA).
- Ability to locally or remotely update other entities without requiring a server restart to initiate the update process.
- Remote configuration with Advanced Settings Utility (ASU). The feature does not apply to blade servers.
- Capability for applications and tools to access the IMM either in-band or out-of-band. Only the in-band IMM connection is supported on blade servers.
- Enhanced remote-presence capabilities. The feature does not apply to blade servers.

IBM System x® Server Firmware is IBM's implementation of Unified Extensible Firmware Interface (UEFI). It replaces BIOS in System x servers and IBM blade servers. The BIOS was the standard firmware code that controlled basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard. IBM System x Server Firmware offers several features that BIOS does not, including UEFI 2.1 compliance, iSCSI compatibility, Active Energy Manager

technology, and enhanced reliability and service capabilities. The Setup utility provides server information, server setup, customization compatibility, and establishes the boot device order.

Notes:

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

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

This document does not contain explanations of errors or messages. IMM errors and messages are described in the *Problem Determination and Service Guide* that came with your server. To find the latest version of this document or the IBM white paper *Transitioning to UEFI and IMM* on the IBM® Support Portal, complete the following steps.

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

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

1. Go to http://www.ibm.com/support/entry/portal.
2. Under **Choose your products**, select **Browse for a product** and expand **Hardware**.
3. Depending on your type of server, click **Systems** > **System x** or **Systems** > **BladeCenter**, and check the box for your server or servers.
4. Under **Choose your task**, click **Documentation**.
5. Under **See your results**, click **View your page**.
6. In the Documentation box, click **More results**.
7. In the Category box, select the **Integrated Management Module (IMM)** check box. Links to the IMM and UEFI documentation appear.

If firmware updates are available, you can download them from the IBM website. The IMM might have features that are not described in the documentation, and the documentation might be updated occasionally to include information about those features, or technical updates might be available to provide additional information that is not included in the IMM documentation.

To check for firmware updates, complete the following steps.

Note: The first time you access the IBM Support Portal, you must choose the product category, product family, and model numbers for your server. The next time you access the IBM Support Portal, the products you selected initially are

preloaded by the website, and only the links for your products are displayed. To change or add to your product list, click the **Manage my product lists** link.

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

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

IMM features

The IMM provides the following functions:

- 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
- Web-based management with standard web browsers

IMM provides two types of IMM functionality: IMM Standard features and IMM Premium features. For information about the type of IMM hardware in your server, see the documentation that came with the server.

IMM Standard features

Note: Some the following features do not apply to blade servers.

- Access to critical server settings
- Access to server vital product data (VPD)
- Advanced Predictive Failure Analysis (PFA) support
- Automatic notification and alerts
- Continuous health monitoring and control
- Choice of a dedicated or shared Ethernet connection (if applicable).

  Note: A dedicated systems-management network port might not be available on your server.
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- E-mail alerts
- Embedded Dynamic System Analysis (DSA)
- Enhanced user authority levels
- LAN over USB for in-band communications to the IMM
- Event logs that are time stamped, saved on the IMM, and can be attached to e-mail alerts
- Industry-standard interfaces and protocols
- OS watchdogs

- Remote configuration through Advanced Settings Utility (ASU)
- Remote firmware updating
- Remote power control
- Seamless remote accelerated graphics
- Secure web server user interface
- Serial over LAN
- Server console redirection
- Simple Network Management Protocol (SNMP) support
- User authentication using a secure connection to a Lightweight Directory Access Protocol (LDAP) server

IMM Premium features

Note: Some the following features do not apply to blade servers.

- Access to critical server settings
- Access to server vital product data (VPD)
- Advanced Predictive Failure Analysis (PFA) support
- Automatic notification and alerts
- Continuous health monitoring and control
- Choice of a dedicated or shared Ethernet connection (if applicable).

  Note: A dedicated systems-management network port might not be available on your server.
- Domain Name System (DNS) server support
- Dynamic Host Configuration Protocol (DHCP) support
- E-mail alerts
- Embedded Dynamic System Analysis (DSA)
- Enhanced user authority levels
- LAN over USB for in-band communications to the IMM
- Event logs that are time stamped, saved on the IMM, and can be attached to e-mail alerts
- Industry-standard interfaces and protocols
- OS watchdogs
- Remote configuration through Advanced Settings Utility (ASU)
- Remote firmware updating
- Remote power control
- Seamless remote accelerated graphics
- Secure web server user interface
- Serial over LAN
- Server console redirection
- Simple Network Management Protocol (SNMP) support
- User authentication using a secure connection to a Lightweight Directory Access Protocol (LDAP) server
- Remote presence, including the remote control of a server
- Operating-system failure screen capture and display through the web interface
- Remote disk, which enables the attachment of a diskette drive, CD/DVD drive, USB flash drive, or disk image to a server

Note: The following features of the Remote Supervisor Adapter II are not in the IMM:

- Display of server MAC addresses
- Multiple NTP server entries

Upgrading from IMM Standard to IMM Premium

If your server has IMM Standard functionality, you can upgrade to IMM Premium by purchasing and installing a virtual media key on your server system board. No new firmware is required.

To order a virtual media key, go to http://www.ibm.com/systems/x/newgeneration.

Note: For information about installing the virtual media key, see the documentation that came with your server.

If you need help with your order, call the toll-free number that is listed on the retail parts page, or contact your local IBM representative for assistance.

Comparing the IMM to other systems-management hardware in System x servers

The following table compares IMM features with BMC and Remote Supervisor Adapter II features in System x servers.

Note: Like the BMC, the IMM uses the standard IPMI specification.

Table 1. Comparison of the IMM features and combined BMC and Remote Supervisor Adapter II features in System x servers

Description	BMC with Remote Supervisor Adapter II	IMM
Network connections	BMC uses a network connection that is shared with a server and an IP address that is different from the Remote Supervisor Adapter II IP address. Remote Supervisor Adapter II uses a dedicated systems-management network connection and an IP address that is different from the BMC IP address.	The IMM provides both BMC and Remote Supervisor Adapter II functionality through the same network connection. One IP address is used for both. If your server has a dedicated systems-management network port, you can choose either a dedicated or a shared network connection. **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 IMM setting available.
Update capabilities	Each server requires a unique update for BMC and Remote Supervisor Adapter II. BIOS and diagnostic tools can be updated in-band.	One IMM firmware image can be used for all of the applicable servers. The IMM firmware, System x server firmware, and Dynamic System Analysis (DSA) firmware can be updated both in-band and out-of-band. The IMM can update itself, the server firmware, and the DSA firmware either locally or remotely without requiring the server to be restarted to initiate the update process.

Table 1. Comparison of the IMM features and combined BMC and Remote Supervisor Adapter II features in System x servers (continued)

Description	BMC with Remote Supervisor Adapter II	IMM
Configuration capabilities	Configuration changes with the ASU are available only in-band. The system requires separate configurations for BMC, Remote Supervisor Adapter II, and BIOS.	The ASU can run either in-band or out-of-band and can configure both the IMM and the server firmware. With the ASU, you can also modify the boot order, iSCSI, and VPD (machine type, serial number, UUID, and asset ID). The server firmware configuration settings are kept by the IMM. Therefore, you can make server firmware configuration changes while the server is turned off or while the operating system is running, and those changes are effective the next time the server is started. The IMM configuration settings can be configured in-band or out-of-band through the following IMM user interfaces: • Web interface • Command-line interface • IBM Systems Director interface • SNMP
Operating-system screen capture	Screen captures are performed by the Remote Supervisor Adapter II when operating-system failures occur. The display of screen captures requires a Java applet.	This feature is available only with IMM Premium. For information about upgrading from IMM Standard to IMM Premium, see "Upgrading from IMM Standard to IMM Premium" on page 5. Screen captures are displayed directly by the web browser without the need for a Java applet.
Error logging	The BMC provides a BMC system-event log (IPMI event log). The Remote Supervisor Adapter II provides a text-based log that includes descriptions of events that are reported by the BMC. This log also contains any information or events detected by the Remote Supervisor Adapter II itself.	The IMM has two event logs: 1. The system-event log is available through the IPMI interface. 2. The chassis-event log is available through the other IMM interfaces. The chassis-event log displays text messages that are generated using the Distributed Management Task Force specifications DSP0244 and DSP8007. **Note:** For an explanation of a specific event or message, see the *Problem Determination and Service Guide* that came with your server.

Table 1. Comparison of the IMM features and combined BMC and Remote Supervisor Adapter II features in System x servers (continued)

Description	BMC with Remote Supervisor Adapter II	IMM
Monitoring	The BMC with Remote Supervisor Adapter II has the following monitoring capabilities: • Monitoring of server and battery voltage, server temperature, fans, power supplies, and processor and DIMM status • Fan speed control • Predictive Failure Analysis (PFA) support • System diagnostic LED control (power, hard disk drive, activity, alerts, heartbeat) • Automatic Server Restart (ASR) • Automatic BIOS Recovery (ABR)	The IMM provides the same monitoring capabilities as the BMC and Remote Supervisor Adapter II. When used in a RAID configuration, expanded hard disk drive status, including disk drive PFA, is supported by the IMM.
Remote presence	The BMC with Remote Supervisor Adapter II has the following remote presence capabilities: • Graphical console redirection over LAN • Remote virtual diskette and CD-ROM • High-speed remote redirection of PCI video, keyboard, and mouse • Video resolution up to 1024 x 768, at 70 Hz, is supported • Data encryption	This feature is available only with IMM Premium. For information about upgrading from IMM Standard to IMM Premium, see "Upgrading from IMM Standard to IMM Premium" on page 5. In addition to the Remote Supervisor Adapter II remote presence features, the IMM also has the following capabilities. **Note:** The IMM requires Java Runtime Environment 1.5 or later, or ActiveX if Internet Explorer is used in Windows. • Video resolution up to 1280 x 1024, at 75 Hz, is supported • USB 2.0 support for virtual keyboard, mouse, and mass storage devices • 15-bit color depth • Choice of either absolute or relative mouse mode • USB flash drive support • Server power and reset control on the Remote Control window • Video on the Remote Control window can be saved in a file The IMM provides two separate client windows. One is for video and keyboard and mouse interaction, and the other one is for virtual media. The IMM web interface has a menu item that allows color depth adjustment to reduce the data transmitted in low-bandwidth situations. The Remote Supervisor Adapter II interface has a bandwidth slider.
Security	Remote Supervisor Adapter II has advanced security features, including Secure Sockets Layer (SSL) and encryption.	The IMM has the same security features as Remote Supervisor Adapter II.

Table 1. Comparison of the IMM features and combined BMC and Remote Supervisor Adapter II features in System x servers (continued)

Description	BMC with Remote Supervisor Adapter II	IMM
Serial redirection	The IPMI Serial over LAN (SOL) function is a standard capability of the BMC. The Remote Supervisor Adapter II provides the ability to redirect server serial data to a Telnet or SSH session. **Note:** This feature is not available on some servers.	The COM1 port is used for SOL on System x servers. COM1 is configurable only through the IPMI interface. The COM2 port is used for serial redirection through Telnet or SSH. COM2 is configurable through all of the IMM interfaces except for the IPMI interface. The COM2 port is used for SOL on blade servers. Both COM port configurations are limited to 8 data bits, null parity, 1 stop bit, and a baud rate choice of 9600, 19200, 38400, 57600, 115200, or 230400. On blade servers, the COM2 port is an internal COM port with no external access. IPMI serial-port sharing is not possible on blade servers. On rack-mounted and tower servers, the IMM COM2 port is an internal COM port with no external access.
SNMP	SNMP support is limited to SNMPv1.	The IMM supports SNMPv1 and SNMPv3.

Using IMM with a BladeCenter advanced management module

The BladeCenter advanced management module is the standard systems-management interface in IBM BladeCenter and IBM blade servers. Although the IMM is now included in some IBM BladeCenter and IBM blade servers, the advanced management module remains the management module for systems-management functions and keyboard, video, and mouse (KVM) multiplexing for BladeCenter and blade servers. The external network interfaces to the IMM are not available in BladeCenter.

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

Web browser and operating-system requirements

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

- Microsoft Internet Explorer version 6.0 or later with the latest Service Pack
- Mozilla Firefox version 1.5 or later

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

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003

- Red Hat Enterprise Linux versions 4.0 and 5.0
- SUSE Linux version 10.0
- Novell NetWare 6.5

Note: The IMM web interface does not support the double-byte character set (DBCS) languages.

Notices used in this book

The following notices are used in the documentation:

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

Chapter 2. Opening and using the IMM web interface

The IMM 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 IMM remotely by using the IMM web interface, you must first log in. This chapter describes the login procedures and the actions that you can perform from the IMM web interface.

Accessing the IMM web interface

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

IMM also supports IPv6, but the IMM does not have a fixed static IPv6 IP address by default. For initial access to the IMM in an IPv6 environment, you can either use the IPv4 IP address or the IPv6 link-local address. The IMM generates a unique link-local IPv6 address, which is shown in the IMM 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 IMM, 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 IMM provides the choice of using a dedicated systems-management network connection (if applicable) or one that is shared with the server. The default connection for rack-mounted and tower servers is to use the dedicated systems-management network connector.

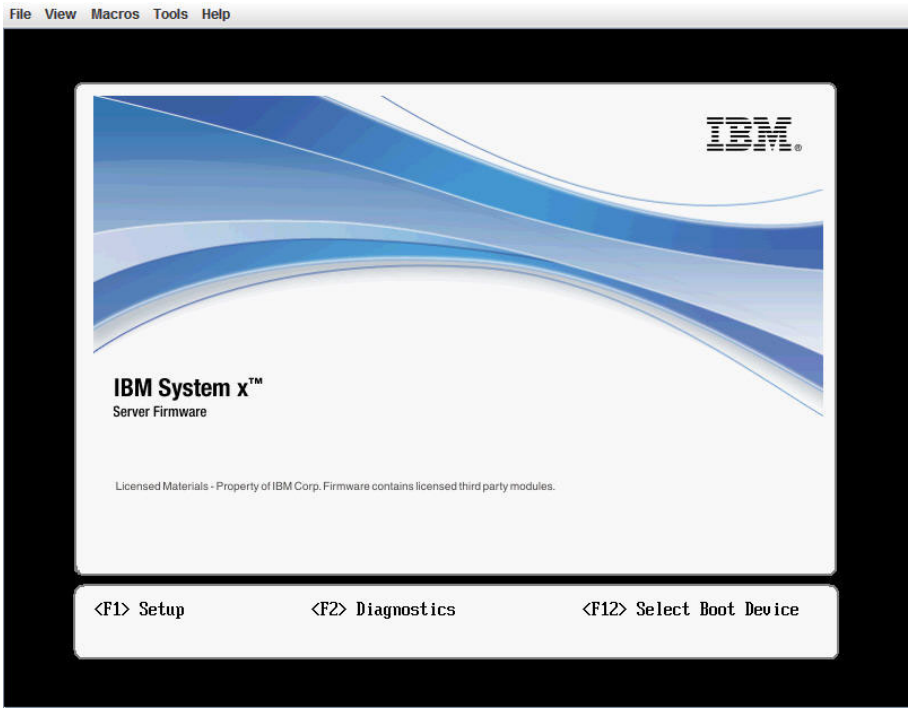
Note: A dedicated systems-management network port might not be available on your server. If your hardware does not have a dedicated network port, the *shared* setting is the only IMM setting available.

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

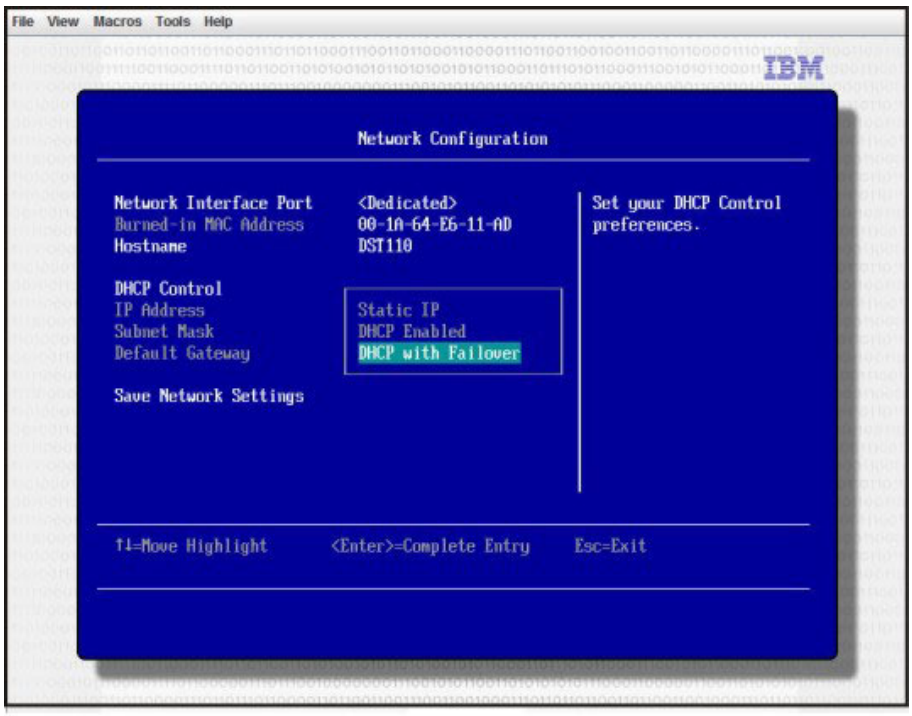
After you start the server, you can use the Setup utility to select an IMM network connection. The server with the IMM hardware must be connected to a Dynamic Host Configuration Protocol (DHCP) server, or the server network must be configured to use the IMM static IP address. To set up the IMM network connection through the Setup utility, complete the following steps:

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

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.



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



7. Select one of the network connection choices.
8. If you choose to use a static IP address, you must specify the IP address, the subnet mask, and the default gateway.
9. You can also use the Setup utility to select a dedicated network connection (if your server has a dedicated network port) or a shared IMM 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 IMM 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 IMM, see the documentation that came with your server.
10. Select **Save Network Settings**.
11. Exit from the Setup utility.

Notes:

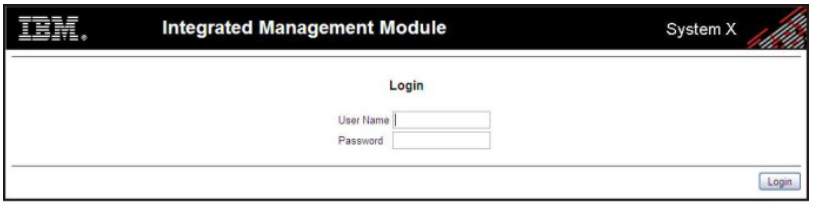
- You must wait approximately 1 minute for changes to take effect before the server firmware is functional again.
- You can also configure the IMM network connection through the IMM web interface. For more information, see “Configuring network interfaces” on page 36.

Logging in to the IMM

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

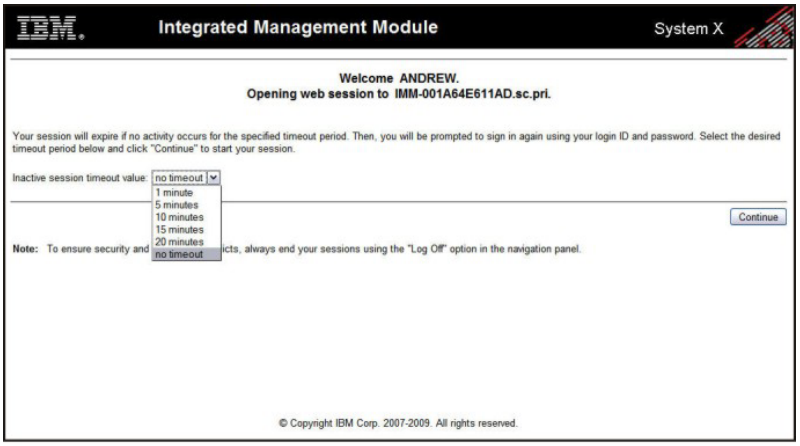
To access the IMM through the IMM web interface, complete the following steps:

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

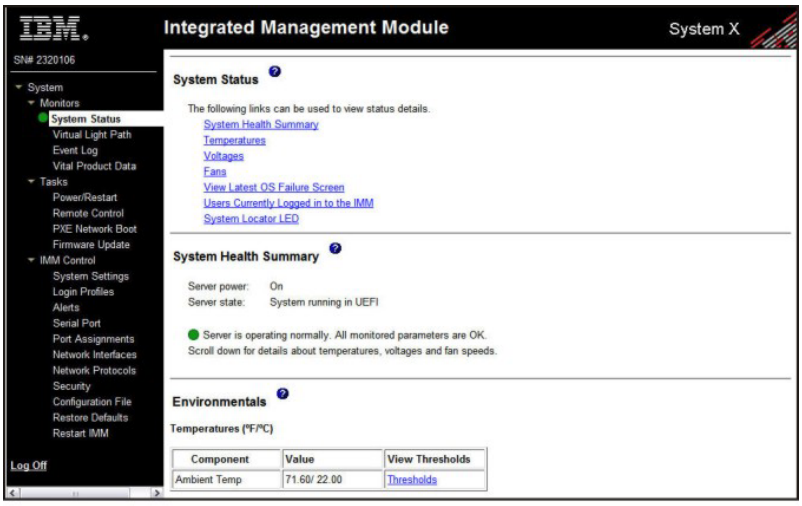


2. Type your user name and password in the IMM Login window. If you are using the IMM for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. Depending on how your system administrator configured the user ID, you might need to enter a new password.
3. On the Welcome webpage, select a timeout value from the drop-down list in the field that is provided. If your browser is inactive for that number of minutes, the IMM logs you off the web interface.

   Note: Depending on how your system administrator configured the global login settings, the timeout value might be a fixed value.



4. Click **Continue** to start the session. The browser opens the System Status page, which gives you a quick view of the server status and the server health summary.



For descriptions of the actions that you can perform from the links in the left navigation pane of the IMM web interface, see "IMM action descriptions." Then, go to Chapter 3, "Configuring the IMM," on page 19.

IMM action descriptions

Table 2 lists the actions that are available when you are logged in to the IMM.

Table 2. IMM actions

Link	Action	Description
System Status	View system health for a server, view the operating-system-failure screen capture, and view the users who are logged in to the IMM	You can monitor the server power and health state, and the temperature, voltage, and fan status of your server on the System Health page. You can also view the image of the last operating-system-failure screen capture and the users who are logged in to the IMM.
Virtual Light Path	View the name, color, and status of every LED on the server light path	The Virtual Light Path page displays the current status of the LEDs on the server.
Event Log	View event logs for remote servers	The Event Log page contains entries that are currently stored in the chassis-event log. The log includes a text description of events that are reported by the BMC, plus information about all remote access attempts and configuration changes. All events in the log are time stamped, using the IMM date and time settings. Some events also generate alerts, if they are configured to do so on the Alerts page. You can sort and filter events in the event log.
Vital Product Data	View the server vital product data (VPD)	The IMM collects server information, server firmware information, and server component VPD. This data is available from the Vital Product Data page.
Power/Restart	Remotely turn on or restart a server	The IMM provides full remote power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability.

Table 2. IMM actions (continued)

Link	Action	Description
Remote Control	Redirect the server video console and use your computer disk drive or disk image as a drive on the server	From the Remote Control page, you can start the Remote Control feature. With Remote Control, you can view 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. You can use your mouse and keyboard to interact with and control 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.
PXE Network Boot	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	If your server firmware and PXE boot agent utility are properly defined, from the PXE Network Boot page you can change the host server startup (boot) sequence for the next restart to attempt a PXE/DHCP network startup. The host startup sequence will be altered only if the host is not under Privileged Access Protection (PAP). After the next restart occurs, the check box on the PXE Network Boot page will be cleared.
Firmware Update	Update firmware on the IMM	Use the options on the Firmware Update page to update the IMM firmware, server firmware, and DSA firmware.
System Settings	View and change the IMM server settings	You can configure the server location and general information, such as the name of the IMM, server timeout settings, and contact information for the IMM, from the System Settings page.
	Set the IMM clock	You can set the IMM clock that is used for time stamping the entries in the event log.
	Enable or disable the USB in-band interface	You can enable or disable the USB in-band (or LAN over USB) interface.
Login Profiles	Configure the IMM login profiles and global login settings	You can define up to 12 login profiles that enable access to the IMM. You can also define global login settings that apply to all login profiles, including enabling Lightweight Directory Access Protocol (LDAP) server authentication and customizing the account security level.
Alerts	Configure remote alerts and remote alert recipients	You can configure the IMM to generate and forward alerts for different events. On the Alerts page, you can configure the alerts that are monitored and the recipients that are notified.
	Configure Simple Network Management Protocol (SNMP) events	You can set the event categories for which SNMP traps are sent.
	Configure alert settings	You can establish global settings that apply to all remote alert recipients, such as the number of alert retries and the delay between the retries.
Serial Port	Configure the IMM serial port settings	From the Serial Port page, you can configure the serial port baud rate that is used by the serial redirection function. You can also configure the key sequence that is used to switch between the serial redirection and command-line interface (CLI) modes.
Port assignments	Change the port numbers of the IMM protocols	From the Port Assignments page, you can view and change the port numbers assigned to the IMM protocols (for example, HTTP, HTTPS, Telnet, and SNMP).

Table 2. IMM actions (continued)

Link	Action	Description
Network Interfaces	Configure the network interfaces of the IMM	From the Network Interfaces page, you can configure network-access settings for the Ethernet connection on the IMM.
Network Protocols	Configure the network protocols of the IMM	You can configure Simple Network Management Protocol (SNMP), Domain Name System (DNS), and Simple Mail Transfer Protocol (SMTP) settings that are used by the IMM from the Network Protocols page. You can also configure LDAP parameters.
Security	Configure the Secure Sockets Layer (SSL)	You can enable or disable SSL and manage the SSL certificates that are used. You can also enable or disable whether an SSL connection is used to connect to an LDAP server.
	Enable Secure Shell (SSH) access	You can enable SSH access to the IMM.
Configuration File	Back up and restore the IMM configuration	You can back up, modify, and restore the configuration of the IMM, and view a configuration summary, from the Configuration File page.
Restore Default Settings	Restore the IMM default settings	**Attention:** When you click **Restore Defaults**, all of the modifications that you made to the IMM are lost. You can reset the configuration of the IMM to the factory defaults.
Restart IMM	Restart the IMM	You can restart the IMM.
Scalable Partitioning	Configure server as a partition in a scalable complex.	If the server is configured in a scalable complex, the IMM allows you to control the system in a complex. If there is a problem with the server being scalable, the IMM will report an error.
Service Advisor	Forwards serviceable event codes to IBM support	When enabled, Service Advisor allows the IMM to forward serviceable event codes to IBM support for further troubleshooting. **Note:** See the documentation for your server to see if your server supports this feature.
Log off	Log off the IMM	You can log off your connection to the IMM.

You can click the **View Configuration Summary** link, which is in the top-right corner on most pages, to quickly view the configuration of the IMM.

Chapter 3. Configuring the IMM

Use the links under **IMM Control** in the navigation pane to configure the IMM.

From the System Settings page, you can:

- Set server information
- Set server timeouts
- Set IMM date and time
- Enable or disable commands on the USB interface

From the Login Profiles page, you can:

- Set login profiles to control access to the IMM
- Configure global login settings, such as the lockout period after unsuccessful login attempts
- Configure the account security level

From the Alerts page, you can:

- Configure remote alert recipients
- Set the number of remote alert attempts
- Select the delay between alerts
- Select which alerts are sent and how they are forwarded

From the Serial Port page, you can:

- Configure the baud rate of serial port 2 (COM2) for serial redirection
- Specify the keystroke sequence that is used to switch between the serial redirection and the command-line interface (CLI)

From the Port Assignments page, you can change the port numbers of IMM services.

From the Network Interfaces page, you can set up the Ethernet connection for the IMM.

From the Network Protocols page, you can configure:

- SNMP setup
- DNS setup
- Telnet protocol
- SMTP setup
- LDAP setup
- Service location protocol

From the Security page, you can install and configure the Secure Sockets Layer (SSL) settings.

From the Configuration File page, you can back up, modify, and restore the configuration of the IMM.

From the Restore Defaults page, you can reset the IMM configuration to the factory defaults.

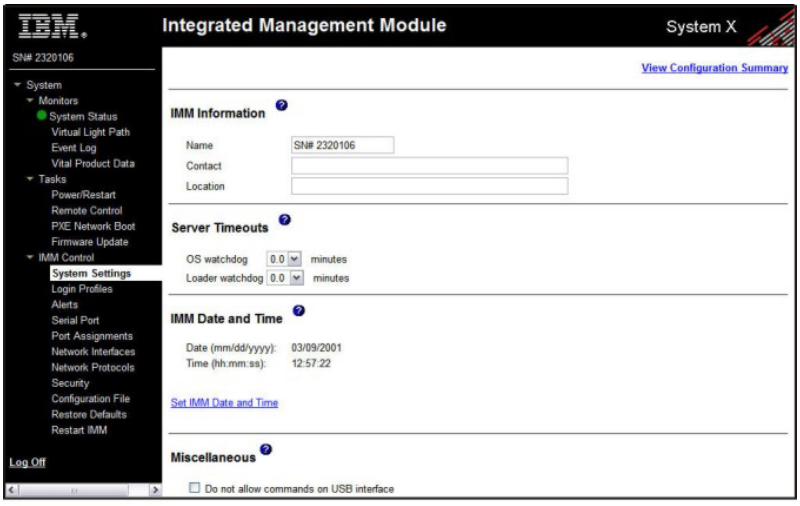
From the Restart IMM page, you can restart the IMM.

Setting system information

To set the IMM system information, complete the following steps:

1. Log in to the IMM where you want to set the system information. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **System Settings**. A page similar to the one in the following illustration is displayed.

   Note: The available fields in the System Settings page are determined by the accessed remote server.



3. In the **Name** field in the **IMM Information** area, type the name of the IMM. Use the **Name** field to specify a name for the IMM in this server. The name is included with e-mail and SNMP alert notifications to identify the source of the alert.

   Note: Your IMM name (in the **Name** field) and the IP host name of the IMM (in the **Hostname** field on the Network Interfaces page) do not automatically share the same name because the **Name** field is limited to 16 characters. The **Hostname** field can contain up to 63 characters. To minimize confusion, set the **Name** field to the nonqualified portion of the IP host name. The nonqualified IP host name consists of up to the first period of a fully qualified IP host name. For example, for the fully qualified IP host name imm1.us.company.com, the nonqualified IP host name is imm1. For information about your host name, see "Configuring network interfaces" on page 36.
4. In the **Contact** field, type the contact information. For example, you can specify the name and phone number of the person to contact if there is a problem with this server. You can type a maximum of 47 characters in this field.
5. In the **Location** field, type the location of the server. Include in this field sufficient detail to quickly locate the server for maintenance or other purposes. You can type a maximum of 47 characters in this field.
6. Scroll to the bottom of the page and click **Save**.

Setting server timeouts

Note: Server timeouts require that the in-band USB interface (or LAN over USB) be enabled to allow commands. For more information about the enabling and disabling commands for the USB interface, see "Disabling the USB in-band interface" on page 23. For information regarding the installation of the required device drivers, see "Installing device drivers" on page 122.

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

1. Log in to the IMM where you want to set the server timeouts. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **System Settings** and scroll down to the **Server Timeouts** area.

   You can set the IMM 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 IMM to respond to automatically.

   OS watchdog

   Use the **OS watchdog** field to specify the number of minutes between checks of the operating system by the IMM. If the operating system fails to respond to one of these checks, the IMM 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 a time interval from the menu. To turn off this watchdog, select **0.0** from the menu. To capture operating-system-failure screens, you must enable the watchdog in the **OS watchdog** field.

   Loader watchdog

   Use the **Loader watchdog** field to specify the number of minutes that the IMM waits between the completion of POST and the starting of the operating system. If this interval is exceeded, the IMM 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 IMM waits for the operating-system startup to be completed. To turn off this watchdog, select **0.0** from the menu.

   Power off delay

   Use the **Power off delay** field to specify the number of minutes that the IMM waits for the operating system to shut down before it turns off the server power (if the power was not turned off by the operating system itself). If you set the power off delay, you can make sure that the operating system has enough time for an orderly shutdown before the server power is turned off. To determine the power off delay for your server, shut down your server and observe the amount of time it takes to shut down. Add a time buffer to that value and use the resulting number as your power off delay setting.

To set the power off delay value, select the desired time value from the menu. A value of X'0' means that the operating system, not the IMM, turns off the server power.

4. Scroll to the bottom of the page and click **Save**.

Setting the IMM date and time

The IMM uses its own real-time clock to time stamp all events that are logged in the event log.

Note: The IMM date and time setting affects only the IMM clock, not the server clock. The IMM real-time clock and the server clock are separate, independent clocks and can be set to different times. To synchronize the IMM clock with the server clock, go to the **Network Time Protocol** area of the page and set the NTP server host name or IP address to the same server host name or IP address that is used to set the server clock. See "Synchronizing clocks in a network" on page 23 for more information.

Alerts that are sent by e-mail and 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 (DST) 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.

To verify the date and time settings of the IMM, complete the following steps:

1. Log in to the IMM where you want to set the IMM date and time values. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **System Settings** and scroll down to the **IMM Date and Time** area, which shows the date and time when the webpage was generated.
3. To override the date and time settings and to enable daylight saving time (DST) and Greenwich mean time (GMT) offsets, click **Set IMM Date and Time**. A page similar to the one in the following illustration is displayed.

4. In the **Date** field, type the numbers of the current month, day, and year.
5. In the **Time** field, type the numbers that correspond to the current hour, minutes, and seconds in the applicable entry fields. The hour (hh) must be a number from 00 - 23 as represented on a 24-hour clock. The minutes (mm) and seconds (ss) must be numbers from 00 - 59.
6. In the **GMT offset** field, select the number that specifies the offset, in hours, from Greenwich mean time (GMT), corresponding to the time zone where the server is located.
7. Select or clear the **Automatically adjust for daylight saving changes** check box to specify whether the IMM clock automatically adjusts when the local time changes between standard time and daylight saving time.
8. Click **Save**.

Synchronizing clocks in a network

The Network Time Protocol (NTP) provides a way to synchronize clocks throughout a computer network, enabling any NTP client to obtain the correct time from an NTP server.

The IMM NTP feature provides a way to synchronize the IMM real-time clock with the time that is provided by an NTP server. You can specify the NTP server that is to be used, specify the frequency with which the IMM is synchronized, enable or disable the NTP feature, and request immediate time synchronization.

The NTP feature does not provide the extended security and authentication that are provided through encryption algorithms in NTP Version 3 and NTP Version 4. The IMM NTP feature supports only the Simple Network Time Protocol (SNTP) without authentication.

To set up the IMM NTP feature settings, complete the following steps:

1. Log in to the IMM on which you want to synchronize the clocks in the network. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **System Settings** and scroll down to the **IMM Date and Time** area.
3. Click **Set IMM Date and Time**. A page similar to the one in the following illustration is displayed.

4. Under **Network Time Protocol (NTP)**, you can select from the following settings:

   NTP auto-synchronization service
   Use this selection to enable or disable automatic synchronization of the IMM clock with an NTP server.

   NTP server host name or IP address
   Use this field to specify the name of the NTP server to be used for clock synchronization.

   NTP update frequency
   Use this field to specify the approximate interval (in minutes) between synchronization requests. Enter a value between 3 - 1440 minutes.

   Synchronize Clock Now
   Click this button to request an immediate synchronization instead of waiting for the interval time to lapse.

5. Click **Save**.

Disabling the USB in-band interface

Important: If you disable the USB in-band interface, you cannot perform an in-band update of the IMM firmware, server firmware, and DSA firmware by using the Linux or Windows flash utilities. If the USB in-band interface is disabled,

use the Firmware Update option on the IMM web interface to update the firmware. For more information, see “Updating firmware” on page 115.

If you disable the USB in-band interface, also disable the watchdog timeouts to prevent the server from restarting unexpectedly. For more information, see “Setting server timeouts” on page 21.

The USB in-band interface, or LAN over USB, is used for in-band communications to the IMM. To prevent any application that is running on the server from requesting the IMM to perform tasks, you must disable the USB in-band interface. For more information about LAN over USB, see Chapter 6, “LAN over USB,” on page 121.

To disable the USB in-band interface, complete the following steps:

1. Log in to the IMM on which you want to disable the USB device driver interface. For more information, see Chapter 2, “Opening and using the IMM web interface,” on page 11.
2. In the navigation pane, click **System Settings** and scroll down to the **Miscellaneous** area. A page similar to the one in the following illustration is displayed.

3. To disable the USB in-band interface, select **Disabled** from the **Allow commands on the USB interface** list. Selecting this option does not affect the USB remote presence functions (for example, keyboard, mouse, and mass storage). When you disable the USB in-band interface, the in-band systems-management applications such as the Advanced Settings Utility (ASU) and firmware update package utilities might not work.

   Note: The ASU works with a disabled USB in-band interface if an IPMI device driver is installed.
   If you try to use systems-management applications while the in-band interface is disabled, they might not work.
4. Click **Save**.

To enable the USB device driver interface after it has been disabled, clear the **Do not allow commands on USB interface** check box and click **Save**.

Note:

1. The USB in-band interface is also called "LAN over USB" and is described in more detail in Chapter 6, “LAN over USB,” on page 121.
2. When you attempt a network installation of some Linux distributions, the installation might fail if the IMM USB in-band interface is enabled. For more information, see http://rhn.redhat.com/errata/RHBA-2009-0127.html.
3. If you are performing a network installation that does not contain the update on the Red Hat website described in the preceding note 2, you must disable the USB in-band interface before you perform the installation and enable it after the installation is complete.

4. For information about the configuration of the LAN over USB interface, see "Configuring the LAN over USB interface manually" on page 122.

Creating a login profile

Use the Login Profiles table to view, configure, or change individual login profiles. Use the links in the Login ID column to configure individual login profiles. You can define up to 12 unique profiles. Each link in the Login ID column is labeled with the configured login ID of the associated profile.

Certain login profiles are shared with the IPMI user IDs, providing a single set of local user accounts (username/password) that work with all of the IMM user interfaces, including IPMI. Rules that pertain to these shared login profiles are described in the following list:

- IPMI user ID 1 is always the null user.
- IPMI user ID 2 maps to login ID 1, IPMI user ID 3 maps to login ID 2, and so on.
- The IMM default user is set to `USERID` and `PASSW0RD` (with a zero, not the letter O) for IPMI user ID 2 and login ID 1.

For example, if a user is added through IPMI commands, that user information is also available for authentication through the web, Telnet, SSH, and other interfaces. Conversely, if a user is added on the web or other interfaces, that user information is available for starting an IPMI session.

Because the user accounts are shared with IPMI, certain restrictions are imposed to provide a common ground between the interfaces that use these accounts. The following list describes IMM and IPMI login profile restrictions:

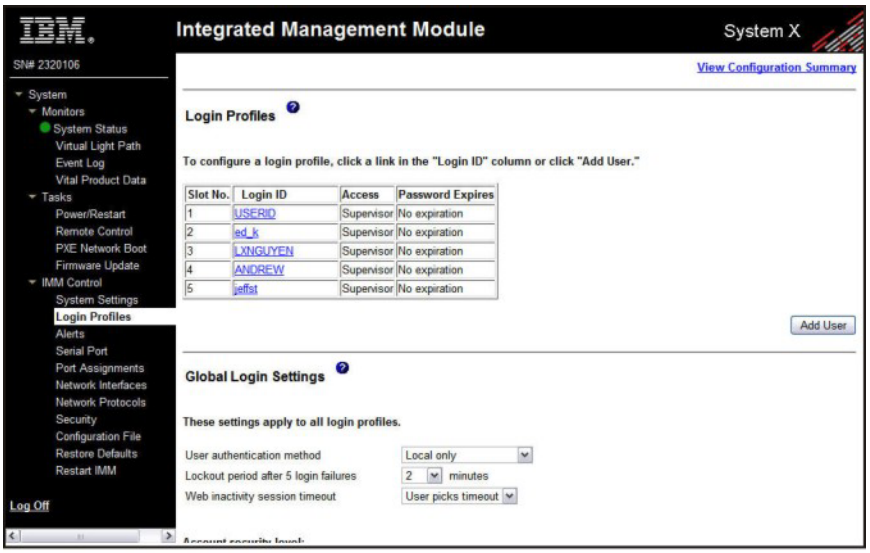
- IPMI allows a maximum of 64 user IDs. The IMM IPMI implementation allows only 12 user accounts.
- IPMI allows anonymous logins (null user name and null password), but the IMM does not.
- IPMI allows multiple user IDs with the same user names, but the IMM does not.
- IPMI requests to change the user name from the current name to the same current name return an `invalid parameter` completion code because the requested user name is already in use.
- The maximum IPMI password length for the IMM is 16 bytes.
- The following words are restricted and are not available for use as local IMM user names:
  - immroot
  - nobody
  - ldap
  - lighttpd
  - sshd
  - daemon
  - immftp

To configure a login profile, complete the following steps:

1. Log in to the IMM where you want to create a login profile. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.

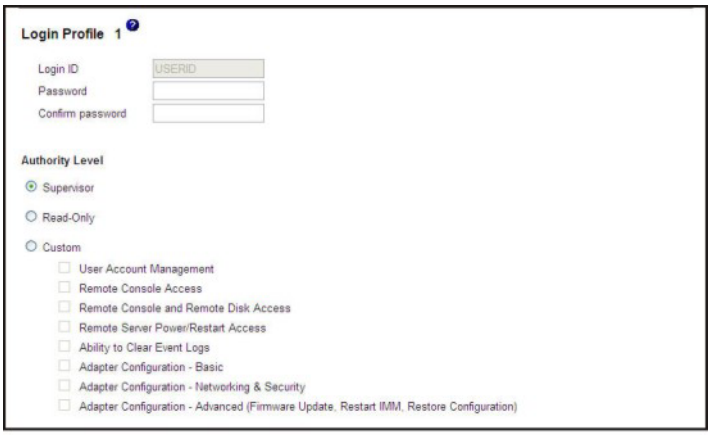
2. In the navigation pane, click **Login Profiles**.

   Note: If you have not configured a profile, it does not appear in the Login Profiles table.
   The Login Profiles page displays each login ID, the login access level, and the password expiration information, as shown in the following illustration.



   Important: By default, the IMM is configured with one login profile that enables remote access using a login user ID of `USERID` and a password of `PASSW0RD` (the 0 is a zero, not the letter O). To avoid a potential security exposure, change this default login profile during the initial setup of the IMM.

3. Click **Add User**. An individual profile page similar to the one in the following illustration is displayed.



4. In the **Login ID** field, type the name of the profile. You can type a maximum of 16 characters in the **Login ID** field. Valid characters are uppercase and lowercase letters, numbers, periods, and underscores.

   Note: This login ID is used to grant remote access to the IMM.

5. In the **Password** field, assign a password to the login ID. A password must contain a minimum of five characters, one of which must be a nonalphabetic character. Null or empty passwords are accepted.

Note: This password is used with the login ID to grant remote access to the IMM.

6. In the **Confirm password** field, type the password again.
7. In the **Authority Level** area, select one of the following options to set the access rights for this login ID:

   Supervisor
   The user has no restrictions.

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

   Custom
   If you select the Custom option, you must select one or more of the following custom authority levels:

   - **User Account Management:** A user can add, modify, or delete users and change the global login settings in the Login Profiles page.
   - **Remote Console Access:** A user can access the remote console.
   - **Remote Console and Virtual Media Access:** A user can access both the remote console and the virtual media feature.
   - **Remote Server Power/Restart Access:** A user can access the power-on and restart functions for the remote server. These functions are available in the Power/Restart page.
   - **Ability to Clear Event Logs:** A user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
   - **Adapter Configuration - Basic:** A user can modify configuration parameters in the System Settings and Alerts pages.
   - **Adapter Configuration - Networking & Security:** A user can modify configuration parameters in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.
   - **Adapter Configuration - Advanced:** A user has no restrictions when configuring the IMM. In addition, the user is said to have administrative access to the IMM, meaning that the user can also perform the following advanced functions: firmware updates, PXE network boot, restore IMM factory defaults, modify and restore IMM configuration from a configuration file, and restart and reset the IMM.

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

   - If the user sets the IMM login ID authority level to Supervisor, the IPMI privilege level is set to Administrator.
   - If the user sets the IMM login ID authority level to Read Only, the IPMI privilege level is set to User
   - If the user sets the IMM login ID authority level to have 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 the user sets the IMM login ID authority level to have Remote Server Power/Restart Access or Ability to Clear Event Logs, the IPMI privilege level is set to Operator.
- If the user sets the IMM login ID authority level to have Adapter Configuration (Basic), the IPMI privilege level is set to User.

Note: To return the login profiles to the factory defaults, click **Clear Login Profiles**.

8. In the **Configure SNMPv3 User** area, select the check box if the user should have access to the IMM by using the SNMPv3 protocol. After you click the check box, an area of the page similar to the one in the following illustration appears.

Use following fields to configure the SNMPv3 settings for the user profile:

Authentication Protocol
Use this field to specify either **HMAC-MD5** or **HMAC-SHA** as the authentication protocol. These are hash algorithms used by the SNMPv3 security model for the authentication. The password for the Linux account will be used for authentication. If you choose **None**, authentication protocol is not used.

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

Privacy Password
Use this field to specify the encryption password.

Confirm Privacy Password
Use this field to confirm the encryption password.

Access Type
Use this field to specify either **Get** or **Set** as the access type. SNMPv3 users with the access type Get can perform only query operations. With the access type Set, SNMPv3 users can both perform query operations and modify settings (for example, setting the password for an user).

Hostname/IP address for traps
Use this field to 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).

9. Click **Save** to save your login ID settings.

Deleting a login profile

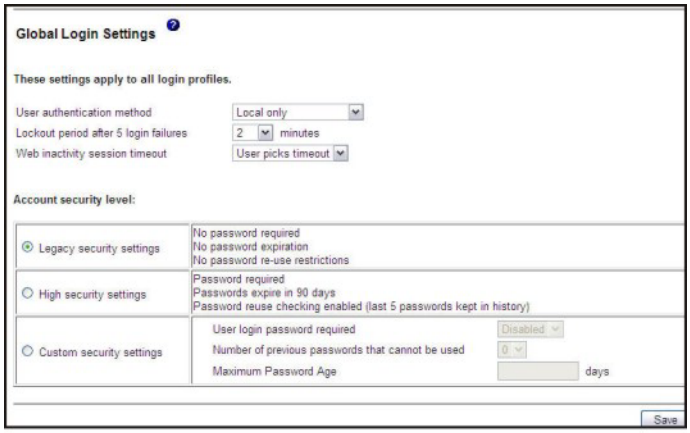
To delete a login profile, complete the following steps:

1. Log in to the IMM for which you want to create a login profile. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Login Profiles**. The Login Profiles page displays each login ID, the login access level, and the password expiration information.
3. Click the login profile that you want to delete. The Login Profile page for that user is displayed
4. Click **Clear Login Profile**.

Configuring the global login settings

Complete the following steps to set conditions that apply to all login profiles for the IMM:

1. Log in to the IMM for which you want to set the global login settings. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Login Profiles**.
3. Scroll down to the **Global Login Settings** area. A page similar to the one in the following illustration is displayed.



4. In the **User authentication method** field, specify how users who are attempting to log in are authenticated. Select one of the following authentication methods:
   - **Local only:** Users are authenticated by a search of a table that is local to the IMM. If there is no match on the user ID and password, access is denied. Users who are successfully authenticated are assigned the authority level that is configured in "Creating a login profile" on page 25.
   - **LDAP only:** The IMM attempts to authenticate the user by using the LDAP server. Local user tables on the IMM are never searched with this authentication method.
   - **Local first, then LDAP:** Local authentication is attempted first. If local authentication fails, LDAP authentication is attempted.
   - **LDAP first, then Local:** LDAP authentication is attempted first. If LDAP authentication fails, local authentication is attempted.

   Note:

a. Only locally administered accounts are shared with the IPMI interface because IPMI does not support LDAP authentication.
b. Even if the **User authentication method** field is set to **LDAP only**, users can log in to the IPMI interface by using the locally administered accounts.

5. In the **Lockout period after 5 login failures** field, specify how long, in minutes, the IMM prohibits remote login attempts if more than five sequential failures to log in remotely are detected. The lockout of one user does not prevent other users from logging in.
6. In the **Web inactivity session timeout** field, specify how long, in minutes, the IMM waits before it disconnects an inactive web session. Select **No timeout** to disable this feature. Select **User picks timeout** if the user will select the timeout period during the login process.
7. (Optional) In the **Account security level** area, select a password security level. The **Legacy security settings** and **High security settings** set the default values as indicated in the requirement list.
8. To customize the security setting, select **Custom security settings** to view and change the account security management configuration.

   User login password required
   Use this field to indicate whether a login ID with no password is allowed.

   Number of previous passwords that cannot be used
   Use this field to indicate 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.

   Maximum Password Age
   Use this field to indicate the maximum password age that is allowed before the password must be changed. Values of 0 - 365 days are supported. Select **0** to disable the password expiration checking.
9. Click **Save**.

Configuring remote alert settings

You can configure remote alert recipients, the number of alert attempts, incidents that trigger remote alerts, and local alerts from the **Alerts** link on the navigation pane.

After you configure a remote alert recipient, the IMM sends an alert to that recipient through a network connection when any event selected from the Monitored Alerts group occurs. The alert contains information about the nature of the event, the time and date of the event, and the name of the system that generated the alert.

Note: If the **SNMP Agent** or **SNMP Traps** fields are not set to **Enabled**, no SNMP traps are sent. For information about these fields, see “Configuring SNMP” on page 42.

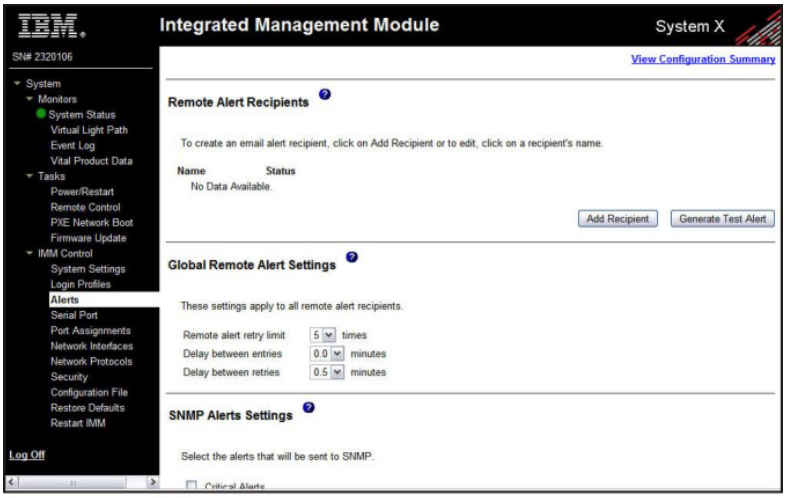
Configuring remote alert recipients

You can define up to 12 unique remote alert recipients. Each link for an alert recipient is labeled with the recipient name and alert status.

Note: If you have not configured an alert recipient profile, the profile does not appear in the remote alert recipients list.

To configure a remote alert recipient, complete the following steps:

1. Log in to the IMM for which you want to configure remote alert settings. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Alerts**. The Remote Alert Recipients page is displayed. You can see the notification method and alert status for each recipient, if they are set.



3. Click one of the remote alert recipient links or click **Add Recipient**. An individual recipient window similar to the one in the following illustration opens.

4. In the **Status** field, click **Enabled** to activate the remote alert recipient.
5. In the **Name** field, type the name of the recipient or other identifier. The name that you type appears as the link for the recipient on the Alerts page.
6. In the **E-mail address** field, enter the alert recipient's e-mail address.
7. Use the check box to include event logs with e-mail alerts.
8. In the **Monitored Alerts** field, select the type of alerts that are sent to the alert recipient. The remote alerts are categorized by the following levels of severity:

   Critical alerts
   Critical alerts are generated for events that signal that a server component is no longer functioning.

   Warning alerts
   Warning alerts are generated for events that might progress to a critical level.

System alerts

System alerts are generated for events that occur as a result of system errors or for events that occur as a result of configuration changes.

All alerts are stored in the event log and sent to all configured remote alert recipients.

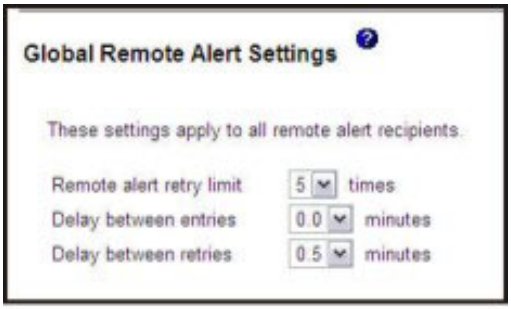
9. Click **Save**.

Configuring global remote alert settings

The global remote alert settings apply only to forwarded alerts.

Complete the following steps to set the number of times that the IMM attempts to send an alert:

1. Log in to the IMM on which you want to set remote alert attempts. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Alerts** and scroll down to the **Global Remote Alert Settings** area.



Use these settings to define the number of remote alert attempts and the length of time between the attempts. The settings apply to all configured remote alert recipients.

Remote alert retry limit

Use the **Remote alert retry limit** field to specify the number of additional times that the IMM attempts to send an alert to a recipient. The IMM does not send multiple alerts; additional alert attempts occur only if there is a failure when the IMM attempts to send the initial alert.

Note: This alert setting does not apply to SNMP alerts.

Delay between entries

Use the **Delay between entries** field to specify the time interval (in minutes) that the IMM waits before sending an alert to the next recipient in the list.

Delay between retries

Use the **Delay between retries** field to specify the time interval (in minutes) that the IMM waits between retries to send an alert to a recipient.

3. Scroll to the bottom of the page and click **Save**.

Configuring SNMP alert settings

The SNMP agent notifies the IMM about events through SNMP traps. You can configure the SNMP to filter the events based on the event type. Event categories that are available for filtering are Critical, Warning and System. The SNMP alert settings are global for all SNMP traps.

Note:

1. The IMM provides two Management Information Base (MIB) files for use with SNMP applications. The MIB files are included in the IMM firmware update packages.
2. IMM supports the SNMPv1 and SNMPv3 standards.

Complete the following steps to select the type or types of alerts that are sent to SNMP:

1. Log in to the IMM on which you want to set remote alert attempts. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Alerts** and scroll down to the **SNMP Alerts Settings** area.
3. Select the type or types of alerts. The remote alerts are categorized by the following levels of severity:
   - Critical
   - Warning
   - System
4. Scroll to the bottom of the page and click **Save**.

Configuring serial port settings

The IMM provides two serial ports that are used for serial redirection.

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

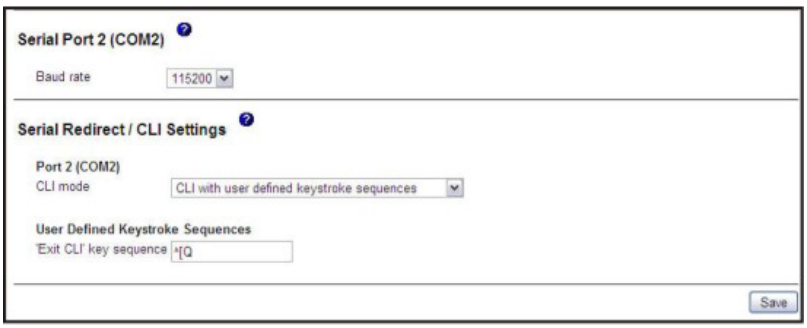
On blade servers, serial port 2 (COM2) is used for SOL. On System x servers, COM2 is used for serial redirection through Telnet or SSH. COM2 is not configurable through the IPMI interface. On rack-mounted and tower servers, COM2 is an internal COM port with no external access.

Both serial ports use 8 data bits, null parity, and 1 stop bit. A baud rate choice of 9600, 19200, 38400, 57600, 115200, and 230400 is available.

You can configure the serial redirection and command-line interface for the COM2 port in the IMM.

To configure the serial data-transfer rate and redirection, complete the following steps:

1. Log in to the IMM on which you want to configure the serial port. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Serial Port**. A page similar to the one in the following illustration is displayed.



3. In the **Baud rate** field, select the data-transfer rate to match the rate of the server COM port that you want to use for serial redirection. Use the **Baud rate** field to specify the data-transfer rate of your serial port connection. To set the baud rate, select the data-transfer rate, in bits per second, that corresponds to your serial port connection.
4. In the **CLI mode** field in the **Serial Redirect/CLI Settings** area, select **CLI with EMS compatible keystroke sequences** if you want to use the Microsoft Windows Server 2003 Emergency Management Services (EMS) compatible key sequence to exit the serial redirection operation, or select **CLI with user defined keystroke sequences** if you want to use your own key sequence.

   Note: If you select **CLI with user defined keystroke sequences**, you must define the key sequence.

   After the serial redirection starts, it continues until the user types the exit key sequence. When the exit key sequence is typed, serial redirection stops and the user is returned to command mode in the Telnet or SSH session. Use this field to specify the exit key sequence.
5. Click **Save**.

Configuring serial-to-Telnet or SSH redirection

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

Example session

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

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

```
ESC Q
```

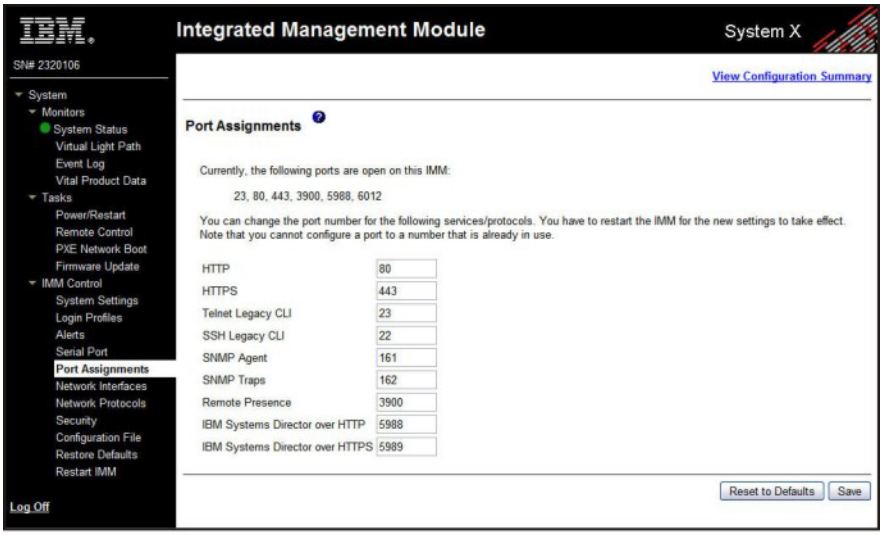
Type the exit key sequence to return to the command-line interface. In this example, press Esc and then type q.

```
Back to LegacyCLI console....
```

Configuring port assignments

To change the port numbers of IMM services, complete the following steps:

1. Log in to the IMM where you want to configure the port assignments. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Port Assignments**. A page similar to the one in the following illustration is displayed.



3. Use the following information to assign values for the fields:

HTTP This is the port number for the HTTP server of the IMM. The default port number is 80. Other valid values are in the range 1 - 65535. If you change this port number, you must add this port number, preceded by a colon, at the end of the web address. For example, if the HTTP port is changed to 8500, type `http://hostname:8500/` to open the IMM web interface. Note that you must type the prefix `http://` before the IP address and port number.

HTTPS
This is the port number that is used for web interface HTTPS (SSL) traffic. The default value is 443. Other valid values are in the range 1 - 65535.

Telnet Legacy CLI
This is the port number for Legacy CLI to log in through the Telnet service. The default value is 23. Other valid values are in the range 1 - 65535.

SSH Legacy CLI
This is the port number that is configured for Legacy CLI to log in through SSH. The default is 22.

SNMP Agent
This is the port number for the SNMP agent that runs on the IMM. The default value is 161. Other valid values are in the range 1 - 65535.

SNMP Traps
This is the port number that is used for SNMP traps. The default value is 162. Other valid values are in the range 1 - 65535.

Remote Presence
This is the port number that the remote control feature uses to view and interact with the server console. The default is 3900 for rack-mounted and tower servers.

Note: The Concurrent Keyboard, Video, and Mouse (cKVM) feature on BladeCenter requires the port number to be 2068. Do not change this port number on a blade server.

IBM Systems Director over HTTP
This is the port number that IBM Systems Director uses to interact with the server console. The default is 5988.

IBM Systems Director over HTTPS
This is the port number that IBM Systems Director uses to interact with the server console through SSL. The default is 5989.

The following port numbers are reserved and can be used only for the corresponding services.

Table 3. Reserved port numbers

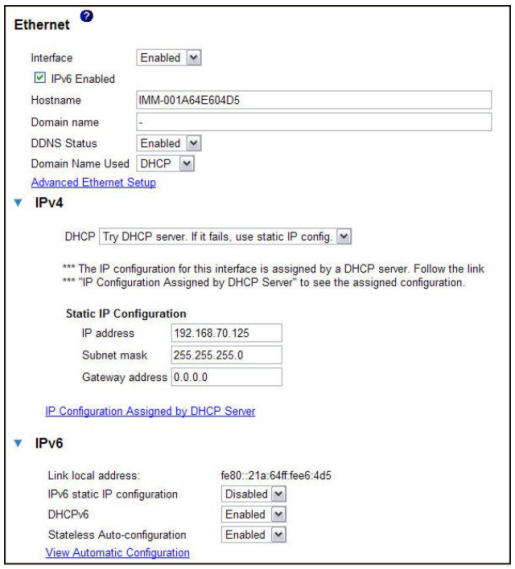
Port number	Services used for
427	SLP
7070 through 7077	Partition management

4. Click **Save**.

Configuring network interfaces

On the Network Interfaces page, you can set access to the IMM by configuring an Ethernet connection to the IMM. To configure the Ethernet setup for the IMM, modify the settings in the Ethernet, IPv4, or IPv6 areas of the Network Interfaces page as necessary. The settings in each area are described in the following sections.

Note: The values in the following image are examples. Your settings will be different.



To see a summary of all current configuration settings, click **View Configuration Summary** on the Network Interfaces page. Before you configure the settings on the Network Interfaces page, review the information in the following sections,

Note: You can also configure the IMM network connection through the Setup utility. For more information, see "Setting up the IMM network connection through the IBM System x Server Firmware Setup utility" on page 11.

Configuring the Ethernet settings

The following settings can be modified in the Ethernet area of the Network Interfaces page.

Interface

Use this field to enable or disable this network interface. To allow network connections through this network interface, select **Enabled**.

IPv6 Enabled

Use this check box to enable or disable IPv6 support on the IMM.

Note: If you clear the **IPv6 Enabled** check box, the **Hide all IPv6 configuration fields when IPv6 is disabled** check box is displayed. If the new check box is selected, the IPv6 area on the Network Interfaces page is hidden on the web interface.

Hostname

Use this field to define a unique hostname for the IMM subsystem. You can type a maximum of 63 characters in this field. The hostname can consist only of alphanumeric characters, hyphens, and underscores.

Note: The hostname by default is `IMM-`, followed by the burned-in MAC address.

Domain name

Use this field to define a DNS domain name.

DDNS Status

Use this field to enable or disable Dynamic DNS (DDNS). DDNS enables IMM to notify a DNS server to change, in real time, the active DNS configuration of its configured hostnames, addresses, or other information

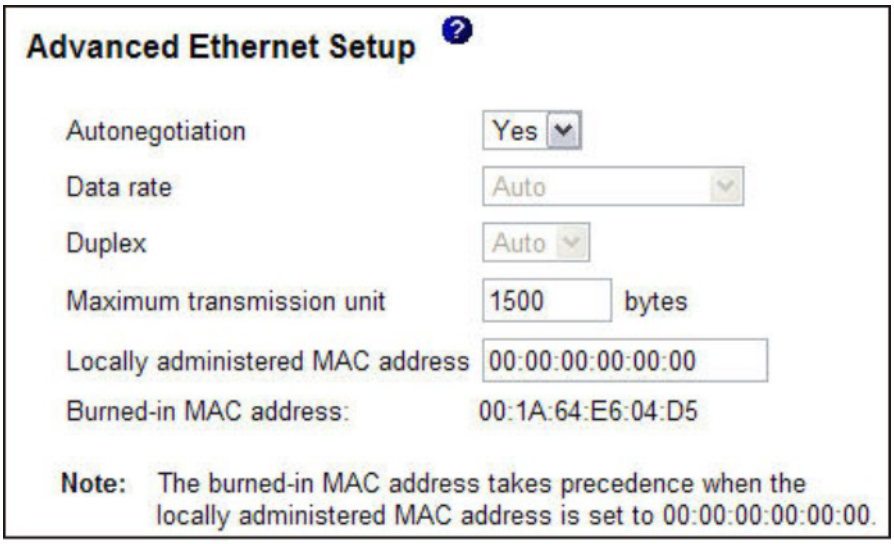
stored in DNS. When DDNS is enabled, IMM notifies the DNS server of the IP address that was received either from a DHCP server or through self-configuration.

Domain Name Used

Use this field to select whether the DHCP- or manually-assigned domain name is sent to the DNS when DDNS is enabled. The value will be set to either DHCP or Manual.

Advanced Interface Setup

Click this link to open the Advanced Interface Setup page, which looks similar to the following image.



From this page, you can view and change additional settings for the interface. The following table describes the settings on the Advanced Ethernet Setup page.

Table 4. Settings on the Advanced Ethernet Setup page

Setting	Function
Autonegotiate	Use this setting to choose whether the Data rate and Duplex network settings are configurable or not. If Autonegotiate is set to **Yes**, the Data rate and Duplex settings are set to **Auto** and are not configurable. If Autonegotiate is set to **No**, the user can configure Data rate and Duplex settings.
Data rate	Use this field to specify the amount of data to be transferred per second over your LAN connection. To set the data rate, select the data transfer rate in Megabits (Mb) that corresponds to your network capability. To detect the data transfer rate automatically, select **Auto**.

Table 4. Settings on the Advanced Ethernet Setup page (continued)

Setting	Function
Duplex	Use this field to specify the type of communication channel that is used in your network. To set the duplex mode, select either **Full** or **Half**. Full duplex allows data to be transferred in both directions at once. A Half-duplex channel allows data to be transferred in one direction or the other, but not both at the same time. To detect the duplex type automatically, select **Auto**.
Maximum transmission unit (MTU)	Use this field to specify the maximum size of a packet (in bytes) for your network interface. To set the MTU value, enter the desired number in the text field. For Ethernet, the valid MTU range is 68 - 1,500.
Locally administered MAC address	Use this field to specify a physical address for this IMM subsystem. If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value between 000000000000 - FFFFFFFFFFFF. This value must be in the form *XX:XX:XX:XX:XX:XX* where *X* is a number between 0 - 9 and A - F. The IMM does not allow use of a multicast address. A multicast address has the least significant bit of the first byte set to 1. Therefore, the first byte must be an even number.
Burned-in MAC address	The burned-in MAC address is a unique physical address assigned to the IMM by the manufacturer.

Configuring the IPv4 settings

The following settings can be modified in the IPv4 area of the Network Interfaces page.

DHCP Use this field to specify whether you want the Ethernet port TCP/IP settings of the IMM subsystem to be set through a Dynamic Host Configuration Protocol (DHCP) server on your network. To use the DHCP configuration, select **Enabled - Obtain IP config. from DHCP server**. To configure your TCP/IP settings manually, select **Disabled - Use static IP configuration**. If you want to try a DHCP server and then revert to the static IP configuration if a DHCP server cannot be reached, select **Try DHCP server. If it fails, use static IP config**.

If the IP configuration is assigned by a DHCP server, click the link **IP Configuration Assigned by DHCP server** to view the configuration details.

Note:

1. There must be an accessible, active, and configured DHCP server on your network if you select the **Enabled - Obtain IP config. from DHCP server** option.

2. The configuration assigned by a DHCP server will override any static IP settings.
3. The **Try DHCP server. If it fails, use static IP config.** option is not supported on all IMMs.

Static IP Configuration

The following fields contain the static IP configuration for this interface. These settings will only be used if DHCP is disabled. If DHCP is enabled, the dynamic IP configuration assigned by the DHCP server will override these static settings.

- **IP address:** Use this field to define the IP address of the IMM subsystem accessed through this network interface. To set the IP address, type the address in the text box. The IP address must contain four integers (from 0 - 255) separated by periods and no spaces.

  Note: The default value for this field is `192.168.70.125`.
- **Subnet mask:** Use this field to define the subnet mask that will be used by the IMM subsystem. To set the subnet mask, type the bit mask in the text box. The subnet mask must contain four integers (from 0 - 255), separated by periods, and no spaces. The bits that are set contiguously starting at the leftmost bit. For example, `0.255.0.0` is not a valid subnet mask. This field can not be set to `0.0.0.0` or `255.255.255.255`.

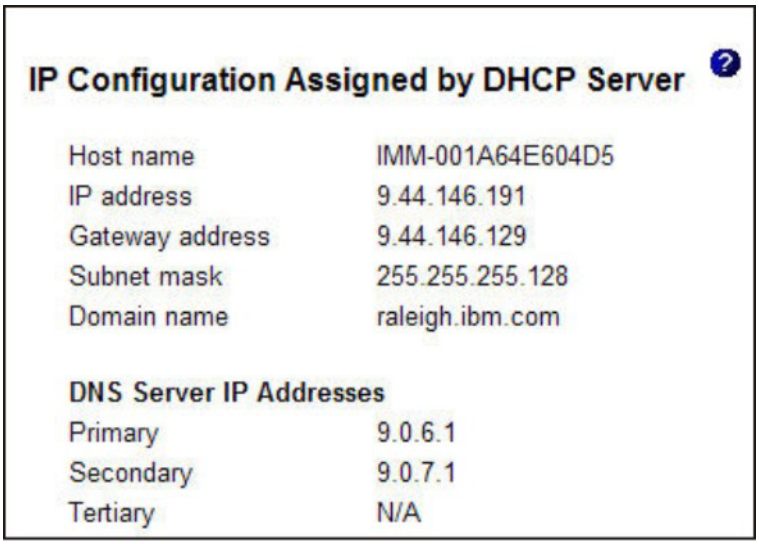
  Note: The default for this field is `255.255.255.0`.
- **Gateway address:** Use this field to identify the IP address of your default gateway. To set the gateway address, type the address in the text box. The gateway address must contain four integers (from 0 - 255) separated by periods, and no spaces or consecutive periods.

  Note: The default for this field is `0.0.0.0`.

IP Configuration Assigned by DHCP Server

Click this link to view the IP configuration assigned by the DHCP server. The IP Configuration Assigned by DHCP Server page, similar to the following image, is displayed.

Note: This option is available only when DHCP is enabled.



Configuring the IPv6 settings

The following settings can be modified in the IPv6 area of the Network Interfaces page.

Note: At least one of the IPv6 configuration options described in this section (IPv6 Static Configuration, DHCPv6, or Stateless Auto-configuration) must be enabled.

Link local address
The link local address is the IPv6 address that is assigned to the IMM. The link local address has a format similar to the following example:

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

IPv6 Static Configuration
Use this field to enable or disable static configuration settings for IPv6. When the **IPv6 Static Configuration** check box is selected, the following choices are available:

- **IP address:** Use this field to define the IPv6 address of the IMM that is accessed through this network interface. To set the IP address, type the IPv6 address in the text box. The value in this field must be a valid IPv6 address.

  Note: The default for this field is `0::0`.
- **Address prefix length (1 - 128):** Use this field to set the prefix length for the static IPv6 address.
- **Default route:** Use this field to set the IPv6 address of your default route. To set the default route, type the IPv6 address in the corresponding box. The value in this field must be a valid IPv6 address.

  Note: The default value for this field is `0::0`.
  .

DHCPv6
Use this field to enable or disable DHCPv6 assigned configuration on the IMM.

Stateless Auto-configuration
Use this field to enable or disable stateless auto-configuration on the IMM.

View Automatic Configuration (link)
To view the IPv6 configuration assigned by the DHCP server, click this link. The IPv6 Automatic Configuration page is displayed.

Configuring network protocols

On the Network Protocols page, you can perform the following functions:

- Configure Simple Network Management Protocol (SNMP)
- Configure Domain Name System (DNS)
- Configure Telnet Protocol
- Configure Simple Mail Transfer Protocol (SMTP)
- Configure Lightweight Directory Access Protocol (LDAP)
- Configure Service Location Protocol (SLP)

Changes to the network protocol settings require that the IMM be restarted for the changes to take effect. If you are changing more than one protocol, you can wait until all of the protocol changes have been made and saved before you restart the IMM.

Configuring SNMP

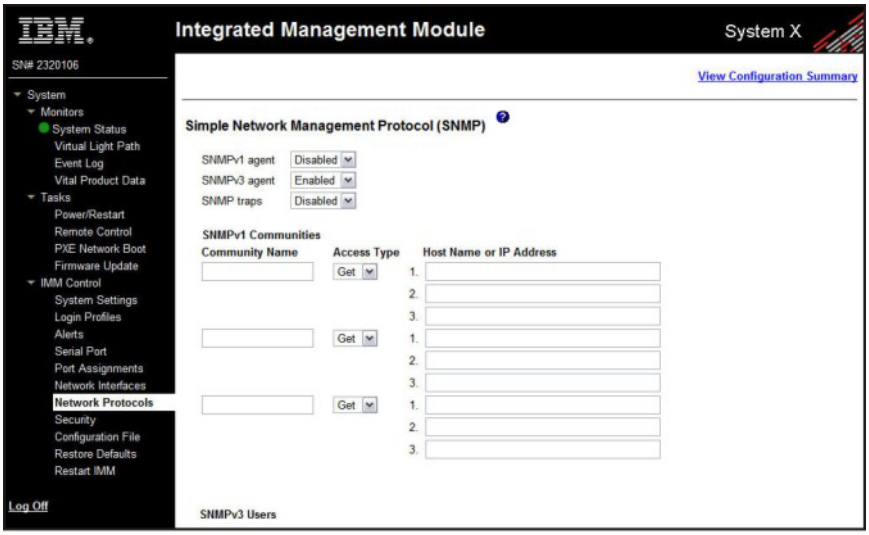
You can use the SNMP agent to collect information and to control the server. The IMM can also be configured to send SNMP alerts to the configured host names or IP addresses.

Note:

1. The IMM provides two Management Information Base (MIB) files for use with SNMP applications. The MIB files are included in the IMM firmware update packages.
2. IMM supports the SNMPv1 and SNMPv3 standards.

To configure SNMP, complete the following steps:

1. Log in to the IMM where you want to configure SNMP. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Network Protocols**. A page similar to the one in the following illustration is displayed.



3. Select **Enabled** in either the **SNMPv1 agent** or the **SNMPv3 agent** field.

   Note: If you enabled the SNMPv3 agent, you must configure SNMPv3 settings for active login profiles for the interaction between the SNMPv3 manager and SNMPv3 agent to work correctly. You can configure these settings at the bottom of the individual login profile settings on the Login Profiles page (see "Creating a login profile" on page 25 for more information). Click the link for the login profile to configure, scroll to the bottom of the page and then click the **Configure SNMPv3 User** check box.
4. Select **Enabled** in the **SNMP traps** field to forward alerts to SNMP communities on your network. To enable the SNMP agent, the following criteria must be met:

- A system contact must be specified on the System Settings page. For information about the System Settings page settings, see "Setting system information" on page 20.
- System location must be specified on the System Settings page.
- At least one community name must be specified.
- At least one valid IP address or host name (if DNS is enabled) must be specified for that community.

Note: Alert recipients whose notification method is SNMP cannot receive alerts unless the **SNMPv1 agent** or **SNMPv3 agent** and the **SNMP traps** fields are set to **Enabled**.

5. Set up a community to define the administrative relationship between SNMP agents and SNMP managers. You must define at least one community. Each community definition consists of the following parameters:
   - Community Name
   - Access Type
   - IP address

   If any of these parameters is not correct, SNMP management access is not granted.

   Note: If an error message window opens, make the necessary adjustments to the fields that are listed in the error window. Then, scroll to the bottom of the page and click **Save** to save your corrected information. You must configure at least one community to enable this SNMP agent.
6. In the **Community Name** field, enter a name or authentication string to specify the community.
7. 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 MIB objects; select **Set** to allow all hosts in the community to receive traps, query, and set MIB objects.
8. In the corresponding **Host Name or IP Address** field, enter the host name or IP address of each community manager.
9. Scroll to the bottom of the page and click **Save**.
10. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring DNS

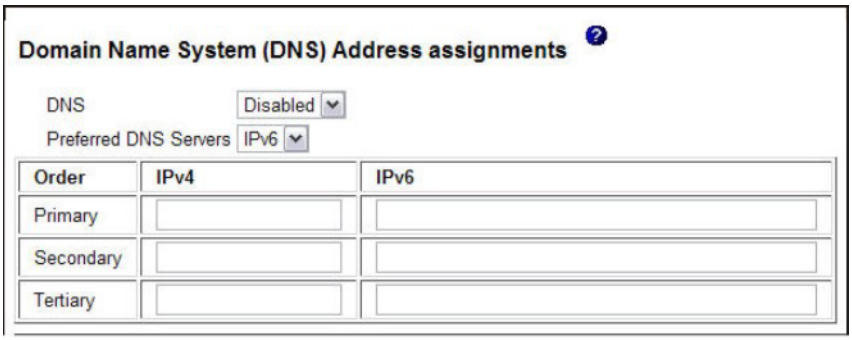
You can configure the Domain Name System (DNS) settings to specify whether additional DNS server addresses should be included in the search order for hostname-to-IP address resolution. DNS lookup is always enabled, and other DNS addresses might be automatically assigned by the DHCP server when DHCP functionality is enabled.

For the additional DNS addresses to be enabled, at least one of them must be a value other than zero. The additional DNS servers are added to the top of the search list, so that the hostname lookup is done on these servers before it occurs on a DNS server that is assigned automatically by a DHCP sever.

To configure the DNS, complete the following steps:

1. Log in to the IMM where you want to configure DNS. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.

2. In the navigation pane, click **Network Protocols** and scroll down to the **Domain Name System (DNS) Address assignments** area of the page. A section of the page similar to the one in the following illustration is displayed.



3. If a DNS server (or servers) is available on your network, select **Enabled** in the **DNS** field. The **DNS** field specifies whether you use a DNS server on your network to translate host names into IP addresses.
4. If you have IPv4 and IPv6 DNS server addresses, select either **IPv4** or **IPv6** in the **Preferred DNS Servers** list to specify which server addresses are preferred.
5. If you enabled DNS, use the Primary, Secondary, and Tertiary text fields to specify the IP addresses of up to six DNS servers on your network. To set the three IPv4 or three IPv6 DNS server addresses, type the addresses in the applicable text fields. Make sure that the IPv4 or IPv6 addresses are in valid formats.
6. Scroll to the bottom of the page and click **Save**.
7. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring Telnet

To configure Telnet, complete the following steps:

1. Log in to the IMM where you want to configure Telnet. For more information, see Chapter 2, “Opening and using the IMM web interface,” on page 11.
2. In the navigation pane, click **Network Protocols** and scroll down to the **Telnet Protocol** area of the page. You can set the maximum number of concurrent Telnet users, or you can disable Telnet access.
3. Scroll to the bottom of the page and click **Save**.
4. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring SMTP

To specify the IP address or host name of the Simple Mail Transfer Protocol (SMTP) server, complete the following steps.

1. Log in to the IMM where you want to configure SMTP. For more information, see Chapter 2, “Opening and using the IMM web interface,” on page 11.
2. In the navigation pane, click **Network Protocols** and scroll down to the **SMTP** area of the page.
3. In the **SMTP Server Host Name or IP address** field, 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.
4. Scroll to the bottom of the page and click **Save**.
5. In the navigation pane, click **Restart IMM** to activate the changes.

Configuring LDAP

Using a Lightweight Directory Access Protocol (LDAP) server, the IMM can authenticate a user by querying or searching an LDAP directory on an LDAP server, instead of going through its local user database. Then, the IMM can remotely authenticate any user access through a central LDAP server. This requires LDAP client support on the IMM. You can also assign authority levels according to information that is found on the LDAP server.

You can also use LDAP to assign users and IMMs to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, an IMM can be associated with one or more groups, and a user would pass group authentication only if the user belongs to at least one group that is associated with the IMM.

Information about configuring the following two LDAP servers is provided in this section:

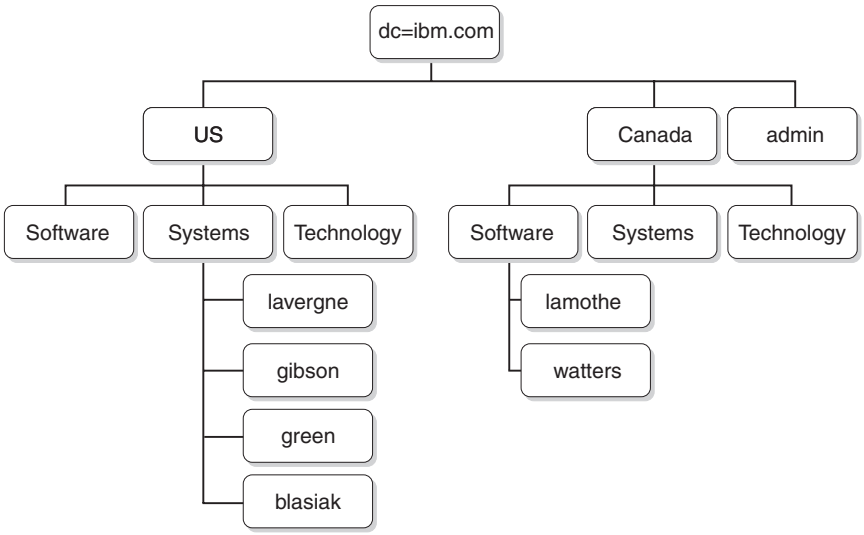
- Novell eDirectory version 8.7.1
- Microsoft Windows Server 2003 Active Directory

User schema example

A simple user schema example is described in this section. This schema example is used throughout the document to illustrate the configuration on both the LDAP client and the LDAP server.

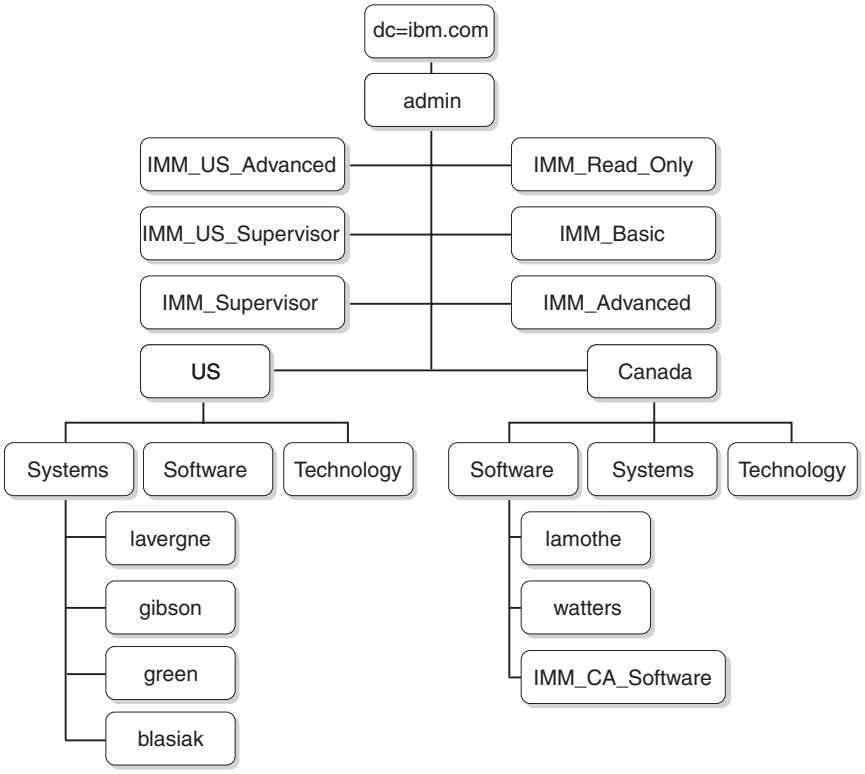
The user schema example is rooted at a domain component called ibm.com. That is, every object in this tree has a root distinguished name equal to dc=ibm,dc=com. Now assume that this tree represents a company that wants to classify users and user groups based on their country and organization. The hierarchy is root → country → organization → people.

The following illustration shows a simplified view of the schema used in this document. Note the use of a user account (userid=admin) directly below the root. This is the administrator.



The following illustration shows the addition of user groups. Six user groups are defined and added to the first level, and another user group is added to the

Software organization in the country Canada.



The users and associated user groups in Table 5 are used to complete the schema.

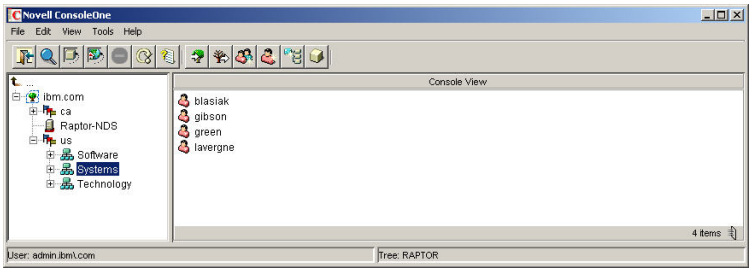
Table 5. User to Group mapping

User distinguished name	**Group membership**
cn=lavergne, o=Systems, c=us, dc=ibm.com	cn=IMM_Supervisor, dc=ibm.com cn=IMM_US_Supervisor, dc=ibm.com
cn=blasiak, o=Systems, c=us, dc=ibm.com	cn=IMM_US_Advanced, dc=ibm.com
cn=gibson, o=Systems, c=us, dc=ibm.com	cn=IMM_Basic, dc=ibm.com
cn=green, o=Systems, c=us, dc=ibm.com	cn=IMM_Read_Only, dc=ibm.com
cn=watters, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com
cn=lamothe, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com

Novell eDirectory schema view

Using the Novell ConsoleOne tool, the schema described in “User schema example” on page 45 was pulled into a Novell eDirectory. The following illustration shows the top level view of the schema, as seen through the ConsoleOne tool.

The following illustration captures the users under o=Systems, c=us, dc=ibm.com.



Group membership

Novell eDirectory uses an attribute called **GroupMembership** to identify the groups to which a user is a member. The User object class specifically uses this attribute. The LDAP client uses a default value of **memberOf** in its search request to the LDAP server when querying the groups to which a user is a member.

You can configure the LDAP client for membership queries using one of the following methods:

- Configure the value **GroupMembership** in the **Group Search Attribute** field on the LDAP client.
- Create an attribute mapping between **GroupMembership** and **memberOf** on the Novell eDirectory LDAP server.

Complete the following steps to configure the default attribute on the LDAP client:

1. In the IMM web interface, in the left navigation pane, click **Network Protocols**.
2. Scroll to the **LDAP Search Attributes** area.
3. In the **Group Search Attribute** field, type the default attribute that you want.

If the **Group Search Attribute** field is blank, it will default to **memberOf** and you will have to configure the Novell eDirectory server to map the attribute **GroupMembership** to **memberOf**. Complete the following steps to configure the Novell eDirectory server to map the attribute **GroupMembership** to **memberOf**.

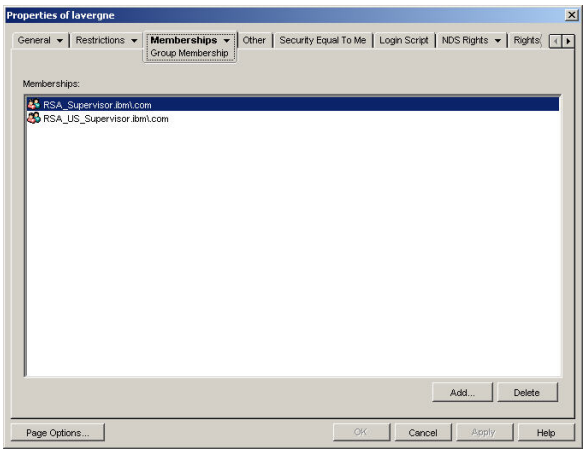
1. Using ConsoleOne tool, right-click the **LDAP Group** icon and click **Properties**. The Properties of LDAP Group window opens.
2. Click the **Attribute Mappings** tab.
3. Click **Add** and then create a mapping between **Group Membership** and **memberOf**.
4. Click **OK**. A page that shows the properties of the LDAP group opens.

Adding users to user groups

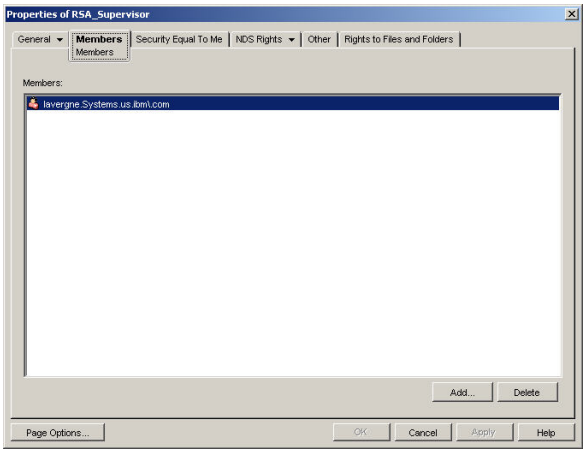
You can add users to the appropriate user groups either by adding the groups to the profile of a user, or adding users to the profile of a group. The end result is identical.

For example, in the previous user schema example, user lavergne is a member of both IMM_US_Supervisor and IMM_Supervisor. Using a browser tool such as Novell ConsoleOne, you can verify the schema (double-click **user lavergne** and select the **Memberships** tab.

A page similar to the one in the following illustration opens.



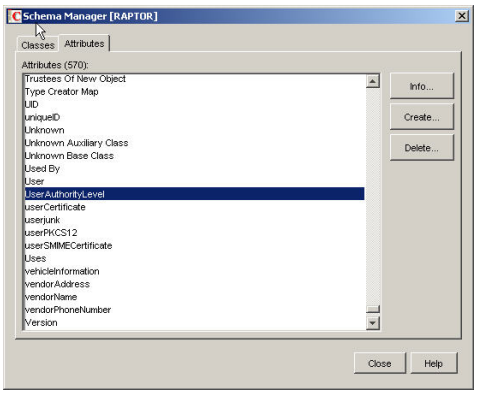
Similarly, if the properties of the IMM_Supervisor group are displayed, and you select the **Members** tab, a page similar to the one in the following illustration opens.



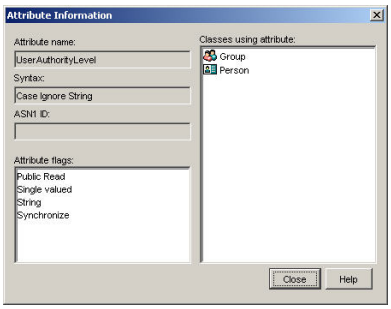
Authority levels

To use the authority levels feature, use ConsoleOne to create a new attribute labeled `UserAuthorityLevel` on the Novell eDirectory. This new attribute will be used to support authority levels..

1. In the Novell ConsoleOne tool, click **Tools** > **Schema Manager**.
2. Click the **Attributes** tab, and click **Create**.
3. Label the attribute **UserAuthorityLevel**. Leave **ASN1 ID** blank or see your LDAP administrator to determine the value to use. Click **Next**.
4. Set the syntax to **Case Ignore String**. Click **Next**.
5. Set the flags as applicable. See your LDAP administrator to make sure these are set correctly. Click the **Public Read** check box; then, click **Next**.
6. Click **Finish**. A page similar to the one in the following illustration opens.



7. Return to the Schema Manager window and click the **Classes** tab.
8. Click the **Person** class and click **Add**. Note that you can use the User object class instead.
9. Scroll down to the **UserAuthorityLevel** attribute, select it, and add it to the attributes for this class. Click **OK**.
10. Click the **Group** class and click **Add**.
11. Scroll down to the **UserAuthorityLevel** attribute, select it, and add it to the attributes for this class. Click **OK**.
12. To verify that the attribute was successfully added to the class, in the Schema Manager window, select the **Attributes** class.
13. Scroll to the **UserAuthorityLevel** attribute; then, click **Info**. A page similar to the one in the following illustration opens.



Setting authority levels

This section explains how to interpret and use the UserAuthorityLevel attribute. The value assigned to the UserAuthorityLevel attribute determines the permissions (or authority levels) assigned to a user after a successful authentication.

The UserAuthorityLevel attribute is read as a bit-string or 0s and 1s. The bits are numbered from left to right. The first bit is bit position 0. The second bit is bit position 1, and so on.

The following table provides an explanation of each bit position.

Table 6. Permission bits

Bit position	Function	Explanation
0	Deny Always	If set, 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	If set, 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	If set, a user has read-only access, and cannot perform any maintenance procedures (for example, restart, remote actions, or firmware updates). Nothing can be modified, using save, clear, or restore functions. Bit position 2 and all other bits are mutually exclusive, with bit position 2 having the lowest precedence. If any other bit is set, this bit will be ignored.
3	Networking & Security	If set, a user can modify the configuration in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port panels.
4	User Account Management	If set, a user can add, modify, or delete users and change the Global Login Settings in the Login Profiles panel.
5	Remote Console Access	If set, a user can access the remote server console and can modify the configuration in the Serial Port panel.
6	Remote Console and Remote Disk Access	If set, a user can access the remote server console and the remote disk functions for the remote server. The user can also modify the configuration in the Serial Port panel.
7	Remote Server Power/Restart Access	If set, a user can access the power on, restart and server timeout functions for the remote server.
8	Basic Adapter Configuration	If set, a user can modify configuration parameters in the System Settings and Alerts panels (excludes Contact, Location and Server Timeout parameters).
9	Ability to Clear Event Logs	If set, a user can clear the event logs. **Note:** All users can view the event logs; but, the user is required to have this level of permission to clear the logs.

Table 6. Permission bits (continued)

Bit position	Function	Explanation
10	Advanced Adapter Configuration	If set, a user has no restrictions when configuring the adapter and the user has administrative access to the IMM. The user can perform the following advanced functions: firmware upgrades, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart/reset the adapter. This excludes Server Power/Restart Control and timeout functions.
11	Reserved	This bit position is reserved for future use (currently ignored).

Notes:

- If bits are not used, the default will be set to Read Only for the user.
- Priority is given to login permissions retrieved directly from the user record. If the user record does not contain a name in the **Login Permission Attribute** field, an attempt will be made to retrieve the permissions from the group that the user belongs to and that match the group filter. In this case the user is assigned the inclusive OR of all the bits for all groups.
- If the Deny Always (bit position zero) bit is set for any of the groups, the user will be refused access. The Deny Always bit has precedence over all bits.
- If a user has the ability to modify basic, networking, or security related adapter configuration parameters, you should consider giving that user the ability to restart the IMM (bit position ten). Without this ability, a user might be able to change a parameter; but, the parameter will not take affect.

The following table contains examples and their descriptions:

Table 7. Example UserLevelAuthority attributes and descriptions

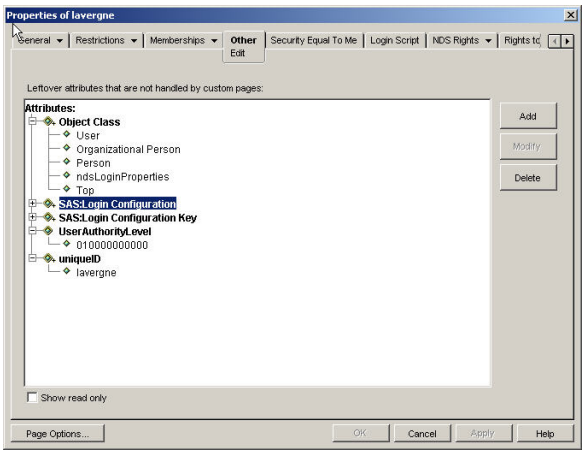
UserLevelAuthority attribute example	Description
IBMRBSPermissions=010000000000	Supervisor Access (bit position 1 is set)
IBMRBSPermissions=001000000000	Read-Only Access (bit position 2 is set)
IBMRBSPermissions=100000000000	No Access (bit position 0 is set)
IBMRBSPermissions=000011111100	All authorities except Advanced Adapter Configuration
IBMRBSPermissions=000011011110	All authorities except access to virtual media

Complete the following steps to add the UserAuthorityLevel attribute to user *lavergne*, and to each of the user groups:

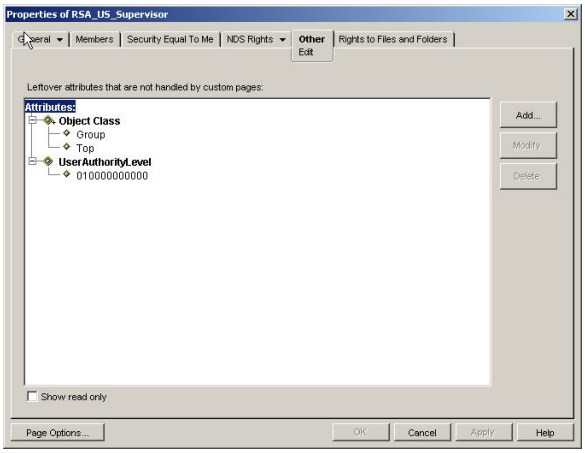
1. Right-click user **lavergne** and click **Properties**.
2. Click the **Other** tab. Click **Add**.
3. Scroll down to the **UserAuthorityAttribute** and click **OK**.
4. Fill in the value that you want for the attribute. For example, if you want to assign Supervisor access, set the attribute to **IBMRBSPermissions=010000000000**. Click **OK**.

5. Repeat steps 1 through 4 for each user group and set the **UserAuthorityLevel** as appropriate.

   The following illustration shows the properties of user *lavergne*.



   The following illustration shows the properties of IMM_US_Supervisor.



   The following table shows the **UserAuthorityLevel** assigned to each of the user groups in the user schema example.

Table 8. UserAuthorityLevel assignments to user groups

User group	UserAuthorityLevel	Translation
IMM_Basic	IBMRBSPermissions=000100000000	Networking and security
IMM_CA_Software	IBMRBSPermissions=000101111010	Networking and security Remote console and virtual media access Remote server power and restart access Basic adapter configuration Advanced adapter configuration
IMM_Advanced	IBMRBSPermissions=000110111100	Networking and security Remote console and virtual media access Remote server power and restart access Basic adapter configuration Advanced adapter configuration Ability to clear event logs

Table 8. UserAuthorityLevel assignments to user groups (continued)

User group	UserAuthorityLevel	Translation
IMM_Supervisor	IBMRBSPermissions=010000000000	Supervisor access
IMM_Read_Only	IBMRBSPermissions=001000000000	Read-only access
IMM_US_Advanced	IBMRBSPermissions=000110111100	Networking and security User account management Remote console and virtual media access Remote server power and restart access Basic adapter configuration Ability to clear event logs
IMM_US_Supervisor	IBMRBSPermissions=010000000000	Supervisor access

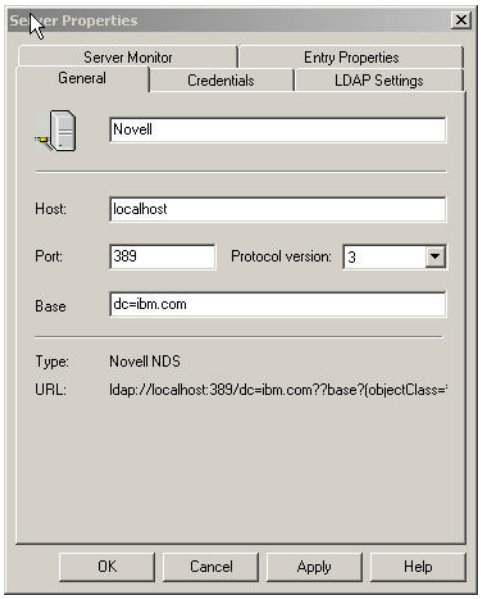
Browsing the LDAP server

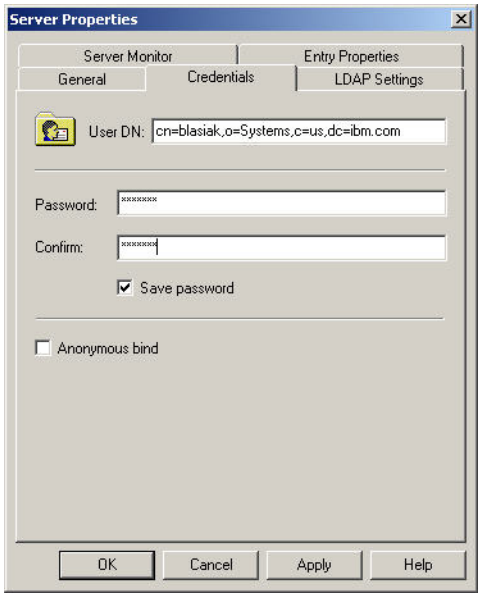
Before you attempt to connect from the LDAP client on the IMM to your LDAP server, connect to your LDAP server using a third-party LDAP browser of your choice. For example, there is a directory browsing tool available from http://www.ldapbrowser.com.

Using the LDAP browser before attempting to use the IMM LDAP client has the following advantages:

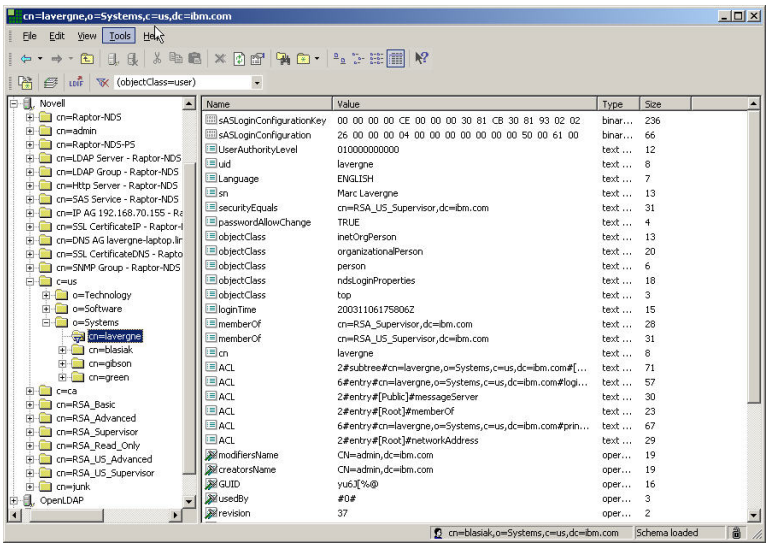
- The ability to bind to a server using various credentials. This will show whether the user accounts on the LDAP server are set up correctly. If you can bind to the server using the browser, but cannot bind to the server using the IMM LDAP client, the LDAP client is configured incorrectly. If you cannot bind using the browser, you will not be able to bind with the LDAP client on the IMM.
- After you successfully bind to the server, you can navigate through the LDAP server database and quickly issue search queries. This will confirm whether the LDAP server is configured the way you want it, with respect to access to the various objects. For example, you might find that you cannot view a particular attribute or you might not see all of the objects you were expecting to see under a specific search request. This indicates that the permissions assigned to the objects (for example, what is publicly visible or what is hidden) are not configured correctly. Contact the LDAP server administrator to correct the problem. It is important to note that the credentials you use to bind determine what privileges you will have on the server.
- Verify the group membership for all users. Verify the **UserAuthorityLevel** attribute assigned to users and user groups.

The following illustrations show various queries and search results made to a Novell eDirectory server configured with the “User schema example” on page 45. In this case, the Softerra LDAP browser tool was used. The initial bind to the server was made with the properties and credentials that are shown in the illustration.

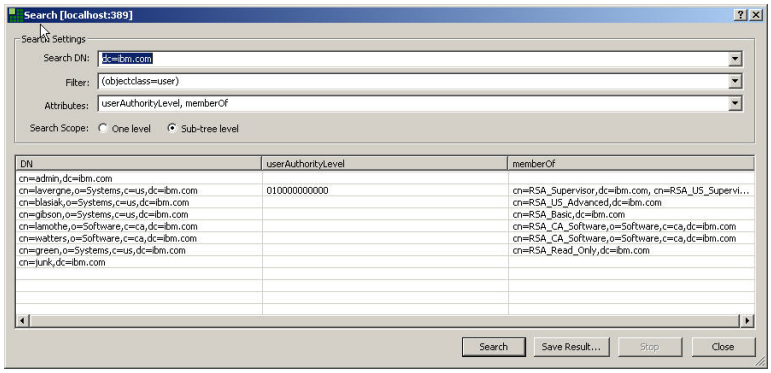




After the initial bind succeeds, the following view of the schema on the Novell eDirectory is displayed.



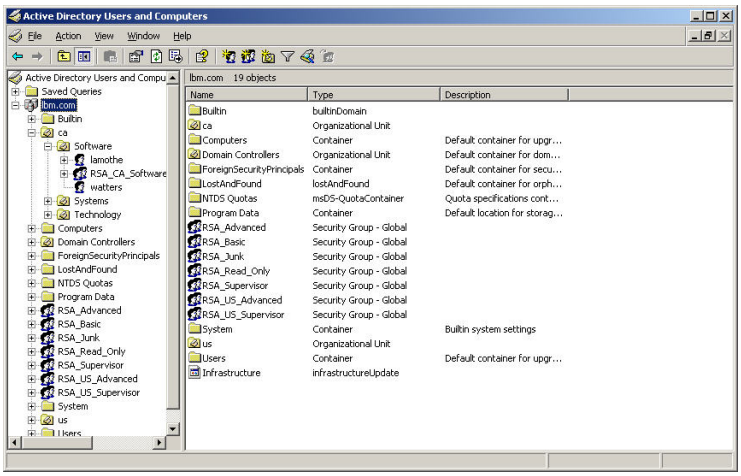
The following illustration shows a query of all users, with a request to retrieve the **userAuthorityLevel** and **memberOf** attributes.



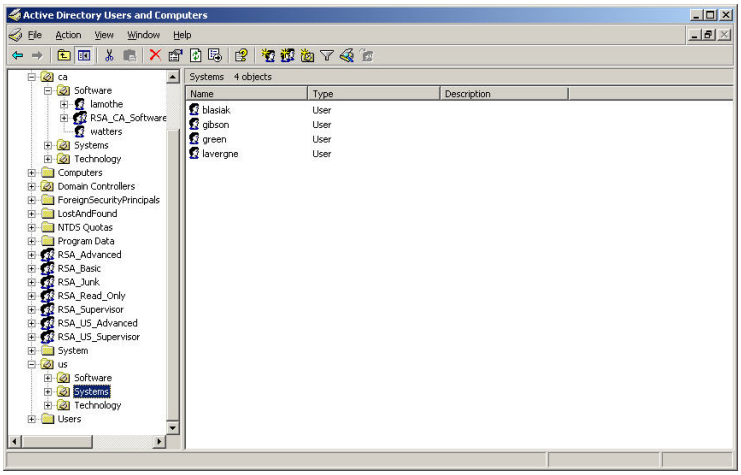
Microsoft Windows Server 2003 Active Directory schema view

This section describes some of the configuration aspects relating to capturing the information in the “User schema example” on page 45 on Microsoft Windows Server 2003 Active Directory.

The following illustration shows the top level view of the schema, as seen through the Active Directory Users and Computers management tool.



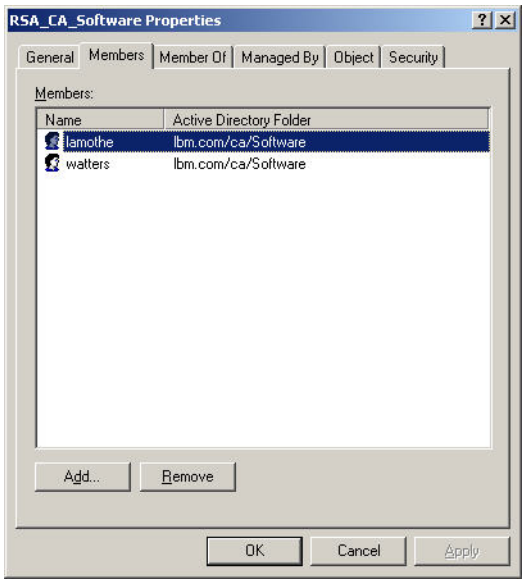
The following illustration shows the users under ou=Systems, ou=us, dc=ibm, dc=com.



Adding users to user groups

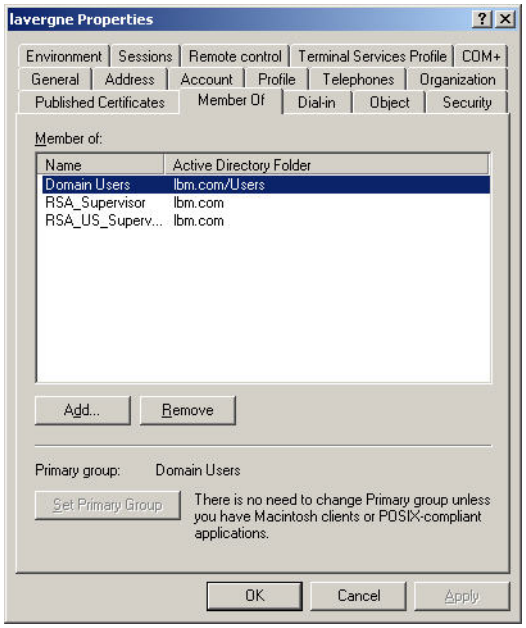
In Active Directory, you can either add groups to a specific user, or add users to a specific group. Right-click the user or user group object; then, click **Properties**.

If you select a user group and then click the **Members** tab, a page similar to the one in the following illustration opens.



To add or delete users from the user group, click **Add** or **Remove**.

If you select a user, and then click the **MembersOf** tab, a page similar to the one in the following illustration opens.



To add or delete users from the user group, click **Add** or **Remove**.

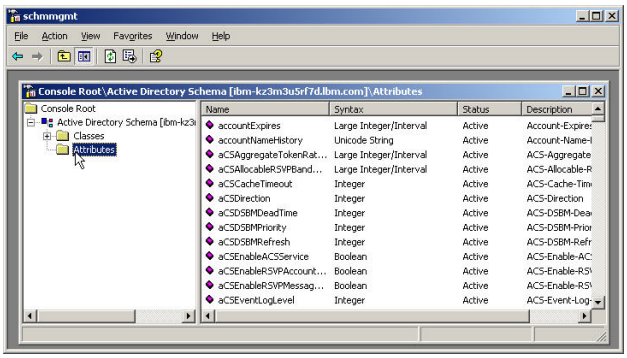
Authority levels

The section "Authority levels" on page 48 describes how to create a new attribute with the Novell eDirectory server to support the concept of authority levels, and how they are assigned to users who authenticate to an LDAP server from an IMM. The attribute created was called **UserAuthorityLevel**. In this section, you will create this attribute on Active Directory.

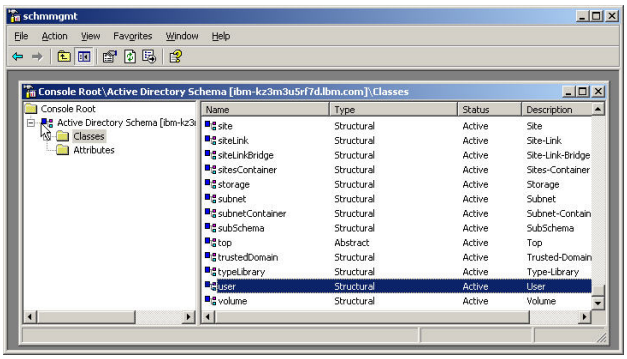
1. Install the Active Directory Schema Snap-In tool. For more information, see the documentation that comes with Active Directory.
2. Start the Active Directory Schema.
3. Click **Action** > **Create Attribute**. Complete the following fields:

a. Set Common Name to **UserAuthorityLevel**
b. Set Syntax to **Case Insensitive String**
c. Set Minimum and Maximum to **12**

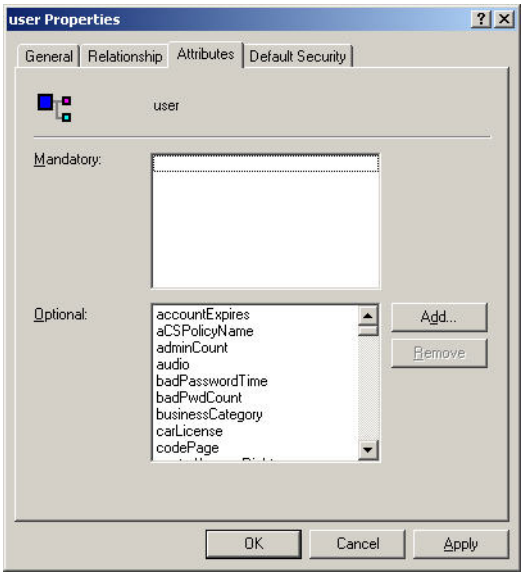
4. Contact your system administrator to assign a new X.500 OID. If you do not want to define a new X.500 OID, use an existing attribute instead of creating a new attribute for the authority level.



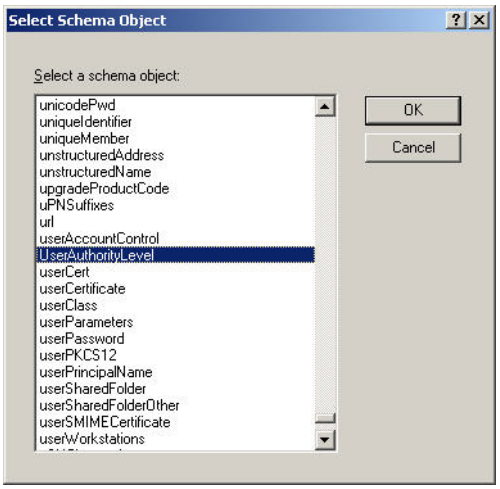
5. After the attribute is saved, select the **Classes** folder.



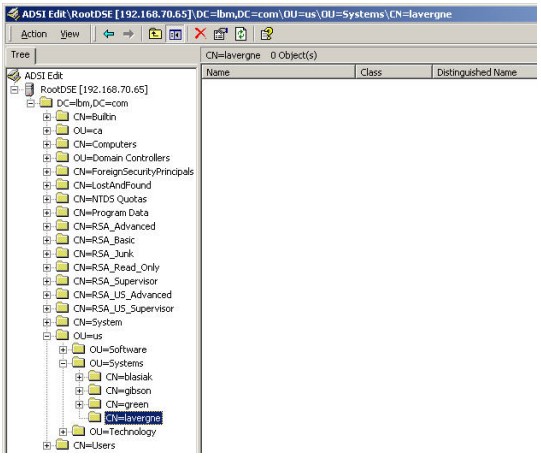
6. Double-click the class **user**. The user Properties window opens.



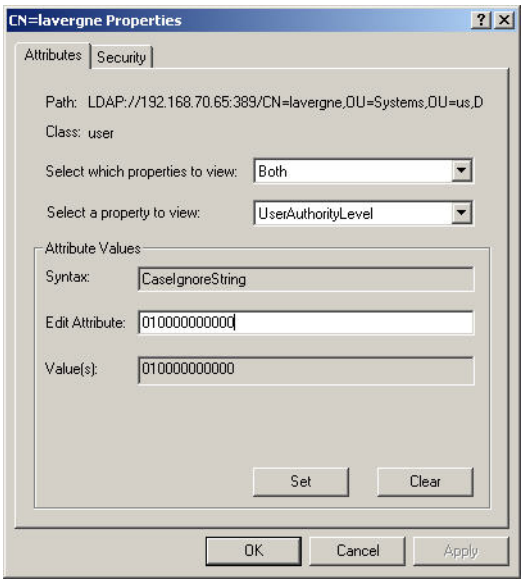
7. Select the **Attributes** tab and then click **Add**. The Select Schema Object window opens.



8. Scroll down to **UserAuthorityLevel** and click **OK**. This attribute will now appear in the list of optional attributes for the user object class.
9. Repeat step 6 on page 58 through step 8 for the class groups. This enables the **UserAuthorityLevel** attribute to be assigned to a user or a user group. These are the only two object classes that need to use this new attribute.
10. Assign the **UserAuthorityLevel** attribute to the appropriate users and user groups. To match the schema defined under the Novell eDirectory server, use the same values as in "Setting authority levels" on page 49. You can use the ADSI Edit tool to do this. The Microsoft ADSI Edit support tool is a Microsoft Management Console (MMC) snap-in used to view all objects in the directory (including schema and configuration information), modify objects, and set access control lists on objects.
11. For this example, assume that you want to add the **UserAuthorityLevel** attribute to user lavergne. Use ADSI Edit to do this. You must supply the appropriate credentials to connect to Active Directory; otherwise, you might not have the proper user privileges to modify objects on the server. The following illustration shows the schema, as seen by ADSI, after connecting to the server.



12. Right-click **lavergne** and click **Properties**. A window similar to the one in the following illustration opens.



13. In the **Select which properties to view** field, select **UserAuthorityLevel**.
14. In the **Edit Attribute** field, type `IBMRBSPermissions=010000000000`, which translates to Supervisor Access. Click **Set**.
15. Click **OK**.
16. You can add this attribute to user groups by following the same steps for the user group object that you want to modify.

Checking Active Directory configuration

Before you attempt to connect the LDAP client to the Active Directory (to authenticate users), browse the Active Directory schema with an LDAP browser. At a minimum, issue the queries listed in the following table to check authority levels and group membership.

Table 9. Checking authority levels and group membership

Search distinguished name	Filter	Attributes
DC=ibm, DC=com	(objectclass=user)	memberOf, userAuthorityLevel
DC=ibm, DC=com	(objectclass=group)	member, userAuthorityLevel

Configuring the LDAP client

You can configure the LDAP to authenticate management module users. The IMM supports both local and remote user authentication. Local authentication uses information provided in the Login Profiles page to authenticate users. Using an LDAP server, a management module can authenticate a user by querying or searching an LDAP directory on a remote LDAP server, instead of going through its local user database.

When any type of remote authentication is used, you can choose to have the permissions for each successfully authenticated user authorized either locally or based on information stored on the LDAP server used for remote authentication. The permissions that are authorized for a user specify the actions that each user can perform while logged in to the IMM. Remote authentication methods are described in the following topics:

- Active directory authentication with local authorization

- Active directory role-based authentication and authorization
- Legacy LDAP authentication and authorization

Active directory authentication with local authorization

You can set up remote LDAP authentication for users, with local user authorization, using Active Directory authentication.

Note: Active Directory authentication with local authorization applies only to a server used in an Active Directory environment.

When using Active Directory authentication with local authorization, the Active Directory servers are used only to authenticate users verifying the credentials for a user. There is no authorization information stored on the Active Directory server for a given user; the IMM stored group profiles must be configured with authorization information. Authorization information used to configure the group profiles can be obtained by retrieving membership information for a user from the Active Directory server. This membership information gives the list of groups that a user belongs to (nested groups are supported). The groups specified on the Active Directory server are then compared to the group names locally configured on the IMM. For each group that the user is a member, the user is assigned permissions from that group. For each group name that is locally configured on the IMM, there is a corresponding authorization profile that is also configured for that group.

The IMM supports up to 16 locally configured group names. Each group name is limited in length to 63 characters. One of the following attributes must be configured as the group name in order to match the group membership information retrieved from the Active Directory servers:

- Distinguished name (DN)
- "cn" attribute
- "name" attribute
- "sAMAccountName" attribute

To configure Active Directory authentication with local authorization for the IMM, complete the following steps:

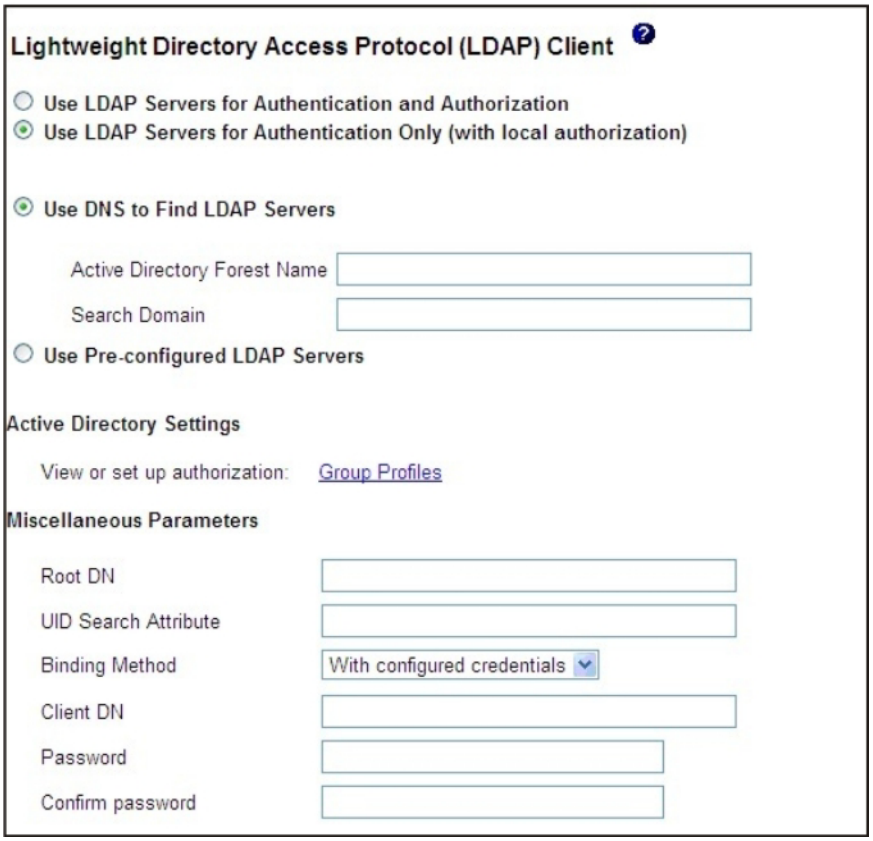
1. In the navigation pane, click **Network Protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** section.
3. Select **Use LDAP Servers for Authentication Only (with local authorization)**.
4. Select one of the following choices, to manually configure or dynamically discover the domain controllers:
   - Select **Use DNS to find LDAP Servers** to dynamically discover the domain controllers based on DNS SVR records.
   - Select **Use Pre-Configured LDAP Servers** (default selection) to manually configure the domain controllers.
5. If you are using DNS to dynamically discover the domain controllers, configure the following settings; then, proceed to step 7 on page 62.

   Note: If using DNS to dynamically discover the domain controller, you must specify the fully qualified domain name of the domain controller.

   - Search Domain
     - Enter the domain name of the domain controller in the **Search Domain** field.

- Active Directory Forest Name
  - This optional field is used to discover global catalogs. Global catalogs are required for users who belong to universal groups in cross-domains. In environments where cross-domain group membership does not apply, this field can be left blank.

The following illustration shows the LDAP Client window when using DNS to dynamically discover the domain controllers.



6. If manually configuring the domain controllers and global catalogs, use the **Use Pre-Configured LDAP Servers** (default) selection; then, configure the **LDAP Server Host Name or IP Address** and **Port** fields.

   Up to four domain controllers can be configured using an IP address or a fully qualified hostname. Global catalog servers are identified using port numbers 3268 or 3269. The use of any other port number indicates that a domain controller is being configured.
7. If you are using group authorization profiles, click **Group Profiles** in the Active Directory Settings section to view or configure them, (see "Group profiles for active directory users" on page 64 for additional information).
8. Return to the Network Protocols page. Click the **LDAP Client section of the Network Protocols page** link that is on the Group Profiles for Active Directory Users page; then, scroll to the **Lightweight Directory Access Protocol (LDAP) Client** section.
9. Configure the Miscellaneous Parameters for the IMM. Refer to the following table for information about the parameters.

Table 10. Miscellaneous parameters

Field	Description	Option
Root DN	The IMM uses the **Root DN** field in DN format as the root entry of the directory tree. This DN will be used as the base object for all searches. An example might look like `dc=mycompany,dc=com`.	
Binding method	The **Binding Method** field is used for initial binds to the domain controller server, select one option.	• With configured credentials: Enter the client DN and Password to be used for the initial bind. If this bind fails, the authentication process also fails. If the bind is successful, a search will attempt to find a user record that matches the client DN entered in the **Client DN** field. The search typically looks for common attributes that match the userid presented during the login process. These attributes include displayName, sAMAccountName, and userPrincipalName. If the **UID search attribute** field is configured, the search also includes this attribute. If the search is successful, a second bind is attempted, this time with the user DN (retrieved from the search) and the password presented during the login process. If the second bind attempt succeeds, the authentication portion succeeds and group membership information for the user is retrieved and matched against the locally configured groups on the IMM. The matched groups will define the authorization permissions assigned to the user. • With login credentials: The initial bind to the domain controller server is made using the credentials presented during the login process. If this bind fails, the authentication process also fails. If the bind is successful, a search will attempt to find the user record. Once located, group membership information for the user is retrieved and matched against the locally configured groups on the IMM. The matched groups will define the authorization permissions assigned to the user. • Anonymously: The initial bind to the domain controller server will be made without a DN or password. This option is discouraged since most servers are configured to disallow search requests on specific user records.

Group profiles for active directory users

Group profiles are configured to provide local authorization specifications for groups of users. Each group profile includes authorization expressed as Authority Level (Roles), exactly the same as in login profiles. To configure group profiles, users must have user account management authorization. To associate users with group profiles, LDAP authentication servers are required.

Group profiles list

The group profiles list is accessed by clicking **IMM Control** > **Login Profiles**. The group ID and role summary is displayed for each group profile (as with login profiles). From this list, new groups can be added, and existing groups can be selected for edit or to be deleted.

The following illustration shows the Group Profiles for Active Directory Users window.

To edit a group profile, click **Edit**. A Group Profile page is opened for that group. To delete a group profile, click **Delete**. You are required to confirm deletion of a group profile. To add a new group profile, click the **Add a group** link. A Group Profile page is opened for you to enter the information for the new group profile. A maximum of 16 group profiles can be added. The group profile names do not need to be unique.

The following table describes the fields on the Group Profile page.

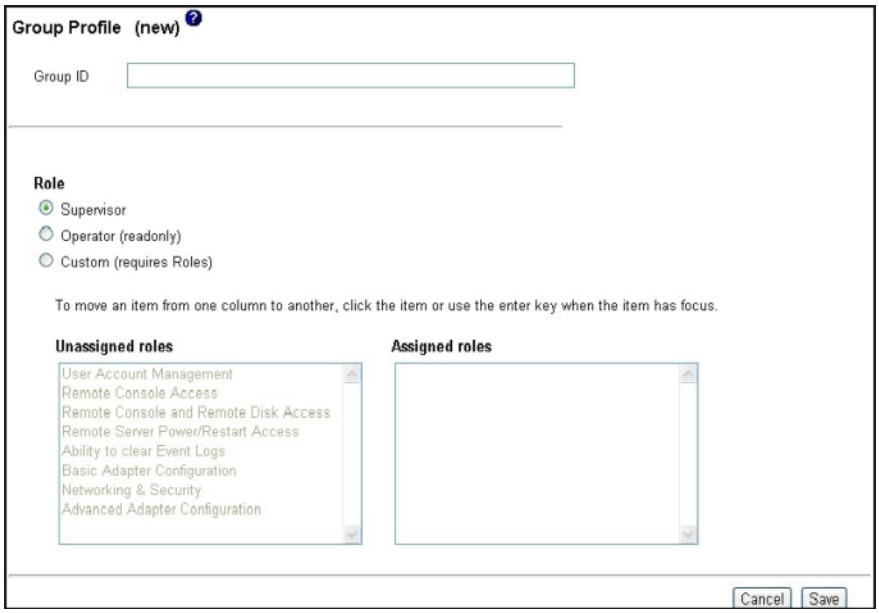
Table 11. Group profiles information

Field	Option	Description
Group ID		This field is used to specify the group id for the group profile. You can enter a maximum of 63 characters. The group id must be the same as their counterparts on the LDAP servers. Examples of group names are IMM Admin Group and IMM/Robert.
Role		Select the roles (authority levels) associated with this login id and transfer them to the **Assigned roles** box. The Enter key or a mouse click can be used to transfer selected items from one box to the other.
	Supervisor	The user has no restrictions except for assigned scope.
	Operator	The user only has read-only access permission and cannot perform any changes, for example, save, modify, and clear. This also includes state affecting operations such as, restart IMM, restore defaults, and upgrade the firmware.

Table 11. Group profiles information (continued)

Field	Option	Description
Role	Custom	The user may or may not have any restrictions, depending on the custom authority level that is assigned to the user. If you select the Custom option, you must select one or more of the following customer authority levels: • Networking and Security – The user can modify the configuration in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port panels. • User account management – The user can add, modify, or delete users and change the Global Login settings in the Login Profiles panel. • Remote Console Access – The users can access the remote server console. • Remote Console and Remote Disk Access – The user can access the remote server console and the remote disk functions for the remote server. • Remote Server Power/Restart Access – The user can access the power on, restart and server timeout functions for the remote server. • Basic Adapter Configuration – The user can modify configuration parameters in the System Settings (excluding Contact, Location, and Server Timeouts) and Alerts panel. • Ability to Clear Event Logs – The user can clear the event logs. **Note:** Everyone can view the event logs; but, this permission is required to clear the logs. • Advanced Adapter Configuration – The user has no restrictions when configuring the adapter and the user has administrative access to the IMM. The user can perform the following advanced functions: firmware upgrades, Preboot Execution Environment (PXE) network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart/reset the adapter. **Note:** This authority level excludes Server Power/Restart Control and timeout functions.
Note: To prevent a situation where there is no user who has read/write access, login profile number one, must be set with at least the ability to modify the login profiles. This user must be given either Supervisor access or User Account Management access. This guarantees that at least one user can perform actions, make configuration changes, and add users to the login profiles who can also perform actions or make configuration changes.		

The following illustration shows the Group Profile window.



Active directory role-based authentication and authorization

You can set up remote LDAP authentication and authorization for users, using the Active Directory.

Notes:

- Active Directory role-based authentication and authorization applies only to a server used in an Active Directory environment.
- The Enhanced role-based Security Snap-in tool is required for Active Directory role-based authentication and authorization.

Active Directory role-based authentication and authorization uses configuration information stored on an Active Directory server to authenticate a user and then associate permissions with the user. Before enabling Active Directory role-based authentication and authorization, use the Enhanced role-based Security Snap-in tool to store the configuration information on the Active Directory server that associates permissions to users. This tool runs on any Microsoft Windows client and can be downloaded from http://www.ibm.com/systems/support/.

The Enhanced role-based Security Snap-in tool allows you to configure roles on an Active Directory server and to associate the IMM, users, and groups to these roles. See the documentation for the Enhanced role-based Security Snap-in tool for information and instructions. Roles identify the permissions assigned to users and groups and identify the command targets, such as the IMM or a blade server, to which a role is attached. Before enabling Active Directory role-based authentication and authorization, roles should be configured on the Active Directory server.

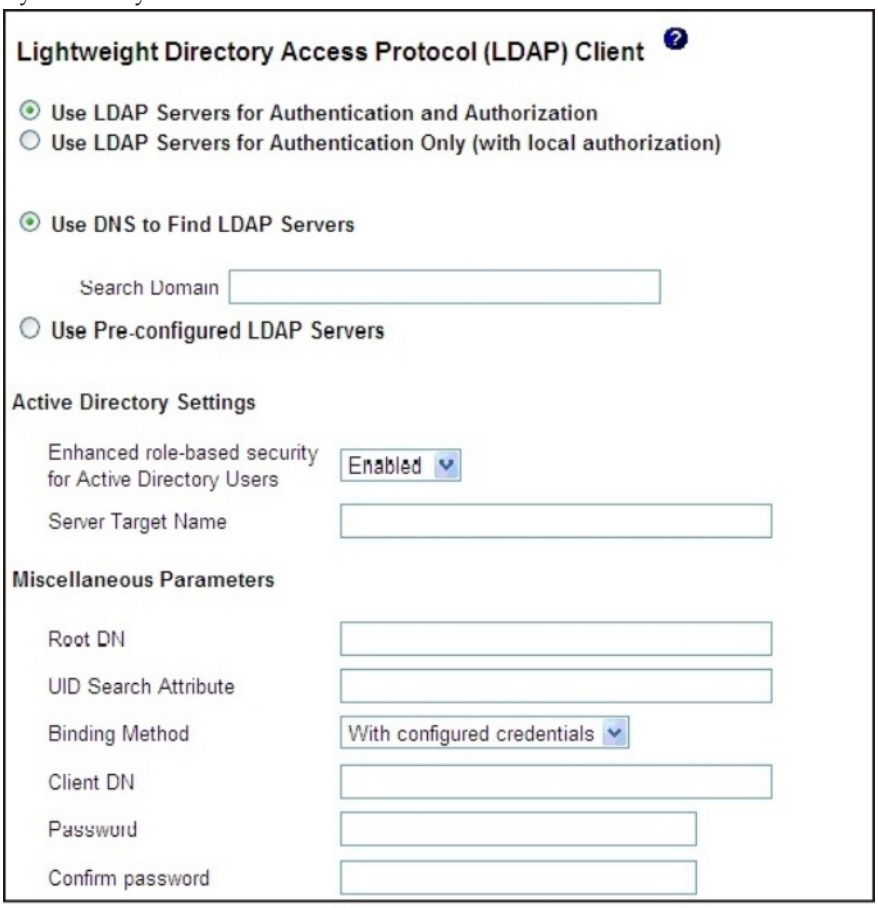
The optional name configured in the **Server Target Name** field identifies a particular IMM and can be associated with one or more roles on the Active Directory server through the role-based Security Snap-In tool. This is accomplished by creating managed targets, giving the targets specific names, and associating the targets with the appropriate roles. If a Server Target Name is configured, it can define specific roles for users and IMM targets that are members of the same role. When a user logs in to the IMM and is authenticated through Active Directory, the roles for this user are retrieved from the directory. The permissions assigned to the

user are extracted from the roles that have a target as a member with a name that matches that IMM, or a target that matches any IMM. The IMM can be given a unique name, or more than one IMM can share the same target name. Assigning more than one IMM to the same target name, groups them together and assigns them to the same role.

To configure Active Directory role-based authentication and authorization for the IMM, complete the following steps:

1. In the navigation pane, click **Network Protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** section.
3. Select **Use LDAP Servers for Authentication and Authorization**.
4. Select **Enabled** for the **Enhanced role-based security for Active Directory Users** field.
5. Select one of the following choices to dynamically discover or manually configure the domain controllers:
   - Select **Use DNS to find LDAP Servers** to dynamically discover the domain controllers based on DNS SVR records.
   - Select **Use Pre-Configured LDAP Servers** (default selection) to manually configure the domain controllers.
6. If you are using DNS to dynamically discover the domain controllers, configure the domain name of the domain controller; then, proceed to step 8 on page 69. You must specify the fully qualified domain name of the domain controller. Enter the domain name of the domain controller in the **Search Domain** field.

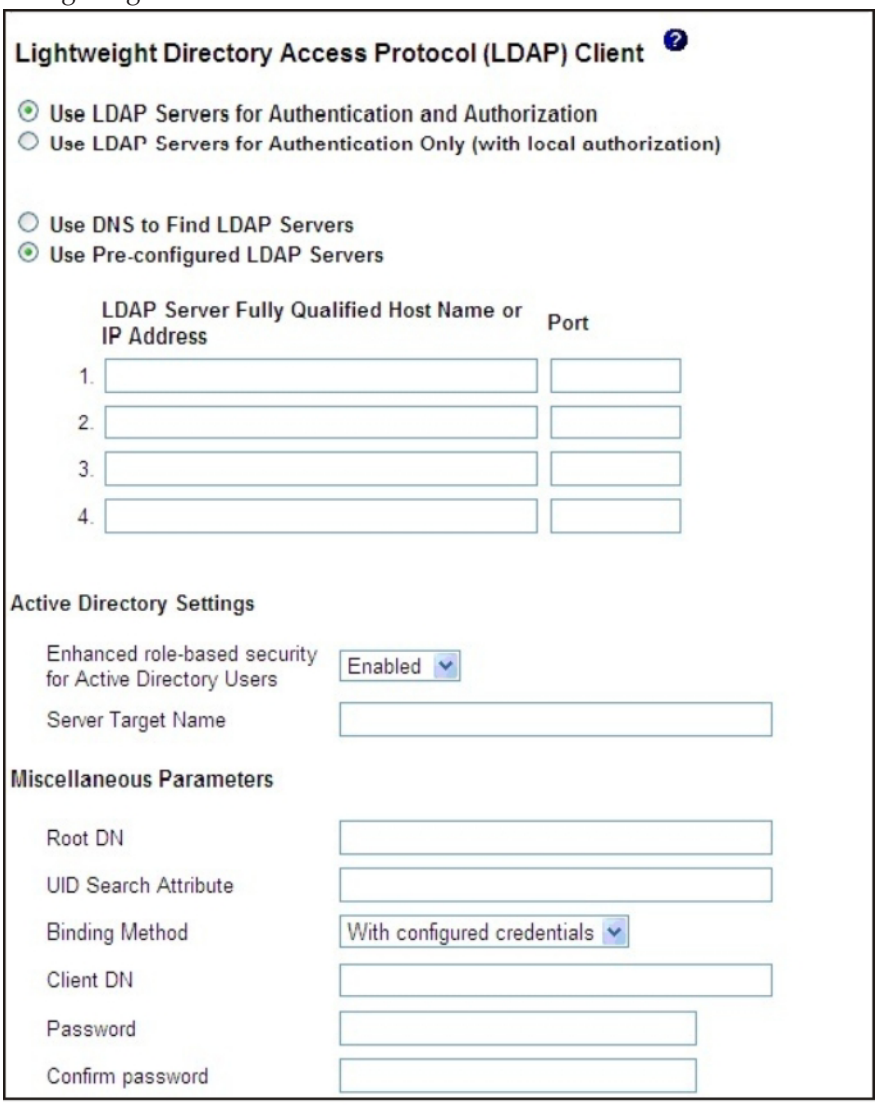
The following window displays the LDAP Client window when using DNS to dynamically discover the domain controllers.



7. If you are manually configuring the domain controllers, configure the **LDAP Server Host Name or IP Address** and **Port** fields.

   Note: Up to four domain controllers can be configured using an IP address or a fully qualified hostname.

The following illustration shows the LDAP Client window when manually configuring the domain controllers.



8. Configure the Active Directory Settings, by selecting **Enabled** from the **Enhanced role-based security for Active Directory Users** menu.
9. Configure the Miscellaneous Parameters. Refer to the following table for information about the parameters.

Table 12. Miscellaneous parameters

Field	Description	Option
Root DN	The IMM uses the **Root DN** field in DN format as the root entry of the directory tree. This DN will be used as the base object for all searches. An example might look like `dc=mycompany,dc=com`.	

Table 12. Miscellaneous parameters (continued)

Field	Description	Option
Binding method	The **Binding Method** field is used for initial binds to the domain controller server, select one option.	• Anonymously: The initial bind to the domain controller server will be made without a DN or password. This option is discouraged since most servers are configured to disallow search requests on specific user records. • With configured credentials: Enter the client DN and Password to be used for the initial bind. • With login credentials: The initial bind to the domain controller server is made using the credentials presented during the login process. The user ID can be provided using a DN, a partial DN, a fully qualified domain name, or through a user ID that matches the **UID Search Attribute** field configured on the IMM. If the credentials resemble a partial DN (e.g. `cn=joe`), this partial DN will be prefixed to the configured Root DN in an attempt to create a DN that matches the user's record. If the bind attemp fails, a final bind attempt will occur by adding the prefix `cn=` to the login credential; then, add the results of the string to the configured Root DN.

Legacy LDAP authentication and authorization

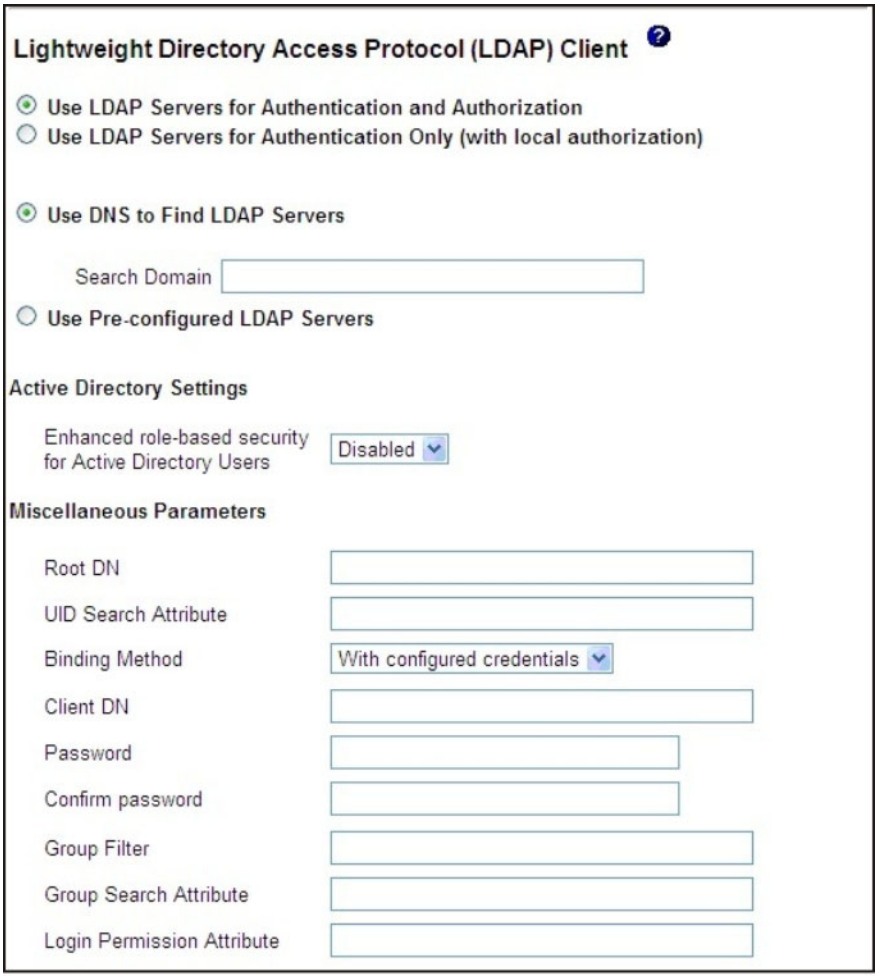
Legacy LDAP authentication and authorization is the original model used with the IMM. Legacy LDAP authentication and authorization supports Active Directory, Novell eDirectory, OpenLDAP environments, and relies on configuration information stored on an LDAP server to associated permissions with a user. Legacy LDAP authentication and authorization is used to authenticate and authorize users through an LDAP server. If the Enhanced Role-based Security for Active Directory Users is disabled on an IMM, you are allowed to configure the LDAP search attributes for the IMM.

To configure legacy LDAP authentication and authorization for the IMM, complete the following steps:

1. In the navigation pane, click **Network Protocols**.
2. Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** section.
3. Select **Use LDAP Servers for Authentication and Authorization**.
4. Select **Disabled** for the **Enhanced role-based security for Active Directory Users** field.
5. Select one of the following choices, to dynamically discover or manually configure the LDAP servers to be used for authentication:
   - Select **Use DNS to find LDAP Servers** to dynamically discover the LDAP servers based on DNS SVR records.
   - Select **Use Pre-Configured LDAP Servers** (default selection) to manually configure the LDAP servers.

6. If you are using DNS to dynamically discover the LDAP servers, configure the domain name of the LDAP server; then, proceed to step 8 on page 72. You must specify the fully qualified domain name of the LDAP server. Enter the domain name of the LDAP server in the **Search Domain** field

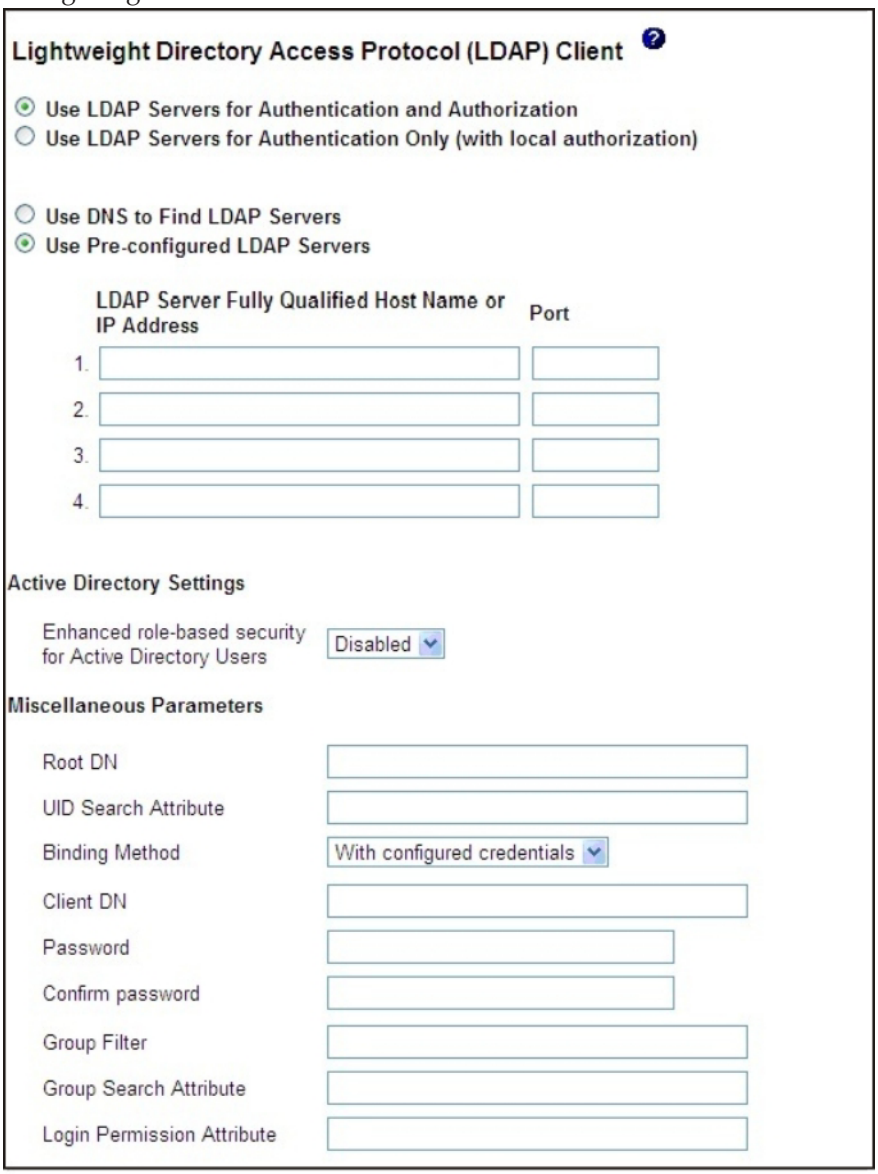
   The following window displays the LDAP Client window when using DNS to dynamically discover the LDAP servers.



7. If you are manually configuring the LDAP servers, configure the **LDAP Server Host Name or IP Address** and **Port** fields; then, proceed to step 8 on page 72.

   Note: Up to four LDAP servers can be configured using an IP address or a fully qualified hostname.

The following window displays the LDAP Client window when manually configuring the LDAP servers.



8. Configure the Active Directory Settings, by selecting **Disabled** from the **Enhanced role-based security for Active Directory Users** menu.
9. Configure the Miscellaneous Parameters. Refer to the following list for a description of required parameter fields.
   - The IMM uses the **Root DN** field in DN format as the root entry of the directory tree. This DN will be used as the base object for all searches. An example might look like `dc=mycompany,dc=com`.
   - The **Binding Method** field is used for initial binds to the domain controller server. Use one of the following binding options:
     - Anonymously:

       The initial bind to the domain controller server will be made without a DN or password. This option is discouraged since most servers are configured to disallow search requests on specific user records.
     - With configured credentials:

       Enter the client DN and Password to be used for the initial bind.

– With login credentials:

  Bind with the credentials supplied during the login process. The user ID can be provided using a DN, a partial DN, a fully qualified domain name, or through a user ID that matches the information in the **UID Search Attribute** field configured on the IMM. If credentials resemble a partial DN (for example, `cn=joe`), this partial DN will be prefixed to the configured Root DN in an attempt to create a DN that matches the user's record. If the bind attempt fails, a final bind attempt will occur by adding the prefix `cn=` to the login credential; then, add the results of the string to the configured Root DN.

- The **Group Filter** field is used for group authentication. It specifies the group the IMM belongs to. If the group filter is left blank, group authentication automatically succeeds. Group authentication, if enabled, takes place after user authentication. An attempt is made to match at least one group in the Group Filter to a group that the user belongs to. If there is no match, the user fails authentication and is denied access. If there is at least one match, group authentication passes. The comparisons are case sensitive.

  When group authentication is disabled, the user's own record must contain the permission attribute; otherwise, access will be denied. For each group that matches the filter, the permissions associated with that group are assigned to the user. The permissions associated with a group are found by retrieving the **Login Permission Attribute** information.

  The filter is limited to 511 characters, and consists of one or more group names. The colon (:) character must be used to specify multiple group names. Leading spaces and trailing spaces are ignored, all other spaces are treated as part of the group name. A group name can be specified as a full DN or using only the *cn* portion. For example, a group with a DN equal to `cn=adminGroup,dc=mycompany,dc=com` can be specified using the actual DN or with adminGroup.

  Note: The previously used asterisk (*) symbol is no longer treated as a wildcard symbol. The wildcard concept was removed for security reasons.

- The **Group Search Attribute** field is used by the search algorithm to find group membership information for a specific user. When the group filter name is configured, the list of groups that the user belongs to must be retrieved from the LDAP server. This list is required to perform group authentication. To retrieve this list, the search filter that is sent to the LDAP server must specify the attribute name that is associated with the groups. The **Group Search Attribute** field specifies the attribute name.

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

- The **Login Permission Attribute** field specifies the attribute name associated with the login permissions for the user. When a user successfully authenticates using a LDAP server, it is necessary to retrieve the login permissions for the user.

Note: This **Login Permission Attribute** field must not be blank; otherwise, it is impossible to retrieve the user's permissions. Without verified permissions, the login attempt will fail.

The attribute value returned by the LDAP server is searched for using the keyword string `IBMRBSPermissions=`. This keyword must be immediately followed by a bit string (up to 12 consecutive 0's or 1's). Each bit represents a particular set of functions. The bits are numbered according to their position. The leftmost bit is bit position 0, and the rightmost bit is bit position 11. A value of 1 at a particular position enables that particular function. A value of 0 disables that function. The string `IBMRBSPermissions=010000000000` is an example.

The `IBMRBSPermissions=` keyword can be placed anywhere in **Login Permission Attribute** field. This allows the LDAP administrator to reuse an existing attribute; therefore, preventing an extension to the LDAP schema and allowing the attribute to be used for its original purpose. The user can now add the keyword string at the beginning, at the end, or any location in this field. The attribute used will allow for a free-formatted string.

The following table provides an explanation of each bit position.

Table 13. Permission bits

Bit position	Function	Explanation
0	Deny Always	If set, 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	If set, 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	If set, a user has read-only access, and cannot perform any maintenance procedures (for example, restart, remote actions, or firmware updates). Nothing can be modified, using save, clear, or restore functions. Bit position 2 and all other bits are mutually exclusive, with bit position 2 having the lowest precedence. If any other bit is set, this bit will be ignored.
3	Networking & Security	If set, a user can modify the configuration in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port panels.
4	User Account Management	If set, a user can add, modify, or delete users and change the Global Login Settings in the Login Profiles panel.
5	Remote Console Access	If set, a user can access the remote server console and can modify the configuration in the Serial Port panel.

Table 13. Permission bits (continued)

Bit position	Function	Explanation
6	Remote Console and Remote Disk Access	If set, a user can access the remote server console and the remote disk functions for the remote server. The user can also modify the configuration in the Serial Port panel.
7	Remote Server Power/Restart Access	If set, a user can access the power on, restart and server timeout functions for the remote server.
8	Basic Adapter Configuration	If set, a user can modify configuration parameters in the System Settings and Alerts panels (excludes Contact, Location and Server Timeout parameters).
9	Ability to Clear Event Logs	If set, a user can clear the event logs. **Note:** All users can view the event logs; but, the user is required to have this level of permission to clear the logs.
10	Advanced Adapter Configuration	If set, a user has no restrictions when configuring the adapter and the user has administrative access to the IMM. The user can perform the following advanced functions: firmware upgrades, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart/reset the adapter. This excludes Server Power/Restart Control and timeout functions.
11	Reserved	This bit position is reserved for future use (currently ignored).

Notes:

- If bits are not used, the default will be set to Read Only for the user.
- Priority is given to login permissions retrieved directly from the user record. If the user record does not contain a name in the **Login Permission Attribute** field, an attempt will be made to retrieve the permissions from the group that the user belongs to and that match the group filter. In this case the user is assigned the inclusive OR of all the bits for all groups.
- If the Deny Always (bit position zero) bit is set for any of the groups, the user will be refused access. The Deny Always bit has precedence over all bits.
- If a user has the ability to modify basic, networking, or security related adapter configuration parameters, you should consider giving that user the ability to restart the IMM (bit position ten). Without this ability, a user might be able to change a parameter; but, the parameter will not take affect.

Configuring security

Use the general procedure in this section to configure security for the IMM web server, for the connection between the IMM and IBM Systems Director, and for the connection between the IMM and an LDAP server. If you are not familiar with the use of SSL certificates, read the information in "SSL certificate overview" on page 77.

Use the following general tasks list to configure the security for the IMM:

1. Configure the secure web server:
   a. Disable the SSL server. Use the **HTTPS Server Configuration for Web Server** area on the Security page.
   b. Generate or import a certificate. Use the **HTTPS Server Certificate Management** area on the Security page (see "SSL server certificate management" on page 78).
   c. Enable the SSL server. Use the **HTTPS Server Configuration for Web Server** area on the Security page (see "Enabling SSL for the secure web server or IBM Systems Director over HTTPS" on page 82).
2. Configure the IBM Systems Director connection:
   a. Disable the Systems Director over HTTPS setting. Use the **IBM Systems Director over HTTPS Server Configuration** area on the Security page.
   b. Generate or import a certificate. Use the **IBM Systems Director over HTTPS Server Certificate Management** area on the Security page (see "SSL server certificate management" on page 78).
   c. Enable the SSL server. Use the **IBM Systems Director over HTTPS Server Configuration** area on the Security page (see "Enabling SSL for the secure web server or IBM Systems Director over HTTPS" on page 82).
3. Configure SSL security for LDAP connections:
   a. Disable the SSL client. Use the **SSL Client Configuration for LDAP Client** area on the Security page.
   b. Generate or import a certificate. Use the **SSL Client Certificate Management** area on the Security page (see "SSL server certificate management" on page 78).
   c. Import one or more trusted certificates. Use the **SSL Client Trusted Certificate Management** area on the Security page (see "SSL client trusted certificate management" on page 82).
   d. Enable the SSL client. Use the **SSL Client Configuration for LDAP Client** area on the Security page (see "Enabling SSL for the secure web server or IBM Systems Director over HTTPS" on page 82).
4. Restart the IMM for SSL server configuration changes to take effect. For more information, see "Restarting IMM" on page 87.

   Note: Changes to the SSL client configuration take effect immediately and do not require a restart of the IMM.

Secure web server, IBM Systems Director, and secure LDAP

Secure Sockets Layer (SSL) is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery.

You can configure the IMM to use SSL support for two types of connections: secure server (HTTPS) and secure LDAP connection (LDAPS). The IMM takes on the role

of SSL client or SSL server depending on the type of connection. The following table shows that the IMM acts as an SSL server for secure web server connections. The IMM acts as an SSL client for secure LDAP connections.

Table 14. IMM SSL connection support

Connection type	SSL client	SSL server
Secure web server (HTTPS)	Web browser of the user (For example: Microsoft Internet Explorer)	IMM web server
Secure IBM Systems Director connection	IBM Systems Director	IMM Systems Director server
Secure LDAP connection (LDAPS)	IMM LDAP client	An LDAP server

You can view or change the SSL settings from the Security page. You can enable or disable SSL and manage the certificates that are required for SSL.

SSL certificate overview

You can use SSL with either 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. It is possible that a third party might impersonate the server and intercept data that is flowing between the IMM and the web browser. If, at the time of the initial connection between the browser and the IMM, 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. To obtain a signed certificate, use the SSL Certificate Management page to generate a certificate-signing request. You must then send the certificate-signing request to a certificate authority and make arrangements to procure a certificate. When the certificate is received, it is then imported into the IMM through the **Import a Signed Certificate** link, and you can enable SSL.

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

The IMM requires a certificate for the secure web server and one for the secure LDAP client. Also, the secure LDAP client requires one or more trusted certificates. The trusted certificate is used by the secure LDAP client to positively identify the LDAP server. The trusted certificate is the certificate of the certificate authority 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.

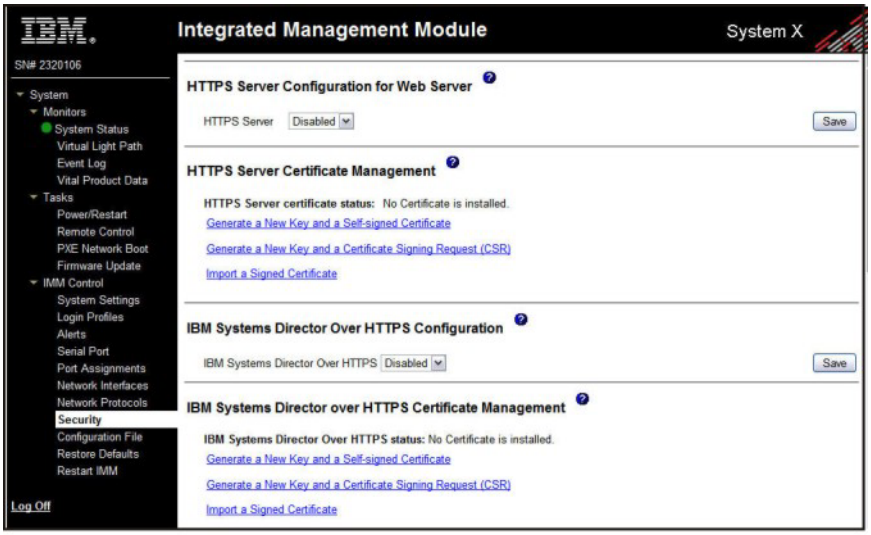
SSL server certificate management

The SSL server requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled. Two methods are available for generating the private key and required certificate: using a self-signed certificate and using a certificate that is signed by a certificate authority. If you want to use a self-signed certificate for the SSL server, see "Generating a self-signed certificate." If you want to use a certificate-authority-signed certificate for the SSL server, see "Generating a certificate-signing request" on page 79.

Generating a self-signed certificate

To generate a new private encryption key and self-signed certificate, complete the following steps:

1. In the navigation plane, click **Security**. A page similar to the one in the following illustration is displayed.



2. In the **SSL Server Configuration for Web Server** area or **IBM Systems Director Over HTTPS Configuration** area, make sure that the setting is **Disabled**. If it is not disabled, select **Disabled** and then click **Save**.

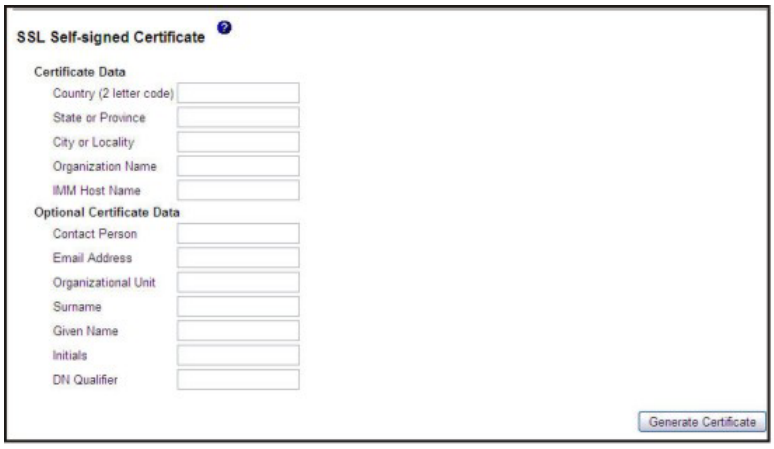
   Note:

   a. The IMM must be restarted before the selected value (**Enabled** or **Disabled**) takes effect.

   b. Before you can enable SSL, a valid SSL certificate must be in place.

   c. To use SSL, you must configure a client web browser to use SSL3 or TLS. Older export-grade browsers with only SSL2 support cannot be used.

3. In the **SSL Server Certificate Management** area, select **Generate a New Key and a Self-signed Certificate**. A page similar to the one in the following illustration is displayed.

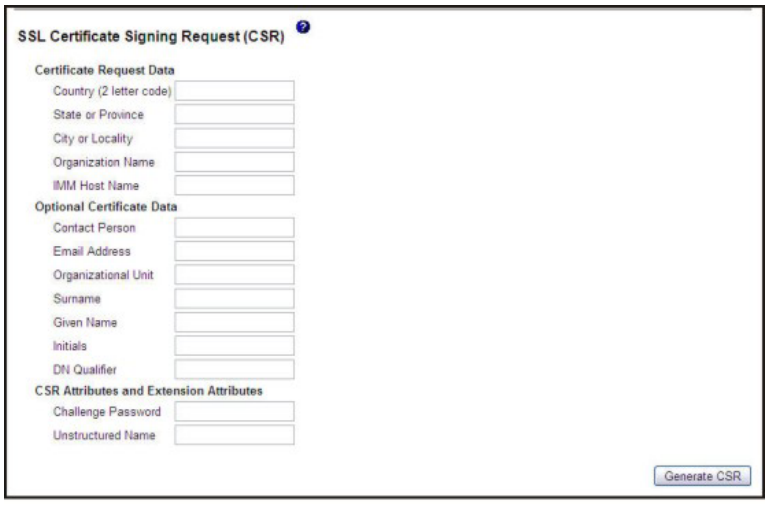


4. Type the information in the required fields and any optional fields that apply to your configuration. For a description of the fields, see "Required certificate data" on page 80. After you finish typing the information, click **Generate Certificate**. Your new encryption keys and certificate are generated. This process might take several minutes. You see confirmation if a self-signed certificate is installed.

Generating a certificate-signing request

To generate a new private encryption key and certificate-signing request, complete the following steps:

1. In the navigation pane, click **Security**.
2. In the **SSL Server Configuration for Web Server** area, make sure that the SSL server is disabled. If it is not disabled, select **Disabled** in the **SSL Server** field and then click **Save**.
3. In the **SSL Server Certificate Management** area, select **Generate a New Key and a Certificate-Signing Request**. A page similar to the one in the following illustration is displayed.



4. Type the information in the required fields and any optional fields that apply to your configuration. The fields are the same as for the self-signed certificate, with some additional fields.

Read the information in the following sections for a description of each of the common fields.

Required certificate data The following user-input fields are required for generating a self-signed certificate or a certificate-signing request:

Country
Use this field to indicate the country where the IMM is physically located. This field must contain the 2-character country code.

State or Province
Use this field to indicate the state or province where the IMM is physically located. This field can contain a maximum of 30 characters.

City or Locality
Use this field to indicate the city or locality where the IMM is physically located. This field can contain a maximum of 50 characters.

Organization Name
Use this field to indicate the company or organization that owns the IMM. When this is used to generate a certificate-signing request, the issuing certificate authority can verify that the organization that is requesting the certificate is legally entitled to claim ownership of the given company or organization name. This field can contain a maximum of 60 characters.

IMM Host Name
Use this field to indicate the IMM host name that currently appears in the browser web address bar.

Make sure that the value that you typed in this field exactly matches the host name as it is known by the web browser. The browser compares the host name in the resolved web address to the name that appears in the certificate. To prevent certificate warnings from the browser, the value that is used in this field must match the host name that is used by the browser to connect to the IMM. For example, if the address in the web address bar is http://mm11.xyz.com/private/main.ssi, the value that is used for the IMM Host Name field must be mm11.xyz.com. If the web address is http://mm11/private/main.ssi, the value that is used must be mm11. If the web address is http://192.168.70.2/private/main.ssi, the value that is used must be 192.168.70.2.

This certificate attribute is generally referred to as the common name.

This field can contain a maximum of 60 characters.

Contact Person
Use this field to indicate the name of a contact person who is responsible for the IMM. This field can contain a maximum of 60 characters.

Email Address
Use this field to indicate the e-mail address of a contact person who is responsible for the IMM. This field can contain a maximum of 60 characters.

Optional certificate data The following user-input fields are optional for generating a self-signed certificate or a certificate-signing request:

Organizational Unit
Use this field to indicate the unit within the company or organization that owns the IMM. This field can contain a maximum of 60 characters.

Surname
Use this field for additional information, such as the surname of a person who is responsible for the IMM. This field can contain a maximum of 60 characters.

Given Name
Use this field for additional information, such as the given name of a person who is responsible for the IMM. This field can contain a maximum of 60 characters.

Initials
Use this field for additional information, such as the initials of a person who is responsible for the IMM. This field can contain a maximum of 20 characters.

DN Qualifier
Use this field for additional information, such as a distinguished name qualifier for the IMM. This field can contain a maximum of 60 characters.

Certificate-Signing request attributes The following fields are optional unless they are required by your selected certificate authority:

Challenge Password
Use this field to assign a password to the certificate-signing request. This field can contain a maximum of 30 characters.

Unstructured Name
Use this field for additional information, such as an unstructured name that is assigned to the IMM. This field can contain a maximum of 60 characters.

5. After you complete the information, click **Generate CSR**. The new encryption keys and certificate are generated. This process might take several minutes.
6. Click **Download CSR** and then click **Save** to save the file to your workstation. The file that is produced when you create a certificate-signing request is in DER format. If your certificate authority expects the data in some other format, such as PEM, you can convert the file by using a tool such as OpenSSL (http://www.openssl.org). If the certificate authority asks you to copy the contents of the certificate-signing request file into a web browser window, PEM format is usually expected.

   The command for converting a certificate-signing request from DER to PEM format using OpenSSL is similar to the following example:

   ```
   openssl req -in csr.der -inform DER -out csr.pem -outform PEM
   ```

7. Send the certificate-signing request to your certificate authority. When the certificate authority returns your signed certificate, you might have to convert the certificate to DER format. (If you received the certificate as text in an e-mail or a webpage, it is probably in PEM format.) You can change the format using a tool that is provided by your certificate authority or using a tool such as OpenSSL (http://www.openssl.org). The command for converting a certificate from PEM to DER format is similar to the following example:

   ```
   openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
   ```

   Go to step 8 after the signed certificate is returned from the certificate authority.
8. In the navigation pane, click **Security**. Scroll to the **SSL Server Certificate Management** area or the **IBM Systems Director Over HTTPS Certificate Management** area.
9. Click **Import a Signed Certificate**.
10. Click **Browse**.

11. Click the certificate file that you want and then click **Open**. The file name (including the full path) is displayed in the field next to the **Browse** button.
12. Click **Import Server Certificate** to begin the process. A progress indicator is displayed as the file is transferred to storage on the IMM. Continue to display this page until the transfer is completed.

Enabling SSL for the secure web server or IBM Systems Director over HTTPS

Complete the following steps to enable the secure web server.

Note: To enable SSL, a valid SSL certificate must be installed.

1. In the navigation pane, click **Security**. The page that is displayed shows that a valid SSL server certificate is installed. If the SSL server certificate status does not show that a valid SSL certificate is installed, go to "SSL server certificate management" on page 78.
2. Scroll to the **SSL Server Configuration for web Server** area or the **IBM Systems Director Over HTTPS Configuration** area, select **Enabled** in the **SSL Client** field, and then click **Save**. The selected value takes effect the next time the IMM is restarted.

SSL client certificate management

The SSL client requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled. Two methods are available for generating the private key and required certificate: using a self-signed certificate, or using a certificate signed by a certificate authority.

The procedure for generating the private encryption key and certificate for the SSL client is the same as the procedure for the SSL server, except that you use the **SSL Client Certificate Management** area of the Security webpage instead of the **SSL Server Certificate Management** area. If you want to use a self-signed certificate for the SSL client, see "Generating a self-signed certificate" on page 78. If you want to use a certificate authority signed certificate for the SSL client, see "Generating a certificate-signing request" on page 79.

SSL client trusted certificate management

The secure SSL client (LDAP client) uses trusted certificates to positively identify the LDAP server. A trusted certificate can be the certificate of the certificate authority that signed the certificate of the LDAP server, or it can be the actual certificate of the LDAP server. At least one certificate must be imported to the IMM before the SSL client is enabled. You can import up to three trusted certificates.

To import a trusted certificate, complete the following steps:

1. In the navigation pane, select **Security**.
2. In the **SSL Client Configuration for LDAP Client** area, make sure that the SSL client is disabled. If it is not disabled, select **Disabled** in the **SSL Client** field and then click **Save**.
3. Scroll to the **SSL Client Trusted Certificate Management** area.
4. Click **Import** next to one of the **Trusted CA Certificate 1** fields.
5. Click **Browse**.
6. Select the certificate file that you want and click **Open**. The file name (including the full path) is displayed in the box next to the **Browse** button.

7. To begin the import process, click **Import Certificate**. A progress indicator is displayed as the file is transferred to storage on the IMM. Continue displaying this page until the transfer is completed.

   The **Remove** button is now available for the Trusted CA Certificate 1 option. If you want to remove a trusted certificate, click the corresponding **Remove** button.

   You can import other trusted certificates by using the Trusted CA Certificate 2 and the Trusted CA Certificate 3 **Import** buttons.

Enabling SSL for the LDAP client

Use the **SSL Client Configuration for LDAP Client** area of the Security page to enable or disable SSL for the LDAP Client. To enable SSL, a valid SSL client certificate and at least one trusted certificate must first be installed.

To enable SSL for the client, complete the following steps:

1. In the navigation pane, click **Security**.

   The Security page shows an installed SSL client certificate and Trusted CA Certificate 1.
2. On the SSL Client Configuration for LDAP Client page, select **Enabled** in the **SSL Client** field.

   Note:

   a. The selected value (Enabled or Disabled) takes effect immediately.
   b. Before you can enable SSL, a valid SSL certificate must be in place.
   c. Your LDAP server must support SSL3 or TLS to be compatible with the SSL implementation that the LDAP client uses.
3. Click **Save**. The selected value takes effect immediately.

Configuring the Secure Shell server

The Secure Shell (SSH) feature provides secure access to the command-line interface and the serial (text console) redirect features of the IMM.

Secure Shell users are authenticated by exchanging user ID and password. The password and user ID are sent after the encryption channel is established. The user ID and password pair can be one of the 12 locally stored user IDs and passwords, or they can be stored on an LDAP server. Public key authentication is not supported.

Generating a Secure Shell server key

A Secure Shell server key is used to authenticate the identity of the Secure Shell server to the client. Secure shell must be disabled before you create a new Secure Shell server private key. You must create a server key before you enable the Secure Shell server.

When you request a new server key, both a Rivest, Shamir, and Adelman key and a DSA key are created to allow access to the IMM from an SSH version 2 client. For security, the Secure Shell server private key is not backed up during a configuration save and restore operation.

To create a new Secure Shell server key, complete the following steps:

1. In the navigation pane, click **Security**.

2. Scroll to the **Secure Shell (SSH) Server** area and make sure that the Secure Shell server is disabled. If it is not disabled, select **Disabled** in the **SSH Server** field and then click **Save**.
3. Scroll to the **SSH Server Key Management** area.
4. Click **Generate SSH Server Private Key**. A progress window opens. Wait for the operation to be completed.

Enabling the Secure Shell server

From the Security page you can enable or disable the Secure Shell server. The selection that you make takes effect only after the IMM is restarted. The value that is displayed on the screen (Enabled or Disabled) is the last selected value and is the value that is used when the IMM is restarted.

Note: You can enable the Secure Shell server only if a valid Secure Shell server private key is installed.

To enable the Secure Shell server, complete the following steps:

1. In the navigation pane, click **Security**.
2. Scroll to the **Secure Shell (SSH) Server** area.
3. Click **Enabled** in the **SSH Server** field.
4. In the navigation pane, click **Restart IMM** to restart the IMM.

Using the Secure Shell server

If you are using the Secure Shell client that is included in Red Hat Linux version 7.3, to start a Secure Shell session to an IMM with network address 192.168.70.132, type a command similar to the following example:

```
ssh -x -l userid 192.168.70.132
```

where -x indicates no X Window System forwarding and -l indicates that the session should use the user ID *userid*.

Restoring and modifying your IMM configuration

You can restore a saved configuration in full, or you can modify key fields in the saved configuration before you restore the configuration to your IMM. By modifying the configuration file before you restore it, you can set up multiple IMMs with similar configurations. You can quickly specify parameters that require unique values such as names and IP addresses, without having to enter common, shared information.

To restore or modify your current configuration, complete the following steps:

1. Log in to the IMM where you want to restore the configuration. For more information, see Chapter 2, “Opening and using the IMM web interface,” on page 11.
2. In the navigation pane, click **Configuration File**.
3. In the **Restore IMM Configuration** area, click **Browse**.
4. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box next to **Browse**.
5. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the IMM configuration information. Make sure that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

If you want to make changes to the configuration file before you restore the configuration, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes are displayed. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window. To modify the contents of a field, click the corresponding text box and enter the data.

Note: When you click **Restore** or **Modify and Restore**, an alert window might open if the configuration file that you are attempting to restore was created by a different type of service processor or was created by the same type of service processor with older firmware (and therefore, with less functionality). This alert message includes a list of systems-management functions that you must configure after the restoration is complete. Some functions require configurations on more than one window.

6. To continue restoring this file to the IMM, click **Restore Configuration**. A progress indicator is displayed as the firmware on the IMM is updated. A confirmation window opens to verify whether the update was successful.

   Note: The security settings on the Security page are not restored by the restore operation. To modify security settings, see "Secure web server, IBM Systems Director, and secure LDAP" on page 76.
7. After you receive a confirmation that the restore process is complete, in the navigation pane, click **Restart IMM**; then, click **Restart**.
8. Click **OK** to confirm that you want to restart the IMM.
9. Click **OK** to close the current browser window.
10. To log in to the IMM again, start the browser, and follow your regular login process.

Using the configuration file

Select **Configuration File** in the navigation pane to back up and restore the IMM configuration.

Important: Security page settings are not saved with the backup operation and cannot be restored with the restore operation.

Backing up your current configuration

You can download a copy of your current IMM configuration to the client computer that is running the IMM web interface. Use this backup copy to restore your IMM configuration if it is accidentally changed or damaged. Use it as a base that you can modify to configure multiple IMMs with similar configurations.

The configuration information that is saved under this procedure does not include System x® server firmware configuration settings or any IPMI settings that are not common with the non-IMPI user interfaces.

To back up your current configuration, complete the following steps:

1. Log in to the IMM where you want to back up your current configuration. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Configuration File**.
3. In the **Backup IMM Configuration** area, click **view the current configuration summary**.

4. Verify the settings and then click **Close**.
5. To back up this configuration, click **Backup**.
6. Type a name for the backup, select the location where the file will be saved, and then click **Save**.

   In Mozilla Firefox, click **Save File**, then click **OK**.

   In Microsoft Internet Explorer, click **Save this file to disk**, then click **OK**.

Restoring and modifying your IMM configuration

You can restore a saved configuration in full, or you can modify key fields in the saved configuration before you restore the configuration to your IMM. By modifying the configuration file before you restore it, you can set up multiple IMMs with similar configurations. You can quickly specify parameters that require unique values such as names and IP addresses, without having to enter common, shared information.

To restore or modify your current configuration, complete the following steps:

1. Log in to the IMM where you want to restore the configuration. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Configuration File**.
3. In the **Restore IMM Configuration** area, click **Browse**.
4. Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box next to **Browse**.
5. If you do not want to make changes to the configuration file, click **Restore**. A new window opens with the IMM configuration information. Make sure that this is the configuration that you want to restore. If it is not the correct configuration, click **Cancel**.

   If you want to make changes to the configuration file before you restore the configuration, click **Modify and Restore** to open an editable configuration summary window. Initially, only the fields that allow changes are displayed. To change between this view and the complete configuration summary view, click the **Toggle View** button at the top or bottom of the window. To modify the contents of a field, click the corresponding text box and enter the data.

   Note: When you click **Restore** or **Modify and Restore**, an alert window might open if the configuration file that you are attempting to restore was created by a different type of service processor or was created by the same type of service processor with older firmware (and therefore, with less functionality). This alert message includes a list of systems-management functions that you must configure after the restoration is complete. Some functions require configurations on more than one window.
6. To continue restoring this file to the IMM, click **Restore Configuration**. A progress indicator is displayed as the firmware on the IMM is updated. A confirmation window opens to verify whether the update was successful.

   Note: The security settings on the Security page are not restored by the restore operation. To modify security settings, see "Secure web server, IBM Systems Director, and secure LDAP" on page 76.
7. After you receive a confirmation that the restore process is complete, in the navigation pane, click **Restart IMM**; then, click **Restart**.
8. Click **OK** to confirm that you want to restart the IMM.
9. Click **OK** to close the current browser window.

10. To log in to the IMM again, start the browser, and follow your regular login process.

Restoring defaults

Use the **Restore Defaults** link to restore the default configuration of the IMM, if you have Supervisor access.

Attention: When you click **Restore Defaults**, you will lose all the modifications that you made to the IMM.

To restore the IMM defaults, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Restore Defaults** to restore default settings of the IMM. If this is a local server, your TCP/IP connection will be broken, and you must reconfigure the network interface to restore connectivity.
3. Log in again to use the IMM web interface.
4. Reconfigure the network interface to restore connectivity. For information about the network interface, see "Configuring network interfaces" on page 36.

Restarting IMM

Use the **Restart IMM** link to restart the IMM. You can perform this function only if you have Supervisor access. Any Ethernet connections are temporarily dropped. You must log in again to use the IMM web interface.

To restart the IMM, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Restart IMM** to restart the IMM. Your TCP/IP or modem connections are broken.
3. Log in again to use the IMM web interface.

Scalable partitioning

The IMM allows you to configure and control the system in a scalable complex.

The IMM allows you to configure and control the system in a scalable complex. If an error exists with the server, the IMM will return an event code to the event logs (see "Viewing the event logs" on page 97).

1. Log in to the IMM where you want to restore the configuration. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Scalable Partitioning** then click **Manage Partitions**.

Service Advisor feature

The Service Advisor feature detects and collects system hardware error events and automatically forwards the data to IBM Support for problem determination. The Service Advisor feature can also collect data about the system errors and forward that data to IBM support. See the documentation for your server to see if your

server supports this feature. Instructions for setting up, testing, and maintaining the Service Advisor are included in the following topics.

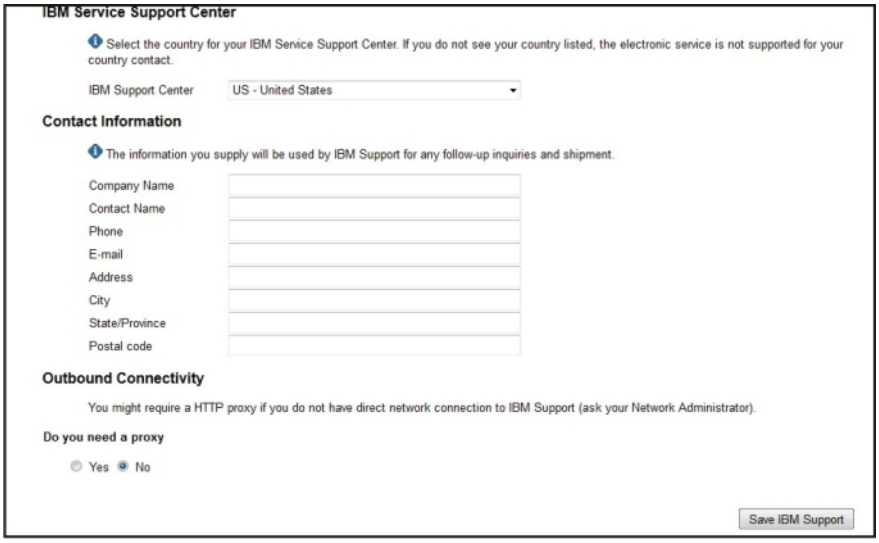
- Configuring Service Advisor
- Using Service Advisor

Configuring Service Advisor

To configure the Service Advisor, complete the following steps.

1. Log in to the IMM where you want to activate the Service Advisor. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Service Advisor**.
3. If this is the first time you use this option, or if the IMM was reset to the default values, you must read and accept the license agreement.
   a. Click **View Terms and Conditions** to view the Service Advisor agreement.
   b. Click **I accept the agreement** on the Terms and Conditions page to activate the Service Advisor.
4. Click the **Service Advisor Settings** tab.

   A page similar to the one in the following illustration is displayed.



5. Enter the contact information for the server administrator. Refer to the following table for an explanation of the **Contact Information** fields.

Table 15. Contact Information

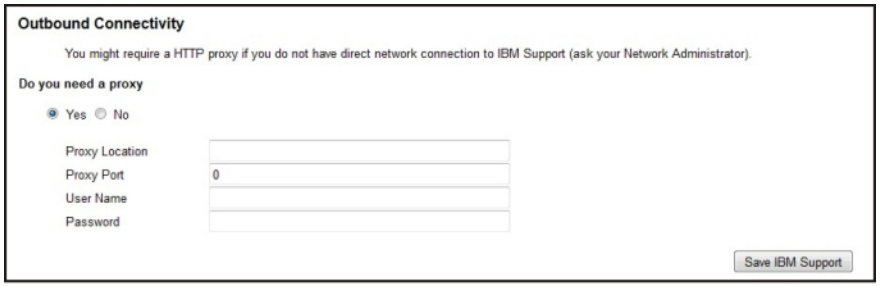
Field	Description
IBM Service Support Center	Specify the country code for the IBM Service Support Center in this field. This is a two-character ISO country code and applies only to those that have IBM Service Support Center access.
Company Name	Specify the organization or company name of the contact person in this field. This field can contain 1 to 30 characters.
Contact Name	Specify the organization or company name of the contact person in this field. This field can contain 1 to 30 characters.
Phone	Specify the telephone number of the contact person in this field. This field can contain 5 to 30 characters.
Email	Specify the email address of the contact person in this field. The maximum length of this field is 30 characters.

Table 15. Contact Information (continued)

Field	Description
Address	Specify the street address where the IMM is physically located in this field. This field can contain 1 to 30 characters.
City	Specify the city or locality where the IMM is physically located in this field.
State/Province	Specify the state or province where the IMM is physically located in this field. This field can contain 2 to 3 characters.
Postal Code	Specify the postal code of the location for this server in this field. This field can contain 1 to 9 characters, (only alphanumeric characters are valid).

6. Create an HTTP proxy if the IMM does not have a direct network connection to IBM Support. Complete the following steps to configure the outbound connectivity information.
   a. In the **Do you need a proxy** field, click **Yes**. Refer to the previous illustration.

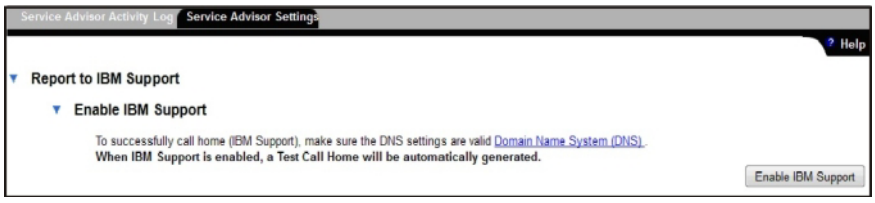
      A page similar to the one in the following illustration is displayed.



   b. Enter the **Proxy Location**, the **Proxy Port**, the **User Name** and the **Password**.
7. Click **Save IBM Support** to save your changes.
8. Click **Enable IBM Support** (which is located near the top of the page) to enable the Service Advisor to contact IBM Support when a serviceable event code is generated.

   Note: After enabling IBM Support, a test code is sent to the IBM support site.
9. Click the **Service Advisor Activity Log** tab to view the status of the test code.

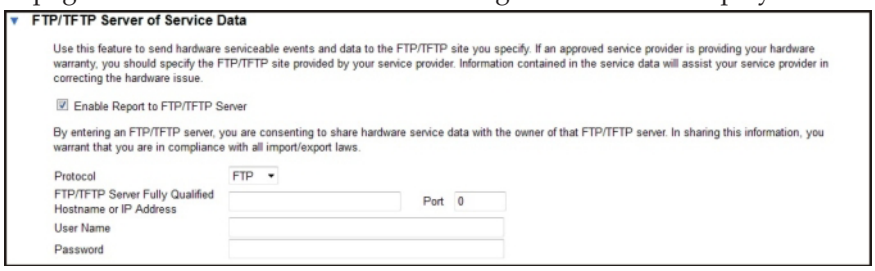
   A page similar to the one in the following illustration is displayed.



10. If you want to allow another service provider to receive the event codes before you contact IBM Support, click **Enable Report to FTP/TFTP Server**.

    Attention: By entering an FTP/TFTP server, you are consenting to share hardware service data with the owner of that FTP/TFTP server. In sharing this information, you warrant that you are in compliance with all import/export laws.

A page similar to the one in the following illustration is displayed.



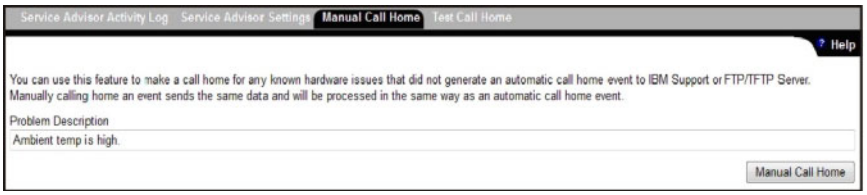
Using Service Advisor

After Service Advisor is set up, you can view the activity log or generate a test message.

Complete the following steps to create a hardware problem report for your server:

1. Log in to the IMM where you want to use the Service Advisor. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Service Advisor**.
3. Click the **Manual Call Home** tab.

   A page similar to the one in the following illustration is displayed.

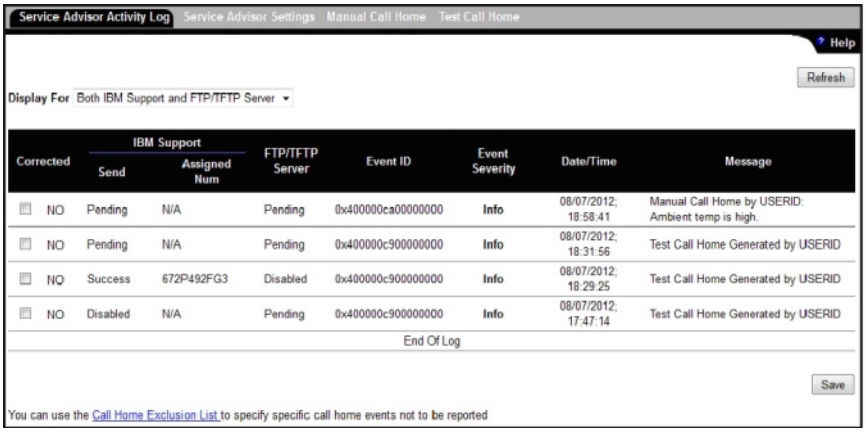


4. Complete the following steps to manually call home an event.
   a. Enter the problem description in the **Problem Description** field.
   b. Click the **Manual Call Home** button.
5. To generate a test message, click the **Test Call Home** tab; then, select the **Test Call Home** button.

   Notes:

   - The test call home menu validates the communication path between IMM and IBM or FTP/TFTP server with the current settings.
   - If the test is not successful, verify the network setup.
   - To report to IBM Support, Service Advisor requires proper setup of the DNS server address on the IMM.
   - If the call is successful an Assigned Service Number or ticket number will be assigned. The ticket that is opened at IBM Support will be identified as a test ticket. No action is required from IBM Support for a test ticket and the call will be closed.
6. Click the **Service Advisor Activity Log** tab to view the status of the activity log.

A page similar to the one in the following illustration is displayed.



Notes:

- The activity log shows the last five Call Home events, including the Test Call Home and Manual Call Home events.
- The results in the **Send** field can be one of the following:

  Success
  The call was successfully received at IBM or FTP/TFTP. The **Assigned Service Number** field includes a problem ticket number.

  Pending
  The Call Home event is in progress.

  Failed The Call Home event failed. In the case of a call home event failure, contact IBM Support to report the hardware service event. Failed Call Home events will not be retried.

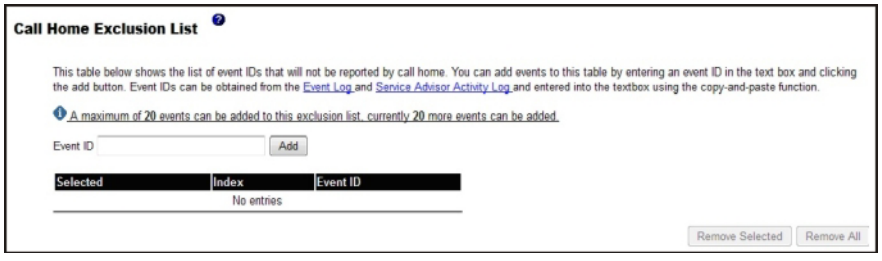
7. After you resolve an event, click the **Corrected** checkbox for that event to make it easier to find unresolved events.

   Note: If the **Corrected** checkbox is not selected for an event, the next occurrence of the same event is not *called home* until five days after the first occurrence of the event.

8. Click **Refresh** to display the latest information.

   Note: The **Assigned Service Number** can be used to reference the Call Home event when communicating with IBM Support.

9. To remove a specified event from the report to IBM Support, perform the following steps:
   a. Click the **Call Home Exclusion List** link. A page similar to the one in the following illustration is displayed.



   b. Enter the hexadecimal Event ID into the **Event ID** field.
   c. Click **Add**.

Logging off

To log off the IMM or another remote server, click **Log Off** in the navigation pane.

Chapter 4. Monitoring server status

Use the links under the **Monitors** heading of the navigation pane to view the status of the server that you are accessing.

From the System Status pages, you can:

- Monitor the power status of the server and view the state of the operating system
- View the server temperature readings, voltage thresholds, and fan speeds
- View the latest server operating-system-failure screen capture
- View the list of users who are logged in to the IMM

From the Virtual Light Path page, you can view the name, color, and status of any LEDs that are lit on a server.

From the Event Log page, you can:

- View certain events that are recorded in the event log of the IMM
- View the severity of events

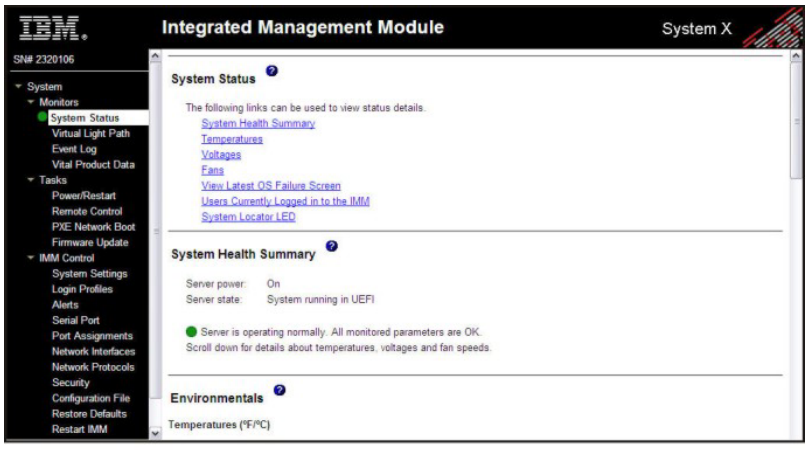
From the Vital Product Data (VPD) page, you can view the vital product data.

Viewing system status

On the System Status page, you can monitor the temperature readings, voltage thresholds, and fan status of your server. You can also view the latest operating-system-failure screen, the users who are logged in to the IMM, and the system locator LED.

To view the system health and environmental information of the server, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **System Status** to view a dynamically-generated update of the overall health of the server. A page similar to the one in the following illustration is displayed.



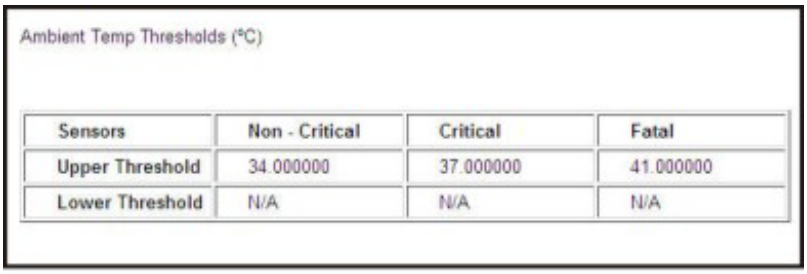
The status of your server determines the message that is shown at the top of the System Health Summary page. One of the following symbols is displayed:

- A solid green circle and the phrase `Server is operating normally`
- Either a red circle that contains an X or a yellow triangle that contains an exclamation point and the phrase `One or more monitored parameters are abnormal`

If the monitored parameters are operating outside normal ranges, a list of the specific abnormal parameters is displayed on the System Health Summary page.

3. Scroll down to the **Temperature** area in the **Environmentals** section of the page, which includes temperature, voltage, and fan speed information.

   The IMM tracks the current temperature readings and threshold levels for system components such as microprocessors, system board, and hard disk drive backplane. When you click a temperature reading, a new window opens.



   The Temperature Thresholds page displays the temperature levels at which the IMM reacts. The temperature threshold values are preset on the remote server and cannot be changed.

   The reported temperatures are measured against the following threshold ranges:

   Non-Critical
   When the temperature reaches a specified value, a temperature alert is sent to the configured remote alert recipients. You must select the **Warning Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page or the **Warning Alerts** check box on the Remote Alert Recipient page for the alert to be sent.

   For more information about selecting alert options, see “Configuring SNMP alert settings” on page 33 or “Configuring remote alert recipients” on page 30.

   Critical
   When the temperature reaches a specified value higher than the warning value (the soft shutdown threshold), a second temperature alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page or the **Critical Alerts** check box on the Remote Alert Recipient page for the alert to be sent.

   For more information about selecting alert options, see “Configuring SNMP alert settings” on page 33 or “Configuring remote alert recipients” on page 30.

   Fatal When the temperature reaches a specified value higher than the soft

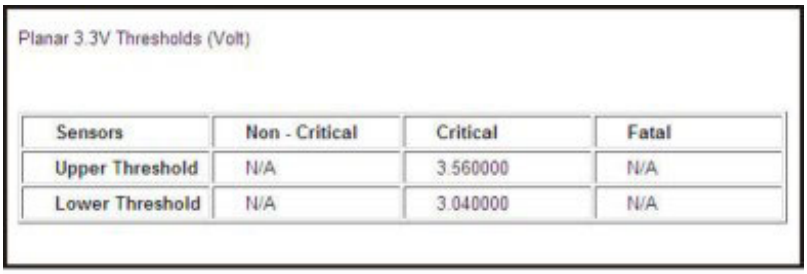
shutdown value (the hard shutdown threshold), the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page or the **Critical Alerts** check box on the Remote Alert Recipient page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 33 or "Configuring remote alert recipients" on page 30.

The IMM generates a non-critical or critical event when the threshold is reached and initiates shutdown actions, if they are required.

4. Scroll down to the **Voltages** area. The IMM will send an alert if any monitored power source voltage falls outside its specified operational ranges.

   If you click a voltage reading, a new window opens.


Planar 3.3V Thresholds (Volt)

Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	3.560000	N/A
Lower Threshold	N/A	3.040000	N/A

The Voltage Thresholds page displays the voltage ranges at which the IMM reacts. The voltage threshold values are preset on the remote server and cannot be changed.

The IMM web interface displays the voltage readings of the system board and the voltage regulator modules (VRM). The system sets a voltage range at which the following actions are taken:

Non-Critical

When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients. You must select the **Warning Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 33.

Critical

When the voltage drops below or exceeds a specified voltage range, a voltage alert is sent to configured remote alert recipients, and the server begins the shutdown process with an orderly operating-system shutdown. The server then turns itself off. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 33.

Fatal When the voltage drops below or exceeds a specified voltage range, the server immediately shuts down and sends an alert to configured remote alert recipients. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

Note: The hard shutdown alert is sent only if a soft shutdown alert has not yet been sent.

For more information about selecting alert options, see the "Configuring SNMP alert settings" on page 33.

The IMM generates a non-critical or critical event when the threshold is reached, and generates any shutdown actions, if they are required.

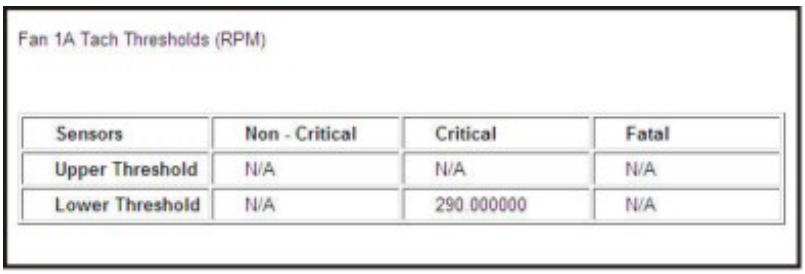
Non-critical

If the IMM indicates that this threshold has been reached, a warning event is generated.

Critical

If the IMM indicates that this threshold has been reached, a critical event is generated.

5. Scroll down to the **Fan Speeds (% of max)** area. The IMM web interface displays the running speed of the server fans (expressed in a percentage of the maximum fan speed). If you click a fan reading, a new window opens.



You receive a fan alert when the fan speeds drop to an unacceptable level or when the fans stop. You must select the **Critical Alerts** check box in the **SNMP Alerts Settings** area of the Alerts page for the alert to be sent.

For more information about selecting alert options, see "Configuring SNMP alert settings" on page 33.

6. Scroll down to the **View Latest OS Failure Screen** area. Click **View OS Failure Screen** to access an image of the operating-system-failure screen that was captured when the server stopped functioning.

Note:

The operating-system-failure screen capture feature is available only with IMM Premium. For information about upgrading from IMM Standard to IMM Premium, see "Upgrading from IMM Standard to IMM Premium" on page 5.

If an event occurs that causes the operating system to stop running, the operating-system watchdog is triggered, which causes the IMM to capture the operating-system-failure screen data and store it. The IMM stores only the most recent error event information, overwriting older operating-system-failure screen data when a new error event occurs.

To remotely access a server operating-system-failure screen image, complete the following steps:

a. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
b. In the navigation pane, click **System Health**, and then scroll down to the **View Latest OS Failure Screen** area.
c. Click **View OS Failure Screen**. The operating-system-failure screen image is displayed on your screen.

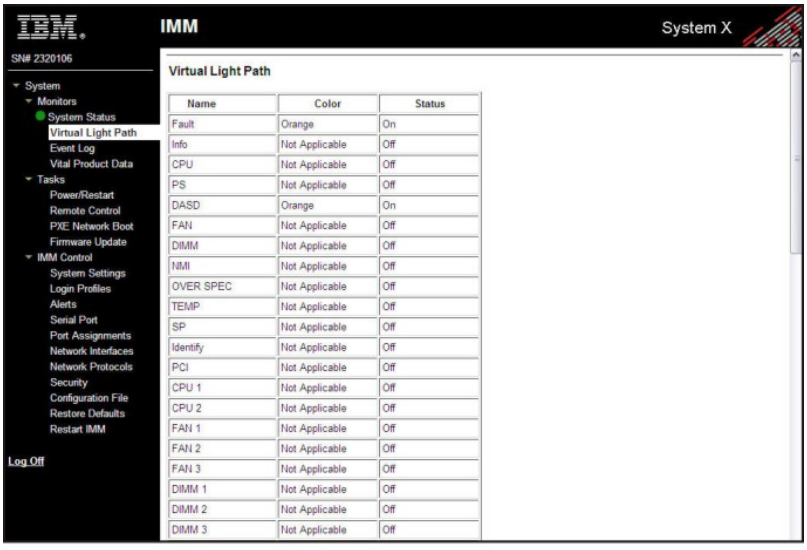
7. Scroll down to the **Users Currently Logged in** area. The IMM web interface displays the login ID and access method of each user who is logged in to the IMM.
8. Scroll down to the **System Locator LED** area. The IMM web interface displays the status of the system locator LED. It also provides buttons to change the state of the LED. For the meaning of the graphics that are displayed in this area, see the online help.

Viewing the Virtual Light Path

The Virtual Light Path screen displays the name, color, and status of any LEDs that are lit on the server.

To access and view the Virtual Light Path, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Virtual Light Path** to view the recent history of events on the server. A page similar to the one in the following illustration is displayed.



3. Scroll down to view the complete contents of the Virtual Light Path.

   Note: If an LED is not lit on the server, the Color column of the Virtual Light Path table indicates that the LED Color is Not Applicable.

Viewing the event logs

Note: For an explanation of a specific event or message, see your server documentation.
Error codes and messages are displayed in the following types of event logs:

- **System-event log:** This log contains POST and system management interrupt (SMI) events and all events that are generated by the BMC that is embedded in the IMM. You can view the system-event log through the Setup utility and through the Dynamic System Analysis (DSA) program (as the IPMI event log).

  The system-event log is limited in size. When it is full, new entries will not overwrite existing entries; therefore, you must periodically save and then clear

the system-event log through the Setup utility. When you are troubleshooting, you might have to save and then clear the system-event log to make the most recent events available for analysis.

Messages are listed on the left side of the screen, and details about the selected message are displayed on the right side of the screen. To move from one entry to the next, use the Up Arrow (↑) and Down Arrow (↓) keys.

The system-event log indicates an assertion event when an event has occurred. It indicates a deassertion event when the event is no longer occurring.

Some IMM sensors cause assertion events to be logged when their setpoints are reached. When a setpoint condition no longer exists, a corresponding deassertion event is logged. However, not all events are assertion-type events.

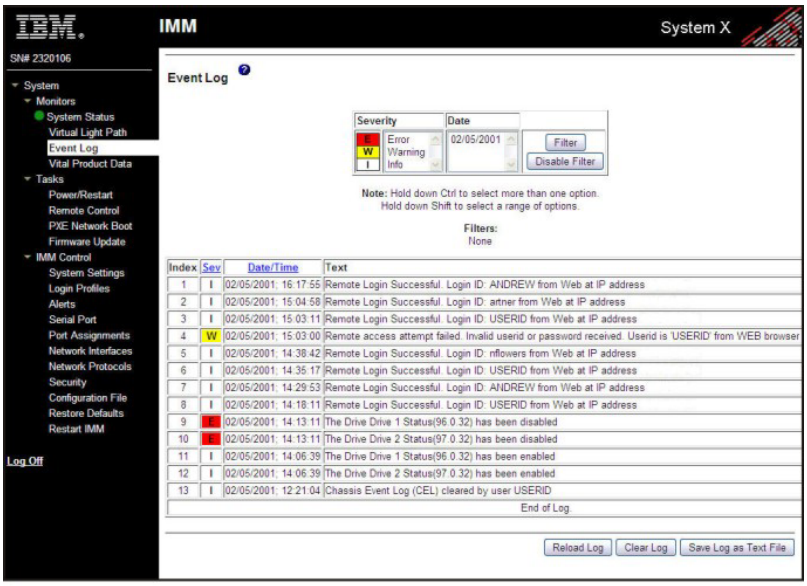
- **Integrated management module (IMM) event log:** This log contains a filtered subset of all IMM, POST, and system management interrupt (SMI) events. You can view the IMM event log through the IMM web interface and through the DSA program (as the ASM event log).
- **DSA log:** This log is generated by the DSA program, and it is a chronologically ordered merge of the system-event log (as the IPMI event log), the IMM chassis-event log (as the ASM event log), and the operating-system event logs. You can view the DSA log through the DSA program.
- **Chassis event log:** The IMM generates text messages for the IPMI assertion and deassertion events and creates entries for them in the chassis-event log. The text is generated for these events through the Distributed Management Task Force (DMTF) specifications DSP0244 and DSP8007. This log also contains entries for events other than IPMI sensor assertions and deassertions, For example, the chassis-event log includes entries when a user changes a network setting or when a user logs into the web interface. This log can be viewed from the IMM web interface.

Viewing the system-event log from the web interface

Note: The system-event log has a limited capacity. When that limit is reached, the older events are deleted in a first-in, first-out order.

To access and view the event log, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, “Opening and using the IMM web interface,” on page 11.
2. In the navigation pane, click **Event Log** to view the recent history of events on the server. A page similar to the one in the following illustration is displayed.



3. Scroll down to view the complete contents of the event log. The events are given the following levels of severity:

   Informational
   This severity level is assigned to an event of which you should take note.

   Warning
   This severity level is assigned to an event that might affect server performance.

   Error This severity level is assigned to an event that needs immediate attention.

   The IMM web interface distinguishes warning events with the letter W on a yellow background in the severity column and error events with the letter E on a red background.
4. Click **Save Log as Text File** to save the contents of the event log as a text file. Click **Reload Log** to refresh the display of the event log. Click **Clear Log** to delete the contents of the event log.

Viewing event logs from the Setup utility

For complete information about using the Setup utility, see the documentation that came with your server.

To view the POST event log or system-event log, complete the following steps:

1. Turn on the server.

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.
2. When the prompt `<F1> Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to view the event logs.
3. Select **System Event Logs** and use one of the following procedures:
   - To view the POST event log, select **POST Event Viewer**.
   - To view the system-event log, select **System Event Log**.

Viewing event logs without restarting the server

If the server is not hung, methods are available for you to view one or more event logs without having to restart the server.

If you have installed Portable or Installable Dynamic System Analysis (DSA), you can use it to view the system-event log (as the IPMI event log), the IMM event log (as the ASM event log), the operating-system event logs, or the merged DSA log. You can also use DSA Preboot to view these logs, although you must restart the server to use DSA Preboot. To install Portable DSA, Installable DSA, or DSA Preboot or to download a DSA Preboot CD image, go to http://www.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=SERV-DSA&brandind=5000008 or complete the following steps.

Note: Changes are made periodically to the IBM website. The actual procedure might vary slightly from what is described in this document.

1. Go to http://www.ibm.com/systems/support/.
2. Under **Product support**, click **System x**.
3. Under **Popular links**, click **Software and device drivers**.
4. Under **Related downloads**, click **Dynamic System Analysis (DSA)** to display the matrix of downloadable DSA files.

If IPMItool is installed in the server, you can use it to view the system-event log. Most recent versions of the Linux operating system come with a current version of IPMItool. For information about IPMItool, go to http://sourceforge.net/.

Note: Changes are made periodically to the IBM website. The actual procedure might vary slightly from what is described in this document.

1. Go to http://publib.boulder.ibm.com/infocenter/toolsctr/v1r0/index.jsp.
2. In the navigation pane, click **IBM System x and BladeCenter Tools Center**.
3. Expand **Tools reference**, expand **Configuration tools**, expand **IPMI tools**, and click **IPMItool**.

For an overview of IPMI, go to http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/liaai/ipmi/liaaiipmi.htm or complete the following steps:

1. Go to http://publib.boulder.ibm.com/infocenter/systems/index.jsp.
2. In the navigation pane, click **IBM Systems Information Center**.
3. Expand **Operating systems**, expand **Linux information**, expand **Blueprints for Linux on IBM systems**, and click **Using Intelligent Platform Management Interface (IPMI) on IBM Linux platforms**.

You can view the IMM event log through the **Event Log** link in the IMM web interface.

The following table describes the methods that you can use to view the event logs, depending on the condition of the server. The first two conditions generally do not require that you restart the server.

Table 16. Methods for viewing event logs

Condition	Action
The server is not hung and is connected to a network.	Use any of the following methods: • Run Portable or Installable DSA to view the event logs or create an output file that you can send to IBM service and support. • Type the IP address of the IMM and go to the Event Log page. • Use IPMItool to view the system-event log.
The server is not hung and is not connected to a network.	Use IPMItool locally to view the system-event log.
The server is hung.	• If DSA Preboot is installed, restart the server and press F2 to start DSA Preboot and view the event logs. • If DSA Preboot is not installed, insert the DSA Preboot CD and restart the server to start DSA Preboot and view the event logs. • Alternatively, you can restart the server and press F1 to start the Setup utility and view the POST event log or system-event log. For more information, see "Viewing event logs from the Setup utility" on page 99.

Viewing vital product data

When the server starts, the IMM collects server information, server firmware information, and server component vital product data (VPD) and stores it in nonvolatile memory. You can access this information at any time from almost any computer. The Vital Product Data page contains key information about the remote managed server that the IMM is monitoring.

To view the server component vital product data, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Vital Product Data** to view the status of the hardware and software components on the server.
3. Scroll down to view the following VPD readings:

   Machine level VPD

   The vital product data for the server appears in this area. For viewing VPD, the machine-level VPD includes a universal unique identifier (UUID).

   Note: The machine-level VPD, component-level VPD, and component activity log provide information only when the server is turned on.

Table 17. Machine-level vital product data

Field	Function
Machine type and model	Identifies the server type and model number that the IMM is monitoring.
Serial number	Identifies the serial number of the server that the IMM is monitoring.
UUID	Identifies the universal unique identifier (UUID), a 32-digit hexadecimal number, of the server that the IMM is monitoring.

Component Level VPD

The vital product data for the components of the remote managed server is displayed in this area.

Table 18. Component-level vital product data

Field	Function
FRU name	Identifies the field replaceable unit (FRU) for each component.
Serial number	Identifies the serial number of each component.
Mfg ID	Identifies the manufacturer ID for each component.

Component Activity Log

You can view a record of component activity in this area.

Table 19. Component activity log

Field	Function
FRU name	Identifies the field replaceable unit (FRU) name of the component.
Serial number	Identifies the serial number of the component.
Mfg ID	Identifies the manufacturer of the component.
Action	Identifies the action taken for each component.
Timestamp	Identifies the date and time of the component action. The date is displayed in the *mm/dd/yy* format. The time is displayed in the *hh:mm:ss* format.

IMM VPD

You can view the IMM firmware, System x server firmware, and Dynamic System Analysis firmware VPD for the remote-managed server in this area.

Table 20. IMM, UEFI, and DSA firmware vital product data

Field	Function
Firmware type	Indicates the type of firmware code.
Version string	Indicates the version of the firmware code.
Release date	Indicates when the firmware was released.

Chapter 5. Performing IMM tasks

Use the functions under the **Tasks** heading in the navigation pane to directly control the actions of the IMM and your server. The tasks that you can perform depend on the server in which the IMM is installed.

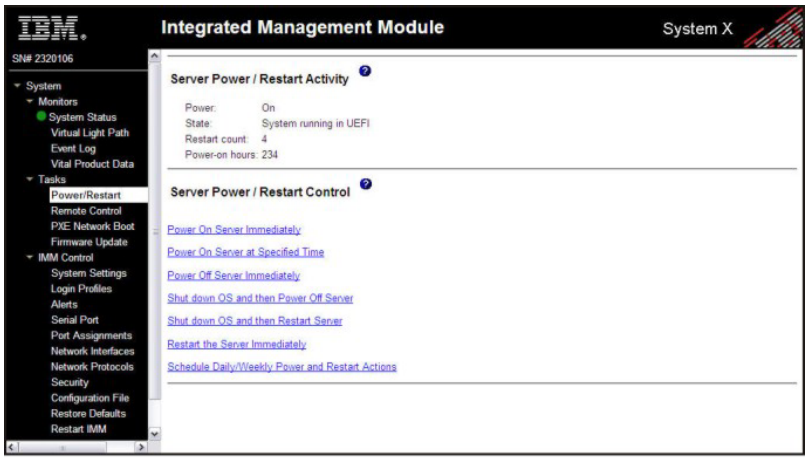
You can perform the following tasks:

- 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
- Update the IMM firmware

Note: Some features are available only on servers running a supported Microsoft Windows operating system.

Viewing server power and restart activity

The **Server Power/Restart Activity** area displays the power status of the server when the webpage was generated.



Power This field shows the power status of the server when the current webpage was generated.

State This field shows the state of the server when the current webpage was generated. The following states are possible:

- System power off/State unknown
- System on/starting UEFI
- System stopped in UEFI (Error detected)
- System running in UEFI
- Booting OS or in unsupported OS (might be in the operating system if the operating system is not configured to support the in-band interface to the IMM)
- OS booted

Restart count
This field shows the number of times that the server has been restarted.

Note: The counter is reset to zero each time the IMM subsystem is cleared to factory defaults.

Power-on hours
This field shows the total number of hours that the server has been turned on.

Controlling the power status of a server

The IMM provides full power control over your server with power-on, power-off, and restart actions. In addition, power-on and restart statistics are captured and displayed to show server hardware availability. To perform the actions in the **Server Power/Restart Control** area, you must have Supervisor access to the IMM.

To perform server power and restart actions, complete the following steps.

Note: Select the following options only in case of an emergency, or if you are offsite and the server is nonresponsive.

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **Power/Restart**. Scroll down to the **Server Power/Restart Control** area.
3. Click one of the following options:

Power on server immediately
Turn on the server and start the operating system.

Power on server at specified time
Turn on the server at a specified time and start the operating system.

Power off server immediately
Turn off the server without shutting down the operating system.

Shut down OS and then power off server
Shut down the operating system and then turn off the server.

Note: If the operating system is in screen saver or locked mode when a "Shut down OS and then power off server" request is attempted, the IMM might not be able to initiate a graceful shutdown. The IMM will perform a hard reset or shutdown after the power off delay interval expires, while the OS might still be up and running.

Shut down OS and then restart server
Restart the operating system.

Note: If the operating system is in screen saver or locked mode when a "Shut down OS and then restart server" request is attempted, the IMM might not be able to initiate a graceful shutdown. The IMM will perform a hard reset or shutdown after the power off delay interval expires, while the OS might still be up and running.

Restart the server immediately
Turn off and then turn on the server immediately without first shutting down the operating system.

Schedule daily/weekly power and restart actions

Shut down the operating system, turn off the server at a specified daily or weekly time (with or without restarting the server), and turn on the server at a specified daily or weekly time.

A confirmation message is displayed if you select any of these options, and you can cancel the operation if it was selected accidentally.

Remote presence

Note:

1. The IMM remote presence function is available only in IMM Premium. For more information about upgrading from IMM Standard to IMM Premium, see "Upgrading from IMM Standard to IMM Premium" on page 5.
2. The remote control feature is available only through the IMM web interface. You must log in to the IMM with a user ID that has Supervisor access to use any of the remote control features.

You can use the remote presence function, or remote control feature in the IMM web interface, to view and interact with the server console. You can also assign to the server a CD or DVD drive, diskette drive, USB flash drive, or disk image that is on your computer.

The remote control feature provides the following functions:

- Remotely viewing video with graphics resolutions up to 1280 x 1024 at 75 Hz, regardless of the server state
- Remotely accessing the server, using the keyboard and mouse from a remote client
- Mapping the CD or DVD drive, diskette drive, and USB flash drive on a remote client, and mapping ISO and diskette image files as virtual drives that are available for use by the server
- Uploading a diskette image to the IMM memory and mapping it to the server as a virtual drive

Updating your IMM firmware and Java or ActiveX applet

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

To correct this problem, complete the following steps:

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

For more information about updating IMM firmware, see “Updating firmware” on page 115.

Enabling the remote presence function

Note: The IMM remote presence function is available only in IMM Premium. For more information about upgrading from IMM Standard to IMM Premium, see “Upgrading from IMM Standard to IMM Premium” on page 5.

To enable the remote presence feature, complete the following steps:

1. Disconnect power from the server by unplugging the power cord.
2. Install the virtual media key into the dedicated slot on the system board.
3. Reconnect power to the server.

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.
4. Turn on the server.

Remote control

The remote control feature of IMM consists of two Java applications in two separate windows:

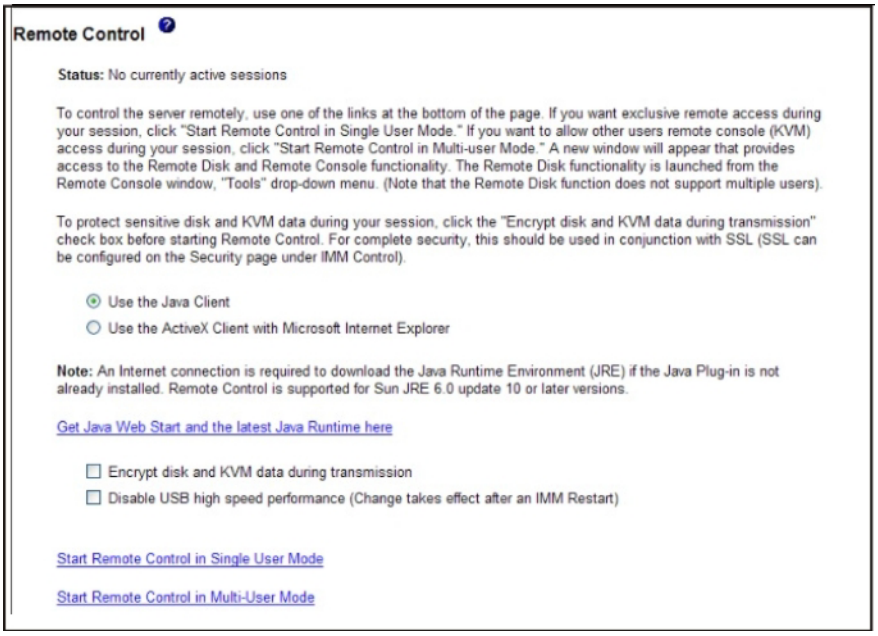
Video Viewer
The Video Viewer uses a remote console for remote systems management. A remote console is an interactive graphical user interface (GUI) display of the server, viewed on your computer. You see on your monitor exactly what is on the server console, and you have keyboard and mouse control of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

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

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

1. Log in to the IMM. For more information, see Chapter 2, “Opening and using the IMM web interface,” on page 11.

2. In the navigation pane, click **Remote Control**. A page similar to the one in the following illustration is displayed.



3. Choose one of the following options:
   - Click **Use the Java Client** to use the Java applet to perform the remote presence.
   - Click **Use the ActiveX Client with Microsoft Internet Explorer** to use the Internet Explorer in Windows Operating Systems and you want to use the ActiveX applet to perform the remote presence function.

     Note: The 32-bit ActiveX Remote Presence Client is available with IMM firmware version 1.28 or later. The 64-bit ActiveX Client is available with IMM firmware version 1.30 or later.
4. To control the server remotely, use one of the links at the bottom of the Remote Control page. If you want exclusive remote access during your session, click **Start Remote Control in Single User Mode**. If you want to allow other users remote console (KVM) access during your session, click **Start Remote Control in Multi-user Mode**. New windows open that provide access to the Remote Disk and Remote Console functionality.

   If the **Encrypt disk and KVM data during transmission** check box was selected before the Remote Control window was opened, the disk data is encrypted with ADES encryption.

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

Notes:

1. Do not close the Virtual Media Session window if a remote disk is currently mapped. See “Remote disk” on page 113 for instructions about closing and unmapping a remote disk.
2. If you have mouse or keyboard problems when you use Remote Control, see the help that is available from the Remote Control page in the web interface.
3. If you use the remote console to change settings for the IMM in the Setup utility program, the server might restart the IMM. You will lose the remote

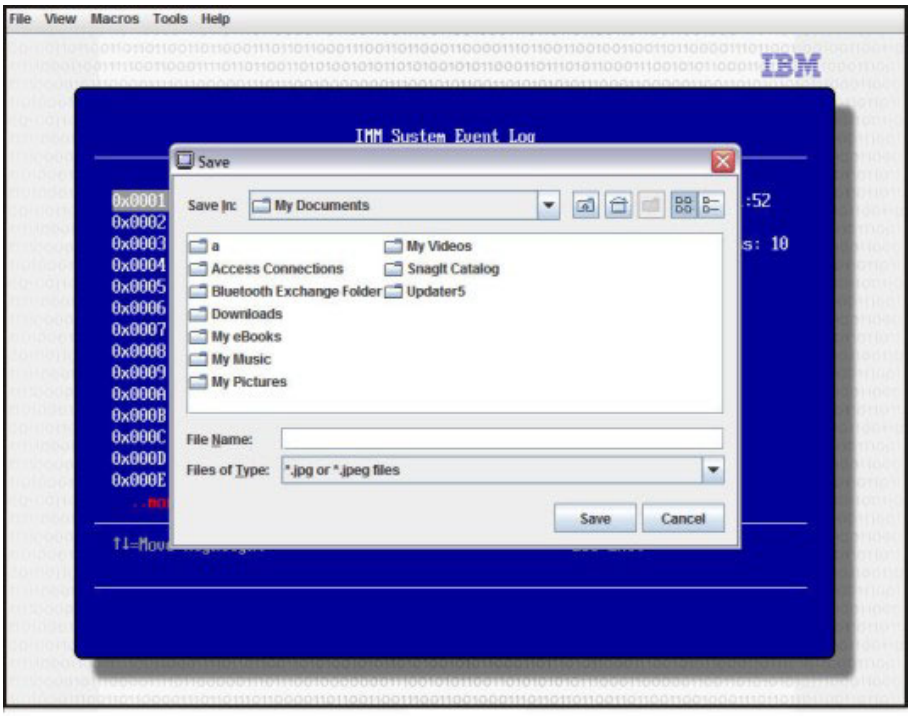
console and the login session. After a short delay you can log in to the IMM again with a new session, start the remote console again, and exit the Setup utility program.

Remote control screen capture

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

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

Note: Screen capture images are saved as JPG or JPEG file types.



Remote control Video Viewer view modes

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

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

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

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

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

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

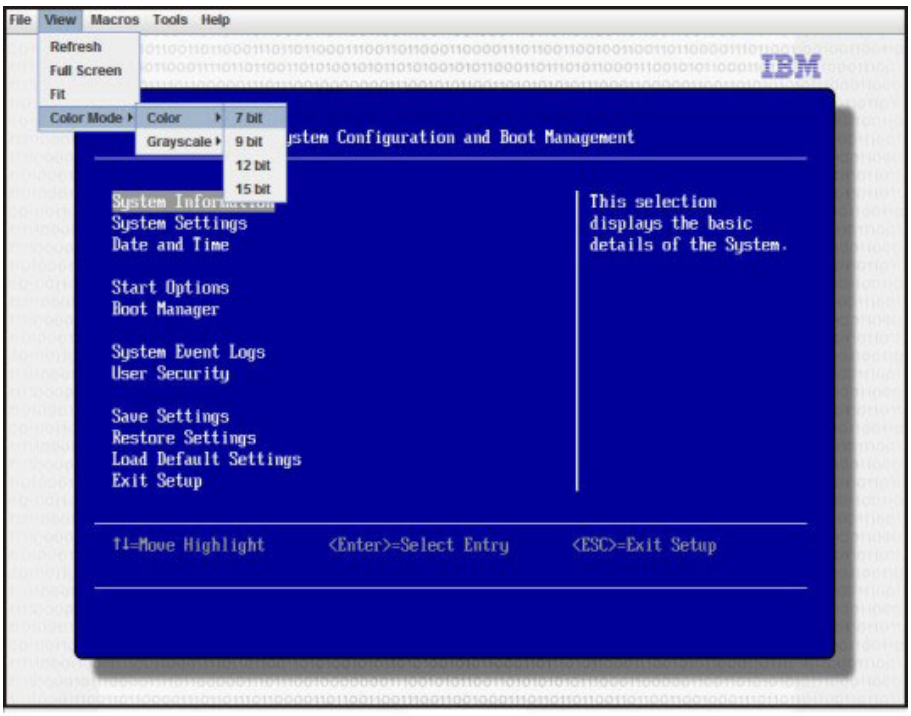
Remote control video color mode

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

Note: Instead of the bandwidth slider in the Remote Supervisor Adapter II interface, the IMM has a menu item that allows color depth adjustment to reduce the data that is transmitted in low-bandwidth situations.

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

1. In the Video Viewer window, click **View**.
2. When you move the mouse pointer over **Color Mode** in the menu, two color-mode choices are displayed:
   - Color: 7, 9, 12, and 15-bit
   - Grayscale: 16, 32, 64, 128 shades

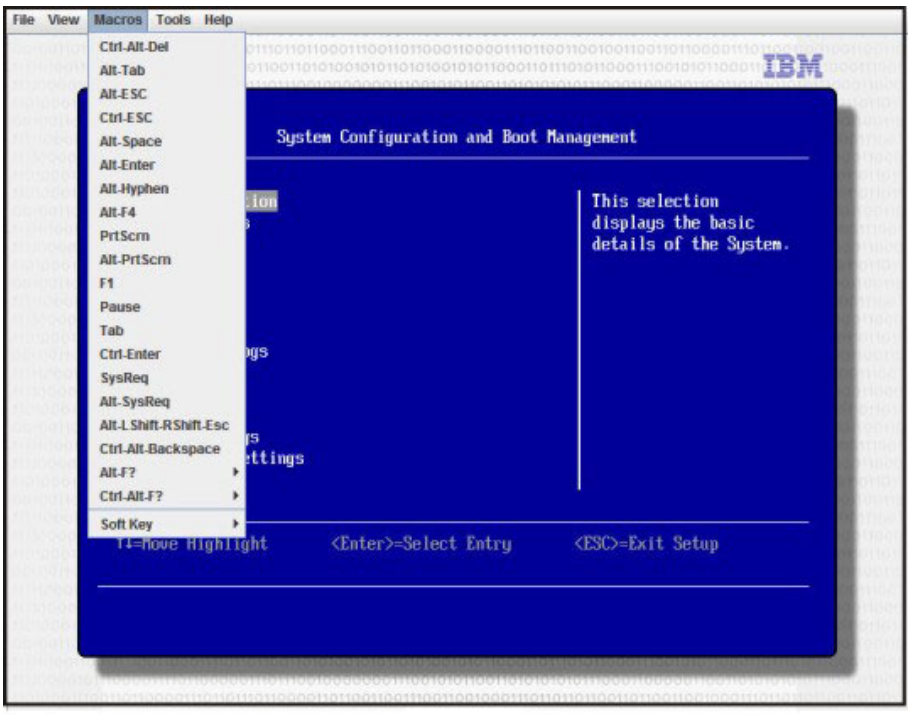


3. Select the color or grayscale setting.

Remote control keyboard support

The operating system on the client server that you are using traps certain key combinations, such as Ctrl+Alt+Del in Microsoft Windows, instead of transmitting them to the server. Other keys, such as F1, might cause an action on your computer as well as on the server. To use key combinations that affect the remote server, and not the local client, complete the following steps:

1. In the Video Viewer window, click **Macros**.
2. Select one of the predefined key combinations from the menu, or select **Soft Key** to choose or add a user-defined key combinations.



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

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

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

International keyboard support

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

Keyboard pass-through mode

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

Some operating systems define certain keystrokes to be outside the control of an application, so the behavior of the pass-through mechanism operates independently of the server. For example, in a Linux X session, the Ctrl+Alt+F2 keystroke combination switches to virtual console 2. There is no mechanism to

intercept this keystroke sequence and, therefore, no way for the client to pass these keystrokes directly to the target. The only option in this case is to use the keyboard macros defined for this purpose.

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

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

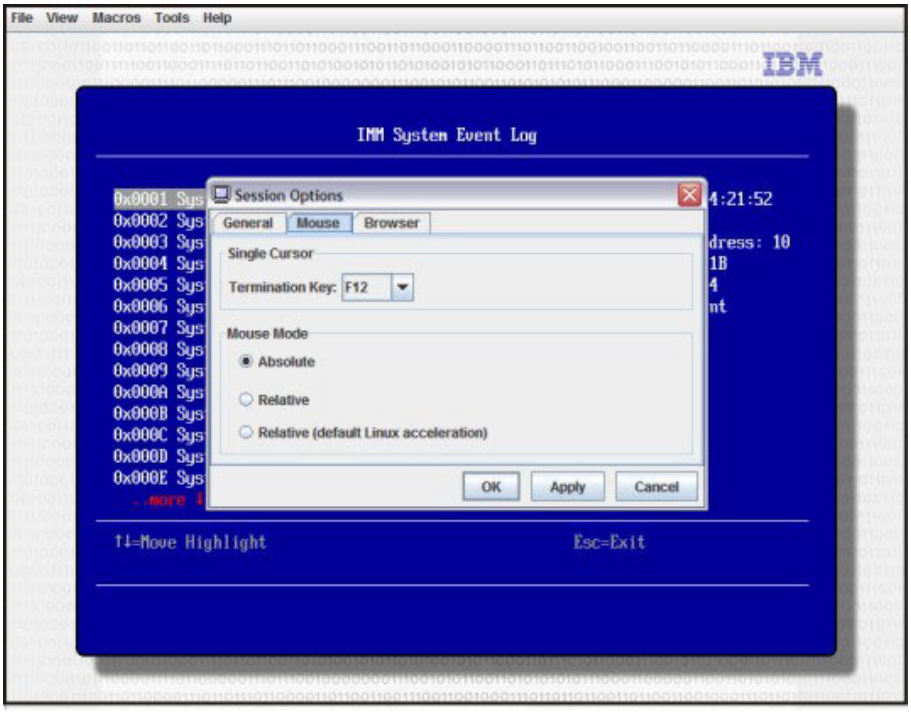
Remote control mouse support

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

Absolute and relative mouse control

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

1. In the Remote Control window, click **Tools**.
2. Select **Session Options** from the menu.
3. When the Session Options window is displayed, click the **Mouse** tab.



4. Select one of the following mouse modes:

Absolute

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

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

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

Single cursor mode

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

To enable single cursor mode, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Select **Single Cursor**.

When the Video Viewer is in single cursor mode, you cannot use the mouse to switch to another window or otherwise click outside the KVM client window, because there is no local cursor. To disable single cursor mode, press the defined termination key. To view the defined termination key, or change the termination key, click **Tools > Session Options > Mouse**.

Remote power control

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

1. In the Video Viewer window, click **Tools**.
2. When you move the mouse pointer over **Power** in the menu, these choices are displayed:

   On Turns on the server power.

   Off Turns off the server power.

   Reboot
   Restarts the server.

   Cycle Turns the server power off, then back on.

Viewing performance statistics

To view the Video Viewer performance statistics, complete the following steps:

1. In the Video Viewer window, click **Tools**.
2. Click **Stats**. The following information is displayed:

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

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

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

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

Starting Remote Desktop Protocol

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

Remote disk

From the Virtual Media Session window, you can assign to the server a CD or DVD drive, a diskette drive, or a 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 use the Remote Control feature to access the remote disk. Drives and disk images are displayed as USB drives on the server.

Notes:

1. The following server operating systems have USB support, which is required for the Remote Disk feature:
   - Microsoft Windows Server 2008
   - Microsoft Windows Server 2003
   - Red Hat Linux versions 4.0 and 5.0
   - SUSE Linux version 10.0
   - Novell NetWare 6.5
2. The client server requires the Java 1.5 Plug-in or later.
3. The client server must have an Intel Pentium III microprocessor or greater, operating at 700 MHz or faster, or equivalent.

Accessing the Remote Control

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

1. Log in to the IMM. For more information, see Chapter 2, “Opening and using the IMM web interface,” on page 11.
2. In the navigation pane, click **Remote Control**.
3. On the Remote Control page, click one of the **Start Remote Control** options:
   - If you want exclusive remote access during your session, click **Start Remote Control in Single User Mode**.
   - If you want to allow other users to have remote console (KVM) access during your session, click **Start Remote Control in Multi-user Mode**.

   The Video Viewer window opens.
4. To open a Virtual Media Session window, click **Tools** > **Launch Virtual Media** in the Video Viewer window.

Note: If the **Encrypt disk and KVM data during transmission** check box was selected before the Remote Control window was opened, the disk data is encrypted with ADES encryption.

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

Mapping and unmapping drives with IMM firmware version 1.03 and later

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

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

Click the **Mount Selected** button to mount and map the selected drive or drives.

If you click **Add Image**, diskette image files and ISO image files can be added to the list of available drives. After the diskette or ISO image file is listed in the Virtual Media Session window, it can be mapped just like the other drives.

To unmap the drives, click the **Unmount All** button. Before the drives are unmapped, you must confirm that you want the drives to be unmapped.

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

You can select a diskette image file and save the diskette image in IMM memory. This enables the disk to remain mounted on the server so that you can access the disk later, even after the IMM web interface session has ended. A maximum of one drive image can be stored on the IMM card. The drive or image contents must be 1.44 MB or smaller. To upload a diskette image file, complete the following steps:

1. Click **RDOC**.
2. When the new window opens, click **Upload**.
3. Click **Browse** to select the image file that you want to use.
4. In the **Name** field, enter a name for the image and click **OK** to upload the file.

   Note: To unload the image file from memory, select the name in the RDOC Setup window and click **Delete**.

Mapping and unmapping drives with IMM firmware version 1.02 and earlier

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

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

If you click **Add Image**, diskette image files and ISO image files can be added to the list of available drives. After the diskette or ISO image file is listed in the Virtual Media Session window, it can be mapped just like the other drives.

To unmap a drive, clear the **Mapped** check box for the drive. Before the drive is unmapped, you must confirm that you want the drive to be unmapped.

You can select a diskette image file and save the diskette image in IMM memory. This enables the disk to remain mounted on the server so that you can access the disk later, even after the IMM web interface session has ended. A maximum of one drive image can be stored on the IMM card. The drive or image contents must be 1.44 MB or smaller. To upload a diskette image file, complete the following steps:

1. Click **RDOC**.
2. When the new window opens, click **Upload**.
3. Click **Browse** to select the image file that you want to use.
4. In the **Name** field, enter a name for the image and click **OK** to upload the file.

   Note: To unload the image file from memory, select the name in the RDOC Setup window and click **Delete**.

Exiting Remote Control

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

Setting up PXE network boot

To set up your server to attempt a Preboot Execution Environment (PXE) network boot at the next server restart, complete the following steps:

1. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
2. In the navigation pane, click **PXE Network Boot**.
3. Select the **Attempt PXE network boot at next server restart** check box.
4. Click **Save**.

Updating firmware

Use the Firmware Update option on the navigation pane to update the IMM firmware, System x server firmware, and Dynamic System Analysis (DSA) firmware.

To update the firmware, complete the following steps.

Note: Changes are made periodically to the IBM website. The actual procedure might vary slightly from what is described in this document.

1. Download the latest firmware update applicable for the server in which the IMM is installed:
   a. Go to http://www.ibm.com/systems/support/.
   b. Under **Product support**, click either **System x** or **BladeCenter**.
   c. Under **Popular links**, click **Software and device drivers**.
   d. Click the applicable link for your server to display the matrix of downloadable files.
   e. Scroll to the IMM, server firmware, or DSA area, select the link for the firmware update, and save the update file.
2. Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM web interface," on page 11.
3. In the navigation pane, click **Firmware Update**.
4. Click **Browse**.
5. Navigate to the update package that you want to update.

Note:

a. The System x server firmware cannot be updated while the server is turned off or while the server is starting.

b. To determine the type of firmware file to use, see the update package readme file. In most cases, the IMM can use either the EXE or BIN file to perform the update.

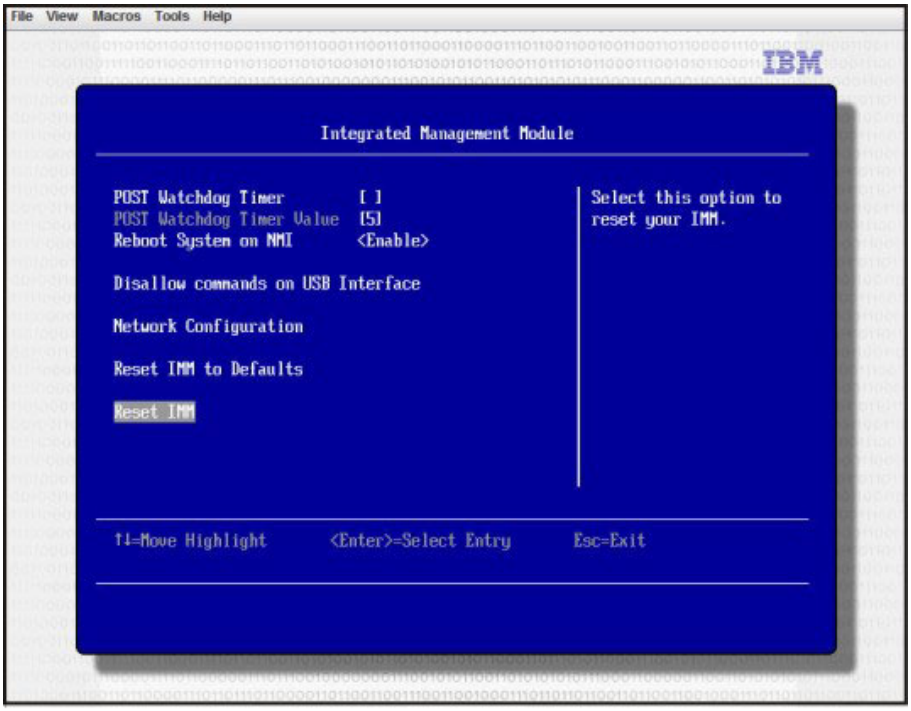
6. Click **Open**. The file (including the full path) is displayed in the box next to **Browse**.
7. To begin the update process, click **Update**. A progress indicator opens as the file is transferred to temporary storage on the IMM. A confirmation window opens when the file transfer is completed.
8. Verify that the file that is shown on the Confirm Firmware Update window is what you intend to update. If it is not, click **Cancel**.
9. To complete the update process, click **Continue**. A progress indicator opens as the firmware is updated. A confirmation window opens to verify that the update was successful.
10. If you are updating the IMM firmware, click **Restart IMM** in the navigation pane and then click **Restart**. The System x server firmware and DSA updates do not require that the IMM be restarted. These updates take effect the next time that the server is started.
11. Click **OK** to confirm that you want to restart the IMM.
12. Click **OK** to close the current browser window.
13. After the IMM restarts, log in to the IMM again to access the web interface.

Resetting the IMM with the Setup utility

To reset the IMM through the Setup utility, complete the following steps:

1. Turn on the server.

   Note: Approximately 2 minutes after the server is connected to ac power, the power-control button becomes active.
2. When the prompt `F1 Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to access the full Setup utility menu.
3. From the Setup utility main menu, select **System Settings**.
4. On the next screen, select **Integrated Management Module**.
5. Select **Reset IMM**.



Note: After you reset the IMM, this confirmation message is displayed immediately:

```
IMM reset command has been sent successfully!! Press ENTER to continue.
```

The IMM reset process is not yet complete. You must wait approximately 4 minutes for the IMM to reset before the IMM is functional again. If you attempt to access sever firmware information while the server is resetting, `Unknown` is displayed in the fields, and the description is `Error retrieving information from IMM`.

Managing tools and utilities with IMM and IBM System x Server Firmware

This section describes the tools and utilities that are supported by IMM and IBM System x Server Firmware. The IBM tools that you use to manage the IMM in-band do not require you to install device drivers. However, if you choose to use certain tools such as IPMItool in-band, you must install the OpenIPMI drivers.

Updates and downloads for IBM systems-management tools and utilities are available on the IBM website. To check for updates to tools and utilities, complete the following steps.

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

1. Go to http://www.ibm.com/systems/support/.
2. Under **Product support**, click **System x**.
3. Under **Popular links**, click **Utilities**.

Using IPMItool

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

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

Using OSA System Management Bridge

OSA System Management Bridge (SMBridge) is a tool that can be used to manage servers remotely. You can use it to administer servers using IPMI 1.5 and Serial over LAN (SOL) protocols.

For more information about SMBridge, go to http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-62198&brandind=5000008 or complete the following steps:

1. Go to http://www.ibm.com/systems/support/.
2. Click **System x**.
3. Under **Support & downloads**, click **Search**.
4. Type `smbridge` in the search field and click **Search**.
5. From the list of results, click the link **SMBridge Tool Help - Servers**.

Using IBM Advanced Settings Utility

IBM Advanced Settings Utility (ASU) version 3.0.0 or later is required to manage IMM. ASU is a tool that you can use to modify firmware settings from the command-line interface on multiple operating-system platforms. It also enables you to issue selected IMM setup commands. You can use ASU in-band or out-of-band to manage and configure the IMM.

Note: If the USB in-band interface (LAN over USB) is disabled, ASU requires the installation of IPMI device drivers.

For more information about the ASU, see http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lndocid=MIGR-55021&brandind=5000008, or complete the following steps:

1. Go to http://www.ibm.com/systems/support/.
2. Click **System x**, select your server from the **Product family** menu, and click **Go**.
3. From the **Refine results** menu, select **Advanced Settings Utility** and click **Go**.
4. Click the link to the latest version of the ASU.

Using IBM Flash utilities

A flash utility enables you to update hardware and server firmware and eliminates the need to manually install new firmware or firmware updates from a physical diskette or other medium. You can use IBM flash utilities for IMM, server firmware, and DSA either in-band or out-of-band. To find a flash utility, complete the following steps:

1. Go to http://www.ibm.com/systems/support/.
2. Under **Product support**, click **System x**.
3. Type `flash utility` in the search field and click **Search**.
4. Click the link to the applicable flash utility.

Other methods for managing the IMM

You can use the following user interfaces to manage and configure the IMM:

- IMM web interface
- SNMPv1
- SNMPv3
- Telnet CLI
- SSH CLI

Chapter 6. LAN over USB

Unlike the BMC and Remote Supervisor Adapter II, the IMM does not require IPMI device drivers or USB daemons for in-band IMM communication. Instead, a LAN over USB interface enables in-band communications to the IMM; the IMM hardware on the system board presents an internal Ethernet NIC from the IMM to the operating system.

Note: LAN over USB is also called the "USB in-band interface" in the IMM web interface.

The IMM IP address for the LAN over USB interface is set to a static address of 169.254.95.118 with a subnet mask of 255.255.0.0. The only exception is for the IMM in the Secondary Node of a multi-node system (for example, x3850 X5 or x3950 X5) where the IMM side IP address of the LAN over USB interface is 169.254.96.118.

Potential conflicts with the LAN over USB interface

In some situations, the IMM LAN over USB interface can conflict with certain network configurations, applications, or both. For example, Open MPI attempts to use all of the available network interfaces on a server. Open MPI detects the IMM LAN over USB interface and attempts to use it to communicate with other systems in a clustered environment. The LAN over USB interface is an internal interface, so this interface does not work for external communications with other systems in the cluster.

Resolving conflicts with the IMM LAN over USB interface

There are several actions that resolve LAN over USB conflicts with network configurations and applications:

- For conflicts with Open MPI, configure the application so that it does not attempt to use the interface.
- Take the interface down (run `ifdown` under Linux).
- Remove the device driver (run `rmmod` under Linux).
- Disable the USB in-band interface on the IMM through either of the following methods.

  Important: If you disable the USB in-band interface, you cannot perform an in-band update of the IMM firmware by using the Linux or Windows flash utilities. If the USB in-band interface is disabled, use the Firmware Update option on the IMM web interface to update the firmware. For more information, see "Updating firmware" on page 115.

  If you disable the USB in-band interface, also disable the watchdog timeouts to prevent the server from restarting unexpectedly. For more information about disabling the watchdogs, see "Setting server timeouts" on page 21.

  – To disable the LAN over USB interface from the IMM web interface, see "Disabling the USB in-band interface" on page 23.
  – To disable the LAN over USB interface from the advanced management module web interface, complete the following steps:
    1. Log in to the advanced management module web interface.

2. In the navigation pane, click **Blade Configuration** under the **Blade Tasks** heading.
3. Scroll down to the service processor LAN over USB interface on the Blade Configuration webpage. The section lists all blade servers in the chassis that are capable of enabling and disabling the LAN over USB interface.
4. Select the check boxes next to the blade servers that you want to enable or disable.
5. Click **Disable** to disable the LAN over USB interface on the selected blade servers.

Configuring the LAN over USB interface manually

For the IMM to use the LAN over USB interface, you might have to complete other configuration tasks if the automatic setup fails or if you prefer to set up the LAN over USB manually. The firmware update package or Advanced Settings Utility (ASU) attempts to perform the setup automatically. For more information about LAN over USB configuration on different operating systems, see the IBM white paper *Transitioning to UEFI and IMM* on the IBM website.

Installing device drivers

For the IMM to use the LAN over USB interface, you might have to install operating-system drivers. If the automatic setup fails or if you prefer to set up the LAN over USB manually, use one of the following procedures. For more information about LAN over USB configuration on different operating systems, see the IBM white paper *Transitioning to UEFI and IMM* on the IBM website.

Installing the Windows IPMI device driver

The Microsoft IPMI device driver is not installed by default on Microsoft Windows Server 2003 R2 operating systems. To install the Microsoft IPMI device driver, complete the following steps:

1. From the Windows desktop, click **Start > Control Panel > Add or Remove Programs**.
2. Click **Add/Remove Windows Components**.
3. From the component list, select **Management and Monitoring Tools**, and then click **Details**.
4. Select **Hardware Management**.
5. Click **Next**. The installation wizard opens and guides you through the installation.

   Note: The Windows installation CD might be required.

Installing the LAN over USB Windows device driver

When you install Windows, an unknown RNDIS device is shown in the Device Manager. You must install a Windows INF file that identifies this device and is required by Windows operating system to detect and use the LAN over USB functionality. The signed version of the INF is included in all of the Windows versions of the IMM, UEFI, and DSA update packages. The file needs to be installed only once. To install the Windows INF file, complete the following steps:

1. Obtain a Windows version of the IMM, server firmware, or DSA update package (see "Updating firmware" on page 115 for more information).

2. Extract the ibm_rndis_server_os.inf and device.cat files from the firmware update package and copy them to the \WINDOWS\inf subdirectory.
3. **For Windows 2003**: Install the ibm_rndis_server_os.inf file by right-clicking on the file and selecting **Install**. This generates a PNF file of the same name in \WINDOWS\inf. **For Windows 2008**: Go to **Computer Management**, then **Device Manager** and locate the RNDIS Device. Select **Properties > Driver > Reinstall driver**. Point the server to the \Windows\inf directory, where it can locate the ibm_rndis_server_os.inf file and install the device.
4. Go to **Computer Management**, then **Device Manager**, right-click **Network adapters**, and select **Scan for hardware changes**. A message confirms that the Ethernet device is found and installed. The New Hardware Wizard starts automatically.
5. When you are prompted Can Windows connect to Windows Update to search for software?, click **No, not this time**. Click **Next** to continue.
6. When you are prompted What do you want the wizard to do?, click **Install from a list or specific location (Advanced)**. Click **Next** to continue.
7. When you are prompted Please choose your search and installation options, click **Don't search. I will choose the driver to install**. Click **Next** to continue.
8. When you are prompted Select a hardware type, and then click Next, click **Network adapters**. Click **Next** to continue.
9. When you are prompted Completing the Found New Hardware Wizard, click **Finish**.

   Note: A new local area connection is displayed and might state This connection has limited or no connectivity. Ignore this message.
10. Go back to the Device Manager. Verify that **IBM USB Remote NDIS Network Device** appears under **Network Adapters**.
11. Open a command prompt, type ipconfig, and press Enter. The local area connection for the IBM USB RNDIS is displayed with an IP address in the range of 169.254.*xxx.xxx* with a subnet mask set to 255.255.0.0.

Installing the LAN over USB Linux device driver

Current versions of Linux, such as RHEL5 Update 2 and SLES10 Service Pack 2, support the LAN over USB interface by default. This interface is detected and displayed during the installation of these operating systems. When you configure the device, use a static IP address of 169.254.95.130 with a subnet mask of 255.255.0.0.

Note: Older Linux distributions might not detect the LAN over USB interface and might require manual configuration. For information about configuring LAN over USB on specific Linux distributions, see the IBM white paper *Transitioning to UEFI and IMM* on the IBM website.

The IMM LAN over USB interface requires that the usbnet and cdc_ether device drivers be loaded. If the device drivers have not been installed, use the modprobe command to install them. When these device drivers are installed, the IMM USB network interface is shown as a network device in the operating system. To discover the name that the operating system has assigned to the IMM USB network interface, type:

```
dmesg | grep -i cdc ether
```

Use the ifconfig command to configure the interface to have an IP address in the range 169.254.*xxx.xxx*. For example:

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

This interface is configured to have an IP address in the 169.254.*xxx.xxx* range each time that the operating system is started.

Chapter 7. Command-line interface

Use the IMM command-line interface (CLI) to access the IMM 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 IMM before you can issue any CLI commands.

Managing the IMM with IPMI

The IMM comes with User ID 2 set initially to a user name of USERID and password of PASSW0RD (with a zero, not the letter O). This user has Supervisor access.

Important: Change this default password during your initial configuration for enhanced security.

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

Command-line interfaces

The command-line interface provides direct access to server-management functions through the IPMI 2.0 protocol. You can use SMBridge or IPMItool to issue commands to control server power, view server information, and identify the server. With SMBridge, you can also save one or more commands in a text file and run the file as a script. For more information about IPMItool, see "Using IPMItool" on page 118. For more information about SMBridge, see "Using OSA System Management Bridge" on page 118.

Serial over LAN

To manage servers from a remote location, use SMBridge or IPMItool to establish a Serial over LAN (SOL) connection. For more information about IPMItool, see "Using IPMItool" on page 118. For more information about SMBridge, see "Using OSA System Management Bridge" on page 118.

Accessing the command line

To access the command line, start a Telnet or SSH session to the IMM IP address (see "Configuring serial-to-Telnet or SSH redirection" on page 34 for more information).

Logging in to the command-line session

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

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

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

Command syntax

Read the following guidelines before you use the commands:

- Each command has the following format:

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

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

  where **ifconfig** is the command, eth0 is an argument, and -i, -g, and -s are options. In this example, all three options have arguments.
- Brackets indicate that an argument or option is optional. Brackets are not part of the command that you type.

Features and limitations

The CLI has the following features and limitations:

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

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

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

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

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

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

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

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

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

Utility commands

The utility commands are as follows:

- exit
- help
- history

exit command

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

help command

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

history command

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

Example:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Monitor commands

The monitor commands are as follows:

- clearlog
- fans
- readlog
- syshealth
- temps
- volts
- vpd

clearlog command

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

fans command

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

Example:

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

readlog command

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

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

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

Syntax:

```
readlog [options]
option:
-f
```

Example:

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

syshealth command

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

Example:

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

temps command

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

Example:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
        WR      W       T      SS      HS
---------------------------------------
CPU1   65/18  72/22  80/27  85/29  90/32
CPU2   58/14  72/22  80/27  85/29  9/320
DASD1  66/19  73/23  82/28  88/31  9/332
Amb    59/15  70/21  83/28  90/32  9/355
system>
```

Notes:

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

volts command

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

Example:

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

Note: The output has the following column headings:

HSL: hard shutdown low

SSL: soft shutdown low

WL: warning low

WRL: warning reset low

V: voltage (current value)

WRH: warning reset high

WH: warning high

SSH: soft shutdown high

HSH: hard shutdown high

vpd command

Use the **vpd** command to display vital product data for the system (sys), IMM, server firmware (bios), and Dynamic System Analysis Preboot (dsa). The same information is displayed as in the web interface.

Syntax:

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

Example:

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

Server power and restart control commands

The server power and restart commands are as follows:

- power
- reset

power command

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

power on turns on the server power.

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

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

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

Syntax:

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

reset command

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

Syntax:

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

Serial redirect command

There is one serial redirect command: console.

console command

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

Syntax:

```
console 1
```

Configuration commands

The configuration commands are as follows:

- dhcpinfo
- dns
- gprofile
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts

- usbeth
- users

dhcpinfo command

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

Syntax:

```
dhcpinfo eth0
```

Example:

```
system> dhcpinfo eth0

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

The following table describes the output from the example.

Option	Description
-server	DHCP server that assigned the configuration
-n	Assigned host name
-i	Assigned IPv4 address
-g	Assigned gateway address
-s	Assigned subnet mask
-d	Assigned domain name
-dns1	Primary IPv4 DNS server IP address
-dns2	Secondary IPv4 DNS IP address
-dns3	Tertiary IPv4 DNS server IP address
-i6	IPv6 address
-d6	IPv6 domain name
-dns61	Primary IPv6 DNS server IP address
-dns62	Secondary IPv6 DNS IP address
-dns63	Tertiary IPv6 DNS server IP address

dns command

Use the **dns** command to view the DNS configuration of the IMM.

Syntax:

```
dns
```

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

Example:

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

system>
```

The following table describes the output from the example.

Option	Description
-state	State of DNS (`enabled` or `disabled`)
-i1	Primary IPv4 DNS server IP address
-i2	Secondary IPv4 DNS IP address
-i3	Tertiary IPv4 DNS server IP address
-i61	Primary IPv6 DNS server IP address
-i62	Secondary IPv6 DNS IP address
-i63	Tertiary IPv6 DNS server IP address
-ddns	State of DDNS (`enabled` or `disabled`)
-dnsrc	Preferred DDNS domain name (`dhcp` or `manual`)
-p	Preferred DNS servers (`ipv4` or `ipv6`)

gprofile command

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

The following table shows the arguments for the options.

Option	Description	Values
-clear	Deletes a group	Enabled, disabled
-n	The name of the group	String of up to 63 characters for *group_name*. The *group_name* must be unique.
-a	Role-based security (authority) level	Supervisor, operator, rbs <role list>: ns | uam | rca | rcrda | rpr | bac | ce | aac Role list values are specified using a pipe separated list of values.
-h	Displays the command usage and options	

Syntax:

```
gprofile [1 - 16] [options]
options:
-clear state
-n  group_name
-a  security level:
    -ns network and security
    -uam user account management
    -rca remote console access
    -rcrda remote console and remote disk access
    -rpr remote server power/restart access
    -bac basic adapter configuration
    -ce ability to clear event logs
    -aac advanced adapter configuration
-h
```

ifconfig command

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

The following table shows the arguments for the options.

Option	Description	Values
-state	Interface state	disabled, enabled
-c	Configuration method	dhcp, static, dthens (dthens corresponds to the **try dhcp server, if it fails use static config** option on the web interface)
-i	Static IP address	Address in valid format
-g	Gateway address	Address in valid format
-s	Subnet mask	Address in valid format
-n	Host name	String of up to 63 characters. The string can include letters, digits, periods, underscores, and hyphens.
-dn	Domain name	Domain name in valid format
-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 IMM. This value is read-only and is not configurable.
-ipv6static	Static IPv6 state	disabled, enabled
-i6	Static IP address	Static IP address for Ethernet channel 0 in IPv6 format
-p6	Address prefix length	Numeric between 1 and 128
-g6	Gateway or default route	IP address for the gateway or default route for Ethernet channel 0 in IPv6
-dhcp6	DHCPv6 state	disabled, enabled
-sa6	IPv6 stateless autoconfig state	disabled, enabled

Option	Description	Values
-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
-auto	Autonegotiation setting, which determines whether the Data rate and Duplex network settings are configurable	true, false
-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).

Syntax:

```
ifconfig eth0 [options]
options:
-state interface_state
-c config_method
-i static_ip_address
-g gateway_address
-s subnet_mask
-n hostname
-r data_rate
-d duplex_mode
-m max_transmission_unit
-l locally_administered_MAC
```

Example:

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-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 IMM.
system>
```

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

ldap command

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

The following table shows the arguments for the options.

Option	Description	Values
-aom	Authentication only mode	Enabled, disabled
-a	User authentication method	Local only, LDAP only, local first then LDAP, LDAP first then local
-b	Binding method	Bind with Anonymous, bind with ClientDN and password, and bind with Login Credential
-c	Client distinguished name	String of up to 63 characters for *client_dn*
-fn	Forest name	Active directory environments, string of up to 127 characters for *forest_name*
-d	Search domain	String of up to 31 characters for *search_domain*
-f	Group filter	String of up to 63 characters for *group_filter*
-g	Group search attribute	String of up to 63 characters for *group_search_attr*
-l	Login permission attribute	String of up to 63 characters for *string*
-p	Client password	String of up to 15 characters for *client_pw*
-pc	Confirm client password	String of up to 15 characters for *confirm_pw* Command usage is: ldap -p *client_pw* -pc *confirm_pw* This option is required when you change the client password. It compares the *confirm_pw* argument with the *client_pw* argument, and the command will fail if they do not match.
-r	Root entry distinguished name (DN)	String of up to 63 characters for *root_dn*
-rbs	Enhanced Role-Based Security for active directory users	Enabled, disabled
s1ip	Server 1 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s2ip	Server 2 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s3ip	Server 3 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
-s4ip	Server 4 host name/IP address	String up to 63 characters or an IP address for *host name/ip_addr*
s1pn	Server 1 port number	A numeric port number up to 5 digits for *port_number.*
s2pn	Server 2 port number	A numeric port number up to 5 digits for *port_number.*
s3pn	Server 3 port number	A numeric port number up to 5 digits for *port_number*
s4pn	Server 4 port number	A numeric port number up to 5 digits for *port_number*

Option	Description	Values
-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 Snap-In.
-u	UID search attribute	String of up to 23 characters for *search_attrib*
-v	Get LDAP server address through DNS	Off, on
-h	Displays the command usage and options	

Syntax:

```
ldap [options]
options:
   -aom enabled|disabled|
   -a loc|ldap|locId|ldloc
   -b anon|client|login
   -c client_dn
   -d search_domain
   -fn forest_name
   -f group_filter
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -r root_dn
   -rbs enabled|disabled
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s4ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -s4pn port_number
   -t name
   -u search_attrib
   -v off|on
   -h
```

ntp command

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

The following table shows the arguments for the options.

Option	Description	Values
-en	Enables or disables the Network Time Protocol	Enabled, disabled
-i	Name or IP address of the Network Time Protocol server	The name of the NTP server to be used for clock synchronization.
-f	The frequency (in minutes) that the IMM clock is synchronized with the Network Time Protocol server	3 - 1440 minutes

Option	Description	Values
-synch	Requests an immediate synchronization with the Network Time Protocol server	No values are used with this parameter.

Syntax:

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

Example:

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

passwordcfg command

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

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

Syntax:

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

Example:

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

portcfg command

Use the **portcfg** command to configure the serial port. 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.

The parameters are set in the hardware and cannot be changed:

- 8 data bits
- no parity
- 1 stop bit

The following table shows the arguments for the options.

Option	Description	Values
-b	Baud rate	9600, 19200, 38400, 57600, 115200, 230400
-climode	CLI mode	none, cliems, cliuser • none: The command-line interface is disabled • cliems: The command-line interface is enabled with EMS-compatible keystroke sequences • cliuser: The command-line interface is enabled with user-defined keystroke sequences

Syntax:

```
portcfg [options]
portcfg [options]
options:
-b baud_rate
-climode cli_mode
-cliauth cli_auth
```

Example:

```
system> portcfg
-b       : 115200
-climode : 2 (CLI with user defined keystroke sequences) system>
system>
```

srcfg command

Use the **srcfg** command to configure the serial redirection. Type `srcfg` to display the current configuration. 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.

The following table shows the arguments for the `-exitcliseq` option.

Option	Description	Values
-exitcliseq	Exit a command-line interface keystroke sequence	User-defined keystroke sequence to exit the CLI. For details, see the values for the -entercliseq option in this table.

Syntax:

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

Example:

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

ssl command

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

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

Option	Description
-ce	Enables or disables an SSL client
-se	Enables or disables an SSL server
-h	Lists usage and options

Syntax:

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

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

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

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

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

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

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

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

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

SSL client CSR key status

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

Private Key and Cert/CSR not available

Private Key and CA-signed cert installed

Private Key and Auto-gen self-signed cert installed

Private Key and Self-signed cert installed

Private Key stored, CSR available for download

timeouts command

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

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

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

Syntax:

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

Example:

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

usbeth command

Use the **usbeth** command to enable or disable the in-band LAN over USB interface. For more information about enabling or disabling this interface, see “Disabling the USB in-band interface” on page 23.

Syntax:

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

Example:

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

users command

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

Read the following guidelines about the **users** command:

- User numbers must be from 1 to 12, inclusive.
- User names must be less than 16 characters and can contain only numbers, letters, periods, and underscores.
- Passwords must be more than 5 and fewer than 16 characters long and must contain at least one alphabetic and one nonalphabetic character.
- The authority level can be one of the following levels:
  - super (supervisor)
  - ro (read only)
  - Any combination of the following values, separated by |:
    - 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])

Syntax:

```
users [options]
options:
-user number
-n username
-p password
-a authority level
```

Example:

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

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

IMM control commands

The IMM control commands are as follows:

- clearcfg
- clock
- identify
- resetsp
- update

clearcfg command

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

clock command

Use the **clock** command to display the current date and time according to the IMM 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 or +10, special daylight saving time settings are required.
- For +2, the daylight saving time options are as follows: off, ee (Eastern Europe), gtb (Great Britain), egt (Egypt), fle (finland).
- For +10, the daylight saving time settings are as follows: off, ea (Eastern Australia), tas (Tasmania), vlad (Vladivostok).
- 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
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 13:15:30 GMT-5:00 dst on
```

identify command

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

Syntax:

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

Example:

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

resetsp command

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

update command

Use the **update** command to update the firmware on the IMM or IMM. To use this command, you must have at least Advanced Adapter Configuration authority. The firmware file (specified by *filename*) is first transferred from the TFTP server (specified by its IP address) to the IMM or IMM and then flashed. The **-v** option specifies verbose mode.

Note: Make sure that the TFTP server is running on the server from which the file will be downloaded.

Option	Description
-i	TFTP server IP address
-l	File name (to be flashed)
-v	Verbose mode

Syntax:

```
update -i TFTP_server_IP_address -l filename
```

Example:In the verbose mode, the flashing progress is displayed in real time in the percentage of completion.

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Downloading image - 66%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flashing image - 45%

system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Firmware update is in progress. Please wait..
Image Downloaded.
Flash operation completed.
system>
```

If the flashing is not in the verbose mode, progress is displayed in consecutive # characters.

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Firmware update is in progress. Please wait..
Downloading image: ################################################
Flashing image: ################################################
Flash operation completed.
```

Service Advisor commands

The Service Advisor commands are as follows:

- autoftp
- chconfig
- chlog
- chmanual
- events
- sdemail

autoftp command

Use the **autoftp** command to display and configure the FTP/TFTP server settings for the Service Advisor.

Note: The Service Advisor terms and conditions must be accepted before using this command.

The following table shows the arguments for the options.

Option	Description	Values
-m	Automated problem reporting mode	*ftp, tftp, disabled*
-i	ftp/tftp server IP address or hostname for automated problem reporting	IP address or host name

Option	Description	Values
-p	ftp/tftp transmission port	Numeric between 1 - 65535 for *port_number*
-u	Quote-delimited ftp user name for problem reporting	String of up to 63 characters for *user_name*
-pw	Quote-delimited ftp password for problem reporting	String of up to 63 characters for *password*
Note: For the *ftp* value, all options (fields -i, -p, -u, and -pw) must be set. For the *tftp* value, only options -i and -p are required.		

Syntax:

```
autoftp [options]
options:
-m ftp|tftp|disable
-i host name|ip_addr
-p port_number
-u user_name
-pw password
```

chconfig command

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

The following table shows the arguments for the options.

Option	Description	Values
-li	View or accept the Service Advisor Terms and Conditions. The Service Advisor Terms and Conditions must be accepted through this option before setting other options.	view, accept
-sa	IBM Support status of Service Advisor	enabled, disabled
-sc	Country code for the IBM Service Support Center	Two character ISO country code
-ca	Quote-delimited address of the machine location	String of up to 30 characters for *address*
-cci	Quote-delimited city of the machine location	String of up to 30 characters for *city*
-ce	Email address of the contact person in form *userid@hostname*	String of up to 30 characters for *email_addr*
-cn	Quote-delimited name of the contact person	String of up to 30 characters for *contact_name*
-co	Quote-delimited organization/company name of the contact person	String of up to 30 characters for *company_name*
-cph	Quote-delimited phone number of the contact person	String between 5 and 30 characters for *phone_number*
-cs	State of the machine location	String between 2 and 3 characters for *state/provice*
-cz	Quote-delimited postal code of the machine location	String of up to 9 characters for *postal_code*

Option	Description	Values
-loc	Fully qualified hostname or IP address for HTTP proxy	String of up to 63 characters or an IP address for *host_name/ip_addr*
-po	HTTP proxy port	A numeric port number between 1 and 65535 for *port_number*
-ps	HTTP proxy status	enabled, disabled
-pw	Quote-delimited HTTP proxy password	String of up to 15 characters for *password*
-u	Quote-delimited HTTP proxy user name	String of up to 30 characters for *user_name*

1. The Service Advisor terms and conditions must be accepted through option -li before setting other options.
2. All contact information fields as well as the IBM Service Support Center fields are required before IBM Support of Service Advisor can be enabled. If a proxy is required, the HTTP proxy fields must be set.

Syntax:

```
chconfig [options]
options:
-li view|accept
-sa service advisor state
-sc country_code
-ca address
-cci city
-ce email_addr
-cn contact_name
-co company_name
-cph phone_number
-cs state/provice
-cz postal_code
-loc host_name/ip_addr
-po port_number
-ps status
-pw password
-u user_name
```

chlog command

Use the **chlog** command to display the last five call home events that were generated either by the system or the user. The most recent call home entry is listed first.

The following table shows the arguments for the options.

Note: The Service Advisor terms and conditions must be accepted before using this command.

Option	Description	Values
-event_index	Specify a call home entry by using the Index from the Activity Log	Numeric between 1 and 5
-ack	Acknowledge/unacknowledged, a call home event has been corrected	yes, no
-s	Only display the result of IBM Support	

Option	Description	Values
-f	Only display the result of FTP/TFTP Server	

Syntax:

```
chlog [options]
options:
-event_index
-ack yes|no
-s
-f
```

chmanual command

Use the **chmanual** command to generate a manual Call Home event or a Test Call Home event.

Note: The Service Advisor terms and conditions must be accepted before using this command.

The following table shows the arguments for the options.

Option	Description	Values
-test	Generate a test Call Home event	
-desc	Quote-delimited problem description	String up to 100 characters for *description*

Syntax:

```
chmanual [options]
options:
-test
-desc description
```

events command

Use the **events** command to view and edit exclusion events.

Note: The Service Advisor terms and conditions must be accepted before using this command.

The following table shows the arguments for the options.

Option	Description	Values
-che	View and edit exclusion events	
-add	Add a call home event into the call home exclusion list	*event_id* in the format 0xhhhhhhhhhhhhhhhh
-rm	Remove a call home event from the call home exclusion list	*event_id*|*all* in the format 0xhhhhhhhhhhhhhhhh, or all

Syntax:

```
events [options]
options: -che {-add}|{-rm}
-add event_id
-rm event_id|all
```

sdemail command

Use the **sdemail** command to configure email service information for the specified recipients.

The following table shows the arguments for the options.

Option	Description	Values
-subj	Quote-delimited email subject	String of up to 119 characters for *email_subject*
-to	Recipient's email address. This option can consist of multiple addresses separated with a comma.	String of up to 119 characters for *email_addrs*

Syntax:

```
sdemail [options]
options:
-subj email_subject
-to email_addrs
```

Appendix A. Getting help and technical assistance

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

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

Before you call

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

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

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your IBM product. The IBM Warranty terms and conditions state that you, the owner of the IBM product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your IBM service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.ibm.com/systems/info/x86servers/serverproven/compat/us to make sure that the hardware and software is supported by your IBM product.
- Go to http://www.ibm.com/supportportal to check for information to help you solve the problem.
- Gather the following information to provide to IBM Support. This data will help IBM Support quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (IBM 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/entry/portal/Open_service_request to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to IBM Support quickly and efficiently. IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

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

Using the documentation

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

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

Getting help and information from the World Wide Web

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

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

How to send DSA data to IBM

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

Before you send diagnostic data to IBM, read the terms of use at http://www.ibm.com/de/support/ecurep/terms.html.

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

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

Creating a personalized support web page

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

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

Software service and support

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

For information about which products are supported by Support Line in your country or region, see http://www.ibm.com/services/supline/products.

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

Hardware service and support

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

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

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

IBM Taiwan product service

Use this information to contact IBM Taiwan product service.

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

IBM Taiwan product service contact information:

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

Appendix B. Notices

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product, and use of those websites is at your own risk.

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

Trademarks

IBM, the IBM logo, and ibm.com are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies.

A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/us/en/copytrade.shtml.

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

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

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

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

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

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

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

Important notes

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

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

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

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

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

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

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

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

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

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

Particulate contamination

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

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

Table 21. Limits for particulates and gases

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

Table 21. Limits for particulates and gases (continued)

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

Documentation format

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

Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.

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

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

Telecommunication regulatory statement

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

Electronic emission notices

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

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio

communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

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

Avis de conformité à la réglementation d'Industrie Canada

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

Australia and New Zealand Class A statement

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

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a nonrecommended modification of the product, including the fitting of non-IBM option cards.

Attention: This is an EN 55022 Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

Responsible manufacturer:

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

European Community contact:

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

Germany Class A statement

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

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

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

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

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

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

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

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

Generelle Informationen:

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

Japan VCCI Class A statement

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

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

Korea Communications Commission (KCC) statement

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

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

Russia Electromagnetic Interference (EMI) Class A statement

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

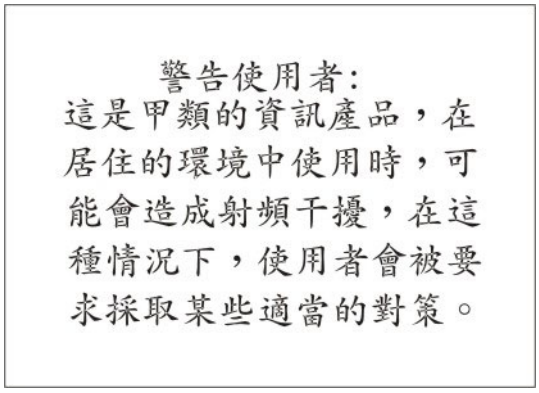
People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明

声 明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Taiwan Class A compliance statement



Index

J

K

L

M

N

O

P

R

S

T

U

V

W

Part Number: 47C9202

Printed in USA

(1P) P/N: 47C9202