Integrated Management Module User Guide

April 14, 2011

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Integrated Management Module User Guide

CONTENTS

CHAPTER 1

Introduction

The integrated management module (IMM) consolidates the service processor and remote management capabilities in a single chip on the server system board.

The IMM offers several benefits:

- Choice of dedicated or shared Ethernet connection.
- One IP address for both the Intelligent Platform Management Interface (IPMI) and the service processor interface.
- Ability to locally or remotely update other entities without requiring a server restart to initiate the update process.
- Capability for applications and tools to access the IMM either in-band or out-of-band.

This document explains how to use the functions of the IMM.

IMM features

The IMM is a common management component for Cisco Mobility Services Engine, Cisco Flex Controller, and Cisco Prime Network Control System. The functionality provided by the IMM is the same across all three products. Product specific differences are highlighted as appropriate througout the document.

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 has the following features.

- Access to critical server settings
- Access to server vital product data (VPD)
- Automatic notification and alerts
- Continuous health monitoring and control
- Choice of a dedicated or shared Ethernet connection
- 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 firmware updating
- Remote power control
- Secure Web server user interface
- Simple Network Management Protocol (SNMP) support
- User authentication using a secure connection to a Lightweight Directory Access Protocol (LDAP) server

Web browser and operating-system requirements

Warning **Do not attempt to update the firmware on the system without proper directions from Cisco TAC. You should update the firmware, as directed by Cisco TAC, and with the firmware certified and released by Cisco. Failure to follow these guidelines can render your system inoperable.**

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

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 and a video controller 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 both static and Dynamic Host Configuration Protocol (DHCP) IP addressing. The default static IP 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 IP address.

The IMM provides the choice of using a dedicated systems-management network connection or one that is shared with the server.

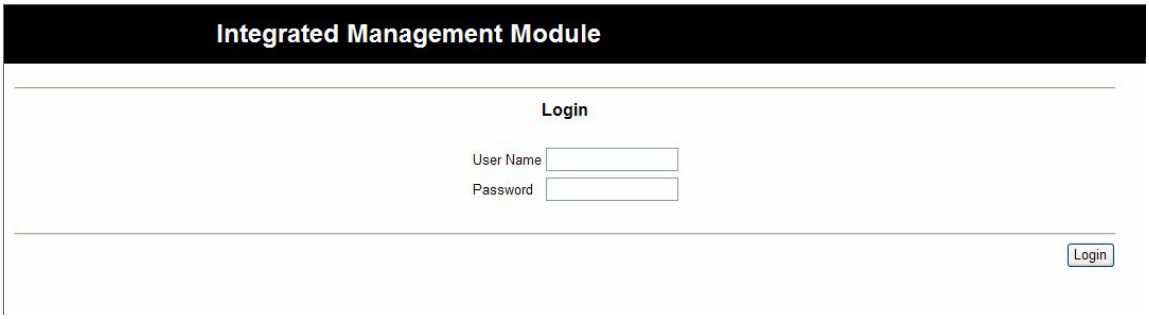
For setting up the IMM network connection, the approach depends on the product. For example, the Cisco Flex 7500 Series Wireless Controller provides a CLI command to configure IMM access, whereas the Cisco 3355 Mobility Services Engine provides a script (immconfig.sh). Refer to the product-specific configuration document for details.

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:

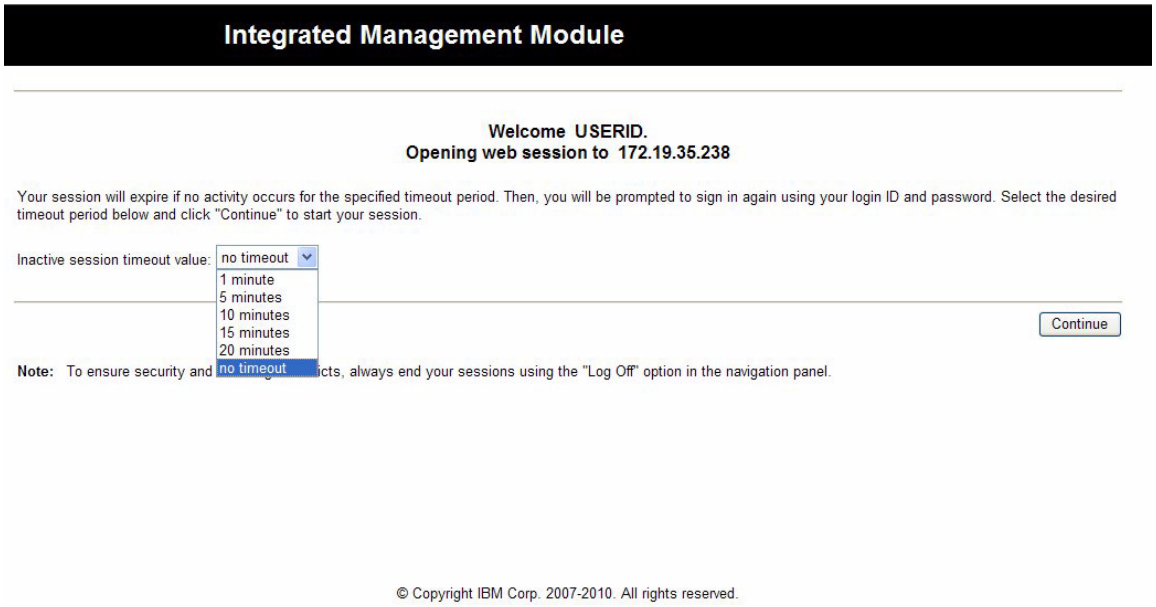
Step 1 Open a Web browser. In the address or URL field, type the IP address or host name of the IMM server to which you want to connect.



Step 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 name, you might need to enter a new password. The default user name is USERID and the default password is PASSW0RD (with a zero).

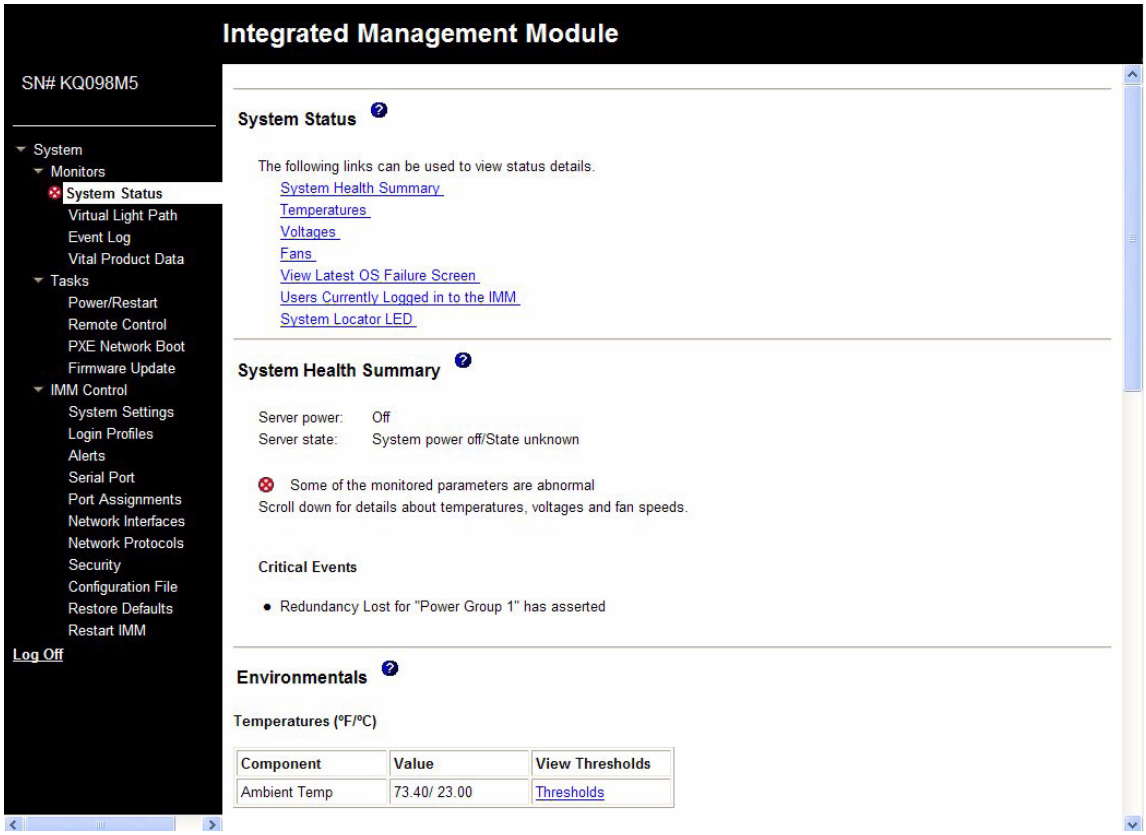
Step 3 On the Welcome Web page, select a timeout value from the drop-down list in the field that is provided. If your browser is inactive for that number of minutes, the IMM logs you off the Web interface.

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



Step 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" section on page 2-3. Then, go to Chapter 3, "Configuring the IMM".

IMM action descriptions

Table 2-1 lists the actions that are available when you are logged in to the IMM.

Table 2-1 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.

Table 2-1 IMM Actions (continued)

Link	Action	Description
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.
Remote Control	Redirect the server video console and use your computer disk drive or disk image as a drive on the server	This feature is not supported.
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	This operation is not supported.
Firmware Update	Update the firmware on the IMM	Do not attempt to update the firmware on the system without proper directions from Cisco TAC. You should update the firmware, as directed by Cisco TAC, and with the firmware certified and released by Cisco. Failure to follow these guidelines can render your system inoperable.
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.  **Note** This operation is not supported on the Cisco Flex Series 7500 Wireless Controller.
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.

Table 2-1 IMM Actions (continued)

Link	Action	Description
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. **Note** This operation is not supported on Cisco Flex 7500 Series Wireless Controller.
	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	Serial port is dedicated for the serial console redirection function. Therefore, it cannot be used for IMM.
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).
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	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.
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 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.

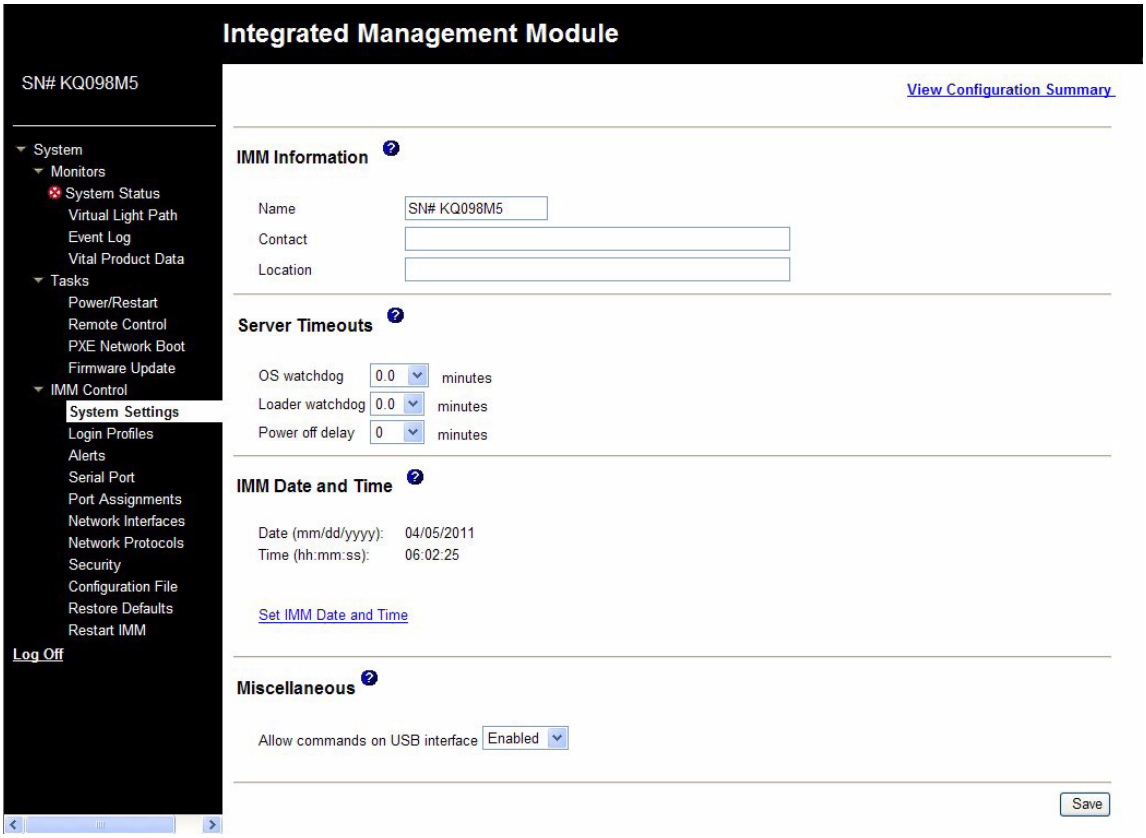
Setting system information

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

Step 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".

Step 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.



Step 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" section on page 3-19

Step 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.

Step 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.

Step 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" section on page 3-6.

Note The LAN over USB and OS Watchdog features are not supported on the Cisco Flex 7500 Series Wireless Controller.

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

Step 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".

Step 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

Step 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.

Step 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" section on page 3-5 for more information.

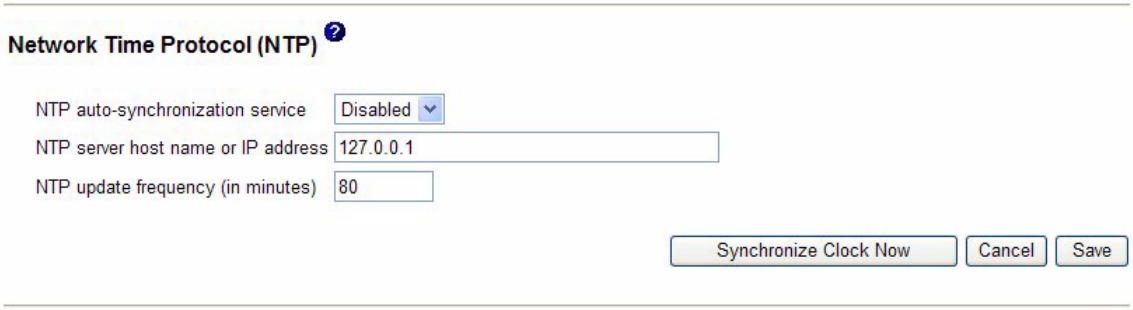
Alerts that are sent by e-mail and SNMP use the real-time clock setting to time stamp the alerts. The clock settings support Greenwich mean time (GMT) offsets and daylight saving time (DST) for added ease-of-use for administrators who are managing systems remotely over different time zones. You can remotely 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:

Step 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".

Step 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 Web page was generated.

Step 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.



Step 4 In the **Date** field, type the numbers of the current month, day, and year.

Step 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.

Step 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.

Step 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.

Step 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.

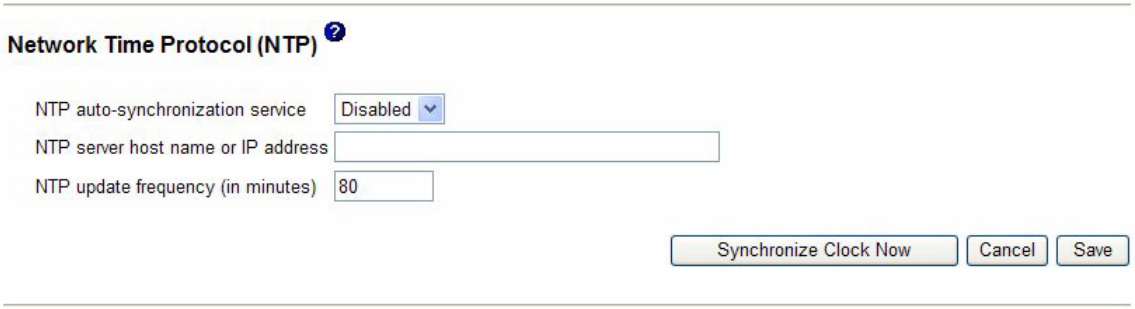
The NTP feature does not provide the extended security and authentication that are provided through encryption algorithms in NTP Version 3 and NTP Version 4. The IMM NTP feature supports only the Simple Network Time Protocol (SNTP) without authentication.

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

Step 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”.

Step 2 In the navigation pane, click **System Settings** and scroll down to the **IMM Date and Time** area.

Step 3 Click **Set IMM Date and Time**. A page similar to the one in the following illustration is displayed.



Step 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.

Step 5 Click **Save**.

Disabling the USB in-band interface

Note The Cisco Flex 7500 Series Wireless Controller does not allow enabling the USB in-band interface. Do not modify this setting.

Note **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 flash utilities. If the USB in-band interface is disabled, use the Firmware Update option on the IMM Web interface to update the firmware.

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" section on page 3-3.

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.

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

Step 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".

Step 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.

Step 3 Select the **Do not allow commands on USB interface** check box to disable the USB in-band interface. 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.

Step 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 The USB in-band interface is also called “LAN over USB”.

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

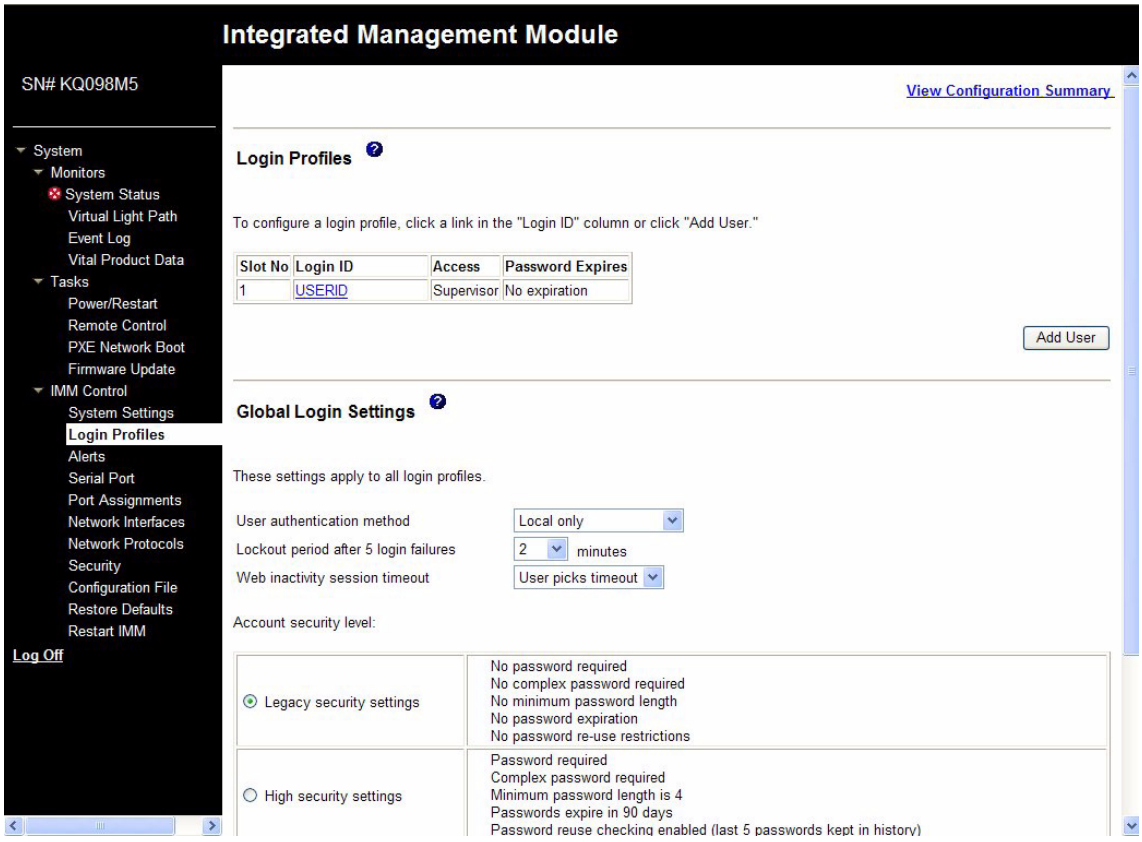
To configure a login profile, complete the following steps:

Step 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".

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

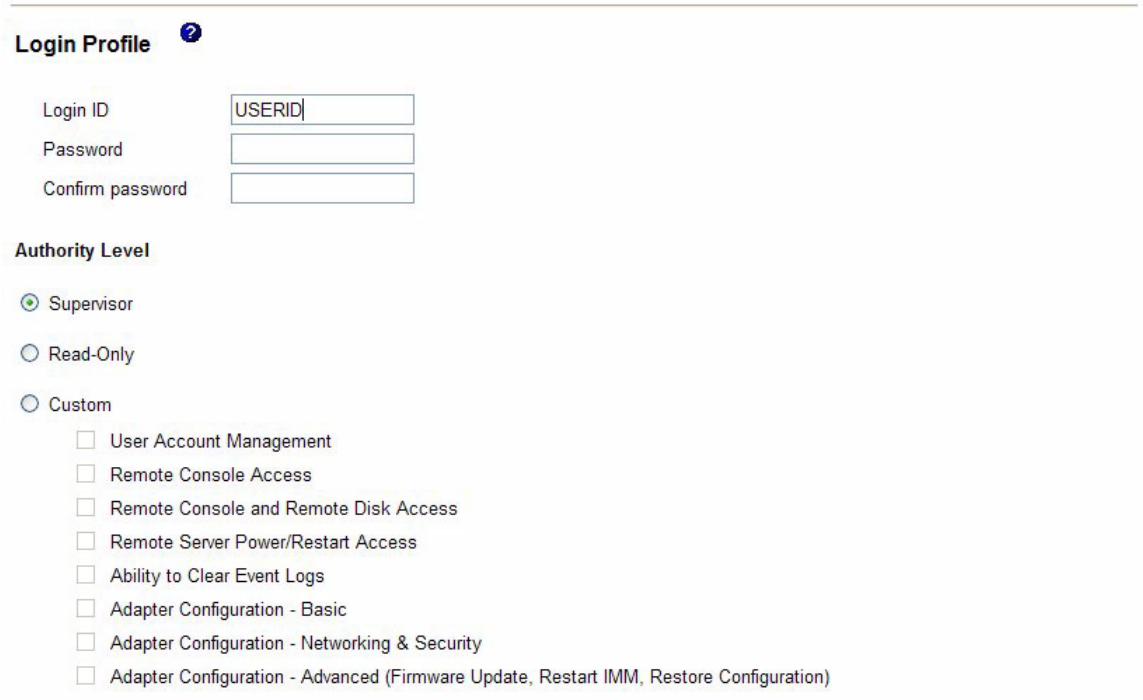
Note If you have not configured a profile, it does not appear in the Login Profiles table.

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.

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



Step 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.

Step 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.

Step 6 In the **Confirm password** field, type the password again.

Step 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:** This is not supported.

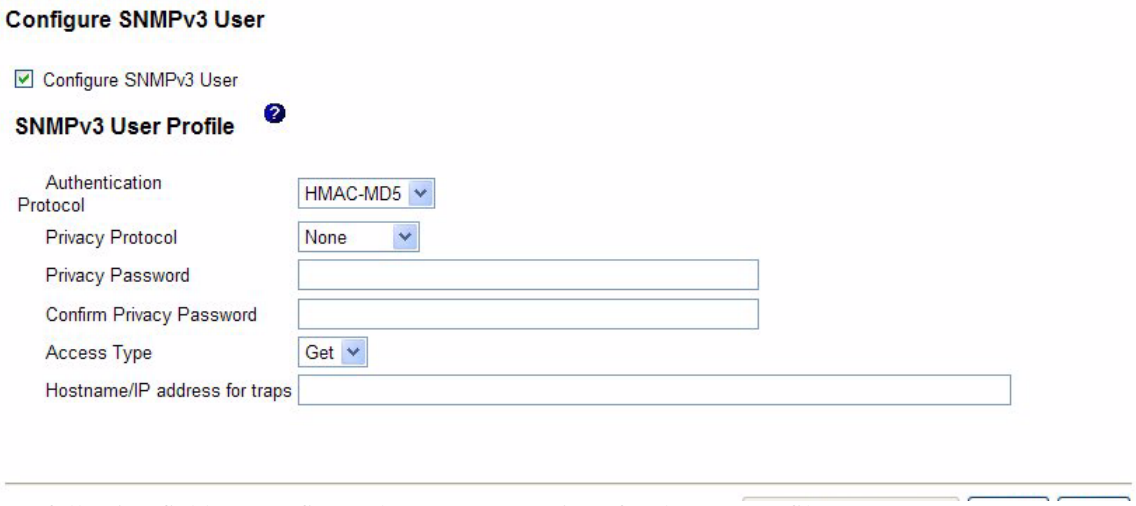
- **Remote Server Power/Restart Access:** A user can access the power-on and restart functions for the remote server. These functions are available in the Power/Restart page.
- **Ability to Clear Event Logs:** A user can clear the event logs. Everyone can look at the event logs, but this particular permission 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.

Step 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).

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

Deleting a login profile

To delete a login profile, complete the following steps:

Step 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”.

Step 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.

Step 3 Click the login profile that you want to delete. The Login Profile page for that user is displayed

Step 4 Click **Clear Login Profile.**

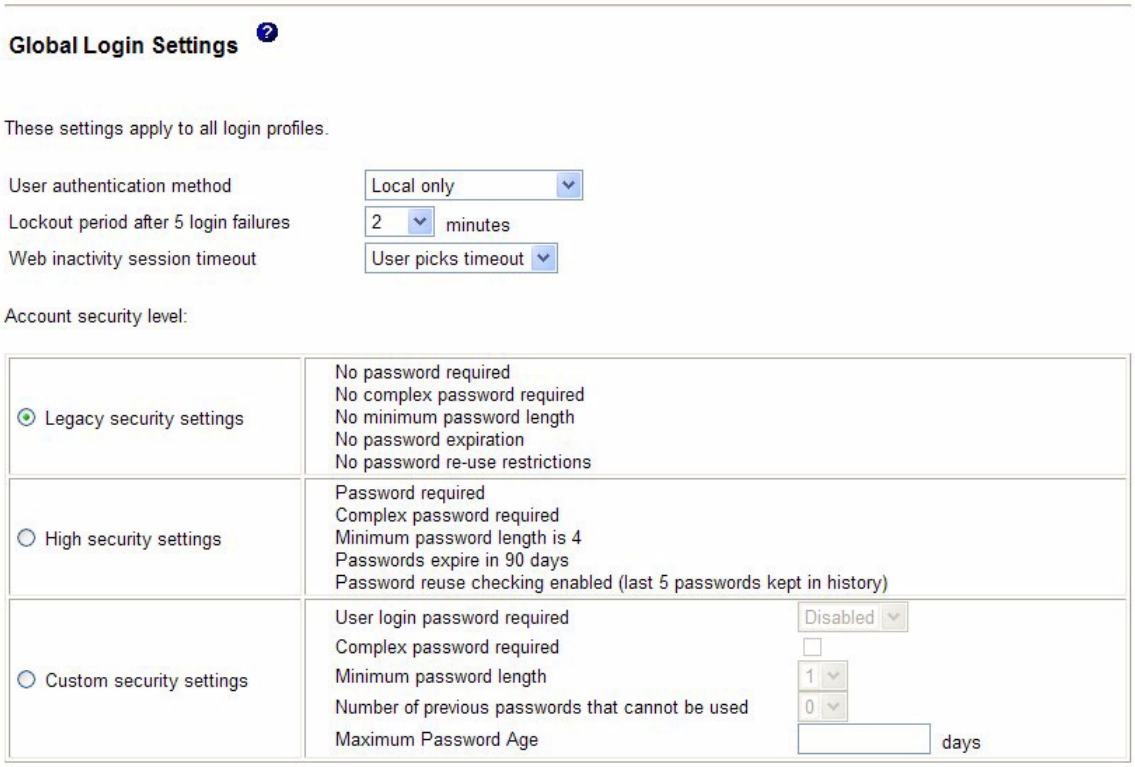
Configuring the global login settings

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

Step 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".

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

Step 3 Scroll down to the **Global Login Settings** area. A page similar to the one in the following illustration is displayed.



Step 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" section on page 3-7.
- **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 Only locally administered accounts are shared with the IPMI interface because IPMI does not support LDAP authentication.

Note 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.

Step 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.

Step 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.

Step 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.

Step 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.

Step 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" section on page 3-22.

Configuring remote alert recipients

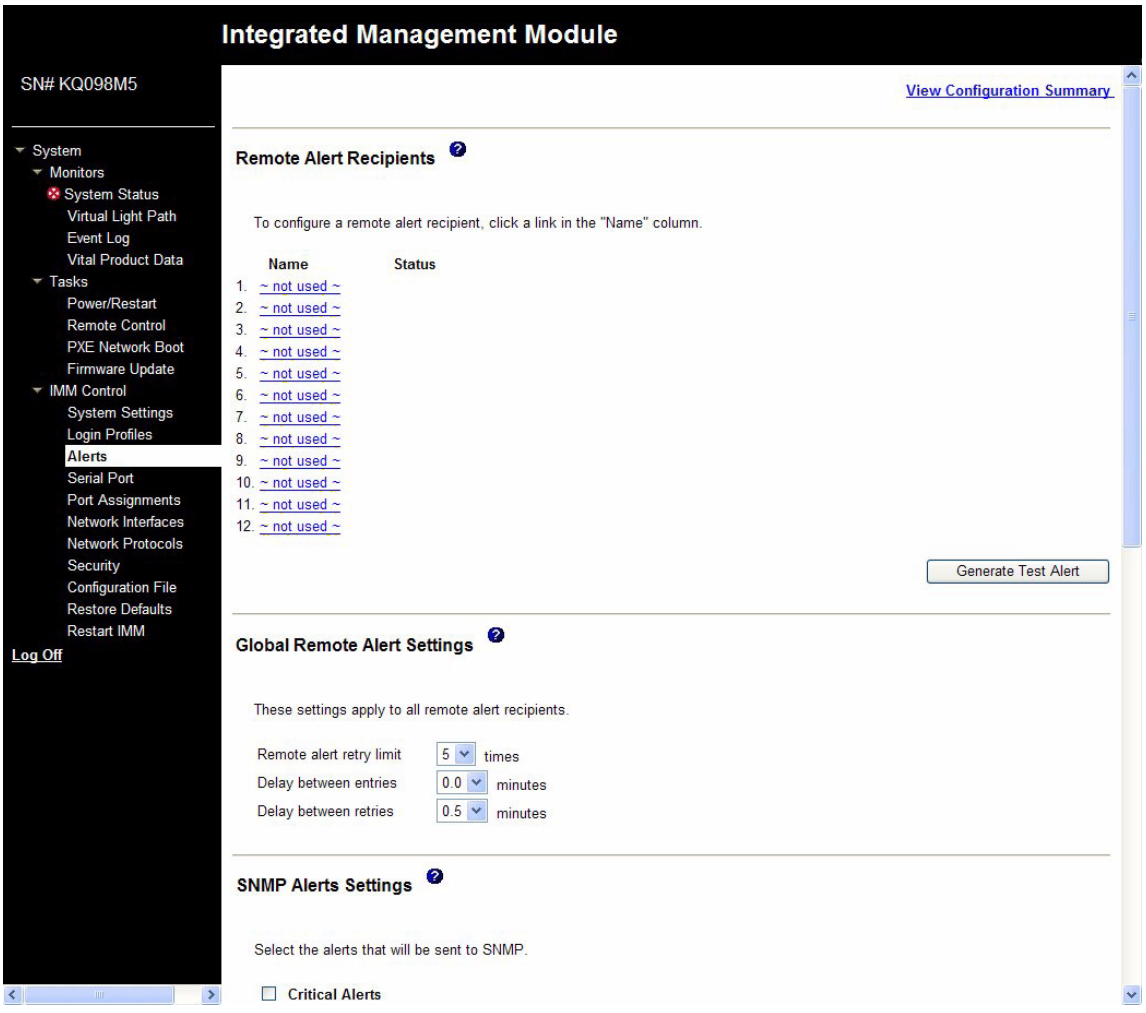
You can define up to 12 unique remote alert recipients. Each link for an alert recipient is labeled with the recipient name and alert status.

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

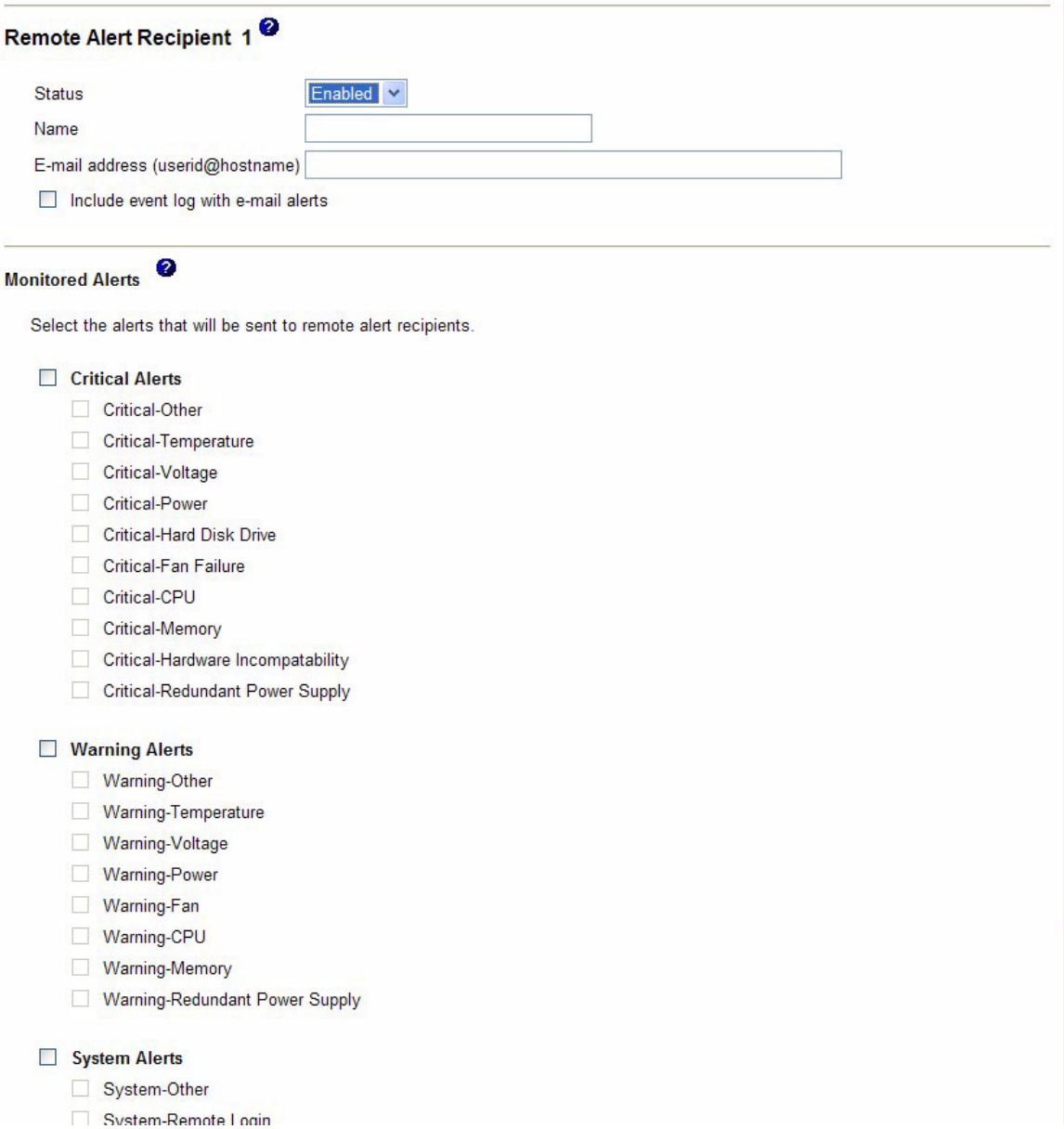
To configure a remote alert recipient, complete the following steps:

Step 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".

Step 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.



Step 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.



Step 4 In the **Status** field, click **Enabled** to activate the remote alert recipient.

Step 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.

Step 6 In the **E-mail address** field, enter the alert recipient's e-mail address.

Step 7 Use the check box to include event logs with e-mail alerts.

Step 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.

Step 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:

Step 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".

Step 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.

Step 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 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.

Note IMM supports the SNMPv1 and SNMPv3 standards.

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

Step 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".

Step 2 In the navigation pane, click **Alerts** and scroll down to the **SNMP Alerts Settings** area.

Step 3 Select the type or types of alerts. The remote alerts are categorized by the following levels of severity:

- Critical
- Warning
- System

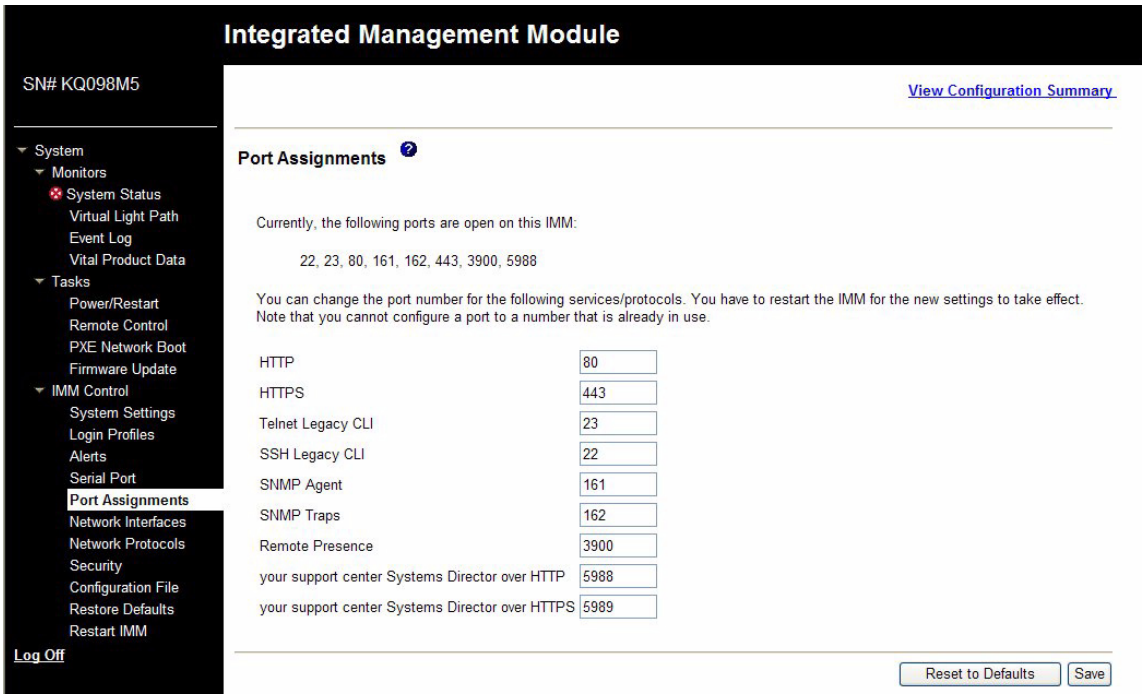
Step 4 Scroll to the bottom of the page and click **Save**.

Configuring port assignments

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

Step 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".

Step 2 In the navigation pane, click **Port Assignments**. A page similar to the one in the following illustration is displayed.



Step 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 feature is not supported on any of the three products.

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

Table 3-1 Reserved port numbers

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

Step 4 Click **Save**.

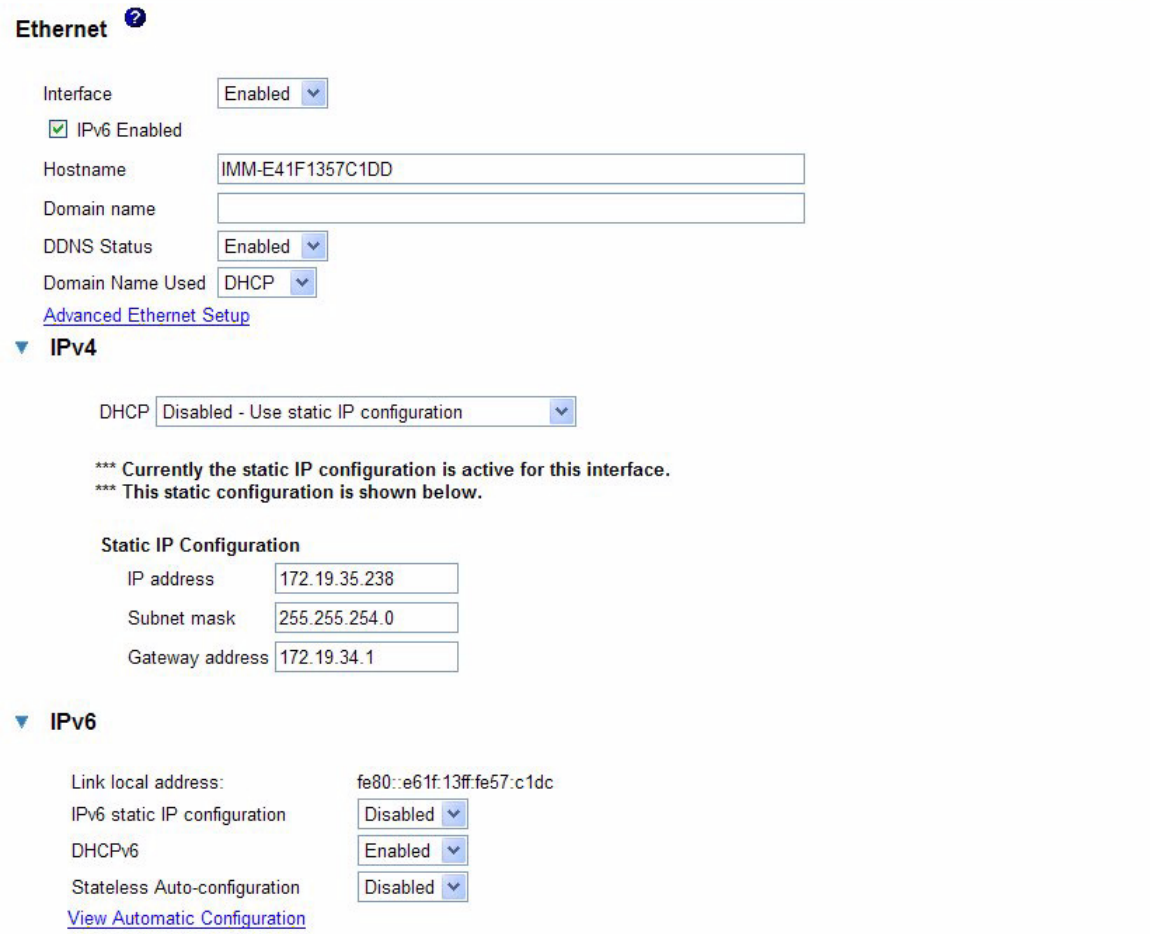
Configuring network interfaces

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, complete the following steps:

Step 1 Log in to the IMM where you want to set up the configuration. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 2 In the navigation pane, click **Network Interfaces**. A page similar to the one in the following illustration is displayed.

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



Step 3 If you want to use an Ethernet connection, select **Enabled** in the **Interface** field. Ethernet is enabled by default.

Note Disabling the Ethernet interface prevents all access to the IMM from the external network.

Step 4 If you want to use a Dynamic Host Configuration Protocol (DHCP) server connection, enable it by clicking either of the following choices in the DHCP field:

- **Enabled - Obtain IP config from DHCP server**
- **Try DHCP server. If it fails, use static IP config.**

The default setting is **Try DHCP server. If it fails, use static IP config.**

Note Do not enable DHCP unless you have an accessible, active, and configured DHCP server on your network. When DHCP is used, the automatic configuration overrides any manual settings.

If you want to assign a static IP address to the IMM, select **Disabled - Use static IP configuration**.

If DHCP is enabled, the host name is assigned as follows:

- If the **Hostname** field contains an entry, the IMM DHCP support requests that the DHCP server use this host name.
- If the **Hostname** field does not contain an entry, the IMM DHCP support requests that the DHCP server assign a unique host name to the IMM.

Step 5 Type the IP host name of the IMM in the **Hostname** field.

You can enter a maximum of 63 characters in this field, which represents the IP host name of the IMM. The host name defaults to IMMA, followed by the IMM burned-in media access control (MAC) address.

Note The IP host name of the IMM (the **Hostname** field) and IMM name (the **Name** field on the System page) do not automatically share the same name, because the **Name** field is limited to 15 characters but 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 "Setting system information" section on page 3-2.

If you enabled DHCP, go to Step 12.

If you have not enabled DHCP, continue with Step 6.

Step 6 In the **IP address** field, type the IP address of the IMM. The IP address must contain four integers from 0 - 255 with no spaces and separated by periods.

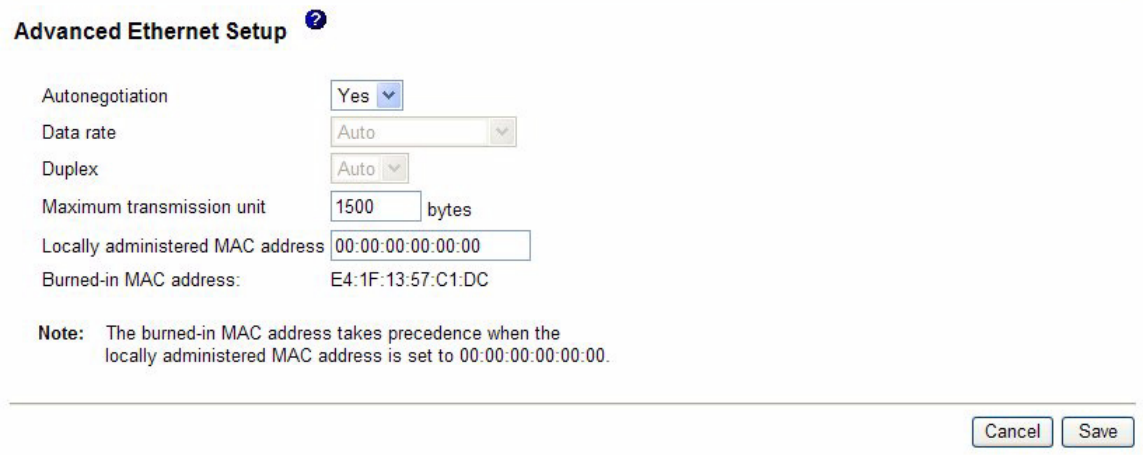
Step 7 In the **Subnet mask** field, type the subnet mask that is used by the IMM. The subnet mask must contain four integers from 0 - 255 with no spaces or consecutive periods and separated by periods.

The default setting is 255.255.255.0.

Step 8 In the **Gateway address** field, type your network gateway router. The gateway address must contain four integers from 0 - 255 with no spaces or consecutive periods and separated by periods.

Step 9 Scroll to the bottom of the page and click **Save**.

Step 10 Click **Advanced Ethernet Setup** if you need to set additional Ethernet settings.



The following table describes the functions on the Advanced Ethernet Setup page.

Table 3-2 Functions on the Advanced Ethernet Setup page

Field	Function
Auto Negotiate	The IMM determines the data rate and duplex settings automatically, according to your switch capabilities.
Data rate	Use the **Data Rate** field to specify the amount of data that is to be transferred per second over your LAN connection. To set the data rate, click the menu and select the data-transfer rate, in Mb[1], that corresponds to the capability of your network. To automatically detect the data-transfer rate, set the **Auto Negotiate** field to **Yes**, which is the default value.
Duplex	Use the **Duplex** field to specify the type of communication channel that is used in your network. To set the duplex mode, select one of the following choices: • **Full** enables data to be carried in both directions at once. • **Half** enables data to be carried in either one direction or the other, but not both at the same time. To automatically detect the duplex type, set the **Auto Negotiate** field to **Yes**, which is the default value.
Maximum transmission unit	Use the **Maximum transmission unit** field to specify the maximum size of a packet (in bytes) for your network interface. For Ethernet, the valid maximum transmission unit (MTU) range is 60 - 1500. The default value for this field is 1500.
Locally administered MAC address	Enter a physical address for the IMM in the **Locally administered MAC address** field. If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value from 000000000000 through FFFFFFFFFFFF. This value must be in the form *xx*:*xx*:*xx*:*xx*:*xx*:*xx*:*xx* where *x* is a number 0 - 9. The IMM does not support the use of a multicast address. The first byte of a multicast address is an odd number (the least significant bit is set to 1). Therefore, the first byte must be an even number.
Burned-in MAC address	The burned-in MAC address is a unique physical address that is assigned to this IMM by the manufacturer. The address is a read-only field.

[1]Mb equals approximately 1,000,000 bits.

Step 11 Modify the advanced Ethernet settings as necessary.

Step 12 Scroll to the bottom of the page and click **Save**.

Step 13 Click **Cancel** to return to the Network Interfaces page. If DHCP is enabled, the server automatically assigns the host name, IP address, gateway address, subnet mask, domain name, DHCP server IP address, and up to three DNS server IP addresses.

Step 14 If DHCP is enabled, to view the DHCP server assigned setting, click **IP Configuration Assigned by DHCP Server**.

Step 15 Click **Save**.

Step 16 Click **View Configuration Summary** to see a summary of all current configuration settings.

Step 17 In the navigation pane, click **Restart IMM** to activate the changes.

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.

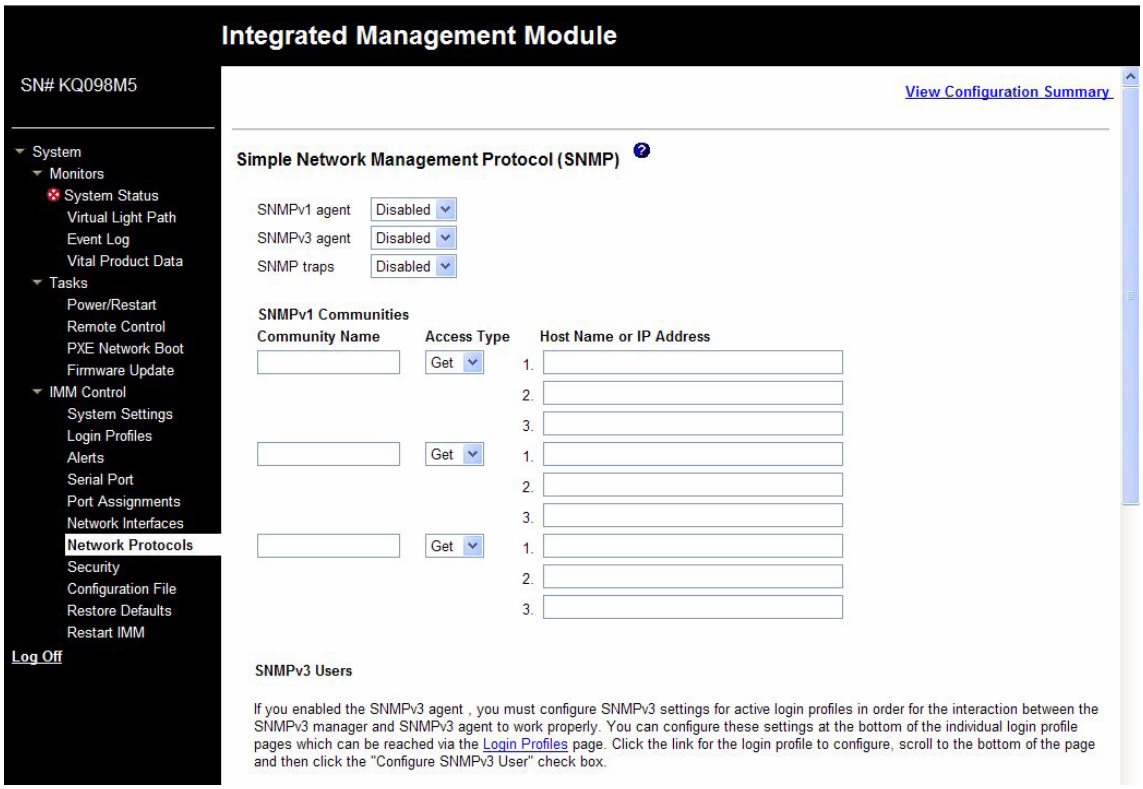
Note The IMM provides two Management Information Base (MIB) files for use with SNMP applications. The MIB files are included in the IMM firmware update packages.

Note IMM supports the SNMPv1 and SNMPv3 standards.

To configure SNMP, complete the following steps:

Step 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”.

Step 2 In the navigation pane, click **Network Protocols**. A page similar to the one in the following illustration is displayed.



Step 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" section on page 3-7 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.

Step 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" section on page 3-2.
- 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**.

Step 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.

Step 6 In the **Community Name** field, enter a name or authentication string to specify the community.

Step 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.

Step 8 In the corresponding **Host Name or IP Address** field, enter the host name or IP address of each community manager.

Step 9 Scroll to the bottom of the page and click **Save**.

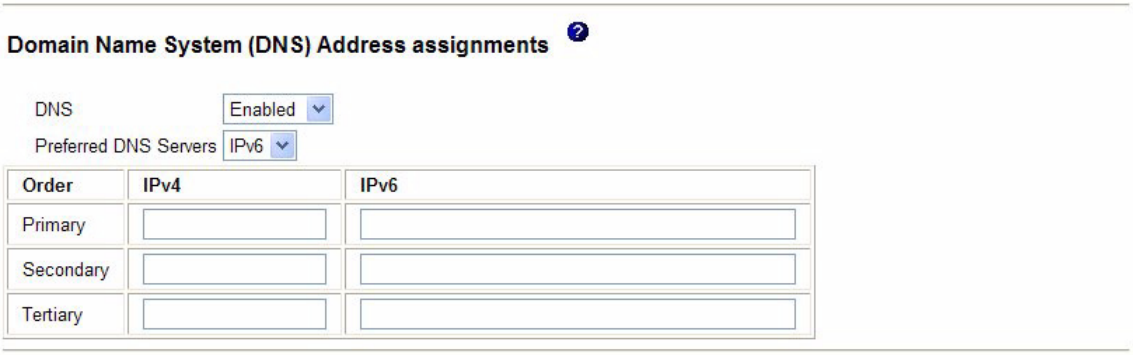
Step 10 In the navigation pane, click **Restart IMM** to activate the changes.

Configuring DNS

To configure the Domain Name System (DNS), complete the following steps:

Step 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".

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



Step 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.

Step 4 If you enabled DNS, in the **DNS server IP address** fields, specify the IP addresses of up to three DNS servers on your network. Each IP address must contain integers from 0 - 255, separated by periods.

Step 5 Scroll to the bottom of the page and click **Save**.

Step 6 In the navigation pane, click **Restart IMM** to activate the changes.

Configuring Telnet

To configure Telnet, complete the following steps:

Step 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".

Step 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.

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

Step 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.

Step 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".

Step 2 In the navigation pane, click **Network Protocols** and scroll down to the **SMTP** area of the page.

Step 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.

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

Step 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.

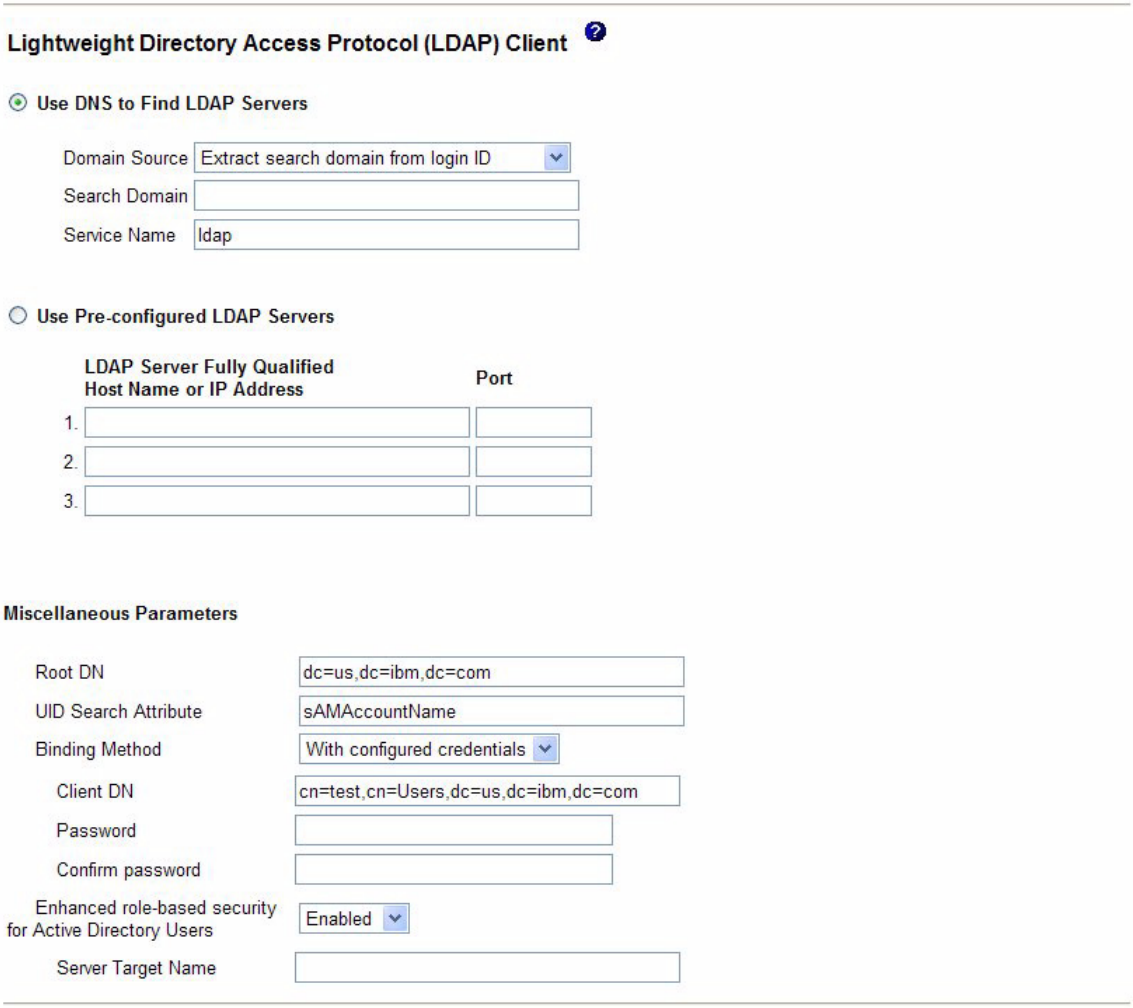
You can also use LDAP to assign users and IMMs to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, an IMM can be associated with one or more groups, and a user would pass group authentication only if the user belongs to at least one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

Setting up a client to use the LDAP server

To set up a client to use the LDAP server, complete the following steps:

Step 1 Log in to the IMM on which you want to set up the client. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 2 In the navigation pane, click **Network protocols** and scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area of the page. A page similar to the one in the following illustration is displayed.



The IMM contains a Version 2.0 LDAP client that you can configure to provide user authentication through one or more LDAP servers. The LDAP server that is to be used for authentication can be discovered dynamically or manually preconfigured.

Step 3 Choose one of the following methods to configure the LDAP client:

- To dynamically discover the LDAP server, select **Use DNS to Find LDAP Servers**.

  If you choose to discover the LDAP server dynamically, the mechanisms that are described by RFC2782 (a DNS RR for specifying the location of services) are applied to find the server. This is known as DNS SRV. The parameters are described in the following list:

  Domain Source - The DNS SRV request that is sent to the DNS server must specify a domain name. The LDAP client determines where to get this domain name according to which option is selected. There are three options:

  - **Extract search domain from login id**. The LDAP client uses the domain name in the login ID. For example, if the login ID is joesmith@mycompany.com, the domain name is mycompany.com. If the domain name cannot be extracted, the DNS SRV fails, causing the user authentication to fail automatically.
  - **Use only configured search domain below**. The LDAP client uses the domain name that is configured in the **Search Domain** parameter.
  - **Try login id first, then configured value**. The LDAP client first attempts to extract the domain name from the login ID. If this is successful, this domain name is used in the DNS SRV request. If no domain name is present in the login ID, the LDAP client uses the configured **Search Domain** parameter as the domain name in the DNS SRV request. If nothing is configured, user authentication fails immediately.

  Search Domain - This parameter can be used as the domain name in the DNS SRV request, depending on how the **Domain Source** parameter is configured.

  Service Name - The DNS SRV request that is sent to the DNS server must also specify a service name. The configured value is used. If this field is left blank, the default value is **ldap**. The DNS SRV request must also specify a protocol name. The default is **tcp** and is not configurable.

- To use a preconfigured LDAP server, select **Use Pre-Configured LDAP Server**.

  Note The port number for each server is optional. If the field is left blank, the default value of 389 is used for nonsecured LDAP connections. For secured connections, the default is 636. You must configure at least one LDAP server.

  You can configure the following parameters:

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

  UID Search Attribute - When the selected binding method is **Anonymously** or **w/ Configured Credentials**, the initial bind to the LDAP server is followed by a search request that is aimed at retrieving specific information about the user, including the user's DN, login permissions, and group membership. This search request must specify the attribute name that is used to represent user IDs on that server. This attribute name is configured here.

  On Active Directory servers, this attribute name is usually **sAMAccountName**. On Novell eDirectory and OpenLDAP servers, it is usually uid. If this field is left blank, it defaults to **uid**.

  Group Filter - This field is used for group authentication. Group authentication is attempted after the user's credentials are successfully verified. If group authentication fails, the user's attempt to log on is denied. When the group filter is configured, it is used to specify to which groups the service processor belongs. This means that the user must belong to at least one of the groups that are configured for group authentication to succeed.

If the **Group Filter** field is left blank, group authentication automatically succeeds. If the group filter is configured, an attempt is made to match at least one group in the list to a group to which the user belongs. If there is no match, the user fails authentication and is denied access. If there is at least one match, group authentication is successful. The comparisons are case sensitive.

The filter is limited to 511 characters and can consist of one or more group names. The colon (:) character must be used to delimit multiple group names. Leading and trailing spaces are ignored, but any other space is treated as part of the group name. A selection to allow or not allow the use of wildcards in the group name is provided. The filter can be a specific group name (for example, IMMWest), a wildcard (*) that matches everything, or a wildcard with a prefix (for example, IMM*). The default filter is IMM*. If security policies in your installation prohibit the use of wildcards, you can choose to not allow the use of wildcards, and the wildcard character (*) is treated as a normal character instead of the wildcard.

A group name can be specified as a full DN or using only the cn portion. For example, a group with a DN of cn=adminGroup,dc=mycompany,dc=com can be specified using the actual DN or with adminGroup.

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

Binding Method - Before the LDAP server can be searched or queried, a bind request must be sent. This parameter controls how this initial bind to the LDAP server is performed. Choose from the following three options:

- **Anonymously**. Bind without a DN or password. This option is strongly discouraged because most servers are configured to not allow search requests on specific user records.
- **w/ Configured Credentials**. Bind with configured client DN and password.
- **w/ Login Credentials**. Bind with the credentials that are supplied during the login process. The user ID can be provided through a Distinguished Name, a fully qualified domain name, or a user ID that matches the UID Search Attribute that is configured on the IMM.

If the initial bind is successful, a search is performed to find an entry on the LDAP server that belongs to the user who is logging in. If necessary, a second attempt to bind is attempted, this time with the DN that is retrieved from the user's LDAP record and the password that was entered during the login process. If this fails, the user is denied access. The second bind is performed only when the Anonymous or Configured Credentials binding methods are used.

Configuring LDAP client authentication

To configure the LDAP client authentication, complete the following steps:

Step 1 In the navigation pane, click **Network protocols**.

Step 2 Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area of the page and click **Set DN and password only if Binding Method used is w/ Configured Credentials**.

Step 3 To use client-based authentication, in the **Client DN** field, type a client distinguished name. Type a password in the **Password** field or leave it blank.

Configuring LDAP search attributes

To configure the LDAP search attributes, complete the following steps:

Step 1 In the navigation pane, click **Network protocols**.

Step 2 Scroll down to the **Lightweight Directory Access Protocol (LDAP) Client** area and click **Set attribute names for LDAP client search algorithm**.

Step 3 To configure the search attributes, use the following information.

UID Search Attribute - When the selected binding method is **Anonymously** or **w/ Configured Credentials**, the initial bind to the LDAP server is followed by a search request that is directed at retrieving specific information about the user, including the distinguished name, login permissions, and group membership. To retrieve this information, the search request must specify the attribute name that is used to represent user IDs on that server. Specifically, this name is used as a search filter against the login ID that is entered by the user. This attribute name is configured here. For example, on Active Directory servers, the attribute name that is used for user IDs is usually sAMAccoutName. On Novell eDirectory and OpenLDAP servers, it is usually uid. If this field is left blank, a default of UID is used during user authentication.

Group Search Attribute - In an Active Directory or Novell eDirectory environment, this parameter specifies the attribute name that is used to identify the groups to which a user belongs. In Active Directory, this is usually memberOf, and with eDirectory, this is usually groupMembership.

In an OpenLDAP server environment, users are usually assigned to groups whose objectClass equals PosixGroup. In that context, this parameter specifies the attribute name that is used to identify the members of a particular PosixGroup. This is usually memberUid.

If this field is left blank, the attribute name in the filter defaults to memberOf.

Login Permission Attribute - When a user is authenticated through an LDAP server successfully, the login permissions for this user must be retrieved. To retrieve these permissions, the search filter that is sent to the server must specify the attribute name that is associated with login permissions. This field specifies this attribute name.

If this field is left blank, the user is assigned a default of read-only permissions, assuming that the user passes the user and group authentication.

The attribute value that is returned by the LDAP server is searched for the keyword string IBMRBSPermissions=. This keyword must be immediately followed by a bit string that is entered as 12 consecutive 0s or 1s. Each bit represents a set of functions. The bits are numbered according to their positions. The leftmost bit is bit position 0, and the rightmost bit is bit position 11. A value of 1 at a position enables the function that is associated with that position. A value of 0 disables that function. The string IBMRBSPermissions=010000000000 is a valid example.

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

When the attribute is retrieved successfully, the value that is returned by the LDAP server is interpreted according to the following information:

- **Deny Always (bit position 0):** If this bit is set, the user always fails authentication. This function can be used to block a user or users who are associated with a particular group.

- **Supervisor Access (bit position 1):** If this bit is set, the user is given administrator privileges. The user has read and write access to every function. When this bit is set, bits 2 through 11 do not have to be set individually.
- **Read Only Access (bit position 2):** If this bit is set, the user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates) or modify anything (using the save, clear, or restore functions). The Read Only Access bit and all other bits are mutually exclusive, with the Read Only Access bit having the lowest precedence. If any other bit is set, the Read Only Access bit is ignored.
- **Networking and Security (bit position 3):** If this bit is set, the user can modify the configuration on the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages.
- **User Account Management (bit position 4):** If this bit is set, the user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page.
- **Remote Console Access (bit position 5):** If this bit is set, the user can access the remote server console.
- **Remote Console and Remote Disk (bit position 6):** If this bit is set, the user can access the remote server console and the remote disk functions for the remote server.
- **Remote Server Power/Restart Access (bit position 7):** If this bit is set, the user can access the power-on and restart functions for the remote server. These functions are available in the Power/Restart page.
- **Basic Adapter Configuration (bit position 8):** If this bit is set, the user can modify configuration parameters on the System Settings and Alerts pages.
- **Ability to Clear Event Logs (bit position 9):** If this bit is set, the user can clear the event logs. All users can view the event logs, but this particular permission is required to clear the logs.
- **Advanced Adapter Configuration (bit position 10):** If this bit is set, the 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 upgrades, PXE network boot, restoring IMM factory defaults, modifying and restoring IMM configuration from a configuration file, and restarting and resetting the IMM.
- **Reserved (bit position 11):** This bit is reserved for future use.

If none of the bits are set, the user has read-only authority.

Priority is given to login permissions that are retrieved directly from the user record. If the login permission attribute is not in the user's record, an attempt is made to retrieve the permissions from the groups to which the user belongs. This is done as part of the group authentication phase. The user is assigned the inclusive OR of all the bits for all of the groups. The Read Only bit is set only if all the other bits are zero. If the Deny Always bit is set for any of the groups, the user is refused access. The Deny Always bit always has precedence over every other bit.

Important: If you give a user the ability to modify basic, networking, and security-related IMM configuration parameters, consider giving this same user the ability to restart the IMM (bit position 10). Otherwise, a user might be able to change parameters (for example, the IP address of the IMM) but cannot make them take effect.

Service Location Protocol (SLP)

To view the SLP setting, complete the following steps:

Step 1 In the navigation pane, click **Network protocols**.

Step 2 Scroll down to the **Service Location Protocol (SLP)** area. The multicast address, which is the IP address that the IMM SLP server listens on, is displayed.

Configuring security

Use the general procedure in this section to configure security for the IMM Web server 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" section on page 3-32.

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" section on page 3-32).
   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" section on page 3-37).
2. 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 client certificate management" section on page 3-37).
   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" section on page 3-37).
   d. Enable the SSL client. Use the **SSL Client Configuration for LDAP Client** area on the Security page (see "Enabling SSL for the LDAP client" section on page 3-38).
3. Restart the IMM for SSL server configuration changes to take effect. For more information, see "Restarting IMM" section on page 3-42.

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

Secure Web server 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 3-3 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 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

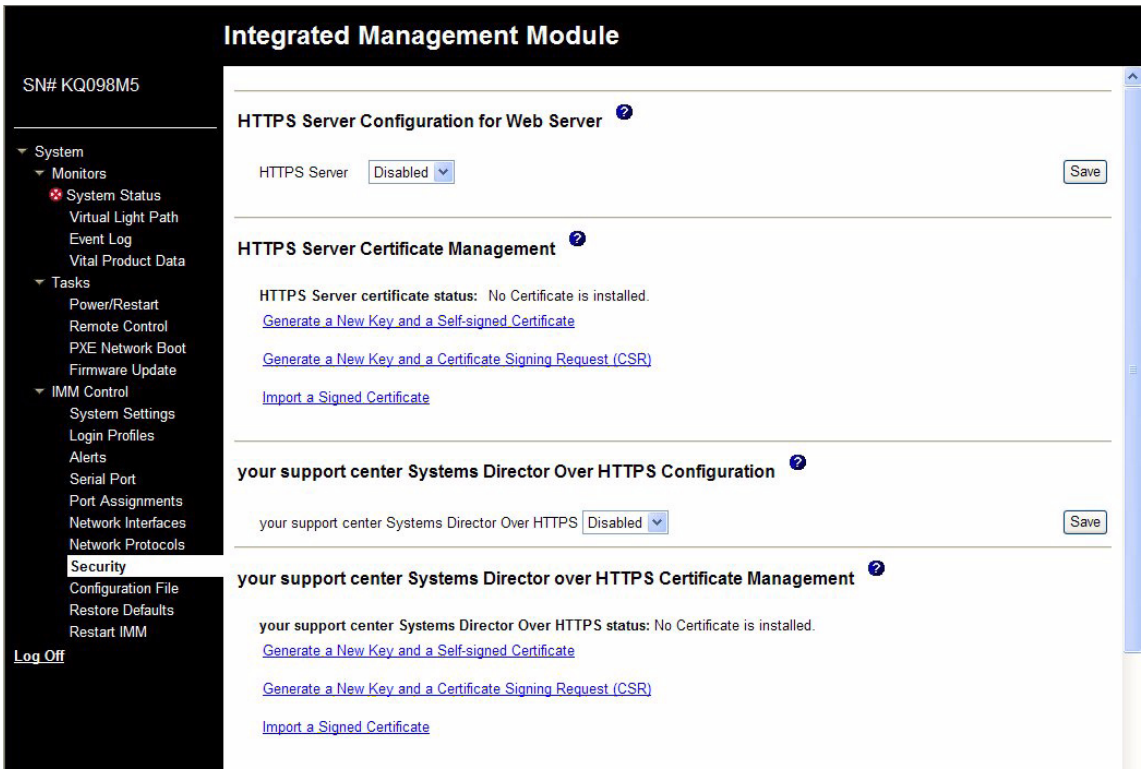
The SSL server requires that a valid certificate and corresponding private encryption key be installed before SSL is enabled. Two methods are available for generating the private key and required certificate: using a self-signed certificate and using a certificate that is signed by a certificate authority.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

to use a self-signed certificate for the SSL server, see "Generating a self-signed certificate" section on page 3-33. If you want to use a certificate-authority-signed certificate for the SSL server, see "Generating a certificate-signing request" section on page 3-34.

Generating a self-signed certificate

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

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



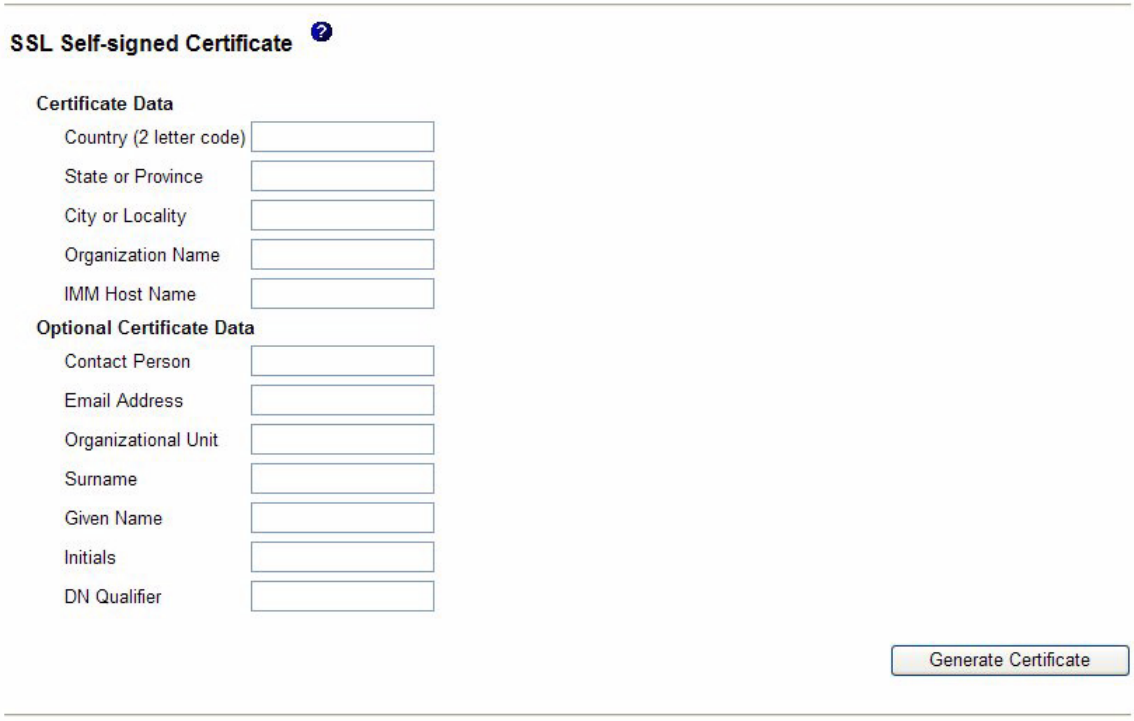
Step 2 In the **SSL Server Configuration for Web Server** area, make sure that the setting is **Disabled**. If it is not disabled, select **Disabled** and then click **Save**.

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

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

Note 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.

Step 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.



Step 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, page 3-35. 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:

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

Step 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**.

Step 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.

Step 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.

Step 5 After you complete the information, click **Generate CSR**. The new encryption keys and certificate are generated. This process might take several minutes.

Step 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
```

Step 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 Web page, 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.

Step 8 In the navigation pane, click **Security**. Scroll to the **SSL Server Certificate Management** area.

Step 9 Click **Import a Signed Certificate**.

Step 10 Click **Browse**.

Step 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.

Step 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

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

Complete the following steps to enable the secure Web server:

Step 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" section on page 3-32.

Step 2 Scroll to the **SSL Server Configuration for Web Server** 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 Web page 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" section on page 3-33. If you want to use a certificate authority signed certificate for the SSL client, see "Generating a certificate-signing request" section on page 3-34.

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:

Step 1 In the navigation pane, select **Security**.

Step 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**.

Step 3 Scroll to the **SSL Client Trusted Certificate Management** area.

Step 4 Click **Import** next to one of the **Trusted CA Certificate 1** fields.

Step 5 Click **Browse**.

Step 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.

Step 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:

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

The Security page shows an installed SSL client certificate and Trusted CA Certificate 1.

Step 2 On the SSL Client Configuration for LDAP Client page, select **Enabled** in the **SSL Client** field.

Note The selected value (Enabled or Disabled) takes effect immediately.

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

Note Your LDAP server must support SSL3 or TLS to be compatible with the SSL implementation that the LDAP client uses.

Step 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:

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

Step 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.

Step 3 Scroll to the **SSH Server Key Management** area.

Step 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:

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

Step 2 Scroll to the **Secure Shell (SSH) Server** area.

Step 3 Click **Enabled** in the **SSH Server** field.

Step 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*.

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:

Step 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”.

Step 2 In the navigation pane, click **Configuration File**.

Step 3 In the **Backup IMM Configuration** area, click **View the current configuration summary**.

Step 4 Verify the settings and then click **Close**.

Step 5 To back up this configuration, click **Backup**.

Step 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:

Step 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".

Step 2 In the navigation pane, click **Configuration File**.

Step 3 In the **Restore IMM Configuration** area, click **Browse**.

Step 4 Click the configuration file that you want; then, click **Open**. The file (including the full path) appears in the box next to **Browse**.

Step 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.

Step 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 and secure LDAP" section on page 3-31.

Step 7 After you receive a confirmation that the restore process is complete, in the navigation pane, click **Restart IMM**; then, click **Restart**.

Step 8 Click **OK** to confirm that you want to restart the IMM.

Step 9 Click **OK** to close the current browser window.

Step 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:

Step 1 Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 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.

Step 3 Log in again to use the IMM Web interface.

Step 4 Reconfigure the network interface to restore connectivity. For information about the network interface, see "Configuring network interfaces" section on page 3-19.

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:

Step 1 Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 2 In the navigation pane, click **Restart IMM** to restart the IMM. Your TCP/IP or modem connections are broken.

Step 3 Log in again to use the IMM Web interface.

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.

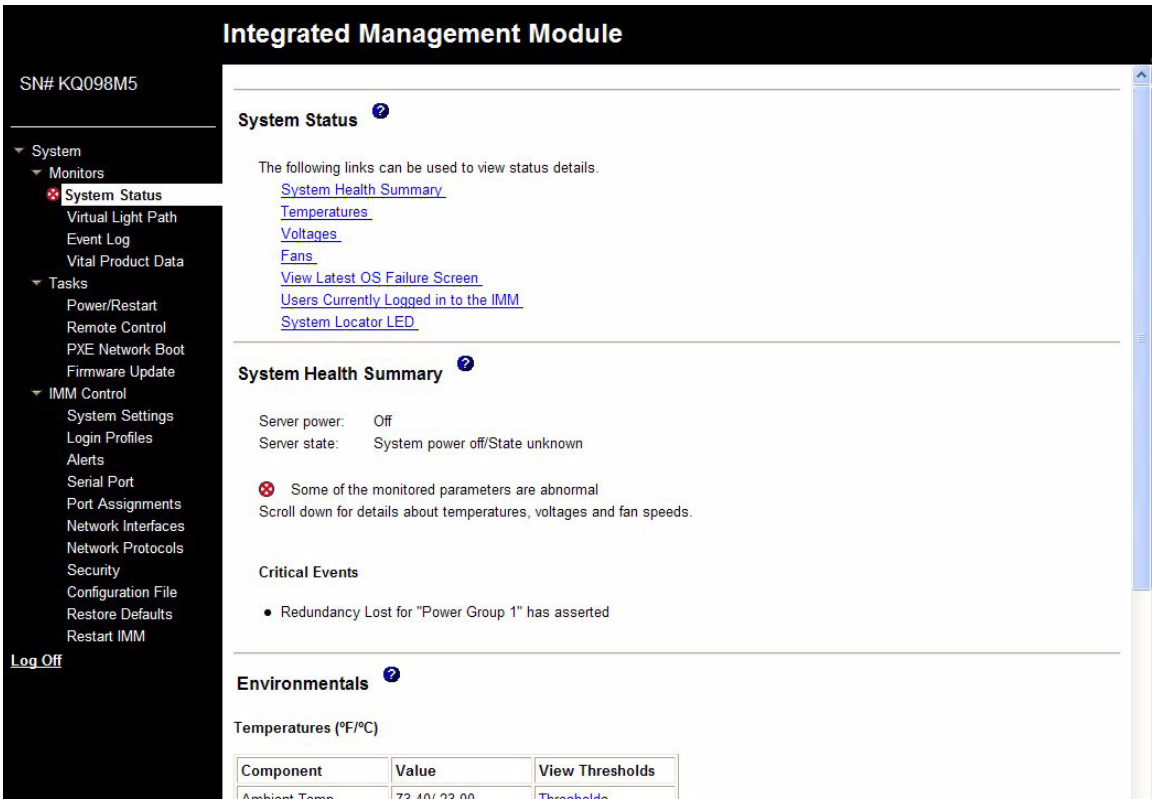
Viewing system status

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:

Step 1 Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 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.

Step 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.

Ambient Temp Thresholds (°F / °C)

Sensors	Noncritical	Critical	Fatal
Upper Threshold	100.40 / 38.00	105.80 / 41.00	113.00 / 45.00
Lower Threshold	N/A	N/A	N/A

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 the "Configuring SNMP alert settings" section on page 3-16 or the "Configuring remote alert recipients" section on page 3-14.

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 the"Configuring SNMP alert settings" section on page 3-16 or the "Configuring remote alert recipients" section on page 3-14.

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 the "Configuring SNMP alert settings" section on page 3-16 or the "Configuring remote alert recipients" section on page 3-14.

Step 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	Noncritical	Critical	Fatal
Upper Threshold	N/A	3.56	N/A
Lower Threshold	N/A	3.04	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 the "Configuring SNMP alert settings" section on page 3-16.

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 the"Configuring SNMP alert settings" section on page 3-16.

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 **Fatal 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" section on page 3-16.

The IMM generates a non-critical, critical, or fatal 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.

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

Step 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.

Fan 1A Tach Thresholds (RPM)

Sensors	Noncritical	Critical	Fatal
Upper Threshold	N/A	N/A	N/A
Lower Threshold	N/A	530.00	N/A

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 the "Configuring SNMP alert settings" section on page 3-16.

Note The **View Latest OS Failure Screen** feature is not supported.

Step 6 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.

Step 7 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.

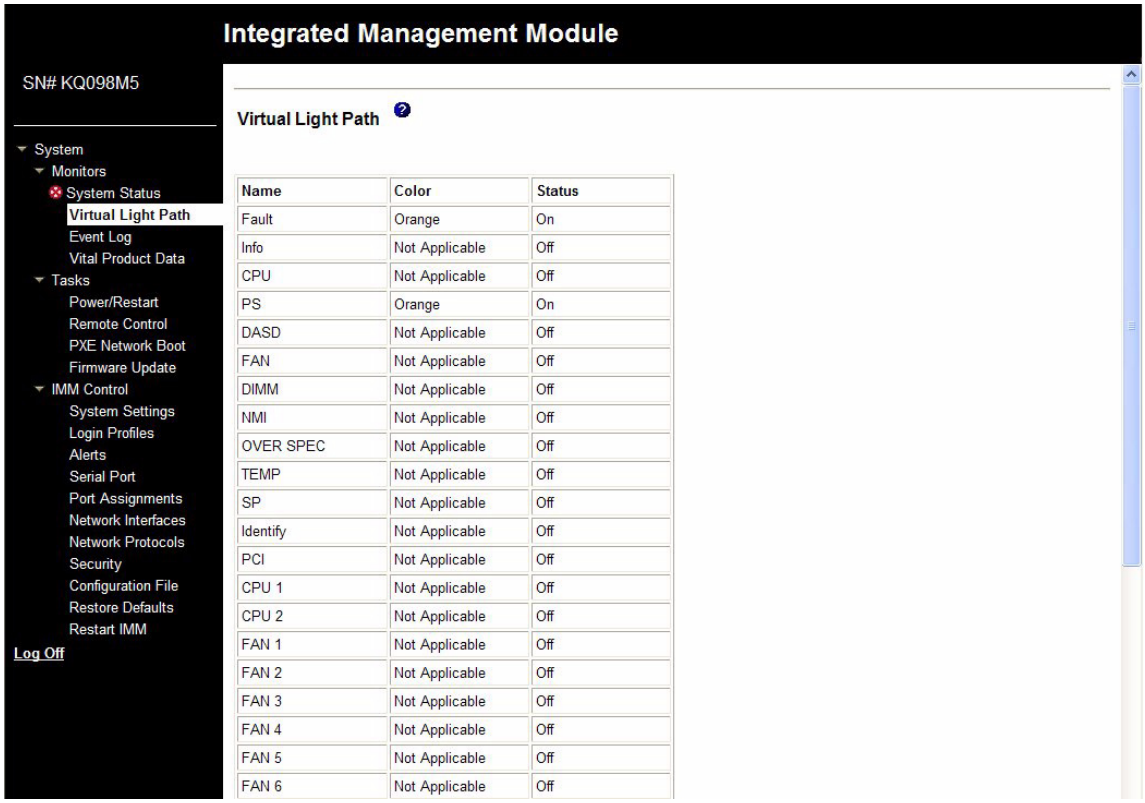
Viewing the Virtual Light Path

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:

Step 1 Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 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.



Name	Color	Status
Fault	Orange	On
Info	Not Applicable	Off
CPU	Not Applicable	Off
PS	Orange	On
DASD	Not Applicable	Off
FAN	Not Applicable	Off
DIMM	Not Applicable	Off
NMI	Not Applicable	Off
OVER SPEC	Not Applicable	Off
TEMP	Not Applicable	Off
SP	Not Applicable	Off
Identify	Not Applicable	Off
PCI	Not Applicable	Off
CPU 1	Not Applicable	Off
CPU 2	Not Applicable	Off
FAN 1	Not Applicable	Off
FAN 2	Not Applicable	Off
FAN 3	Not Applicable	Off
FAN 4	Not Applicable	Off
FAN 5	Not Applicable	Off
FAN 6	Not Applicable	Off

Step 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.

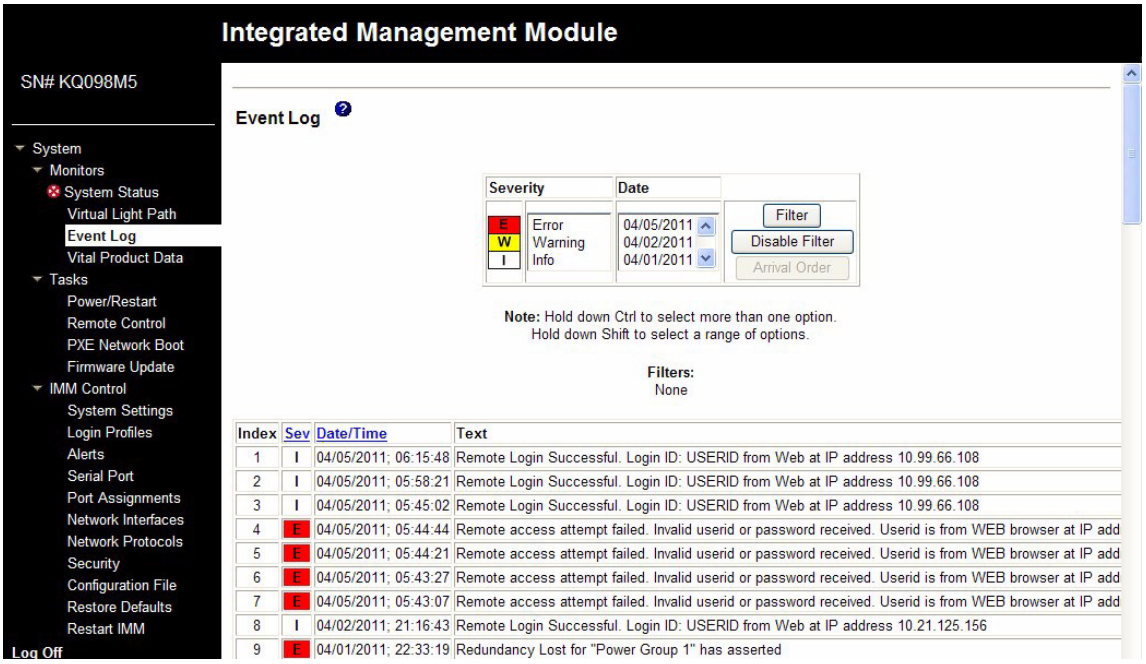
Viewing the system-event log from the Web interface

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:

Step 1 Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 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.



Step 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.

Step 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 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:

Step 1 Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 2 In the navigation pane, click **Vital Product Data** to view the status of the hardware and software components on the server.

Step 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 4-1 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 4-2 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 4-3 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.

Table 4-3 Component activity log

Field	Function
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 4-4 Component-level 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

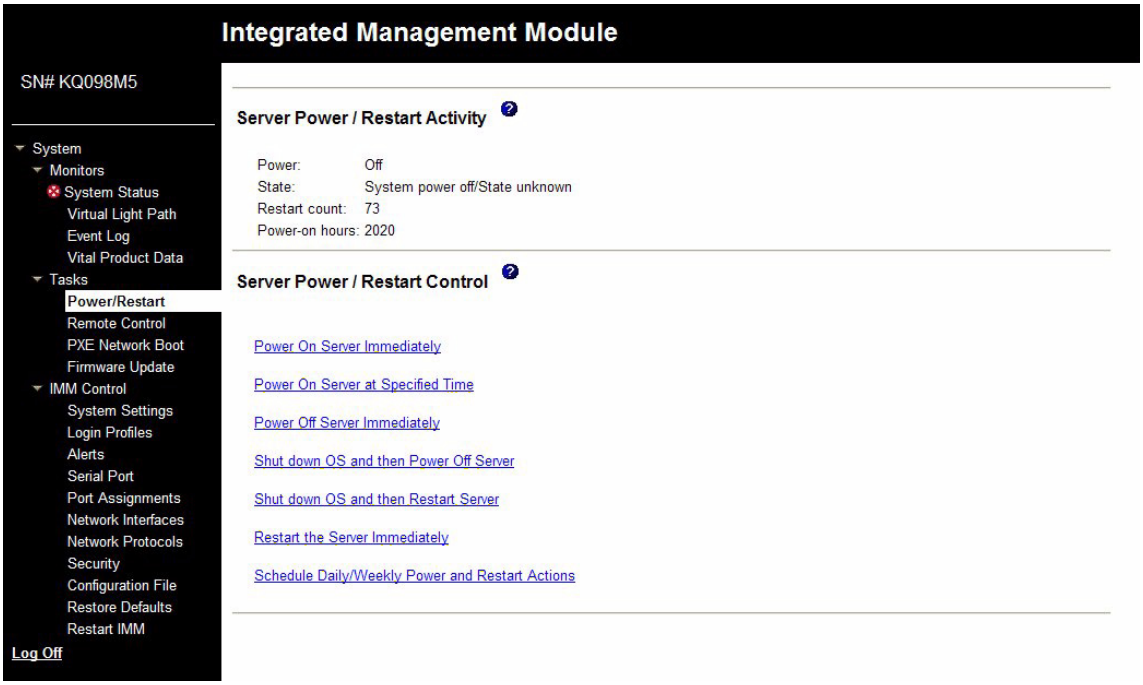
Use the functions under the **Tasks** heading in the navigation pane to directly control the actions of the IMM and your server. The tasks that you can perform depend on the server in which the IMM is installed.

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

Viewing server power and restart activity

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



Power - This field shows the power status of the server when the current Web page was generated.

State - This field shows the state of the server when the current Web page 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 Contro**l 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 off-site and the server is nonresponsive.

Step 1 Log in to the IMM. For more information, see Chapter 2, "Opening and using the IMM Web interface".

Step 2 In the navigation pane, click **Power/Restart.** Scroll down to the **Server Power/Restart Control** area.

Step 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.

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

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 using 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 IPMItool to issue commands to control server power, view server information, and identify the server.

Accessing the command line

To access the command line, start a Telnet or SSH session to the IMM IP address.

Logging in to the command-line session

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

Step 1 Establish a connection with the IMM.

Step 2 At the user name prompt, type the user ID.

Step 3 At the password prompt, type the password that you use to log in to the 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

Description

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

help command

Description

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

Description

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

clearlog command

Description

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

Description

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

Syntax

```
readlog [options]
option:
-f
```

Description

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.

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

Description

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

Description

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

Description

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

Syntax

```
vpd sys
vpd IMM
vpd bios
vpd dsa
```

Description

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.

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

Syntax

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

Description

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.

reset command

Syntax

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

Description

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.

Configuration commands

The configuration commands are as follows:

- dhcpinfo
- ifconfig
- ldap
- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts
- usbeth
- users

dhcpinfo command

Syntax

```
dhcpinfo eth0
```

Description

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.

Example

```
system> dhcpinfo eth0
-server 192.168.70.29
-n IMMA00096B9E003A
-i 192.168.70.202
-g 192.168.70.29
-s 255.255.255.0
-d linux-test.cisco.com
-dns1 192.168.70.29
-dns2 0.0.0.0
-dns3 0.0.0.0
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 IP address
-g	Assigned gateway address
-s	Assigned subnet mask
-d	Assigned domain name
-dns1	Primary DNS server IP address
-dns2	Secondary DNS IP address
-dns3	Tertiary DNS server IP address

ifconfig command

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
```

Description

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	Valid IP address format
-g	Gateway address	Valid IP address format
-s	Subnet mask	Valid IP address format
-n	Host name	String of up to 63 characters. Can include letters, digits, periods, underscores, and hyphens.
-r	Data rate	10, 100, auto
-d	Duplex mode	full, half, auto
-m	MTU	Numeric between 60 and 1500
-l	LAA	MAC address format. Multicast addresses are not allowed (the first byte must be even).

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

Syntax

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

Description

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

The following table shows the arguments for the options.

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

Option	Description	Values
-pc	Confirm client password	String of up to 15 characters for *confirm_pw* Command usage is: ldap -p *client_pw* -pc *confirm_pw* This option is required when you change the client password. It compares the *confirm_pw* argument with the *client_pw* argument, and the command will fail if they do not match.
-r	Root entry distinguished name (DN)	String of up to 63 characters for *root_dn*
s1ip	Server 1 host name/IP address	String up to 63 characters or an IP address for *host* name/ip_addr
s2ip	Server 2 host name/IP address	String up to 63 characters or an IP address for *host* name/ip_addr
s3ip	Server 3 host name/IP address	String up to 63 characters or an IP address for *host* name/ip_addr
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*.
-u	UID search attribute String	String of up to 23 characters for *search_attrib*
-v	Get LDAP server address through DNS	Off, on
-w	Allows wildcards in the group name	Off, on
-h	Displays the command usage and options	

ntp command

Syntax

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

Description

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
-synch	Requests an immediate synchronization with the Network Time Protocol server	No values are used with this parameter.

Example

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

passwordcfg command

Syntax

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

Description

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)

Option	Description
-nul	Allows accounts with no password (yes | no)
-h	Displays the command usage and options

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

Syntax

```
portcfg [options]
portcfg [options]
options:
-b baud_rate
-climode cli_mode
-cliauth cli_auth
```

Description

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	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

Example

```
system> portcfg
-b       : 115200
-climode : 2 (CLI with user defined keystroke sequences) system>
system>
```

srcfg command

Syntax

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

Description

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.

Example

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

ssl command

Syntax

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

Description

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

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

Option	Description
-ce	Enables or disables an SSL client
-se	Enables or disables an SSL server
-h	Lists usage and options

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

Syntax

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

Description

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

Example

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

```
-l 3.5
```

usbeth command

Syntax

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

Description

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" section on page 3-6.

Example

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

users command

Syntax

```
users [options]
options:
-user number
-n username
-p password
-a authority level
```

Description

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])

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

Description

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

Syntax

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

Description

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.

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

Syntax

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

Description

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.

Example

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

resetsp command

Description

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