XClarity Controller 3
User's Guide

Note: Before using this information, read the general information in Appendix B "Notices" on page 203.

Third Edition (January 2025)

Contents

Chapter 1. Introduction

The Lenovo XClarity Controller 3 (XCC3) is the next generation management controller for Lenovo ThinkSystem servers.

The controller consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board. It provides features such as the following:

- Choice of a dedicated or shared Ethernet connection for systems management
- Support for HTML5
- Support for access via XClarity Mobile
- XClarity Provisioning Manager
- Remote configuration using XClarity Essentials or XClarity Controller CLI.
- Capability for applications and tools to access the XClarity Controller either locally or remotely
- Enhanced remote-presence capabilities.
- REST API (Redfish schema) support for additional web-related services and software applications.

Notes:

- The XClarity Controller currently supports Redfish Scalable Platforms Management API Specification 1.16.0 and schema 2022.2
- In the XClarity Controller web interface, BMC is used in referring to the XCC.
- A dedicated systems-management network port may not be available on some ThinkSystem servers; for these servers access to the XClarity Controller is only available through a network port that is shared with the server operating system.

This document explains how to use the functions of the XClarity Controller in a ThinkSystem server. The XClarity Controller works with the XClarity Provisioning Manager and UEFI to provide systems-management capability for ThinkSystem servers.

To check for firmware updates, complete the following steps.

Note: The first time you access the Support Portal, you must choose the product category, product family, and model numbers for your server. The next time you access the Support Portal, the products you selected initially are preloaded by the website, and only the links for your products are displayed. To change or add to your product list, click the **Manage my product lists** link. Changes are made periodically to the website. Procedures for locating firmware and documentation might vary slightly from what is described in this document.

1. Go to http://datacentersupport.lenovo.com.
2. Under **Support**, select **Data Center**.
3. When the content is loaded, select **Servers**.
4. Under **Select Series**, first select the particular server hardware series, then under **Select SubSeries**, select the particular server product subseries, and finally, under **Select Machine Type** select the particular machine type.

XClarity Controller Standard and Premier level features

With the XClarity Controller, Standard and Premier levels of XClarity Controller functionality are offered. See the documentation for your server for more information about the level of XClarity Controller installed in your server. All levels provide the following:

- Around-the-clock remote access and management of your server
- Remote management independent of the status of the managed server
- Remote control of hardware and operating systems

XClarity Controller Standard level features

The following is a list of XClarity Controller Standard level features:

Industry Standard Management Interfaces

- IPMI 2.0 Interface
- Redfish
- DCMI 1.5
- SNMPv3

Other Management Interfaces

- Web
- SSH CLI
- Front Panel USB - virtual operator panel via mobile device

Power / Reset Control

- Power On
- Hard/Soft Shutdown
- Scheduled Power Control
- System Reset
- Boot Order Control

Event Logs

- IPMI SEL
- Human Readable Log
- Audit Log
- Mini-log

Environmental Monitoring

- Agent Free Monitoring
- Sensor Monitoring
- Fan Control
- LED Control
- Chipset Errors (Caterr, IERR, etc.)
- System Health Indication

- OOB Performance Monitoring for I/O adapters
- Inventory Display and Export

RAS

- Virtual NMI
- Automatic Firmware Recovery
- Automated promotion of backup firmware
- POST Watchdog
- OS Loader Watchdog
- OS Watchdog
- Blue Screen Capture (OS Failure, in FFDC)
- Embedded Diagnostic Tools
- Call Home

Network Configuration

- IPv4
- IPv6
- IP Address, Subnet Mask, Gateway
- IP Address Assignment Modes
- Host name
- Programmable MAC address
- Dual MAC Selection (if supported by server hardware)
- Network Port Reassignments
- VLAN Tagging

Network Protocols

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SSL
- SSH
- SMTP
- LDAP client
- NTP
- SSDP
- LLDP

Alerts

- PET Traps
- SNMP v1, v2c and v3 TRAPs

- E-mail
- Redfish Notification Subscriptions

Remote Presence

- Remote Disk On Card (RDOC)

Serial Redirection

- IPMI SOL
- Serial port configuration including authority and speed
- Serial console buffer (120s)

Security

- Non-host processor CRTM
- Digitally signed firmware updates
- Role Based Access Control (RBAC)
- Local User Accounts
- LDAP/AD User Accounts
- Secure Rollback of Firmware
- NIST SP 800-131a
- Chassis intrusion detection (if supported by server hardware)
- Only secure, encrypted protocols enabled
- Audit logging of configuration changes and server actions
- Public-key (PK) Authentication
- System Retire/Repurpose (RTD/ERTD)
- PFR support
- FIPS 140-3
- Security Modes and Security Dashboard
- Secure Password Storage

Power Management

- Real time Power Meter

Features on Demand

- Activation Key Repository

Deployment & Configuration

- Remote Configuration
- OS pass-through
- Embedded Deployment & Configuration Tools and Driver Packs
- Configuration Backup and Restore
- Extended RDOC size (with MicroSD card)
- Configurable thermal profiles

Firmware Updates

- Agent Free Update
- Remote Update

XClarity Controller Premier level features

The following is a list of XClarity Controller Premier level features:

All of the "XClarity Controller Standard level features" on page 2.

Event Logs

- Component Replacement Log

RAS

- Boot Capture
- Crash Video Capture

Alerts

- Syslog

Remote Presence

- Remote KVM
- Mounting of local client ISO/IMG files
- Quality/Bandwidth Control
- Virtual Media mounting of remote ISO/IMG files http, Samba & NFS

Serial Redirection

- Serial Redirection via SSH-CLI

Security

- Single Sign-On
- Security Key Lifecycle Manager (SKLM/KMIP)
- IP address blocking
- Enterprise Strict Security mode (CNSA compliant)
- System Guard

Power Management

- Power Capping
- OOB Performance Monitoring - System Performance metrics
- Real time Power Graphics
- Historical Power Counters
- Temperature Graphics

Deployment & Configuration

- Remote OS Deployment

Firmware Updates

- Sync with Repository
- System Pack Firmware Bundle Update
- Firmware rollback from the local repository in MicroSD card

Upgrading XClarity Controller

If your server came with the Standard level of the XClarity Controller firmware functionality, you might be able to upgrade the XClarity Controller functionality in your server. For more information about available upgrade levels and how to order, see Chapter 9 “License Management” on page 87.

Web browser and operating-system requirements

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

The XClarity Controller web interface requires one of the following web browsers:

- Chrome 64.0 or above (64.0 or above for Remote Console)
- Firefox ESR 78.0 or above
- Microsoft Edge 79.0 or above
- Safari 12.0 or above (iOS 7 or later and OS X)

Note: Support for the remote console feature is not available through the browser on mobile device operating systems.

The browsers listed above match those currently supported by the XClarity Controller firmware. The XClarity Controller firmware may be enhanced periodically to include support for other browsers.

Depending upon the version of the firmware in the XClarity Controller, web browser support can vary from the browsers listed in this section. To see the list of supported browsers for the firmware that is currently on the XClarity Controller, click the **Supported Browsers** menu list from the XClarity Controller login page.

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

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

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

Multiple language support

Use the information in this topic to view the list of languages supported by the XClarity Controller.

By default, the chosen language for the XClarity Controller web interface is English. The interface is capable of displaying multiple languages. These include the following:

- French
- German
- Italian
- Japanese
- Korean
- Portuguese (Brazil)
- Russian
- Simplified Chinese
- Spanish (International)
- Traditional Chinese

To choose the language of your preference, click the arrow beside the currently selected language. A drop-down menu will appear to let you choose your preferred language.

Text strings that are generated by the XClarity Controller firmware are displayed in the language dictated by the browser. If the browser specifies a language other than one of the translated languages listed above, the text is displayed in English. In addition, any text string that is displayed by the XClarity Controller firmware, but is not generated by the XClarity Controller (for example messages generated by UEFI, PCIe adapters, etc…) are displayed in English.

The input of language-specific text other than English, such as the **Trespass message** is currently not supported. Only text typed in English is supported.

MIBs Introduction

Use the information in this topic to access Management Information Base.

The SNMP MIBs can be downloaded from the https://support.lenovo.com/ (Search by machine type on the portal). It includes the following four MIBs.

- The **SMI MIB** describes the Structure of Management Information for the Lenovo Data Center Group.
- The **Product MIB** describes the object identifier for Lenovo Products.
- The **XCC MIB** provides the inventory and monitoring information for Lenovo XClarity Controller.
- The **XCC Alert MIB** defines traps for alert conditions detected by Lenovo XClarity Controller.

Note: The import order for the four MIBs is **SMI MIB** → **Product MIB** → **XCC MIB** → **XCC Alert MIB**.

Notices used in this document

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

The following notices are used in the documentation:

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

Chapter 2. Opening and Using the XClarity Controller Web Interface

This topic describes the login procedures and the actions that you can perform from the XClarity Controller web interface.

The XClarity Controller combines service processor functions, a video controller, and remote presence function in a single chip. You must first log in using the XClarity Controller web interface to access the XClarity Controller remotely. This chapter describes the login procedures and the actions that you can perform from the XClarity Controller web interface.

Accessing the XClarity Controller web interface

The information in this topic explains how to access the XClarity Controller web interface.

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

The XClarity Controller also supports IPv6, but it does not have a fixed static IPv6 IP address by default. For initial access to the XClarity Controller in an IPv6 environment, you can either use the IPv4 IP address or the IPv6 link-local address. The XClarity Controller generates a unique link-local IPv6 address, using the IEEE 802 MAC address by inserting two octets, with hexadecimal values of 0xFF and 0xFE in the middle of the 48-bit MAC as described in RFC4291 and flipping the 2nd bit from the right in the first octet of the MAC address. For example if the MAC address is 08-94-ef-2f-28-af, the link-local address would be as follows:

```
fe80::0a94:efff:fe2f:28af
```

When you access the XClarity Controller, the following IPv6 conditions are set as default:

- Automatic IPv6 address configuration is enabled.
- IPv6 static IP address configuration is disabled.
- DHCPv6 is enabled.
- Stateless auto-configuration is enabled.

The XClarity Controller provides the choice of using a **dedicated** systems-management network connection (if applicable) or one that is **shared** with the server. The default connection for rack-mounted and tower servers is to use the **dedicated** systems-management network connector.

The dedicated systems-management network connection on most servers is provided using a separate 1Gbit network interface controller. However, on some systems the dedicated systems-management network connection may be provided using the Network Controller Sideband Interface (NCSI) to one of the network ports of a multi-port network interface controller. In this case, the dedicated systems-management network connection is limited to the 10/100 speed of the sideband interface. For information and any limitations on the implementation of the management port on your system, see your system documentation.

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

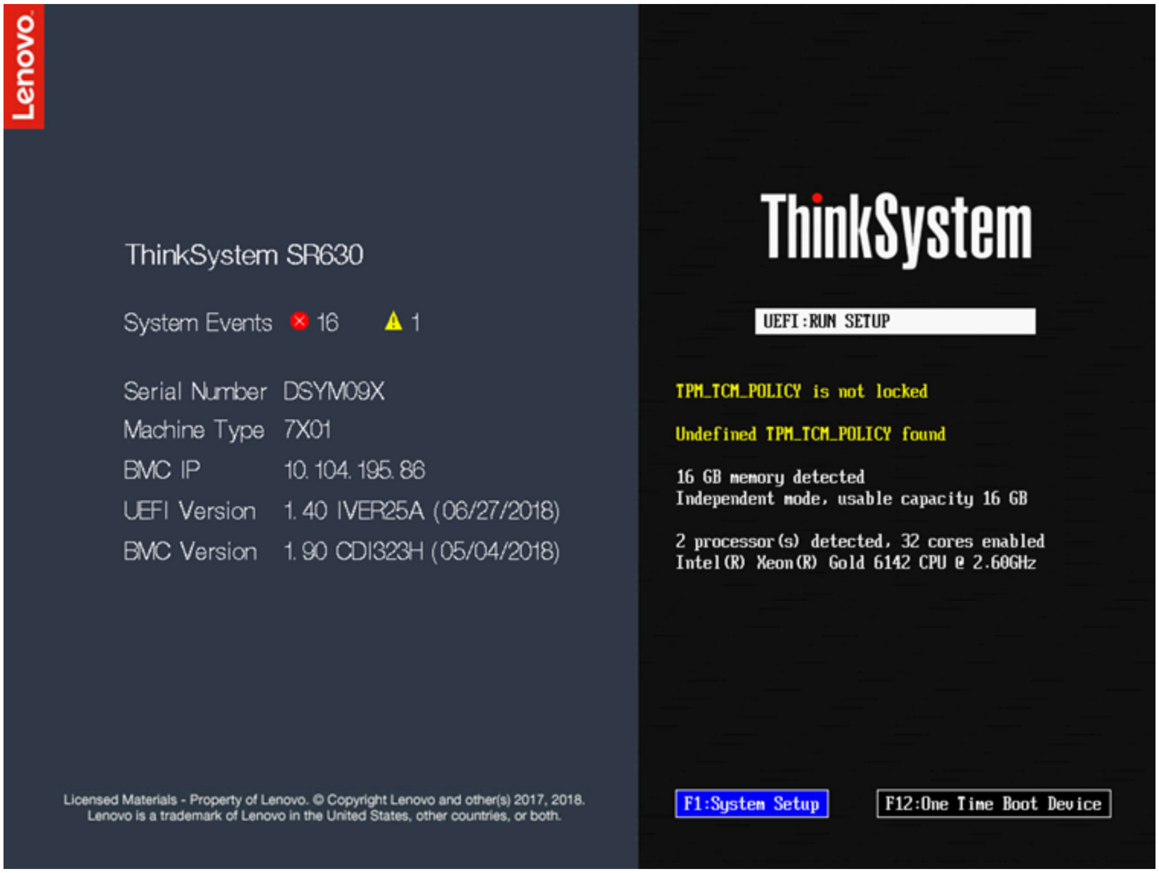
Setting up the XClarity Controller network connection through the XClarity Provisioning Manager

Use the information in this topic to set up an XClarity Controller network connection through the XClarity Provisioning Manager.

After you start the server, you can use the XClarity Provisioning Manager to configure the XClarity Controller network connection. The server with the XClarity Controller must be connected to a DHCP server, or the server network must be configured to use the XClarity Controller static IP address. To set up the XClarity Controller network connection through the Setup utility, complete the following steps:

Step 1. Turn on the server. The ThinkSystem welcome screen is displayed.

Note: It may take up to 40 seconds after the server is connected to AC power for the power-control button to become active.



ThinkSystem SR630

System Events ✖ 16 ⚠ 1

Serial Number DSYM09X
Machine Type 7X01
BMC IP 10.104.195.86
UEFI Version 1.40 IVER25A (06/27/2018)
BMC Version 1.90 CDI323H (05/04/2018)

```
TPM_TCM_POLICY is not locked

Undefined TPM_TCM_POLICY found

16 GB memory detected
Independent mode, usable capacity 16 GB

2 processor(s) detected, 32 cores enabled
Intel(R) Xeon(R) Gold 6142 CPU @ 2.60GHz
```

Licensed Materials - Property of Lenovo. © Copyright Lenovo and other(s) 2017, 2018.
Lenovo is a trademark of Lenovo in the United States, other countries, or both.

Figure 1. Welcome screen of ThinkSystem

Step 2. When the prompt `<F1> System Setup` is displayed, press F1. If you have set both a power-on password and an administrator password, you must type the administrator password to access the XClarity Provisioning Manager.

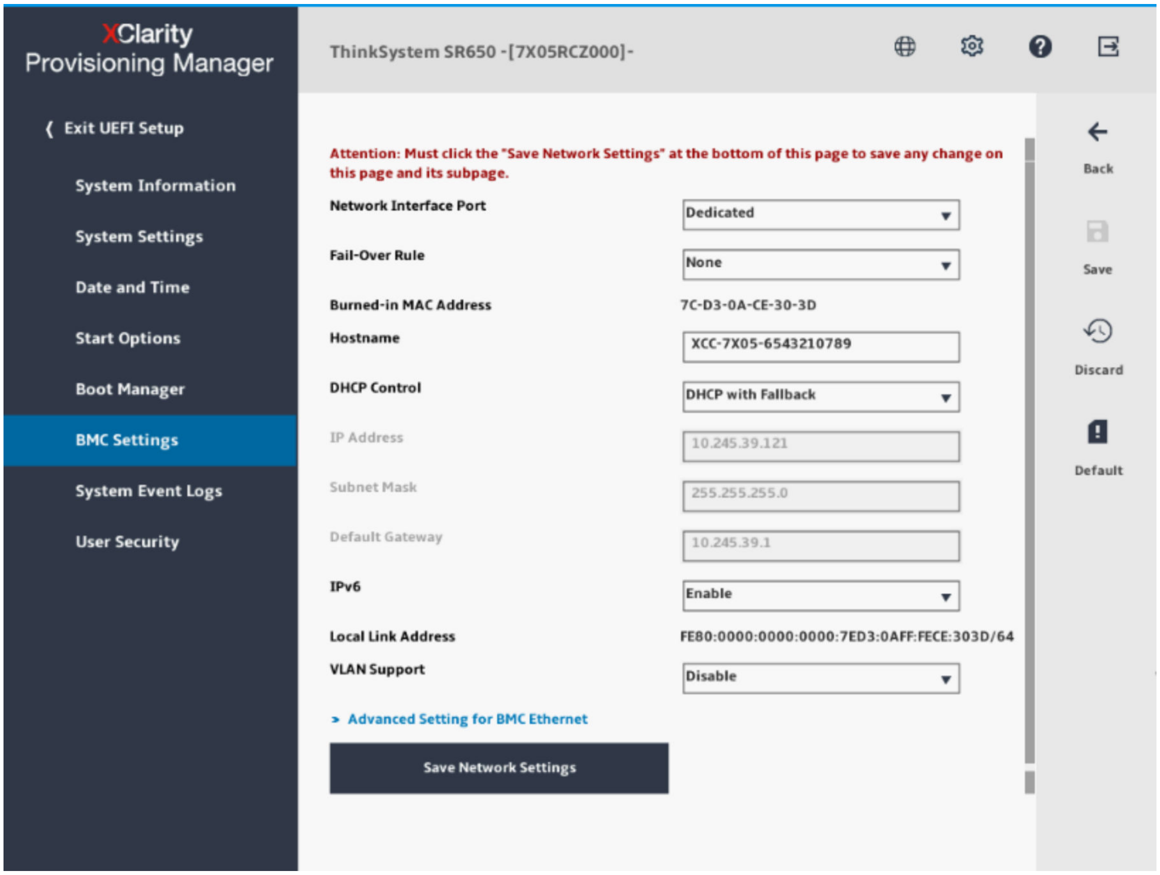
Step 3. From the XClarity Provisioning Manager main menu, select **UEFI Setup**.

Step 4. On the next screen, select **BMC Settings**; then, click **Network Settings**.

Step 5. There are three XClarity Controller network connection choices in the **DHCP Control** field:

- Static IP

- DHCP Enabled
- DHCP with Fallback



Attention: Must click the "Save Network Settings" at the bottom of this page to save any change on this page and its subpage.

Network Interface Port	Dedicated ▾
Fail-Over Rule	None ▾
Burned-in MAC Address	7C-D3-0A-CE-30-3D
Hostname	XCC-7X05-6543210789
DHCP Control	DHCP with Fallback ▾
IP Address	10.245.39.121
Subnet Mask	255.255.255.0
Default Gateway	10.245.39.1
IPv6	Enable ▾
Local Link Address	FE80:0000:0000:0000:7ED3:0AFF:FECE:303D/64
VLAN Support	Disable ▾

> Advanced Setting for BMC Ethernet

Figure 2. Network connection settings

Step 6. Select one of the network connection choices.

Step 7. If you choose to use a static IP address, you must specify the IP address, the subnet mask, and the default gateway.

Step 8. You can also use the Lenovo XClarity Controller Manager to select a dedicated network connection (if your server has a dedicated network port) or a shared XClarity Controller network connection.

Notes:

- A dedicated systems-management network port might not be available on your server. If your hardware does not have a dedicated network port, the **shared** setting is the only XClarity Controller setting available. On the **Network Configuration** screen, select **Dedicated** (if applicable) or **Shared** in the **Network Interface Port** field.
- To find the locations of the Ethernet connectors on your server that are used by the XClarity Controller, see the documentation that came with your server.

Step 9. Click **Save**.

Step 10. Exit from the XClarity Provisioning Manager.

Notes:

- You must wait approximately 1 minute for changes to take effect before the server firmware is functional again.

- You can also configure the XClarity Controller network connection through the XClarity Controller web interface or command-line interface (CLI). In the XClarity Controller web interface, network connections can be configured by clicking **BMC Configuration** from the left navigation panel, and then selecting **Network**. In the XClarity Controller CLI, network connections are configured using several commands that depend on the configuration of your installation.

Logging in to the XClarity Controller

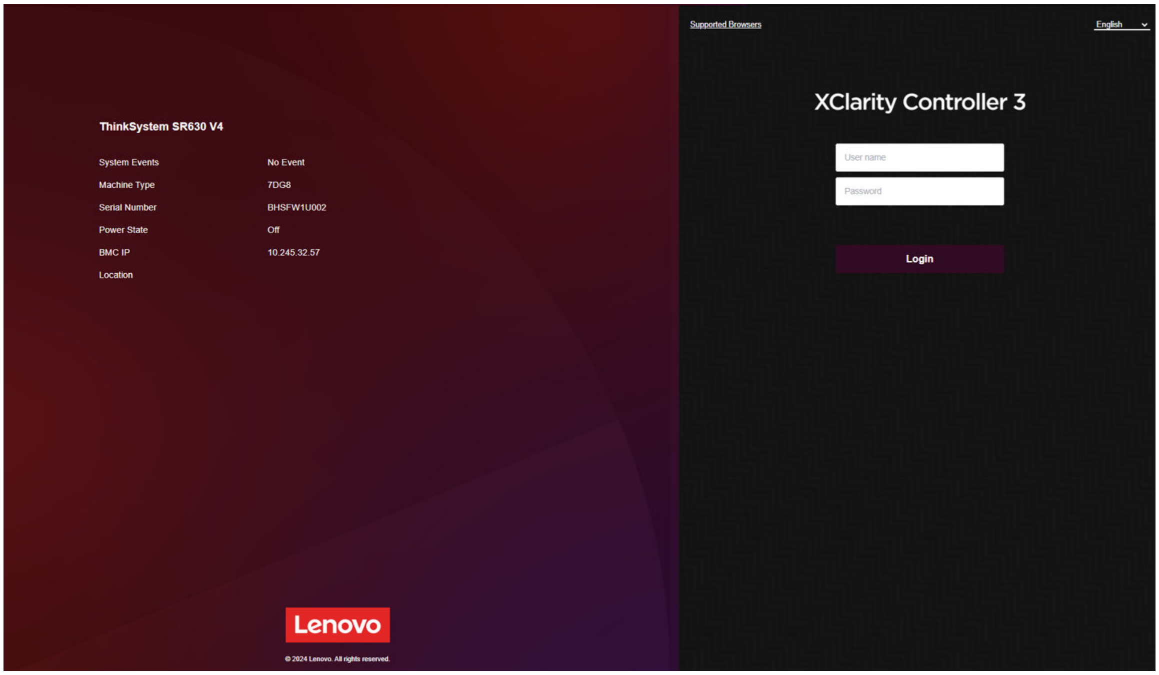
Use the information in this topic to access the XClarity Controller through the XClarity Controller web interface.

Important: The XClarity Controller is set initially with a user name of `USERID` and password of `PASSW0RD` (with a zero, not the letter O). This default user setting has Supervisor access. Change this user name and password during your initial configuration for enhanced security. After making the change, you are unable to set `PASSW0RD` as the login password again.

To access the XClarity Controller through the XClarity Controller web interface, complete the following steps:

Step 1. Open a web browser. In the address or URL field, type `https://` followed by the IP address or host name of the XClarity Controller to which you want to connect.

Step 2. Select the desired language from the language drop-down list.



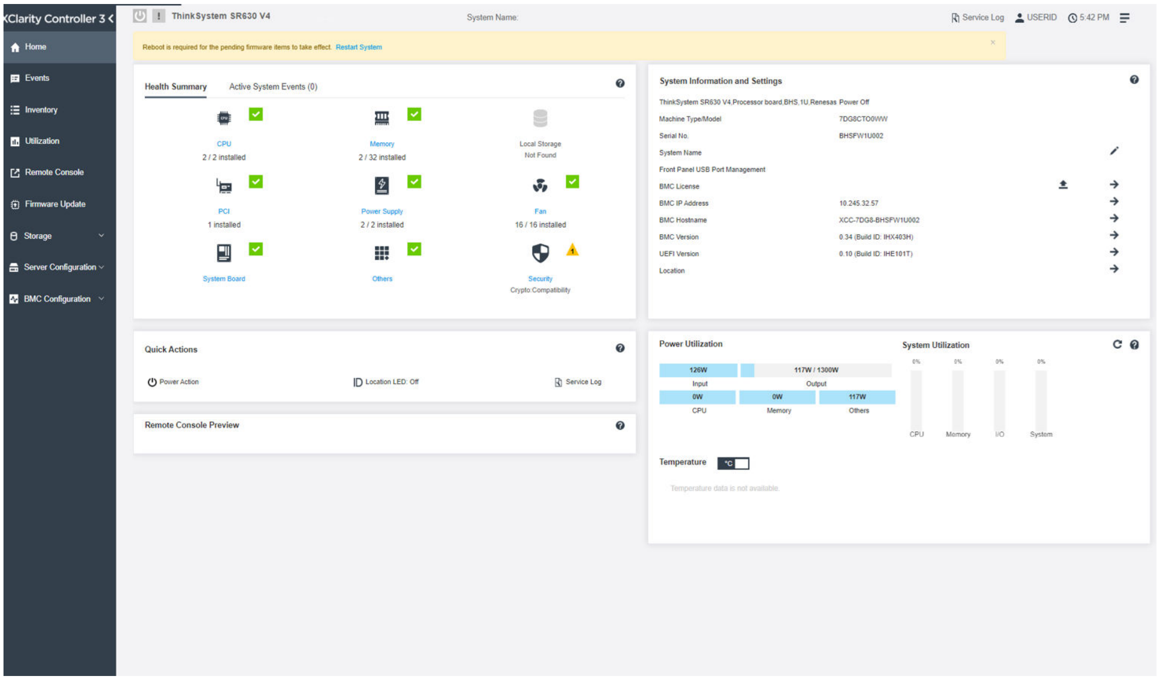
ThinkSystem SR630 V4

System Events	No Event
Machine Type	7DG8
Serial Number	BHSFW1U002
Power State	Off
BMC IP	10.245.32.57
Location	

Figure 3. Login page

Step 3. Type your user name and password in the XClarity Controller Login window. If you are using the XClarity Controller for the first time, you can obtain your user name and password from your system administrator. All login attempts are documented in the event log. Depending on how your system administrator configured the user ID, you might need to enter a new password after logging in.

Step 4. Click **Login** to start the session. The browser opens the XClarity Controller home page, as shown in the following illustration. The home page displays information about the system that the XClarity Controller manages plus icons indicating how many critical errors 1 and how many warnings 1 are currently present in the system.



Reboot is required for the pending firmware items to take effect. Restart System

System Information and Settings

ThinkSystem SR630 V4,Processor board,BHS,1U,Renesas Power Off

Machine Type/Model	7DG8CTO0WW
Serial No.	BHSFW1U002
System Name	
Front Panel USB Port Management	
BMC License	
BMC IP Address	10.245.32.57
BMC Hostname	XCC-7DG8-BHSFW1U002
BMC Version	0.34 (Build ID: IHX403H)
UEFI Version	0.10 (Build ID: IHE101T)
Location	

Temperature data is not available.

Figure 4. Home page

The home page is essentially divided into two sections. The first section is the left navigation panel, which is a set of topics that allow you to perform the following actions:

- Monitor the server status
- Configure the server
- Configure the XClarity Controller or BMC
- Update the firmware

The second section is the graphical information provided to the right of the navigation panel. The modular format gives you a quick view of the server status and some quick actions that can be performed.

Description of XClarity Controller functions on web interface

The information in this topic explains the XClarity Controller functions on the web interface.

The following is a table that describes the XClarity Controller functions in the left navigation panel.

Note: When navigating the web interface, you can also click the question mark icon for online help.

Tab	Selection	Description
Home	Health Summary/Active System Events	Shows the current status of the major hardware components in the system.
	System Information and Settings	Provides a summary of common system information.
	Quick Actions	Provides a quick link to control the server power and location LED, and a button to download the service data.
	Power Utilization/Temperature	Provides a quick overview of the current power utilization and overall server temperature.

Tab	Selection	Description
	Remote Console Preview	Control the server at the operating system level. You can view and operate the server console from your computer. The remote console section in the XClarity Controller home page displays a screen image with a Launch button.
Events	Event Log	Provides a historical list of all hardware and management events.
	Audit Log	Provides a historical record of user actions, such as logging in to the Lenovo XClarity Controller, creating a new user, and changing a user password. You can use the audit log to track and document authentication and controls in IT systems.
	Maintenance History	Displays all the firmware update, configuration and hardware replacement history.
	Alert Recipients	Manage who will be notified of system events. It allows you to configure each recipient, and manage settings that apply to all event recipients. You can also generate a test event to verify the notification configuration settings.
Inventory		Displays all the components in the system, along with their status and key information. You can click on a device to display additional information. **Note:** Refer to SMM3 web interface for more details of solution power status.
Utilization		Displays ambient/component temperature, power utilization, and fan speed information of the server and its components in either graphic or tabular formats.
Remote Console		Provides access to remote console functionality. You can use the virtual media feature to mount ISO or IMG files that are located on your system or on a network location that can be accessed by the BMC using CIFS, NFS, HTTPS, or SFTP. The mounted disk appears as a USB disk drive or DVD ROM that is attached to the server.
Firmware Update		• Displays firmware levels. • Update the XClarity Controller firmware and server firmware. • Update the XClarity Controller firmware from Repository.
Storage	Detail	Displays the storage devices' physical structure and storage configuration.
	RAID Setup	View or modify current RAID configuration, including the information of virtual disks and physical storage devices.
Server Configuration	Adapters	Displays information of the network adapters installed and the settings that can be configured via the XClarity Controller.
	Boot Options	• Select the boot device for one-time boot during next server restart. • Change boot mode and boot order settings.

Tab	Selection	Description
	Power Policy	• Configure the power redundancy during the event of a power supply failure. • Configure power capping policy. • Configure power restore policy. **Note:** Refer to SMM3 web interface fore more details of solution power status.
	Server Properties	• Monitor various properties, status conditions, and settings for your server. • Manage server power off delays. • Manage server start timeouts to detect and recover from server hang. • Create Trespass Message. A Trespass Message is a message that you can create for users to see when they log in to the XClarity Controller.
BMC Configuration	Backup and Restore	Reset the configuration of the XClarity Controller to factory defaults, backup current configuration or restore configuration from a file.
	License	Manage activation keys for optional XClarity Controller features.
	Network	Configure networking properties, status, and settings for the XClarity Controller.
	Security	Configure security properties, status, and settings for the XClarity Controller.
	User/LDAP	• Configure the XClarity Controller login profiles and global login settings. • View user accounts that are currently logged in to the XClarity Controller. • The LDAP tab configures user authentication for use with one or more LDAP servers. It also allows you to enable or disable LDAP security and manage its certificates.
	Call Home	Configure call home option to collect information about system and send it to Lenovo for services.

Chapter 3. Configuring the XClarity Controller

Use the information in this chapter to understand the options available for XClarity Controller configurations.

When configuring the XClarity Controller, the following key options are available:

- Backup and Restore
- License
- Network
- Security
- User/LDAP
- Call Home

Configuring user accounts/LDAP

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

Click **User/LDAP** under **BMC Configuration** to create, modify, and view user accounts, and to configure LDAP settings.

The **Local User** tab shows the user accounts that are configured in the XClarity Controller, and which are currently logged in to the XClarity Controller.

The **LDAP** tab shows the LDAP configuration for accessing user accounts that are kept on an LDAP server.

User authentication method

Use the information in this topic to understand the modes that the XClarity Controller can use to authenticate login attempts.

Click the drop-down menu beside **Allow login from** to select how user login attempts are authenticated. You can select one of the following authentication methods:

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

Notes:

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

Creating a new role

Use the information in this topic to create a new role.

Create role

Click on **roles** tab, and click on **Create** to create a custom role.

Complete the following fields: **Role Name** and **Authority Level**. For further details on the authority level, see the following section.

The created role is provided to the user in the role drop-down menu in the user section.

Note: Role used in User and LDAP is not allowed to edit and delete the role name, but has access to modifying the corresponding custom permission.

Authority level

A custom role are allowed to enable any combinations of the following privileges:

Configuration - Networking and BMC Security
A user can modify configuration parameters on BMC Security and Network pages.

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

Remote Console Access
A user can access the remote console.

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

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

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

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

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

Configuration - UEFI Security
A user can modify UEFI Security settings.

Predefined roles

The following roles are predefined and cannot be edited or deleted:

Administrator
The Administrator role has no restrictions and can perform all operations.

Read only

The Read Only role can display server information but cannot perform operation that affects the state of the system, such as save, modify, clear, reboot, and update firmware.

Operator

User with Operator role has the following privileges:

- Configuration - Networking and BMC Security
- Remote Server Power/Restart
- Configuration - Basic
- Ability to Clear Event Logs
- Configuration - Advanced (Firmware Update, Restart BMC, Restore Configuration)

Creating a new user account

Use the information in this topic to create a new local user.

Create user

Click on **local users** tab, and click on **Create** to create a new user account.

Complete the following fields: **User name**, **Password**, **Confirm Password**, and select a **Role** from drop-down menu. For further details on **Role**, see the following section.

Role

The following roles are predefined while new custom role can be created according to user's needs:

Administrator

The Administrator role has no restrictions and can perform all operations.

Read only

The Read Only role can display server information but cannot perform operation that affects the state of the system, such as save, modify, clear, reboot, and update firmware.

Operator

User with Operator role has the following privileges:

- Configuration - Networking and BMC Security
- Remote Server Power/Restart
- Configuration - Basic
- Ability to Clear Event Logs
- Configuration - Advanced (Firmware Update, Restart BMC, Restore Configuration)

SNMPv3 Settings

To enable SNMPv3 access for a user, click the **Edit** button next to the corresponding user, then check **SNMP** under the drop down list of **User Accessible Interface**. The following user access options are explained:

Access type

Only **GET** operations are supported. The XClarity Controller does not support SNMPv3 **SET** operations. SNMP3 can only perform query operations.

Authentication protocol

This algorithm is used by the SNMPv3 security model for authentication. The following protocols are supported:

- None
- HMAC-SHA (default)
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512

Privacy protocol

The data transfer between the SNMP client and the agent can be protected using encryption. The following methods are supported:

- None
- CBC-DES
- AES (default)
- AES192
- AES256
- AES192C
- AES256C

Notes: Even if repetitive strings of a password is used by an SNMPv3 user, access will still be allowed to the XClarity Controller. Two examples are shown for your reference.

- If the password is set to “**11111111**” (eight-digit number containing eight 1's), the user can still access the XClarity Controller if the password is accidentally inputted with more than eight 1’s. For example, if the password is inputted as “**1111111111** (ten-digit number containing ten 1's), access will still be granted. The repetitive string will be considered having the same key.
- If the password is set to “**bertbert**”, the user can still access the XClarity Controller if the password is accidentally inputted as “**bertbertbert**”. Both passwords are considered to have the same key.

For further details, refer to **Security Considerations** in the Internet Standard of RFC 3414 document (https://tools.ietf.org/html/rfc3414).

SSH Key

The XClarity Controller supports SSH Public Key Authentication (RSA key type). To add a SSH key to the local user account, click the **Edit** button next to the corresponding user, then check **SSH Key** under the drop down list of **User Accessible Interface**. The following two options are provided:

Select key file

Select the SSH key file to be imported into the XClarity Controller from your server.

Enter key into a text field

Paste or type the data from your SSH key into the text field.

Notes:

- Some of Lenovo’s tools may create a temporary user account for accessing the XClarity Controller when the tool is run on the server operating system. This temporary account is not viewable and does not use any of the 12 local user account positions. The account is created with a random user name (for example, “20luN4SB”) and password. The account can only be used to access the XClarity Controller on the internal Ethernet over USB interface, and only for the Redfish and SFTP interfaces. The creation and removal of this temporary account is recorded in the audit log as well as any actions performed by the tool with these credentials.

- For the SNMPv3 Engine ID, the XClarity Controller uses a HEX string to denote the ID. This HEX string is converted from the default XClarity Controller host name. See the example below:

  The host name "XCC-7X06-S4AHJ300" is first converted into ASCII format: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  The HEX string is built using the ASCII format (ignore the spaces in between): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

Deleting a user account

Use the information in this topic to remove a local user account.

To delete a local user account, click the trash can icon on the row of the account that you wish to remove. If you are authorized, you can remove your own account or the account of other users, unless it is the only account remaining with **User Account Management** privileges.

Using hashed passwords for authentication

Use the information in this topic to understand how to use hashed passwords for authentication.

Aside from the use of passwords and LDAP/AD user accounts, the XClarity Controller also supports third-party hashed passwords for authentication. The special password uses a one-way hash (SHA256) format and is supported by the XClarity Controller web, OneCLI, and CLI interfaces. However, please note that authentication of XCC SNMP, IPMI and CIM interfaces do not support third-party hashed passwords. Only the OneCLI tool and XCC CLI interface can create a new account with a hashed password or perform a hashed password update. The XClarity Controller also allows the OneCLI tool and XClarity Controller CLI interface to retrieve the hashed password if the capability of reading hashed password is enabled.

Setting hashed password via XClarity Controller web

Click **Security** under **BMC Configuration**, and scroll to the **Security Password Manager** section to enable or disable the **Third-party Password** function. If enabled, a third-party hashed password is employed for log-in authentication. Retrieval of the third-party hashed password from the XClarity Controller can also be enabled of disabled.

Note: By default, the **Third-party Password** and **Allow Third-party Password Retrieval** functions are disabled.

To check if the user password is **Native** or a **Third-party Password**, click **User/LDAP** under **BMC Configuration** for details. The information will be under the **Advanced Attribute** column.

Notes:

- Users will not be able to change a password if it is a third-party password, and the **Password** and **Confirm password** fields will be greyed out.
- If the third-party password has expired, a warning message will be shown during the user login process.

Setting hashed password via OneCLI function

- Enabling feature

```
$ sudo OneCli config set IMM.ThirdPartyPassword Enabled
```

- Creating hashed password (No Salt). The following shows an example logging to the XClarity Controller using the **password123** password.

```
$ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`
$ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

$ sudo OneCli config set IMM.Loginid.2 admin

$ sudo OneCli config set IMM.SHA256Password.2 $pwhash

$ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
```

- Creating user with hashed password (With Salt). The following shows an example logging to the XClarity Controller using the **password123** password. Salt=abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  $ sudo OneCli config set IMM.Loginid.3 Admin

  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- Retrieving the hashed password and salt.

  ```
  $ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled

  $ sudo OneCli config show IMM.SHA256Password.3

  $ sudo OneCli config show IMM.SHA256PasswordSalt.3
  ```

- Deleting the hashed password and salt.

  ```
  $ sudo OneCli config set IMM.SHA256Password.3 ""

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
  ```

- Setting the hashed password to an existing account.

  ```
  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.Password.2 Passw0rd123abc

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

  Note: While the hashed password is being set, this password will immediately take effect. The original standard password will no longer be effective. In this example, the original standard password **Passw0rd123abc** cannot be used anymore until the hashed password is deleted.

Setting hashed password via CLI function

- Enabling feature

  ```
  > hashpw -sw enabled
  ```

- Creating hashed password (No Salt). The following shows an example logging to the XClarity Controller using the **password123** password.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  > users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
  super
  ```

- Creating user with hashed password (With Salt). The following shows an example logging to the XClarity Controller using the **password123** password. Salt=abc.

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`
```

```
$ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
```

```
> users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
-ssalt 'abc' -a super
```

- Retrieving the hashed password and salt.

  ```
  > hashpw -re enabled
  ```

  ```
  > users -3 -ghp -gsalt
  ```

- Deleting the hashed password and salt.

  ```
  > users -3 -shp "" -ssalt ""
  ```

- Setting the hashed password to an existing account.

  ```
  > users -2 -n admin -p Passw0rd123abc -shp
  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
  ```

  Note: While the hashed password is being set, this password will immediately take effect. The original standard password will no longer be effective. In this example, the original standard password **Passw0rd123abc** cannot be used anymore until the hashed password is deleted.

After the hashed password has been set up, remember you do not use this to login to the XClarity Controller. When logging in, you will need to use the plaintext password. In the example shown below, the plaintext password is “password123”.

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}'’
```

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

```
> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Configuring global login settings

Use the information in this topic to configure login and password policy settings that apply to all users.

Web inactivity session timeout

Use the information in this topic to set the web inactivity session timeout option.

In the **Web inactivity session timeout** field, you can specify how long, in minutes, the XClarity Controller waits before it disconnects an inactive web session. The maximum wait time is 1,440 minutes. If set to 0, the web session never expires.

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

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

Account security policy settings

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

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

Force to change password on first access

After setting up a new user with a default password, selection of this checkbox will force that user to change their password the first time that the user logs in. The default value for this field is to have the checkbox enabled.

Complex password required

The option box is checked by default and the complex password must adhere to the following rules:

- Only contain the following characters (no white-space characters allowed): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- Must contain at least one letter
- Must contain at least one number
- Must contain at least two of the following combinations:
  - At least one upper-case letter.
  - At least one lower-case letter.
  - At least one special character.
- No other characters (in particular, spaces or white-space characters) are allowed
- Passwords may have no more than two consecutive instances of the same character (i.e., “aaa”).
- The password cannot be literary same as the user name, simply repeating the user name one or more times, or a reverse character order of the user name.
- Passwords must be a minimum of 8 and a maximum of 255 characters long.

If the option box is not checked, the number specified in the minimum password length can be set as 0-255 characters. The account password may be blank if minimum password length is set as 0.

Password expiration period (days)

This field contains the maximum password age that is permitted before the password must be changed.

Password expiration warning period (days)

This field contains the number of days a user is warned before their password expires.

Minimum password length (characters)

This field contains the minimum length of the password.

Minimum password reuse cycle (times)

This field contains the number of previous passwords that cannot be reused.

Minimum password change interval (hours)

This field contains how long a user must wait between password changes.

Maximum number of login failures (times)

This field contains the number of failed login attempts that are allowed before the user is locked out for a period of time.

Note: When the maximum number of login failures has been reached, a warning message will be displayed at the next login attempt.

Lockout period after maximum login failures (minutes)

This field specifies how long (in minutes), the XClarity Controller subsystem will disable remote login attempts after the maximum number of login failures has been reached.

Configuring LDAP

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

LDAP support includes:

- Support for LDAP protocol version 3 (RFC-2251)
- Support for the standard LDAP client APIs (RFC-1823)
- Support for the standard LDAP search filter syntax (RFC-2254)
- Support for Lightweight Directory Access Protocol (v3) Extension for Transport Layer Security (RFC-2830)

The LDAP implementation supports the following LDAP servers:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Microsoft Active Directory Application Mode (Windows 2003, Windows 2008)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Novell eDirectory Server, version 8.7 and 8.8
- OpenLDAP Server 2.1, 2.2, 2.3, 2.4, 2.5 and 2.6

Click the **LDAP** tab to view or modify XClarity Controller LDAP settings.

The XClarity Controller can remotely authenticate a user's access through a central LDAP server instead of, or in addition to the local user accounts that are stored in the XClarity Controller itself. Privileges can be designated for each user account using the valur of "Login Permission attribute". You can also use the LDAP server to assign users to groups and perform group authentication, in addition to the normal user (password check) authentication. For example, an XClarity Controller can be associated with one or more groups, the user will pass group authentication only if the user belongs to at least one group that is associated with the XClarity Controller.

To configure an LDAP server, complete the following steps:

1. Under **LDAP Server Information**, the following options are available from the item list:

   - **Use LDAP server for Authentication only (with local authorization)**: This selection directs the XClarity Controller to use the credentials only to authenticate to the LDAP server and to retrieve group membership information. The group names and roles can be configured in the **Groups for Local Authorization** section.
   - **Use LDAP server for Authentication and Authorization**: This selection directs the XClarity Controller to use the credentials both to authenticate to the LDAP server and to identify a user's permission.

   Note: The LDAP servers to be used for authentication can either be configured manually or discovered dynamically via DNS SRV records.

   - **Use Pre-Configured Servers**: You can configure up to three LDAP servers by entering each server's IP address or host name if DNS is enabled. The port number for each server is optional. If this field is left blank, the default value of 389 is used for non-secured LDAP connections. For secured connections, the default port value is 636. You must configure at least one LDAP server.
   - **Use DNS to Find Servers**: You can choose to discover the LDAP server(s) dynamically. The mechanisms described in RFC2782 (A DNS RR for specifying the location of services) are used to locate the LDAP server(s). This is known as DNS SRV. You need to specify a fully qualified domain name (FQDN) to be used as the domain name in the DNS SRV request.

- **AD Forest**: In an environment with universal groups in cross domains, the forest name (set of domains) must be configured to discover the required Global Catalogs (GC). In an environment where cross-domain group membership does not apply, this field can be left blank.
- **AD Domain**: You will need to specify a fully qualified domain name (FQDN) to be used as the domain name in the DNS SRV request.

If you wish to enable secure LDAP, click the **Enable Secure LDAP** checkbox. In order to support secure LDAP, a valid SSL certificate must be in place and at least one SSL client trusted certificate must be imported into the XClarity Controller. Your LDAP server must support Transport Layer Security (TLS) version 1.2 to be compatible with the XClarity Controller secure LDAP client. For more information about certificate handling, see "SSL certificate handling" on page 42.

2. Fill in information under **Additional Parameters**. Below are explanations of the parameters.

LDAP type

Select the LDAP server type for LDAP based authentication. The following server types are available:

- **OpenLDAP**

  OpenLDAP

- **Active Directory**

  Directory: Windows Active Directory

- **Other**

  Directory: Apache Directory, eDirectory, etc.

Binding method

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

- **Use Configured Credentials**

  Use this method to bind with the configured client DN and password.

- **Use Login Credentials**

  Use this method to bind with the credentials that are supplied during the login process. The user ID can be provided through a DN, a partial DN, a fully qualified domain name, or through a user ID that matches the UID Search Attribute that is configured on the XClarity Controller. If the credentials that are presented resemble a partial DN (e.g. cn=joe), this partial DN will be prepended to the configured Root DN in an attempt to create a DN that matches the user's record. If the bind attempt fails, a final attempt will be made to bind by prepending cn= to the login credential, and prepending the resulting string to the configured Root DN.

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

Client distinguished name

The Client Distinguished Name (DN) to be used for the initial bind. And it is limited to a maximum of 300 characters.

Client password

The password for this Distinguished Client.

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 search requests.

User's Login Name Search Attribute

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

Group Filter

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

The comparisons are case sensitive. The filter is limited to 511 characters and can consist of one or more group names. The colon (:) character must be used to delimit multiple group names. Leading and trailing spaces are ignored, but any other space is treated as part of the group name.

Note: The wildcard character (*) is no longer treated as a wildcard. The wildcard concept has been discontinued to prevent security exposures. A group name can be specified as a full DN or by 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.

Group Membership Search Attribute

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

Login Permission Attribute

When a user is authenticated through an LDAP server successfully, the login permissions for the user must be retrieved. To retrieve the login permissions, the search filter that is sent to the server must specify the attribute name that is associated with login permissions. The **Login Permission Attribute** field specifies the attribute name. If using LDAP server for Authentication and Authorization, but this field is left blank, the user will be refused access.

The attribute value that is returned by the LDAP server searches should be a bit string that is entered as 13 consecutive 0s or 1s, or a bit string as 13 consecutive 0s or 1s in total. Each bit represents a set of functions. The bits are numbered according to their positions. The left-most bit is bit position 0, and the right-most bit is bit position 12. A value of 1 at a bit position enables the function that is associated with that bit position. A value of 0 at a bit position disables the function that is associated with that bit position.

The string 0100000000000 is a valid example, which is used to allow it to be placed in any field. The attribute that you use can allow for a free-formatted string. When the attribute is retrieved successfully, the value that is returned by the LDAP server is interpreted according to the information in the following table.

Table 1. Permission bits

Three column table containing bit position explanations.

Bit position	Function	Explanation
0	Deny Always	A user will always fail authentication. This function can be used to block a particular user or users associated with a particular group.
1	Supervisor Access	A user is given administrator privileges. The user has read/write access to every function. If you set this bit, you do not have to individually set the other bits.
2	Read Only Access	A user has read-only access, and cannot perform any maintenance procedures (for example, restart, remote actions, or firmware updates) or make modifications (for example, the save, clear, or restore functions). Bit position 2 and all other bits are mutually exclusive, with bit position 2 having the lowest precedence. When any other bit is set, this bit will be ignored.
3	Configuration - Networking and BMC Security	A user can modify the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port configurations.
4	User Account Management	A user can add, modify, or delete users and change the Global Login Settings in the Login Profiles window.
5	Remote Console Access	A user can access the remote server console.
6	Remote Console and Remote Disk Access	A user can access the remote server console and the remote disk functions for the remote server.
7	Remote Server Power/ Restart Access	A user can access the power on and restart functions for the remote server.
8	Configuration - Basic	A user can modify configuration parameters in the System Settings and Alerts windows.
9	Ability to Clear Event Logs	A user can clear the event logs. **Note:** All users can view the event logs; but, to clear the event logs the user is required to have this level of permission.
10	Configuration - Advanced (Firmware Update, Restart BMC, Restore Configuration)	A user has no restrictions when configuring the XClarity Controller. In addition the user has administrative access to the XClarity Controller. The user can perform the following advanced functions: firmware upgrades, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart/ reset the adapter.
11	Configuration - UEFI Security	A user can configure UEFI security related settings, which can also be configured from UEFI F1 security setup page.
12	Reserved	Reserved for future use, and currently ignored.

If none of the bits are set, the user will be refused access

Note: Note that priority is given to login permissions retrieved directly from the user record. If the user does not have the login permission attribute in its record, an attempt will be made to retrieve the permissions from the group(s) that the user belongs to, and, if configured, that match the group filter. In this case the user will be assigned the inclusive OR of all the bits for all of the groups. Similarly, the **Read Only Access** bit will only be set if all the other bits are zero. Moreover, note that if the **Deny Always** bit is set for any of the groups, the user will be 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/or security related adapter configuration parameters, you should consider giving this same user the ability to restart the XClarity Controller (bit position 10). Otherwise, without this ability, a user might be able to change parameters (for example, IP address of the adapter), but will not be able to have them take effect.

3. If **Use LDAP server for Authentication only (with local authorization)** mode is used, configure the **Groups for Local Authorization**. Group Name, Group Domain and Role are configured to provide local authorization for groups of users. Each group can be assigned with a Role (permissions) that is the same as configured in the roles in Local User. User accounts are assigned to different groups on LDAP server. An user account will be assigned with the Role (permissions) of the group this user account belongs to after login to BMC. Group Domain should be in the same format as Distinguished Name, like: dc= mycompany,dc=com, will be used as the base object for group searches. If the field is left blank, it will use the same value as the "Root DN" field. Additional groups can be added by clicking the "+" icon or deleted by clicking the "x" icon.
4. Select the attribute used for displaying the user name from the **Specify the attribute used for displaying user name** drop-down menu.

Configuring network protocols

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

Configuring the Ethernet settings

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

Notes:

- AMD servers do not support Ethernet failover function.
- On platforms that have both Ethernet Port 1 and Ethernet Port 2 enabled, make sure to configure the following external servers accessible from the subnet of Ethernet Port 1:
  - LDAP server for authentication
  - HTTP/HTTPS, NFS, CIFS, FTP and SFTP servers for firmware update and virtual media
  - SMTP server for email alert
  - Syslog server for syslog alert
  - SNMP trap receiver server for SNMP trap
  - HTTPS server for Redfish alert
  - NTP server for time sync
  - DNS server

The XClarity Controller uses two network controllers. One network controller is connected to the dedicated management port and the other network controller is connected to the shared port. Each of the network controllers is assigned its own burned in MAC address. If DHCP is being used to assign an IP address to the XClarity Controller, when a user switches between network ports or when a failover from the dedicated network port to the shared network port occurs, a different IP address may be assigned to the XClarity Controller by the DHCP server. It is recommended that when using DHCP, users should use the host name to access the XClarity Controller rather than relying on an IP address. Even if the XClarity Controller network ports are not changed, the DHCP server could possibly assign a different IP address to the XClarity Controller when the DHCP lease expires, or when the XClarity Controller reboots. If a user needs to access the XClarity Controller using an IP address that will not change, the XClarity Controller should be configured for a static IP address rather than DHCP.

Click **Network** under **BMC Configuration** to modify XClarity Controller Ethernet settings.

Configuring the XClarity Controller Host Name

The default XClarity Controller host name is generated using a combination of the string "XCC-" followed by the server machine type and server serial number (for example. "XCC-7X03-1234567890"). You can change the XClarity Controller host name by entering up to a maximum of 63 characters in this field. The host name must not include a period (.) and can contain only alphabet, numeric, hyphen and underscore characters.

Ethernet Ports

This setting controls the enablement of Ethernet ports used by management controller, including the shared and dedicated ports.

Once **disabled**, all Ethernet ports will not be assigned any IPv4 or IPv6 addresses, and prevents any further changes to any Ethernet configurations.

Note: This setting does not affect the USB LAN interface or the USB management port at the front of the server. Those interfaces have their own dedicated enablement settings.

Configuring IPv4 network settings

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

1. Enable the **IPv4** option.

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

2. From the **Method** field, select one of the following options:
   - **Obtain IP from DHCP**: The XClarity Controller will obtain its IPv4 address from a DHCP server.
   - **Use static IP address**: The XClarity Controller will use the user specified value for its IPv4 address.
   - **First DHCP, then static IP address**: The XClarity Controller will attempt to obtain its IPv4 address from a DHCP server, but if that attempt fails, the XClarity Controller will use user specified value for its IPv4 address.

3. In the **Static IPv4 address** field, type the IP address that you want to assign to the XClarity Controller.

   Note: The IP address must contain four integers from 0 to 255 with no spaces and separated by periods. This field will not be configurable if the method is set to **Obtain IP from DHCP**.

4. In the **Network mask** field, type the subnet mask that is used by the XClarity Controller.

   Note: The subnet mask must contain four integers from 0 to 255 with no spaces or consecutive periods and separated by periods. The default setting is 255.255.255.0. This field will not be configurable if the method is set to **Obtain IP from DHCP**.

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

   Note: The gateway address must contain four integers from 0 to 255 with no spaces or consecutive periods and separated by periods. This field will not be configurable if the method is set to **Obtain IP from DHCP**.

Configuring advanced Ethernet settings

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

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

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

- **Use burned-in MAC address**

  The Burned-in MAC address option is a unique physical address that is assigned to this XClarity Controller by the manufacturer. The address is a read-only field.

- **Use custom MAC address**

  If a value is specified, the locally administered address overrides the burned-in MAC address. The locally administered address must be a hexadecimal value from `000000000000` through `FFFFFFFFFFFF`. This value must be in the form **xx:xx:xx:xx:xx:xx** where **x** is a hexadecimal number from 0 to 9 or "a" through "f". The XClarity Controller does not support the use of a multicast address. The first byte of a multicast address is an odd number (the least significant bit is set to 1); therefore, the first byte must be an even number.

In the **Data rate and duplex** field, select **auto-negotiate** or **custom** to specify the data rate and duplex.

In the **MTU (Maximum transmission unit)** field, specify the maximum transmission unit of a packet (in bytes) for your network interface. The maximum transmission unit range is from 1000 to 1500. The default value for this field is 1500.

Configuring IPv6 network settings

1. Enable the **IPv6** option.
2. Assign an IPv6 address to the interface using one of the following assignment methods:
   - Use stateless address autoconfiguration
   - Use stateful address configuration (DHCPv6)
   - Use statically assigned IP address

     Notes: When the **Use statically assigned IP addres** is chosen, you will be asked to type the following information:

     - IPv6 Address
     - Prefix length
     - Gateway

Configuring DNS

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

Click **Network** under **BMC Configuration** to view or modify XClarity Controller DNS settings.

If you click the **Use additional DNS address servers** checkbox, specify the IP addresses of up to three Domain Name System servers on your network. Each IP address must contain integers from 0 to 255, separated by periods. These DNS server addresses are added to the top of the search list, so a host name lookup is done on these servers before one that is automatically assigned by a DHCP server.

If you click the **Use DNS to discover Lenovo XClarity Administrator** checkbox, the XClarity Manager must be selected.

Configuring DDNS

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

Click **Network** under **BMC Configuration** to view or modify XClarity Controller DDNS settings.

Click the **Enable DDNS** checkbox, to enable DDNS. When DDNS is enabled, the XClarity Controller notifies a domain name server to change in real time, the active domain name server configuration of the XClarity Controller configured host names, addresses or other information that is stored in the domain name server.

Choose an option from the item list to decide how you want the domain name of the XClarity Controller to be selected.

- **Use custom domain name**: You can specify the domain name to which the XClarity Controller belongs.
- **Use domain name obtained from the DHCP server**: The domain name to which the XClarity Controller belongs is specified by the DHCP server.

Configuring Ethernet over USB

Use the information in this topic to control the Ethernet over USB interface used for in-band communication between the server and the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify the XClarity Controller Ethernet over USB settings.

The Ethernet over USB is used for in-band communications to the XClarity Controller. Click the checkbox to enable or disable the Ethernet over USB interface.

Important:

- If you disable **Ethernet Over USB**, you cannot perform an in-band update of the XClarity Controller firmware or server firmware using the XClarity Essentials in-band update utility. Use the Firmware Update option on the XClarity Controller Web interface or the XClarity Essentials out-of-band update utility to update the firmware.
- It is important to disable the Watchdog timeouts to prevent the server from restarting unexpectedly when USB in-band interface is disabled.
- To use this interface, the operating system drivers that support this function (RNDIS for Windows, cdc_ether and usbnet for Linux) must be installed. The XClarity Controller provides an INF file for Windows that allows Windows to recognize the XClarity Controller USB device as an RNDIS device.

Select the method that The XClarity Controller uses to assign addresses to the endpoints of the Ethernet over USB interface.

- **Use IPv6 link-local address for Ethernet over USB**: This method uses IPv6 addresses based off the MAC address that have been allocated to the endpoints of the Ethernet over USB interface. Normally, the IPv6 link local address is generated using the MAC address (RFC 4862) but Windows 2008 and newer 2016 operating systems do not support a static link local IPv6 address on the host end of the interface. Instead the default Windows behavior regenerates random link local addresses while running. If the XClarity Controller Ethernet over USB interface is configured to use the IPv6 link local address mode, various functions that make use of this interface will not work because the XClarity Controller does not know what address Windows has assigned to the interface. If the server is running Windows use one of the other Ethernet over USB address configuration methods, or disable the default Windows behavior by using this command:

  ```
  netsh interface ipv6 set global randomizeidentifiers=disabled
  ```

- **Configure IPv4 setting for Ethernet over USB**: With this method, it specifies the IP addresses and network mask that are assigned to the XClarity Controller and the server side of the Ethernet over USB interface.

  Notes:

  - You need to manually configure the IP address of Ethernet over USB interface in the local operating system after you configure the XClarity Controller IP address, OS IP address, and Network mask.
  - The OS IP address setting is used to make XClarity Controller aware of the opposite end of Ethernet over USB network (Operating System) for communication purposes, such as Watchdog status monitoring or in-band firmware update.

Mapping of external Ethernet port numbers to Ethernet over USB port numbers is controlled by clicking the **Enable external Ethernet to Ethernet over USB port forwarding** checkbox and completing the mapping information for ports you wish to have forwarded from the management network interface to the server.

Configuring SNMP

Use the information in this topic to configure SNMP agents.

Complete the following steps to configure the XClarity Controller SNMP alert settings.

1. Click **Network** under **BMC Configuration**.
2. Check the corresponding checkbox to enable the **SNMPv3 Agent**, **SNMPv1 Trap**, **SNMPv2 Trap** and/or **SNMPv3 Trap**.

   Notes:

   - To enable the **SNMPv3 Agent**, a BMC contact and location must be specified.
   - Once the **SNMPv3 Agent** is enabled, you can configure SNMPv3 for each XClarity Controller user account.
   - In order to receive traps, both SNMP traps and the SNMPv3 agent must be enabled
3. If enabling the **SNMPv1 Trap** or **SNMPv2 Trap**, complete the following fields:
   a. In the **Community Name** field, enter the community name. Community Name cannot be empty.
   b. In the **Host** field, enter host address.
4. If enabling the **SNMPv3 Trap**, complete the following fields:
   a. In the **Engine ID** field, enter the engine ID. Engine ID cannot be empty.
   b. In the **Trap Receiver Port** field, enter the port number. Default port number is 162.
5. If enabling the SNMP Traps, select the following event types you wish to be alerted:
   - **Critical**
   - **Attention**
   - **System**

   Note: Click on each major category to further select their sub-category event types you wish to be alerted.
6. If enabling the **SNMPv3 Agent**, complete the following:
   a. Click **User/LDAP** under **BMC Configuration**.
   b. Click the **Edit** button next to the corresponding user, then check **SNMP** under the drop-down list of **User Accessible Interface**.

Note: Click the **Send** button next to **Send a test trap** to verify the SNMP settings.

Enabling IPMI Network Access

Use the information in this topic to control IPMI network access to the XClarity Controller.

Complete the following steps to enable IPMI over LAN access.

1. Click **Network** under **BMC Configuration** to view or modify XClarity Controller IPMI settings.
2. Click the **IPMI over LAN** switch under **Service Enablement and Port Assignment** to enable IPMI network access to the XClarity Controller.
3. Click **User/LDAP** under **BMC Configuration**.
4. Click the **Edit** button next to the corresponding user, then check **IPMI over Lan** under the drop-down list of **User Accessible Interface**.

Important:

- If you are not using any tools or applications that access the XClarity Controller through the network using the IPMI protocol, it is highly recommended that you disable IPMI network access for improved security.
- IPMI over LAN access to the XClarity Controller is disabled by default.

Configuring Network Settings with IPMI commands

Use the information in this topic to configure the network settings using IPMI commands.

Because each BMC network setting is configured using separate IPMI requests and in no particular order, the BMC does not have the complete view of all of the network settings until the BMC is restarted to apply the pending network changes. The request to change a network setting may succeed at the time that the request is made, but later be determined to be invalid when additional changes are requested. If the pending network settings are incompatible when the BMC is restarted, the new settings will not be applied. After restarting the BMC, you should attempt to access the BMC using the new settings to ensure that they have been applied as expected.

Service Enablement and Port Assignment

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

Click **Network** under **BMC Configuration** to view or modify XClarity Controller port assignments. Complete the following fields to view or modify port assignments:

HTTPS (Web/Redfish)

This item is always Enabled. In this field specify the port number for Web Over HTTPS. The default value is 443.

Remote Presence

This item is always Enabled. The port number is 443.

IPMI over LAN

The port number is 623. This field is not user-configurable.

Note: Ensure that **IPMI over LAN** is selected and applied at the **User Accessible Interface** field for the corresponding user in the User/LDAP page.

SSDP

The port number is 1900. This field is not user-configurable.

SSH

In this field specify the port number that is configured to access the command line interface through the SSH protocol. The default value is 22.

SNMP Agent

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

Note: Ensure that **SNMP** is selected and applied at the **User Accessible Interface** field for the corresponding user in the User/LDAP page.

Configuring Access Restriction

Use the information in this topic to view or change the settings that block access from IP addresses or MAC addresses to the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller access control settings.

Block List and Time Restriction

These options allow you to block specific IP/Mac addresses for specific period of time.

- **List of Blocked IP Addresses**
  - You can enter up to three IPv4 addresses or ranges and three IPv6 addresses or ranges separated by commas, which are not allowed to access the XClarity Controller. Refer to the IPv4 examples below:
  - Single IPv4 address sample: 192.168.1.1
  - Supernet IPv4 address sample: 192.168.1.0/24
  - IPv4 range sample: 192.168.1.1–192.168.1.5
- **List of Blocked MAC address**
  - You can enter up to three MAC addresses separated by commas, which are not allowed to access the XClarity Controller. For example: 11:22:33:44:55:66.
- **Restricted Access (one time)**
  - You can schedule a one-time time interval during which the XClarity Controller cannot be accessed. For the time interval that you specify:
  - The beginning date and time must be later than the current XCC time.
  - The ending date and time must be later than the beginning date and time.
- **Restricted Access (daily)**
  - You can schedule one or more daily time intervals during which the XClarity Controller cannot be accessed. For each time interval that you specify:
  - The ending date and time must be later than the beginning date and time.

Externally Triggered Block List

These options allow you to setup automatic blocking of specific IP addresses (IPv4 and IPv6) from which client successively attempted to log in to XClarity Controller with different incorrect username or password.

Automatic blocking will dynamically determines when excessive login failures occur from a particular IP address and blocks that address from accessing XClarity Controller for a predetermined amount of time.

- **Maximum number of login failures from a particular IP**
  - The maximum number of times indicates the number of login failures allowed for a user with an incorrect password from a specific IP address before it becomes locked-out.
  - If set to 0, IP address will never be locked due to login failures.

  - The failed login counter for the specific IP address will be reset to zero after successful login from that IP address.
- **Lockout period for blocking an IP**
  - The minimum amount of time (in minutes) that must pass before a user can attempt to log back in again from a locked IP address.
  - If set to 0, access from the locked IP address remains blocked-out until the administrator explicitly unlocks it.
- **Block List**
  - The table Block List displays all locked IP addresses. You can unlock one or all IP addresses from the Block List.

Configuring Front Panel USB Port to Management

Use the information in this topic to configure the XClarity Controller Front Panel USB Port to Management.

On some servers the front panel USB port can be switched to attach either to the server or to the XClarity Controller. Connection to the XClarity Controller is primarily intended for use with a mobile device running the Lenovo XClarity Mobile app. When a USB cable is connected between the mobile device and the server's front panel, an Ethernet over USB connection will be established between the mobile app running on the device and the XClarity Controller.

On some servers the front panel USB port can be switched to attach either to the server or to the XClarity Controller.

Click **Network** under **BMC Configuration** to view or modify XClarity Controller front panel USB port to management settings.

There are four types of settings that you can choose from:

Host Only Mode
The front panel USB port is always connected only to the server.

BMC Only Mode
The front panel USB port is always connected only to the XClarity Controller.

Shared Mode: owned by BMC
The front panel USB port is shared by both the server and the XClarity Controller, but the port is switched to the XClarity Controller.

Shared Mode: owned by Host
The front panel USB port is shared by both the server and the XClarity Controller, but the port is switched to the host.

For additional information about the Mobile app, see the following site:

https://pubs.lenovo.com/lxca/lxca_usemobileapp.html

Notes:

- If the front panel USB port is configured for Shared Mode, the port is connected to the XClarity Controller when there is no power, and is connected to the server when there is power. When there is power, the control of the front panel USB port can be switched back and forth between the server and the XClarity Controller. In shared mode, the port can also be switched between the host and the XClarity Controller by pressing and holding the front panel Identification button (for compute nodes it may be the USB management button) for more than 3 seconds.

- When configured in Shared Mode and the USB port is currently connected to the server, the XClarity Controller can support a request to switch the front panel USB port back to the XClarity Controller. When this request is executed, the front panel USB port will remain connected to the XClarity Controller until there is no USB activity to the XClarity Controller for the period specified by the inactivity timeout.

Configuring security settings

Use the information in this topic to configure security protocols.

Note: The default minimum TLS version setting is TLS 1.2, but you can configure the XClarity Controller to use other TLS versions if needed by your browser or management applications. For more information, see "tls command" on page 155.

Click **Security** under **BMC Configuration** to access and configure security properties, status, and settings for your XClarity Controller.

Security dashboard

This topic is an overview of the security dashboard.

The security dashboard provides an overall security assessment and status of the system.

- **BMC Security Events** report events asserted by security issues, such as chassis intrusion, PFR detected corruption, System Guard detected hardware inconsistency, security jumper open on planar, etc.
- **BMC Security Mode** provides an overall status of Security Mode compliance.
- **BMC Services & Ports** enumerate all insecure services/ports enabled but non-compliant with the current Security Mode.
- **BMC Certificates** list all non-compliant certificates used by XCC.
- **BMC User Accounts** provide general suggestions on how to make the account and password management more secure.

Note: The dashboard shows a warning icon if there is any risk in these security areas scanned by XCC. The **Details** link under each category also brings the user to the setup page to solve the issues.

Security mode

This topic is an overview of the security mode.

The XCC Standard license enables the users to configure their servers in one of the two Security Modes: Standard Mode and Compatibility Mode. These are available in all V4 servers.

The Lenovo XClarity Controller 3 Premier Upgrade license comes with a third Security Mode: Enterprise Strict Mode. This mode is most suitable for high-level security requirements.

Note: By default, XCC uses an ECDSA self-signed certificate and only ECDSA based algorithms are available. To use RSA based certificate, generate a CSR and sign it with an internal or external CA, then import the signed certificate to XCC.

Enterprise Strict Security Mode

- Enterprise Strict Security Mode is the most secure mode.
- BMC operates in FIPS 140-3 validated mode.

- Requires enterprise strict grade certificates.
- Only services that support enterprise strict level cryptography are allowed.
- Requires the Lenovo XClarity Controller 3 Premier Upgrade license to enable.
- CNSA cryptography algorithms are available for use.

Standard Security Mode

- Standard Mode is the default security mode.
- All cryptography algorithms used by BMC are FIPS 140-3 compliant.
- BMC operates in FIPS 140-3 validated mode.
- Requires standard grade certificates.
- Services that require cryptography that do not support standard level cryptography are disabled by default.
- CNSA algorithms are available when the Lenovo XClarity Controller 3 Premier Upgrade license is installed.

Compatibility Mode

- Compatibility Mode is the mode to use when services and clients require cryptography that is not enterprise strict/standard compliant.
- A wider range of cryptography algorithms are supported.
- When this mode is enabled, BMC is NOT operating in FIPS 140-3 validated mode.
- Allows all services to be enabled.
- Supports a wide range of cipher suits for maximum compatibility.

Supported TLS cipher suites

The TLS Cryptography Setting is to restrict the supported TLS cipher suites against BMC services.

TLS cipher suites	Security Mode	TLS Version
TLS_AES_256_GCM_SHA384	• Enterprise Strict • Standard* • Compatibility*	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	• Compatibility	TLS 1.3
TLS_AES_128_GCM_SHA256	• Standard • Compatibility	TLS 1.3
TLS_AES_128_CCM_8_SHA256	• Standard • Compatibility	TLS 1.3
TLS_AES_128_CCM_SHA256	• Standard • Compatibility	TLS 1.3
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• Enterprise Strict • Standard* • Compatibility*	TLS 1.2

TLS cipher suites	Security Mode	TLS Version
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	• Enterprise Strict • Standard* • Compatibility*	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	• Enterprise Strict • Standard* • Compatibility*	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• Standard • Compatibility	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	• Compatibility	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	• Standard • Compatibility	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	• Standard • Compatibility	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305	• Compatibility	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• Compatibility	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• Compatibility	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	• Compatibility	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	• Compatibility	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	• Compatibility	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	• Compatibility	TLS 1.2

Note: Security modes with an asterisk (*) listed in the table require Lenovo XClarity Controller 3 Premier Upgrade license.

Service matrix in three Security Modes

Feature/ Service	Uses Crypto	Default State Out of Box	Supported in Strict Mode	Supported in Standard Mode	Supported in Compatibility Mode
IPMI-over-KCS	No	Enabled	Yes	Yes	Yes
IPMI-over-LAN	Yes	Disabled	No	Yes	Yes
SNMPv1 traps	No	Not Configured	No	Yes	Yes

Feature/ Service	Uses Crypto	Default State Out of Box	Supported in Strict Mode	Supported in Standard Mode	Supported in Compatibility Mode
SNMPv3 traps	Yes	Not Configured	No	Yes If enabled, will alert for use of non-FIPS crypto	Yes
SNMPv3 agent	Yes	Not Configured	No	Yes If enabled, will alert for use of non-FIPS crypto	Yes
Email Alerts	Yes	Not Configured	Yes Can NOT be enabled with CRAM-MD5 Authentication	Yes If CRAM-MD5 is required, will alert for use of non-FIPS crypto.	Yes
Syslog Alerts	No	Not Configured	No	Yes	Yes
TLS 1.2	Yes	Enabled	Yes	Yes	Yes
TLS 1.3	Yes	Enabled	Yes	Yes	Yes
Web over HTTPS	Yes	Enabled	Yes	Yes	Yes
Redfish over HTTPS	Yes	Enabled	Yes	Yes	Yes
SSDP	No	Enabled	Yes	Yes	Yes
SSH-CLI	Yes	Enabled	Yes	Yes	Yes
SFTP	Yes	Disabled	Yes	Yes	Yes
LDAP	No	Not configured	No	Yes	Yes
Secure LDAP	Yes	Not configured	Yes	Yes	Yes
Security Key Management	Yes	Not Configured	Yes	Yes	Yes
Remote Console	Yes	Enabled	Yes	Yes	Yes
Virtual media - CIFS	Yes	Not configured	No	Yes	Yes
Virtual media - NFS	No	Not configured	No	Yes	Yes
Virtual media - HTTPFS	Yes	Not configured	Yes	Yes	Yes

Feature/ Service	Uses Crypto	Default State Out of Box	Supported in Strict Mode	Supported in Standard Mode	Supported in Compatibility Mode
RDOC - Local	Yes	Not Configured	Yes	Yes	Yes
RDOC - CIFS	Yes	Not Configured	No	Yes	Yes
RDOC - HTTP	No	Not Configured	No	Yes	Yes
RDOC - HTTPS	Yes	Not Configured	Yes	Yes	Yes
RDOC - FTP	No	Not Configured	No	Yes	Yes
RDOC - SFTP	Yes	Not Configured	Yes	Yes	Yes
FFDC upload (SFTP)	Yes	Enabled	Yes	Yes	Yes
FFDC upload (TFTP)	No	Enabled	No	Yes	Yes
Update from repository – CIFS	Yes	Not configured	No	Yes	Yes
Update from repository - NFS	No	Not configured	No	Yes	Yes
Update from repository – HTTP	No	Not configured	No	Yes	Yes
Update from repository – HTTPS	Yes	Not configured	Yes	Yes	Yes
Call home	Yes	Disabled	Yes	Yes	Yes
Third-party Password	Yes	Not configured	No	Yes	Yes
Port Forwarding	N/A	Disabled	Yes	Yes	Yes

Security mode switching

Use the information in this topic to switch and validate security mode.

Standard Mode is the default security mode.

In general, if XCC detects any setting non-compliant with Standard Mode, XCC will display a notification, but does not require the user to change the mode. In this case, XCC will enter Standard security mode with override (non-compliance).

User can open the drop-down menu to select different mode and use the **Validate** function to determine how many non-compliant items are detected by XCC.

When user click on **Apply**, XCC will also validate the compliant items.

SSL overview

This topic is an overview of the SSL security protocol.

SSL is a security protocol that provides communication privacy. SSL enables client/server applications to communicate in a way that prevents eavesdropping, tampering, and message forgery. You can configure the XClarity Controller to use SSL support for different types of connections, such as secure web server (HTTPS), secure LDAP connection (LDAPS), CIM over HTTPS, and SSH server, and to manage the certificates that are required for SSL.

SSL certificate handling

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

The WEB, Redfish, and LDAP client use the same certificate configuration. SSL connection must be re-established whenever you wish to change the SSL certificate configuration. SSL can be used either with a self-signed certificate or with a certificate signed by a third party Certificate Authority. Using a self-signed certificate is the most straightforward method for using SSL, but at the cost of 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 attempted between the client and server. It is possible that a malicious third party could impersonate the server and intercept data flowing between the XClarity Controller and the browser. If (at the time of the initial connection between the browser and the XClarity Controller) the self-signed certificate is imported into the browser's certificate store, all future communications will be secure for that browser (assuming the initial connection was not compromised by an attack). After using the SSL Certificate Management page to generate a key pair and a self-signed certificate, SSL may be enabled.

For more complete security, use a certificate that is signed by a certificate authority (CA). To obtain a signed certificate:

- Select **Generate CSR (certificate signing request)** from the **Generate** icon under **SSL Certificate Management**.
- Fill in the required fields and select **Generate**.
- After a self-signed certificate is generated, it will be shown in the **SSL Certificate Management**.
- Select **Download Certificate Signing Request (CSR)** from the **Download** icon to download the signed certificate.
- When the signed certificate is downloaded, select the **Import Signed Certificate** icon under **CA Certificate Management** to import it into the XClarity Controller.

  Note: It will take about 15 minutes to activate the new certificate after it is imported.

The function of the CA is to verify the identity of the XClarity Controller. A certificate contains digital signatures for the CA and the BMC. If a well-known CA issues the certificate or if the CA's certificate has already been imported into the web browser, the browser will be able to validate the certificate and positively identify the BMC web server.

Note that SSL compares the XClarity Controller Host Name (or Common Name) in the certificate with the host name as seen by your web browser.

SSL certificate management

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

Click **Security** under **BMC Configuration** to configure the SSL certificate management.

When managing XClarity Controller certificates, you are presented with the following actions:

Download Signed Certificate

Use this link to download a copy of the currently installed certificate. The certificate can be downloaded in either PEM or DER format. The contents of the certificate can be viewed using a third-party tool such as OpenSSL (http://www.openssl.org). An example of the command line for viewing the contents of the certificate using OpenSSL would look something like the following:

```
openssl x509 -in cert.der -inform DER -text
```

Download Certificate Signing Request (CSR)

Use this link to download a copy of the certificate signing request. The CSR can be downloaded in either PEM or DER format.

Generate Signed Certificate

Generate a self-signed certificate. After the operation is completed, SSL may be enabled using the new certificate.

Note: When performing the **Generate Signed Certificate** action, a Generate self-signed certificate for HTTPS window opens. You will be prompted to complete the required and optional fields. You **must** complete the required fields. Once you have entered your information, click **Generate** to complete the task. It will take about 15 minutes to activate the new certificate after it is generated.

Generate Certificate Signing Request (CSR)

Generate a certificate signing request (CSR). After the operation is completed, the CSR file may be downloaded and sent to a certificate authority (CA) for signing.

Note: When performing the **Generate Certificate Signing Request (CSR)** action, a Generate Certificate Signing Request for HTTPS window opens. You will be prompted to complete the required and optional fields. You **must** complete the required fields. Once you have entered your information, click **Generate** to complete the task.

Import a Signed Certificate

Use this to import a signed certificate. To obtain a signed certificate, a certificate signing request (CSR) must first be generated and sent to a certificate authority (CA).

Note: It will take about 15 minutes to activate the new certificate after it is imported.

Configuring the Secure Shell server

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

Click **Network** under **BMC Configuration** to configure the Secure Shell server.

To use the SSH protocol, a key needs to be generated first to enable the SSH server.

Notes:

- No certificate management is required to use this option.
- The XClarity Controller will initially create a SSH server key. If you wish to generate a new SSH server key, click **Network** under **BMC Configuration**; then, click **Generate key** under **SSH Server**.
- After you complete the action, you must restart the XClarity Controller for your changes to take effect.

IPMI over Keyboard Controller Style (KCS) Access

Use the information in this topic to control IPMI over Keyboard Controller Style (KCS) access to the XClarity Controller.

The XClarity Controller provides an IPMI interface via the KCS channel that does not require authentication.

Click **Security** under **BMC Configuration** to enable or disable **IPMI over KCS Access**.

Notes:

- After you change the settings, you must restart the XClarity Controller for your changes to take effect.
- **Disabled (enable on demand)** will disable the KCS channel most of the time, but allow some Lenovo tools to exchange information with the XClarity Controller during the system firmware update window. When that occurs, the KCS channel is enabled briefly for a few minutes and then disabled upon completion or upon timeout.

Important: If you are not running any tools or applications on the server that access the XClarity Controller through the IPMI protocol, it is highly recommended that you disable the IPMI KCS access for improved security. XClarity Essentials does use the IPMI over KCS interface to the XClarity Controller. If you disabled the IPMI over KCS interface, re-enable it prior to running XClarity Essentials on the server. Then disable the interface after you have finished.

Prevent System Firmware Down-Level

Use the information in this topic to prevent system firmware from being changed to older firmware levels.

This feature allows you to decide whether or not to allow the system firmware to return to an older firmware level.

Click **Network** under **BMC Configuration** to enable or disable **Prevent System Firmware Down-Level**.

Any changes that are made will take effect immediately without the XClarity Controller requiring a restart.

Configuring the Security Key Management (SKM)

Use the information in this topic to create and manage security keys.

This feature uses centralized Key Management server to provide keys that unlock storage hardware, to gain access to data stored on SEDs in a ThinkSystem server. The Key Management server includes SKLM - IBM SED Key Management server, and KMIP - Thales/Gemalto SED Key Management servers (KeySecure and CipherTrust).

Note: This feature will be supported in a future update.

Security password manager

Use the information in this topic to allow Third-party password.

This feature allows user to decide whether or not to allow third-party password being used.

- **Third-Party Password** : once enabled, BMC will be able to use a user provided password hash for authentication.
- **Allow Third-Party Password Retrieval** : User can also enable or disable the retrieval of the third-party password hash from BMC.

Extended Audit Log

Use the information in this topic to control extended audit log.

This feature allows you to decide whether or not to include the log entries of IPMI set command (raw data) from LAN and KCS channels into the audit log.

Click **Security** under **BMC Configuration** on XCC web to enable/disable extended audit log.

Note: If the IPMI set command is from LAN channel, user name and source IP address will be included in the log message. And all IPMI commands with sensitive security information (e.g. password) are excluded.

Limit concurrent login per user account

Use the information in this topic to limit concurrent sessions per user account.

This feature allows user to decide how many concurrent sessions are allowed per user account..

- **Number of Web concurrent sessions**: Can be set from 1 to 10 sessions.
- **Number of Command Line concurrent sessions**: Can be set from 1 or 2 sessions.
- **Number of Redfish concurrent sessions**: Can be set from 1 to 16 sessions.

Note: If the total number of sessions exceeds the number set, user can no longer create a new session.

System guard

This topic is an overview of System guard.

The System Guard feature takes a snapshot of the hardware component inventory as trusted reference, then monitors for any deviation from the reference snapshot. When deviation occurs, it can report an event to the user, optionally, can also prevent the server from booting into the OS and prompt the user for response.

User can take a snapshot at any time even while the feature is disabled. The generation of snapshot takes around one minute. User can select a subset of hardware components to enforce, and select a corresponding action to take when deviation is detected.

Note: Deviation detection is executed at server power on (POST) or system reboot. For example, while the OS is still running, if a disk drive is being pulled out and then plugged back in a moment later, System Guard is not going to record the event or take any action. If the pulled out disk drive remains absent until next reboot, then System Guard would get in action.

Notes: During AC restore followed by first power on, XCC may not notify UEFI to prevent OS boot if the following conditions are met:

- System Guard enabled with:
  - **CPU** or **DIMM** hardware selected
  - **Prevent OS booting** option selected
- A hardware configuration change that doesn't match trusted snapshot.

The XCC will report a configuration mismatch after POST, and this limitation will not persist in subsequent OS reboot.

Enabling system guard

Use the information in this topic to enable system guard..

The System Guard feature is disabled by default. It is enabled before shipment as per the requirement of the end user.

XCC reset-to-default option also disables System Guard and clears the settings except snapshot history.

While enabling System Guard, the user is asked to confirm the settings, use the existing trusted snapshot, or capture inventory as a new trusted snapshot before turning on System Guard protection. Once it is turned on:

- If the system power is off, System Guard starts to harvest the hardware inventory right away.
- If the system power is on, System Guard compares the component inventory data with the trusted snapshot.

If the result of the comparison indicates a deviation from the trusted snapshot, XCC displays a warning **Noncompliance due to hardware configuration mismatch**. The details of the mismatch list each missing/ changed/new hardware component with location/identifier/description attributes, compared with the trusted snapshot.

User can configure System Guard's scope and action and decide which action to take when system becomes noncompliant via the Scope and Action panel.

TLS Version Support

Use the information in this topic to understand different supported TLS version.

The following TLS version are supported:

- TLS 1.2 and higher
- TLS 1.3

For a full list of the supported TLS cipher suites, see "Supported TLS cipher suites" on page 38

Configuring Call Home

Use the information in this topic to configure call home.

You can create a service forwarder that automatically sends service data for any managed device to Lenovo Support using the Call Home function.

Lenovo is committed to security. When enabled, Call Home automatically contacts Lenovo to open a service ticket and sends in service data collected from a managed device whenever that device reports a hardware failure. Service data that you would typically upload manually to Lenovo Support is automatically sent to the Lenovo Support Center over HTTPS using TLS 1.2 or later, your business data is never transmitted. Access to service data in the Lenovo Support Center is restricted to authorized service personnel.

Entering the call home page for the first time

When entering the Call Home page for the first time, you'll see a warning window, click on **View Terms and Conditions** to continue.

Attention: You must accept the **Lenovo Privacy Statement** before you can transfer data to Lenovo Support. This action only needs to be once when first enter the page.

Note: You can find "View Terms and Conditions" and **Lenovo Privacy Statement** on top of the page to review them anytime.

Configure Call Home

There are nine required fields to be filled in:

- Country
- Contact Name
- Phone
- Email
- Postal Code

Attention: All the required fields must be filled in or you won't be able to apply the changes and enable **Reporting to Lenovo Service**.

Activity Log

The displayed event information content includes Severity, Case Number, Event ID, Message, Date, Status and Action.

Each ticket can have one of the following five status:

- **Pending:** The service information is being sent or waiting for response.
- **Active:** The service information was sent successfully and the problem is currently being processed.
- **Failed:** The service information was not sent successfully.
- **Closed:** The problem has been processed and closed.
- **Cancelled:** The problem has been processed and cancelled.

You can perform one of the following two actions for each ticket:

- **Action — Cancel:** When a ticket's status is "Active", you can click the "Undo" icon in the "Action" column to cancel the ticket.
- **Action — Note:** When you click the "Note" icon in the "Action" column, you'll be prompted to leave notes for the corresponding event.

  Note: Both **Notes Title** and **Notes Message** must be filled in to be sent successfully. This function **ONLY sends information to the server**. It is not for saving and displaying the information. If you click Note again, you'll be prompted with a new Note window to leave another message.

Test Call Home

You can test call home function by clicking on **Test Call Home** in the **Activity Log** section, a message will display on top of the page to indicate whether the operation was successful, and you will be able to check the event log below for test result.

Attention: To successfully Call Home, please ensure that DNS settings are valid and a connection exists to the Internet address required by Call Home. If XClarity Controller access the Internet through an HTTP proxy, ensure that the proxy server is configured to use basic authentication and is set up as a non-terminating proxy.

HTTP Proxy

HTTP Proxy serves two intermediary roles as an HTTP Client and an HTTP Server for security, management, and caching functionality. The HTTP Proxy routes HTTP Client requests from a Web browser to the Internet, while supporting the caching of Internet data.

- **Proxy Location:** This field is required to enable the HTTP Proxy. It can only accept a maximum of 63 characters, allowing users to specify IP address or hostname. The host name only contains alphanumeric, hyphen ('-'), and underscore ('_') characters.
- **Proxy Port:** This field is required to specify the port of the HTTP Proxy. This field only allows numbers to be entered, ranging from 1-65535.
- **Test Proxy:** To enable this feature, you need to fill in the correct Proxy Location and Proxy Port to test whether the current HTTP Proxy function is available.
- **User Name:** If the **Requires authentication** option is checked, the username will be required and represent a proxy credential. This field allows a maximum length of 30 characters and spaces are invalid.
- **Password:** This field is optional and will be displayed if the **Requires authentication** option is checked. This field allows a maximum length of 15 characters and spaces are invalid.

Backing up and Restoring the BMC configuration

The information in this topic describes how to restore or modify the BMC configuration.

Select **Backup and Restore** under **BMC Configuration** to perform the following actions:

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

Backing up the BMC configuration

The information in this topic describes how to back up the BMC configuration.

Select **Backup and Restore** under **BMC Configuration**. At the very top is the **Backup BMC configuration** section.

If a backup was previously made, you will see the details in the **Last backup** field.

To backup the current BMC configuration, follow the steps shown below:

1. Specify the password for the BMC backup file.
2. Select if you wish to encrypt the whole file or only sensitive data.
3. Begin the backup process by clicking **Start Backup**. During the process, you are not allowed to perform any restore/reset actions.
4. When the process is completed, a button will appear to let you download the and save the file.

Note: When the user sets up a new XClarity Controller user/password and performs a backup of the configuration, the default account/password (`USERID/PASSWORD`) is included as well. Subsequently deleting the default account/password from the backup will result in the system showing a message notifying the user that there is a failure in restoring the XClarity Controller account/password. Users can ignore this message.

Restoring the BMC configuration

The information in this topic describes how to restore the BMC configuration.

Select **Backup and Restore** under **BMC Configuration**. Located below **Backup BMC Configuration** is the **Restore BMC from Configuration File** section.

To restore the BMC to a previously saved configuration, follow the steps shown below:

1. Browse to select the backup file and input the password when prompted, then click **Next >**.
2. Verify the file by clicking **View Details**.
3. After verifying the content, click **Start Restore**.

Resetting the BMC to Factory Default

The information in this topic describes how to reset the BMC to the factory default settings.

Select **Backup and Restore** under **BMC Configuration**. Located below **Restore BMC from Configuration File** is the **Reset BMC to Factory Default** section.

To reset the BMC to factory defaults, follow the steps shown below:

1. Click **Start to Reset BMC to Factory Defaults**.

   Notes:

   - Only users with Supervisor user authority level can perform this action.
   - The Ethernet connection is temporarily disconnected. You must log in the XClarity Controller web interface again after the reset operation is completed.
   - Once you click **Start to Reset BMC to Factory Defaults**, a confirmation window will pop up and you can select the checkboxes to retain the following settings:
     - **Retain Local User Settings**: Current User/Role/Global Setting will be backed up. It restores content CLI command “users”/”roles”/”accesscfg”. For example: User name/Role name/ Password expiration warning time period/ Password complexity rules enabled etc.
     - **Retain Network Settings**: Current network Setting will be backed up. It restores the network output of the “ifconfig” CLI command. For example: Host Name/Ipv4 address/Ipv6 address/ gateway etc.
   - Once you click **Ok**, all previous configuration changes will be lost except the ones you choose to retain.
   - If you wish to enable LDAP when restoring the BMC configuration, you will need to first import a trusted security certificate before doing so.
   - If you are working from the BMC local system, you will lose your TCP/IP connection as a result. You will need to reconfigure the BMC network interface to restore connectivity.
   - After the process is completed, the XClarity Controller will be restarted.
   - Resetting the BMC to Factory Default will not affect UEFI settings and access mode (single/multi user) of Remote Console (this is saved into browser cookies).

Restarting the XClarity Controller

The information in this topic explains how to restart your XClarity Controller.

For details on how to restart the XClarity Controller, see “Power actions” on page 62

Chapter 4. Monitoring the server status

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

Once you log into the XClarity Controller, a system status page will be displayed. From this page, you can view the server hardware status, event and audit logs, system status, maintenance history and alert recipients.

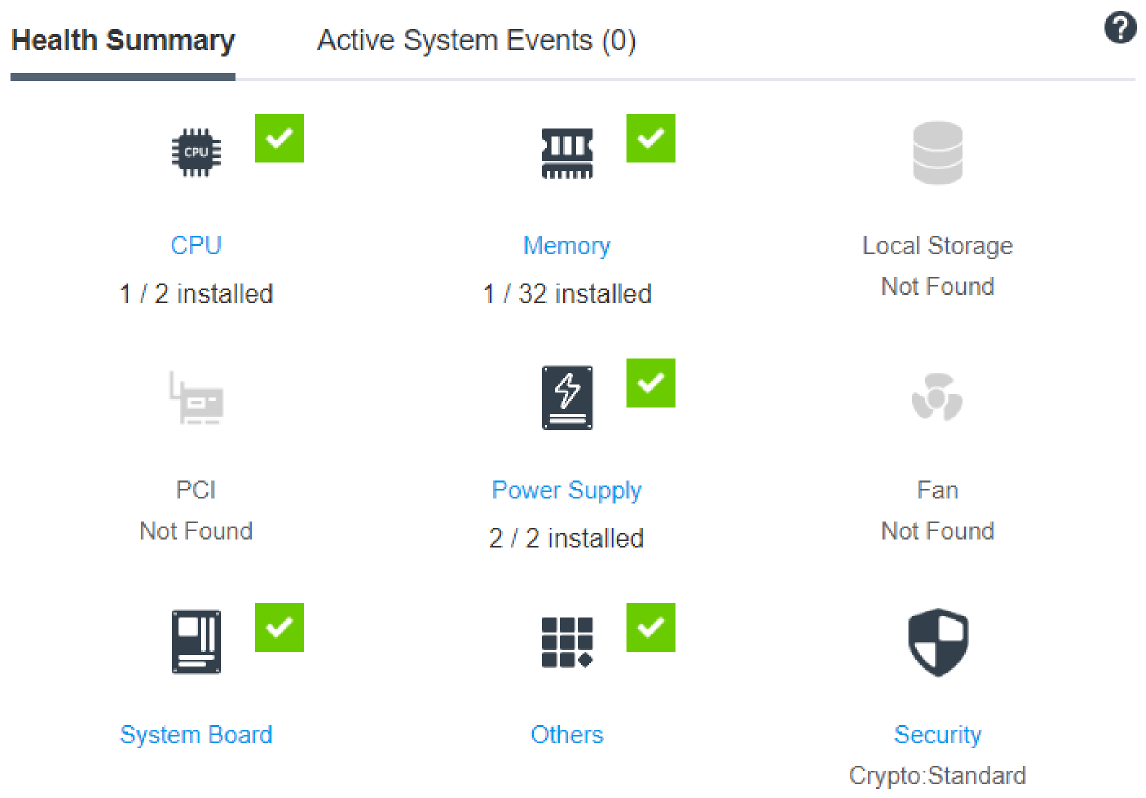
Viewing the Health Summary/Active System Events

Use the information in this topic to understand how to view the Health Summary/Active System Events.

When you access the XClarity Controller home page, the **Health Summary** is shown by default. A graphical representation is given, which shows the number of hardware components that have been installed and their respective health status. The hardware components that are being monitored include the following:

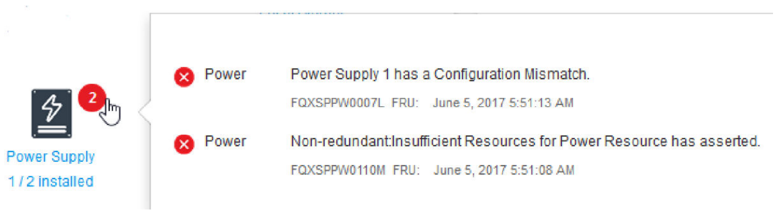
- CPU (Processor)
- Memory
- Local Storage
- PCI Adapters
- Power Supply
- Fan
- System Board
- Others
- Security

Note: Local Storage may show **not available** on the Status Icon on systems with a simple swap back-plane configuration.



CPU ✓ 1 / 2 installed	Memory ✓ 1 / 32 installed	Local Storage Not Found
PCI Not Found	Power Supply ✓ 2 / 2 installed	Fan Not Found
System Board ✓	Others ✓	Security Crypto:Standard

If any of the hardware components is not operating normally, it will be marked by a critical or warning icon. A critical condition is indicated by a red circle icon, while a warning condition is indicated by a yellow triangle icon. By hovering the mouse icon over the critical or warning sign, up to three currently active events for that component will be shown.



⊗	Power	Power Supply 1 has a Configuration Mismatch. FQXSPPW0007L FRU: June 5, 2017 5:51:13 AM
⊗	Power	Non-redundant:Insufficient Resources for Power Resource has asserted. FQXSPPW0110M FRU: June 5, 2017 5:51:08 AM

To view the other events, click the **Active System Events** tab. A window will appear showing the events that are currently active in the system. Click **View all event logs** to view the entire event history.

If the hardware component is marked by a green check mark, it is operating normally, and there are no active events.

The text underneath the hardware component states the number of components installed. If you click the text (link), you will be directed to the **Inventory** page.

Viewing the System Information

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

The **System Information and Settings** panel located to the right of the home page provides a summary of common server information, which includes the following:

- Machine name, power and operating system state
- Machine Type/Model
- Serial Number
- System Name
- Front Panel USB Port Management

  Note: This feature will be supported in a future update.
- BMC License
- BMC IP Address
- BMC Hostname
- BMC version
- UEFI version
- Location

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

Table 2. System state descriptions

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

State	Description
System power off/State unknown	The server is powered off.
System on/starting UEFI	The server is powered on; but, UEFI is not running.
System running in UEFI	The server is powered on and UEFI is running.
Booting operating system or in unsupported operating system (the system might be in this state if the OS does not respond to pings)	The server might be in this state for one of the following reasons: • The operating system loader has started; but, the operating system is not running • The BMC Ethernet over USB interface is disabled. • The operating system does not have the drivers loaded that support the Ethernet over USB interface.
Operating system booted	The server operating system is running.
System running in memory test	The server is powered on and running memory diagnostic tools.
System running in Setup	The server is powered on and the system has booted into UEFI F1 setup menu or LXPM menu.
System running in LXPM maintenance mode	The server is powered on and the system has booted into the LXPM maintenance mode under which users can’t navigate through the LXPM menu.

If you wish to change the system name, click the pencil icon. Type the system name you wish to use; then, click the green check mark.

If your server has a license other than the XClarity Controller Premier level license, you may be able to purchase a license upgrade to enable enhanced features. To install the upgrade license after you have obtained an upgrade license, click the upward-pointing arrow icon.

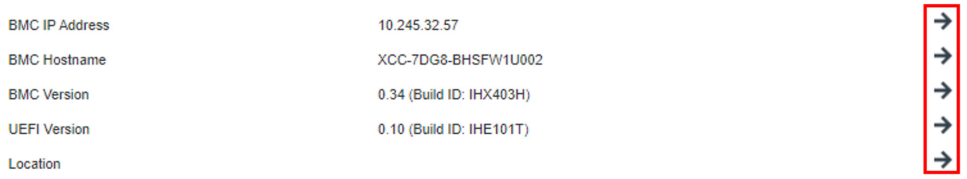
BMC License

To add, delete or export a license, click the rightward-pointing arrow icon.

BMC License

To change the relevant settings for the BMC IP address, BMC host name, UEFI version, BMC version and location items, click the right-ward pointing arrow.

- For the IP address and host name, you will be led to the **Ethernet Configuration** section under **Network**.
- For the UEFI and BMC version items, you will be led to the **Firmware Update** page.
- For the location item, you will be led to the **Server Properties** section on the **Server Configuration** page.



BMC IP Address	10.245.32.57	→
BMC Hostname	XCC-7DG8-BHSFW1U002	→
BMC Version	0.34 (Build ID: IHX403H)	→
UEFI Version	0.10 (Build ID: IHE101T)	→
Location		→

Viewing the System Utilization

By clicking **Utilization** in the left pane, a summary of common server utilization information is provided.

System utilization is a composite metric based on the real-time utilization of processor, memory, and I/O subsystems. The utilization data can be viewed in either Graphic View or Table View, which includes the following:

- **Temperature**
  - Display real time ambient temperature and the key component temperatures.
  - Hovering the mouse cursor over a memory module will show its current temperature.
  - The History tab displays the historical temperatures charts for up to the past 24 hours.
- **Power Utilization**
  - Display current power consumption pie chart, as well as the historical power consumption charts for up to last 24 hours.
  - Hovering the mouse cursor over the pie chart will show its current power consumption.
  - Current power consumption pie chart consists of four categories: CPU, Memory, Other and Spare. “Other” means the total system power consumption minus CPU and Memory power consumption. “Spare” means the total available allocated power minus the total system power consumption.
  - Voltage tab displays the current voltage readings and status on all voltage sensors supported by hardware.
- **System Utilization**
  - Represents the current utilization snapshot of the system, processor, memory and I/O subsystems.

    Note: This feature will be supported in a future update.
- **Fan Speed (RPM)**
  - The fan speed section shows the fan speeds as a percentage of the maximum speed.
  - User can click on the gear icon to access **Fan Speed Boost** options.

  - This setting allows additional cooling to the server based on ambient temperature. It can increase the fan over normal speed by controlled thermal algorithm. There will be no change if the fans are already running at full speed.

Viewing Event Logs

The **Event Log** provides a historical list of all hardware and management events.

Select the **Event Log** tab in **Events** to display the **Event Log** page. All events in the log are time stamped, using the XClarity Controller date and time settings. Some events also generate alerts when they occur, if they are configured to do so in **Alert Recipients**. You can sort and filter events in the event log.

The following is a description of the actions that can be performed in the **Event Log** page.

- **Customize table**: Select this action item to choose the type of information you wish to display in the table. A sequence number can be displayed to assist in determining the order of events when more than one event has the same timestamp.

  Note: Some sequence numbers are used by internal BMC processes, so it is normal that there may be gaps in the sequence numbers when the events are sorted by sequence number.
- **Clear logs**: Select this action item to delete the event logs.
- **Refresh**: Select this action item to update the display with any event log entries that may have occurred since the page was last displayed.
- **Type**: Select which event types to show. The event types include the following:
  - ❌ Shows Error entries in the log
  - ⚠ Shows Warning entries in the log
  - ℹ Shows Informational entries in the log

  Click each icon to turn off or on the types of errors to be displayed. Clicking the icon successively will toggle between showing and not showing the events. A black box surrounding the icon indicates that type of event will be displayed.
- **Source type filter**: Select an item from the drop-down menu to display only the type of event log entries that you wish to be shown.
- **Time filter**: Select this action item to specify the interval of the events that you want to show.
- **Search**: To search for specific types of events or keywords, click the magnifying glass icon, and type a word to search for in the **Search** box. Note that the input is case-sensitive.

Note: The maximum number of event log records is 1024. When the event logs are full, the new log entry will automatically overwrite the oldest one.

Viewing Audit Logs

The **Audit Log** provides a historical record of user actions, such as logging in to the XClarity Controller, creating a new user, and changing a user password.

You can use the audit log to track and document authentication, changes, and system actions.

Both the event log and the audit log support similar maintenance and viewing actions. To see the description of the display and filtering actions that can be performed on the Audit Log page, see "Viewing Event Logs" on page 55.

Notes:

- After running Lenovo's tools on your server operating system, the Audit Log may contain records showing actions performed by a username (for example user "20luN4SB") that you may not recognize. When some of the tools are run on the server operating system, they may create a temporary user account for accessing the XClarity Controller. The account is created with a random username and password and can only be used to access the XClarity Controller on the internal Ethernet over USB interface. The account can only be used to access the XClarity Controller Redfish and SFTP interfaces. The creation and removal of this temporary account is recorded in the audit log as well any actions performed by the tool with these credentials.
- The maximum number of audit log records is 1024. When the audit logs are full, the new log entry will automatically overwrite the oldest one.

Viewing the Maintenance History

The **Maintenance History** page includes information about the firmware update, configuration and hardware replacement history.

The contents of the maintenance history can be filtered to display certain types of events or certain intervals of time.

Note: The maximum number of maintenance history records is 250. When the maintenance history logs are full, the new log entry will automatically overwrite the oldest one.

Configuring Alert Recipients

Use the information in this topic to add and modify email and syslog notifications or SNMP TRAP recipients.

The following is a description of the actions that can be performed in the **Alert Recipients** tab.

The following actions items can be performed in the **Email/Syslog Recipients** section.

- **Create**: Select this action item to create additional new Email recipients and Syslog recipients. Up to 12 Email and Syslog recipients can be configured.
  - **Create Email Recipient**: Select this action item to create an Email recipient.
    - Enter the name and Email address of the recipient.
    - Select to enable or disable the event notification. If disable is selected, the account will remain configured, but no Emails will be sent.
    - Select the types of events that the recipient will be notified of. If you click the arrow next to the Critical, Attention, or System category labels you can select or deselect notifications for specific components in the category.
    - You can choose whether or not to have the event log contents included in the email alert.
    - The index specifies which of the 12 recipient slots is assigned.
    - Enter the IP address or host name of the SMTP Email Server.
    - You can configure the Email server to which the events will be forwarded here or by clicking the SMTP Server action at the top of the section. See SMTP Server below for configuration details.

  - **Create Syslog Recipient**: Select this action item to create syslog recipients.
    - Enter the name of the recipient.
    - Enter the IP address or host name of the Syslog server.
    - Select to enable or disable the event notification. If disable is selected, the account will remain configured but no Emails will be sent.
    - The index specifies which of the 12 recipient slots is assigned.
    - Select the types of events that will be sent to the Syslog server. If you click the drop-down menu next to the Critical, Attention, or System category labels you can select or deselect notifications for specific components in the category.
- **SMTP Server**: Select this action item to configure the relevant settings for the SMTP Email server. Only one Email server can be configured. The same Email configuration is used when sending alerts to all of the configured Email recipients. The XClarity Controller automatically switch from an secure connection to an encrypted connection for mail transfer using the StartTLS command uniformly via port 587, if the target mail server supports it.
  - Enter the host name or IP address and network port number of the Email server.
  - If the Email server requires authentication, select the **Requires authentication** checkbox and enter the username and password. Select the type of authentication that is required by the Email server, either a challenge-response method (**CRAM-MD5**) or simple credentials (**LOGIN**).
  - Some networks may block outgoing Emails if the reverse path value is not as expected. By default, the XClarity Controller will use alertmgr@domain, where the domain is the Domain name as specified in the DDNS section of the XClarity Controller network web page. You can specify your own sender information in place of the default.
  - You can test the connection to the Email server to ensure that the Email settings have been configured correctly. The XClarity Controller will display a message indicating whether or not the connection is successful.
- **Retry and Delay**: Select this action item to configure the relevant settings for the retry and delay options.
  - The retry limit specifies the number of times that the XClarity Controller will attempt to send an alert if the initial attempt did not succeed.
  - The delay between entries specifies the amount of time that the XClarity Controller will wait after sending an alert to one recipient before sending an alert to the next recipient.
  - The delay between attempts specifies the amount of time that the XClarity Controller will wait after a failed attempt before retrying to send the alert.
- **Protocol**: Select this action item to configure the relevant settings for connection protocol.
  - You can choose between **TCP Protocol** or **UDP Protocol**, please note that this setting will apply to all syslog recipients.
- If Email or Syslog Recipients have been created, they will be listed in this section.
  - To edit the settings for an Email or Syslog Recipient click the pencil icon below the action header on the row next of the recipient that you wish to configure.
  - To delete an Email or Syslog Recipient click the trash can icon.
  - To send a test alert to an Email or Syslog Recipient, click the paper airplane icon.

The following actions can be performed in the **SNMPv3 Trap User** section.

- SNMPv3 user, please go to the SNMP setup card on the network page and create it under Enable SNMPv3 Trap.
- **Create**: Select this action item to create SNMPv3 TRAP recipients.

- Select the user account that is to be associated with the SNMPv3 TRAPs. The user account must be one of the twelve local user accounts.
- Specify the host name or IP address of the SNMPv3 manager that will receive the SNMPv3 TRAPs.
- The XClarity Controller uses the HMAC-SHA hash algorithm to authenticate with the SNMPv3 manager. This is the only algorithm supported.
- The privacy password is used with the privacy protocol to encrypt the SNMP data.
- The **SNMPv3 global setting** applies to all SNMPv3 TRAP recipients. These settings can be configured while creating an SNMPv3 TRAP recipient or by clicking the SNMPv3 Settings action at the top of the **SNMPv3** user segment.
  - Select to enable or disable SNMPv3 TRAPs. If disabled, the settings will remain configured but no SNMPv3 TRAPs will be sent.
  - The BMC Contact and Location information is required and is configured on the Server Properties web page. See "Setting Location and Contact" on page 66 for more information.
  - Select the types of events that will be cause TRAPs to be sent to the SNMPv3 manager. If you click the drop-down menu next to the Critical, Attention, or System category labels you can select or deselect notifications for specific components in the category.

Note: Data transfer between the SNMP client and the agent can be protected using encryption. The supported methods for **privacy protocol** are CBC-DES and AES.

- If SNMPv3 TRAP recipients have been created, they will be listed in this section.
  - To edit the settings for a SNMPv3 recipient, click the pencil icon below the action header on the row next of the recipient that you wish to configure.
  - To delete a SNMPv3 recipient, click the trash can icon.

Chapter 5. Configuring the Server

Use the information in this chapter to understand the options available for server configurations.

When configuring the server, the following options are available:

- Adapters
- Boot options
- Power policy
- Server properties

Viewing the adapter information and configuration settings

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

Click **Adapters** under **Server Configuration** to view information about the adapters installed in the server.

Note: If the adapter does not support status monitoring, it will not be visible for monitoring or configuration. For inventory related information of all the installed PCI adapters, refer to the **Inventory** page.

Configuring system boot mode and order

To configure the system boot mode and order, use the information in this topic.

When you select **Boot Options** under **Server Configuration**, you can configure the system boot order.

Note: No unauthenticated in-band method is allowed to change security related system settings. For example, Secure Boot must NOT be able to configure over unauthenticated in-band APIs from the OS or UEFI shell. This includes OneCLI running in-band and obtaining temporary credentials using IPMI, or any tools and APIs to configure Secure Boot, TPM, UEFI Setup password related settings. All security related settings must require proper authentication with sufficient privilege.

To configure the system boot order, select a device from the list of **Available devices** and click the right arrow to add the device to the boot order. To remove a device from the boot order, select a device from the boot order list and click the left arrow to move the device back to the list of available devices. To change the boot order, select a device and click the up or down arrow to move the device up or down in priority.

When you make a change to the boot order, you must select a restart option before applying the change. The following options are available:

- **Restart server immediately**: The boot order changes are saved and the server is restarted immediately without shutting down the operating system.
- **Restart server normally**: The boot order changes are saved and the operating system is shutdown before restarting the server.
- **Manually restart later**: The boot order changes will be saved, but will not take effect until the next time the server is rebooted.

Configuring one-time boot

To temporarily ignore the configured boot and instead boot to a specified device one time, use the information in this topic.

Click **Boot Options** under **Server Configuration** and select a device from the drop-down menu to configure the device that the system will boot to one-time on the next server restart. The following choices are available:

PXE network
Sets up your server to attempt a Preboot Execution Environment network boot.

Primary removable media
The server is booted from the default USB device.

Default CD/DVD
The server is booted from the default CD/DVD drive.

F1 system setup
The server is booted into the Lenovo XClarity Provisioning Manager.

Diagnostic Partition
The server is booted into the Diagnostics section of the Lenovo XClarity Provisioning Manager.

Default Hard Disk
The server is booted from the default disk drive.

Primary remote media
The server is booted from the mounted virtual media.

Mounted
The configured boot order is used. There is no one-time boot override of the configured boot order.

No one-time boot
The configured boot order is used. There is no one-time boot override of the configured boot order.

When you select a one-time change to the boot order, you must select a restart option before applying the change.

- **Restart server immediately**: The boot order change is saved and the server is restarted immediately without shutting down the operating system.
- **Restart server normally**: The boot order change is saved and the operating system is shutdown before restarting the server.
- **Manually restart later**: The boot order change is saved, but will not take effect until the next time the server is rebooted.

Managing the server power

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

Select **Power Policy** under **Server Configuration** to view power management information and perform power management functions.

Note: In an enclosure containing high-density server nodes, the chassis cooling and power is controlled by the SMM instead of the XClarity Controller. Refer to SMM3 web interface fore more details of solution power status.

Configuring the power redundancy

To configure the power redundancy, use the information in this topic.

Notes:

- AMD servers do not support configuring the power policy function.

- When 2 power supply units are installed, the redundancy mode is set to Redundant (N+N). With this 2 Power supply units configuration, if one of the power supply units fail, AC lost or has been removed, it will report redundant lost event in XCC event log.
- When only 1 power supply unit is installed after shipping, the redundancy mode will be automatically set to Non-redundant mode.

Available fields in the Power Redundancy section include the following:

- **Redundant (N+N)**: There are two or more independent power sources that are capable of supplying power to the system simultaneously. This means that if one or more power sources fails, the other source (s) can continue to supply power to the system without any interruption. N+N redundancy provides a high level of fault tolerance and ensures that the system remains operational even in the event of multiple failures.
  - **Zero Output Mode**: Once enabled under Redundant configuration, some PSUs will automatically enter into standby state under light load conditions. In this manner, the remaining PSU delivers the entire power load to increase efficiency.
- **Non-redundant mode**: In this mode, the server is not guaranteed to remain operational if a power supply is lost. The server will throttle if a power supply fails in an attempt to remain running.

Click **Apply** after making the configuration changes.

Configuring the power capping policy

To configure the power capping policy, use the information in this topic.

Notes:

- AMD servers do not support configuring the power capping policy function.
- In an enclosure containing high-density server nodes, the chassis cooling and power is controlled by the SMM instead of the XClarity Controller. Refer to SMM3 web interface fore more details of solution power status.

You can choose to enable or disable the power capping function. If power capping is enabled, a selection can be made to limit the amount of power used by the server. If power capping is disabled, the maximum power used by the server is determined by the Power Redundancy policy. To change the setting, first click **Reset**. Choose your preferred setting; then, click **Apply**.

Total Power Capacity is being calculated based on power redundancy mode and number of PSUs installed in the system. The manual setting of maximum power limit can be over the actual power capacity.

When power capping is enabled, the system may be throttled in order to maintain the power limit.

Note: Even when power capping is disabled, the system may be throttled under certain fault conditions, such as power supply failure, cooling issue, etc.

Power capping can be enabled using **Output** measurements. There are two ways to change the power capping value:

- **Method 1**: Move the slider mark to the desired wattage to set the overall server power limit.
- **Method 2**: Input the value in the input box. The slider mark will automatically move to the corresponding position.

Click **Apply** after making the configuration changes. Changes will take effect immediately.

Configuring the power restore policy

To configure how the server reacts when the power is restored after a power loss, use the information in this topic.

When configuring the power restore policy, the following three options are available:

Always Off

The server will remain powered off even when power is restored.

Restore

The server will automatically be powered on when power is restored if the server was powered on at the time that the power failure occurred. Otherwise, the server power will remain off when power is restored.

Note: Select the checkbox below to set a random delay between 1 and 15 seconds for Power On if the server was on before the power failure occurred.

Always On

The server will automatically power on when power is restored.

Click **Apply** after making the configuration changes.

Power actions

See the information in this topic to understand the power actions that can be made to the server.

Click **Power Action** in the **Quick Action** section of the XClarity Controller home page.

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

Table 3. Power actions and descriptions

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

Power Action	Description
Power On Server	Select this action item to power on the server and boot the operating system.
Power Off Server Normally	Select this action item to shut down the operating system and power off the server.
Power Off Server Immediately	Select this action item to power off the server without first shutting down the operating system.
Restart Server Normally	Select this action item to shut down the operating system and power cycle the server.
Restart Server Immediately	Select this action item to power cycle the server immediately without first shutting down the operating system.
Boot Server to System Setup	Select this item to power on or reboot the server and automatically boot into system setup without needing to press F1 during boot.

Table 3. Power actions and descriptions (continued)

Power Action	Description
Trigger NMI (non-maskable interrupt)	Select this action item to force a Non-maskable Interrupt (NMI) on a “hung” system. Selection of this action item allows the platform operating system to perform a memory dump that can be used for debug purposes of the system hang condition. The auto reboot on NMI setting from the F1 system setup menu determines whether or not the XClarity Controller will reboot the server after the NMI.
Schedule Power Actions	Select this action item to schedule daily and weekly power and restart actions for the server.
Restart Management Controller	Select this action item to restart the XClarity Controller
AC Power Cycle Server	Select this action to power cycle the server.
Notes: • If the operating system is in the screen saver or locked mode when a shutdown of the operating system is attempted, the XClarity Controller might not be able to initiate a normal shutdown. The XClarity Controller will perform a hard reset or shutdown after the power off delay interval expires, while the operating system might still be running. • If the power LED on the front panel is rapidly blinking, the XClarity Controller may not be able to initiate a normal power-on sequence. The XClarity Controller can power on the system once the power LED begins to blink slowly.	

Managing and monitoring power consumption with IPMI commands

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

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

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

Managing the server power using Node Manager commands

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

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

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

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

To enable native Node Manager IPMI commands type:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x01**

To disable native Node Manager IPMI commands type:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x00**

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

Notes:

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

Power monitoring using the Get Global System Power Statistics, (command code 0xC8): Request: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00** Response:57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Power capping using the Set Intel Node Manager Policy, (command code 0xC1): Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**Response:57 01 00

Power savings using the Set Intel Node Manager Policy, (command code 0xC1): Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**

Get device ID function using the Get Intel Management Engine Device ID: Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x06 0x01**Response:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

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

Managing the server power using DCMI commands

Use the information in this topic to manage the server power using DCMI commands.

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

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

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

Get Power Reading: Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x02 0xdc 0x01 0x00 0x00** Response:`dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40`

Set Power Limit: Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **PASSW0RD** `raw` **0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03** Response:`dc`

Get Power Cap: Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x03 0xdc 0x00 0x00** Response:`dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00`

Activate the Power Limit: Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x01 0x00 0x00** Response:`dc`

Deactivate the Power Limit: Request:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x00 0x00 0x00** Response:`dc`

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

For the complete list of commands that are supported by the DCMI specification, see the latest release of the **Data Center Manageability Interface Specification** at https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf.

Downloading service data log

Use the information in this topic to collect service information about your server. This process is normally only done at the request of service personnel to assist in resolving a server problem.

In the XClarity Controller home page, click the **Service Log** option in the **Quick Action** section and select **Service Data Log**.

By default, the service log will contains the following data: system information, system inventory, system utilization, SMBIOS table, sensors reading, events log, FOD key, SLP key, UEFI configuration and XClarity Controller 3 configuration.

Move the mouse over the Basic Information option and click on the floating window to see some of the actual data that will be exported.

While Basic Information is mandatory, the following information can also be exported:

- Network Information (IP, hostname)
- Telemetry (24 hours data)
- Audit Log (contains username)
- Latest Failure Screen

Click **Export** to download the service data log.

The process of collecting the service and support data may takes a few minutes to complete. The file will be saved to your default download folder. The naming convention for the service data file follows this convention: `<machine type and model>_<serial number>_xcc3_ServiceData_<date>-<time>.zip`

For example: 7X2106Z01A_2345678_xcc3_ServiceData_240517-112857.zip.

In addition to the service data in .zip format, the debug log can also be downloaded in .tar.zst file format via **Browse History...**. The naming convention for the debug lodf file follows this convention: `<machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst`

For example: 7X2106Z01A_2345678_xcc3_DebugLog_240517-112857.zip.

Notes:

- **Browse History...** will also retain recently exported service logs.
- .tar.zst file format uses a different compression algorithm and can be extracted with the package “zstd”. For example:

```
tar --use-compress-program=unzstd -xvf <machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst
```

Server Properties

Use the information in this topic to change or view relevant server properties.

Setting Location and Contact

Use the information in this topic to set various parameters to help identify the system for operations and support personnel.

Select **Server Properties** under **Server Configuration**, to configure the **Location and Contact** information.

Contact
Allows you to specify the name and phone number of the person who should be contacted if the system experiences a problem.

Note: This field is the same as the Contact field in the SNMPv3 configuration and is required to enable SNMPv3.

Rack Name
Allows you to locate the server more easily by specifying which rack it is in.

Room Number
Allows you to locate the server more easily by specifying which room it is in.

Building
Allows you to locate the server more easily by specifying which building it is in.

Lowest U
Allows you to locate the server more easily by specifying the position in the rack.

Address
Allows you to specify the full postal address where the server is located.

Note: When the relevant information has been inputted, it will appear as a single line in the **Location** field in the SNMPv3 section and XClarity Controller home page.

Setting server timeouts

Use the information in this topic to set timeouts for the server.

These timeouts are used to restore operation to a server that has hung.

Select **Server Properties** under **Server Configuration**, to configure the server timeouts. The following server timeout selections are provided:

OS Watchdog
The OS watchdog is used to monitor the operating system to ensure that it is not hung. The Ethernet over USB interface must be enabled for this feature. See "Configuring Ethernet over USB" on page 32 for details. The XClarity Controller contacts the operating system at an interval configured in the **OS Watchdog Time** selection. If the operating system does not respond before it is time for the next check, the XClarity Controller assumes that the operating system has hung. The XClarity Controller will capture the contents of the server display and then reboot the server in an attempt to restore operation. The XClarity Controller will reboot the server only once. If the operating system continues to hang after the reboot, instead of continually rebooting the server, the server will be left in the hung state so that the

problem can be investigated and corrected. To rearm the OS watchdog, power the server off and back on. To enable the OS watchdog, select an interval from the OS Watchdog Time drop-down and click **Apply**. To disable the OS watchdog, select **None** on the OS Watchdog Time drop-down menu.

Use this field to specify how often, in minutes, the BMC subsystem will check to confirm that the operating system is running properly. If the operating system fails to respond within 6 seconds to one of these checks, the BMC subsystem will generate an OS Timeout alert and automatically restart the system one time. After the watchdog is tripped and the system is restarted, the OS Watchdog is automatically disabled until the operating system is shutdown and the server is power cycled. This watchdog is not related to the IPMI watchdog.

Make sure that the operating system you are booting has configured the firewall's inbound rules to allow ICMP type 8 (echo requests) packets to be acknowledged in order for the Server Timeout watchdog to function correctly.

To enable the OS watchdog, select an interval from the OS Watchdog Time drop-down and click **Apply**. To disable the OS watchdog, select **None** on the OS Watchdog Time drop-down menu.

Loader Watchdog

The loader watchdog monitors the interval between the completion of POST and when the operating system begins running. The Ethernet over USB interface must be enabled for this feature. See "Configuring Ethernet over USB" on page 32 for details. When POST is completed, the XClarity Controller starts a timer and begins to contact the operating system. If the operating system does not respond with the time configured in the Loader Watchdog selection, the XClarity Controller assumes that the operating system boot has hung. The XClarity Controller will then reboot the server in an attempt to restore operation. The XClarity Controller will reboot the server only once. If the operating system boot continues to hang after the reboot, instead of continually rebooting the server, the server will be left in the hung state so that the problem can be investigated and corrected. The loader watchdog is rearmed when server is switched off and back on or when the server successfully boots into the operating system. To enable the loader watchdog, select an interval from the Loader Watchdog drop-down and click **Apply**. To disable the loader watchdog select **None** on the Loader Watchdog drop-down.

Use this field to specify the number of minutes that the BMC subsystem will wait between the completion of POST and the end of loading of the operating system. If this interval is exceeded, the BMC subsystem will generate a Loader Timeout alert and automatically restart the system one time. After the watchdog is tripped and the system is restarted, the Loader Timeout is automatically disabled until the operating system is shutdown and the server is power cycled. This watchdog is not related to the IPMI watchdog.

Make sure that the operating system you are booting has configured the firewall's inbound rules to allow ICMP type 8 (echo requests) packets to be acknowledged in order for the Server Timeout watchdog to function correctly.

To enable the loader watchdog, select an interval from the Loader Watchdog drop-down and click **Apply**. To disable the loader watchdog select **None** on the Loader Watchdog drop-down.

Enable Power Off Delay

Use this field to specify the number of minutes that the BMC subsystem will wait for the operating system to shutdown before powering off the system.

To set the power off delay timeout value, select time interval from the drop-down and click **Apply**. To disable the XClarity Controller from forcing power off, select **None** from the drop-down selection.

Trespass message

To create a message that is displayed when a user logs in to the XClarity Controller, use the information in this topic.

Select **Server Properties** under **Server Configuration**. Use the **Trespass Message** option to configure a message that you want displayed to the user. When you are finished, click **Apply**.

The message text will be displayed in the Message area of the XClarity Controller login page when a user logs in.

USB Ports Enablement

Use the information in this topic to enable or disable an USB port.

Select **USB Ports Enablement** under **Server Configuration**. Supported USB ports can be enabled or disabled on this page.

Note: For more information on configuring the XClarity Controller Front Panel USB Port to Management, see "Configuring Front Panel USB Port to Management" on page 36.

Solution service

Use the information in this topic to enable or disable solution service.

Select **Solution Service** under **Server Configuration**. Enable this setting to indicate that this server should be serviced differently from a general purpose server, and it should be treated as part of a solution or as an appliance.

Setting the XClarity Controller date and time

Use the information in this topic to understand XClarity Controller date and time settings. Instructions are provided to configure the XClarity Controller date and time. The XClarity Controller date and time is used to time stamp all events that are logged in the event log and alerts that are sent.

At the XClarity Controller home page, click the clock icon on the upper right-hand corner to view or change the XClarity Controller date and time. The XClarity Controller does not have its own real-time clock. You can configure the XClarity Controller to sync its time and date with a Network Time Protocol server or with the server's real-time clock hardware.

Syncing with NTP

Complete the following steps to synchronize the XClarity Controller clock with the NTP server:

- Select **Sync up time with NTP** and specify the NTP server address.
- Additional NTP servers can be specified by clicking the "+" icon.
- Specify how frequently you want the XClarity Controller to sync with the NTP server.
- The time obtained from the NTP server is in Coordinated Universal Time (UTC) format.
  - If you want the XClarity Controller to adjust its time and date for your local region, select the time zone offset for your locale from the drop-down menu.
  - If your location observes Daylight Saving Time, tick the **Automatically adjust for Daylight Saving Time (DST)** checkbox.
- When your configuration changes are complete, click **Apply**.

Syncing with the Host

The time kept in the server's real-time clock hardware may be in Coordinated Universal Time (UTC) format or may already have been adjusted and stored in local time format. Some operating systems store the real-time clock in UTC format while others store the time as local time. The server real-time clock does not indicate which format the time is in. Therefore when the XClarity Controller is configured to sync with the host's real-time clock, the user can choose how the XClarity Controller uses the time and date that is obtained from the real-time clock.

- Local (example: Windows): In this mode, the XClarity Controller treats the time and date that is obtained from the real-time clock as local time with any applicable time zone and DST offsets already applied. If your location observes Daylight Saving Time, you can also tick the **Automatically adjust for Daylight Saving Time (DST)** checkbox.
- UTC (example: Linux): In this mode, the XClarity Controller treats the time and date that is obtained from the real-time clock as Coordinated Universal Time, with no time zone or DST offsets already applied. In this mode, you can choose to adjust the time and date for your local region by selecting the time zone offset for your locale from the drop-down menu. If your location observes Daylight Saving Time, you can also tick the **Automatically adjust for Daylight Saving Time (DST)** checkbox.
- When your configuration changes are complete, click **Apply**.

Note: When daylight saving occurs, any actions that were scheduled for the XClarity Controller to perform during the interval when the clock jumps forward will not be performed. For example, if the US daylight start time is 2:00 am on March 12th, and a power action is scheduled for 2:10 am on March 12th, this action will not occur. Once the time reaches 2:00 am, the XClarity Controller will instead read the time as 3:00 am.

Chapter 6. Remote Console Functionality

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

You can use the remote console functionality in the XClarity Controller web interface to view and interact with the server console. You can assign a disk image (ISO or IMG file) as a virtual drive on the server. The remote console functionality is available with the XClarity Controller Premier level features and is only available through the web interface. You must log in to the XClarity Controller with a user ID that has Supervisor access or Remote Console Access privileges to use the remote console features. For more information about upgrading from XClarity Controller Standard level to XClarity Controller Premier level, see "Upgrading XClarity Controller" on page 6.

Use the remote console features to do the following:

- Remotely view video with graphic resolution up to 1920x1200 32bpp@60Hz, regardless of the server state.
- Remotely access the server using the keyboard and mouse from a remote client.
- Mount ISO and IMG files that are located on your local system or on a remote system as virtual drives that are available for use by the server.
- Upload an IMG or ISO image to the XClarity Controller memory and mount it to the server as a virtual drive. Up to two files with a maximum total size of 100 MB may be uploaded into the XClarity Controller memory.

Notes:

- When the remote console feature is started in multi-user mode, (the XClarity Controller with the XClarity Controller Premier level feature set supports up to six simultaneous sessions), the remote disk feature can be exercised by only one session at a time.
- The remote console is able to display only the video that is generated by the video controller on the system board. If a separate video controller adapter is installed and is used in place of the system's video controller, the XClarity Controller remote console cannot display the video content from the added adapter.
- If you have firewalls in your network, a network port must be opened to support the remote console feature. To view or change the network port number used by the remote console feature, see "Service Enablement and Port Assignment" on page 34.
- The remote console feature uses HTML5 for displaying the server video on web pages. To use this feature your browser must support displaying video content using HTML5 elements.
- If you are using self-signed certificates and an IPv6 address to access the BMC with the Internet Explorer browser, the remote console session may fail to start due to a certificate error. To avoid this issue, the self-signed certificate can be added to the Internet Explorer Trust Root certificate Authorities:
  - Select **Security** under **BMC Configuration** and download the self-signed certificate.
  - Change certificate file extension to *.crt and double-click the Web certificate file.
  - Clear IE11 browser cache.
  - Click **Install Certificate** to install the certificate to the Certificate Store by following the Certificate Import Wizard steps.

Enabling the remote console functionality

This topic provides information about the remote console functionality.

The XClarity Controller remote console functionality is available only in the XClarity Controller Premier level features. If you do not have the privilege to operate the remote console, you will see a lock icon.

After you have purchased and obtained the activation key for the XClarity Controller Premier level upgrade, install it using the instructions under "Installing an activation key" on page 87.

To use the remote console functionality, click the image with a white diagonally pointing arrow in the **Remote Console Preview** section of the XClarity Controller home page or the **Remote Console** web page.

Remote power control

This topic explains how to send server power and restart commands from the remote console window.

You can send server power and restart commands from the remote console window without returning to the main web page. To control the server power with the remote console, click **Power** and select one of the following commands:

Power On Server
Select this action item to power on the server and boot the operating system.

Power Off Server Normally
Select this action item to shut down the operating system and power off the server.

Power Off Server Immediately
Select this action item to power off the server without first shutting down the operating system.

Restart Server Normally
Select this action item to shut down the operating system and power cycle the server.

Restart Server Immediately
Select this action item to power cycle the server immediately without first shutting down the operating system.

Boot Server to System Setup
Select this item to power on or reboot the server and automatically boot into system setup without needing to press F1 during boot.

Remote console capture screen

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

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

Step 1. In the remote console window, click **Capture Screen**.

Step 2. In the pop-up window, click **Save File** and press **OK**. The file will be named rpviewer.png and will be saved to your default download folder.

Note: The screen capture image is saved as a JPG file type.

Remote console keyboard support

In the remote console window under **Keyboard**, the following option items are provided:

- Click **Virtual Keyboard** to launch the virtual keyboard. This feature is useful if you are using a tablet device that does not have a physical keyboard. The following options can be used to create macros and key combinations that can be sent to the server. The operating system on the client system that you are using may trap certain key combinations (for example Ctrl+Alt+Del) instead of transmitting them to the server. Other keys, such as F1 or Esc, may be intercepted by the program or browser that you are using. Macros provides a mechanism to send keystrokes to the server that the user might not be able to send.

- Click **Server Macros** to use server defined macros. Some server macros are predefined by the XClarity Controller firmware.

Remote console screen modes

Use the information in this topic to configure the remote console screen modes.

To configure the remote console screen modes, click **Screen Mode**.

The following menu options are available:

Full Screen

This mode fills the client desktop with the video display. Pressing the Esc key in this mode will exit full screen mode. Because the remote console menu is not visible in full screen mode, you will have to exit full screen mode to use any of the features provided by the remote console menu such as the keyboard macros.

Fit Screen

This is the default setting when the remote console is launched. In this setting, the target desktop is completely displayed without scroll bars. The aspect ratio is maintained.

Media mount methods

Use the information in this topic to understand how to perform media mounts.

Three mechanisms are provided to mount ISO and IMG files as virtual drives.

- Virtual drives can be added to the server from the remote console session by clicking **Media**.
- Directly from the remote console web page, without establishing a remote console session.
- Standalone tool.

Users need **Remote Console and Remote Disk Access** privileges to use the virtual media features.

Files can be mounted as virtual media from your local system or from a remote server, and can be accessed over the network or uploaded into the XClarity Controller memory using the RDOC feature. These mechanisms are described below.

- Local media are ISO or IMG files that are located on the system that you are using to access the XClarity Controller. This mechanism is only available through the remote console session, not directly from the remote console web page and is only available with the XClarity Controller Premier level features. To mount local media, click **Mount all local media** in the **Mount Local Media File** section. Up to four files can be concurrently mounted to the server.
- Files that are located on a remote system can also be mounted as virtual media. Up to four files can be concurrently mounted as virtual drives. The XClarity Controller supports the following file sharing protocols:
  - **CIFS - Common Internet File System**:
    - Enter the URL that locates the file on the remote system.
    - If you want the file to be presented to the server as read-only virtual media, tick the checkbox.

    - Enter the credentials that are needed for the XClarity Controller to access the file on the remote system.

      Note: The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space.

    - Mount options are optional and defined by the CIFS protocol.
    - If the remote server belongs to a collection of servers, where the security is centrally handled, enter the domain name to which the remote server belongs.

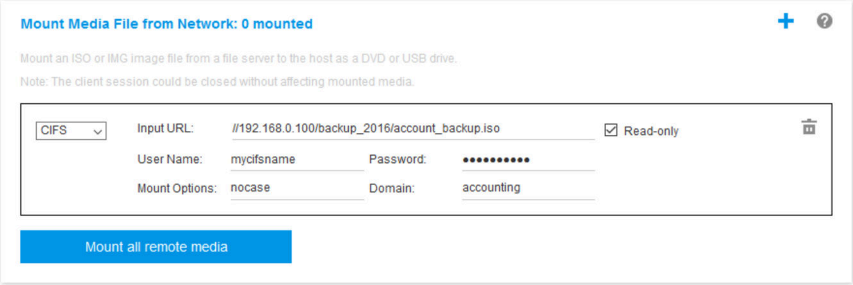
  - **NFS - Network File System**:
    - Enter the URL that locates the file on the remote system.
    - If you want the file to be presented to the server as read-only virtual media, tick the checkbox.
    - Mount options are optional and defined by the NFS protocol. Both NFSv3 and NFSv4 are supported. For example, to use NFSv3, you need to specify option 'nfsvers=3'. If the NFS server uses AUTH_SYS security flavor to authenticate NFS operations, you need to specify option 'sec=sys'.
  - **HTTPFS - HTTP Fuse-based File System**:
    - Enter the URL that locates the file on the remote system
    - If you want the file to be presented to the server as read-only virtual media, tick the checkbox.

  Note: Errors may occur during the mounting process for security certificates generated by Microsoft IIS. If this occurs, see "Media mount error issues" on page 77.

  Click **Mount all remote media** to mount the file as virtual media. To remove virtual media, click the trash can icon to the right of the mounted media.

- Up to two files can be uploaded in the XClarity Controller memory and mounted as virtual media using the XClarity Controller RDOC feature. The total size for both files must not exceed 100 MB. These files will remain in the XClarity Controller memory until they are removed, even if the remote console session has ended. The RDOC feature supports the following mechanisms when uploading the files:
  - **CIFS - Common Internet File System**: See the description above for details. **Example**:

    To mount an ISO file named account_backup.iso that is located on the backup_2016 directory of a CIFS server at the 192.168.0.100 IP address as a read-only virtual drive on the server, you would fill in the fields as shown in the figure below. In this example, the server located at 192.168.0.100 is a member of a collection of servers under the domain "accounting". The domain name is optional. If your CIFS server is not part of a domain, leave the **Domain** field blank. The CIFS "nocase" mount option is specified in the **Mount Options** field in this example indicating to the CIFS server that the uppercase/lowercase checking of the file name should be ignored. The **Mount Options** field is optional. The information entered by the user in this field is not used by the BMC and is simply passed on to the CIFS server when the mount request is made. Refer to the documentation for your CIFS server implementation to determine which options are supported by your CIFS server.



Mount Media File from Network: 0 mounted

Mount an ISO or IMG image file from a file server to the host as a DVD or USB drive.

Note: The client session could be closed without affecting mounted media.

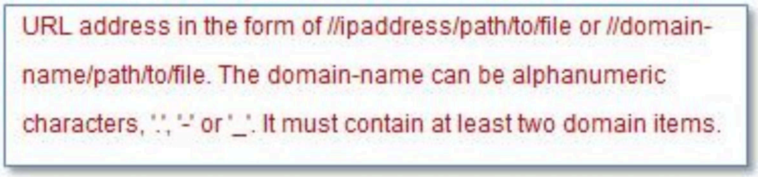
CIFS

Input URL: //192.168.0.100/backup_2016/account_backup.iso ☑ Read-only

User Name: mycifsname Password: ••••••••••

Mount Options: nocase Domain: accounting

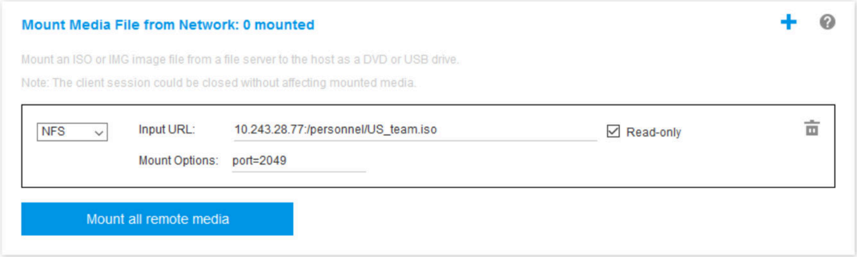
The BMC provides guidance when specifying the URL. If the URL being entered is not valid, the mount button will be greyed out and red text will be displayed under the URL field showing the expected format for the URL.



URL address in the form of //ipaddress/path/to/file or //domain-name/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items.

– **NFS - Network File System**: See the description above for details. **Example**:

To mount an ISO file named US_team.iso that is located on the “personnel” directory of an NFS server at the 10.243.28.77 IP address as a read-only virtual drive on the server, you would fill in the fields as shown in the figure below. The NFS “port=2049” mount option specifies that network port 2049 should be used to transfer the data. The **Mount Options** field is optional. The information entered by the user in this field is passed on to the NFS server when the mount request is made. Refer to the documentation for your NFS server implementation to determine which options are supported by your NFS server.



Mount Media File from Network: 0 mounted

Mount an ISO or IMG image file from a file server to the host as a DVD or USB drive.

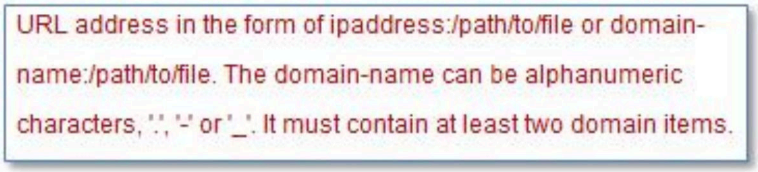
Note: The client session could be closed without affecting mounted media.

NFS

Input URL: 10.243.28.77:/personnel/US_team.iso ☑ Read-only

Mount Options: port=2049

The BMC provides guidance when specifying the URL. If the URL being entered is not valid, the mount button will be greyed out and red text will be displayed under the URL field showing the expected format for the URL.



URL address in the form of ipaddress:/path/to/file or domain-name:/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items.

– **HTTPS - Hypertext Transfer Protocol Secure**:

  – Enter the URL that locates the file on the remote system.

  – If you want the file to be presented to the server as read-only virtual media, tick the checkbox.

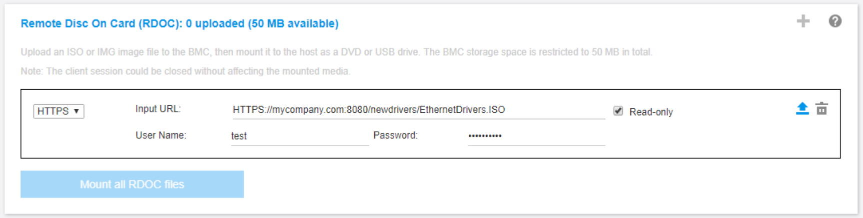
  – Enter the credentials that are needed for the XClarity Controller to access the file on the remote system.

Notes:

  – Errors may occur during the mounting process for security certificates generated by Microsoft IIS. If this occurs, see “Media mount error issues” on page 77.

  – The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space. **Example**:

To mount an ISO file named EthernetDrivers.ISO that is located on the “newdrivers” directory of a HTTPS server with the domain name “mycompany.com” using network port 8080 as a read-only virtual drive on the server, you would fill in the fields as shown in the figure below.



Remote Disc On Card (RDOC): 0 uploaded (50 MB available)

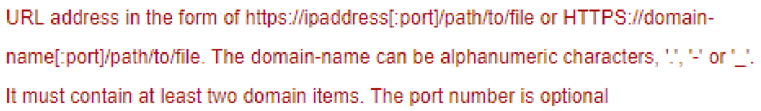
Upload an ISO or IMG image file to the BMC, then mount it to the host as a DVD or USB drive. The BMC storage space is restricted to 50 MB in total.

Note: The client session could be closed without affecting the mounted media.

HTTPS ▾ Input URL: HTTPS://mycompany.com:8080/newdrivers/EthernetDrivers.ISO ☑ Read-only

User Name: test Password: ••••••••••

The BMC provides guidance when specifying the URL. If the URL being entered is not valid, the mount button will be greyed out and red text will be displayed under the URL field showing the expected format for the URL.



URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- **SFTP - SSH File Transfer Protocol**
  - Enter the URL that locates the file on the remote system.
  - If you want the file to be presented to the server as read-only virtual media, tick the checkbox.
  - Enter the credentials that are need to for the XClarity Controller to access the file on the remote system.

  Notes:

  - The XClarity Controller does not support spaces in the user name, password, or URL. Make sure that the CIFS server does not have login credentials configured with a space in the user name or password and that the URL does not contain a space.
  - When the XClarity Controller connects to a HTTPS server, a pop-up window will appear showing information of the security certificate used by the HTTPS sever. The XClarity Controller is unable to verify the authentic of the security certificate.
- **LOCAL - Common Internet File System**:
  - Browse your system for the ISO or IMG file that you want to mount.
  - If you want the file to be presented to the server as read-only virtual media, check the checkbox.

Click **Mount all RDOC files** to mount the file as virtual media. To remove the virtual media, click the trash can icon to the right of the mounted media.

Standalone tool

For users that require mounting of the devices or images(.iso / .img) using the XClarity Controller, users can use the rdmount standalone code part of the OneCLI package. Specifically, rdmount will open a connection to XClarity Controller and will mount the device or images to the host.

rdmount has the following syntax:

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Example to mount an iso file:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

Media mount error issues

Use the information in this topic to troubleshoot media mount error issues.

When using security certificates generated by Microsoft IIS, you may encounter errors during the mounting process. If this occurs, replace the security certificate with a new one generated by openssl. Specifically, the newly generated pfx file is loaded into the Microsoft IIS server.

Below is an example showing how the new security certificate is generated via openssl in the Linux operating system.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
..........................................++++++
.......................................................++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key
```

```
$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

Exiting the remote console session

This topic explains how to end your remote console session.

To exit your remote console session, close the remote console and the virtual media session windows.

Chapter 7. Configuring the Storage

Use the information in this chapter to understand the options available for storage configurations.

When configuring the storage, following options are available:

- Storage Detail
- RAID Setup

Storage Detail

For using Storage detail function, use the information in this topic.

This function displays the storage devices' physical structure and storage configuration along with details like their location, manufacturer, product name, status, capacity, interface, media, form factor and other info.

A warning or critical event will be triggered when the SSD drive remaining life value reaches the threshold or is lower. The default remaining life value for warning and critical event is 8% and 4% respectively. Click the gear icon next to **Storage Detail** to set the threshold value.

To configure SAS/SATA/NVMe (AnyBay) backplanes that supports **PCIe lane x1** mode, click the gear icon next to **Backplane**, then select the drive bay group and click the **Apply** button to save the configuration.

RAID Setup

To perform RAID setup functions, use the information in this topic.

Use the information in this topic to view and configure storage pools, associated virtual disks and drives for the RAID adapter. If the system is powered off, power it on in order to view the RAID information.

Viewing and configuring the virtual drives

Use the information in this topic to view and configure the virtual drives.

When you select **RAID Setup** under **Server Configuration**, the **Array Configuration** tab will be chosen and the existing virtual disks will be displayed by default. The logical drives are sorted by disk arrays and controllers. Detailed information about the virtual disk, such as the virtual disk strip size and bootable information is displayed.

To configure the RAID settings, click **Enable Edit mode**.

In edit mode, you can click the controller action menu, view the current RAID virtual disks and create new RAID virtual disks.

From the Controller Actions menu, you can perform the following actions:

Clear RAID configuration

Clears all the configuration and data on the selected controller.

Import foreign drives

Import any foreign drives that were detected. A foreign drive is a drive that was moved from a different RAID configuration to the current RAID controller

Note: You will be notified if no foreign drives are detected.

Manage foreign configuration

Import any foreign drives that were detected. A foreign drive is a drive that was moved from a different RAID configuration to the current RAID controller

Note: You will be notified if no foreign drives are detected.

Information of the current RAID virtual disks for a particular controller are shown as respective "Virtual Disk Cards". Each card displays information such as the virtual disk name, status, capacity and actions. The pencil icon allows you to edit the information, and the trash can icon enables you to delete the "Virtual Disk Cards".

Note: The capacity and RAID level cannot be changed.

If you click the virtual disk name, a virtual disk properties window will appear.

Creating a new RAID virtual disk

To create a new RAID virtual disk, follow the steps shown below:

Note: If there is no remaining storage capacity, you are unable to create a new virtual disk.

1. **Select drives or a disk array which has free storage capacity**
   a. When creating a virtual disk in a new disk array, you need to specify the RAID level.

      Note: If there are not enough drives to select, and you click **Next**, an error message will appear under the RAID level field.

   b. For some RAID levels, span is required. There is also a minimum amount of drives that need to be present in the span. For these types of situations, specifiy the span number in the **Span Number** field, select **Member** or **Hot Spare** from the drop-down menu next to the drives, then tick the checkbox next to the drives that will be used to create the virtual disk.
   c. To create virtual disks in an existing disk array, you need to select a disk array that has free capacity.
2. **Creating a virtual disk**
   a. By default, creating a virtual disk will use all the storage capacity. The **Add** icon is disabled when all of the storage is used. You can click the pencil icon to change the capacity or other properties.
   b. When you edit the first virtual disk to use only some of the storage capacity, the **Add** icon will be enabled. Click the icon to show the **Add Virtual Disk** window.
   c. Click the **Remove** icon to remove a virtual disk. This icon will not be shown if there is only one virtual disk. When you click the **Remove** icon, the selected row will be immediately deleted. There will be no confirmation window as the virtual disk has not been created yet.
   d. Click **Start Creating** to start the process.

Note: When the controller is not supported, a message will appear.

Viewing and configuring the storage inventory

Use the information in this topic to view and configure the storage inventory.

Under the **Storage Inventory** tab, you can view and configure disk arrays, associated virtual drives and drives for the RAID controller.

- **For storage devices that support RAID configuration**:
  1. If the controller includes configured disk arrays, it will display the installed drives based on the disk array. The following describes the items that appear in the window.

- **Table title**: Shows the disk array ID, RAID level and the total number of drives.
- **Table content**: Lists basic properties such as drive name, drive state, type, product, manufacturer, serial number, and actions. You can go to the **Inventory** page to view all the properties that the XClarity Controller can detect.
- **Actions**: The following shows the action items that can be performed. Some actions will not be available when the drive is in a different state.
  - **Assign hot spare**: Specifies the drive as global hot spare or a dedicated hot spare.
  - **Remove hot spare**: Removes the drive from the hot spare.
  - **Make disk drive offline**: Sets the drive to offline.
  - **Make disk drive online**: Sets the drive to online.
  - **Start Rebuild**: Rebuild the RAID.
  - **Make disk drive as reusable**: Sets the drive to reusable.
  - **Make disk drive as missing**: Sets the drive as missing.
  - **Make drive good to JBOD**: Adds drive to JBOD disk arrangement.
  - **Make drive unconfigured good**: Makes the drive available to be configured into an array, or for use as an emergency hot spare.
  - **Make drive unconfigured bad**: Marks the drive bad, preventing it from being used in an array or as an emergency hot spare.
  - **Make disk drive as prepare for removal**: Sets the drive for removal.

2. If the controller includes drives that have not yet been configured, they will be displayed in the **Non-RAID disk drives** table. By clicking the **Convert JBOD to Ready to Configure** option, a window will appear showing all the drives that support this action item. You can select one or more drives to convert.

For storage devices that do not support RAID configuration: The XClarity Controller may not be able to detect the properties of some drives.

Chapter 8. Updating Server Firmware

To update server firmware, use information in this topic.

Firmware update overview

General Information about updating server firmware.

By clicking **Firmware Update** in the left pane, an overview of the firmware information is provided.

- **Update from Repository:** Sync server firmware with remote CIFS/NFS repository for batch update, see "Update From Repository" on page 84.
- **System Firmware:** Overview of system firmware status, version, and system firmware update.

  Note: Click **Auto Sync** to enable or disable **Auto Promote Primary BMC to Backup**. When this setting is enabled, the pending backup bank firmware will be synced from the primary bank after the primary bank passes the Image Stability Metric (ISM) measurement.
- **Adapter Firmware:** Overview of adapter firmware installed, status, version, and adapter firmware update.
- **Power Supply Unit Firmware:** Overview of power supply unit firmware version, and PSU firmware update.
- **Drive Backplane PSoc Firmware:** Overview of backplane firmware version. And to perform system firmware update.

The current status and firmware versions for the BMC, UEFI, LXPM, LXPM drivers, embedded OS, FPGA, and adapters are displayed, including the BMC primary and backup versions. There are three categories for the firmware status:

- **Active:** The firmware is active.
- **Inactive:** The firmware is not active.
- **Pending restart:** The firmware image has been updated and will become effective after the server of the BMC is restarted.
- **N/A:** No firmware has been installed for this component.

Attention:

- XCC and IMM must be updated to the latest version before updating UEFI. Updating in different order may result in incorrect behavior.
- Installing the wrong firmware update might cause the server to malfunction. Before you install a firmware or device-driver update, read any readme and change history files that are provided with the downloaded update. These files contain important information about the update and the procedure for installing the update, including any special procedure for updating from an early firmware or device-driver version to the latest version. As the web browser may contain XCC cache data, it is recommended to reload the web page after the XCC firmware has been upgraded.
- With the exception of SATA M.2 adapter, AMD processor servers do not support out-of-band adapter firmware update.
- Some firmware updates require system restarting, which performs firmware activation or internal update. This process in system booting is called "system maintenance mode", that does not allow user power actions temporarily. The mode is also enabled during firmware update. User shall not disconnect AC power when the system enters maintenance mode.

System, Adapter and PSU Firmware Update

Steps to update System firmware, Adapter firmware and PSU firmware.

To manually apply update for **System Firmware**, **Adapter Firmware** and **PSU Firmware**, complete the following steps:

1. Click **Update Firmware** within each feature. The Update Server Firmware window opens.
2. Click **Browse...** to select the firmware update file that you want to use.
3. Navigate to the file you want to select and click **Open**. You are returned to the Update Server Firmware window with the selected file displayed.
4. Click **Next** to begin the upload and verify process on the selected file. A progress meter will be displayed as the file is being uploaded and verified. You can view this status window to verify that the file you selected to update is the correct file. For **System Firmware**, the status window will have information regarding the type of firmware file that is to be updated such as BMC, UEFI, or LXPM. After the firmware file is uploaded and verified successfully, click **Next** to select the device you want to update.
5. Click **Update** to begin the firmware update. A progress meter shows the progress of the update. When the firmware update is completed successfully, click **Finish**. If the update requires the XClarity Controller to be restarted in order to take effect, a warning message will be displayed. For details on how to restart the XClarity Controller, see "Power actions" on page 62.

Update From Repository

Update server firmware from a remote repository

Overview

Notes:

- CIFS/NFS/HTTPS/Onboard Firmware History functionality requires XCC Premier license.
- If the machine is not in idle state, or if the file upload, download, or unzip is not completed, the update from repository function will be temporary disabled.

XCC has introduced updating firmware on a server using the Update Bundles (Service Packs) package. This feature simplifies the process by using a single API or Redfish client tool to update all firmware in the system, including both OOB and IB firmware packages. The process involves identifying applicable firmware packages, downloading and extracting them from a remote HTTP/HTTPS server or uploading them to BMC internal storage via a web browser, or mounting them from a CIFS or NFS shared directory.

The metadata (JSON format) files need to be placed in the root directory of the network shared file system if using CIFS or NFS mount, with firmware payloads specified in the metadata. The server's microSD device can store historical repositories, allowing users to roll back firmware levels.

If the firmware packages contain any payloads that do not support out-of-band firmware update, the BMC will start the server and configure it to boot from the embedded OS image installed in BMC before performing the update.

Update Bundle and metadata

The Update Bundle (Service Packs) is a compressed file of a firmware bundle. It contains one or multiple firmware packages for the components in a system. XCC's Update from Repository feature consumes the Update Bundle file. The unzipped bundle file contains metadata and payload binaries. JSON metadata files provide information to XCC about the kind of firmware images the bundle file contains, and payload binaries provide the firmware images.

Firmware repository inside XCC

The Update Bundle can contain multiple firmware packages, and XCC reserves 2GB of space in its flash for new features. When a new bundle is received, XCC cleans up old data. Some platforms use a MicroSD card to provide additional storage, and XCC moves the last Updated Bundle to the SD card's historic repository. The firmware history repository can store up to three bundles, and users can use the Firmware Rollback feature to revert to a previous bundle.

Notes:

- If the Update Bundle only includes the OOB firmware package available to the system, XCC does not change the system power state. To update PCI device firmware, it requires the system to be powered on.
- If the Update Bundle includes the IB firmware package available to the system, XCC stores the system power state before updating and restore the power state after the Update Bundle is updated. During the update process, XCC reboots the host into the embedded OS.
- If the Update Bundle includes a prerequisite level of UEFI firmware and the current installed UEFI version does not meet or is behind that level, XCC powers off the system to perform a UEFI firmware update first.
- If the Update Bundle includes a prerequisite level of XCC firmware and the current installed XCC version does not meet or is behind that level, XCC reboots first after upgrading itself.

Update with WebGUI

With **Update from Repository**, user can configure XCC to sync server firmware with a remote CIFS/NFS/HTTP/HTTPS firmware repository, or use the Internal Storage or Onboard Firmware History. The firmware repository should contain packages including binary and metadata files, or Update Bundle metadata JSON and corresponding binary files. XCC parses the metadata JSON files to pick out firmware packages that support OOB update for this specific system hardware then starts a batch update.

To update from repository, complete the following steps:

1. When using Internal Storage, click **Import Firmware Package** and browse for the firmware package (. tgz or zip format).
2. When using HTTP or HTTPS, enter the firmware package URL.
3. When using CIFS or NFS, enter the remote repository information and click **Mount**.
   - Example of a CIFS remote share: (use forward slash instead of backslash)
     `//fileserver.mycompany.com/repository`
   - Example of a NFS remote share: (hostname or IP address are both valid)
     `192.168.100.120:/home/user1/repository`
4. Click **Update System** to start the batch update.

   Note: When using HTTPS mode, the certificate information will be displayed first.
5. Click **View Details** to see updating status.
   - **Green check mark** ✅ **:** The firmware’s upgrade has finished successfully.
   - **Red X mark** ❌ **:** The firmware’s upgrade has failed.
   - **Updating:** The firmware is undergoing the process of upgrading.
   - **Cancel:** The firmware’s upgrade is cancelled.
   - **Waiting:** The firmware’s upgrade is waiting to be deployed.

   Note: Click **Stop Updating** will cancel the updates in queue after the current installation package update is complete.
6. When using CIFS or NFS, click **Unmount** to disconnect from the remote repository.

7. If the update requires the XClarity Controller to be restarted in order to take effect, a warning message will be displayed. For details on how to restart the XClarity Controller, see “Power actions” on page 62.

Note: If the system has MicroSD card installed, you can see the update history of the Update Bundle and select the index of the Update Bundle to perform firmware rollback. The process is similar to updating from repository, except the historical Update Bundle is placed inside MicroSD.

Chapter 9. License Management

The Lenovo XClarity Controller License Management allows you to install and manage optional server and systems management features.

There are multiple levels of XClarity Controller firmware functionality and features available for your server. The level of the firmware features installed on your server vary based on hardware type.

You can upgrade the XClarity Controller functionality by purchasing and installing an activation key.

To order an activation key, contact your sales representative or business partner.

Use the XClarity Controller web interface or the XClarity Controller CLI to manually install an activation key that lets you use an optional feature you have purchased. Before activating a key:

- The activation key must be on the system that you are using to login to the XClarity Controller.
- You must have ordered the license key and received its authorization code via mail or e-mail.

See "Installing an activation key" on page 87, "Removing an activation key" on page 87 or "Exporting an activation key" on page 88 for information about managing an activation key using the XClarity Controller web interface. See "keycfg command" on page 136 for information about managing an activation key using the XClarity Controller CLI.

To register an ID in administering your XClarity Controller license, click the following link: https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome

Additional information about license management for Lenovo servers is available at the following **Lenovo Press** website:

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

Installing an activation key

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

To install an activation key, complete the following steps:

Step 1. Click **License** under **BMC Configuration**.

Step 2. Click **Upgrade License**.

Step 3. In the **Add a new license** window, click **Browse**; then, select the activation key file to add in the File Upload window and click **Open** to add the file. To finish adding the key, click **Import** in the Add Activation Key window.

Note: If the activation key is not valid, an error window will appear.

Removing an activation key

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

To remove a activation key, complete the following steps:

Step 1. Click **License** under **BMC Configuration**.

Step 2. Select the activation key to remove; then, click **Delete**.

Step 3. In the Confirm Activation Key Deletion window, click **OK** to confirm activation key deletion. The selected activation key will be removed from the server and no longer appears in the License Management page.

Exporting an activation key

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

To export an activation key, complete the following steps:

Step 1. Click **License** under **BMC Configuration**.

Step 2. From the License Management page, select the activation key to export; then, click **Export**.

Step 3. In the **Export the selected license** window, click **Export** to confirm activation key exporting request.

Step 4. Select the directory to save the file. The selected activation key will be exported from the server.

Chapter 10. Lenovo XClarity Controller Redfish REST API

The Lenovo XClarity Controller provides a Redfish compliant set of easy-to-use REST APIs that can be used to access Lenovo XClarity Controller data and services from applications running outside of the Lenovo XClarity Controller framework.

This allows for easy integration of Lenovo XClarity Controller capabilities into other software, whether the software is running on the same system as the Lenovo XClarity Controller server, or on a remote system within the same network. These APIs are based on the industry standard Redfish REST API and are accessed via the HTTPS protocol.

The XClarity Controller Redfish REST API user guide can be found here: https://pubs.lenovo.com/xcc3-restapi/xcc3_restapi_book.pdf.

Lenovo provides open source sample Redfish scripts that can be used as reference for developing software that communicates with Lenovo Redfish REST API. These sample scripts can be found here:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

DMTF specifications related to the Redfish API are available at: https://redfish.dmtf.org/. This website provides general specifications and other reference material on the Redfish REST API.

Chapter 11. Command-line interface

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

XClarity Controller command line interface (CLI)

Use the XClarity Controller command line interface (CLI) to access the XClarity Controller 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 **SSH session**. You **must** be authenticated by the XClarity Controller before you can issue any CLI commands.

Lenovo XClarity Essentials OneCLI

Lenovo XClarity Essentials OneCLI is a collection of several command-line applications, which can be used to configure the server, collect service data for the server, update firmware and device drivers, and perform power-management functions on the server. For more information on using Lenovo XClarity Essentials OneCLI, see https://pubs.lenovo.com/lxce-onecli/.

Note: The format of UEFI and BMC settings have been changed in XCC3. For more information on the BMC setting names mapping between XCC3 and XCC2/XCC, see "Setting names in XClarity Controller 3" on page 91.

Setting names in XClarity Controller 3

This section describes the setting names in XClarity Controller 3.

The format of UEFI and BMC settings have been changed in XCC3 to adopt OpenBMC and aiming for full Redfish alignment. **UpdateXpress 5.x**, **BOMC 14.x**, and **XClarity Essentials OneCLI 5.x** must be used to read and configure UEFI and BMC settings.

- The command parameter is the same as previous versions of OneCLI, but the setting names have been changed from legacy `IMM.xyz` style to reflect new Redfish style.
- For example:
  - On ThinkSystem V1/V2/V3:
    - `onecli config set Processors.TurboMode Enabled`
    - `onecli config set IMM.SSLPort 443`
  - ThinkSystem V4:
    - `onecli config set UEFI.Processors_TurboMode Enabled`
    - `onecli config set BMC.HTTPSPort 443`
- This is applicable to all ThinkSystem V4 servers with Intel and AMD processors with XCC3.
- To run one batch configuration command for servers of multiple generations, there is a `-c` feature for backward compatibility so that the existing configuration file can be retained across servers.
  - OneCLI 5.x will translate the old format settings to the new format when applying to a ThinkSystem V4 server, but compatibility mode does not cover all settings, only partial support.
  - The settings that are not translated by compatibility mode will cause error 104 at runtime. Testing is advised.

The table below illustrates the mapping between setting names of XCC3 and XCC2/XCC.

Table 4. BMC setting names mapping

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.HTTPSPort	IMM.SSLPort
BMC.RemotePresenceEnabled	IMM.RemotePresencePortControl
BMC.RemoteConsolePort	IMM.RemoteConsolePort
BMC.SSHEnabled	IMM.SSHLegacyPortControl IMM.SSH_Enable
BMC.SSHPort	IMM.SSHPort
BMC.SSDPEnabled	IMM.SSDPPortControl
BMC.SecurityModeLevel	IMM.Security_Mode
BMC.TLSLevel	IMM.TLSLevel
BMC.HTTPSEnabled	IMM.HttpsPortControl IMM.SSL_Server_Enable
BMC.TPMTCMPolicy	IMM.TpmTcmPolicy
BMC.TPMTCMPolicyLock	IMM.TpmTcmPolicyLock
BMC.UEFIMemoryTest	IMM.UEFIMemoryTest
BMC.UEFIMemoryTestPolicy	IMM.UEFIMemoryTestPolicy
BMC.UEFIDebugLevel	IMM.UEFIDebugLevel
BMC.SMTPServerHostName	IMM.SMTP_ServerName
BMC.SMTPUserPassword	IMM.SMTP_Password
BMC.SMTPPort	IMM.SMTP_Port
BMC.SMTPAuthEnabled	IMM.SMTP_Authentication
BMC.SMTPUserName	IMM.SMTP_UserName
BMC.SMTPAuthMethod	IMM.SMTP_AuthMethod
BMC.SMTPReversePath	IMM.SMTP_ReversePath
BMC.FanBoost	IMM.FanSpeedPolicies
BMC.PowerRedundancyMode	IMM.PSUOversubscriptionMode
BMC.PowerZeroOutputEnabled	IMM.ZeroOutput
BMC.PowerRestorePolicy	IMM.PowerRestorePolicy
BMC.ServerConfigSystemName	IMM.IMMInfo_Name
BMC.ServerConfigBuilding	IMM.IMMInfo_Location
BMC.ServerConfigContact	IMM.IMMInfo_Contact
BMC.ServerConfigRackName	IMM.IMMInfo_RackId
BMC.ServerConfigRoomNo	IMM.IMMInfo_RoomId
BMC.ServerConfigAddress	IMM.IMMInfo_FullPostalAddress

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.ServerConfigLowestU	IMM.IMMInfo_Lowest_U
BMC.ServerConfigHeightU	IMM.IMMInfo_Height
BMC.ServerConfigBladeBay	IMM.IMMInfo_BladeBay
BMC.AutoROMPromotionEnabled	IMM.AutoROMPromotion
BMC.BackupAutoPromoteEnabled	IMM.backupautopromote
BMC.SSDWearWarningThreshold	IMM.SSDWearThreshold
BMC.SSDWearCriticalThreshold	IMM.SSDWearThreshold
BMC.PCIeResetFlowCtrl	IMM.PCIeResetFlowCtrl
BMC.ComplexPassword	IMM.ComplexPassword
BMC.PasswordChangeOnFirstAccess	IMM.FirstAccessPwChange
BMC.MinimumPasswordChangeIntervalHours	IMM.PwChangeInterval
BMC.AccountLockoutDurationSeconds	IMM.LockoutPeriod
BMC.AccountLockoutThreshold	IMM.PwMaxFailure
BMC.MinimumPasswordLength	IMM.MinPasswordLen
BMC.MinimumPasswordReuseCycle	IMM.PasswordReuse
BMC.IPLockoutThreshold	IMM.IPMaxLoginFail
BMC.IPLockoutDurationMinutes	IMM.IPLockoutPeriod
BMC.WebUISessionTimeoutMinutes	IMM.WebTimeout
BMC.ThirdPartyPasswordEnabled	IMM.ThirdPartyPasswordEnable
BMC.ThirdPartyPasswordReadable	IMM.ThirdPartyPasswordReadable
BMC.AuthMode	IMM.User_Authentication_Method
BMC.LoginID_1	IMM.LoginId.1
BMC.LoginID_2	IMM.LoginId.2
BMC.LoginID_3	IMM.LoginId.3
BMC.LoginID_4	IMM.LoginId.4
BMC.LoginID_5	IMM.LoginId.5
BMC.LoginID_6	IMM.LoginId.6
BMC.LoginID_7	IMM.LoginId.7
BMC.LoginID_8	IMM.LoginId.8
BMC.LoginID_9	IMM.LoginId.9
BMC.LoginID_10	IMM.LoginId.10
BMC.LoginID_11	IMM.LoginId.11
BMC.LoginID_12	IMM.LoginId.12
BMC.AccessibleInterfaces_1	IMM.Accessible_Interfaces.1
BMC.AccessibleInterfaces_2	IMM.Accessible_Interfaces.2

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.AccessibleInterfaces_3	IMM.Accessible_Interfaces.3
BMC.AccessibleInterfaces_4	IMM.Accessible_Interfaces.4
BMC.AccessibleInterfaces_5	IMM.Accessible_Interfaces.5
BMC.AccessibleInterfaces_6	IMM.Accessible_Interfaces.6
BMC.AccessibleInterfaces_7	IMM.Accessible_Interfaces.7
BMC.AccessibleInterfaces_8	IMM.Accessible_Interfaces.8
BMC.AccessibleInterfaces_9	IMM.Accessible_Interfaces.9
BMC.AccessibleInterfaces_10	IMM.Accessible_Interfaces.10
BMC.AccessibleInterfaces_11	IMM.Accessible_Interfaces.11
BMC.AccessibleInterfaces_12	IMM.Accessible_Interfaces.12
BMC.AuthorityLevel_1	IMM.LoginRole.1
BMC.AuthorityLevel_2	IMM.LoginRole.2
BMC.AuthorityLevel_3	IMM.LoginRole.3
BMC.AuthorityLevel_4	IMM.LoginRole.4
BMC.AuthorityLevel_5	IMM.LoginRole.5
BMC.AuthorityLevel_6	IMM.LoginRole.6
BMC.AuthorityLevel_7	IMM.LoginRole.7
BMC.AuthorityLevel_8	IMM.LoginRole.8
BMC.AuthorityLevel_9	IMM.LoginRole.9
BMC.AuthorityLevel_10	IMM.LoginRole.10
BMC.AuthorityLevel_11	IMM.LoginRole.11
BMC.AuthorityLevel_12	IMM.LoginRole.12
BMC.Password_1	IMM.Password.1
BMC.Password_2	IMM.Password.2
BMC.Password_3	IMM.Password.3
BMC.Password_4	IMM.Password.4
BMC.Password_5	IMM.Password.5
BMC.Password_6	IMM.Password.6
BMC.Password_7	IMM.Password.7
BMC.Password_8	IMM.Password.8
BMC.Password_9	IMM.Password.9
BMC.Password_10	IMM.Password.10
BMC.Password_11	IMM.Password.11
BMC.Password_12	IMM.Password.12
BMC.Hash256PasswordSalt_1	IMM.SHA256PasswordSalt.1

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.Hash256PasswordSalt_2	IMM.SHA256PasswordSalt.2
BMC.Hash256PasswordSalt_3	IMM.SHA256PasswordSalt.3
BMC.Hash256PasswordSalt_4	IMM.SHA256PasswordSalt.4
BMC.Hash256PasswordSalt_5	IMM.SHA256PasswordSalt.5
BMC.Hash256PasswordSalt_6	IMM.SHA256PasswordSalt.6
BMC.Hash256PasswordSalt_7	IMM.SHA256PasswordSalt.7
BMC.Hash256PasswordSalt_8	IMM.SHA256PasswordSalt.8
BMC.Hash256PasswordSalt_9	IMM.SHA256PasswordSalt.9
BMC.Hash256PasswordSalt_10	IMM.SHA256PasswordSalt.10
BMC.Hash256PasswordSalt_11	IMM.SHA256PasswordSalt.11
BMC.Hash256PasswordSalt_12	IMM.SHA256PasswordSalt.12
BMC.Hash256Password_1	IMM.SHA256Password.1
BMC.Hash256Password_2	IMM.SHA256Password.2
BMC.Hash256Password_3	IMM.SHA256Password.3
BMC.Hash256Password_4	IMM.SHA256Password.4
BMC.Hash256Password_5	IMM.SHA256Password.5
BMC.Hash256Password_6	IMM.SHA256Password.6
BMC.Hash256Password_7	IMM.SHA256Password.7
BMC.Hash256Password_8	IMM.SHA256Password.8
BMC.Hash256Password_9	IMM.SHA256Password.9
BMC.Hash256Password_10	IMM.SHA256Password.10
BMC.Hash256Password_11	IMM.SHA256Password.11
BMC.Hash256Password_12	IMM.SHA256Password.12
BMC.RoleName_1	IMM.AuthorityRoleName.1
BMC.RoleName_2	IMM.AuthorityRoleName.2
BMC.RoleName_3	IMM.AuthorityRoleName.3
BMC.RoleName_4	IMM.AuthorityRoleName.4
BMC.RoleName_5	IMM.AuthorityRoleName.5
BMC.RoleName_6	IMM.AuthorityRoleName.6
BMC.RoleName_7	IMM.AuthorityRoleName.7
BMC.RoleName_8	IMM.AuthorityRoleName.8
BMC.RoleName_9	IMM.AuthorityRoleName.9
BMC.RoleName_10	IMM.AuthorityRoleName.10
BMC.RoleName_11	IMM.AuthorityRoleName.11
BMC.RoleName_12	IMM.AuthorityRoleName.12

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.RoleName_13	IMM.AuthorityRoleName.13
BMC.RoleName_14	IMM.AuthorityRoleName.14
BMC.RoleName_15	IMM.AuthorityRoleName.15
BMC.RoleName_16	IMM.AuthorityRoleName.16
BMC.RoleName_17	IMM.AuthorityRoleName.17
BMC.RoleName_18	IMM.AuthorityRoleName.18
BMC.RoleName_19	IMM.AuthorityRoleName.19
BMC.RoleName_20	IMM.AuthorityRoleName.20
BMC.RoleName_21	IMM.AuthorityRoleName.21
BMC.RoleName_22	IMM.AuthorityRoleName.22
BMC.RoleName_23	IMM.AuthorityRoleName.23
BMC.RoleName_24	IMM.AuthorityRoleName.24
BMC.RoleName_25	IMM.AuthorityRoleName.25
BMC.RoleName_26	IMM.AuthorityRoleName.26
BMC.RoleName_27	IMM.AuthorityRoleName.27
BMC.RoleName_28	IMM.AuthorityRoleName.28
BMC.RoleName_29	IMM.AuthorityRoleName.29
BMC.RoleName_30	IMM.AuthorityRoleName.30
BMC.RoleName_31	IMM.AuthorityRoleName.31
BMC.RoleName_32	IMM.AuthorityRoleName.32
BMC.RolePrivileges_1	IMM.AuthorityRolePriv.1
BMC.RolePrivileges_2	IMM.AuthorityRolePriv.2
BMC.RolePrivileges_3	IMM.AuthorityRolePriv.3
BMC.RolePrivileges_4	IMM.AuthorityRolePriv.4
BMC.RolePrivileges_5	IMM.AuthorityRolePriv.5
BMC.RolePrivileges_6	IMM.AuthorityRolePriv.6
BMC.RolePrivileges_7	IMM.AuthorityRolePriv.7
BMC.RolePrivileges_8	IMM.AuthorityRolePriv.8
BMC.RolePrivileges_9	IMM.AuthorityRolePriv.9
BMC.RolePrivileges_10	IMM.AuthorityRolePriv.10
BMC.RolePrivileges_11	IMM.AuthorityRolePriv.11
BMC.RolePrivileges_12	IMM.AuthorityRolePriv.12
BMC.RolePrivileges_13	IMM.AuthorityRolePriv.13
BMC.RolePrivileges_14	IMM.AuthorityRolePriv.14

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.RolePrivileges_15	IMM.AuthorityRolePriv.15
BMC.RolePrivileges_16	IMM.AuthorityRolePriv.16
BMC.RolePrivileges_17	IMM.AuthorityRolePriv.17
BMC.RolePrivileges_18	IMM.AuthorityRolePriv.18
BMC.RolePrivileges_19	IMM.AuthorityRolePriv.19
BMC.RolePrivileges_20	IMM.AuthorityRolePriv.20
BMC.RolePrivileges_21	IMM.AuthorityRolePriv.21
BMC.RolePrivileges_22	IMM.AuthorityRolePriv.22
BMC.RolePrivileges_23	IMM.AuthorityRolePriv.23
BMC.RolePrivileges_24	IMM.AuthorityRolePriv.24
BMC.RolePrivileges_25	IMM.AuthorityRolePriv.25
BMC.RolePrivileges_26	IMM.AuthorityRolePriv.26
BMC.RolePrivileges_27	IMM.AuthorityRolePriv.27
BMC.RolePrivileges_28	IMM.AuthorityRolePriv.28
BMC.RolePrivileges_29	IMM.AuthorityRolePriv.29
BMC.RolePrivileges_30	IMM.AuthorityRolePriv.30
BMC.RolePrivileges_31	IMM.AuthorityRolePriv.31
BMC.RolePrivileges_32	IMM.AuthorityRolePriv.32
BMC.PasswordExpirationPeriodDays	IMM.PasswordAge
BMC.PasswordExpirationWarningPeriodDays	IMM.PwExpWarningPeriod
BMC.LDAPLocalAuthorizationEnabled	IMM.AuthorizationMethod
BMC.LDAPBindingMethod	IMM.BindingMethod
BMC.LDAPClientDN	IMM.ClientDN
BMC.LDAPClientPassword	IMM.Client_Password
BMC.LDAPForestName	IMM.Forest_Name
BMC.LDAPServerSearchMethod	IMM.Select_LDAP_Servers
BMC.LDAPGroupFilter	IMM.GroupFilter
BMC.LDAPGroupSearchAttribute	IMM.Group_Search_Attribute
BMC.LDAPLoginPermissionAttribute	IMM.Login_Permission_Attribute
BMC.LDAPRootDN	IMM.Root_DN
BMC.LDAPUserSearchAttribute	IMM.UID_Search
BMC.LDAPSearchDomain	IMM.Search_Domain
BMC.LDAPSecureEnabled	IMM.SSL_Client_Enable
BMC.LDAPGroupDomain_1	IMM.GRP_GroupDomain.1

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.LDAPGroupDomain_2	IMM.GRP_GroupDomain.2
BMC.LDAPGroupDomain_3	IMM.GRP_GroupDomain.3
BMC.LDAPGroupDomain_4	IMM.GRP_GroupDomain.4
BMC.LDAPGroupDomain_5	IMM.GRP_GroupDomain.5
BMC.LDAPGroupDomain_6	IMM.GRP_GroupDomain.6
BMC.LDAPGroupDomain_7	IMM.GRP_GroupDomain.7
BMC.LDAPGroupDomain_8	IMM.GRP_GroupDomain.8
BMC.LDAPGroupDomain_9	IMM.GRP_GroupDomain.9
BMC.LDAPGroupDomain_10	IMM.GRP_GroupDomain.10
BMC.LDAPGroupDomain_11	IMM.GRP_GroupDomain.11
BMC.LDAPGroupDomain_12	IMM.GRP_GroupDomain.12
BMC.LDAPGroupDomain_13	IMM.GRP_GroupDomain.13
BMC.LDAPGroupDomain_14	IMM.GRP_GroupDomain.14
BMC.LDAPGroupDomain_15	IMM.GRP_GroupDomain.15
BMC.LDAPGroupDomain_16	IMM.GRP_GroupDomain.16
BMC.LDAPGroupName_1	IMM.GRP_GroupName.1
BMC.LDAPGroupName_2	IMM.GRP_GroupName.2
BMC.LDAPGroupName_3	IMM.GRP_GroupName.3
BMC.LDAPGroupName_4	IMM.GRP_GroupName.4
BMC.LDAPGroupName_5	IMM.GRP_GroupName.5
BMC.LDAPGroupName_6	IMM.GRP_GroupName.6
BMC.LDAPGroupName_7	IMM.GRP_GroupName.7
BMC.LDAPGroupName_8	IMM.GRP_GroupName.8
BMC.LDAPGroupName_9	IMM.GRP_GroupName.9
BMC.LDAPGroupName_10	IMM.GRP_GroupName.10
BMC.LDAPGroupName_11	IMM.GRP_GroupName.11
BMC.LDAPGroupName_12	IMM.GRP_GroupName.12
BMC.LDAPGroupName_13	IMM.GRP_GroupName.13
BMC.LDAPGroupName_14	IMM.GRP_GroupName.14
BMC.LDAPGroupName_15	IMM.GRP_GroupName.15
BMC.LDAPGroupName_16	IMM.GRP_GroupName.16
BMC.LDAPGroupRole_1	IMM.GRP_GroupRole.1
BMC.LDAPGroupRole_2	IMM.GRP_GroupRole.2
BMC.LDAPGroupRole_3	IMM.GRP_GroupRole.3

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.LDAPGroupRole_4	IMM.GRP_GroupRole.4
BMC.LDAPGroupRole_5	IMM.GRP_GroupRole.5
BMC.LDAPGroupRole_6	IMM.GRP_GroupRole.6
BMC.LDAPGroupRole_7	IMM.GRP_GroupRole.7
BMC.LDAPGroupRole_8	IMM.GRP_GroupRole.8
BMC.LDAPGroupRole_9	IMM.GRP_GroupRole.9
BMC.LDAPGroupRole_10	IMM.GRP_GroupRole.10
BMC.LDAPGroupRole_11	IMM.GRP_GroupRole.11
BMC.LDAPGroupRole_12	IMM.GRP_GroupRole.12
BMC.LDAPGroupRole_13	IMM.GRP_GroupRole.13
BMC.LDAPGroupRole_14	IMM.GRP_GroupRole.14
BMC.LDAPGroupRole_15	IMM.GRP_GroupRole.15
BMC.LDAPGroupRole_16	IMM.GRP_GroupRole.16
BMC.LDAPServerHostName_1	IMM.LDAP_Server1_HostName_IPAddress
BMC.LDAPServerHostName_2	IMM.LDAP_Server2_HostName_IPAddress
BMC.LDAPServerHostName_3	IMM.LDAP_Server3_HostName_IPAddress
BMC.LDAPServerHostName_4	IMM.LDAP_Server4_HostName_IPAddress
BMC.LDAPServerPort_1	IMM.LDAP_Server1_Port
BMC.LDAPServerPort_2	IMM.LDAP_Server2_Port
BMC.LDAPServerPort_3	IMM.LDAP_Server3_Port
BMC.LDAPServerPort_4	IMM.LDAP_Server4_Port
BMC.Eth1Enabled	IMM.Network2
BMC.Eth1IPv4Enabled	IMM.Network2
BMC.Eth1IPv4ConfigMode	IMM.DHCP2
BMC.Eth1IPv6Enabled	IMM.IPv6Network2
BMC.Eth1IPv6StaticEnabled	IMM.IPv6Static2
BMC.Eth1LinkAutoNegEnabled	IMM.AutoNegotiate2
BMC.Eth1LinkFullDuplexEnabled	IMM.Duplex2
BMC.Eth1LinkSpeed	IMM.LANDataRate2
BMC.Eth1StaticDomainName	IMM.Custom_Domain
BMC.Eth1DHCPDNSEnabled	IMM.DNS_Enable
BMC.Eth1IPv4DefaultGateway	IMM.GatewayIPAddress2 IMM.DHCPAssignedGateway2
BMC.Eth1IPv6DefaultGateway	IMM.IPv6GatewayIPAddress2

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.Eth1IPv6AcceptRAEnabled	IMM.IPv6Stateless2
BMC.Eth1MTU	IMM.MTU2
BMC.Eth1StaticIPv4Address	IMM.HostIPAddress2
BMC.Eth1StaticIPv4Subnet	IMM.HostIPSubnet2
BMC.Eth1StaticIPv6AddressWithPrefix	IMM.IPv6HostIPAddressWithPrefix2
BMC.Eth1MACAddress	IMM.MACAddress2
BMC.Eth1DHCPAssignedIP	IMM.DHCPAssignedHostIP2
BMC.Eth1DHCPAssignedSubnet	IMM.DHCPAssignedNetMask2
BMC.Eth1DHCPAssignedIPv4DNSServer_1	IMM.DHCPAssignedPrimaryDNS2
BMC.Eth1DHCPAssignedIPv4DNSServer_2	IMM.DHCPAssignedSecondaryDNS2
BMC.Eth1DHCPAssignedIPv4DNSServer_3	IMM.DHCPAssignedTertiaryDNS2
BMC.Eth1IPv6DHCPEnabled	IMM.IPv6DHCP2
BMC.Eth1IPv6LinkLocalIP	IMM.IPv6LinkLocalIPAddress2
BMC.Eth1IPv6DHCPAssignedIP	IMM.IPv6DHCPAssignedHostIP2
BMC.Eth1BurnedInMACAddress	IMM.BurnedInMacAddress2
BMC.StaticHostName	IMM.HostName1
BMC.LXCADNSDiscoveryEnabled	IMM.LXCADNSDiscovery
BMC.Eth0DDNSEnabled	IMM.DDNS_Enable
BMC.Eth0Enabled	IMM.Network1
BMC.Eth0IPv4Enabled	IMM.Network1
BMC.Eth0IPv4ConfigMode	IMM.DHCP1
BMC.Eth0IPv6Enabled	IMM.IPv6Network1
BMC.Eth0IPv6StaticEnabled	IMM.IPv6Static1
BMC.Eth0LinkAutoNegEnabled	IMM.AutoNegotiate1
BMC.Eth0LinkFullDuplexEnabled	IMM.Duplex1
BMC.Eth0LinkSpeed	IMM.LANDataRate1
BMC.Eth0StaticDNSEnabled	IMM.DNS_Enable
BMC.Eth0StaticDNSIPv6Preferred	IMM.DNSPreference
BMC.Eth0StaticDomainName	IMM.Custom_Domain
BMC.Eth0SyncSettingEnabled	IMM.NetworkSettingSync
BMC.Eth0DHCPDNSEnabled	IMM.DNS_Enable
BMC.Eth0DHCPDomainEnabled	IMM.DDNSPreference
BMC.Eth0IPv4DefaultGateway	IMM.GatewayIPAddress1 IMM.DHCPAssignedGateway1
BMC.Eth0IPv6DefaultGateway	IMM.IPv6GatewayIPAddress1

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.Eth0IPv6AcceptRAEnabled	IMM.IPv6Stateless1
BMC.Eth0MTU	IMM.MTU1
BMC.Eth0StaticIPv4DNSServer_1	IMM.DNS_IP_Address1
BMC.Eth0StaticIPv4DNSServer_2	IMM.DNS_IP_Address2
BMC.Eth0StaticIPv4DNSServer_3	IMM.DNS_IP_Address3
BMC.Eth0StaticIPv6DNSServer_1	IMM.IPv6DNS_IP_Address1
BMC.Eth0StaticIPv6DNSServer_2	IMM.IPv6DNS_IP_Address2
BMC.Eth0StaticIPv6DNSServer_3	IMM.IPv6DNS_IP_Address3
BMC.Eth0StaticIPv4Address	HostIPAddress1
BMC.Eth0StaticIPv4Subnet	IMM.HostIPSubnet1
BMC.Eth0StaticIPv6AddressWithPrefix	IMM.IPv6HostIPAddressWithPrefix1
BMC.Eth0MACAddress	IMM.MACAddress1
BMC.Eth0FailoverMode	IMM.FailoverMode
BMC.Eth0SharedNICMode	IMM.SharedNicMode
BMC.Eth0DHCPAssignedIP	IMM.DHCPAssignedHostIP1
BMC.Eth0DHCPAssignedSubnet	IMM.DHCPAssignedNetMask1
BMC.Eth0DHCPAssignedDomainName	IMM.DHCPAssignedDomainName
BMC.Eth0IPv4DHCPDAssignedDNSServer_1	IMM.DHCPAssignedPrimaryDNS1
BMC.Eth0IPv4DHCPDAssignedDNSServer_2	IMM.DHCPAssignedSecondaryDNS1
BMC.Eth0IPv4DHCPDAssignedDNSServer_3	IMM.DHCPAssignedTertiaryDNS1
BMC.Eth0IPv6DHCPEnabled	IMM.IPv6DHCP1
BMC.Eth0IPv6LinkLocalIP	IMM.IPv6LinkLocalIPAddress1
BMC.Eth0IPv6StatelessIP	IMM.IPv6StatelessIPAddress1
BMC.Eth0IPv6DHCAssignedIP	IMM.IPv6DHCPAssignedHostIP1
BMC.Eth0IPv6DHCPAssignedDomainName	IMM.IPv6DHCPAssignedDomainName
BMC.Eth0IPv6DHCPAssignedDNSServer_1	IMM.IPv6DHCPAssignedPrimaryDNS1
BMC.Eth0IPv6DHCPAssignedDNSServer_2	IMM.IPv6DHCPAssignedSecondaryDNS1
BMC.Eth0IPv6DHCPAssignedDNSServer_3	IMM.IPv6DHCPAssignedTertiaryDNS1
BMC.Eth0BurnedInMACAddress	IMM.BurnedInMacAddress
BMC.NTPEnabled	IMM.NTPAutoSynchronization
BMC.NTPServerHostName1	IMM.NTPHost1
BMC.NTPServerHostName2	IMM.NTPHost2
BMC.NTPServerHostName3	IMM.NTPHost3
BMC.NTPServerHostName4	IMM.NTPHost4
BMC.NTPSyncFrequency	IMM.NTPFrequency
BMC.EthOverUSBEnabled	IMM.LanOverUsb

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.EthOverUSBIPMode	IMM.LanOverUsbAddressType
BMC.EthOverUSBCustomBMCIPv4Address	IMM.LanOverUsbIMMIP
BMC.EthOverUSBCustomHostIPv4Address	IMM.LanOverUsbHostIP
BMC.EthOverUSBCustomIPv4PrefixLength	IMM.LanOverUsbIMMNetmask
BMC.EthOverUSBPortForwardingEnabled	IMM.PortForwarding
BMC.SNMPv1TrapEnabled	IMM.SNMPv1Traps
BMC.SNMPv1TrapCommunityName	IMM.snmpv1_trapcommunityname
BMC.SNMPv1TrapDestination1	IMM.snmpv1_traphostname
BMC.SNMPv1TrapDestination2	IMM.snmpv1_traphostname2
BMC.SNMPv1TrapDestination3	IMM.snmpv1_traphostname3
BMC.SNMPv2TrapEnabled	IMM.snmpv2traps
BMC.SNMPv2TrapCommunityName	IMM.snmpv2_trapcommunityname
BMC.SNMPv2TrapDestination1	IMM.snmpv2_traphostname
BMC.SNMPv2TrapDestination2	IMM.snmpv2_traphostname2
BMC.SNMPv2TrapDestination3	IMM.snmpv2_traphostname3
BMC.SNMPv3AgentEnabled	IMM.SNMPv3Agent IMM.SNMPAgentPortControl
BMC.SNMPv3TrapEnabled	IMM.SNMPTraps
BMC.SNMPv3AgentPort	IMM.SNMP_AgentPort
BMC.SNMPv3EngineID	IMM.SNMPv3EngineId
BMC.SNMPTrapPort	IMM.SNMP_TrapPort
BMC.SNMPAlertCritical	IMM.SNMPAlerts_CriticalAlertCategory
BMC.SNMPAlertWarning	IMM.SNMPAlerts_WarningAlertCategory
BMC.SNMPAlertSystem	IMM.SNMPAlerts_SystemAlertCategory
BMC.SNMPv3TrapUser_1	IMM.LoginId.1
BMC.SNMPv3TrapUser_2	IMM.LoginId.2
BMC.SNMPv3TrapUser_3	IMM.LoginId.3
BMC.SNMPv3TrapAuthProtocol_1	IMM.SNMPv3_AuthenticationProtocol.1
BMC.SNMPv3TrapAuthProtocol_2	IMM.SNMPv3_AuthenticationProtocol.2
BMC.SNMPv3TrapAuthProtocol_3	IMM.SNMPv3_AuthenticationProtocol.3
BMC.SNMPv3TrapAuthPassword_1	IMM.Password.1
BMC.SNMPv3TrapAuthPassword_2	IMM.Password.2
BMC.SNMPv3TrapAuthPassword_3	IMM.Password.3
BMC.SNMPv3TrapPrivacyProtocol_1	IMM.SNMPv3_PrivacyProtocol.1

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.SNMPv3TrapPrivacyProtocol_2	IMM.SNMPv3_PrivacyProtocol.2
BMC.SNMPv3TrapPrivacyProtocol_3	IMM.SNMPv3_PrivacyProtocol.3
BMC.SNMPv3TrapPrivacyPassword_1	IMM.SNMPv3_PrivacyPassword.1
BMC.SNMPv3TrapPrivacyPassword_2	IMM.SNMPv3_PrivacyPassword.2
BMC.SNMPv3TrapPrivacyPassword_3	IMM.SNMPv3_PrivacyPassword.3
BMC.SNMPv3TrapDestination1_1	IMM.SNMPv3_TrapHostname1.1
BMC.SNMPv3TrapDestination1_2	IMM.SNMPv3_TrapHostname1.2
BMC.SNMPv3TrapDestination1_3	IMM.SNMPv3_TrapHostname1.3
BMC.SNMPv3TrapDestination2_1	IMM.SNMPv3_TrapHostname2.1
BMC.SNMPv3TrapDestination2_2	IMM.SNMPv3_TrapHostname2.2
BMC.SNMPv3TrapDestination2_3	IMM.SNMPv3_TrapHostname2.3
BMC.SNMPv3TrapDestination3_1	IMM.SNMPv3_TrapHostname3.1
BMC.SNMPv3TrapDestination3_2	IMM.SNMPv3_TrapHostname3.2
BMC.SNMPv3TrapDestination3_3	IMM.SNMPv3_TrapHostname3.3
BMC.TimeZone	IMM.TimeZone
BMC.DST	IMM.DST
BMC.CrashSnapshotEnabled	IMM.FEHScreenshot
BMC.RemoteAlertRecipientName_1	IMM.RemoteAlertRecipient_Name.1
BMC.RemoteAlertRecipientName_2	IMM.RemoteAlertRecipient_Name.2
BMC.RemoteAlertRecipientName_3	IMM.RemoteAlertRecipient_Name.3
BMC.RemoteAlertRecipientName_4	IMM.RemoteAlertRecipient_Name.4
BMC.RemoteAlertRecipientName_5	IMM.RemoteAlertRecipient_Name.5
BMC.RemoteAlertRecipientName_6	IMM.RemoteAlertRecipient_Name.6
BMC.RemoteAlertRecipientName_7	IMM.RemoteAlertRecipient_Name.7
BMC.RemoteAlertRecipientName_8	IMM.RemoteAlertRecipient_Name.8
BMC.RemoteAlertRecipientName_9	IMM.RemoteAlertRecipient_Name.9
BMC.RemoteAlertRecipientName_10	IMM.RemoteAlertRecipient_Name.10
BMC.RemoteAlertRecipientName_11	IMM.RemoteAlertRecipient_Name.11
BMC.RemoteAlertRecipientName_12	IMM.RemoteAlertRecipient_Name.12
BMC.RemoteAlertRecipientCriticalAlertsCategory_1	IMM.RemoteAlertRecipient_CriticalAlertsCategory.1
BMC.RemoteAlertRecipientCriticalAlertsCategory_2	IMM.RemoteAlertRecipient_CriticalAlertsCategory.2
BMC.RemoteAlertRecipientCriticalAlertsCategory_3	IMM.RemoteAlertRecipient_CriticalAlertsCategory.3
BMC.RemoteAlertRecipientCriticalAlertsCategory_4	IMM.RemoteAlertRecipient_CriticalAlertsCategory.4
BMC.RemoteAlertRecipientCriticalAlertsCategory_5	IMM.RemoteAlertRecipient_CriticalAlertsCategory.5

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.RemoteAlertRecipientCriticalAlertsCategory_6	IMM.RemoteAlertRecipient_CriticalAlertsCategory.6
BMC.RemoteAlertRecipientCriticalAlertsCategory_7	IMM.RemoteAlertRecipient_CriticalAlertsCategory.7
BMC.RemoteAlertRecipientCriticalAlertsCategory_8	IMM.RemoteAlertRecipient_CriticalAlertsCategory.8
BMC.RemoteAlertRecipientCriticalAlertsCategory_9	IMM.RemoteAlertRecipient_CriticalAlertsCategory.9
BMC.RemoteAlertRecipientCriticalAlertsCategory_10	IMM.RemoteAlertRecipient_CriticalAlertsCategory.10
BMC.RemoteAlertRecipientCriticalAlertsCategory_11	IMM.RemoteAlertRecipient_CriticalAlertsCategory.11
BMC.RemoteAlertRecipientCriticalAlertsCategory_12	IMM.RemoteAlertRecipient_CriticalAlertsCategory.12
BMC.RemoteAlertRecipientWarningAlertsCategory_1	IMM.RemoteAlertRecipient_WarningAlertsCategory.1
BMC.RemoteAlertRecipientWarningAlertsCategory_2	IMM.RemoteAlertRecipient_WarningAlertsCategory.2
BMC.RemoteAlertRecipientWarningAlertsCategory_3	IMM.RemoteAlertRecipient_WarningAlertsCategory.3
BMC.RemoteAlertRecipientWarningAlertsCategory_4	IMM.RemoteAlertRecipient_WarningAlertsCategory.4
BMC.RemoteAlertRecipientWarningAlertsCategory_5	IMM.RemoteAlertRecipient_WarningAlertsCategory.5
BMC.RemoteAlertRecipientWarningAlertsCategory_6	IMM.RemoteAlertRecipient_WarningAlertsCategory.6
BMC.RemoteAlertRecipientWarningAlertsCategory_7	IMM.RemoteAlertRecipient_WarningAlertsCategory.7
BMC.RemoteAlertRecipientWarningAlertsCategory_8	IMM.RemoteAlertRecipient_WarningAlertsCategory.8
BMC.RemoteAlertRecipientWarningAlertsCategory_9	IMM.RemoteAlertRecipient_WarningAlertsCategory.9
BMC.RemoteAlertRecipientWarningAlertsCategory_10	IMM.RemoteAlertRecipient_WarningAlertsCategory.10
BMC.RemoteAlertRecipientWarningAlertsCategory_11	IMM.RemoteAlertRecipient_WarningAlertsCategory.11
BMC.RemoteAlertRecipientWarningAlertsCategory_12	IMM.RemoteAlertRecipient_WarningAlertsCategory.12
BMC.RemoteAlertRecipientSystemAlertsCategory_1	IMM.RemoteAlertRecipient_SystemAlertsCategory.1
BMC.RemoteAlertRecipientSystemAlertsCategory_2	IMM.RemoteAlertRecipient_SystemAlertsCategory.2
BMC.RemoteAlertRecipientSystemAlertsCategory_3	IMM.RemoteAlertRecipient_SystemAlertsCategory.3
BMC.RemoteAlertRecipientSystemAlertsCategory_4	IMM.RemoteAlertRecipient_SystemAlertsCategory.4
BMC.RemoteAlertRecipientSystemAlertsCategory_5	IMM.RemoteAlertRecipient_SystemAlertsCategory.5
BMC.RemoteAlertRecipientSystemAlertsCategory_6	IMM.RemoteAlertRecipient_SystemAlertsCategory.6
BMC.RemoteAlertRecipientSystemAlertsCategory_7	IMM.RemoteAlertRecipient_SystemAlertsCategory.7
BMC.RemoteAlertRecipientSystemAlertsCategory_8	IMM.RemoteAlertRecipient_SystemAlertsCategory.8
BMC.RemoteAlertRecipientSystemAlertsCategory_9	IMM.RemoteAlertRecipient_SystemAlertsCategory.9
BMC.RemoteAlertRecipientSystemAlertsCategory_10	IMM.RemoteAlertRecipient_SystemAlertsCategory.10
BMC.RemoteAlertRecipientSystemAlertsCategory_11	IMM.RemoteAlertRecipient_SystemAlertsCategory.11
BMC.RemoteAlertRecipientSystemAlertsCategory_12	IMM.RemoteAlertRecipient_SystemAlertsCategory.12
BMC.RemoteAlertRecipientMethod_1	IMM.RemoteAlertRecipient_Method.1
BMC.RemoteAlertRecipientMethod_2	IMM.RemoteAlertRecipient_Method.2
BMC.RemoteAlertRecipientMethod_3	IMM.RemoteAlertRecipient_Method.3

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.RemoteAlertRecipientMethod_4	IMM.RemoteAlertRecipient_Method.4
BMC.RemoteAlertRecipientMethod_5	IMM.RemoteAlertRecipient_Method.5
BMC.RemoteAlertRecipientMethod_6	IMM.RemoteAlertRecipient_Method.6
BMC.RemoteAlertRecipientMethod_7	IMM.RemoteAlertRecipient_Method.7
BMC.RemoteAlertRecipientMethod_8	IMM.RemoteAlertRecipient_Method.8
BMC.RemoteAlertRecipientMethod_9	IMM.RemoteAlertRecipient_Method.9
BMC.RemoteAlertRecipientMethod_10	IMM.RemoteAlertRecipient_Method.10
BMC.RemoteAlertRecipientMethod_11	IMM.RemoteAlertRecipient_Method.11
BMC.RemoteAlertRecipientMethod_12	IMM.RemoteAlertRecipient_Method.12
BMC.RemoteAlertRecipientEmail_1	IMM.RemoteAlertRecipient_Email.1
BMC.RemoteAlertRecipientEmail_2	IMM.RemoteAlertRecipient_Email.2
BMC.RemoteAlertRecipientEmail_3	IMM.RemoteAlertRecipient_Email.3
BMC.RemoteAlertRecipientEmail_4	IMM.RemoteAlertRecipient_Email.4
BMC.RemoteAlertRecipientEmail_5	IMM.RemoteAlertRecipient_Email.5
BMC.RemoteAlertRecipientEmail_6	IMM.RemoteAlertRecipient_Email.6
BMC.RemoteAlertRecipientEmail_7	IMM.RemoteAlertRecipient_Email.7
BMC.RemoteAlertRecipientEmail_8	IMM.RemoteAlertRecipient_Email.8
BMC.RemoteAlertRecipientEmail_9	IMM.RemoteAlertRecipient_Email.9
BMC.RemoteAlertRecipientEmail_10	IMM.RemoteAlertRecipient_Email.10
BMC.RemoteAlertRecipientEmail_11	IMM.RemoteAlertRecipient_Email.11
BMC.RemoteAlertRecipientEmail_12	IMM.RemoteAlertRecipient_Email.12
BMC.RemoteAlertRecipientAddress_1	IMM.RemoteAlertRecipient_Address.1
BMC.RemoteAlertRecipientAddress_2	IMM.RemoteAlertRecipient_Address.2
BMC.RemoteAlertRecipientAddress_3	IMM.RemoteAlertRecipient_Address.3
BMC.RemoteAlertRecipientAddress_4	IMM.RemoteAlertRecipient_Address.4
BMC.RemoteAlertRecipientAddress_5	IMM.RemoteAlertRecipient_Address.5
BMC.RemoteAlertRecipientAddress_6	IMM.RemoteAlertRecipient_Address.6
BMC.RemoteAlertRecipientAddress_7	IMM.RemoteAlertRecipient_Address.7
BMC.RemoteAlertRecipientAddress_8	IMM.RemoteAlertRecipient_Address.8
BMC.RemoteAlertRecipientAddress_9	IMM.RemoteAlertRecipient_Address.9
BMC.RemoteAlertRecipientAddress_10	IMM.RemoteAlertRecipient_Address.10
BMC.RemoteAlertRecipientAddress_11	IMM.RemoteAlertRecipient_Address.11
BMC.RemoteAlertRecipientAddress_12	IMM.RemoteAlertRecipient_Address.12
BMC.RemoteAlertRecipientPort_1	IMM.RemoteAlertRecipient_Port.1

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.RemoteAlertRecipientPort_2	IMM.RemoteAlertRecipient_Port.2
BMC.RemoteAlertRecipientPort_3	IMM.RemoteAlertRecipient_Port.3
BMC.RemoteAlertRecipientPort_4	IMM.RemoteAlertRecipient_Port.4
BMC.RemoteAlertRecipientPort_5	IMM.RemoteAlertRecipient_Port.5
BMC.RemoteAlertRecipientPort_6	IMM.RemoteAlertRecipient_Port.6
BMC.RemoteAlertRecipientPort_7	IMM.RemoteAlertRecipient_Port.7
BMC.RemoteAlertRecipientPort_8	IMM.RemoteAlertRecipient_Port.8
BMC.RemoteAlertRecipientPort_9	IMM.RemoteAlertRecipient_Port.9
BMC.RemoteAlertRecipientPort_10	IMM.RemoteAlertRecipient_Port.10
BMC.RemoteAlertRecipientPort_11	IMM.RemoteAlertRecipient_Port.11
BMC.RemoteAlertRecipientPort_12	IMM.RemoteAlertRecipient_Port.12
BMC.RemoteAlertRecipientIncludeEventLog_1	IMM.RemoteAlertRecipient_IncludeEventLog.1
BMC.RemoteAlertRecipientIncludeEventLog_2	IMM.RemoteAlertRecipient_IncludeEventLog.2
BMC.RemoteAlertRecipientIncludeEventLog_3	IMM.RemoteAlertRecipient_IncludeEventLog.3
BMC.RemoteAlertRecipientIncludeEventLog_4	IMM.RemoteAlertRecipient_IncludeEventLog.4
BMC.RemoteAlertRecipientIncludeEventLog_5	IMM.RemoteAlertRecipient_IncludeEventLog.5
BMC.RemoteAlertRecipientIncludeEventLog_6	IMM.RemoteAlertRecipient_IncludeEventLog.6
BMC.RemoteAlertRecipientIncludeEventLog_7	IMM.RemoteAlertRecipient_IncludeEventLog.7
BMC.RemoteAlertRecipientIncludeEventLog_8	IMM.RemoteAlertRecipient_IncludeEventLog.8
BMC.RemoteAlertRecipientIncludeEventLog_9	IMM.RemoteAlertRecipient_IncludeEventLog.9
BMC.RemoteAlertRecipientIncludeEventLog_10	IMM.RemoteAlertRecipient_IncludeEventLog.10
BMC.RemoteAlertRecipientIncludeEventLog_11	IMM.RemoteAlertRecipient_IncludeEventLog.11
BMC.RemoteAlertRecipientIncludeEventLog_12	IMM.RemoteAlertRecipient_IncludeEventLog.12
BMC.RemoteAlertRecipientStatus_1	IMM.RemoteAlertRecipient_Status.1
BMC.RemoteAlertRecipientStatus_2	IMM.RemoteAlertRecipient_Status.2
BMC.RemoteAlertRecipientStatus_3	IMM.RemoteAlertRecipient_Status.3
BMC.RemoteAlertRecipientStatus_4	IMM.RemoteAlertRecipient_Status.4
BMC.RemoteAlertRecipientStatus_5	IMM.RemoteAlertRecipient_Status.5
BMC.RemoteAlertRecipientStatus_6	IMM.RemoteAlertRecipient_Status.6
BMC.RemoteAlertRecipientStatus_7	IMM.RemoteAlertRecipient_Status.7
BMC.RemoteAlertRecipientStatus_8	IMM.RemoteAlertRecipient_Status.8
BMC.RemoteAlertRecipientStatus_9	IMM.RemoteAlertRecipient_Status.9
BMC.RemoteAlertRecipientStatus_10	IMM.RemoteAlertRecipient_Status.10
BMC.RemoteAlertRecipientStatus_11	IMM.RemoteAlertRecipient_Status.11

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.RemoteAlertRecipientStatus_12	IMM.RemoteAlertRecipient_Status.12
BMC.RemoteAlertRetryLimit	IMM.RetryLimit
BMC.RemoteAlertEntriesDelay	IMM.EntriesDelay
BMC.RemoteAlertRetryDelay	IMM.RetryDelay
BMC.SNMPv3AgentAuthProtocol_1	IMM.SNMPv3_AuthenticationProtocol.1
BMC.SNMPv3AgentAuthProtocol_2	IMM.SNMPv3_AuthenticationProtocol.2
BMC.SNMPv3AgentAuthProtocol_3	IMM.SNMPv3_AuthenticationProtocol.3
BMC.SNMPv3AgentAuthProtocol_4	IMM.SNMPv3_AuthenticationProtocol.4
BMC.SNMPv3AgentAuthProtocol_5	IMM.SNMPv3_AuthenticationProtocol.5
BMC.SNMPv3AgentAuthProtocol_6	IMM.SNMPv3_AuthenticationProtocol.6
BMC.SNMPv3AgentAuthProtocol_7	IMM.SNMPv3_AuthenticationProtocol.7
BMC.SNMPv3AgentAuthProtocol_8	IMM.SNMPv3_AuthenticationProtocol.8
BMC.SNMPv3AgentAuthProtocol_9	IMM.SNMPv3_AuthenticationProtocol.9
BMC.SNMPv3AgentAuthProtocol_10	IMM.SNMPv3_AuthenticationProtocol.10
BMC.SNMPv3AgentAuthProtocol_11	IMM.SNMPv3_AuthenticationProtocol.11
BMC.SNMPv3AgentAuthProtocol_12	IMM.SNMPv3_AuthenticationProtocol.12
BMC.SNMPv3AgentPrivacyProtocol_1	IMM.SNMPv3_PrivacyProtocol.1
BMC.SNMPv3AgentPrivacyProtocol_2	IMM.SNMPv3_PrivacyProtocol.2
BMC.SNMPv3AgentPrivacyProtocol_3	IMM.SNMPv3_PrivacyProtocol.3
BMC.SNMPv3AgentPrivacyProtocol_4	IMM.SNMPv3_PrivacyProtocol.4
BMC.SNMPv3AgentPrivacyProtocol_5	IMM.SNMPv3_PrivacyProtocol.5
BMC.SNMPv3AgentPrivacyProtocol_6	IMM.SNMPv3_PrivacyProtocol.6
BMC.SNMPv3AgentPrivacyProtocol_7	IMM.SNMPv3_PrivacyProtocol.7
BMC.SNMPv3AgentPrivacyProtocol_8	IMM.SNMPv3_PrivacyProtocol.8
BMC.SNMPv3AgentPrivacyProtocol_9	IMM.SNMPv3_PrivacyProtocol.9
BMC.SNMPv3AgentPrivacyProtocol_10	IMM.SNMPv3_PrivacyProtocol.10
BMC.SNMPv3AgentPrivacyProtocol_11	IMM.SNMPv3_PrivacyProtocol.11
BMC.SNMPv3AgentPrivacyProtocol_12	IMM.SNMPv3_PrivacyProtocol.12
BMC.SNMPv3AgentAccessType_1	IMM.SNMPv3_AccessType.1
BMC.SNMPv3AgentAccessType_2	IMM.SNMPv3_AccessType.2
BMC.SNMPv3AgentAccessType_3	IMM.SNMPv3_AccessType.3
BMC.SNMPv3AgentAccessType_4	IMM.SNMPv3_AccessType.4
BMC.SNMPv3AgentAccessType_5	IMM.SNMPv3_AccessType.5
BMC.SNMPv3AgentAccessType_6	IMM.SNMPv3_AccessType.6

Table 4. BMC setting names mapping (continued)

XCC3 Setting Name	XCC2/XCC Setting Name
BMC.SNMPv3AgentAccessType_7	IMM.SNMPv3_AccessType.7
BMC.SNMPv3AgentAccessType_8	IMM.SNMPv3_AccessType.8
BMC.SNMPv3AgentAccessType_9	IMM.SNMPv3_AccessType.9
BMC.SNMPv3AgentAccessType_10	IMM.SNMPv3_AccessType.10
BMC.SNMPv3AgentAccessType_11	IMM.SNMPv3_AccessType.11
BMC.SNMPv3AgentAccessType_12	IMM.SNMPv3_AccessType.12
BMC.SNMPv3AgentPrivacyPassword_1	IMM.SNMPv3_PrivacyPassword.1
BMC.SNMPv3AgentPrivacyPassword_2	IMM.SNMPv3_PrivacyPassword.2
BMC.SNMPv3AgentPrivacyPassword_3	IMM.SNMPv3_PrivacyPassword.3
BMC.SNMPv3AgentPrivacyPassword_4	IMM.SNMPv3_PrivacyPassword.4
BMC.SNMPv3AgentPrivacyPassword_5	IMM.SNMPv3_PrivacyPassword.5
BMC.SNMPv3AgentPrivacyPassword_6	IMM.SNMPv3_PrivacyPassword.6
BMC.SNMPv3AgentPrivacyPassword_7	IMM.SNMPv3_PrivacyPassword.7
BMC.SNMPv3AgentPrivacyPassword_8	IMM.SNMPv3_PrivacyPassword.8
BMC.SNMPv3AgentPrivacyPassword_9	IMM.SNMPv3_PrivacyPassword.9
BMC.SNMPv3AgentPrivacyPassword_10	IMM.SNMPv3_PrivacyPassword.10
BMC.SNMPv3AgentPrivacyPassword_11	IMM.SNMPv3_PrivacyPassword.11
BMC.SNMPv3AgentPrivacyPassword_12	IMM.SNMPv3_PrivacyPassword.12
BMC.WatchdogOSLoadTimeoutMinutes	IMM.LoaderWatchdog
BMC.WatchdogOSTimeoutValueMinutes	IMM.OSWatchdog
BMC.LLDPEnabled	IMM.LLDPControl
BMC.KMIPServerHostName1	IMM.SKR_Server1_HostName_IPAddress
BMC.KMIPServerHostName2	IMM.SKR_Server2_HostName_IPAddress
BMC.KMIPServerHostName3	IMM.SKR_Server3_HostName_IPAddress
BMC.KMIPServerHostName4	IMM.SKR_Server4_HostName_IPAddress
BMC.KMIPPort1	IMM.SKR_Server1_Port
BMC.KMIPPort2	IMM.SKR_Server2_Port
BMC.KMIPPort3	IMM.SKR_Server3_Port
BMC.KMIPPort4	IMM.SKR_Server4_Port

Accessing the command-line interface

Use the information in this topic to access the CLI.

To access the CLI, start an SSH session to the XClarity Controller IP address (see "Configuring serial-to-SSH redirection" on page 109 for more information).

Logging in to the command-line session

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

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

Step 1. Establish a connection with the XClarity Controller.

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 XClarity Controller.

Note: The command-line prompt is `system>`. The command-line session continues until you type `exit` at the command line. You are logged off and the session is ended.

Configuring serial-to-SSH redirection

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

Serial-to-SSH redirection enables a system administrator to use the XClarity Controller as a serial terminal server. A server serial port can be accessed from a SSH connection when serial redirection is enabled.

Note: The CLI `console 1` command is used to start a serial redirection session with the COM port.

Example session

```
$ ssh USERID@10.240.1.12
Password:

system>
```

All traffic from the SSH session is routed to COM2.

```
ESC (
```

Type the exit key sequence to return to the CLI. In this example, press Esc and then type a left parenthesis. The CLI prompt displays to indicate return to the IMM CLI.

```
system>
```

Command syntax

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

Read the following guidelines before you use the commands:

- Each command has the following format:
  `command [arguments] [-options]`
- The command syntax is case sensitive.
- The command name is all lowercase.
- All arguments must immediately follow the command. The options immediately follow the arguments.
- Each option is always preceded by a hyphen (-). An option can be a short option (single letter) or a long option (multiple letters).
- If an option has an argument, the argument is mandatory, for example:
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`

Where `ifconfig` is the command, `eth0` is an argument, and -i, -g, and -s are options. In this example, all three options have arguments.

- Brackets indicate that an argument or option is optional. Brackets are not part of the command that you type.

Features and limitations

This topic contains information about CLI features and limitations.

The CLI has the following features and limitations:

- Multiple concurrent CLI sessions are allowed via SSH.
- One command is allowed per line (1024-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 XClarity ControllerA00096B9E003A
  -r auto
  -d auto
  -m 1500
  -b 00:09:6B:9E:00:3A
  -l 00:00:00:00:00:00
  system >
  ```

- In the CLI, the output buffer limit is 2 KB. There is no buffering. The output of an individual command cannot exceed 2048 characters. This limit does not apply in serial redirect mode (the data is buffered during serial redirect).
- Simple text messages are used to denote command execution status, as in the following example:

  ```
  system> power on
  ok
  system> power state
  Power: On
  State: System power off/State unknown
  system>
  ```

- The command syntax is case sensitive.
- There must be at least one space between an option and its argument. For example, `ifconfig eth0 -i192.168.70.133` is incorrect syntax. The correct syntax is `ifconfig eth0 -i 192.168.70.133`.
- All commands have the `-h`, `-help`, and `?` options, which give syntax help. All of the following examples will give the same result:

  ```
  system> power -h
  system> power -help
  system> power ?
  ```

- Some of the commands that are described in the following sections might not be available for your system configuration. To see a list of the commands that are supported by your configuration, use the `help` or ? option, as shown in the following examples:

```
system> help
system> ?
```

Alphabetical command listing

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

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

- "accseccfg command" on page 124
- "adapter command" on page 176
- "alertcfg command" on page 125
- "alertentries command" on page 160
- "asu command" on page 126
- "backup command" on page 129
- "batch command" on page 163
- "chconfig command" on page 165
- "chlog command" on page 168
- "chmanual command" on page 168
- "clearlog command" on page 113
- "clock command" on page 163
- "dbgshbmc command" on page 178
- "dhcpinfo command" on page 129
- "dns command" on page 130
- "encaps command" on page 131
- "ethtousb command" on page 131
- "exit command" on page 112
- "fans command" on page 114
- "firewall command" on page 132
- "fuelg command" on page 123
- "gprofile command" on page 133
- "hashpw command" on page 134
- "help command" on page 113
- "history command" on page 113
- "ifconfig command" on page 135
- "info command" on page 164
- "keycfg command" on page 136
- "ldap command" on page 137
- "led command" on page 115
- "lldp command" on page 139

- “mhlog command” on page 114
- “ntp command” on page 140
- “portcontrol command” on page 140
- “ports command” on page 141
- “power command” on page 121
- “pxeboot command” on page 124
- “rdmount command” on page 142
- “readlog command” on page 116
- “reset command” on page 123
- “restore command” on page 142
- “roles command” on page 143
- “rtd command” on page 144
- “seccfg command” on page 144
- “securityinfo command” on page 145
- “securitymode command” on page 145
- “servicelog command” on page 117
- “snmp command” on page 146
- “snmpalerts command” on page 148
- “spreset command” on page 165
- “sshcfg command” on page 149
- “sslcfg command” on page 150
- “storage command” on page 168
- “syncrep command” on page 153
- “syshealth command” on page 119
- “syslock command” on page 152
- “temps command” on page 120
- “thermal command” on page 154
- “tls command” on page 155
- “trespass command” on page 155
- “uefipw command” on page 156
- “usbeth command” on page 156
- “users command” on page 157
- “volts command” on page 120
- “vpd command” on page 121

Utility commands

This topic provides an alphabetic list of utility CLI commands.

exit command

Use this command to log off the CLI session, Use the `exit` command to log off and end the CLI session.

help command

This command displays a list of all commands.

Use the `help` command to display a list of all commands with a short description for each. You can also type ? at the command prompt.

history command

This command provides a list of previously issued commands.

Use the `history` command to display an indexed history list of the last eight commands that were issued. The indexes can then be used as shortcuts (preceded by !) to reissue commands from this history list.

Example:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Monitor commands

This topic provides an alphabetic list of monitor CLI commands.

clearlog command

This command is used to clear the IMM event log.

Use the `clearlog` command to clear the event log of the IMM. You must have the authority to clear event logs to use this command.

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

Syntax:

```
clearlog [-options]
```

Table 5. clearlog options

Option	Description	Values
-t	Event type, choose which type of event to clear. If not specified, all event types will be selected.	• all: All event type, including platform event and audit event. • platform: Platform event type. • audit: Audit event type.

Example:

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

fans command

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

Use the `fans` command to display the speed for each of the server fans.

Example:

```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

mhlog command

Use this command to display maintenance history activity log entries.

Syntax:

```
mhlog [-options]
```

Table 6. mhlog options

Option	Description	Values
-c	Display count entries	Between 1 and 250
-i	Display entries starting at index	Between 1 and 250
-f	Remote filename of log file	Valid file name for filename of log file
-ip	Address of tftp/sftp server	Valid IP address for TFTP/SFTP server
-pn	Port number of tftp/sftp server	Valid port number for TFTP/SFTP server (default 69/22)
-u	Username for sftp server	Valid user name for SFTP server
-pw	Password for sftp server	Valid password for SFTP server

Example:

```
system> mhlog
Type            Message                                                  Time
-------------   ------------                                             ----
Hardware       SAS Backplane1(SN: XXXX9CE009L) is added.              05/08/2020,04:23:18
Hardware       CPU 1(SKU NO: 50844440) is added.                      05/08/2020,04:23:22
Hardware       CPU 2(SKU NO: 50844440) is added.                      05/08/2020,04:23:22
Hardware       M2 Card(SN: R1SH9AJ0037) is added.                     05/08/2020,04:23:22
Firmware       Primary XCC firmware is updated to TGBT99T by XCC Web.   05/08/2020,06:40:37
Firmware       Primary XCC firmware is activated to TGBT99T.         05/08/2020,06:41:26
Hardware       PSU1(SN: D1DG94C0075) is added.                        05/08/2020,06:43:28
system>
```

led command

Use this command to display and set LED states.

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

- Running the `led` command with no options displays the status of the front panel LEDs.
- The `led -d` command option must be used with `led -identify on` command option.

Syntax:

```
led [-options]
```

Table 7. led options

Option	Description	Values
`-l`	Get the status of all system and system subcomponent LEDs	
`-identify`	Change state of enclosure identify LED	`off`, `on`, `blink`
`-d`	Turn on identification LED for specified time period	Time period (seconds)

Example:

```
system> led
Fault                 Off
Identify              On            Blue
Chklog                Off
Power                 Off

system> led -l
Label                 Location                  State         Color
Battery               Planar                    Off
BMC Heartbeat         Planar                    Blink         Green
BRD                   Lightpath Card            Off
Channel A             Planar                    Off
Channel B             Planar                    Off
Channel C             Planar                    Off
Channel D             Planar                    Off
Channel E             Planar                    Off
Chklog                Front Panel               Off
CNFG                  Lightpath Card            Off
CPU                   Lightpath Card            Off
CPU 1                 Planar                    Off
CPU 2                 Planar                    Off
DASD                  Lightpath Card            Off
```

```
DIMM                    Lightpath Card             Off
DIMM 1                  Planar                     Off
DIMM 10                 Planar                     Off
DIMM 11                 Planar                     Off
DIMM 12                 Planar                     Off
DIMM 13                 Planar                     Off
DIMM 14                 Planar                     Off
DIMM 15                 Planar                     Off
DIMM 16                 Planar                     Off
DIMM 2                  Planar                     Off
DIMM 3                  Planar                     Off
DIMM 4                  Planar                     Off
DIMM 5                  Planar                     Off
DIMM 6                  Planar                     Off
DIMM 7                  Planar                     Off
DIMM 8                  Planar                     Off
DIMM 9                  Planar                     Off
FAN                     Lightpath Card             Off
FAN 1                   Planar                     Off
FAN 2                   Planar                     Off
FAN 3                   Planar                     Off
Fault                   Front Panel (+)            Off
Identify                Front Panel (+)            On             Blue
LINK                    Lightpath Card             Off
LOG                     Lightpath Card             Off
NMI                     Lightpath Card             Off
OVER SPEC               Lightpath Card             Off
PCI 1                   FRU                        Off
PCI 2                   FRU                        Off
PCI 3                   FRU                        Off
PCI 4                   FRU                        Off
Planar                  Planar                     Off
Power                   Front Panel (+)            Off
PS                      Lightpath Card             Off
RAID                    Lightpath Card             Off
Riser 1                 Planar                     Off
Riser 2                 Planar                     Off
SAS ERR                 FRU                        Off
SAS MISSING             Planar                     Off
SP                      Lightpath Card             Off
TEMP                    Lightpath Card             Off
VRM                     Lightpath Card             Off
system>
```

readlog command

This command displays the IMM event logs.

Use the `readlog` command to display the IMM event log entries. Five event logs are displayed at a time. The entries are displayed from the most recent to the oldest.

Notes:

- R - invalid
- I - info
- W - warning
- E - critical

Syntax:

```
readlog [-options]
```

Table 8. readlog options

Option	Description	Values
`-a`	Displays all entries in the event log, starting with the most recent.	
`-f`	Resets the counter and displays the first 5 entries in the event log, starting with the most recent.	
`-date`	Displays event log entries for the specified date	Use the following format: mm/dd/yyyy
`-sev`	Displays event log entries for the specified severity level.	`R`, `I`, `W`, `E`
`-i`	Sets the IPv4 or IPv6 IP address of the TFTP or SFTP server where the event log is saved. The **-i** and **-l** command options are used together to specify the location.	Valid IP address
`-l`	Sets the file name of the event log file. The **-i** and **-l** command options are used together to specify the location.	Valid filename
`-pn`	Displays or sets the port number of the TFTP or SFTP server.	Valid port number (default 69/22)
`-u`	Specifies the user name for the SFTP server.	Valid user name
`-pw`	Specifies the password for the SFTP server.	Valid password
`-di`	Extended audit log capability	`none`, `ipmi`

Example:

```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
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>
```

servicelog command

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

Note: This command used to be `ffdc` command.

Use the servicelog command to generate and transfer service data to Support.

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

The following table shows the arguments for the options.

Syntax:

```
servicelog [subset_command] [-options]
```

Table 9. servicelog subset commands

Option	Description
generate	Create a new service data file
status	Check status of service data file
copy	Copy existing service data
delete	Delete existing service data

Table 10. servicelog options

Option	Description	Values
-t	Service log type	• 1: Debug log (FFDC, default) • 2: Service data log • 3: Service data log coupled debug log, which is only valid when copying log files
Additional options for generate command		
-c	Dump data category selection. The data category won't be contained if not specified with this option.	• For type 1 (ffdc): corefile • For type 2 (service data log): network, audit, telemetry, osscreen
Additional options for generate and copy commands		
-f	Remote filename or sftp target directory.	For sftp, use full path or trailing / on directory name (~/ or /tmp/). The default value is the system generated name.
-ip	Address of the tftp/sftp server.	Valid IP address
-pn	Port number of the tftp/sftp server.	Valid port number (default 69/22)
-u	Username for the sftp server.	Valid user name
-pw	Password for the sftp server.	Valid password
-timeout	Minutes to allow for foreground copy.	Between 1 and 5 (default 1)

Example:

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

```
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -ip 192.168.70.230
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

syshealth command

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

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

Syntax:

```
syshealth [arguments]
```

Table 11. syshealth arguments

Arguments	Description
`summary`	Display the system health summary.
`activeevents`	Display active events.
`cooling`	Display cooling devices health status.
`power`	Display power modules health status.
`storage`	Display local storage health status.
`processors`	Display processors health status.
`memory`	Display memory health status.

Example:

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

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

temps command

This command displays all temperature and temperature threshold information.

Use the `temps` command to display all the temperatures and temperature thresholds. The same set of temperatures are displayed as in the web interface.

Syntax:
```
temps
```

Example:
```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
               WR          W      T             SS             HS
------------------------------------------------------------------------------
Ambient Temp   109.40/43   N/A    78.80/26.00  109.40/43.00  122.00/50.00
Exhaust Temp   N/A          N/A    32.00/0 .00  116.60/47.00  N/A
system>
```

Notes:

1. The output has the following column headings:

   WR: warning reset (Positive-going Threshold Hysteresis value)

   W: warning (Upper non-critical Threshold)

   T: temperature (Current value)

   SS: soft shutdown (Upper critical Threshold)

   HS: hard shutdown (Upper non-recoverable Threshold)
2. All temperature values are in degrees Fahrenheit/Celsius.
3. N/A represents not applicable.

volts command

Use this command to display the server voltage information.

Use the `volts` command to display all the voltages and voltage thresholds. The same set of voltages are displayed as in the web interface.

Syntax:
```
volts
```

Example:
```
system> volts
               HSL  SSL    WL    WRL   V      WRH   WH    SSH   HSH
---------------------------------------------------------------------
CMOS Battery  N/A   2.25  2.39  0.03  3.12  0.03  N/A  N/A    N/A
system>
```

Note: The output has the following column headings:

HSL: hard shutdown low (Lower non-recoverable Threshold)

SSL: soft shutdown low (Lower critical Threshold)

WL: warning low (Lower non-critical Threshold)

WRL: warning reset low (Negative-going Threshold Hysteresis value)

V: voltage (current value)

WRH: warning reset high (Positive-going Threshold Hysteresis value)

WH: warning high (Upper non-critical Threshold)

SSH: soft shutdown high (Upper critical Threshold)

HSH: hard shutdown high (Upper non-recoverable Threshold)

vpd command

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

Use the `vpd` command to display vital product data for the system (sys), IMM (bmc), server BIOS (uefi), Lenovo XClarity Provisioning Manager (lxpm), server firmware (fw), server components (comp) and PCIe devices (pcie). The same information is displayed as in the web interface.

Syntax:

```
vpd [arguments]
```

Table 12. vpd arguments

Arguments	Description
`vpd sys`	Displays Vital Product Data for the system.
`vpd bmc`	Displays Vital Product Data for the management controller.
`vpd uefi`	Displays Vital Product Data for system BIOS.
`vpd lxpm`	Displays Vital Product Data for system LXPM.
`vpd fw`	Displays Vital Product Data for the system firmware.
`vpd comp`	Displays Vital Product Data for the system components.
`vpd pcie`	Displays Vital Product Data for PCIe devices.

Example:

```
system> vpd bmc
Type            Status      Version    Build      ReleaseDate
-------------   -------     -------    ------     ------------
BMC (Primary)   Active      0.00       DVI399T    2017/06/06
BMC (Backup)    Inactive    1.00       TEI305J    2017/04/13
system>
```

Server power and restart control commands

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

power command

This command describes how to control the server power.

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

Syntax:

```
power on [-options]
power off [-options]
power cycle [-options]
power uefi
power state
```

Table 13. power commands

Command	Description
`power on`	Use this command to turn on the server power.
`power off`	Use this command to turn off the server power.
`power cycle`	Use this command to turn off the server power and then turn on the server power.
`power uefi`	Use this command to boot into UEFI's F1 setup.
`power state`	Use this command to display the server power state and the current state of the server.

Table 14. power options

Option	Description	Values
`-s`	Use this option to shut down the operating system before the server is turned off. **Note:** The `-s` option is implied when using the `-every` option for the `power off` and `power cycle` commands.	
`-every`	Use this option with the `power on`, `power off`, and `power cycle` commands to control the server power. You can set up the dates, times, and frequency (daily or weekly) to power on, power off, or power cycle your server.	`Sun`, `Mon`, `Tue`, `Wed`, `Thu`, `Fri`, `Sat`, `Day`, `clear`
`-t`	Use this option to specify the time in hours and minutes to power on the server, shut down the operating system, and power off or restart the server.	Use the following format: hh:mm
`-d`	Use this option to specify the date to power on the sever. This is an additional option for the `power on` command. **Note:** The `-d` and `-every` options, cannot be used together on the same command.	Use the following format: mm/dd/yyyy
`-clear`	Use this option to clear the scheduled power on date. This is an additional option for the `power on` command.	

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

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

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

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

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

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

```
system> power on -every Mon -t 1:30
```

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

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

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

```
system> power cycle -every clear
```

reset command

This command describes how to reset the server.

Use the `reset` command to restart the server. To use this command, you must have power and restart access authority.

Syntax:

```
reset [-options]
```

Table 15. reset options

Option	Description	Values
`-s`	Shut down the operating system before the server is reset.	
`-d`	Delay performing the reset for the given number of seconds.	0 - 120
`-nmi`	Generate a non-maskable interrupt (NMI) on the server.	

fuelg command

This command displays information about the server power.

Use the `fuelg` command to display information about server power usage and configure server power management. This command also configures policies for power redundancy loss.

Syntax:

```
fuelg [-options]
```

Table 16. fuelg options

Option	Description	Values
`-pme`	Enable or disable power management and capping on the server.	`on`, `off`
`-pcapmode`	Set the power capping mode for the server.	`output`, `input`
`-pcap`	A numeric value that falls within the range of power capping values displayed when running the fuelg command, with no options, on the target.	numeric wattage value
`-history`	Display power consumption or performance history.	`pc`, `perf`
`-period`	A numeric value to display history.	`1`, `6`, `12`, `24` hours
`-pm`	Set the policy mode for loss of redundant power.	• `bt`- basic with throttling • `rt`- redundant with throttling (default)
`-zm`	Enable or disable zero output mode. This setting can only be set when the policy mode is set to redundant with throttling.	`on`, `off`

Table 16. fuelg options (continued)

Option	Description	Values
-perf	Display the current compute utilization, including system, processor, memory module, and I/O.	
-pc	Display current power consumption	• output- display current output power consumption of the system, processor, memory module and other components. • input- Display current input power consumption, including system power consumption. **Note:** For AMD servers, current output power consumption will not display some of the components.

pxeboot command

This command displays and sets the condition of the Preboot eXecution Environment.

Syntax:
```
pxeboot [-options]
```

Table 17. pxeboot options

Option	Description	Values
-en	Sets the Preboot eXecution Environment condition for the next system restart.	enabled, disabled

Configuration commands

This topic provides an alphabetic list of configuration CLI commands.

accseccfg command

Use this command to display and configure account security settings.

Syntax:
```
accseccfg [-options]
```

Table 18. accseccfg options

Option	Description	Values
-am	Sets user authentication method.	local, ldap, localldap, ldaplocal
-lp	Lockout period after maximum login failures (minutes).	Between 0 and 2880, 0 = lockout period does not expire
-pe	Password expiration time period (days).	Between 0 and 365, 0 = never expire

Table 18. accseccfg options (continued)

Option	Description	Values
`-pew`	Password expiration warning time period **Note:** The Password expiration warning time period must be less than Password expiration time period.	Between 0 and 30, 0 = never warn
`-pc`	Password complexity rules enabled.	`on`, `off`
`-pl`	Password length.	If password complexity rules are enabled, the password length is between 8 and 32. Otherwise, it is between 0 and 32.
`-ci`	Minimum password change interval (hours).	between 0 and 240, 0 = change immediately
`-lf`	Maximum number of login failures.	Between 0 and 10, 0 = never locked
`-chgnew`	Change new user password after first login.	`on`, `off`
`-rc`	Password reuse cycle.	Between 0 and 10, 0 = reuse immediately
`-wt`	Web and Secure Shell inactivity session timeout (minutes).	Between 0 and 1440

Example:

```
system> accseccfg
  -am: local
  -lp: 60
  -pe: none
  -pew: 0
  -pc: on
  -pl: 10
  -ci: 0
  -lf: 5
  -chgnew: on
  -rc: 5
  -wt: 20
system>
```

alertcfg command

Use this command to display and configure the IMM global remote alert parameters.

Syntax:

```
accseccfg [-options]
```

Table 19. alertcfg options

Option	Description	Values
`-dr`	Sets wait time between retries before the IMM resends an alert.	0.0 to 4.0 minutes, in 0.5 minute increments
`-da`	Sets wait time before the IMM sends an alert to the next recipient in the list.	0.0 to 4.0 minutes, in 0.5 minute increments

Table 19. alertcfg options (continued)

Option	Description	Values
`-rl`	Set the number of additional times that the XCC subsystem attempts to send an alert, if previous attempts were unsuccessful.	0 to 8
`-tcp`	Set the option to be enabled that the syslog will transport by TCP protocal	`enabled`, `disabled`

Example:

```
system> alertcfg
 -dr 2.0
 -da 2.0
 -rl 5
 -tcp disabled
system>
```

asu command

This command is used to configure UEFI settings.

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

Syntax:

```
asu [subset_command]
```

Table 20. asu subset commands

Command	Description	Value
`help`	Use this command to display help information for one or more settings.	**setting_name**
`set`	Use this command to change the value of a setting. Set the UEFI setting to the input value. **Notes:** • Set one or more setting/value pairs. • The setting can contain wildcards if it expands to a single setting. • The value must be enclosed in quotes if it contains spaces. • Ordered list values are separated by the equal symbol (=). For example, set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."	**setting_name=value**
`show`	Use this command to display the current value of one or more settings.	**setting_name**

Table 20. asu subset commands (continued)

Command	Description	Value
`showvalues`	Use this command to display all possible values for one or more settings. **Notes:** • This command will display information about the allowable values for the setting. • The minimum and maximum number of instances allowed for the setting is displayed. • The default value will be displayed if available. • The default value is enclosed with opening and closing angle brackets (< and >). • Text values show the minimum and maximum length and regular expression.	**setting_name**
`showgroups`	Use this command to display the available setting groups. This command displays the names of known groups. Group names may vary depending on the installed devices.	

Notes:

- In the command syntax, **setting_name** is the name of a setting that you want to view or change, and **value** is the value that you are placing on the setting.
- **setting_name** can be more than one name, except when using the `set` command.
- **setting_name** can contain wildcards, for example an asterisk (*) or a question mark (?).
- **setting_name** can be a group, a setting name, or `all`.

Examples:

- To display all of the asu command options enter `asu help`.
- To display help for one command enter `asu help setting_name`.
- To change a value enter `asu set setting_name=value`.
- To display the current value enter `asu show setting_name`.
- To display all possible values for a setting enter `asu showvalues setting_name`. Example show values command:

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

- To display the available setting groups enter `asu showgroups`.

The following table shows the arguments for the options.

Table 21. asu options

Option	Description
`-b`	Display in batch format.
`-help`[1]	Display command usage and options. The -help option is placed before the command, for example `asu -help show`.
`-l`	Long format setting name (include the configuration set).

Table 21. asu options (continued)

Option	Description
`-m`	Mixed format setting name (use the configuration id).
`-v`[2]	Verbose output.
1. The `-help` option can be used with any command. 2. The `-v` option is used only between `asu` and the command.	

Syntax:

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

Note: See individual commands for more command options.

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

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

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

Table 22. asu transaction commands

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

Command	Description	Value
`tropen` **id**	This command creates a new transaction file containing several settings to be set.	**Id** is the identifying string, 1 - 3 alphanumeric characters.
`trset` **id**	This command adds one or more settings or value pairs to a transaction.	**Id** is the identifying string, 1 - 3 alphanumeric characters.
`trlist` **id**	This command displays the contents of the transaction file first. This can be useful when the transaction file is created in the CLI shell.	**Id** is the identifying string, 1 - 3 alphanumeric characters.
`trcommit` **id**	This command commits and executes the contents of the transaction file. The results of the execution and any errors will be displayed.	**Id** is the identifying string, 1 - 3 alphanumeric characters.
`trrm` **id**	This command removes the transaction file after it has been committed.	**Id** is the identifying string, 1 - 3 alphanumeric characters.

Example of establishing multiple UEFI settings:

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

backup command

Use this command to create a backup file containing the current system security settings.

Syntax:

```
backup [-options]
```

Table 23. backup options

Option	Description	Values
-f	Filename of backup file	Valid filename
-pp	Password or quote delimited phrase used to encrypt the passwords inside the backup file	Valid password or quote-delimited pass-phrase
-ip	IP address of TFTP/SFTP server	Valid IP address
-pn	Port number of TFTP/SFTP server	Valid port number (default 69/22)
-u	Username for SFTP server	Valid user name
-pw	Password for SFTP server	Valid password
-fd	Filename for XML description of backup CLI commands	Valid filename

Example:

```
system> backup -f xcc-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

dhcpinfo command

Use this command to view the DHCP server-assigned IP configuration for eth0.

Use the `dhcpinfo` command to view the DHCP server-assigned IP configuration for eth0, if the interface is configured automatically by a DHCP server. You can use the `ifconfig` command to enable or disable DHCP.

Syntax:

```
dhcpinfo [ethernet_number]
```

Example:

```
dhcpinfo eth1
```

The following table describes the output from the example.

Table 24. dhcpinfo output

Field	Description
`-server`	DHCP server that assigned the configuration
`-n`	Assigned host name
`-i`	Assigned IPv4 address
`-i6`	Assigned IPv6 address
`-g`	Assigned gateway address
`-s`	Assigned subnet mask
`-d`	Assigned IPv4 domain name
`-d6`	Assigned IPv6 domain name
`-dns1`	Primary IPv4 DNS server IP address
`-dns2`	Secondary IPv4 DNS IP address
`-dns3`	Tertiary IPv4 DNS server IP address
`-i6`	IPv6 address
`-d6`	IPv6 domain name
`-dns61`	Primary IPv6 DNS server IP address
`-dns62`	Secondary IPv6 DNS IP address
`-dns63`	Tertiary IPv6 DNS server IP address

dns command

Use this command to view and set the DNS configuration of the IMM.

Syntax:

```
dns [-options]
```

Table 25. dns options

Option	Description	Values
`-state`	State of DNS	`on`, `off`
`-i1`	Primary IPv4 DNS server IP address	IP address in dotted decimal IP address format.
`-i2`	Secondary IPv4 DNS IP address	IP address in dotted decimal IP address format.
`-i3`	Tertiary IPv4 DNS server IP address	IP address in dotted decimal IP address format.
`-i61`	Primary IPv6 DNS server IP address	IP address in IPv6 format.
`-i62`	Secondary IPv6 DNS IP address	IP address in IPv6 format.
`-i63`	Tertiary IPv6 DNS server IP address	IP address in IPv6 format.
`-ddns`	State of DDNS	`enabled`, `disabled`
`-dnsrc`	Preferred DDNS domain name	`dhcp`, `manual`
`-ddn`	Manually specified DDN	
`-ddncur`	Current DDN (read only)	

Table 25. dns options (continued)

Option	Description	Values
`-p`	Preferred DNS servers	`ipv4`, `ipv6`
`-dscvry`	discovery of LXCA addresses	`enabled`, `disabled`
`-dsclist`	LXCA list of DNS SRV	
`-dscxm`	Configure the XClarity Manager	

The following example shows an IMM configuration where DNS is disabled:

```
system> dns
   -state    :  disabled
   -i1       :  0.0.0.0
   -i2       :  0.0.0.0
   -i3       :  0.0.0.0
   -i61      :  ::
   -i62      :  ::
   -i63      :  ::
   -ddns     :  enabled
   -dnsrc    :  DHCP
   -ddn      :
   -ddncur   :  labs.lenovo.com
   -p        :  ipv6
   -dscvry   :  enabled
system>
```

encaps command

Use this command to let the BMC quit encapsulation mode.

Syntax:

```
encaps [arguments]
```

Table 26. encaps arguments

Arguments	Description
`lite off`	Let BMC quit encapsulation mode and open global access to all users

ethtousb command

Use the **ethtousb** command to display and configure Ethernet to Ethernet-over-USB port mapping.

The command allows you to map an external Ethernet port number to a different port number for Ethernet-over-USB.

Syntax:

```
ethtousb [-options]
```

Table 27. ethtousb command

Option	Description	Values
`-en`	Ethernet-over-USB state.	`enabled`, `disabled` **Note:** Enable Ethernet over USB interface via `usbeth` to make port mapping effective.
`-m[x]` **port1:port2**	Configure port mapping for index **x**.	Where: • The port index number, **x**, is specified as an integer from 1 to 10 in the command option. • **port1** of the port pair is the External Ethernet port number. • **port2** of the port pair is the Ethernet-over-USB port number.
`-rm` **map_ index**	Remove port mapping for specified index.	The port index number, **map_index**, is specified as an integer from 1 to 10 in the command option. **Note:** Port map indexes are displayed using the `ethtousb` command with no options.

Example:

```
system> ethtousb -en enabled -m1 100:200 -m2 101:201
system> ethtousb
        ethtousb : On
        ===============
         1:   100:  200
         2:   101:  201
system>
```

firewall command

Use this command to configure the firewall to restrict access from certain addresses and optionally limits access time frame. If no option is specified, the current settings will be displayed.

Syntax:

```
firewall [-options]
```

Table 28. firewall options

Option	Description	Values
The following option is for IP address whitelist		
`-wips`	Show/configure the whitelist IP addresses.	• **Valid IP addresses**: Permit 1-3 IP addresses (comma separated, CIDR or range) **Note:** IPv4 and IPv6 addresses can use CIDR format to block a range of addresses. • `-clr`: Clear the whitelist
The following options are for Block List and Time Restriction		
`-bips`	Block 1-3 IP addresses (comma separated, CIDR or range)	Valid IP addresses **Note:** IPv4 and IPv6 addresses can use CIDR format to block a range of addresses.
`-bmacs`	Block 1-3 MAC addresses (comma separated)	Valid MAC addresses **Note:** MAC address filtering works only with specific addresses.

Table 28. firewall options (continued)

Option	Description	Values
`-bbt`	Block begin time, must be later than current time	Time with format <YYYY-MM-DD HH:MM>
`-bet`	Block end time, must be later than begin time	Time with format <YYYY-MM-DD HH:MM>
`-bti`	Block 1-3 time intervals (comma separated) e.g., **firewall - bti 01:00–02:00,05:05–10:30** will block access during 01:00-02:00 & 05:05-10:30 every day	Time range with format <HH:MM-HH:MM>
`-clr`	Clear the firewall rule for a given type	`ip`, `mac`, `datetime`, `interval`, `all`
The following options are for IP address blocking		
`-iplp`	IP address lockout period in minutes.	Numeric value between 0 and 2880, 0 = never expire
`-iplf`	Maximum number of login failures before IP address is locked out.	Numeric value between 0 and 32, 0 = never lock **Note:** If this value is not 0, then it must be greater than or equal to **Maximum number of login failures** that is set by `accseccfg -lf`
`-ipbl`	Show/configure the list of IP addresses being locked out.	• `-del`: delete an IPv4 or IPv6 address from block list • `-clrall`: clear all blocking IP • `-show`: show all blocking IPs

Examples of the syntax for the `firewall` command are presented in the following list:

- To show all options' value and IP addresses blocking list enter `firewall`.
- To block the access from multi IPs enter `firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5`.
- To block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day enter `firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00`.
- To clear all rules of Block List and Time Restriction enter `firewall –clr all`.
- To set IP address lockout period to 60 minutes enter `firewall -iplp 60`.
- To set maximum number of login failures to 5 times enter `firewall -iplf 5`.
- To delete 192.168.100.1 from IP address blocking list enter `firewall -ipbl -del 192.168.100.1`.
- To delete 3fcc:1234::2 from IP address blocking list enter `firewall –ipbl -del 3fcc:1234::2`.
- To delete all blocking IP addresses enter `firewall –ipbl –clrall`.
- To show all blocking IP addresses enter `firewall –ipbl –show`.

gprofile command

Use this command to display and configure group profiles for the IMM.

Syntax:

```
gprofile [1 - 16 group_profile_slot_number] [-options]
```

Table 29. gprofile options

Option	Description	Values
`-[1–16]`	Group profile slot number	1–16
`-clear`	Delete a group based on the index	
`-n [group_name]`	The name of the group	String of up to 64 characters for `group_name`. The `group_name` must be unique.
`-r [role_name]`	Role name as listed in roles command	
`-d [group_name]`	Group domain (use root dn by default if group domain is not set)	
`-h`	Display the command usage and options	

Syntax:

```
system> gprofile -1 -n name -r Administrator -d domain
ok
system> gprofile
1. name
   Role:Administrator
   Domain:domain

system> gprofile -1
-n name
-r Role:Administrator
-d Domain:domain
system> gprofile -clear
Invalid group index: -clear
system> gprofile -1 -clear
ok
system> gprofile
No groups found
```

hashpw command

Use this command with the -sw option to enable/disable the third-party password function or with the -re option to enable/disable the allowance of retrieving third-party password.

Syntax:

```
hashpw [-options]
```

Table 30. hashpw options

Option	Description	Values
`-sw`	Third-Party Password switch status	`enabled`, `disabled`
`-re`	Third-Party Password read status **Note:** Read can be set if the switch is enabled.	`enabled`, `disabled`

Example:

```
system> hashpw –sw enabled –re enabled
system> users -5 –n guest5 –shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f – r Administrator
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
```

```
system> users
Account       Login ID      Advanced Attribute             Role                Password Expires
-------       --------       ------------------              ------              ----------------
1             USERID         Native                         Administrator      Password doesn't expire
5             guest5         Third-party Password          Administrator      90 day(s)
```

ifconfig command

Use this command to configure the Ethernet interface.

Use the `ifconfig` command 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.

Syntax:

```
ifconfig [ethernet_number] [-options]
```

Example:

```
dhcpinfo eth1 -b
```

Table 31. ifconfig 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)
`-ghn`	Obtain hostname from DHCP	`disabled`, `enabled`
`-i`	Static IP address	Address in valid format.
`-g`	Gateway address	Address in valid format.
`-s`	Subnet mask	Address in valid format.
`-n`	Host name	String of up to 63 characters. The string can include letters, digits, periods, underscores, and hyphens.
`-auto`	Autonegotiation setting, which determines whether the Data rate and Duplex network settings are configurable	`true`, `false`
`-vlan`	Enable or disable the VLAN tagging	`enabled`, `disabled`
`-vlanid`	VLAN ID	Numeric value between 1 and 4094.
`-r`	Data rate	`10`, `100`, `1000`
`-d`	Duplex mode	`full`, `half`
`-m`	MTU	Numeric between 60 and 1500.
`-l`	LAA	MAC address format. Multicast addresses are not allowed (the first byte must be even).
`-b`	Burned-in MAC Address (read only)	
`-dn`	Domain name (read only)	
`-ipv6`	IPv6 state	`disabled`, `enabled`
`-ipv6static`	Static IPv6 state	`disabled`, `enabled`

Table 31. ifconfig options (continued)

Option	Description	Values
`-i6`	Static IP address	Static IP address for Ethernet channel 0 in IPv6 format.
`-p6`	Address prefix length	Numeric value between 1 and 128.
`-g6`	Gateway or default route	IP address for the gateway or default route for Ethernet channel 0 in IPv6.
`-dhcp6`	IPv6 DHCP mode	`enabled`, `disabled`
`-sa6`	IPv6 Stateless mode	`enabled`, `disabled`
`-lla`	Link-local address (read only)	
`-ncsi`	NCSI NIC port selection	`nic[x]:port[y]` **Note:** Use comma as the delimiter if there are two or more settings.
`-nic`	Switch NIC mode[1]	`shared`, `dedicated`, `shared:nic[x]`[2]
`-failover`[2]	Failover mode	`none`, `shared`, `shared:nic[x]`
`-nssync`[3]	Network setting synchronization	`enabled`, `disabled`
`-address_table`	Table of automatically-generated IPv6 addresses and their prefix lengths (read only) **Note:** The option is visible only if IPv6 and stateless auto-configuration are enabled.	

Notes:

1. `-nic` will also show the status of nic. [active] indicates which nic XCC is currently using.

   For example:
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   Indicates that nic3 is in shared mode, on slot 5, nic2 is on slot3, nic1 is XCC dedicated port and XCC is using nic3.
2. The shared:nic[x] value is available on servers that have an optional mezzanine network card installed. This mezzanine network card can be used by the IMM.
3. If the IMM is configured to use the dedicated management network port, the -failover option will direct the IMM to switch to the shared network port if the dedicated port is disconnected.
4. If the failover mode is enabled, the -nssync option directs the IMM to use the same network settings that are used on the dedicated management network port for the shared network port.

Example:

```
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

keycfg command

Use this command to display, add, or delete activation keys.

Activation keys control access to optional IMM functionality.

Notes:

- Add new activation keys through file transfer.
- Delete old keys by specifying the number of the key or the type of key. When deleting keys by type, only the first key of a given type is deleted.

Syntax:

```
keycfg [-options]
```

Table 32. keycfg options

Option	Description	Values
`-add`	Add activation key	• `-ip`: IP address of TFTP/SFTP server with activation key to add • `-pn`: Port number for TFTP/SFTP server with activation key to add (default 69/22) • `-u`: User name for SFTP server with activation key to add • `-pw`: Password for SFTP server with activation key to add • `-f`: Filename for activation key to add
`-del`	Delete activation key by index number	Valid activation key index number from `keycfg` listing
`-deltype`	Delete activation key by key type	Valid key type value

When the `keycfg` command is run without any options, the list of installed activation keys is displayed. Key information displayed includes an index number for each activation key, the type of activation key, the date through which the key is valid, the number of uses remaining, the key status, and a key description.

Example:

```
system> keycfg
ID  Type  Valid           Uses           Status    Description
1   4     10/10/2010      5                "valid"   "IMM remote presence"
2   3     10/20/2010      2                "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

Note: The **Description** field for ID number 3 is displayed on separate lines due to space limitations.

ldap command

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

Syntax:

```
ldap [-options]
```

Table 33. ldap options

Option	Description	Values
`-aom`	Authentication only mode for Active Directory Users	`enabled`, `disabled`
`-a`	User authentication method	• `loc`: local only • `ldap`: LDAP only • `locld`: local first then LDAP • `ldloc`: LDAP first then local

Table 33. ldap options (continued)

Option	Description	Values
-b	Binding method	• anon: anonymous • client: bind with ClientDN and password • login: bind with Login Credential
-c	Client distinguished name	String of up to 127 characters for **client_dn**
-d	Search domain	String of up to 63 characters for **search_domain**
-fn	Forest name	For active directory environments. String of up to 127 characters.
-f	Group filter	String of up to 127 characters for **group_filter**
-g	Group search attribute	String of up to 63 characters for **group_search_attr**
-l	Login permission attribute	String of up to 63 characters for **string**
-p	Client password	String of up to 15 characters for **client_pw**
-pc	Confirm client password	String of up to 15 characters for **confirm_pw** Command usage is: ldap -p **client_pw** -pc **confirm_pw** This option is required when you change the client password. It compares the **confirm_pw** argument with the **client_pw** argument. The command will fail if the arguments do not match.
-r	Root entry distinguished name (DN)	String of up to 127 characters for **root_dn**
-s1ip	Server 1 host name/IP address	String up to 127 characters or an IP address for **host name/ip_addr**
-s2ip	Server 2 host name/IP address	String up to 127 characters or an IP address for **host name/ip_addr**
-s3ip	Server 3 host name/IP address	String up to 127 characters or an IP address for **host name/ip_addr**
-s4ip	Server 4 host name/IP address	String up to 127 characters or an IP address for **host name/ip_addr**
-s1pn	Server 1 port number	A numeric port number up to 5 digits for **port_number**
-s2pn	Server 2 port number	A numeric port number up to 5 digits for **port_number**
-s3pn	Server 3 port number	A numeric port number up to 5 digits for **port_number**
-s4pn	Server 4 port number	A numeric port number up to 5 digits for **port_number**
-u	User's login name search attribute	String of up to 63 characters for **search_attrib**
-v	Get LDAP server address through DNS	off, on
-h	Displays the command usage and options	

Example:

```
system> ldap
   -aom enable
   -a   locld
   -b   client
   -c    cn=admin,dc=lenovo,dc=com
   -d
   -fn
   -f    example.com
   -g    cn
   -l    XCC3RBSPermissions
   -r
   -s1ip 10.241.99.94
   -s2ip
   -s3ip
   -s4ip
   -s1pn 389
   -s2pn 389
   -s3pn 389
   -s4pn 389
   -u uid
   -v off
system>
```

lldp command

Use this command to display and set lldp.

Use the `lldp` command to display and configure link layer discovery protocol (LLDP). The following table shows the arguments for the options

Syntax:

```
led [-options]
```

Table 34. led options

Option	Description	Values
`-en`	Enable or disable LLDP transmit. **Note:** If the machine has two network ports, enable/disable will operate on both ports simultaneously, and local port and peer information will also display information for multiple ports separately.	`enable`, `disable`

Example:

```
system> lldp
-en: disabled

system> lldp -en enabled
ok
system> lldp
-en: enabled

Local Port:          eth1
Local Addresses:     MAC: c4:c6:e6:80:49:fc; IPv4: 10.240.218.128;  IPv6: fe80::c6c6:e6ff:fe80:49fc

Peer Discover:
System Name:           LNSHx11-ConvSw45-1.lenovo.com
Chassis Id:
Management Address:  10.240.192.19
System Description:  Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Soft-ware (cat4500es8-UNIVERSAL-M), Version
Port Description:    GigabitEthernet2/29

Local Port:          eth2.1
Local Addresses:     MAC: c4:c6:e6:80:49:ff; IPv4: 192.168.70.126;  IPv6: fe80::c6c6:e6ff:fe80:49ff

Peer Discover:
System Name:
Chassis Id:
Management Address:
System Description:
Port Description:
```

ntp command

Use this command to display and configure the Network Time Protocol (NTP).

Syntax:

```
ntp [-options]
```

Table 35. ntp command

Option	Description	Values
`-en`	Enables or disables the Network Time Protocol.	`enabled`, `disabled`
`-i[x]`	Name or IP address of the Network Time Protocol server for index **x**.	The name of the NTP server to be used for clock synchronization. The range of the index number of the NTP server is from -i1 through -i4. **Note:** -i is the same as i1.
`-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
```

portcontrol command

Use this command to turn a network service port on or off.

Syntax:

```
portcontrol [-options]
```

Table 36. portcontrol options

Option	Description	Values
`-ipmi`	Enable or disable the ipmi access via LAN	`on`, `off`
`-ipmi-kcs`	Enable on demand, enable, or disable ipmi access from server	`auto`, `on`, `off`
`-rest`	Enable or disable REST discovery	`on`, `off`

Table 36. portcontrol options (continued)

Option	Description	Values
`-snmp`	Enable or disable SNMP discovery	`on`, `off`
`-ssdp`	Enable or disable SSDP discovery	`on`, `off`
`-cli`	Enable or disable CLI discovery	`on`, `off`
`-web`	Enable or disable WEB discovery	`on`, `off`
`-all`	Enable or disable all interfaces and discovery protocols	`on`, `off`

Example:

```
system> portcontrol
ipmi : on
ipmi-kcs : on
rest : on
snmp : off
ssdp : on
cli : on
web : on
system>
```

ports command

Use this command to display and configure IMM ports.

Syntax:

```
ports [-options]
```

Table 37. ports options

Option	Description	Values
`-open`	Display open ports (read only)	
`-reset`	Reset ports to default settings (read only)	
`-http`	HTTP port number	Default port number: 80
`-https`	HTTPS port number	Default port number: 443
`-ssh`	SSH legacy CLI port number	Default port number: 22
`-snmpa`	SNMP agent port number	Default port number: 161
`-snmpt`	SNMP traps port number	Default port number: 162
`-rp`	Remote presence port number	Default port number: 3900

Example:

```
system> ports
  -http 80
  -https 443
  -rp 3900
  -snmpa 161
  -snmpt 162
  -ssh 22
system>
```

rdmount command

Use this command to mount remote disk images or network shares

Notes:

- Up to two files can be uploaded in the XClarity Controller memory and mounted as virtual media using the XClarity Controller RDOC feature. The total size for both files must not exceed 50 MB. The uploaded images are read only unless the `-rw` option is used.
- When using the HTTP, SFTP, or FTP protocols to mount or map the images, the total size for all the images must not exceed 50 MB. There is no size limit if the NFS or SAMBA protocols are used.

Syntax:
`rdmount [-options]`

Table 38. rdmount options

Option	Description
`-r`	rdoc operation (if used, must be first option) • `-r -map`: mount the RDOC images • `-r -unmap <filename>`: unmount the mounted RDOC images • `-r -maplist`: shows the mounted RDOC images via the XClarity Controller web browser and the CLI interface
`-map`	• `-t <samba|nfs|http|sftp|ftp>`: filesystem type • `-ro`: read-only • `-rw`: read-write • `-u`: user • `-p`: password • `-l`: file location (URL format) • `-o`: option (extra option string for samba and nfs mounts) • `-d`: domain (domain for samba mount)
`-maplist`	Shows the mapped images
`-unmap`	• `id`: use id with network images • `fname`: use filename with rdoc
`-mount`	Mount the mapped images
`-unmount`	Unmount the mounted images

restore command

Use this command to restore system settings from a backup file.

Syntax:
`restore [-options]`

Table 39. restore options

Option	Description	Values
`-f`	Backup file name	Valid file name
`-pp`	Password or pass-phrase used to encrypt passwords inside the backup file	Valid password or quote-delimited pass-phrase
`-ip`	IP address of TFTP/SFTP server	Valid IP address
`-pn`	Port number of TFTP/SFTP server	Valid port number (default 69/22)
`-u`	Username for SFTP server	Valid user name
`-pw`	Password for SFTP server	Valid password

Example:

```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

roles command

Use this command to display or configure roles.

Syntax:

```
roles role_account[3-31] [-options]
```

Table 40. roles options

Option	Description	Values
`-n`	Role name	Limited to 32 characters
`-p`	Set privileges	`custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us` • `am`: User account management access • `rca`: Remote console access • `rcvma`: Remote console and remote disk (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) • `us`: UEFI Security **Note:** The above custom permission flags can be used in any combination
`-d`	Delete a row	

Example:

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok
```

```
system> roles
Account               Role                             Privilege                    Assigned To
------- -----------------------------------    --------------------------     --------------------------------
    0                    Administrator         all                         USERID
    1                         ReadOnly          none
    2                         Operator          custom:pr|cel|bc|nsc
    3                            test1           custom:am|rca|rcvma
```

rtd command

Use this command to restore all BMC settings to the factory default.

Note: This command used to be `restoredefaults` and `clearcfg` command.

Syntax:

```
rtd [-options]
```

Table 41. rtd options

Option	Description
`-all`	Reset all BMC settings to factory defaults.
`-eu`	Reset all BMC Settings to factory defaults except user Settings
`-en`	Reset all BMC Settings to factory defaults except network Settings.
`-eun`	Reset all BMC Settings to factory defaults except user and network Settings.

Example:

```
system> rtd -all

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

seccfg command

Use this command to perform firmware rollback.

Syntax:

```
seccfg [-options]
```

Table 42. seccfg options

Option	Description	Value
`-fwrb`	Allows firmware rollback to previous versions.	`enabled`, `disabled`
`-aubp`	Enable or disable the function of auto backup to primary promotion.	`enabled`, `disabled`

securityinfo command

This command is used to display security related information.

Syntax:
```
securityinfo [-options]
```

Table 43. securityinfo options

Option	Description
`-event`	Display security events.
`-cryptomode`	Display security cryptomode status.
`-service`	Display security status of services and ports.
`-cert`	Display security status of the certificate.
`-account`	Display security status of user accounts.

securitymode command

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

Syntax:
```
securitymode [-options]
```

Table 44. securitymode options

Option	Description	Values
`-mode`	Selects the security mode. • CNSA - Enterprise Strict • FIPS - Standard • COMPAT- Compatibility	• `CNSA`: Only services that support enterprise strict level cryptography are allowed; requires Feature on Demand Key to enable. • `FIPS`: Services that require cryptography that do not support standard level cryptography are disabled by default. • `COMPAT`: When this mode is enabled, XCC is NOT operating in standard-validated mode; allows all services to be enabled.
`-h`	List usage and options.	

set command

Use this command to change some IMM settings.

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

The following table shows the arguments for the options.

Table 45. set command

Option	Description	Values
value	Set value for specified path or setting	Appropriate value for specified path or setting.

Syntax:

```
set [-options]
option:
  value
```

snmp command

Use this command to display and configure SNMP interface information.

Syntax:

```
snmp [-options]
```

Table 46. snmp options

Option	Description	Values
`-a3`	SNMPv3 agent	`on`, `off` **Notes:** To enable the SNMPv3 agent, the following criteria must be met: • IMM contact specified using the -cn command option. • IMM location specified using the -l command option.
`-t`	SNMPv3 traps	`on`, `off`
`-tn`	SNMPv3 trap user name	Valid user name
`-tauth`	SNMPv3 trap authentication protocol	`none`, `HMAC-SHA`
`-tapw`	SNMPv3 trap authentication password	Valid password
`-tpriv`	SNMPv3 trap privacy protocol	`none`, `CBC-DES`, `AES`
`-tppw`	SNMPv3 trap privacy password	Valid password
`-tix`	Community IP address or host name **x**	Valid IP address or hostname (limited to 63 characters, **x** can range 1 to 3). **Notes:** • An IP address or host name can only contain dots, underscores, minus signs, letters and digits. No embedded spaces or consecutive periods are allowed. • Clear an community IP address or host name by specifying no argument.
`-l`	IMM location	String (limited to 47 characters). **Notes:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear the IMM location by specifying no argument or by specifying an empty string as the argument, such as `""`.
`-cn`	IMM contact name	String (limited to 47 characters). **Notes:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear the IMM contact name by specifying no argument or by specifying an empty string as the argument, such as `""`.

Table 46. snmp options (continued)

Option	Description	Values
`-t1`	SNMPv1 traps	`on`, `off`
`-c`	SNMP community name	String (limited to 15 characters). **Notes:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear an SNMP community name by specifying no argument or by specifying an empty string as the argument, such as "".
`-ci`	Community IP address/host name 1	Valid IP address or hostname (limited to 63 characters). **Notes:** • An IP address or host name can only contain dots, underscores, minus signs, letters and digits. No embedded spaces or consecutive periods are allowed. • Clear an community IP address or host name by specifying no argument.
`-c1iy`	Community IP address/host name **y**	Valid IP address or hostname (limited to 63 characters, **y** can range 2 or 3). **Notes:** • An IP address or host name can only contain dots, underscores, minus signs, letters and digits. No embedded spaces or consecutive periods are allowed. • Clear an community IP address or host name by specifying no argument.
`-t2`	SNMPv2 traps	`on`, `off`
`-ct`	SNMPv2 trap community name	String (limited to 15 characters). **Notes:** • Arguments containing spaces must be enclosed in quotation marks. No leading or trailing spaces are allowed in arguments. • Clear the IMM contact name by specifying no argument or by specifying an empty string as the argument, such as "".
`-cti`	SNMPv2 trap community IP address/hostname 1	Valid IP address or hostname (limited to 63 characters). **Notes:** • An IP address or host name can only contain dots, underscores, minus signs, letters and digits. No embedded spaces or consecutive periods are allowed. • Clear an SNMP community IP address or host name by specifying no argument.
`-eid`	SNMP engine id	String (limited 1 to 27 characters)
`-send`	Send a test trap information	

Example:

```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
```

```
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

snmpalerts command

Use this command to manage alerts sent via the SNMP.

Syntax:
`snmpalerts [-options]`

Table 47. snmpalerts options

<table>
<tr><th>Option</th><th>Description</th><th>Values</th></tr>
<tr><td>-status</td><td>SNMP alert status</td><td>on, off</td></tr>
<tr><td>-crt</td><td>Sets critical events that send alerts</td><td>all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot|pc
Custom critical alert settings are specified using a pipe separated list of values of the form snmpalerts -crt custom:te|vo, where custom values are:
• te: critical temperature threshold exceeded
• vo: critical voltage threshold exceeded
• po: critical power failure
• di: hard disk drive failure
• fa: fan failure
• cp: microprocessor failure
• me: memory failure
• in: hardware incompatibility
• re: power redundancy failure
• ot: all other critical events
• pc: PCIe critical events</td></tr>
</table>

Table 47. snmpalerts options (continued)

Option	Description	Values
`-wrn`	Sets warning events that send alerts	`all`, `none`, `custom:rp|te|vo|po|fa|cp|me|ot|pw` Custom warning alert settings are specified using a pipe separated list of values of the form `snmpalerts -wrn custom:rp|te`, where custom values are: • `rp`: power redundancy warning • `te`: warning temperature threshold exceeded • `vo`: warning voltage threshold exceeded • `po`: warning power threshold exceeded • `fa`: non-critical fan event • `cp`: microprocessor in degraded state • `me`: memory warning • `ot`: all other warning events • `pw`: PCIe warning events
`-sys`	Sets routine events that send alerts	`all`, `none`, `custom:lo|tio|ot|po|bf|til|pf|el|ne|nl|dh|oa` Custom routine alert settings are specified using a pipe separated list of values of the form `snmpalerts -sys custom:lo|tio`, where custom values are: • `lo`: successful remote login • `tio`: operating system timeout • `ot`: all other informational and system events • `po`: system power on/off • `bf`: operating system boot failure • `til`: operating system loader watchdog timeout • `pf`: predicted failure (PFA) • `el`: event log 75% full • `ne`: network change • `nl`: host NIC link down/up • `dh`: drive hotplug • `oa`: all other audit events

sshcfg command

Use this command to display and configure SSH parameters.

Syntax:

```
sshcfg [-options]
```

Table 48. sshcfg options

Option	Description	Values
`-cstatus`	State of SSH CLI	`enabled`, `disabled`
`-hk`	Server key	• `gen`: Generate SSH server private key • `all`: Display server public key

Example:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

sslcfg command

Use this command to display and configure the SSL for the IMM and manage certificates.

The `sslcfg` command is used to generate a new encryption key and self-signed certificate or certificate signing request (CSR).

Syntax:

```
sslcfg [-options]
```

Table 49. sslcfg options

Option	Description	Values
`-server`	Web over HTTPS status	`enabled`, `disabled` **Notes:** • Web over HTTPS can only be enabled if a certificate is in place. • Use `-rm` to completely disable the certificate.
`-client`	Secure LDAP status	`enabled`, `disabled` **Note:** The SSL client can be enabled only if a valid server or client certificate is in place.
`-cert`	Generate self-signed certificate	`server`, `client`, `sysdir`, `storekey` **Notes:** • Values for the `-c`, `-sp`, `-cl`, `-on`, and `-hn` command options are required when generating a self-signed certificate. • Values for the `-cp`, `-ea`, `-ou`, `-s`, `-gn`, `-in`, and `-dq` command options are optional when generating a self-signed certificate.
`-csr`	Generate a CSR	`server`, `client`, `sysdir`, `storekey` **Notes:** • Values for the `-c`, `-sp`, `-cl`, `-on`, and `-hn` command options are required when generating a CSR. • Values for the `-cp`, `-ea`, `-ou`, `-s`, `-gn`, `-in`, `-dq`, `-cpwd`, and `-un` command options are optional when generating a CSR.
`-form`	Format of the CSR or certificate that will be exported.	`der`, `pem` (default pem)
`-algo`	CSR algorithm	`p256`, `p384`, `rsa2048`, `rsa3072`, `rsa4096` **Note:** A default value (p256) will be set if there is not a `-algo` option.
`-rm`	Remove the certificate	`server`, `storekey` **Note:** A default self-signed certificate (server) would be generated automatically after the current one is removed.
`-i`	IP address for TFTP/SFTP server	Valid IP address **Note:** An IP address for the TFTP or SFTP server must be specified when uploading a certificate, or downloading a certificate or CSR.

Table 49. sslcfg options (continued)

Option	Description	Values
`-pn`	Port number of TFTP/SFTP server	Valid port number (default 69/22)
`-u`	User name for SFTP server	Valid user name
`-pw`	Password for SFTP server	Valid password
`-l`	Certificate filename	Valid filename **Note:** A filename is required when downloading or uploading a certificate or CSR. If no filename is specified for a download, the default name for the file is used and displayed.
`-dnld`	Exports the specified file to the remote host	This option takes no arguments; but must be used with `-cert` or `-csr`; as well as `-i`, and `-l` command options.
`-upld`	Imports certificate file	This option takes no arguments, but must also specify values for the `-cert`, `-i`, and `-l` command options.
`-tc[x]`	Trusted certificate **x** for SSL client	import, download, remove **Note:** The trusted certificate number, **x**, is specified as an integer from 1 to 4 in the command option.
Required options for generating a self-signed certificate or CSR **Note:** Required when generating a self-signed certificate or CSR.		
-c	Country	Country code (2 letters)
-sp	State or province	Quote-delimited string (maximum 60 characters)
-cl	City or locality	Quote-delimited string (maximum 50 characters)
-on	Organization name	Quote-delimited string (maximum 60 characters)
-hn	BMC host name	String (maximum 60 characters)
Optional options for generating a self-signed certificate or CSR **Note:** Optional when generating a self-signed certificate or CSR.		
-cp	Contact person	Quote-delimited string (maximum 60 characters)
-ea	Contact person email address	Valid email address (maximum 60 characters)
-ou	Organizational unit	Quote-delimited string (maximum 60 characters)
-s	Surname	Quote-delimited string (maximum 60 characters)
-gn	Given name	Quote-delimited string (maximum 60 characters)
-in	Initials	Quote-delimited string (maximum 20 characters)
-dq	Domain name qualifier	Quote-delimited string (maximum 60 characters)
Optional options for generating a CSR **Note:** Optional when generating a CSR.		
-cpwd	Challenge password	String (minimum 6 characters, maximum 30 characters)
-un	Unstructured name	Quote-delimited string (maximum 60 characters)

Examples:

```
system> sslcfg
-server enabled
-client disabled
```

```
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

Client certificate examples:

- To generate a CSR for a storage key, enter the following command:

```
system> sslcfg -csr storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou""
ok
```

- To download a certificate from the IMM to another server, enter the following command:

```
system> sslcfg -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
ok
```

- To upload the certificate processed by the Certificate Authority (CA), enter the following command:

```
system> sslcfg -cert storekey -upld -i 192.168.70.230 -l tklm.der
```

- To generate a self-signed certificate, enter the following command:

```
system> sslcfg -cert storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou "
ok
```

SKLM Server certificate example:

- To import the SKLM server certificate, enter the following command:

```
system> storekeycfg -add -ip 192.168.70.200 -f tklm-server.der
ok
```

syslock command

Use this command to display and configure system lockdown settings.

Syntax:

```
syslock [-options]
```

Table 50. syslock options

Option	Description	Values
`-en`	Enable or disable system configuration lock function. **Note:** Enable with **-e** option can promote the current inventory as trusted snapshot.	`enabled`, `disabled`
`-e`	Enable system configuration lock settings with or without enforcing current inventory into trusted snapshot. **Note:** A default value will be set if there is not a **-e** option.	`enabled`, `disabled`
`-l [x]`	List inventory of specific snapshot at index **x**.	The index number, x, is specified as an integer in the command option.

Table 50. syslock options (continued)

Option	Description	Values
`-m`	Take manual snapshot.	
`-d`	Description for manual snapshot.	String of up to 32 characters.
`-c`	List inventory difference from trusted snapshot.	
`-po`	Set lockdown policy. **Note:** The action will prevent server booting if System Guard is in noncompliant status.	`none`, `osboot`, `pperm`
`-cpu`	Set cpu lockdown.	`on`, `off`
`-dimm`	Set dimm lockdown.	`on`, `off`
`-pci`	Set pci lockdown.	`on`, `off`
`-drive`	Set drive lockdown.	`on`, `off`
`-riser`	Set riser lockdown.	`on`, `off`
`-bp`	Set bp lockdown.	`on`, `off`

syncrep command

Use this command to launch firmware sync from remote repository.

Syntax:

```
syncrep [-options]
```

Table 51. syncrep options

Option	Description	Values
`-t`	Protocol to connect repository **Note:** System might reboot for a variable duration depending on the amount and type of updates to be applied.	`samba`, `nfs`
`-l`	Location of remote repository	URL format
`-u`	User	
`-p`	Password	
`-o`	Option **Note:** To use a lower version of SMB protocol, option `vers` should be specified (Example, `syncrep -t samba -l url -u user -p password -o vers=1.0`). By default, SMB3 is used.	Extra option string for samba and nfs mounts
`-d`	Domain	Domain for samba mount
`-q`	Query current update status	
`-c`	Cancel the sync process	
`-r [repo_index]`	Firmware rollback	
`-gl`	Get repository list	

Example

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password

(2) query current update status
system> syncrep -q

(3) cancel the sync process
system> syncrep -c

(4) rollback
system> syncrep -gl
index    BundleID                  Timestamp
---------------------------------------------------------------------
0         current                   2021-08-15 10:26:48
N-1
```

thermal command

Use this command to display and configure the thermal mode policy of the host system.

Running the `thermal` command with no options displays the thermal mode policy. The following table shows the arguments for the options.

Syntax:

```
thermal [-options]
```

Table 52. thermal options

Option	Description	Values
`-mode`	Display the thermal mode policy and configures the thermal table of the host systems (read only)	• General Computing - Power Efficiency • General Computing - Peak Frequency • General Computing - Max Performance • Virtualization - Power Efficiency • Virtualization - Max Performance • Database - Transaction Processing • Low Latency • High Performance Computing • Custom • Unknown
`-table [table_ number]`	**table_number** specifies which alternate thermal table to use.	1 = Low: Slight boost in fan speed 2 = Medium: Moderate boost in fan speed 3 = High: Large boost in fan speed 0 = Normal: No fan speed boost

Example:

```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

tls command

Use this command to set the minimum TLS level.

Syntax:

```
tls [-options]
```

Table 53. tls options

Option	Description	Values
`-min`	Select the minimum TLS level	`1.2, 1.3` **Note:** When the cryptography mode is set to the NIST-800-131A Compliance mode, the TLS version must be set to 1.2.
`-h`	List the usage and options	
Notes: 1. When the cryptography mode is set to the NIST-800-131A Compliance mode, the TLS version must be set to 1.2.		

Examples:

To get the usage for the tls command, issue the following command:

```
system> tls
-h
system>
```

To obtain the current tls version, issue the following command:

```
system> tls
-min 1.2
system>
```

To change the current tls version to 1.2, issue the following command:

```
system> tls -min 1.2
ok
system>
```

trespass command

Use this command to configure and display the trespass messages.

The **trespass** command can be used to configure and display the trespass messages. The trespass messages will be displayed to any user logging in through the WEB or CLI interface.

Syntax:

```
trespass [-options]
```

Table 54. trespass options

Option	Description
`-s`	Configure trespass messages
`-h`	Lists usage and options

Example:

```
system> trespass -s testingmessage
ok
system> trespass
```

```
testingmessage
system>
system> trespass -s "testing message"
ok
system> trespass
testing message
system>
```

uefipw command

Use this command to configure UEFI admin passwords. The password is write-only.

The `uefipw` command can be used with the `-p` option to configure the UEFI admin password for XCC or with the `-ep` option for LXCA to configure the UEFI admin password by CLI interface. The password is write-only.

Syntax:
`uefipw [-options]`

Table 55. uefipw options

Option	Description
`-cp`	Current password (limited to 20 characters)
`-p`	New password (limited to 20 characters)

usbeth command

Use this command to enable or disable the in-band LAN over USB interface.

Notes:

- The OS IP configuration settings is not used to set the OS IP address of Ethernet Over USB interface but is used to notify BMC that OS IP address of Ethernet over USB has changed.
- Before you configure three IP settings for Ethernet over USB, you need to manually configure the OS IP address of Ethernet over USB interface in your local operating system.

Syntax:
`usbeth [-options]`

Table 56. usbeth options

Option	Description	Values
`-en`	Enable or disable the inband (Ethernet over USB) interface.	`enabled`, `disabled`
`-am`	Select address mode IPv4 or IPv6 LLA.	`ipv4`, `ipv6lla`
Note: `-ip`, `-sn`, and `-ipos` options are only valid when the `-am ipv4` mode is selected		
`-ip`	Ethernet over USB interface IP address for BMC.	Valid IP address
`-sn`	Ethernet over USB interface subnet mask for BMC.	Valid IP address
`-ipos`	Ethernet over USB interface IP address for OS.	Valid IP address

Example:

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

users command

Use this command to access all user accounts and their authority levels.

The `users` command is also used to create new user accounts and modify existing accounts. Running the `users` command with no options displays a list of users and some basic user information.

Syntax:

```
users [-user_index] [-options]
```

Table 57. users options

Option	Description	Values
`-[user_index]`	User account index number.	Where `[user_index]` is 1 to 12 (inclusive), or `all` for all users.
`-l`	Display password expiration days	
`-n`	User account name	Unique string containing only numbers, letters, periods, and underscores. Minimum of 4 characters and maximum of 16 characters.
`-p`	User account password	String that contains at least one alphabetic and one non-alphabetic character. Minimum of 6 characters and maximum of 255 characters. Null creates an account without a password that the user must set during their first login.
`-shp`	Set hash password	Total 64 characters
`-ssalt`	Set salt	Limited to 64 characters
`-ghp`	Get hashpassword	
`-gsalt`	Get salt	
`-ep`	Encryption password (for backup/restore)	Valid password
`-esalt`	salt for encrypted password	Only for backup or restore
`-r`	Role name	`Administrator`, `Operator`, `ReadOnly`. As listed in "roles command" on page 143 command.
`-clear`	Erase specified user account	User account index number to erase must be specified, following the form: `users -clear -user_index` **Note:** If you are authorized, you can remove your own account or the account of other users, even if they are currently logged in, unless it is the only account remaining with User Account Management privileges. Sessions that are already in progress when user accounts are deleted will not be automatically terminated.
`-curr`	Display users currently logged in	

Table 57. users options (continued)

Option	Description	Values
`-ai`	User accessible Interface	`web`, `ssh`, `redfish`, `ipmi`, `snmp`, `all` **Note:** A default value (`web|ssh|redfish`) will be set if there is no `-ai` option.
`-sauth`	SNMPv3 authentication protocol	`None`, `HMAC_MD5`, `HMAC_SHA96`, `HMAC128_SHA224`, `HMAC192_SHA256`, `HMAC256_SHA384`, `HMAC384_SHA512`
`-spriv`	SNMPv3 privacy protocol	`None`, `CBC_DES`, `CFB128_AES128`, `AES192`, `AES256`, `AES192C`, `AES256C`
`-spw`	SNMPv3 privacy password	Valid password
`-sepw`	SNMPv3 privacy password (encrypted)	Valid password
`-sacc`	SNMPv3 access type	`get`
`-strap1`	SNMPv3 trap host name 1	Valid host name
`-strap2`	SNMPv3 trap host name 2	Valid host name
`-strap3`	SNMPv3 trap host name 3	Valid host name
`-pk`	Display SSH public key for user	User account index number. **Notes:** • Each SSH key assigned to the user is displayed, along with an identifying key index number. • When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk`. • All keys are in OpenSSH format.
The following options are used along with `-pk`		
`-e`	Display entire SSH key in OpenSSH format **(SSH public key option)**	This option takes no arguments and must be used exclusive of all other `users -pk` options. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk -e`.
`-remove`	Remove SSH public key from user **(SSH public key option)**	Public key index number to remove must be given as a specific `-key_index` or `-all` for all keys assigned to the user. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk -remove -1`.

Table 57. users options (continued)

Option	Description	Values
`-add`	Add SSH public key for user **(SSH public key option)**	Quote-delimited key in OpenSSH format **Notes:** • The `-add` option is used exclusive of all other `users -pk` command options. • When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/ aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="`
`-upld`	Upload an SSH public key in OpenSSH or RFC4716 format **(SSH public key option)**	Requires the `-i` and `-l` options to specify key location. **Notes:** • The `-upld` option is used exclusive of all other `users -pk` command options (except for `-i` and `-l`). • To replace a key with a new key, you must specify a `-key_index`. To add a key to the end of the list of current keys, do not specify a key index. • When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`.
`-dnld`	Download the specified SSH public key to a TFTP/ SFTP server **(SSH public key option)**	Requires a `-key_index` to specify the key to download and the `-i` and `-l` options to specify the download location on another computer running a TFTP server. **Notes:** • The `-dnld` option is used exclusive of all other `users -pk` command options (except for `-i`, `-l`, and `-key_index`). • When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
`-i`	IP address of TFTP/SFTP server for uploading or downloading a key file **(SSH public key option)**	Valid IP address **Note:** The `-i` option is required by the `users -pk -upld` and `users -pk -dnld` command options.
`-pn`	Port number of TFTP/SFTP server **(SSH public key option)**	Valid port number (default 69/22) **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
`-u`	User name for SFTP server **(SSH public key option)**	Valid user name **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.
`-pw`	Password for SFTP server **(SSH public key option)**	Valid password **Note:** An optional parameter for the `users -pk -upld` and `users -pk -dnld` command options.

Table 57. users options (continued)

Option	Description	Values
`-l`	File name for uploading or downloading a key file via TFTP or SFTP **(SSH public key option)**	Valid file name **Note:** The `-l` option is required by the `users -pk -upld` and `users -pk -dnld` command options.
`-af`	Accept connections from host **(SSH public key option)**	A comma-separated list of hostnames and IP addresses, limited to 511 characters. Valid characters include: alphanumeric, comma, asterisk, question mark, exclamation point, period, hyphen, colon and percent sign.
`-cm`	Comment **(SSH public key option)**	Quote-delimited string of up to 255 characters. **Note:** When using the SSH public key options, the `-pk` option must be used after the user index (`-userindex` option), of the form: `users -2 -pk -cm "This is my comment."`.

Example:

```
system> users
 Login ID     Name      Advanced Attribute     Role            Password Expires
 --------     ----      ------------------     ------            ----------------
    1         USERID                 Native     Administrator          89 day(s)
system> users -2 -n sptest -p Passw0rd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Login ID     Name      Advanced Attribute      Role               Password Expires
 --------     ----      ------------------      ------               ----------------
    1         USERID                 Native      Administrator            90 day(s)
    2         sptest                 Native      Administrator     Password expired
system> hashpw –sw enabled –re enabled
system> users -5 –n guest5 –shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee –ssalt abc –r  Administr
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system>
```

IMM control commands

This topic provides an alphabetic list of IMM control CLI commands.

alertentries command

Use this command to manage alert recipients.

Notes:

- `alertentries` with no options display all alert entry settings.
- `alertentries -number -test` generates a test alert to the given recipient index number.
- `alertentries -number` (where number is 0 - 12) display alert entry settings for the specified recipient index number or allow you to modify the alert settings for that recipient.

Syntax:

```
alertentries [-options]
```

Table 58. alertentries command

Option	Description	Values
-[number]	Alert recipient index number to display, add, modify, or delete	1 through 12
-type	Alert type	email, syslog
-status	Alert recipient status	on, off
-log	Include event log in alert e-mail	on, off
-n [name]	Alert recipient name	String
-e [email_address]	Alert recipient e-mail address	Valid email address
-del	Delete specified recipient index number	
-test	Generate a test alert to specified recipient index number	
-ip [ipaddr|hostName]	Syslog IP address or host name	Valid IP address or host name
-pn [port_number]	Syslog port number	Valid port number
-crt	Sets critical events that send alerts	all, none, custom:te|vo|po|di|fa|cp|me|in|re|pc|ot Custom critical alert settings are specified using a pipe separated list of values of the form alertentries -crt custom:te|vo, where custom values are: • te: critical temperature threshold exceeded • vo: critical voltage threshold exceeded • po: critical power failure • di: hard disk drive failure • fa: fan failure • cp: microprocessor failure • me: memory failure • in: hardware incompatibility • re: power redundancy failure • pc: critical PCIe events • ot: all other critical events

Table 58. alertentries command (continued)

Option	Description	Values
`-wrn`	Sets warning events that send alerts	`all`, `none`, `custom:rp|te|vo|po|fa|cp|me|pc|ot` Custom warning alert settings are specified using a pipe separated list of values of the form `alertentries -wrn custom:rp|te`, where custom values are: • `rp`: power redundancy warning • `te`: warning temperature threshold exceeded • `vo`: warning voltage threshold exceeded • `po`: warning power threshold exceeded • `fa`: non-critical fan event • `cp`: microprocessor in degraded state • `me`: memory warning • `pc`: warning PCIe events • `ot`: all other warning events
`-sys`	Sets routine events that send alerts	`all`, `none`, `custom:lo|tio|ot|po|bf|til|pf|ne|au|nl|dh` Custom routine alert settings are specified using a pipe separated list of values of the form `alertentries -sys custom:lo|tio`, where custom values are: • `lo`: successful remote login • `tio`: operating system timeout • `ot`: all other informational and system events • `po`: system power on/off • `bf`: operating system boot failure • `til`: operating system loader watchdog timeout • `pf`: predicted failure (PFA) • `ne`: network change • `au`: all other audit events • `nl`: host NIC link down/up • `dh`: drive hotplug

Example:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -2
-type: syslog
-status: on
-log: off
```

```
-n: syslog
-e:
-ip: 12.12.1.2
-pn: 514
-crt: all
-wrn: custom:rp|te|vo|po|fa|cp|me|pc
-sys: all
```

batch command

Use this command to execute one or more CLI commands that are contained in a file.

Notes:

- Comment lines in the batch file begin with a #.
- When running a batch file, commands that fail are returned along with a failure return code.
- Batch file commands that contain unrecognized command options might generate warnings.

Syntax:

```
batch [-options]
```

Table 59. batch options

Option	Description	Values
`-f`	Batch file name	Valid file name
`-ip`	IP address of TFTP/SFTP server	Valid IP address
`-pn`	Port number of TFTP/SFTP server	Valid port number (default 69/22)
`-u`	Username for SFTP server	Valid user name
`-pw`	Password for SFTP server	Valid password

Example:

```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

clock command

Use this command to display the current date and time. You can set the UTC offset and daylight saving time settings.

Syntax:

```
clock [-options]
```

Table 60. clock options

Option	Description	Values
`-u`	UTC offset	UTC offset of +2, -7, -6, -5, -4 and -3 special daylight saving time settings are required. • For +2, the daylight saving time options are as follows: off, ee (Eastern Europe), tky (Turkey), bei (Beirut), amm (Amman), jem (Jerusalem). • For -7, the daylight saving time settings are as follows: off, mtn (Mountain), maz (Mazatlan). • For -6, the daylight saving time settings are as follows: off, mex (Mexico), cna (Central North America). • For -5, the daylight saving time settings are as follows: off, cub (Cuba), ena (Eastern North America). • For -4, the daylight saving time settings are as follows: off, asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantic). • For -3, the daylight saving time settings are as follows: off, gtb (Godthab), bre (Brazil - East).
`-dst`	Daylight saving time	`on`, `off`, `special case`
`-host`	Format of time obtained from host (default: utc)	`local`, `utc` **Note:** Windows systems use local, Linux uses utc

Notes:

- The BMC obtains the time from the host server or NTP server.
- The time obtained from the host may be local time or UTC time. The host option should be set to UTC if NTP is not used and the host uses UTC format.
- UTC offset can be in the format of +0200, +2:00, +2, or 2, for positive offsets, and -0500, -5:00 or -5, for negative offsets.
- UTC offset and daylight savings times are used with NTP or when the host mode is UTC.

Example:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

info command

Use this command to display and configure information about the BMC.

Syntax:

```
info [-options]
```

Table 61. info options

Option	Description	Values
`-name`	BMC name	String
`-contact`	Name of BMC contact person	String
`-location`	BMC location	String
`-postal`	Full postal address of the BMC	String

Table 61. info options (continued)

Option	Description	Values
-room	BMC room identifier	String
-rack	BMC rack identifier	String
-rup	Position of BMC in rack	String

Example:

```
system> info
  -name: BMCName
  -location: location
  -contact: contact
  -rack: rack
  -room: room
  -postal: postal
  -rup: 1
system>
```

spreset command

Use this command to restart the IMM.

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

Syntax:

```
spreset
```

Service advisor commands

This topic provides an alphabetic list of service advisor CLI commands.

chconfig command

Use this command to display and configure the Service Advisor settings.

Notes:

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

Syntax:

```
chconfig [-options]
```

Table 62. chconfig options

Option	Description	Values
`-li`	View or accept the Service Advisor Terms and Conditions **Note:** Terms and Conditions must be accepted before configuring any other parameters.	`view`, `accept`
`-sa`	Support status of the Service Advisor **Notes:** To enable Service Advisor, the following criteria must be met: • The country code is required. • All options in the Service Advisor Contact Information are required.	`enabled`, `disabled`
`-sc`	Country code for the Service Support Center	Two-character ISO country code
`-ccm`	Preferred contact method, default value is Email.	`Phone`, `Email`
Service Advisor Contact Information:		
`-cn`	Name of contact person	Quote-delimited string (30 characters maximum)
`-cph`	Phone number of contact person	Quote-delimited string (5 - 30 characters)
`-ce`	Email address of contact person **Note:** Alphanumeric characters '.', '-' or '_' are acceptable as userid or hostname. Email address must contain at least two domain items.	Valid email address of the form `userid@hostname` (240 characters maximum)
`-co`	Organization or company name of contact person	Quote-delimited string (30 characters maximum)
`-ca`	Address of contact person	Quote-delimited string (30 characters maximum)
`-cci`	City of contact person	Quote-delimited string (30 characters maximum)
`-cs`	State of contact person	Quote-delimited string (30 characters maximum)
`-cz`	Postal code of contact person	Quote-delimited string (9 characters maximum)
On-site Service Advisor Contact Information:		
`-an`	Name of on-site contact person	Quote-delimited string (30 characters maximum)
`-aph`	Phone number of on-site contact person	Quote-delimited string (5 - 30 characters)
`-ae`	Email address of on-site contact person **Note:** Alphanumeric characters '.', '-' or '_' are acceptable as userid or hostname. Email address must contain at least two domain items.	Valid email address of the form `userid@hostname` (240 characters maximum)
`-ao`	Organization or company name of on-site contact person	Quote-delimited string (30 characters maximum)
`-aa`	Address of on-site contact person location	Quote-delimited string (30 characters maximum)
`-aci`	City of on-site contact person location	Quote-delimited string (30 characters maximum)
`-as`	State of on-site contact person location	Quote-delimited string (30 characters maximum)

Table 62. chconfig options (continued)

Option	Description	Values
-az	Postal code of on-site contact person location	Quote-delimited string (9 characters maximum)
Machine Location Information:		
-ma	Address of the machine location	Quote-delimited string (30 characters maximum)
-mci	City of the machine location	Quote-delimited string (30 characters maximum)
-ms	State of the machine location	Quote-delimited string (30 characters maximum)
-mz	Postal code of the machine location	Quote-delimited string (9 characters maximum)
HTTP proxy settings options:		
-loc	HTTP proxy location	Fully qualified host name or IP address for HTTP proxy (63 characters maximum)
-po	HTTP proxy port	Valid port number (1 - 65535)
-ps	HTTP proxy status	enabled, disabled
-pw	HTTP proxy password	Valid password, quote-delimited (15 characters maximum)
-u	HTTP proxy user name	Valid user name, quote-delimited (30 characters maximum)
-test	Test http proxy	

Example:

```
system> chconfig
-li: accept
-sa: enabled
-sc: CN
-ccm: Email
-cn: cn
-cph: 13111111111
-ce: test@lenovo.com
-co: co
-ca: ca
-cci: cci
-cs: cs
-cz: 1234567
-an: an
-aph: 18888888888
-ae: test@lenovo.com
-ao: ao
-aa: aa
-aci: aci
-as: as
-az: 123456789
-ma: ma
-mci: mci
-ms: ms
-mz: 1234567
-loc: 192.2.2.2
-po: 6552
-ps: disabled
-u: username
```

chmanual command

Use this command to generate a manual call home request.

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

Syntax:

```
chmanual [-options]
```

Table 63. chmanual options

Option	Description
`-test`	Generates a test message to call home recipients

chlog command

Use this command to display the last five call home events and cancel the case associated with the event by caseNumber.

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

Syntax:

```
chlog [-options]
```

Table 64. chconfig options

Option	Description
`-c`	Cancel the case associated with the event by caseNumber

Example:

```
system> chlog
Date                       Severity    EventID        Case Number    State       Msg
10/31/2024 12:09:59 AM    Critical   FQXSPPU0016N   N/A             Failed     An Uncor-rectable Error has occurred on CPUs.
10/30/2024 05:31:25 AM    Critical   FQXSPPU0016N   N/A             Failed     An Uncor-rectable Error has occurred on CPUs.
```

Agent-less commands

This topic provides an alphabetic list of Agent-less commands.

storage command

Use this command to display and configure (if supported by the platform) information about the server's storage devices that are managed by the IMM.

Syntax:

```
storage [-options]
```

Table 65. storage options

Option	Description	Values
`-list`	List the storage targets managed by the IMM.	• `controllers`: list the supported RAID controllers[1] • `pools`: list the storage pools associated with the RAID controller[1] • `volumes`: list the storage volumes associated with the RAID controller[1] • `drives`: list the storage drives associated with the RAID controller[1]

`-list [storage targets]`
`-target [target_id]`
	List the `[storage targets]` managed by the IMM according to the `[target_id]`.	Where `[storage targets]` and `[target_id]` are:
		• `pools` and `ctrl[x]`: list the storage pools associated with the RAID controller, based on the target_id[1]
		• `volumes` and `ctrl[x]|pool[x]`: list the storage volumes associated with the RAID controller, based on the target_id[1]
		• `drives` and `ctrl[x]|pool[x]`: list the storage drives associated with the RAID controller, based on the target_id[1]

`-list devices`	Display the status of all disks managed by the IMM.	
`-show [target_id]`	Display information for the selected target that is managed by the IMM.	Where `[target_id]` is `ctrl[x]|vol[x]|disk[x]|pool[x]`[3]
`-show [target_id] info`	Display detailed information for the selected target that is managed by the IMM.	Where `[target_id]` is `ctrl[x]|vol[x]|disk[x]|pool[x]`[3]
`-show [target_id] firmware`[3]	Display the firmware information for the selected target that is managed by the IMM.	Where `[target_id]` is `ctrl[x]|disk[x]`[2]
`-showinfo nvme`	Display firmware information of Nvme disk.	
`-wthre show`	Display critical and warning SSD wear threshold.	Threshold value (1 to 99)
`-wthre -ct [threshold value]`	Set SSD wear critical threshold.	Threshold value (1 to 99)
`-wthre -wt [threshold value]`	Set SSD wear warning threshold.	Threshold value (1 to 99) **Note:** The warning value needs to be greater than the critical.
`-config ctrl -scanforgn -target [target_id]`[3]	Detect the foreign RAID configuration.	Where `[target_id]` is `ctrl[x]`[5]
`-config ctrl -imptforgn -target [target_id]`[3]	Import the foreign RAID configuration.	Where `[target_id]` is `ctrl[x]`[5]
`-config ctrl -clrforgn -target [target_id]`[3]	Clear the foreign RAID configuration.	Where `[target_id]` is `ctrl[x]`[5]
`-config ctrl -clrcfg -target [target_id]`[3]	Clear the RAID configuration.	Where `[target_id]` is `ctrl[x]`[5]

Table 65. storage options (continued)

Option	Description	Values
`-config ctrl -bootdevice -vd [volume] -target [target_id]`	Set boot device by volume.	Where `[target_id]` is `ctrl[x]` and `[volume]` is a value in the first column of "list volumes" output.
`-config ctrl -bootdevice -pd [drive] -target [target_id]`	Set boot device by drive.	Where `[target_id]` is `ctrl[x]` and `[drive]` is a value in the first column of "list drives" output.
`-config ctrl -bootdevice -index [index] -target [target_id]`	Set boot device by index.	Where `[target_id]` is `ctrl[x]` and `[index]` is a value in "[]" which is the output of "display" option.
`-config ctrl -bootdevice -display -target [target_id]`	Show bootable device.	
`-config drv -mkoffline -target [target_id]`[3]	Change the drive state from online to offline.	Where `[target_id]` is `disk[x]`[5]
`-config drv -mkonline -target [target_id]`[3]	Change the drive state from offline to online.	Where `[target_id]` is `disk[x]`[5]
`-config drv -mkmissing -target [target_id]`[3]	Mark the offline drive as an unconfigured good drive.	Where `[target_id]` is `disk[x]`[5]
`-config drv -prprm -target [target_id]`[3]	Prepare an unconfigured good drive for removal.	Where `[target_id]` is `disk[x]`[5]
`-config drv -undoprprm -target [target_id]`[3]	Cancel the prepare an unconfigured good drive for removal operation.	Where `[target_id]` is `disk[x]`[5]
`-config drv -mkbad -target [target_id]`[3]	Change the unconfigured good drive to a unconfigured bad drive.	Where `[target_id]` is `disk[x]`[5]
`-config drv -mkgood -target [target_id]`[3]	Change an unconfigured bad drive to a unconfigured good drive. or Convert the just a bunch of disks (JBOD) drive to an unconfigured good drive.	Where `[target_id]` is `disk[x]`[5]
`-config drv -mkjbod -target [target_id]`[3]	Make unconfigured good as JBOD.	Where `[target_id]` is `disk[x]`[5]
`-config drv -rebuild -target [target_id]`[3]	Start rebuild drive.	Where `[target_id]` is `disk[x]`[5]
`-config drv -addhsp -target [target_id]`[3]	Assign the selected drive as a hot spare to one controller or to existing storage pools.	Where `[target_id]` is `disk[x]`[5]
`-config drv -dedicated pools -target [target_id]`[3]	Assign drive as dedicated hot spare to the selected storage pools.	Where `[target_id]` is `disk[x]`[5]
`-config drv -rmhsp -target [target_id]`[3]	Remove the hot spare.	Where `[target_id]` is `disk[x]`[5]
`-config vol -remove -target [target_id]`[3]	Remove one volume.	Where `[target_id]` is `disk[x]`[5]

Table 65. storage options (continued)

Option	Description	Values
`-config vol -set [-N] [-w] [-r ] [-i] [-a] [-d] [-b] -target [target_id]`[3]	Modify the properties of one volume.	• [-N **volume_name**] is the name of the volume • [-w **<0|1|2|3>**] is the cache write policy: – Type **0** for the Write Through policy – Type **1** for the Protected Write Back policy – Type **2** for the Unprotected Write Back policy – Type **3** for no policy • [-r **<0|1>**] is the cache read policy: – Type **0** for the No Read Ahead policy – Type **1** for the Read Ahead Policy • [-i **<0|1>**] is the cache I/O policy: – Type **0** for the Direct I/O policy – Type **1** for the Cached I/O policy • [-a **<0|2|3>**] is the access policy: – Type **0** for the Read Write policy – Type **2** for the Read Only policy – Type **3** for the Blocked policy • [-d **<0|1|2>**] is the disk cache policy: – Type **0** if the policy is unchanged – Type **1** to enable policy[6] – Type **2** to disable policy • [-b **<0|1>**] is the background initialization: – Type **0** to enable initialization – Type **1** to disable initialization • **-target_id** is **vol[x]**[5]
`-config vol -add [-R] [-D disk] [-H disk] [-1 hole] [-N] [-w] [-r]`[3,7]	Create one volume for a new storage pool when the target is a controller. or Create one volume with an existing storage pool when the target is a storage pool.	• [-R **<0|1|5|1E|6|10|50|60|00>**] This option defines the RAID level and is only used with a new storage pool • [-D disk **[id11]:disk[id12]:..disk[id21]:disk [id22]:..**] This option defines the drive group (including spans) and is only used with a new storage pool • [-H disk **[id1]:disk[id2]:..**] This option defines the hot spare group and is only used with a new storage pool • [-1 hole] This option defines the index number of the free hole space for an existing storage pool • [-N **volume_name**] is the name of the volume • [-w **<0|1|2|3>**] is the cache write policy: – Type **0** for the Write Through policy – Type **1** for the Protected Write Back policy – Type **2** for the Unprotected Write Back policy – Type **3** for no policy

Table 65. storage options (continued)

Option	Description	Values
		• [-r **<0|1>**] is the cache read policy: – Type **0** for the No Read Ahead policy – Type **1** for the Read Ahead Policy
`-config vol -add [-i] [-a] [-d] [-f] [-S] [-P] -target [target_id]`[3]	Create one volume for a new storage pool when the target is a controller. or Create one volume with an existing storage pool when the target is a storage pool.	• [-i **<0|1>**] is the cache I/O policy: – Type **0** for the Direct I/O policy – Type **1** for the Cached I/O policy • [-a **<0|2|3>**] is the access policy: – Type **0** for the Read Write policy – Type **2** for the Read Only policy – Type **3** for the Blocked policy • [-d **<0|1|2>**] is the disk cache policy: – Type **0** if the policy remains unchanged – Type **1** to enable the policy[6] – Type **2** to disable the policy • [-f **<0|1|2>**] is the type of initialization: – Type **0** for no initialization – Type **1** for quick initialization – Type **2** for full initialization • [-S **volume_size**] is the size of the new volume in MB • [-P **strip_size**] is the volume strip size for example, 512B, 4K, 128K, 1M, and so on • -target **target_id** is: – **ctrl[x]** (new storage pool)[5] – **pool[x]** (existing storage pool)[5]
`-config vol -getfreecap [-R] [-D disk] [-H disk] -target [target_id]`[3]	Get the free capacity amount of the drive group.	• [-R **<0|1|5|1E|6|10|50|60|00>**] This option defines the RAID level and is only used with a new storage pool • [-D disk **[id11]:[id12]:..[id21]:[id22]:..**] This option defines the drive group (including spans) and is only used with a new storage pool • [-H disk **[id1]:[id2]:..**]This option defines the hot spare group and is only used with a new storage pool • -target **target_id** is **ctrl[x]**[5]
`-fgi vol[idx]`	Fast initialize the specified volume (s)	Where `vol[idx]` is `vol[id1],vol[id2]:..`

Table 65. storage options (continued)

Option	Description	Values
`-help`	Display the command usage and options	
Notes: 1. This command is only supported on servers where the IMM can access the RAID controller. 2. Firmware information is displayed only for associated controllers, disks, and Flash DIMMs. Firmware information for associated pools and volumes are not displayed. 3. Information is displayed on multiple lines due to space limitations. 4. This command is only supported on servers that support RAID logs. 5. This command is only supported on servers that support RAID configurations. 6. The **Enable** value does not support RAID level 1 configurations. 7. A partial list of available options are listed here. The remaining options for the `storage -config vol -add` command are listed in the following row.		

Examples:

```
system> storage -config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage -config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage -config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage -config drv -addhsp -target disk[0-0]
ok
system>
system> storage -config drv -mkbad -target disk[0-0]
ok
system>
system> storage -config drv -mkgood -target disk[0-0]
ok
system>
system> storage -config drv -mkmissing -target disk[0-0]
ok
system>
system> storage -config drv -mkoffline -target disk[0-0]
ok
system>
system> storage -config drv -mkonline -target disk[0-0]
ok
system>
system> storage -config drv -prprm -target disk[0-0]
ok
system>
system> storage -config drv -rmhsp -target disk[0-0]
ok
system>
system> storage -config drv -undoprprm -target disk[0-0]
ok
system>
system> storage -config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage -config vol -add -R 1 -D
disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage -config vol -getfreecap -R 1 -D
disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage -config vol -remove -target vol[0-1]
ok
system>
system> storage -config vol -set -N LD_volume
-w 0 -target vol[0-0]
ok
system>
system> storage -list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage -list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage -list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage -list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage -list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
```

```
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage -show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 12345678901
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0] Storage Pool 0
pool[0-1] Storage Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage -show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
```

```
Part No.:
system>
system> storage -show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage -show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage -show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

adapter command

This command is used to display PCIe adapter inventory information.

Syntax:

```
adapter [-options]
```

Table 66. adapter options

Option	Description	Values
`-list`	List all PCIe adapters in the server.	
`-show [target_id]`	Show the detailed information for the target PCIe adapter.	`target_id [info|firmware|ports]` Where: • `info`: display the hardware information for the adapter • `firmware`: display all firmware information for the adapter • `ports`: display all Ethernet port information for the adapter

If the `adapter` command is not supported, the server responds with the following message when the command is issued:
`Your platform does not support this command.`

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

Examples:

```
system> adapter -list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
system>
system> adapter -show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2
Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
```

```
Connector Layout: pci x
Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
system>
```

Support commands

This topic provides an alphabetic list of Support commands.

dbgshbmc command

Use this command to unlock network access to the secure debug shell.

Note: This command used to be `dbgshimm` command.

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

The following table shows the arguments for the options.

Syntax:

```
dbgshbmc [subset_command]
```

Table 67. dbgshbmc subset commands

Option	Description
`status`	Display status
`enable`	Enable debug access (default if no option specified)
`disable`	Disable debug access

Chapter 12. IPMI interface

This chapter describes the IPMI interface supported by the XClarity Controller.

For details of the standard IPMI commands, refer to the Intelligent Platform Management Interface (IPMI) Specification document (version 2.0 or above). This document provides descriptions on the OEM parameters used with the standard IPMI and OEM IPMI commands supported by the XClarity Controller firmware.

Managing the XClarity Controller with IPMI

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

The XClarity Controller comes with a user ID set initially to a user name of USERID and password of PASSW0RD (with a zero, not the letter O). This user has Supervisor access.

Important: Change this user name and password during your initial configuration for enhanced security.

In a Flex System, a user can configure a Flex System CMM to centrally manage the XClarity Controller IPMI user accounts. In this circumstance, you might not be able to access the XClarity Controller using the IPMI until the CMM has configured the IPMI user IDs.

Note: The user ID credentials configured by the CMM might be different than the USERID/PASSW0RD combination described above. If no IPMI user IDs have been configured by the CMM, the network port associated with the IPMI protocol will be closed.

The XClarity Controller also provides the following IPMI remote server management capabilities:

IPMI Command-line interfaces

The IPMI command line interface provides direct access to server-management functions through the IPMI 2.0 protocol. You can use the IPMItool to issue commands to control server power, view server information, and identify the server. For more information about the IPMItool, see "Using IPMItool" on page 179.

Serial over LAN

To manage servers from a remote location, use the IPMItool to establish a Serial over LAN (SOL) connection. For more information about the IPMItool, see "Using IPMItool" on page 179.

Using IPMItool

Use the information in this topic to access information about the IPMItool.

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

For more information about the IPMItool, or to download the IPMItool, go to https://github.com/ipmitool/ipmitool.

IPMI Commands with OEM Parameters

Get / Set LAN Configuration Parameters

In order to reflect the capabilities provided by the XCC for some of the network settings, the values for some of the parameter data is defined as shown below.

DHCP

In addition to the usual methods of obtaining an IP address, the XCC provides a mode where it attempts to obtain an IP address from a DHCP server for a given period of time and if unsuccessful fails over to using a static IP address.

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

Parameter	#	Parameter Data
IP Address Source	4	data 1 [7:4] – reserved [3:0] – address source 0h = unspecified 1h = static address (manually configured) 2h = address obtained by XCC running DHCP 3h = address obtained by BIOS or system software 4h = address obtained by XCC running other address assignment protocol. The XCC uses the value 4h to indicate the address mode of DHCP with failover to static.

Ethernet Interface Selection

The XCC hardware contains dual 10/100 Ethernet MACs with RMII interfaces. The XCC hardware also contains dual 1Gbps Ethernet MACs with RGMII interfaces. One of the MACs is usually connected to the shared server NIC and the other MAC is used as a dedicated system management port. Only one Ethernet port on a server is active at a given time. Both ports will not be simultaneously enabled.

On some servers, the system designers may choose to connect up only one or the other of these Ethernet interfaces on the system planar. In those systems, only the Ethernet interface that is connected on the planar is supported by the XCC. A request to use the unconnected port returns a CCh completion code.

The package IDS for all optional network cards are numbered as follows:

- optional card #1, package ID = 03h (eth2),
- optional card #2, package ID = 04h (eth3),

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

Parameter	#	Parameter Data
OEM Parameter This parameter number is used by the XCC to indicate which of the possible Ethernet ports (logical packages) should be used. This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes, or optionally 4 bytes if the device is in an NCSI package. Byte 1 = completion code Byte 2 = revision Byte 3 = 00h for eth0, or 01h for eth1, etc… Byte 4 = (optional) channel number, if the device is an NCSI package	C0h	data1 00h = eth0 01h = eth1 02h = eth2 etc… FFh = disable all external network ports) XCC supports a 2nd optional data byte to specify which channel in a package is used data2 00h = channel 0 01h = channel 1 etc… If data2 is not specified in the request, channel 0 is assumed

The data1 byte is used to specify the logical package. It may be a dedicated systems management NIC or an NCSI interface into the NIC shared with the server.

The data2 byte is used to specify the channel for logical package, if the package is an NCSI device. If the data2 is not specified in the request and the logical package is an NCSI device, channel 0 is assumed. If data2 is specified in the request but the logical package is not an NCSI device, the channel information is ignored.

Examples:

Appendix A. If channel 2 of the shared NIC on the planar (package ID = 0, eth0) is to be used as the management port , the input data would be: 0xC0 0x00 0x02

Appendix B: If the first channel of the first network mezzanine card is to be used, the input would be: 0xC0 0x02 0x0

Ethernet over USB Enable/Disable

The parameter below is used to enable or disable the XCC inband interface.

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

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to enable or disable the Ethernet over USB interface.) This parameter in the Get LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (disabled), or 01h (enabled)	C1h	data 1 0x00 = disabled 0x01 = enabled

The data1 byte is used to specify the logical package. It may be a dedicated systems management NIC or an NCSI interface into the NIC shared with the server.

The data2 byte is used to specify the channel for logical package, if the package is an NCSI device. If the data2 is not specified in the request and the logical package is an NCSI device, channel, 0 is assumed. I data2 is specified in the request but the logical package is not an NCSI device, the channel information is ignored.

Examples:

Appendix A. If channel 2 of the shared NIC on the planar (package ID = 0, eth0) is to be used as the management port , the input data would be: 0xC0 0x00 0x02

Appendix B: If the first channel of the first network mezzanine card is to be used, the input would be: 0xC0 0x02 0x0

IPMI option for getting the DUID-LLT

An additional read-only value that needs to be exposed via IPMI is the DUID. According to RFC3315, this format of DUID is based on the Link Layer Address Plus Time.

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to enable or disable the Ethernet over USB interface.) This parameter in the Get LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3 = length of following data bytes (16 bytes currently) Byte 4-n DUID_LLT	C2h	

Ethernet configuration parameters

The parameters below may be used to configure specific Ethernet settings.

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to enable or disable Auto-negotiation setting for Ethernet Interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (disabled), or 01h (enabled)	C3h	data 1 0x00 = disabled 0x01 = enabled Note: On Flex and ThinkSystem D2 Enclosure (ThinkSystem SD530 Compute Node) systems the auto-negotiation setting is not changeable because it could break the network communication path via the CMM and SMM.
OEM Parameter (This parameter number is used by the XCC to get or set the Data rate of Ethernet Interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (10Mb), or 01h (100Mb)	C4h	data 1 0x00 = 10Mbit 0x01 = 100Mbit

Parameter	#	Parameter Data
OEM Parameter (This parameter number is used by the XCC to get or set the Duplex setting of the Ethernet interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (Half Duplex), or 01h (Full Duplex)	C5h	data 1 0x00 = Half Duplex 0x01 = Full Duplex
OEM Parameter (This parameter number is used by the XCC to get or set the Maximum transmission unit (MTU) of the Ethernet interface.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3-4 = size of MTU	C6h	data 1 Size of MTU
OEM Parameter (This parameter number is used by the XCC to get or set Locally administered MAC address.) The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 – 8 = Mac Address	C7h	data 1 - 6 Mac Address

IPMI option for getting the Link-Local Address

This is a read-only parameter to retrieve the IPV6 Link-Local Address.

Parameter	#	Parameter Data
OEM Parameter This parameter is used to obtain the Link-Local address of the XCC: The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3 = IPV6 address prefix length Byte 4-19 Local Link address in binary format	C8h	

IPMI option for enabling/disabling IPv6

This is a read/write parameter to enable/disable IPV6 in the XCC.

Parameter	#	Parameter Data
OEM Parameter This parameter is used to enable/ disable IPv6 in the XCC The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3 = 00h (disabled), or 01h (enabled)	C9h	data 1 0x00 = disabled 0x01 = enabled

Ethernet-over-USB Pass-through to external network

The parameter below is used to configure the Ethernet-over-USB to external Ethernet pass-through.

Parameter	#	Parameter Data
OEM Parameter This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The Get response data will return the following: Byte 1 = completion code Byte 2 = revision Byte 3 = reserved (00h) Bytes 4:5 = Ethernet-over-USB Port number (LSByte first) Bytes 6:7 = External Ethernet Port number (LSByte first) The number of bytes to follow can vary (1, 4, or 16 bytes) depending upon the addressing mode: • Byte 8 = pre-defined modes: 00h = the pass-through is disabled 01h = the CMM's IP address is used Bytes 8:11 = IPv4 external network IP address in binary form Bytes 8:23 = IPv6 external network IP address in binary form Completion codes: 00h – success 80h – parameter not supported C1h – command not supported C7h – request data length invalid	CAh	Set LAN Configuration Parameters: data 1 reserved (= 00h) data 2:3 Ethernet over USB Port number, LSByte first data 4:5 External Ethernet Port number, LSByte first The number of bytes to follow can vary (1, 4, or 16 bytes) depending upon the addressing mode: data 6 00h = disable the pass-through 01h = use the CMM's IP address data 6:9 IPv4 external network IP address in binary form data 6:21 IPv6 external network IP address in binary form
OEM Parameter This parameter is used to set and get the lan over usb ip address and netmask of the XCC: The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec)	CBh	Data 1:4 IP address of XCC -side lan over usb interface. Data 5:8 Netmask of XCC -side lan over usb interface

Parameter	#	Parameter Data
Byte 3:10 = IP address and Netmask value (MS-byte) first		
OEM Parameter This parameter is used to set and get the lan over usb ip address of the Host OS: The response data will return the following: Byte 1 = completion code Byte 2 = Parameter Revision (as in IPMI spec) Byte 3:6 = IP address (MS-byte) first	CCh	Data 1:4 IP address of Host-side lan over usb interface.

Query Logical Package Inventory

The parameter below is used to query NCSI package inventory.

Parameter	#	Parameter Data
OEM Parameter This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. Query package inventory operation The query package information operation is performed by issuing the request with two 0x00 data bytes besides the D3h parameter number. Query package inventory : --> 0x0C 0x02 0x00 0xD3 0x00 0x00 The XCC response includes a byte of information for each package that is present: bits 7:4 = number of NCSI channels in the package bits 3:0 = the logical package number Response --> 0x00 0x00 0x40 0x01 0x32 indicates that 3 logical packages are present: package 0 has 4 NCSI channels package 1 is not an NCSI NIC , so it does not support NCSI channels package 2 has 3 NCSI channels	D3h	Get/Set LAN Configuration Parameters:

Get/Set Logical Package Data

The parameter below is used to read and to set the priority assigned to each package.

Parameter	#	Parameter Data
OEM Parameter This parameter in the Get/Set LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The command supports 2 operations: • Read package priority • Set package priority Read package priority operation The read package priority operation is performed by issuing the request with two 0x00 data bytes besides the D4h parameter number. Read package priority: --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Response --> 0x00 0x00 0x00 0x12 0x23 logical package 0 = priority 0 logical package 2 = priority 1 logical package 3 = priority 2 Set package priority operation The set package priority operation is performed by issuing the request with one or more parameters in addition to the D4h parameter number. Set package priority: --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 set logical package 0 = priority 0 set logical package 2 = priority 1 set logical package 3 = priority 2 Response:	D4	Get/Set LAN Configuration Parameters: Bit [7-4] = priority of the logical package (1 = highest, 15 = lowest) Bit [3-0] = logical package number

Parameter	#	Parameter Data
completion code only, no additional data		

Get/Set XCC networking synchronization status

Parameter	#	Parameter Data
OEM Parameter The byte is used to config to synchronize networking setting between dedicated and shared nic mode This parameter in the Get LAN Configuration Parameters command does not use a Set Selector or a require Block Selector, so these fields should be set to 00h. The response data will return 3 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = 00h (enabled) , or 01h (disabled)	D5h	data 1 0x00 = Synchronization 0x01 = Independence

The byte is used to config to synchronize networking setting between dedicated and shared nic mode , the default value was 0h here, it mean XCC will automatically update networking setting between mode change and use shared nic (on board) as major reference , if set as 1h , each networking setting will be independent here , which is we can configure different networking setting between mode, such as VLAN enable on Dedicated and set VLAN disable on Shared NIC mode.

Get/Set XCC networking mode

Parameter	#	Parameter Data
OEM Parameter This parameter is used to get/set network mode of XCC management NIC. The response data will return 4 bytes: Byte 1 = completion code Byte 2 = revision Byte 3 = applied/specified netmode Byte 4 = package id of applied netmode Byte 5 = channel id of applied netmode	D6h	Set LAN Configuration Parameters: data 1 Netmode to set Get LAN Configuration Parameters: data 1 Netmode to get, This is an optional data, defaults to query current netmode

OEM IPMI Commands

The XCC supports the following IPMI OEM commands. Each command requires a different level of privilege as listed as below.

Code	Netfn 0x2E Commands	Privilege
0xCC	Reset XCC to Default	PRIV_USR

Code	Netfn 0x3A Commands	Privilege
0x00	Query Firmware version	PRIV_USR
0x1E	Chassis Power Restore Delay Options	PRIV_USR
0x49	Initiate Data Collection	PRIV_USR
0x4A	Push File	PRIV_USR
0x4D	Data Collection Status	PRIV_USR
0x50	Get Build Information	PRIV_USR
0x55	Get/Set Host Name	PRIV_USR
0x6B	Query FPGA Firmware Revision Level	PRIV_USR
0x6C	Query Board Hardware Revision Level	PRIV_USR

Code	Netfn 0x3A Commands	Privilege
0x6D	Query PSoC Firmware Revision Level	PRIV_USR
0x98	FP USB Port Control	PRIV_USR

Reset XCC to Default Command

This command resets the XCC configuration setting to the default values.

Net Function = 0x2E			
Code	**Command**	**Request, Response Data**	**Description**
0xCC	Reset XCC to Default	**Request:** Byte 1 – 0x66 Byte 2 – 0x4A Byte 3 – 0x00 **Response:** Byte 1 – Completion Code Byte 2 – 0x66 Byte 3 – 0x4A Byte 4 – 0x00 Byte 5 – 0x0A Byte 6 – 0x01 Byte 7 – Response Data 0 = Success non-zero = Failure	This command resets the XCC configuration settings to the default values.

Board / Firmware Information Commands

This section lists the commands for querying the board and firmware information.

Net Function = 0x3A			
Code	**Command**	**Request, Response Data**	**Description**
0x00	Query Firmware Version	**Request**: No data on request **Response**: Byte 1 – Completion Code Byte 2 – Major version Byte 3 – Minor version	This command returns the major and minor version numbers of the firmware. If the command is made with the optional 1 byte of request data, the XCC response also returns the third field (Revision) of the version. (Major.Minor.Revision)
0x50	Query Build Information	**Request**: N/A **Response**: Byte 1 – Completion Code. Bytes 2:10 – ASCIIZ Build Name Bytes 11:23 – ASCIIZ Build Date Bytes 24:31 – ASCII Build Time	This command returns the build name, build date, and build time. The build name and build date strings have a zero termination. The format of the build date is YYYY-MM-DD. e.g. “ZUBT99A ” “2005-03-07” “23:59:59”
0x6B	Query FPGA Firmware Revision Level	**Request**: Byte 1 – FPGA Device Type1 FPGA Device Type 0 = Local (Active level) 1 = CPU Card 1 (Active level) **Response**: Byte 1 – Completion Code Byte 2 – Major revision level Byte 3 – Minor revision level Byte 4 – Sub-Minor revision level (Test Byte on XCC platforms)	This command returns the revision level of the FPGA firmware. **Notes:** 1. If Byte 1 is omitted then Local (Active level) will be selected

Net Function = 0x3A			
Code	**Command**	**Request, Response Data**	**Description**
0x6C	Query Board Hardware Revision Level	**Request**: No Data. **Response**: Byte 1 – Completion Code Byte 2 – Revision level	This command returns the revision level of the board hardware where the FPGA resides.
0x6D	Query PSoC Firmware Revision Level	**Request**: None **Response**: Byte 1 – Completion Code Byte 2 – bin# Byte 3 – APID Byte 4 – Rev Byte 5-6 – FRU ID Bytes 6:N – repeat of Bytes 2-6 for each detected PSoC	This command returns the revision level of all of the detected PSoC devices. Note: bin# represents a physical location. Consult the system specification for details.

System Control Commands

The IPMI specification provides basic power and reset control. Lenovo adds additional control functions.

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td>0x1E</td><td>Chassis Power Restore Delay Options</td><td><b>Request:</b><table><tr><td>Byte 1</td><td>Request Type:
0x00 = Set Delay Options
0x01 = Query Delay Options</td></tr><tr><td>Byte 2</td><td>(if byte 1 = 0x00)
0x00 = Disabled (default)
0x01 = Random
0x02 - 0xFF Reserved</td></tr></table><b>Response</b>:
Byte 1 – Completion Code
Byte 2<table><tr><td>00h:</td><td>Switch to host</td></tr><tr><td>01h:</td><td>Switch to BMC</td></tr></table><b>Response</b>:
Byte 1 – Completion Code
Byte 2 – Delay Options (for Query request only)</td><td>This setting is used, when the chassis power restore policy is set to always power-on or restore to power-on (if previously powered-on), after AC is applied/returns. There are 2 choices: Disabled (the default setting, no delay when powered-on), and Random. The random delay setting, provides a random delay between 1 and 15 seconds, from the time AC is applied/returns and when the server is automatically powered-on.
The command is supported by XCC only on Rack servers.</td></tr>
</table>

Miscellaneous Commands

This section is for commands that do not fit into any other section.

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td>0x49</td><td>Initiate Service Log Collection</td><td><b>Request:</b>
<table>
<tr><td>Byte 1 – Service Log Type</td><td>Request Type:
01h = Service Debug Log (FFDC)
02h = Data Log (Mini-log)</td></tr>
<tr><td>Byte 2 – Flag (Optional)[1]</td><td>For Type 02:
0000 0001b – Include "Network" category.
0000 0010b – Include "Audit" category.
0000 0100b – Include "Telemetry" category.
0000 1000b – Include "Latest failure screen" category.</td></tr>
</table>
<b>Response</b>:
<table>
<tr><td>Byte 1</td><td>Completion code
01h = Dump already in Progress
CCh = Unsupported Data Collection Type</td></tr>
<tr><td>Byte 2</td><td>FFDC dump timeout value[2] (minutes based)</td></tr>
</table></td><td>This command provides a means to initiate service log collection on a system.
<b>Notes:</b>
1. The Flag byte is optional. If not specified, those categories won’t be included for the service log Type.
2. The timeout value (in minutes) is provided to the requestor to specify the maximum wait time for the FFDC package file to complete generation.</td></tr>
<tr><td>0x4D</td><td>Service Log Collection Status</td><td><b>Request:</b></td><td>This command provides a means to report the status for data (dump) collection on a system.
<b>Notes:</b>
1. The response may be either 2 or 3 bytes in length. If it is unable</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr><td></td><td></td><td><table><tr><td>Byte 1 — Data Collection Type</td><td>Request Type:
01h = Debug Log (FFDC)
02h = Service Data Log (Mini-log)</td></tr></table>
<b>Response</b>[1]:
<table><tr><td>Byte 1</td><td>Completion code</td></tr><tr><td>Byte 2</td><td>Collection Status:
00h – no data, no collection in progress
01h – data ready for collection
02h – collection in progress</td></tr><tr><td>Byte 3 (optional)</td><td>Percentage Complete[2]</td></tr></table></td><td>to report a percentage complete, the response will contain only byte 1 and byte 2. If it is able to report a percentage complete, the response will also contain byte 3.
2. Percentage Complete (optional). This is an approximation of collection activity progress with value between 0 and 100.</td></tr>
<tr><td>0x55</td><td>Get/Set Hostname</td><td><b>Request Length = 0</b>:
Empty Request Data
<b>Response</b>:
<table><tr><td>Byte 1</td><td>Completion Code</td></tr><tr><td>Bytes 2-65</td><td>Current Hostname.
ASCIIZ, Null terminated string.</td></tr></table>
<b>Request Length 1-64</b>:
<table><tr><td>Bytes 1-64</td><td>DHCP Hostname
ASCIIZ Terminate with 00h</td></tr></table></td><td>Use this command to Get/Set the Hostname.
When setting the Hostname, the desired value must be terminated by a 00h. The hostname is limited to 63 characters plus the null.</td></tr>
</table>

<table>
<tr><th colspan="4">Net Function = 0x3A</th></tr>
<tr><th>Code</th><th>Command</th><th>Request, Response Data</th><th>Description</th></tr>
<tr>
<td>0x98</td>
<td>FP USB Port Control</td>
<td>
<b>Request</b>:
Byte 1
<table>
<tr><td>01h:</td><td>Get current owner of front panel USB port</td></tr>
</table>
<b>Response</b>:
Byte 1 – Completion Code
Byte 2
<table>
<tr><td>00h:</td><td>Owned by host</td></tr>
<tr><td>01h:</td><td>Owned by BMC</td></tr>
</table>
<b>Request</b>:
Byte 1
<table>
<tr><td>04h:</td><td>Set the owner of front panel USB port manually if it is in shared mode</td></tr>
</table>
Byte 2
<table>
<tr><td>00h:</td><td>Switch to host</td></tr>
<tr><td>01h:</td><td>Switch to BMC</td></tr>
</table>
<b>Response</b>:
Byte 1 – Completion Code
</td>
<td>This command is used for query owner of FP USB port, and switch USB port owner between host and BMC.</td>
</tr>
</table>

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support are available at:

http://datacentersupport.lenovo.com

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for ThinkSystem.

Before you call

Before you call, there are several steps that you can take to try and solve the problem yourself. If you decide that you do need to call for assistance, gather the information that will be needed by the service technician to more quickly resolve your problem.

Attempt to resolve the problem yourself

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

You can find the product documentation for your ThinkSystem products at the following location:

https://pubs.lenovo.com/

You can take these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://www.lenovo.com/serverproven/ to make sure that the hardware and software is supported by your product.
- Go to http://datacentersupport.lenovo.com and check for information to help you solve the problem.
  - Check the Lenovo forums at https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg to see if someone else has encountered a similar problem.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Gathering information needed to call Support

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call. You can also see http://datacentersupport.lenovo.com/warrantylookup for more information about your product warranty.

Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.

- Hardware and Software Maintenance agreement contract numbers, if applicable
- Machine type number (Lenovo 4-digit machine identifier)
- Model number
- Serial number
- Current system UEFI and firmware levels
- Other pertinent information such as error messages and logs

As an alternative to calling Lenovo Support, you can go to https://www-947.ibm.com/support/servicerequest/Home.action to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The Lenovo service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Collecting service data

To clearly identify the root cause of a server issue or at the request of Lenovo Support, you might need collect service data that can be used for further analysis. Service data includes information such as event logs and hardware inventory.

Service data can be collected through the following tools:

- **Lenovo XClarity Controller**

  You can use the Lenovo XClarity Controller web interface or the CLI to collect service data for the server. The file can be saved and sent to Lenovo Support.

  - For more information about using the web interface to collect service data, see https://pubs.lenovo.com/xcc3/nn1ia_c_servicesandsupport.html.
  - For more information about using the CLI to collect service data, see https://pubs.lenovo.com/xcc3/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator can be set up to collect and send diagnostic files automatically to Lenovo Support when certain serviceable events occur in Lenovo XClarity Administrator and the managed endpoints. You can choose to send diagnostic files to Lenovo Support using Call Home or to another service provider using SFTP. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

  You can find more information about setting up automatic problem notification within the Lenovo XClarity Administrator at https://pubs.lenovo.com/lxca/admin_setupcallhome.html.

- **Lenovo XClarity Provisioning Manager**

Use the Collect Service Data function of Lenovo XClarity Provisioning Manager to collect system service data. You can collect existing system log data or run a new diagnostic to collect new data.

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials can be run in-band from the operating system. In addition to the hardware service data, Lenovo XClarity Essentials can collect information about the operating system, such as the operating system event log.

  To obtain service data, you can run the `getinfor` command. For more information about running the `getinfor`, see https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html.

Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/us/en/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/us/en/supportphonelist for your region support details.

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, ThinkSystem, Flex System, System x, NeXtScale System, and x Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

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

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 68. Limits for particulates and gases

Contaminant	**Limits**
Particulate	• The room air must be continuously filtered with 40% atmospheric dust spot efficiency (MERV 9) according to ASHRAE Standard 52.2[1]. • Air that enters a data center must be filtered to 99.97% efficiency or greater, using high-efficiency particulate air (HEPA) filters that meet MIL-STD-282. • The deliquescent relative humidity of the particulate contamination must be more than 60%[2]. • The room must be free of conductive contamination such as zinc whiskers.
Gaseous	• Copper: Class G1 as per ANSI/ISA 71.04-1985[3] • Silver: Corrosion rate of less than 300 Å in 30 days

[1] ASHRAE 52.2-2008 - **Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size**. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] The deliquescent relative humidity of particulate contamination is the relative humidity at which the dust absorbs enough water to become wet and promote ionic conduction.

[3] ANSI/ISA-71.04-1985. **Environmental conditions for process measurement and control systems: Airborne contaminants**. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Telecommunication regulatory statement

This product may not be certified in your country for connection by any means whatsoever to interfaces of public telecommunications networks. Further certification may be required by law prior to making any such connection. Contact a Lenovo representative or reseller for any questions.

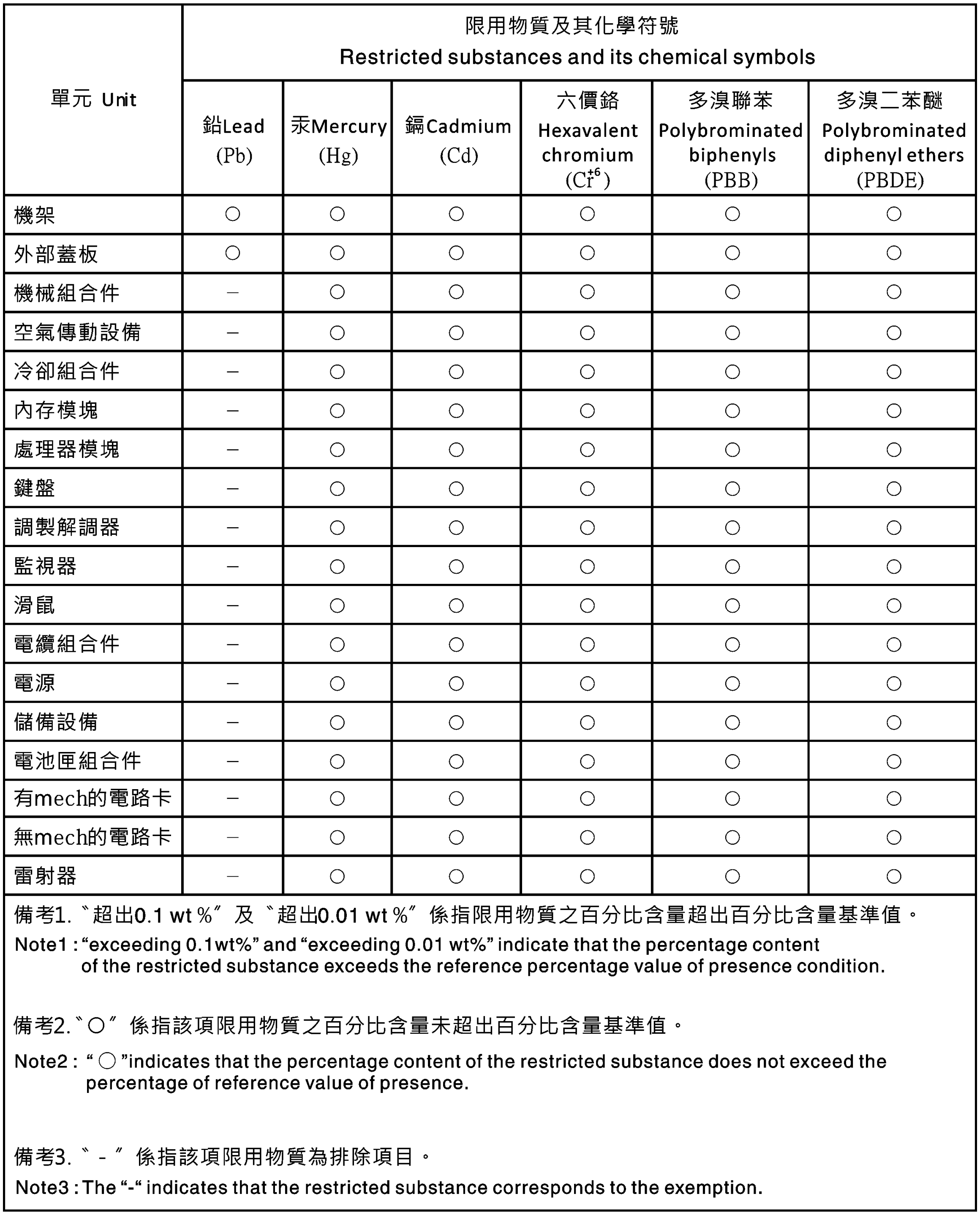
Electronic emission notices

When you attach a monitor to the equipment, you must use the designated monitor cable and any interference suppression devices that are supplied with the monitor.

Additional electronic emissions notices are available at:

https://pubs.lenovo.com/

Taiwan BSMI RoHS declaration



單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及 〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : "exceeding 0.1wt%" and "exceeding 0.01 wt%" indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : " ○ "indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝 - 〞係指該項限用物質為排除項目。

Note3 : The "-" indicates that the restricted substance corresponds to the exemption.

Taiwan import and export contact information

Contacts are available for Taiwan import and export information.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Index

Lenovo