Lenovo

Flex System Chassis Management Module Installation Guide
(For Type 7893, 8721, and 8724 chassis only)

Note

Before using this information and the product it supports, read the general information in Appendix B "Notices" on page 55, the *Warranty Information* document, and the *Safety Information* and the *Environmental Notices and User Guide* documents on the Lenovo documentation CD.

Sixth Edition (December 2017)

Contents

Safety

Before installing this product, read the Safety Information.

قبل تركيب هذا المنتج، يجب قراءة الملاحظات الآمنية

Antes de instalar este produto, leia as Informaçes de Segurança.

在安装本产品之前，请仔细阅读 Safety Information (安全信息)。

安裝本產品之前，請先閱讀「安全資訊」。

Prije instalacije ovog produkta obavezno pročitajte Sigurnosne Upute.

Před instalací tohoto produktu si přečtěte příručku bezpečnostních instrukcí.

Ls sikkerhedsforskrifterne, før du installerer dette produkt.

Lees voordat u dit product installeert eerst de veiligheidsvoorschriften.

Ennen kuin asennat tämän tuotteen, lue turvaohjeet kohdasta Safety Information.

Avant d'installer ce produit, lisez les consignes de sécurité.

Vor der Installation dieses Produkts die Sicherheitshinweise lesen.

Πριν εγκαταστήσετε το προϊόν αυτό, διαβάστε τις πληροφορίες ασφάλειας (safety information).

לפני שתתקינו מוצר זה, קראו את הוראות הבטיחות.

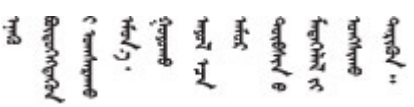
A termék telepítése előtt olvassa el a Biztonsági előírásokat!

Prima di installare questo prodotto, leggere le Informazioni sulla Sicurezza.

製品の設置の前に、安全情報をお読みください。

본 제품을 설치하기 전에 안전 정보를 읽으십시오.

Пред да се инсталира овој продукт, прочитајте информацијата за безбедност.



Les sikkerhetsinformasjonen (Safety Information) før du installerer dette produktet.

Przed zainstalowaniem tego produktu, należy zapoznać się z książką "Informacje dotyczące bezpieczeństwa" (Safety Information).

Antes de instalar este produto, leia as Informaçes sobre Segurança.

Перед установкой продукта прочтите инструкции по
технике безопасности.

Pred inštaláciou tohto zariadenia si pečítaje Bezpečnostné predpisy.

Pred namestitvijo tega proizvoda preberite Varnostne informacije.

Antes de instalar este producto, lea la informacin de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་རྫས་འདི་བདེ་སྤྱོད་མ་བྱས་གོང་། ཞོར་ཐྱི་ཡིད་གཟབ་
བྱ་འདྲ་མིན་ཡོད་པའི་འོད་སྣེར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

مەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ.

Youq mwngz yungh canjbinj neix gaxgonq, itdingh aeu doeg aen
canjbinj soengq cungj vahgangj ancien siusik.

Safety statements

These statements provide the caution and danger information that is used in this documentation.

Important: Each caution and danger statement in this documentation is labeled with a number. This number is used to cross reference an English-language caution or danger statement with translated versions of the caution or danger statement in the *Safety Information* document.

For example, if a caution statement is labeled `Statement 1`, translations for that caution statement are in the *Safety Information* document under `Statement 1`.

Be sure to read all caution and danger statements in this documentation before you perform the procedures. Read any additional safety information that comes with your system or optional device before you install the device.

Statement 1

DANGER

Electrical current from power, telephone, and communication cables is hazardous.

To avoid a shock hazard:

- **Do not connect or disconnect any cables or perform installation, maintenance, or reconfiguration of this product during an electrical storm.**
- **Connect all power cords to a properly wired and grounded electrical outlet.**
- **Connect to properly wired outlets any equipment that will be attached to this product.**
- **When possible, use one hand only to connect or disconnect signal cables.**
- **Never turn on any equipment when there is evidence of fire, water, or structural damage.**
- **Disconnect the attached power cords, telecommunications systems, networks, and modems before you open the device covers, unless instructed otherwise in the installation and configuration procedures.**
- **Connect and disconnect cables as described in the following table when installing, moving, or opening covers on this product or attached devices.**

To Connect:	**To Disconnect:**
1. Turn everything OFF.	1. Turn everything OFF.
2. First, attach all cables to devices.	2. First, remove power cords from outlet.
3. Attach signal cables to connectors.	3. Remove signal cables from connectors.
4. Attach power cords to outlet.	4. Remove all cables from devices.
5. Turn device ON.	

Statement 2

CAUTION:
When replacing the lithium battery, use only Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of. *Do not:*

- **Throw or immerse into water**
- **Heat to more than 100°C (212°F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

Chapter 1. Introduction

The Flex System Chassis Management Module is a hot-swap Flex System Enterprise Chassis module that you use to configure and manage components in your Flex System Enterprise Chassis environment.

Note: The Flex SystemChassis Management Module is compatible with only Type 7893, 8721, and 8724 chassis.

The Flex System Enterprise Chassis automatically detects installed modules and node devices and stores their vital product data (VPD). You can configure and manage Flex System Enterprise Chassis components from a remote location via an Ethernet connection through the Flex System Chassis Management Module web interface, the Flex System Chassis Management Module command-line interface (CLI), or SNMPv1 and SNMPv3. You can also configure and manage Flex System Enterprise Chassis components through a local serial connection by using the Flex System Chassis Management Module CLI.

Note: You can also configure some I/O modules directly, by using an external I/O-module port. See the documentation that comes with each I/O module for information.

The Flex System Chassis Management Module, referred to throughout this document as the CMM, provides system-management functions for all devices in the Flex System Enterprise Chassis. It provides a mini-USB serial-management connector for local management connection and a 10/100/1000 Mbps remote management and console (Ethernet) connector for local or remote management connection.

Note: An optional cable kit with adapters is available to convert the CMM mini-USB connector for RJ-45, DB-7, or standard USB cable connection. See http://static.lenovo.com/us/en/serverproven/index.shtml for available Flex System Enterprise Chassis options.

The Flex System Enterprise Chassis comes with at least one CMM and supports CMM redundancy. Only one CMM can be primary in each Flex System Enterprise Chassis. If you install a standby CMM, it remains inactive until it is switched to act as the primary CMM.

Notes:

- If two CMMs are installed in a Flex System chassis, they should be of the same type.
- The illustrations in this document might differ slightly from your hardware.

This documentation provides the following information about setting up the CMM:
- External indicators, controls, and connectors
- Installing the CMM
- Configuring the CMM

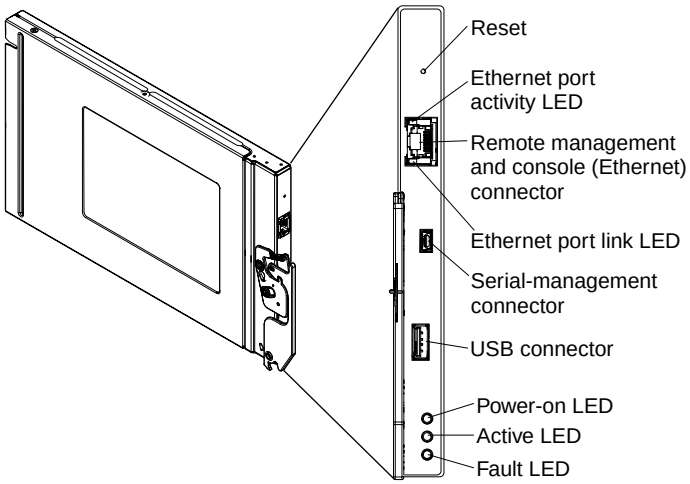
If your Flex System Enterprise Chassis is configured for redundant operation and a second CMM is installed, both will have the same level of firmware after the primary CMM updates the standby CMM after it is installed. The primary and standby CMMs can have the same IP address, or they can have different IP addresses so that the standby CMM can be accessed while it is inactive. The firmware must support redundant CMM function, to ensure changeover of control from the primary CMM to the standby CMM. The latest level of CMM firmware is available at http://datacentersupport.lenovo.com.

The management processor in the CMM communicates with the system-management processor in each compute node to support features such as compute node power-on requests and error and event reporting.

Record information about the CMM in the following table.

Product name	Flex System Chassis Management Module
Serial number	
Media access control (MAC) address	

The product name, serial number, and media access control (MAC) address are on the identification label on the side of the CMM. Information that you need to connect to the CMM for the first time is on the network access tag that is attached to the front of the CMM (see “CMM network access tag” on page 29 for information). Note that the network access tag might have been removed from your CMM during installation. The following illustration shows the controls, indicators and connectors on the CMM.



You can obtain up-to-date information about your CMM and other Flex system products at http://flexsystem.lenovofiles.com/help/index.jsp.

Related documentation

Use this information to identify and locate CMM-related documentation.

This *Installation Guide* contains general information about the CMM, including how to install and configure it. The following documentation is also available:

- *Safety Information*This document contains translated caution and danger statements. Each caution and danger statement that appears in the documentation has a number that you can use to locate the corresponding statement in your language in the *Safety Information* document.
- *Warranty Information* This document contains information about the terms of the CMM warranty.
- *Environmental Notices and User Guide* This document contains translated environmental notices.
- *Flex System Chassis Management Module User's Guide*This document provides information about configuring the CMM and managing components in an Flex System Enterprise Chassis by using the web interface.
- *Flex System Chassis Management Module Command-Line Interface Reference Guide*This document explains how to use the CMM command-line interface (CLI) to directly access Flex System Enterprise Chassis management functions. The command-line interface also provides access to the text-console command prompt on each compute node through a Serial over LAN (SOL) connection.

The CMM might have other features that are not described in the documentation that comes with the CMM. The documentation might be updated occasionally to include information about those features, or technical

updates might be available to provide additional information that is not included in the CMM documentation. These updates are available from the Lenovo website. To check for updated documentation, go to http://flexsystem.lenovofiles.com/help/index.jsp.

Notices and statements in this document

Use this information to understand the most common documentation notices and statements and how they are used.

The caution and danger statements in this document are also in the multilingual *Safety Information* document, which is on the Lenovo documentation CD. Each statement is numbered for reference to the corresponding statement in the *Safety Information* document.

The following notices and statements are used in this document:

- **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 possible damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.
- **Caution:** These statements indicate situations that can be potentially hazardous to you. A caution statement is placed just before the description of a potentially hazardous procedure step or situation.
- **Danger:** These statements indicate situations that can be potentially lethal or hazardous to you. A danger statement is placed just before the description of a potentially lethal or hazardous procedure step or situation.

Software requirements for the CMM web interface

The CMM web interface supports the following web browsers for remote (client) access.

- Microsoft Internet Explorer version 9 or later, but earlier than 11
- Mozilla Firefox versions 17 through 31 (Firefox is recommended for JAWS users)

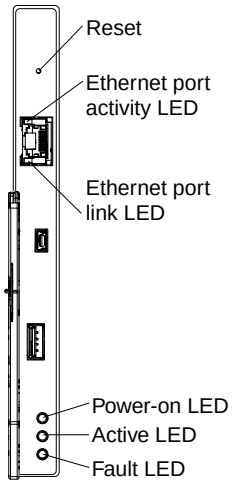
The CMM web interface does not support double-byte character set (DBCS) languages. For information about using the compute node integrated management module (IMM) interface, see the compute node or IMM documentation.

Chapter 2. CMM controls, connectors, and LEDs

Use this information for details about the indicators, controls, and external connectors on the CMM.

CMM controls and indicators

The Flex System Chassis Management Module (CMM) has LEDs and controls that you can use to obtain status information and restart the CMM.



The CMM has the following LEDs and controls:

Reset button

Use this button to restart the Chassis Management Module. Insert a straightened paper clip into the reset button pinhole; then, press and hold the button in for at least one second to restart the CMM. The restart process initiates upon release of the reset button but might not be immediately apparent in some cases.

Attention: If you press the reset button, hold it for at least 10 seconds, then release it, the CMM will restart and reset back to the factory default configuration. Be sure to save your current configuration before you reset the CMM back to factory defaults. The combined reset and restart process initiates upon release of the reset button but might not be immediately apparent in some cases.

Note: Both the CMM restart and reset to factory default processes require a short period of time to complete.

Power-on LED

When this LED is lit (green), it indicates that the CMM has power.

Active LED

When this LED is lit (green), it indicates that the CMM is actively controlling the chassis.

Only one CMM actively controls the chassis. If two CMMs are installed in the chassis, this LED is lit on only one CMM.

Fault LED

When this LED is lit (yellow), an error has been detected in the CMM. When the error LED is lit, the chassis fault LED is also lit.

Ethernet port link (RJ-45) LED

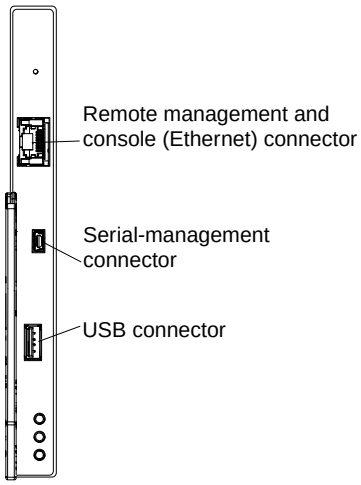
When this LED is lit (green), it indicates that there is an active connection through the remote management and console (Ethernet) port to the management network.

Ethernet port activity (RJ-45) LED

When this LED is flashing (green), it indicates that there is activity through the remote management and console (Ethernet) port over the management network.

CMM input and output connectors

The Flex System Chassis Management Module provides one serial connector (mini-USB) and one Ethernet connector for remote management and one standard USB connector.



Remote management and console (Ethernet) connector

The remote management and console connector (RJ-45) is the management network connector for all chassis components. This 10/100/1000 base T Ethernet connector is usually connected to the management network through a top-of-rack switch. During the initial setup of an optional management node, the system console is connected to the top-of-rack switch that is connected to this Ethernet port.

Serial-management connector

The serial-management connector (RS-232, mini-USB form factor) is used to connect the CMM to a management device, through a serial cable or serial management network, to manage the chassis. This connector provides local access for the CMM to the Serial over LAN (SOL) interface of any compute node. For example, you can connect a notebook computer to the serial-management connector and use a terminal emulator program to configure the IP addresses, user accounts, and other settings.

USB connector

This is a standard USB connector (future use).

CMM serial port pin assignments

The Flex System Chassis Management Module serial-management connector is an EIA-561 (mini-USB) connector with the following pin assignments.

Contact (pin number)	Signal name
1	NC
2	Receive (RX)
3	Transmit (TX)

Contact (pin number)	Signal name
4	NC
5	Ground (GND)

Chapter 3. Installing, removing, and replacing components

Use these instructions to install a CMM in the Flex System Enterprise Chassis and replace CMM components. CMM removal instructions are also provided. See the *Installation and Service Guide* that comes with your Flex System Enterprise Chassis for CMM bay locations and other chassis-specific installation information.

Installation guidelines

Use these guidelines before you install the CMM.

- Before you begin, read “Safety” on page iii and “Handling static-sensitive devices” on page 10. This information will help you work safely.
- When you install a CMM, take the opportunity to download and apply the most recent firmware updates. This step will help to ensure that any known issues are addressed and that your CMM is ready to function at maximum levels of performance.
  - You can update CMM firmware using the CMM web interface on the Firmware page (select **Firmware** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.
  - You can update CMM firmware using the CMM CLI `update` command (see "update command," in the *Flex SystemFlex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).
  - You can also update CMM firmware through SNMP.
- Observe good housekeeping in the area where you are working. Place removed covers and other parts in a safe place.
- Back up all important data before you make changes.
- You do not have to shut down the Flex System Enterprise Chassis before you remove a CMM.
- The orange color on components and labels in your Flex System Enterprise Chassis identifies hot-swap components. You can install or remove hot-swap modules and, with some restrictions, hot-swap compute nodes while the Flex System Enterprise Chassis is running. For details about installing or removing a CMM, see the detailed information in this section.
- Blue on a component indicates touch points, where you can grip the component to remove it or install it, open or close a latch, and so on.
- For a list of supported optional devices for your Flex System Enterprise Chassis, see http://static.lenovo.com/us/en/serverproven/index.shtml.

System reliability guidelines

Use these guidelines to make sure that the Flex System Enterprise Chassis meets cooling and system reliability requirements.

- You do not operate the Flex System Enterprise Chassis without a device or filler installed in each bay. See the documentation for your Flex System Enterprise Chassis for additional information.
- Each of the module bays on the front and rear of the Flex System Enterprise Chassis has either a module or a module filler installed in it.
- Each of the node bays on the front of the Flex System Enterprise Chassis has either a node device or a node filler installed in it.
- Each of the drive bays in a node device has either a hot-swap drive or a panel filler installed in it.

- You replace a removed hot-swap module, node device, or drive within 1 minute of removal. Failure to replace a node device or module with another node device, module, node filler, or module filler within 1 minute can affect performance of the compute nodes.
- Cables for optional modules are routed according to the documents that come with the modules.
- You replace a failed fan module as soon as possible to maintain cooling redundancy. See the *Flex System Enterprise Chassis Installation and Service Guide* for instructions.

Handling static-sensitive devices

To reduce the possibility of damage from electrostatic discharge, observe these precautions.

Attention: Static electricity can damage the CMM and other electronic devices. To avoid damage, keep static-sensitive devices in their static-protective packages until you are ready to install them.

- When you work on a system that has an electrostatic discharge (ESD) connector, use a wrist strap, especially when you handle modules, optional devices, or compute nodes. To work correctly, the wrist strap must have a good contact at both ends (touching your skin at one end and firmly connected to the ESD connector on the front or back of the system). See the documentation for your Flex System Enterprise Chassis to locate the ESD connector.
- Limit your movement. Movement can cause static electricity to build up around you.
- Handle the device carefully, holding it by its edges or its frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Do not leave the device where others can handle and damage it.
- While the device is still in its static-protective package, touch it to an *unpainted* metal part of the Flex System Enterprise Chassis or any *unpainted* metal surface on any other grounded rack component in the rack in which you are installing the device for at least 2 seconds. This drains static electricity from the package and from your body.
- Remove the device from its package and install it directly without setting down the device. If it is necessary to set down the device, put it back into its static-protective package. Do not place the device on a metal surface.
- Take additional care when you handle devices during cold weather. Heating reduces indoor humidity and increases static electricity.

Returning a device or component

If you are instructed to return a device or component, follow all packaging instructions, and use any packaging materials for shipping that are supplied to you.

Removing a Chassis Management Module

Use these instructions to remove a Flex System Chassis Management Module from the Flex System Enterprise Chassis.

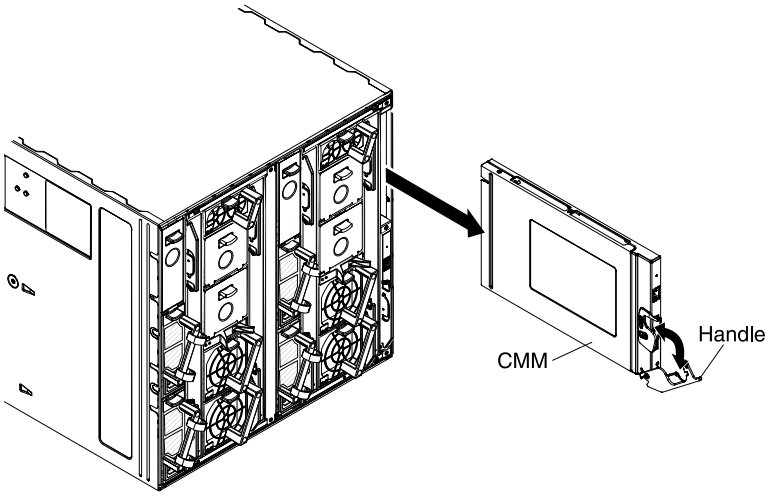
Note: These instructions assume that the chassis is connected to power.

Before you remove a CMM, complete the following steps.

Important: If you have just installed a standby CMM in the chassis, do not remove the primary CMM until the **Active** LED on the standby CMM is lit (indicating that the standby CMM is controlling the chassis). The standby CMM requires about 2 minutes to become active and receive initial status information and firmware from the primary CMM.

1. If the CMM that you are replacing is the only CMM in the chassis and the CMM is functioning, save the configuration file before you proceed.
   - In the CMM web interface, configurations are saved in the Manage Configuration page (select **Configuration** from the **Mgt Module Management** menu). All fields and options are described in the CMM web interface online help.
   - You can also use the **write** command in the CMM command-line interface (CLI). See " write command" in the *Flex System Chassis Management Module Command-Line Interface Reference Guide* for information about commands.
2. If you are removing the primary CMM in the chassis, stop all CMM local and remote sessions before you proceed, to avoid an unexpected termination of sessions.
3. Remove any external devices that block access to the rear of the chassis.
4. Disconnect all cables from the CMM.

To remove the CMM, complete the following steps.



Step 1. Press the release latch down and rotate the handle down until it stops, to disengage the CMM from the chassis.

Step 2. Slide the CMM out of the chassis and place it on a flat, static-protective surface.

Note: If the chassis has only one CMM and you remove the CMM, the fan modules will automatically accelerate to full speed. The fan modules will continue to run at full speed until the CMM is replaced.

Replacing a Chassis Management Module

Use these instructions to install a CMM in a Flex System chassis. You can install a CMM while the chassis is powered on.

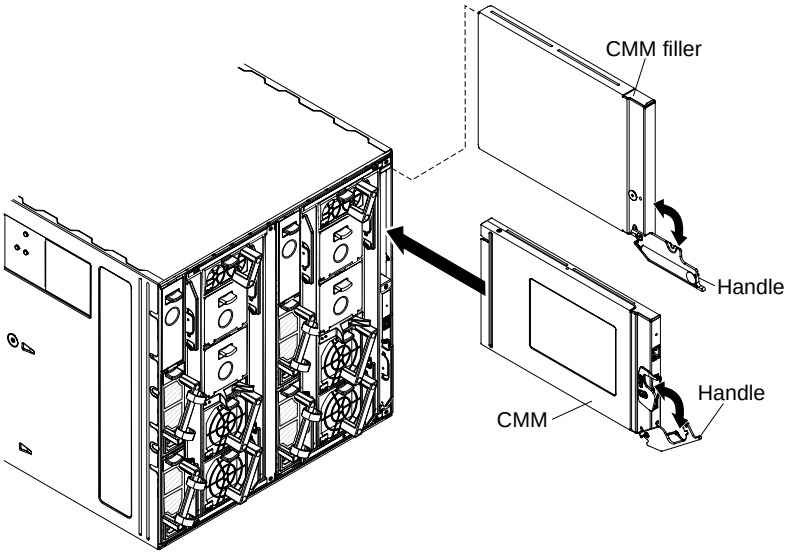
Note: If two CMMs are installed in a Flex System chassis, they should be of the same type.

Before you install the CMM, complete the following steps:

1. Read the installation instructions in the documentation that comes with the CMM.
2. If you are installing a standby CMM, see “Preparing for CMM redundancy” on page 27.
3. If you have not already done so, touch the static-protective package that contains the replacement CMM to an *unpainted* metal part of the chassis or any *unpainted* surface on any other grounded rack component for at least 2 seconds.

4. Remove the CMM from its static-protective package.

To install a Chassis Management Module (CMM), complete the following steps.



Step 1. If a filler is installed in the CMM bay, remove it. Rotate the release handle on the filler down and slide it out of the bay.

Step 2. Press the CMM release latch down and rotate the CMM handle down until it stops.

Step 3. Align the CMM with the bay and slide it into the bay until it is seated.

Step 4. Close the handle (rotate the handle up) so that it locks in place.

Note: Make sure that the power-on LED on the CMM is lit. This indicates that the CMM is operating correctly. See “CMM controls and indicators” on page 5 to locate the LED.

When you install a CMM, if the chassis is not connected to a DHCP server on the network, it takes up to 3 minutes for the CMM to use the default (static) IP address.

After failover, you might have to wait as long as 5 minutes to establish a network connection to the CMM. Some networks include switches, routers, and hubs that do not allow (or relay) an address resolution protocol (ARP) from the new CMM to update the network cached ARP table. Without this information relay, the new MAC address/IP association will not recognize the CMM. This condition will correct itself after the ARP table times out. To prevent this condition, reconfigure the network-routing setup tables to enable ARPs to be relayed from the CMM.

After you install the CMM, complete the following steps:

1. Replace any components that you removed to gain access to the CMM bay.
2. Connect all cables to the CMM.
3. Depending on your system configuration, you might have to manually configure the CMM:
   - If this is a standby CMM and you followed the instructions in “Preparing for CMM redundancy” on page 27, no configuration is necessary.

     Note: The standby CMM receives the configuration and status information automatically from the primary CMM. The transfer of information to the standby CMM can take up to 45 minutes after it is installed.
   - If this is the only CMM in the chassis, configure the new CMM:

- If you saved the CMM configuration file before you replaced the CMM, you can apply the saved configuration file to the replacement CMM.
  - In the CMM web interface, saved configurations are applied in the Manage Configuration page (select **Configuration** from the **Mgt Module Management** menu). All fields and options are described in the CMM web interface online help.
  - In the CMM command-line interface (CLI), use the **read** command (see "read command" in the *Flex System Chassis Management Module Command-Line Interface Reference Guide* for information about this command).
- If you did not save the CMM configuration file before you replaced the CMM, see Chapter 4 “Configuring the CMM” on page 23 for information.

Removing the battery

Use this information to remove the battery from the CMM.

Note: When a CMM is no longer needed, remove the battery and recycle or properly dispose of both the CMM and battery according to applicable local and national ordinances or regulations. (See the *Environmental Notices and User Guide* document on the Lenovo documentation CD for additional information.)

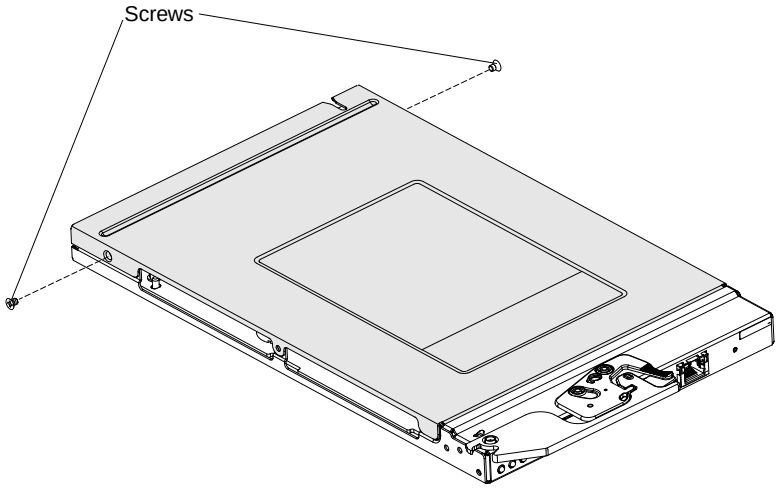
Before you remove the battery, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 9.
2. If the CMM is installed in an Flex System Enterprise Chassis, remove it (see “Removing a Chassis Management Module” on page 10 for instructions).

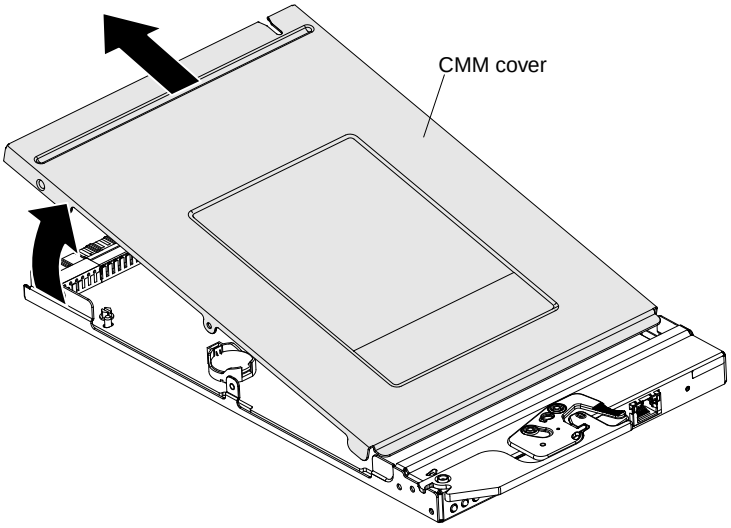
To remove the battery, complete the following steps:

Step 1. Carefully lay the CMM on a flat, static-protective surface, with the release handle side up, and the bezel pointing toward you.

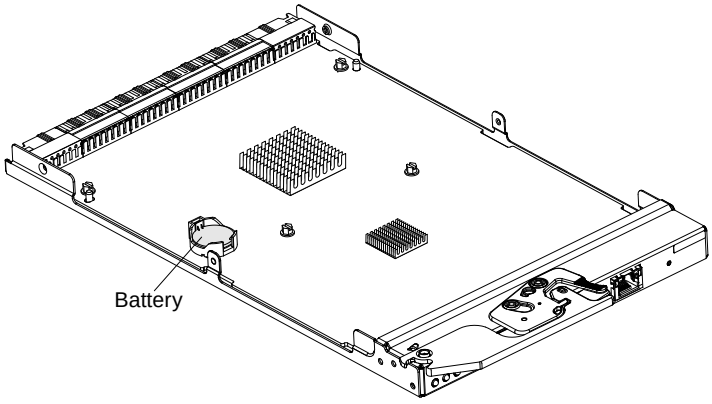
Step 2. Remove the screws on each side of the CMM cover, toward the rear of the CMM.



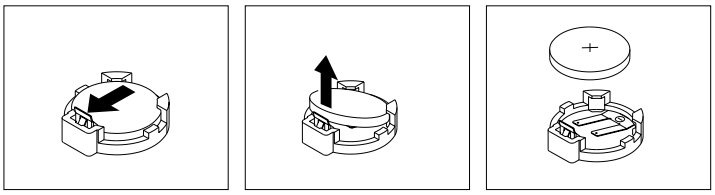
Step 3. Open and remove the CMM cover by lifting the rear edge.



Step 4. Locate the battery. The battery is typically toward the side of the CMM system board.



Step 5. Using your fingernail, press the battery retaining clip. The battery should pop free.



Step 6. Lift the battery from the socket.

After removing the battery, dispose of the battery as required by local ordinances or regulations.

Replacing the battery

Use this information to install the battery in the CMM.

Before you install the battery, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 9.
2. If the CMM is installed in an Flex System Enterprise Chassis, remove it (see “Removing a Chassis Management Module” on page 10 for instructions).

The following notes describe information that you must consider when you replace the battery in the Chassis Management Module:

- You must replace the battery with a lithium battery of the same type from the same manufacturer.
- To order replacement batteries, call 1-800-426-7378 within the United States, and 1-800-465-7999 or 1-800-465-6666 within Canada. Outside the U.S. and Canada, call your Lenovo sales representative or Lenovo reseller.
- After you replace the battery, you must reconfigure the Chassis Management Module and reset the date and time.
- To avoid possible danger, read and follow the following safety statement.

Statement 2

CAUTION:
When replacing the lithium battery, use only Part Number 33F8354 or an equivalent type battery recommended by the manufacturer. If your system has a module containing a lithium battery, replace it only with the same module type made by the same manufacturer. The battery contains lithium and can explode if not properly used, handled, or disposed of. *Do not:*

- **Throw or immerse into water**
- **Heat to more than 100° C (212° F)**
- **Repair or disassemble**

Dispose of the battery as required by local ordinances or regulations.

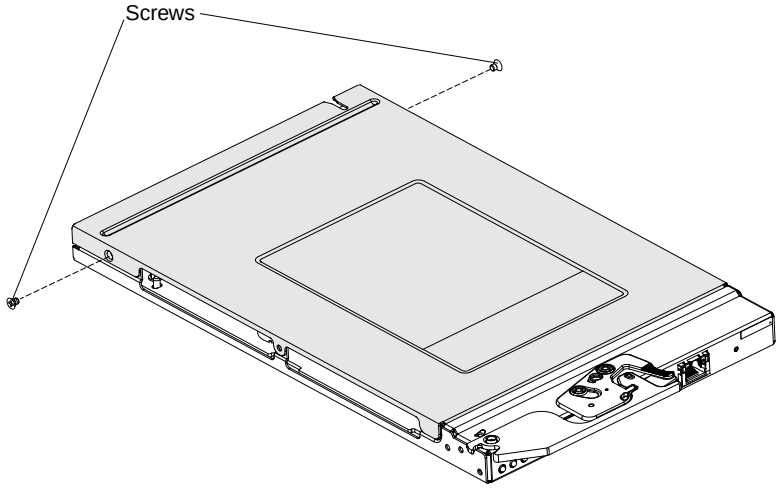
Attention: Touching the battery on a metal surface, such as the side of the Chassis Management Module, when you replace the battery can cause it to fail.

To install the battery, complete the following steps:

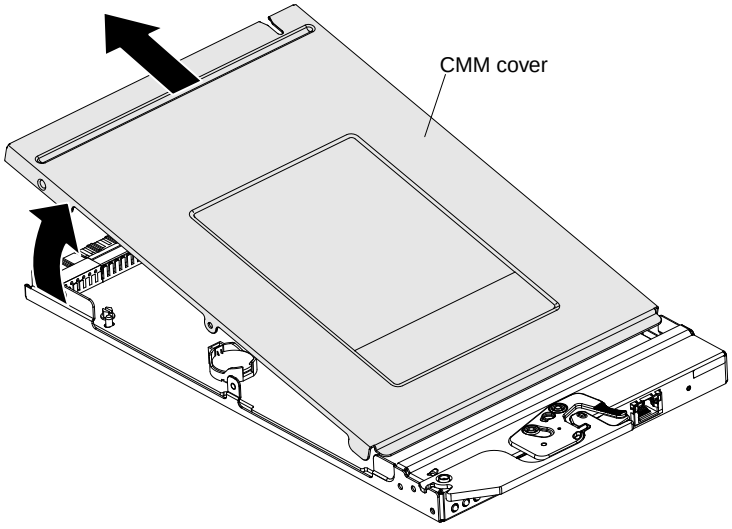
Step 1. Make sure that the CMM is on a flat, static-protective surface, with the release handle side up and the bezel pointing toward you.

Step 2. If the CMM cover is installed, remove it:

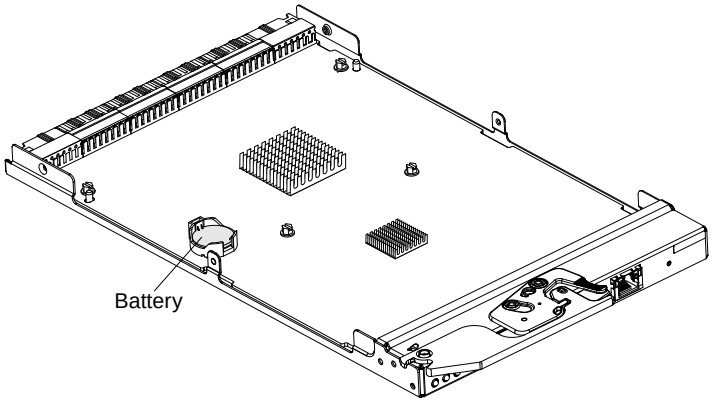
a. Locate and remove the screws on each side of the CMM cover, toward the rear of the CMM.



b. Open and remove the CMM cover by lifting the rear edge.

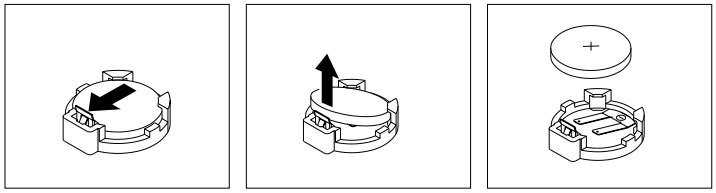


Step 3. Locate the battery. The battery is typically toward the side of the CMM system board.



Step 4. If a battery is already installed, remove it:

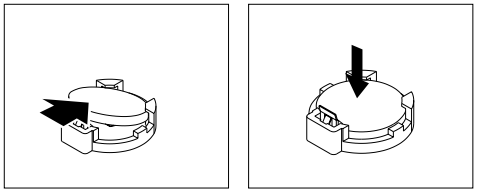
a. Using your fingernail, press the battery retaining clip. The battery should pop free.



b. Lift the battery from the socket.

Step 5. Follow any special handling and installation instructions that come with the battery.

Step 6. Tilt the battery so that you can insert it into the socket.

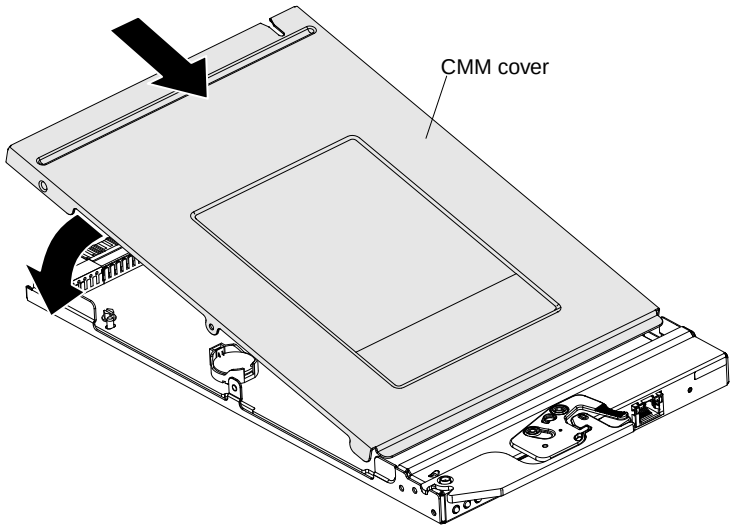


Step 7. As you slide the battery into place, press the battery down into the socket.

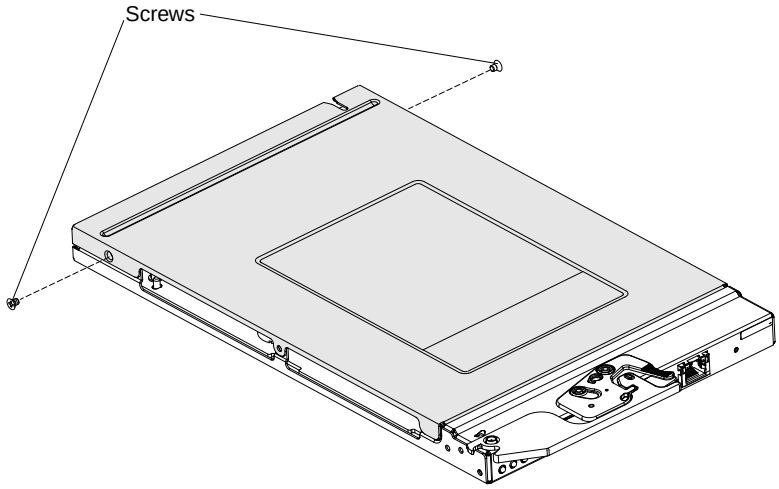
Step 8. Install the CMM cover:

a. Orient the cover so that the front edge of the cover slides into the slot on the CMM; then, lower the rear edge of the cover to close it.

Note: Before you close the cover, make sure that all components are installed and seated correctly and that you have not left loose tools or parts inside the CMM.



b. Install the screws on each side of the CMM cover, toward the rear of the CMM.



After you install the battery, complete the following steps:

1. Install the Chassis Management Module into the chassis (see “Replacing a Chassis Management Module” on page 11 and “Cabling the CMM” on page 19 for instructions).
2. Configure the Chassis Management Module (see Chapter 4 “Configuring the CMM” on page 23 for instructions).

Removing jumpers

Use this information to remove the jumpers from the CMM.

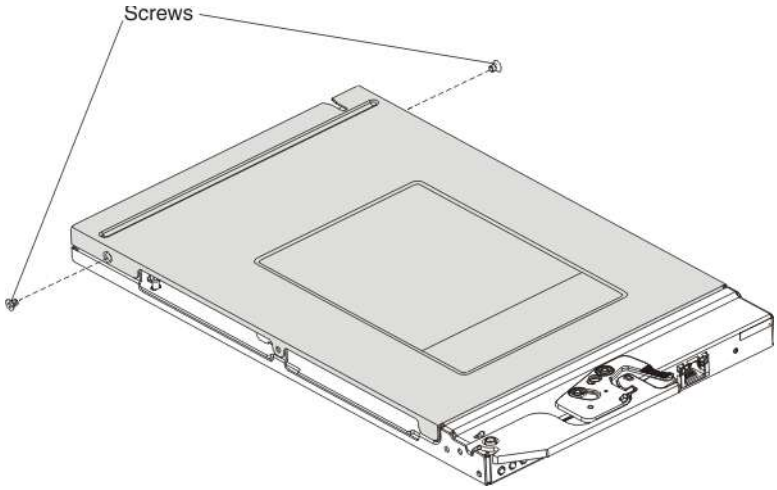
Before you remove the jumpers inside the CMM, complete the following steps:

1. Read “Safety” on page iii and “Installation guidelines” on page 9.
2. If the CMM is installed in an Flex System Enterprise Chassis, remove it (see “Removing a Chassis Management Module” on page 10 for instructions).

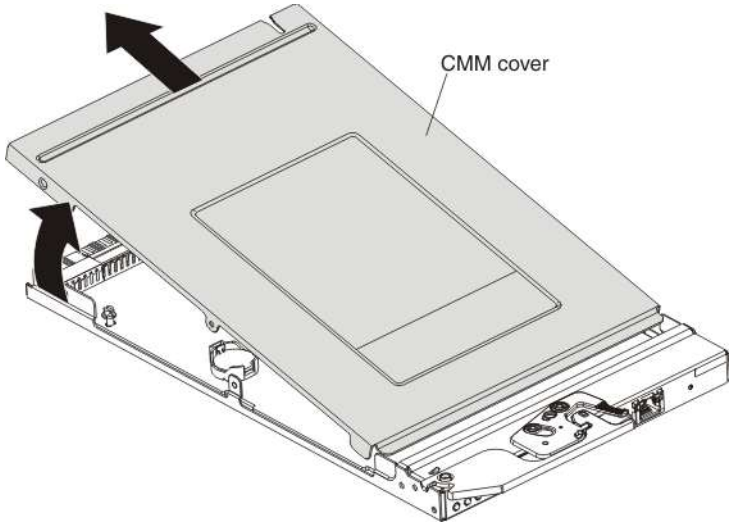
To remove the jumpers, complete the following steps:

Step 1. Carefully lay the CMM on a flat, static-protective surface, with the release handle side up, and the bezel pointing toward you.

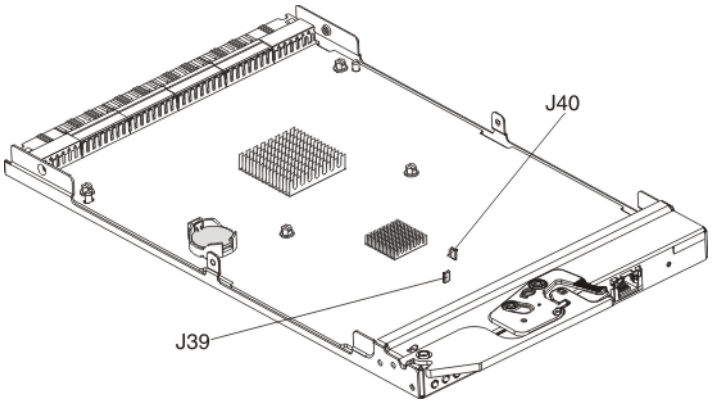
Step 2. Remove the screws on each side of the CMM cover, toward the rear of the CMM.



Step 3. Open and remove the CMM cover by lifting the rear edge.



Step 4. Locate jumpers J39 and J40. The jumpers are typically toward the center of the bezel end of the CMM system board.



Step 5. Remove jumpers J39 and J40, if either is installed.

After you remove the jumpers, complete the following steps:

1. Install the Chassis Management Module into the chassis (see “Replacing a Chassis Management Module” on page 11 and “Cabling the CMM” on page 19 for instructions).
2. Verify the Chassis Management Module configuration is correct and configure the Chassis Management Module, as necessary (see Chapter 4 “Configuring the CMM” on page 23 for instructions).

Cabling the CMM

You can cable the CMM to support a management connection that best matches your site configuration.

You must connect a client system to the CMM to configure and manage operation of the Flex System Enterprise Chassis. The CMM supports Ethernet (local or remote) and serial management connections.

You can manage the Flex System Enterprise Chassis by using the command-line interface that you access through Telnet or through the serial-management connector. You can also use the CMM web interface, which you access through the remote management and console (Ethernet) connector, to manage Flex System Enterprise Chassis devices. Use an SOL session through the CMM command-line interface, to access the operating system text console of a compute node or the system-management processor of compute nodes that have a Unified Extensible Firmware Interface (UEFI).

To access the CMM management interfaces, you need the following equipment and information:

- For connection through the CMM web interface:
  - A system with Ethernet connection capability. To facilitate connections at multiple locations, you can use a notebook computer.
  - The CMM IP address (the default CMM IP address is 192.168.70.100).
  - For networked connection to the CMM, a standard Ethernet cable and a local Ethernet network port (facility connection).
  - For direct connection of a system to the CMM remote management and console (Ethernet) connector, a standard Ethernet cable or an Ethernet crossover cable.
- For connection through the CMM CLI:
  - A system with Ethernet or serial connection capability. To facilitate connections at multiple locations, you can use a notebook computer.
  - The CMM MAC address (listed on the label on the CMM).
  - For networked connection to the CMM, a standard Ethernet cable and a local Ethernet network port (facility connection).

– For direct connection of a system to the CMM remote management and console (Ethernet) connector, a standard Ethernet cable or an Ethernet crossover cable.
– For serial connection of a system to the CMM mini-USB serial-management connector, a serial cable.

The following topics describe how to cable to the CMM to configure and manage the Flex System Enterprise Chassis.

Networked connection

You can use an Ethernet cable to connect the CMM to a management network.

To connect an Ethernet cable to the CMM for management network connection, complete the following steps:

Step 1. Connect one end of a Category 5 or higher Ethernet cable to the Ethernet connector of the CMM.
Step 2. Connect the other end of the Ethernet cable to the management network.
Step 3. Check the Ethernet LEDs on the CMM to make sure that the network connection is working. (See “CMM controls and indicators” on page 5 for Ethernet LED locations.)
- When the green Ethernet port link LED is lit, there is an active connection through the port to the network.
- When the green Ethernet port active LED is flashing, it indicates that there is activity through the port over the network link.

Direct client connection

You can use an Ethernet cable to connect the CMM directly to a client computer.

To connect a client computer directly to the CMM by using an Ethernet cable, complete the following steps.

Note: A CMM can perform an automatic media dependent interface (MDI) crossover, eliminating the need for crossover cables or cross-wired (MDIX) ports. You might have to use a crossover cable to connect your system to the CMM, if the network interface card in the client system is very old.

Step 1. Connect one end of a Category 5 or higher Ethernet cable or a Category 5 or higher Ethernet crossover cable to the Ethernet connector of the CMM.
Step 2. Connect the other end of the cable to the Ethernet connector on the client system.
Step 3. Check the Ethernet LEDs on the CMM to make sure that the network connection is working. (See “CMM controls and indicators” on page 5 for Ethernet LED locations.)
- When the green Ethernet port link LED is lit, there is an active connection through the port to the network.
- When the green Ethernet port active LED is flashing, it indicates that there is activity through the port over the network link.

Serial cable connection

You can use a serial cable to connect the CMM to a client computer or a serial-management network.

See “CMM serial port pin assignments” on page 6 for serial-management connector pin assignments.

Note: An optional cable kit with adapters is available to convert the CMM mini-USB connector for RJ-45, DB-9, or standard USB cable connection. See http://static.lenovo.com/us/en/serverproven/index.shtml for available Flex System options.

To connect a serial cable to the CMM for a management connection, complete the following steps:

Step 1. Connect one end of a serial cable to the mini-USB serial-management connector on the CMM.

Step 2. Connect the other end of the serial cable to the serial connector on the client system, such as a notebook computer, or to a serial-management network.

Step 3. Configure the serial device that the CMM connects to as follows:

a. Baud rate = 115200

b. Parity = none

c. Stop bits = 1

Chapter 4. Configuring the CMM

You configure only the primary CMM. If a standby CMM is installed, it receives the configuration and status information automatically from the primary CMM.

If a CMM is a replacement for the only CMM in the Flex System Enterprise Chassis and you saved the configuration file before you replaced the CMM, you can apply the saved configuration file to the replacement CMM (see “Restoring a saved CMM configuration” on page 24 for information).

When the Flex System Enterprise Chassis starts for the first time, the CMM automatically configures its remote management and console (Ethernet) connector (see “Configuring the CMM for remote access” on page 27 for information) so that you can establish a management connection.

All CMMs are preconfigured with the same static IP address. You must have a unique static IP address for each CMM.

If you do not use DHCP, you can add only one CMM at a time to the network for discovery. Adding multiple CMMs to the network without a unique IP address assignment for each will result in IP address conflicts.

Use either of the following tools to configure the CMM:

- The CMM web interface (see the *Flex System Chassis Management Module User's Guide*). To access the setup wizard, click **Initial Setup Wizard** button on the Manage Configuration page (select **Configuration** from the **Mgt Module Management** menu).
- The CMM CLI (see the *Flex System Chassis Management Module Command-Line Interface Reference Guide*).

Note: Some components such as CMMs, fan packs, fan mux cards, power supplies, and I/O modules for example, do not have a machine serial number. When a machine serial number is not available, the message Not Available is displayed in the command-line interface.

Updating the CMM firmware

Use this information to update the CMM to the latest release.

Attention: Installing the wrong firmware update might cause the CMM to malfunction. Before you install a firmware 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 version to the latest version.

Important: Some Flex System solutions require specific code levels or coordinated code updates. If the CMM is part of one of these solutions, verify that the level of code is supported for the solution before you update the code.

Note: For additional information about updating firmware for Flex System, see the *Firmware Update Best Practices Guide* athttps://support.lenovo.com/solutions/HT116912 (you might need to register to access this content).

If your Flex System Enterprise Chassis is configured for redundant operation and a second CMM is installed, both will have the same level of firmware after the primary CMM updates the standby CMM after it is installed. The latest level of CMM firmware is available at http://datacentersupport.lenovo.com.

You can update the CMM firmware in two ways:

- In the CMM web interface, select **Firmware** from the **Mgt Module Management** menu. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **update** command (see "update command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

If the CMM is not responsive over a network connection and you are unable to repair the problem, you might need to connect to the CMM directly (see “Resolving CMM connection problems” on page 35) or restore it to its default manufacturing configuration (see “Restoring the CMM manufacturing default configuration” on page 24) to establish a connection for updating firmware.

Restoring the CMM manufacturing default configuration

Use this information to restore the CMM to its manufacturing default configuration.

Attention: When you restore the CMM to its manufacturing default configuration, all configuration settings that you made are erased. Be sure to save your current configuration before you restore the CMM to its default configuration, if you intend use your previous settings.

You can restore the CMM to its manufacturing default configuration in three ways:

- In the CMM web interface, select **Reset to Defaults** from the **Mgt Module Management** menu. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **clear** command (see "clear command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).
- If you have physical access to the CMM, push the reset button and hold it for approximately 10 seconds (see “CMM controls and indicators” on page 5 for the reset button location).

For information about restoring a saved CMM configuration, see “Restoring a saved CMM configuration” on page 24 for information.

Restoring a saved CMM configuration

Use this information to restore a saved CMM configuration.

Attention: When you restore a saved CMM configuration, all current configuration settings are erased. Be sure to save your current configuration before you restore, if you intend use the current settings.

You can restore the CMM to a saved configuration in two ways:

- In the CMM web interface, a saved configuration is applied from the Manage Configuration page (select **Configuration** from the **Mgt Module Management** menu). See "Restoring a CMM configuration," in the *Flex System Chassis Management Module User's Guide*, for more information. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **read** command (see "read command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Saving a CMM configuration

Use this information to save a CMM configuration.

Attention:

- Please make sure local user account passwords are known **before** unmanaging from LXCA or FSM.
- Unmanage from LXCA or FSM **before** backing up the configuration.

- You should save the CMM configuration. Saving the configuration allows you to restore the saved settings if a CMM is replaced or if configuration information is corrupted or lost. You must save the CMM configuration before replacing a CMM or restoring a CMM to the manufacturing default configuration, if you intend to restore the configuration.
- If you are managing you chassis using an external management device, record the management device password in use at the time of the backup: this password will be required to restore the backup.

You can save the CMM configuration in two ways:

- In the CMM web interface, configurations are applied from the Manage Configuration page (select **Configuration** from the **Mgt Module Management** menu). See "Saving a CMM configuration," in the *Flex System Chassis Management Module User's Guide*, for more information. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **write** command (see "write command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

CMM reset

Use this information to reset the CMM.

The CMM supports three levels of reset:

- Standard reset (restart) performs an immediate reset and restart of the CMM.
- Service-level reset (virtual reseat) simulates removing the CMM from the chassis to remove power and then reinserting it.
- Resetting the CMM to its factory default configuration restarts the CMM and restores the CMM to its original unconfigured state.

You can reset a CMM when you have physical access to it or by using one of the CMM management interfaces (CMM web interface or the CMM command-line interface).

Reset procedures for when you have physical access to the CMM

If you have physical access to the CMM:

Standard reset (with physical access to CMM):
You can perform a standard reset (restart) of the CMM by pressing the reset button for between 1 and 10 seconds (see “CMM controls and indicators” on page 5 for more information).

Service-level reset (with physical access to CMM):
You can perform a service-level reset (virtual reseat) of the CMM by removing it from the chassis and then reinserting it (see “Removing a Chassis Management Module” on page 10 and “Replacing a Chassis Management Module” on page 11 for instructions).

Restore the CMM to its factory default configuration (with physical access to CMM):

You can restore the CMM to its factory default configuration by pressing the reset button for at least 10 seconds (see “CMM controls and indicators” on page 5 for more information).

Attention: When restoring the CMM to its factory default configuration by pressing the reset button, all CMM log files and configuration settings are lost.

- You will need to configure the CMM after restoring the CMM to its factory default configuration. Save the CMM configuration before restoring the CMM to its factory default configuration, if you intend to reuse your configuration settings (see “Saving a CMM configuration” on page 24 for information about saving up the CMM configuration).

- To retain the log files to assist with troubleshooting CMM problems during CMM replacement, restore the CMM to its factory default configuration using the CMM web interface or the CMM command-line interface, as described in the information that follows.

Important: Restoring the CMM to its factory default configuration takes several minutes. Do not remove power from the CMM or from the Flex System Enterprise Chassis while the CMM is restoring.

Reset procedures for using the CMM management interfaces

If you do not have physical access to the CMM, you can reset the CMM using the CMM web interface or the CMM command-line interface.

Standard reset (using a CMM management interface):

To performing a standard reset (restart) of the CMM using one of its management interfaces, complete one of the following procedures.

Important: All existing network connections will be temporarily lost when you reset the CMM. You will need to reconnect to the CMM after the reset completes.

- In the CMM web interface, select **Restart** from the **Mgt Module Management** menu. See "CMM management options," in the *Flex System Chassis Management Module User's Guide*, for more information. All fields and options are fully described in the CMM web interface online help. Several restart options are available for the Flex System Chassis Management Module, depending on your system configuration.
- In the CMM CLI, use the **reset** command (see "reset command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use). Several **reset** command options are available for the Flex System Chassis Management Module.

Service-level reset (using a CMM management interface):

To perform a service-level reset (virtual reseat) of the CMM using one of its management interfaces, complete one of the following procedures.

Attention: If you are managing your Flex System chassis using the optional Flex System Manager software, you must unmanage and remanage the chassis when performing service-level reset (virtual reseat) of the primary CMM. See http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.8731.doc/product_page.html for more information.

- In the CMM web interface, reset the CMM by choosing **Reset > Virtual Reseat** from the Service Reset tab on the Advanced Status page (select **Advanced Status > Service Reset** from the **Service and Support** menu). See "Service and support options," in the *Flex System Chassis Management Module User's Guide*, for more information. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **service -vr** command (see "service command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Restore the CMM to its factory default configuration (using a CMM management interface):

To restore the CMM to its factory default configuration using one of its management interfaces, complete one of the following procedures.

Attention: All existing network connections will be lost when you restore the CMM to its factory default configuration. You will need to configure the CMM after restoring the CMM to its factory default configuration. Save the CMM configuration before restoring the CMM to its factory default configuration,

if you intend to reuse your configuration settings (see “Saving a CMM configuration” on page 24 for information about saving up the CMM configuration).

Important: When restoring the CMM to its factory default configuration, you should retain the log files to assist with troubleshooting CMM problems during CMM replacement. Log information is retained automatically when restoring the factory default configuration using the CMM CLI and is the default selection when restoring the factory default configuration using the CMM web interface.

- In the CMM web interface, to reset the CMM, select **Reset to Defaults** from the **Mgt Module Management** menu; then, click **OK** to confirm. You can remove the check from **Preserve Logs** , if you do not wish to save log files. See "Resetting the CMM to manufacturing defaults," in the *Flex System Chassis Management Module User's Guide*, for more information. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **clear -cfg** command (see "clear command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Important: Restoring the CMM to its factory default configuration takes several minutes. Do not remove power from the CMM or from the Flex System Enterprise Chassis while the CMM is restoring.

Configuring the CMM for remote access

Use this information to understand how remote access is configured for the CMM.

After you connect the primary CMM to the network, the remote management and console (Ethernet) port connection, which is used for remote access, is automatically configured in either of the following ways:

- If there is an accessible, active, and configured DHCP server on the network, the host name, IP address, gateway address, subnet mask, and Dynamic Name Server (DNS) server IP address are set automatically.
- If the DHCP server does not respond within 3 minutes after the port is connected to the network, the CMM uses the manufacturing default URL (IPv4 static IP address) and default subnet address. The CMM is inaccessible during this time.

To connect to the CMM via the remote management and console (Ethernet) port by using a web browser or Telnet, use the following information:

- If the IP address was assigned through a DHCP server, get the IP address from your network administrator. If the IP configuration was assigned by the DHCP server, the network administrator can use the MAC address of the CMM network interface to determine which IP address and host name are assigned.
- The manufacturing default URL (IPv4 static IP address) is 192.168.70.100, the default subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxx* is the burned-in media access control (MAC) address.

Note: The MAC address is on the identification label on the side of the CMM. Information that you need to connect to the CMM for the first time is on the network access tag that is attached to the front of the CMM (see “CMM network access tag” on page 29 for information). Note that a network access tag might have been removed from your CMM during installation.

Preparing for CMM redundancy

Use these instructions to prepare your CMM for redundant operation.

To prepare your CMM for redundancy, complete the following steps:

Step 1. Install the standby CMM in the available CMM bay.

Step 2. Wait approximately 2 minutes while the primary CMM transfers firmware and configuration information to the standby CMM.

Notes:

- Whenever power is restored to an Flex System Enterprise Chassis that has two functional CMMs, the CMM in CMM bay 1 is typically prioritized as the primary CMM, even if the CMM in CMM bay 2 was the primary CMM before power was removed, however, sometimes the CMM in bay 2 will be prioritized, making it the primary CMM.
- For the most recent version of the optional Flex System Manager management software, which you can use to manage an Flex System Enterprise Chassis with a redundant CMM, go to http://datacentersupport.lenovo.com.

Step 3. Configure CMM failover response:

Configure failover response for loss of the primary CMM:

Note: Changes made to advanced failover settings take effect after the next reset of the primary CMM.

– In the CMM web interface, CMM failover is configured on the **Advanced Failover** page on the Management Module Properties page (select **Properties** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.

– In the CMM CLI, use the **advfailover** command (see "advfailover command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Configure failover response for loss of the management network (uplink) connection to the primary CMM:

Notes: Failure of the management network (uplink) connection to the primary CMM is indicated when all of the following conditions occur:

– Loss of CMM eth0 input and output packets

– Network noise

– Failures when pinging the CMM gateway and a designated station

– In the CMM web interface, uplink failover is configured on the **Ethernet** page on the Network Protocol Properties page (select **Network** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.

– In the CMM CLI, use the **uplink** command (see "uplink command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

– If an Flex System Enterprise Chassis is set up for redundant CMM operation and both CMMs experience an unrecoverable failure, the chassis will attempt to switch control between the CMMs indefinitely. If this condition occurs, replace one CMM to return the chassis to operation or replace both CMMs to return the chassis to redundant operation. Depending on how each CMM failed, you might need to configure the replacement CMM or restore its configuration from a backup, if one is available. A failure of both CMMs might be an indication of other problems with the Flex System Enterprise Chassis; make sure that the chassis is operating properly before replacing either CMM. See Troubleshooting chassis for information about diagnosing problems with a Flex System Enterprise Chassis.

Connecting to the CMM

Use these instructions to connect a client computer to the CMM as a remote console to perform configuration of the Flex System Enterprise Chassis.

Note: By default, the CMM does not have a fixed static IPv6 IP address. For initial access to the CMM in an IPv6 environment, you can either use the IPv4 IP address or the IPv6 link-local address. See “IPv6 addressing for initial connection” on page 30 for information about how to determine the IPv6 address to use for initial CMM access.

The CMM has the following default settings:

- IP address: 192.168.70.100
- Subnet: 255.255.255.0
- User ID: USERID (all capital letters)
- Password: PASSW0RD (note the number zero, not the letter O, in PASSW0RD)

By default, the CMM is configured to respond to DHCP first before it uses its static IP address.

The client computer that you connect to the CMM must be configured to operate on the same subnet as the CMM. The IP address of the CMM must also be in the same local domain as the client computer. To connect to the CMM for the first time, you might have to change the Internet Protocol properties on the client computer.

There are two built-in interfaces that you can use to connect to the CMM for the first time: the web interface and the CLI. If you are connecting to the CMM through an Ethernet connection, you can open a web browser and use the web interface, or you can use Telnet to connect to the CMM and use the CLI to configure the CMM. If you are connecting through a serial connection, you can use a terminal emulator to access the CLI.

Note: If your web browser advises you that a connection is untrusted or a security certificate is invalid, you might be able to correct the condition by removing and re-importing security certificates in your web browser or by switching to a different web browser. See "External authentication of certificates," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, and the documentation for your web browser for more information.

CMM network access tag

Information that you need to initially connect to the CMM is on the network access tag.

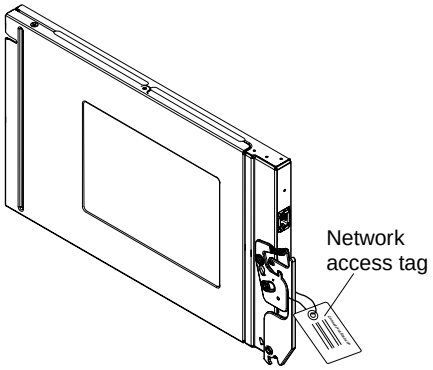
Important: Remove the network access tag from the CMM, before you install the CMM in an Flex System Enterprise Chassis.

The network access tag lists the following initial connection information for the CMM:

- MAC address
- Default host name
- IPv6 link local address (LLA)
- Default URL (IPv4 static IP address): 192.168.70.100
- Default user name (USERID)
- Default password (PASSW0RD, note the number zero, not the letter O, in PASSW0RD

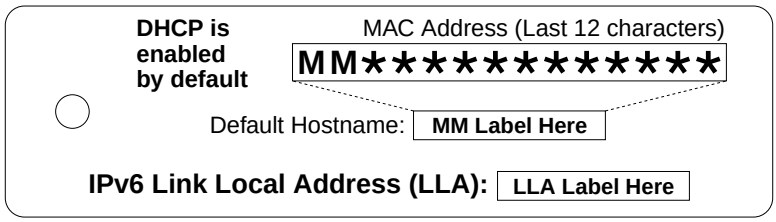
The network access tag is attached to the front of the CMM, as shown in the following illustration.

Note: If DHCP connection (default setting) fails, connection is attempted using the IPv4 static IP address.



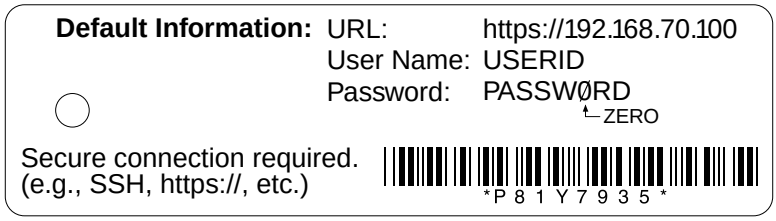
The front of the network access tag lists the CMM MAC address, default host name, and IPv6 link local address (LLA), as shown in the following illustration.

Front



The rear of the of the network access tag lists the CMM default URL (IPv4 static IP address), default user name, and default password, as shown in the following illustration.

Rear



IPv6 addressing for initial connection

When you use IPv6 addressing, use the IPv6 link-local address to complete the initial connection to the CMM.

The link-local address is a unique IPv6 address for the CMM that is automatically generated according to its MAC address. It is of the form `FE80::3BA7:94FF:FE07:CBD0`.

Determine the link-local address of the CMM in any of the following ways:

- Read the CMM link-local address on the network access tag that is attached to the front of the CMM (see “CMM network access tag” on page 29 for information). Note that the network access tag might have been removed from your CMM during installation.
- If you are able to log in to the CMM command-line interface (CLI) using IPv4 addressing, view the link-local address by using the **ifconfig** command (see "ifconfig command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

- If you are able to log in to the CMM web interface using IPv4 addressing, view the link-local address on the IPv6 page on the Ethernet page on the Network Protocol Properties page (select **Network** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.

If the CMM does not have a network access tag and you are unable to access the CMM by using IPv4, complete the following steps to calculate link-local address:

Step 1. Write down the MAC address of the CMM. It is on a label on the CMM, near the reset button. The label reads MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the MAC address. For example:

```
39-A7-94-07-CB-D0
```

Step 2. Split the MAC address into two parts and insert FF-FE in the middle.For example:

```
39-A7-94-FF-FE-07-CB-D0
```

Step 3. Convert the two hexadecimal digits at the left end of the string to binary.For example:

- **39**-A7-94-FF-FE-07-CB-D0
- **00111001**-A7-94-FF-FE-07-CB-D0

Step 4. Invert the value of bit 7 of the binary string.For example:

- 0011100**0**1-A7-94-FF-FE-07-CB-D0
- 0011101**1**1-A7-94-FF-FE-07-CB-D0

Step 5. Convert the binary digits at the left end of the string back to hexadecimal.For example:

- **00111011**-A7-94-FF-FE-07-CB-D0
- **3B**-A7-94-FF-FE-07-CB-D0

Step 6. Combine the hexadecimal digit pairs into 4-digit groups.For example:

- 3B**-**A7-94**-**FF-FE**-**07-CB**-**D0
- 3BA7-94FF-FE07-CBD0

Step 7. Replace dash (-) separators with colon (:) separators.For example:

- 3BA7**-**94FF**-**FE07**-**CBD0
- 3BA7**:**94FF**:**FE07**:**CBD0

Step 8. Add FE80:: to the left of the string.For example:

FE80::3BA7:94FF:FE07:CBD0

For a MAC address of 39-A7-94-07-CB-D0, the link-local address that is used for initial IPv6 access is FE80::3BA7:94FF:FE07:CBD0.

Ethernet connection

Use these instructions to connect to the CMM through an Ethernet connection to use the CMM web interface. The Ethernet connection is also used to connect to the CMM via SNMPv1 and SNMPv3.

Notes:

- The HTTP connection is not available when the CMM security policy is set to Secure (the manufacturing default setting). When the security policy is set to Secure, Ethernet connections must be made using HTTPS.
- Before you can connect to the CMM via SNMPv1 and SNMPv3, the CMM must be configured to use this protocol.

– For the CMM web interface, SNMP is configured in the **SNMP** tab on the Network Protocol Properties page (select **Network** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.
– For the CMM CLI, use the `snmp` command (see "snmp command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

After you connect an Ethernet cable from the client computer to the CMM (direct connection or through a network), complete the following steps to access the CMM web interface:

Step 1. Make sure that the subnet of the client computer is set to the same value as the CMM (the default CMM subnet is 255.255.255.0). The IP address of the CMM must also be in the same local domain as the client computer. To connect to the CMM for the first time, you might have to change the Internet Protocol properties on the client computer.

Step 2. Open a web browser on the client computer, and direct it to the CMM IP address.For the first connection to the CMM, use the default IP address of the CMM; if a new IP address has been assigned to the CMM, use that one instead.

Note: The manufacturing default static IPv4 IP address is 192.168.70.100, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the CMM, below the reset button (see “CMM controls and indicators” on page 5 for the reset button location). See “IPv6 addressing for initial connection” on page 30 for information about determining IPv6 addressing for the initial connection.

Step 3. Enter the CMM user name and password to start the remote session.

- The same user ID and password are used for all methods of connecting to the CMM. The password is case sensitive. The user ID is *not* case sensitive.
- The default CMM user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

Step 4. Follow the instructions on the screen and be sure to set the timeout value that you want for your web session.

Step 5. If you are connecting to the CMM for the first time, perform the initial configuration of the Flex System Enterprise Chassis.

Serial connection

You can connect to the CMM CLI through a serial connection.

After you connect the serial cable from the CMM to the client computer, complete the following steps:

Step 1. Make sure that the serial port settings of the client system match the settings of the serial port on the CMM.The default CMM serial port settings are as follows:

- Baud rate (BPS): 115200
- Data bits: 8
- Parity: no parity
- Stop bits: 1
- Flow control: none

Step 2. If any of the serial port settings for the client system were changed, reset the CMM.

Reset the CMM manually by pressing the reset button (see “CMM controls and indicators” on page 5 for the location of the reset button).

Attention: If you push the paper clip in all the way and hold it for approximately 10 seconds, the CMM is reset to the default configuration.

Reset the CMM by using the CMM CLI **reset** command (see "reset command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Reset the CMM by using the CMM web interface by selecting **Restart** from the **Mgt Module Management** menu. All fields and options are fully described in the CMM web interface online help.

Step 3. Open a terminal emulator window on the client computer and establish a connection to the CMM serial port.

Step 4. At the login prompt, type the CMM user ID. At the password prompt, type the CMM password.

- The same user ID and password are used for all methods of connecting to the CMM. The password is case sensitive. The user ID is *not* case sensitive.
- The default CMM user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

The CLI command prompt is displayed. You can now enter commands for the CMM.

Step 5. If you are connecting to the CMM for the first time, perform the initial configuration of the Flex System Enterprise Chassis (see Chapter 4 “Configuring the CMM” on page 23 for information).

Telnet connection

You can connect to the CMM CLI through a Telnet session.

Note: The Telnet connection is not available when the CMM security policy is set to Secure (the manufacturing default setting).

After you connect an Ethernet cable from the client computer to the CMM (direct connection or through a network), complete the following steps:

Step 1. Make sure that the subnet of the client computer is set to the same value as the CMM (default CMM subnet is 255.255.255.0). The IP address of the CMM must also be in the same local domain as the client computer. To connect to the CMM for the first time, you might have to change the Internet Protocol properties on the client computer.

Step 2. From a command prompt on the client computer, type `telnetip_address` (where *ip_address* is the CMM IP address), and press Enter. For the first connection to the CMM, use the default IP address of the CMM; if a new IP address has been assigned to the CMM, use that one instead.

Note: The manufacturing default static IPv4 IP address is 192.168.70.100, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the CMM, below the reset button (see “CMM controls and indicators” on page 5 for the location of the reset button). See “IPv6 addressing for initial connection” on page 30 for information about determining IPv6 addressing for initial connection.

Step 3. At the login prompt, type the CMM user ID. At the password prompt, type the CMM password.

- The same user ID and password are used for all methods of connecting to the CMM. The password is case sensitive. The user ID is *not* case sensitive.
- The default CMM user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

The CLI command prompt is displayed. You can now enter commands for the CMM.

Step 4. If you are connecting to the CMM for the first time, perform the initial configuration of the Flex System Enterprise Chassis (see Chapter 4 “Configuring the CMM” on page 23 for information).

Secure Shell (SSH) connection

You can connect to the CMM CLI through a Secure Shell (SSH) connection.

After you connect an Ethernet cable from the client computer to the CMM (direct connection or through a network), complete the following steps:

Step 1. Make sure that the SSH server on the Flex SystemCMM is enabled (SSH is enabled by default).

- In the CMM web interface:
  - Set the SSH port on the Port Assignments page on the Network Protocol Properties page (select **Network** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.
  - Enable the SSH server on the SSH Server page on the Security page (select **Security** from the **Mgt Module Management** menu). All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI:
  - Set the SSH port by using the **ports -sshe** command (see "ports command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).
  - Enable the SSH server by using the **sshcfg -cstatus** command (see "sshcfg command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Step 2. Start an SSH session to the CMM by using the SSH client of your choice. For example, if you are using the cygwin client, from a command prompt on the network-management workstation, type **sship_address (where *ip_address* is the CMM IP address), and press Enter.** For the first connection to the CMM, use the default IP address of the CMM; if a new IP address has been assigned to the CMM, use that one instead.

Note: The manufacturing default static IPv4 IP address is 192.168.70.100, the default IPv4 subnet address is 255.255.255.0, and the default host name is MM*xxxxxxxxxxxx*, where *xxxxxxxxxxxx* is the burned-in MAC address. The MAC address is on a label on the CMM, below the reset button. See “IPv6 addressing for initial connection” on page 30 for information about determining IPv6 addressing for the initial connection.

Step 3. At the login prompt, type the CMM user ID. At the password prompt, type the CMM password.

- The same user ID and password are used for all methods of connecting to the CMM. The password is case sensitive. The user ID is *not* case sensitive.
- The default CMM user name is USERID, and the default password is PASSW0RD (note the number zero, not the letter O, in PASSW0RD).

The CLI command prompt is displayed. You can now enter commands for the CMM.

Step 4. If you are connecting to the CMM for the first time, perform the initial configuration of the Flex System Enterprise Chassis (see Chapter 4 “Configuring the CMM” on page 23 for information).

SSH CLI exit codes

The SSH CLI commands return exit codes.

All CLI commands that are run in an SSH client single-command environment provide exit codes to indicate their outcomes. The following table shows exit codes that are supported; other exit codes are reserved for future use.

Table 1. SSH CLI exit codes

Name	Value (decimal)	Description
EX_OK	0	Successful command execution.
EX_USAGE	64	Command-line usage error: syntax error, wrong command arguments or number of arguments, or invalid command target.
EX_DATAERR	65	Input data error: invalid configuration file or SSH key parsing error.
EX_NOINPUT	66	The input file does not exist or is not readable.
EX_UNAVAILABLE	69	The command-line interface is not available: CLI oversubscribed, CLI disabled, or the data returned by a command has an unexpected value.
EX_SOFTWARE	70	Internal software error. Check the CMM event log for other error indications.
EX_TEMPFAIL	75	The command could not perform a write operation because the device or CMM was not in the correct state. Check for conflicting tasks or conditions and try to run the command again.
CLI_ERR_NOT_ AUTHORIZED	126	Authorization error: the user does not have sufficient privileges to execute the command.
CLI_ERR_CNF	127	Command not found.

Resolving CMM connection problems

Use this information to help solve problems connecting to your CMM.

If you are unable to establish a connection to your CMM, check the following:

- Make sure that the CMM port you are trying to access, the remote management and console (Ethernet) port or the serial port, is correctly cabled (see “Cabling the CMM” on page 19).
- To test a remote management and console (Ethernet) port connection, you can ping the IP address of the CMM.
- If you are unable to connect to your CMM via the remote management and console (Ethernet) port, connect to the CMM serial port and verify that the network configuration is correct by using the CMM CLI. See “Serial cable connection” on page 20 and “Serial connection” on page 32 for information about connecting to and using the CMM serial port. See the *Flex System Chassis Management Module Command-Line Interface Reference Guide* for information about the CMM CLI.
- See "External authentication of certificates," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about authentication of certificates.If a screen displays during connection with a message such as “The security certificate presented by this website was issued for a different website address” or “The certificate is only valid for the following names,” it might mean that you are accessing the website using a host name that is not listed in the certificate. Try to access the website using its IP address or, if there are no other certificate error messages on the page and you are confident that you are not experiencing an attack, select the button or link and continue to the website.
- If you are unable to connect to your CMM from all user accounts because you have forgotten the account IDs and passwords, you must restore the CMM to the manufacturing default configuration (see “Restoring the CMM manufacturing default configuration” on page 24 for information).

- If you are unable to connect to the CMM from a single user account because it has been locked, you can unlock it using the `users -unlock -n` *user_name* command (where *user_name* is the user account ID). See "users command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use.
- If your CMM is managed by an Flex System Manager management node and you are unable to connect to the CMM from a user account because it has been locked, you can unlock it through the Flex System Manager management software web interface. See "CMM access problems," in the *Flex System Manager Management Software Troubleshooting and Support Guide*, for information about command use.

CMM security

Unsecured systems-management tools can damage hardware and software and place your data at risk. You must understand all security risks in your system environment and what you can do to minimize these risks. The CMM offers advanced security capabilities and user-management settings to help you secure your environment.

Security policies

A CMM security policy is a set of security-related characteristics that define a particular level of protection from security exposures. The CMM security policies include hardware-related communication-protocol controls and account-related access controls.

The CMM enforces the chosen security policy for all Flex System Enterprise Chassis resources. The CMM offers two levels of security policy: *Legacy* and *Secure*. Security policies are not customizable, but you can modify the user account policies that the security policies access (see “User account policies” on page 37 for information).

An administrator or a user with administrative privileges can use the CMM CLI or web interface to change the security policy settings.

Important: If the security policy settings are changed after the compute nodes are up and running, the security policy status will remain in the Pending state until the compute nodes in the chassis have been restarted.

Secure security policy

The CMM Secure security policy is the most secure and least flexible setting that is available for your configuration.

The Secure security policy establishes a more restrictive chassis infrastructure with a higher level of control over users and chassis configuration. It helps secure the chassis environment and enforces the following conditions:

- Stronger complex password policies for CMM user accounts.

  Note: For more information about the default password policy settings for the Secure security policy, see “High user account policy settings” on page 40.
- Mandatory change of password for all user accounts at first login. Updated passwords that replace the manufacturing default passwords are required after the initial setup.
- Only secure communication protocols can be enabled. Communication protocols that are not secure are disabled: FTP, SNMPv1, Telnet, TFTP, FTP, and non-secure TCP command mode.

You can select the Secure security policy by using the CMM web interface or the CMM CLI.

Note: The compute node system-management processors need to be reset when changing the security policy. The compute node web interface indicates Flex System Enterprise Chassis components that must be restarted for security policy changes to take effect.

- In the CMM web interface, select **Security** from the **Mgt Module Management** menu; then, on the Security Policies page use the slider bar to select **Secure**, and click **Apply**. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **security -p secure** command (see "security command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Note: You cannot access the CMM CLI through Telnet while using the Secure security policy setting.

Legacy security policy

The CMM Legacy security policy is the least secure and most flexible setting that is available for your configuration.

The Legacy level of management software security policy provides flexibility in managing the chassis infrastructure, but this policy is the least secure. It permits the use of the following conditions:

- Weaker password policies for CMM user accounts

  Note: For more information about the default password policy settings for the Legacy security policy, see “Legacy user account policy settings” on page 41.
- No requirement that passwords for user accounts be changed at first login
- Availability of all communication protocols, both secure and unencrypted

You can select the Legacy security policy by using the CMM web interface or the CMM CLI.

Note: The compute node system-management processors need to be reset when changing the security policy. The compute node web interface indicates Flex System Enterprise Chassis components that must be restarted for security policy changes to take effect.

- In the web interface, select **Security** from the **Mgt Module Management** menu; then, on the Security Policies page use the slider bar to select **Legacy**, and click **Apply**. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **security -p legacy** command (see "security command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Note: You cannot access the CMM CLI through Telnet while using the Secure security policy setting.

User account policies

A CMM user account policy is a set of criteria that determine how CMM user account security, including passwords, is implemented.

User account policy conditions affect all users of the CMM. They help enforce the security policy that is chosen for the Flex System Enterprise Chassis environment (see “Security policies” on page 36 for information).

The CMM offers two initial user account policy choices: *Legacy* and *High*. You can customize the default values of each of these choices to create a *Custom* user account policy for your Flex System Enterprise Chassis chassis environment.

Although you can change individual user account policy settings from the default values for each user account policy type, the security policy of the CMM might require that specific user account policy settings have secure values. For example, if you attempt to change the CMM security policy level from Legacy to Secure, the CMM might require that you change some user account policy settings to secure values before you can change the security policy to Secure. However, if you change the CMM security policy from Secure to Legacy but you do not manually modify any of the user account policy settings, some of these setting will retain their previous secure values.

User account policy settings

You can modify the CMM user account policy settings to create a Custom policy.

The individual user account policy settings are configured to default values according to the security policy setting, Legacy or Secure, that is set for the CMM. Modifying any of the individual user account policy settings automatically sets the CMM user account policy to Custom. User account policy settings cannot conflict with the security policy setting that has been set for Flex System Enterprise Chassis resources. An error will occur if you attempt to set values that are incompatible.

You can view or modify the user account security policy settings from their default values using the CMM web interface or the CMM CLI:

- In the CMM web interface, user account security policy settings are on the General tab of the Account Security Level page in the Global Login Settings window. The location of each setting is identified in Table 2 “User account policy settings” on page 38. Access these settings as follows:
  1. Select **User Accounts** from the **Mgt Module Management** menu.
  2. Click **Global Login Settings** on the **Accounts** page on the User Accounts page.
  3. Click the **General** tab or the **Account Security Level** tab in the Global Login Settings window, as indicated for each setting.
  4. If you clicked the **Account Security Level** tab, select **Custom Security Settings** to access the custom settings.
- In the CMM CLI, access the user account security policy settings by using the various **accseccfg** command options (see "accseccfg command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

The following table lists the user account policy settings for the CMM, and their default values for the Legacy and High policy levels, if applicable. Also listed are the CMM web interface fields and CMM CLI **accseccfg** command options that can modify any values that can be changed in each interface.

Table 2. User account policy settings

User account policy setting	Description	Default Legacy setting	Default High setting	Web interface field	CLI command
User authentication method	The method for authenticating CMM users (local, LDAP, or both)	Retains the set value	Retains the set value	User authentication method *(**General** tab)*	`accseccfg -am`
Maximum simultaneous user sessions	The number of concurrent login sessions allowed for each user through all CMM interfaces	Retains the set value	Retains the set value	Number of simultaneous active sessions for LDAP users *(**General** tab)*	`accseccfg -mls`

Table 2. User account policy settings (continued)

User account policy setting	Description	Default Legacy setting	Default High setting	Web interface field	CLI command
Log new login events from same user	Whether the CMM logs multiple simultaneous login sessions from the same user	Retains the set value	Retains the set value	Do not log new authentication events for the same user *(**General** tab)*	`accseccfg -ici`
Authentication logging timeout	The amount of time that the CMM will not log repeated logins by the same user	Retains the set value	Retains the set value	Authentication logging timeout *(**General** tab)*	`accseccfg -alt`
Web session inactivity timeout	The amount of time a web interface session can be inactive before it automatically terminates	Retains the set value	Retains the set value	Web inactivity session timeout *(**General** tab)*	`accseccfg -wt`
CLI session inactivity timeout	The amount of time a CLI session can be inactive before it automatically terminates	Retains the set value	Retains the set value	CLI inactivity session timeout (in seconds) *(**General** tab)*	`accseccfg -ct`
User inactivity alert	The amount of time a user account can be inactive before it generates an alert	No limit	120 days	Inactivity alert period (in days) *(**Account Security Level** tab)*	`accseccfg -ia`
User inactivity disable	The amount of time a user account can be inactive before it is disabled and generates an alert	No limit	180 days	Inactivity alert and disable period (in days) *(**Account Security Level** tab)*	`accseccfg -id`
Maximum login failures	The maximum number of failed login attempts by a user before the account is locked out	20 attempts	20 attempts	Maximum number of login failures *(**Account Security Level** tab)*	`accseccfg -lf`
Lockout period login failure	The amount of time a user account is locked out after the maximum number of unsuccessful login attempts has been reached	2 minutes	60 minutes	Lockout period after maximum login failures (in minutes) *(**Account Security Level** tab)*	`accseccfg -lp`
Complex password	Whether the CMM follows more secure complex password rules	Off	On	Complex password rules *(**Account Security Level** tab)*	`accseccfg -cp`

Table 2. User account policy settings (continued)

User account policy setting	Description	Default Legacy setting	Default High setting	Web interface field	CLI command
Minimum number of different password characters	The minimum number of different character types that must be used in a password.	Not checked	2 characters	Minimum different characters in passwords *(**Account Security Level** tab)*	`accseccfg -dc`
Default 'USERID' account password must be changed on next login	The requirement that the default user must change the password at the next login in to the CMM	Off	On	Factory default 'USERID' account password must be changed on next login *(**Account Security Level** tab)*	`accseccfg -de`
Password change on first access	The requirement that users change their password the first time they log in to the CMM	Off	On	Force user to change password on first access *(**Account Security Level** tab)*	`accseccfg -pc`
Password expiration period	The amount of time a user password remains valid before requiring change	No limit	90 days	Password expiration period (days) *(**Account Security Level** tab)*	`accseccfg -pe`
Minimum password change interval	The minimum amount of time between user password changes	No limit	24 hours	Minimum password change interval (hours) *(**Account Security Level** tab)*	`accseccfg -pi`
Password reuse cycle	The number of password changes before a password can be reused	Not checked	5 cycles	Minimum password reuse cycle *(**Account Security Level** tab)*	`accseccfg -rc`

High user account policy settings

When the CMM security policy is set to Secure, aCMM user account policy of High can be used without modification.

The High user account policy establishes a higher level of control over users. It provides a more secure chassis environment than the Legacy setting. If the High user account policy is selected, you can override its default values to create a Custom policy by using the CMM web interface or the CMM CLI. See “User account policy settings” on page 38 for information about user account policy settings, how to modify these settings, and the differences between the High and Legacy user account policies.

You can select the user account security policy by using the CMM web interface or the CMM CLI:

- In the CMM web interface, to select the High user security policy, click **Mgt Module Management** and then select **User Accounts** from the menu. On the Accounts page, click **Global Login Settings**, and click the **Account Security Level** tab. Select **High Security Settings** from the menu and click **OK**. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the `accseccfg -high` command (see "accseccfg command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Legacy user account policy settings

When the CMM security policy is set to Legacy, CMM user account policy settings are not restricted. The default Legacy user account policy settings can be used or these settings can be modified.

The Legacy user account policy establishes a lower level of control over users. It provides a less secure chassis environment than the High setting. If the Legacy user account policy is selected, you can override its default values to create a Custom policy by using the CMM web interface or the CMM CLI. See “User account policy settings” on page 38 for information about user account policy settings, how to modify these settings, and the differences between the High and Legacy user account policies.

You can select the user account security policy by using the CMM web interface or the CMM CLI:

- In the CMM web interface, to select the Legacy security policy, click **Mgt Module Management** and select **User Accounts** from the menu. On the Accounts page, click **Global Login Settings**, and click the **Account Security Level** tab. Select **Legacy Security Settings** from the menu and click **OK**. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the `accseccfg -legacy` command (see "accesccfg command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Configuring NIST 800-131A compliance

The CMM can be configured to enforce NIST 800-131A cryptography for compute nodes in the chassis managed by the CMM and the CMM itself.

The CMM supports the National Institute of Standards and Technology (NIST) SP 800-131A compliance framework. This provides stricter cryptography options for the CMM and compute nodes in the chassis that are managed by the CMM. I/O modules are not presently subject to NIST compliance.

Two NIST mode settings are available for the Flex System chassis, **Compatibility** and **NIST SP 800-131A**. The default Compatibility setting enforces no restrictions on the allowed key lengths and algorithms. The NIST SP 800-131A setting only allows key lengths and algorithms acceptable by NIST SP 800-131A recommendations.

Note: A transition from Compatibility mode to NIST SP 800-131A mode is only allowed if compute nodes in the chassis have firmware installed that implements NIST SP 800-131A compliance levels, otherwise the transition is canceled and notification is sent to the user.

Enabling one of the two NIST modes affects cryptographic material generated on the CMM and externally generated cryptographic material that is imported to the CMM. The following is a list of user-accessible cryptographic items that might be affected by the configuration of NIST mode settings:

- X.509 certificates and their associated keys (CMM CA certificate, CMM certificate, compute node certificates, external LDAP certificates)
- CMM SSH server private key and user SSH public keys
- SNMPv3 user authentication and privacy algorithms selected in the CMM user interface

- Features on Demand (FoD) licenses on the CMM

When any of the previously listed user-accessible cryptographic items are not compliant, the NIST mode is changed to an intermediate *NIST SP 800-131A Custom* mode and waivers are created for each of the user-defined or externally provided cryptographic items requiring manual intervention to become compliant. After all non-compliant items are updated to be NIST SP 800-131A compliant, the system automatically transitions to the *NIST SP 800-131A Strict* mode. Waivers might be needed for the following items:

- External LDAP X.509 certificates or externally signed CMM Web certificate
- SNMPv3 user authentication or privacy algorithms selected in the CMM user interface
- Features on Demand (FoD) licenses on the CMM

There are additional TLS/SSL settings available for each of the two NIST mode settings. The TLS/SSL setting can be selected separately for each NIST mode. The following TLS/SSL settings are available from the **Mgt Module Management > Security** page, **Cryptography** tab:

- **Legacy:** No enforcement, SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2 are allowed.
- **TLS 1.2 Server Only:** Server applications on the CMM are restricted to TLS 1.2.
- **TLS 1.2 Server and Client:** Server and client applications on the CMM are restricted to TLS 1.2.

Important: When the CMM is in NIST SP 800-131A mode, **TLS 1.2 Server Only** or **TLS 1.2 Server and Client** modes are accepted. However, you must select **TLS 1.2 Server and Client** for the CMM to completely transition to the NIST SP 800-131A mode. If **TLS 1.2 Server Only** is selected, the CMM will not be able to transition to the NIST SP 800-131A mode, only to the intermediate NIST SP800-131A Custom mode.

Before transitioning from Compatibility mode to NIST SP 800-131A mode, there are some functions to consider. Most of these are completed automatically when transitioning from Compatibility mode to NIST SP 800-131A mode, however, the user must manually select the TLS version. Some of the automatic functions have limitations and additional action might be needed by the user. The following list contains functions and descriptions of any additional action that might be needed to achieve NIST SP 800-131A compliancy:

- Automatic certificate regeneration using NIST SP 800-131A compliant key lengths and hash algorithms: If a chassis CA certificate is imported into the browser trust store before changing to NIST SP 800-131A mode, when using a web interface to connect to a device in the chassis such as a compute node or CMM, a message about an untrusted server certificate will be displayed. To continue accessing the web interface, a new chassis CA certificate must be imported into the trust store. It is recommended that you do not ignore the untrusted server certificate message.
- Automatic SSH server keys regeneration using NIST SP 800-131A compliant key lengths: If you connected to the CMM using SSH protocol and added the SSH server to the CMM known hosts list before changing to NIST SP 800-131A mode, when connecting to the CMM through SSH after changing to NIST 800-131A mode, an error message will be displayed about server keys mismatch. To access the CLI using SSH, the CMM known host list must be updated with the new SSH server keys.
- Automatic selection of the algorithms used for encryption and hashing operations: To maintain NIST SP 800 -131A compliance, the selection of algorithms for all encryption is centrally-managed by the CMM, and strictly follows the cryptographic NIST SP 800-131A mode. Some protocols implemented on the CMM are not NIST SP 800-131A compliant. This is because some protocols strictly define the algorithm to be used. The following is a list of exceptions from the NIST 800-131A requirements, determined by the algorithm used:
  - SHA1 hashing algorithm can be used for SNMPv3 authentication while in NIST SP 800-131A mode.
  - SHA1 hashing can be used for IPMI while in NIST SP 800-131A mode.
- User configured **TSL/SSL:** The NIST SP 800-131A mode setting is activated only when the SSL/TLS mode is set to either **TLS 1.2 Server and Client** or **TLS 1.2 Server Only**. The TLS 1.2 Server Only option

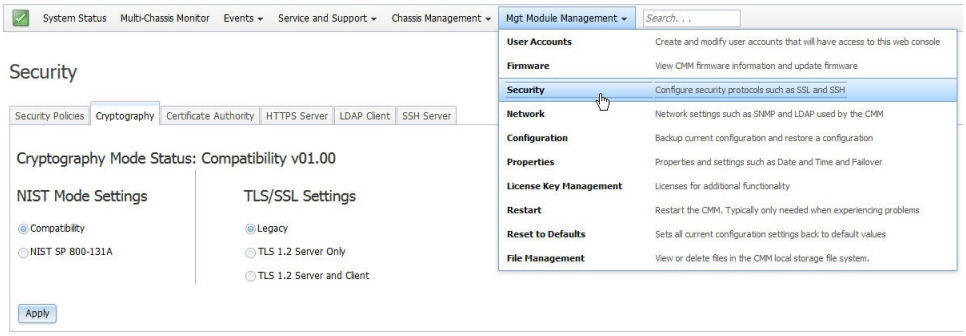
is only valid on the CMM. This is required to make sure that all TLS/SSL connections between chassis components or between chassis components and external entities meet the cryptographic requirements of NIST SP 800-131A. Setting this option to TLS 1.2 Server Only will cause the chassis to be placed in NIST SP 800-131A Custom mode, instead of the NIST SP 800-131A Strict mode. Consider the following guidelines about the limitations and possible effects of each TLS/SSL setting:

- **Legacy:** All TLS/SSL capable servers and clients use the default configuration. No functional limitation should be noticed by the user.
- **TLS 1.2 Server Only:** This value can be only be selected on the CMM. All TLS/SSL capable servers are configured to use only TLS 1.2. The user might not be able to connect to a component web interface, unless the web browser supports TLS 1.2. The latest versions of Internet Explorer and Chrome browsers support TLS 1.2, however in Internet Explorer support has to be enabled explicitly. Firefox supports TLS 1.2 beginning with version 27. Client connections from chassis components to external TLS/SSL capable servers should not be affected in any way.
- **TLS 1.2 Server and Client:** All TLS/SSL capable servers are configured to use only TLS 1.2. The user might not be able to connect to a component web interface unless the web browser supports TLS 1.2. The latest versions of Internet Explorer and Chrome browsers support TLS 1.2, however, support in Internet Explorer must be enabled explicitly. Firefox supports TLS 1.2 beginning with version 27. All client connections from chassis components to external TLS/SSL capable servers are configured to use TLS 1.2. If the external TLS/SSL capable servers do not support TLS 1.2, all client connections to those servers will fail. This limitation affects client connections for file transfer and authentication to external TLS/SSL capable LDAP servers. If the chassis is configured to use external authentication only and the external LDAP severs support TLS/SSL connections, but do not support TLS 1.2, setting the TLS 1.2 Server and Client value causes the user to be logged out and lose access to all chassis components. In this case it is recommended that you use the TLS 1.2 Server Only option.

You can set the cryptography mode for the CMM through the CMM web interface or from the command-line interface (CLI). To set the cryptography mode for the CMM through the CLI, use the `crypto` command. See “crypto command” in the *Flex System Chassis Management Module Command-Line Interface Reference Guide* for information.

To set the cryptography mode for the CMM through the web interface, use the following procedure:

1. From the CMM web interface click **Mgt Module Management > Security > Cryptography**.

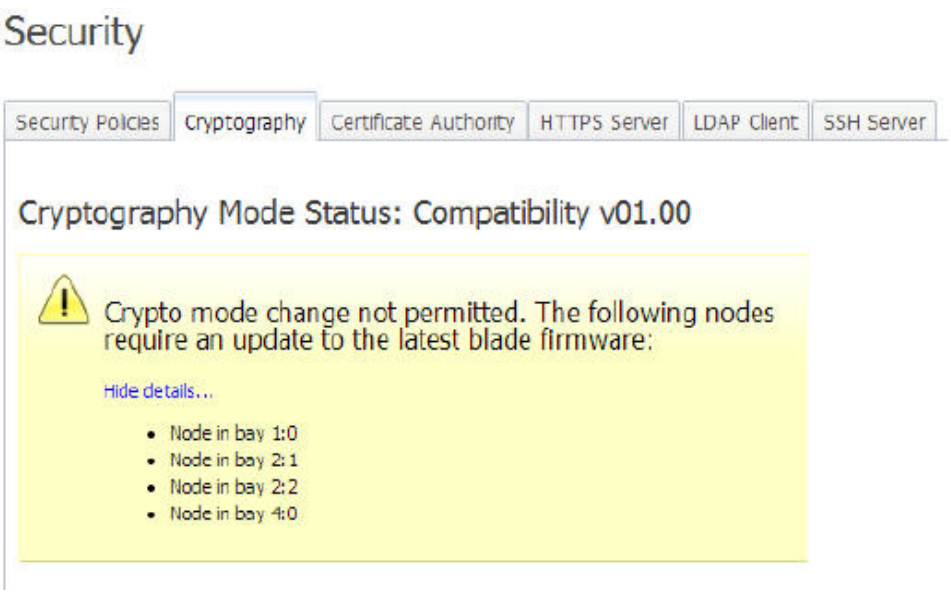


2. Select **NIST SP 800-131A**. The options for TLS/SSL settings will then be restricted to the following options, of which the user must select one:
   - **TLS 1.2 Server Only:** Starts the creation of waivers for uncompliant items.
   - **TLS 1.2 Server and Client:** Required option for the chassis to achieve NIST SP 800-131A Strict compliance.

Note: The option for Cipher Strength located at **Mgt Module Management > Security > Certificate Authority** is automatically restricted to **RSA2048-SHA256**, which is the only NIST SP 800-131A compliant option.

3. Click **Apply** and a cryptographic mode change message warning is displayed, stating that changing the cryptographic mode will reboot the CMM, but changing the TLS/SSL settings will only restart the associated services, and that both situations make the web interface unusable while processing. Click **OK** to make the change.
4. Restart the CMM for the changes to take effect. After restarting the CMM, check for uncompliant settings that are not automatically changed on the CMM. Each uncompliant setting will generate a waiver and the mode will be set to NIST SP 800-131A Custom. In this mode, new uncompliant cryptographic items cannot be configured on the CMM. If no waivers are generated, the mode will be NIST SP 800-131A Strict, and the Cryptography tab will indicate the mode.

Note: If all compute nodes and CMMs in the chassis do not have firmware that supports NIST SP 800-131A compliance, the mode change will fail and a message will appear, indicating the nodes that have uncompliant firmware.



For more information about achieving NIST 800-131A compliance for your chassis, see http://flexsystem.lenovofiles.com/help/topic/com.lenovo.acc.common.nav.doc/nist_implementing_a_compliant_environment.html?cp=0_2.

Communicating with the optional Flex System Manager management software

The optional Flex System Manager program communicates with the Flex System Enterprise Chassis through the remote management and console Ethernet port on the primary CMM.

To communicate with the Flex System Enterprise Chassis, the optional Flex System Manager management software needs a managed object (in the Group Contents pane of the optional Flex System Manager management console main window) that represents the Flex System Enterprise Chassis. If the CMM IP address is known, the network administrator can create an Flex System Manager managed object for the unit. If the IP address is not known, the optional Flex System Manager software can automatically discover the Flex System Enterprise Chassis (out-of-band, using the remote management and console Ethernet port on the CMM) and create a managed object for the unit.

For the optional Flex System Manager software to discover the Flex System Enterprise Chassis, your network must initially provide connectivity from the optional Flex System Manager management server to the CMM remote management and console (Ethernet) connector. To establish connectivity, the CMM attempts to use DHCP to acquire its initial IP address for the remote management and console Ethernet port. If the DHCP request fails, the CMM uses the static IP address that is assigned to it. Therefore, the DHCP server (if used) must be on the management LAN for your Flex System Enterprise Chassis.

Note: For I/O-module communication with the optional Flex System Manager management server through the CMM remote management and console Ethernet port, the I/O-module internal network interface and the CMM external interfaces must be on the same subnet.

If you do not want to keep the manufacturing default static values, you can configure the static IP address, host name, and subnet mask for the CMM through the web interface or the CMM CLI.

Preparing site firewalls and proxies for the CMM call-home feature

You must configure your firewalls and proxy server to enable operation of the CMM call-home feature, if you have firewalls in your network.

The CMM must be able to access remote systems over the Internet to deliver call-home information. To enable this access, you must configure the firewalls and proxies in your network to allow access by the CMM.

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

Step 1. Identify the CMM ports that you will use for your systems-management configuration (see Table 3 “Required connections for the CMM call-home feature” on page 46) and make sure that these ports are open.

- In the CMM web interface, select the **Port Assignments** tab from the **Mgt Module Management > Network** page. Ensure that the ports you plan to use for your systems-management configuration are open. All fields and options are fully described in the CMM web interface online help.
- In the CMM CLI, use the **ports** command (see "ports command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Step 2. Make sure that a connection exists to the Internet address in Table 3 “Required connections for the CMM call-home feature” on page 46 that is required by the CMM call-home feature.

Notes:

- IP addresses can change, so use the DNS name when possible.
- If your CMM is configured for secure operation, the FTP port (port 21) will be disabled.

Table 3. Required connections for the CMM call-home feature

DNS name	IP address	Port(s)	Protocol(s)
www-945.ibm.com	IPv4: • 129.42.26.224 • 129.42.42.224 • 129.42.50.224 IPv6: • 2620:0:6C0:1::10-00 • 2620:0:6C2:1::10-00 • 2620:0:6C4:1::10-00	443 (HTTPS) 80 (default listener port) 21 (FTP) 22 (SFTP)	https, ftps
The following connections might not be required in all cases:			
eccgw01.boulder.ibm.com	207.25.252.197	443	https
eccgw02.rochester.ibm.com	129.42.160.51	443	https
www6.software.ibm.com	170.225.15.41	443	https
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216	443 80 (optional)	https, http
www-03.ibm.com	204.146.30.17	443 80 (optional)	https, http

Step 3. If the CMM does not have direct Internet access with your network configuration, make sure that the selected proxy server is configured to use basic authentication.

Make sure that the following items in the CMM are configured to support call-home communication using your network:

- Enable DNS in the CMM and configure it to match the DNS settings for your network.
  - In the CMM web interface, select the **DNS** tab from the **Mgt Module Management > Network** page, and check the **Enable DNS** checkbox. Ensure that the DNS settings match the DNS settings for your network. All fields and options are fully described in the CMM web interface online help.
  - In the CMM CLI, use the **dns** command (see "dns command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).
- If required for your network, enable the CMM service advisor HTTP proxy and configure it to match the proxy settings for your network.
  - In the CMM web interface, select the **IBM Support** tab from the **Service and Support > Settings** page. In the **Outbound Connectivity** section, check the **Use proxy** checkbox, then click **Apply**. All fields and options are fully described in the CMM web interface online help.
  - In the CMM CLI, use the **chconfig** command (see "chconfig command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

- Configure CMM service advisor contact information.
  - In the CMM web interface, select the **IBM Support** tab from the **Service and Support > Settings** page. Enter the service advisor contact information in the **Contact Information** section, then click **Apply**. All fields and options are fully described in the CMM web interface online help.
  - In the CMM CLI, use the **chconfig** command (see "chconfig command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).
- Accept all CMM service advisor terms and conditions and enable the CMM service advisor.
  - In the CMM web interface, select the **IBM Support** tab from the **Service and Support > Settings** page. Check the **Enable IBM Support** checkbox, then click **Apply**. All fields and options are fully described in the CMM web interface online help.
  - In the CMM CLI, use the **chconfig** command (see "chconfig command," in the *Flex System Chassis Management Module Command-Line Interface Reference Guide*, for information about command use).

Chapter 5. Parts listing - Chassis Management Module

Replaceable components are available for the Flex System Enterprise ChassisChassis Management Module.

Replaceable components are of four types:

- **Consumable part:** Purchase and replacement of consumable parts (components, such as batteries and printer cartridges, that have depletable life) is your responsibility. If Lenovo acquires or installs a consumable part at your request, you will be charged for the service.
- **Field replaceable unit (FRU):** FRUs must be installed only by a trained service technician, unless they are classified as customer replaceable units (CRUs).
  - **Tier 1 customer replaceable unit (CRU):** Replacement of Tier 1 CRUs is your responsibility. If Lenovo installs a Tier 1 CRU at your request, you will be charged for the installation.
  - **Tier 2 customer replaceable unit:** You may install a Tier 2 CRU yourself or request Lenovo to install it, at no additional charge, under the type of warranty service that is designated for your server.

For information about the terms of the warranty and getting service and assistance, see the *Warranty Information* document.

The replaceable components in the following table are Tier 1 CRUs.

Description	CRU part number (Tier 1)
Flex System Chassis Management Module	68Y7032
Battery, 3.0 volt	33F8354

Appendix A. Getting help and technical assistance

If you need help, service, or technical assistance or just want more information about Lenovo products, you will find a wide variety of sources available from Lenovo to assist you.

Use this information to obtain additional information about Lenovo and Lenovo products, and determine what to do if you experience a problem with your Lenovo system or optional device.

Note: This section includes references to IBM web sites and information about obtaining service. IBM is Lenovo's preferred service provider for the System x, Flex System, and NeXtScale System products.

Before you call

Before you call, make sure that you have taken these steps to try to solve the problem yourself.

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call.

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check http://static.lenovo.com/us/en/serverproven/index.shtml to make sure that the hardware and software is supported by your product.
- Go to http://datacentersupport.lenovo.com to check for information to help you solve the problem.
- Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.
  - Hardware and Software Maintenance agreement contract numbers, if applicable
  - Machine type number (Lenovo 4-digit machine identifier)
  - Model number
  - Serial number
  - Current system UEFI and firmware levels
  - Other pertinent information such as error messages and logs
- Go to http://www.ibm.com/support/entry/portal/Open_service_request to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The IBM service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

You can solve many problems without outside assistance by following the troubleshooting procedures that Lenovo provides in the online help or in the Lenovo product documentation. The Lenovo product documentation also describes the diagnostic tests that you can perform. The documentation for most systems, operating systems, and programs contains troubleshooting procedures and explanations of error messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Using the documentation

Information about your Lenovo system and preinstalled software, if any, or optional device is available in the product documentation. That documentation can include printed documents, online documents, readme files, and help files.

See the troubleshooting information in your system documentation for instructions for using the diagnostic programs. The troubleshooting information or the diagnostic programs might tell you that you need additional or updated device drivers or other software. Lenovo maintains pages on the World Wide Web where you can get the latest technical information and download device drivers and updates. To access these pages, go to http://datacentersupport.lenovo.com.

Getting help and information from the World Wide Web

Up-to-date information about Lenovo products and support is available on the World Wide Web.

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support is available at http://datacentersupport.lenovo.com. The most current version of the product documentation is available in the following product-specific Information Centers:

Flex System products:
http://flexsystem.lenovofiles.com/help/index.jsp

System x products:
http://systemx.lenovofiles.com/help/index.jsp

NeXtScale System products:
http://nextscale.lenovofiles.com/help/index.jsp

How to send DSA data

You can use the Enhanced Customer Data Repository to send diagnostic data to IBM.

Before you send diagnostic data to IBM, read the terms of use at http://www.ibm.com/de/support/ecurep/terms.html.

You can use any of the following methods to send diagnostic data:

- **Standard upload:**
http://www.ibm.com/de/support/ecurep/send_http.html
- **Standard upload with the system serial number:**
http://www.ecurep.ibm.com/app/upload_hw
- **Secure upload:**
http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Secure upload with the system serial number:**
https://www.ecurep.ibm.com/app/upload_hw

Creating a personalized support web page

You can create a personalized support web page by identifying Lenovo products that are of interest to you.

To create a personalized support web page, go to https://support.lenovo.com. From this personalized page, you can subscribe to weekly email notifications about new technical documents, search for information and downloads, and access various administrative services.

Software service and support

Through IBM Support Line, you can get telephone assistance, for a fee, with usage, configuration, and software problems with your Lenovo products.

For more information about Support Line and other IBM services, see http://www.ibm.com/services or see http://www.ibm.com/planetwide for support telephone numbers. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

Hardware service and support

IBM is Lenovo's preferred service provider for the System x, Flex System and NeXtScale System products.

You can receive hardware service through your Lenovo reseller or from IBM. To locate a reseller authorized by Lenovo to provide warranty service, go to http://www.ibm.com/partnerworld and click **Business Partner Locator**. For IBM support telephone numbers, see http://www.ibm.com/planetwide. In the U.S. and Canada, call 1-800-IBM-SERV (1-800-426-7378).

In the U.S. and Canada, hardware service and support is available 24 hours a day, 7 days a week. In the U.K., these services are available Monday through Friday, from 9 a.m. to 6 p.m.

Taiwan product service

Use this information to contact IBM Taiwan product service.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路 7 號 3 樓
電話：0800-016-888

IBM Taiwan product service contact information:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Appendix B. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc.
1009 Think Place - Building One
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, Flex System, System x, NeXtScale System, and x Architecture are trademarks of Lenovo in the United States, other countries, or both.

Intel and Intel Xeon are trademarks of Intel Corporation in the United States, other countries, or both.

Internet Explorer, Microsoft, and Windows are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

Other company, product, or service names may be trademarks or service marks of others.

Important notes

Processor speed indicates the internal clock speed of the microprocessor; other factors also affect application performance.

CD or DVD drive speed is the variable read rate. Actual speeds vary and are often less than the possible maximum.

When referring to processor storage, real and virtual storage, or channel volume, KB stands for 1 024 bytes, MB stands for 1 048 576 bytes, and GB stands for 1 073 741 824 bytes.

When referring to hard disk drive capacity or communications volume, MB stands for 1 000 000 bytes, and GB stands for 1 000 000 000 bytes. Total user-accessible capacity can vary depending on operating environments.

Maximum internal hard disk drive capacities assume the replacement of any standard hard disk drives and population of all hard-disk-drive bays with the largest currently supported drives that are available from Lenovo.

Maximum memory might require replacement of the standard memory with an optional memory module.

Each solid-state memory cell has an intrinsic, finite number of write cycles that the cell can incur. Therefore, a solid-state device has a maximum number of write cycles that it can be subjected to, expressed as `total bytes written` (TBW). A device that has exceeded this limit might fail to respond to system-generated commands or might be incapable of being written to. Lenovo is not responsible for replacement of a device that has exceeded its maximum guaranteed number of program/erase cycles, as documented in the Official Published Specifications for the device.

Lenovo makes no representations or warranties with respect to non-Lenovo products. Support (if any) for the non-Lenovo products is provided by the third party, not Lenovo.

Some software might differ from its retail version (if available) and might not include user manuals or all program functionality.

Recycling information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to:

http://www.lenovo.com/recycling

Particulate contamination

Attention: Airborne particulates (including metal flakes or particles) and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the device that is described in this document.

Risks that are posed by the presence of excessive particulate levels or concentrations of harmful gases include damage that might cause the device to malfunction or cease functioning altogether. This specification sets forth limits for particulates and gases that are intended to avoid such damage. The limits must not be viewed or used as definitive limits, because numerous other factors, such as temperature or moisture content of the air, can influence the impact of particulates or environmental corrosives and gaseous contaminant transfer. In the absence of specific limits that are set forth in this document, you must implement practices that maintain particulate and gas levels that are consistent with the protection of human health and safety. If Lenovo determines that the levels of particulates or gases in your environment have caused damage to the device, Lenovo may condition provision of repair or replacement of devices or parts on implementation of appropriate remedial measures to mitigate such environmental contamination. Implementation of such remedial measures is a customer responsibility.

Table 4. 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 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.

Federal Communications Commission (FCC) statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Lenovo is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that might cause undesired operation.

Industry Canada Class A emission compliance statement

This Class A digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Australia and New Zealand Class A statement

Attention: This is a Class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

European Union EMC Directive conformance statement

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class A Information Technology Equipment according to European Standard EN 55022. The limits for Class A equipment were derived for commercial and industrial environments to provide reasonable protection against interference with licensed communication equipment.

Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

Germany Class A statement

Deutschsprachiger EU Hinweis: Hinweis fr Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Deutschsprachiger EU Hinweis:Hinweis fr Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG (frher 89/336/EWG) zur Angleichung der Rechtsvorschriften ber die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbchern beschrieben zu installieren und zu betreiben. Des Weiteren drfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo bernimmt keine Verantwortung fr die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes ber die elektromagnetische Verträglichkeit von Betriebsmittein
Dieses Produkt entspricht dem Gesetz ber die elektromagnetische Verträglichkeit von Betriebsmitteln EMVG (frher Gesetz ber die elektromagnetische Verträglichkeit von Geräten). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG (frher 89/336/EWG) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz ber die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (frher Gesetz ber die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (frher 89/336/EWG), fr Geräte der Klasse A.

Dieses Gerät ist berechtigt, in bereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu fhren. Verantwortlich fr die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4:
Das Gerät erfllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Nach der EN 55022: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstrungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Manahmen durchzufhren und dafr aufzukommen.

Nach dem EMVG: Geräte drfen an Orten, fr die sie nicht ausreichend entstrt sind, nur mit besonderer Genehmigung des Bundesministers fr Post und Telekommunikation oder des Bundesamtes fr Post und Telekommunikation betrieben werden. Die Genehmigung wird erteilt, wenn keine elektromagnetischen Strungen zu erwarten sind. (Auszug aus dem EMVG, Paragraph 3, Abs. 4). Dieses Genehmigungsverfahren ist nach Paragraph 9 EMVG in Verbindung mit der entsprechenden Kostenverordnung (Amtsblatt 14/93) kostenpflichtig.

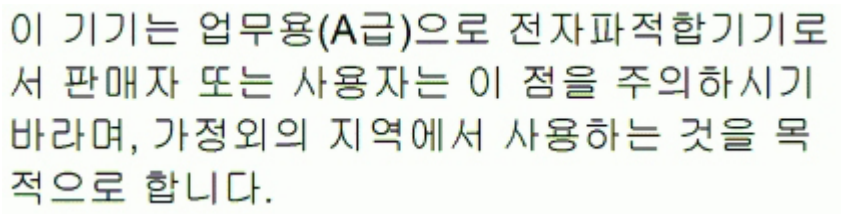
Anmerkung: Um die Einhaltung des EMVG sicherzustellen sind die Geräte, wie in den Handbchern angegeben, zu installieren und zu betreiben.

Japan VCCI Class A statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI). If this equipment is used in a domestic environment, radio interference may occur, in which case the user may be required to take corrective actions.

Korea Communications Commission (KCC) statement



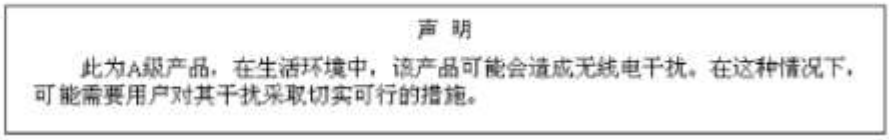
This is electromagnetic wave compatibility equipment for business (Type A). Sellers and users need to pay attention to it. This is for any areas other than home.

Russia Electromagnetic Interference (EMI) Class A statement

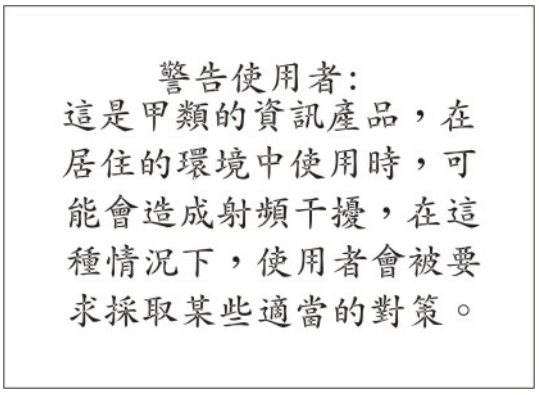
ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

People's Republic of China Class A electronic emission statement

中华人民共和国“A类”警告声明



Taiwan Class A compliance statement



Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

P

R

S

T

U

V

W

Lenovo

Part Number: SP47A31811

Printed in China

(1P) P/N: SP47A31811