Lenovo

ThinkSystem SE350 and ThinkSystem SE350 Enclosures
Setup Guide

Machine Type: 7Z46, 7D1X, 7D27, and 7D1R

Note

Before using this information and the product it supports, be sure to read and understand the safety information and the safety instructions, which are available at:
https://pubs.lenovo.com/safety_documentation/

In addition, be sure that you are familiar with the terms and conditions of the Lenovo warranty for your server, which can be found at:
http://datacentersupport.lenovo.com/warrantylookup

Thirty-sixth Edition (June 2024)

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 Informações 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.

Læs 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.

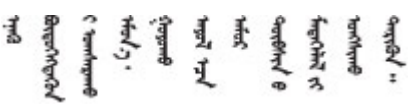
A termék telepítése előtt olvassa el a Biztonsági előírásokat!

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 Informações 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 información de seguridad.

Läs säkerhetsinformationen innan du installerar den här produkten.

ཐོན་རྫས་འདི་བདེ་སྤྱོད་མ་བྱས་གོང་། ·སྐྱོ་ཤི་ཡིད་གཟབ· བྱ་འདྲ་མེན་ཡོད་པའི་འོད་སྣེར་བལྟ་དགོས།

Bu ürünü kurmadan önce güvenlik bilgilerini okuyun.

ھەزكۇر مەھسۇلاتنى ئورنىتىشتىن بۇرۇن بىخەتەرلىك ئۇچۇرلىرىنى ئوقۇپ چىقىڭ.

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

Safety inspection checklist

Use the information in this section to identify potentially unsafe conditions with your server. As each machine was designed and built, required safety items were installed to protect users and service technicians from injury.

Notes:

1. The product is not suitable for use at visual display workplaces according to §2 of the Workplace Regulations.
2. The set-up of the server is made in the server room only.

CAUTION:
This equipment must be installed or serviced by trained personnel, as defined by the NEC, IEC 62368-1 & IEC 60950-1, the standard for Safety of Electronic Equipment within the Field of Audio/Video, Information Technology and Communication Technology. Lenovo assumes you are qualified in the servicing of equipment and trained in recognizing hazards energy levels in products. Access to the equipment is by the use of a tool, lock and key, or other means of security, and is controlled by the authority responsible for the location.

Important: Electrical grounding of the server is required for operator safety and correct system function. Proper grounding of the electrical outlet can be verified by a certified electrician.

Use the following checklist to verify that there are no potentially unsafe conditions:

1. Make sure that the power is off and the power cord is disconnected.
2. Check the power cord.
   - Make sure that the third-wire ground connector is in good condition. Use a meter to measure third-wire ground continuity for 0.1 ohm or less between the external ground pin and the frame ground.
   - Make sure that the power cord is the correct type.

     To view the power cords that are available for the server:

     a. Go to:

http://dcsc.lenovo.com/#/

b. Click **Preconfigured Model** or **Configure to order**.

c. Enter the machine type and model for your server to display the configurator page.

d. Click **Power → Power Cables** to see all line cords.

- Make sure that the insulation is not frayed or worn.

3. Check for any obvious non-Lenovo alterations. Use good judgment as to the safety of any non-Lenovo alterations.
4. Check inside the server for any obvious unsafe conditions, such as metal filings, contamination, water or other liquid, or signs of fire or smoke damage.
5. Check for worn, frayed, or pinched cables.
6. Make sure that the power-supply cover fasteners (screws or rivets) have not been removed or tampered with.

Chapter 1. Introduction

The ThinkSystem SE350 (Type 7Z46, 7D1X, and 7D27) is a new edge server offering. It is specifically designed to meet the needs of edge computing, edge AI, hybrid cloud, and workloads at the edge locations. ThinkSystem SE350 is a rugged compact sized edge solution with a focus on smart connectivity, business security and manageability for the harsh environment. Built for long life and dependable performance to support your demanding IoT workloads at the Edge. Compact and rugged it is designed for the non-datacenter environment, ideal for remote locations such as retail, manufacturing and factory locations.

Notes:

- *SE350 with Security Pack* is also known simply as *SE350* prior to July 2021.
- You can check whether your system is SE350 with Security Pack or SE350 Standard in Lenovo XClarity Controller.

SE350 with Security Pack	SE350 Standard (Security Pack disabled)
• SE350 automatic data protection, including intrusion sensor and motion sensor, can be enabled. • SED data access can be locked up at tamper events. • The system will need to be claimed and activated in order to unlock and access data. • Requires activation to boot up and fully functional.	• SE350 automatic data protection, including intrusion sensor and motion sensor, is disabled. • Data access will never be locked up. SED management is disabled. Tamper setting is disabled. • No activation is required. • Claiming the system is optional. Secure Activation Code is needed for claiming.

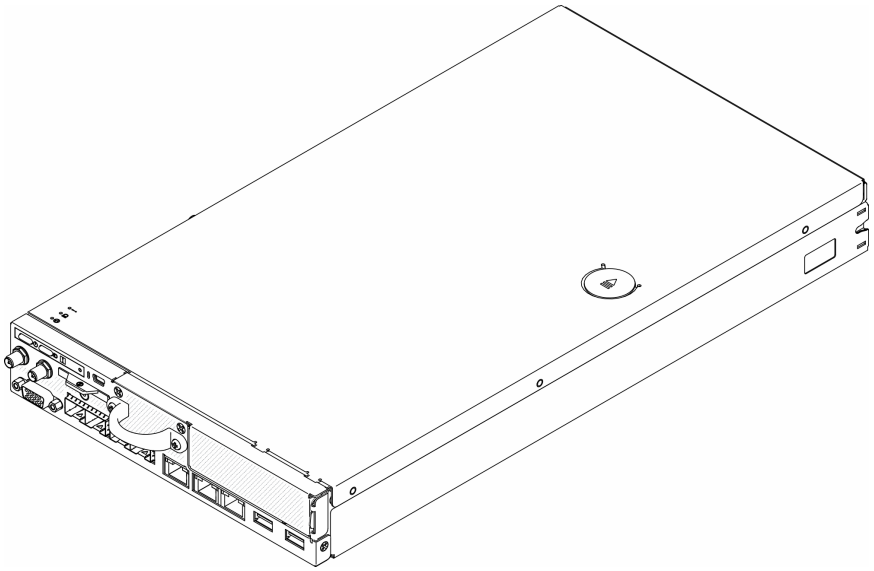


Figure 1. ThinkSystem SE350

The server comes with a limited warranty. For details about the warranty, see:
https://support.lenovo.com/us/en/solutions/ht503310

For details about your specific warranty, see:
http://datacentersupport.lenovo.com/warrantylookup

Server package contents

When you receive your server, verify that the shipment contains everything that you expected to receive.

The server package includes the following items:

Note: Some of the items listed are available on select models only.

- Server
- Rail installation kit (optional). Detailed instructions for installing the rail installation kit are provided in the package with the rail installation kit.
- Material box, including items such as power cords, rack installation template, and accessory kit.

Features

Performance, ease of use, reliability, and expansion capabilities were key considerations in the design of your server. These design features make it possible for you to customize the system hardware to meet your needs today and provide flexible expansion capabilities for the future.

Your server implements the following features and technologies:

- **Features on Demand**

  If a Features on Demand feature is integrated in the server or in an optional device that is installed in the server, you can purchase an activation key to activate the feature. For information about Features on Demand, see:

  https://fod.lenovo.com/lkms

- **Lenovo XClarity Controller (XCC)**

  The Lenovo XClarity Controller is the common management controller for Lenovo ThinkSystem server hardware. The Lenovo XClarity Controller consolidates multiple management functions in a single chip on the server system board.

  Some of the features that are unique to the Lenovo XClarity Controller are enhanced performance, higher-resolution remote video, and expanded security options. For additional information about the Lenovo XClarity Controller, refer to the XCC documentation compatible with your server at:

  https://pubs.lenovo.com/lxcc-overview/

  Important: Lenovo XClarity Controller (XCC) supported version varies by product. All versions of Lenovo XClarity Controller are referred to as Lenovo XClarity Controller and XCC in this document, unless specified otherwise. To see the XCC version supported by your server, go to https://pubs.lenovo.com/lxcc-overview/.

- **UEFI-compliant server firmware**

  Lenovo ThinkSystem firmware is Unified Extensible Firmware Interface (UEFI) compliant. UEFI replaces BIOS and defines a standard interface between the operating system, platform firmware, and external devices.

  Lenovo ThinkSystem servers are capable of booting UEFI-compliant operating systems, BIOS-based operating systems, and BIOS-based adapters as well as UEFI-compliant adapters.

  Note: The server does not support Disk Operating System (DOS).

- **Large system-memory capacity**

The server supports synchronous dynamic random-access memory (SDRAM) registered dual inline memory modules (DIMMs) with error correcting code (ECC). For more information about the specific types and maximum amount of memory, see “Specifications” on page 3.

- **Integrated network support**

  There two optional packages for the server: 10G SFP+ LOM Package or Wireless enabled LOM Package. You can utilize 10Gb SFP+ connectors, 10/100MB/1Gb conductors and WLAN function depending on the package you choose.

- **Integrated Trusted Platform Module (TPM)**

  This integrated security chip performs cryptographic functions and stores private and public secure keys. It provides the hardware support for the Trusted Computing Group (TCG) specification. You can download the software to support the TCG specification.

  For more information on TPM configurations, see “Enable TPM” in the *Maintenance Manual*.

  Note: For customers in Chinese Mainland, a Lenovo-qualified TPM 2.0 adapter or a TPM card may be pre-installed.

- **Large data-storage capacity**

  The server supports up to eight M.2 NVMe drives.

- **Front operator panel**

  Front operator panel provides LEDs to help you diagnose problems. For more information about the front operator panel, see “Front operator panel” on page 20.

- **Mobile access to Lenovo Service Information website**

  The server provides a QR code on the system service label, which is on the cover of the server, that you can scan using a QR code reader and scanner with a mobile device to get quick access to the Lenovo Service Information website. The Lenovo Service Information website provides additional information for parts installation, replacement videos, and error codes for server support.

- **Active Energy Manager**

  Lenovo XClarity Energy Manager is a power and temperature management solution for data centers. You can monitor and manage the power consumption and temperature of Converged, NeXtScale, System x, and ThinkServer servers, and improve energy efficiency using Lenovo XClarity Energy Manager.

- **Redundant cooling and optional power capabilities**

  The server supports a maximum of two 240-watt hot-swap power adapters and three internal fans, which provide redundancy for a typical configuration. The redundant cooling by the fans in the server enables continued operation if one of the fans fails.

- **ThinkSystem RAID support**

  The ThinkSystem RAID adapter provides hardware redundant array of independent disks (RAID) support to create configurations. The software RAID controller supports RAID levels 0, 1, 5, and 10.

Specifications

The following information is a summary of the features and specifications of the server. Depending on the model, some features might not be available, or some specifications might not apply.

Table 1. Server Specifications

Specification	Description
Security option (depending on the model)	• SE350 with Security Pack – SE350 automatic data protection, including intrusion sensor and motion sensor, can be enabled. – SED data access can be locked up at tamper events. – The system will need to be claimed and activated in order to unlock and access data. – Requires activation to boot up and fully functional. • SE350 Standard (Security Pack disabled) – SE350 automatic data protection, including intrusion sensor and motion sensor, is disabled. – Data access will never be locked up. SED management is disabled. Tamper setting is disabled. – No activation is required. – Claiming the system is optional. Secure Activation Code is needed for claiming. **Notes:** • *SE350 with Security Pack* is also known simply as *SE350* prior to July 2021. • You can check whether your system is SE350 with Security Pack or SE350 Standard in Lenovo XClarity Controller.
Size	Node • Height: 43.2 mm (1.7 inches) • Width: 209 mm (8.2 inches) • Depth: 376.1 mm (14.8 inches) E1 Enclosure (1U 2-node): • Height: 43 mm (1.69 inches) • Width: 439.2 mm (17.29 inches, from EIA bracket to EIA bracket) • Depth: 773.12 mm (30.44 inches) • Weight: 10 kg (with 1 node and 2 power adapters), 15 kg (with 4 power adapters) E2 Enclosure (2U 2-node): • Height: 86.9 mm (3.42 inches) • Width: 439.2 mm (17.29 inches, from EIA bracket to EIA bracket) • Depth: 476.12 mm (18.74 inches) • Weight: 10 kg (with 1 node and 2 power adapters), 15 kg (with 4 power adapters)
Weight	Node • Maximum: 3.6 kg (7.9 lbs)
Processor (depending on the model)	One Intel® Xeon® processor D-2100 product family **Notes:** 1. Use the Setup utility to determine the type and speed of the processors in the node. 2. For a list of supported processors, see https://serverproven.lenovo.com/server/se350.

Table 1. Server Specifications (continued)

Specification	Description
Memory	See "Memory module installation rules and order" on page 36 for detailed information about memory configuration and setup. • Slots: 4 DIMM slots • Minimum: 8 GB (1 x 8GB RDIMM) • Maximum: 256 GB (4 x 64GB LRDIMM) • Types: – TruDDR4 2666 MHz RDIMM: 8GB (1Rx8), 16GB (2Rx8), 32GB (2Rx4), 64GB (4Rx4) – TruDDR4 3200 MHz RDIMM: 16GB (2Rx8), 32GB (2Rx4) **Note:** For a list of supported memory modules, see https://serverproven.lenovo.com/server/se350.
M.2 drive	M.2 boot adapter • Supports up to two identical M.2 SATA drives • Supports three different physical sizes of M.2 drives: – 42 mm (2242) – 60 mm (2260) – 80 mm (2280) M.2 data adapter • PCIe and M.2 riser assembly: – Supports up to four M.2 SATA/NVMe drives • M.2 riser assembly – Supports up to eight M.2 NVMe drives – Supports up to four NVMe and four SATA drives • Supports four different physical sizes of M.2 drives: – 42 mm (2242) – 60 mm (2260) – 80 mm (2280) – 110 mm (22110) **Notes:** • M.2 drives installed on boot adapter and on data adapter are not swappable. • M.2 connector type: socket 3 (M key) • Mixing SATA drives and NVMe drives in the same M.2 SATA/NVMe 4-bay data adapter is not supported.
PCIe riser assembly	PCIe and M.2 riser assembly: • Slot 6: PCI Express 3.0 x16, (supports <75W, low profile, half-height, half-length PCIe adapter)

Table 1. Server Specifications (continued)

Specification	Description
WLAN	• WLAN: IEEE 802.11 a/b/g/n/ac • MIMO: 2x2 MIMO • Interfaces: WLAN: PCIe x1 • Antenna configuration: 2xIPEX (MHF4) connector • Form factor: M.2 2230 • Maximum number of concurrent user connection (AP mode): eight • Security: – AP mode supports WPA2 Personal – Station mode supports both WPA2 Enterprise and Personal • Working Band: – AP Mode: 2.4GHz – Station Mode: 2.4GHz/5GHz **Notes:** • WLAN performance may vary depending on your configuration and environment. • Wireless signal quality may be affected when installed in a rack or cabinet.
LTE	• 3GPP Release 11 • Category: Cat9 • Region: Global • Operating mode: FDD/TDD • Data transmission: up to 450Mbps DL/50Mbps UL • Function interface: USB 3.0 • Antenna configuration: 2xIPEX (MHF4) connector • Form factor: M.2 3042 **Notes:** • LTE performance may vary depending on your configuration and environment. • Wireless signal quality may be affected when installed in a rack or cabinet.

Table 1. Server Specifications (continued)

Specification	Description
Integrated functions	• Lenovo XClarity Controller, which provides service processor control and monitoring functions, video controller, and remote keyboard, video, mouse, and remote drive capabilities. • Front operator panel • LOM module connector (front of server): – 10G SFP+ LOM Package – Two USB 3.1 Gen 1 connectors – Two 1Gb Ethernet connectors – Two Lenovo XClarity Controller network connectors – Two 10Gb SFP+ connectors – One VGA connector – Wireless enabled LOM Package – Two USB 3.1 Gen 1 connectors – Two 1Gb Ethernet connectors – One Lenovo XClarity Controller network connector – Two 1Gb SFP connectors – Two 10Gb SFP+ connectors – One VGA connector – 10G BASE-T LOM Package – Two Lenovo XClarity Controller network connector – Two 10Gb BASE-T RJ45 connectors – Two 1Gb Ethernet connectors – Two USB 3.1 Gen 1 connectors – One VGA connector • Rear I/O connectors (rear of server): – Two WLAN Antenna connectors – One RS-232 port (RJ-45) – Two LTE Antenna connectors – Two USB 2.0 connectors – Two types of power distribution module: – 12V power distribution module (PDM) with two power connectors – -48V power distribution module (PDM) with one power connector
RAID controllers	Software RAID: A software RAID controller is integrated on the system board, supporting RAID levels 0, 1, 5, and 10. • Supports standard Intel SATA software RAID, RSTe • Supports Intel VROC NVMe RAID – VROC Intel-SSD-Only supports RAID levels 0, 1, 5, and 10 with Intel NVMe drives. – VROC Premium requires an activation key and supports RAID levels 0, 1, 5, and 10 with non-Intel NVMe drives. For more information about acquiring and installing the activation key, see https://fod.lenovo.com/lkms.

Table 1. Server Specifications (continued)

Specification	Description
	Hardware RAID: An M.2 hardware RAID module is needed for hardware RAID storage, supporting RAID levels 0 and 1.
Video controller (integrated into Lenovo XClarity Controller)	Matrox G200 • ASPEED • SVGA compatible video controller • Avocent Digital Video Compression • 16 MB of video memory (not expandable) **Note:** Maximum video resolution is 1920 x 1200 at 60 Hz.
Fans	Three 40 mm system fans
Power adapters	External power adapters: Sine-wave input (50–60 Hz) required • 240W external power adapter 100-127 V ac / 200-240 V ac, 3.2/1.6 A **Notes:** • Power adapters is supported only by 12V PDM **CAUTION:** – **Power adapters to the node must be with the same brand, power rating, wattage or efficiency level.** – **To distinguish the power adapters, check the size, the position of connector, and the label of the power adapters.** • When GPU is installed, system must be installed with two power adapters EU ErP (EcoDesign) Directive (2009/125/EC) Implementing Measure (COMMISSION REGULATION (EU) 2019/1782 of 1 October 2019) requires manufacturers to provide the energy efficiency and rating information. Lenovo products are designed to work with a range of compatible chargers and different chargers may be shipped in box or purchased subsequently. A list of suitable chargers can be found on the EU Declaration of Conformity (DoC) accessible here (https://www.lenovo.com/us/en/compliance/eu-doc). In order to access the applicable energy efficiency information for your charger, please access the following web page, search for your product using the full model number and select the applicable user guide or power supply data sheet. https://support.lenovo.com/

Table 1. Server Specifications (continued)

Specification	Description
Acoustical noise emissions (base configuration)	• Operation: – Minimum: 5.3 bels – Typical: 5.4 bels – Maximum: 5.7 bels • Idle – Minimum: 4.9 bels – Typical: 5.0 bels – Maximum: 5.4 bels **Notes:** 1. These sound power levels are measured in controlled acoustical environments according to procedures specified by ISO 7779 and are reported in accordance with ISO 9296. 2. The declared acoustic noise levels are based on specified configurations, which may change slightly depending on configurations/conditions. 3. The options supported in this server vary in function, power consumption, and required cooling. Any increase in cooling required by these options will increase the fan speed and generated sound level. The actual sound pressure levels measured in your installation depend upon a variety of factors, including: the number of racks in the installation; the size, materials, and configuration of the room; the noise levels of other equipment; the room ambient temperature and barometric pressure; and the location of employees in relation to the equipment.
Heat output	Approximate heat output: • Minimum configuration: 287.46 BTU per hour (84.25 watts) • Maximum configuration : 783.02 BTU per hour (229.49 watts)
Electrical input	Power distribution module: 12V PDM • Supports 12.2V/20A per power adapter • Each node supports up to two power adapters Power distribution module: -48V PDM • -48V - -60V DC / 8.4 A max direct -48V input **Notes:** • Power redundancy is in dual power mode when system power consumption is under 210W. • System operates in capping/throttling mode when power resource is insufficient. • Install two power adapters when system power consumption is higher than 210W.

Table 1. Server Specifications (continued)

Specification	Description
Cautions and regulatory compliance statements for NEBS	Follow NEBS GR-1089-CORE cautions, regulatory compliance statements, and requirements. • Supports Common Bonding Network (CBN) installation. • System can be installed in network telecommunication facilities where the National Electric Code applies. • It is required to turn ON UEFI “Power Restore Policy” when set the test condition in “MIN OPERATING VOLTAGE ” • The 1Gb Ethernet and SFP+ cables evaluated by NEBS measurement are required shielded. • The typical system boot up time under NEBS section 4 evaluation is 4 minutes and 55 seconds. • WARNING: The intra-building port(s) (1Gb Ethernet and SFP+ ports) of the equipment or subassembly is suitable for connection to intra-building or unexposed wiring or cabling only. The intra-building port(s) of the equipment or subassembly MUST NOT be metallically connected to interfaces that connect to the OSP or its wiring for more than 6 meters (approximately 20 feet). These interfaces are designed for use as intra-building interfaces only (Type 2 port as described in GR-1089) and require isolation from the exposed OSP cabling. The addition of Primary Protectors is not sufficient protection in order to connect these interfaces metallically to an OSP wiring system.
Environment	The ThinkSystem SE350 complies with ASHRAE class A4 specifications. System performance may be impacted when operating temperature is outside ASHRAE A4 Specification or fan failed condition outside A2 Specification. The ThinkSystem SE350 is supported in the following environment: • Standard: – Server on: 0°C to 45°C (32°F to 113°F) – Server off: 0°C to 45°C (32°F to 113°F) • ASHRAE Class A4 – Server on: 5°C to 45°C (41°F to 113°F); decrease the maximum ambient temperature by 1°C for every 125 m (410 ft) increase in altitude above 900 m (2,953 ft). – Sever off: 5°C to 45°C (41°F to 113°F) • Extended operation temperature (with limited configuration1): – Server on: 0°C to 55°C (32°F to 131°F) – Server off: 0°C to 55°C (32°F to 131 °F) **Notes:** Limited configuration1: – No GPU – No Micron/LITE-ON M.2 – Only Lenovo certified PCIe cards, for example: • ThinkSystem Broadcom NX-E PCIe 10Gb 2-Port Base-T Ethernet Adapter • ThinkSystem Mellanox ConnectX-4 Lx 10/25GbE SFP28 2-port PCIe Ethernet Adapter • Shipping/storage: -40 to 60°C (-40 to 140°F) • Maximum altitude: 3050 m (10 000 ft)

Table 1. Server Specifications (continued)

Specification	Description
	• Relative Humidity (non-condensing): – Operating: 8% to 90%, maximum dew point : 24°C (75.2°F) – Shipment/storage: 8% to 90%, maximum dew point : 27°C (80.6°F) • Non-operating (unpacked) storage can pass the following condition: 5% to 95% at 38.7°C (101.7°F) maximum dry-bulb temperature for 48 hrs. • Particulate contamination **Attention:** Airborne particulates and reactive gases acting alone or in combination with other environmental factors such as humidity or temperature might pose a risk to the server. For information about the limits for particulates and gases, see "Particulate contamination" in *ThinkSystem SE350 Maintenance Manual*. **Note:** ThinkSystem SE350 supports the use of a set of dust filter installed inside the enclosure front shipping bracket or the security bezel. The dust filter has a Minimum Efficiency Rating Vlue (MERV) of 4, per ASHRAE Standard 52.2–2017.
Operating systems	Supported and certified operating systems: • Microsoft Windows Server • VMware ESXi **Note:** Boot drives for **VMware ESXI**: For VMware ESXi boot support, only certain M.2 drives are supported, based on their endurance. For more specific information, see Lenovo support tip HT512201. • Red Hat Enterprise Linux • SUSE Linux Enterprise Server References: • Complete list of available operating systems: https://lenovopress.lenovo.com/osig. • OS deployment instructions: "Deploy the operating system" on page 122.

Shock and vibration specifications

The following information is a summary of the shock and vibration specifications of the server. Depending on the model, some features might not be available, or some specifications might not apply.

SE350 system configuration		Vibration (when server is in operation)	Shock (when server is in operation)	Environmental vibration criteria		
Left wing	Right wing			IEC Stationary 0.15Grms, 30mins15G, 11ms	3.06 Grms, 15mins 30G, 11ms	3.06 Grms, 60mins 30G, 11ms
Four M.2 SATA drives	None	3.06Grms, 3-500 Hz, 60 min/axis	30G, 11ms, half-sine, ±X, ±Y, ±Z	√	√	√
Four M.2 SATA drives	NVIDIA T4 GPU	3.06Grms, 3-500 Hz, 15 min/axis	30G, 11ms, half-sine, ±X, ±Y, ±Z	√	√	
Four M.2 NVMe drives (with heatsink)	Four M.2 NVMe drives (with heatsink)	0.21Grms, 5-500 Hz, 15 min/axis	15G, 3ms, half-sine, ±X, ±Y, ±Z	√		
Four M.2 NVMe drives (with heatsink)	NVIDIA T4 GPU	0.21Grms, 5-500 Hz, 15 min/axis	15G, 3ms, half-sine, ±X, ±Y, ±Z	√		

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 2. Limits for particulates and gases

Contaminant	Limits
Reactive gases	Severity level G1 as per ANSI/ISA 71.04-1985[1]: • The copper reactivity level shall be less than 200 Angstroms per month (Å/month ≈ 0.0035 µg/cm^2-hour weight gain).[2] • The silver reactivity level shall be less than 200 Angstroms per month (Å/month ≈ 0.0035 µg/cm^2-hour weight gain).[3] • The reactive monitoring of gaseous corrosivity must be conducted approximately 5 cm (2 in.) in front of the rack on the air inlet side at one-quarter and three-quarter frame height off the floor or where the air velocity is much higher.
Airborne particulates	Data centers must meet the cleanliness level of ISO 14644-1 class 8. For data centers without airside economizer, the ISO 14644-1 class 8 cleanliness might be met by choosing one of the following filtration methods: • The room air might be continuously filtered with MERV 8 filters. • Air entering a data center might be filtered with MERV 11 or preferably MERV 13 filters. For data centers with airside economizers, the choice of filters to achieve ISO class 8 cleanliness depends on the specific conditions present at that data center. • The deliquescent relative humidity of the particulate contamination should be more than 60% RH.[4] • Data centers must be free of zinc whiskers.[5]

[1] 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.

[2] The derivation of the equivalence between the rate of copper corrosion growth in the thickness of the corrosion product in Å/month and the rate of weight gain assumes that Cu_2S and Cu_2O grow in equal proportions.

[3] The derivation of the equivalence between the rate of silver corrosion growth in the thickness of the corrosion product in Å/month and the rate of weight gain assumes that Ag_2S is the only corrosion product.

[4] 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.

[5] Surface debris is randomly collected from 10 areas of the data center on a 1.5 cm diameter disk of sticky electrically conductive tape on a metal stub. If examination of the sticky tape in a scanning electron microscope reveals no zinc whiskers, the data center is considered free of zinc whiskers.

Management options

The XClarity portfolio and other system management options described in this section are available to help you manage the servers more conveniently and efficiently.

Overview

Options	Description
Lenovo XClarity Controller	Baseboard management controller (BMC). Consolidates the service processor functionality, Super I/O, video controller, and remote presence capabilities into a single chip on the server system board. **Interface** • CLI application • Web GUI interface • Mobile application • REST API **Usage and downloads** https://pubs.lenovo.com/lxcc-overview/
Lenovo XClarity Administrator	Centralized interface for multi-server management. **Interface** • Web GUI interface • Mobile application • REST API **Usage and downloads** http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html
Lenovo XClarity Essentials toolset	Portable and light toolset for server configuration, data collection, and firmware updates. Suitable both for single-server or multi-server management contexts. **Interface** • **OneCLI**: CLI application • **Bootable Media Creator**: CLI application, GUI application • **UpdateXpress**: GUI application **Usage and downloads** https://pubs.lenovo.com/lxce-overview/
Lenovo XClarity Provisioning Manager	UEFI-based embedded GUI tool on a single server that can simplify management tasks. **Interface** • Web GUI interface (BMC remote access) **Usage and downloads** https://pubs.lenovo.com/lxpm-overview/ **Important:** Lenovo XClarity Provisioning Manager (LXPM) supported version varies by product. All versions of Lenovo XClarity Provisioning Manager are referred to as Lenovo XClarity Provisioning Manager and LXPM in this document, unless specified otherwise. To see the LXPM version supported by your server, go to https://pubs.lenovo.com/lxpm-overview/.

Options	Description
Lenovo XClarity Integrator	Series of applications that integrate the management and monitoring functionalities of the Lenovo physical servers with the software used in a certain deployment infrastructure, such as VMware vCenter, Microsoft Admin Center, or Microsoft System Center while delivering additional workload resiliency. **Interface** GUI application **Usage and downloads** https://pubs.lenovo.com/lxci-overview/
Lenovo XClarity Energy Manager	Application that can manage and monitor server power and temperature. **Interface** • Web GUI interface **Usage and downloads** https://datacentersupport.lenovo.com/solutions/lnvo-lxem
Lenovo Capacity Planner	Application that supports power consumption planning for a server or rack. **Interface** • Web GUI interface **Usage and downloads** https://datacentersupport.lenovo.com/solutions/lnvo-lcp

Functions

Options		Functions							
		Multi-system mgmt	OS deploy-ment	System configu-ration	Firm-ware up-dates[1]	Event-s/alert moni-toring	Inven-tory/ logs	Pow-er mgmt	Power planning
Lenovo XClarity Controller				√	√[2]	√	√[4]		
Lenovo XClarity Administrator		√	√	√	√[2]	√	√[4]		
Lenovo XClarity Essen-tials toolset	OneCLI	√		√	√[2]	√	√[4]		
	Bootable Media Creator			√	√[2]		√[4]		
	UpdateXpress			√	√[2]				
Lenovo XClarity Provisioning Manager			√	√	√[3]		√[5]		
Lenovo XClarity Integrator		√	√[6]	√	√	√	√	√[7]	
Lenovo XClarity Energy Manager		√				√		√	
Lenovo Capacity Planner									√[8]

Notes:

1. Most options can be updated through the Lenovo tools. Some options, such as GPU firmware or Omni-Path firmware require the use of supplier tools.
2. The server UEFI settings for option ROM must be set to **Auto** or **UEFI** to update firmware using Lenovo XClarity Administrator, Lenovo XClarity Essentials, or Lenovo XClarity Controller.
3. Firmware updates are limited to Lenovo XClarity Provisioning Manager, Lenovo XClarity Controller, and UEFI updates only. Firmware updates for optional devices, such as adapters, are not supported.
4. The server UEFI settings for option ROM must be set to **Auto** or **UEFI** for detailed adapter card information, such as model name and firmware levels, to be displayed in Lenovo XClarity Administrator, Lenovo XClarity Controller, or Lenovo XClarity Essentials.
5. Limited inventory.
6. The Lenovo XClarity Integrator deployment check for System Center Configuration Manager (SCCM) supports Windows operating system deployment.
7. Power management function is supported only by Lenovo XClarity Integrator for VMware vCenter.
8. It is highly recommended that you check the power summary data for your server using Lenovo Capacity Planner before purchasing any new parts.

Chapter 2. Server components

Use the information in this section to learn about each of the components associated with your server.

Important product information

This section provides information to help you locate the following:

- **Machine type and model information:** When you contact Lenovo for help, the machine type, model, and serial number information help support technicians to identify your server and provide faster service. The model number and serial number are on the ID label. The following illustration shows the location of the ID label containing the machine type, model, and serial number.
- **FCC ID and IC Certification information:** The FCC and IC Certification information is identified by a label located on the edge server as shown in the following illustration.

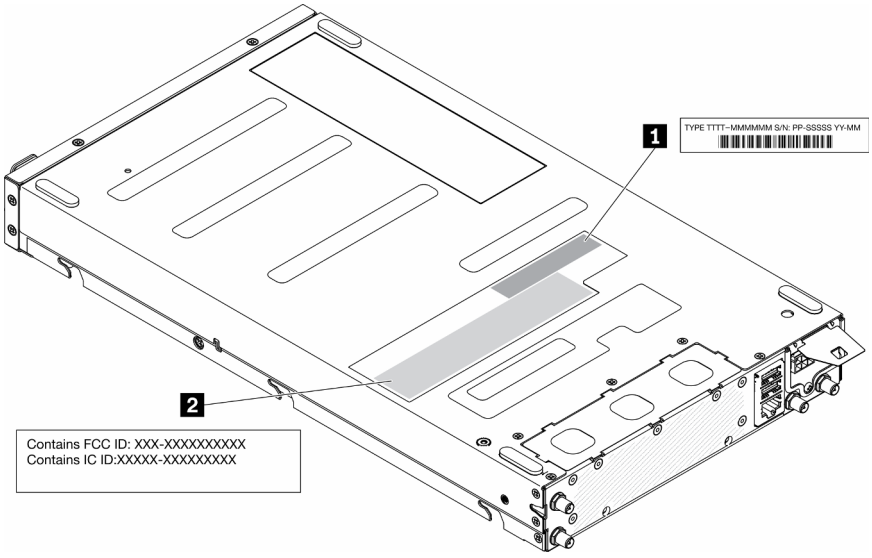


Figure 2. Location of the ID label and FCC ID/IC label

Table 3. ID label and FCC ID/IC label

1 ID label (machine type and model information)	**2** FCC ID and IC Certification label

For a preinstalled wireless module, this label identifies the actual FCC ID and IC certification number for the wireless module installed by Lenovo.

Note: Do not remove or replace a preinstalled wireless module by yourself. For module replacement, you must contact Lenovo service first. Lenovo is not responsible for any damage caused by unauthorized replacement.

Network access tag

The network access tag can be found on the front of the server. You can pull way the network access tag to paste your own label for recording some information such as the hostname, the system name and the inventory bar code. Please keep the network access tag for future reference.

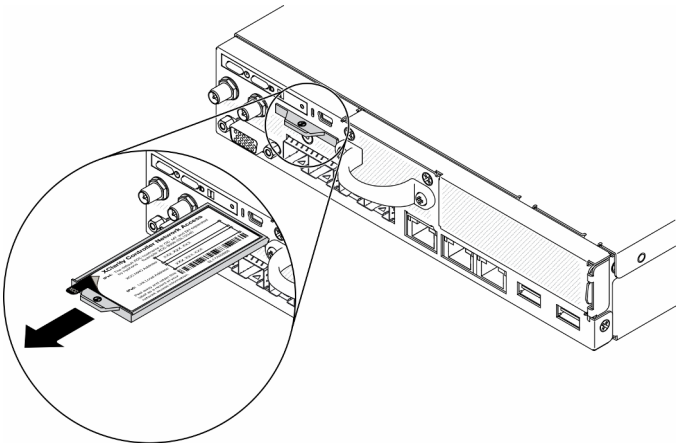


Figure 3. Location of the network access tag

QR code

In addition, the system Service Card that is located on the top cover of the server, provides a quick reference (QR) code for mobile access to service information. You can scan the QR code with a mobile device using a QR code reader application and get quick access to the Service Information web page. The Service Information web page provides additional information for parts installation and replacement videos, and error codes for server support.

Figure 4. SE350 QR code

Front view

The front view of the server varies by the model.

Front view of the server

- 10G SFP+ LOM Package

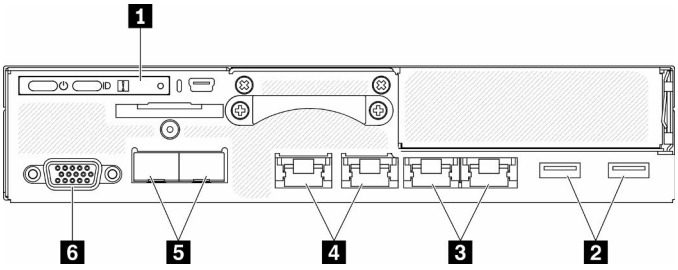


Figure 5. 10G SFP+ LOM Package front view

Table 4. Components on the 10G SFP+ LOM Package front view

1 Front operator panel	4 Shared XClarity Controller (XCC) network connectors The wrench icon on the connector indicates that this connector can be set to connect to Lenovo XClarity Controller. **Attention:** Only one network IP can be used. 2x RJ45 ports to support daisy-chain connection. The dual-port provide the ability to daisy-chain the Ethernet management connections thereby reducing the number of ports in the management switches and reducing the overall cable density needed for systems management. With this feature, user can connect the first XCC management port to the management network and the second XCC management port to the next server system.
2 USB 3.1 Gen 1 connectors	5 10Gb SFP+ Ethernet connectors
3 1Gb Ethernet connectors	6 VGA connector

- Wireless enabled LOM Package

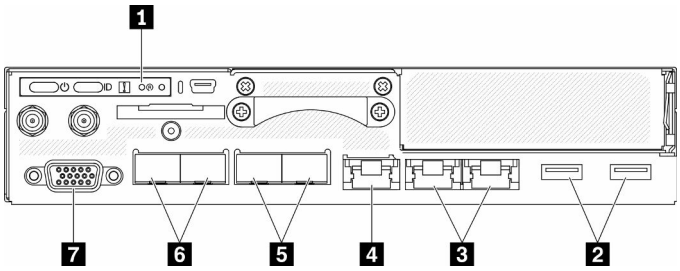


Figure 6. Wireless enabled LOM Package front view

Table 5. Components on the Wireless enabled LOM Package front view

1 Front operator panel	5 1Gb SFP connectors
2 USB 3.1 Gen 1 connectors	6 10Gb SFP+ Ethernet connectors
3 1Gb Ethernet connectors	7 VGA connector
4 XClarity Controller (XCC) network connector The wrench icon on the connector indicates that this connector can be set to connect to Lenovo XClarity Controller.	

Front I/O fillers

Install the I/O fillers when the connectors are not used. The connectors could be damaged without proper protection of the fillers.

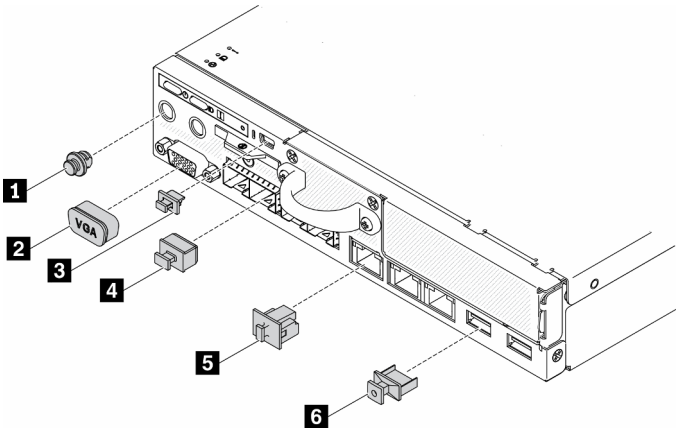


Figure 7. Fillers

Table 6. Fillers

1 Antenna port filler (x2 or not available, depending on the model)	4 SFP filler (x2 or x4, depending on the model)
2 VGA cover	5 RJ-45 filler (x3 or x4, depending on the model)
3 Mini USB filler	6 USB filler x2

Front operator panel

The front operation information panel of the server provides controls, connectors, and LEDs. The front operator panel varies by model.

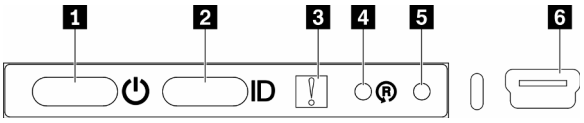


Figure 8. Front operator panel

Table 7. Front operator panel controls and indicators

1 Power button/LED (green)	4 Wireless enabled LOM package reset button
2 Identification button/LED (blue)	5 NMI button
3 System-error LED (yellow)	6 XClarity Controller mini USB connector

1 Power button/LED (green): Press this button to turn the server on and off manually. The states of the power LED are as follows:

Off: Power is not present or the power adapter, or the LED itself has failed.

Flashing rapidly (4 times per second): The server is turned off and is not ready to be turned on. The power button is disabled. This will last approximately 5 to 10 seconds.

Flashing slowly (once per second): The server is turned off and is ready to be turned on. You can press the power button to turn on the server.

On: The server is turned on.

2 Identification button/LED (blue): Use this blue LED to visually locate the server among other servers. This LED is also used as a presence detection button. You can use Lenovo XClarity Administrator to light this LED remotely. The states of the identification LED are as follows:

Off: Presence detection off.

Flashing rapidly (4 times per second): (on XCC firmware version 3.10 or later) The server is not activated yet and has no power permission. See *Activation guide* to activate the system.

Flashing slowly (once per second): Presence detection on.

On: Presence detection on.

3 System-error LED (yellow): When this yellow LED is lit, it indicates that a system error has occurred.

4 Wireless enabled LOM module reset button: The reset pin for the wireless enabled LOM module.

5 NMI button: Press this button to force a nonmaskable interrupt (NMI) to the processor. By this way, you can blue screen the server and take a memory dump. You might have to use a pen or the end of a straightened paper clip to press the button.

6 XClarity Controller mini USB connector: Used to attach a mini USB to manage the system using XClarity Controller.

Rear view

The rear of the server provides access to several components, including the power supplies, PCIe adapters, serial port, and Ethernet port.

Rear view of the server

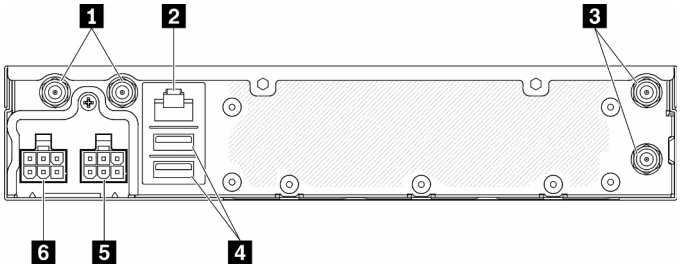


Figure 9. Rear view - 12V power distribution module (PDM)

Table 8. Rear view - 12V power adapter model

1 WLAN Antenna connectors (available only when M.2 WLAN module is installed)	4 USB 2.0 connectors
2 RS-232 port (RJ-45)	5 Power connector 1
3 LTE Antenna connectors (available only when M.2 LTE module is installed)	6 Power connector 2

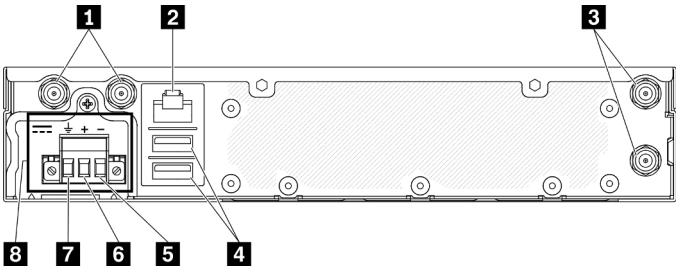


Figure 10. Rear view - -48V power distribution module (PDM)

Table 9. Rear view - -48V power adapter model

1 WLAN Antenna connectors (available only when M.2 WLAN module is installed)	5 Vin- terminal
2 RS-232 port (RJ-45)	6 Vin+ terminal
3 LTE Antenna connectors (available only when M.2 LTE module is installed)	7 GND terminal
4 USB 2.0 connectors	8 Power connector

Rear I/O fillers

Install the I/O fillers when the connectors are not used. The connectors could be damaged without proper protection of the fillers.

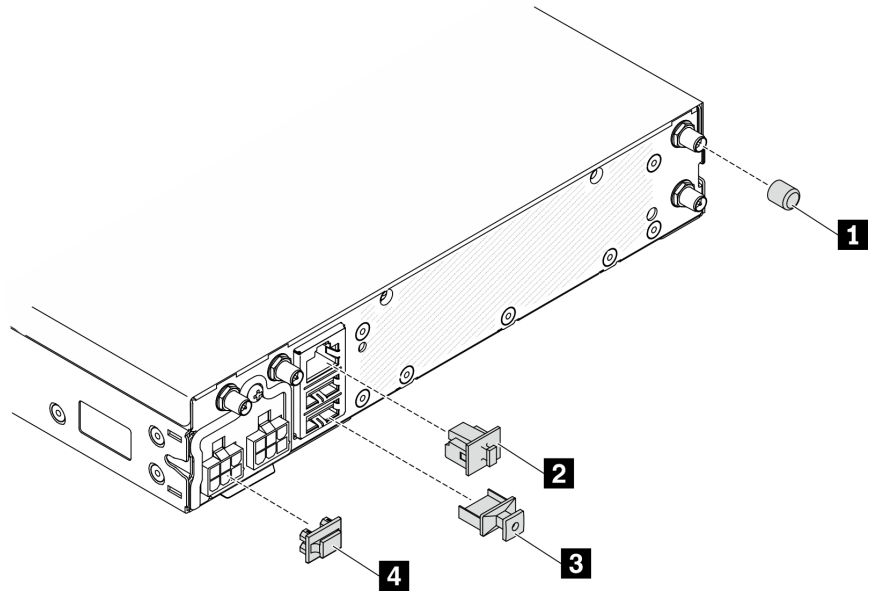


Figure 11. Fillers

Table 10. Fillers

1 Antenna cover x4 (If no antennas are installed, use antenna port fillers. See “Front view” on page 18.)	3 USB filler x2
2 RJ-45 filler	4 Power connector filler

System-board connectors

The following illustrations show the connectors on the system board.

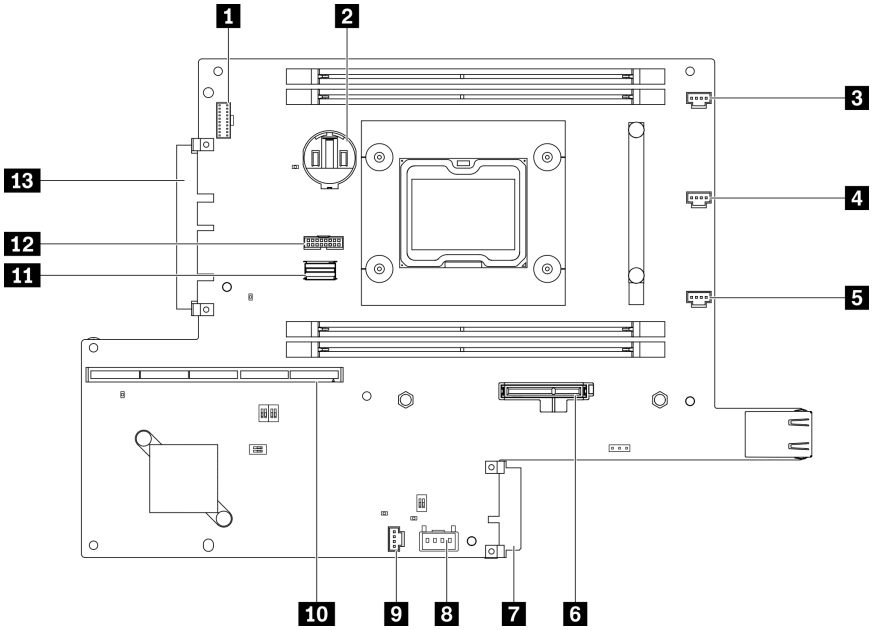


Figure 12. System-board connectors

Table 11. System-board connectors

1 Front operator panel connector	8 Lock switch connector
2 3V Battery (CR2032)	9 Intrusion switch connector
3 Fan 1 connector	10 Riser connector
4 Fan 2 connector	11 SATA Cable connector
5 Fan 3 connector	12 TPM connector
6 M.2 boot adapter connector	13 LOM module connector
7 Power distribution module connector	

LOM packages

The following illustrations show the wireless enabled LOM package, 10G SFP+ LOM package, and 10G BASE-T LOM Package.

Depending on the server configuration, connect one of the LOM packages to the LOM module connector on the system board (see “System-board connectors” on page 23).

Wireless enabled LOM package

Wireless enabled LOM package enables the wireless function of the server. The connector on the package is designed for M.2 WLAN/LTE wireless adapter. There are two types of the wireless adapter, both are installed in the same method. For more information, see “Install the M.2 WLAN/LTE wireless adapter” on page 56.

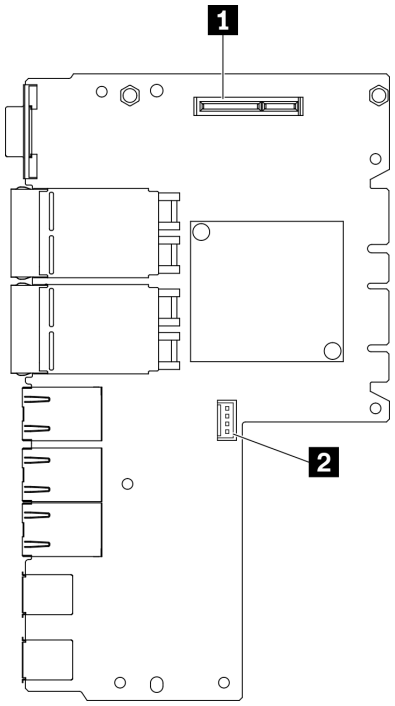


Figure 13. Wireless enabled LOM package

Table 12. Wireless enabled LOM package

1 M.2 WLAN/LTE wireless connector	2 Service-only connector

Note: The service-only connector is available on some models and reserved for service only.

10G SFP+ LOM package

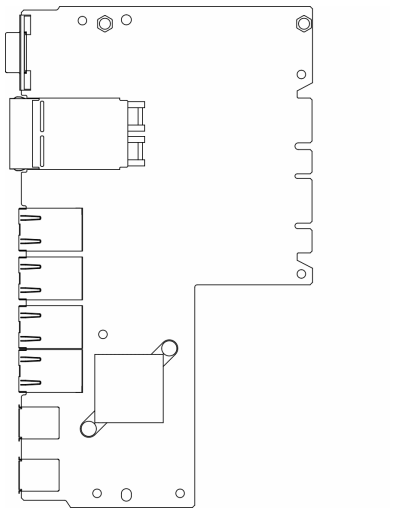


Figure 14. 10G SFP+ LOM package

10G BASE-T LOM Package

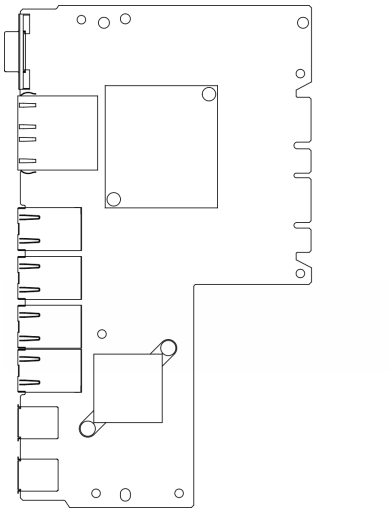


Figure 15. 10G BASE-T LOM Package

PCIe riser assembly

Use this information to locate the connectors on the PCIe riser assembly.

PCIe and M.2 riser assembly

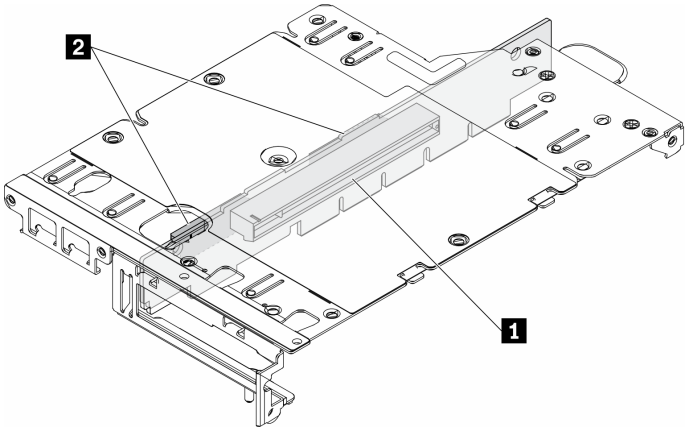


Figure 16. PCIe and M.2 riser assembly

Table 13. PCIe and M.2 riser assembly

1 Slot 6: PCIe 3.0 x16, (supports <75W, low profile, half-height, half-length PCIe adapter)	2 Drives (Slot) 2-5, M.2 data adapters

M.2 riser assembly

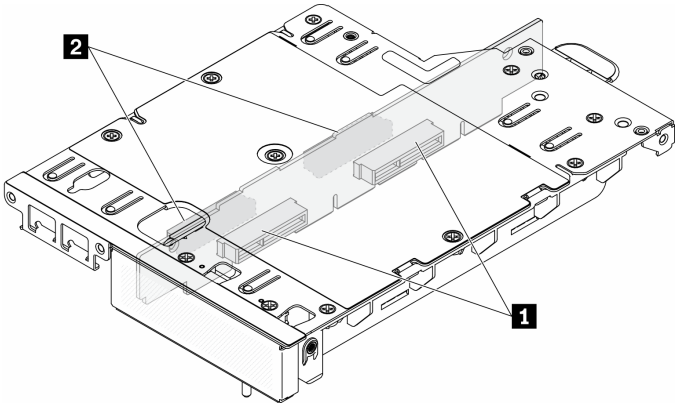


Figure 17. M.2 riser assembly

Table 14. M.2 riser assembly

1 Drives (Slot) 6-9, M.2 data adapters	2 Drives (Slot) 2-5, M.2 data adapters

M.2 drive and slot numbering

Use this information to locate the M.2 drive and slot numbering

M.2 boot adapter

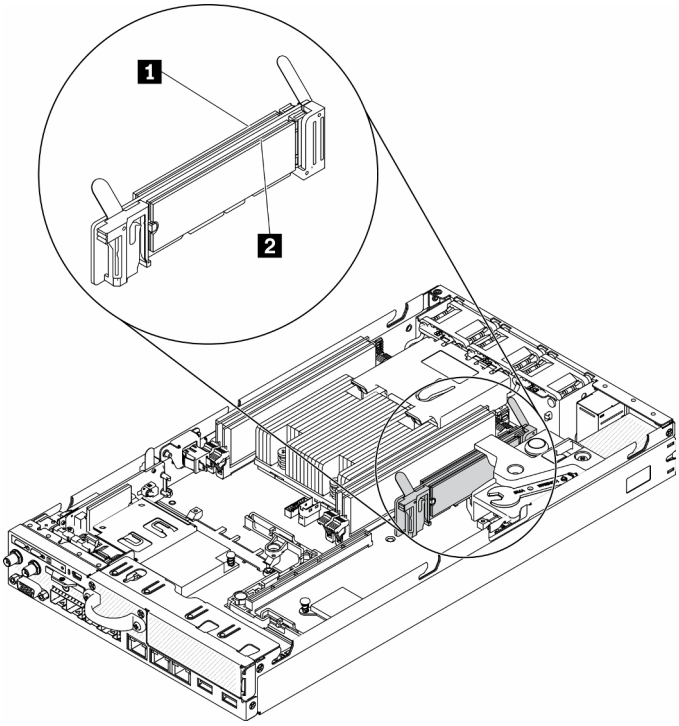


Figure 18. M.2 boot adapter

Important: The M.2 drives on opposite sides of the adapter must be of the same form factor (that is, the same physical length) because they share the same mounting clip.

Table 15. M.2 boot adapter slot numbering

1 Drive 0	2 Drive 1

M.2 data adapter

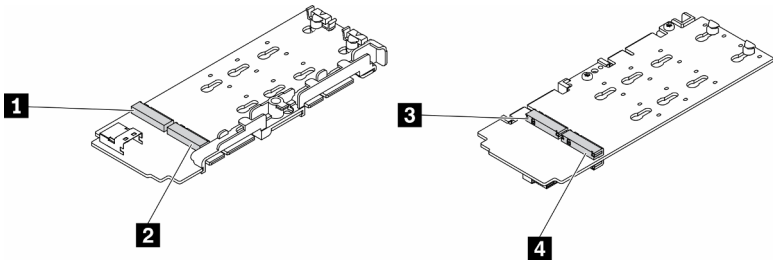


Figure 19. M.2 data adapter

Important: For the data drive adapter and the boot drive adapter, the pairs of M.2 drives on opposite sides of the adapter must be of the same form factor (that is, the same physical length) because they share the same mounting clip.

In this illustration of M.2 data adapter,

- Drive positions 1 and 4 must be of the same form factor (that is, the same physical length)
- Drive positions 2 and 3 must be of the same form factor (that is, the same physical length)

Table 16. M.2 data adapter

1 Drive 2 or 9	3 Drive 5 or 6
2 Drive 4 or 7	4 Drive 3 or 8

The following tables demonstrate the M.2 drive and slot numbering.

- PCIe and M.2 riser assembly

Left-wing (M.2 data adapter)		Right-wing (PCIe adapter)	
The drive numbering on the adapter	**The slot numbering in the UEFI Setup Menu**	**The drive numbering on the adapter**	**The slot numbering in the UEFI Setup Menu**
Drive 2	Slot 2	PCIe adapter	Slot 6
Drive 3	Slot 3		
Drive 4	Slot 4		
Drive 5	Slot 5		

Left-wing (M.2 data adapter with hardware RAID)		Right-wing (PCIe adapter)	
The drive numbering on the adapter	**The slot numbering in the UEFI Setup Menu**	**The drive numbering on the adapter**	**The slot numbering in the UEFI Setup Menu**
Drive 2	Slot 2/3	PCIe adapter	Slot 6
Drive 3			
Drive 4	Slot 4/5		
Drive 5			

- M.2 riser assembly with two M.2 data adapters

Left-wing (M.2 data adapter)		Right-wing (M.2 data adapter)	
The drive numbering on the adapter	**The slot numbering in the UEFI Setup Menu**	**The drive numbering on the adapter**	**The slot numbering in the UEFI Setup Menu**
Drive 2	Slot 2	Drive 9	Slot 9
Drive 3	Slot 3	Drive 8	Slot 8
Drive 4	Slot 4	Drive 7	Slot 7
Drive 5	Slot 5	Drive 6	Slot 6

Left-wing (M.2 data adapter with hardware RAID)		Right-wing (M.2 data adapter with hardware RAID)	
The drive numbering on the adapter	**The slot numbering in the UEFI Setup Menu**	**The drive numbering on the adapter**	**The slot numbering in the UEFI Setup Menu**
Drive 2	Slot 2/3	Drive 9	Slot 8/9
Drive 3		Drive 8	
Drive 4	Slot 4/5	Drive 7	Slot 6/7
Drive 5		Drive 6	

Parts list

Use the parts list to identify each of the components that are available for your server.

For more information about ordering the parts shown in the Figure 20 “Server components ” on page 29:

https://datacentersupport.lenovo.com/products/servers/thinksystem/se350/parts

Note: Depending on the model, your server might look slightly different from the illustration.

The parts listed in the following table are identified as one of the following:

- **Tier 1 customer replaceable unit (CRU):** Replacement of Tier 1 CRUs is your responsibility. If Lenovo installs a Tier 1 CRU at your request with no service agreement, you will be charged for the installation.
- **Tier 2 customer replaceable unit (CRU):** 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.
- **Field replaceable unit (FRU):** FRUs must be installed only by trained service technicians.
- **Consumable and Structural parts:** Purchase and replacement of consumable and structural parts (components, such as a cover or bezel) is your responsibility. If Lenovo acquires or installs a structural component at your request, you will be charged for the service.

Server components

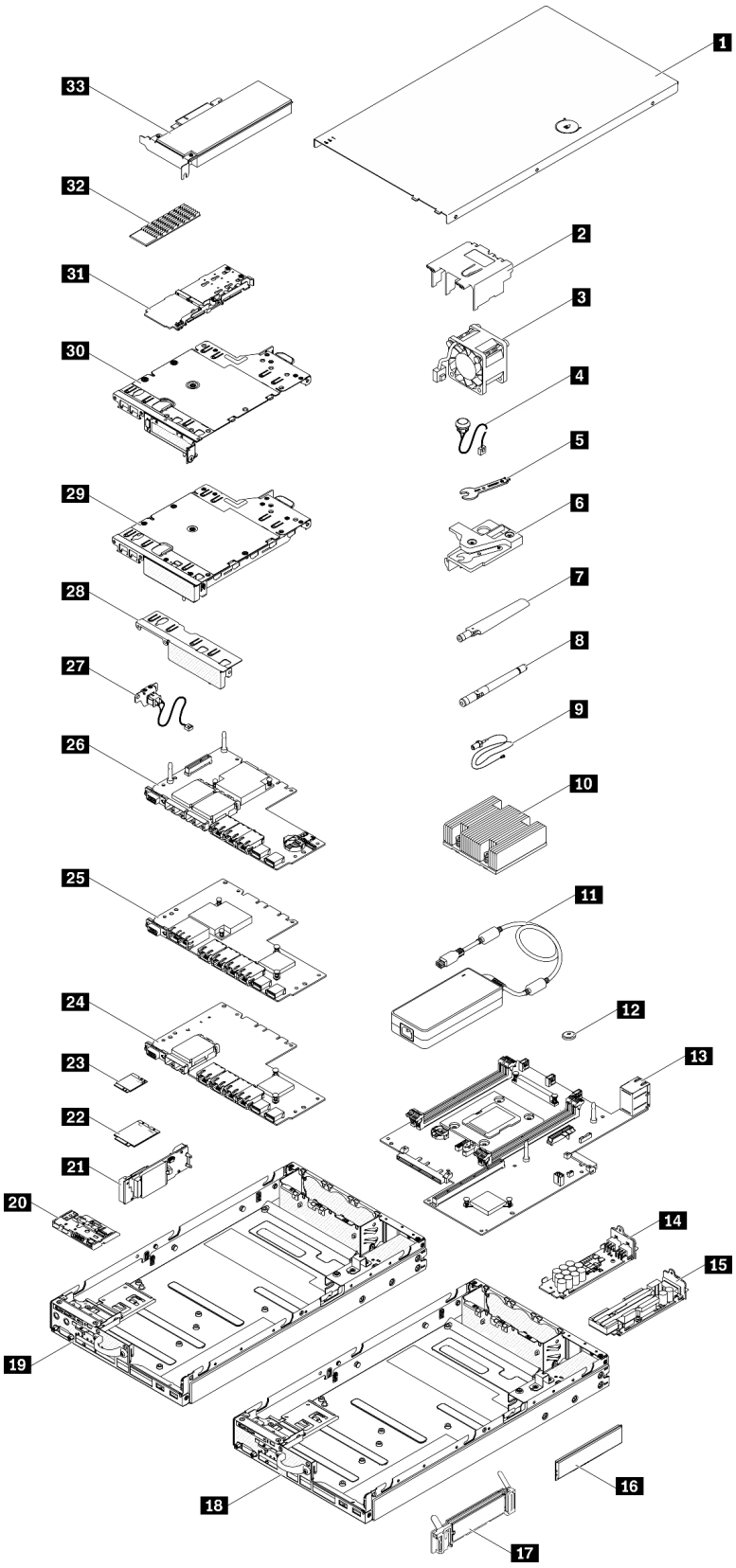


Figure 20. Server components

Table 17. Parts listing

Index	Description	Tier 1 CRU	Tier 2 CRU	FRU	Consumable and Structural part
For more information about ordering the parts shown in Figure 20 “Server components ” on page 29: https://datacentersupport.lenovo.com/products/servers/thinksystem/se350/parts					
1	Top cover				√
2	Air baffle				√
3	Fan	√			
4	Intrusion switch cable	√			
5	Screwdriver in Misc kit				√
6	Intrusion switch	√			
7	LTE Antenna	√			
8	WLAN Antenna	√			
9	M.2 WLAN/LTE module cable			√	
10	Processor heat sink			√	
11	Power adapter	√			
12	CMOS battery (CR2032)				√
13	System board			√	
14	12 V power distribution module		√		
15	-48 V power distribution module		√		
16	DIMM	√			
17	M.2 boot adapter		√		
18	10G SFP+ LOM package chassis				√
19	Wireless enabled LOM package chassis				√
20	Front operator panel				√
21	M.2 WLAN/LTE wireless adapter			√	
22	M.2 LTE module			√	
23	M.2 WLAN module			√	
24	10G SFP+ LOM package				√
25	10G BASE-T LOM Package				√
26	Wireless enabled LOM package				√
27	Locking cable	√			
28	Front filler				√
29	M.2 riser assembly		√		

Table 17. Parts listing (continued)

Index	Description	Tier 1 CRU	Tier 2 CRU	FRU	Consumable and Structural part
30	PCIe and M.2 riser assembly		√		
31	M.2 SATA/NVMe data adapter		√		
32	M.2 SATA/NVMe heat sink				√
33	PCIe adapter		√		

Power cords

Several power cords are available, depending on the country and region where the server is installed.

To view the power cords that are available for the server:

1. Go to:

   http://dcsc.lenovo.com/#/

2. Click **Preconfigured Model** or **Configure to order**.
3. Enter the machine type and model for your server to display the configurator page.
4. Click **Power → Power Cables** to see all line cords.

Notes:

- For your safety, a power cord with a grounded attachment plug is provided to use with this product. To avoid electrical shock, always use the power cord and plug with a properly grounded outlet.
- Power cords for this product that are used in the United States and Canada are listed by Underwriter's Laboratories (UL) and certified by the Canadian Standards Association (CSA).
- For units intended to be operated at 115 volts: Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a parallel blade, grounding-type attachment plug rated 15 amperes, 125 volts.
- For units intended to be operated at 230 volts (U.S. use): Use a UL-listed and CSA-certified cord set consisting of a minimum 18 AWG, Type SVT or SJT, three-conductor cord, a maximum of 15 feet in length and a tandem blade, grounding-type attachment plug rated 15 amperes, 250 volts.
- For units intended to be operated at 230 volts (outside the U.S.): Use a cord set with a grounding-type attachment plug. The cord set should have the appropriate safety approvals for the country in which the equipment will be installed.
- Power cords for a specific country or region are usually available only in that country or region.

Chapter 3. Server hardware setup

To set up the server, install any options that have been purchased, cable the server, configure and update the firmware, and install the operating system.

Server setup checklist

Use the server setup checklist to ensure that you have performed all tasks that are required to set up your server.

The server setup procedure varies depending on the configuration of the server when it was delivered. In some cases, the server is fully configured and you just need to connect the server to the network and an ac power source, and then you can power on the server. In other cases, the server needs to have hardware options installed, requires hardware and firmware configuration, and requires an operating system to be installed.

The following steps describe the general procedure for setting up a server:

1. Unpack the server package. See “Server package contents” on page 2.
2. Set up the server hardware.
   a. Install any required hardware or server options. See the related topics in “Install server hardware options” on page 37.
   b. If necessary, install the server into a standard rack cabinet by using the rail kit shipped with the server. See the *Rack Installation Instructions* that comes with optional rail kit.
   c. Connect the Ethernet cables and power cords to the server. See “Rear view” on page 21 to locate the connectors. See “Cable the server” on page 75 for cabling best practices.
   d. Power on the server. See “Power on the server” on page 75.

      Note: You can access the management processor interface to configure the system without powering on the server. Whenever the server is connected to power, the management processor interface is available. For details about accessing the management server processor, see:

      “Opening and Using the XClarity Controller Web Interface” section in the XCC documentation version compatible with your server at https://pubs.lenovo.com/lxcc-overview/.
   e. Validate that the server hardware was set up successfully. See Validate server setup.
3. Configure the system.
   a. Follow the steps in “Activate the system” on page 77 to activate the system.
   b. Connect the Lenovo XClarity Controller to the management network. See Set the network connection for the Lenovo XClarity Controller.
   c. Update the firmware for the server, if necessary. See “Update the firmware” on page 80.
   d. Configure the firmware for the server. See “Configure the firmware” on page 84.

      The following information is available for RAID configuration:

      - https://lenovopress.com/lp0578-lenovo-raid-introduction
      - https://lenovopress.com/lp0579-lenovo-raid-management-tools-and-resources
   e. Install the operating system. See “Deploy the operating system” on page 122.
   f. Back up the server configuration. See “Back up the server configuration” on page 123.
   g. Install the applications and programs for which the server is intended to be used.

Installation Guidelines

Use the installation guidelines to install components in your server.

Before installing optional devices, read the following notices carefully:

Attention: Prevent exposure to static electricity, which might lead to system halt and loss of data, by keeping static-sensitive components in their static-protective packages until installation, and handling these devices with an electrostatic-discharge wrist strap or other grounding system.

- Read the safety information and guidelines to ensure that you work safely.
  - A complete list of safety information for all products is available at:

    https://pubs.lenovo.com/safety_documentation/
  - The following guidelines are available as well: "Handling static-sensitive devices" on page 36 and "Working inside the server with the power on" on page 35.
- Make sure the components you are installing are supported by the server. For a list of supported optional components for the server, see https://serverproven.lenovo.com/server/se350.
- When you install a new server, download and apply the latest firmware. This will help ensure that any known issues are addressed, and that your server is ready to work with optimal performance. Go to ThinkSystem SE350 Drivers and Software to download firmware updates for your server.

  Important: Some cluster solutions require specific code levels or coordinated code updates. If the component is part of a cluster solution, verify the latest Best Recipe code level menu for cluster supported firmware and driver before you update the code.
- It is good practice to make sure that the server is working correctly before you install an optional component.
- Keep the working area clean, and place removed components on a flat and smooth surface that does not shake or tilt.
- Do not attempt to lift an object that might be too heavy for you. If you have to lift a heavy object, read the following precautions carefully:
  - Make sure that you can stand steadily without slipping.
  - Distribute the weight of the object equally between your feet.
  - Use a slow lifting force. Never move suddenly or twist when you lift a heavy object.
  - To avoid straining the muscles in your back, lift by standing or by pushing up with your leg muscles.
- Make sure that you have an adequate number of properly grounded electrical outlets for the server, monitor, and other devices.
- Back up all important data before you make changes related to the disk drives.
- Have a small flat-blade screwdriver, a small Phillips screwdriver, and a T8 torx screwdriver available.
- To view the error LEDs on the system board and internal components, leave the power on.
- You do not have to turn off the server to remove or install hot-swap power supplies, hot-swap fans, or hot-plug USB devices. However, you must turn off the server before you perform any steps that involve removing or installing adapter cables, and you must disconnect the power source from the server before you perform any steps that involve removing or installing a riser card.
- Blue on a component indicates touch points, where you can grip to remove a component from or install it in the server, open or close a latch, and so on.
- Terra-cotta on a component or an terra-cotta label on or near a component indicates that the component can be hot-swapped if the server and operating system support hot-swap capability, which means that you can remove or install the component while the server is still running. (Terra-cotta can also indicate

touch points on hot-swap components.) See the instructions for removing or installing a specific hot-swap component for any additional procedures that you might have to perform before you remove or install the component.

- The Red strip on the drives, adjacent to the release latch, indicates that the drive can be hot-swapped if the server and operating system support hot-swap capability. This means that you can remove or install the drive while the server is still running.

  Note: See the system specific instructions for removing or installing a hot-swap drive for any additional procedures that you might need to perform before you remove or install the drive.
- After finishing working on the server, make sure you reinstall all safety shields, guards, labels, and ground wires.

System reliability guidelines

Review the system reliability guidelines to ensure proper system cooling and reliability.

Make sure the following requirements are met:

- When the server comes with redundant power, a power adapter must be installed in each power-adapter bay.
- Adequate space around the server must be spared to allow server cooling system to work properly. Leave approximately 50 mm (2.0 in.) of open space around the front and rear of the server. Do not place any object in front of the fans.
- For proper cooling and airflow, refit the server cover before you turn the power on. Do not operate the server for more than 30 minutes with the server cover removed, for it might damage server components.
- Cabling instructions that come with optional components must be followed.
- A failed fan must be replaced within 48 hours since malfunction.
- A removed hot-swap fan must be replaced within 30 seconds after removal.
- A removed hot-swap drive must be replaced within two minutes after removal.
- A removed hot-swap power adapter must be replaced within two minutes after removal.
- Every air baffle that comes with the server must be installed when the server starts (some servers might come with more than one air baffle). Operating the server with a missing air baffle might damage the processor.
- All processor sockets must contain either a socket cover or a processor with heat sink.
- When more than one processor is installed, fan population rules for each server must be strictly followed.

Working inside the server with the power on

Guidelines to work inside the server with the power on.

Attention: The server might stop and loss of data might occur when internal server components are exposed to static electricity. To avoid this potential problem, always use an electrostatic-discharge wrist strap or other grounding systems when working inside the server with the power on.

- Avoid loose-fitting clothing, particularly around your forearms. Button or roll up long sleeves before working inside the server.
- Prevent your necktie, scarf, badge rope, or long hair from dangling into the server.
- Remove jewelry, such as bracelets, necklaces, rings, cuff links, and wrist watches.
- Remove items from your shirt pocket, such as pens and pencils, in case they fall into the server as you lean over it.
- Avoid dropping any metallic objects, such as paper clips, hairpins, and screws, into the server.

Handling static-sensitive devices

Use this information to handle static-sensitive devices.

Attention: Prevent exposure to static electricity, which might lead to system halt and loss of data, by keeping static-sensitive components in their static-protective packages until installation, and handling these devices with an electrostatic-discharge wrist strap or other grounding system.

- Limit your movement to prevent building up static electricity around you.
- Take additional care when handling devices during cold weather, for heating would reduce indoor humidity and increase static electricity.
- Always use an electrostatic-discharge wrist strap or other grounding system, particularly when working inside the server with the power on.
- While the device is still in its static-protective package, touch it to an unpainted metal surface on the outside of the server for at least two seconds. This drains static electricity from the package and from your body.
- Remove the device from the package and install it directly into the server without putting it down. If it is necessary to put the device down, put it back into the static-protective package. Never place the device on the server or on any metal surface.
- When handling a device, carefully hold it by the edges or the frame.
- Do not touch solder joints, pins, or exposed circuitry.
- Keep the device from others' reach to prevent possible damages.

Memory module installation rules and order

Memory modules must be installed in a specific order based on the memory configuration that you implement on your server.

The following illustration shows the system-board components, including DIMM connectors.

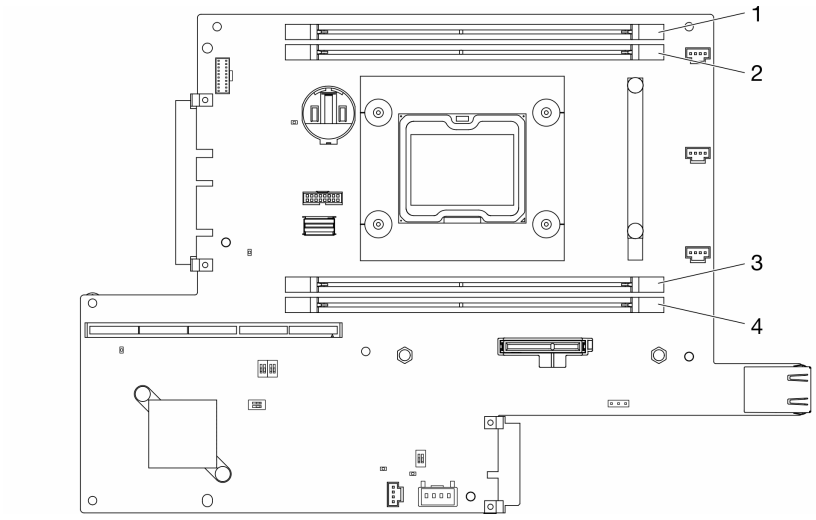


Figure 21. DIMM connectors

The following table show the sequence of DIMM installation

Total DIMM installed	DIMM 1	DIMM 2	DIMM 3	DIMM 4
1	√			
2	√			√
3	√	√		√
4	√	√	√	√

Install server hardware options

This section includes instructions for performing initial installation of optional hardware. Each component installation procedure references any tasks that need to be performed to gain access to the component being replaced.

Installation procedures are presented in the optimum sequence to minimize work.

Attention: To ensure the components you install work correctly without problems, read the following precautions carefully.

- Make sure the components you are installing are supported by the server. For a list of supported optional components for the server, see https://serverproven.lenovo.com/server/se350.
- Always download and apply the latest firmware. This will help ensure that any known issues are addressed, and that your server is ready to work with optimal performance. Go to ThinkSystem SE350 Drivers and Software to download firmware updates for your server.
- It is good practice to make sure that the server is working correctly before you install an optional component.
- Follow the installation procedures in this section and use appropriate tools. Incorrectly installed components can cause system failure from damaged pins, damaged connectors, loose cabling, or loose components.

Remove a node

Use this information to remove a node.

Before you remove a node, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Procedure

Step 1. To remove the node from the enclosure, complete the following steps.

a. Remove the five screws, and loosen the two thumb screws of the shipping bracket.

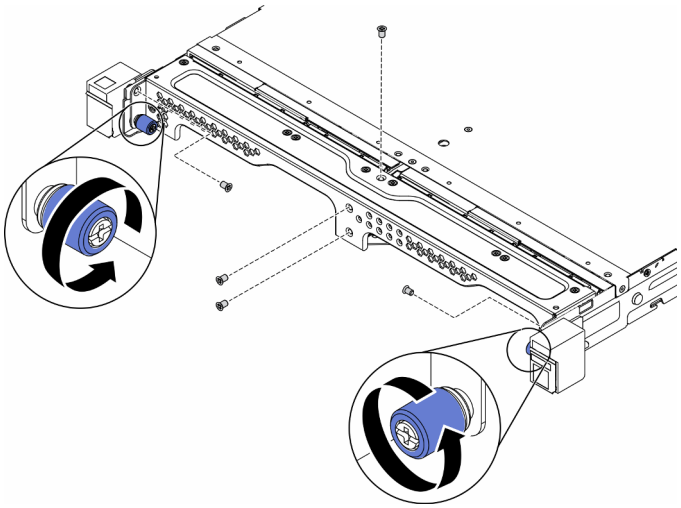


Figure 22. Node removal

b. Remove the shipping bracket from the enclosure.

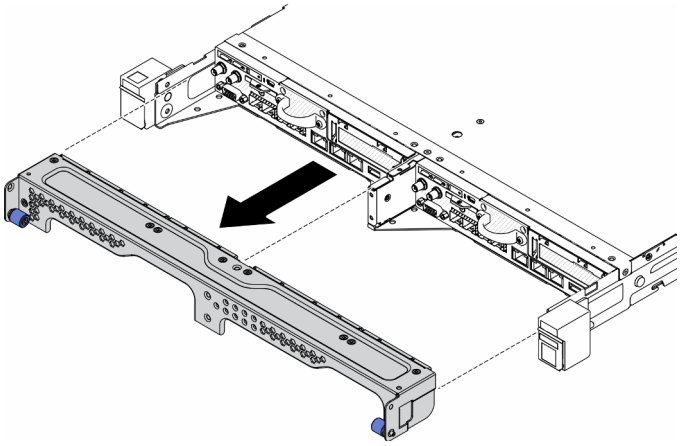


Figure 23. Node removal

c. Press on the release button and slide the node out of the enclosure.
   - E1 Enclosure (1U 2-node)

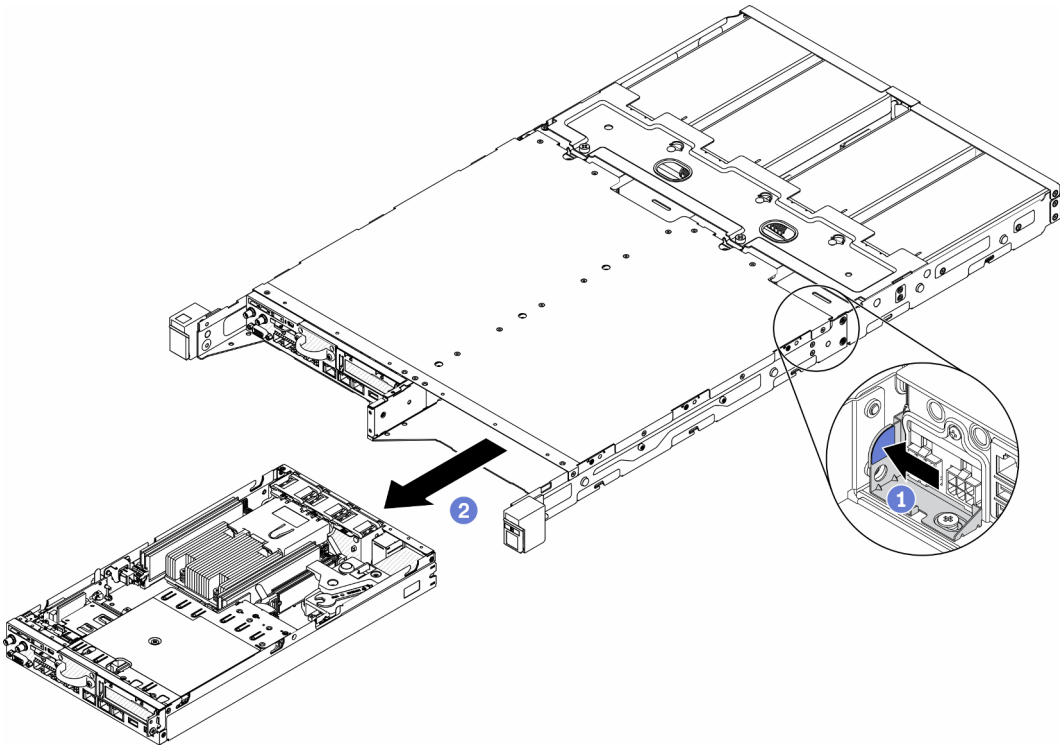


Figure 24. Node removal

- E2 Enclosure (2U 2-node)

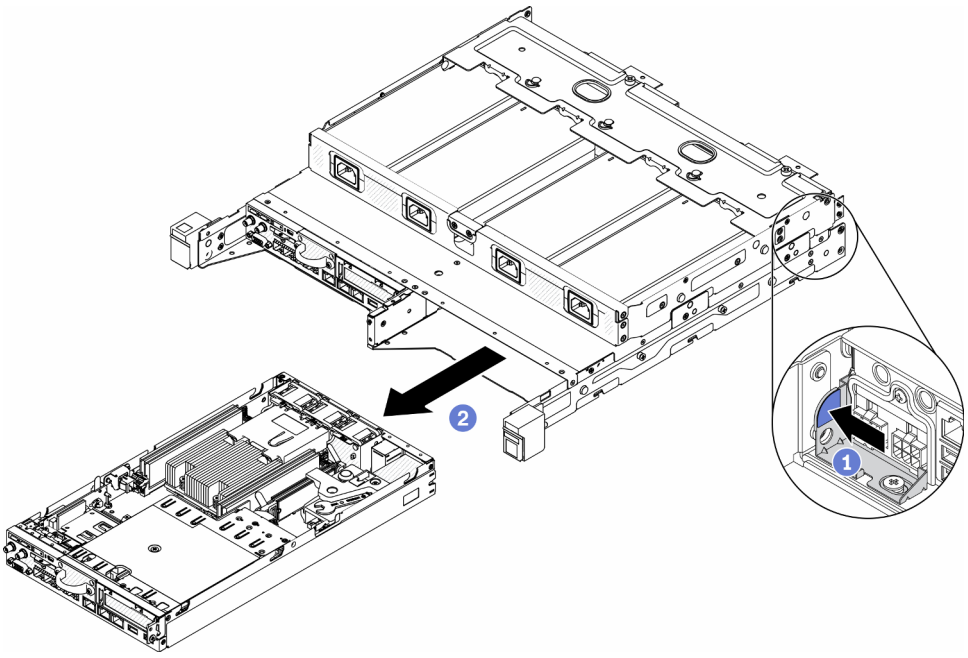


Figure 25. Node removal

Notes:

- The node removed from the enclosure is without top cover. If the node is not to be reinstalled to an enclosure, make sure to install the top cover. See “Install the top cover” on page 69.

- If the node is removed from an E1 Enclosure (1U 2-node) and is not to be reinstalled to the E1 Enclosure, change the vital product data (VPD) to the default mode for proper operation.See *Change the VPD for E1 Enclosure configuration (trained technician only)* in *Maintenance Manual*.

Step 2. To remove the node from the node sleeve, complete the following steps.

a. Loosen the two thumbscrews and slide the node of the node sleeve.

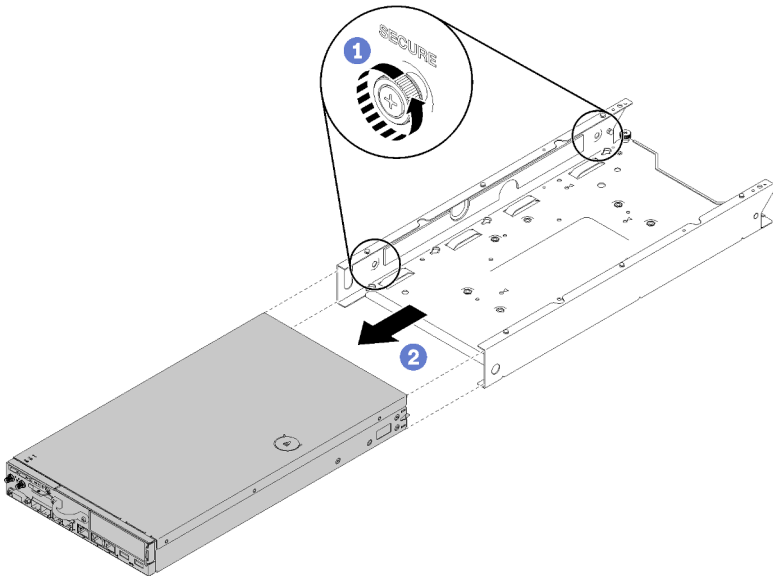


Figure 26. Node removal

Note: See *Configuration Installation Guide* for the bookshelf configuration, DIN rail configuration and wall-mounted configuration installation details if necessary.

If you are instructed to return the defective component, please package the part to prevent any shipping damage. Reuse the packaging the new part arrived in and follow all packaging instructions.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=N_3TsrEYPP0

Remove the top cover

Use this information to remove the top cover.

To avoid possible danger, read and follow the following safety information.

S012

CAUTION:
Hot surface nearby.

S014

CAUTION:
Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the label is attached.

S033

CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

Before you remove the top cover, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - "Installation Guidelines" on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see "Power off the server" on page 75).

Procedure

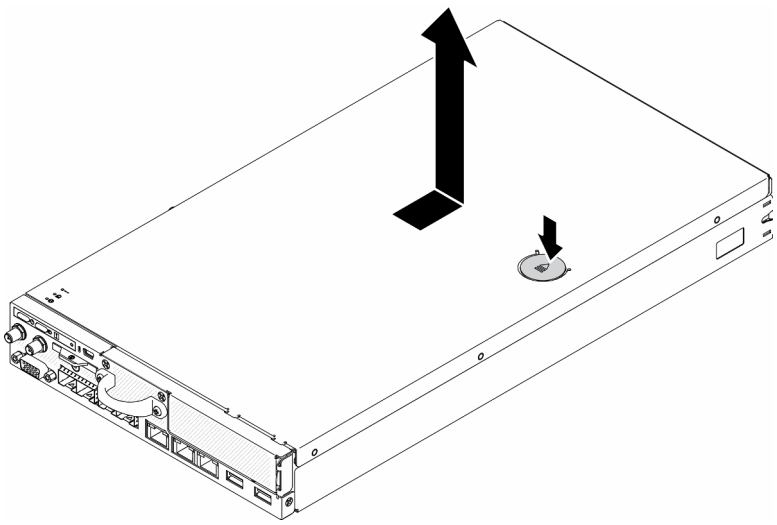


Figure 27. Top cover removal

Step 1. Press on the release button and the push point at the same time; then, slide the cover toward the rear of the server.

Step 2. Lift the top cover away from the server.

If you are instructed to return the defective component, please package the part to prevent any shipping damage. Reuse the packaging the new part arrived in and follow all packaging instructions.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=7pGlqu5xVNk

Remove the air baffle

Use this information to remove the air baffle.

To avoid possible danger, read and follow the following safety statement.

- **S012**

CAUTION:
Hot surface nearby.

Before you remove the air baffle, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Remove the node from the enclosure if needed (see “Remove a node” on page 37).

Procedure

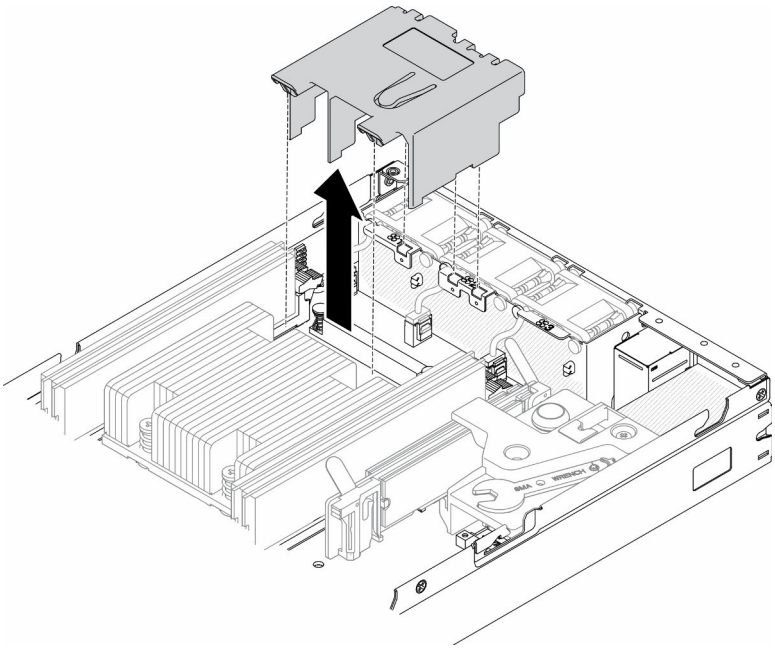


Figure 28. Air baffle removal

Step 1. Lift the air baffle up and set it aside.

Attention: For proper cooling and airflow, reinstall the air baffle before you turn on the server. Operating the server with the air baffle removed might damage server components.

If you are instructed to return the defective component, please package the part to prevent any shipping damage. Reuse the packaging the new part arrived in and follow all packaging instructions.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=Oiu0xpF9-XY

Remove the PCIe riser assembly

Use this information to remove the PCIe riser assembly .

To avoid possible danger, read and follow the following safety statement.

- **S012**

CAUTION:
Hot surface nearby.

Before you remove the PCIe riser assembly , complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Remove the node from the enclosure if needed (see “Remove a node” on page 37).

Procedure

Step 1. Remove the seven screws as shown.

Step 2. Grasp the PCIe riser assembly by its edge and the blue tab; then, carefully lift it out of the server.

Notes:

1. The following illustration might differ slightly from your hardware.
2. Carefully lift the PCIe riser assembly straight up. Avoid tilting the PCIe riser assembly at a large angle, tilting might cause damage to the connector.

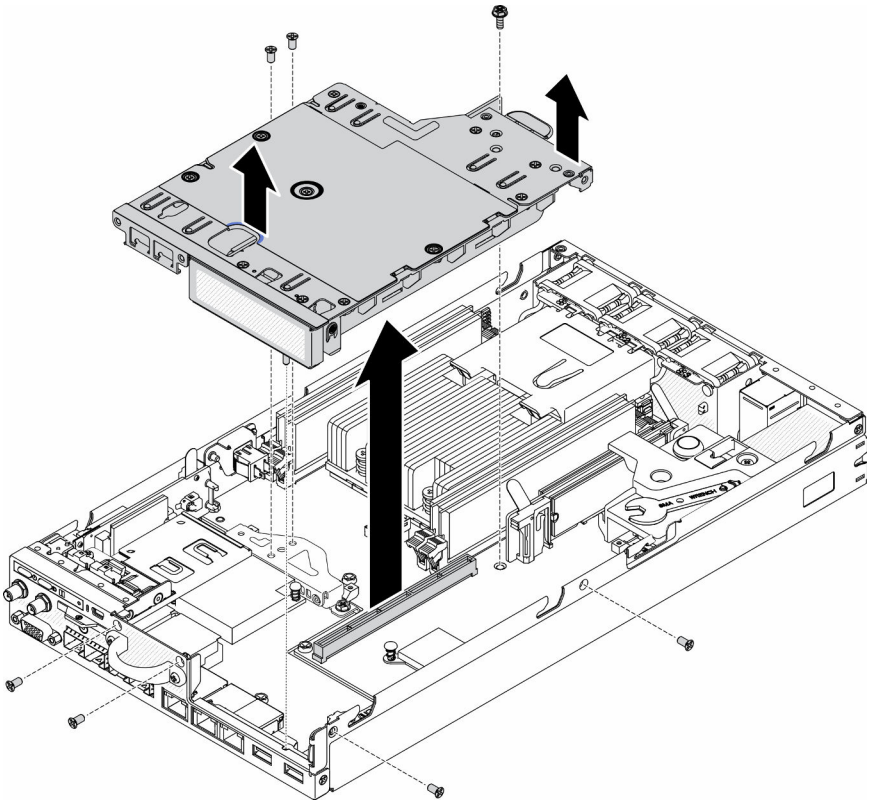


Figure 29. PCIe riser assembly removal

After you remove the PCIe riser assembly, complete the following steps:

1. Install the filler and fasten the three screws.

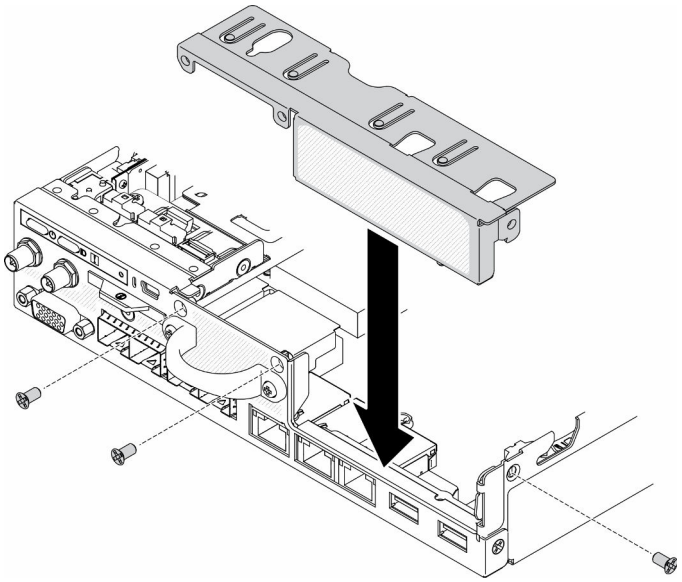


Figure 30. Filler installation

2. If you are instructed to return the defective component, please package the part to prevent any shipping damage. Reuse the packaging the new part arrived in and follow all packaging instructions.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=TPQz8cyiqGM

Remove the front operator panel

Use this information to remove the front operator panel .

Before you remove the front operator panel , complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Remove the node from the enclosure if needed (see “Remove a node” on page 37).
4. Remove the M.2 WLAN/LTE wireless adapter if needed.
5.
6. Remove the lock position switch if installed (see “Remove the lock position switch” on page 45).

Procedure

Step 1. Carefully remove the cable from the metal pull tab holder.

Step 2. Carefully press the cable latches and disconnect the two Y-cable connectors.

Step 3. Remove the screw.

Step 4. Pull the release tab.

Step 5. Slide the front operator panel out of the server.

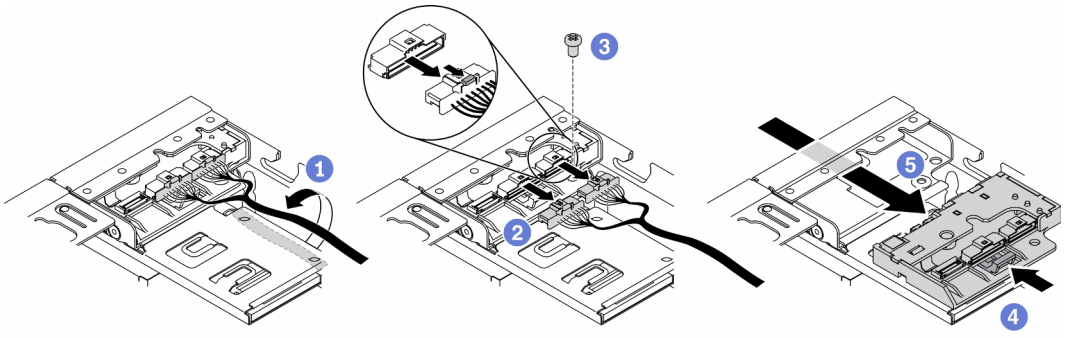


Figure 31. Front operator panel removal

If you are instructed to return the defective component, please package the part to prevent any shipping damage. Reuse the packaging the new part arrived in and follow all packaging instructions.

Demo video

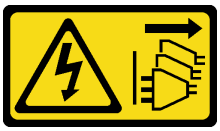
- Watch the procedure on YouTube: https://www.youtube.com/watch?v=qE1pfiR1T3M

Remove the lock position switch

Use this information to remove the lock position switch.

To avoid possible danger, read and follow the following safety information.

S002



CAUTION:
The power-control button on the device and the power switch on the power supply do not turn off the electrical current supplied to the device. The device also might have more than one power cord. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.

S009

CAUTION:
To avoid personal injury, disconnect the fan cables before removing the fan from the device.

Before you remove the lock position switch, complete the following steps:Before you install the lock position switch, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Remove the node from the enclosure if needed (see “Remove a node” on page 37).
4. Remove the PCIe riser cage (see “Remove the PCIe riser assembly” on page 43).

Procedure

Step 1. Disconnect the cable.

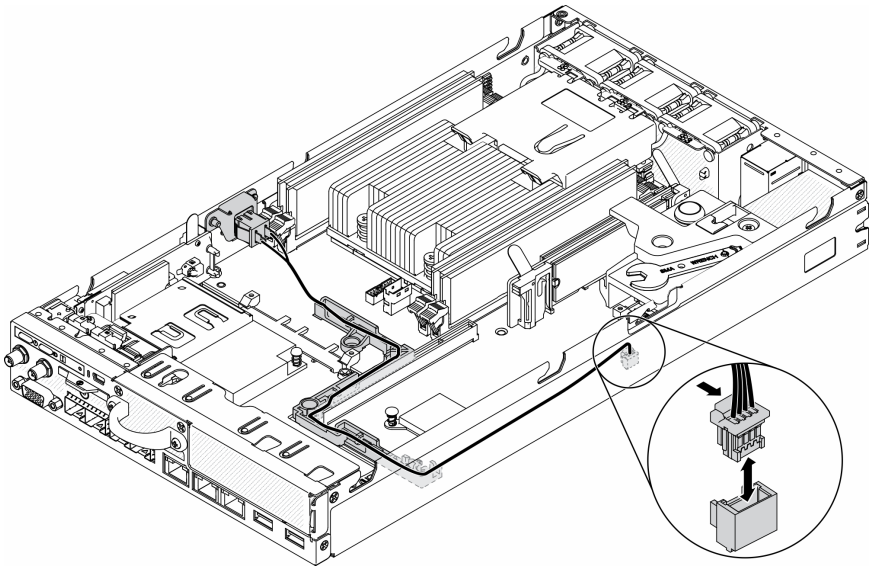


Figure 32. Lock position switch cable

Step 2. Remove the screw.

Step 3. Slightly push the lock position switch rightward and remove it from the server.

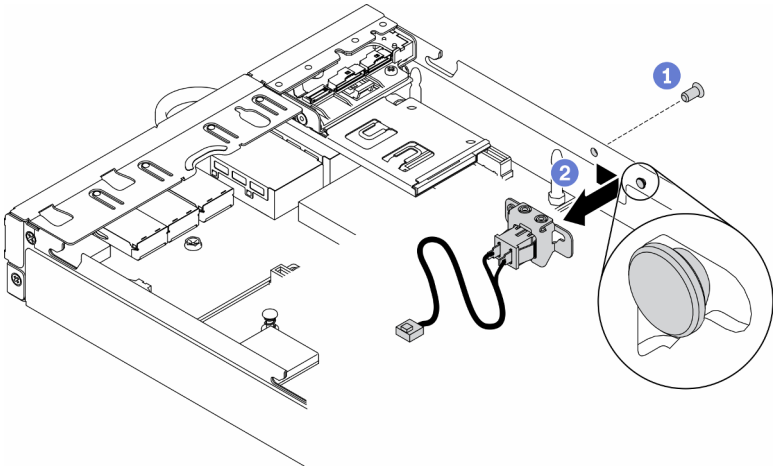


Figure 33. Lock position switch removal

If you are instructed to return the defective component, please package the part to prevent any shipping damage. Reuse the packaging the new part arrived in and follow all packaging instructions.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=z1Fh-VkIA0A

Remove the intrusion switch cable

Use this information to remove the intrusion switch cable.

Before you remove the intrusion switch cable, complete the following steps:

1. Read the following sections to ensure that you work safely.

- “Installation Guidelines” on page 34

2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Remove the node from the enclosure if needed (see “Remove a node” on page 37).

Procedure

Step 1. Loosen the two screws.
Step 2. Press and hold the cable latch.
Step 3. Disconnect the cable from the connector.
Step 4. Carefully lift the intrusion switch carrier out of the server.

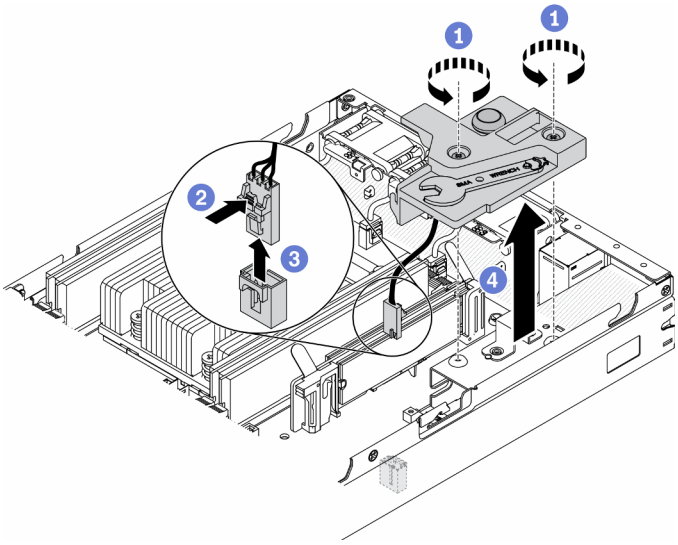


Figure 34. Intrusion switch cable removal

Step 5. Press and hold the latches on the both side of the cable.
Step 6. Remove the intrusion switch cable from the carrier.

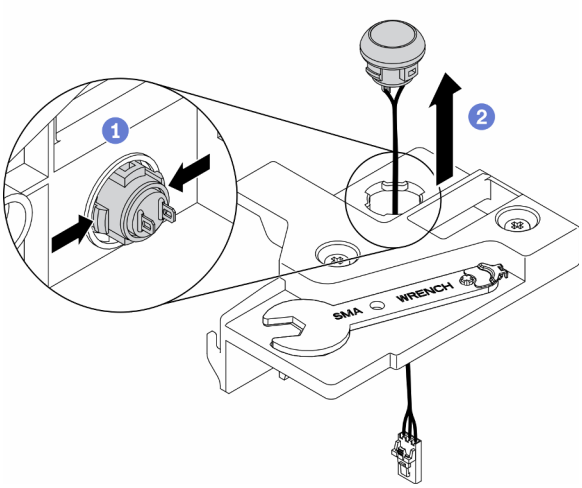


Figure 35. Intrusion switch cable removal

If you are instructed to return the defective component, please package the part to prevent any shipping damage. Reuse the packaging the new part arrived in and follow all packaging instructions.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=MPb1b7dJCjY

Install a power adapter

Use this information to install a power adapter.

As required by COMMISSION REGULATION (EU) 2019/1782 of 1 October 2019 laying down ecodesign requirements for external power supplies pursuant to Directive 2009/125/EC of the European Parliament and of the Council and repealing Commission Regulation (EC) No 278/2009 (ErP Lot7) for the external power supply of the product.

Table 18. ThinkEdge 240W 230V/115V External Power Supply

Information published	Value and precision	Unit
Manufacturer's name	Lenovo	-
Model identifier	FSP240-A12C14	-
Input voltage	100-240	V
Input AC frequency	50-60	Hz
Output voltage	12.2	V
Output current	20.0	A
Output power	240.0	W
Average active efficiency	92.73	%
Efficiency at low load (10 %)	87.35	%
No-load power consumption	0.13	W

Table 19. ThinkEdge 240W 230V/115V External Power Supply v2

Information published	Value and precision	Unit
Manufacturer's name	Lenovo	-
Model identifier	GA240SD1-12020000	-
Input voltage	100-240	V
Input AC frequency	50-60	Hz
Output voltage	12.2	V
Output current	20.0	A
Output power	240.0	W
Average active efficiency	93.21	%
Efficiency at low load (10 %)	79.0	%
No-load power consumption	0.097	W

Before you install a power adapter, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Remove the node from the enclosure if needed (see “Remove a node” on page 37).

CAUTION:

- **Power adapters to the node must be with the same brand, power rating, wattage or efficiency level.**
- **To distinguish the power adapters, check the size, the position of connector, and the label of the power adapters.**

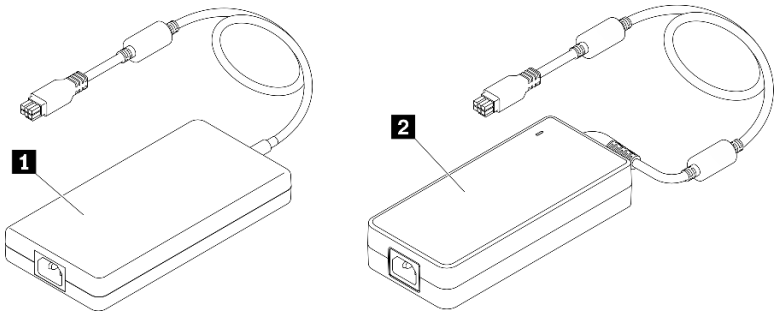


Table 20. Power adapters

1 ThinkEdge 240W 230V/115V External Power Supply	2 ThinkEdge 240W 230V/115V External Power Supply v2

Note: To tell the difference between the power adapters, you can check the physical size, the label and the connector position of the power connectors.

Figure 36. Power adapters

Procedure

Step 1. Install the power adapter.

- If you are installing a power adapter while a node is installed in an enclosure, complete the following steps.
  1. Insert the power adapter into the cage.
     - E1 Enclosure (1U 2-node)

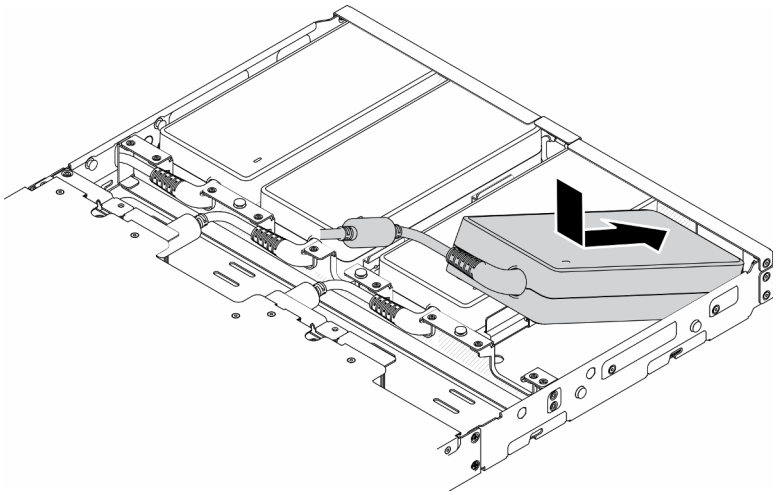


Figure 37. Power adapter installation

– E2 Enclosure (2U 2-node)

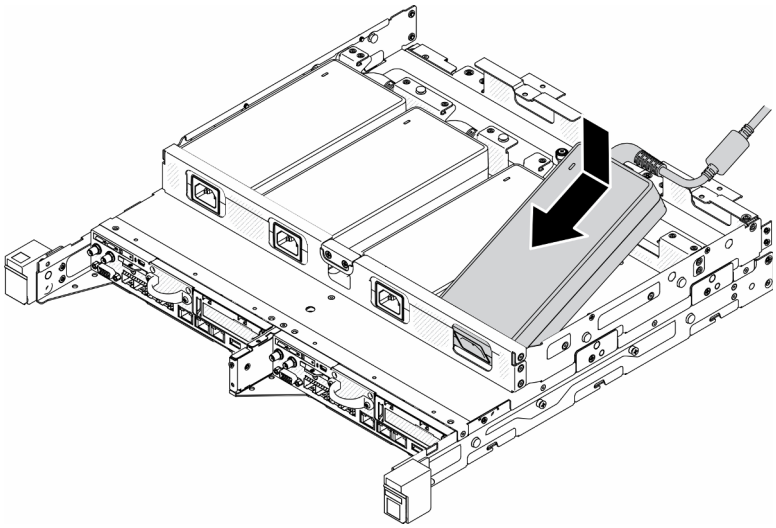


Figure 38. Power adapter installation

2. Slightly push the bracket backward and install the bracket.
3. Install the two screws.
   – E1 Enclosure (1U 2-node)

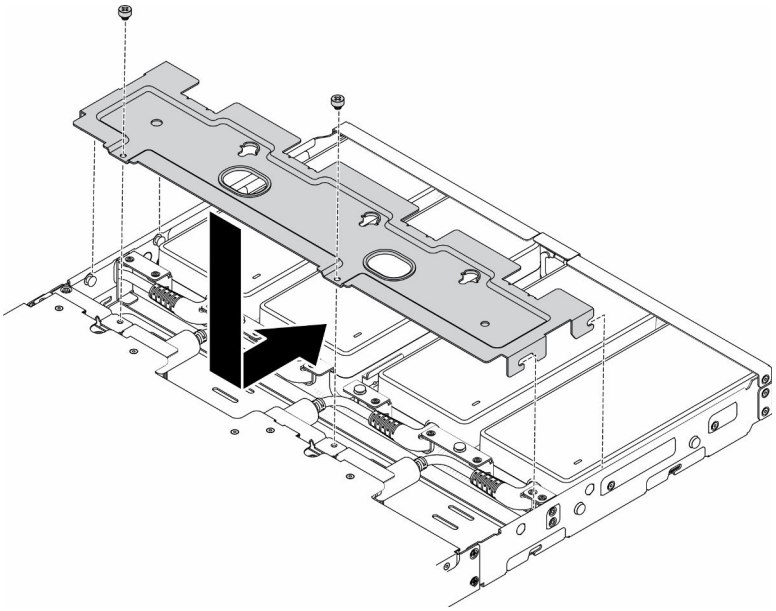


Figure 39. Bracket installation

– E2 Enclosure (2U 2-node)

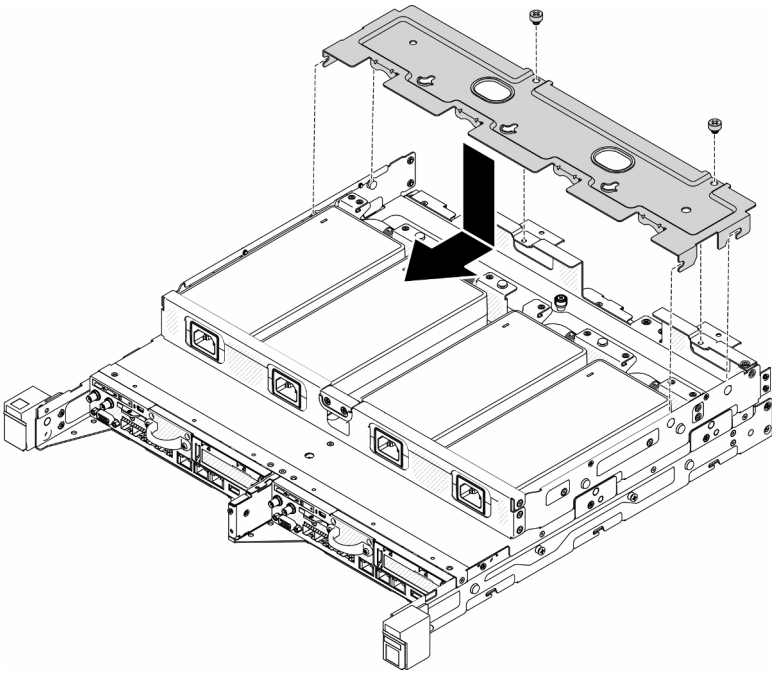


Figure 40. Bracket installation

- If you are installing a power adapter into a power adapter bracket, complete the following steps.
  1. Align the power adapter with the power adapter bracket; then, slide the power adapter into place.
  2. Align the tab with the slot and carefully hook the tab into place.
  3. Fasten the thumbscrew.

Note: See *Configuration Installation Guide* for the DIN rail configuration and wall-mounted configuration installation details if necessary.

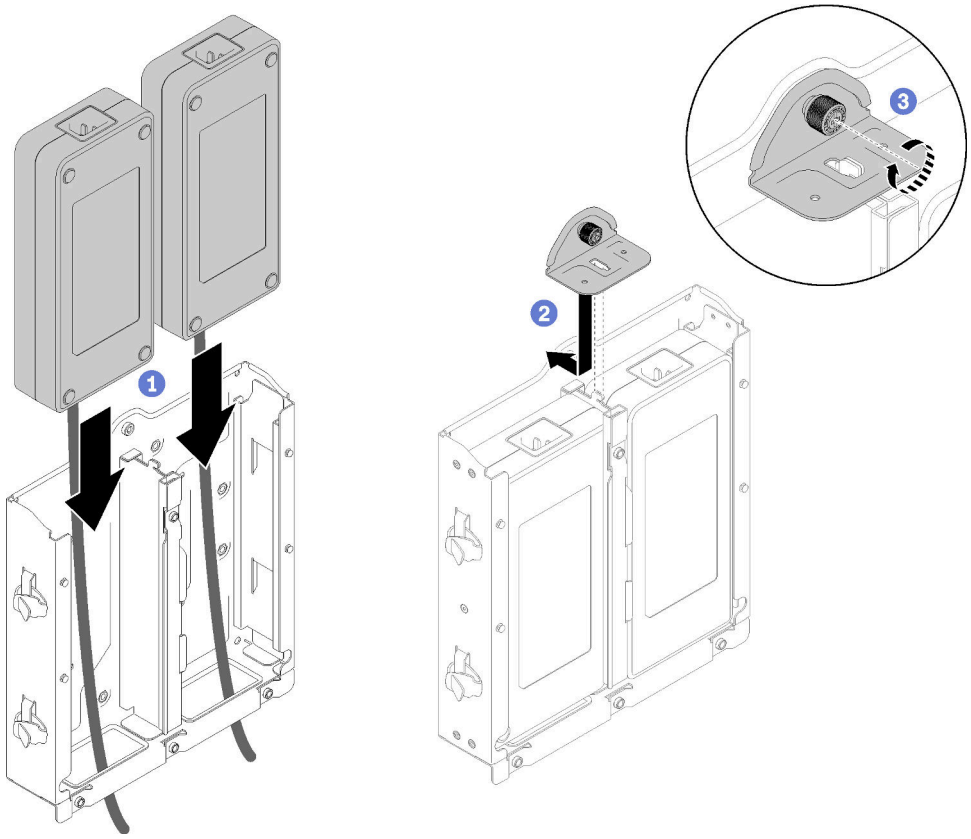


Figure 41. Power adapter installation

1. Install the enclosure into rack if necessary.
2. Refer to *Configuration Installation Guide* for the DIN rail configuration and wall-mounted configuration installation details if necessary.
3. Reconnect power cords and all external cables.
4. Turn on the server (see “Power on the server” on page 75).

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=MyPVTlRwTkk

Install the M.2 boot adapter

Use this information to install the M.2 boot adapter.

Before you install the M.2 boot adapter, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Important:

- Boot drives for **VMware ESXI**: For VMware ESXi boot support, only certain M.2 drives are supported, based on their endurance. For more specific information, see Lenovo support tip HT512201.
- The M.2 drives on opposite sides of the adapter must be of the same form factor (that is, the same physical length) because they share the same mounting clip.

  For more details about the M.2 drive and slot numbering, see “M.2 drive and slot numbering” on page 26.

For more information about the M.2 adapter, see https://lenovopress.com/lp0769-thinksystem-m2-drives-adapters.

Procedure

Step 1. Align the M.2 boot adapter with the connector on the system board, and press the adapter straight into the connector.

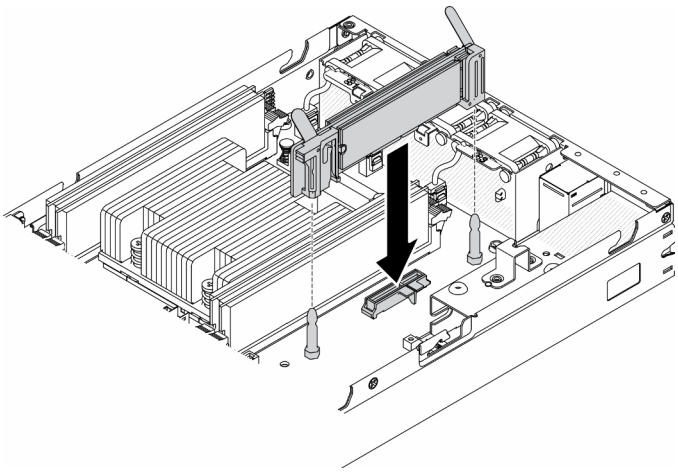


Figure 42. M.2 boot adapter installation

After you install the M.2 boot adapter, complete the following steps:

1. Install the intrusion switch (see “Install the intrusion switch cable” on page 63).
2. Install the node if needed (see “Install a node” on page 71).
3. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=UQCntTJVQ_o

Install a M.2 data adapter

Use this information to install a M.2 data adapter.

Before you install a M.2 data adapter, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Note: For more details about the M.2 drive and slot numbering, see “M.2 drive and slot numbering” on page 26.

Procedure

Step 1. Align the M.2 data adapter with the slot on the riser card; then, carefully press the M.2 data adapter straight into the slot until it is securely seated.

Step 2. Install the screw.

- M.2 riser assembly

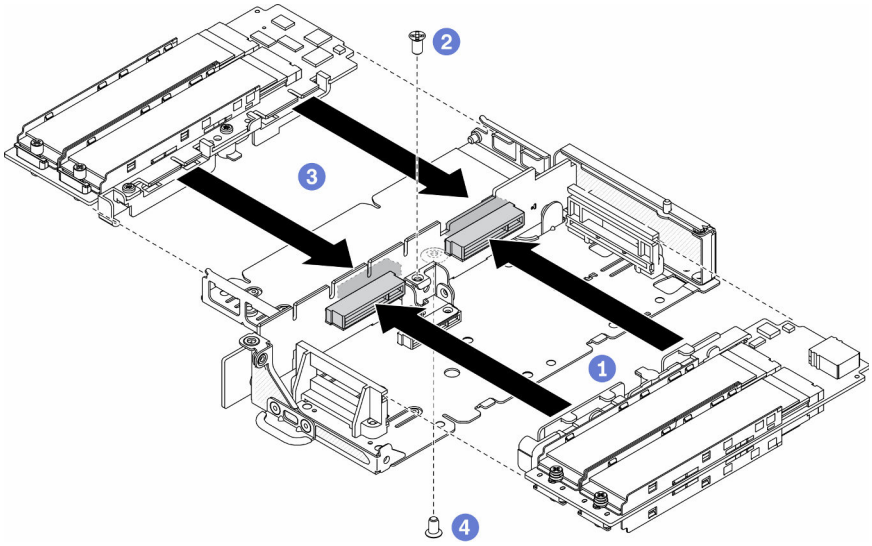


Figure 43. M.2 data adapter installation

- PCIe and M.2 riser assembly

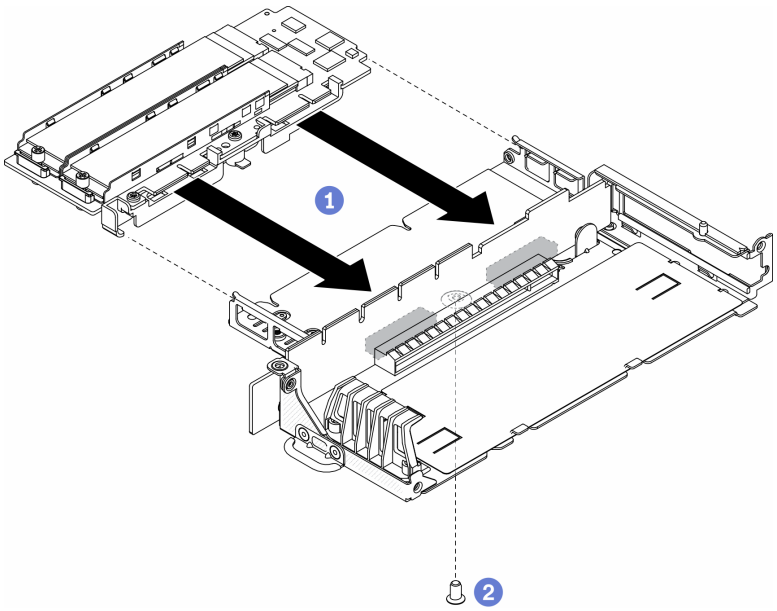


Figure 44. M.2 data adapter installation

Step 3. Insert the bezels to the riser assembly on the both sides and install the six screws as shown.

Note: The color and the size of the screws on each side are different, make sure to install the short ones one the left and long ones on the right.

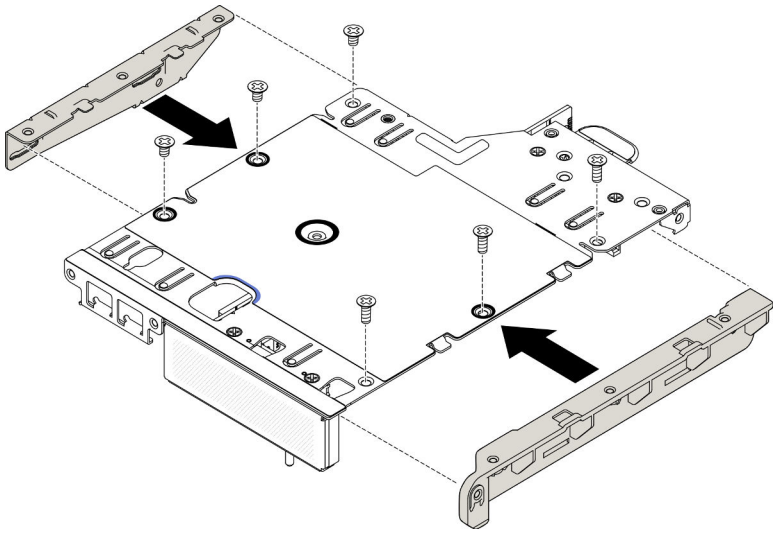


Figure 45. M.2 data adapter installation

After you install a M.2 data adapter, complete the following steps:

1. Install the PCIe riser assembly (see “Install the PCIe riser assembly” on page 60 for instructions).
2. Install the node if needed (see “Install a node” on page 71).
3. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=bucg3_aMYLY

Install the M.2 WLAN/LTE wireless adapter

Use this information to install the M.2 WLAN/LTE wireless adapter.

Before you install the M.2 WLAN/LTE wireless adapter, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Notes:

- LTE and WLAN performance may vary depending on your configurations and environments.
- There are two types of the wireless adapter for the server, only one can be used at a time. Both are installed in the same method:
  - M.2 WLAN/LTE wireless adapter that comes with both WLAN and 4G LTE modules.
  - M.2 WLAN wireless adapter comes only with WLAN module
- The absence, removal, or the defectiveness of the WLAN/LTE modules could cause a system error event.

If the WLAN/LTE configuration error event occurred, follow the steps below:

1. Ensure the system firmware (UEFI, XCC, etc.) and switch board firmware are up-to-date.
2. Power off the system and check if the WLAN/LTE module is installed properly, re-seat it if necessary. WLAN/LTE module is required for server operation.
3. Replace the module if the message persists after proper reinstallation. The module may be defective in this situation.

Procedure

Step 1. Align the M.2 wireless adapter with the connector on the system board, and press the adapter straight into the connector.

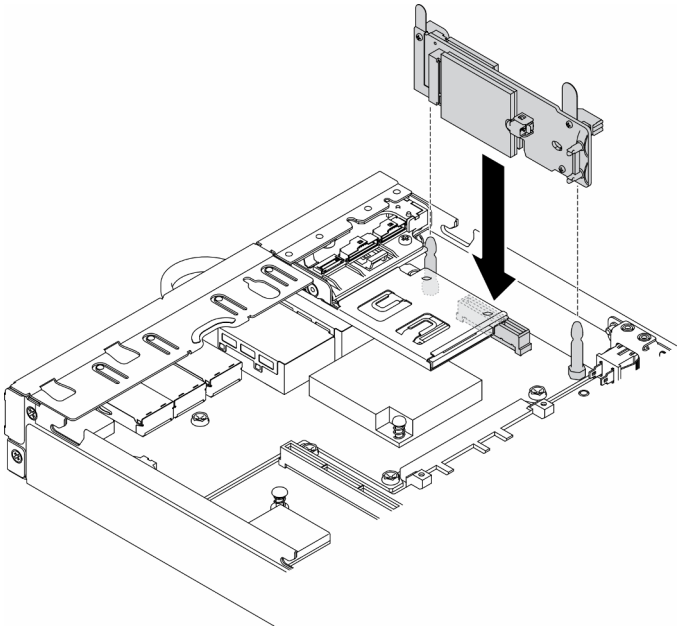


Figure 46. M.2 WLAN/LTE wireless adapter installation

After you install the M.2 WLAN/LTE wireless adapter, complete the following steps:

1. Install the lock position switch if removed (see “Install the lock position switch” on page 67).
2. Install the node if needed (see “Install a node” on page 71).
3. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=T3SEbjlZYCI

Install the SIM card

Use this information to install the SIM card.

Before you install the SIM card, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34

2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Note: To enable LTE, SIM card installation is required. LTE service is provided by authorized mobile service carriers in respective countries or regions. Server must have a cellular plan from a service carrier to connect to the LTE network.

Procedure

Step 1. Locate the SIM card position on the M.2 WLAN/LTE wireless adapter.

Step 2. Slide the retainer cover backward and rotate it up.

Step 3. Carefully place the SIM card on the slot.

Step 4. Rotate the retainer cover down and slide it frontward.

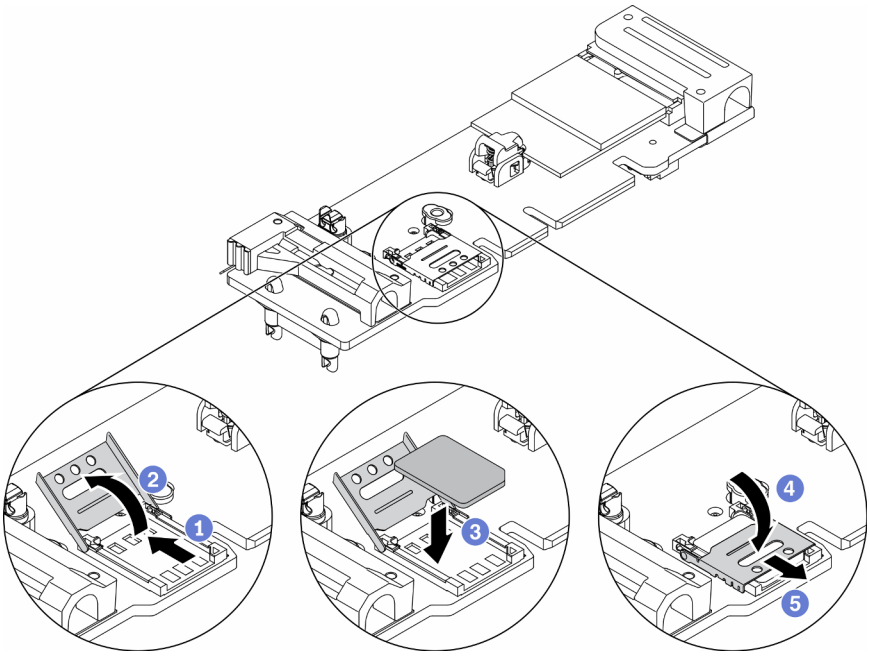


Figure 47. SIM card installation

After you install the SIM card, complete the following steps:

1. Install the M.2 WLAN/LTE wireless adapter (see “Install the M.2 WLAN/LTE wireless adapter” on page 56).
2. Install the node if needed (see “Install a node” on page 71).
3. Reconnect power cords and all external cables.
4. Follow the setup process to enable SIM card:

   Note: Obtain the PIN code, APN, and other settings from your carrier or SIM provider and keep it in a safe place.

   - PIN code:
     - When the PIN code of the SIM card is required, use the following command lines (using 1234 as an example of PIN code):

```
sudo uci set network.lte_wan.pincode='1234'
sudo uci commit network
sudo /etc/init.d/network restart
```

  - When the PIN code of the SIM card is not required, use the following command lines:

```
sudo uci del network.lte_wan.pincode
sudo uci del network.lte_wan.auth
sudo uci del network.lte_wan.username
sudo uci commit network
sudo reboot
```

- APN:
  - When APN setting is required, use the following command lines (using 1234 as an example of APN):

```
sudo uci set network.lte_wan.apn='1234'
sudo uci commit network
sudo reboot
```

  - When the APN setting is not required, use the following command lines:

```
sudo uci set network.lte_wan.apn='internet'
sudo uci commit network
sudo reboot
```

Note: For more information about configuring the LTE settings, see **Configure LTE setting** under "Embedded switch CLI for wireless LOM Package configuration" on page 97.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=izsv4NKEj_E

Install the PCIe adapter

Use this information to install the PCIe adapter.

To avoid possible danger, read and follow the following safety statement.

- **S012**

CAUTION:
Hot surface nearby.

Before you install the PCIe adapter, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Procedure

Remove the filler on the rear side of the riser assembly. Remove the screws of the adapter retainer and remove the adapter.

Step 1. Align the adapter with the slot on the riser card; then, carefully press the adapter straight into the slot until it is securely seated.

Step 2. Install the screw of the adapter.

Step 3. Install the screws of the adapter retainer.

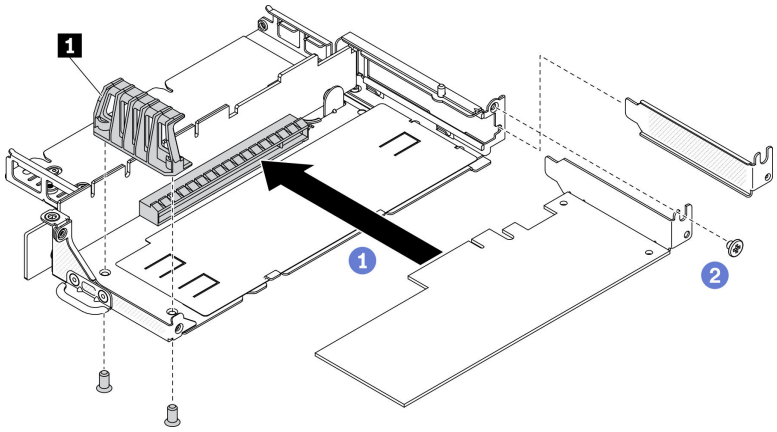


Figure 48. PCIe adapter installation

Table 21. PCIe adapter installation

1 Adapter retainer

After you install the PCIe adapter, complete the following steps:

1. Install the PCIe riser assembly (see “Install the PCIe riser assembly” on page 60 for instructions).
2. Install the node if needed (see “Install a node” on page 71).
3. Reconnect power cords and all external cables.
4. When installing an L4 GPU, make sure to update the system firmware to the latest version (see “Update the firmware” on page 80).

Install the PCIe riser assembly

Use this information to install the PCIe riser assembly.

To avoid possible danger, read and follow the following safety statement.

- **S012**

CAUTION:
Hot surface nearby.

Before you install the PCIe riser assembly, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Install the required adapters.
4. Remove the filler if it is installed.
   a. Remove the three screws.
   b. Grasp the filler by its edges and carefully lift it out of the server.

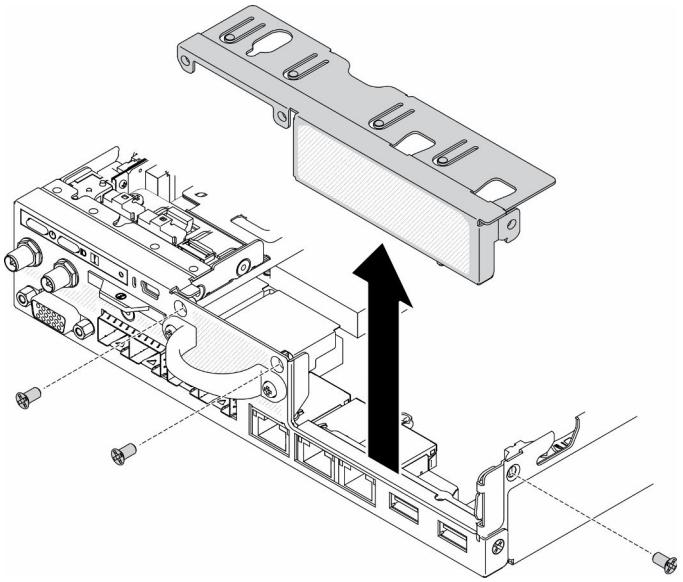


Figure 49. Filler removal

Procedure

Step 1. If the adapter bracket is not installed, install it by fastening the two screws as shown.

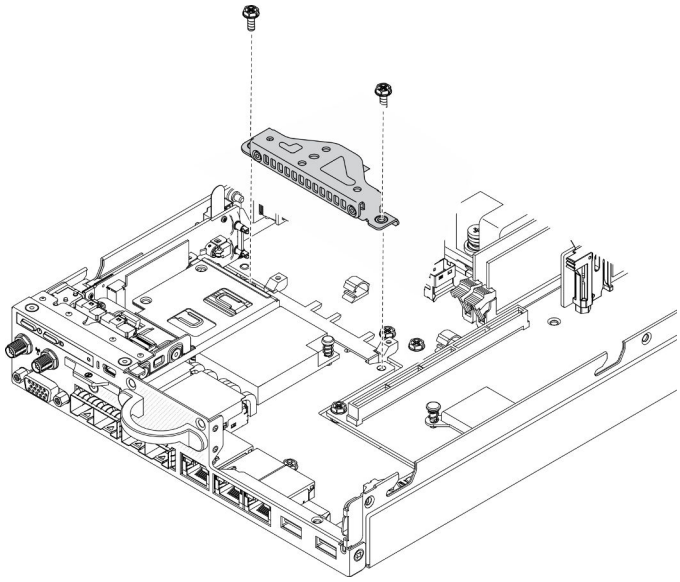


Figure 50. PCIe riser assembly installation

Step 2. Lower the PCIe riser assembly into the chassis and press the PCIe riser assembly down until it is securely seated.

Step 3. Install the seven screws.

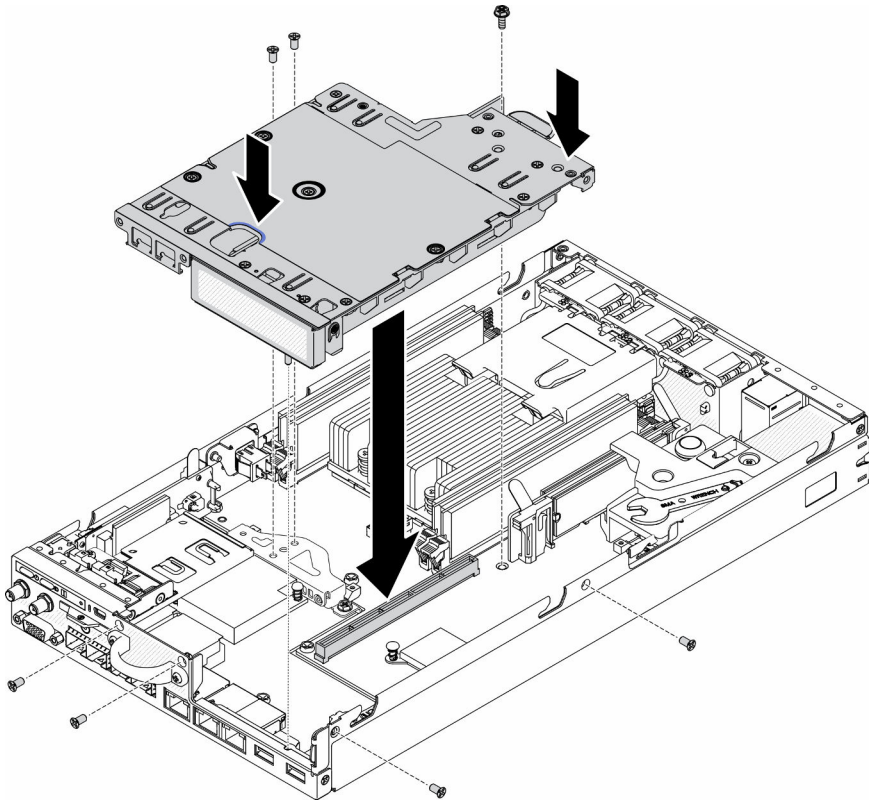


Figure 51. PCIe riser assembly installation

After you install the PCIe riser assembly, complete the following steps:

1. Install the node if needed (see “Install a node” on page 71).
2. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=gb2GUg6zM5U

Install the intrusion switch cable

Use this information to install the intrusion switch cable.

Before you install the intrusion switch cable, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Procedure

Insert the intrusion switch cable through the hole on the carrier.

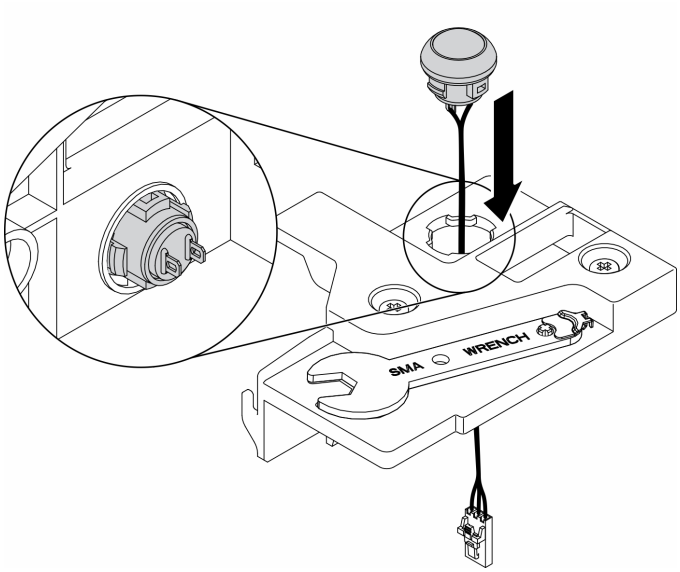


Figure 52. Intrusion switch cable installation

Step 1. Lower the intrusion switch carrier into the chassis and press the intrusion switch carrier down until it is securely seated.

Step 2. Fasten the two screws.

Step 3. Connect the cable to the connector and press it down until it clicks.

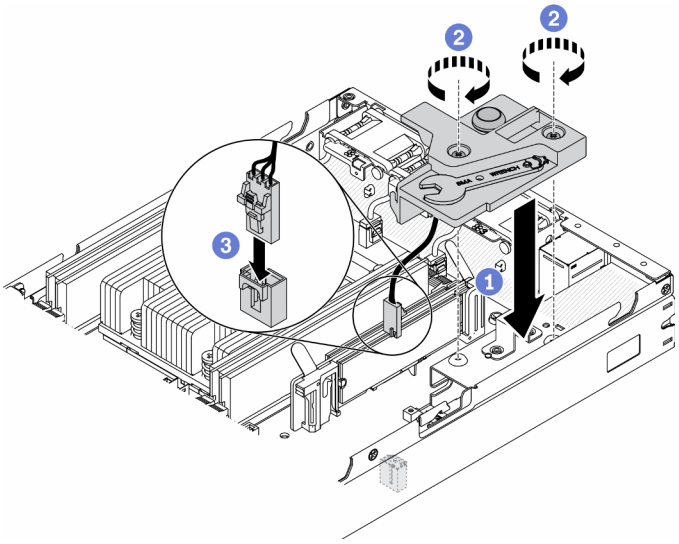


Figure 53. Intrusion switch installation

After you install the intrusion switch, complete the following steps:

1. Install the node if needed (see “Install a node” on page 71).
2. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=NREyfSHp0so

Install a DIMM

Use this information to install a DIMM.

See “Memory module installation rules and order” on page 36 for detailed information about memory configuration and setup.

Before you install a DIMM, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Touch the static-protective package that contains the component to any unpainted metal surface on the server; then, remove it from the package and place it on a static-protective surface.

The following illustration shows the system-board components, including DIMM connectors.

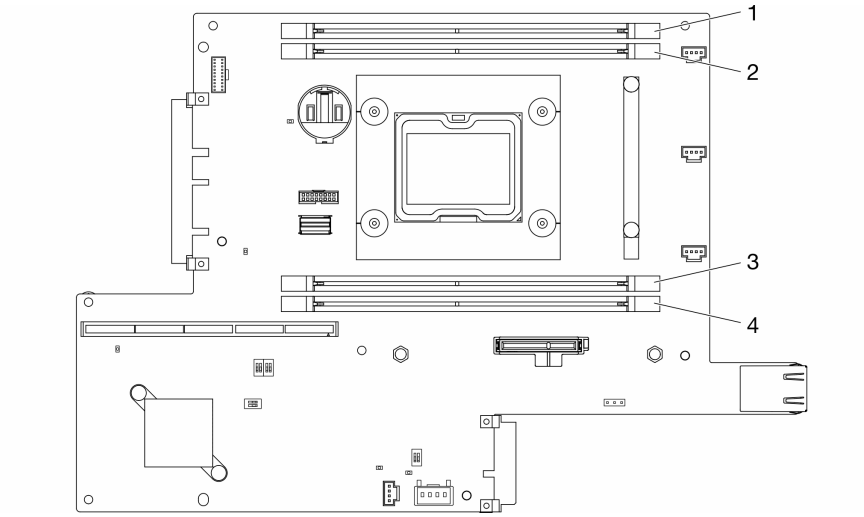


Figure 54. DIMM connectors

To install a DIMM, complete the following steps:

Attention: Memory modules are sensitive to static discharge and require special handling. In addition to the standard guidelines for "Handling static-sensitive devices" on page 36:

- Always wear an electrostatic-discharge strap when removing or installing memory modules. Electrostatic-discharge gloves can also be used.
- Never hold two or more memory modules together so that they touch. Do not stack memory modules directly on top of each other during storage.
- Never touch the gold memory module connector contacts or allow these contacts to touch the outside of the memory-module connector housing.
- Handle memory modules with care: never bend, twist, or drop a memory module.

Procedure

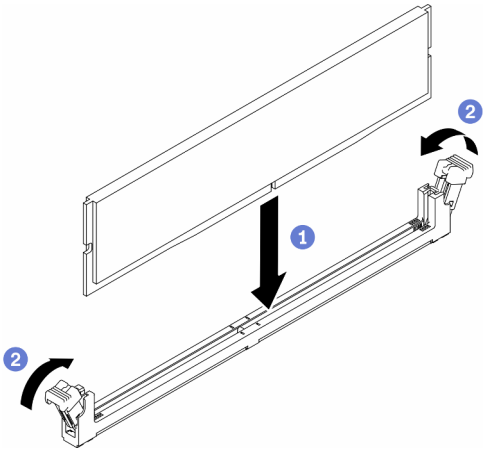


Figure 55. DIMM installation

Step 1. Make sure the retaining clips are in the fully-open position; then, align the keys on the DIMM with the connector.

Step 2. Firmly press both ends of the DIMM straight down into the connector until the retaining clips snap into the locked position.

Step 3. If you are installing additional DIMMs, do so now.

After you install the DIMM, complete the following steps:

1. Reinstall the air baffle if it is removed (see “Install the air baffle” on page 68).
2. Install the node if needed (see “Install a node” on page 71).
3. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=rdNqcD88sKs

Install the front operator panel

Use this information to install the front operator panel.

Before you install the front operator panel, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Procedure

Step 1. Slide the front operator panel into the assembly bay.

Step 2. Install the screw to secure the front operator panel.

Step 3. Carefully connect the two Y-cable connectors.

Step 4. Carefully route the cable underneath the metal pull tab holder.

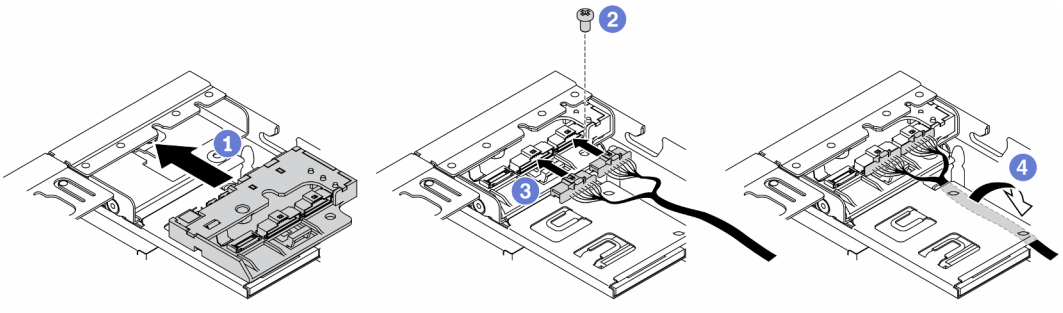


Figure 56. Front operator panel installation

After you install the front operator panel, complete the following steps:

1. Install the M.2 WLAN/LTE wireless adapter if needed.
2.
3. Install the lock position switch if removed (see “Install the lock position switch” on page 67).
4. Install the node if needed (see “Install a node” on page 71).
5. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=brflcu2bLa8

Install the lock position switch

Use this information to install the lock position switch.

Before you install the lock position switch, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Procedure

Step 1. Hook the lock position switch onto the pin; then, slightly push it leftward.

Step 2. Install and fasten the screw.

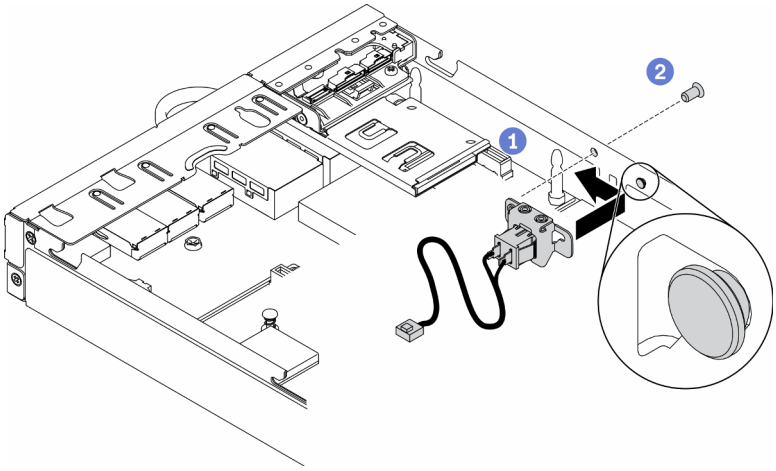


Figure 57. Lock position switch installation

Step 3. Carefully route the cables as the following illustration and connect the connector.

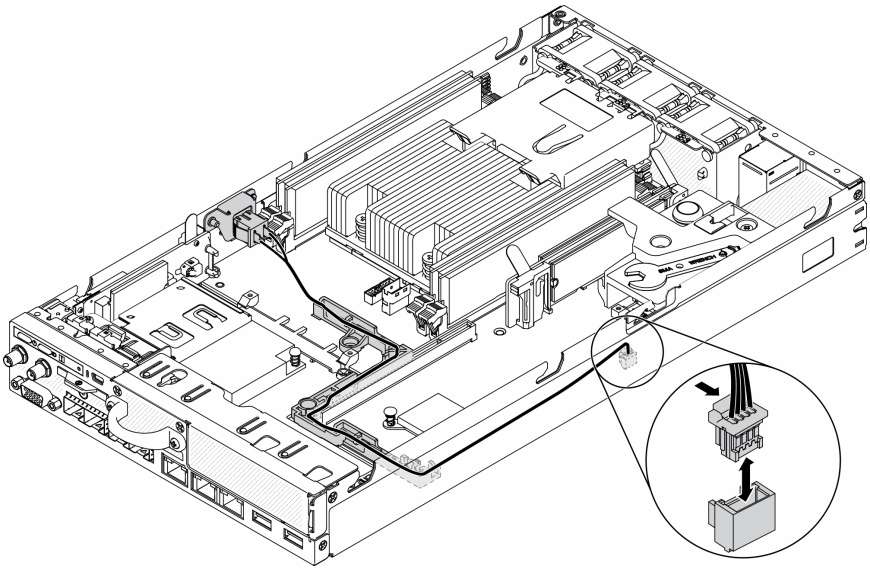


Figure 58. Lock position switch cable

After you install the lock position switch, complete the following steps:

1. Reinstall the PCIe riser cage (see “Install the PCIe riser assembly” on page 60).
2. Install the node if needed (see “Install a node” on page 71).
3. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=6kb5ahC0UFs

Install the air baffle

Use this information to install the air baffle.

To avoid possible danger, read and follow the following safety statement.

- **S012**

CAUTION:
Hot surface nearby.

Before you install the air baffle, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).

Procedure

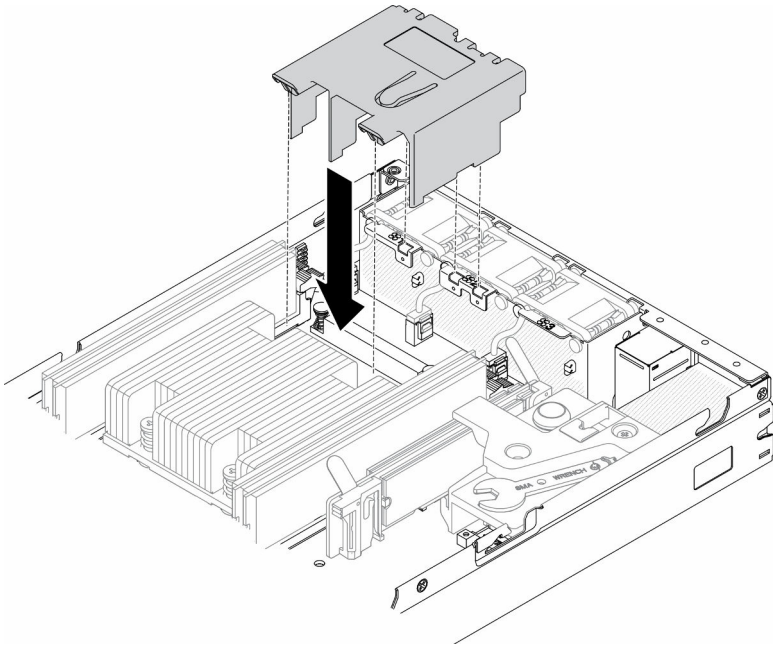


Figure 59. Air baffle installation

Step 1. Align the tabs on both sides of the air baffle with the corresponding slots; then, lower the air baffle into the chassis and press the air baffle down until it is securely seated.

After you install the air baffle, complete the following steps:

1. Install the node if needed (see “Install a node” on page 71).
2. Reconnect power cords and all external cables.

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=5HpaVy2ZgOM

Install the top cover

Use this information to install the top cover.

To avoid possible danger, read and follow the following safety information.

S012

CAUTION:
Hot surface nearby.

S014

CAUTION:
Hazardous voltage, current, and energy levels might be present. Only a qualified service technician is authorized to remove the covers where the label is attached.

S033

CAUTION:
Hazardous energy present. Voltages with hazardous energy might cause heating when shorted with metal, which might result in spattered metal, burns, or both.

Before you install the top cover, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Turn off the server. Disconnect the power cords and all external cables (see “Power off the server” on page 75).
3. Make sure all the removed components are installed, and all the disconnected cables inside the server are reconnected.

Procedure

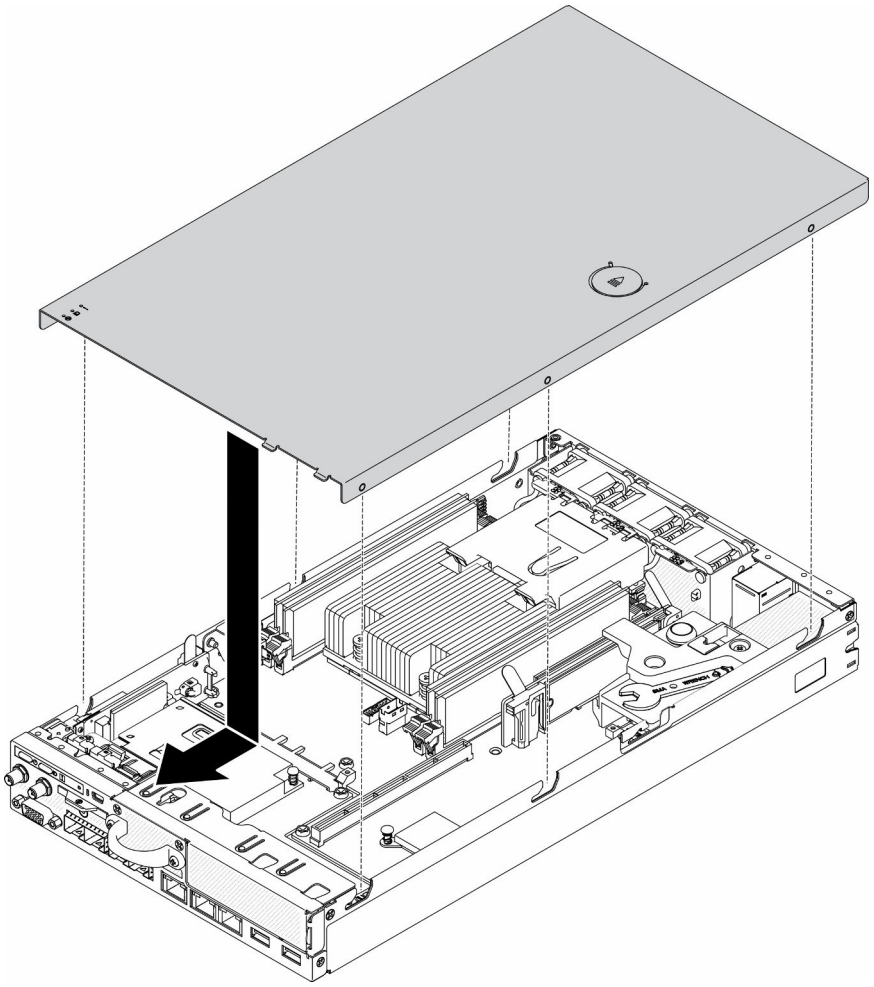


Figure 60. Top cover installation

Step 1. Align the posts inside the top cover with the slots on the chassis.

Step 2. Hold the front of the server and slide the top cover towards the front server until it clicks into place.

After you install the top cover, complete the following steps:

1. Reconnect power cords and all external cables.
2. Turn on the server (see “Power on the server” on page 75).

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=84O4Mv7aaiw

Install a node

Use this information to install a node.

Before you install a node, complete the following steps:

1. Read the following sections to ensure that you work safely.
   - “Installation Guidelines” on page 34
2. Make sure all the removed components are installed, and all the disconnected cables inside the server are reconnected.

Procedure

Step 1. To install the node into the node sleeve, complete the following steps.

a. Align the node with the node sleeve and slide the node into place.

b. Fasten the two thumbscrews.

Note: See *Configuration Installation Guide* for the bookshelf configuration, DIN rail configuration and wall-mounted configuration installation details if necessary.

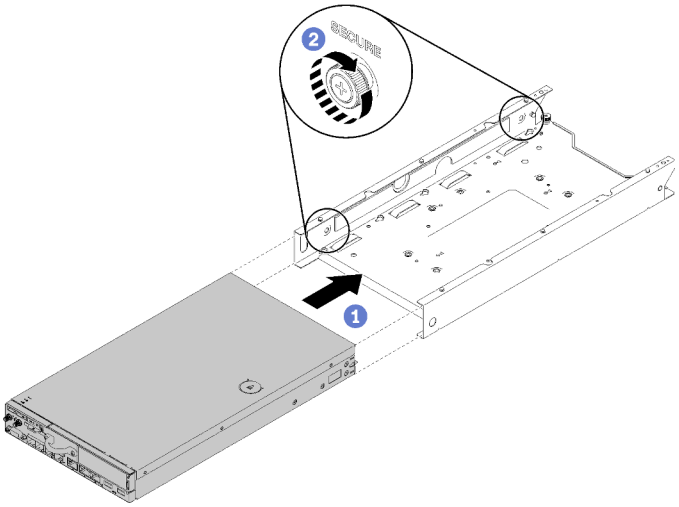


Figure 61. Node installation

Step 2. To install the node into the enclosure, complete the following steps.

Attention: If the node is to be installed in an E1 Enclosure (1U 2-node), change the vital product data (VPD) for proper operation. See *Change the VPD for E1 Enclosure configuration (trained technician only)* in *Maintenance Manual*.

a. Determine the node bay to install the node.

b. Insert the node into the node bay until it stops.

- E1 Enclosure (1U 2-node)

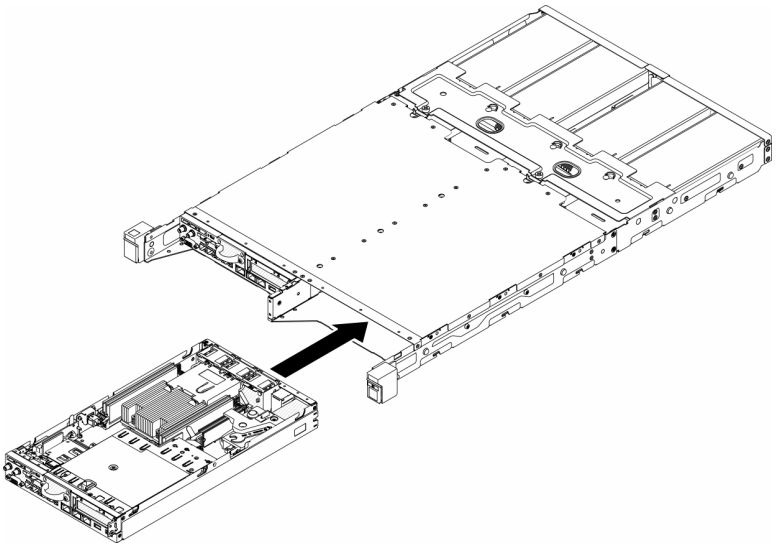


Figure 62. Node installation

- E2 Enclosure (2U 2-node)

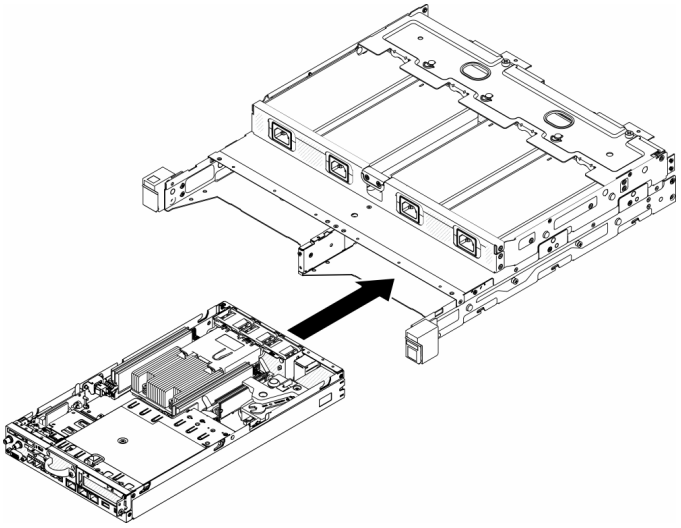


Figure 63. Node installation

c. Align and insert the shipping bracket onto the front of the enclosure.

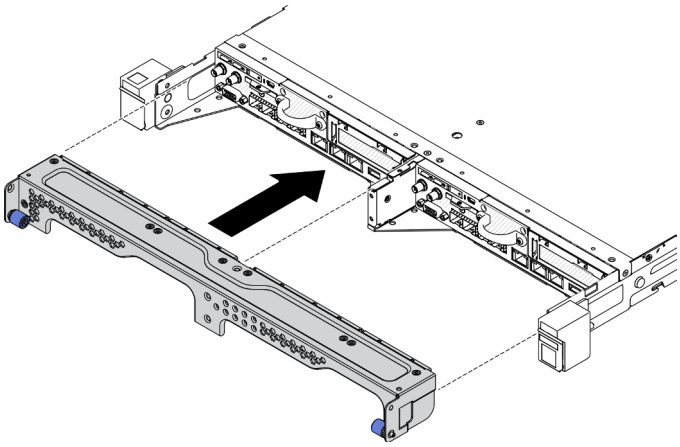


Figure 64. Node installation

d. Install the five screws and fasten the two thumb screws to secure the shipping bracket.

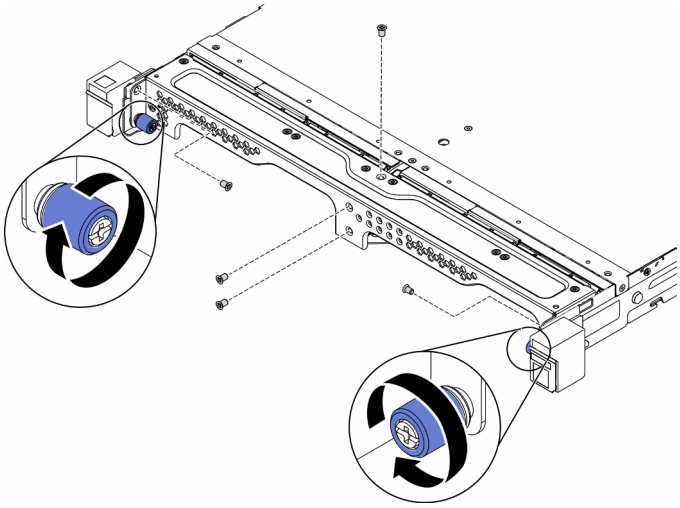


Figure 65. Node installation

After you install a node, complete the following steps:

1. Install the enclosure into rack if necessary.
2. Reconnect power cords and all external cables.
3. Turn on the server (see “Power on the server” on page 75).

Demo video

- Watch the procedure on YouTube: https://www.youtube.com/watch?v=SkYYnMect9w

Install the server in a rack

To install the server in a rack, follow the instructions that are provided below.

To install the enclosure into a rack, see the links below.

- For the installation guides of different rail kits, see ThinkEdge and ThinkSystem edge server rail options.

- For the procedures of installing a node to the enclosure, see “Install a node” on page 71.

The instructions are also provided in hardcopy with the Rail Installation Kit for the rails on which the enclosure will be installed.

Cable the server

Attach all external cables to the server. Typically, you will need to connect the server to a power source, to the data network, and to storage. In addition, you will need to connect the server to the management network.

Connect to power

Connect the server to power.

Connect to the network

Connect the server to the network.

Connect to storage

Connect the server to any storage devices.

Power on the server

After the server performs a short self-test (power status LED flashes quickly) when connected to input power, it enters a standby state (power status LED flashes once per second).

The server can be turned on (power LED on) in any of the following ways:

- You can press the power button.
- The server can restart automatically after a power interruption.
- The server can respond to remote power-on requests sent to the Lenovo XClarity Controller.

For information about powering off the server, see “Power off the server” on page 75.

Validate server setup

After powering up the server, make sure that the LEDs are lit and that they are green.

Power off the server

The server remains in a standby state when it is connected to a power source, allowing the Lenovo XClarity Controller to respond to remote power-on requests. To remove all power from the server (power status LED off), you must disconnect all power cables.

To place the server in a standby state (power status LED flashes once per second):

Note: The Lenovo XClarity Controller can place the server in a standby state as an automatic response to a critical system failure.

- Start an orderly shutdown using the operating system (if supported by your operating system).
- Press the power button to start an orderly shutdown (if supported by your operating system).
- Press and hold the power button for more than 4 seconds to force a shutdown.

When in a standby state, the server can respond to remote power-on requests sent to the Lenovo XClarity Controller. For information about powering on the server, see “Power on the server” on page 75.

Chapter 4. System configuration

Complete these procedures to configure your system. For SE350 with Security Pack, automatic data protection is enabled, SED data access can be locked up at tamper events, and you will need to claim and activate the system in order to unlock and access data. SE350 Standard does not lock up data access at all, SED management and tamper setting are disabled on SE350 Standard.

Notes:

- *SE350 with Security Pack* is also known simply as *SE350* prior to July 2021.
- You can check whether your system is SE350 with Security Pack or SE350 Standard in Lenovo XClarity Controller.

Before using the SE350 with Security Pack, the following procedures must be completed.

- "Activate the system" on page 77
- "Lockdown Mode and Motion Detection" on page 78
- "Backup the Self Encryption Drive Authentication Key (SED AK) " on page 79

Activate the system

ThinkSystem SE350 with Security Pack is shipped in locked state for security. Before operation, the server needs to be activated to be able to boot up and fully functional. Follow the detailed steps below to activate the system.

Create a Lenovo ID

Use existing Lenovo ID or create a new one to log in the ThinkSystem Key Vault Portal or ThinkShield mobile APP.

- For Lenovo ID setup, see https://passport.lenovo.com.
- To log in the Lenovo ThinkSystem Key Vault Portal, see https://portal.thinkshield.lenovo.com.

Activation methods

There are two different methods to active the system. Depending on the environment of the server, decide the most suitable way to activate the server.

1. **Mobile App activation**

   For Mobile App activation method, you will need an Android or iOS based smartphone with cellular data connection and the USB cable that came with the smartphone. An additional mini-USB dongle is provided to go into the XCC management USB port.

   Note: When the smart phone prompts for the USB connection purpose, choose data transfer.

   a. Connect the power cable to your ThinkSystem SE350 with Security Pack.
   b. Download the ThinkShield Edge Mobile Management App from Google Play Store, Apple App Store, Baidu or Lenovo App Store to your Android or iOS phone (search term: "ThinkShield Edge").
   c. Log-in to the ThinkShield Edge Mobile Management App using your Organization registered ID.
   d. When App instructs to do so, connect USB cable with USB mobile phone charging cable to ThinkSystem SE350 with Security Pack.
   e. Follow the "Activate Device" on-screen instructions to complete secure activation of ThinkSystem SE350.

f. When activated successfully, ThinkShield Edge Mobile Management App will provide “Device Activated” screen.

For the detailed steps, see https://download.lenovo.com/servers_pdf/thinkshield-mobile-application-user-guide-v6.pdf or https://support.lenovo.com/tw/en/solutions/ht509033.

2. **Internet connection activation**

For Internet connection activation, you will need the Machine Type, Serial Number, and Activation Code.

a. Connect the power cable to your ThinkSystem SE350 with Security Pack.

b. Connect the XClarity Controller Management Ethernet port to a network that has access to the internet.

Note: Outbound TCP port 443 (HTTPS) must be open for activation to occur.

c. Log in to the ThinkShield Key Vault Portal with your Organization registered ID.

d. To claim the ThinkSystem SE350 with Security Pack, add the device by clicking the orange plus sign next to “Devices” in Device Manager. Enter machine type, serial number, and secure activation code in the corresponding fields.

e. From the Device Manager, select the server you plan to activate and click activate. The status of the server will change to Ready.

f. Server will be activated within 15 minutes and power on automatically. After successful activation, the status of the server will change to Active on the ThinkShield Key Vault Portal.

Note: If the server activation is not initiated within 2 hours after the power cable plug in, perform a disconnect then re-connect of the power cable to your ThinkSystem SE350 with Security Pack.

For the detailed steps, see https://download.lenovo.com/servers_pdf/thinkshield-web-application-user-guide-v2.pdf.

Customer's responsibility:

- Keep Secure Activation Code (provided in flyer).
- Maintain a back up of SED AK, see “Backup the Self Encryption Drive Authentication Key (SED AK) ” on page 79.
- Move SE350 system to a safe working place for service.
- Prepare the cable of mobile phone.
- Engage IT department so they can help to claim or activate device when required.
- Confirm if the SE350 system is claimed. If not, work with IT department to claim the device.
- Restore SED AK from the back up file and set the password.
- Place SE350 system back to the working place after service.
- Confirm the wireless (network) connectivity is working. Service technician cannot help examine the connection of the device to network.

Lockdown Mode and Motion Detection

ThinkSystem SE350 with Security Pack is shipped in locked state for security. Status can be changed through XCC.

See more information on https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/system_lockdown_mode.html.

Backup the Self Encryption Drive Authentication Key (SED AK)

After setting up the ThinkSystem SE350 with Security Pack or making changes to the configuration, backing up the Self Encryption Drive Authentication Key (SED AK) is a must operation to prevent data loss in the hardware failure case.

SED Authentication Key (AK) Manager

Find SED Authentication Key (AK) Manager in Lenovo XClarity Controller to change, backup, or recover the SED AK of the server. See https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.doc/dw1lm_c_ch1_introduction.html for more information.

Change the SED AK

- **Generate SED AK from Passphrase:** Set the password and reenter it for the confirmation. Click **Re-generate** to get the new SED AK.
- **Generate a Random SED AK:** Click Re-generate to get a Random SED AK.

  Note: If System Lockdown Mode is enabled, generating SED AK function is not available.

Backup the SED AK

Set the password and re-enter it for the confirmation. Click **Start Backup** to back the SED AK; then, download the SED AK file and store it safely for future use.

Note: If you use the backup SED AK file to restore a configuration, the system will ask for the password that you set here.

Recover the SED AK

- **Recover SED AK using Passphrase:** Use the password that set in **Generate SED AK from Passphrase** mode to recover the SED AK.
- **Recover SED AK from Backup file:** Upload the backup file generated in **Backup the SED AK** mode and enter the corresponding backup file password to recover the SED AK.

Set the network connection for the Lenovo XClarity Controller

Before you can access the Lenovo XClarity Controller over your network, you need to specify how Lenovo XClarity Controller will connect to the network. Depending on how the network connection is implemented, you might need to specify a static IP address as well.

The following methods are available to set the network connection for the Lenovo XClarity Controller if you are not using DHCP:

- If a monitor is attached to the server, you can use Lenovo XClarity Provisioning Manager to set the network connection.

  Complete the following steps to connect the Lenovo XClarity Controller to the network using the Lenovo XClarity Provisioning Manager.

  1. Start the server.
  2. Press the key specified in the on-screen instructions to display the Lenovo XClarity Provisioning Manager interface. (For more information, see the “Startup” section in the LXPM documentation compatible with your server at https://pubs.lenovo.com/lxpm-overview/.)
  3. Go to **LXPM → UEFI Setup → BMC Settings** to specify how the Lenovo XClarity Controller will connect to the network.

  - If you choose a static IP connection, make sure that you specify an IPv4 or IPv6 address that is available on the network.
  - If you choose a DHCP connection, make sure that the MAC address for the server has been configured in the DHCP server.

4. Click **OK** to apply the setting and wait for two to three minutes.
5. Use an IPv4 or IPv6 address to connect Lenovo XClarity Controller.

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

- If no monitor attached to the server, you can set the network connection through the Lenovo XClarity Controller interface. Connect an Ethernet cable from your laptop to Lenovo XClarity Controller connector, which is located at the front of the server. For the location of the Lenovo XClarity Controller connector, see "Front view" on page 18.

  Note: Make sure that you modify the IP settings on the laptop so that it is on the same network as the server default settings.

  The default IPv4 address and the IPv6 Link Local Address (LLA) is provided on the Lenovo XClarity Controller Network Access label that is affixed to the Pull Out Information Tab.

- If you are using the Lenovo XClarity Administrator Mobile app from a mobile device, you can connect to the Lenovo XClarity Controller through the Lenovo XClarity Controller USB connector on the front of the server. For the location of the Lenovo XClarity Controller USB connector, see "Front view" on page 18.

  Note: The Lenovo XClarity Controller USB connector mode must be set to manage the Lenovo XClarity Controller (instead of normal USB mode). To switch from normal mode to Lenovo XClarity Controller management mode, hold the blue ID button on the front panel for at least 3 seconds until its LED flashes slowly (once every couple of seconds).

  To connect using the Lenovo XClarity Administrator Mobile app:

  1. Connect the USB cable of your mobile device to the Lenovo XClarity Administrator USB connector on the front panel.
  2. On your mobile device, enable USB tethering.
  3. On your mobile device, launch the Lenovo XClarity Administrator mobile app.
  4. If automatic discovery is disabled, click **Discovery** on the USB Discovery page to connect to the Lenovo XClarity Controller.

  For more information about using the Lenovo XClarity Administrator Mobile app, see:

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

Update the firmware

Several options are available to update the firmware for the server.

You can use the tools listed here to update the most current firmware for your server and the devices that are installed in the server.

- Best practices related to updating firmware is available at the following site:
  - http://lenovopress.com/LP0656
- The latest firmware can be found at the following site:

  - https://datacentersupport.lenovo.com/products/servers/thinksystem/se350/downloads
- You can subscribe to product notification to stay up to date on firmware updates:
  - https://datacentersupport.lenovo.com/tw/en/solutions/ht509500

UpdateXpress System Packs (UXSPs)

Lenovo typically releases firmware in bundles called UpdateXpress System Packs (UXSPs). To ensure that all of the firmware updates are compatible, you should update all firmware at the same time. If you are updating firmware for both the Lenovo XClarity Controller and UEFI, update the firmware for Lenovo XClarity Controller first.

Update method terminology

- **In-band update**. The installation or update is performed using a tool or application within an operating system that is executing on the server's core CPU.
- **Out-of-band update**. The installation or update is performed by the Lenovo XClarity Controller collecting the update and then directing the update to the target subsystem or device. Out-of-band updates have no dependency on an operating system executing on the core CPU. However, most out-of-band operations do require the server to be in the S0 (Working) power state.
- **On-Target update.** The installation or update is initiated from an installed operating system executing on the target server itself.
- **Off-Target update.** The installation or update is initiated from a computing device interacting directly with the server's Lenovo XClarity Controller.
- **UpdateXpress System Packs (UXSPs)**. UXSPs are bundled updates designed and tested to provide the interdependent level of functionality, performance, and compatibility. UXSPs are server machine-type specific and are built (with firmware and device driver updates) to support specific Windows Server, Red Hat Enterprise Linux (RHEL) and SUSE Linux Enterprise Server (SLES) operating system distributions. Machine-type-specific firmware-only UXSPs are also available.

Firmware updating tools

See the following table to determine the best Lenovo tool to use for installing and setting up the firmware:

Tool	Update Methods Supported	Core System Firmware Updates	I/O Devices Firmware Updates	Graphical user interface	Command line interface	Supports UXSPs
Lenovo XClarity Provisioning Manager (LXPM)	In-band[2] On-Target	√		√		
Lenovo XClarity Controller (XCC)	Out-of-band Off-Target	√	Selected I/O devices	√		

Tool	Update Methods Supported	Core System Firmware Updates	I/O Devices Firmware Updates	Graphical user interface	Command line interface	Supports UXSPs
Lenovo XClarity Essentials OneCLI (OneCLI)	In-band Out-of-band On-Target Off-Target	√	All I/O devices		√	√
Lenovo XClarity Essentials UpdateXpress (LXCE)	In-band Out-of-band On-Target Off-Target	√	All I/O devices	√		√
Lenovo XClarity Essentials Bootable Media Creator[3] (BoMC)	In-band Out-of-band Off-Target	√	All I/O devices	√ (BoMC application)	√ (BoMC application)	√
Lenovo XClarity Administrator (LXCA)	In-band[1] Out-of-band[2] Off-Target	√	All I/O devices	√		√
Lenovo XClarity Integrator (LXCI) for VMware vCenter	Out-of-band Off-Target	√	Selected I/O devices	√		
Lenovo XClarity Integrator (LXCI) for Microsoft Windows Admin Center	In-band Out-of-band On-Target Off-Target	√	All I/O devices	√		√

Tool	Update Methods Supported	Core System Firmware Updates	I/O Devices Firmware Updates	Graphical user interface	Command line interface	Supports UXSPs
Lenovo XClarity Integrator (LXCI) for Microsoft System Center Configuration Manager	In-band On-Target	√	All I/O devices	√		√
Notes: 1. For I/O firmware updates. 2. For BMC and UEFI firmware updates.						

- **Lenovo XClarity Provisioning Manager**

  From Lenovo XClarity Provisioning Manager, you can update the Lenovo XClarity Controller firmware, the UEFI firmware, and the Lenovo XClarity Provisioning Manager software.

  Note: By default, the Lenovo XClarity Provisioning Manager Graphical User Interface is displayed when you start the server and press the key specified in the on-screen instructions. If you have changed that default to be the text-based system setup, you can bring up the Graphical User Interface from the text-based system setup interface.

  For additional information about using Lenovo XClarity Provisioning Manager to update firmware, see:

  "Firmware Update" section in the LXPM documentation compatible with your server at https://pubs.lenovo.com/lxpm-overview/

- **Lenovo XClarity Controller**

  If you need to install a specific update, you can use the Lenovo XClarity Controller interface for a specific server.

  Notes:

  – To perform an in-band update through Windows or Linux, the operating system driver must be installed and the Ethernet-over-USB (sometimes called LAN over USB) interface must be enabled.

    For additional information about configuring Ethernet over USB, see:

    "Configuring Ethernet over USB" section in the XCC documentation version compatible with your server at https://pubs.lenovo.com/lxcc-overview/

  – If you update firmware through the Lenovo XClarity Controller, make sure that you have downloaded and installed the latest device drivers for the operating system that is running on the server.

  For additional information about using Lenovo XClarity Controller to update firmware, see:

  "Updating Server Firmware" section in the XCC documentation compatible with your server at https://pubs.lenovo.com/lxcc-overview/

- **Lenovo XClarity Essentials OneCLI**

  Lenovo XClarity Essentials OneCLI is a collection of command line applications that can be used to manage Lenovo servers. Its update application can be used to update firmware and device drivers for your servers. The update can be performed within the host operating system of the server (in-band) or remotely through the BMC of the server (out-of-band).

  For additional information about using Lenovo XClarity Essentials OneCLI to update firmware, see:

  https://pubs.lenovo.com/lxce-onecli/onecli_c_update

- **Lenovo XClarity Essentials UpdateXpress**

  Lenovo XClarity Essentials UpdateXpress provides most of OneCLI update functions through a graphical user interface (GUI). It can be used to acquire and deploy UpdateXpress System Pack (UXSP) update packages and individual updates. UpdateXpress System Packs contain firmware and device driver updates for Microsoft Windows and for Linux.

  You can obtain Lenovo XClarity Essentials UpdateXpress from the following location:

  https://datacentersupport.lenovo.com/solutions/lnvo-xpress

- **Lenovo XClarity Essentials Bootable Media Creator**

  You can use Lenovo XClarity Essentials Bootable Media Creator to create bootable media that is suitable for firmware updates, VPD updates, inventory and FFDC collection, advanced system configuration, FoD Keys management, secure erase, RAID configuration, and diagnostics on supported servers.

  You can obtain Lenovo XClarity Essentials BoMC from the following location:

  https://datacentersupport.lenovo.com/solutions/lnvo-bomc

- **Lenovo XClarity Administrator**

  If you are managing multiple servers using the Lenovo XClarity Administrator, you can update firmware for all managed servers through that interface. Firmware management is simplified by assigning firmware-compliance policies to managed endpoints. When you create and assign a compliance policy to managed endpoints, Lenovo XClarity Administrator monitors changes to the inventory for those endpoints and flags any endpoints that are out of compliance.

  For additional information about using Lenovo XClarity Administrator to update firmware, see:

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/update_fw.html

- **Lenovo XClarity Integrator offerings**

  Lenovo XClarity Integrator offerings can integrate management features of Lenovo XClarity Administrator and your server with software used in a certain deployment infrastructure, such as VMware vCenter, Microsoft Admin Center, or Microsoft System Center.

  For additional information about using Lenovo XClarity Integrator to update firmware, see:

  https://pubs.lenovo.com/lxci-overview/

Configure the firmware

Several options are available to install and set up the firmware for the server.

Important: Do not configure option ROMs to be set to **Legacy** unless directed to do so by Lenovo Support. This setting prevents UEFI drivers for the slot devices from loading, which can cause negative side effects for Lenovo software, such as Lenovo XClarity Administrator and Lenovo XClarity Essentials OneCLI, and to the Lenovo XClarity Controller. The side effects include the inability to determine adapter card details, such as model name and firmware levels. When adapter card information is not available, generic information for the model name, such as "Adapter 06:00:00" instead of the actually model name, such as "ThinkSystem RAID 930-16i 4GB Flash." In some cases, the UEFI boot process might also hang.

- **Lenovo XClarity Provisioning Manager**

  From Lenovo XClarity Provisioning Manager, you can configure the UEFI settings for your server.

  Notes: The Lenovo XClarity Provisioning Manager provides a Graphical User Interface to configure a server. The text-based interface to system configuration (the Setup Utility) is also available. From Lenovo XClarity Provisioning Manager, you can choose to restart the server and access the text-based interface.

In addition, you can choose to make the text-based interface the default interface that is displayed when you start LXPM. To do this, go to **Lenovo XClarity Provisioning Manager → UEFI Setup → System Settings → <F1>Start Control → Text Setup**. To start the server with Graphic User Interface, select **Auto** or **Tool Suite**.

See the following documentations for more information:

  - *Lenovo XClarity Provisioning Manager User Guide*
    - Search for the LXPM documentation version compatible with your server at https://pubs.lenovo.com/lxpm-overview/
  - *UEFI User Guide*
    - https://pubs.lenovo.com/uefi-overview/

- **Lenovo XClarity Essentials OneCLI**

  You can use the config application and commands to view the current system configuration settings and make changes to Lenovo XClarity Controller and UEFI. The saved configuration information can be used to replicate or restore other systems.

  For information about configuring the server using Lenovo XClarity Essentials OneCLI, see:

  https://pubs.lenovo.com/lxce-onecli/onecli_c_settings_info_commands

- **Lenovo XClarity Administrator**

  You can quickly provision and pre-provision all of your servers using a consistent configuration. Configuration settings (such as local storage, I/O adapters, boot settings, firmware, ports, and Lenovo XClarity Controller and UEFI settings) are saved as a server pattern that can be applied to one or more managed servers. When the server patterns are updated, the changes are automatically deployed to the applied servers.

  Specific details about updating firmware using Lenovo XClarity Administrator are available at:

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/server_configuring.html

- **Lenovo XClarity Controller**

  You can configure the management processor for the server through the Lenovo XClarity Controller Web interface or through the command-line interface.

  For information about configuring the server using Lenovo XClarity Controller, see:

  “Configuring the Server” section in the XCC documentation compatible with your server at https://pubs.lenovo.com/lxcc-overview/

Memory configuration

Memory performance depends on several variables, such as memory mode, memory speed, memory ranks, memory population and processor.

More information about optimizing memory performance and configuring memory is available at the Lenovo Press website:

https://lenovopress.com/servers/options/memory

In addition, you can take advantage of a memory configurator, which is available at the following site:

http://1config.lenovo.com/#/memory_configuration

For specific information about the required installation order of memory modules in your server based on the system configuration and memory mode that you are implementing, see “Install a DIMM” on page 64.

RAID configuration

Using a Redundant Array of Independent Disks (RAID) to store data remains one of the most common and cost-efficient methods to increase server's storage performance, availability, and capacity.

RAID increases performance by allowing multiple drives to process I/O requests simultaneously. RAID can also prevent data loss in case of a drive failure by reconstructing (or rebuilding) the missing data from the failed drive using the data from the remaining drives.

RAID array (also known as RAID drive group) is a group of multiple physical drives that uses a certain common method to distribute data across the drives. A virtual drive (also known as virtual disk or logical drive) is a partition in the drive group that is made up of contiguous data segments on the drives. Virtual drive is presented up to the host operating system as a physical disk that can be partitioned to create OS logical drives or volumes.

An introduction to RAID is available at the following Lenovo Press website:

https://lenovopress.com/lp0578-lenovo-raid-introduction

Detailed information about RAID management tools and resources is available at the following Lenovo Press website:

https://lenovopress.com/lp0579-lenovo-raid-management-tools-and-resources

Notes:

- Before setting up RAID for NVMe drives, follow the below steps to enable VROC:
  1. Restart the system. Before the operating system starts up, press **F1** to enter the Setup Utility.
  2. Go to **System settings → Devices and I/O Ports → Intel VMD** and enable the option.
  3. Save the changes and reboot the system.
- VROC Intel-SSD-Only supports RAID levels 0, 1, 5, and 10 with Intel NVMe drives.
- VROC Premium requires an activation key and supports RAID levels 0, 1, 5, and 10 with non-Intel NVMe drives. For more information about acquiring and installing the activation key, see https://fod.lenovo.com/lkms.

Wireless enabled LOM package configuration

Use this information to set configuration of wireless enabled LOM package.

To enable wireless function of the server, complete the following steps:

1. Install the wireless enabled LOM package.
2. Define the usage scenario and choose the most suitable one from the preset topologies, see “Wireless enabled LOM package preset” on page 89.
3. If no topology in presets are applicable, it is optional to create a customized one, see Customized configuration.
4. Enable **Wi-Fi/LTE Connectivity** on Lenovo XClarity Controller.

Note: To enable LTE, SIM card installation is required (see “Install the SIM card” on page 57). LTE service is provided by authorized mobile service carriers in respective countries or regions. Server must have a cellular plan from a service carrier to connect to the LTE network.

Inside the wireless enabled LOM package, there is an embedded switch. It works as a router with LTE function, WLAN (AP/Client mode), and 1 GbE ports for uplink and downlink.See more information of the ports:

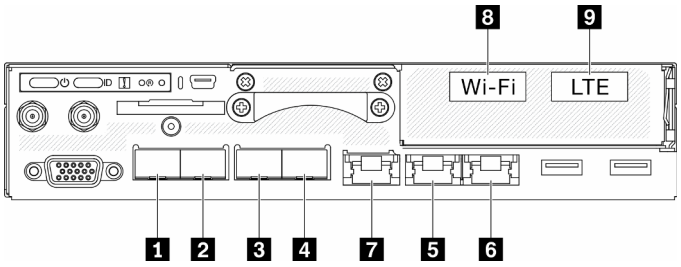


Figure 66. Wired/Wireless port on front panel

Table 22. Wired/Wireless port on front panel

	Physical Ports	**Interface Name (Used in Embedded Switch CLI)**
1	10 GbE SFP+	N/A
2	10 GbE SFP+	N/A
3	1 GbE SFP	eth6
4	1 GbE SFP	eth3
5	1 GbE RJ45	eth1
6	1 GbE RJ45	eth2
7	1 GbE RJ45	eth4
8	Wi-Fi (WLAN)	wlan0
9	LTE	wwan0

- 2x 1GbE SFP ports (port 3 and 4): support 1000 Base–X SFP only
- 2x 1GbE RJ45 ports (port 5 and 6): support 10/100/1000 Mbps
- WLAN interface: work as uplink in client mode or downlink in AP mode
- LTE interface: work as uplink port only. Supports only nano SIM
- Dedicated internal 10GbE port: connected to the OS (it is called “LOM1-Switchboard” in Windows OS)
- Embedded Switch CLI can be accessed by SSH from Management port (port 7) but dedicated address (192.168.70.254)
  - User name: oper
  - Password: (use the same password as XCC)
- By default, Embedded Switch has active DHCP server on all its physical down-link ports, included Wi-Fi if it is in AP mode
- IP assignment range:
  - Downlink ports: 192.168.71.x
  - WLAN (AP mode): 192.168.74.x

– Dedicated internal 10GbE port to the OS (it is called “LOM1-Switchboard” in Windows OS): 192.168.73.x

Wired networking ports (port 1 – 7) are enabled by default. LOM1-Switchboard, Uplink, Downlink, Management, WLAN and LTE interface belong to different VLANs. Embedded switch operates at L3 routing.

- LOM1-Switchboard (br-x86_lan): default IP is 192.168.73.254/24. DHCP server is enabled by default
- Uplink (cloud_wan / lte_wan / wifi_wan_sta): default setting is DHCP client
- Downlink (br-edge_lan): default IP is 192.168.71.254/24. DHCP server is enabled by default
- WLAN in AP Mode (br-wifi_lan_ap): default IP is 192.168.74.254/24. DHCP server is enabled by default
- WLAN in Client Mode (wifi_wan_sta): default setting is DHCP client
- Management port (br-mgmt_xcc_lan)
- XCC: Can be accessed from Management port only by default. Default setting is DHCP client, fallback IP for XCC is 192.168.70.125/24. Default IP is 192.168.70.254/24. Can be set to DHCP client, or be set as DHCP server.

Notes:

- Uplink/Downlink ports will be changed based on topology preset. Users can adapt configuration via “uci” CLI commands and save it to customized preset.
- Fail-over (Cloud Port & LTE) feature is disabled by default, users need to enable it through embedded Switch CLI as follows:

```
sudo uci set network.cloud_wan.metric='10'
sudo uci set network.lte_wan.metric='30'
sudo uci set network.wifi_wan_sta.metric='20'
sudo uci commit network
sudo /etc/init.d/network restart
```

  After completing the setting, system starts the function of fail-over/fall-back among port 6 (cloud_wan/eth2), WLAN in Client mode (wifi_wan_sta/wlan0), and LTE port (lte_wan/wwan0).

WLAN configuration

WLAN networking (AP mode and client mode) is disabled by default in ThinkSystem SE350. Users can enable/disable wireless networking and choose mode in XCC GUI (Edge Networking page) or via Embedded switch CLI.

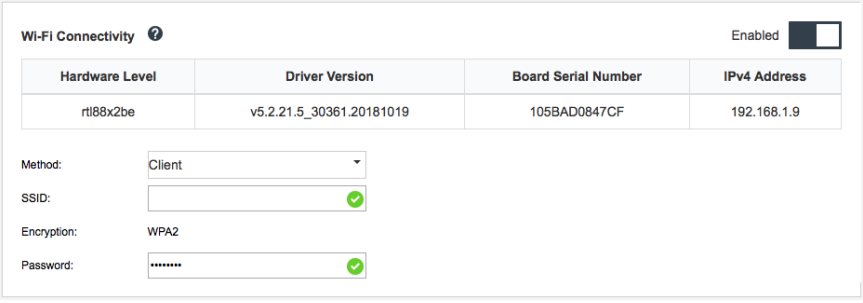


Figure 67. WLAN setting

LTE configuration

Wireless networking (LTE) is disabled by default in ThinkSystem SE350. Users can Enabled/Disabled LTE via XCC GUI (Edge Networking page) or via Embedded Switch CLI.

- Use embedded switch CLI to set LTE configuration.
- SIM card PIN number and APN are needed to enable LTE.

Figure 68. LTE setting

BMC network bridge

BMC network bridge is an configuration to select the outbound interface to access to BMC management port. There are four options as shown below. The default is “None”, which means only management port can access XCC interface.

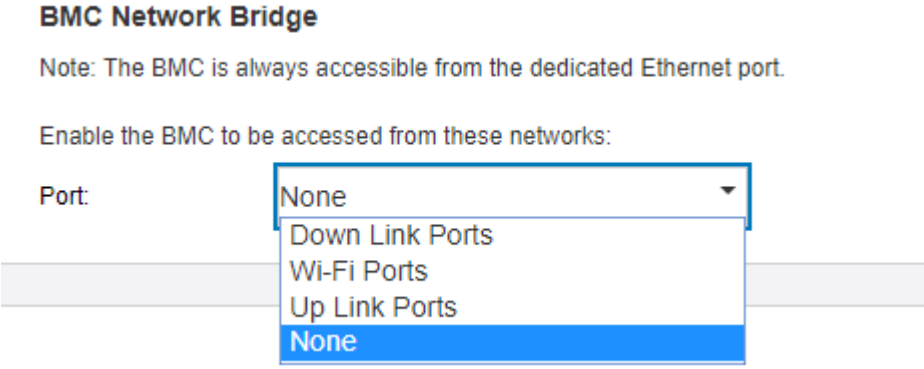


Figure 69. BMC network bridge

Notes:

- Ports assignment varies with network topology preset, set up this parameter along with "network topology preset".
- When "Uplink ports" is configured to "BMC Network Bridge" and network preset #1 to #4 is selected, "DHCP server" must be enabled via the XCC GUI (Edge Networking page).

Wireless enabled LOM package preset

Use this information to apply preset configuration of wireless enabled LOM package.

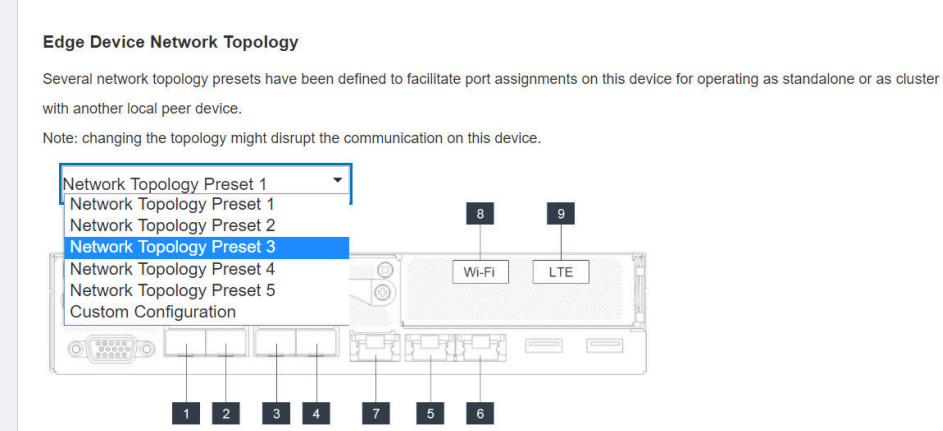
Setting up the network topology

A network topology is an arrangement of network in which all nodes connect with each other using network links. Several network topologies presets have been defined to facilitate port assignment of the server. Depends on usage scenario, server can operate as a standalone system or as a cluster with other peer servers.

There are six types of network topology available for chosen (configuration 1-5 are preset, configuration 6 is available for customized).

To change between topologies, use Lenovo XClarity Controller or Embedded Switch CLI (access through SSH):

- Lenovo XClarity Controller: select topology type in **Edge Networking**



- Embedded Switch CLI (access through SSH): use command `sudo set_topology 1`
  - Change topology by changing the number in the command. Number could be 1-6. Noted that topology 6 could only be used after customized setting had been created.

Notes:

- LTE/WLAN and IPMI over KCS Access are disabled by default, it is required to enable them through XCC.
- System resets the network settings of ports to default after users change network topology.

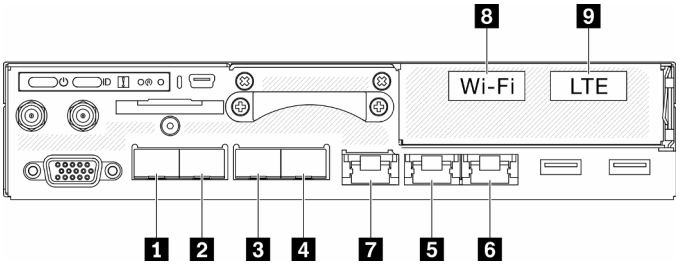


Figure 70. Ports on the front of the server

Table 23. Wired/Wireless port on front panel

	Physical Ports	Interface Name (Used in Embedded Switch CLI)
1	10 GbE SFP+	N/A
2	10 GbE SFP+	N/A
3	1 GbE SFP	eth6
4	1 GbE SFP	eth3
5	1 GbE RJ45	eth1
6	1 GbE RJ45	eth2
7	1 GbE RJ45	eth4
8	Wi-Fi	wlan0
9	LTE	wwan0

Configuration 1:

In configuration 1, most of the ports are used as downlink port (edge port). Server provides maximum capacity of connection for other devices, but without failover protection. LTE and WLAN AP mode are both applicable for usage in this configuration.

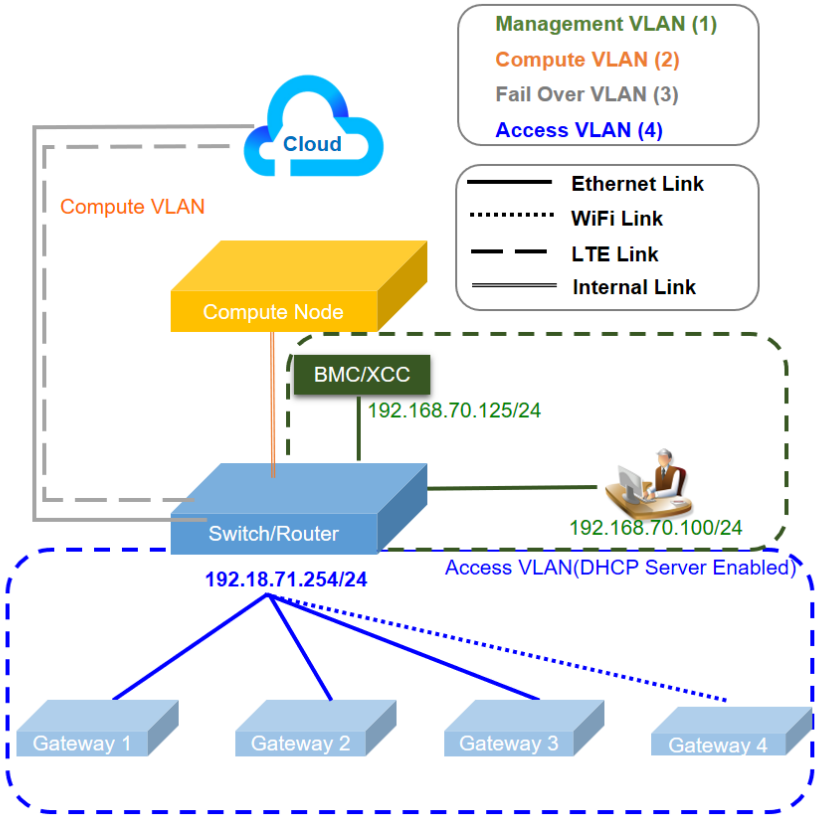


Table 24. Configuration 1 - maximum access links to IOT gateway (default configuration)

Function	Port
Host port	1 and 2 Two 10Gb Ethernet SFP+
XCC Management port	7 1Gb Ethernet RJ45
Uplink port (cloud port)	6 1Gb Ethernet RJ45 9 LTE (an adapter inside the node, not a physical port, default is disabled)
Downlink port (edge port)	3 and 4 Two 1Gb Ethernet SFP 5 1Gb Ethernet RJ45 8 WLAN AP (an adapter inside the node, not a physical port, default is disabled)

Configuration 2:

In configuration 2, port 3 is used as cluster port (inter-switch port). Server provides redundancy, backup, or other usage depends on setting. LTE and WLAN AP mode are both applicable for usage in this configuration.

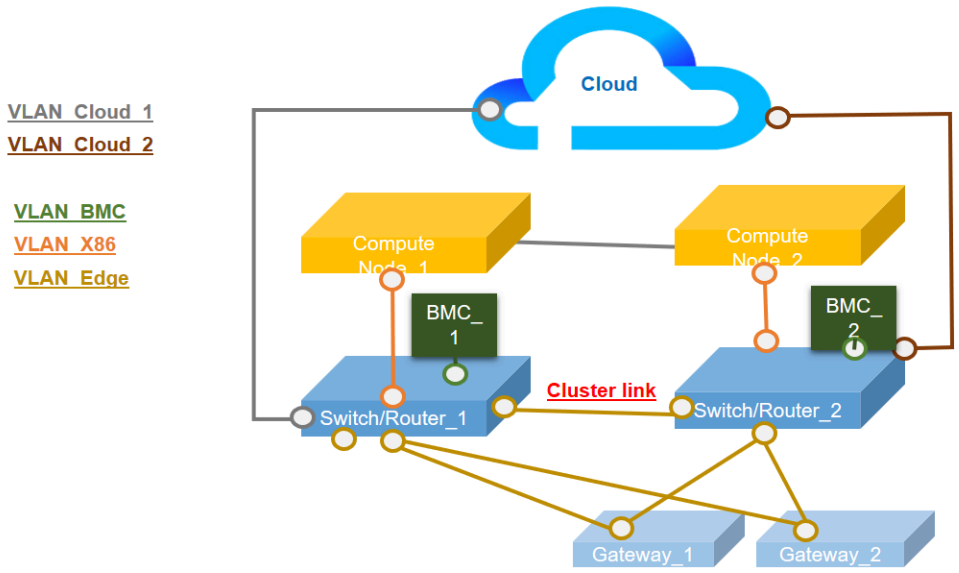


Table 25. Configuration 2 - Two ThinkSystem SE350 are connected as redundancy in cluster mode

Function	Port
Host port	1 and 2 Two 10Gb Ethernet SFP+
XCC Management port	7 1Gb Ethernet RJ45
Uplink port (cloud port)	6 1Gb Ethernet RJ45 9 LTE (an adapter inside the node, not a physical port, default is disabled)
Cluster port (inter-switch port)	3 1Gb Ethernet SFP
Downlink port (edge port)	4 1Gb Ethernet SFP 5 1Gb Ethernet RJ45 8 WLAN AP (an adapter inside the node, not a physical port, default is disabled)

Configuration 3:

In configuration 3, port 3 and port 4 are used as cluster port (inter-switch port). Server provides its maximum level of cluster toppology (three servers in maximum). LTE and WLAN AP mode are both applicable for usage in this configuration.

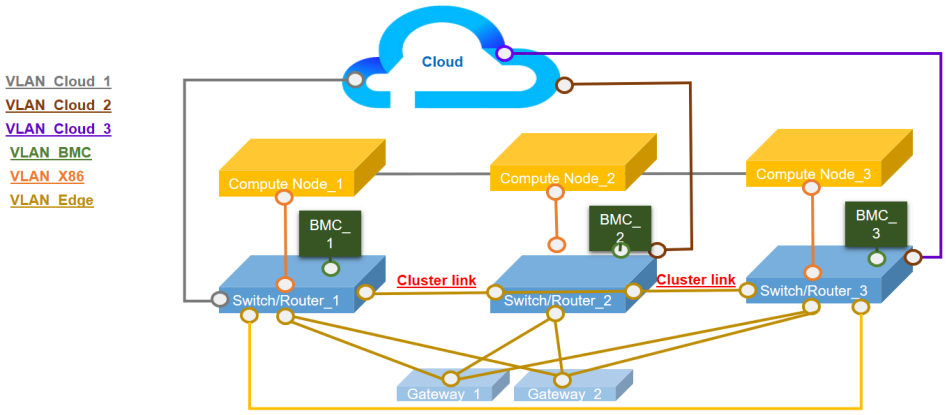


Table 26. Configuration 3 - Three ThinkSystem SE350 are connected as redundancy in cluster mode

Function	Port
Host port	1 and 2 Two 10Gb Ethernet SFP+
XCC Management port	7 1Gb Ethernet RJ45
Uplink port (cloud port)	6 1Gb Ethernet RJ45 9 LTE (an adapter inside the node, not a physical port, default is disabled)
Cluster port (inter-switch port)	3 and 4 Two 1Gb Ethernet SFP
Downlink port (edge port)	5 1Gb Ethernet RJ45 8 WLAN AP (an adapter inside the node, not a physical port, default is disabled)

Configuration 4:

In configuration 4, port 8 is used as WLAN client port for failover backup. Server connects to the existing Wi-fi as a client, users can access to Lenovo XClarity Controller through Wi-fi rather than physical wired connection. Only WLAN client mode is applicable for usage in this configuration.

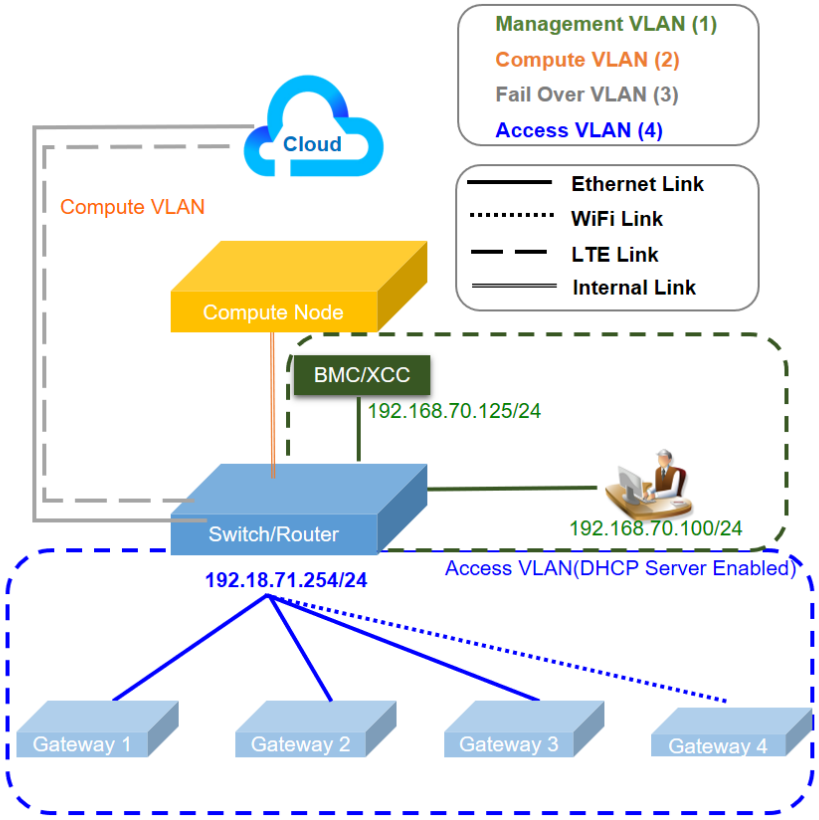


Table 27. Configuration 4 - WLAN port work as a uplink fail-over

Function	Port
Host port	1 and 2 Two 10Gb Ethernet SFP+
XCC Management port	7 1Gb Ethernet RJ45
Uplink port (cloud port)	6 1Gb Ethernet RJ45 8 WLAN client (an adapter inside the node, not a physical port, default is disabled) 9 LTE (an adapter inside the node, not a physical port, default is disabled)
Downlink port (edge port)	3 and 4 2x GbE SFP 5 1Gb Ethernet RJ45

Configuration 5:

In configuration 5, LTE/WLAN function is an optional. Server can work in wired environment.

Table 28. Configuration 5- Extra WLAN client as a uplink fail-over

Function	Port
Host port	1 and 2 Two 10Gb Ethernet SFP+
Plate (No pre-configured IP setting, ports in plate are like L2 dumb switch)	3 and 4 1 GbE SFP 5 and 6 1 GbE RJ45
User configuration	8 WLAN (an adapter inside the node, not a physical port, default is disabled)
XCC Management port	7 1Gb Ethernet RJ45
Uplink port (cloud port)	9 LTE (an adapter inside the node, not a physical port, default is disabled)

Configuration 6 (Custom Configuration):

If no configuration is found to meet the requirements, the customized configuration is available. It is best practice to select a preset which is similar to the requirements, and then adjust the setting through Embedded Switch CLI, see example commands in below:

Table 29. Configuration 6- customized configuration

```
# Disable DHCP server on Down Link ports
sudo uci set dhcp.lan.dhcpv4=disabled
sudo uci commit dhcp
sudo /etc/init.d/dnsmasq restart

# Includes physical ports into Down link
# Refer to Wired/wireless table in the manual for the detailed interface name
sudo uci set network.edge_lan.ifname='eth1 eth3 eth6'
sudo uci commit network.edge_lan
sudo /etc/init.d/network restart


# Configure static IP of Down link ports
sudo uci set network.edge_lan.proto=static
sudo uci set network.edge_lan.ipaddr=192.168.70.254
sudo uci set network.edge_lan.netmask=255.255.255.0
sudo uci commit network.edge_lan
sudo /etc/init.d/network restart


# Save the change into custom preset
sudo save_topology_config


# Change to custom preset (Or go to XCC web,"Edge Networking", select "custom configuration")
sudo set_topology 6
```

Note: To see content of custom configuration, go to "Configuration display" in "Embedded switch CLI for wireless LOM Package configuration" on page 97.

BMC network bridge

BMC network bridge is an configuration to select the outbound interface to access to BMC management port. There are four options as shown below. The default is "None", which means only management port can access XCC interface.

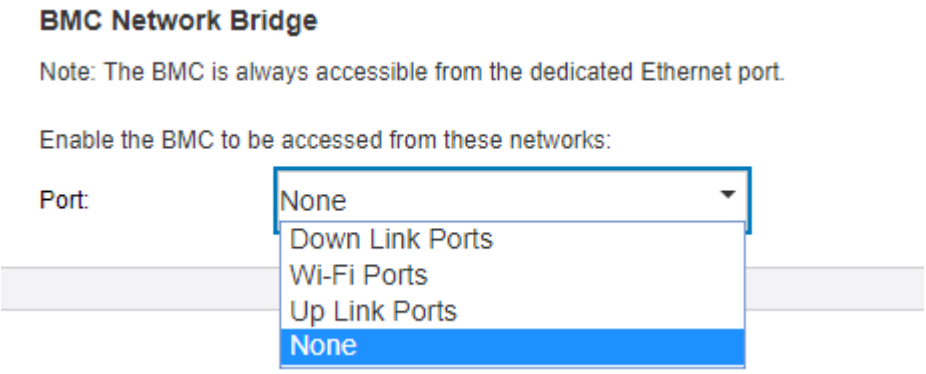


Figure 71. BMC network bridge

Embedded switch CLI for wireless LOM Package configuration

Use this information to set configuration of wireless LOM package.

Use UCI (Unified Configuration Interface) to configure wireless LOM package core services.

Embedded Switch CLI can be accessed by SSH from Management port but dedicated address (192.168.70.254)

- User name: oper
- Password: (use the same password as XCC)

Configuration display

To show the configuration of system wireless function, use the commands below:

- `sudo uci show` → Show entire system configuration
- `sudo uci show config_profile` → Show specific configure profile of all interfaces
- `sudo uci show config_profile.interface` → Show configure profile of specific interface
- `sudo uci show config_profile.interface.configName` → Show specific configure setting

Table 30. Common profiles

Configure profile	Description
dhcp	DHCP and DNS setting
firewall	firewall (NAT), packet filter, and port forwarding setting
network	Switch, interface, and route configuration
wireless	Wireless settings and wifi network definition

Table 31. Common interfaces

Interface name	Description
mgmt_xcc_lan	Management Port of XCC access
edge_lan	Downlink ports
cloud_wan	Uplink ports (Wireline)
x86_lan	Dedicated internal 10Gb port to the OS (in Windows is called “LOM1-Switchboard”)

Table 31. Common interfaces (continued)

Interface name	Description
lte_wan	4G LTE port
wifi_lan_ap	WLAN port (AP mode)
wifi_wan_sta	WLAN port (Station mode)

Commands example:

```
sudo uci show network
sudo uci show network.edge_lan
sudo uci show network.edge_lan.ipaddr
```

Configuration setting

Table 32. Configure a DHCP server (Profile dhcp)

Syntax

```
sudo uci set dhcp.<name>=dhcp
sudo uci set dhcp.<name>.ignore=<ignore>
sudo uci set dhcp.<name>.interface=<interface>
sudo uci set dhcp.<name>.start=<start>
sudo uci set dhcp.<name>.limit=<limit>
sudo uci set dhcp.<name>.leasetime=<leasetime>
sudo uci set dhcp.<name>.dynamicdhcp=<dynamicdhcp>
sudo uci set dhcp.<name>.force=<force>
sudo uci set dhcp.<name>.netmask=<netmask>
sudo uci set dhcp.<name>.dhcp_option=<dhcp_option>
sudo uci set dhcp.<name>.ra=<ra>
sudo uci set dhcp.<name>.dhcpv6=<dhcpv6>
sudo uci set dhcp.<name>.ndp=<ndp>
sudo uci set dhcp.<name>.ra_management=<ra_management>
sudo uci set dhcp.<name>.ra_default=<ra_default>
sudo uci add_list dhcp.<name>.dns=<dns>
sudo uci add_list dhcp.<name>.domain=<domain>
sudo uci commit dhcp
```

Table 33. Parameters

Name	Type	Required	Default	Description
name	string	no	none	Dhcp pool name.
ignore	boolean	no	0	Specifies whether dnsmasq should ignore this pool if set to 1.

Table 33. Parameters (continued)

Name	Type	Required	Default	Description
interface	logical interface name	yes	none	Specifies the interface associated with this DHCP address pool; must be one of the interfaces defined in /etc/config/network.
start	integer	yes	100	Specifies the offset from the network address of the underlying interface to calculate the minimum address that may be leased to clients. It may be greater than 255 to span subnets.
limit	integer	yes	150	Specifies the size of the address pool (e. g. with start=100, limit=150, maximum address will be .249).
leasetime	string	yes	12h	Specifies the lease time of addresses handed out to clients, for example 12h or 30m
dynamicdhcp	boolean	no	1	Dynamically allocate client addresses, if set to 0 only clients present in the ethers files are served.
force	boolean	no	0	Forces DHCP serving on the specified interface even if another DHCP server is detected on the same network segment.

Table 33. Parameters (continued)

Name	Type	Required	Default	Description
dhcp_option	list of strings	no	none	The ID dhcp_option here must be with written with an underscore. It will be translated to –dhcp-option, with a hyphen, as ultimately used by dnsmasq. Multiple option values can be given for this network-id, with a a space between them and the total string between ””. E.g. '26,1470' or 'option: mtu, 1470' that can assign an MTU per DHCP. Your client must accept MTU by DHCP for this to work. Or “3,192.168.1.1 6,192.168.1.1” to give out gateway and dns server addresses.
ra	string	no	none	Specifies whether Router Advertisements should be enabled (server), relayed (relay) or disabled (disabled).
dhcpv6	string	no	none	Specifies whether DHCPv6 server should be enabled (server), relayed (relay) or disabled (disabled).
ndp	string	no	none	Specifies whether NDP should be relayed relay or disabled none.
ra_management	integer	no	1	RA management mode : no M-Flag but A-Flag (0), both M and A flags (1), M flag but not A flag (2).

Table 33. Parameters (continued)

Name	Type	Required	Default	Description
ra_default	integer	no	0	Default router lifetime in the RA message will be set if default route is present and a global IPv6 address (0) or if default route is present but no global IPv6 address (1) or neither of both conditions (2).
dns	string	no	none	Announced DNS servers.
domain	string	no	none	Announced DNS domains.

Commands example:

Table 34. Configure a DHCPv4 server

Configure a DHCPv4 server listening on the downlink /internal link to x86/ WiFi AP/dedicated management ports

For downlink ports, IP assignment range :1~100
`# sudo uci set dhcp.edge.start='1'`
`# sudo uci set dhcp.edge.limit='100'`
`# sudo uci commit dhcp`
`# sudo /etc/init.d/dnsmasq restart`

For internal link (to X86) , IP assignment range :1~100(preset 5 no x86_lan interface): 1~100
`# sudo uci set dhcp.x86.start='1'`
`# sudo uci set dhcp.x86.limit='100'`
`# sudo uci commit dhcp`
`# sudo /etc/init.d/dnsmasq restart`

For WiFi AP mode (Except for preset 4 due to WiFi is configured to station mode): 1~100
`# sudo uci set dhcp.wifi_lan_ap.start='1'`
`# sudo uci set dhcp.wifi_lan_ap.limit='100'`
`# sudo uci commit dhcp`
`# sudo /etc/init.d/dnsmasq restart`

For dedicated management port, IP assignment range :1~100
`sudo uci set dhcp.lan.start='1'`
`sudo uci set dhcp.lan.limit='100'`
`sudo uci commit dhcp`
`sudo /etc/init.d/dnsmasq restart`

Configure IP related setting (Profile: network)

Table 35. Configure IP related setting (Profile: network)

Syntax

```
sudo uci set network.<interface>=interface
sudo uci set network.<interface>.ifname=<ifname>
sudo uci set network.<interface>.proto=static
sudo uci set network.<interface>.ipaddr=<ipaddr>
sudo uci set network.<interface>.netmask=<netmask>
sudo uci set network.<interface>.gateway=<gateway>
sudo uci set network.<interface>.broadcast=<broadcast>
sudo uci set network.<interface>.dns=<dns>
sudo uci set network.<interface>.ip6assign=<ip6assign>
sudo uci set network.<interface>.ip6hint=<ip6hint>
sudo uci set network.<interface>.ip6ifaceid=<ip6ifaceid>
sudo uci set network.<interface>.auto=<auto>
sudo uci set network.<interface>.force_link=<force_link>
sudo uci set network.<interface>.macaddr=<macaddr>
sudo uci set network.<interface>.mtu=<mtu>
sudo uci set network.<interface>.metric=<metric>
```

Table 36. Parameters

Name	Type	Required	Default	Description
interface	string	yes	none	Logical interface name you want to create.
ifname	string	yes	none	physical interface name on the device
ipaddr	ip address	yes, if no ip6addr is set.	none	IP address. It could be a list of ipaddr , that is: several ipaddresses will be assigned to the interface. If, instead of a list, several ipaddr are specified as options, only the last is applied.
netmask	netmask	yes, if no ip6addr is sets	none	Netmask.
gateway	ip address	no	none	Default gateway.
broadcast	ip address	no	none	Broadcast address (autogenerated if not set).
dns	list of ip addresses	no	none	DNS server(s).

Table 36. Parameters (continued)

Name	Type	Required	Default	Description
ip6assign	prefix length	no	none	Delegate a prefix of given length to this interface (Barrier Breaker and later only).
ip6hint	prefix hint (hex)	no	none	Hint the subprefix-ID that should be delegated as hexadecimal number (Barrier Breaker and later only)
ip6ifaceid	ipv6 suffix	no	::1	Allowed values: 'eui64', 'random', fixed value like '::1:2'. When IPv6 prefix (like 'a:b:c:d::') is received from a delegating server, use the suffix (like '::1') to form the IPv6 address ('a:b:c:d::1') for this interface. Useful with several routers in LAN.
auto	boolean	no	0 for proto none, else 1	Specifies whether to bring up interface on boot.
force_link	boolean	no	1 for protocol static, else 0	Specifies whether ip address, route, and optionally gateway are assigned to the interface regardless of the link being active ('1') or only after the link has become active ('0'); when set to '1', carrier sense events do not invoke hotplug handlers
macaddr	mac address	no	none	Override MAC address of this interface.
mtu	number	no	none	Override the default MTU on this interface.
metric	integer	no	0	Specifies the default route metric to use.

Commands example:

Table 37. Modify base IP of downlink /internal link to x86/ WiFi AP/dedicated management ports

Modify base IP of downlink /internal link to x86/ WiFi AP/dedicated management ports
Configure downlink port to 192.168.71.254 # sudo uci set network.edge_lan.ipaddr='192.168.71.254' # sudo uci commit network # sudo /etc/init.d/network restart
Configure internal link(to X86) to 192.168.73.254(preset 5 has no x86_lan interface): # sudo uci set network.x86_lan.ipaddr='192.168.73.254' # sudo uci commit network # sudo /etc/init.d/network restart
Configure WiFI ports (AP mode,preset 4 is station mode): 192.168.74.254 # sudo uci set network.wifi_lan_ap.ipaddr='192.168.74.254' # sudo uci commit network # sudo /etc/init.d/network restart
Configure dedicated management port to 192.168.70.254 # sudo uci set network.mgmt_xcc_lan.ipaddr='192.168.70.254' # sudo uci commit network # sudo /etc/init.d/network restart

Remove eth3 and eth6 edge_lan:

```
# show interfaces in edge ports

sudo uci show network.edge_lan.ifname



# Remove eth3 and eth6 from edge_lan.ifname

sudo uci set network.edge_lan.ifname='eth1'

sudo uci commit

sudo /etc/init.d/network restart
```

Note: For those ports(ethx) which are not assigned into any network interface, will be set as **disable**

Configure Wireless setting (WLAN)

The wifi-device refer to physical radio devices present on the system. The options present in this section describe properties common across all wireless interfaces on this radio device, such as channel.

Table 38. Wireless devices

Syntax
`sudo uci set wireless.radio0.type=<type>`
`sudo uci set wireless.radio0.channel=<channel>`
`sudo uci set wireless.radio0.hwmode=<hwmode>`
`sudo uci set wireless.radio0.htmode=<htmode>`
`sudo uci set wireless.radio0.disabled=<disabled>`

Table 39. Parameters

Name	Type	Required	Default	Description
type	string	yes	(auto detected)	The type is determined on firstboot during the initial radio device detection - it is usually not required to change it.
hwmode	string	no	11n	Selects the wireless protocol to use, possible values are 11b, 11g, and 11a. Note that 11ng and 11na are not available options
htmode	string	no	HT40	Specifies the channel width in 802.11n and 802.11ac mode, possible values are: HT20, HT40-, HT40+, HT40, or VHT20, VHT40, VHT80, VHT160, NOHT disables 11n
disabled	boolean	no	1	Disables the radio adapter if set to 1. Removing this option or setting it to 0 will enable the adapter
channel	integer (1-11)	yes	11	Specifies the wireless channel to use.

Commands example:

Table 40. Default channel setting

To enable wireless function in 802.11n mode, set default channel to 11
`sudo uci set wireless.radio0.channel='11'`
`sudo uci set wireless.radio0.hwmode='11n'`
`sudo uci set wireless.radio0.disabled='0'`
`sudo uci commit wireless`
`sudo wifi`

Wireless Interface

Table 41. Wireless Interface

Syntax
`sudo uci set wireless.default_radio0.encryption=<encryption>`
`sudo uci set wireless.default_radio0.ssid=<ssid>`
`sudo uci set wireless.default_radio0.mode=<mode>`
`sudo uci set wireless.default_radio0.key=<key>`
`sudo uci set wireless.default_radio0.network=<network>`

Table 42. Parameters

Name	Type	Required	Default	Description
network	string	yes	wifi_lan_ap	Specifies the network interface to attach the wireless to. Possible values are wifi_lan_ap,wifi_wan_sta.
mode	string	yes	ap	Selects the operation mode of the wireless network interface controller. Possible values are ap, sta.
ssid	string	yes	hodaka_ap	The broadcasted SSID of the wireless network and for managed mode the SSID of the network you’re connecting to

Table 42. Parameters (continued)

Name	Type	Required	Default	Description
encryption	string	yes	psk2	Wireless encryption method. 1.AP mode: WPA2 personal only, value : psk2 2.Station mode: WPA2 Enterprise and Personal.
key	integer or string	yes	user defined	In any **WPA-PSK** mode, this is a string that specifies the pre-shared passphrase from which the pre-shared key will be derived. The clear text key has to be 8-63 characters long. If a 64-character hexadecimal string is supplied, it will be used directly as the pre-shared key instead. IIn any **WPA-Enterprise AP** mode, this option has a different interpretation.

WPA Enterprise (client mode)

Listing of Client related options for WPA Enterprise:

Name	Default	Description
eap_type	(none)	Defines the EAP protocol to use, possible values are tls for EAP-TLS and peap or ttls for EAP-PEAP
auth	MSCHAPV2	“auth=PAP”/PAP/MSCHAPV2 - Defines the phase 2 (inner) authentication method to use, only applicable if eap_type is peap or ttls
identity	(none)	EAP identity to send during authentication
password	(none)	Password to send during EAP authentication
ca_cert	(none)	Specifies the path the CA certificate used for authentication
client_cert	(none)	Specifies the client certificate used for the authentication

Name	Default	Description
priv_key	(none)	Specifies the path to the private key file used for authentication, only applicable if eap_typeis set to tls
priv_key_pwd	(none)	Password to unlock the private key file, only works in conjunction with priv_key

Note: When using WPA Enterprise type PEAP with Active Directory Servers, the “auth” option must be set to “auth=MSCHAPV2” or “auth=PAP”.

Commands example:

Table 43. Wireless client mode

To configure wireless to station mode, and connect to AP which SSID is Hoda-WF2G-TEST with WPA2 personal.

```
sudo uci set wireless.default_radio0.encryption='psk2'
sudo uci set wireless.default_radio0.ssid='Hoda-WF2G-TEST'
sudo uci set wireless.default_radio0.mode='sta'
sudo uci set wireless.default_radio0.key='hodaka#1'
sudo uci set wireless.default_radio0.network='wifi_wan_sta'
sudo uci commit wireless
sudo wifi
```

To configure wireless to station mode, and connect to AP which SSID is Hoda-WF2G-TEST with WPA2 enterprise.

```
sudo uci set wireless.default_radio0.network='wifi_wan_sta'
sudo uci set wireless.default_radio0.mode='sta'
sudo uci set wireless.default_radio0.ssid='Hoda-WF2G-TEST'
sudo uci set wireless.default_radio0.encryption='wpa2'
sudo uci set wireless.default_radio0.doth='1'
sudo uci set wireless.default_radio0.eap_type='peap'
sudo uci set wireless.default_radio0.auth='EAP-MSCHAPV2'
sudo uci set wireless.default_radio0.identity='123'
sudo uci set wireless.default_radio0.password='123'
sudo uci commit wireless
sudo wifi
```

Configure LTE setting

Table 44. Configure LTE setting

Syntax

```
sudo uci set network.lte_wan.apn=<apn>
sudo uci set network.lte_wan.pincode=<pincode>
sudo uci set network.lte_wan.username=<username>
sudo uci set network.lte_wan.password=<password>
sudo uci set network.lte_wan.pdptype=<pdptype>
sudo uci set network.lte_wan.auth=<auth>
```

Table 45. Parameters

Name	Type	Required	Default	Description
apn	string	yes	internet	Used APN
pincode	number	no	(none)	PIN code to unlock SIM card
username	string	no	(none)	Username for PAP/ CHAP authentication
password	string	no	(none)	Password for PAP/ CHAP authentication
auth	string	no	chap	Authentication type: **pap**, **chap**, **both**, **none**
pdptype	string	no	IPV4	Used IP-stack mode, IP (for IPv4), IPV6 (for IPv6) or IPV4V6 (for dual-stack)
plmn	number	no	(none)	First three digits are the **mcc** (mobile country code) and the last three digits are the **mnc** (mobile network code), for example if plmn= 338020, then the mcc is 338 and the mnc is 020

Commands example:

```
sudo uci set network.lte_wan.pincode='0000'
sudo uci set network.lte_wan.apn='testapn'
sudo uci set network.lte_wan.username='Name1'
sudo uci set network.lte_wan.password='Password'
sudo uci commit network
sudo /etc/init.d/network restart
```

Configuration import and export

Table 46. Configuration import and export

Back up embedded switch configuration to local PC.
 	
`# Generate backup`
 	
`sudo sysupgrade -b /tmp/backup.tar.gz`
 	
`ls /tmp/backup.tar.gz`
 	
`# Download backup`
 	
`scp oper@192.168.70.254://tmp/backup.tar.gz ./`

Restore previously saved embedded switch configuration from local PC.
 	
`# Upload backup`
 	
`scp backup.tar.gz oper@192.168.70.254://tmp/backup.tar.gz`
 	
`# Restore backup`
 	
`ls /tmp/backup.tar.gz`
 	
`sudo sysupgrade -r /tmp/backup.tar.gz`
 	
`sudo reboot`

Note: If you have modified the configurations in the backup file, after untarring and modifying the backup file, go to the root directory which contains the “home” and “etc” folder and run the following command to re-tar the backup file:`tar cvfz backup.tar.gz`

Upgrade firmware of embedded switch

1. Connect your laptop to BMC management port, and configure ip of laptop to "192.168.70.xxx" .
2. Transfer image from client to switch board by scp:
   - [Linux OS] `$> scp -o StrictHostKeyChecking=no -o UserKnownHostsFile=/dev/null ./se350-hyl403g-r378-bd144013.bin.sign oper@192.168.70.254://tmp/`
   - [Windows OS] `.\pscp.exe -scp .\se350-hyl403g-r378-bd144013.bin.sign oper@192.168.70.254://tmp/`
3. Update FW in CLI of switch board: (all settings will be reset to factory default if "sudo sysupgrade -n") `$> sudo sysupgrade /tmp/se350-hyl403g-r378-bd144013.bin.sign`

Static route for remote configuration on embedded switch

If cloud ports are active, the default gateway obtained from cloud ports will overwrite existing default gateway of embedded switch. User will not be allowed to connect to embedded switch ip remotely (from different ip segment) due to network traffic back to management port will be redirected to cloud ports. Following example demonstrates how to add "static route" to allow remote configuration to embedded switch ip when the cloud ports are active.

```
#.If ip domain of management port is "172.18.x.x", with default gateway "172.18.221.254".
```

```
#.To force traffic targets to 172.18.0.0/16 & 10.0.0.0/8 to go through gateway 172.18.221.254


sudo uci set network.rtmgmt1=route

sudo uci set network.rtmgmt1.interface='mgmt_xcc_lan'

sudo uci set network.rtmgmt1.target='172.18.0.0'

sudo uci set network.rtmgmt1.netmask='255.255.0.0'

sudo uci set network.rtmgmt1.gateway='172.18.221.254'


sudo uci set network.rtmgmt2=route

sudo uci set network.rtmgmt2.interface='mgmt_xcc_lan'

sudo uci set network.rtmgmt2.target='10.0.0.0'

sudo uci set network.rtmgmt2.netmask='255.0.0.0'

sudo uci set network.rtmgmt2.gateway='172.18.221.254'


sudo uci commit

sudo /etc/init.d/network restart
```

Firewall settings

Use this information to set configuration of firewall.

Set default firewall

The default section declares global firewall settings which do not belong to specific zones.

Table 47. Set default firewall

Syntax

```
sudo uci set firewall.@defaults[0].input=<input>
sudo uci set firewall.@defaults[0].output=<output>
sudo uci set firewall.@defaults[0].forward=<forward>
sudo uci set firewall.@defaults[0].syn_flood=<syn_flood>
sudo uci set firewall.@defaults[0].drop_invalid=<drop_invalid>
```

Table 48. Parameters

Name	Type	Required	Default	Description
input	string	no	REJECT	Set policy for the INPUT chain of the filter table.
output	string	no	REJECT	Set policy for the OUTPUT chain of the filter table.
forward	string	no	REJECT	Set policy for the FORWARD chain of the filter table.
syn_flood	boolean	no	0	Enable SYN flood protection (obsoleted by synflood_protect setting).
drop_invalid	boolean	no	0	Drop invalid packets (e.g. not matching any active connection).

Commands example:

Table 49. Commands example

```
sudo uci set firewall.@defaults[0].input=ACCEPT
sudo uci set firewall.@defaults[0].output= ACCEPT
sudo uci set firewall.@defaults[0].forward= ACCEPT
sudo uci set firewall.@defaults[0].syn_flood=1
sudo uci set firewall.@defaults[0].drop_invalid=1
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

Add a new Zone

This section defines common properties of “test”. The input and output options set the default policies for traffic entering and leaving this zone while the forward option describes the policy for forwarded traffic between different networks within the zone. Covered networks specify which available networks are members of this zone.

Table 50. Add a new Zone

Syntax

```
sudo uci add firewall zone
sudo uci set firewall.@zone[-1].name=<name>
sudo uci set firewall.@zone[-1].input=<input>
sudo uci set firewall.@zone[-1].output=<output>
sudo uci set firewall.@zone[-1].forward=<forward>
sudo uci set firewall.@zone[-1].masq=<masq>
sudo uci set firewall.@zone[-1].mtu_fix=<mtu_fix>
sudo uci set firewall.@zone[-1].network=<network>
sudo uci set firewall.@zone[-1].family=<family>
sudo uci set firewall.@zone[-1].masq_src=<masq_src>
sudo uci set firewall.@zone[-1].masq_dest=<masq_dest>
sudo uci set firewall.@zone[-1].conntrack=<conntrack>
sudo uci set firewall.@zone[-1].log=<log>
sudo uci set firewall.@zone[-1].log_limit=<log_limit>
udo uci commit firewall
```

Table 51. Parameters

Parameter	Type	Required	Default	Description
name	zone name	yes	none	Unique zone name. 11 characters is the maximum working firewall zone name length.
input	string	no	REJECT	Set policy for the INPUT chain of the filter table.
output	string	no	REJECT	Set policy for the OUTPUT chain of the filter table.
forward	string	no	REJECT	Set policy for the FORWARD chain of the filter table.
masq	boolean	no	0	Specifies whether outgoing zone traffic should be masqueraded - this is typically enabled on the wan zone.
mtu_fix	boolean	no	0	Enable MSS clamping for outgoing zone traffic.

Table 51. Parameters (continued)

Parameter	Type	Required	Default	Description
network	list	no	none	List of interfaces attached to this zone. If omitted and neither extra* options, subnets or devices are given, the value of name is used by default. Alias interfaces defined in the network config cannot be used as valid 'standalone' networks. Use list syntax as explained in uci.
family	string	no	0	Protocol family (ipv4, ipv6 or any) to generate iptables rules for.
masq_src	list of subnets	no	0.0.0.0/0	Limit masquerading to the given source subnets. Negation is possible by prefixing the subnet with !; multiple subnets are allowed.
masq_dest	list of subnets	no	0.0.0.0/0	Limit masquerading to the given destination subnets. Negation is possible by prefixing the subnet with !; multiple subnets are allowed.
conntrack	boolean	no	1 if masquerading is used, 0 otherwise	Force connection tracking for this zone (see Note on connection tracking).
log	boolean	no	0	Create log rules for rejected and dropped traffic in this zone.
log_limit	string	no	10/minute	Limits the amount of log messages per interval.

Commands example:

Table 52. Commands example

```
sudo uci add firewall zone
sudo uci set firewall.@zone[-1].name=test
sudo uci set firewall.@zone[-1].input=ACCEPT
sudo uci set firewall.@zone[-1].output= ACCEPT
sudo uci set firewall.@zone[-1].forward= ACCEPT
sudo uci set firewall.@zone[-1].masq=<masq>
sudo uci set firewall.@zone[-1].mtu_fix=<mtu_fix>
sudo uci set firewall.@zone[-1].network=<network>
sudo uci set firewall.@zone[-1].family=<family>
sudo uci set firewall.@zone[-1].masq_src=<masq_src>
sudo uci set firewall.@zone[-1].masq_dest=<masq_dest>
sudo uci set firewall.@zone[-1].conntrack=<conntrack>
sudo uci set firewall.@zone[-1].log=<log>
sudo uci set firewall.@zone[-1].log_limit=<log_limit>
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

Add a new forwarding

The forwarding sections control the traffic flow between zones and may enable MSS clamping for specific directions. Only one direction is covered by a forwarding rule. To allow bidirectional traffic flows between two zones, two forwardings are required, with src and dest reversed in each.

Table 53. Add a new forwarding

Syntax

```
sudo uci set firewall.@zone[-1].src=<src>
sudo uci set firewall.@zone[-1].dest=<dest>
sudo uci commit firewall
```

Table 54. Parameters

Parameter	Type	Required	Default	Description
src	zone name	yes	none	Specifies the traffic source zone. Must refer to one of the defined zone names.
dest	zone name	yes	none	Specifies the traffic destination zone. Must refer to one of the defined zone names.

Commands example:

Table 55. Commands example

```
sudo uci set firewall.@zone[-1].src=test
sudo uci set firewall.@zone[-1].dest=lan
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

Add a new port forwards

Port forwardings (DNAT) are defined by redirect sections. All incoming traffic on the specified source zone which matches the given rules will be directed to the specified internal host. Redirects are also commonly known as "port forwarding", and "virtual servers". Port ranges are specified as start:stop, for instance 6666:6670. This is similar to the iptables syntax.

Table 56. Add a new port forwards

Syntax

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].enabled=<enabled>
sudo uci set firewall.@redirect[-1].name=<name>
sudo uci set firewall.@redirect[-1].proto=<proto>
sudo uci set firewall.@redirect[-1].src=<src>
sudo uci set firewall.@redirect[-1].src_mac=<src_mac>
sudo uci set firewall.@redirect[-1].src_ip=<src_ip>
sudo uci set firewall.@redirect[-1].src_port=<src_port>
sudo uci set firewall.@redirect[-1].src_dip=<src_dip>
sudo uci set firewall.@redirect[-1].src_dport=<src_dport>
sudo uci set firewall.@redirect[-1].dest=<dest>
sudo uci set firewall.@redirect[-1].dest_ip=<dest_ip>
sudo uci set firewall.@redirect[-1].dest_port=<dest_port>
sudo uci set firewall.@redirect[-1].reflection=<reflection>
sudo uci commit firewall
```

Table 57. Parameters

Parameter	Type	Required	Default	Description
enabled	string	no	1 or yes	Enable the redirect rule or not.
name	string	no	none	Unique redirect name.
proto	protocol name or number	yes	tcp udp	Match incoming traffic using the given protocol.
src	zone name	no	yes for DNAT target	Specifies the traffic source zone. Must refer to one of the defined zone names. For typical port forwards this usually is wan.

Table 57. Parameters (continued)

Parameter	Type	Required	Default	Description
src_mac	mac address	no	none	Match incoming traffic from the specified mac address.
src_ip	ip address	no	none	Match incoming traffic from the specified source ip address.
src_port	port or range	no	none	Match incoming traffic originating from the given source port or port range (ex: '5000-5100') on the client host.
src_dip	ip address	yes for SNAT target	none	For DNAT, match incoming traffic directed at the given destination ip address. For SNAT rewrite the source address to the given address.
src_dport	port or range	no	none	For DNAT, match incoming traffic directed at the given destination port or port range (ex: '5000-5100') on this host. For SNAT rewrite the source ports to the given value.
dest	zone name	yes for SNAT target	none	Specifies the traffic destination zone. Must refer to one of the defined zone names. For DNAT target on Attitude Adjustment, NAT reflection works only if this is equal to lan.

Table 57. Parameters (continued)

Parameter	Type	Required	Default	Description
dest_ip	ip address	yes for DNAT target	none	For DNAT, redirect matched incoming traffic to the specified internal host. For SNAT, match traffic directed at the given address. For DNAT if the dest_ip value matches the local ip addresses of the router, as shown in the ifconfig, then the rule is translated in a DNAT + input 'accept' rule. Otherwise it is a DNAT + forward rule.
dest_port	port or range	no	none	For DNAT, redirect matched incoming traffic to the given port on the internal host. For SNAT, match traffic directed at the given ports. Only a single port or range can be specified (ex: '5000-5100'), not disparate ports as with Rules (below).
reflection	boolean	no	1	Activate NAT reflection for this redirect - applicable to DNAT targets.

Commands example:

Table 58. Forwards http (not HTTPS) traffic to the webserver running on 192.168.1.10:

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].enabled=1
sudo uci set firewall.@redirect[-1].proto=tcp
sudo uci set firewall.@redirect[-1].src=wan
sudo uci set firewall.@redirect[-1].src_dport=80
sudo uci set firewall.@redirect[-1].dest=lan
sudo uci set firewall.@redirect[-1].dest_ip=192.168.1.10
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

Add a new traffic rule

Port forwardings (DNAT) are defined by redirect sections. All incoming traffic on the specified source zone which matches the given rules will be directed to the specified internal host. Redirects are also commonly known as “port forwarding”, and “virtual servers”. Port ranges are specified as start:stop, for instance 6666:6670. This is similar to the iptables syntax.

Table 59. Add a new traffic rule

Syntax

```
sudo uci add firewall rule
sudo uci set firewall.@rule[-1].enabled=<enabled>
sudo uci set firewall.@rule[-1].name=<name>
sudo uci set firewall.@rule[-1].family=<family>
sudo uci set firewall.@rule[-1].proto=<proto>
sudo uci set firewall.@rule[-1].src=<src>
sudo uci set firewall.@rule[-1].src_mac=<src_mac>
sudo uci set firewall.@rule[-1].src_ip=<src_ip>
sudo uci set firewall.@rule[-1].src_port=<src_port>
sudo uci set firewall.@rule[-1].dest=<dest>
sudo uci set firewall.@rule[-1].dest_ip=<dest_ip>
sudo uci set firewall.@rule[-1].dest_port=<dest_port>
sudo uci set firewall.@rule[-1].target=<target>
sudo uci set firewall.@rule[-1].weekdays=<weekdays>
sudo uci set firewall.@rule[-1].monthdays=<monthdays>
sudo uci set firewall.@rule[-1].start_time=<start_time>
sudo uci set firewall.@rule[-1].stop_time=<stop_time>
sudo uci set firewall.@rule[-1].start_date=<start_date>
sudo uci set firewall.@rule[-1].stop_date=<stop_date>
sudo uci set firewall.@rule[-1].utc_time=<utc_time>
uci commit firewall
```

Table 60. Parameters

Parameter	Type	Required	Default	Description
enabled	boolean	no	yes	Enable or disable rule.
name	string	no	none	Unique rule name.
family	string	no	any	Protocol family (ipv4, ipv6 or any) to generate iptables rules for.
proto	protocol name or number	no	tcp udp	Match incoming traffic using the given protocol. Can be one of tcp, udp, tcpudp, udplite, icmp, esp, ah, sctp, or all or it can be a numeric value, representing one of these protocols or a different one. A protocol name from /etc/protocols is also allowed. The number 0 is equivalent to all.

Table 60. Parameters (continued)

Parameter	Type	Required	Default	Description
src	zone name	yes (optional since Firewall v2, version 58 and above)	none	Specifies the traffic source zone. Must refer to one of the defined zone names.
src_mac	mac address	no	none	Match incoming traffic from the specified mac address.
src_ip	ip address	no	none	Match incoming traffic from the specified source ip address.
src_port	port or range	no	none	Match incoming traffic from the specified source port or port range (ex: '5000:5100', port range does not apply to all protocols), if relevant proto is specified. Multiple ports can be specified like '80 443 465' 1.
dest	zone name	no	none	Specifies the traffic destination zone. Must refer to one of the defined zone names, or * for any zone. If specified, the rule applies to forwarded traffic; otherwise, it is treated as input rule.
dest_ip	ip address	no	none	Match incoming traffic directed to the specified destination ip address. With no dest zone, this is treated as an input rule!
dest_port	port or range	no	none	Match incoming traffic directed at the given destination port or port range (ex: '5000:5100', port range does not apply to all protocols), if relevant proto is specified. Multiple ports can be specified like '80 443 465' 1.
target	string	yes	DROP	Activate NAT reflection for this redirect - applicable to DNAT targets.
weekdays	list of weekdays	no	(always)	If specified, only match traffic during the given week days, e.g. sun mon thu fri to only match on sundays, mondays, thursdays and fridays. The list can be inverted by prefixing it with an exclamation mark, e.g. ! sat sun to always match but on saturdays and sundays.
monthdays	list of dates	no	(always)	If specified, only match traffic during the given days of the month, e.g. 2 5 30 to only match on every 2nd, 5th and 30rd day of the month. The list can be inverted by prefixing it with an exclamation mark, e.g. ! 31 to always match but on the 31st of the month.
start_time	time (hh:mm:ss)	no	(always)	If specified, only match traffic after the given time of day (inclusive).
stop_time	time (hh:mm:ss)	no	(always)	If specified, only match traffic before the given time of day (inclusive).
start_date	date (yyyy-mm-dd)	no	(always)	If specified, only match traffic after the given date (inclusive).

Table 60. Parameters (continued)

Parameter	Type	Required	Default	Description
stop_date	date (yyyy-mm-dd)	no	(always)	If specified, only match traffic before the given date (inclusive).
utc_time	boolean	no	0	Treat all given time values as UTC time instead of local time.

Commands example:

Table 61. Blocks all connection attempts to connect the specified host address.

```
sudo uci add firewall rule
sudo uci set firewall.@rule[-1].enabled=1
sudo uci set firewall.@rule[-1].src=lan
sudo uci set firewall.@rule[-1].dest=wan
sudo uci set firewall.@rule[-1].dest_ip=123.45.67.89
sudo uci set firewall.@rule[-1].target=REJECT
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

Add a new Source NAT

Source NAT changes an outgoing packet so that it looks as though the Embedded Switch system is the source of the packet.

Commands example:

Table 62. Define source NAT for UDP and TCP traffic

Define source NAT for UDP and TCP traffic directed to port 123 originating from the host with the IP address 10.55.34.85.

The source address is rewritten to 63.240.161.99:

```
sudo uci add firewall redirect
sudo uci set firewall.@redirect[-1].enabled=1
sudo uci set firewall.@redirect[-1].src=lan
sudo uci set firewall.@redirect[-1].src_ip=10.55.34.85
sudo uci set firewall.@redirect[-1].src_dip=63.240.161.99
sudo uci set firewall.@redirect[-1].dest=wan
sudo uci set firewall.@redirect[-1].dest_port=123
sudo uci set firewall.@redirect[-1].target=SNAT
sudo uci commit firewall
sudo /etc/init.d/firewall restart
```

OpenVPN client settings

Use this information to apply Open VPN client settings.

Before applying OpenVPN client settings, make sure the SE350 meets the following prerequisites:

- Cloud port (Internet connection) has been setup.
- The system time of the SE350 is correct (Check the upper-right corner in the XCC Web UI).
- SE350 only supports OpenVPN (SSL VPN) client.
- Request configuration files from the VPN service provider before VPN setup.

To import OpenVPN configuration files (for example, my-vpn.conf and pass.txt) that are provided by the VPN service provider:

Step 1. Transfer the configuration files (my-vpn.conf and pass.txt) to /home/oper/openvpn/ using SCP.

```
oper@OpenWrt:~$ scp jackshih@192.168.70.200:/home/jackshih/my-vpn.conf /home/oper/openvpn/my-vpn.conf
oper@OpenWrt:~$ scp jackshih@192.168.70.200:/home/jackshih/pass.txt /home/oper/openvpn/pass.txt
```

Note: You can also change the 'config' option of the OpenVPN to specify your configuration file name.

```
oper@OpenWrt:~$ sudo uci set openvpn.custom_config.config='/home/oper/openvpn/my-vpn.conf'
oper@OpenWrt:~$ sudo uci commit openvpn
```

Step 2. Enable the VPN client.

```
oper@OpenWrt:~$ sudo uci set openvpn.custom_config.enabled='1'
oper@OpenWrt:~$ sudo uci commit openvpn
```

Step 3. Configure the network.

Note: The network interface name for the VPN client is based on the tunnel device in your VPN configuration file. For example, you should set to "tun0" if "dev tun0" is in my-vpn.conf.

```
oper@OpenWrt:~$ sudo uci set network.vpn.ifname='tunnel_name'
oper@OpenWrt:~$ sudo uci commit network
oper@OpenWrt:~$ sudo /etc/init.d/network restart
```

Step 4. Restart the service.`oper@OpenWrt:~$ sudo /etc/init.d/openvpn restart`

Step 5. Check the interface name (for example, "tun0") a few seconds later to see if the IP address is obtained.

Deploy the operating system

Several options are available to deploy an operating system on the server.

Available operating systems

- Microsoft Windows Server
- VMware ESXi

  Note: Boot drives for **VMware ESXI**: For VMware ESXi boot support, only certain M.2 drives are supported, based on their endurance. For more specific information, see Lenovo support tip HT512201.
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server

Complete list of available operating systems: https://lenovopress.lenovo.com/osig.

Tool-based deployment

- **Multi-server**

Available tools:

- Lenovo XClarity Administrator

  http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/compute_node_image_deployment.html
- Lenovo XClarity Essentials OneCLI

  https://pubs.lenovo.com/lxce-onecli/onecli_r_uxspi_proxy_tool
- Lenovo XClarity Integrator deployment pack for SCCM (for Windows operating system only)

  https://pubs.lenovo.com/lxci-deploypack-sccm/dpsccm_c_endtoend_deploy_scenario

- **Single-server**

  Available tools:

  - Lenovo XClarity Provisioning Manager

    “OS Installation” section in the LXPM documentation compatible with your server at https://pubs.lenovo.com/lxpm-overview/
  - Lenovo XClarity Essentials OneCLI

    https://pubs.lenovo.com/lxce-onecli/onecli_r_uxspi_proxy_tool
  - Lenovo XClarity Integrator deployment pack for SCCM (for Windows operating system only)

    https://pubs.lenovo.com/lxci-deploypack-sccm/dpsccm_c_endtoend_deploy_scenario

Manual deployment

If you cannot access the above tools, follow the instructions below, download the corresponding *OS Installation Guide*, and deploy the operating system manually by referring to the guide.

1. Go to https://datacentersupport.lenovo.com/solutions/server-os.
2. Select an operating system from the navigation pane and click **Resources**.
3. Locate the “OS Install Guides” area and click the installation instructions. Then, follow the instructions to complete the operation system deployment task.

Back up the server configuration

After setting up the server or making changes to the configuration, it is a good practice to make a complete backup of the server configuration.

Make sure that you create backups for the following server components:

- **Management processor**

  You can back up the management processor configuration through the Lenovo XClarity Controller interface. For details about backing up the management processor configuration, see:

  “Backing up the BMC configuration” section in the XCC documentation compatible with your server at https://pubs.lenovo.com/lxcc-overview/.

  Alternatively, you can use the `save` command from Lenovo XClarity Essentials OneCLI to create a backup of all configuration settings. For more information about the `save` command, see:

  https://pubs.lenovo.com/lxce-onecli/onecli_r_save_command
- **Operating system**

  Use your backup methods to back up the operating system and user data for the server.

Update the Vital Product Data (VPD)

After initial setup of the system, you can update some Vital Product Data (VPD), such as asset tag and Universal Unique Identifier (UUID).

Update the Universal Unique Identifier (UUID)

Optionally, you can update the Universal Unique Identifier (UUID).

There are two methods available to update the UUID:

- From Lenovo XClarity Provisioning Manager

  To update the UUID from Lenovo XClarity Provisioning Manager:

  1. Start the server and press the key according to the on-screen instructions. (For more information, see the “Startup” section in the LXPM documentation compatible with your server at https://pubs.lenovo.com/lxpm-overview/.) The Lenovo XClarity Provisioning Manager interface is displayed by default.
  2. If the power-on Administrator password is required, enter the password.
  3. From the System Summary page, click **Update VPD**.
  4. Update the UUID.

- From Lenovo XClarity Essentials OneCLI

  Lenovo XClarity Essentials OneCLI sets the UUID in the Lenovo XClarity Controller. Select one of the following methods to access the Lenovo XClarity Controller and set the UUID:

  – Operate from the target system, such as LAN or keyboard console style (KCS) access
  – Remote access to the target system (TCP/IP based)

  To update the UUID from Lenovo XClarity Essentials OneCLI:

  1. Download and install Lenovo XClarity Essentials OneCLI.

     To download Lenovo XClarity Essentials OneCLI, go to the following site:

     https://datacentersupport.lenovo.com/solutions/HT116433
  2. Copy and unpack the OneCLI package, which also includes other required files, to the server. Make sure that you unpack the OneCLI and the required files to the same directory.
  3. After you have Lenovo XClarity Essentials OneCLI in place, type the following command to set the UUID:

     ```
     onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID [access_method]
     ```

     Where:

     [access_method]
     The access method that you select to use from the following methods:

     – Online authenticated LAN access, type the command:

       ```
       [--bmc-username <xcc_user_id> --bmc-password <xcc_password>]
       ```

       Where:

       xcc_user_id
       The BMC/IMM/XCC account name (1 of 12 accounts). The default value is USERID.

       xcc_password

The BMC/IMM/XCC account password (1 of 12 accounts).

Example command is as follows:

```
onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID --bmc-username <xcc_user_id>
--bmc-password <xcc_password>
```

– Online KCS access (unauthenticated and user restricted):

You do not need to specify a value for *access_method* when you use this access method.

Example command is as follows:

```
onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID
```

Note: The KCS access method uses the IPMI/KCS interface, which requires that the IPMI driver be installed.

– Remote LAN access, type the command:

```
[--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>]
```

Where:

xcc_external_ip
The BMC/IMM/XCC external IP address. There is no default value. This parameter is required.

xcc_user_id
The BMC/IMM/XCC account name (1 of 12 accounts). The default value is USERID.

xcc_password
The BMC/IMM/XCC account password (1 of 12 accounts).

Note: BMC, IMM, or XCC external IP address, account name, and password are all valid for this command.

Example command is as follows:

```
onecli config createuuid SYSTEM_PROD_DATA.SysInfoUUID
--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>
```

4. Restart the Lenovo XClarity Controller.
5. Restart the server.

Update the asset tag

Optionally, you can update the asset tag.

There are two methods available to update the asset tag:

- From Lenovo XClarity Provisioning Manager

  To update the asset tag from Lenovo XClarity Provisioning Manager:

  1. Start the server and press the key specified in the on-screen instructions to display the Lenovo XClarity Provisioning Manager interface.
  2. If the power-on Administrator password is required, enter the password.
  3. From the System Summary page, click **Update VPD**.
  4. Update the asset tag information.
- From Lenovo XClarity Essentials OneCLI

Lenovo XClarity Essentials OneCLI sets the asset tag in the Lenovo XClarity Controller. Select one of the following methods to access the Lenovo XClarity Controller and set the asset tag:

- Operate from the target system, such as LAN or keyboard console style (KCS) access
- Remote access to the target system (TCP/IP based)

To update the asset tag from Lenovo XClarity Essentials OneCLI:

1. Download and install Lenovo XClarity Essentials OneCLI.

   To download Lenovo XClarity Essentials OneCLI, go to the following site:

   https://datacentersupport.lenovo.com/solutions/HT116433

2. Copy and unpack the OneCLI package, which also includes other required files, to the server. Make sure that you unpack the OneCLI and the required files to the same directory.
3. After you have Lenovo XClarity Essentials OneCLI in place, type the following command to set the DMI:

   ```
   onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> [access_method]
   ```

   Where:

   <asset_tag>
   The server asset tag number. Type `aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa`, where *aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa* is the asset tag number.

   [access_method]
   The access method that you select to use from the following methods:

   - Online authenticated LAN access, type the command:

     ```
     [--bmc-username <xcc_user_id> --bmc-password <xcc_password>]
     ```

     Where:

     xcc_user_id
     The BMC/IMM/XCC account name (1 of 12 accounts). The default value is USERID.

     xcc_password
     The BMC/IMM/XCC account password (1 of 12 accounts).

     Example command is as follows:

     ```
     onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag> --bmc-username <xcc_user_id>
     --bmc-password <xcc_password>
     ```

   - Online KCS access (unauthenticated and user restricted):

     You do not need to specify a value for *access_method* when you use this access method.

     Example command is as follows:

     ```
     onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>
     ```

     Note: The KCS access method uses the IPMI/KCS interface, which requires that the IPMI driver be installed.

   - Remote LAN access, type the command:

     ```
     [--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>]
     ```

     Where:

xcc_external_ip
The BMC/IMM/XCC IP address. There is no default value. This parameter is required.

xcc_user_id
The BMC/IMM/XCC account (1 of 12 accounts). The default value is USERID.

xcc_password
The BMC/IMM/XCC account password (1 of 12 accounts).

Note: BMC, IMM, or XCC internal LAN/USB IP address, account name, and password are all valid for this command.

Example command is as follows:

```
onecli config set SYSTEM_PROD_DATA.SysEncloseAssetTag <asset_tag>

--bmc <xcc_user_id>:<xcc_password>@<xcc_external_ip>
```

4. Reset the Lenovo XClarity Controller to the factory defaults. See “Resetting the BMC to Factory Default” section in the XCC documentation compatible with your server at https://pubs.lenovo.com/lxcc-overview/.

Chapter 5. Resolving installation issues

Use this information to resolve issues that you might have when setting up your system.

Use the information in this section to diagnose and resolve problems that you might encounter during the initial installation and setup of your server.

Server does not power on

Complete the following steps until the problem is resolved:

1. Check the event log for any events related to the server not powering on.
2. Check for any LEDs that are flashing amber.
3. Check the power LED on the system board.
4. Reseat the power adapter.
5. Replace the power adapter and check the power button function after installing each one.
6. If the issue cannot be resolved by above actions, please call service to review the issue symptom and see whether the system board replacement is necessary.

The server immediately displays the POST Event Viewer when it is turned on

Complete the following steps until the problem is solved.

1. Correct any errors that are indicated by the front operator panel and error LEDs.
2. Make sure that the server supports the processor and that the processor matches in speed and cache size.

   You can view processor details from system setup.

   To determine if the processor is supported for the server, see https://serverproven.lenovo.com/server/se350.
3. (Trained technician only) Make sure that system board is seated correctly
4. (Trained technician only) Make sure that processor is seated correctly
5. Replace the following components one at a time, in the order shown, restarting the server each time:
   a. (Trained technician only) Processor
   b. (Trained technician only) System board

Embedded hypervisor is not in the boot list

Complete the following steps until the problem is solved.

1. If the server has been installed, moved, or serviced recently, or if this is the first time the embedded hypervisor is being used, make sure that the device is connected properly and that there is no physical damage to the connectors.

2. See the documentation that comes with the optional embedded hypervisor flash device for setup and configuration information.
3. Check https://serverproven.lenovo.com/server/se350 to validate that the embedded hypervisor device is supported for the server.
4. Make sure that the embedded hypervisor device is listed in the list of available boot options. From the management controller user interface, click **Server Configuration → Boot Options**.

   For information about accessing the management controller user interface, see "Opening and Using the XClarity Controller Web Interface" section in the XCC documentation compatible with your server at:

   https://pubs.lenovo.com/lxcc-overview/
5. Check http://datacentersupport.lenovo.com for any tech tips (service bulletins) related to the embedded hypervisor and the server.
6. Make sure that other software works on the server to ensure that it is working properly.

Displayed system memory less than installed physical memory

Complete the following procedure to solve the problem.

Note: Each time you install or remove a memory module, you must disconnect the server from the power source; then, wait 10 seconds before restarting the server.

1. Make sure that:
   - No error LEDs are lit on the operator information panel.
   - No memory module error LEDs are lit on the system board.
   - Memory mirrored channel does not account for the discrepancy.
   - The memory modules are seated correctly.
   - You have installed the correct type of memory module (see "Specifications" on page 3 for requirements).
   - After changing or replacing a memory module, memory configuration is updated accordingly in the Setup Utility.
   - All banks of memory are enabled. The server might have automatically disabled a memory bank when it detected a problem, or a memory bank might have been manually disabled.
   - There is no memory mismatch when the server is at the minimum memory configuration.
2. Reseat the memory modules, and then restart the server.
3. Check the POST error log:
   - If a memory module was disabled by a systems-management interrupt (SMI), replace the memory module.
   - If a memory module was disabled by the user or by POST, reseat the memory module; then, run the Setup Utility and enable the memory module.
4. Run memory diagnostics. When you start a solution and press the key according to the on-screen instructions, the LXPM interface is displayed by default. (For more information, see the "Startup" section in the LXPM documentation compatible with your server at https://pubs.lenovo.com/lxpm-overview/.) You can perform memory diagnostics with this interface. From the Diagnostic page, go to **Run Diagnostic → Memory test** .
5. Re-enable all memory modules using the Setup Utility, and then restart the server.
6. (Trained technician only) Replace the system board.

A Lenovo optional device that was just installed does not work.

1. Make sure that:

- The device is supported for the server (see https://serverproven.lenovo.com/server/se350).
- You followed the installation instructions that came with the device and the device is installed correctly.
- You have not loosened any other installed devices or cables.
- You updated the configuration information in system setup. When you start a server and press the key according to the on-screen instructions to display the Setup Utility. (For more information, see the "Startup" section in the LXPM documentation compatible with your server at https://pubs.lenovo.com/lxpm-overview/.) Whenever memory or any other device is changed, you must update the configuration.

2. Reseat the device that you just installed.
3. Replace the device that you just installed.
4. Reseat the cable connection and check there is no physical damage to the cable.
5. If there is any cable damages, then replace the cable.

Voltage planar fault is displayed in the event log

Complete the following steps until the problem is solved.

1. Revert the system to the minimum configuration. See "Specifications" on page 3 for the minimally required number of processors and DIMMs.
2. Restart the system.
   - If the system restarts, add each of the items that you removed one at a time, restarting the system each time, until the error occurs. Replace the item for which the error occurs.
   - If the system does not restart, suspect the system board.

Appendix A. Getting help and technical assistance

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

On the World Wide Web, up-to-date information about Lenovo systems, optional devices, services, and support are available at:

http://datacentersupport.lenovo.com

Note: IBM is Lenovo's preferred service provider for ThinkSystem.

Before you call

Before you call, there are several steps that you can take to try and solve the problem yourself. If you decide that you do need to call for assistance, gather the information that will be needed by the service technician to more quickly resolve your problem.

Attempt to resolve the problem yourself

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

You can find the product documentation for your ThinkSystem products at the following location:

http://thinksystem.lenovofiles.com/help/index.jsp

You can take these steps to try to solve the problem yourself:

- Check all cables to make sure that they are connected.
- Check the power switches to make sure that the system and any optional devices are turned on.
- Check for updated software, firmware, and operating-system device drivers for your Lenovo product. The Lenovo Warranty terms and conditions state that you, the owner of the Lenovo product, are responsible for maintaining and updating all software and firmware for the product (unless it is covered by an additional maintenance contract). Your service technician will request that you upgrade your software and firmware if the problem has a documented solution within a software upgrade.
- If you have installed new hardware or software in your environment, check https://serverproven.lenovo.com/server/se350 to make sure that the hardware and software is supported by your product.
- Go to http://datacentersupport.lenovo.com and check for information to help you solve the problem.
  - Check the Lenovo forums at https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg to see if someone else has encountered a similar problem.

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

messages and error codes. If you suspect a software problem, see the documentation for the operating system or program.

Gathering information needed to call Support

If you believe that you require warranty service for your Lenovo product, the service technicians will be able to assist you more efficiently if you prepare before you call. You can also see http://datacentersupport.lenovo.com/warrantylookup for more information about your product warranty.

Gather the following information to provide to the service technician. This data will help the service technician quickly provide a solution to your problem and ensure that you receive the level of service for which you might have contracted.

- Hardware and Software Maintenance agreement contract numbers, if applicable
- Machine type number (Lenovo 4-digit machine identifier)
- Model number
- Serial number
- Current system UEFI and firmware levels
- Other pertinent information such as error messages and logs

As an alternative to calling Lenovo Support, you can go to https://support.lenovo.com/servicerequest to submit an Electronic Service Request. Submitting an Electronic Service Request will start the process of determining a solution to your problem by making the pertinent information available to the service technicians. The Lenovo service technicians can start working on your solution as soon as you have completed and submitted an Electronic Service Request.

Collecting service data

To clearly identify the root cause of a server issue or at the request of Lenovo Support, you might need collect service data that can be used for further analysis. Service data includes information such as event logs and hardware inventory.

Service data can be collected through the following tools:

- **Lenovo XClarity Provisioning Manager**

  Use the Collect Service Data function of Lenovo XClarity Provisioning Manager to collect system service data. You can collect existing system log data or run a new diagnostic to collect new data.

- **Lenovo XClarity Controller**

  You can use the Lenovo XClarity Controller web interface or the CLI to collect service data for the server. The file can be saved and sent to Lenovo Support.

  - For more information about using the web interface to collect service data, see the “Downloading service data” section in the XCC documentation version compatible with your server at https://pubs.lenovo.com/lxcc-overview/.
  - For more information about using the CLI to collect service data, see the “ffdc command” section in the XCC documentation version compatible with your server at https://pubs.lenovo.com/lxcc-overview/.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator can be set up to collect and send diagnostic files automatically to Lenovo Support when certain serviceable events occur in Lenovo XClarity Administrator and the managed endpoints. You can choose to send diagnostic files to Lenovo Support using Call Home or to another service provider using SFTP. You can also manually collect diagnostic files, open a problem record, and send diagnostic files to the Lenovo Support Center.

You can find more information about setting up automatic problem notification within the Lenovo XClarity Administrator at http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html.

- **Lenovo XClarity Essentials OneCLI**

  Lenovo XClarity Essentials OneCLI has inventory application to collect service data. It can run both in-band and out-of-band. When running in-band within the host operating system on the server, OneCLI can collect information about the operating system, such as the operating system event log, in addition to the hardware service data.

  To obtain service data, you can run the `getinfor` command. For more information about running the `getinfor`, see https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.

Contacting Support

You can contact Support to obtain help for your issue.

You can receive hardware service through a Lenovo Authorized Service Provider. To locate a service provider authorized by Lenovo to provide warranty service, go to https://datacentersupport.lenovo.com/serviceprovider and use filter searching for different countries. For Lenovo support telephone numbers, see https://datacentersupport.lenovo.com/supportphonelist for your region support details.

Index