

Dell PowerEdge XR8610t

Installation and Service Manual

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Chapter 1: About this document	6
Chapter 2: Dell PowerEdge XR8610t system configurations and features	7
System configurations - front view for PowerEdge XR8610t.....	7
System configurations - rear view for PowerEdge XR8610t.....	9
System configurations - inside view for PowerEdge XR8610t.....	10
Locating the Express Service Code and Service Tag.....	10
System information label.....	11
Chapter 3: Technical specifications	15
Sled dimensions	15
System weight.....	16
Processor specifications.....	16
Cooling fan specifications.....	16
Supported operating systems.....	16
System battery specifications.....	16
Memory specifications.....	16
Expansion card riser specifications.....	17
Drives.....	17
Ports and connectors specifications.....	17
USB ports specifications.....	17
Network port specifications.....	17
Serial connector specifications.....	18
Display port.....	18
iDRAC port specifications.....	18
RJ-45 dry contact port.....	18
Video specifications.....	19
Environmental specifications.....	20
Environmental considerations.....	21
Thermal restriction matrix.....	22
Chapter 4: Initial system setup and configuration	25
Setting up the system.....	25
iDRAC configuration.....	25
Options to set up iDRAC IP address.....	25
Options to log in to iDRAC.....	26
Resources to install operating system.....	27
Options to download drivers and firmware	27
Options to download and install OS drivers	27
Downloading drivers and firmware.....	28
Chapter 5: Pre-operating system management applications	29
System Setup.....	29
System BIOS.....	30

iDRAC Settings.....	48
Device Settings.....	48
Chapter 6: Minimum configuration to POST	49
Chapter 7: Installing and removing system components	50
Safety instructions.....	50
Before working inside your system	50
After working inside your system.....	50
XR8000r chassis.....	51
Removing a sled blank.....	51
Installing a sled blank.....	51
Removing a sled.....	52
Installing a sled	53
Sled cover.....	54
Removing the sled cover.....	54
Installing the sled cover.....	55
Cooling fans.....	56
Removing a cooling fan.....	56
Installing a cooling fan.....	57
Expansion cards and expansion card risers.....	58
Expansion card installation guidelines.....	59
Removing the expansion card riser 2.....	60
Installing the expansion card riser 2.....	61
Removing the PCIe card from riser.....	62
Installing the PCIe card on riser.....	64
BOSS-N1 card.....	66
Installing the BOSS-N1 card.....	66
Installing the BOSS-N1 card.....	67
Removing the M.2 SSD module from the BOSS-N1 card.....	68
Installing the M.2 SSD module on the BOSS-N1 card.....	69
Power distribution board.....	70
Removing the 1U power distribution board.....	70
Installing the power distribution board.....	71
System memory.....	72
System memory guidelines.....	72
General memory module installation guidelines.....	74
Removing a memory module.....	74
Installing a memory module.....	75
Processor and heat sink module.....	76
Removing the processor and heat sink module.....	76
Removing the processor.....	78
Installing the processor.....	79
Installing the processor and heat sink module.....	83
System battery	85
Replacing the system battery.....	85
System board.....	87
Removing the system board.....	87
Installing the system board	88

Trusted Platform Module.....	90
Upgrading the Trusted Platform Module.....	90
Initializing TPM for users.....	91
Initializing the TPM 2.0 for users.....	91
Chapter 8: Jumpers and connectors.....	93
System board jumpers and connectors	93
System board jumper settings.....	94
Disabling a forgotten password.....	95
Chapter 9: Using system diagnostics.....	96
Dell Embedded System Diagnostics.....	96
Running the Embedded System Diagnostics from Boot Manager.....	96
Running the Embedded System Diagnostics from the Dell Lifecycle Controller.....	96
System diagnostic controls.....	97
Chapter 10: Getting help.....	98
Recycling or End-of-Life service information.....	98
Contacting Dell Technologies.....	98
Accessing system information by using QRL.....	98
Quick Resource Locator for PowerEdge XR8610t system.....	99
Receiving automated support with Secure Connect Gateway (SCG).....	99
Chapter 11: Documentation resources.....	101

About this document

This document provides an overview about the system, information about installing and replacing components, diagnostic tools, and guidelines to be followed while installing certain components.

Dell PowerEdge XR8610t system configurations and features

The PowerEdge XR8610t system is a 1U half-width, single processor server sled that supports:

- One 5th Generation Intel Xeon Scalable processor with up to 16 cores or One 4th Generation Intel Xeon Scalable processor with up to 32 cores
- Eight DDR5 DIMM slots
- PCI Express® (PCIe) 5.0 enabled expansion slots
- 2 x M.2 2280 on BOSS-N1 card

CAUTION: Do not install GPUs, network cards, or other PCIe devices on your system that are not validated and tested by Dell. Damage caused by unauthorized and invalidated hardware installation will null and void the system warranty.

Topics:

- [System configurations - front view for PowerEdge XR8610t](#)
- [System configurations - rear view for PowerEdge XR8610t](#)
- [System configurations - inside view for PowerEdge XR8610t](#)
- [Locating the Express Service Code and Service Tag](#)
- [System information label](#)

System configurations - front view for PowerEdge XR8610t

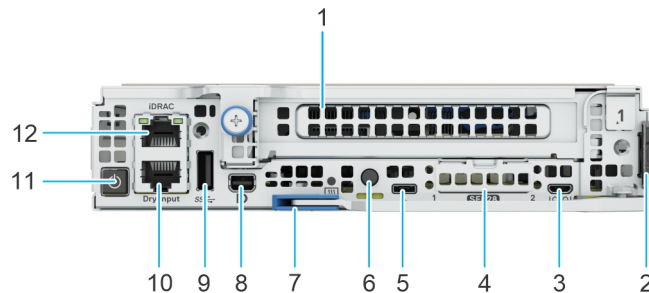


Figure 1. Front view for PowerEdge XR8610t

Table 1. Front view of the sled

Item	Ports, panels, or slots	Icon	Description
1	PCIe expansion card slot 1	N/A	Enables you to access the PCIe expansion card installed on Riser 2 in the system.
2	Information Tag	N/A	The Information tag is a slide-out label panel that contains Service Tag, QRL barcode and iDRAC MAC address.
3	Serial port	⏏	Enables you to connect a serial device to the system.

Table 1. Front view of the sled (continued)









Item	Ports, panels, or slots	Icon	Description
			<p> NOTE: The serial port is a micro USB type port. It only supports serial connection functions. The serial port does not support any USB functions.</p> <p> NOTE: When Intel(R) Ethernet 100G 2P adapter or Intel(R) Ethernet 25G 4P adapter with RBT cable connected, Micro USB does not function.</p>
4	SFP28 LAN on Motherboard (LOM) ports (optional)	N/A	Optional two SFP28 LAN on Motherboard (LOM) ports for networking.
5	iDRAC Direct port (Micro-AB USB)		The iDRAC Direct (Micro-AB USB) port enables you to access the iDRAC direct Micro-AB USB features. For more information, see the <i>Integrated Dell Remote Access Controller User's Guide</i> at PowerEdge Manuals .
6	System identification button		<p>The System Identification (ID) button is available on the front of the system. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access the BIOS using the step-through mode. When pressed, the system ID LED in the front panel blinks until the front button is pressed again. Press the button to toggle between on or off mode.</p> <p> NOTE: If the server stops responding during POST, press and hold the System ID button for more than five seconds to enter the BIOS progress mode.</p> <p> NOTE: To reset the iDRAC (if not disabled on the iDRAC setup page by pressing F2 during system boot), press and hold the System ID button for more than 15 seconds.</p>

Table 1. Front view of the sled (continued)

Item	Ports, panels, or slots	Icon	Description
7	Sled handle	N/A	Enables you to remove the sled from the enclosure.
8	Mini-DisplayPort		Enables you to connect a display device to the system.
9	USB 3.0 port		The USB port is 9-pin, 3.0-compliant. This port enables you to connect USB device to the system.
10	RJ-45 Dry Input	N/A	It is a RJ-45 Dry Input port. These are interruptible inputs to iDRAC. Dry means that no energy is supplied to the contacts.
11	Sled power button	N/A	Enables you to power on the sled. Indicates if the system is powered on or off. Press the power button to manually power on or off the system. i NOTE: When XR8610t is installed in the XR8000r chassis, the power button LED indicator status may be delayed for up to two minutes while the sled is initializing. The power button LED will start slowly blinking to indicate the system is performing the power on sequence after this time period.
12	iDRAC9 RJ-45 dedicated port	iDRAC	Enables you to remotely access iDRAC. For more information, see the <i>Integrated Dell Remote Access Controller User's Guide</i> at PowerEdge Manuals .

System configurations - rear view for PowerEdge XR8610t

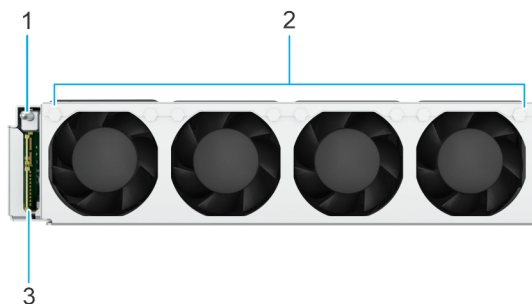


Figure 2. Rear view for PowerEdge XR8610t

Table 2. Rear view of the sled

Item	Ports, panels, or slots	Icon	Description
1	1U Guiding pin	N/A	Guiding pin for the 1U sled.
2	Fans rear view	N/A	Supports four cabled cooling fans
3	1U Power Distribution Board (PDB)	N/A	Provides power to bottom-layer cooling fans

System configurations - inside view for PowerEdge XR8610t

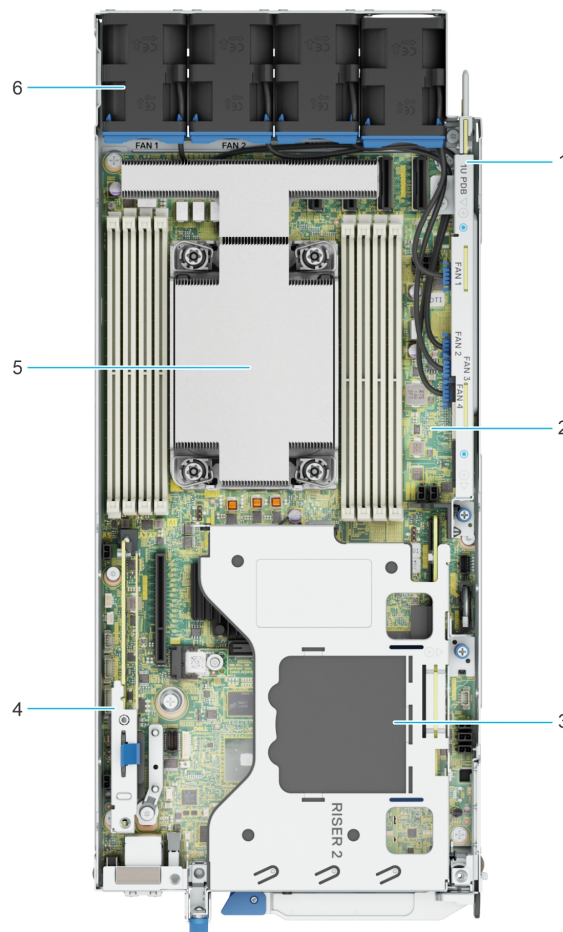


Figure 3. Inside view of the PowerEdge XR8610t sled

- | | |
|-----------------------------------|-----------------|
| 1. Power Distribution Board (PDB) | 2. System Board |
| 3. Riser 2 | 4. BOSS-N1 |
| 5. Processor | 6. Cooling fans |

Locating the Express Service Code and Service Tag

The unique Express Service Code and Service Tag are used to identify the system.

The information tag is located on the front of the system that includes system information such as iDRAC MAC address, Express Service Tag label, Quick Resource Locator.

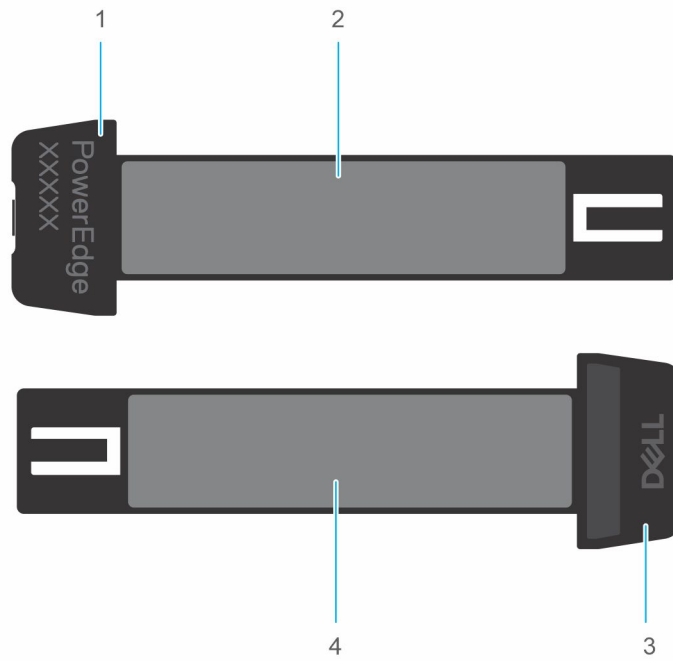


Figure 4. Locating the Service Tag of your system

1. Information tag (right view)
2. iDRAC MAC address information label
3. Information tag (left view)
4. Express Service Tag label and QRL

System information label

The system information label is located on the back of the system cover.

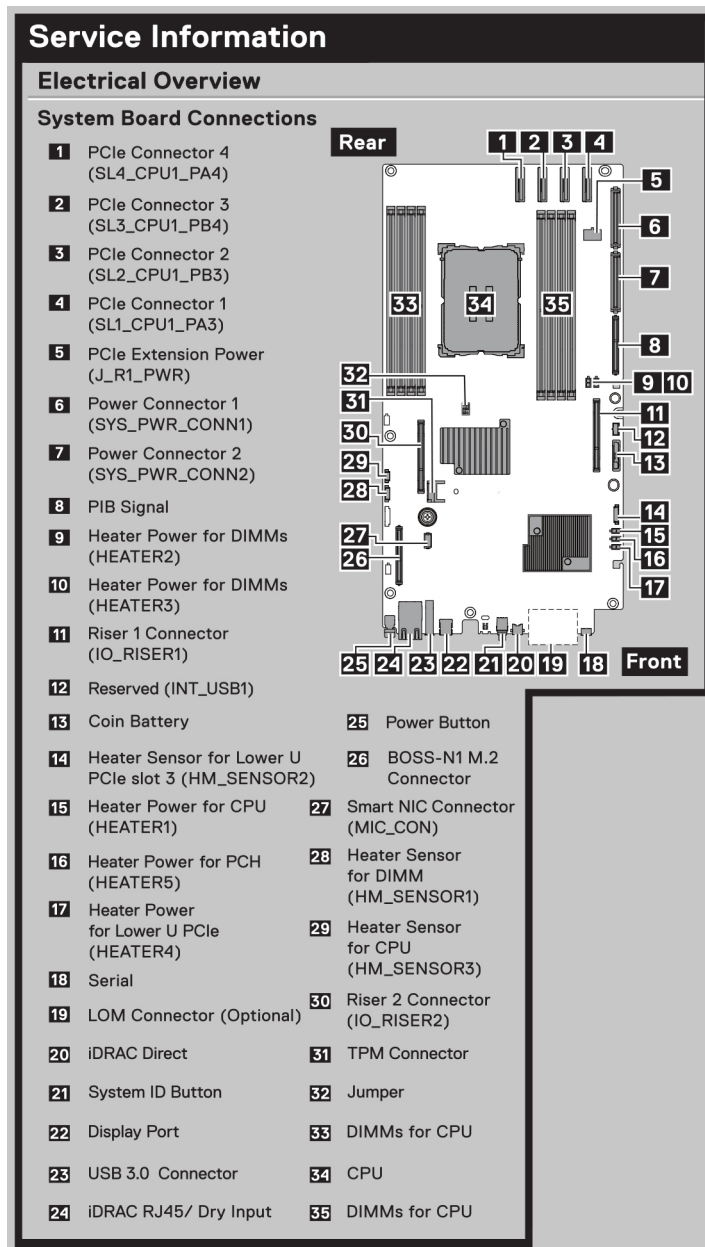


Figure 5. Service information

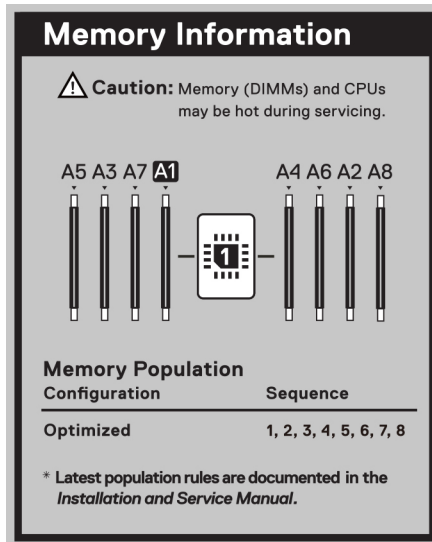


Figure 6. Memory information

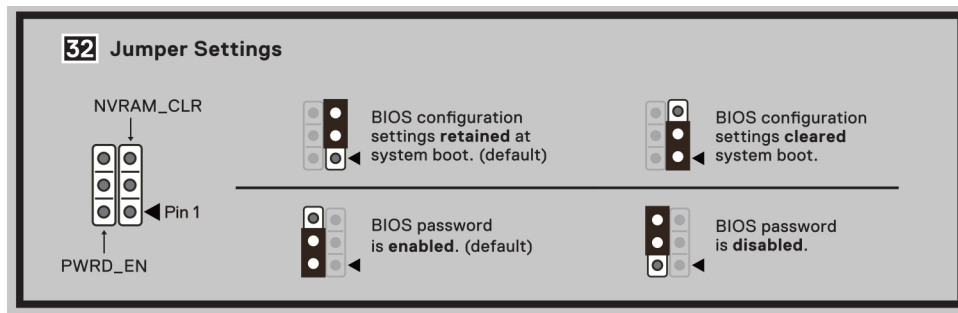


Figure 7. Jumper information

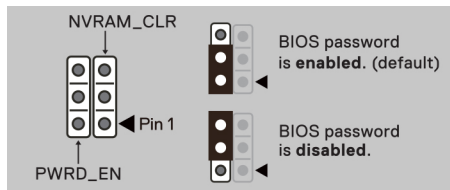


Figure 8. Jumper information

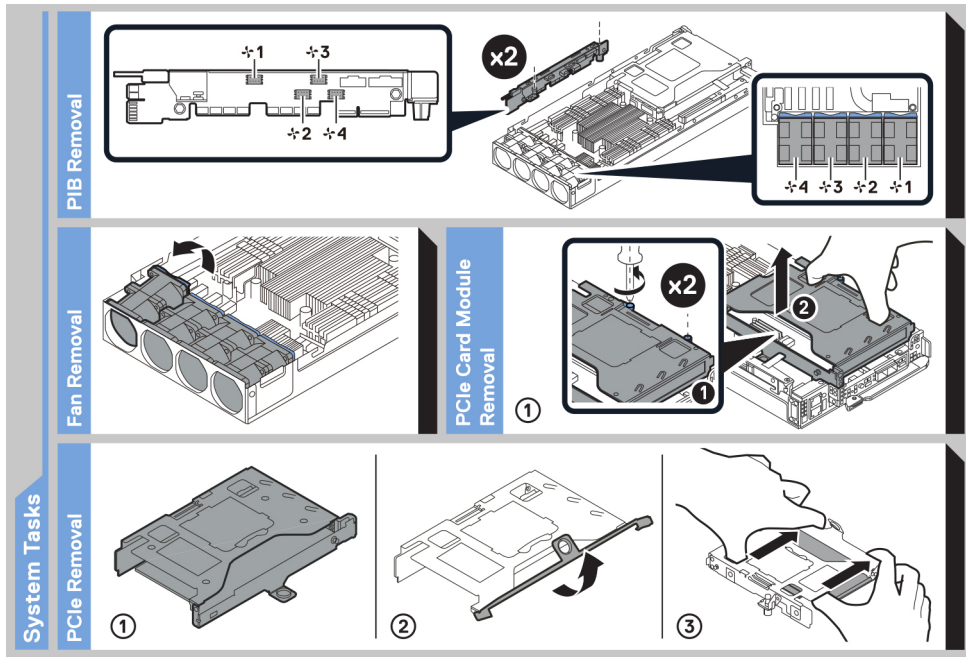


Figure 9. System tasks

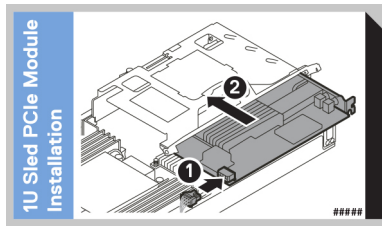


Figure 10. 1U sled PCIe module installation



Figure 11. Icon legend

Technical specifications

The technical and environmental specifications of your system are outlined in this section.

Topics:

- Sled dimensions
- System weight
- Processor specifications
- Cooling fan specifications
- Supported operating systems
- System battery specifications
- Memory specifications
- Expansion card riser specifications
- Drives
- Ports and connectors specifications
- Video specifications
- Environmental specifications

Sled dimensions

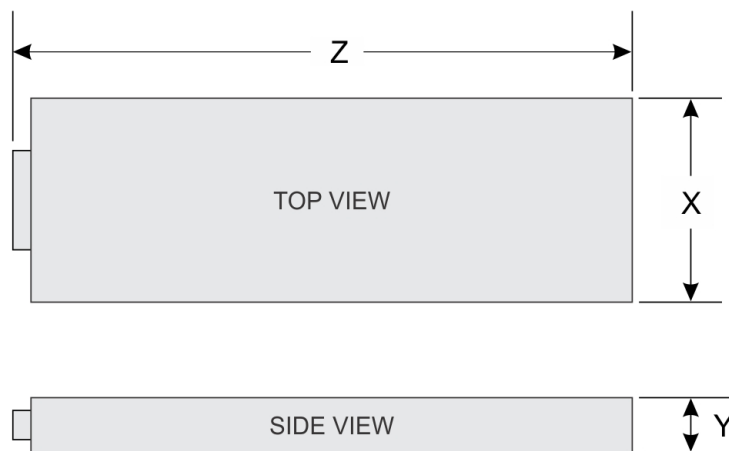


Figure 12. Sled dimensions

Table 3. PowerEdge XR8610t sled dimensions

X	Y	Z (handle closed)
184.8 mm (7.27 inches)	41.25 (1.62 inches)	433.5 mm (17.06 inches)

System weight

Table 4. PowerEdge XR8610t system weight

System configuration	Maximum weight (with all SSDs)
8 x DIMMS, 1 x processor, 2 x 2280 M.2 NVMe SSDs on BOSS-N1 card	3.90 kg (8.59 pound)

Processor specifications

Table 5. PowerEdge XR8610t processor specifications

Supported processor	Number of processors supported
5 th Generation Intel Xeon Scalable and Edge-Enhanced processors with up to 16 cores or 4 th Generation Intel Xeon Scalable and Edge-Enhanced processors with up to 32 cores	One

NOTE: It is recommended to use a maximum of two add-in cards with SPR EE-LCC CPU. Three add-in cards are supported, but this may result in an overall system performance degradation. .

Cooling fan specifications

The PowerEdge XR8610t system supports up to four cabled cooling fans.

Supported operating systems

The PowerEdge XR8610t system supports the following operating systems:

- Red Hat Enterprise Linux
- SUSE Linux Enterprise Linux
- WindRiver Solution
- VMware

For more information, go to [OS support](#).

System battery specifications

The PowerEdge XR8610t system supports CR 2032 3.0-V lithium coin cell system battery.

Memory specifications

The PowerEdge XR8610t system supports the following memory specifications for optimized operation.

Table 6. Memory specifications

DIMM type	DIMM rank	DIMM capacity	Single processor	
			Minimum RAM	Maximum RAM
RDIMM	Single rank	16 GB	32 GB	128 GB
	Dual rank	32 GB	64 GB	256 GB
	Dual rank	64 GB	128 GB	512 GB

Table 7. Memory module sockets

Memory module sockets	Speed
8, 288-pin	5600 MT/s, 4800 MT/s

NOTE: The processor may reduce the performance of the rated DIMM speed.

NOTE: Memory DIMM slots are not hot swappable.

Expansion card riser specifications

WARNING: Consumer-Grade GPU should not be installed or used in the Enterprise Server products.

The PowerEdge XR8610t system supports one PCI express (PCIe) expansion card riser.

Table 8. Expansion card slots supported on the 1U sled

PCIe slots	Expansion card riser	Processor connection	Height	Length	Slot width
Slot 1	R2A	Processor 1	Full Height	Half Length	x16 PCIe (Gen5) Single width

Drives

The PowerEdge XR8610t system supports up to 2 x M.2 NVMe SSDs (M.2 2280) installed BOSS-N1 card.

Ports and connectors specifications

USB ports specifications

Table 9. PowerEdge XR8610t USB specifications

Front	
USB port type	No. of ports
USB 3.0-compliant port	One
iDRAC Direct port (Micro-AB USB 2.0-compliant port)	One

NOTE: The micro USB 2.0 compliant port can only be used as an iDRAC Direct or a management port.

Network port specifications

The PowerEdge XR8610t system supports two (optional) SFP28 LAN on Motherboard (LOM) ports.

Table 10. Network port specification for the system

Feature	Specifications
LOM	2 x 25 GbE SFP 28 LOM connectors (optional).

Serial connector specifications

The PowerEdge XR8610t system supports one Micro USB Type B serial connector, on front of the system.

Display port

The PowerEdge XR8610t system supports One Mini-DisplayPort on front of the system.

iDRAC port specifications

The PowerEdge XR8610t system supports one RJ45 with port status LEDs for iDRAC remote management (dedicated port only) on front of the system.

RJ-45 dry contact port

The PowerEdge XR8610t system supports 1 x RJ45 for dry contact on front of the system.

To enhance usage in the IoT space, the XR8610t comes with a dry input sensor. Each input is configurable and manageable in the iDRAC interface. These are interruptible inputs to iDRAC. Dry means that no energy is supplied to the contacts. The dry contact connection cable with RJ45 connector on one end is custom to each installation and must be provided by the end user.

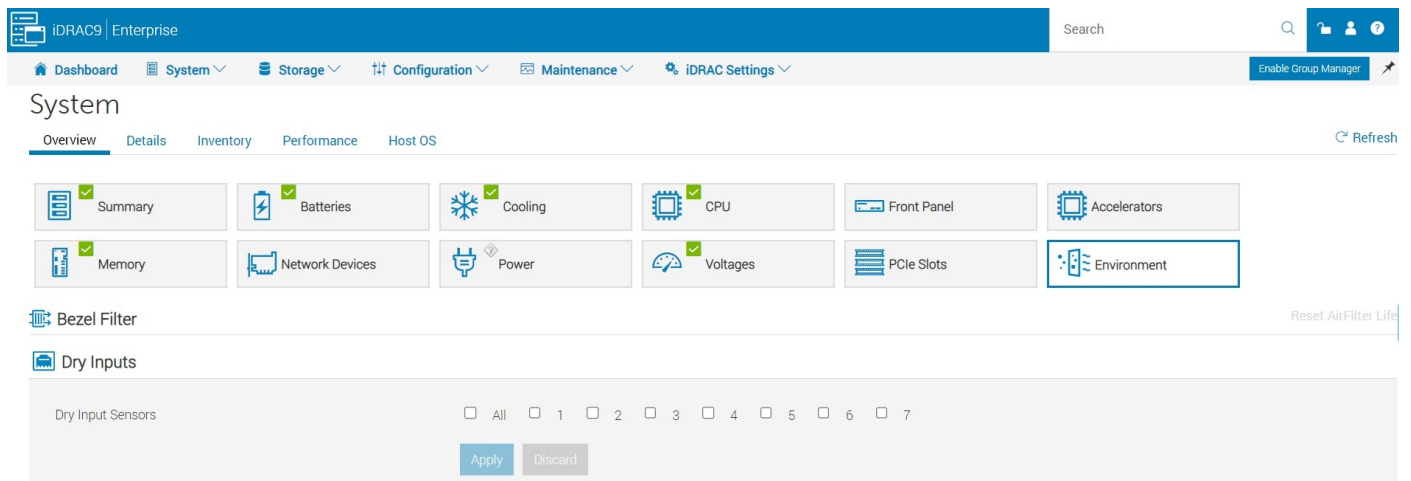


Figure 13. iDRAC interface for Dry Input sensors

NOTE: The RJ45 for dry contact does not support IP function.

The default states of the dry inputs are off/disabled. The user has seven (one for each dry input) enable/disable (default) control that must be enabled before logging occurs.

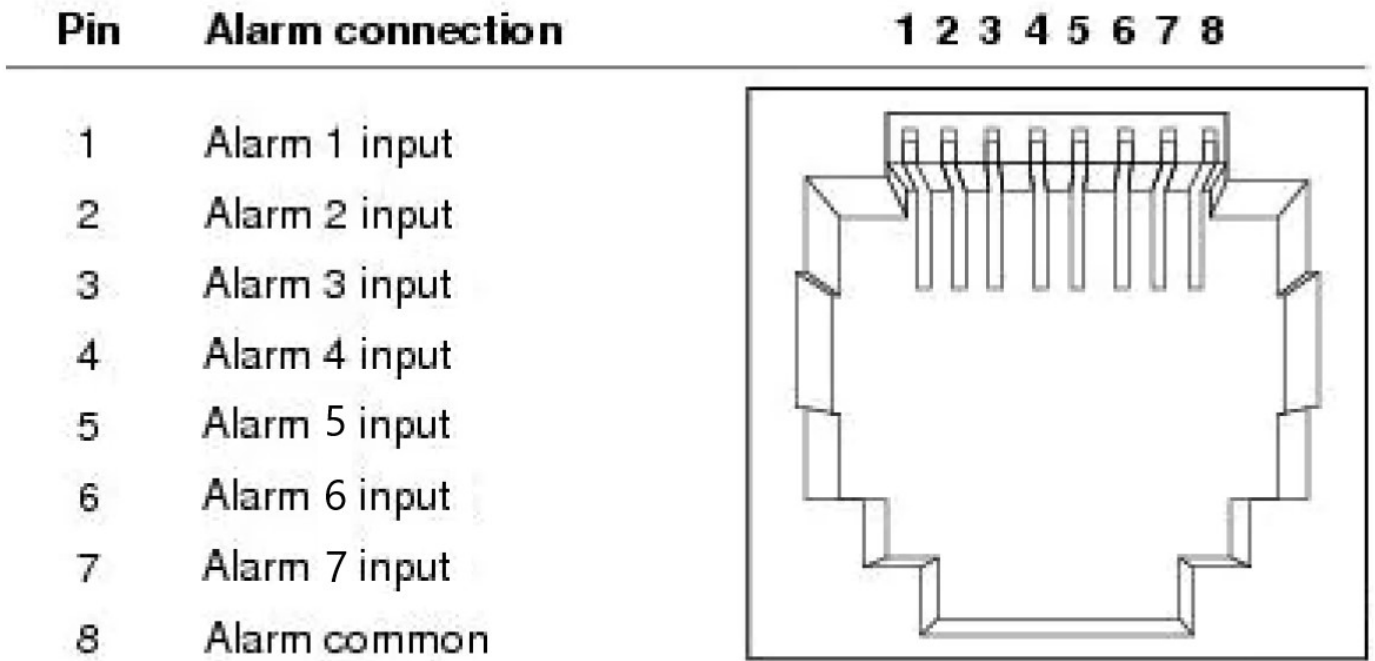


Figure 14. Dry input connection diagram

The seven dry inputs are interruptible inputs to iDRAC. They have the following characteristics:

- Monitored by iDRAC for state transition and LC event are for each state transition.
- NOT modeled as IPMI sensors but LC event only sensors. The current state of the input is not monitored or displayed anywhere.
- Event log - transitions (Open to close or close to Open) are logged in LC only.

Debounce — A debounce of 100mseconds is provided on all inputs.

Table 11. Event and Error Messages

Message ID	Message	RRA	DD	Severity
DCI1000	Dry input <input index> is transitioned to Open state.	None.	None	Severity -3 (Info)
DCI1001	Dry input <input index> is transitioned to Close state.	None.	None	Severity -3 (Info)

Video specifications

The PowerEdge XR8610t system supports integrated Matrox G200 graphics controller embedded in the iDRAC(BMC) chip, with 16 MB of video frame buffer.

Table 12. Supported video resolution options

Resolution	Refresh rate (Hz)	Color depth (bits)
640 x 480	60	8, 16, 32
800 x 600	60	8, 16, 32
1024 x 768	60	8, 16, 32
1152 x 864	60	8, 16, 32
1280 x 800	60	8, 16, 32

Table 12. Supported video resolution options (continued)

Resolution	Refresh rate (Hz)	Color depth (bits)
1280 x 1024	60	8, 16, 32
1360 x 768	60	8, 16, 32
1400 x 1050	60	8, 16, 32
1440 x 900	60	8, 16, 32
1600 x 1200	60	8, 16, 32
1680 x 1050	60	8, 16, 32
1920 x 1080	60	8, 16, 32
1920 x 1200	60	8, 16, 32

Environmental specifications

The PowerEdge XR8610t operates in these environmental categories: ASHRAE A2 and NEBS3.

i **NOTE:** For additional information about environmental certifications, refer to the Product Environmental Datasheet located with the Documentation > Regulatory Information on [Dell Support](#).

Table 13. Continuous operation specifications for ASHRAE A2

Feature	Allowable continuous operations
Temperature range for altitudes <= 900 m (<= 2953 ft)	10–35°C (50–95°F) with no direct sunlight on the equipment
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 80% RH with 21°C (69.8°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/300 m (1.8°F/984 Ft) above 900 m (2953 Ft)

Table 14. Continuous operation specifications for NEBS3

Feature	Allowable continuous operations
Temperature range for altitudes <= 900 m (<= 2953 ft)	-5° to 55°C (23 to 131°F) with no direct sunlight on the equipment
Humidity percent range (non-condensing at all times)	8% RH with -12°C minimum dew point to 90% RH with 24°C (75.2°F) maximum dew point
Operational altitude de-rating	Maximum temperature is reduced by 1°C/80 m (1.8°F/263 Ft) above 900 m (2953 Ft)

Table 15. Common environmental specifications for ASHRAE A2 and NEBS3

Feature	Allowable continuous operations
Maximum temperature gradient (applies to both operation and non-operation).	20°C in an hour* (36°F in an hour) and 5°C in 15 minutes (9°F in 15 minutes), 5°C in an hour* (9°F in an hour) for tape hardware
Non-operational temperature limits	-40 to 65°C (-40 to 149°F).
Non-operational humidity limits (Non-Condensing at all times)	5% to 95%RH with 27°C (80.6°F) maximum dew point
Maximum non-operational altitude	12,000 meters (39,370 feet)
Maximum operational altitude	3,050 meters (10,006 feet)

Table 16. Maximum vibration specifications

Maximum vibration	Specifications
Operating	0.21 G _{rms} at 5 Hz to 500 Hz (all operation orientations)
Storage	1.88 G _{rms} at 10 Hz to 500 Hz for 15 minutes (all six sides tested)

Table 17. Maximum shock pulse specifications

Maximum shock pulse	Specifications
Operating	Six consecutively executed shock pulses in the positive and negative x, y, and z axis of 6 G for up to 11 ms (4 pulse on each side on the system)
Storage	Six consecutively executed shock pulses in the positive and negative x, y, and z axis (one pulse on each side of the system) of 71 G for up to 2 ms

Particulate and gaseous contamination specifications

The following table defines the limitations that help avoid any equipment damage or failure from particulates and gaseous contamination. If the levels of particulates or gaseous pollution exceed the specified limitations and result in equipment damage or failure, you may need to rectify the environmental conditions. Remediation of environmental conditions is the responsibility of the customer.

Table 18. Particulate contamination specifications

Particulate contamination	Specifications
Conductive dust	Air must be free of conductive dust, zinc whiskers, or other conductive particles. <i>i</i> NOTE: This condition applies to data center and non-data center environments.
Corrosive dust	<ul style="list-style-type: none"> Air must be free of corrosive dust. Residual dust present in the air must have a deliquescent point less than 60% relative humidity. <i>i</i> NOTE: This condition applies to data center and non-data center environments.

Table 19. Gaseous contamination specifications

Gaseous contamination	Specifications
Copper coupon corrosion rate	<300 Å/month per Class G1 as defined by ANSI/ISA71.04-2013
Silver coupon corrosion rate	<200 Å/month as defined by ANSI/ISA71.04-2013

Environmental considerations

The PowerEdge system is targeted for edge deployments and it meets all the additional standards for thermal, shock, vibration parameters.

Table 20. Environmental considerations

Industry	Configuration	Description
Telco	GR-1089-CORE	Electromagnetic Compatibility and Electrical Safety – Generic Criteria for Network Telecommunications Equipment
	GR-63-CORE	NEBS Requirements: Physical Protection
	SR-3580 (NEBS Level 3)	NEBS Criteria Levels

Table 20. Environmental considerations (continued)

Industry	Configuration	Description
	GR-3108-CORE (Class 1)	Network Equipment in the Outside Plant (OSP). An exception is made for cold boot at +5C instead of -5C for systems without the heater subsystem enabled.
Military	N/A	
Marine	N/A	
Power Industry	N/A	
Safety	N/A	LDV, IEC/EN, CFR, CSA
EMC	N/A	EN, CISPR, ES, DTAG, CFR, ICES, VCCI
EMV	N/A	RoHS, WEEE, EN, ECE

Particulate and gaseous contamination specifications

The following table defines the limitations that help avoid any equipment damage or failure from particulates and gaseous contamination. If the levels of particulates or gaseous pollution exceed the specified limitations and result in equipment damage or failure, you may need to rectify the environmental conditions. Remediation of environmental conditions is the responsibility of the customer.

Table 21. Particulate contamination specifications

Particulate contamination	Specifications
Conductive dust	Air must be free of conductive dust, zinc whiskers, or other conductive particles <i>i</i> NOTE: This condition applies to data center and non-data center environments.
Corrosive dust	<ul style="list-style-type: none"> Air must be free of corrosive dust Residual dust present in the air must have a deliquescent point less than 60% relative humidity <i>i</i> NOTE: This condition applies to data center and non-data center environments.

Table 22. Gaseous contamination specifications

Gaseous contamination	Specifications
Copper coupon corrosion rate	<300 Å/month per Class G1 as defined by ANSI/ISA71.04-2013
Silver coupon corrosion rate	<200 Å/month as defined by ANSI/ISA71.04-2013

Thermal restriction matrix

Table 23. XR8610t Thermal Restriction - CPU and Memory

Config			Thermal Restriction	
Ambient Temperature			ASHARE A2 (Max 35°C)	NEBS3 (Max 55°C)
CPU	Intel® Xeon® Gold 4514Y	150W	Supported	Supported
CPU	Intel® Xeon® Gold 6433N	205W	Supported	Supported
	Intel® Xeon® Gold 6423N	195W	Supported	Supported
	Intel® Xeon® Gold 6403N	185W	Supported	Supported
	Intel® Xeon® Gold 4510	150 W	Supported	Supported

Table 23. XR8610t Thermal Restriction - CPU and Memory (continued)

Config			Thermal Restriction	
Ambient Temperature			ASHARE A2 (Max 35°C)	NEBS3 (Max 55°C)
CPU	Intel® Xeon® Gold 5423N	145 W	Supported	Supported
	Intel® Xeon® Gold 4509Y	125 W	Supported	Supported
	Intel® Xeon® Gold 6438N	205W	Supported	Supported
	Intel® Xeon® Gold 6421N	185W	Supported	Supported
	Intel® Xeon® Gold 5411N	165W	Supported	Supported
Memory	DDR5 RDIMM 4800 MT/s 64G		Supported	Supported
	DDR5 RDIMM 4800 MT/s 32G		Supported	Supported
	DDR5 RDIMM 4800 MT/s 16G		Supported	Supported
	DDR5 RDIMM 5600 MT/s 96G		Supported	Supported
	DDR5 RDIMM 5600 MT/s 64G		Supported	Supported
	DDR5 RDIMM 5600 MT/s 32G		Supported	Supported
	DDR5 RDIMM 5600 MT/s 16G		Supported	Supported

NOTE: Do not perform a cold startup below 5°C.

Table 24. XR8610t Thermal Restriction - Controller and storage

Config				Thermal Restriction		
Ambient Temperature				ASHARE A2 (Max 35°C)	NEBS3 (Max 55°C)	
Mancini BOSS-N1 M2 2280	Micron 7400	2280	480G	Supported	Supported	
		Hynix PE8010	2280	800G	Supported	Supported
			2280	960G	Supported	Supported
	Micron 7450	2280	480G	Supported	Supported	
		2280	960G	Supported	Supported	
		Hynix PE9010	2280	480G	Supported	Supported
	2280		960G	Supported	Supported	
	2280		1.92T	Supported	Supported	

Table 25. XR8610t Thermal Restriction - Commodities


Config	Thermal Restriction
Ambient Temperature	ASHARE A2 (Max 35°C) NEBS3 (Max 55°C)
PCIe Card	Non-Dell PCIe cards are not supported.
PSU	Dual PSUs are required for NEBS3


Table 26. XR8610t Thermal Restriction - RAN DPU

Sled Config	XR8620t Thermal Restriction	
Ambient Temperature	ASHRAE A2 (Max 35°C)	NEBS3 (Max 55°C)
Qualcomm X100 DPU	Supported	Supported
Dell 100GbE QSFP28 DPU	Supported	Supported

Table 26. XR8610t Thermal Restriction - RAN DPU (continued)

Sled Config	XR8620t Thermal Restriction	
	ASHRAE A2 (Max 35°C)	NEBS3 (Max 55°C)
Ambient Temperature		
Nokia Cloud RAN SmartNIC 2x QSFP56-DD DPU	Supported	Supported

 **NOTE:** Do not perform a cold startup below 5°C.

 **NOTE:** Do not perform a cold startup below 5°C.

XR8610t- Other Restrictions

- Hot-swap fans are not supported.
- Minimum cold boot temperature +5°C.
- Do not perform a cold startup below 5°C.
- DIMM Blank is required in empty slots.
- Sled blank is required in empty slots.
- PCIE blank is required in the empty slot (slot 1).
- PSU blank is required in empty slots.

Initial system setup and configuration

This section describes the tasks for initial setup and configuration of the Dell system. The section also provides general steps to set up the system and the reference guides for detailed information.

Topics:


- [Setting up the system](#)
- [iDRAC configuration](#)
- [Resources to install operating system](#)

Setting up the system

Perform the following steps to set up the system:

Steps

1. Unpack the system.
2. Remove the I/O connector cover from the system connectors.


 **CAUTION:** While installing the system, ensure that it is properly aligned with the slot on the enclosure to prevent damage to the system connectors.


3. Install the system in the enclosure.
4. Power on the sled.

Alternatively, you can also power on the system by using iDRAC by any of the below :

- For more information about powering on the system using iDRAC, see the [Options to log in to iDRAC](#).
- Open OpenManage Enterprise-Modular (OME-M 1.3 or later versions), after the iDRAC is configured on the OME. For more information, see the *OME-Modular User's Guide* at [PowerEdge Manuals](#).

For more information about setting up the system, see the *Getting Started Guide* that is shipped with your system.

 **NOTE:** When XR8610t is installed in the XR8000r chassis, the power button LED indicator status may be delayed for up to two minutes while the sled is initializing. The power button LED will start slowly blinking to indicate the system is performing the power on sequence after this time period.


 **NOTE:** For information about managing the basic settings and features of the system, see the [Pre-operating system management applications](#) chapter.

iDRAC configuration

The Integrated Dell Remote Access Controller (iDRAC) is designed to make you more productive as a system administrator and improve the overall availability of Dell servers. iDRAC alerts you to system issues, helps you to perform remote management, and reduces the need for physical access to the system.

Options to set up iDRAC IP address

To enable communication between your system and iDRAC, you must first configure the network settings based on your network infrastructure. The network settings option is set to **DHCP**, by default.

 **NOTE:** For static IP configuration, you must request for the settings at the time of purchase.

You can set up the iDRAC IP address using one of the interfaces in the table below. For information about setting up iDRAC IP address, see the documentation links provided in the table below.

Table 27. Interfaces to set up iDRAC IP address

Interface	Documentation links
iDRAC Settings utility	Integrated Dell Remote Access Controller User's Guide at iDRAC Manuals or for system specific Integrated Dell Remote Access Controller User's Guide, go to PowerEdge Manuals > Product Support page of your system > Documentation . <i>i</i> NOTE: To determine the most recent iDRAC release for your platform and for latest documentation version, see KB article KB78115 .
OpenManage Deployment Toolkit	Dell OpenManage Deployment Toolkit User's Guide available at OpenManage Manuals > OpenManage Deployment Toolkit.
iDRAC Direct	Integrated Dell Remote Access Controller User's Guide at iDRAC Manuals or for system specific Integrated Dell Remote Access Controller User's Guide, go to PowerEdge Manuals > Product Support page of your system > Documentation . <i>i</i> NOTE: To determine the most recent iDRAC release for your platform and for latest documentation version, see KB article KB78115 .
Lifecycle Controller	Dell Lifecycle Controller User's Guide at iDRAC Manuals or for system specific Dell Lifecycle Controller User's Guide, go to PowerEdge Manuals > Product Support page of your system > Documentation . <i>i</i> NOTE: To determine the most recent iDRAC release for your platform and for latest documentation version, see KB article KB78115 .

i **NOTE:** To access iDRAC, ensure that you connect the ethernet cable to the iDRAC dedicated network port or use the iDRAC Direct port by using the micro USB (type AB) cable. You can also access iDRAC through the shared mode, if the system is set it to share iDRAC port with OS as an OS NIC or shared LOM mode enabled.

Options to log in to iDRAC

To log in to the iDRAC Web User Interface, open a browser and enter the IP address.

You can log in to iDRAC as:

- iDRAC user
- Microsoft Active Directory user
- Lightweight Directory Access Protocol (LDAP) user

In the login screen displayed, if you have opted for secure default access to iDRAC, the default username is `root` and enter the iDRAC secure default password available on the back of the Information Tag. If you opted for legacy password, use the iDRAC legacy username and password - `root` and `calvin`, the iDRAC default password will be blank on the information tag. Then you are prompted to create a password of your choice before proceeding. You can also log in by using your Single Sign-On or Smart Card.

i **NOTE:** Ensure that you change the default username and password after setting up the iDRAC IP address.

For more information about logging in to the iDRAC and iDRAC licenses, see the latest [Integrated Dell Remote Access Controller User's Guide](#)

i **NOTE:** To determine the most recent iDRAC release for your platform and for the latest documentation version, see KB article [KB78115](#).



You can also access iDRAC using command-line protocol - RACADM. For more information, see the [Integrated Dell Remote Access Controller RACADM CLI Guide](#).


You can also access iDRAC using automation tool - Redfish API. For more information, see the [Integrated Dell Remote Access Controller User's Guide Redfish API Guide](#).

Resources to install operating system

If the system is shipped without an operating system, you can install a supported operating system by using one of the resources provided in the table below. For information about how to install the operating system, see the documentation links provided in the table below.

Table 28. Resources to install the operating system

Resource	Documentation links
iDRAC	Integrated Dell Remote Access Controller User's Guide or for system specific Integrated Dell Remote Access Controller User's Guide, go to PowerEdge Manuals > Product Support page of your system > Documentation .  NOTE: To determine the most recent iDRAC release for your platform and for latest documentation version, see KB article at KB78115 .
Lifecycle Controller	Dell Lifecycle Controller User's Guide at iDRAC Manuals or for system specific Dell Lifecycle Controller User's Guide, go to PowerEdge Manuals > Product Support page of your system > Documentation . Dell recommends using Lifecycle Controller to install the OS, since all required drivers are installed on the system.  NOTE: To determine the most recent iDRAC release for your platform and for latest documentation version, see KB article at KB78115 .
OpenManage Deployment Toolkit	OpenManage Manuals > OpenManage Deployment Toolkit
Dell certified VMware ESXi	Virtualization solutions

 **NOTE:** For more information about installation and how-to videos for operating systems supported on PowerEdge systems, see [Supported Operating Systems for Dell PowerEdge systems](#).

Options to download drivers and firmware

You can download the firmware from the Dell support site. For information about downloading firmware, see the [Downloading drivers and firmware](#) section.

You can also choose any one of the following options to download the firmware. For information about how to download the firmware, see the documentation links provided in the table below.

Table 29. Options to download firmware

Option	Documentation link
Using Integrated Dell Remote Access Controller Lifecycle Controller (iDRAC with LC)	iDRAC Manuals
Using Dell Repository Manager (DRM)	OpenManage Manuals
Using Dell Server Update Utility (SUU)	OpenManage Manuals
Using Dell OpenManage Deployment Toolkit (DTK)	OpenManage Manuals
Using iDRAC virtual media	iDRAC Manuals

Options to download and install OS drivers

You can choose any one of the following options to download and install OS drivers. For information about how to download or install OS drivers, see the documentation links provided in the table below.

Table 30. Options to download and install OS drivers

Option	Documentation
Dell support site	Downloading drivers and firmware section.
iDRAC virtual media	<p>Integrated Dell Remote Access Controller User's Guide or for system specific, go to Integrated Dell Remote Access Controller User's Guide > Product Support page of your system > Documentation .</p> <p>i NOTE: To determine the most recent iDRAC release for your platform and for latest documentation version, see Integrated Dell Remote Access Controller Release Notes.</p>

Downloading drivers and firmware

It is recommended that you download and install the latest BIOS, drivers, and systems management firmware on the system.

Prerequisites

Ensure that you clear the web browser cache before downloading the drivers and firmware.

Steps

1. Go to [Drivers](#).
2. Enter the Service Tag of the system in the **Enter a Dell Service Tag, Dell Product ID or Model** field, and then press Enter.

i **NOTE:** If you do not have the Service Tag, click **Browse all products**, and navigate to your product.
3. On the displayed product page, click **Drivers & Downloads**.
On the **Drivers & Downloads** page, all drivers that are applicable to the system are displayed.
4. Download the drivers to a USB drive, CD, or DVD.

Pre-operating system management applications

You can manage basic settings and features of a system without booting to the operating system by using the system firmware.

Options to manage the pre-operating system applications

You can use any one of the following options to manage the pre-operating system applications:

- System Setup
- Dell Lifecycle Controller
- Boot Manager
- Preboot Execution Environment (PXE)

i **NOTE:** To enable TDC/SGS features, requires populating all DIMM slots to support and enable in BIOS setup menu.

Topics:

- [System Setup](#)

System Setup

Using the

System Setup option, you can configure the BIOS settings, iDRAC settings, and device settings of the system.

You can access system setup by using any one of the following interfaces:

- Graphical User interface—To access go to iDRAC Dashboard, click **Configurations > BIOS Settings**.
- Text browser—To enable the text browser, use the Console Redirection.

To view

System Setup, power on the system, press F2, and click **System Setup Main Menu**.

i **NOTE:** If the operating system begins to load before you press F2, wait for the system to finish booting, and then restart the system and try again.

The options on the

System Setup Main Menu screen are described in the following table:

Table 31. System Setup Main Menu

Option	Description
System BIOS	Enables you to configure the BIOS settings.
iDRAC Settings	Enables you to configure the iDRAC settings. The iDRAC settings utility is an interface to set up and configure the iDRAC parameters by using UEFI (Unified Extensible Firmware Interface). You can enable or disable various iDRAC parameters by using the iDRAC settings utility. For more information about this utility, see <i>Integrated Dell Remote Access Controller User's Guide</i> at PowerEdge Manuals .

Table 31. System Setup Main Menu (continued)

Option	Description
Device Settings	Enables you to configure device settings for devices such as storage controllers or network cards.
Service Tag Settings	Enables you to configure the System Service Tag.

System BIOS

To view the **System BIOS** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS**.

Table 32. System BIOS details

Option	Description
System Information	Provides information about the system such as the system model name, BIOS version, and Service Tag.
Memory Settings	Specifies information and options related to the installed memory.
Processor Settings	Specifies information and options related to the processor such as speed and cache size.
NVMe Settings	Specifies options to change the NVMe settings.
Boot Settings	Specifies options to specify the Boot Mode (UEFI). Enables you to modify UEFI boot settings.
Network Settings	Specifies options to manage the UEFI network settings and boot protocols. Legacy network settings are managed from the Device Settings menu.
Integrated Devices	Specifies options to manage integrated device controllers and ports, specifies related features, and options.
Serial Communication	Specifies options to manage the serial ports, its related features, and options.
System Profile Settings	Specifies options to change the processor power management settings, memory frequency.
System Security	Specifies options to configure the system security settings, such as system password, setup password, Trusted Platform Module (TPM) security, and UEFI secure boot. It also manages the power button on the system.
Redundant OS Control	Sets the redundant OS information for redundant OS control.
Miscellaneous Settings	Specifies options to change the system date and time.

System Information

To view the **System Information** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > System Information**.

Table 33. System Information details

Option	Description
System Model Name	Specifies the system model name.
System BIOS Version	Specifies the BIOS version installed on the system.
System Management Engine Version	Specifies the current version of the Management Engine firmware.
System Service Tag	Specifies the system Service Tag.
System Manufacturer	Specifies the name of the system manufacturer.

Table 33. System Information details (continued)

Option	Description
System Manufacturer Contact Information	Specifies the contact information of the system manufacturer.
System CPLD Version	Specifies the current version of the system Complex Programmable Logic Device (CPLD) firmware.
UEFI Compliance Version	Specifies the UEFI compliance level of the system firmware.

Memory Settings

To view the **Memory Settings** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Memory Settings**.

Table 34. Memory Settings details

Option	Description
System Memory Size	Specifies the size of the system memory.
System Memory Type	Specifies the type of memory that is installed in the system.
System Memory Speed	Specifies the speed of the system memory.
Video Memory	Specifies the size of video memory.
System Memory Testing	Specifies whether the system memory tests are run during system boot. The two options available are Enabled and Disabled . This option is set to Disabled by default.
Memory Operating Mode	Specifies the memory operating mode. The option is available and is set to Optimizer Mode , by default. Options such as Fault Resilient Mode and NUMA Fault Resilient Mode are available for support when the Advanced RAS capability processor is installed on the system.
Current State of Memory Operating Mode	Specifies the current state of the memory operating mode.
Fault Resilient Mode Memory Size [%]	Select to define the percent of total memory size that must be used by the fault resilient mode, when selected in the Memory Operating mode. When Fault Resilient Mode is not selected, this option is grayed out and not used by Fault Resilient Mode. Option is displayed when 8 DIMMs are installed on the sled.
Node Interleaving	Enables or disables the Node interleaving option. Specifies if the Non-Uniform Memory Architecture (NUMA) is supported. If this field is set to Enabled , memory interleaving is supported if a symmetric memory configuration is installed. If the field is set to Disabled , the system supports NUMA (asymmetric) memory configurations. This option is set to Disabled by default.
ADDDC Setting	Enables or disables the ADDDC Setting feature. When Adaptive Double DRAM Device Correction (ADDDC) is enabled, failing DRAMs are dynamically mapped out. When set to Enabled it can impact the system performance under certain workloads. This feature is applicable for x4 DIMMs only. This option is set to Enabled by default.
Memory Training	<p>When the option is set to Fast and memory configuration is not changed, the system uses previously saved memory training parameters to train the memory subsystems. The system boot time is also reduced. If memory configuration is changed, the system automatically enables Retrain at Next Boot to force one-time full memory training steps, and then go back to Fast afterward.</p> <p>When option is set to Retrain at Next Boot, the system performs the force one-time full memory training steps at next power on and boot time is slowed on next boot.</p>

Table 34. Memory Settings details (continued)

Option	Description
	When option is set to Enable , the system performs the force full memory training steps on every power on and boot time is slowed on every boot.
DIMM Self Healing (Post Package Repair) on Uncorrectable Memory Error	Enables or disables Post Package Repair (PPR) on uncorrectable memory error. This option is set to Enabled by default.
Correctable Error Logging	Enables or disables correctable error logging. This option is set to Disabled by default.
Memory Paging Policy	This field sets memory paging policy.
Memory Map Out	This option controls DIMM slots on the system. This option is set to Enabled by default. It allows to disable system installed DIMMs.

Processor Settings

To view the **Processor Settings** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Processor Settings**.

Table 35. Processor Settings details

Option	Description
Logical Processor	Each processor core supports up to two logical processors. If this option is set to Enabled , the BIOS reports all the logical processors. If this option is set to Disabled , the BIOS reports only one logical processor per core. This option is set to Enabled by default.
Virtualization Technology	Enables or disables the virtualization technology for the processor. This option is set to Enabled by default.
Kernel DMA Protection	This option is set to Disabled by default. When option is set to Enabled , BIOS and Operating System will enable direct memory access protection for DMA capable peripheral devices using virtualization technology.
Directory Mode	Enables or disables the directory mode. This option is set to Enabled by default.
Adjacent Cache Line Prefetch	Optimizes the system for applications that need high utilization of sequential memory access. This option is set to Enabled by default. You can disable this option for applications that need high utilization of random memory access.
Hardware Prefetcher	Enables or disables the hardware prefetcher. This option is set to Enabled by default.
DCU Streamer Prefetcher	Enables or disables the Data Cache Unit (DCU) streamer prefetcher. This option is set to Enabled by default.
DCU IP Prefetcher	Enables or disables the Data Cache Unit (DCU) IP prefetcher. This option is set to Enabled by default.
Sub NUMA Cluster	Enables or disables the Sub NUMA Cluster. This option is set to Disabled by default.
MADT Core Enumeration	Determines how BIOS enumerates processor cores in the ACPI MADT table. When set to Round Robin , processor cores are enumerated in round robin order to evenly distribute

Table 35. Processor Settings details (continued)



Option	Description
	interrupt controllers for the OS across all Sockets and Dies. When set to Linear , processor cores are enumerated across all Dies within a socket before enumerating additional sockets for a linear distribution.
UMA Based Clustering Status	It is a read-only field and displays as Quadrant , when Sub NUMA Cluster is set to 2Way or 4Way then it displays as Disable .
UPI Prefetch	Enables you to get the memory read started early on DDR bus. The Ultra Path Interconnect (UPI) Rx path spawns the MemSpecRD to Integrated Memory Controller (iMC) directly. This option is set to Enabled by default.
XPT Prefetch	This option is set to Enabled by default.
LLC Prefetch	Enables or disables the LLC Prefetch on all threads. This option is set to Enabled by default.
Dead Line LLC Alloc	Enables or disables the Dead Line LLC. This option is set to Enabled by default. You can enable this option to opportunistically fill the dead lines in LLC or disable the option to not fill the dead lines in LLC.
Directory AtoS	Enables or disables the Directory AtoS. AtoS optimization reduces remote read latencies for repeat read accesses without intervening writes. This option is set to Disabled by default.
AVX P1	Enables you to reconfigure the processor Thermal Design Power (TDP) levels during POST based on the power and thermal delivery capabilities of the system. TDP verifies the maximum heat the cooling system is must dissipate. This option is set to Normal by default.  NOTE: This option is only available on certain stock keeping units (SKUs) of the processors.
Dynamic SST -Performance Profile	Enables you to reconfigure the processor via Dynamic or Static SST-PP Select. This option is set to Disabled by default.
SST-Performance Profile	Enables you to reconfigure the processor via Speed Select Technology(SST).
Intel SST-BF	Enables Intel SST-BF. This option is displayed if Performance Per Watt (OS) or Custom (when OSPM is enabled) system profiles are selected. This option is set to Disabled by default.  NOTE: This option requires a supported CPU.
Intel SST-CP	Enables Intel SST-CP. This knob controls whether SST-CP is enabled. When enabled it activates per core power budgeting. This option is set to Disabled by default.
x2APIC Mode	Enables or disables x2APIC mode. This option is set to Enabled by default.
AVX ICCP Pre-Grant License	Enables or disables AVX ICCP Pre-Grant License. This option is set to Disabled by default.
Opportunistic Snoop Broadcast	Opportunistic Snoop Broadcast(OSB) is a feature within the PCIe protocol that enhances system performance by reducing latency and improving data transfer efficiency. Auto is default and controlled by SI Compatibility and Directory Mode Enabled/Disabled .

Table 35. Processor Settings details (continued)


Option	Description
Dell Controlled Turbo	
Dell Controlled Turbo Setting	Controls the turbo engagement. Enable this option only when System Profile is set to Performance or Custom , and CPU Power Management is set to Performance . This option is set to Disabled by default.
Dell AVX Scaling Technology	Enables you to configure the Dell AVX scaling technology. This option is set to 0 by default. Enter the value from 0 to 12 bins. The value that is entered decreases the Dell AVX Scaling Technology frequency when the Dell-controlled Turbo feature is enabled.
Number of Cores per Processor	Controls the number of enabled cores in each processor. This option is set to All by default.
CPU Physical Address Limit	Limit CPU physical address to 46 bits to support older Hyper-V. If enabled, automatically disables TME-MT. This option is set to Enabled by default.
AMP Prefetch	This option enables one of the Mid-Level Cache (MLC) AMP hardware Prefetcher. This option is set to Disabled by default.
Homeless Prefetch	This option allows L1 Data Cache Unit (DCU) to prefetch, when the Fill Buffers (FB) is full. Auto maps to hardware default setting. This option is set to Auto by default.
Uncore Frequency RAPL	This setting controls whether the Running Average Power Limit (RAPL) balancer is enabled or not. If enabled, it activates the uncore power budgeting. This option is set to Enabled by default.
Processor Core Speed	Specifies the maximum core frequency of the processor.
Local Machine Check Exception	Enables or disables the local machine check exception. This is an extension of the MCA Recovery mechanism providing the capability to deliver Uncorrected Recoverable (UCR) Software Recoverable Action Required (SRAR) errors to one or more specific logical processors threads receiving previously poisoned or corrupted data. When enabled, the UCR SRAR Machine Check Exception is delivered only to the affected thread rather than broadcast to all threads in the system. The feature supports operating system recovery for cases of multiple recoverable faults that are detected close, which would otherwise result in a fatal machine check event. The feature is available only on Advanced RAS processors. This option is set to Enabled by default.
CPU Crash Log Support	This field controls Intel CPU Crash Log feature for collection of previous crash data from shared SRAM of Out-of-Band Management Service Module at post reset. This option is set to Disabled by default.
PROCESSOR n	<p> NOTE: Depending on the number of processors, there might be up to n processors listed.</p> <p>The following settings are displayed for each processor:</p>

Table 36. Processor n details

Option	Description
Family-Model-Stepping	Specifies the family, model, and stepping of the processor as defined by Intel.

Table 36. Processor n details (continued)

Option	Description
Brand	Specifies the brand name.
Level 2 Cache	Displays the amount of memory in the processor cache.
Level 3 Cache	Displays the amount of memory in the processor cache.
Number of Cores	Specifies the number of cores per processor.
Microcode	Specifies the processor microcode version.

NVMe Settings

This option sets the NVMe drive mode.

To view the **NVMe Settings** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > NVMe Settings**.

Table 37. NVMe Settings details

Option	Description
NVMe Mode	If the system contains NVMe drives that you want to configure in a RAID array, you must set both this field and the Embedded SATA field on the SATA Settings menu to RAID Mode . You may also need to change the Boot Mode setting to UEFI . Otherwise, you should set this field to Non RAID Mode . The option is set to Non RAID mode by default.
BIOS NVMe Driver	Dell Qualified NVMe drives always use the UEFI NVMe driver built into the Dell BIOS. When this option is set to All Drives , the BIOS driver will also be used with any NVMe drives in the system that has not been qualified by Dell. <i>i</i> NOTE: When this option is set to All Drives and non-Dell qualified NVMe drives are present, you have a configuration that has not been validated which may lead to unexpected behavior. The available options are Dell Qualified Drives and All Drives . This option is set to Dell Qualified Drives by default.

Boot Settings

Boot Settings enables you to specify the boot order. The **Boot Settings** only support **UEFI** mode.

- **UEFI:** The Unified Extensible Firmware Interface (UEFI) is a new interface between operating systems and platform firmware. The interface consists of data tables with platform related information, boot and runtime service calls that are available to the operating system and its loader. The following benefits are available when the **Boot Mode** is set to **UEFI**:
 - Support for drive partitions larger than 2 TB.
 - Enhanced security (e.g., UEFI Secure Boot).
 - Faster boot time.

i **NOTE:** You must use only the UEFI boot mode in order to boot from NVMe drives.

To view the **Boot Settings** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Boot Settings**.

Table 38. Boot Settings details

Option	Description
Boot Mode	Enables you to set the boot mode of the system. This option is set to UEFI by default.
Boot Sequence Retry	Enables or disables the Boot sequence retry feature or resets the system. When this option is set to Enabled and the system fails to boot, the system re-attempts the boot sequence after 30 seconds. When this option is set to Reset and the

Table 38. Boot Settings details (continued)


Option	Description
	system fails to boot, the system reboots immediately. This option is set to Enabled by default.
Generic USB Boot	Enables or disables the generic USB boot placeholder. This option is set to Disabled by default.
Hard-disk Drive Placeholder	Enables or disables the Hard-disk drive placeholder. This option is set to Disabled by default.
Clean all SysPrep variables and order	When this option is set to None , BIOS will do nothing. When set to Yes , BIOS will delete variables of SysPrep #### and SysPrepOrder this option is a onetime option, will reset to none when deleting variables. This setting is only available in UEFI Boot Mode . This option is set to None by default.
UEFI Boot Settings	Specifies the UEFI boot sequence. Enables or disables UEFI Boot options.  NOTE: This option controls the UEFI boot order. The first option in the list will be attempted first.

Table 39. UEFI Boot Settings

Option	Description
UEFI Boot Sequence	Enables you to change the boot device order.
Boot Option Enable/Disable	Enables you to select the enabled or disabled boot devices

Network Settings

To view the **Network Settings** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Network Settings**.


 **NOTE:** Network Settings are not supported in BIOS boot mode.

Table 40. Network Settings details

Option	Description
UEFI PXE Settings	Enables you to control the configuration of the UEFI PXE device.
Number of PXE Devices	This field specifies the number of PXE devices. This option is set to 4 by default.
PXE Device n (n = 1 to 4)	Enables or disables the device. When enabled, a UEFI PXE boot option is created for the device.
PXE Device n Settings (n = 1 to 4)	Enables you to control the configuration of the PXE device.
UEFI HTTP Settings	Enables you to control the configuration of the UEFI HTTP device.
HTTP Device n (n = 1 to 4)	Enables or disables the device. When enabled, a UEFI HTTP boot option is created for the device.
HTTP Device n Settings (n = 1 to 4)	Enables you to control the configuration of the HTTP device.
UEFI iSCSI Settings	Enables you to control the configuration of the iSCSI device.
iSCSI Initiator Name	Specifies the name of the iSCSI initiator in IQN format.
iSCSI Device1	Enables or disables the iSCSI device. When disabled, a UEFI boot option is created for the iSCSI device automatically. This is set to Disabled by default.
iSCSI Device1 Settings	Enables you to control the configuration of the iSCSI device.
UEFI NVMe-oF Settings	Enables you to control the configuration of the NVMe-oF devices.

Table 40. Network Settings details (continued)

Option	Description
NVMe-oF	Enables or disables the NVMe-oF feature. When enabled, it allows to configure the host and target parameters needed for fabric connection. This is set to Disabled by default.
NVMe-oF Host NQN	This field specifies the name of the NVMe-oF host NQN. Allowed input is in the following format: nqn.yyyy-mm.<Reserved Domain Name>:<Unique String>. Leave it empty to use system generated value with following format: nqn.1988-11.com.dell:<Model name>.<Model number>.<Service Tag>. This is set to nqn.1988-11.com.dell:<model name>.<model number>.<service tag> by default.
NVMe-oF Host Id	This field specifies a 16 bytes value of the NVMe-oF host identifier that uniquely identifies this host with the controller in the NVM subsystem. Allowed input is a hexadecimal-encoded string in this format: 00112233-4455-6677-8899-aabbccddeeff. Leave it empty to use system generated value. A value of all FF is not allowed. This is set to FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFFFF by default.
Host Security Key Path	This field specifies the Host security key path.
NVMe-oF SubSystem Settings	This field controls the parameters for the NVMe-oF subsystem n connections.

Table 41. PXE Device n Settings details

Option	Description
Interface	Specifies NIC interface used for the PXE device.
Protocol	Specifies Protocol used for PXE device. This option is set to IPv4 or IPv6 . This option is set to IPv4 by default.
VLAN	Enables VLAN for PXE device. This option is set to Enabled or Disabled . This option is set to Disabled by default.
VLAN ID	Shows the VLAN ID for the PXE device
VLAN Priority	Shows the VLAN Priority for the PXE device.

Table 42. HTTP Device n Settings details

Option	Description
Interface	Specifies NIC interface used for the HTTP device.
Protocol	Specifies Protocol used for HTTP device. This option is set to IPv4 or IPv6 . This option is set to IPv4 by default.
VLAN	Enables VLAN for HTTP device. This option is set to Enable or Disable . This option is set to Disable by default.
VLAN ID	Shows the VLAN ID for the HTTP device
VLAN Priority	Shows the VLAN Priority for the HTTP device.
DHCP	Enables or disables DHCP for this HTTP device. This option is set to Enable by default.
IP Address	Specifies IP address for the HTTP device.
Subnet Mask	Specifies subnet mask for the HTTP device.
Gateway	Specifies gateway for the HTTP device.
DNS info via DHCP	Enables or disables DNS Information from DHCP. This option is set to Enable by default.
Primary DNS	Specifies the primary DNS server IP address for the HTTP Device.
Secondary DNS	Specifies the secondary DNS server IP address for the HTTP Device.

Table 42. HTTP Device n Settings details (continued)

Option	Description
URI (will obtain from DHCP server if not specified)	Obtain URI from the DHCP server if not specified
TLS Authentication Configuration	Specifies the option for TLS authentication configuration.

Table 43. TLS Authentication Configuration screen details

Option	Description
TLS Authentication Mode	View or modify the device's boot TLS Authentication Mode. This option is set to One Way by default. None means the HTTP server and the client will not authenticate each other for this boot.
Root Certificate Configuration	Import, delete, or export the root certificate.

Table 44. iSCSI Device1 Settings screen details


Option	Description
Connection 1	Enables or disables the iSCSI connection. This option is set to Disabled by default.
Connection 2	Enables or disables the iSCSI connection. This option is set to Disabled by default.
Connection 1 Settings	Enables you to control the configuration for the iSCSI connection.
Connection 2 Settings	Enables you to control the configuration for the iSCSI connection.
Connection Order	Enables you to control the order for which the iSCSI connections will be attempted.
iSCSI F1/F2 Prompt on Error	<p>This field determines whether the BIOS stops and displays a prompt when iSCSI connection errors occur during POST. The BIOS will display the prompt when this setting is Enabled; otherwise, the BIOS will continue through POST and attempt to boot an operating system.</p> <p> NOTE: This setting will be grayed out if F1/F2 Prompt on Error in the Miscellaneous Settings menu is Disabled</p>

Table 45. Connection n Settings screen details

Option	Description
Interface	NIC interface used for this iSCSI connection.
Protocol	This field controls the Internet Protocol used for this iSCSI connection.
VLAN	VLAN Enable/Disable for this iSCSI connection.
VLAN ID	VLAN ID for this iSCSI connection.
VLAN Priority	VLAN priority for this iSCSI connection.
Retry Count	Retry Count for this iSCSI connection.
Timeout	Timeout for this iSCSI connection in milliseconds.
DHCP	DHCP Enable/Disable for this iSCSI connection.
Initiator IP Address	Initiator IP Address for this iSCSI connection.
Initiator Subnet Mask	Initiator Subnet Mask for this iSCSI connection.
Initiator Gateway	Initiator Gateway for this iSCSI connection.
Target info via DHCP	Target DHCP Enable/Disable for this iSCSI connection.
Target Name	Target name for this iSCSI connection in IQN format.

Table 45. Connection n Settings screen details (continued)

Option	Description
Target IP Address	Target IP Address for this iSCSI connection.
Target Port	Target Port for this iSCSI connection. The standard port number for iSCSI connections is 3260.
Target Boot Lun	Target LUN for this iSCSI connection. The value format is a string containing a hexadecimal-encoded representation of the 64-bit SCSI Logical Unit Number in the format described in the T10 SCSI Architecture Model specification. This format consists of four 2-byte fields separated by dashes. In most cases, the human-oriented logical unit number will be in the high-order two bytes and the low-order six bytes will be zero. Examples are: 4752-3A4F-6b7e-2F99, 6734-9-156f-127, 4186-9 or 0.
ISID	ISID (Initiator Session ID) to use for this iSCSI connection. The value is 6 hexadecimal numbers - such as 3ABBCCDDEEFF or 000000000000. If left blank, the ISID will be derived from the MAC ID of the assigned NIC interface for the connection.
Authentication Type	Authentication type for this iSCSI connection.
CHAP Type	CHAP type for this iSCSI connection.
CHAP Name	CHAP name for this iSCSI connection.
CHAP Secret	CHAP secret for this iSCSI connection. Minimum length is 12 and maximum is 16.
Reverse CHAP Name	Reverse CHAP name for this iSCSI connection.
Reverse CHAP Secret	Reverse CHAP secret for this iSCSI connection. Minimum length is 12 and maximum is 16.

Table 46. NVMe-oF SubSystem Settings screen details

Option	Description
NVMe-oF SubSystem n (n = 1 to 4)	Enables or disables NVMe-oF SubSystem. This option is set to Disabled by default.
NVMe-oF SubSystem n Settings (n = 1 to 4)	Enables you to control the configuration of the NVMe-oF SubSystem, if Enabled .

Table 47. NVMe-oF SubSystem Settings

Option	Description
Interface	NIC interface used for NVMe-oF connections.
Transport Type	This field sets the value of transport type for NVMe-oF connection. This option is set to TCP by default.
Protocol	This field sets the value of protocol type for NVMe-oF connection. This option is set to IPv4 by default.
VLAN	Enables or disables VLAN for this NVMe-oF connections. This option is set to Disabled by default.
VLAN ID	Specifies the VLAN Id for this NVMe-oF connection. This option is set to 1 by default.
VLAN Priority	Specifies the VLAN priority for this NVMe-oF connection. This option is set to 0 by default.
Retry Count	Specifies the retry count for this NVMe-oF connection. This option is set to 3 by default.
Timeout	Specifies the time out for this NVMe-oF connection. This option is set to 10000 by default.

Table 47. NVMe-oF SubSystem Settings (continued)

Option	Description
DHCP	Enables and disables the DHCP for this NVMe-oF connection. This option is set to Disabled by default.
Host IP Address	Specifies the Host IP Address for this NVMe-oF connection.
Host Subnet Mask	Specifies the Host Subnet Mask for this NVMe-oF connection.
Host Gateway	Specifies the Host Gateway for this NVMe-oF connection.
NVMe-oF Subsystem info via DHCP	Enables and disables the NVMe-oF subsystem's DHCP for this connection. This option is set to Disabled by default.
NVMe-oF Subsystem NQN	Specifies the NVMe-oF subsystem's NQN for this connection.
NVMe-oF Subsystem Address	Specifies the NVMe-oF subsystem's IP address for this connection.
NVMe-oF Subsystem Port	Specifies the NVMe-oF subsystem's port for this connection. This option is set to 4420 by default.
NVMe-oF Subsystem NID	Specifies the NamespaceID (NID) for this NVMe-oF connection.
NVMe-oF Subsystem Controller ID	Specifies the NVMe-oF subsystem's Controller ID for this connection. This option is set to 0 by default.
Security	Enables or disables the security option for this NVMe-oF connection. This option is set to Disabled by default.
Authentication Type	Specifies the authentication type for this NVMe-oF connection. This option is set to None by default.
SecurityKeyPath	Specifies the SecuritykeyPath for this NVMe-oF connection.

Integrated Devices

To view the **Integrated Devices** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Integrated Devices**.

Table 48. Integrated Devices details

Option	Description
User Accessible USB Ports	Configures the user accessible USB ports. Selecting All Ports Off disables all USB ports. ; Selecting All Ports Off (Dynamic) disables all USB ports during POST. Front ports can be enabled or disabled dynamically by authorized users without resetting the system. This option is set to All Ports On by default. The USB keyboard and mouse still function in certain USB ports during the boot process, depending on the selection. After the boot process is complete, the USB ports will be enabled or disabled as per the setting.
iDRAC Direct USB Port	The iDRAC Direct USB port is managed by iDRAC exclusively with no host visibility. This option is set to ON or OFF . When set to OFF , iDRAC does not detect any USB devices that are installed in this managed port. This option is set to On by default.
Embedded NIC1 and NIC2	Enables or disables the Embedded NIC1 and NIC2. If set to Disabled (OS) , the NIC may still be available for shared network access by the embedded management controller. This option is set to Enabled by default.
I/OAT DMA Engine	Enables or disables the I/O Acceleration Technology (I/OAT) option. I/OAT is a set of DMA features designed to accelerate network traffic and lower CPU utilization. Enable only if the hardware and software support the feature. This option is set to Disabled by default.
Embedded Video Controller	Enables or disables the use of the Embedded Video Controller as the primary display. When set to Enabled , the Embedded Video Controller will be the

Table 48. Integrated Devices details (continued)

Option	Description
	<p>primary display even if add-in graphic cards are installed. When set to Disabled, an add-in graphics card is used as the primary display. BIOS will output displays to both the primary add-in video and the embedded video during the POST and preboot environment. The embedded video will then be disabled right before the operating system boots. This option is set to Enabled by default.</p> <p>NOTE: When there are multiple add-in graphic cards that are installed in the system, the first card that is discovered during PCI enumeration is selected as the primary video. You might have to rearrange the cards in the slots in order to control which card is the primary video.</p>
I/O Snoop HoldOff Response	<p>Selects the number of cycles PCI I/O can withhold snoop requests from the CPU, to allow time to complete its own write to LLC. This setting can help improve performance on workloads where throughput and latency are critical. The available option is 2K Cycles by default.</p>
Current State of Embedded Video Controller	<p>Displays the current state of the embedded video controller. The Current State of Embedded Video Controller option is a read-only field. If the Embedded Video Controller is the only display capability in the system (that is, no add-in graphics card is installed), then the Embedded Video Controller is automatically used as the primary display even if the Embedded Video Controller setting is set to Disabled.</p>
SR-IOV Global Enable	<p>Enables or disables the BIOS configuration of Single Root I/O Virtualization (SR-IOV) devices. This option is set to Disabled by default.</p>
OS Watchdog Timer	<p>If your system stops responding, this watchdog timer aids in the recovery of your operating system. When this option is set to Enabled, the operating system initializes the timer. When this option is set to Disabled (the default), the timer does not have any effect on the system.</p>
NIC ACPI	<p>Enables or disables NIC ACPI device name information. When set to Enabled, publish ACPI device name for NICs on PCIe slots. This option is set to Disabled by default.</p> <p>NOTE: Changing this setting will cause the NIC name to change under Linux.</p>
Empty Slot Unhide	<p>Enables or disables the root ports of all the empty slots that are accessible to the BIOS and operating system. This option is set to Disabled by default.</p>
IIO PCIe Data Link Feature Exchange	<p>This field allows globally disabling PCIe Data Link Feature Exchange. This may be needed to support certain legacy hardware.</p>
Slot Disablement	<p>Enables or disables the available PCIe slots on your system. The slot disablement feature controls the configuration of the PCIe cards that are installed in the specified slot. Slots must be disabled only when the installed peripheral card prevents booting into the operating system or causes delays in system startup. If the slot is disabled, both the Option ROM and UEFI drivers are disabled. Only slots that are present on the system will be available for control. Slot n: Enables or disables or only the boot driver is disabled for the PCIe slot n. This option is set to Enabled by default.</p>
Slot Bifurcation	<p>Auto Discovery Bifurcation Settings allows Platform Default Bifurcation, Auto Discovery of Bifurcation and Manual Bifurcation Control.</p>
	<p>This option is set to Platform Default Bifurcation by default. The slot bifurcation field is accessible when set to Manual Bifurcation Control and is grayed out when set to Platform Default Bifurcation and Auto Discovery of Bifuraction.</p> <p>NOTE: The slot bifurcation supports on PCIe slot only, does not support slot type from Paddle card to Riser and Slimline connector to Riser.</p>

Serial Communication

To view the **Serial Communication** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Serial Communication**.

NOTE: The serial port is optional for the PowerEdge XR8610t system. The Serial Communication option is applicable only if the serial COM port is installed in the system.

Table 49. Serial Communication details

Option	Description
Serial Communication	<p>Enables the serial communication options. Selects serial communication devices (Serial Device 1 and Serial Device 2) in BIOS. BIOS console redirection can also be enabled, and the port address can be specified.</p> <p>The options available for System are On without Console Redirection, On with Console Redirection via COM1, On with Console Redirection via COM2, Off, Auto. This option is set to Auto by default.</p>
Serial Port Address	<p>Enables you to set the port address for serial devices. This option is set to Serial Device1=COM2, Serial Device2=COM1 by default.</p> <p>NOTE: You can use only Serial Device 2 for the Serial Over LAN (SOL) feature. To use console redirection by SOL, configure the same port address for console redirection and the serial device.</p> <p>NOTE: Every time the system boots, the BIOS syncs the serial MUX setting that is saved in iDRAC. The serial MUX setting can independently be changed in iDRAC. Loading the BIOS default settings from within the BIOS setup utility may not always revert the serial MUX setting to the default setting of Serial Device 1.</p>
External Serial Connector	<p>Enables you to associate the External Serial Connector to Serial Device 1, Serial Device 2, or the Remote Access Device by using this option. This option is set to Serial Device 1 by default.</p> <p>NOTE: Only Serial Device 2 can be used for Serial Over LAN (SOL). To use console redirection by SOL, configure the same port address for console redirection and the serial device.</p> <p>NOTE: Every time the system boots, the BIOS syncs the serial MUX setting saved in iDRAC. The serial MUX setting can independently be changed in iDRAC. Loading the BIOS default settings from within the BIOS setup utility may not always revert this setting to the default setting of Serial Device 1.</p>
Failsafe Baud Rate	<p>Specifies the failsafe baud rate for console redirection. The BIOS attempts to determine the baud rate automatically. This failsafe baud rate is used only if the attempt fails, and the value must not be changed. This option is set to 115200 by default.</p>
Remote Terminal Type	<p>Sets the remote console terminal type. This option is set to VT100/VT220 by default.</p>
Redirection After Boot	<p>Enables or disables the BIOS console redirection when the operating system is loaded. This option is set to Enabled by default.</p>

System Profile Settings

To view the **System Profile Settings** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > System Profile Settings**.

Table 50. System Profile Settings details

Option	Description
System Profile	Sets the system profile. If you set the System Profile option to a mode other than Performance Per Watt (DAPC) , the BIOS automatically sets the rest of the options. You can only change the rest of the options if the mode is set to Custom . This option is set to Performance Per Watt (DAPC) by default. Other options include Performance , Performance Per Watt (OS) , Workstation Performance and Custom . i NOTE: All the parameters on the system profile setting screen are available only when the System Profile option is set to Custom .
Optimized Power Mode	When set to Enabled , processor is tuned for lower power consumption. Also sets C1E to Enabled , sets CPU Power Management to System DBPM mode, sets Energy-Efficient Policy to Performance, sets Uncore Frequency to Dynamic, and sets Dynamic Load Line Switch to Enabled .
CPU Power Management	Sets the CPU power management. This option is set to System DBPM (DAPC) by default. Other options include Maximum Performance , OS DBPM .
Memory Frequency	Sets the speed of the system memory. This option is set to Maximum Performance by default.
Turbo Boost	Enables or disables the processor to operate in the turbo boost mode. This option is set to Enabled by default.
Energy Efficient Turbo	Energy Efficient Turbo (EET) is a mode of operation where a processor's core frequency is adjusted within the turbo range based on workload. This option is set to Enabled by default.
C1E	Enables or disables the processor to switch to a minimum performance state when it is idle. This option is set to Enabled by default.
C-States	Enables or disables the processor to operate in all available power states. C-States allow the processor to enter lower power states when idle. When set to Enabled (OS controlled) or when set to Autonomous (if hardware controlled is supported), the processor can operate in all available Power States to save power, but may increase memory latency and frequency jitter. This option is set to Enabled by default.
Memory Patrol Scrub	Sets the memory patrol scrub mode. This option is set to Standard by default.
Memory Refresh Rate	Sets the memory refresh rate, this option is set to 1x by default.
Uncore Frequency	Enables you to select the Uncore Frequency option. Dynamic enables the processor to optimize power resources across cores and uncores during runtime. The optimization of the uncore frequency to either save power or optimize performance is influenced by the setting of the Energy Efficiency Policy option.
Dynamic Load Line Switch	Dynamic Load Line Switch control. Dynamic Load Line (DLL) is a Power Management feature, which dynamically switches to the performance mode during periods of high CPU utilization. Read-only unless System Profile is set to Custom .
Energy Efficient Policy	Enables you to select the Energy Efficient Policy option. The CPU uses the setting to manipulate the internal behavior of the processor and determines whether to target higher performance or better power savings. This option is set to Balanced Performance by default.
Monitor/Mwait	Enables the Monitor/Mwait instructions in the processor. This option is set to Enabled for all system profiles, except Custom by default. i NOTE: This option can be disabled only if the C States option in the Custom mode is set to disabled. i NOTE: When C States is set to Enabled in the Custom mode, changing the Monitor/Mwait setting does not impact the system power or performance.
Workload Profile	This option allows the user to specify the targeted workload of a server. It allows optimization of performance based on the workload type. This option is set to Not Configured by default. Below is the list of available profiles: <ul style="list-style-type: none"> ● Not Configured ● HPC Profile

Table 50. System Profile Settings details (continued)

Option	Description
	<ul style="list-style-type: none"> • Low Latency Optimized Profile • Virtualization Optimized Performance Profile • Virtualization Optimized Performance Per Watt Profile • Database Optimized Performance Profile • Database Optimized Performance Per Watt Profile • SDS Optimized Performance Profile • SDS Optimized Performance Per Watt Profile • Telco Optimized Profile • NFVI FP Optimized Turbo Profile • NFVI FP Energy-Balance Turbo Profile
CPU Interconnect Bus Link Power Management	Enables or disables the CPU Interconnect Bus Link Power Management. This option is set to Enabled by default.
PCI ASPM L1 Link Power Management	Enables or disables the PCI ASPM L1 Link Power Management . This option is set to Enabled by default.
Workload Configuration	This field controls the Energy Performance Bias settings to allow BIOS to choose a configuration that improves performance on certain workload. The two options for selection are Balance and IO Sensitive . This option is set to Balance by default.

System Security

To view the **System Security** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > System Security**.

Table 51. System Security details

Option	Description
CPU AES-NI	Improves the speed of applications by performing encryption and decryption by using the Advanced Encryption Standard Instruction Set (AES-NI). This option is set to Enabled by default.
Strong Password Status	If Enabled , you must set up a password that has at least one character in lowercase, uppercase, digit, and a special character. Also, you have the option to set the minimum number of characters in both the new passwords. If Disabled , you can set a password that has any character in it but the password must not have more than 32 characters. Changes that are made by enabling or disabling this feature become immediately effective.
Strong Password Minimum Length (8 to 32)	Controls the minimum number of characters when setting a system or setup password. You can specify 8-32 characters.
System Password	Sets the system password. This option is read-only if the password jumper is not installed in the system.
Setup Password	Sets the setup password. This option is read-only if the password jumper is not installed in the system.
Password Status	Locks the system password. This option is set to Unlocked by default.
TPM Information	Indicates the type of Trusted Platform Module, if present.

Table 52. TPM 2.0 security information


Option	Description
TPM Information	
TPM Security	 NOTE: The TPM menu is available only when the TPM module is installed.

Table 52. TPM 2.0 security information (continued)

Option	Description
	Enables you to control the reporting mode of the TPM. When set to Off, the presence of the TPM is not reported to the OS. When set to On, the presence of the TPM is reported to the OS. The TPM Security option is set to Off by default.
	When TPM 2.0 is installed, the TPM Security option is set to On or Off . This option is set to Off by default.
TPM Information	Indicates the type of Trusted Platform Module, if present.
TPM Firmware	Indicates the firmware version of the TPM.
TPM Hierarchy	Enables, disables, or clears the storage and endorsement hierarchies. When set to Enabled , the storage and endorsement hierarchies can be used.
	When set to Disabled , the storage and endorsement hierarchies cannot be used.
	When set to Clear , the storage and endorsement hierarchies are cleared of any values, and then reset to Enabled .
TPM Advanced Settings	Specifies TPM Advanced Settings details.

Table 53. System Security details

Option	Description
Intel(R) TXT	Enables you to set the Intel Trusted Execution Technology (TXT) option. To enable the Intel TXT option, virtualization technology and TPM Security must be enabled with Pre-boot measurements. This option is set to Off by default. It is set On for Secure Launch (Firmware Protection) support.
Memory Encryption	Enables or disables the Intel Total Memory Encryption (TME) and Multi-Tenant (Intel® TME-MT). When option is set to Disabled , BIOS disables both TME and TME-MT technology. When option is set to Single Key BIOS enables the TME technology. When option is set to Multiple Keys , BIOS enables the TME-MT technology. This option is set to Disabled by default.
Global Memory Integrity	Allows enabling or disabling of the Intel Global Memory Integrity. The Global Mem Integrity can be enabled only if Processor Settings -> CPU Physical Address Limit is disabled .
TME Encryption Bypass	Enables you to bypass the Intel Total Memory Encryption. This option is set to Disabled by default.
Intel Trust Domain Extension(TDX)	Intel Trust Domain Extension (TDX) is a hardware-based trusted execution environment. It is designed to protect sensitive data and applications in Trust Domain(TD) or Virtual Machine(VM) from unauthorized access. Memory Encryption must be set to Multiple Keys for TDX to be enabled. TDX is set to Disabled by default
TME-MT/TDX Key Spilt to non-zero value	When the TME-MT/TDX Key Spilt to non-zero value is set to 1, 2, 3, 4, 5, or 6, it designates the number of bits for TDX usage, while the rest will be used by TME-MT. It is set to 1 by default.
TDX Secure Arbitration Mode Loader(SEAM)	This SW module runs in a new CPU Secure Arbitration Mode (SEAM) as peer virtual machine manager (VMM). This SEAM module supports TD entry and exit using the existing virtualization infrastructure. It is set to Disabled by default.
Intel(R) SGX	Enables you to set the Intel Software Guard Extension (SGX) option. To enable the Intel SGX option, processor must be SGX capable, memory population must be compatible (minimum x8 identical DIMM1 to DIMM8 per CPU socket, not support on persistent memory configuration), memory operating mode must be set at optimizer mode, memory encryption must be enabled and node interleaving must be disabled. This option is set to Off by default. When this option is to Off , BIOS disables the SGX technology. When this option is to On , BIOS enables the SGX technology.
Power Button	Enables or disables the power button on the front of the system. This option is set to Enabled by default.

Table 53. System Security details (continued)

Option	Description
AC Power Recovery	Sets how the system behaves after AC power is restored to the system. This option is set to Last by default. i NOTE: The host will not power up until iDRAC completes cryptographic verification of BIOS to ensure platform security. Host power on will be delayed by few minutes after AC power is applied.
AC Power Recovery Delay	Sets the time delay for the system to power up after AC power is restored to the system. This option is set to Immediate by default. When this option is set to Immediate , there is no delay for power up. When this option is set to Random , the system creates a random delay for power up. When this option is set to User Defined , the system delay time is manually to power up.
User Defined Delay (120 s to 600 s)	Sets the User Defined Delay option when the User Defined option for AC Power Recovery Delay is selected. The actual AC recovery time needs to add iDRAC cryptographic verification of BIOS time.
UEFI Variable Access	Provides varying degrees of securing UEFI variables. When set to Standard (the default), UEFI variables are accessible in the operating system per the UEFI specification. When set to Controlled , selected UEFI variables are protected in the environment and new UEFI boot entries are forced to be at the end of the current boot order.
In-Band Manageability Interface	When set to Disabled , this setting hides the Management Engine's (ME), HECI devices, and the system's IPMI devices from the operating system. This prevents the operating system from changing the ME power capping settings, and blocks access to all in-band management tools. All management should be managed through out-of-band. This option is set to Enabled by default. i NOTE: BIOS update requires HECI devices to be operational, and DUP updates require IPMI interface to be operational. This setting needs to be set to Enabled to avoid updating errors.
SMM Security Mitigation	Enables or disables the UEFI SMM security mitigation protections. It is set to Disabled by default.
Intel (R) In-Field Scan	The Intel(R) In-field Scan feature allows software to scan processor cores for latent faults. The scan can be performed in the field after the server is deployed. When this setting is Enabled , the BIOS configures all processors to respond to software scan requests. When this setting is Disabled , the processors will not respond to software scan requests.
Secure Boot	Enables Secure Boot, where the BIOS authenticates each pre-boot image by using the certificates in the Secure Boot Policy. Secure Boot is set to Disabled by default.
Secure Boot Policy	When the Secure Boot policy is set to Standard , the BIOS uses the system manufacturer's key and certificates to authenticate pre-boot images. When the Secure Boot policy is set to Custom , the BIOS uses the user-defined key and certificates. The secure Boot policy is set to Standard by default.
Secure Boot Mode	Configures how the BIOS uses the Secure Boot Policy Objects (PK, KEK, db, dbx). Below are the details of different boot modes available in the Secure Boot Mode option. User Mode In User Mode , PK must be installed, and BIOS performs signature verification on programmatic attempts to update policy objects. The BIOS allows unauthenticated programmatic transitions between modes. Deployed Mode Deployed Mode is the most secure mode. In Deployed Mode , PK must be installed and the BIOS performs signature verification on programmatic attempts to update policy objects. Deployed Mode restricts the programmatic mode transitions.

Table 53. System Security details (continued)

Option	Description
Secure Boot Policy Summary	Specifies the list of certificates and hashes that secure boot uses to authenticate images.
Secure Boot Custom Policy Settings	Configures the Secure Boot Custom Policy. To enable this option, set the Secure Boot Policy to Custom option.
UEFI CA Certificate Scope	This field specifies how Secure Boot uses the UEFI CA certificate in the Authorized Signature Database (db). When this field is set to Device Firmware and OS, Secure Boot will apply the UEFI CA certificate to all images, including device firmware, operating system loaders, and UEFI applications. When this field is set to Device Firmware, Secure Boot will apply the UEFI CA certificate only to device boot firmware, such as UEFI drivers for RAID or NIC devices. In this case, operating system loaders and UEFI applications will not execute if they are signed only by the UEFI CA key, even though the UEFI CA certificate is in db. This field is configurable only when the Secure Boot Policy is Custom . Otherwise, the value of this field is selected automatically based on the Secure Boot Policy setting.

Redundant OS Control

To view the **Redundant OS Control** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Redundant OS Control**.

Table 54. Redundant OS Control details

Option	Description
Redundant OS Location	Enables you to select a backup disk from the following devices: <ul style="list-style-type: none"> None BOSS PCIe Cards (Internal M.2 Drives) <p>i NOTE: RAID configurations and NVMe cards are not included, as BIOS does not have the ability to distinguish between individual drives in those configurations.</p>
Redundant OS State	<p>i NOTE: This option is disabled if Redundant OS Location is set to None.</p> <p>When set to Visible, the backup disk is visible to the boot list and OS. When set to Hidden, the backup disk is disabled and is not visible to the boot list and OS. This option is set to Visible by default.</p> <p>i NOTE: BIOS disables the device in hardware, so it is not accessed by the OS.</p>
Redundant OS Boot	<p>i NOTE: This option is disabled if Redundant OS Location is set to None or if Redundant OS State is set to Hidden.</p> <p>When set to Enabled, BIOS boots to the device specified in Redundant OS Location. When set to Disabled, BIOS preserves the current boot list settings. This option is set to Disabled by default.</p>


Miscellaneous Settings

To view the **Miscellaneous Settings** screen, power on the system, press F2, and click **System Setup Main Menu > System BIOS > Miscellaneous Settings**.

Table 55. Miscellaneous Settings details

Option	Description
System Time	Enables you to set the time on the system.
System Date	Enables you to set the date on the system.
Time Zone	Enables you to set the time zone on the system.

Table 55. Miscellaneous Settings details (continued)

Option	Description
Daylight Savings Time	Enables you to set whether the Daylight Savings Time is enabled or disabled.
Asset Tag	Specifies the asset tag and enables you to modify it for security and tracking purposes.
Keyboard NumLock	Enables you to set whether the system boots with the NumLock enabled or disabled. This option is set to On by default.  NOTE: This option does not apply to 84-key keyboards.
F1/F2 Prompt on Error	Enables or disables the F1/F2 prompt on error. This option is set to Enabled by default. The F1/F2 prompt also includes keyboard errors.
Load Legacy Video Option ROM	Enables you to let the system BIOS determine whether it will load legacy video (INT 10h) option ROM from the video controller, in UEFI Boot Mode. This option is set to disabled by default
Dell Wyse P25/P45 BIOS Access	Enables or disables the Dell Wyse P25/P45 BIOS Access. This option is set to Enabled by default.
Power Cycle Request	Enables or disables the Power Cycle Request. This option is set to None by default.

iDRAC Settings

The iDRAC settings is an interface to set up and configure the iDRAC parameters by using UEFI. You can enable or disable various iDRAC parameters by using the iDRAC settings.

 **NOTE:** Accessing some of the features on the iDRAC settings needs the iDRAC Enterprise License upgrade.

For more information about using iDRAC, see *Dell Integrated Dell Remote Access Controller User's Guide* at [iDRAC Manuals](#).


Device Settings

Device Settings enables you to configure device parameters such as storage controllers or network cards.

Minimum configuration to POST

The components listed below are the minimum configuration to POST:

- One processor (CPU) in processor socket
- Two memory module (DIMM) in socket A1 and A2
- One power supply unit
- XR8000r chassis (Power Distribution Board, cables)
- System board
- XR8610t sled

 **NOTE:** The system may generate errors when it is in a minimum to POST configuration. This behavior is expected as the configuration is not validated for operational use, instead, only for troubleshooting or diagnostic purposes.

Installing and removing system components

Topics:

- Safety instructions
- Before working inside your system
- After working inside your system
- XR8000r chassis
- Sled cover
- Cooling fans
- Expansion cards and expansion card risers
- BOSS-N1 card
- Power distribution board
- System memory
- Processor and heat sink module
- System battery
- System board
- Trusted Platform Module

Safety instructions

Before working inside your system

Prerequisites

Follow the safety guidelines listed in the [Safety instructions](#).

Steps

1. Power off the sled.
2. Remove the sled from the enclosure.

After working inside your system

Prerequisites

Follow the safety guidelines listed in [Safety instructions](#).

Steps

1. Replace the system cover.
2. If applicable, remove the I/O connector cover from the system connectors. Install the sled into the enclosure.
3. Reconnect the peripherals and connect the system to the electrical outlet, and then power on the system.

XR8000r chassis

Removing a sled blank

Prerequisites

Follow the safety guidelines listed in [Safety instructions](#).

Steps

Pull the sled blank to remove it from the enclosure.



Figure 15. Removing a sled blank

Next steps

Install a sled or sled blank.

Installing a sled blank

Prerequisites

Follow the safety guidelines listed in [Safety instructions](#).

Steps

1. Align the sled blank with the bay of the chassis.
2. Insert and push the sled blank, until it locks into place.



Figure 16. Installing a sled blank


Removing a sled

Prerequisites

1. Follow the safety guidelines listed in the [Safety instructions](#).
2. Remove the front bezel, if applicable.

Steps

1. Pull the blue lever on the sled to release the sled handle.
2. Holding the sled handle, slide the sled out of the enclosure.

 **NOTE:** The numbers on the image do not depict the exact steps. The numbers are for representation of sequence.

 **CAUTION:** Support the system with both hands while sliding it out of the enclosure.



Figure 17. Removing a sled from XR8000r

Next steps

[Installing the sled](#)

Installing a sled

Prerequisites

Follow the safety guidelines listed in [Safety instructions](#).

Steps

1. Pull the blue lever on the sled to free the sled handle.
2. Holding the sled with both hands, align the sled along the sled-bay into the chassis.
3. Slide the sled into the chassis, ensure that the sled handle is in lock position.
4. Push the sled handle inwards so that it locks into place and secures the sled in the chassis.

NOTE: The numbers on the image do not depict the exact steps. The numbers are for representation of sequence.



Figure 18. Installing a sled into XR8000r

Next steps

Follow the procedure listed in [After working inside your system.](#)

Sled cover

Removing the sled cover

Prerequisites

1. Follow the safety guidelines listed in the [Safety instructions.](#)
2. Power off the sled, and remove any attached peripherals.
3. Follow the steps for [Removing a sled.](#)
4. Place the sled on the flat surface with the top cover facing upwards.

Steps

1. Loosen the captive screw by rotating in counter clockwise direction.
2. Slide and lift the cover to the front of the sled.



Figure 19. Removing the sled cover

Next steps

Follow the procedure listed in [Replace the sled cover](#).

Installing the sled cover

Prerequisites

1. Follow the safety guidelines listed in the [Safety instructions](#).
2. Ensure that all internal cables are connected and routed properly, and no tools or extra parts are left inside the system.

Steps

1. Align the tabs on the sled cover with the guide slots on the sled and place down the sled cover.
2. Slide the cover towards the rear of the system until it locks in to place and fasten the captive screw.

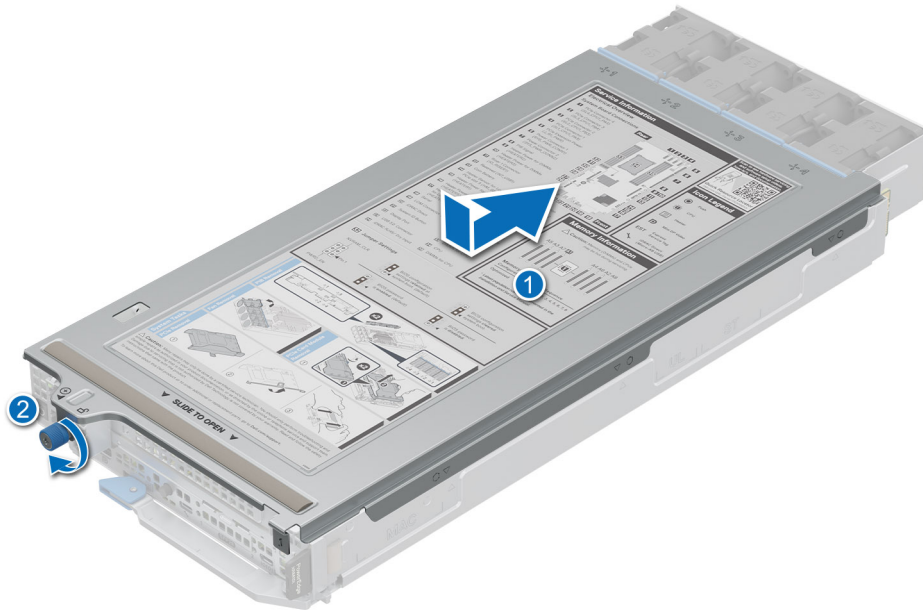


Figure 20. Installing the sled cover

Next steps

Follow the procedure listed in [After working inside your system](#).

Cooling fans

Removing a cooling fan

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
 2. Follow the procedure listed in [Before working inside your system](#).
- NOTE:** Observe the fan cable routing or make a note of the fan cable routing.

Steps

1. Route the fan cables properly through the fan guard and disconnect the fan cable that is connected to the connector on the power distribution board (PDB) of the sled.
- NOTE:** Fans 1, 2, 3 and 4 are connected to the 1U PDB.

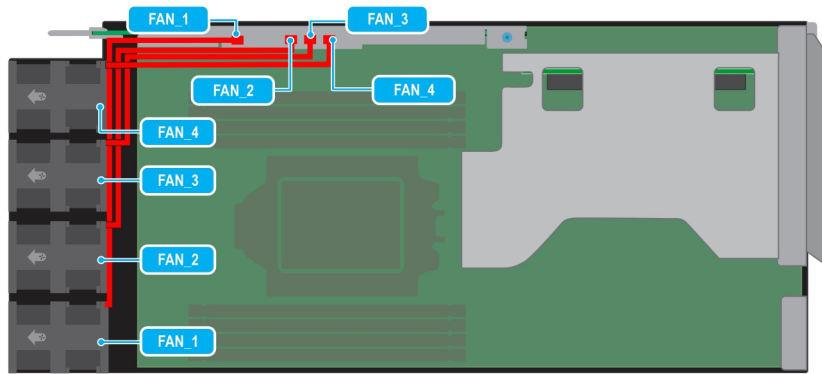


Figure 21. Cable routing

2. Pull slightly to disengage the fan cable from the fan guard and then lift the fan module out of the fan cage.

NOTE: The airflow directional arrow outward on the fan indicates Reverse-Air-Flow (RAF).

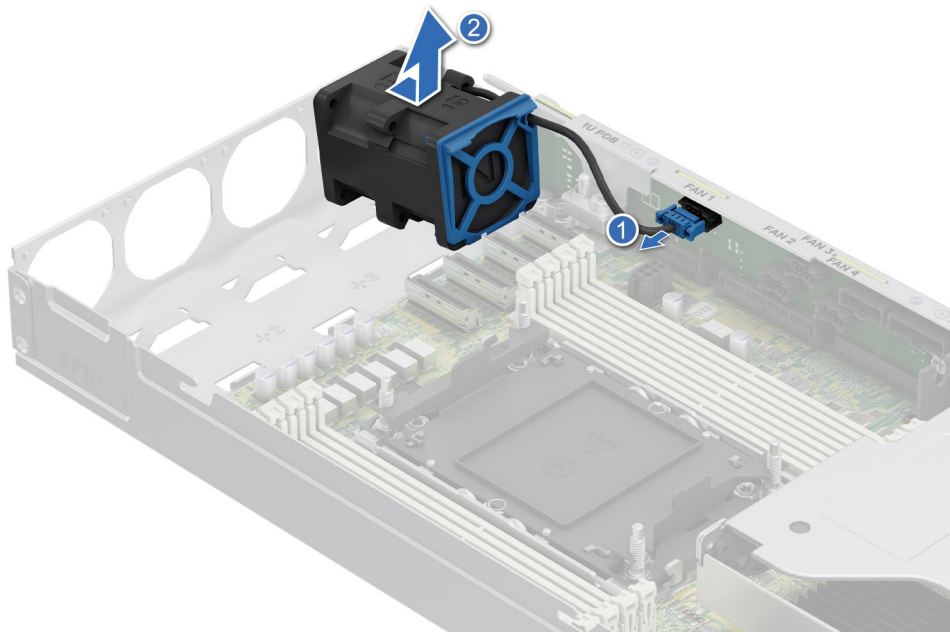


Figure 22. Removing a cooling fan

Next steps

Replace a fan on 1U sled

Installing a cooling fan

Prerequisites

1. Follow the safety guidelines listed in [Safety Instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

NOTE: Observe the fan cable routing or make a note of the fan cable routing.

Steps

1. Lower the fan module into the cage until it is seated firmly.

NOTE: The airflow directional arrow outward on the fan indicates Reverse-Air-Flow (RAF).

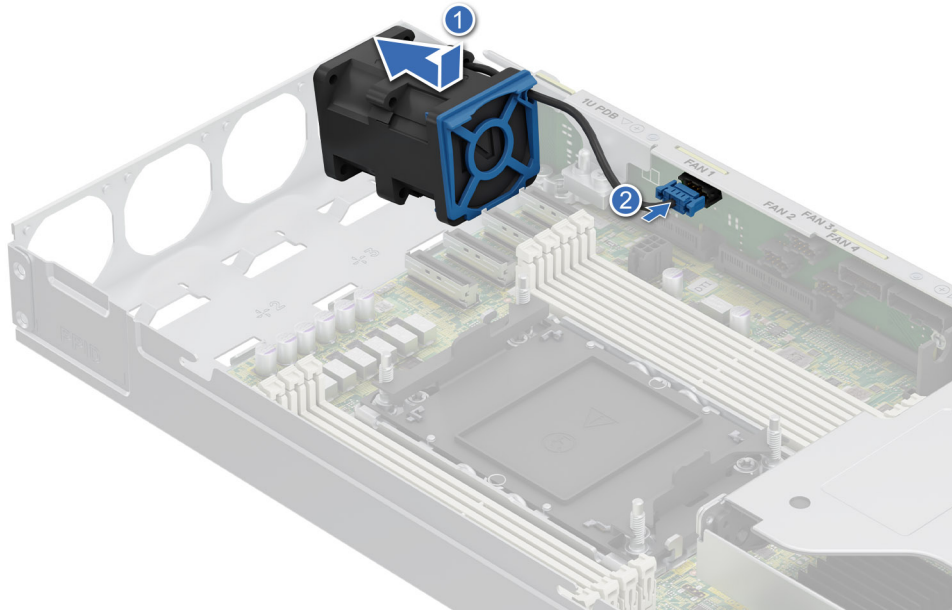


Figure 23. Installing a cooling fan

2. Route the fan cables properly through the fan guard and connect the cable to the connector on the power distribution board (PDB) of the sled as shown in the image below.

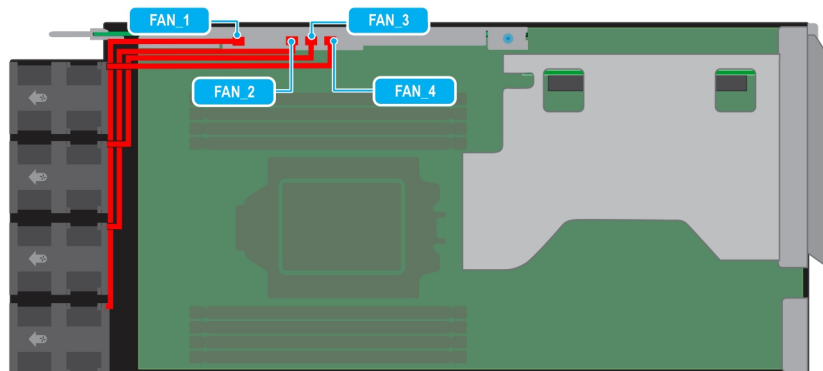


Figure 24. Sled fan cable routing

Next steps

Install the sled cover.

Expansion cards and expansion card risers

NOTE: When an expansion card is not supported or missing, the iDRAC and Lifecycle Controller logs an event. This does not prevent your system from booting. However, if a F1/F2 pause occurs with an error message, see Troubleshooting expansion cards section in the PowerEdge Servers Troubleshooting Guide at [PowerEdge Manuals](#).

Expansion card installation guidelines

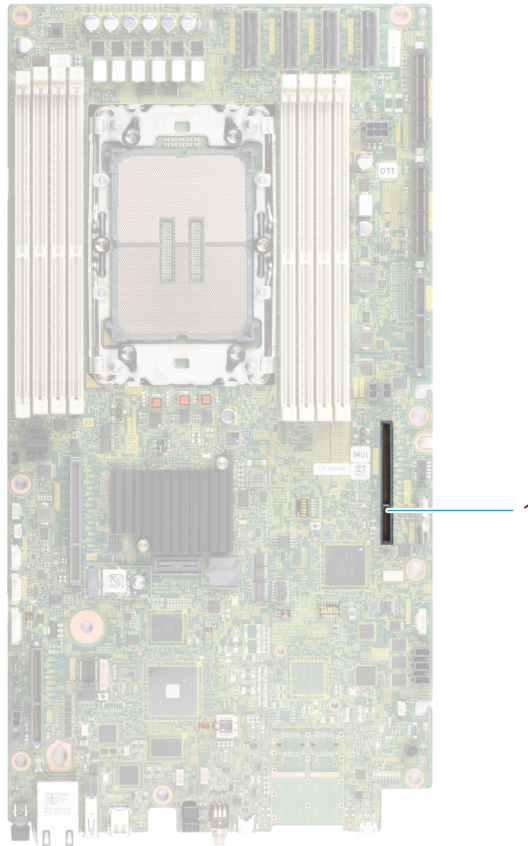


Figure 25. Expansion card slot connector

1. Riser connector (Riser 2)

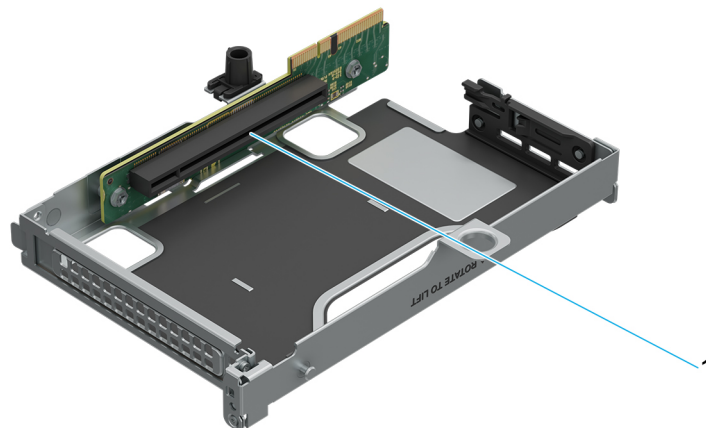



Figure 26. Riser 2A slot

1. Slot 1

Table 56. Riser Configurations

Config	Riser Configuration	CPUs	PERC type supported	Rear storage	x16 CPU1	X16 CPU2
0	No riser	1	No	No	0	0
1	R2A	1	No	No	1	0

 **NOTE:** The expansion-card slots are not hot-swappable.

The following table provides guidelines for installing expansion cards to ensure proper cooling and mechanical fit. The expansion cards with the highest priority should be installed first using the slot priority indicated. All the other expansion cards should be installed in the card priority and slot priority order.

Table 57. Configuration 0: No Riser

Card type	Slot priority	Maximum number of cards
BOSS-N1	Integrated slot	1

Table 58. Configuration 1: R2A

Card type	Slot priority	Maximum number of cards
INTEL (NIC: 25 GB, FH, adapter)	1	1
INTEL (NIC: 100 GB, FH, adapter)	1	1
INTEL(NIC: ACC100, FH, adapter)	1	1
Mellanox (NIC: 100 GB, FH)	1	1
Dell (Interface, PCIE: 3.0)	1	1
Nokia (NIC: 100GB, FH)	1	1
Qualcomm (NIC: 100GB, FH)	1	1
BOSS-N1	Integrated slot	1

Removing the expansion card riser 2

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).
3. Remove the [system cover](#).

Steps

1. Loosen the captive screw on the riser.
2. Hold the expansion card riser 2 by the edges and lift the expansion card riser from the riser connector on the system board.

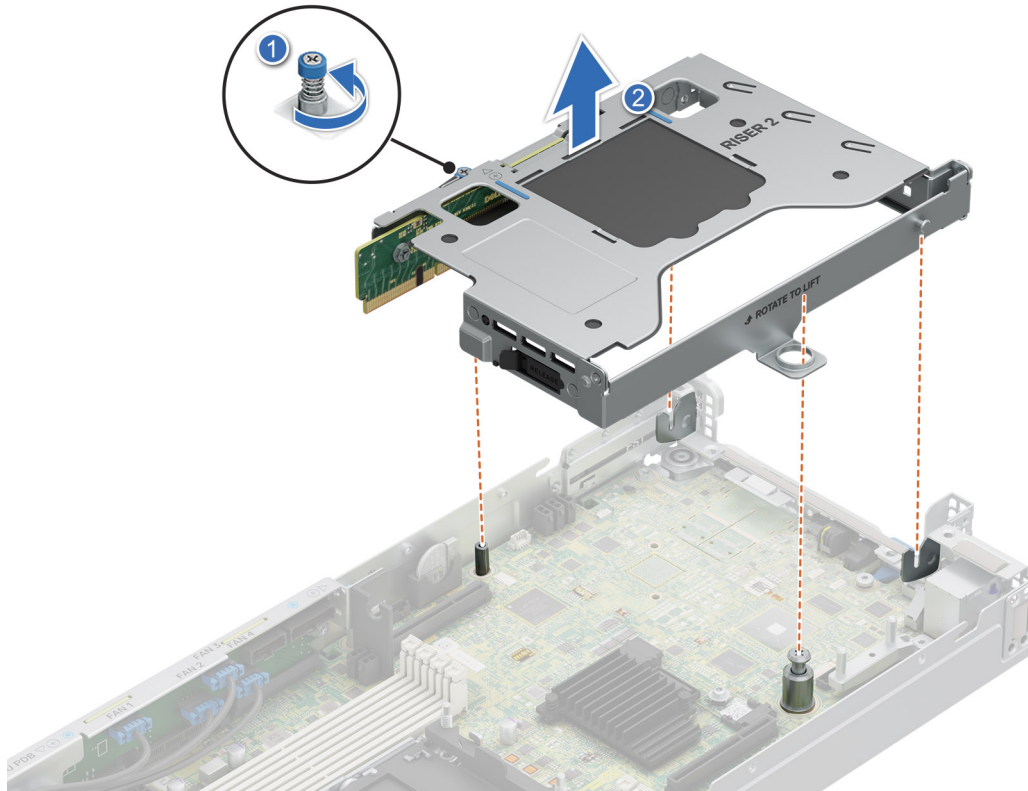


Figure 27. Removing the expansion card riser 2

Next steps

Replace the expansion card riser 2.

Installing the expansion card riser 2

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

Steps

1. Align the riser with the riser slot on the sled.
2. Using both hands, lower the riser 2 until it is seated firmly.
3. Using a Phillips 2 screwdriver, tighten the captive screw to secure the expansion card riser 2 on to the 1U sled.

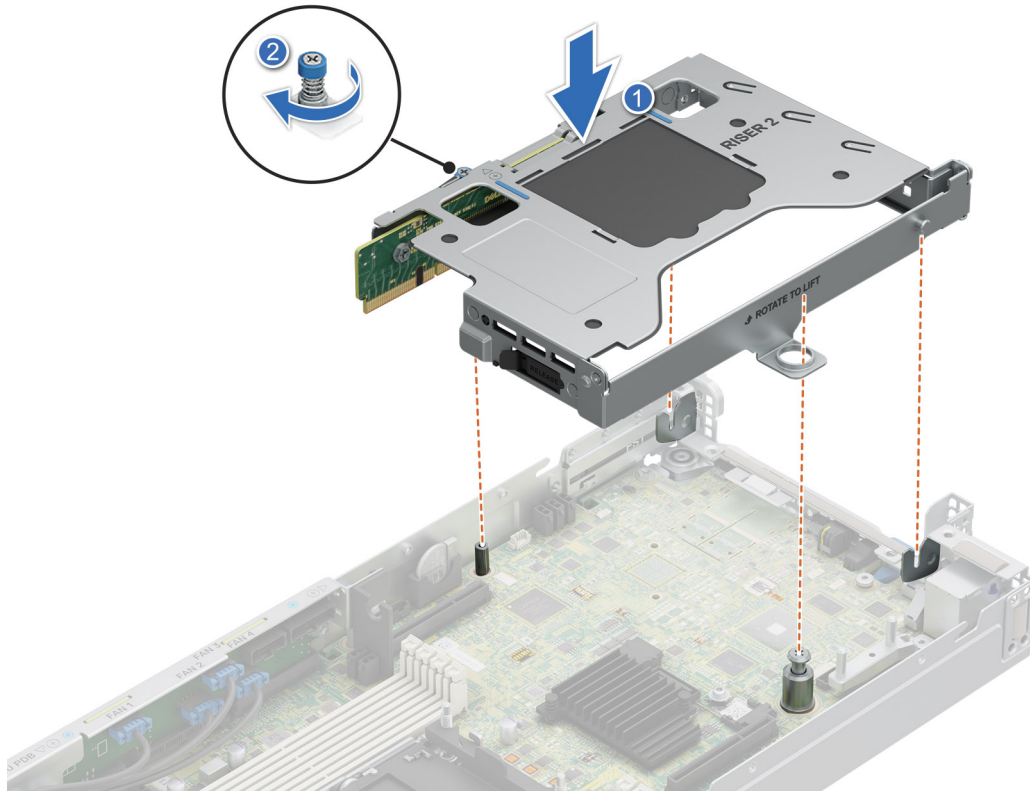


Figure 28. Installing the expansion card riser 2

Next steps

Install the system cover.

Removing the PCIe card from riser

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).
3. [Remove the sled cover](#).
4. [Remove the riser](#).

Steps

1. Rotate the riser plate up in order to access the PCIe card.
2. Using both hands, hold the PCIe card by the edges and pull the card from the riser slot.

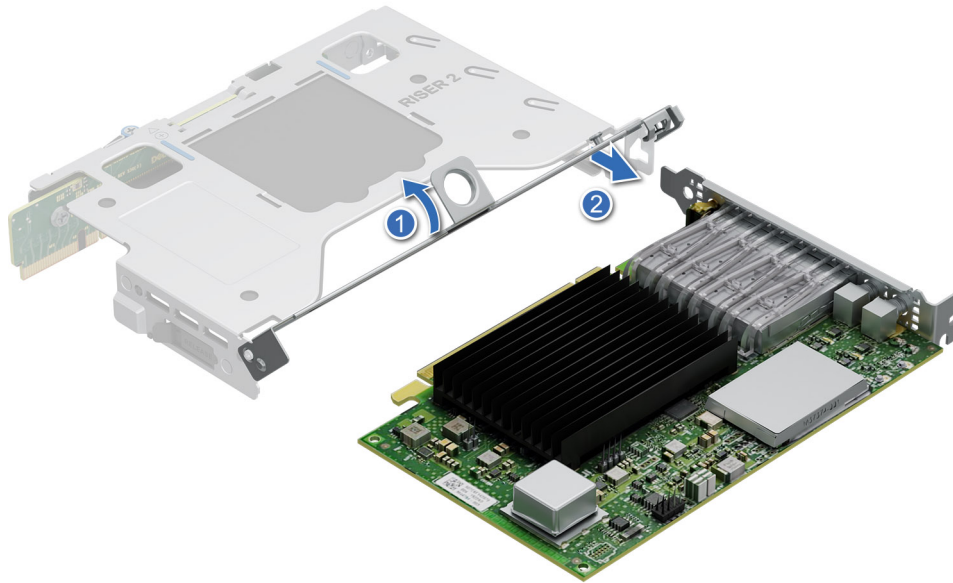


Figure 29. Removing the PCIe card from riser

3. Replace the expansion card filler bracket and rotate the riser plate below.

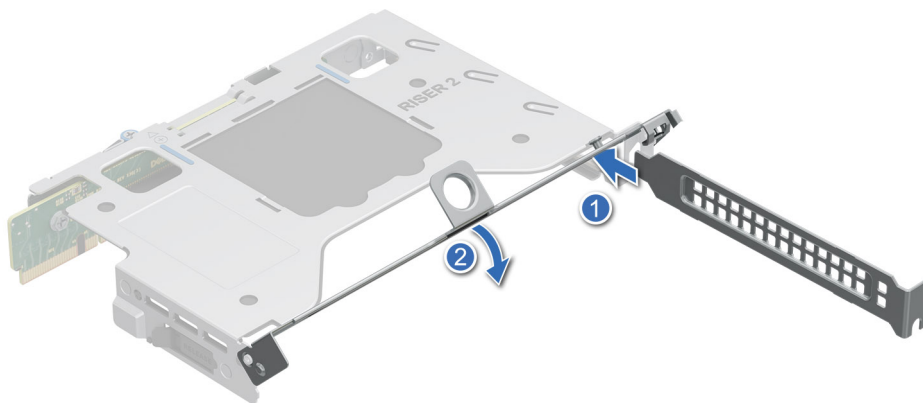


Figure 30. Installing the expansion card filler bracket

4. Using the Phillips 1 screwdriver, loosen the captive screws. Using both hands, hold the PCIe card by the edges and pull the card away from the riser slot.

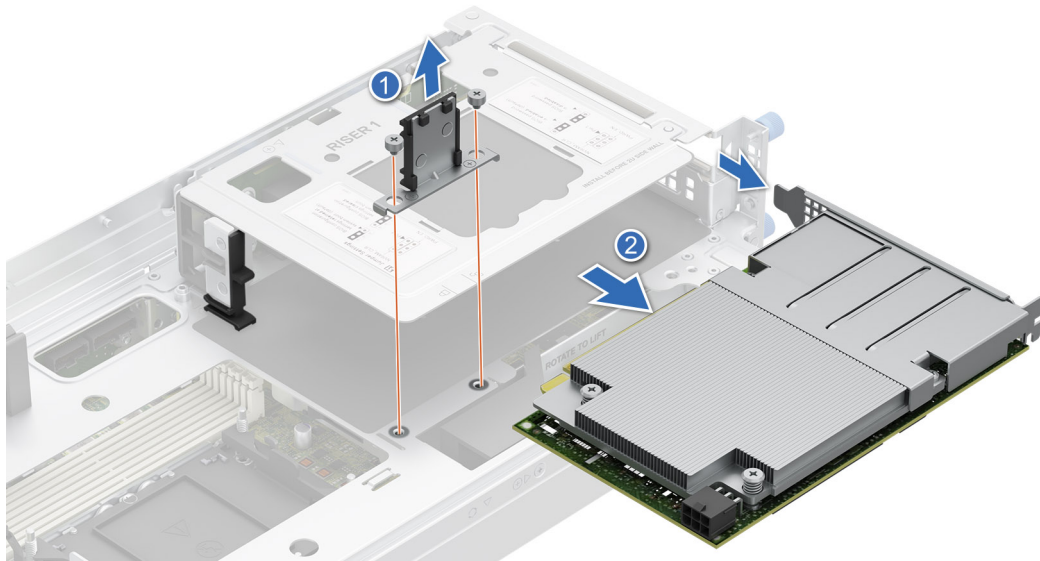


Figure 31. Removing the Dell 100GbE QSFP28 card from Riser 1

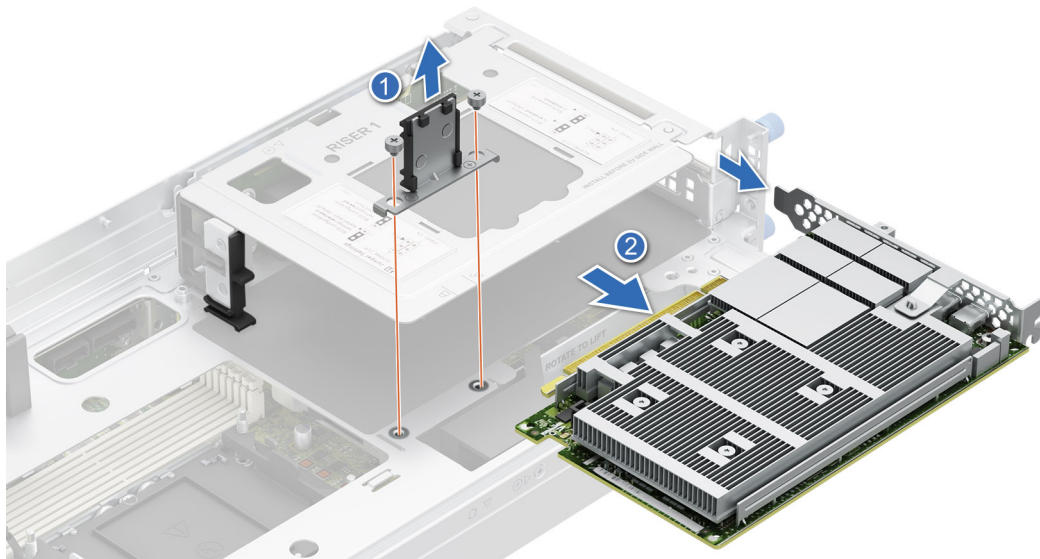


Figure 32. Removing the Nokia Cloud RAN SmartNIC 2x QSFP56-DD card from Riser 1

Next steps

Replace the PCIe card on riser.

Installing the PCIe card on riser

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).
3. [Remove the sled cover](#).

Steps

1. Rotate the riser plate up and remove the expansion card filler bracket by sliding it out of the riser.

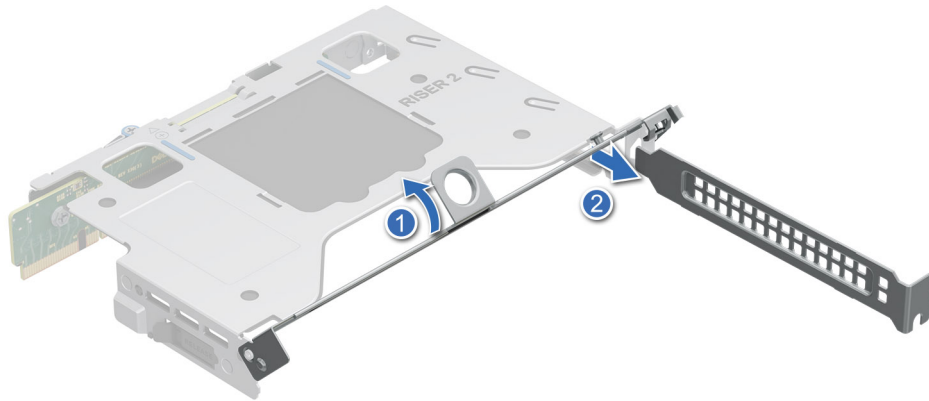


Figure 33. Removing the expansion card filler bracket

2. Using both hands, insert the PCIe card into the riser slot till it clicks into place.

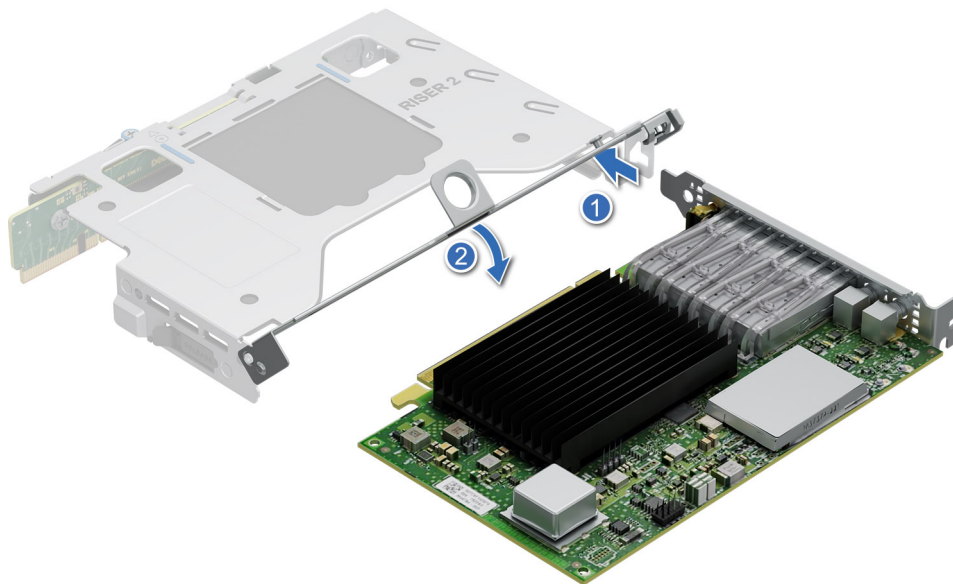


Figure 34. Installing the PCIe card on riser

3. Using both hands, insert the PCIe card into the riser slot till it clicks into place. Using the Phillips 1 screwdriver, tighten the captive screws to secure the card into the riser.

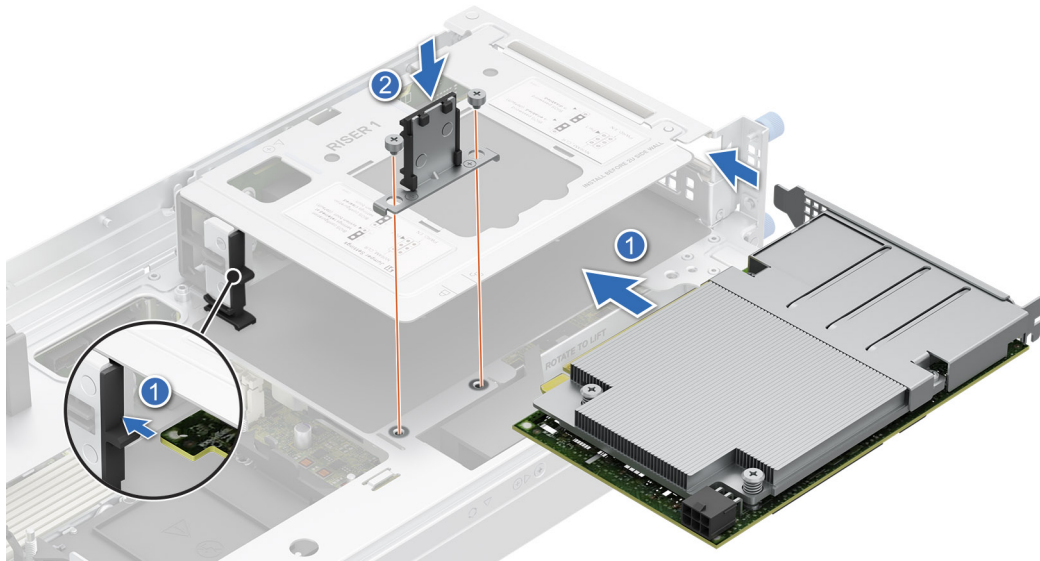


Figure 35. Installing the Dell 100GbE QSFP28 card into riser 1

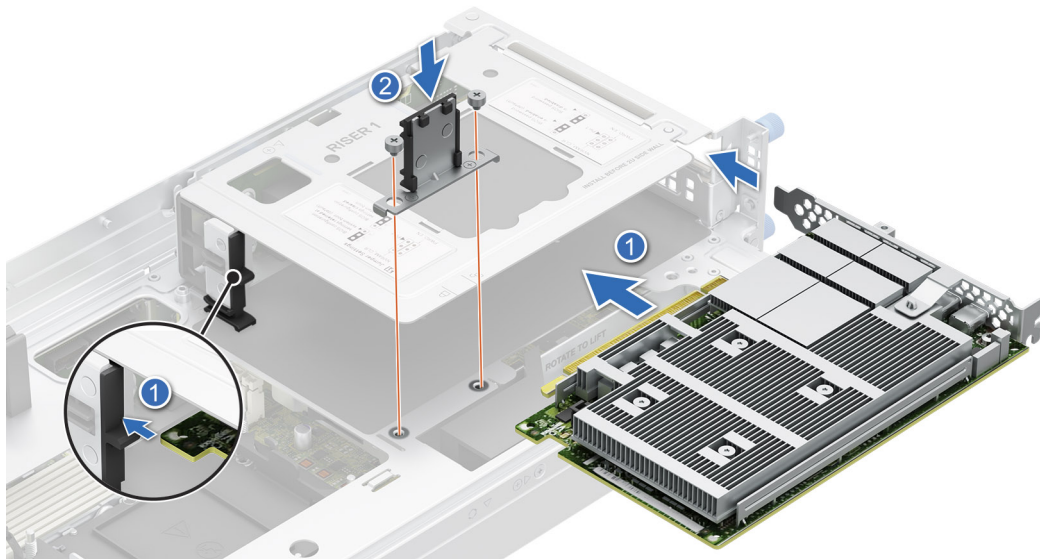


Figure 36. Installing the Nokia Cloud RAN SmartNIC 2x QSFP56-DD card into the riser 1

4. Rotate the riser plate down to secure the PCIe card on the riser.

Next steps

Install the riser on the system board.

BOSS-N1 card

Installing the BOSS-N1 card

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

Steps

1. Press the latch on the system board to unlock the BOSS-N1 card from the system.
2. Pull the blue pull tab to remove the BOSS-N1 card from the slot on the system board.

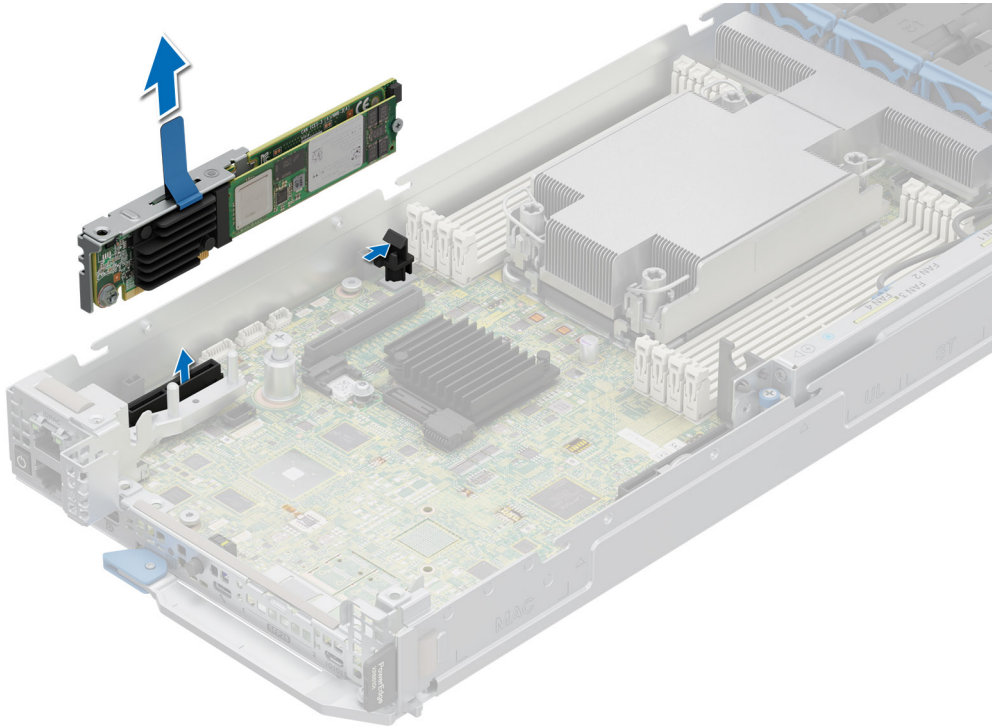


Figure 37. Removing the BOSS-N1 card

Next steps

Follow the procedure listed in [Replace the BOSS-N1 card](#).

Installing the BOSS-N1 card

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

Steps

1. Align the notch on the BOSS-N1 card with the slot on the system board.
2. Press the BOSS-N1 card and insert it firmly until the card is fully seated in the slot and locked to the latch on the system board.

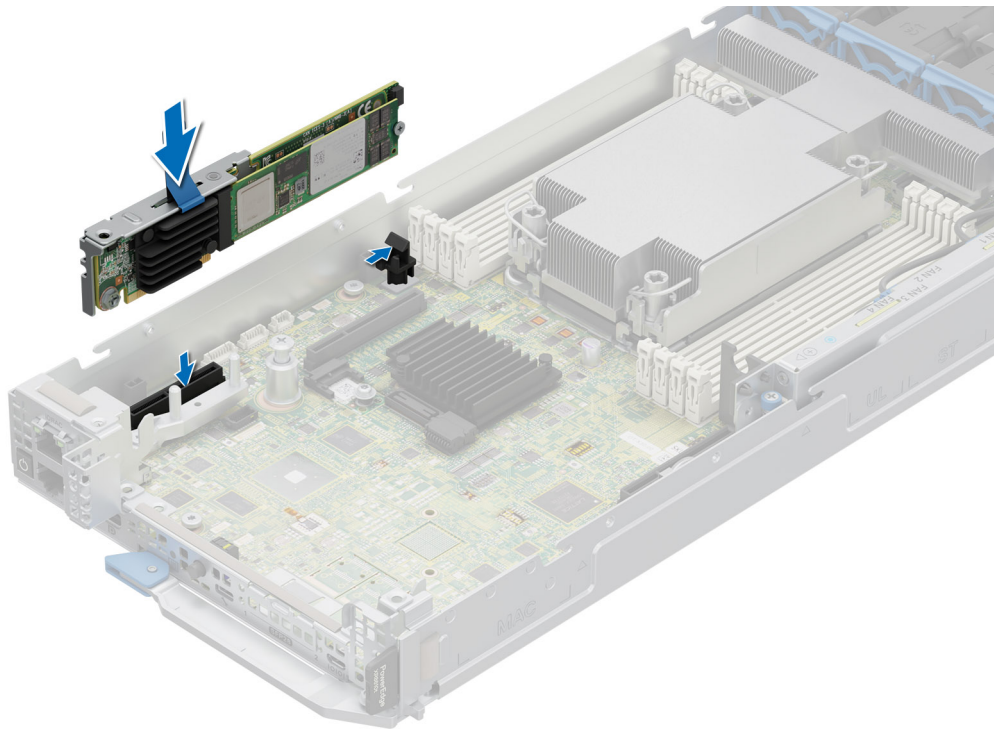


Figure 38. Installing the BOSS-N1 card

Next steps

Follow the procedure listed in [After working inside your system](#).

Removing the M.2 SSD module from the BOSS-N1 card

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

Steps

1. Remove the screw that is on the BOSS-N1 card using Philips 2 screwdriver.
2. Pull the M.2 SSD module from the M.2 slot on the BOSS-N1 card.

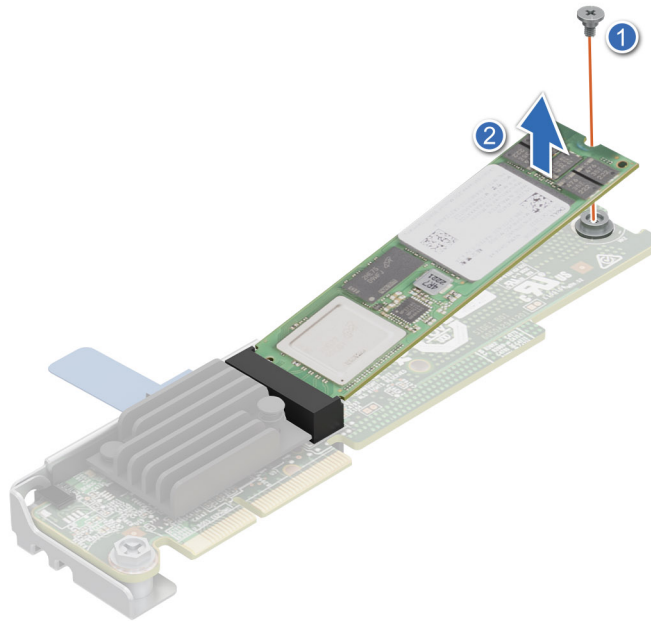


Figure 39. Removing the M.2 SSD module

Next steps

Replace the M.2 SSD module.

Installing the M.2 SSD module on the BOSS-N1 card

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

Steps

1. Align the M.2 NVMe module at an angle with the M.2 direct riser connector on BOSS-N1 card.
2. Insert the M.2 NVMe module firmly until it is fully seated in the M.2 direct riser connector.
3. Replace the screw and tighten it to secure the M.2 SSD module on the BOSS-N1 card.

NOTE: The BOSS-N1 card can accommodate two M.2 SSD modules, repeat the same procedure to install the second M.2 SSD module.

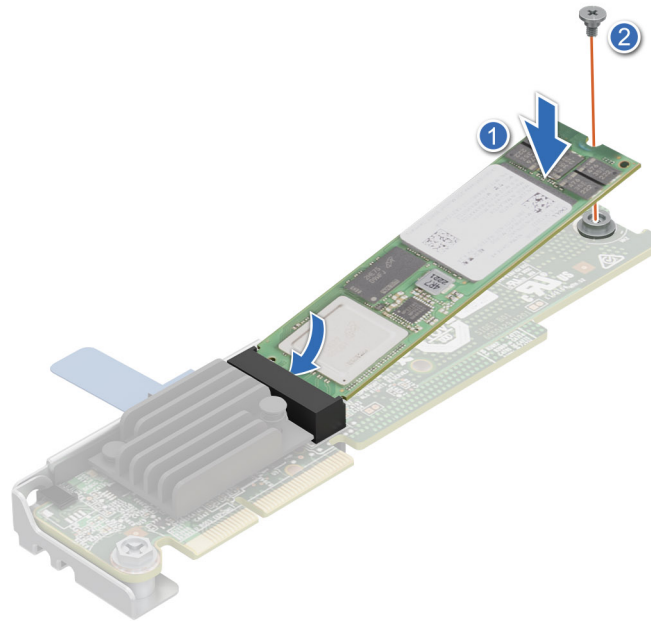


Figure 40. Installing the M.2 SSD module

Next steps

1. [Installing the BOSS-N1 card.](#)
2. Follow the procedure listed in the [After working inside your system.](#)

Power distribution board

This is a service technician replaceable part only.

Removing the 1U power distribution board

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions.](#)
2. Follow the procedure listed in [Before working inside your system.](#)
3. Disconnect the cables that are connected from cooling fans and system board to the power distribution board (PDB).

(i) NOTE: Observe the routing of the cable as you remove it from the system.

Steps

1. Using a Phillips 2 screwdriver, remove the screws that secure the PDB to the system.

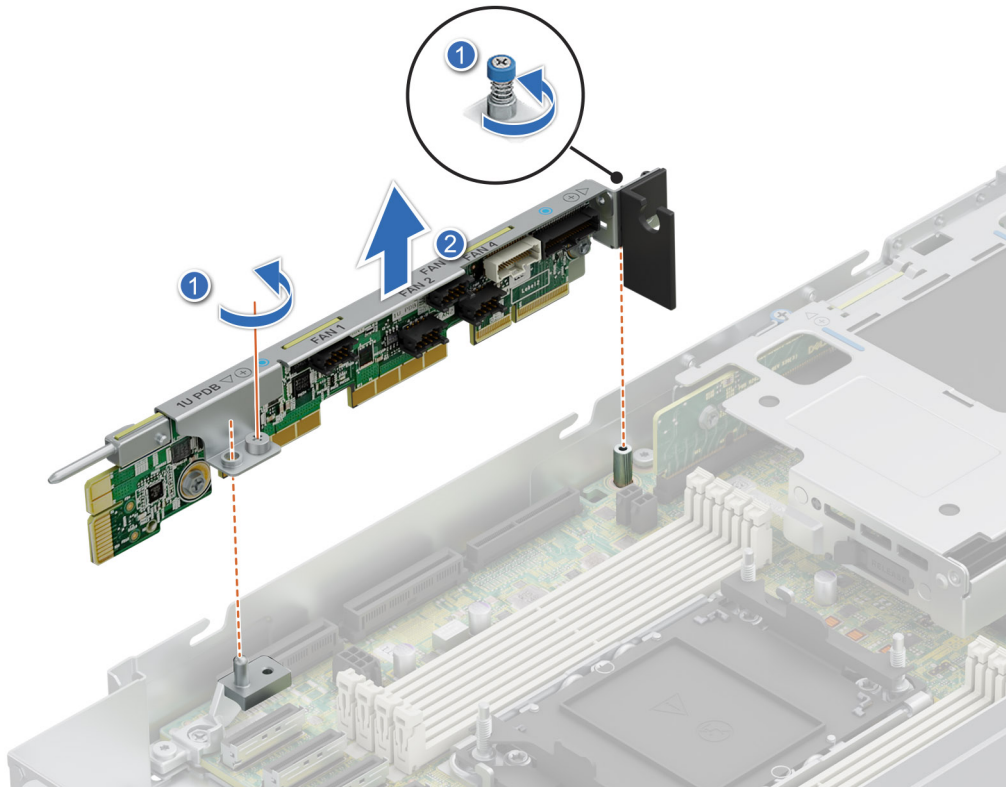


Figure 41. Removing the power distribution board

2. Lift the board to remove it from the system.

Next steps

Replace the power distribution board.

Installing the power distribution board

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

Steps

1. Align the slots of the Power distribution board (PDB) with the fix hook on the 1U sled.
2. Using a Phillips 2 screwdriver, tighten the screws to secure the PDB on the 1U sled.

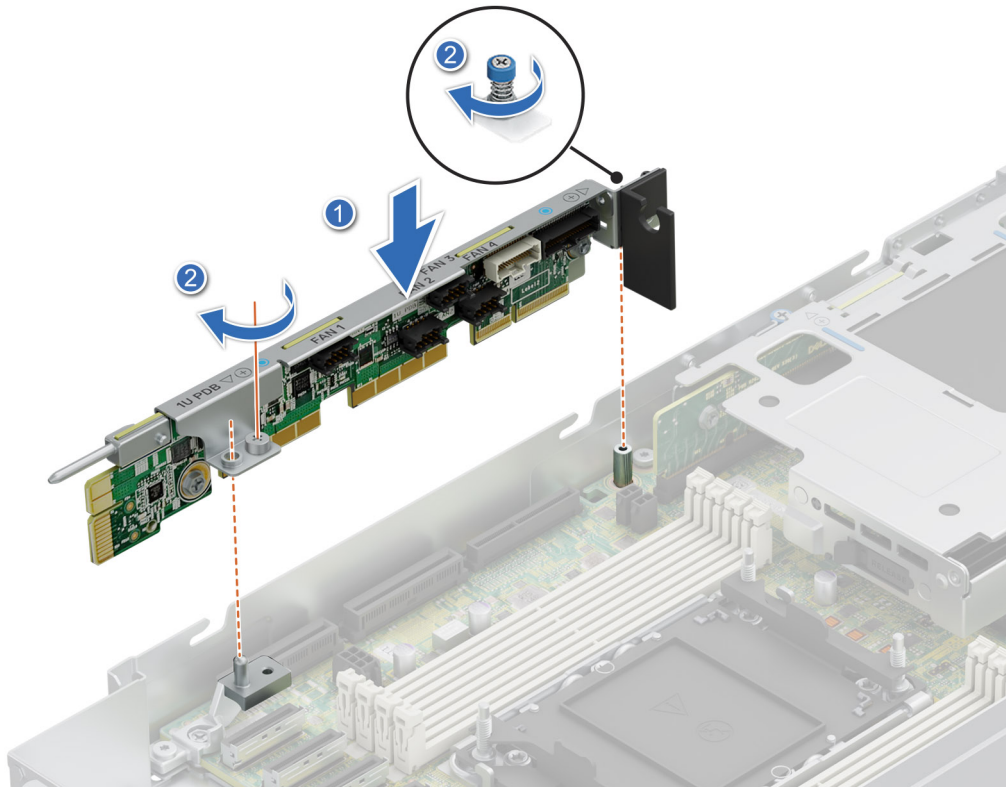


Figure 42. Installing the power distribution board

Next steps

Connect the cables that are connected from cooling fans and system board to the power distribution board (PDB).

System memory

System memory guidelines

The PowerEdge XR8610t system supports DDR5 registered DIMMs (RDIMMs). System memory holds the instructions that are performed by the processor.

Your system memory is organized into eight channels(one memory slot per channel).

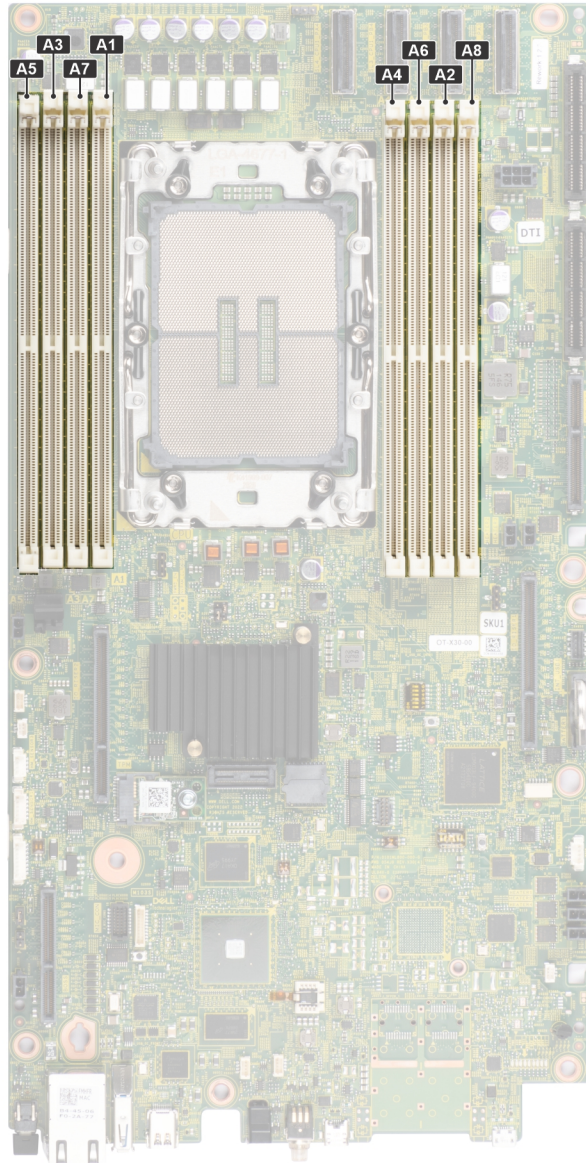


Figure 43. Memory channels

Memory channels are organized as follows:

Table 59. Memory channels

Processor	Channel A	Channel B	Channel C	Channel D	Channel E	Channel F	Channel G	Channel H
Processor 1	Slots A1	Slots A7	Slots A3	Slots A5	Slots A4	Slots A6	Slots A2	Slots A8

Table 60. Supported memory matrix

DIMM type	Rank	Capacity	DIMM rated voltage	Operating Speed
				1 DIMM per channel (DPC)
RDIMM	1 R	16 GB	DDR5 (1.1 V)	4800 MT/s
	2 R	32 GB, 64 GB	DDR5 (1.1 V)	4800 MT/s

NOTE: The processor may reduce the performance of the rated DIMM speed.

General memory module installation guidelines

To ensure optimal performance of your system, observe the following general guidelines when configuring your system memory. If your system's memory configuration fails to observe these guidelines, your system might not boot, stop responding during memory configuration, or operate with reduced memory.

The memory bus may operate at speeds of 5600 MT/s depending on the following factors:

- System profile selected (for example, Performance, Performance Per Watt Optimized (OS), or Custom [can be run at high speed or lower])
- Maximum supported DIMM speed of the processors
- Maximum supported speed of the DIMMs

NOTE: MT/s indicates DIMM speed in MegaTransfers per second.

The following are the recommended guidelines for installing memory modules:

- All DIMMs must be DDR5.
- If memory modules with different speeds are installed, they operate at the speed of the slowest installed memory module(s).
- Populate memory module sockets only if a processor is installed.
- In **Optimizer Mode**, the DRAM controllers operate independently in the 64-bit mode and provide optimized memory performance.

Table 61. Memory population rules

Processor	Memory population	Memory population information
Single processor	A{1}, A{2}, A{3}, A{4}, A{5}, A{6}, A{7}, A{8}	8 DIMMs are supported per system.

- Not more than two DIMM part numbers allowed in the system.
- x4 and x8 DRAM based memory modules can be mixed.
- For best performance, populate all memory channels equally (8DIMMs per CPU) using identical DIMMs.
- Supported total number of RDIMMs in system: 2DIMMs, 4DIMMs, 6DIMMs, 8DIMMs.
- 3 DIMMs, 5 DIMMs, 7DIMMs configurations are not supported.
- Population order requires the largest capacity DIMM be placed first. For example, if we are populating with 32GB and 64GB RDIMMs, we would populate 64GB RDIMMs first.

Removing a memory module

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

WARNING: The memory modules are hot to touch for some time after the system has been powered off. Allow the memory modules to cool before handling them.

NOTE: To ensure proper system cooling, memory module blanks must be installed in any memory socket that is not occupied. Remove memory module blanks only if you intend to install memory modules in those sockets.

Steps

1. Locate the appropriate memory module socket.
2. To release the memory module from the socket, simultaneously press the ejectors on both ends of the memory module socket to fully open.

CAUTION: Handle each memory module only by the card edges, ensuring not to touch the middle of the memory module or metallic contacts.

3. Lift the memory module away from the system.

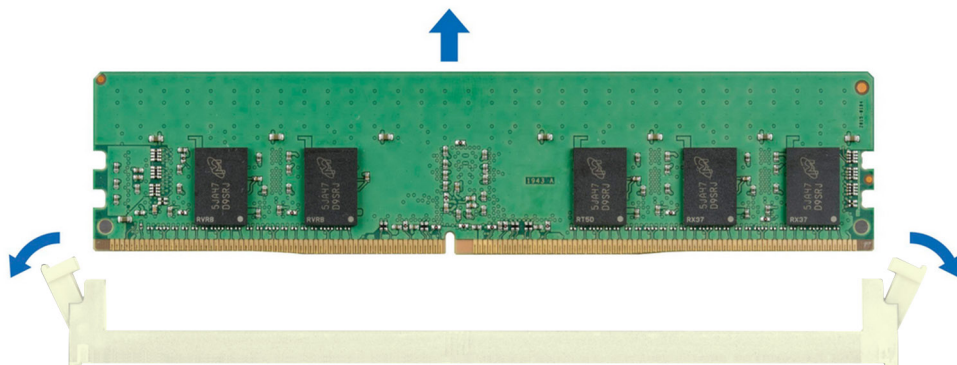


Figure 44. Removing a memory module

Next steps

1. [Installing the memory module.](#)
2. If you are removing the memory module permanently, install a memory module blank. The procedure to install a memory module blank is similar to that of the memory module.

Installing a memory module

Prerequisites

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).

Steps

1. Locate the appropriate memory module socket.

CAUTION: Handle each memory module only by the card edges, ensuring not to touch the middle of the memory module or metallic contacts.

2. Align the edge connector of the memory module with the alignment key of the memory module socket, and insert the memory module in the socket.

CAUTION: To prevent damage to the memory module or the memory module socket during installation, do not bend or flex the memory module; insert both ends of the memory module simultaneously.

NOTE: The memory module socket has an alignment key that enables you to install the memory module in the socket in only one orientation.

CAUTION: Do not apply pressure at the center of the memory module; apply pressure at both ends of the memory module evenly.

3. Press the memory module with your thumbs until the ejectors firmly click into place. When the memory module is properly seated in the socket, the levers on the memory module socket align with the levers on the other sockets that have memory modules that are installed.

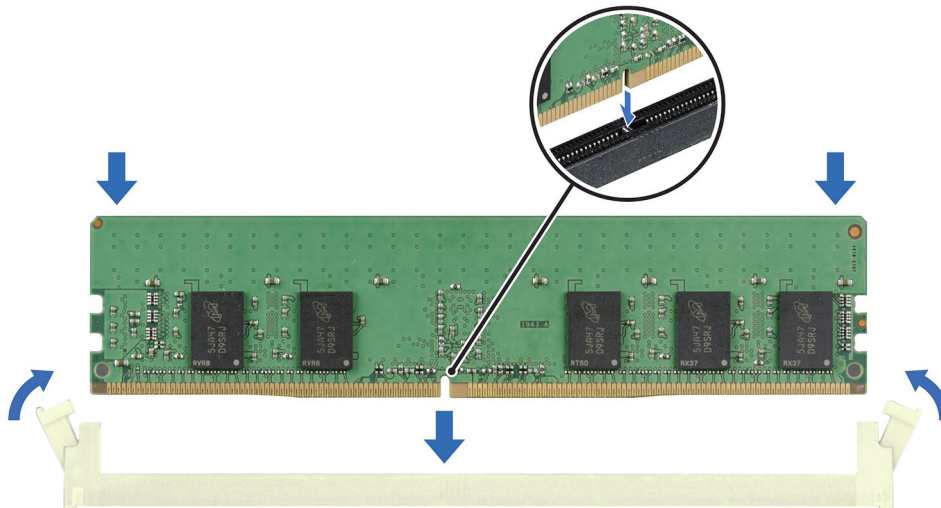


Figure 45. Installing a memory module

Next steps

1. Follow the procedure listed in [After working inside your system](#).
2. To verify if the memory module has been installed properly, press F2 and navigate to **System Setup Main Menu > System BIOS > Memory Settings**. In the **Memory Settings** screen, the System Memory Size must reflect the updated capacity of the installed memory.
3. If the System Memory Size is incorrect, one or more of the memory modules may not be installed properly. Ensure that the memory modules are firmly seated in their sockets.
4. Run the system memory test in system diagnostics.

Processor and heat sink module

This is a service technician replaceable part only.

Removing the processor and heat sink module

Prerequisites

1. Follow the safety guidelines listed in the [Safety instructions](#).
2. Follow the procedure listed in the [Before working inside your system](#).
 - NOTE:** The heat sink and processor are hot to touch for some time after the system has been powered off. Allow the heat sink and processor to cool down before handling them.
3. [Remove the sled cover](#).
4. [Remove the memory modules](#).

Steps

1. Ensure all four anti-tilt wires are in the locked position (outward position), and then using a Torx T30 screwdriver, loosen the captive nuts on the processor heat sink module (PHM) in the order that is mentioned below:
 - a. Loosen the first nut three turns.
 - b. Loosen the nut diagonally opposite to the nut you loosened first.
 - c. Repeat the procedure for the remaining two nuts.

d. Return to the first nut and loosen it completely.

i **NOTE:** Ensure that the anti-tilt wires on the PHM are in locked position when loosening the captive nuts.

2. Set all the anti-tilt wires to unlocked position (inward position).

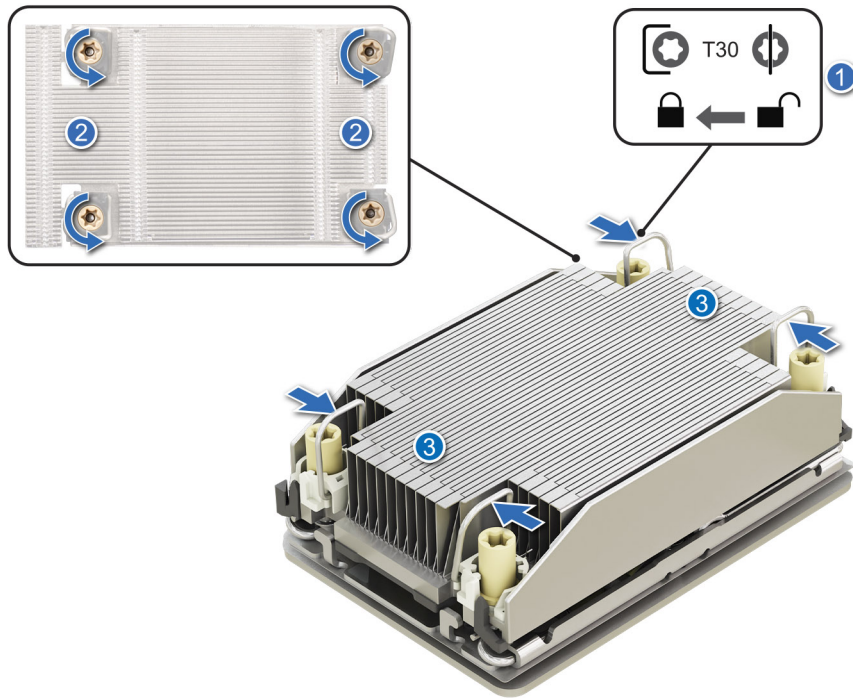


Figure 46. Removing the processor heat sink module

3. Lift the PHM from the system and set the PHM aside with the processor side facing up.

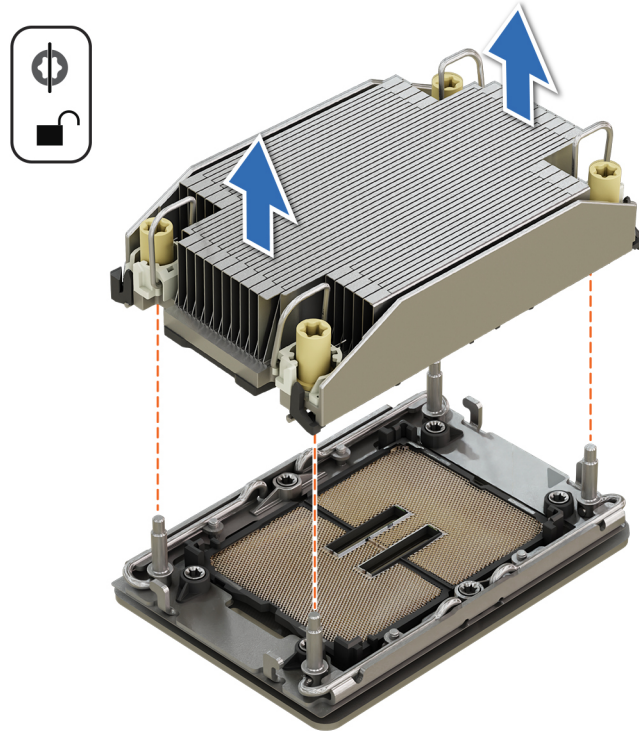


Figure 47. Removing a heat sink

Next steps

If you are removing a faulty heat sink [replace the heat sink](#), if not [remove the processor](#).

Removing the processor

Prerequisites

WARNING: Remove the processor from processor and heat sink module (PHM) only if you are replacing the processor or heat sink.

1. Follow the safety guidelines listed in the [Safety instructions](#).
2. Follow the procedure listed in the [Before working inside your system](#).
3. [Remove the sled cover](#).
4. [Remove the memory modules](#).
5. [Remove the processor heat sink](#).

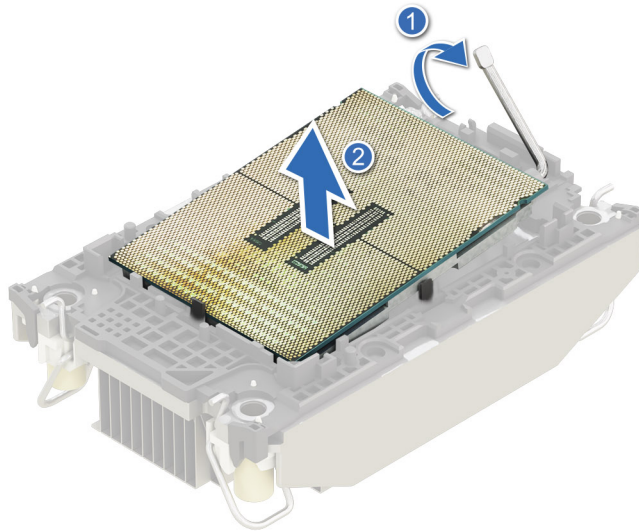
CAUTION: You may find the CMOS battery loss or CMOS checksum error that is displayed during the first instance of powering on the system after the processor or system board replacement which is expected. To fix this, simply go to setup option to configure the system settings.

Steps

1. Place the heat sink with the processor side facing up.
2. Using your thumb, lift the thermal interface material (TIM) break lever to release the processor from the TIM and retaining clip.
3. Holding the processor by the edges, lift the processor away from the retaining clip.

NOTE: Ensure to hold the retaining clip to the heat sink as you lift the TIM break lever.

Figure 48. Removing the processor



NOTE: Ensure to return the TIM break lever back to its original position.

4. Using your thumb and index finger, first hold the retaining clip release tab at the pin 1 connector, pull out the tip of the retaining clip release tab, and then lift the retaining clip partially from the heat sink.
5. Repeat the procedure at the remaining three corners of the retaining clip.
6. After all the corners are released from the heat sink, lift the retaining clip from the pin 1 corner of the heat sink.

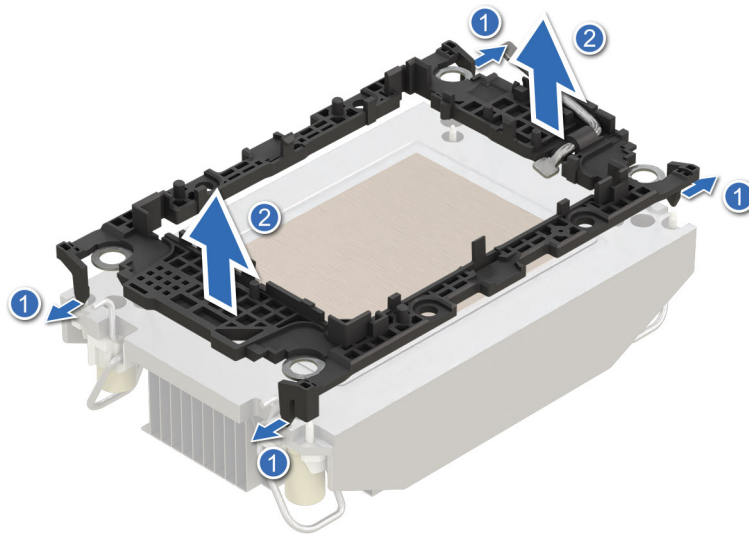


Figure 49. Removing the retaining clip

Next steps

Replace the processor.

Installing the processor

Prerequisites

1. Follow the safety guidelines listed in the [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).
3. [Remove the sled cover](#).

4. Remove the memory modules.
5. Remove the processor.

Steps

1. Place the processor in the processor tray.

i **NOTE:** Ensure the pin 1 indicator on the processor tray is aligned with the pin 1 indicator on the processor.

2. Place the retaining clip on top of the processor in the processor tray aligning pin 1 indicator on the processor.

i **NOTE:** Ensure the pin 1 indicator on the retaining clip is aligned with the pin 1 indicator on the processor before placing the retaining clip on the processor.

i **NOTE:** Before you install the heat sink, ensure to place the processor and retaining clip in the tray.

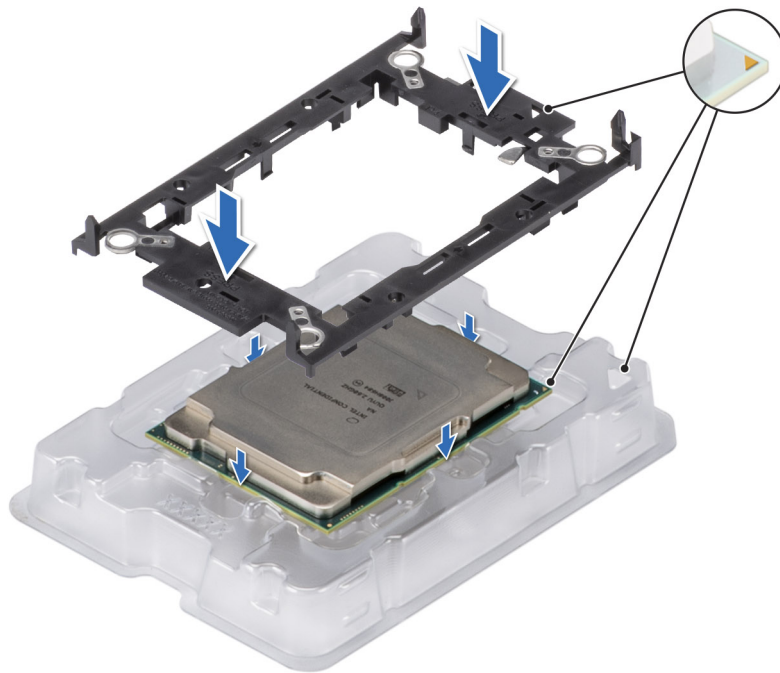


Figure 50. Installing the retaining clip

3. Align the processor with a retaining clip, by using your fingers press the retaining clip on all the four sides until it clicks into place.

i **NOTE:** Ensure that the processor is securely latched to the retaining clip.

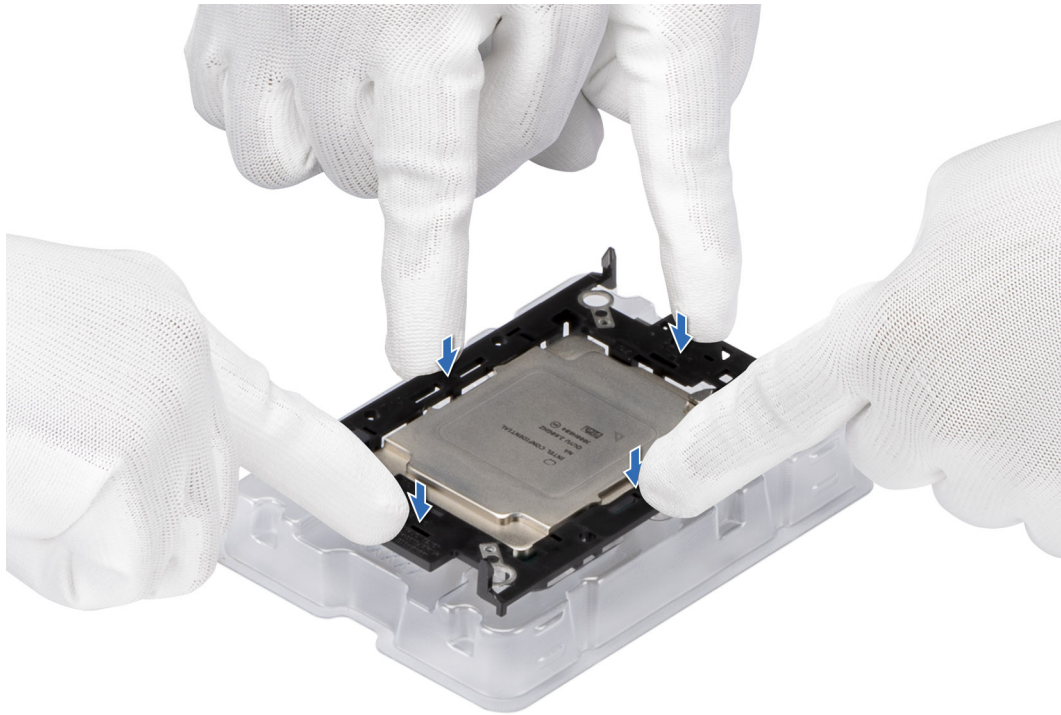


Figure 51. Press the retaining clip on the four sides

4. If you are using an existing heat sink, remove the thermal grease from the heat sink by using a clean lint-free cloth.
5. Apply the thermal grease in a thin spiral design on the bottom of the heat sink.

CAUTION: Applying too much thermal grease can result in excess grease coming in contact with and contaminating the processor socket.

NOTE: The thermal grease syringe is intended for single use only. Dispose the syringe after you use it.

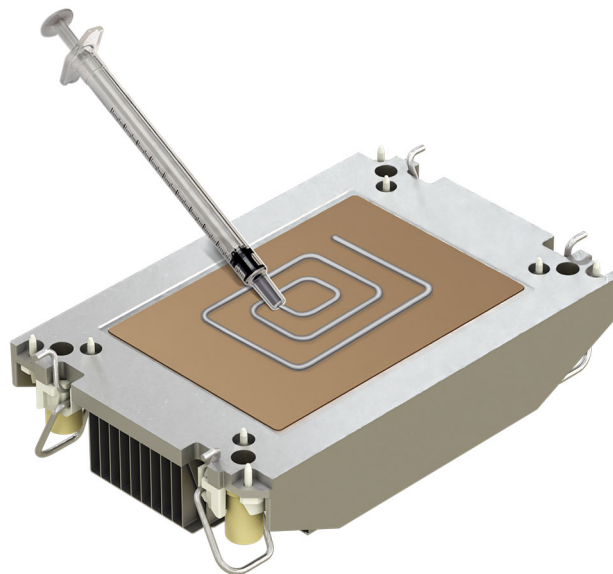


Figure 52. Applying thermal grease

6. For a new heat sink, pull and remove the plastic cover from the base of the heat sink.

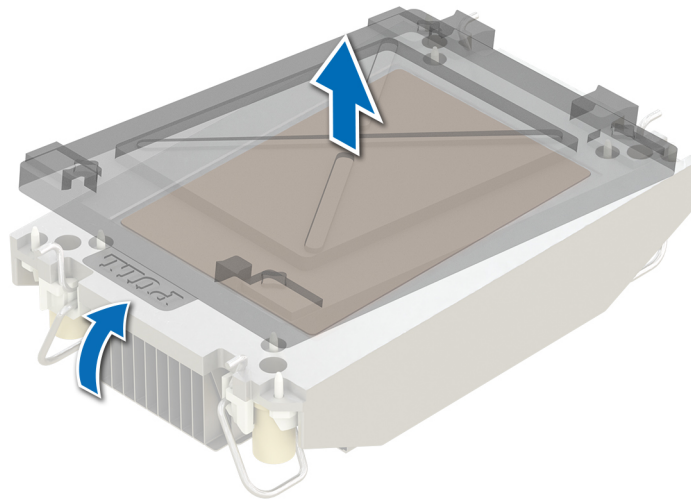


Figure 53. Removing the cover

7. Place the heat sink on the processor and press the base of the heat sink until the retaining clip locks onto the heat sink at all the four corners.

CAUTION: To avoid damaging the fins on the heat sink, do not press down on the heat sink fins.

NOTE:

- Ensure latching features on retaining clip, and heat sink are aligned during assembly.
- Ensure that the pin 1 indicator on the heat sink is aligned with the pin 1 indicator on the retaining clip before placing the heat sink onto the retaining clip.

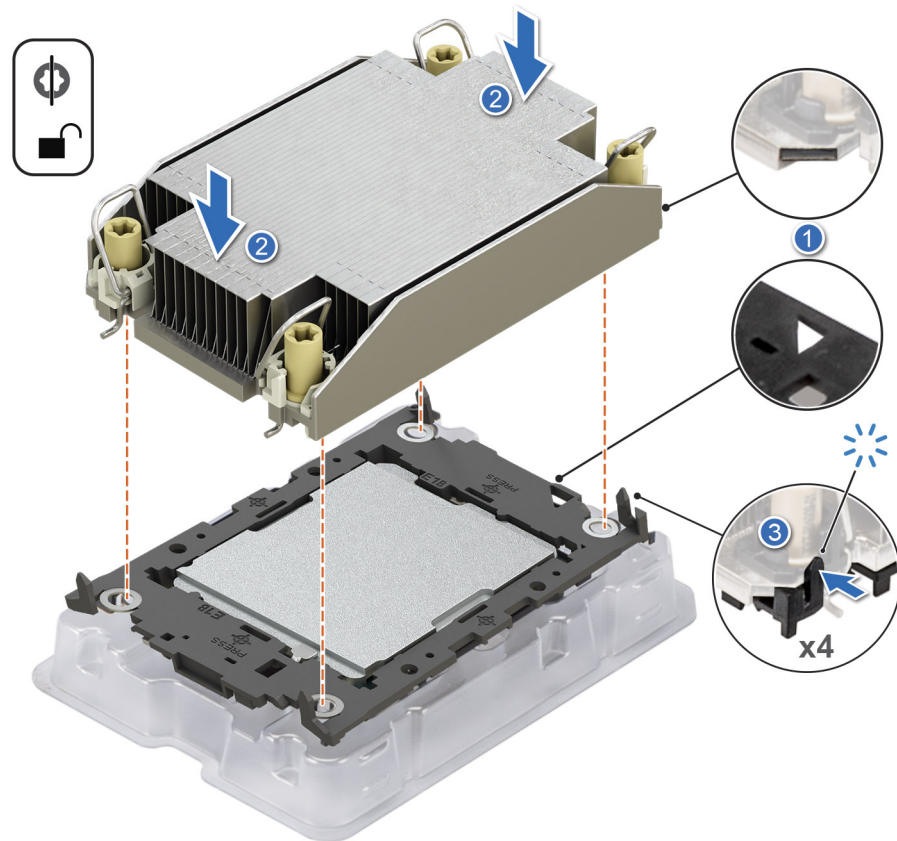


Figure 54. Installing the heat sink onto the processor

Next steps

1. Install the processor heat sink module.
2. Follow the procedure listed in [After working inside your system](#).

Installing the processor and heat sink module

Prerequisites

Never remove the heat sink from a processor unless you intend to replace the processor or heat sink. The heat sink is necessary to maintain proper thermal conditions.

1. Follow the safety guidelines listed in the [Safety instructions](#).
2. Follow the procedure listed in the [Before working inside your system](#).
3. If installed, remove the processor dust cover.

Steps

1. Set the anti-tilt wires to the unlocked position on the heat sink (inward position).
2. Align the pin 1 indicator of the heat sink to the system board, and then place the processor heat sink module (PHM) on the processor socket.

CAUTION: To avoid damaging the fins on the heat sink, do not press down on the heat sink fins.

NOTE: Ensure that the PHM is held parallel to the system board to prevent damaging the components.

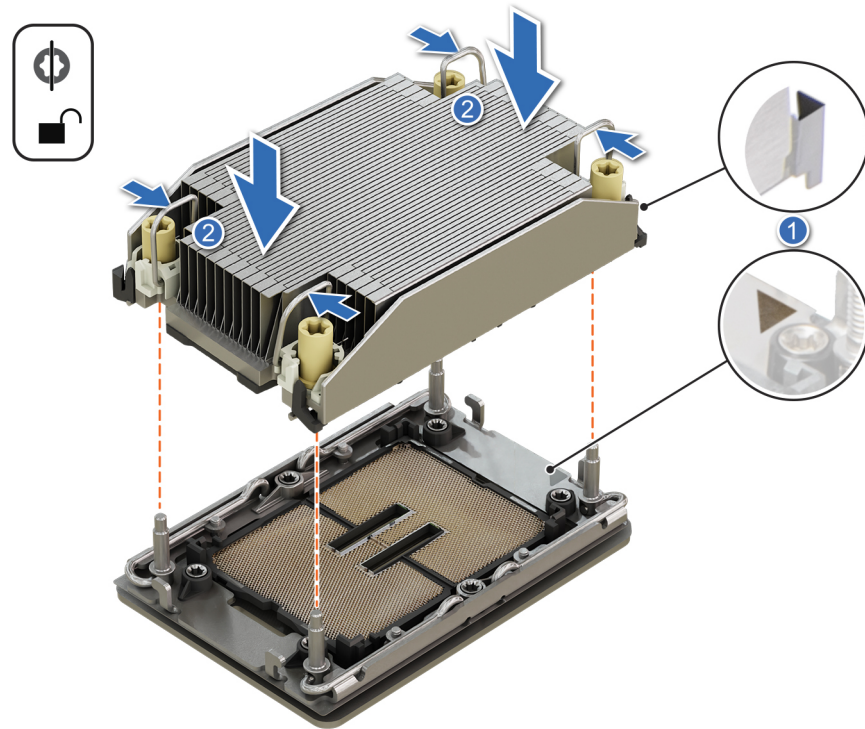


Figure 55. Installing the processor heat sink

3. Set the anti-tilt wires to the locked position (outward position), and then using the Torx T30 screwdriver, tighten the captive nuts (8 in-lbf) on the heat sink in the order below:
 - a. In a random order, tighten the first nut three turns.
 - b. Tighten the nut diagonally opposite to the nut that you tighten first.
 - c. Repeat the procedure for the remaining two nuts.
 - d. Return to the first nut to tighten it completely.
 - e. Check all the nuts to ensure they are firmly secured.

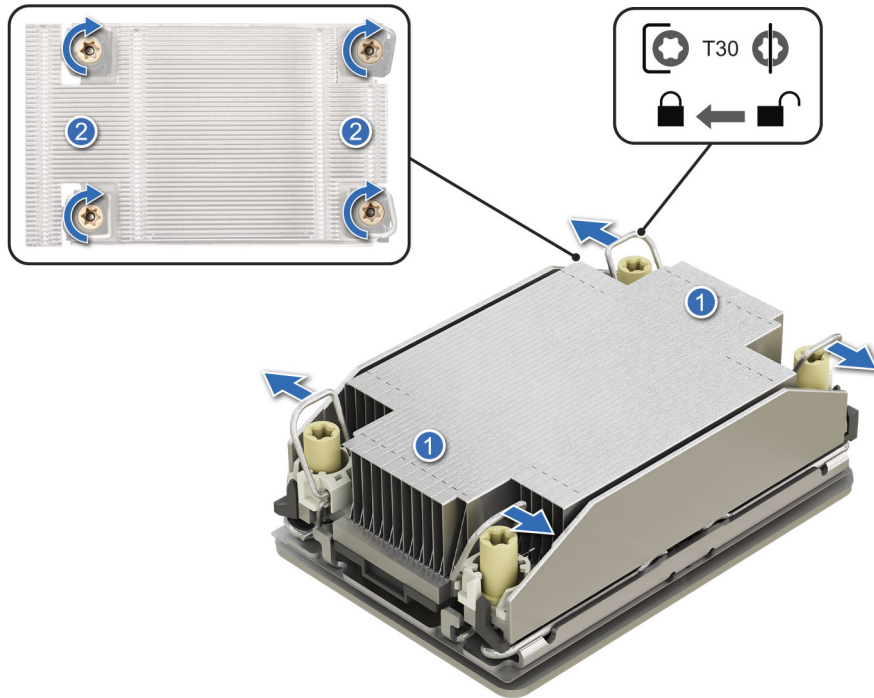


Figure 56. Set the anti-tilt wires to the locked position and tightening the nuts

Next steps

1. [Install the memory modules.](#)
2. [Install the sled cover.](#)
3. Follow the procedure listed in the [After working inside your system.](#)

System battery

This is a service technician replaceable part only.

Replacing the system battery

Prerequisites

⚠ WARNING: There is a danger of a new battery exploding if it is incorrectly installed. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions. See the Safety instructions that came with your system for more information.

1. Follow the safety guidelines listed in [Safety instructions.](#)
2. Follow the procedure listed in [Before working inside your system.](#)

Steps

1. To remove the battery:
 - a. Use a plastic scribe to pry out the system battery.

⚠ CAUTION: To avoid damage to the battery connector, you must firmly support the connector while installing or removing a battery.

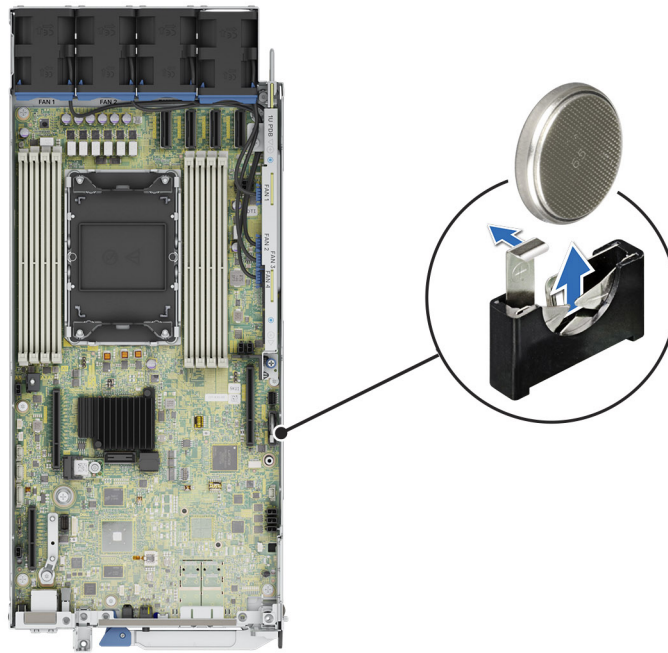


Figure 57. Removing the system battery

2. To install a new system battery:
 - a. Hold the battery with the positive side facing up and slide it under the securing tabs.
 - b. Press the battery into the connector until it snaps into place.

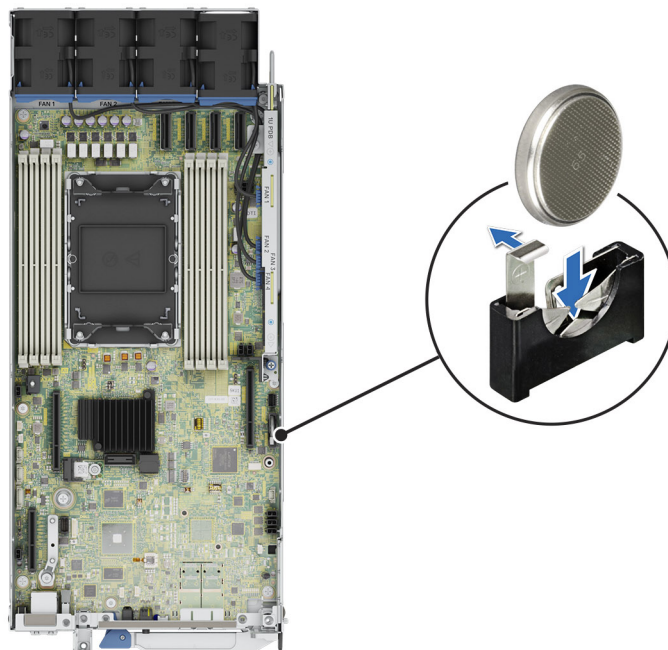


Figure 58. Installing the system battery

Next steps

1. Follow the procedure listed in the [After working inside your system](#).
2. Confirm that the battery is operating properly, by performing the following steps:
 - a. Enter the System Setup, while booting, by pressing F2.
 - b. Enter the correct time and date in the System Setup **Time** and **Date** fields.


- c. **Exit** the System Setup.
- d. To test the newly installed battery, remove the system from the enclosure for at least an hour.
- e. Reinstall the system into the enclosure after an hour.
- f. Enter the System Setup and if the time and date are still incorrect, see [Getting help](#) section.


System board

This is a service technician replaceable part only.


Removing the system board

Prerequisites

 **CAUTION:** If you are using the Trusted Platform Module (TPM) with an encryption key, you may be prompted to create a recovery key during program or System Setup. Be sure to create and safely store this recovery key. If you replace this system board, you must supply the recovery key when you restart your system or program before you can access the encrypted data on your drives.

 **CAUTION:** To avoid damage to the system board, ensure that the system board does not touch the side walls of the sled chassis, while sliding the system board into the sled.

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).
3. Remove the following components:
 - a. [Sled cover](#)
 - b. [Cooling fans](#)
 - c. [Power distribution board](#)
 - d. [Riser 2](#)
 - e. [Memory modules](#)
 - f. [Heatsink](#)
 - g. [Processor](#)
 - h. [Trusted platform module \(TPM\)](#).

 **NOTE:** The TPM Module must be replaced only while installing a new system board.

- i. Disconnect all cables from the system board.

 **CAUTION:** Take care not to damage the system identification button while removing the system board from the system.

Steps

1. Using a Phillips 2 screwdriver, remove the screws that secure the system board to the chassis.
2. To disengage the ports from the slots on the chassis, slide the system board toward the rear of the chassis. Lift the system board out of the chassis.

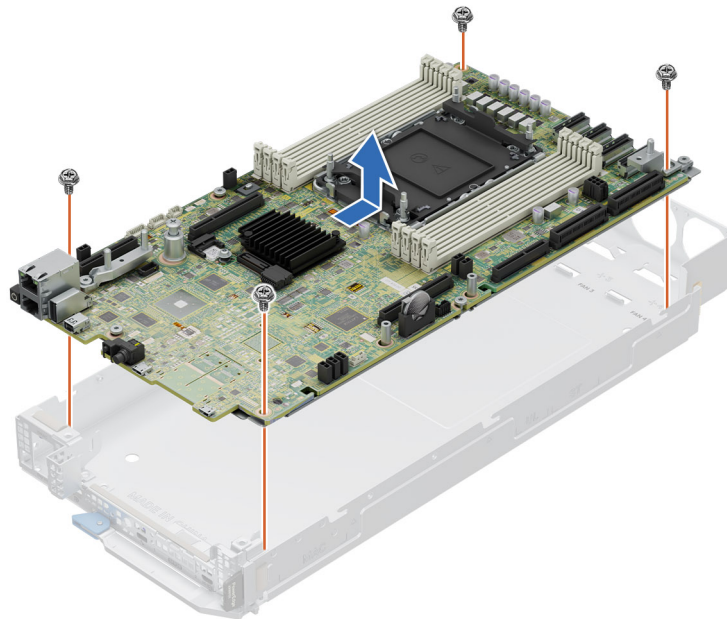


Figure 59. Removing the system board

Next steps

Installing the system board.

Installing the system board

Prerequisites

NOTE: Before replacing the system board, replace the old iDRAC MAC address label in the Information tag with the iDRAC MAC address label of the replacement system board..

1. Follow the safety guidelines listed in [Safety instructions](#).
2. Follow the procedure listed in [Before working inside your system](#).
3. If you are replacing the system board, remove all the components that are listed in [removing the system board](#) section.

CAUTION: To avoid damage to the system board, ensure that the system board does not touch the side walls of the sled chassis, while sliding the system board into the sled.

Steps

1. Unpack the new system board assembly.

CAUTION: Do not lift the system board by holding a memory module, processor, or other components.

CAUTION: Take care not to damage the system identification button while placing the system board into the chassis.

2. Holding the system board by the edges, lower the system board into the chassis.
3. Incline the system board at an angle and align the connectors on the system board with the slots on the front of the chassis until the connectors are firmly seated in the slots.
4. Using a Phillips 2 screwdriver, tighten the screws that secure the system board to the chassis.

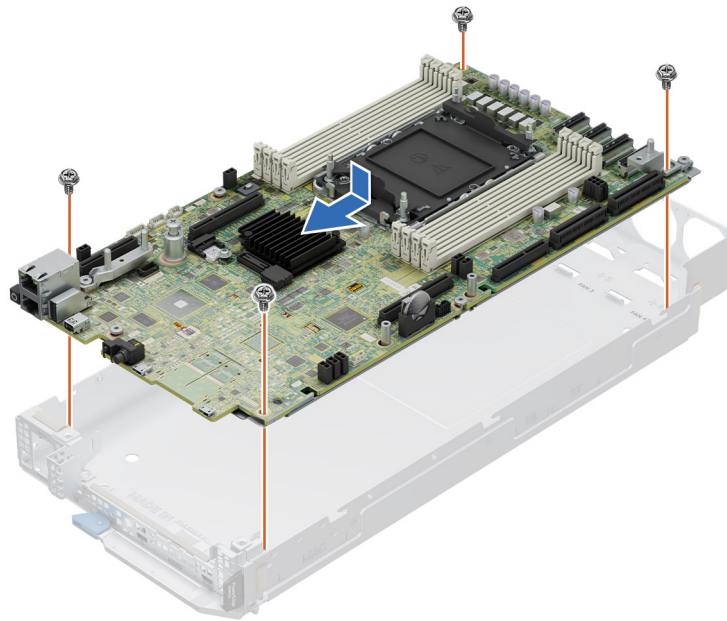


Figure 60. Installing the system board

Next steps

1. Replace the following components:
 - a. [Trusted platform module \(TPM\)](#).
i **NOTE:** The TPM Module must be replaced only while installing a new system board.
 - b. [Processor](#)
 - c. [Heatsink](#)
 - d. [Memory modules](#)
 - e. [Riser 2](#)
 - f. [Power distribution board](#)
 - g. [Cooling fans](#)
 - h. [BOSS-N1 card](#)
2. Reconnect all cables to the system board.
i **NOTE:** Ensure that the cables inside the system are routed along the chassis wall and secured using the cable securing bracket.
3. Ensure that you perform the following steps:
 - a. Use the Easy Restore feature to restore the Service Tag. See the [Restoring the system by using the Easy Restore feature](#) section.
 - b. If the service tag is not backed up in the backup flash device, enter the system service tag manually. See the [Manually update the Service Tag by using System Setup](#) section.
 - c. Update the BIOS and iDRAC versions.
Re-enable the Trusted Platform Module (TPM). See the [upgrading the Trusted Platform Module](#) section.
4. If you are not using Easy Restore, import your new or existing iDRAC Enterprise license. For more information, see the [Integrated Dell Remote Access Controller User's Guide](#)
5. Follow the procedure listed in [After working inside your system](#).

Restoring the system using Easy Restore


The Easy Restore feature enables you to restore your service tag, license, UEFI configuration, and the system configuration data after replacing the system board. All data is backed up in a backup flash device automatically. If BIOS detects a new system board, and the service tag in the backup flash device, BIOS prompts the user to restore the backup information.

About this task


Below is a list of options/steps available:

Steps

1. Restore the service tag, license, and diagnostics information, press **Y**
2. Navigate to the Lifecycle Controller based restore options, press **N**
3. Restore data from a previously created **Hardware Server Profile**, press **F10**

 **NOTE:** When the restore process is complete, BIOS prompts to restore the system configuration data.

4. Restore data from a previously created **Hardware Server Profile**, press **F10**
5. To restore the system configuration data, press **Y**
6. To use the default configuration settings, press **N**

 **NOTE:** After the restore process is complete, system reboots.

Manually update the Service Tag


After replacing a system board, if Easy Restore fails, follow this process to manually enter the Service Tag, using **System Setup**.

About this task

If you know the system service tag, use the **System Setup** menu to enter the service tag.

Steps

1. Power on the system.
2. To enter the **System Setup**, press **F2**.
3. Click **Service Tag Settings**.
4. Enter the service tag.

 **NOTE:** You can enter the service tag only when the **Service Tag** field is empty. Ensure that you enter the correct service tag. Once the service tag is entered, it cannot be updated or changed. Incorrectly entered service tag will lead to system board replacement.

5. Click **OK**.

Trusted Platform Module

This is a service technician replaceable part only.


Upgrading the Trusted Platform Module

Removing the TPM

Prerequisites

NOTE:

- Ensure the operating system is compatible with the TPM version you are installing.
- Ensure that you download and install the latest BIOS firmware on your system.
- Ensure that the BIOS is configured to enable UEFI boot mode.

 **CAUTION:** The TPM plug-in module is cryptographically bound to that particular system board after it is installed. When the system is powered on, any attempt to remove an installed TPM plug-in module breaks the

cryptographic binding, and the removed TPM cannot be installed on another system board. Ensure any keys you have stored on the TPM have been securely transferred.

Steps

1. Locate the TPM connector on the system board. For more information, see [System board connectors](#).
2. Press to hold the module down and remove the screw using the security Torx 8-bit shipped with the TPM module.
3. Slide the TPM module out from its connector.
4. Push the plastic rivet away from the TPM connector and rotate it 90° counterclockwise to release it from the system board.
5. Pull the plastic rivet out of its slot on the system board.

Installing the TPM

Steps

1. To install the TPM, align the edge connectors on the TPM with the slot on the TPM connector.
2. Insert the TPM into the TPM connector such that the plastic rivet aligns with the slot on the system board.
3. Press the plastic rivet until the rivet snaps into place.

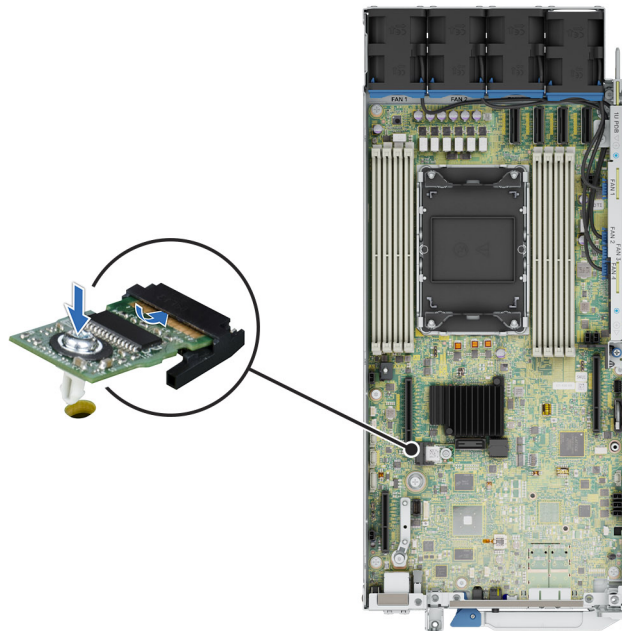


Figure 61. Installing the TPM

Initializing TPM for users

Steps

1. Initialize the TPM.
For more information, see [Initializing the TPM 2.0 for users](#).
2. The **TPM Status** changes to **Enabled, Activated**.

Initializing the TPM 2.0 for users

Steps

1. While booting your system, press F2 to enter System Setup.

2. On the **System Setup Main Menu** screen, click **System BIOS > System Security Settings**.
3. From the **TPM Security** option, select **On**.
4. Save the settings.
5. Restart your system.

Jumpers and connectors

This topic provides some basic and specific information about jumpers and switches. It also describes the connectors on the various boards in the system. Jumpers on the system board help to disable the system and reset the passwords. To install components and cables correctly, you must know the connectors on the system board.

Topics:

- [System board jumpers and connectors](#)
- [System board jumper settings](#)
- [Disabling a forgotten password](#)

System board jumpers and connectors

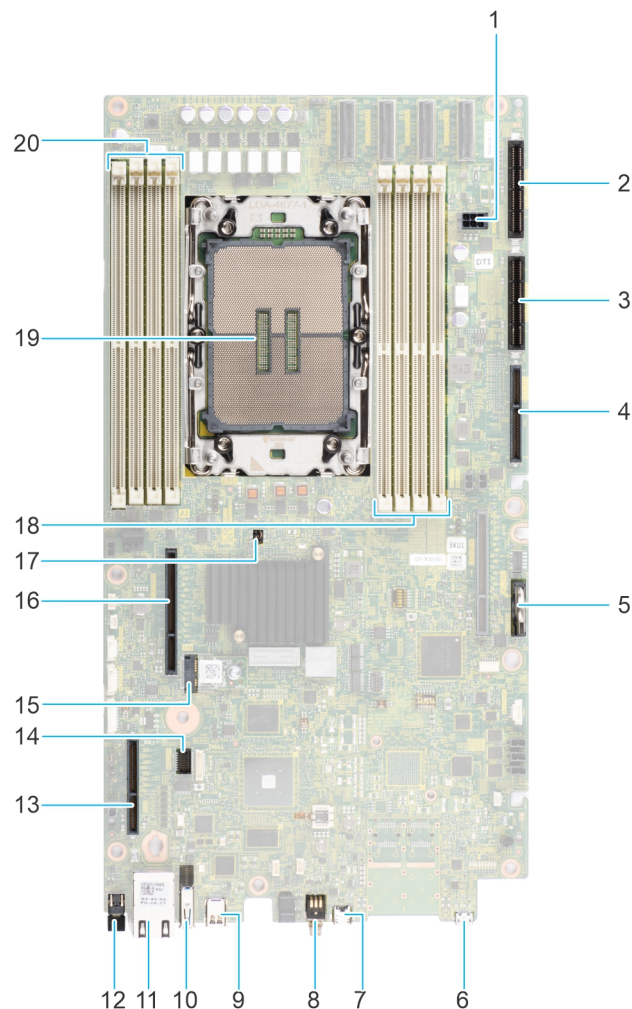


Figure 62. System board connectors

Table 62. System board connectors description





Item	Connector	Description
1	J_R1_PWR	PCIe Extension Power
2	SYS_PWR_CONN1	Power connector 1
3	SYS_PWR_CONN2	Power connector 2
4	PIB Signal	PIB Signal connector
5	Coin cell battery	Coin cell battery
6	Micro-USB Serial	Micro-USB Serial Port
7	iDRAC_DIRECT	iDRAC Direct Port
8	SYS_ID	System ID button
9	Display	Display Port
10	USB	USB 3.0 connector
11	iDRAC RJ45/Dry Input	iDRAC RJ45/Dry Input
12	POWER	Power button
13	BOSS-N1	BOSS-N1 M.2 connector
14	MIC_CON	Smart NIC connector
15	TPM	TPM connector
16	Reserved(IO_RISER2)	Riser 2 connector
17	JUMPER	BIOS password and NVRAM jumper
18	A4, A6, A2, A8	DIMM slots (A4, A6, A2, A8)
19	CPU	Processor socket
20	A5, A3, A7, A1	DIMM slots (A5, A3, A7, A1)

NOTE: J_R1 PWR1 and J_R1_PWR2 is for PCIE Riser1 Slot1 Slimline power and Slot2 Slimline power. They are located on 2U PDB board

System board jumper settings

For information about resetting the password jumper to disable a password, see the [Disabling a forgotten password](#) section.

Table 63. System board jumper settings


Jumper	Setting	Description
PWRD_EN	 2 4 6 (default)	The BIOS password feature is enabled.
	 2 4 6	The BIOS password feature is disabled. The BIOS password is now disabled and you are not allowed to set a new password.
NVRAM_CLR	 1 3 5 (default)	The BIOS configuration settings are retained at system boot.
	 1 3 5	The BIOS configuration settings are cleared at system boot.

CAUTION: You should be cautious when changing the BIOS settings. The BIOS interface is designed for advanced users. Any changes in the setting might prevent your system from starting correctly and may even result in data loss.



Disabling a forgotten password

The software security features of the system include a system password and a setup password. The password jumper enables or disables password features and clears any password(s) currently in use.

Prerequisites

 **CAUTION:** Many repairs may only be done by a certified service technician. You should only perform troubleshooting and simple repairs as authorized in your product documentation, or as directed by the online or telephone service and support team. Damage due to servicing that is not authorized by Dell is not covered by your warranty. Read and follow the safety instructions that are shipped with your product.

Steps

1. Power off the system and all attached peripherals. Disconnect the system from the electrical outlet, and disconnect the peripherals.
2. [Remove the system cover.](#)
3. Move the jumper on the system board from pins 2 and 4 to pins 4 and 6.
4. [Replace the system cover.](#)
 -  **NOTE:** The existing passwords are not disabled (erased) until the system boots with the jumper on pins 4 and 6. However, before you assign a new system and/or setup password, you must move the jumper back to pins 2 and 4.
 -  **NOTE:** If you assign a new system and/or setup password with the jumper on pins 4 and 6, the system disables the new password(s) the next time it boots.
5. Reconnect the peripherals and connect the system to the electrical outlet, and then power on the system.
6. Power off the system.
7. [Remove the system cover.](#)
8. Move the jumper on the system board from pins 4 and 6 to pins 2 and 4.
9. [Replace the system cover.](#)
10. Reconnect the peripherals and connect the system to the electrical outlet, and then power on the system.
11. Assign a new system and/or setup password.

Using system diagnostics

If you experience an issue with the system, run the system diagnostics before contacting Dell for technical assistance. The purpose of running system diagnostics is to test the system hardware without using additional equipment or risking data loss. If you are unable to fix the issue yourself, service and support personnel can use the diagnostics results to help you solve the issue.

Topics:

- [Dell Embedded System Diagnostics](#)

Dell Embedded System Diagnostics

NOTE: The Dell Embedded System Diagnostics is also known as Enhanced Pre-boot System Assessment (ePSA) diagnostics.

The Embedded System Diagnostics provide a set of options for particular device groups or devices allowing you to:

- Run tests automatically or in an interactive mode
- Repeat tests
- Display or save test results
- Run thorough tests to introduce additional test options to provide extra information about the failed device(s)
- View status messages that inform you if tests are completed successfully
- View error messages that inform you of issues encountered during testing

Running the Embedded System Diagnostics from Boot Manager

Run the Embedded System Diagnostics (ePSA) if your system does not boot.

Steps

1. When the system is booting, press F11.
2. Use the up arrow and down arrow keys to select **System Utilities > Launch Diagnostics**.
3. Alternatively, when the system is booting, press F10, select **Hardware Diagnostics > Run Hardware Diagnostics**. The **ePSA Pre-boot System Assessment** window is displayed, listing all devices detected in the system. The diagnostics starts executing the tests on all the detected devices.

Running the Embedded System Diagnostics from the Dell Lifecycle Controller

Steps

1. When the system is booting, press F10.
2. Select **Hardware Diagnostics → Run Hardware Diagnostics**. The **ePSA Pre-boot System Assessment** window is displayed, listing all devices detected in the system. The diagnostics start executing the tests on all the detected devices.

System diagnostic controls

Table 64. System diagnostic controls

Menu	Description
Configuration	Displays the configuration and status information of all detected devices.
Results	Displays the results of all tests that are run.
System health	Provides the current overview of the system performance.
Event log	Displays a time-stamped log of the results of all tests run on the system. This is displayed if at least one event description is recorded.

Getting help

Topics:

- [Recycling or End-of-Life service information](#)
- [Contacting Dell Technologies](#)
- [Accessing system information by using QRL](#)
- [Receiving automated support with Secure Connect Gateway \(SCG\)](#)

Recycling or End-of-Life service information

Take back and recycling services are offered for this product in certain countries. If you want to dispose of system components, visit [How to Recycle](#) and select the relevant country.

Contacting Dell Technologies

Dell provides online and telephone based support and service options. If you do not have an active internet connection, you can find Dell contact information on your purchase invoice, packing slip, bill or Dell product catalog. The availability of services varies depending on the country and product, and some services may not be available in your area. To contact Dell for sales, technical assistance, or customer service issues follow these steps:

Steps

1. Go to [Dell Support](#).
2. Select your country from the drop-down menu on the lower right corner of the page.
3. For customized support:
 - a. Enter the system Service Tag in the **Enter a Service Tag, Serial Number, Service Request, Model, or Keyword** field.
 - b. Click **Search**.
The support page that lists the various support categories is displayed.
4. For general support:
 - a. Select your product category.
 - b. Select your product segment.
 - c. Select your product.
The support page that lists the various support categories is displayed.
5. For contact details of Dell Global Technical Support:
 - a. Click [Contact Technical Support](#).
 - b. The **Contact Technical Support** page is displayed with details to call, chat, or e-mail the Dell Global Technical Support team.

Accessing system information by using QRL

There is also another QRL for accessing product information on the back of the system cover.

Prerequisites

Ensure that your smartphone or tablet has a QR code scanner installed.

The QRL includes the following information about your system:

- How-to videos

- Reference materials, including the Installation and Service Manual, and mechanical overview
- The system service tag to quickly access the specific hardware configuration and warranty information
- A direct link to Dell to contact technical assistance and sales teams

Steps

1. Go to [qrl](#), and navigate to your specific product or
2. Use your smart phone or tablet to scan the model-specific Quick Resource (QR) code on your system or in the Quick Resource Locator section.

Quick Resource Locator for PowerEdge XR8610t system



Figure 63. Quick Resource Locator for PowerEdge XR8610t system

Receiving automated support with Secure Connect Gateway (SCG)

Dell Secure Connect Gateway (SCG) is an optional Dell Services offering that automates technical support for your Dell server, storage, and networking devices. By installing and setting up a Secure Connect Gateway (SCG) application in your IT environment, you can receive the following benefits:

- Automated issue detection — Secure Connect Gateway (SCG) monitors your Dell devices and automatically detects hardware issues, both proactively and predictively.
- Automated case creation — When an issue is detected, Secure Connect Gateway (SCG) automatically opens a support case with Dell Technical Support.
- Automated diagnostic collection — Secure Connect Gateway (SCG) automatically collects system state information from your devices and uploads it securely to Dell. This information is used by Dell Technical Support to troubleshoot the issue.

- Proactive contact — A Dell Technical Support agent contacts you about the support case and helps you resolve the issue. The available benefits vary depending on the Dell Service entitlement purchased for your device. For more information about Secure Connect Gateway (SCG), go to [secureconnectgateway](#).

Documentation resources

This section provides information about the documentation resources for your system.

To view the document that is listed in the documentation resources table:


- From the Dell support site:
 1. Click the documentation link that is provided in the Location column in the table.
 2. Click the required product or product version.
-  **NOTE:** To locate the model number, see the front of your system.
- 3. On the Product Support page, click **Documentation**.
- Using search engines:
 - Type the name and version of the document in the search box.

Table 65. Additional documentation resources for your system

Task	Document	Location
Setting up your system	For information about setting up your system, see the <i>Getting Started Guide</i> document that is shipped with your system.	PowerEdge Manuals
Configuring your system	For information about the iDRAC features, configuring and logging in to iDRAC, and managing your system remotely, see the Integrated Dell Remote Access Controller User's Guide.	PowerEdge Manuals
	For information about understanding Remote Access Controller Admin (RACADM) subcommands and supported RACADM interfaces, see the RACADM CLI Guide for iDRAC.	
	For information about Redfish and its protocol, supported schema, and Redfish Eventing implemented in iDRAC, see the Redfish API Guide.	
	For information about iDRAC property database group and object descriptions, see the Attribute Registry Guide.	
	For information about Intel QuickAssist Technology, see the Integrated Dell Remote Access Controller User's Guide.	
	For information about earlier versions of, the iDRAC documents. To identify the version of iDRAC available on your system, on the iDRAC web interface, click ? > About .	iDRAC Manuals
	For information about installing the operating system, see the operating system documentation.	Operating System Manuals
	For information about updating drivers and firmware, see the Methods to download firmware and drivers section in this document.	Drivers

Table 65. Additional documentation resources for your system (continued)

Task	Document	Location
Managing your system	For information about systems management software offered by Dell, see the Dell OpenManage Systems Management Overview Guide.	PowerEdge Manuals
	For information about setting up, using, and troubleshooting OpenManage, see the Dell OpenManage Server Administrator User's Guide.	OpenManage Manuals
	For information about installing and using Dell Secure Connect Gateway, see the Dell Secure Connect Gateway Enterprise User's Guide.	serviceability tools
	For information about partner programs enterprise systems management, see the OpenManage Connections Enterprise Systems Management documents.	OpenManage Manuals
Working with the Dell PowerEdge RAID controllers (if applicable)	For information about understanding the features of the Dell PowerEdge RAID controllers (PERC), Software RAID controllers, or BOSS card and deploying the cards, see the Storage controller documentation.	Storage Controller Manuals
Understanding event and error messages	For information about the event and error messages generated by the system firmware and agents that monitor system components, go to QRL > Look Up > Error Code , type the error code, and then click Look it up .	QRL
Troubleshooting your system	For information about identifying and troubleshooting the PowerEdge server issues, see the Server Troubleshooting Guide.	PowerEdge Manuals