

# Taking action

Troubleshooting based on symptoms, hardware replacement procedures, and actions that should be taken after solving a problem

Lenovo

# Problem determination map

Refer to the map for details of which logs to capture for different problems, and also where to look for further problem determination diagnostics.

Scenario	Event log	Service Data (FFDC)	Memory Dump	Screen Shot	PD Diagnostics
Will not power on/boot/POST hangs	Yes (if still accessible). Refer to session Log collection – event log.	Yes (if still accessible). Refer to session Collecting service data.			<a href="#">Refer to Boot (POST) issue</a>
No DC power	Same as above	Same as above			<a href="#">Refer to Power related issue</a>
OS hangs	Yes	Yes	Yes	Yes	Refer to <a href="#">Collect service data</a> to collect OneCLI html report
Machine check error	Yes	Yes			Refer to <a href="#">Light path</a>
Unexpected reboots	Yes	Yes	Yes	Yes	Refer to <a href="#">Unexpected reboot</a>
RAID / disk	Yes	Yes			Refer to <a href="#">Storage issue</a>
M.2	Yes	Yes			Refer to <a href="#">M.2 issue</a>
NVMe	Yes	Yes			Refer to <a href="#">NVMe issue</a>
Temperature/fan	Yes	Yes			Refer to <a href="#">Over temperature / fan issue</a>
Memory	Yes	Yes			Refer to <a href="#">Memory issue</a>
CPU	Yes	Yes			Refer to <a href="#">Microprocessor issue</a>
Network	Yes	Yes			Refer to <a href="#">Ethernet controller issue</a>
PCIe device	Yes	Yes			Refer to <a href="#">PCIe device issue</a>
TPM/TCM	Yes	Yes			Refer to <a href="#">TPM/TCM issue</a>

## Power-related issues

First, determine whether any changes had been applied to the machine directly before the problem occurred.

- A hardware change can result in a DC short; it can also result in a cable being knocked loose, preventing the computer from starting.
- Adding additional components when the power supplies are not all installed or plugged in can result in the computer receiving insufficient power.
- When servers are moved to new locations, they might be plugged in to unproven power sources, and internal power cables can be shaken loose.

Actions to take:

- Confirm each step from the [Before you begin](#) section.
- Check the event logs for any events related to the server not turning on.
- Check for any LEDs that are flashing amber.
- Reseat the hot-swap power supply.
- Replace the power supply.

## Boot (POST) issues

Servers can sometimes hang or restart during the boot (POST) sequence before entering the OS boot process. When this happens, first determine whether any changes had been applied to the machine directly before the problem occurred.

- Is it a brand new or recently shipped computer?
  - Components might not be securely installed.
  - BIOS might not be updated to a level that will support options that were added to the server.
  - The CMOS might not have been properly configured.
- Has new hardware been installed?
  - There might be an unsupported configuration or incompatible BIOS level.
- Has a USB or other external storage device been attached?
  - This can affect the boot sequence and generate boot disk failures.

Click [HERE](#) to see the service actions.

## Boot (POST) issues



Actions to take:

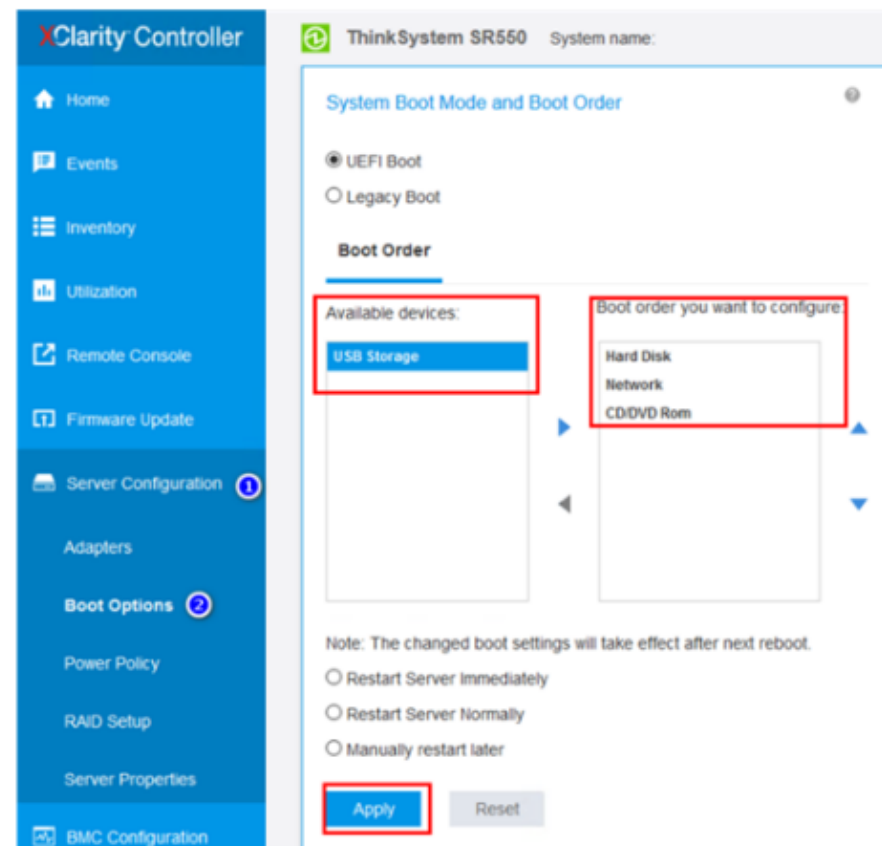
- Confirm each step from the [Before you begin](#) section.
- Check the event logs for any events related to booting issues.
- Check for any LEDs that are flashing amber.
- Boot the server with the minimum configuration: one microprocessor and one DIMM. Before doing this, confirm the processor and DIMM function is good.
  - If the server can boot properly with the minimum configuration, reinstall the other components one at a time until the failure occurs.
- If the server still fails to boot, collect service data for analysis. System board replacement might be needed.



## Boot device issues

If the server cannot boot to the OS properly, users can take the following actions:

- Confirm each step from the [Before you begin](#) section.
- Check for any LEDs that are flashing amber.
- Make sure that the boot device – for example, the HDD, M.2, or USB device – is listed in the boot order.
- The boot order can be set from the XCC web interface by selecting **Server Configuration → Boot Options**.
  - If the server can boot properly with the minimum configuration, reinstall the other components one at a time until the failure occurs.
  - To change the boot order, select devices and use the horizontal arrows to move them into or out of the **Boot order you want to configure** list. You can then select devices and use the up and down arrows to change their order in the list.
  - Select **Apply** to save the changes. The changed boot settings will take effect after the next reboot.



## Unexpected reboots

A computer reboot is the primary method a computing system uses to reset itself and recover from an error. Unexpected reboots can be caused by a hardware or OS failure.

Actions to take:

- Confirm each step from the [Before you begin](#) section.
- Check whether there have been any recent OS updates.
  - New OS service packs or updates can fail to install correctly. They can also replace stable device drivers with less stable drivers.
- Check for recent utility power disturbances.
  - A brief power outage can leave the service processor in a corrupt state resulting in reboots for false watchdog events.
- Check for any LEDs that are flashing amber.
- Check the event logs for any events related to server reboots.
- Check the OS watchdog to isolate why the service processor is unable to detect a functioning OS for a period of time.
- Collect the Blue Screen of Death (BSOD), memory dump, service data, and OneCLI HTML report to analyze and isolate the cause of the reboot.

## Temperature/fan issues

ThinkSystem servers are designed for fan redundancy, provided that a full compliment of fans has been installed. If one fan fails, the remaining fans should speed up to compensate for the reduced airflow. When multiple fan failures occur, the potential for a thermal increase within the chassis becomes high. Over-temperature conditions, particularly when temperatures reach a high thermal threshold, can trigger sudden system shutdowns to avoid potential damage to the server.

Actions to take:

- Make sure there is sufficient airflow through the front rack doors.
- Ensure the rear chassis or rack air vents are not blocked and that nothing is blocking airflow through the power supplies (both front and rear).
- Check the overall ambient temperature of the room. The ambient room temperature of most server/rack environments will be maintained at 22°C (70°F) or lower.
- Check for any LEDs that are flashing amber.
- Check the event logs for any events related to high temperatures.
- Replace any fans reported as failed.



## Memory issues

DIMM errors are not always caused by the DIMM itself. They can be caused by the CPU memory controller, system board DIMM slot, system board CPU socket, memory card, or CPU/memory expansion board.

Some servers only support particular types of DIMMs (UDIMMs or RDIMMs), and some only support one particular voltage type at a time. This information can be found in the system's Maintenance Manual.

Make sure that:

- No error LEDs on the operator information panel (light path) are turned on
- No DIMM error LEDs on the system board are turned on
- The memory mirrored channel does not account for the discrepancy
- The memory modules are seated correctly
- The correct type of memories are installed
- If memory has been changed, the memory configuration in the Setup Utility (F1) has been updated accordingly
- All banks of memory are enabled. The server might have automatically disabled a memory bank when it detected a problem, or a memory bank might have been manually disabled.
- There is no memory mismatch when the server is at the minimum memory configuration.

# Memory problem determination procedure

Work through the following steps until the problem has been solved.

1. Reseat the DIMMs, and then restart the server.
2. Make sure all the DIMMs are initialized in the Setup Utility
3. Check the POST error log:
  - If a DIMM was disabled by a systems management interrupt (SMI), replace the DIMM.
  - If a DIMM was disabled by the user or by POST, go to step 4.
4. Swap the DIMMs of the same microprocessor between the channels, re-enable and reinstall all the DIMMS, and then restart the server. If the problem is related to a DIMM, replace the failing DIMM, and then run memory diagnostics in LXPM.
5. After reversing the DIMMs, if a DIMM is still reported as failed in the same DIMM slot, it might be a microprocessor or system board issue.
6. If the server has two microprocessors, swap the microprocessors, re-enable all the DIMMS, and then restart the server.
  - If the DIMM is still reported as failed in the same DIMM slot, replace the system board.
  - If the failed DIMM slot changes with the microprocessor, replace the microprocessor.
7. If the server only has one microprocessor, replace the microprocessor and re-enable all the DIMMS. Then, restart the server.
  - If the DIMM error is still reported for the same DIMM slot, replace the system board.

**Note:** Each time a DIMM is installed or removed, users must disconnect the server from the power source and then wait 10 seconds before restarting the server.

## Microprocessor issues

First, determine whether any changes had been applied to the machine before the problem occurred.

Actions to take:

- Confirm each step from the [Before you begin](#) section.
- Check whether there have been any recent OS installations or updates.
  - One common problem is that an OS has been installed that will not support the number of processor cores installed in the server.
- Check whether a new PCI device has been installed.
  - PCI adapters can introduce parity error/SMI error (PERR/SEERR) errors on the PCI bus that can cause a processor to report a machine check. A down level or wrong device driver can cause the server to reboot. This can be perceived to be a processor problem.
- Check for memory issues.
  - Failed memory can cause an NMI reboot, as the device will be removed from the system configuration.
- Check if any LEDs on the operator information panel (light path) are turned on.
- Check the event logs for any events related to the microprocessor.

# Ethernet controller issues

The process used to test the Ethernet controller depends on the operating system being used. Check the operating system documentation for information about Ethernet controllers, and then check the Ethernet controller device driver README file for more information.

Actions to take:

- Make sure that the correct device drivers, which come with the server, are installed and that they are at the latest level.
- Make sure that the Ethernet cable is installed correctly.
  - The cable must be securely attached at all connections. If the cable is attached, but the problem remains, try a different cable.
- Use the XCC inventory page to check Ethernet controller port status. Click [HERE](#) to see an example.
- Use switch CLI commands to check the port status:
  - Cisco switch command: `show interface status`. Click [HERE](#) to see an example.
  - Brocade switch command: `portshow`. Click [HERE](#) to see an example.
  - For other brand switches, refer to their user guide for the information about CLI commands.
- Check the Ethernet controller LEDs on the rear panel of the server. These LEDs indicate whether there is a problem with the connector, cable, or hub.
  - The Ethernet link status LED will turn on when the Ethernet controller receives a link pulse from the hub. If the LED is off, there might be a defective connector or cable, or a problem with the hub.
- Check if the LAN activity LED on the rear of the server is turned on when data is active on the Ethernet network. If the LAN activity LED is off, make sure that the hub and network are operating and that the correct device drivers are installed.
- Make sure that the device drivers on the client and server are using the same protocol.
- If the Ethernet controller still cannot connect to the network but the hardware appears to be working, the network administrator must investigate other possible causes of the error.



# Ethernet controller issues



**XClarity Controller**

Home Events Inventory Utilization Remote Console Firmware Update Server Configuration

**ThinkSystem SR550** System name:SR550-3 Export USERID 1

OnBoard	Adapter 00:11:05	SATA Controller	OnBoard	N/A	>
OnBoard	Intel X722 LOM		OnBoard	N/A	
Intel X722 LOM B1:00:00		Ethernet			▼

▶ Asset Summary  
▶ PCI Summary  
▶ Firmware  
▶ Network Adapter Summary  
▼ Physical Ports

Port Name	Burned-in Address	Connector	Link Speed (Gbps)	Link Status
Physical Port 1	0894EF4F9934	OnBoard	10	up

Quick Link

- CPU
- DIMM
- DISK
- PSU
- Fan
- PCI
- SYS Board

- If the Ethernet controller still cannot connect to the network but the hardware appears to be working, the network administrator must investigate other possible causes of the error.



# Ethernet controller issues



For Cisco switches, use the `show interface status` command to display the port status.

```
Switch# show interface status
```

Port	Name	Status	Vlan	Duplex	Speed	Type
Gil/0/1		connected	1	a-full	a-1000	10/100/1000BaseTX
Gil/0/2		connected	1	a-full	a-1000	10/100/1000BaseTX
Gil/0/3		connected	1	a-full	a-1000	10/100/1000BaseTX
Gil/0/4		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/5		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/6		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/7		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/8		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/9		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/10		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/11		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/12		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/13		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/14		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/15		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/16		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/17		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/18		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/19		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/20		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/21		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/22		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/23		notconnect	1	auto	auto	10/100/1000BaseTX
Gil/0/24		notconnect	1	auto	auto	10/100/1000BaseTX

- If the Ethernet controller still cannot connect to the network but the hardware appears to be working, the network administrator must investigate other possible causes of the error.

# Ethernet controller issues



For Brocade switches, use the `portshow <port number>` command to display the port status.

```
switch:admin> portshow 28
portName: port28
portHealth: Fabric vision license not present
Authentication: None
portDisableReason: None
portCFlags: 0x1
portFlags: 0x10004103 PRESENT ACTIVE E_PORT \
G_PORT D_PORT U_PORT LOGIN LED
LocalSwcFlags: 0x0
portType: 24.0
POD Port: Port is licensed
portState: 1 Online
Protocol: FC
portPhys: 6 In_Sync portScn: 0 Flow control mode 4
port generation number: 0
state transition count: 1
portId: 2dlc00
portIfId: 43020028
portWwn: 20:1c:00:05:33:13:2f:b3
portWwn of device(s) connected:
Distance: normal
portSpeed: 8Gbps
FEC: Inactive
LE domain: 0
FC Fastwrite: OFF
Interrupts: 0 Link_failure: 0 Frjt: 0
Unknown: 0 Loss_of_sync: 1 Fbsy: 0
```

- If the Ethernet controller still cannot connect to the network but the hardware appears to be working, the network administrator must investigate other possible causes of the error.

## **Storage issues – hard disk drives and RAID adapters**

The event log, service data (FFDC), and hard disk drive status LEDs can normally indicate a failed HDD. If the HDD has failed, replace it. However, the symptoms of failure are not always obvious.

HDD issues can be divided into the following scenarios:

- The server fails to recognize a hard disk drive
- Multiple hard drives fail
- Multiple hard drives are offline
- A replacement hard disk drive does not rebuild
- The green hard disk drive activity LED does not represent the actual state of the associated drive
- The yellow hard disk drive activity LED does not represent the actual state of the associated drive

## Server fails to recognize a hard disk drive

### Actions to take:

- Verify that the drive is supported on this compute node. Check the [ServerProven](#) website for a list of supported hard drives.
- Make sure that the drive is seated in the drive bay properly and that there is no physical damage to the drive connectors.
- For slots that only support SAS/SATA drives, NVMe SSDs are not supported. The HDD LED behavior can be referenced to identify this problem.
- Use the XCC inventory page or the OneCLI inventory command to verify whether the drive's firmware is the most recent version. A drive with down-level firmware might cause a drive failure issue.
- Check the server's firmware version, as old versions of XCC or UEFI might not recognize some hard disk drives.



## After replacing a failed HDD

After replacing the drive, open LXPM, go to the **Run Diagnostics** page, and run the **Disk Drive Test**. If the drive fails the diagnostic test, or if it passes the test but is still not recognized, consider replacing the following components:

- Affected backplane signal cable
- Affected backplane
- Affected adapter
- HDD (again)

The screenshot shows the XClarity Provisioning Manager interface. On the left is a dark sidebar with navigation options: Dashboard, Memory Test, Disk Drive Test (highlighted), RAID Log, and DCPMM Test. The main area is titled 'Disk Drive Test' and contains a 'Storage Test Option' section with radio buttons for 'Short Self Test' (selected) and 'Long Self Test'. Below this is a 'Storage Test Status' table with columns for Device Name, Status, Progress, and Duration. The table lists two drives, both with a status of '[Not Run]' and 0% progress. A notice at the bottom states: 'Notice: The Disk Drive Test will take a few minutes. Press ESC to exit.'

Device Name	Status	Progress	Duration
<input checked="" type="checkbox"/> Select All			
<input checked="" type="checkbox"/> 09:ST1000NM0055:ZBS0VWAZ	[Not Run]	0%	0seconds
<input checked="" type="checkbox"/> 10:ST1000NM0055:ZBS0V1HW	[Not Run]	0%	0seconds



## Multiple HDD failures

A power outage or vibration issue can cause multiple HDDs to fail. Check XCC event logs for any events related to power supplies or vibration issues. Resolve those issues before taking any further action.

Actions to take:

- Make sure that the drives, SAS/SATA RAID adapter, server device drivers, and firmware are at the most recent levels. Use the XCC inventory page or OneCLI inventory command to verify the drive's firmware version.
- Consider replacing the drive backplane or backplane cable.
- Collect service data to check hard drive wear/usage information.

**Attention:** Some cluster solutions require specific code levels or coordinated code updates. If the device is part of a cluster solution, verify that the latest level of code is supported for the cluster solution before updating the code.

## Multiple HDDs are offline

A power outage or vibration issue can cause multiple HDDs to go offline. Check XCC event logs for any events related to power supplies or vibration issues. Resolve those issues before taking any further action.

Actions to take:

- Review the storage subsystem logs for indications of problems within the storage subsystem, and resolve those events.
- Check the storage subsystem logs to identify the first HDD that either failed or went offline. Only on the advice of the next level of support, manually switch the other hard drives back online and then replace the first hard drive to suffer a problem.

## **A replacement drive does not rebuild**

Actions to take:

- Make sure that the drive is recognized by the adapter (the green HDD activity LED is blinking).
- Make sure the replacement hard drive FRU/CRU is the same as that of the failed hard drive.
- Make sure the replacement drive shows as an unconfigured good drive.
  - If the replacement drive came from another RAID array, clear the foreign configuration and set it to unconfigured good.
- Check if the controller has a hot spare drive defined.
  - The controller will not use the replacement drive until the rebuild to the hot spare is complete.
- Check for the state of the virtual drive to be rebuilt.
  - Rebuilds will only start for degraded virtual drives.

**Green HDD activity LED does not represent the actual state of the associated drive**

If the green drive activity LED does not blink when the drive is in use, work through the following procedure:

- Check XCC for drive error events
- If there are no error messages in XCC, run the LXPM HDD diagnostic test.
- If the drive passes the test, replace the backplane.
- If the drive fails the test, replace the drive.
- Drive LED description:

Drive LED	LED behavior	Status description
Drive activity LED (green)	Solid green	The drive is powered, but not active
	Blinking	The drive is active
Drive status LED (yellow)	Solid yellow	The drive failed
	One blink per second	The drive is rebuilding
	Three blinks per second	The drive has been located

## **Yellow drive activity LED does not represent the actual state of the associated drive**

Work through the following procedure until the problem is solved.

- Turn off the server.
- Reseat the SAS/SATA adapter.
- Reseat the backplane signal cable and backplane power cable.
- Reseat the hard disk drive.
- Turn on the server and monitor the activity of the drive LEDs.



## **Storage issues – RAID adapter**

RAID adapter issues can be divided into the following scenarios:

- Drives/arrays are not recognized by the OS
- Drive slot numbers are incorrect
- RAID adapter firmware update fails with XCC
- RAID adapter firmware update fails with OS flash

# Drives/arrays are not recognized by the OS

Work through the following steps to determine what actions you should take:

## Check if the correct device driver has been loaded.

Go to the [Lenovo Support Portal](#), navigate to the support page for the server, and download and install the appropriate driver to the server.

## If the drives are seen by the controller, check what states the drives are in.

- Drives must be in an array or JBOD state to be seen by the OS. Unconfigured drives and failed/missing arrays cannot be seen by the OS.
- If drives are marked as foreign, there is a configuration that is not yet active. Import the configuration or clear the foreign data and create a new configuration.

## Go to one of the following locations to check if the drives are seen by the controller:

- The Human Interface Infrastructure (HII) page (**F1 Setup -> System Settings -> Storage -> Main Menu -> Physical Drive Management**)
- LXPm (**F1 Setup -> Graphical menu -> RAID Setup**)
- The XCC web interface (**Inventory - Storage Devices** section)
  - If a message stating **The following drives are installed in the system. There are no inventory details for them** is displayed, this indicates that a drive is installed but cannot be seen by the controller.
  - This is because XCC is able to detect the presence of a drive directly from a backplane, regardless of whether a controller can see the drive itself.

## If the drives are not seen by the controller, take the following actions:

- Reseat the controller and reconnect all the cables connected to the HDD backplane and controller.
- If the problem still exists, try to replace the following components one at a time until the problem is solved.
  - HDD
  - RAID adapter
  - HDD backplane
  - SAS/SATA signal cable(s)

## Drive slot numbers are incorrect

Slot numbering is set by XCC during the system boot. XCC detects the backplanes, how many slots they have, and where they are located. It then programs the slot numbering to each backplane. When the controller starts, it reads the backplane's slot information with the Serial General Purpose Input/Output (SGPIO) and uses this information to override internal default slot numbering.

Incorrect slot numbering in the controller is a very rare controller issue.

If there are slot numbering issues, this may be an XCC, UEFI, or backplane firmware issue. (Note that backplane firmware updates are integrated into XCC updates.)

Actions to take:

- Confirm the supported XCC and UEFI firmware levels on the current system.
- Confirm the cable connection order is correct between the RAID adapter and the HDD backplane.

## Adapter firmware update fails with XCC

Actions to take:

- If retrying the update does not work, try booting to an OS and loading the supported RAID adapter driver. Then perform the update with XCC.
- If this does not work, users might need to try the in-band (with an OS/BoMC) method.
- If all of the above fails, an FFDC capture after the failure will be required for further analysis.

## Adapter firmware update fails with OS flash

Generally, the only failure with regards to in-band package flashing (executing a firmware update package from inside the OS) happens because the firmware executable package is not able to detect that the appropriate adapter is present.

Actions to take:

- Check that a supported RAID adapter driver has been loaded for the device
- Restart the system – after the driver installation, this might need to be done before the firmware executable package can detect the adapter
- For any other kind of flash failure, controller logs and the specific output of the firmware executable package will need to be collected
- If the flash failure is from within another tool, such as OneCLI or LXCA, it is recommended to run the firmware executable package itself (either in-band or with XCC) to determine if the issue is between the other tools and the package or if the issue is with the firmware executable package itself

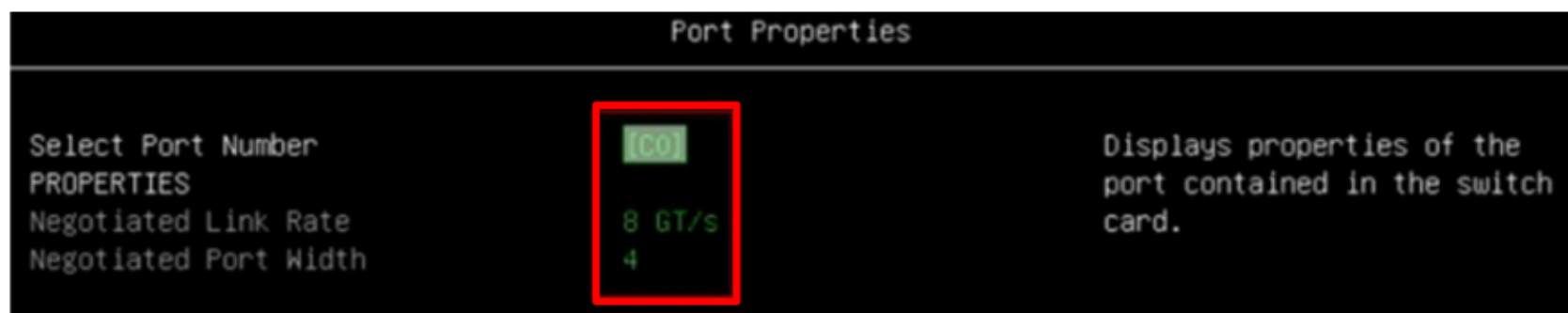


## NVMe issues

The most common issue is that the NVMe device cannot be detected.

Actions to take:

- Check hot-add is supported during pre-boot.
  - Make sure NVMe devices are installed prior to the system boot.
  - Make sure hot-add/hot-remove is supported in the OS.
- Check NVMe cables are properly installed.
  - Verify in HII that the link is established on all connectors (C0 through C3).
  - Select **System Settings** → **Storage** → **1610-4P** → **Port Properties**.
  - If one of the connectors is expected to have a link but does not, check to make sure it is properly installed on the switch and backplane.



## M.2 device issues

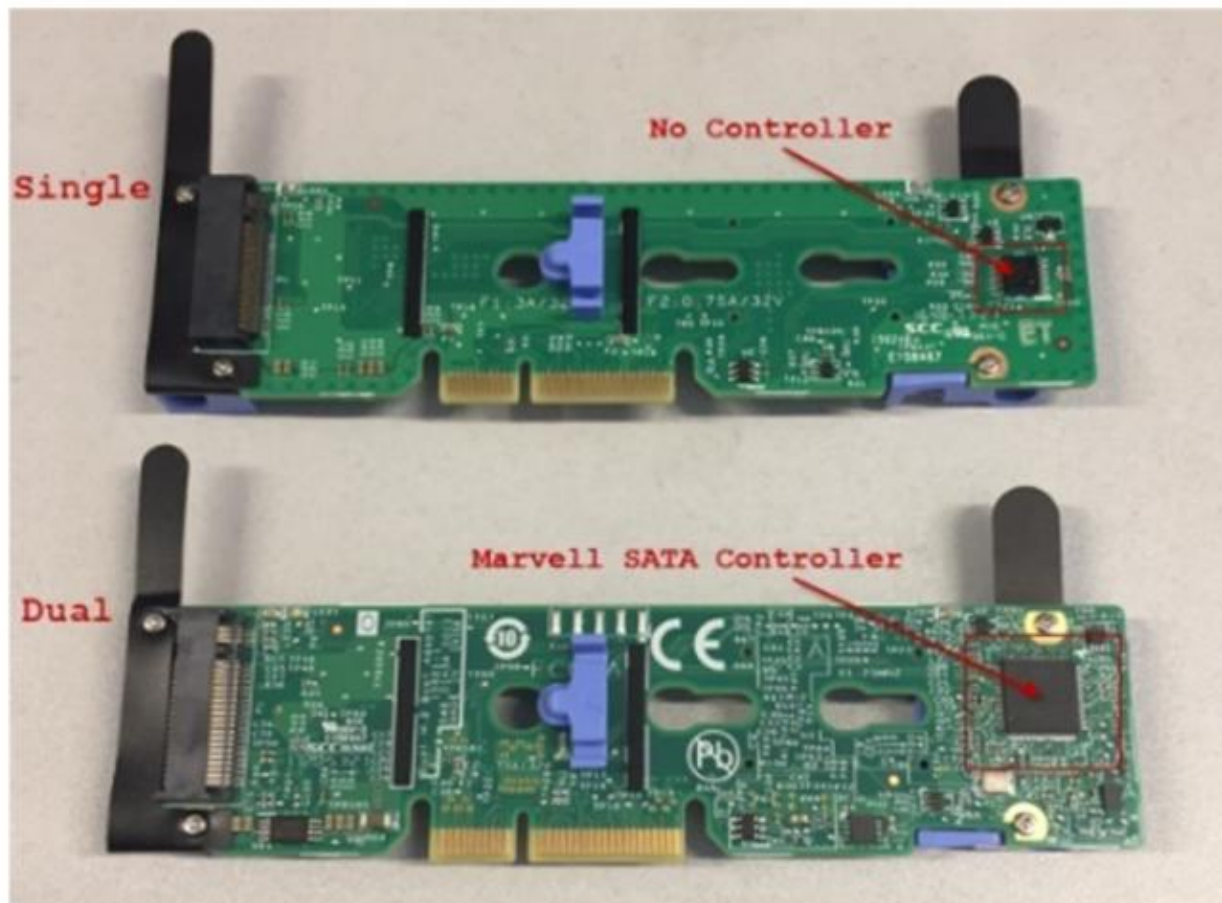
The M.2 device should be installed on a single or dual M.2 backplane, and the backplane should be installed on the system board. To physically identify a single or dual M.2 backplane:

- Check the number of connectors on the M.2 backplane.
- Check if the Marvell SATA controller is present on the M.2 backplane.

The most common issue is that the M.2 device cannot be detected.

Actions to take:

- Confirm that the M.2 is properly installed on the M.2 backplane.
- Confirm that the M.2 drive retainer is properly seated.
- Confirm that the M.2 backplane is properly installed on the system board.



## PCIe device issues

Actions to take:

- Confirm each step from the [Before you begin](#) section.
- Verify that the device is supported for this server. Check the [ServerProven](#) website for a list of supported devices.
- Check the event logs and resolve any issues related to the device.
- Make sure that the adapter is installed in a correct slot.
- Make sure that the proper device drivers are installed for the device.
- Resolve any resource conflicts if running legacy mode (UEFI).
- Check the [Lenovo Support](#) for any tech tips that might be related to the adapter.
- Make sure all adapter external connections are correct and that the connectors are not physically damaged.

## TPM/TCM issues

ThinkSystem servers support Trusted Platform Module (TPM) version 1.2 by default, and they can be upgraded to support version 2.0. The TPM is embedded on the system board.

For customers in the People's Republic of China (PRC), TPM is not supported. However, customers in the PRC can install a Trusted Cryptographic Module (TCM) adapter (sometimes called a daughter card) instead.

When a system board is replaced, users must make sure that the TPM/TCM policy is set correctly or an error will occur. The following three points need special attention:

- Setting the TPM/TCM policy
- Asserting physical presence
- Setting the TPM version



## Setting the TPM/TCM policy

By default, replacement system boards are shipped with the TPM/TCM policy set to undefined. Servicers must modify this setting so that it matches the setting in place on the original system board.

The TPM/TCM policy can be set using LXPM. Work through the following procedure to set the TPM/TCM policy:

Click each number in turn to see the procedure.

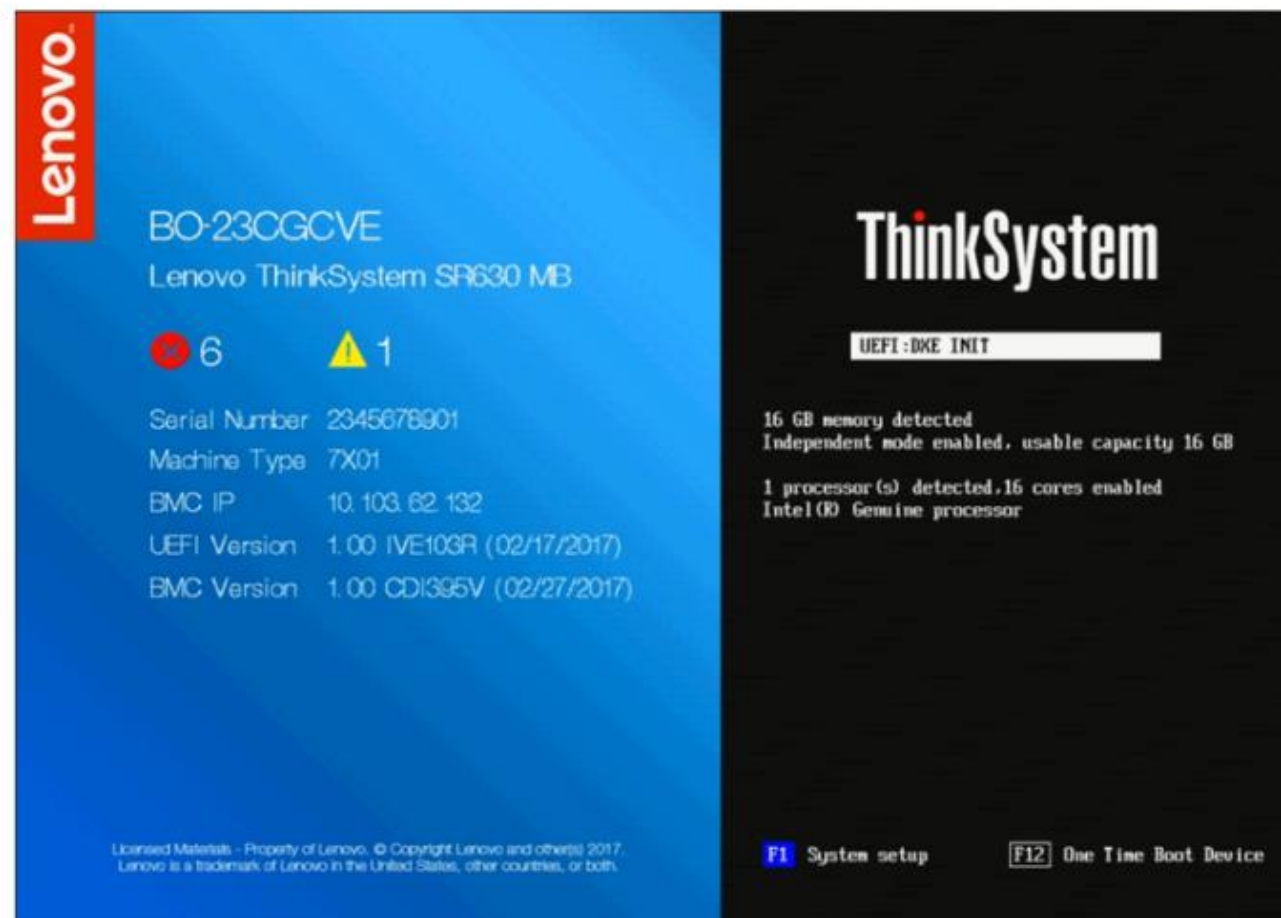
Step





## Setting the TPM/TCM policy

Press **F1** during the POST, and LXPM will launch by default. If the power-on Administrator password is required, enter the password.

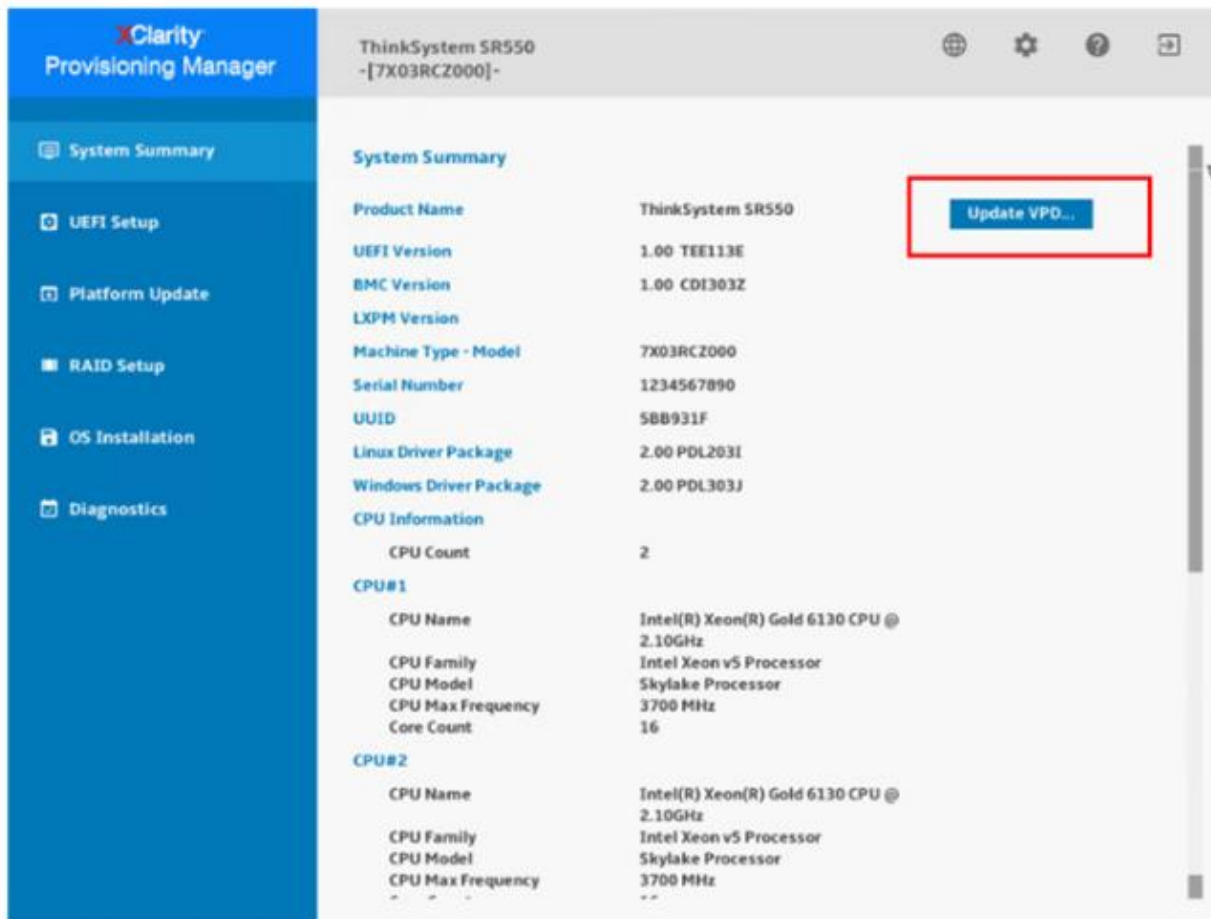


Step



# Setting the TPM/TCM policy

On the **System Summary** page, click **Update VPD**.



The screenshot shows the XClarity Provisioning Manager interface for a ThinkSystem SR550. The left sidebar contains navigation links: System Summary, UEFI Setup, Platform Update, RAID Setup, OS Installation, and Diagnostics. The main content area displays system information under the 'System Summary' heading. A red rectangle highlights the 'Update VPD...' button in the top right corner of the main content area.

System Summary	
Product Name	ThinkSystem SR550
UEFI Version	1.00 TEE113E
BMC Version	1.00 CDI303Z
LXPM Version	
Machine Type - Model	7X03RCZ000
Serial Number	1234567890
UUID	SBB931F
Linux Driver Package	2.00 PDL203I
Windows Driver Package	2.00 PDL303J
CPU Information	
CPU Count	2
CPU#1	
CPU Name	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz
CPU Family	Intel Xeon v5 Processor
CPU Model	Skylake Processor
CPU Max Frequency	3700 MHz
Core Count	16
CPU#2	
CPU Name	Intel(R) Xeon(R) Gold 6130 CPU @ 2.10GHz
CPU Family	Intel Xeon v5 Processor
CPU Model	Skylake Processor
CPU Max Frequency	3700 MHz
	--

Step



Taking action

# Setting the TPM/TCM policy

Select a TPM/TCM policy

Clarity Provisioning Manager

ThinkSystem SR550

System Summary

UEFI Setup

Platform Update

RAID Setup

OS Installation

Diagnostics

Update VPD

Manufacturer Name:

Machine Type - Model:

Serial Number:

Asset Tag:

UUID:

TPM/TCM policy

Step



## Setting the TPM/TCM policy

There are four TPM/TCM policy options

- **Undefined**
  - Select this option if the users do not want to set the TPM/TCM policy.
- **TPM enabled – ROW**
  - Users outside of the PRC should choose this setting.
- **TCM enabled – China only**
  - Users in the PRC should choose this setting if a TCM adapter is installed.
- **Permanently disabled**
  - Users in the PRC should use this setting if no TCM adapter is installed.

TPM/TCM policy

Undefined ▼

Undefined  
TPM enabled - ROW  
TCM enabled - China only  
Permanently disabled

Apply

Step 1—2—3—4—5



## Setting the TPM/TCM policy

After clicking **Apply**, a window will be displayed with a message stating **Warning - The policy cannot be changed and the options will be hidden once it is set. Do you want to proceed?**

Once the policy has been set, the **TPM/TCM policy** section will be hidden.

Step **1**—**2**—**3**—**4**—**5**

The screenshot shows a web interface for 'Update VPD'. It includes input fields for 'Manufacturer Name' (Lenovo) and 'Machine Type - Model' (TX038CZ000). A confirmation dialog box is overlaid on the interface, displaying the warning: 'Warning - The policy cannot be changed and the options will be hidden once it is been set. Do you want to proceed?'. The dialog has 'Yes' and 'No' buttons. Below the dialog, the 'TPM/TCM policy' section is visible, showing a dropdown menu set to 'TPM enabled - ROW' and an 'Apply' button.





## Asserting Physical Presence

Physical Presence is required to change the TPM enable value and TPM version. Before asserting Physical Presence, the Physical Presence Policy must be enabled. By default, the Physical Presence Policy is enabled with a timeout of 30 minutes.

Work through the following procedure to assert Physical Presence.

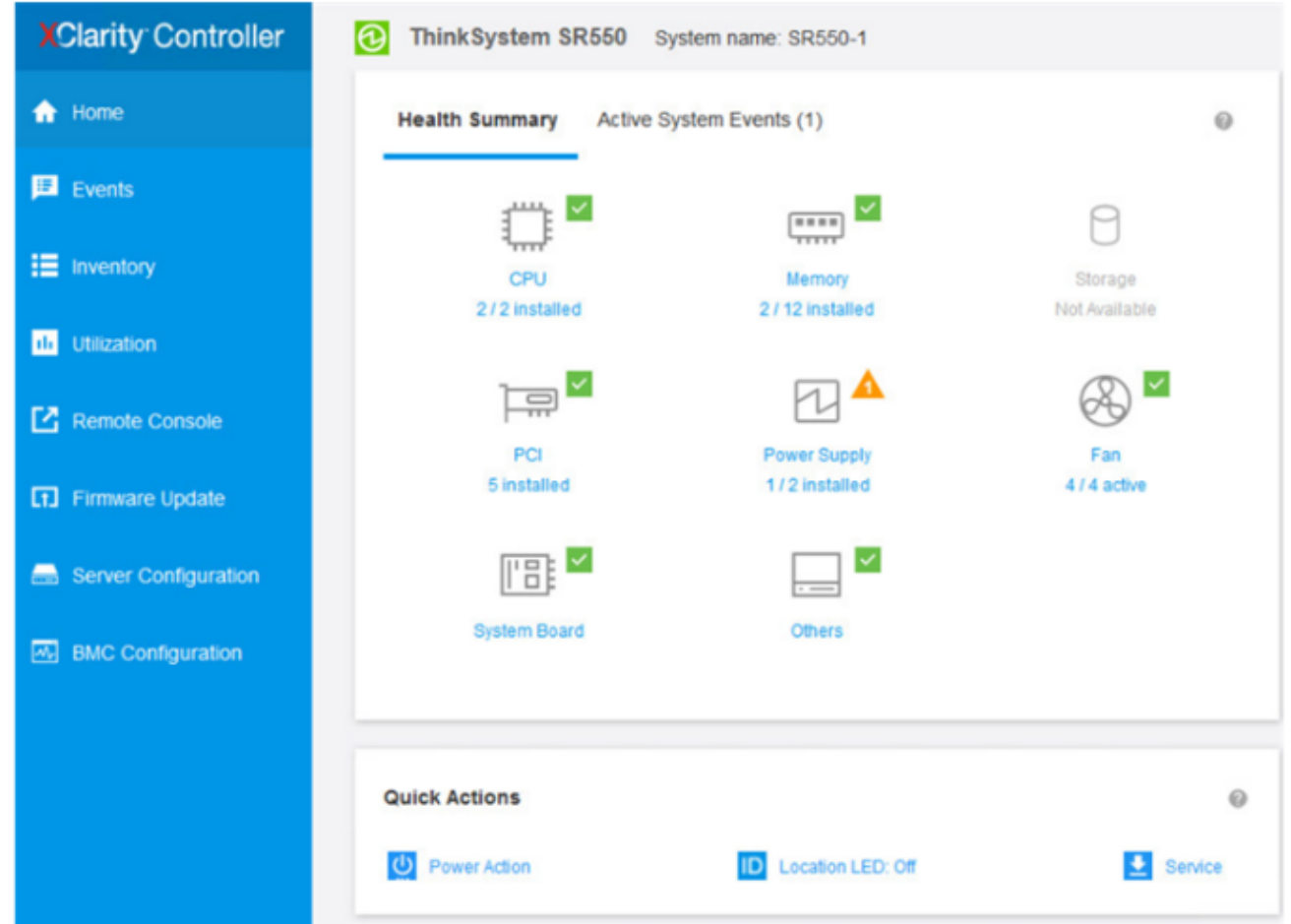
Click each number in turn to see the procedure.

Step



# Asserting Physical Presence

Log in to the XCC web interface.



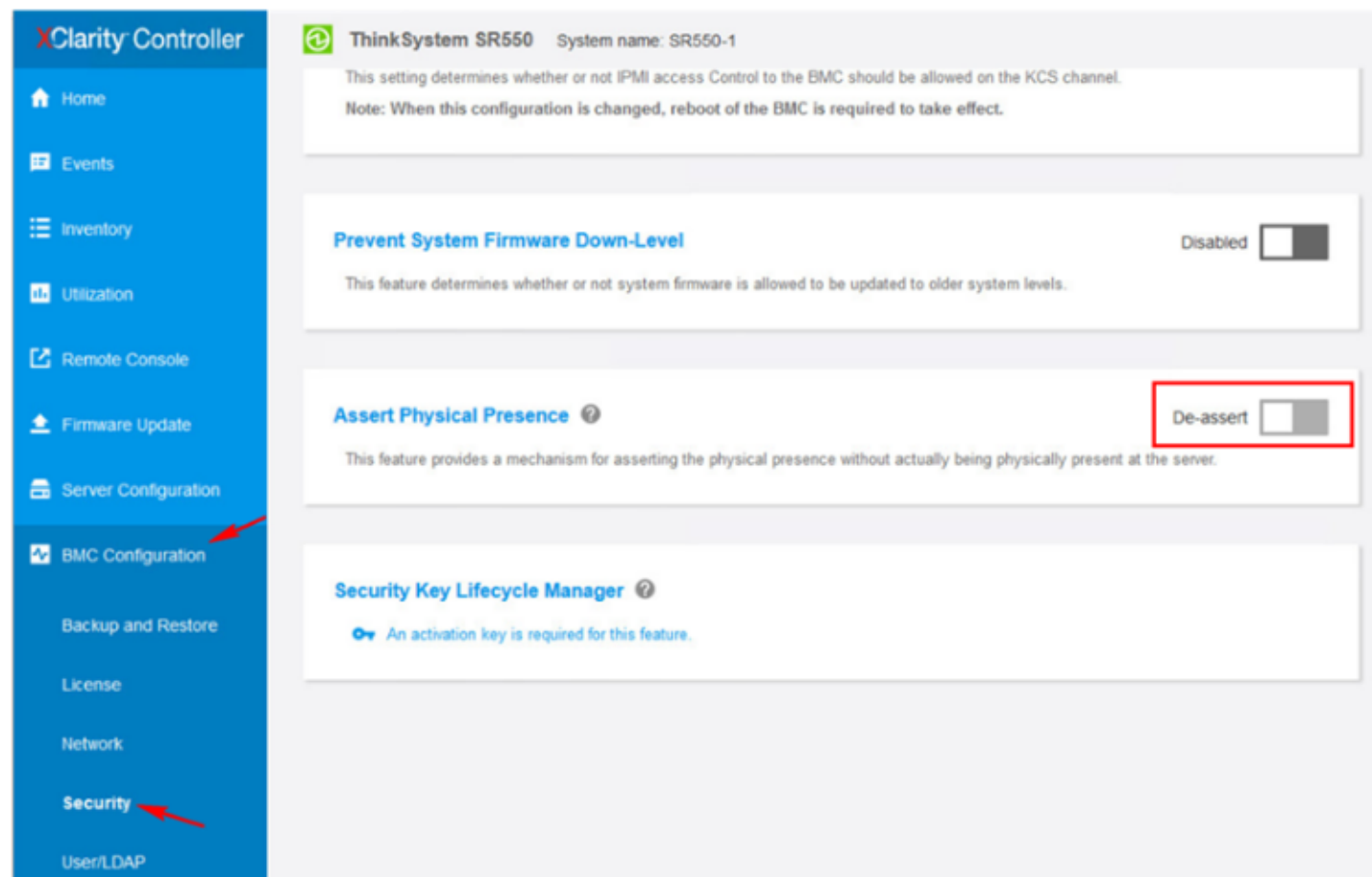
Step ①—②—③—④



# Asserting Physical Presence

Select **BMC Configuration** > **Security** and verify that **Assert Physical Presence** is set to **Assert**.

If the status is **De-assert** and cannot be chosen, that means the Physical Presence Policy has been disabled. Go to step 3 for details of how to change the Physical Presence Policy.

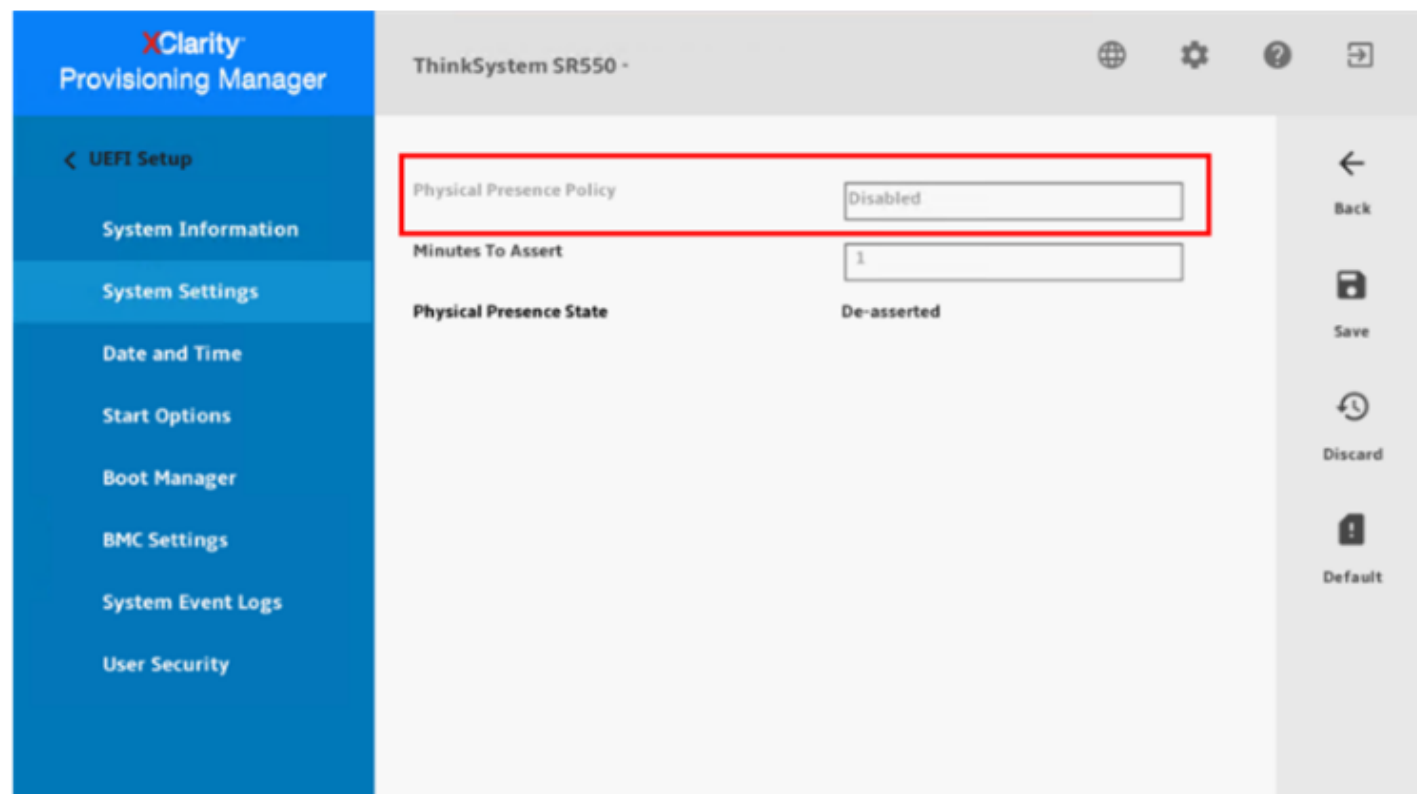


Step **1**—**2**—**3**—**4**



# Asserting Physical Presence

Enable the Physical Presence Policy using LXPM. Go to **UEFI Setup > System Settings > Security > Physical Presence Policy Configuration**. Change the **Physical Presence Policy** status to **Enable**. If the setting cannot be chosen, it means the hardware Physical Presence jumper on the system board is not set to assert. Go to step 4 for details of how to change the hardware Physical Presence jumper setting.



Step

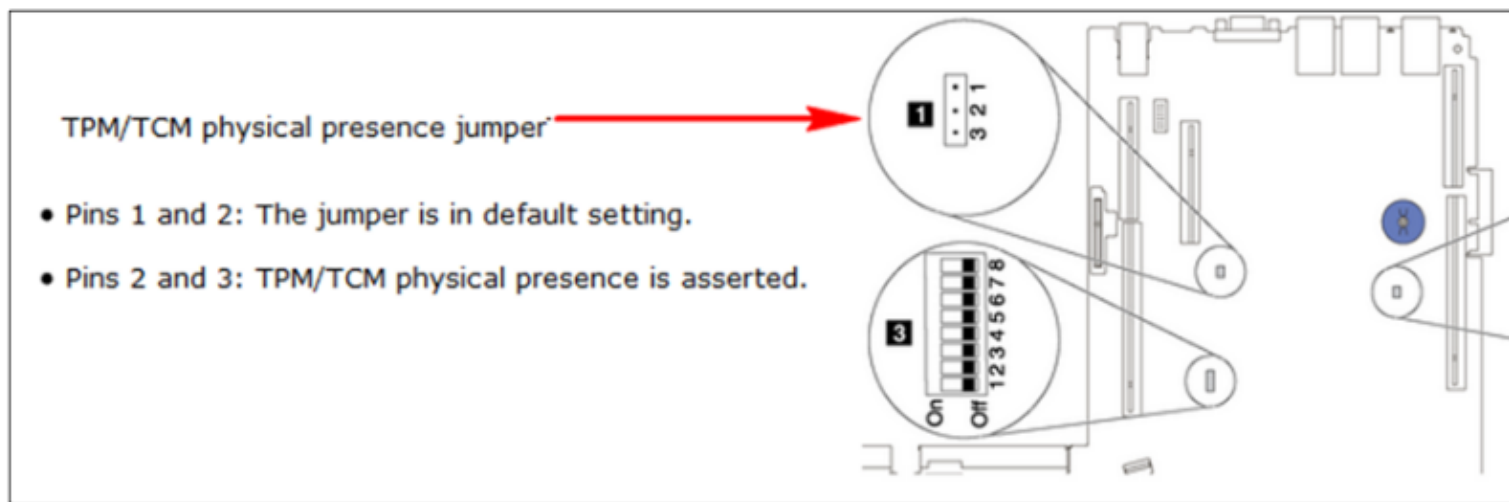


# Asserting Physical Presence

Check the **System-board switches, jumpers, and buttons** section in the Maintenance Manual for the relevant ThinkSystem server models.

The SR550 system board is referenced in this example.

Move the jumper to pins 2 and 3 to set the TPM/TCM physical presence to asserted. Then, go back to step 3 to enable the physical presence policy, and then return to step 2 to assert physical presence.



Step **1** — **2** — **3** — **4**





## Setting the TPM version

To set the TPM version, Physical Presence must be asserted. Use OneCLI to set the TPM version.

Use the following command to set the TPM version to 2.0:

```
OneCli.exe config set TPMVersion.TPMVersion "Update to TPM2.0 compliant" -v --override --bmc ip_address --user <userid> --password <password>@
```

Use the following command to set the TPM version to 1.2:

```
OneCli.exe config set TPMVersion.TPMVersion "Update to TPM1.2 compliant" -v --override --bmc ip_address --user <userid> --password <password>@
```

Where <userid>:<password> is the user ID and password used to access the XCC web interface of the server. The default user ID is USERID, and the default password is PASSWORD (zero, not an uppercase o).

<ip\_address> is the IP address of XCC.

## System board replacement summary if TPM/TCM is enabled

- For users in the PRC, if there is no TCM module on the old system board, replace the board and set the **TPM/TCM policy in LXPm** to **Permanently disabled**.
- For users in the PRC, if there is a TCM module, unplug the TCM daughter card from the old system board and insert it into the new system board. Then, set the **TPM/TCM policy in LXPm** to **TCM enabled – China only**.
- For users outside the PRC, the servicer should confirm the TPM version at the customer's site. The TPM version can be captured from the FFDC data if the old system board is not completely unusable, or you can ask the customer if they had TPM version 1.2 or 2.0. TPM 1.2 will be the default setting. If necessary, use OneCLI to change the TPM version.
  - Migrations back and forth from TPM 1.2 and TPM 2.0 are limited to 128 iterations.

## Hardware replacement action overview

After logs have been analyzed and it has been determined that the correct service action is to replace parts, service personnel should take the following actions:

- Check the system's Maintenance Manual for part replacement steps.
  - After replacing a system board, service personnel must update the system VPD
  - It is recommended to upgrade the firmware of replacement parts to the latest version
  - For solution-level product parts replacement, service personnel must follow the Best Recipe to upgrade the firmware after parts replacement
- Watch parts replacement videos on Lenovo Learning Management System (LMS) or YouTube.

## Hardware replacement reference documents

Each system's hardware replacement procedures can be found in the following places:

- Downloadable PDF – Maintenance Manual on the [Lenovo Support](#) website
- Online resource – Hardware replacement procedures section on the [ThinkSystem Documentation](#) website

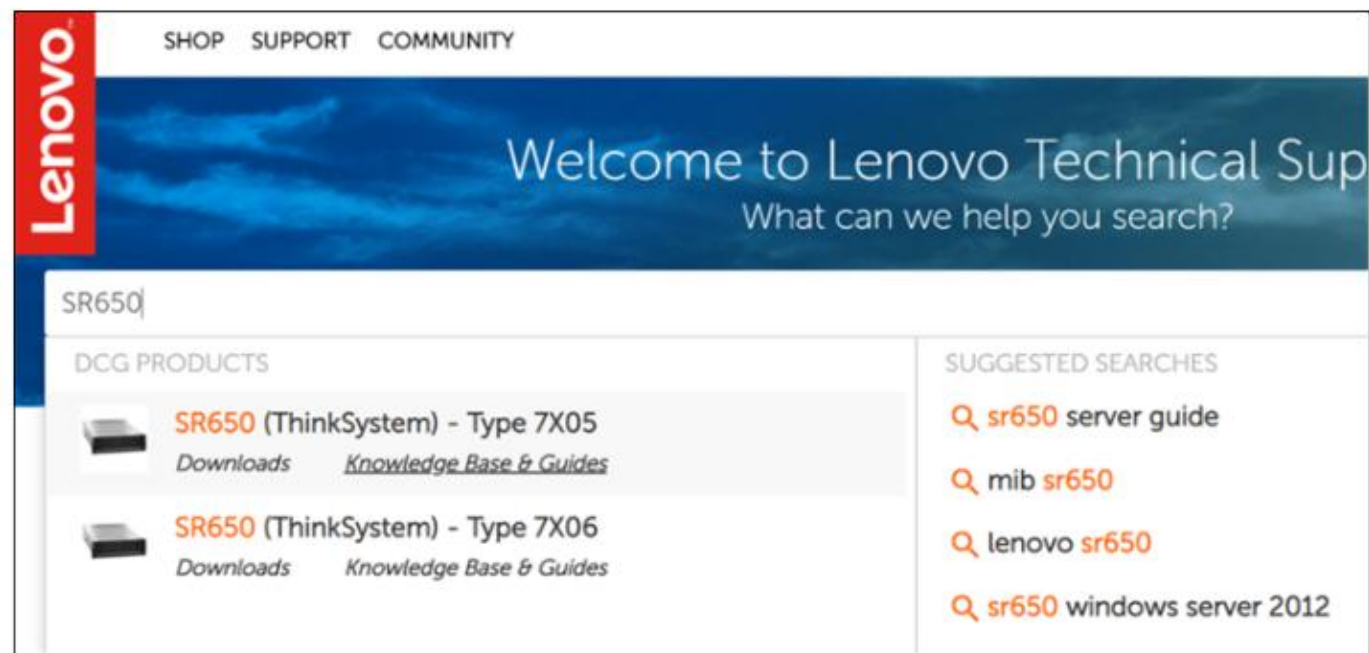
Click each number in turn to see more information.

Step



## Hardware replacement reference documents

To download the Maintenance Manual PDF, go to the [Lenovo Support](#) website and enter the system product name or machine type in the search bar. In this example, the SR650 machine type 7X05 was searched for.



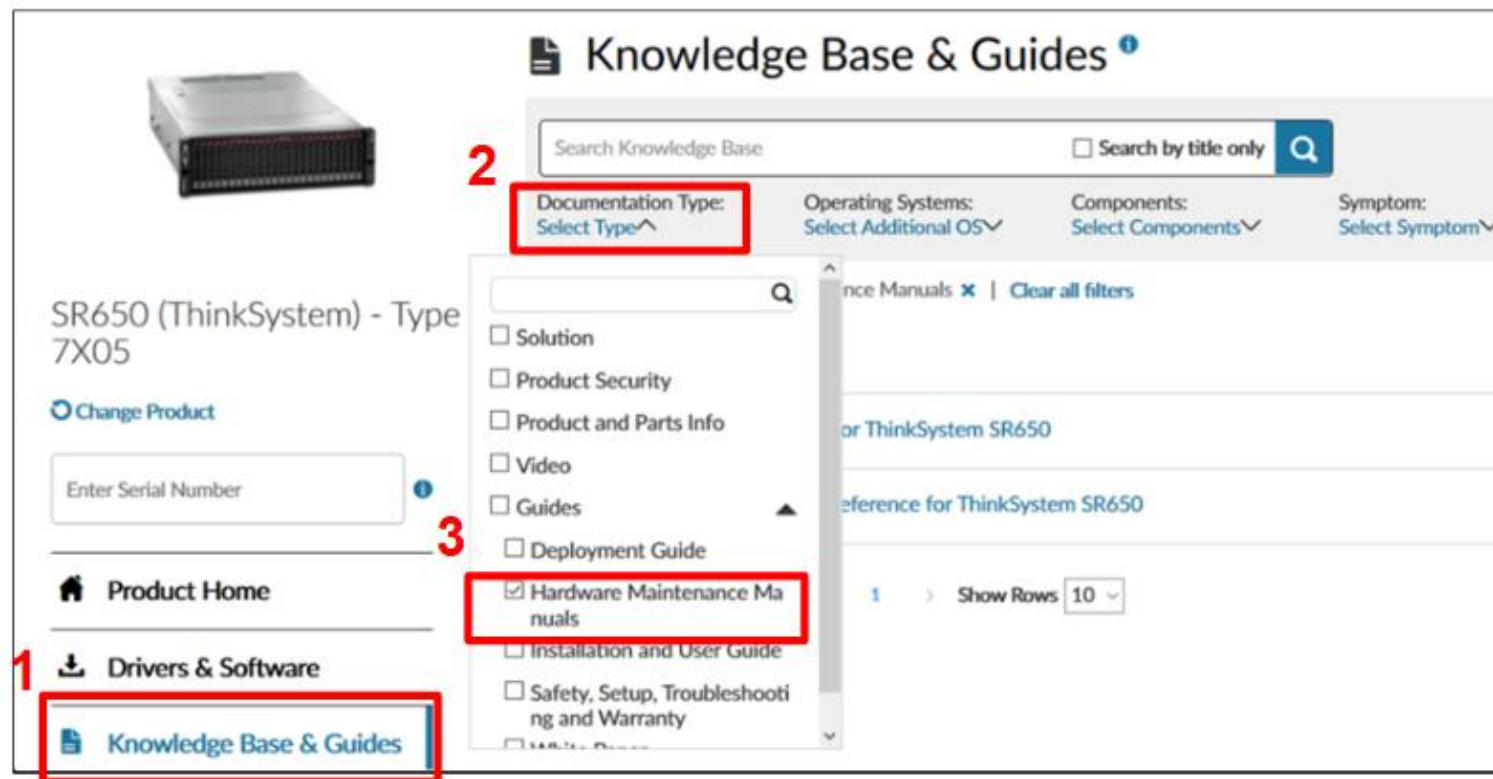
Step





# Hardware replacement reference documents

On the system download page, go to **Knowledge Base & Guides** → **Documentation Type**, and select **Hardware Maintenance Manuals**.




Step



# Hardware replacement reference documents

Click **Maintenance Manual** to see the PDF.




SR650 (ThinkSystem) - Type 7X05

[Change Product](#)

Enter Serial Number ?

## Knowledge Base & Guides ?

☐ Search by title only 

Documentation Type:  
[Select Type](#)▼



Operating Systems:  
[Select Additional OS](#)▼

Components:  
[Select Components](#)▼

Symptom:  
[Select Symptom](#)▼

Language:  
[Select Language](#)▼

Found 2 results: [Guides](#) ✕ | [Hardware Maintenance Manuals](#) ✕ | [Clear all filters](#)

Type	Title	Sort By <a href="#">Newest</a> ▼ Date
	<a href="#">Maintenance Manual for ThinkSystem SR650</a>	27 Oct 2017
	<a href="#">Messages and Codes reference for ThinkSystem SR650</a>	27 Oct 2017

Step

1

2

3

4

5

6

7

8

9



# Hardware replacement reference documents

In the Maintenance Manual table of contents, go to **Hardware replacement procedures**, and click a part name to jump to that section.

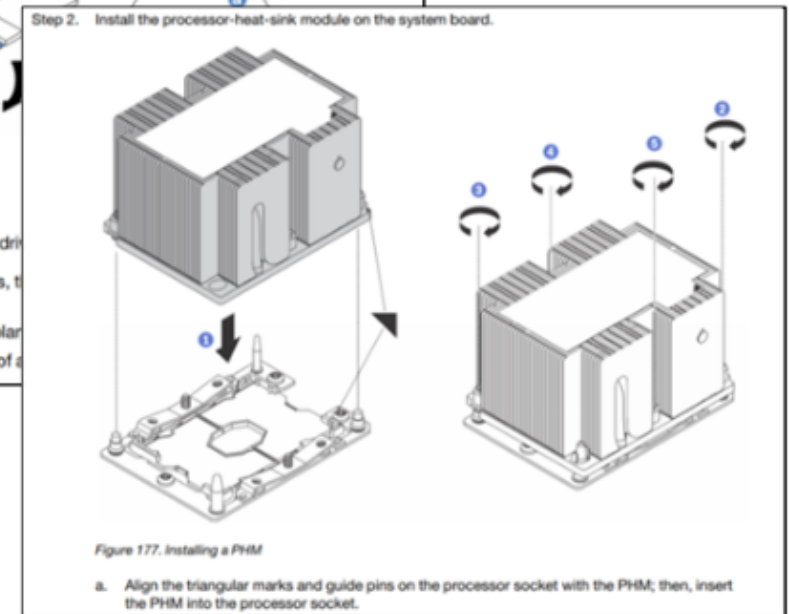
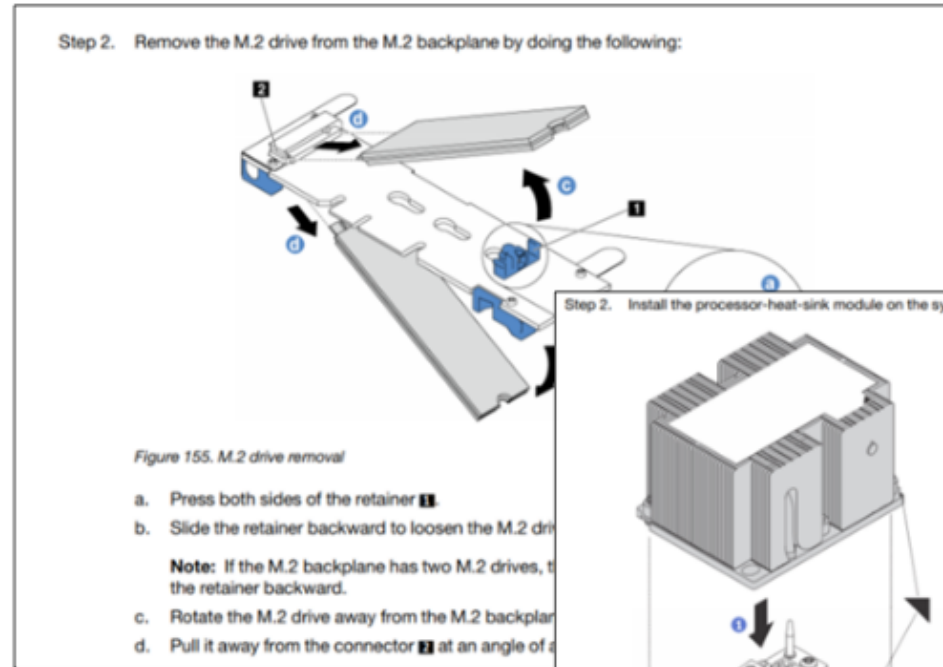
<b>Chapter 3. Hardware replacement procedures . . . . .</b>	<b>127</b>
Installation Guidelines . . . . .	127
System reliability guidelines . . . . .	128
Working inside the server with the power on . . . . .	128
Handling static-sensitive devices . . . . .	129
Security bezel replacement . . . . .	130
Remove the security bezel . . . . .	130
Install the security bezel . . . . .	131
Rack latches replacement . . . . .	133
Remove the rack latches . . . . .	133
Install the rack latches . . . . .	137
Top cover replacement . . . . .	141
Remove the top cover . . . . .	141
Install the top cover . . . . .	143
RAID super capacitor module replacement . . . . .	144

Step



# Hardware replacement reference documents

Refer to the procedures in the Maintenance Manual to replace the part.



Step





# Hardware replacement reference documents

For the online documents, go to the [ThinkSystem Documentation](#) website.



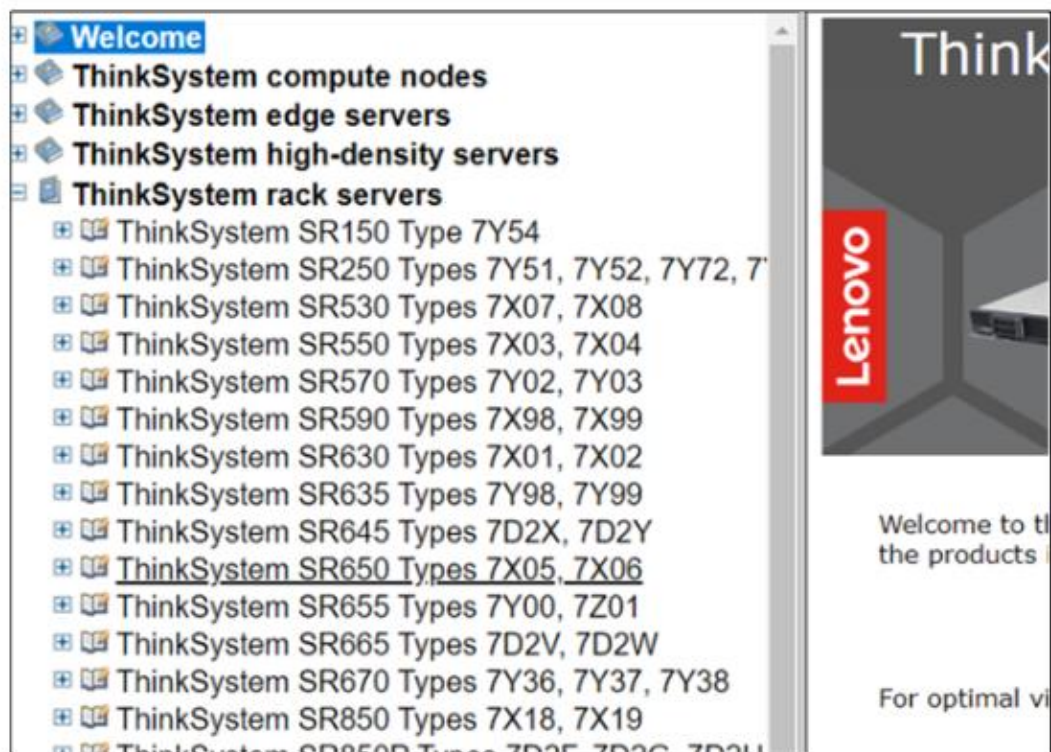
Step





# Hardware replacement reference documents

Select the system name from the left panel. In this example, the ThinkSystem SR650 was selected.

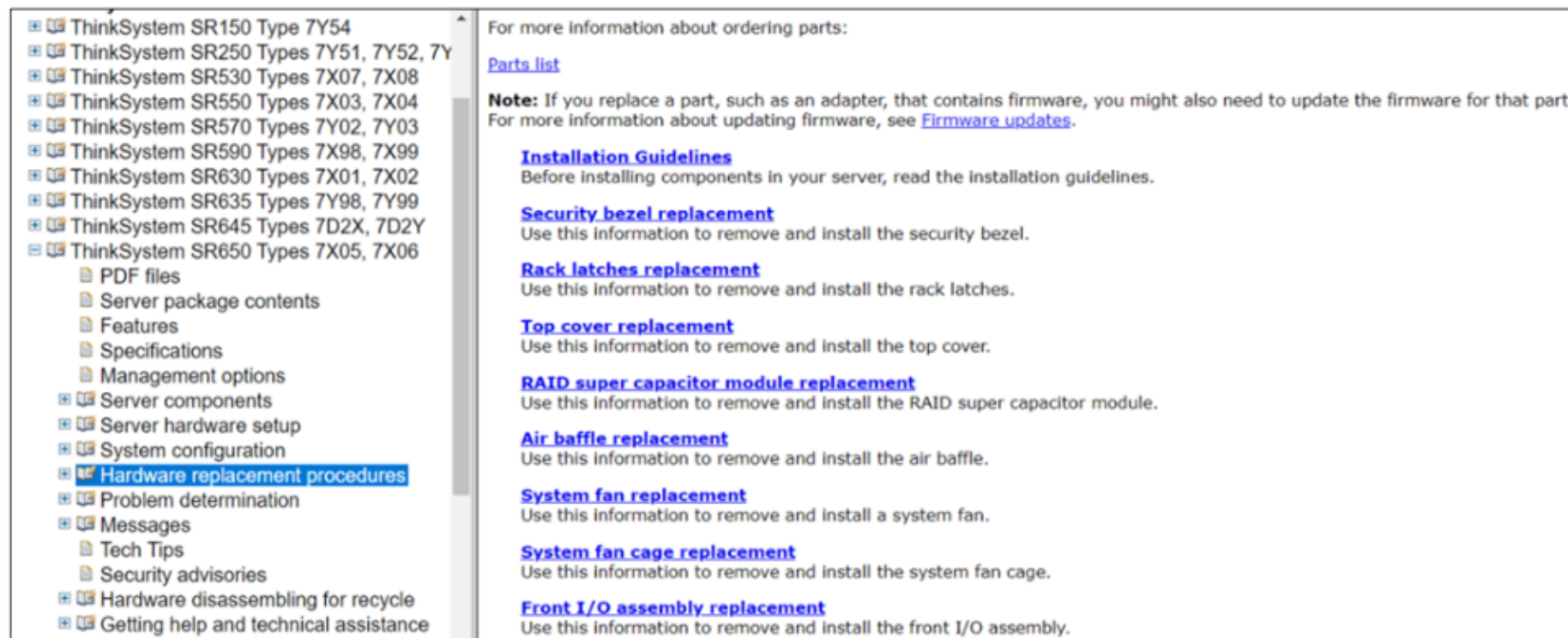


Step



# Hardware replacement reference documents

Under the system name, select **Hardware replacement procedures**.



The screenshot displays the Lenovo support website interface. On the left, a navigation menu lists various system models and categories. The 'Hardware replacement procedures' link is highlighted. The main content area on the right provides detailed information and links for hardware replacement.

For more information about ordering parts:  
[Parts list](#)

**Note:** If you replace a part, such as an adapter, that contains firmware, you might also need to update the firmware for that part. For more information about updating firmware, see [Firmware updates](#).

**Installation Guidelines**  
Before installing components in your server, read the installation guidelines.

**Security bezel replacement**  
Use this information to remove and install the security bezel.

**Rack latches replacement**  
Use this information to remove and install the rack latches.

**Top cover replacement**  
Use this information to remove and install the top cover.

**RAID super capacitor module replacement**  
Use this information to remove and install the RAID super capacitor module.

**Air baffle replacement**  
Use this information to remove and install the air baffle.

**System fan replacement**  
Use this information to remove and install a system fan.

**System fan cage replacement**  
Use this information to remove and install the system fan cage.

**Front I/O assembly replacement**  
Use this information to remove and install the front I/O assembly.

Step



# Hardware replacement reference documents

Select a specific part name to see the replacement procedures.

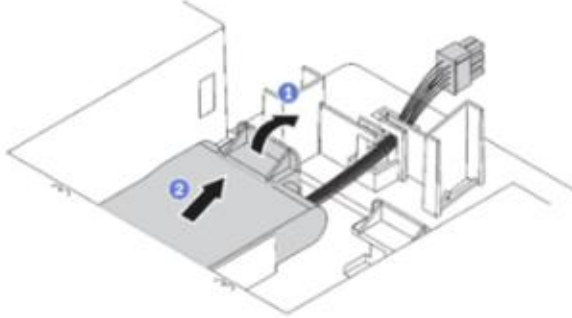
- PDF files
- Server package contents
- Features
- Specifications
- Management options
- Server components
- Server hardware setup
- System configuration
- Hardware replacement procedures
  - Installation Guidelines
  - Security bezel replacement
  - Rack latches replacement
  - Top cover replacement
  - RAID super capacitor module replacement
    - Remove a RAID super capacitor module**
    - Install a RAID super capacitor module
  - Air baffle replacement
  - System fan replacement
  - System fan cage replacement
  - Front I/O assembly replacement
  - Hot-swap drive replacement
  - Backplane replacement
  - memory module replacement
  - RAID adapter replacement
  - CMOS battery replacement
  - Riser card replacement
  - PCIe adapter replacement

To remove a RAID super capacitor module, complete the following steps:

**Watch the procedure.** A video of the removal process is available:

- Youtube: [Youtube](#)
- Youku: [Youku](#)

*Figure 1. RAID super capacitor module removal*



1. Gently press the tab on the air baffle as shown.
2. Remove the RAID super capacitor module from the air baffle.

If you are instructed to return the old RAID super capacitor module, follow all packaging instructions and use any packaging materials that are provided.

**Parent topic:** [RAID super capacitor module replacement](#)

Step





## After solving the problem

After solving the problem, service personnel should take the following actions:

- If support personnel had to replace a DIMM, drive, or DCPMM, use LXPM to run diagnostics to make sure the system status is healthy.
- Use OneCLI's `onecli logmr clearall` command to clear the BMC logs and system event logs (SEL) on the system.
  - The logs have already been captured and uploaded to the Lenovo Systems Care website.
  - There is a limit on the creation of SEL in UEFI (the maximum is 512). If logs are not cleared, it might not be possible for new logs to be created for problems in the future.

## How to run diagnostics in LXPM

After replacing a DIMM, HDD, or DCPMM, service personnel can use LXPM to run diagnostics to make sure the system works normally.

Complete the following steps to run diagnostics in LXPM.

**Note:** Do not use LXPM diagnostics to determine a problem. When a hardware issue occurs, XCC should report the error and there will be no need to run diagnostics. For problem determination, use the XCC dashboard, XCC service data, or OneCLI FFDC logs.

Click each number in turn to see the procedure.

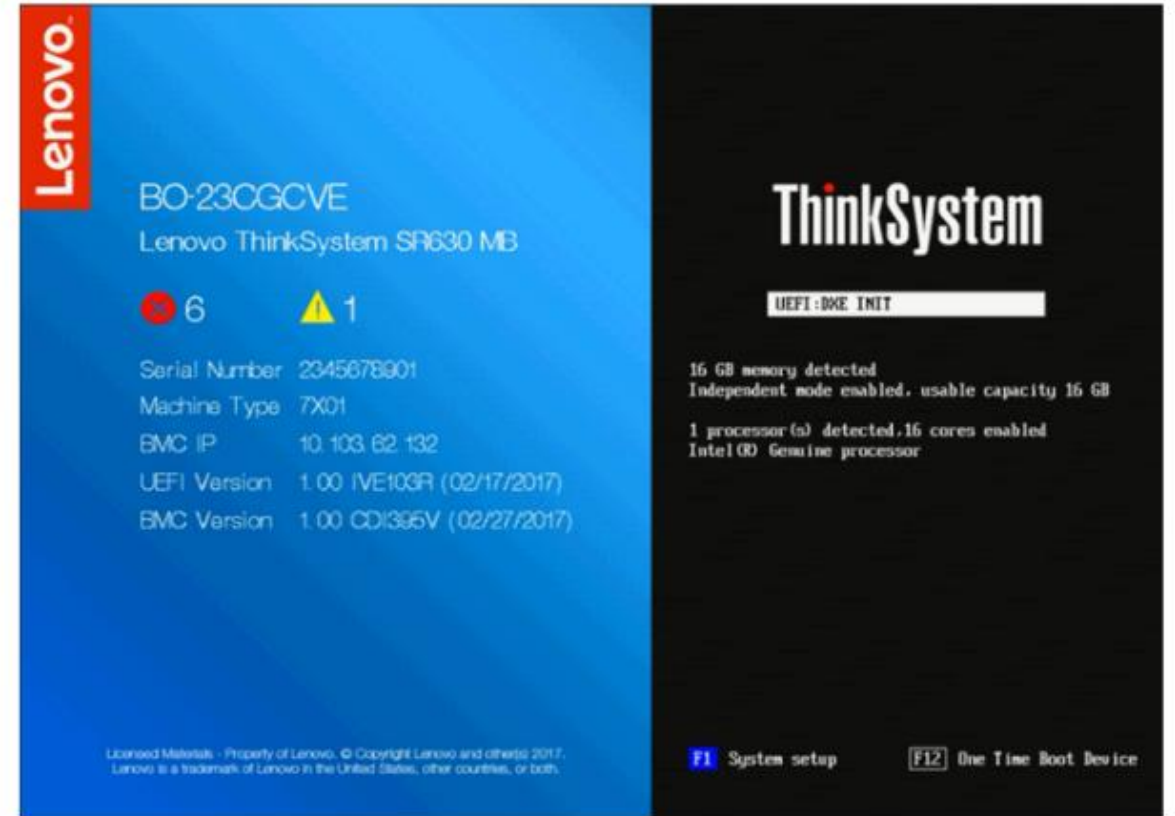
Step





# How to run diagnostics in LXPM

Press **F1** during the POST, and LXPM will be launched by default.

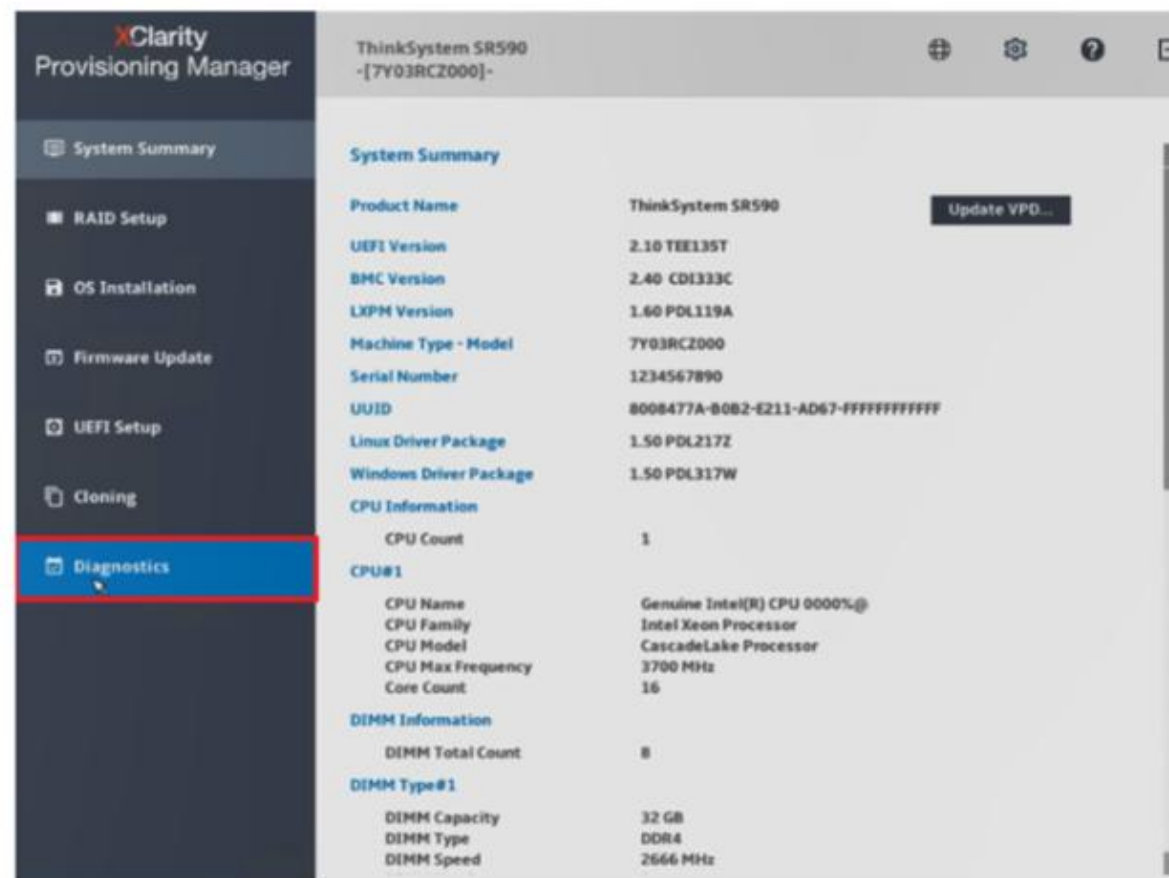


Step



# How to run diagnostics in LXPM

Select **Diagnostics** from the navigation menu.

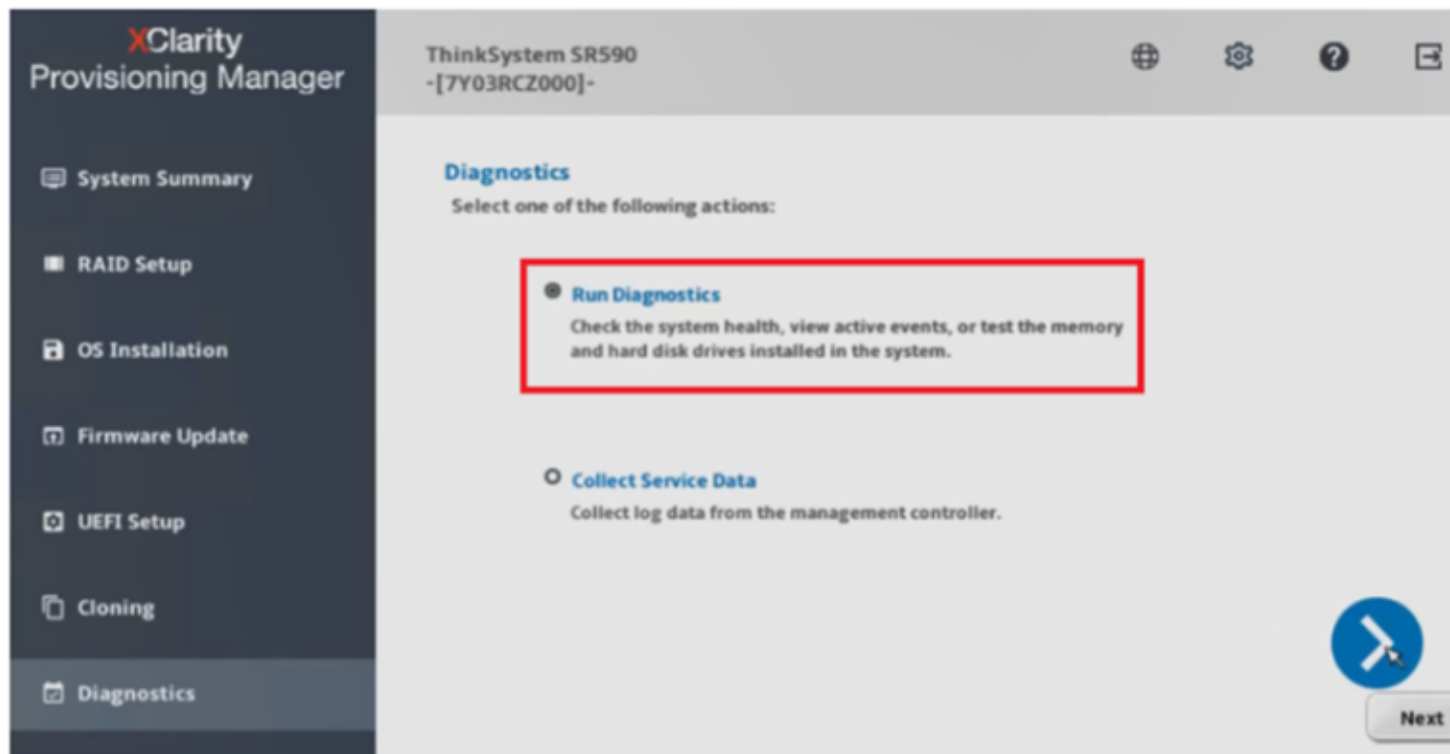


Step



# How to run diagnostics in LXPM

Select **Run Diagnostics**, and then click the **blue arrow**.



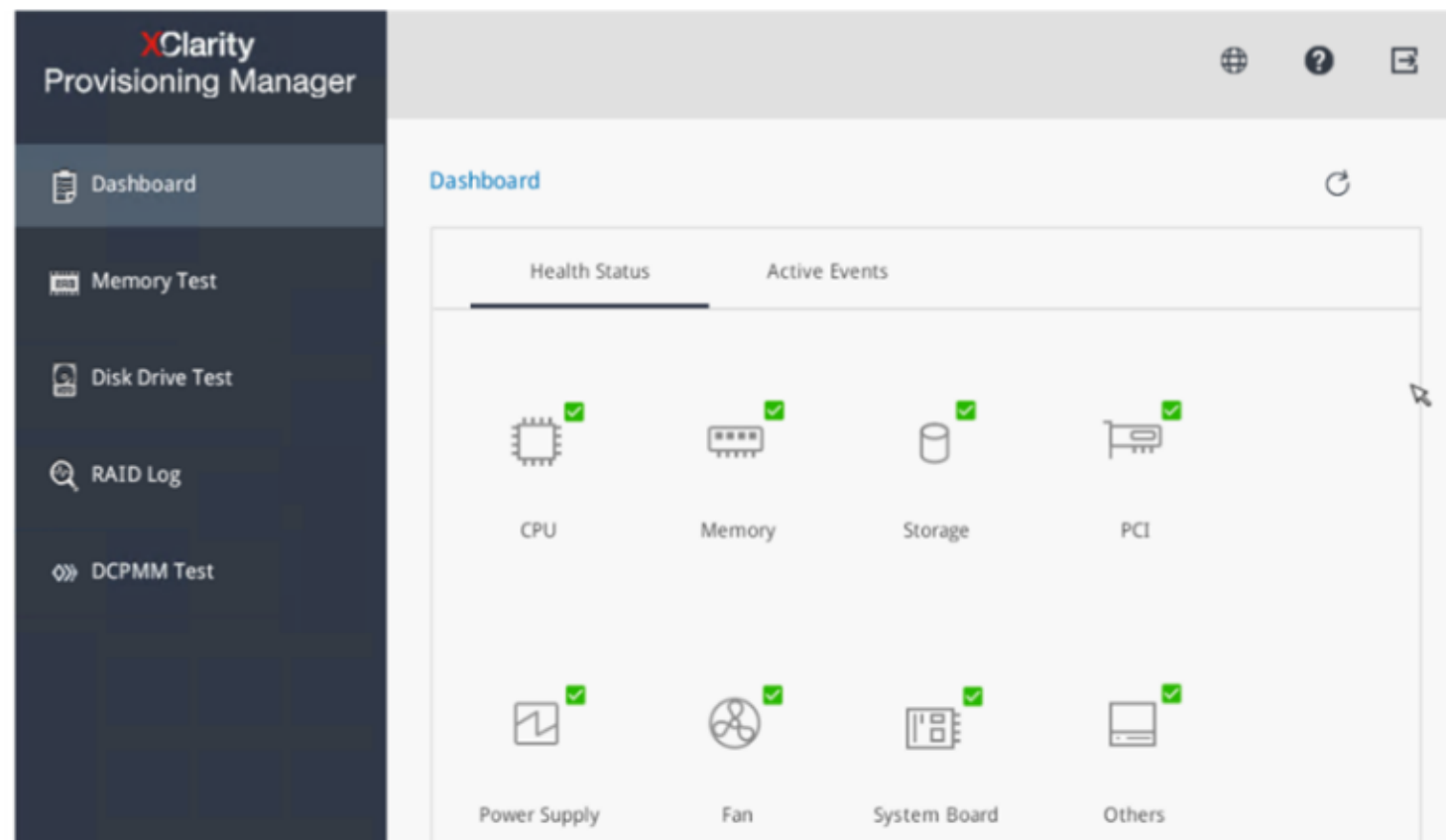
Step



# How to run diagnostics in LXPM

Three diagnostic tools are available in the diagnostics section:

- Memory Test
- Disk Drive Test
- DCPMM Test

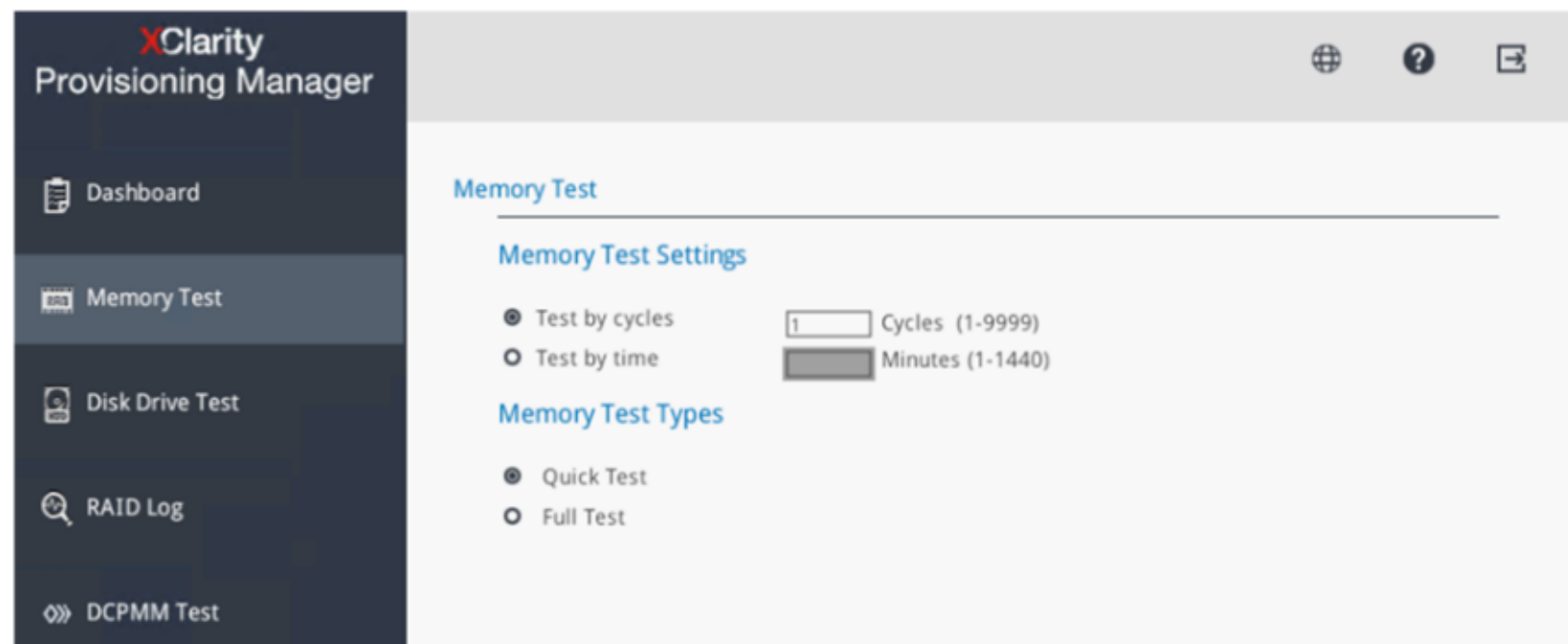


Step



# How to run diagnostics in LXPM

The **Memory Test** page allows users to run quick or full tests on the DIMMs installed in the server. Quick Tests run one test algorithm, while Full Tests run five test algorithms. Users can choose to run tests based on test cycles or test duration.



Step





# How to run diagnostics in LXPM

The **Disk Drive Test** page allows users to run quick or full tests on the drives installed in the server.

The screenshot shows the XClarity Provisioning Manager interface. On the left is a dark sidebar with navigation links: Dashboard, Memory Test, Disk Drive Test (highlighted), RAID Log, and DCPMM Test. The main content area is titled 'Disk Drive Test' and includes a 'Storage Test Option' section with radio buttons for 'Short Self Test' (selected) and 'Long Self Test'. Below this is a 'Storage Test Status' table with columns for Device Name, Status, Progress, and Duration. The table lists two drives, both with a status of '[Not Run]' and 0% progress. A 'Select All' checkbox is present at the top of the table. At the bottom of the main area, a notice states: 'Notice: The Disk Drive Test will take a few minutes. Press ESC to exit.'

Device Name	Status	Progress	Duration
<input checked="" type="checkbox"/> Select All			
<input checked="" type="checkbox"/> 09:ST1000NM0055:ZB50VWAZ	[Not Run]	0%	0seconds
<input checked="" type="checkbox"/> 10:ST1000NM0055:ZB50V1HW	[Not Run]	0%	0seconds

Step

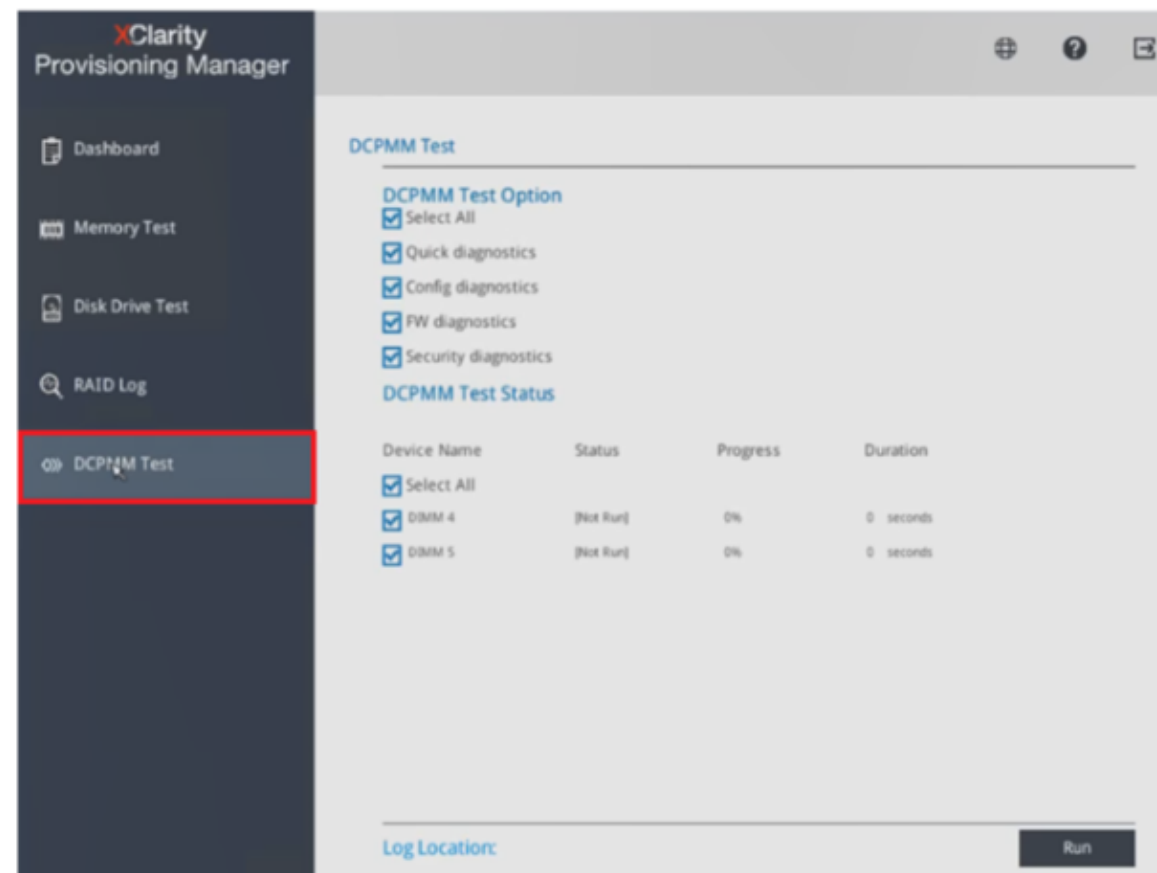


# How to run diagnostics in LXPM

The **DCPMM Test** page allows users to run tests on the DCPMMs installed in the server.

For more information about DCPMM Test, refer to the technical tips on the Lenovo website:

<https://datacentersupport.lenovo.com/us/en/products/servers/thinksystem/sr860/7x70/solutions/ht508255>



Step **1**—**2**—**3**—**4**—**5**—**6**—**7**



## Key takeaways

- Know what the possible issues are with different system components
- Understand the corresponding service actions for different server components
- Understand how to find the hardware replacement procedures on the Lenovo website
- Understand what actions need to be taken after solving the problem – this might include updating the VPD or clearing system event logs

## Quiz

Q: Which action shouldn't engineers take when the server LED light is lit?

**Collect service data from XCC**

**Run diagnostics on server components**

**Manually turn off the lit LED**