Tools for the ThinkSystem V3 server platform – overview

New tool features

Overview

The following software tools have been updated to support the ThinkSystem V3 platform:

- Lenovo XClarity Controller 2 (XCC2)
- Lenovo XClarity Provisioning Manager 4 (LXPM4)
- Lenovo XClarity Essentials
- UEFI
- Lenovo XClarity Administrator 4.0 (LXCA 4.0)

A new firmware and Root of Trust (RoT) security module mezzanine card will also be installed in V3 servers and the SE450 to provide an additional layer of security. The module is necessary for a system boot.
This card and the new versions of the software tools will be introduced in more detail in the following sections of this course.

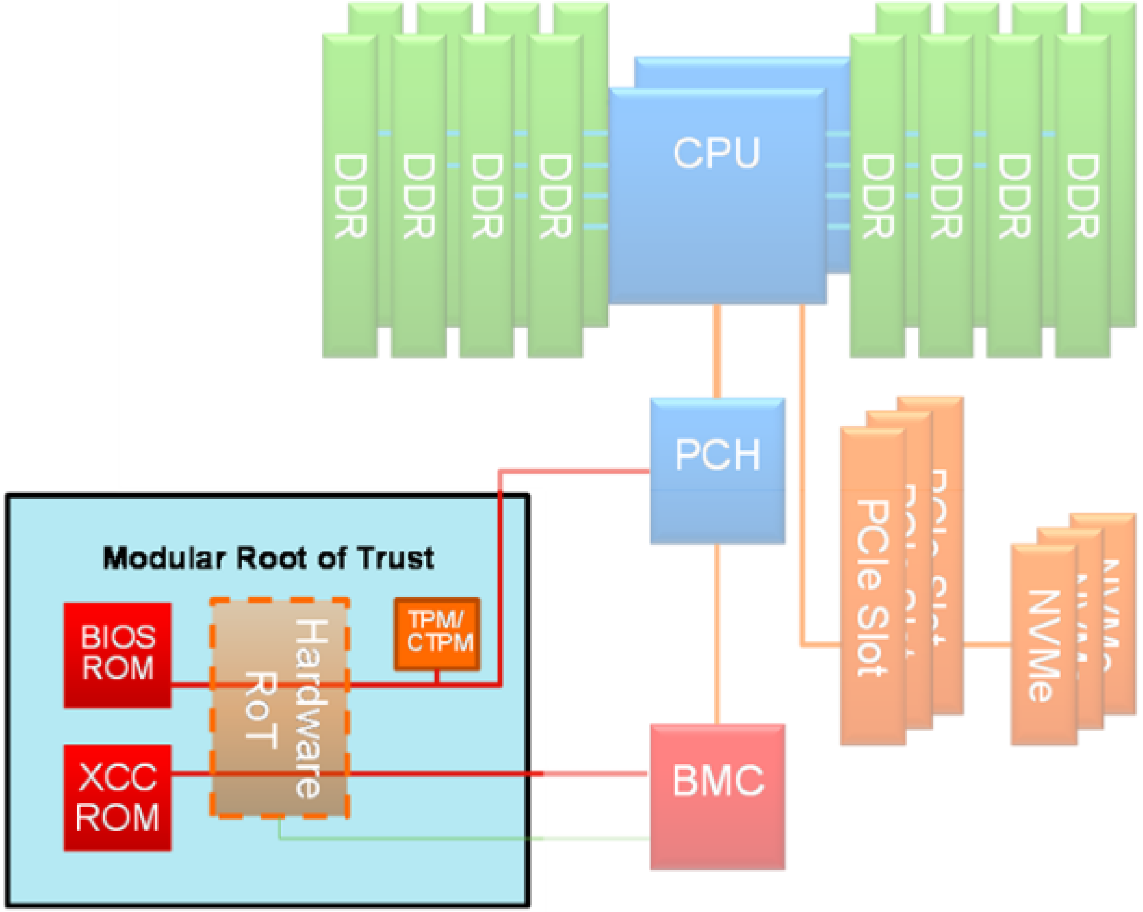
Firmware and Root of Trust security module

Features and problem determination

Firmware and Root of Trust security module overview

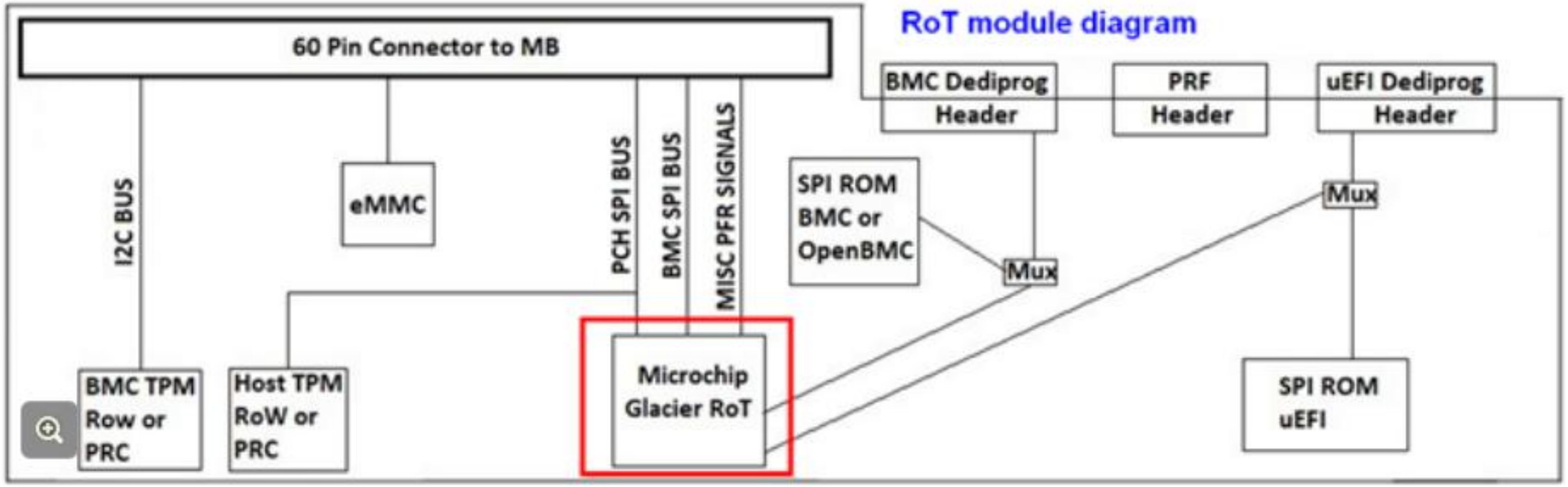
The firmware and Root of Trust (RoT) security module is a mezzanine card containing a Trusted Platform Module (TPM), UEFI SPI flash chip, XCC SPI flash chip, XCC eMMC storage, and Root of Trust silicon. The module is necessary for a system boot.

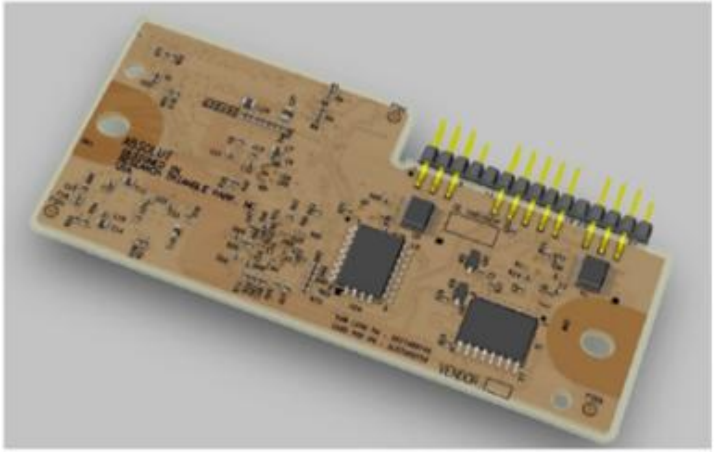
This module performs power-on time protection and validation of core boot elements for both XCC firmware and UEFI/BIOS firmware in a cryptographically secure fashion.

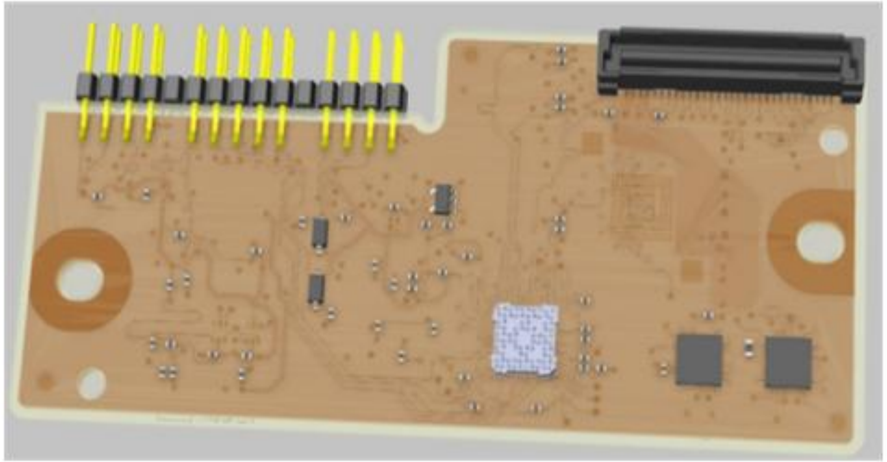


Note: The ASPEED AST2600 is the main BMC (XCC) chipset, and it's placed on the system board. While its firmware (XCC) is stored separately in an XCC SPI flash chip, the flash chip is now located on the firmware and RoT security module.

Firmware and RoT security module block diagram







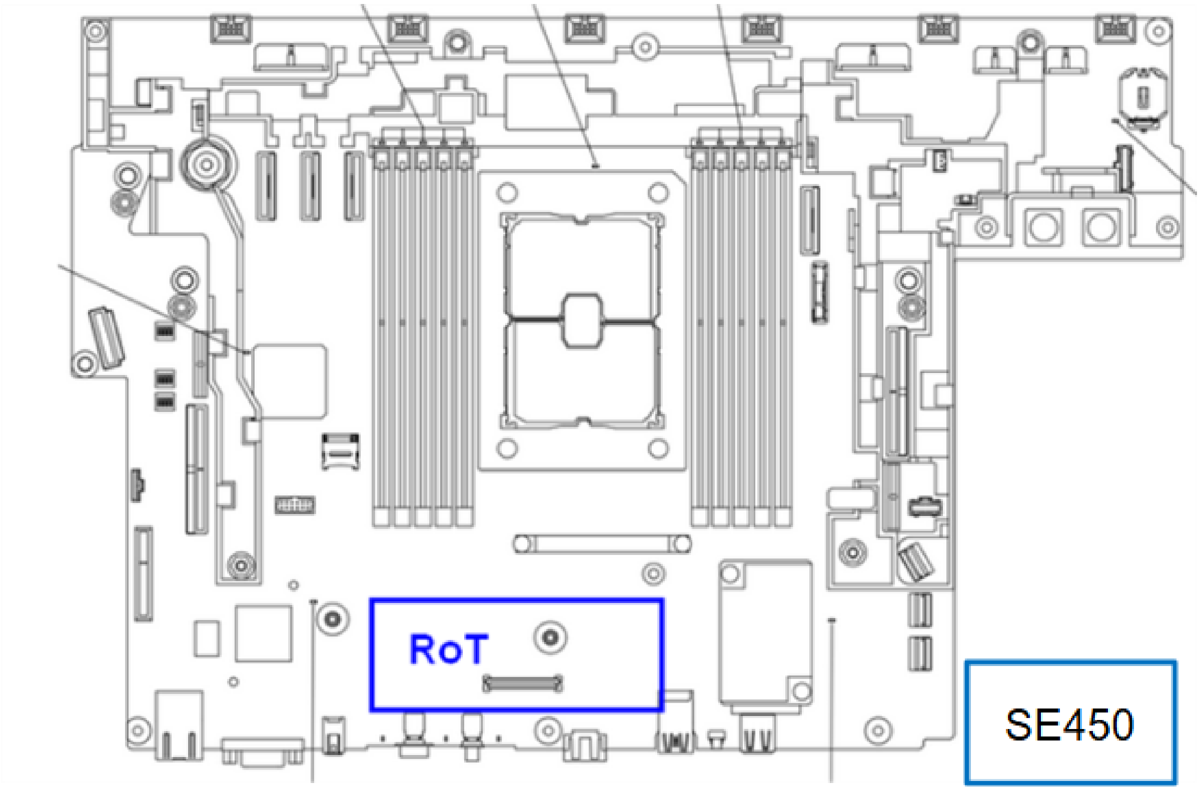
Modular RoT field support model

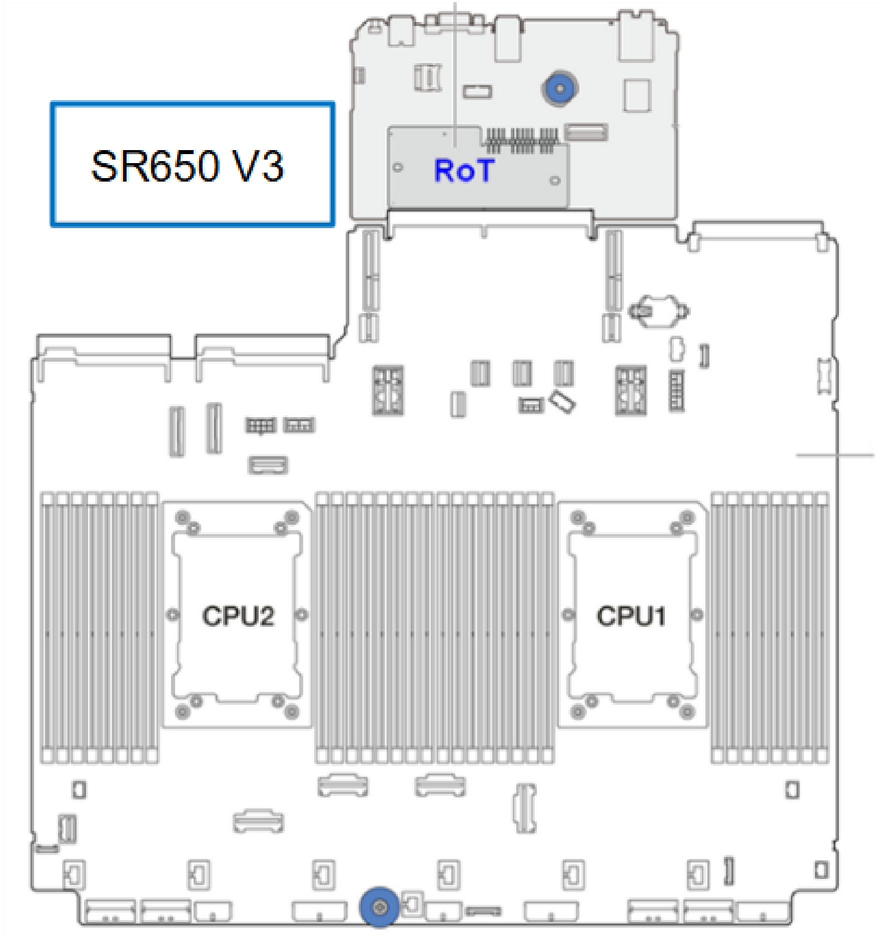
The firmware and RoT security module has a modular design, providing the following benefits for field servicing:

- The modular RoT card is small and contains relatively few components and no active regulation
  - Lessened risk of hardware fault verses a system planar
- The modular RoT card contains the main platform firmware
  - Enables field recovery of fully firmware-corrupted systems without requiring a system board replacement
  - Enables field replacement of system board FRU while maintaining customer code levels and configuration settings
- Single FRU model per RoT variant
  - Service stocks a single RoT FRU in each geographic region
    - All V3 servers use the same RoT FRU, but the SE450 uses a different version
  - Field support uses a pre-provisioned USB key in the service port, or conducts an offline update through the management network port to load platform-appropriate firmware. For more information, refer to the Updating RoT module firmware on V3 systems page in this course.

Locating the firmware and RoT security module

With the ThinkSystem V3 platform, the firmware and RoT security module is installed on the system I/O board. On the ThinkEdge SE450, it is installed on the system board. The two RoT module locations are shown below.





Firmware and RoT security module troubleshooting

V3 servers cannot boot without the firmware and RoT security module. If the system does not start, work through the following troubleshooting methods to identify whether the module or system board has failed.

Note: The power-control button will not function for approximately five to 10 seconds after the server has been connected to power.

Click each step in turn to see the procedure

Step 1 2

Firmware and RoT security module troubleshooting

If an additional optional device has recently been installed, remove it and turn on the server again. If the server now starts, it indicates that the optional device uses more power than the system can afford.

Check the power button LED:

- If the power button LED is lit, check the system event log.
  - If there is a readable system event log without UEFI errors, replace the system board.
  - If there is a readable system event log with UEFI errors, replace the firmware and roT security module.
  - If there is no readable system event log, but the power button LED is still lit, run diagnostic isolation on the replacement units listed below, and replace the faulty parts:
    - System board
    - Firmware and RoT security module

Step ① — ❷

Firmware and RoT security module troubleshooting

If the power button LED is not lit:

- Disconnect and reconnect the power cable.
- Make sure the power supplies are of the same type (the system-error LED would be lit if the power supply units do not match) and reseat all the units.
- Check if any power supply error LEDs are lit and replace any faulty units.
- If the problem persists, run diagnostic isolation on the replacement units listed below, and replace the faulty parts:
  - Power backplane
  - System board
  - Firmware and RoT security module

Step ❶—②

Common questions about the firmware and RoT security module

Scroll down for more information

Question	Answer
Can V3 servers boot without the firmware and RoT security module ?	The UEFI and XCC flash chips are on this module, and systems cannot boot without it.
Which configurations are on the firmware and RoT security module, and which configurations are on the system board? For example, XCC, UEFI, Intel VROC RAID configuration, hardware VPD	• The UEFI and XCC flash chips are on the firmware and RoT security module. • The VROC configuration is stored in the VROC member disks. • Hardware VPD is on system board.
Can you back up configurations from the firmware and RoT security module ?	• The UEFI and XCC flash chips are on this module. UEFI stores the system UEFI configuration in XCC, and you can back up and restore these configurations while the system is normal. The procedure used to back up and restore UEFI and XCC configurations is the same as on ThinkSystem servers. • Hardware VPD is on the system board. • The VROC configuration is stored in the VROC member disks. Unless there has been data corruption of the NVMe drives, the VROC configuration will not be lost. **Attention**: For the VROC configuration, users should keep VMD on. If the VMD is disabled and the OS is rebooted, it might trigger an OS data recovery mechanism that corrupts the VROC configuration/metadata, especially with a Windows OS.

Common questions about the firmware and RoT security module

Scroll down for more information

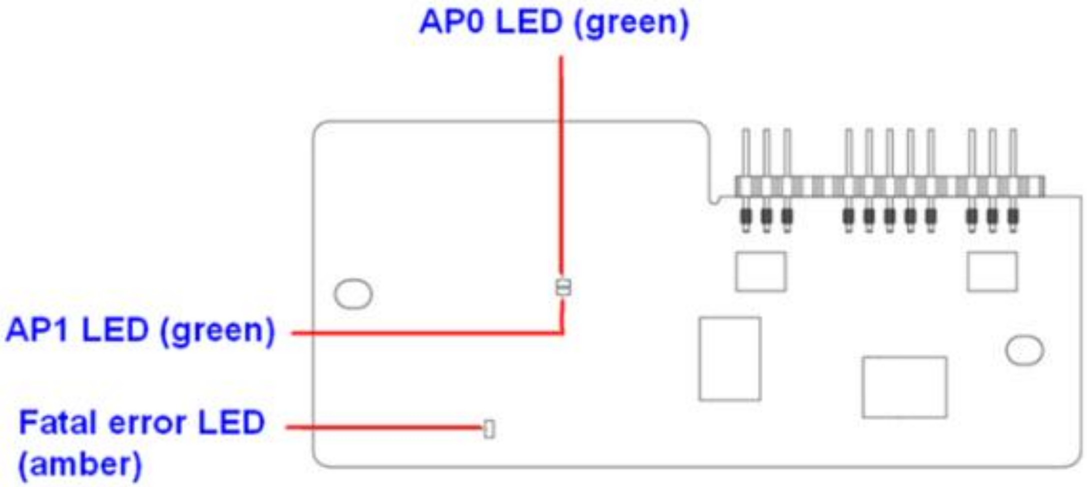
Question	Answer
Can you back up configurations from the firmware and RoT security module ?	• The UEFI and XCC flash chips are on this module. UEFI stores the system UEFI configuration in XCC, and you can back up and restore these configurations while the system is normal. The procedure used to back up and restore UEFI and XCC configurations is the same as on ThinkSystem servers. • Hardware VPD is on the system board. • The VROC configuration is stored in the VROC member disks. Unless there has been data corruption of the NVMe drives, the VROC configuration will not be lost. **Attention**: For the VROC configuration, users should keep VMD on. If the VMD is disabled and the OS is rebooted, it might trigger an OS data recovery mechanism that corrupts the VROC configuration/metadata, especially with a Windows OS.
Which service action should be taken after replacing the firmware and RoT security module but not the system board?	Restore the UEFI/XCC user configuration manually or by using OneCLI script.
Which service action should be taken after replacing the system board but not the firmware and RoT security module ?	Restore the necessary data in VPD.

Note: Refer to the Lenovo XClarity Controllers guide for more information.

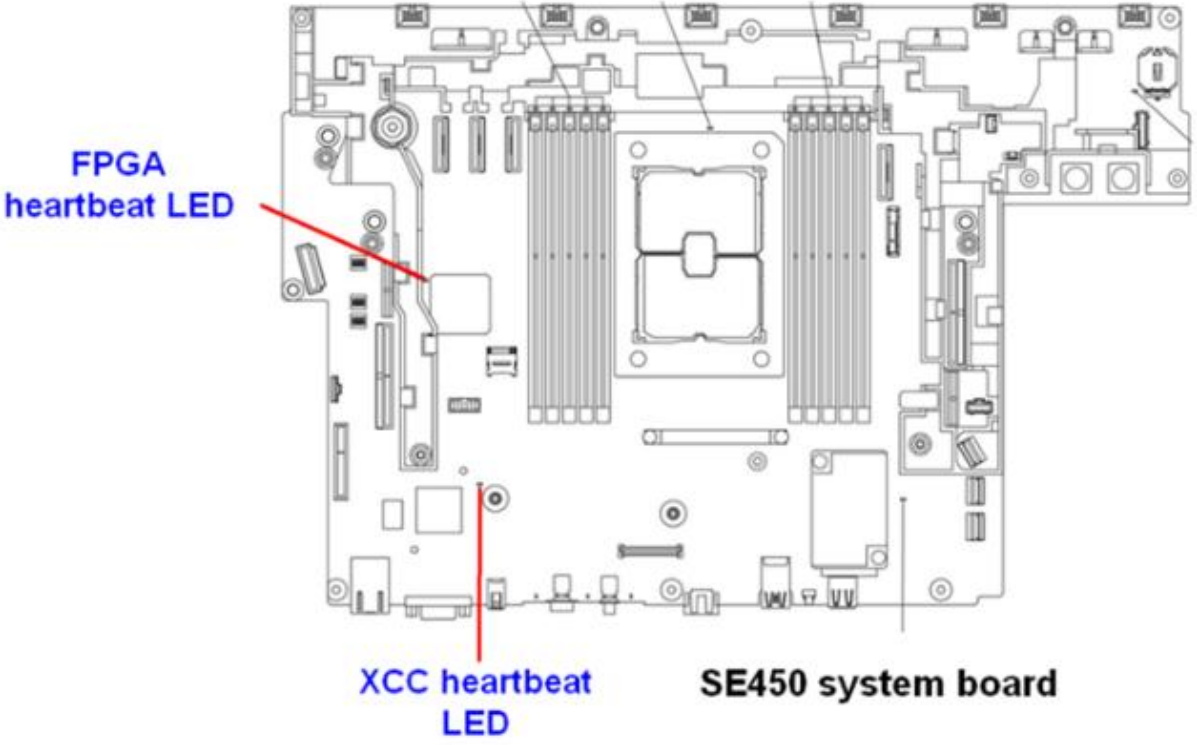
Firmware and RoT security module LEDs for troubleshooting

The firmware and RoT security module has additional LEDs that can help with the further investigation of issues. Servicers can use the LEDs on the firmware and RoT security module and on the system board to identify issues.

This example uses the SE450; refer to the next page for descriptions of these LEDs.



Firmware and RoT Security Module



SE450 system board

Firmware and RoT security module LEDs

Scroll down for more information

Scenario	AP0 LED	AP1 LED	Fatal error LED	FPGA heartbeat LED	XCC heartbeat LED	Actions
RoT security module fatal firmware failure	Off	Off	On	N/A	N/A	Replace the firmware and RoT security module
	Blinking	N/A	On	N/A	N/A	Replace the firmware and RoT security module
	Blinking	N/A	On	On	N/A	Replace the firmware and RoT security module
No system power (FPGA heartbeat LED off)	Off	Off	Off	Off	Off	If AC power is on, but the system board does not have power: 1. Check the power supply units (PSU) or power distribution board (PDB). If there is a PSU or PDB error, replace the defective PSU or PDB. 2. If the PSU and PDB are good, replace the system board (trained technicians only).
XCC firmware recoverable error	Blinking	N/A	Off	N/A	N/A	Information only – no action is required
XCC firmware has recovered from an error	On	N/A	Off	N/A	N/A	Information only – no action is required

Firmware and RoT security module LEDs

Scroll down for more information

Scenario	AP0 LED	AP1 LED	Fatal error LED	FPGA heartbeat LED	XCC heartbeat LED	Actions
off)						board does not have power: 1. Check the power supply units (PSU) or power distribution board (PDB). If there is a PSU or PDB error, replace the defective PSU or PDB. 2. If the PSU and PDB are good, replace the system board (trained technicians only).
XCC firmware recoverable error	Blinking	N/A	Off	N/A	N/A	Information only – no action is required
XCC firmware has recovered from an error	On	N/A	Off	N/A	N/A	Information only – no action is required
UEFI firmware authentication failure	N/A	Blinking	Off	N/A	N/A	Information only – no action is required
UEFI firmware has recovered from an authentication failure	N/A	On	Off	N/A	N/A	Information only – no action is required
System is OK (FPGA heartbeat LED is On)	On	On	Off	On	On	Information only – no action is required

Updating RoT module firmware on V3 systems

After replacing a firmware and RoT security module, servicers must update UEFI and LXPM firmware to the latest versions supported by the system before turning the system on. If this is not done, the system cannot start normally, and the user will not be able to access the system OS.

Use one of the following methods to update the UEFI, and LXPM firmware on the system:

- OneCLI commands
- A USB boot kit with UEFI firmware and LXPM firmware packages
  - For more information on how to create a USB boot kit, refer to the following GLOSSE article: How to create USB boot kit with OneCLI for RoT replacement in the field.

For the complete procedures, refer to the following GLOSSE tip page:

How to do RoT Module FW update on ThinkSystem V3 machines