Lenovo

ThinkSystem SR655
Messages and Codes Reference

Machine Types: 7Y00 and 7Z01

Note

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

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

Fifteenth Edition (May 2025)

Contents

Chapter 1. Messages

When attempting to resolve issues with your server, the best practice is to begin with the event log of the application that is managing the server:

The event log contains server hardware events that are recorded by the Lenovo ThinkSystem System Manager or by UEFI.In addition, events can be generated when you perform diagnostic testing on hard drives or memory through the Lenovo XClarity Provisioning Manager (although these events are not stored in the event (although these events are not stored in the event log).

Use this section to view the events that can be generated by Lenovo ThinkSystem System Manager or UEFI. For each event, a user action is available to help you understand what must be done to resolve the issue.

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

Chapter 2. BMC error messages

When a hardware event is detected by the BMC on the server, the BMC writes that event in the system-event log on the server.

For information about viewing the event log, see the *ThinkSystem SR655 Maintenance Manual*. For additional information about the BMC event log, see https://thinksystem.lenovofiles.com/help/topic/7Y00/bmc_user_guide.pdf.

For each event code, the following fields are displayed:

Event identifier
An identifier that uniquely identifies an event.

Explanation
Provides additional information to explain why the event occurred.

Severity
An indication of the level of concern for the condition. The following severities can be displayed.

- **Informational**. The event was recorded for audit purposes, usually a user action or a change of states that is normal behavior.
- **Warning**. The event is not as severe as an error, but if possible, the condition should be corrected before it becomes an error. It might also be a condition that requires additional monitoring or maintenance.
- **Error**. The event is a failure or critical condition that impairs service or an expected function.

Serviceable
Specifies whether user action is required to correct the problem.

Automatically contact Service
You can configure the Lenovo XClarity Administrator to automatically notify Support (also known as call home) if certain types of errors are encountered. If you have configured this function and this field is set to Yes,Lenovo Support will be notified automatically if the event is generated. While you wait for Lenovo Support to call, you can perform the recommended actions for the event.

Note: This documentation includes references to IBM web sites, products, and information about obtaining service. IBM is Lenovo's preferred service provider for the Lenovo server products.

For more information about enabling Call Home from Lenovo XClarity Administrator, see http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/admin_setupcallhome.html.

User response
Indicates what actions you should perform to solve the event. Perform the steps listed in this section in the order shown until the problem is solved. If you cannot solve the problem after performing all steps, contact Lenovo Support.

BMC events that automatically notify Support

You can configure the XClarity Administrator to automatically notify Support (also known as *call home*) if certain types of errors are encountered. If you have configured this function, see the table for a list of events that automatically notify Support.

Table 1. Events that automatically notify Support

Event ID	Message String
A01011009	The specified temperature upper critical going high asserted
A0101200B	The specified temperature upper non recoverable going high asserted
A02010800	The specified voltage lower non critical going low asserted
A02010807	The specified voltage upper non critical going high asserted
A02011009	The specified voltage upper critical going high asserted
A02012004	The specified voltage lower non recoverable going low asserted
A0201200B	The specified voltage upper non recoverable going high asserted
A04011002	The specified Fan speed lower critical going low asserted
A086F1001	This message is for the use case when an implementation has detected a Power Supply has failed.
A0D6F1001	The specified drive fault asserted
A216F1000	The specified cable/card detected a Fault asserted.

BMC events organized by severity

The following table lists all BMC events, organized by severity (Information, Error, and Warning).

Table 2. Events organized by severity

Event ID	Message String	Severity
A01810400	Inlet_Temp temperature lower non critical going low deasserted	Informational
A01810407	The specified temperature upper non critical going high deasserted	Informational
A01810409	The specified temperature upper critical going high deasserted	Informational
A0181040B	The specified temperature upper non recoverable going high deasserted	Informational
A02810400	The specified voltage lower non critical going low deasserted	Informational
A02810402	The specified voltage lower critical going low deasserted	Informational
A02810404	The specified voltage lower non recoverable going low deasserted	Informational
A02810407	The specified voltage upper non critical going high deasserted	Informational
A02810409	The specified voltage upper critical going high deasserted	Informational
A0281040B	The specified voltage upper non recoverable going high deasserted	Informational
A04090200	The specified PSU Fan device disabled asserted	Informational
A04810400	The specified Fan speed lower non critical going low deasserted	Informational
A04810402	The specified Fan speed lower critical going low deasserted	Informational
A056F0200	Chassis_Intr or physical_security intrusion asserted	Informational
A05EF0200	Chassis_Intr or physical_security intrusion deasserted	Informational
A07030201	The specified processor state asserted	Informational

Table 2. Events organized by severity (continued)

Event ID	Message String	Severity
A07830201	The specified processor state asserted	Informational
A086F0200	The specified power supply presence detected asserted	Informational
A08870202	This message is for the use case when an implementation has detected a **Power Supply** type asserted event.	Informational
A08EF0200	The specified power supply presence detected deasserted	Informational
A08EF0401	The specified power supply failure deasserted	Informational
A08EF0402	The specified power supply predictive failure deasserted	Informational
A08EF0403	The specified power supply input lost ac or dc deasserted	Informational
A08EF0406	The specified power supply configuration error deasserted	Informational
A0B8B0206	Cooling_Status redundancy degraded from fully redundant deasserted	Informational
A0C6F0204	The specified memory device disabled asserted	Informational
A0D6F0200	The specified drive presence asserted	Informational
A0D6F0207	The specified drive rebuild or remap in progress asserted	Informational
A0DEF0200	The specified drive presence deasserted	Informational
A0DEF0207	The specified drive rebuild or remap in progress deasserted	Informational
A0DEF0401	The specified drive fault deasserted	Informational
A106F0202	Log area reset asserted	Informational
A106F0204	sel full asserted	Informational
A136F0200	Front Panel NMI / Diagnostic Interrupt deasserted	Informational
A146F0200	power button pressed asserted	Informational
A16090201	BMC_Boot_Up asserted	Informational
A1B6F0200	The specified cable is connected asserted	Informational
A21EF0400	The specified cable/card detected a Fault deasserted.	Informational
A226F0200	ACPI in s0/g0 working State	Informational
A226F0205	ACPI in s5/g2 soft off state	Informational
A236F0200	Watchdog2 timer expired asserted	Informational
A236F0201	Watchdog2 hard reset asserted	Informational
A236F0202	Watchdog2 power down asserted	Informational
A236F0203	Watchdog2 power cycle asserted	Informational
A236F0208	Watchdog2 timer interrupt asserted	Informational
A01010800	Inlet_Temp temperature lower non critical going low asserted	Warning
A01010807	The specified temperature upper non critical going high asserted	Warning
A02010800	The specified voltage lower non critical going low asserted	Warning
A02010807	The specified voltage upper non critical going high asserted	Warning

Table 2. Events organized by severity (continued)

Event ID	Message String	Severity
A04010800	The specified Fan speed lower non critical going low asserted	Warning
A08070802	The specified power supply transition to critical from less severe asserted	Warning
A086F0802	The specified power supply predictive failure asserted asserted	Warning
A086F0803	The specified power supply input lost ac or dc asserted	Warning
A0B0B0806	Cooling_Status redundancy degraded from fully redundant asserted	Warning
A106F0805	sel almost full asserted	Warning
A01011009	The specified temperature upper critical going high asserted	Error
A0101200B	The specified temperature upper non recoverable going high asserted	Error
A02011002	The specified voltage lower critical going low asserted	Error
A02011009	The specified voltage upper critical going high asserted	Error
A02012004	The specified voltage lower non recoverable going low asserted	Error
A0201200B	The specified voltage upper non recoverable going high asserted	Error
A04011002	The specified Fan speed lower critical going low asserted	Error
A080B1001	The specified power supply redundancy lost asserted	Error
A086F1001	This message is for the use case when an implementation has detected a Power Supply has failed.	Error
A086F1006	The specified power supply configuration error asserted	Error
A0C071002	This message is for the use case when an implementation has detected a **Memory** type asserted event.	Error
A0C6F1007	This message is for the use case when an implementation has detected a Memory DIMM configuration error.	Error
A0D6F1001	The specified drive fault asserted	Error
A136F1000	This message is for the use case when an implementation has detected a Front Panel NMI / Diagnostic Interrupt.	Error
A1B6F1001	Fan type configuration error asserted	Error
A216F1000	The specified cable/card detected a Fault asserted.	Error

List of BMC events

This section lists all messages that can be sent from BMC.

- **A01010800: Inlet_Temp temperature lower non critical going low asserted**

  Lower Non-Critical - Going Low

  Severity: Warning
  Serviceable: No
  Automatically notify Support: No

  User Action:

No action

- **A01010807: The specified temperature upper non critical going high asserted**

  Upper Non-Critical - Going High

  Severity: Warning
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Check the BMC event logs for any cooling issues.
  2. Make sure that the airflow in the front and rear of the chassis is not obstructed and that fillers are correctly installed in place.
  3. Make sure that the room temperature is within the range specified in the operating environment specifications.
  4. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A01011009: The specified temperature upper critical going high asserted**

  Upper Critical - Going High

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. Check the BMC event logs for any cooling issues.
  2. Make sure that the airflow in the front and rear of the chassis is not obstructed and that fillers are correctly installed in place.
  3. Make sure that the room temperature is within the range specified in the operating environment specifications.
  4. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A0101200B: The specified temperature upper non recoverable going high asserted**

  Upper Non_Recoverable-Going High

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. Check the BMC event logs for any cooling issues.
  2. Make sure that the airflow in the front and rear of the chassis is not obstructed and that fillers are correctly installed in place.
  3. Make sure that the room temperature is within the range specified in the operating environment specifications.

4. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A01810400: Inlet_Temp temperature lower non critical going low deasserted**

  Lower Non-Critical - Going Low

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A01810407: The specified temperature upper non critical going high deasserted**

  Upper Non-Critical - Going High

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A01810409: The specified temperature upper critical going high deasserted**

  Upper Critical - Going High

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A0181040B: The specified temperature upper non recoverable going high deasserted**

  Upper Non_Recoverable-Going High

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A02010800: The specified voltage lower non critical going low asserted**

  Lower Non-Critical - Going Low

  Severity: Warning
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. If the specified sensor is VDD_33_RUN, VDD_5_DUAL, or VDD_5_RUN, replace the system board (trained technician only).

2. If the specified sensor is P12V_RUN, check BMC event logs for power-supply-related issues and resolve those issues.
3. If the problem remains, replace the system board (trained technician only).
4. Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.
5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A02010807: The specified voltage upper non critical going high asserted**

  Upper Non-Critical - Going High

  Severity: Warning
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. If the specified sensor is VDD_33_RUN, VDD_5_DUAL, or VDD_5_RUN, replace the system board (trained technician only).
  2. If the specified sensor is P12V_RUN, check BMC event logs for power-supply-related issues and resolve those issues.
  3. If the problem remains, replace the system board (trained technician only).
  4. Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.
  5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A02011002: The specified voltage lower critical going low asserted**

  Lower Critical - Going Low

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. If the specified sensor is VDD_33_RUN, VDD_5_DUAL, or VDD_5_RUN, replace the system board (trained technician only).
  2. If the specified sensor is P12V_RUN, check BMC event logs for power-supply-related issues and resolve those issues.
  3. If the problem remains, replace the system board (trained technician only).
  4. Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.
  5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A02011009: The specified voltage upper critical going high asserted**

  Upper Critical - Going High

  Severity: Error
  Serviceable: Yes

Automatically notify Support: Yes

User Action:

Complete the following steps until the problem is solved:

1. If the specified sensor is VDD_33_RUN, VDD_5_DUAL, or VDD_5_RUN, replace the system board (trained technician only).
2. If the specified sensor is P12V_RUN, check BMC event logs for power-supply-related issues and resolve those issues.
3. If the problem remains, replace the system board (trained technician only).
4. Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.
5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A02012004: The specified voltage lower non recoverable going low asserted**

  Lower Non_Recoverable-Going Low

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. If the specified sensor is VDD_33_RUN, VDD_5_DUAL, or VDD_5_RUN, replace the system board (trained technician only).
  2. If the specified sensor is P12V_RUN, check BMC event logs for power-supply-related issues and resolve those issues.
  3. If the problem remains, replace the system board (trained technician only).
  4. Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.
  5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A0201200B: The specified voltage upper non recoverable going high asserted**

  Upper Non_Recoverable-Going High

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. If the specified sensor is VDD_33_RUN, VDD_5_DUAL, or VDD_5_RUN, replace the system board (trained technician only).
  2. If the specified sensor is P12V_RUN, check BMC event logs for power-supply-related issues and resolve those issues.
  3. If the problem remains, replace the system board (trained technician only).
  4. Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A02810400: The specified voltage lower non critical going low deasserted**

  Lower Non-Critical - Going Low

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A02810402: The specified voltage lower critical going low deasserted**

  Lower Critical - Going Low

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A02810404: The specified voltage lower non recoverable going low deasserted**

  Lower Non_Recoverable-Going Low

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A02810407: The specified voltage upper non critical going high deasserted**

  Upper Non-Critical - Going High

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A02810409: The specified voltage upper critical going high deasserted**

  Upper Critical - Going High

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A0281040B: The specified voltage upper non recoverable going high deasserted**

  Upper Non_Recoverable-Going High

Severity: Information
Serviceable: No
Automatically notify Support: No

User Action:

No action

- **A04010800: The specified Fan speed lower non critical going low asserted**

  Lower Non-Critical - Going Low

  Severity: Warning
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Reseat the failing fan indicated by BMC event logs.
  2. If the event still exists, replace the fan.
  3. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A04011002: The specified Fan speed lower critical going low asserted**

  Lower Critical - Going Low

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. Reseat the failing fan indicated by BMC event logs.
  2. If the event still exists, replace the fan.
  3. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A04090200: The specified PSU Fan device disabled asserted**

  Device Disabled

  Severity: Information
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Make sure that there are no obstructions, such as bundled cables, to power-supply airflow.
  2. Reseat power supply n. If the problem persists, replace power supply n. (n = power supply number)
  3. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A04810400: The specified Fan speed lower non critical going low deasserted**

  Lower Non-Critical - Going Low

Severity: Information
Serviceable: No
Automatically notify Support: No

User Action:

No action

- **A04810402: The specified Fan speed lower critical going low deasserted**

  Lower Critical - Going Low

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A056F0200: Chassis_Intr or physical_security intrusion asserted**

  General Chassis Intrusion

  Severity: Information
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Reseat the chassis cover.
  2. Check if the Intrusion Switch is present. If yes, inspect Intrusion Switch Cable for damage and make sure it's not loose.
  3. Check the active events and confirm that the "chassis sensor" has de-asserted.
  4. If the problem continues, collect the Service Data log and contact Lenovo Support.

- **A05EF0200: Chassis_Intr or physical_security intrusion deasserted**

  General Chassis Intrusion

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A07030201: The specified processor state asserted**

  State Asserted

  Severity: Information
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  If the specified sensor is CPU_ALERT, replace the processor (trained technician only). If the specified sensor is CPU_Prochot, complete the following steps until the problem is solved:

  1. Check the BMC event logs for any fan, cooling or power related issues.

2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are correctly installed in place.
3. Make sure that the room temperature is within the range specified in the operating environment specifications.
4. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

If the specified sensor is CPU_Thermaltrip, complete the following steps until the problem is solved:

1. Check the BMC event logs for any fan or cooling issues.
2. Make sure that the airflow at the front and rear of the chassis is not obstructed and that fillers are in place and correctly installed.
3. Make sure that the room temperature is within the range specified in operating environment specifications.
4. Make sure that the processor and heat sink are securely installed.
5. Make sure that the thermal grease is correctly applied.
6. If the problem persists, replace the processor and heat sink(trained technician only).
7. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A07830201: The specified processor state asserted**

  State deasserted

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A08070802: The specified power supply transition to critical from less severe asserted**

  Transition to critical from less severe

  Severity: Warning
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  The two power supply units installed on the server are of different input type and power rating. Complete the following steps until the problem is solved:

  1. Check the input type and power rating of the installed power supply units to make sure they match.
  2. Re-calculate the required power capacity by using Lenovo Capacity Planner (https://datacentersupport.lenovo.com/solutions/lnvo-lcp).
  3. Install matching power supply units (same input type and wattage) and confirm they meet the system power requirements.
  4. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A080B1001: The specified power supply redundancy lost asserted**

  Redundancy Lost

  Severity: Error

Serviceable: Yes
Automatically notify Support: No

User Action:

Complete the following steps until the problem is solved:

1. Check the LEDs for both power supplies.
2. If the AC LED is not lit, check power cord and input voltage.
3. If the DC LED is not lit, remove and reinstall the power supply.
4. If the error LED is lit, replace the power supply.
5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A086F0200: The specified power supply presence detected asserted**

Presence detected

Severity: Information
Serviceable: No
Automatically notify Support: No

User Action:

No action

- **A086F0802: The specified power supply predictive failure asserted asserted**

Predictive Failure

Severity: Warning
Serviceable: Yes
Automatically notify Support: No

User Action:

Complete the following steps until the problem is solved:

1. Check the LEDs for both power supplies.
2. If the AC LED is not lit, check power cord and input voltage.
3. If the DC LED is not lit, remove and reinstall the power supply.
4. If the error LED is lit, replace the power supply.
5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A086F0803: The specified power supply input lost ac or dc asserted**

Power Supply input lost (AC/DC)

Severity: Warning
Serviceable: Yes
Automatically notify Support: No

User Action:

Complete the following steps until the problem is solved:

1. Check the power cord connections. Ensure that the power cords are correctly connected.
2. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A086F1001: This message is for the use case when an implementation has detected a Power Supply has failed.**

  Power Supply Failure detected

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. Check if the power supplies come with the same input and power rating.
  2. If not, replace one of them to ensure that the power supplies are of the same input and power rating.
  3. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A086F1006: The specified power supply configuration error asserted**

  Configuration error

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Check if the power supplies come with the same input and power rating.
  2. If not, replace one of them to ensure that the power supplies are of the same input and power rating.
  3. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A08870202: This message is for the use case when an implementation has detected a **Power Supply** type asserted event.**

  Transition to Critical from less severe

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A08EF0200: The specified power supply presence detected deasserted**

  Presence detected

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A08EF0401: The specified power supply failure deasserted**

  Power Supply Failure detected

Severity: Information
Serviceable: No
Automatically notify Support: No

User Action:

No action

- **A08EF0402: The specified power supply predictive failure deasserted**

  Predictive Failure

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A08EF0403: The specified power supply input lost ac or dc deasserted**

  Power Supply input lost (AC/DC)

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A08EF0406: The specified power supply configuration error deasserted**

  Configuration error

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A0B0B0806: Cooling_Status redundancy degraded from fully redundant asserted**

  Redundancy Degraded from Fully Redundant

  Severity: Warning
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Check the BMC event logs to identify any fan errors.
  2. Reseat the fans. If the problem persists, replace any failed fans.
  3. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A0B8B0206: Cooling_Status redundancy degraded from fully redundant deasserted**

  Redundancy Degraded from Fully Redundant

Severity: Information
Serviceable: No
Automatically notify Support: No

User Action:

No action

- **A0C071002: This message is for the use case when an implementation has detected a **Memory** type asserted event.**

  Transition to Critical from less severe

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. If the problem persists, check whether any reported DIMMs are not properly seated. If yes, reseat them.
  2. If the problem persists, visually inspect the DIMMs for physical damage, dust, or any other contamination on the connector or circuits. If yes, dust off the DIMMs, clean the contacts, and install them.
  3. If the problem persists, visually inspect the DIMM slot for physical damage. Look for cracked or broken plastic on the slot. If yes, move the DIMM to another DIMM slot.
  4. If the problem persists, perform a power cycle on the server from the management console.
  5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

  Notes: DIMM installation rules can be found in the Maintenance Manual.

  – SR635: https://thinksystem.lenovofiles.com/help/topic/7Y98/pdf_files.html
  – SR655: https://thinksystem.lenovofiles.com/help/topic/7Y00/pdf_files.html

- **A0C6F0204: The specified memory device disabled asserted**

  Memory Device Disabled

  Severity: Information
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. If the problem persists, check whether any reported DIMMs are not properly seated. If yes, reseat them.
  2. If the problem persists, visually inspect the DIMMs for physical damage, dust, or any other contamination on the connector or circuits. If yes, dust off the DIMMs, clean the contacts, and install them.
  3. If the problem persists, visually inspect the DIMM slot for physical damage. Look for cracked or broken plastic on the slot. If yes, move the DIMM to another DIMM slot.
  4. If the problem persists, perform a power cycle on the server from the management console.

5. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

Notes: DIMM installation rules can be found in the Maintenance Manual.

- SR635: https://thinksystem.lenovofiles.com/help/topic/7Y98/pdf_files.html
- SR655: https://thinksystem.lenovofiles.com/help/topic/7Y00/pdf_files.html

- **A0C6F1007: This message is for the use case when an implementation has detected a Memory DIMM configuration error.**

  Configuration error

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Check ServerProven website to see whether any reported DIMMs are not supported by the server. If yes, replace them with supported ones.
  2. If the problem persists, check whether any reported DIMMs are not populated according to the DIMM installation rules. If yes, re-populate them by following the rules.
  3. If the problem persists, check whether any reported DIMMs are not properly seated. If yes, reseat them.
  4. If the problem persists, visually inspect any reported DIMMs for physical damage, dust, or any other contamination on the connector or circuits. If yes, dust off the DIMMs, clean the contacts, and install them.
  5. If the problem persists, visually inspect the DIMM slot for physical damage. Look for cracked or broken plastic on the slot. If yes, move the DIMM to another DIMM slot.
  6. If the problem persists, perform a power cycle on the server from the management console.
  7. If the problem persists, collect service data log from the BMC Web interface and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

  Notes: DIMM installation rules can be found in the Maintenance Manual.

  - SR635: https://thinksystem.lenovofiles.com/help/topic/7Y98/pdf_files.html
  - SR655: https://thinksystem.lenovofiles.com/help/topic/7Y00/pdf_files.html

- **A0D6F0200: The specified drive presence asserted**

  Drive Presence

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A0D6F0207: The specified drive rebuild or remap in progress asserted**

  Rebuild/Remap in progress

  Severity: Information
  Serviceable: No

Automatically notify Support: No

User Action:

No action

- **A0D6F1001: The specified drive fault asserted**

  Drive Fault

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. Search for any applicable service bulletins, Tech Tips or firmware updates related to this drive from the Support portal (https://datacentersupport.lenovo.com).
  2. If the problem persists, collect service data logs from the management console and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider) .

- **A0DEF0200: The specified drive presence deasserted**

  Drive Presence

  Severity: Information
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Search for any applicable service bulletins, Tech Tips or firmware updates related to this drive from the Support portal(https://datacentersupport.lenovo.com).
  2. Check the system event logs for any other RAID-related errors. If yes, identify any affected drives and reseat them.
  3. If the problem persists, replace any affected drives.
  4. If the problem persists, collect service data logs from the management console and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A0DEF0207: The specified drive rebuild or remap in progress deasserted**

  Rebuild/Remap in progress

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A0DEF0401: The specified drive fault deasserted**

  Drive Fault

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

User Action:

No action

- **A106F0202: Log area reset asserted**

  Log Area Reset/Cleared

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A106F0204: sel full asserted**

  SEL Full

  Severity: Information
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Clean the system event logs.

- **A106F0805: sel almost full asserted**

  SEL Almost Full

  Severity: Warning
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Clean the system event logs.

- **A136F0200: Front Panel NMI / Diagnostic Interrupt deasserted**

  Front Panel NMI/Diagnostic Interrupt

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A136F1000: This message is for the use case when an implementation has detected a Front Panel NMI / Diagnostic Interrupt.**

  Front Panel NMI/Diagnostic Interrupt

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Log in to the BMC Web interface and navigate to Settings > Capture BSOD.

2. Check the system snapshot taken by the BMC.
   - If you have triggered the NMI yourself in the management console.
     a. Save the snapshot for future crash analysis.
     b. Restart the system.
   - If you have no idea why the system crashed.
     a. Analyze the errors in the snapshot and take appropriate action.
     b. Restart the system and check whether it has returned to normal operating state.
     c. If any problem persists, collect the system snapshot and any service data logs from the management console and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A146F0200: power button pressed asserted**

  Power Button pressed

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A16090201: BMC_Boot_Up asserted**

  Device Enabled

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A1B6F0200: The specified cable is connected asserted**

  Cable/Interconnect is connected

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A1B6F1001: Fan type configuration error asserted**

  Configuration Error

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: No

  User Action:

  Complete the following steps until the problem is solved:

  1. Disconnect the power from the chassis and check if the fan and fan board are properly connected.
  2. Check if the fan type used is correct and complies with technical rules for system fans.

3. If the problem persists, collect service data logs from the management console and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A216F1000: The specified cable/card detected a Fault asserted.**

  Fault Status asserted

  Severity: Error
  Serviceable: Yes
  Automatically notify Support: Yes

  User Action:

  Complete the following steps until the problem is solved:

  1. Disconnect the power from the chassis and check if the cable/card are connected correctly.
  2. Check if the corresponding relationship between the cable and card used is correct.
  3. If the problem persists, collect service data logs from the management console and contact Lenovo Support (https://datacentersupport.lenovo.com/serviceprovider).

- **A21EF0400: The specified cable/card detected a Fault deasserted.**

  Fault Status asserted

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A226F0200: ACPI in s0/g0 working State**

  S0/G0 'working

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A226F0205: ACPI in s5/g2 soft off state**

  S5/G2 - soft-off

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A236F0200: Watchdog2 timer expired asserted**

  Timer expired - status only (No action)

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

No action

- **A236F0201: Watchdog2 hard reset asserted**

  Hard Reset

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A236F0202: Watchdog2 power down asserted**

  Power Down

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A236F0203: Watchdog2 power cycle asserted**

  Power Cycle

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

- **A236F0208: Watchdog2 timer interrupt asserted**

  Timer interrupt

  Severity: Information
  Serviceable: No
  Automatically notify Support: No

  User Action:

  No action

Chapter 3. UEFI events

UEFI error messages can be generated when the server starts up (POST) or while the server is running. UEFI error messages are logged in the BMC event log in the server.

For each event code, the following fields are displayed:

Event identifier
An identifier that uniquely identifies an event.

Event description
The logged message string that appears for an event.

Explanation
Provides additional information to explain why the event occurred.

Severity
An indication of the level of concern for the condition. The severity is abbreviated in the event log to the first character. The following severities can be displayed:

- **Information**. The event was recorded for audit purposes, usually a user action or a change of states that is normal behavior.
- **Warning**. The event is not as severe as an error, but if possible, the condition should be corrected before it becomes an error. It might also be a condition that requires additional monitoring or maintenance.
- **Error**. The event is a failure or critical condition that impairs service or an expected function.

User Action
Indicates what actions you should perform to solve the event. Perform the steps listed in this section in the order shown until the problem is solved. If you cannot solve the problem after performing all steps, contact Lenovo Support.

UEFI events organized by severity

The following table lists all UEFI events, organized by severity (Information, Error, and Warning).

Table 3. Events organized by severity

Event ID	Message String	Severity
FQXSFDD0012I	SATA Hard Drive Error: [arg1] was recovered.	Informational
FQXSFIO0027I	The Bus:[arg1] Device:[arg2] Fun:[arg3] is attempted to boot PXE.	Informational
FQXSFMA0001I	DIMM [arg1] Disable has been recovered. [arg2]	Informational
FQXSFMA0002I	The uncorrectable memory error state has been cleared.	Informational
FQXSFMA0006I	[arg1] DIMM [arg2] has been detected, the DIMM serial number is [arg3].	Informational
FQXSFMA0007I	[arg1] DIMM number [arg2] has been replaced. [arg3]	Informational
FQXSFMA0008I	DIMM [arg1] POST memory test failure has been recovered. [arg2]	Informational

Table 3. Events organized by severity (continued)

Event ID	Message String	Severity
FQXSFMA0026I	DIMM [arg1] Self-healing, attempt post package repair (PPR) succeeded. [arg2]	Informational
FQXSFMA0029I	The PFA of DIMM [arg1] has been deasserted after applying PPR for this DIMM. [arg2]	Informational
FQXSFMA0030I	A correctable memory error has been detected on DIMM [arg1]. [arg2]	Informational
FQXSFPU0021I	The TPM physical presence state has been cleared.	Informational
FQXSFPU0023I	Secure Boot Image Verification Failure has been cleared as no failure in this round boot.	Informational
FQXSFPU0025I	The default system settings have been restored.	Informational
FQXSFPU0038I	A correctable error (Type [arg1]) has been detected by processor [arg2].	Informational
FQXSFPU4034I	TPM Firmware recovery is finished, rebooting system to take effect.	Informational
FQXSFPU4038I	TPM Firmware recovery successful.	Informational
FQXSFPU4041I	TPM Firmware update is in progress. Please DO NOT power off or reset system.	Informational
FQXSFPU4042I	TPM Firmware update is finished, rebooting system to take effect.	Informational
FQXSFPU4044I	The current TPM firmware version could not support TPM version toggling.	Informational
FQXSFPU4046I	TPM Firmware will be updated from TPM1.2 to TPM2.0.	Informational
FQXSFPU4047I	TPM Firmware will be updated from TPM2.0 to TPM1.2.	Informational
FQXSFPU4049I	TPM Firmware update successful.	Informational
FQXSFPU4059I	User requested to skip freezing lock of AHCI-attached SATA drives. System UEFI accepted the request and will execute prior to OS boot.	Informational
FQXSFPU4060I	Skipped freezing lock of AHCI-attached SATA drives.	Informational
FQXSFPU4061I	Restored default locking behavior of AHCI-attached SATA drives.	Informational
FQXSFPU4070I	Platform secure boot fuse is enabled.	Informational
FQXSFPU4071I	Platform secure boot fuse is disabled.	Informational
FQXSFPU4080I	Host Power-On password has been changed.	Informational
FQXSFPU4081I	Host Power-On password has been cleared.	Informational
FQXSFPU4082I	Host Admin password has been changed.	Informational
FQXSFPU4083I	Host Admin password has been cleared.	Informational
FQXSFPU4084I	Host boot order has been changed.	Informational
FQXSFPU4085I	Host WOL boot order has been changed.	Informational
FQXSFSM0007I	The XCC System Event log (SEL) is full.	Informational
FQXSFDD0001G	DRIVER HEALTH PROTOCOL: Missing Configuration. Requires Change Settings From F1.	Warning
FQXSFDD0002M	DRIVER HEALTH PROTOCOL: Reports 'Failed' Status Controller.	Warning

Table 3. Events organized by severity (continued)

Event ID	Message String	Severity
FQXSFDD0003I	DRIVER HEALTH PROTOCOL: Reports 'Reboot' Required Controller.	Warning
FQXSFDD0005M	DRIVER HEALTH PROTOCOL: Disconnect Controller Failed. Requires 'Reboot'.	Warning
FQXSFDD0006M	DRIVER HEALTH PROTOCOL: Reports Invalid Health Status Driver.	Warning
FQXSFDD0007G	Security Key Lifecycle Manager (SKLM) IPMI Error.	Warning
FQXSFIO0013I	The device found at Bus [arg1] Device [arg2] Function [arg3] could not be configured due to resource constraints. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].	Warning
FQXSFIO0021J	PCIe Error Recovery has occurred in physical [arg1] number [arg2]. The [arg3] may not operate correctly.	Warning
FQXSFIO0022J	PCIe Link Width has degraded from [arg1] to [arg2] in physical [arg3] number [arg4].	Warning
FQXSFIO0023J	PCIe Link Speed has degraded from [arg1] to [arg2] in physical [arg3] number [arg4].	Warning
FQXSFIO0029G	Correctable CPU link error has been detected on processor [arg1].	Warning
FQXSFMA0012L	The [arg1] PFA Threshold limit has been exceeded on DIMM [arg2] at address [arg3]. [arg4]	Warning
FQXSFMA0027M	DIMM [arg1] Self-healing, attempt post-package repair (PPR) failed at Rank [arg2] Sub Rank [arg3] Bank [arg4] Row [arg5] on Device [arg6]. [arg7]	Warning
FQXSFMA0028M	DIMM [arg1] Self-healing, attempt post-package repair (PPR) exceeded DIMM level threshold [arg2] at Rank [arg3] Sub Rank [arg4] Bank [arg5] Row [arg6] on Device [arg7]. [arg8]	Warning
FQXSFPU0021G	Hardware physical presence is in asserted state.	Warning
FQXSFPU0022G	The TPM configuration is not locked.	Warning
FQXSFPU0023G	Secure Boot Image Verification Failure Warning.	Warning
FQXSFPU4033F	TPM Firmware recovery is in progress. Please DO NOT power off or reset system.	Warning
FQXSFPU4035M	TPM Firmware recovery failed. TPM chip may be damaged.	Warning
FQXSFPU4040M	TPM selftest has failed.	Warning
FQXSFPU4043G	TPM Firmware update aborted. System is rebooting...	Warning
FQXSFPU4045G	Physical Presence is not asserted, abort TPM Firmware upgrade.	Warning
FQXSFPU4050G	Failed to update TPM Firmware.	Warning
FQXSFPU4051G	Undefined TPM_POLICY found	Warning
FQXSFPU4052G	TPM_POLICY is not locked	Warning
FQXSFPU4053G	System TPM_POLICY does not match the planar.	Warning
FQXSFPU4054G	TPM card logical binding has failed.	Warning
FQXSFPU4072G	Platform secure boot policy is not defined.	Warning

Table 3. Events organized by severity (continued)

Event ID	Message String	Severity
FQXSFPU4073G	Platform secure boot fuse is enabled but CPU 1 is unfused.	Warning
FQXSFPU4074G	Platform secure boot fuse is enabled but CPU 2 is unfused.	Warning
FQXSFPU4075G	Platform secure boot fuse is enabled but CPU 1, 2 are unfused.	Warning
FQXSFPU4076G	Platform secure boot fuse is disabled but CPU 1 is fused.	Warning
FQXSFPU4077G	Platform secure boot fuse is disabled but CPU 2 is fused.	Warning
FQXSFPU4078G	Platform secure boot fuse is disabled but CPU 1, 2 are fused.	Warning
FQXSFSM0002N	Boot Permission denied by Management Module: System Halted.	Warning
FQXSFSM0003N	Timed Out waiting on boot permission from Management Module: System Halted.	Warning
FQXSFSM0004M	An XCC communication failure has occurred.	Warning
FQXSFSR0003G	The number of boot attempts has been exceeded. No bootable device found.	Warning
FQXSFTR0001L	An invalid date and time have been detected.	Warning
FQXSFDD0004M	DRIVER HEALTH PROTOCOL: Reports 'System Shutdown' Required Controller.	Error
FQXSFDD0012K	SATA Hard Drive Error: [arg1].	Error
FQXSFIO0010M	An Uncorrectable PCIe Error has Occurred at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical [arg6] number is [arg7].	Error
FQXSFIO0011M	A PCIe parity error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].	Error
FQXSFIO0012M	A PCIe system error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].	Error
FQXSFIO0014J	A bad option ROM checksum was detected for the device found at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].	Error
FQXSFIO0019J	PCIe Resource Conflict.	Error
FQXSFIO0030M	Uncorrectable CPU link error has been detected on processor [arg1].	Error
FQXSFMA0001M	DIMM [arg1] has been disabled due to an error detected during POST. [arg2]	Error
FQXSFMA0002M	An uncorrectable memory error has been detected on DIMM [arg1] at address [arg2]. [arg3]	Error
FQXSFMA0008M	DIMM [arg1] has failed the POST memory test. [arg2]	Error
FQXSFPU0019N	An uncorrectable error has been detected on processor [arg1].	Error
FQXSFPU0030N	A firmware fault has been detected in the UEFI image.	Error
FQXSFPU0031N	The number of POST attempts has reached the value configured in F1 setup. The system has booted with default UEFI settings. User specified settings have been preserved and will be used on subsequent boots unless modified before rebooting.	Error

Table 3. Events organized by severity (continued)

Event ID	Message String	Severity
FQXSFPU0034L	The TPM could not be initialized properly.	Error
FQXSFPU4056M	TPM card is changed, need install back the original TPM card which shipped with the system.	Error
FQXSFSM0008M	Boot permission timeout detected.	Error

List of UEFI events

This section lists all messages that can be sent from UEFI.

- **FQXSFDD0001G: DRIVER HEALTH PROTOCOL: Missing Configuration. Requires Change Settings From F1.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Go to F1 Setup > System Settings > Settings > Driver Health Status List and find a driver/controller reporting Configuration Required status.
  2. Search for the driver menu from System Settings and change settings appropriately.
  3. Save settings and restart the system.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFDD0002M: DRIVER HEALTH PROTOCOL: Reports 'Failed' Status Controller.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Reboot the system.
  2. Reflash the adapter firmware.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFDD0003I: DRIVER HEALTH PROTOCOL: Reports 'Reboot' Required Controller.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. No action required - system will reboot at the end of POST.
  2. Reflash the adapter firmware.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFDD0004M: DRIVER HEALTH PROTOCOL: Reports 'System Shutdown' Required Controller.**

  Severity: Fatal

  User Action:

  Complete the following steps:

  1. Reboot the system.

2. Reflash the adapter firmware.
3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFDD0005M: DRIVER HEALTH PROTOCOL: Disconnect Controller Failed. Requires 'Reboot'.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Reboot the system to reconnect the controller.
  2. Reflash the adapter firmware.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFDD0006M: DRIVER HEALTH PROTOCOL: Reports Invalid Health Status Driver.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Reboot the system.
  2. Reflash the adapter firmware.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFDD0007G: Security Key Lifecycle Manager (SKLM) IPMI Error.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Check Lenovo Support site for an applicable service bulletin or UEFI firmware update that applies to this error.
  2. A/C cycle the system.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFDD0012I: SATA Hard Drive Error: [arg1] was recovered.**

  Severity: Info

  Parameters:

  [arg1] Slot/bay label name in system

  User Action:

  Information only; no action is required.

- **FQXSFDD0012K: SATA Hard Drive Error: [arg1].**

  Severity: Error

  Parameters:

  [arg1] Slot/bay label name in system

  User Action:

  Complete the following steps:

1. Power down the server.
2. Re-insert SATA Drive to ensure it is fully connected to the backplane.
3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFIO0010M: An Uncorrectable PCIe Error has Occurred at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical [arg6] number is [arg7].**

  Severity: Error

  Parameters:

  [arg1] Bus

  [arg2] Device

  [arg3] Function

  [arg4] VID

  [arg5] DID

  [arg6] Slot/Bay

  [arg7] Instance number

  User Action:

  Complete the following steps:

  1. Check Lenovo Support site for an applicable device driver, firmware update, version of service information for this product or other information that applies to this error. Load new device driver and any required firmware updates.
  2. If this device and/or any attached cables were recently installed, moved, serviced or upgraded.
     a. Reseat adapter or disk and any attached cables.
     b. Reload Device Driver.
     c. If device is not recognized, reconfiguring slot to lower speed may be required. Gen1/Gen2/Gen3 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports ->PCIe Gen1/Gen2/Gen3/Gen4 Speed Selection, or the OneCLI utility.
     d. If a PCIe error has also been reported on a second slot within the same node, ensure steps a, b, and c above are also performed for that adapter or disk before proceeding.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFIO0011M: A PCIe parity error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].**

  Severity: Error

  Parameters:

  [arg1] Bus

  [arg2] Device

  [arg3] Function

  [arg4] VID

  [arg5] DID

  [arg6] Instance number

User Action:

Complete the following steps:

1. Check Lenovo Support site for an applicable device driver, firmware update, version of service information for this product or other information that applies to this error. Load new device driver and any required firmware updates.
2. If this node and/or any attached cables were recently installed, moved, serviced or upgraded.
   a. Reseat Adapter and any attached cables.
   b. Reload Device Driver.
   c. If device is not recognized, reconfiguring slot to Gen1 or Gen2 may be required. Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports ->PCIe Gen1/Gen2/Gen3 Speed Selection, or the OneCLI utility.
   d. If a PCIe error has also been reported on a second slot within the same node, ensure steps a, b, and c above are also performed for that adapter before proceeding.
3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFIO0012M: A PCIe system error has occurred on Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The Physical slot number is [arg6].**

  Severity: Error

  Parameters:

  [arg1] Bus

  [arg2] Device

  [arg3] Function

  [arg4] VID

  [arg5] DID

  [arg6] Instance number

  User Action:

  Complete the following steps:

  1. Check Lenovo Support site for an applicable device driver, firmware update, version of service information for this product or other information that applies to this error. Load new device driver and any required firmware updates.
  2. If this device and/or any attached cables were recently installed, moved, serviced or upgraded.
     a. Reseat Adapter and any attached cables.
     b. Reload Device Driver.
     c. If device is not recognized, reconfiguring slot to Gen1 or Gen2 may be required. Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports ->PCIe Gen1/Gen2/Gen3 Speed Selection, or the OneCLI utility.
     d. If a PCIe error has also been reported on a second slot within the same node, ensure steps a, b, and c above are also performed for that adapter before proceeding.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0013I: The device found at Bus [arg1] Device [arg2] Function [arg3] could not be configured due to resource constraints. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].**

  Severity: Warning

  Parameters:

  [arg1] Bus

  [arg2] Device

  [arg3] Function

  [arg4] VID

  [arg5] DID

  [arg6] Instance number

  User Action:

  Complete the following steps:

  1. If this PCIe device and/or any attached cables were recently installed, moved, serviced or upgraded, reseat adapter and any attached cables.
  2. Check Lenovo Support site for any applicable service bulletin or UEFI or adapter firmware update that applies to this error.(NOTE: It may be necessary to disable unused option ROMs from UEFI F1 setup, OneCLI utility, or using adapter manufacturer utilities so that adapter firmware can be updated.)
  3. Move the adapter to a different slot. If a slot is not available or error recurs, replace the adapter.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0014J: A bad option ROM checksum was detected for the device found at Bus [arg1] Device [arg2] Function [arg3]. The Vendor ID for the device is [arg4] and the Device ID is [arg5]. The physical slot number is [arg6].**

  Severity: Error

  Parameters:

  [arg1] Bus

  [arg2] Device

  [arg3] Function

  [arg4] VID

  [arg5] DID

  [arg6] Instance number

  User Action:

  Complete the following steps:

  1. If this PCIe device and/or any attached cables were recently installed, moved, serviced or upgraded. Reseat adapter and any attached cables.
  2. Move adapter to a different system slot, if available.

3. Check Lenovo Support site for any applicable service bulletin or UEFI or adapter firmware update that applies to this error.

   Note: It may be necessary to configure slot to Gen1 or to use special utility software so that adapter firmware can be upgraded. Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports ->PCIe Gen1/Gen2/Gen3 Speed Selection, or the OneCLI utility.
4. If the problem persists, collect Service Data logs and contact Lenovo Support.

   Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0019J: PCIe Resource Conflict.**

  Severity: Error

  User Action:

  Complete the following steps:

  1. If this PCIe device and/or any attached cables were recently installed, moved, serviced or upgraded, reseat the adapter and any attached cables.
  2. Move the adapter to a different system slot, if available.
  3. Check Lenovo Support site for any applicable service bulletin or UEFI or adapter firmware update that applies to this error.

     Note: It may be necessary to configure slot to Gen1 or to use special utility software so that adapter firmware can be upgraded. Gen1/Gen2 settings can be configured via F1 Setup -> System Settings -> Devices and I/O Ports ->PCIe Gen1/Gen2/Gen3 Speed Selection, or the OneCLI utility.
  4. If the problem persists, collect Service Data logs.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0021J: PCIe Error Recovery has occurred in physical [arg1] number [arg2]. The [arg3] may not operate correctly.**

  Severity: Warning

  Parameters:

  [arg1] Slot/bay

  [arg2] Instance number

  [arg3] Adapter/disk

  User Action:

  Complete the following steps:

  1. Check the log for a separate error related to an associated PCIe device or NVME disk and resolve that error.
  2. Check the Lenovo Support site for an applicable service bulletin or firmware update for the system or adapter that applies to this error.
  3. Check the system spec to make sure that the PCIe device or NVME disk is installed in the compatible PCIe slot or bay and a compatible cable is used. If not, performance of this device might be impacted.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0022J: PCIe Link Width has degraded from [arg1] to [arg2] in physical [arg3] number [arg4].**

  Severity: Warning

  Parameters:

  [arg1] x16/x8/x4/x2/x1

  [arg2] x16/x8/x4/x2/x1

  [arg3] Slot/bay

  [arg4] Instance number

  User Action:

  Complete the following steps:

  1. Check the log for a separate error related to an associated PCIe device or NVME disk and resolve that error.
  2. Check the Lenovo Support site for an applicable service bulletin or firmware update for the system or adapter that applies to this error.
  3. Check the system spec to make sure that the PCIe device or NVME disk is installed in the compatible PCIe slot or bay and a compatible cable is used. If not, performance of this device might be impacted.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0023J: PCIe Link Speed has degraded from [arg1] to [arg2] in physical [arg3] number [arg4].**

  Severity: Warning

  Parameters:

  [arg1] 32 GT/s / 16 GT/s / 8.0 GT/s / 5.0 GT/s / 2.5 GT/s

  [arg2] 32 GT/s / 16 GT/s / 8.0 GT/s / 5.0 GT/s / 2.5 GT/s

  [arg3] Slot/bay

  [arg4] Instance number

  User Action:

  Complete the following steps:

  1. Check the log for a separate error related to an associated PCIe device or NVME disk and resolve that error.
  2. Check the Lenovo Support site for an applicable service bulletin or firmware update for the system or adapter that applies to this error.
  3. Check the system spec to make sure that the PCIe device or NVME disk is installed in the compatible PCIe slot or bay and a compatible cable is used. If not, performance of this device might be impacted.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0027I: The Bus:[arg1] Device:[arg2] Fun:[arg3] is attempted to boot PXE.**

  Severity: Info

  Parameters:

  [arg1] Bus

  [arg2] Device

  [arg3] Function

  User Action:

  Information only; no action is required.

- **FQXSFIO0029G: Correctable CPU link error has been detected on processor [arg1].**

  Severity: Warning

  Parameters:

  [arg1] Cpu Silk screen label, 1-based

  User Action:

  Complete the following steps:

  1. Reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFIO0030M: Uncorrectable CPU link error has been detected on processor [arg1].**

  Severity: Error

  Parameters:

  [arg1] Cpu Silk screen label, 1-based

  User Action:

  Complete the following steps:

  1. Check Lenovo Support site for an applicable service bulletin or firmware update that applies to this error.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFMA0001I: DIMM [arg1] Disable has been recovered. [arg2]**

  Severity: Info

  Parameters:

  [arg1] DIMM slot silk label

  [arg2] DIMM identifier consists of S/N, FRU and UDI, e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

Information only; no action is required.

- **FQXSFMA0001M: DIMM [arg1] has been disabled due to an error detected during POST. [arg2]**

  Severity: Error

  Parameters:

  [arg1] DIMM slot silk label

  [arg2] DIMM identifier consists of S/N, FRU and UDI, e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Complete the following steps:

  1. Search for other event messages pointing to the same DIMM, and if exist, prioritize resolving them at first.
  2. Reseat the affected DIMM.
  3. Boot to UEFI setup and try to enable DIMM via System Settings->Memory->System Memory Details page (if applicable) and reboot the system to see if the DIMM could be re-enabled successfully.
  4. If the problem persists, update UEFI firmware to the latest version.
  5. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFMA0002I: The uncorrectable memory error state has been cleared.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFMA0002M: An uncorrectable memory error has been detected on DIMM [arg1] at address [arg2]. [arg3]**

  Severity: Error

  Parameters:

  [arg1] DIMM Silk Label, 1-based

  [arg2] Address of the system where error occurred

  [arg3] DIMM identifier consists of S/N, FRU and UDI, e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Complete the following steps:

  1. Check Lenovo Support site for an applicable service bulletin or firmware update that applies to this memory error.
  2. Search for other event messages pointing to the same DIMM, and if exist, prioritize resolving them at first.
  3. Reseat the affected DIMM.
  4. Swap the affected DIMM to another known good slot and verify whether the issue still be observed or not.
  5. If the problem persists, collect Service Data logs and contact Lenovo Support.

Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFMA0006I: [arg1] DIMM [arg2] has been detected, the DIMM serial number is [arg3].**

  Severity: Info

  Parameters:

  [arg1] Unqualified/Non Lenovo

  [arg2] DIMM Silk Label, 1-based

  [arg3] DIMM serial number.

  User Action:

  Complete the following steps:

  1. If this information event is logged in the XCC event log, the server does have unqualified memory installed.
  2. The memory installed may not be covered under warranty.
  3. Without qualified memory, speeds supported above industry standards will not be enabled.
  4. Contact your Local Sales Representative or Authorized Business Partner to order qualified memory to replace the unqualified DIMM(s).
  5. After you install qualified memory and power up the server, check to ensure this informational event is not logged again.
  6. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFMA0007I: [arg1] DIMM number [arg2] has been replaced. [arg3]**

  Severity: Info

  Parameters:

  [arg1] Unqualified/Non Lenovo

  [arg2] DIMM Silk Label, 1-based

  [arg3] DIMM info (S/N, FRU and UDI.), e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Complete the following steps:

  1. This event should be followed by a recent FQXSFMA0006I event denoting the server does have unqualified memory installed.
  2. Information only; no action is required.

- **FQXSFMA0008I: DIMM [arg1] POST memory test failure has been recovered. [arg2]**

  Severity: Info

  Parameters:

  [arg1] DIMM slot silk label

  [arg2] DIMM identifier consists of S/N, FRU and UDI, e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Information only; no action is required.

- **FQXSFMA0008M: DIMM [arg1] has failed the POST memory test. [arg2]**

Severity: Error

Parameters:

[arg1] DIMM slot silk label

[arg2] DIMM identifier consists of S/N, FRU and UDI, e.g. "739E68ED-VC10 FRU 0123456"

User Action:

Complete the following steps:

1. If the DIMM configuration was changed prior to this failure verify that the DIMMs are installed in the correct population sequence.
2. RESEAT the DIMM that failed POST memory test and the DIMMs on adjacent slots if populated. Boot to F1 setup and enable the DIMM. Reboot the system.
3. Swap the DIMM from failure location to another known good location to see if the failure follow the DIMM or DIMM slot.
4. If this problem was encountered during an XCC / UEFI update process:
   a. Power cycle the system by removing power for a few seconds.
   b. Clear CMOS settings by removing battery for a few seconds.
5. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFMA0012L: The [arg1] PFA Threshold limit has been exceeded on DIMM [arg2] at address [arg3]. [arg4]**

  Severity: Warning

  Parameters:

  [arg1] Legacy PFA threshold reach, "High", "Low".

  [arg2] DIMM Silk Label, 1-based

  [arg3] Address of the system where error occurred

  [arg4] DIMM info (S/N, FRU and UDI.), e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Complete the following steps:

  1. Reseat affected DIMM.
  2. Check Lenovo Support site for an applicable service bulletin or firmware update that applies to this memory error.
  3. Swap the DIMM to another known good location.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFMA0026I: DIMM [arg1] Self-healing, attempt post package repair (PPR) succeeded. [arg2]**

  Severity: Info

  Parameters:

  [arg1] DIMM Silk Label, 1-based

  [arg2] DIMM info (S/N, FRU and UDI.), e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

Complete the following steps:

1. Information only; no action is required.
2. Note: Post Package Repair (PPR) – is the memory Self-Healing process of substituting the access to a bad cell or address row with a spare row within the DRAM device.
   a. Soft Post Package Repair (sPPR) - repairs a row for the current boot cycle. If system power is removed or the system is rebooted (reset), the DIMM reverts to its original state.
   b. Hard Post Package Repair (hPPR) – permanently repairs a row.

- **FQXSFMA0027M: DIMM [arg1] Self-healing, attempt post-package repair (PPR) failed at Rank [arg2] Sub Rank [arg3] Bank [arg4] Row [arg5] on Device [arg6]. [arg7]**

  Severity: Warning

  Parameters:

  [arg1] DIMM Silk Label, 1-based

  [arg2] Rank number

  [arg3] Subrank number

  [arg4] Bank number

  [arg5] Row number

  [arg6] DramDevice

  [arg7] DIMM identifier consists of S/N, FRU and UDI, e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Complete the following steps:

  1. Search for other event messages pointing to the same DIMM, and if exist, prioritize resolving them at first.
  2. Reseat the affected DIMM.
  3. Boot to F1 setup and enable the DIMM. Reboot the system.
  4. Update UEFI firmware to the latest version.
  5. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFMA0028M: DIMM [arg1] Self-healing, attempt post-package repair (PPR) exceeded DIMM level threshold [arg2] at Rank [arg3] Sub Rank [arg4] Bank [arg5] Row [arg6] on Device [arg7]. [arg8]**

  Severity: Warning

  Parameters:

  [arg1] DIMM Silk Label, 1-based

  [arg2] PprAttemptThreshold

  [arg3] Rank number

  [arg4] Subrank number

  [arg5] Bank number

  [arg6] Row number

[arg7] DramDevice

[arg8] DIMM identifier consists of S/N, FRU and UDI, e.g. "739E68ED-VC10 FRU 0123456"

User Action:

Complete the following steps:

1. Search for other event messages pointing to the same DIMM, and if exist, prioritize resolving them at first.
2. Reseat the affected DIMM.
3. Boot to F1 setup and re-enable the DIMM. Reboot the system.
4. Update UEFI firmware to the latest version.
5. If the problem persists, collect Service Data logs and contact Lenovo Support.

   Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFMA0029I: The PFA of DIMM [arg1] has been deasserted after applying PPR for this DIMM. [arg2]**

  Severity: Info

  Parameters:

  [arg1] DIMM Silk Label, 1-based

  [arg2] DIMM info (S/N, FRU and UDI.), e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Information only; no action is required.

- **FQXSFMA0030I: A correctable memory error has been detected on DIMM [arg1]. [arg2]**

  Severity: Info

  Parameters:

  [arg1] DIMM Silk Label, 1-based

  [arg2] DIMM info (S/N, FRU and UDI.), e.g. "739E68ED-VC10 FRU 0123456"

  User Action:

  Information only; no action is required.

- **FQXSFPU0019N: An uncorrectable error has been detected on processor [arg1].**

  Severity: Error

  Parameters:

  [arg1] Socket number, 1-based.

  User Action:

  Complete the following steps:

  1. Check Lenovo Support site for an applicable service bulletin or UEFI firmware update that applies to this error.
  2. Power off the system and remove A/C power.
  3. Restore A/C power and power on the system.

4. Determine if there have been recent changes to the hardware, firmware or operating system. Reverse them if possible.
5. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU0021G: Hardware physical presence is in asserted state.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Complete any administrative tasks requiring the TPM physical presence switch to be in the "ON" position.
  2. Restore the physical presence switch to the "OFF" position and reboot the system.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU0021I: The TPM physical presence state has been cleared.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU0022G: The TPM configuration is not locked.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU0023G: Secure Boot Image Verification Failure Warning.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. It's a security warning message when user want to boot from an unauthorized UEFI image or OS while Secure Boot is enabled and Secure Boot Mode is in User Mode. If customer does not want to boot any unauthorized UEFI image or OS, remove that bootable device.
  2. If customer does want to boot this unauthorized UEFI image or OS, there're two ways to allow system boot from this unauthorized image, the first is to disable Secure Boot, the second is to enroll the unauthorized image into DB(Authorized Signature Database).
     a. Disable Secure Boot: assert Physical Presence and then change Secure Boot Setting to Disable (in F1 Setup -> System Settings -> Security -> Security Boot Configuration -> Security Boot Setting).
     b. Enroll the unauthorized UEFI Image. assert the Physical Presence and then change Secure Boot Policy to Custom Policy (in Setup -> System Settings -> Security -> Security Boot Configuration -> Security Boot Policy), then enter into "Security Boot Custom Policy" Menu, press the "Enroll Efi Image" button, select the unauthorized UEFI Image in the popup box.
     c. NOTE: There're two ways to assert Physical Presence:
        1) Switch Physical Presence Jumper to ON;

2) If the Physical Presence Policy has been set to enabled (F1 Setup -> System Settings -> Security -> Physical Presence Policy Configuration), user is allowed to assert remote Physical Presence via IPMI tool.)

3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU0023I: Secure Boot Image Verification Failure has been cleared as no failure in this round boot.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU0025I: The default system settings have been restored.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU0030N: A firmware fault has been detected in the UEFI image.**

  Severity: Error

  User Action:

  Complete the following steps:

  1. Check Lenovo Support site for an applicable service bulletin or firmware update that applies to this error.
  2. Reflash UEFI image.
  3. Undo recent system changes (settings or devices added). Verify that the system boots. Then, re-install options one at a time to locate the problem.
  4. If problem persists, save customer's UEFI configurations, then remove and re-install CMOS battery for 30 seconds to clear CMOS contents. If it boots successfully, then restore system settings.
  5. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFPU0031N: The number of POST attempts has reached the value configured in F1 setup. The system has booted with default UEFI settings. User specified settings have been preserved and will be used on subsequent boots unless modified before rebooting.**

  Severity: Error

  User Action:

  Complete the following steps:

  1. Original UEFI settings are still present. If customer desires to continue using the original settings, select Save Settings.
  2. If User did not intentionally trigger the reboots, check logs for probable cause. For example, if there is a battery fault event, follow the steps to resolve that event.
  3. Undo recent system changes (settings or devices added). Verify that the system boots. Then, re-install options one at a time to locate the problem.
  4. Check Lenovo Support site for an applicable service bulletin or firmware update that applies to this error. Update UEFI firmware if applicable.

5. Save customer's UEFI configurations, then remove and re-install CMOS battery for 30 seconds to clear CMOS contents. If it boots successfully, then restore system settings.
6. If the problem persists, collect Service Data logs and contact Lenovo Support.

   Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFPU0034L: The TPM could not be initialized properly.**

  Severity: Error

  User Action:

  Complete the following steps:

  1. Reboot the system. Reflash UEFI image.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFPU0038I: A correctable error (Type [arg1]) has been detected by processor [arg2].**

  Severity: Info

  Parameters:

  [arg1] Error type, “1” indicate PIE “2” indicate NBIO “3” indicate SMU “4” indicate PSP “5” indicate MP5

  [arg2] Cpu silk label, 1-based

  User Action:

  Complete the following steps:

  1. A correctable error detected by CPU. No action is needed.
  2. Below list provides the description for error type:
     a. “1” indicate PIE(Power Management, Interrupts, Etc.) error.
     b. “2” indicate NBIO(Northbridge IO) error.
     c. “3” indicate SMU(System Management Unit) error.
     d. “4” indicate PSP(Platform Security Processor) error.
     e. “5” indicate MP5(Microprocessor5 Management Controller) error.

- **FQXSFPU4033F: TPM Firmware recovery is in progress. Please DO NOT power off or reset system.**

  Severity: Warning

  User Action:

  Information only; no action is required.

  Note: The system will not respond to power off signal (FQXSFPU4034I) while TPM firmware recovery in progress.

- **FQXSFPU4034I: TPM Firmware recovery is finished, rebooting system to take effect.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4035M: TPM Firmware recovery failed. TPM chip may be damaged.**

Severity: Warning

User Action:

Complete the following steps:

1. Reboot the system.
2. If the error recurs TPM related features will not work.
3. If the problem persists, collect Service Data logs and contact Lenovo Support.

Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFPU4038I: TPM Firmware recovery successful.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4040M: TPM selftest has failed.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Reboot the system.
  2. If the error recurs TPM related features will not work.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

  Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFPU4041I: TPM Firmware update is in progress. Please DO NOT power off or reset system.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4042I: TPM Firmware update is finished, rebooting system to take effect.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4043G: TPM Firmware update aborted. System is rebooting...**

  Severity: Warning

  User Action:

  Information only; no action is required.

- **FQXSFPU4044I: The current TPM firmware version could not support TPM version toggling.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4045G: Physical Presence is not asserted, abort TPM Firmware upgrade.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. ASSERT TPM Physical presence jumper by following System Service Manual, ref. https://thinksystem.lenovofiles.com/help/index.jsp navigate to ThinkSystem SR850P Types 7D2F, 7D2G, 7D2H > Hardware replacement procedures > motherboard replacement > Enable TPM/TCM > Assert Physical Presence.
  2. Boot system into F1 setup, check TPM status make sure TPM is available, and the TPM firmware version support TPM Toggling, ref. https://thinksystem.lenovofiles.com/help/index.jsp navigate to UEFI manual for ThinkSystem server > ThinkSystem server with AMD EPYC (1-socket, 1st, 2nd, 3rd Gen) > System Setup Utility interface > Security menu > TPM Toggling.
  3. Reboot system and retry the TPM FW toggle, ref. https://thinksystem.lenovofiles.com/help/index.jsp navigate to ThinkSystem SR850P Types 7D2F, 7D2G, 7D2H > Hardware replacement procedures > motherboard replacement>Enable TPM/TCM>Set the TPM version.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4046I: TPM Firmware will be updated from TPM1.2 to TPM2.0.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4047I: TPM Firmware will be updated from TPM2.0 to TPM1.2.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4049I: TPM Firmware update successful.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4050G: Failed to update TPM Firmware.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Clear TPM via TPM operation and retry TPM firmware update by following the instructions in your product user guides. Go to https://thinksystem.lenovofiles.com/help/topic/com.lenovo.thinksystem.common.nav.doc/portfolio.html and click your product link. Usually, the TPM update information is located in “System board replacement” section in “Hardware replacement procedures”.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4051G: Undefined TPM_POLICY found**

  Severity: Warning

  User Action:

  Complete the following steps:

1. Reboot the system.
2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4052G: TPM_POLICY is not locked**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4053G: System TPM_POLICY does not match the planar.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Remove any newly added TPM card from the planar or re-install the original TPM card that shipped with the system.
  2. Reboot the system.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4054G: TPM card logical binding has failed.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4056M: TPM card is changed, need install back the original TPM card which shipped with the system.**

  Severity: Error

  User Action:

  Complete the following steps:

  1. Re-install the original TPM card that shipped with the system.
  2. Reboot the system.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFPU4059I: User requested to skip freezing lock of AHCI-attached SATA drives. System UEFI accepted the request and will execute prior to OS boot.**

  Severity: Info

  User Action:

  Complete the following steps:

  1. Change SystemOobCustom.SkipAhciFreezeLock from Disable to Enable using OneCLI tool.(use OneCLI command “OneCli config set SystemOobCustom.SkipAhciFreezeLock “Enabled” --imm IMM_USERID:IMM_PASSWORD@IMM_IP --override”).

2. Reboot the system into OS.

- **FQXSFPU4060I: Skipped freezing lock of AHCI-attached SATA drives.**

  Severity: Info

  User Action:

  Information only; no action is required.
- **FQXSFPU4061I: Restored default locking behavior of AHCI-attached SATA drives.**

  Severity: Info

  User Action:

  Information only; no action is required.
- **FQXSFPU4070I: Platform secure boot fuse is enabled.**

  Severity: Info

  User Action:

  Information only; no action is required.
- **FQXSFPU4071I: Platform secure boot fuse is disabled.**

  Severity: Info

  User Action:

  Information only; no action is required.
- **FQXSFPU4072G: Platform secure boot policy is not defined.**

  Severity: Warning

  User Action:

  Contact Lenovo Support.
- **FQXSFPU4073G: Platform secure boot fuse is enabled but CPU 1 is unfused.**

  Severity: Warning

  User Action:

  Complete the following steps:
  1. If a CPU has been replaced with a new one, roll back the original CPU and reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.
- **FQXSFPU4074G: Platform secure boot fuse is enabled but CPU 2 is unfused.**

  Severity: Warning

  User Action:

  Complete the following steps:
  1. If a CPU has been replaced with a new one, roll back the original CPU and reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.
- **FQXSFPU4075G: Platform secure boot fuse is enabled but CPU 1, 2 are unfused.**

  Severity: Warning

  User Action:

  Complete the following steps:

1. If a CPU has been replaced with a new one, roll back the original CPU and reboot the system.
2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4076G: Platform secure boot fuse is disabled but CPU 1 is fused.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. If a CPU has been replaced with a new one, roll back the original CPU and reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4077G: Platform secure boot fuse is disabled but CPU 2 is fused.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. If a CPU has been replaced with a new one, roll back the original CPU and reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4078G: Platform secure boot fuse is disabled but CPU 1, 2 are fused.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. If a CPU has been replaced with a new one, roll back the original CPU and reboot the system.
  2. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFPU4080I: Host Power-On password has been changed.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4081I: Host Power-On password has been cleared.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4082I: Host Admin password has been changed.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4083I: Host Admin password has been cleared.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFPU4084I: Host boot order has been changed.**

Severity: Info

User Action:

Information only; no action is required.

- **FQXSFPU4085I: Host WOL boot order has been changed.**

  Severity: Info

  User Action:

  Information only; no action is required.

- **FQXSFSM0002N: Boot Permission denied by Management Module: System Halted.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. AC cycle the system.
  2. Check XCC logs, and make sure the PSU installation follows support guide line.
  3. Review power policies and system configuration settings in the XCC GUI.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFSM0003N: Timed Out waiting on boot permission from Management Module: System Halted.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. AC cycle the system.
  2. Check XCC logs, and make sure the PSU installation follows support guide line.
  3. Review power policies and system configuration settings in the XCC GUI.
  4. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFSM0004M: An XCC communication failure has occurred.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. AC cycle the system.
  2. Make sure XCC and UEFI FW are operating with same compatible level.
  3. Check Lenovo Support site for an applicable service bulletin or firmware update that applies to this error.
  4. Reflash XCC Firmware.
  5. If the problem persists, collect Service Data logs and contact Lenovo Support.

     Note: The solution for this error may involve a system board replacement. If TPM encryption has been enabled, back up TPM Encryption Recovery Key.

- **FQXSFSM0007I: The XCC System Event log (SEL) is full.**

  Severity: Info

  User Action:

Complete the following steps:

1. Use BMC Web Interface to clear event logs.
2. If BMC communication is unavailable, use F1 Setup to access System Event Logs Menu and Choose Clear BMC System Event Logs and Restart Server.

- **FQXSFSM0008M: Boot permission timeout detected.**

  Severity: Error

  User Action:

  Complete the following steps:

  1. Review XCC logs for communication errors and resolve.
  2. AC cycle the system.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFSR0003G: The number of boot attempts has been exceeded. No bootable device found.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Remove AC power from the system.
  2. Connect at least one bootable device to the system.
  3. Connect AC power to the system.
  4. Power on system and retry.
  5. If the problem persists, collect Service Data logs and contact Lenovo Support.

- **FQXSFTR0001L: An invalid date and time have been detected.**

  Severity: Warning

  User Action:

  Complete the following steps:

  1. Check the XCC event logs. This event should immediately precede an FQXSFPW0001L error. Resolve that event or any other battery related errors.
  2. Use F1 Setup to reset date and time.
  3. If the problem persists, collect Service Data logs and contact Lenovo Support.

Notes

For the following event IDs:

- **B136F0807**
- **B136F1004**
- **B136F1008**
- **B136F2005**
- **B136F200A**
- **B136F100B**

If the event log is triggered by the sensor **NVMEs_AER_00-15** or **NVMEs_AER_16-31**, the user can get the BayID from the OEM data that was carried on log. BayID is represented by bit 4~7 in OEM data1.

Note: Bit 4~7: These four bits indicate 16 BayID in a range of 0~15. But to calculate the exact BayID, the user also needs to combine the sensor of this event.

- If the sensor is **NVMEs_AER_00-15**, BayID = value of bit 4~7 in OEM data1 + 0*16
- If the sensor is **NVMEs_AER_16-31**, BayID = value of bit 4~7 in OEM data1 + 1*16

Appendix A. Getting help and technical assistance

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

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

http://datacentersupport.lenovo.com

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

Before you call

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

Attempt to resolve the problem yourself

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

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

You can find the product documentation for your ThinkSystem products at https://pubs.lenovo.com/

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

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

Gathering information needed to call Support

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

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

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

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

Collecting service data

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

Service data can be collected through the following tools:

- **Lenovo XClarity Provisioning Manager**

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

- **Lenovo ThinkSystem System Manager**

  You can use the BMC Web user interface or the CLI to collect service data for the server. The file can be saved and sent to Lenovo Support.

  – For more information about using the Web interface to collect service data, see https://thinksystem.lenovofiles.com/help/topic/7Y00/bmc_user_guide.pdf.

Contacting Support

You can contact Support to obtain help for your issue.

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

Index

C

E

G

H

S

T

U