Cisco Intersight Alarms Reference Guide

First Published: 2023-08-24

Last Modified: 2024-03-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Communications, Services, Bias-free Language, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Documentation Feedback

To provide feedback about Cisco technical documentation, use the feedback form available in the right pane of every online document.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.

Bias-Free Language

The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on standards documentation, or language that is used by a referenced third-party product.

CHAPTER 1

Intersight Alarms Overview

Alarms in Intersight

Intersight provides fault monitoring capabilities to track and set up alarms for all managed targets. An alarm alerts you about a failure in the endpoint (a fault) or a threshold that has been crossed. An alarm in Intersight includes information about the operational state of the affected object at the time the fault was raised.

Intersight displays the total number of alarms in the **Critical** and **Warning** states next to the **Alarms** icon (bell icon representation). Click on the icon to view details of the component reporting the issue like the severity, alarm code, and the date/time the alarm was created under the **Active**, **Acknowledged**, **Suppressed**, or **Cleared** tabs.

- **Critical**— This alarm type is raised when a service-affecting condition requires an immediate corrective action. For example, the severity could indicate that the managed object is out of service and its capability must be restored immediately.
- **Warning**— This alarm is raised when a potential or impending service-affecting fault occurs. This fault could have no significant or immediate effects on the system. A warning status indicates that you must take the appropriate action to diagnose the fault and correct the problem to prevent it from becoming a more serious service-affecting fault.
- **Informational (Info)**—This alarm type displays the status information or notifications about the device. These alarms are generally non-critical and informational. For example, an Info alarm is triggered when a user triggers alarm suppression a specific server or a group of servers.

Click on a specific alarm to view the fault code, the source type and name, component on which the fault occurred, and a description of the fault.

For Cisco UCS FI-Attached and Standalone servers, faults are updated through events as and when they are received from the endpoints. In addition, faults are updated daily for claimed targets and on a weekly basis for unclaimed targets.

The following table shows the mapping of faults/alarms from the endpoint to the alarm severity in Intersight.

Intersight Alarm Severity	UCS Faults	HyperFlex Alarms
Critical	Critical and major faults	Red
Warning	Minor and warning faults	Yellow

Intersight Alarm Severity	UCS Faults	HyperFlex Alarms
Informational	Informational faults	Alarm not raised
Cleared	Alarm is deleted at the endpoint	Green

Note

- Intersight Managed devices must be running with firmware version of 4.1(3) or later releases to generate alarms.
- Cisco UCS Manager faults that are in flapping state are not inventoried by Intersight until they move out of this state.
- Cisco UCS Manager FSM faults are not inventoried in Intersight.

To learn more about the UCS and HyperFlex faults and alarms, see:

- UCS Faults and Error Messages
- HyperFlex HX Data Platform Events

Acknowledge Alarms

Intersight provides the ability to acknowledge alarms raised by targets connected to Intersight. You can acknowledge alarms from the Alarms details view, the Servers General tab, and from the Alarms drawer. When you acknowledge an alarm, the alarm will be moved from the Active tab to the Acknowledged tab.

Note

- You must have Account Administrator privileges to acknowledge or unacknowledge an alarm.
- There is no change to alarm severity when an alarm is acknowledged.
- The alarm is acknowledged only in Intersight. The change will not reflect on the faults at the endpoints.
- Health of the affected object will be recomputed and the alarm will be muted.

To acknowledge an alarm, do either one of the following:

- To acknowledge an alarm from the **Alarms** drawer, click the **Alarms** icon and click on the Acknowledge icon (crossed bell icon representation).
- To acknowledge alarms from the **Alarms** page, you can either select multiple or individual alarms and click the acknowledge icon (crossed bell icon representation) or click **Acknowledge** from the ellipsis icon (…) on the far right column.

  To acknowledge alarms from the **Servers** > **General** tab, click the acknowledge icon for the alarm under the **Events** > **Alarms** panel.

Unacknowledge Alarms

From the Acknowledged tab, you can unacknowledge an alarm to move it back to the list of Active alarms, by clicking **Unacknowledge** from the ellipsis icon (…) on the far right or by clicking the unacknowledge icon (bell representation).

To view the date/time an alarm was acknowledged/unacknowledged and user details, click **Settings** (gear icon representation) > **Audit Logs**. You can also view the date/time and user details of who acknowledged the alarm from the Acknowledge tab.

Clear Alarms

When a fault condition is rectified, the associated alarm is swiftly transitioned to the *Cleared* tab. This function enables efficient monitoring and retrospective analysis of alarm activities. Cisco Intersight displays the cleared alarms under the *Cleared* tab for a period of 30 days.

Alarm Suppression

Alarm suppression enables you to temporarily mute the alarms notifications generated by servers connected to Intersight. This functionality reduces the non-essential or redundant notifications during scheduled maintenance, updates, or other planned activities, without compromising the ability to receive critical alerts. Suppressing alarms allows you to manage (start/stop) alarm notifications and pay attention to crucial alerts.

You can *Start Alarm Suppression* or *Stop Alarm Suppression* from Server Table View or Server Details View. For more information, see Alarm Suppression.

Note Alarm Suppression is currently supported only for server actions.

Alarm classifications for default server maintenance refer to the distinct categories of alarms that the system has established. These system-defined alarm groups, or alarm classifications, operate as a single entity to determine which alarms must be suppressed for a server. The alarm suppression feature allows you to temporarily silence the alarm notifications using these alarm classifications.

For more information, see:

- *Alarm Classifications - Intersight Managed Mode Servers* and *UCS Standalone Servers tables* in Alarm Suppression
- Server Component Alarms

Sample Alarms

Intersight GUI displays the alarms in the following format:

Table 1: Server Component Alarm

Message	Severity	Code	Source Name	Source Type	Date/Time
vHBA aa02-6536/server-3 /adapter-UCSC-M-V5D200G_FCH263973NN /FC-NVMe-5G-Fabric-B is not operational.	Critical	AdapterHostFcInterfaceDown	aa02-6536/server-3/adapter-UCSC-M-V5D200G_FCH263973NN /FC-NVMe-5G-Fabric-B	Intersight Managed Server	Jul 28, 2023 2:05 AM

In the above example, the name of alarm is HostFcInterfaceDown and the MO of the alarm is adapter.HostFcInterface. As the **Source Type** is Intersight Managed Server, therefore the recommended action for the alarm can be found in the Server Components Alarms section of this document.

Table 2: Chassis Component Alarm

Message	Severity	Code	Source Name	Source Type	Date/Time
Fan TEST-4GFI/chassis-1/fanmodule-4/fan-1 is unresponsive	Critical	EquipmentChassisFanUnresponsive	TEST-4GFI/chassis-1/fanmodule-4/fan-1	Chassis	Jul 22, 2023 7:05 AM

In the above example, the name of alarm is ChassisFanUnresponsive and the MO of the alarm is equipment.Fan. As the **Source Type** is Chassis, therefore the recommended action for the alarm can be found in the Chassis Components Alarms section of this document.

Table 3: Fabric Interconnect Component Alarm

Message	Severity	Code	Source Name	Source Type	Date/Time
Power supply FF21-CDS-5G /switch-A/psu-1 is shutdown	Critical	EquipmentSwitchPsuPoweredOff	FF21-CDS-5G/switch-A/psu-1	Intersight Managed Domain	Jul 26, 2023 9:43 AM

Code represents the name and the MO of the alarm.

In the above example, the name of alarm is SwitchPsuPoweredOff and the MO of the alarm is equipment.psu. As the **Source Type** is Intersight Managed Domain, therefore the recommended user action for the alarm can be found in the Fabric Interconnect.

Managing Alarms using API

You can also manage the alarms in your Intersight account using an API. For more information, see Alarms API.

CHAPTER 2

Server Alarms

Server Components Alarms

Following table shows the description of the supported alarms for servers.

Name	MO	Severity	Explanation	Recommended Action
BladeMigrationDetected	compute.Blade	Critical	This alarm occurs when a server has been detected in a slot different than the one it was discovered in.	**1.** Reacknowledge the server in the current slot. **2.** If the issue persists, remove the server from the current slot and reinsert it in the correct slot. **3.** Reacknowledge the server in the correct slot. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
PhysicalMissing	compute.Physical	Critical	This alarm occurs when a server has been removed from the slot it was discovered in.	**1.** Make sure a server is inserted in the slot. **2.** Check the Power-On-Self-Test (POST) results for the server. **3.** Check the power state of the server. **4.** If the server is off, turn the server on. **5.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
PhysicalWillBoot	compute.Physical	Critical	The UCS Will Boot is a cursory check to ensure that the blade is configured properly to allow the BIOS to proceed. This alarm indicates that a critical Will boot error is encountered on the server. This error occurs when the CPU and DIMM configuration check fails.	**1.** Verify that the DIMMs are installed in a supported configuration. **2.** Verify that an adapter and CPU are installed. **3.** Download the System Event Logs file from the GUI by clicking **Servers>Server Name>... >System>Download System Event Log** **4.** Review the SEL statistics on the DIMM to determine which threshold was crossed. **5.** Create a `show tech-support file` and contact Cisco TAC to see if the DIMM needs replacement.
BoardTemperatureWarning	compute.Board	Warning	The motherboard has a warning temperature threshold condition.	**1.** Review the product specifications to determine the operating temperature range. **2.** Power off unused blade servers and rack servers. **3.** Verify that the server fans are working properly. **4.** Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat. **5.** Set the power profiling, power priority of the server, and the power restore state of the system through server Power Policy. **6.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
BoardTemperatureCritical	compute.Board	Critical	The motherboard has a critical temperature threshold condition.	**1.** Verify that the server fans are working properly. **2.** Wait for 24 hours to see if the problem resolves itself. **3.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
BoardVoltageWarning	compute.Board	Warning	The motherboard has a warning voltage threshold condition.	**1.** Ensure that the motherboard is supplied with the required input voltage as per the product specifications. **2.** Create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
BoardVoltageCritical	compute.Board	Critical	The motherboard has a critical voltage threshold condition.	1. Ensure that the motherboard is supplied with the required input voltage as per the product specifications. 2. Create a `show tech-support` file and contact Cisco TAC.
BoardPower	compute.Board	Critical	The motherboard has a critical power problem. This occurs when the motherboard power consumption exceeds certain threshold limits. At that time the power usage sensors on a server detect a problem.	1. Ensure that the motherboard is supplied with the required input voltage as per the product specifications. 2. Create a `show tech-support` file and contact Cisco TAC to see if the motherboard needs replacement.
ServerAdapterUnitDeprecated	compute.Physical	Critical	One or more adapters connected to the server are deprecated, or are not supported in the current Intersight release.	1. Verify that only the supported adapters are installed on the server. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
RackUnitHealthWarning	compute.RackUnit	Warning	The server's health state has reached the warning threshold.	1. Read fault summary and determine course of action. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
RackUnitHealthCritical	compute.RackUnit	Critical	The server's health state has reached the critical threshold.	1. Read fault summary and determine course of action. 2. If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
PciNodeInsertedPowerOnRequired	compute.Blade	Warning	This alarm occurs if PCIe node is inserted when the compute node is in powered off state.	1. After inserting the PCIe node, power on the PCIe node's paired compute node. 2. After the paired compute node is completely powered on, rediscover the PCIe node.

Name	MO	Severity	Explanation	Recommended Action
PciNodeRemovedPowerOnRequired	compute.Blade	Warning	This alarm occurs if PCIe node is removed when the compute node is in powered off state.	After removing the PCIe node, power on the PCIe node's paired compute node.
PciNodeInsertedPowerCycleRequired	compute.Blade	Warning	This alarm occurs if PCIe node is inserted when the compute node is in powered on state.	**1.** Power down the paired compute down. **2.** After the paired compute node is completely powered off. Remove the PCIe node. **3.** Before re-inserting a PCIe node, make sure that its paired compute node is powered off. **4.** After the paired compute node has completely powered off, insert the PCIe node. Insert the PCIe node. **5.** Power on the PCIe node's paired compute node. **6.** After the paired compute node is completely powered on, rediscover the PCIe node.
PciNodeRemovedPowerCycleRequired	compute.Blade	Warning	This alarm occurs if PCIe node is removed when the compute node is in powered on state.	**1.** Power down the paired compute down. **2.** After the paired compute node is completely powered off. Remove the PCIe node. **3.** Power on the PCIe node's paired compute node. **4.** After the paired compute node is completely powered on, rediscover the PCIe node.
PciNodeUnsupported	compute.Blade	Warning	Unsupported PCIe node detected. PCIe node will remain powered off.	**1.** Verify that the PCIe node is running the recommended firmware version by checking here **Servers>Server Name>Inventory>GPUs** **>PCIe-Node-GPU Name>General** **2.** Verify that the paired compute node is running the recommended firmware version by checking here **Servers>Server Name>General** **3.** If the firmware versions are compatible, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
PciNodeUnidentified	compute.Blade	Warning	Unidentified PCIe node detected. PCIe node will remain powered off.	**1.** Verify that the inserted PCIe node is running the recommended firmware version here **Servers>Server Name>Inventory>** **GPUs>PCIe-Node-GPU Name>General** **2.** If the firmware is supported, create a `show tech-support` file and contact Cisco TAC.
HostEthInterfaceDown	adapter.HostEthInterface	Critical	The uplink interface is shut down, or a transient error caused the vNIC to fail.	**1.** If an associated port is disabled, enable the port. **2.** Reacknowledge the server with the Ethernet adapter that has the failed link. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
HostEthInterfaceStandByActive	adapter.HostEthInterface	Warning	The preferred path for the failover enabled vNIC is down and hence the secondary path is currently active.	**1.** Update the configuration of the port or port channel to include the primary VLAN. **2.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
HostFcInterfaceDown	adapter.HostFcInterface	Critical	The uplink interface is shut down, or a transient error caused the vHBA to fail.	**1.** If an associated port is disabled, enable the port. **2.** Reacknowledge the server with the Fibre Channel adapter that has the failed link. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
NotReachable	adapter.Unit	Warning	Adapter is not reachable or the connectivity is not discovered from the Fabric Interconnects or FEX.	**1.** Check if the corresponding Input/Output module is inserted in the chassis. **2.** Check if CIMC/BIOS are running recommended firmware version. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
CardTemperatureWarning	graphics.Card	Warning	The GPU has a warning temperature threshold condition.	**1.** Verify that the server fans are working properly. **2.** Wait for 24 hours to see if the problem resolves itself. **3.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
CardTemperatureCritical	graphics.Card	Critical	The GPU has a critical temperature threshold condition.	**1.** Verify that the server fans are working properly. **2.** Wait for 24 hours to see if the problem resolves itself. **3.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
UnitTemperatureWarning	memory.UnitPSU	Warning	The memory unit has a warning temperature threshold condition.	**1.** Verify that the server fans are working properly. **2.** Wait for 24 hours to see if the problem resolves itself. **3.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
UnitTemperatureCritical	memory.Unit	Critical	The memory unit has a critical temperature threshold condition.	**1.** Verify that the server fans are working properly. **2.** Wait for 24 hours to see if the problem resolves itself. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitUncorrectableError	memory.Unit	Critical	The memory unit has encountered an uncorrectable ECC error.	**1.** Monitor the error statistics of the degraded DIMM. **2.** Create a `show tech-support` file and contact Cisco TAC to see if the inoperable DIMM needs a replacement.
UnitBankError	memory.Unit	Warning	The memory unit has encountered a Bank Virtual lock step (VLS) error.	**1.** Restart the host so that the DIMM gets auto-repaired. **2.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitRankError	memory.Unit	Warning	The memory unit has encountered a Rank Virtual lock step (VLS) error.	**1.** Restart the host so that the DIMM gets auto-repaired. **2.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitInvalidPopulation	memory.Unit	Critical	The DIMM slot has been invalidly populated.	**1.** Reseat the DIMM into the correct slot. **2.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
UnitRasModeError	memory.Unit	Critical	The memory unit has encountered a RAS Mode error.	**1.** Reboot the server. **2.** If the issue persists, verify that the DIMMs are installed in a supported configuration. **3.** Reseat the DIMM. **4.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the DIMM needs a replacement.
UnitMismatchError	memory.Unit	Critical	A memory mismatch has been detected on this memory unit.	Create a `show tech-support file` and contact Cisco TAC to see if the mismatched DIMM needs a replacement.
UnitSpdError	memory.Unit	Critical	The memory unit has encountered a SPD error.	Create a `show tech-support file` and contact Cisco TAC to see if the faulty component of the DIMM needs a replacement.
UnitBistError	memory.Unit	Critical	The memory unit has encountered a BIST error.	Create a `show tech-support file` and contact Cisco TAC to see if the faulty component of the DIMM needs a replacement.
UnitInvalidTypeError	memory.Unit	Critical	The memory unit type is invalid.	Create a `show tech-support file` and contact Cisco TAC to see if the failed DIMM needs a replacement.
UnitCatErr	processor.Unit	Critical	The processor has encountered a CATERR error. The system event log (SEL) contains events related to the processor's catastrophic error (CATERR) sensor.	Create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
UnitThermtrip	processor.Unit	Critical	The processor has encountered a THERMTRIP error.	1. Review the product specifications to determine the temperature operating range of the server. 2. Verify that the server fans are working properly. 3. Verify that the air flows on the Cisco UCS chassis or rack server are not obstructed. 4. Power off unused blade servers and rack servers. 5. Set the power profiling, power priority of the server, and the power restore state of the system through server Power Policy. 6. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitTemperatureWarning	processor.Unit	Warning	The processor has a warning temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
UnitTemperatureCritical	processor.Unit	Critical	The processor has a critical temperature threshold condition.	1. Verify that the server fans are working properly. 2. Wait for 24 hours to see if the problem resolves itself. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
NodeRiser1Missing	pci.Node	Warning	The PCIe node Riser 1 is missing. No PCIe lanes to CPU1 can be utilized.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Ensure that all the required hardware are installed as per the guide. 3. If the issue still persists, create a `show tech-support` file and contact Cisco TAC.
NodeRiserMismatch	pci.Node	Warning	The PCIe node Riser type mismatch. Risers will remain powered off.	1. Review the Cisco UCS X440p PCIe Node Installation and Service Guide. 2. Mixing of GPU models are not supported in the compute node. Ensure that each PCIe node is configured with the same type of GPU.

Name	MO	Severity	Explanation	Recommended Action
NodeRiser2PresentCPU2Absent	pci.Node	Warning	PCIe node Riser 2 is present, but CPU2 is absent. PCIe slots on Riser 2 are not connected.	**1.** Review the Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Ensure that all the required hardware are installed as per the guide. **3.** If the issue still persists, create a `show tech-support` file and contact Cisco TAC.
NodePCIeLinkConfigIssue	pci.Node	Warning	PCIe link or port configuration issue detected. PCIe links may not be up or configured properly between PCIe slots and CPUs.	**1.** Review the Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Ensure that all the required hardware are installed as per the guide. **3.** If the issue still persists, create a `show tech-support` file and contact Cisco TAC.
NodeRiser1PowerFault	pci.Node	Critical	PCIe node Riser 1 power fault detected.	**1.** Review the Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Verify that the Power cable for Riser 1 is inserted correctly in the PCIe node. **3.** Verify that the Power cable for Riser 1 is connected to the power source.
NodeRiser2PowerFault	pci.Node	Critical	PCIe node Riser 2 power fault detected.	**1.** Review the Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Verify that the Power cable for Riser 2 is inserted correctly in the PCIe node. **3.** Verify that the Power cable for Riser 2 is connected to the power source.
NodePowerFault	pci.Node	Critical	PCIe node power fault detected.	**1.** Review the Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Verify that the PCIe node has two dark colored GPU cables that carry power and data. **3.** Verify that the Power cables are connected to the power source and inserted into the PCIe node.

Name	MO	Severity	Explanation	Recommended Action
NodeUnsupportedPCIeCardPresentOnRiser1	pci.Node	Warning	PCIe node has an unsupported PCIe card present on Riser 1. Riser will remain powered off.	**1.** Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Install the recommended type of GPU on Riser 1. **3.** Power on the riser.
NodeUnsupportedPCIeCardPresentOnRiser2	pci.Node	Warning	PCIe node has an unsupported PCIe card present on Riser 2. Riser will remain powered off.	**1.** Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Install the recommended type of GPU on Riser 2. **3.** Power on the riser.
NodeUnknownPCIeCardPresentOnRiser1	pci.Node	Warning	PCIe node has an unknown PCIe card present on Riser 1. Riser will remain powered off.	**1.** Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Install the recommended type of GPU on Riser 1. **3.** Power on the riser.
NodeUnknownPCIeCardPresentOnRiser2	pci.Node	Warning	PCIe node has an unknown PCIe card present on Riser 2. Riser will remain powered off.	**1.** Review the Cisco UCS X210c M6 Compute Node Installation and Service Note and Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Install the recommended type of GPU on Riser 1. **3.** Power on the riser.
NodePresentXFM1Absent	pci.Node	Warning	PCIe node detected with missing XFM1. PCIe node cannot be fully managed without both XFMs being present.	**1.** Review the Cisco UCS X440p PCIe Node Installation and Service Guide. **2.** Ensure that all the required hardware are installed as per the guide. **3.** If the issue still persists, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
ControllerLostConfiguration	storage.Controller	Critical	This alarm occurs when the storage controller has lost its configuration data.	When you replace a RAID controller, the RAID configuration that is stored in the controller is lost. Use this procedure to restore your RAID configuration to the new RAID Controller. • For Legacy mode 1. Power off the server, replace your RAID controller. 2. Reboot the server . 3. Press **F** to import foreign configuration(s) when you see the on-screen prompt. • For UEFI Boot mode, 1. Check if the server is configured in Unified Extensible Firmware Interface (UEFI) mode. 2. Power off the server, replace the RAID controller. 3. Reboot the server. 4. Press **F2** when prompted to enter the BIOS Setup utility. 5. Under **Setup Utility**, navigate to **Advanced > Select controller > Configure**, and click Import foreign configuration to Import. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ControllerFailed	storage.Controller	Critical	This alarm occurs when the storage controller is in failed state.	If the Storage controller is in **`failed`** state, create a `show tech-support` file and contact Cisco TAC to see if the controller needs replacement.
ControllerFlashDegraded	storage.Controller	Critical	This alarm occurs when the storage controller is functional, but the on-board flash has degraded.	If you see this fault, take the following action: 1. Reset the CIMC and update Board Controller firmware. 2. For PCI and mezz-based controllers, check the seating of the storage controller. If the problem persists, create a `show tech-support` file and contact Cisco TAC to see if the controller needs replacement.

Name	MO	Severity	Explanation	Recommended Action
ControllerFlashFailed	storage.Controller	Critical	This alarm occurs when the storage controller is functional but the on-board flash has failed.	If the flash is in **`failed`** state, create a `show tech-support` file and contact Cisco TAC to see if the controller needs replacement.
ControllerInvalidFirmware	storage.Controller	Critical	This alarm occurs when the storage controller contains invalid firmware.	**1.** Update the firmware of the Storage Controller. **2.** Reboot the controller. **3.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
ControllerAuthFailure	storage.Controller	Critical	This alarm occurs when SPDM authentication fails for the storage controller.	If you see this fault, take the following actions: **1.** Check whether the storage controller is in the list of supported controllers, if not, create a `show tech-support file` and contact Cisco TAC to replace with a supported controller. **2.** If the Storage Controller firmware has been updated, reboot the controller.
ControllerInvalidConfiguration	storage.Controller	Critical	This alarm occurs when the storage controller contains invalid configuration.	**1.** Check whether the storage controller is in the list of supported controllers. **2.** If not, create a `show tech-support file` and contact Cisco TAC to replace with a supported controller. **3.** If the above actions do not resolve the issue,
ControllerUnresponsive	storage.Controller	Critical	This alarm occurs when contact with the storage controller is probably lost, and the storage controller has become unresponsive.	For PCI and mezz-based storage controllers, check the seating of the storage controller. If the problem persists, create a `show tech-support file` and contact Cisco TAC to see if the controller needs replacement.

Name	MO	Severity	Explanation	Recommended Action
ControllerForeignConfig	storage.Controller	Critical	This alarm occurs when foreign configurations are present in the physical drives attached to the storage controller.	If you see this fault, take the following actions: **1.** On the GUI, click **Clear Foreign Configuration** under ellipsis menu by navigating as follows: **Servers>Server Name> Inventory>Storage Controller>Controller Name** **2.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
PhysicalDiskFailed	storage.PhysicalDisk	Critical	This alarm occurs when the storage physical disk is in failed state.	If the drive state is in **`failed`** state, create a `show tech-support file` and contact Cisco TAC to see if the disk needs to be replaced.
PhysicalDiskPredictiveFailure	storage.PhysicalDisk	Critical	This alarm occurs when storage physical disk is in predictive failure state.	If the drive state is in **`predictive-failure`** state, create a `show tech-support file` and contact Cisco TAC to see if the disk needs to be replaced.
PhysicalDiskOffline	storage.PhysicalDisk	Critical	This alarm occurs when storage physical disk is in Offline state.	If you see this fault, take the following actions: **1.** Verify the presence and health of physical disks. **2.** If applicable, reseat the disks. **3.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to replace the used disks.
PhysicalDiskUnConfiguredBad	storage.PhysicalDisk	Warning	This alarm occurs when the storage physical disk is in Unconfigured Bad state and is not available for RAID volume.	If you see this fault, take the following actions: **1.** Verify the connectivity between physical disks RAID Controller. **2.** Verify the presence and health of physical disks. **3.** Reseat the disks. **4.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the used disks need replacement.

Name	MO	Severity	Explanation	Recommended Action
PhysicalDiskForeignConfig	storage.PhysicalDisk	Critical	This alarm occurs when the storage physical disk contains a foreign configuration.	If you see this fault, take the following actions: **1.** Review Storage Policy configuration in the service profile and verify that the selected server meets the requirements in the policy. **2.** If applicable, reseat the disks. **3.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the disks need replacement.
PhysicalDiskSelfTestFail	storage.PhysicalDisk	Critical	This alarm occurs when the self-test on a storage physical disk has failed.	Create a `show tech-support file` and contact Cisco TAC.
VirtualDriveDegraded	storage.VirtualDrive	Critical	This alarm occurs when the storage virtual drive is in degraded state.	If you see this fault, take the following actions: **1.** If the drive is performing a consistency check operation, wait for the operation to complete. **2.** Verify the presence and health of disks that are used by the virtual drive. **3.** If applicable, reseat the disks. **4.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the used disks need to be replaced.
VirtualDrivePartiallyDegraded	storage.VirtualDrive	Critical	The storage virtual drive is partially degraded. The operating condition of the virtual drive is not optimal.	If you see this fault, take the following actions: **1.** If the drive is performing a consistency check operation, wait for the operation to complete. **2.** Verify the presence and health of disks that are used by the virtual drive. **3.** If applicable, reseat the disks. **4.** If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the disks need replacement.

Name	MO	Severity	Explanation	Recommended Action
VirtualDriveOffline	storage.VirtualDrive	Critical	This alarm occurs when the storage virtual drive is in offline state.	If you see this fault, take the following actions: 1. Verify the presence and health of disks that are used by the virtual drive. 2. If applicable, reseat the disks. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the disks need replacement.
RaidBatteryDegraded	storage.BatteryBackupUnit	Critical	This alarm occurs when the storage battery backup unit is in degraded state.	If you see this fault, take the following actions: 1. If the fault reason indicates the backup unit is in a relearning cycle, wait for relearning to complete. 2. If the fault reason indicates the backup unit is about to fail, create a `show tech-support file` and contact Cisco TAC to see if backup unit needs replacement.
FruMissing	equipment.Fru	Critical	This alarm typically occurs when any hardware component is missing in a server, chassis, FEX or FI and the server or chassis is not rediscovered manually.	If you see this fault, take the following actions: 1. Make sure the hardware component is inserted in the correct slot in the server. 2. Check whether the hardware component is connected and configured properly and is running the recommended firmware version. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
FruReplaced	equipment.Fru	Critical	This alarm typically occurs when any adapter is replaced in a server and the server is not decommissioned and recommissioned.	If you see this fault, take the following actions: 1. For rack servers, decommission and recommission the server if any hardware component is changed. 2. For non-rack servers, acknowledge the server if any hardware component is changed. 3. If no hardware component was changed, Create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
RackFanSpeedCritical	equipment.Fan	Critical	The server fan has a speed threshold condition. This fault typically occurs when a fan is running at a speed that is too slow or too fast. A malfunctioning fan can affect the operating temperature of the rack server.	If you see this fault, take the following actions: 1. If the fan is running below the expected speed, ensure that the fan blades are not blocked. 2. If the fan is running above the expected speed, remove and re-insert the fan. 3. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC to see if the fan needs replacement.
RackPsuInputLost	equipment.Psu	Warning	The power supply has no AC input.	1. Monitor the PSU status. 2. Verify that the power cord is properly connected to the power supply and to the power source. 3. If possible, remove and reseat the PSU. 4. If the above actions do not resolve the issue, create a `show tech-support file` and contact Cisco TAC.
RackPsuTemperatureCritical	equipment.Psu	Critical	The power supply has a temperature threshold condition.	1. Monitor the PSU status. 2. Verify that the server fans are working properly. 3. Create a `show tech-support` file and contact Cisco TAC to see if the fan needs replacement.
RackPsuTemperatureWarning	equipment.Psu	Warning	The power supply has a temperature threshold condition.	1. Monitor the PSU status. 2. Verify that the server fans are working properly. 3. Create a `show tech-support` file and contact Cisco TAC to see if the faulty fan needs replacement.
RackPsuOutputCurrentCritical	equipment.Psu	Critical	The power supply has a output current threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputCurrentWarning	equipment.Psu	Warning	The power supply has a output current threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputVoltageCritical	equipment.Psu	Critical	The power supply has an output voltage threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.

Name	MO	Severity	Explanation	Recommended Action
RackPsuOutputVoltageWarning	equipment.Psu	Warning	The power supply has an output voltage threshold condition.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputPowerCritical	equipment.Psu	Critical	The server power supply has an output power threshold condition. This fault occurs if the current output of the PSU in the rack server is far above or below the non-recoverable threshold value.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
RackPsuOutputPowerWarning	equipment.Psu	Warning	The server power supply has an output power threshold condition. This fault occurs if the current output of the PSU in the rack server is far above or below the non-recoverable threshold value.	Create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ServerProfileStateOutOfSyncWarning	server.profile	Warning	The server profile moved to Out-of-sync state.	**1.** Evaluate the differences between the server profile configuration and the end-point configuration. **2.** Redeploy server profile to apply the configuration in server profile.
ServerProfileStatePendingChangesWarning	server.profile	Warning	The server profile has moved to pending-changes state.	Check the server policy configuration for Pending-changes and deploy the server profile again to apply the changes.
ComputeCimcFirmwareNotSupported	compute.BladeIdentity	Warning	This fault indicates that one of the IO modules is missing.	Intersight Managed Mode does not support the existing firmware version. Upgrade the server using the firmware upgrade option in the Chassis tab.
ComputeServerNotConnected	compute.BladeIdentity	Warning	Server discovery failed because the device is not connected.	Server discovery failed because the device is not connected. For further assistance, contact Cisco TAC.
ComputeServerDisconnected	compute.Physical	Warning	Server is not reachable.	If you see this alarm, take the following actions. Check the server's network connectivity.

Name	MO	Severity	Explanation	Recommended Action
ComputePhysicalBiosPostTimeOut	compute.Physical	Critical	This alarm typically occurs when the server has encountered a BIOS POST timeout.	For further assistance, contact Cisco TAC.
StoragePhysicalDiskReadyForRemoval	storage.PhysicalDisk	Informational (Info)	The physical disk is in quiesced state and ready for removal.	For further assistance, contact Cisco TAC.
StoragePhysicalDiskRebuilding	storage.PhysicalDisk	Informational (Info)	The physical disk is in rebuilding state.	For further assistance, contact Cisco TAC.
StorageVirtualDriveCacheDegraded	storage.VirtualDrive	Warning	Virtual drive cache is in degraded state.	For further assistance, contact Cisco TAC.

CHAPTER 3

Chassis and FEX Alarms

Chassis and FEX Components Alarms

Following table shows the description of the supported alarms for chassis and FEX components.

Name	MO	Severity	Explanation	Recommended Action
IoCardTemperatureCritical	equipment.IoCard	Critical	The I/O Card has a critical temperature threshold condition.	**1.** View the acceptable temperature and voltage parameters and determine how much of the outlet or inlet temperature has reached or exceeded over the major or minor threshold value. **2.** Monitor other environmental events and ensure the temperature ranges are within recommended ranges. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
IoCardTemperatureWarning	equipment.IoCard	Warning	The I/O Card has a warning temperature threshold condition.	**1.** View the acceptable temperature and voltage parameters and determine how much of the outlet or inlet temperature has reached or exceeded over the major or minor threshold value. **2.** Monitor other environmental events and ensure the temperature ranges are within recommended ranges. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
ChassisInputPowerCritical	equipment.Chassis	Critical	The chassis input power has crossed the threshold condition.	**1.** Monitor the PSU status. **2.** Verify that the input power cord is appropriate as per the spec sheet. **3.** If possible, remove and reset the PSU. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ChassisInputPowerWarning	equipment.Chassis	Warning	The chassis input power has reached the threshold condition.	**1.** Monitor the PSU status. **2.** Verify that the input power cord is appropriate as per the spec sheet. **3.** If possible, remove and reset the PSU. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ChassisOutputPowerCritical	equipment.Chassis	Critical	The chassis output power has crossed the threshold condition.	**1.** Monitor the PSU status. **2.** Verify that the output power matches the maximum rated output power as per the spec sheet. **3.** If possible, remove and reset the PSU. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ChassisOutputPowerWarning	equipment.Chassis	Warning	The chassis output power has reached the threshold condition.	**1.** Monitor the PSU status. **2.** Verify that the output power matches the maximum rated output mentioned in the spec sheet. **3.** If possible, remove and reseat the PSU. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
ChassisFansMissing	equipment.Chassis	Critical	Multiple chassis fans are not operational or missing.	**1.** Check the fans operational state on the GUI. **Chassis>Inventory>Thermal>Fan Modules>Fan Module Name>Fans** **2.** Check the fan-related syslog messages to see the exact reason for the failure. **3.** Create a `show tech-support` file and contact Cisco TAC to see if the fans need replacement.
ChassisFanMissing	equipment.Chassis	Warning	A single chassis fan is not operational or missing.	**1.** Check the fans operational state on the GUI. **Chassis>Inventory>Thermal>Fan Modules>Fan Module <ID>>Fans** **2.** Check the fan-related syslog messages to see the exact reason for the failure. **3.** Create a `show tech-support` file and contact Cisco TAC to see if the fan needs replacement.
ChassisPsuRedundancyLost	equipment.Chassis	Critical	The chassis power supply redundancy lost.	**1.** Consider adding more PSUs to the chassis. **2.** If the issue still persists, create a `show tech-support` file and contact Cisco TAC.
IoCardLowMemory	equipment.IoCard	Critical	The I/O Card has a critical low memory error.	Create a `show tech-support` file and contact Cisco TAC.
IoCardFruState	equipment.IoCard	Critical	The I/O Card Field Replacement Unit (FRU) is not readable.	Create a `show tech-support` file and contact Cisco TAC.
ChassisFruState	equipment.Chassis	Critical	The Chassis Field Replacement Unit (FRU) is not readable.	**1.** Verify that a supported adapter is installed. **2.** Create a `show tech-support` file and contact Cisco TAC to see if the adapter needs replacement.
IoCardPost	equipment.IoCard	Warning	The I/O Card has a POST error.	Create a `show tech-support` file and contact Cisco TAC.
IoCardAsicPost	equipment.IoCard	Warning	The I/O Card ASIC has a POST error	Create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
IoCardSelectedImage	equipment.IoCard	Warning	There is some issue with the current I/O Card firmware image.	**1.** Review the fault and the error message on **Chassis>Inventory>IO Modules** to determine why the firmware image is unusable. **2.** If the firmware image is bad or corrupted, upgrade the server firmware/HSU bundle. **3.** If the issue still persists, create a `show tech-support` file and contact Cisco TAC.
IoCardAlternateImage	equipment.IoCard	Warning	There is some issue with the alternate firmware image of the I/O Card.	**1.** Review the fault and the error message on **Chassis>Inventory>IO Modules** to determine why the firmware image is unusable. **2.** If the firmware image is bad or corrupted, upgrade the server firmware/HSU bundle. **3.** If the image is present and the fault persists, create a `show tech-support` file and contact Cisco TAC.
ChassisPowerCritical	equipment.Chassis	Critical	The chassis power supply has critical issue.	**1.** Review the product specifications to determine the operating temperature range of the PSU module. **2.** Power off unused blade servers and rack servers. **3.** Check the power supply unit that has the problem, as follows: • On the CLI, run the following command on chassis IFM/ IOM to get the power details: `pwrmgrcli -a` • On the GUI, view the PSUs tab here: **Chassis>Inventory>Power>PSUs** **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
ChassisPowerWarning	equipment.Chassis	Warning	The chassis power supply has warning issue.	1. Review the product specifications to determine the temperature operating range of the PSU module. 2. Power off unused blade servers and rack servers. 3. Check the power supply unit that has the problem, as follow: • On the CLI, run the following command on chassis IFM/ IOM to get the power details: `pwrmgrcli -a` • On the GUI, view the PSUs tab here: **Chassis>Inventory>** **Power>PSUs** 4. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ChassisPsuFruState	equipment.Psu	Critical	The power supply Field Replacement Unit (FRU) is not readable.	Create a `show tech-support` file and contact Cisco TAC.
ChassisPsuUnresponsive	equipment.Psu	Critical	The power supply is unresponsive.	1. Check the power supply unit that has the problem, as follow: • On the CLI, run the following command on chassis IFM/ IOM to get the power details: `pwrmgrcli -a` • On the GUI, view the PSUs tab here: **Chassis>Inventory>Power>PSUs** 2. Verify that the power cord is properly connected to the power supply and to the power source. 3. Ensure that the power supply is properly inserted and plugged in. 4. If problem persists, remove and re-insert the power-supply unit. 5. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
ChassisPsuInputOutOfRange	equipment.Psu	Warning	The chassis power supply has out of range AC input.	**1.** Check the power supply unit that has the problem, as follow: • On the CLI, run the following command on chassis IFM/ IOM to get the power details: `pwrmgrcli -a` • On the GUI, view the PSUs tab here: **Chassis>Inventory>Power>PSUs** **2.** Verify that the power cord is properly connected to the power supply and to the power source. **3.** Ensure that the power supply is properly inserted and plugged in. **4.** If problem persists, remove and re-insert the power-supply unit. **5.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ChassisPsuInputLost	equipment.Psu	Warning	The power supply has no AC input.	**1.** Monitor the PSU status. **2.** Verify that the power cord is properly connected to the power supply and to the power source. **3.** If possible, remove and reseat the PSU. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ChassisPsuOutput	equipment.Psu	Critical	The power supply has an error condition that prevents DC output.	**1.** Monitor the PSU status. **2.** Verify that the power cord is properly connected to the power supply and to the power source. **3.** Remove and reseat the PSU. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
ChassisPsuTemperatureCritical	equipment.Psu	Critical	The power supply has a temperature threshold condition.	**1.** Monitor the PSU status. **2.** Verify that the server fans are working properly. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.

Name	MO	Severity	Explanation	Recommended Action
ChassisPsuTemperatureWarning	equipment.Psu	Warning	The power supply has a temperature threshold condition.	1. Monitor the PSU status. 2. Verify that the server fans are working properly. 3. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
ChassisPsuInputVoltageCritical	equipment.Psu	Critical	The power supply input voltage has crossed threshold condition.	1. Verify that the power cord is properly connected to the PSU and the power source. 2. Verify that the power source is within the input voltage range mentioned in the spec sheet. 3. Verify that the PSU is properly installed in the chassis. 4. Remove the PSU and reinstall it. 5. If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ChassisPsuInputVoltageWarning	equipment.Psu	Warning	The power supply input voltage has reached threshold condition.	1. Verify that the power cord is properly connected to the PSU and the power source. 2. Verify that the power source is within the input voltage range mentioned in the spec sheet. 3. Verify that the PSU is properly installed in the chassis. 4. Remove the PSU and reinstall it. 5. If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ChassisPsuOutputCurrentCritical	equipment.Psu	Critical	The power supply output current has crossed the threshold condition.	1. Monitor the PSU status. 2. Remove and reseat the PSU. 3. If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ChassisPsuOutputCurrentWarning	equipment.Psu	Warning	The power supply output current has reached the threshold condition.	1. Monitor the PSU status. 2. Remove and reseat the PSU. 3. If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.

Name	MO	Severity	Explanation	Recommended Action
ChassisPsuOutputVoltageCritical	equipment.Psu	Critical	The power supply output voltage has crossed the threshold condition.	**1.** Verify that the power cord is properly connected to the PSU and the power source. **2.** Verify that the power source is within the output voltage range mentioned in the spec sheet. **3.** Verify that the PSU is properly installed in the chassis. **4.** Remove the PSU and reinstall it. **5.** If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ChassisPsuOutputVoltageWarning	equipment.Psu	Warning	The power supply output voltage has reached the threshold condition.	**1.** Verify that the power cord is properly connected to the PSU and the power source. **2.** Verify that the power source is within the output voltage range mentioned in the spec sheet. **3.** Verify that the PSU is properly installed in the chassis. **4.** Remove the PSU and reinstall it. **5.** If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ChassisPsuOutputPowerCritical	equipment.Psu	Critical	The power supply output power has crossed the threshold condition.	**1.** Verify that the power cord is properly connected to the PSU and the power source. **2.** Verify that the output power matches the maximum rated output mentioned in the spec sheet. **3.** Verify that the PSU is properly installed in the chassis. **4.** Remove the PSU and reinstall it. **5.** If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
ChassisFanFruState	equipment.Fan	Critical	The fan Field Replacement Unit (FRU) is not readable.	If you see this fault, take the following actions: **1.** Remove fan module and re-install the fan module again. Remove only one fan module at a time. **2.** Create a `show tech-support` file and contact Cisco TAC to see if the fan module needs to be replaced with a different fan module.

Name	MO	Severity	Explanation	Recommended Action
ChassisFanUnresponsive	equipment.Fan	Critical	The chassis fan is unresponsive.	If you see this fault, take the following actions: **1.** Check the status of the fan module here for Cisco UCS X-Series Chassis **Chassis>Chassis Name>Inventory>Intelligent Fabric Modules>IFM name>Fan Modules>Fans** or Check the status of the fan module here for chassis other than Cisco UCS X-Series. **Chassis>Chassis Name>Inventory>Thermal>Fan Modules>Fans** **2.** Check the operational state of the fan. **3.** Create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
ChassisFanTemperatureCritical	equipment.Fan	Critical	The chassis fan has a temperature threshold condition.	**1.** Review the product specifications to determine the temperature operating range of the fan module. **2.** Power off unused blade servers and rack servers. **3.** Verify that the site cooling system is operating properly. **4.** Set the value of the Fan Control Mode for the chassis using Chassis Thermal policy. **5.** Create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
ChassisFanTemperatureWarning	equipment.Fan	Warning	The chassis fan has a temperature threshold condition.	**1.** Review the product specifications to determine the temperature operating range of the fan module. **2.** Power off unused blade servers and rack servers. **3.** Verify that the site cooling system is operating properly. **4.** Set the value of the Fan Control Mode for the chassis using Chassis Thermal policy. **5.** Create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.

Name	MO	Severity	Explanation	Recommended Action
ChassisFanSpeedCritical	equipment.Fan	Critical	The chassis fan has a speed threshold condition.	If you see this fault, take the following actions: **1.** If the fan is running below the expected speed, ensure that the fan blades are not blocked. **2.** If the fan is running above the expected speed, remove and re-insert the fan. **3.** If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
ChassisFanSpeedWarning	equipment.Fan	Warning	The chassis fan has a speed threshold condition.	If you see this fault, take the following actions: **1.** If the fan is running below the expected speed, ensure that the fan blades are not blocked. **2.** If the fan is running above the expected speed, remove and re-insert the fan. **3.** If the issue persists, create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
FexPsuInoperable	equipment.Psu	Critical	This alarm occurs if a Power Supply is not operational.	**1.** Check the PSU status by navigating on the GUI as follows: **Chassis >Chassis Name >Inventory> Power>PSUs** **2.** Create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.

Name	MO	Severity	Explanation	Recommended Action
FexPsuPoweredOff	equipment.Psu	Critical	This alarm occurs if a Power Supply is powered off either due to higher than expected power or due to higher than expected temperatures or because of the failure of a fan.	**1.** Check the power supply unit that has the problem, as follow: • On the GUI, view the PSUs tab here: on the GUI **Fabric Interconnects > Fabric Interconnect Name > Connections > Fabric Extenders>Inventory>PSUs** **2.** Verify that the power cord is properly connected to the power supply and to the power source. **3.** Ensure that the power supply is properly inserted and plugged in. **4.** Ensure that the PSU is operating in the permissible temperature range. **5.** Verify that the fans are working properly. **6.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
FexFanInoperable	equipment.Fan	Critical	This alarm occurs if a fan is not operational.	**1.** Check the fan status on the GUI **Fabric Interconnects > Fabric Interconnect Name > Connections > Fabric Extenders>Inventory>Fan Modules** **2.** Check the fan-related syslog messages to see the exact reason for the failure. **3.** Create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.

Name	MO	Severity	Explanation	Recommended Action
FexFanPoweredOff	equipment.Fan	Critical	This alarm occurs if a fan is shutdown.	**1.** Check the fan status on the GUI **Fabric Interconnects > Fabric Interconnect Name > Connections > Fabric Extenders>Inventory>Fan Modules** **2.** Check the fan-related syslog messages to see the exact reason for the failure. **3.** If the fan is OK, Check the PSU status **Fabric Interconnects > Fabric Interconnect Name > Connections > Fabric Extenders>Inventory>PSUs** **4.** Verify that the power cord is properly connected to the power supply and to the power source. **5.** Ensure that the power supply is properly inserted and plugged in. **6.** If problem persists, remove and re-insert the power-supply unit. **7.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
IoCardOffline	equipment.IoCard	Critical	The I/O Card is offline. This fault typically occurs because an I/O module has lost its connection to the Fabric Interconnects.	**1.** Wait a few minutes to see if the fault clears. This is typically a temporary issue, and can occur after a firmware upgrade. **2.** If the fault does not clear after a few minutes, remove, and reinsert the I/O card. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
IoCardMissing	equipment.IoCard	Critical	I/O Card is missing or removed.	**1.** Reinsert the I/O card and configure the Fabric Interconnect ports connected to it as server ports and wait a few minutes to see if the fault clears. **2.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

CHAPTER 4

Fabric Interconnect Alarms

Fabric Interconnect Components Alarms

Following table shows the description of the supported alarms for Fabric Interconnect components.

Name	MO	Severity	Explanation	Recommended Action
PeerFirmwareOutOfSync	network.element	Info	This alarm is triggered when there is a discrepancy in the firmware version between peer fabric interconnects, indicating that they are not synchronized.	1. Initiate the firmware upgrade process on the peer fabric interconnect to align its firmware version with the other interconnect. 2. Verify that both fabric interconnects are operating on identical firmware versions post-upgrade to ensure synchronization.
fpgaUpgrade	network.Element	Critical	This alarm occurs when you update to Infrastructure Release 4.1(3) or a later version on Cisco UCS 6400 Series Fabric Interconnects, you may notice a specific message on one or both Fabric Interconnects, depending on the original factory-shipped code for the device. There is no production risk involved. However, it's important to note that the security level may be slightly lower.	To enhance the security of your Field-Programmable Gate Array (FPGA), execute the 'activate secure-fpga' command on the target device through your console's Command Line Interface (CLI). For more information, see Intersight Help Center.
NetworkSwitchEvacuated	network.Element	Info	This alarm is triggered when the Fabric Interconnect is evacuated. For example, Evacuation enabled for DomainName/switch-B.	Disable the Fabric Evacuation on the Fabric Interconnect for the alarm to get cleared.

Name	MO	Severity	Explanation	Recommended Action
SwitchFanModuleInoperable	equipment.FanModule	Critical	This alarm occurs if a fan module is not operational. It can occur when one or more fans in a fan module are not operational.	**1.** Check the fan module status on the GUI **Fabric Interconnects>Inventory>Fan Modules** **2.** Ensure that at least one fan is installed and functioning properly. **3.** Check the fan-related syslog messages to see the exact reason for the failure. **4.** Create a `show tech-support` file and contact Cisco TAC to see if the fan needs replacement.
SwitchFanInoperable	equipment.Fan	Critical	This alarm occurs if a fan is not operational.	**1.** Check the fan status on the GUI **Fabric Interconnects>Inventory>Fan Modules** **2.** Check the fan-related syslog messages to see the exact reason for the failure. **3.** Create a `show tech-support` file and contact Cisco TAC to see if the fan needs replacement.
SwitchFanPoweredOff	equipment.Fan	Critical	This alarm occurs if a fan is shutdown.	**1.** Check the fan status on the GUI **Fabric Interconnects>Inventory>Fan Modules** **2.** Check the fan-related syslog messages to see the exact reason for the failure. **3.** If the fan is OK, Check the PSU status **Fabric Interconnects>Inventory>PSUs** **4.** Verify that the power cord is properly connected to the power supply and to the power source. **5.** Ensure that the power supply is properly inserted and plugged in. **6.** If problem persists, remove and re-insert the power-supply unit. **7.** If the status continues to show fail or shutdown, create a `show tech-support` file and contact Cisco TAC to see if the faulty power supply unit needs replacement.

Name	MO	Severity	Explanation	Recommended Action
SwitchPsuInoperable	equipment.Psu	Critical	This alarm occurs if a Power Supply is not operational.	**1.** Check the power supply unit that has the problem, as follow: • On the GUI, view the PSUs tab here: **Fabric Interconnects>Inventory>PSUs** **2.** Verify that the power cord is properly connected to the power supply and to the power source. **3.** Ensure that the power supply is properly inserted and plugged in. **4.** If problem persists, remove and re-insert the power-supply unit. **5.** If the power supply light is still not green and the status continues to show fail or shutdown, create a `show tech-support` file and contact Cisco TAC to see if the PSU needs replacement.
SwitchPsuPoweredOff	equipment.Psu	Critical	This alarm occurs if a Power Supply is powered off either due to higher than expected power or due to higher than expected temperatures, or because of the failure of a fan.	**1.** Check the power supply unit that has the problem, as follow: • On the GUI, view the PSUs tab here: on the GUI **Fabric Interconnects>Inventory>PSUs** **2.** Verify that the power cord is properly connected to the power supply and to the power source. **3.** Ensure that the power supply is properly inserted and plugged in. **4.** Ensure that the PSU is operating in the permissible temperature range. **5.** Verify that the server fans are working properly. **6.** Create a `show tech-support` file and contact Cisco TAC to see if any hardware needs replacement.
VlanPortCountThreshold	network.VlanPortInfo	Warning	This alarm typically occurs when the total number of configured VLANs in the Cisco UCS instance has exceeded 90% of the allowed maximum number of configured VLANs on the Fabric Interconnect.	**1.** Ensure that Port VLAN Count with **VLAN Port Count Optimization Enabled** on Cisco UCS 6400 Series and 6500 Series FI in Intersight Managed Mode does not exceed 97200. **2.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
VlanPortCountExceeded	network.VlanPortInfo	Critical	This alarm typically occurs when the total number of configured VLANs in the Cisco UCS instance has exceeded the allowed maximum number of configured VLANs on the Fabric Interconnect.	**1.** Ensure that Port VLAN Count with **VLAN Port Count Optimization Enabled** on Cisco UCS 6400 Series and 6500 Series FI in Intersight Managed Mode does not exceed 108000. **2.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
SwitchDisconnected	network.Element	Critical	This alarm typically occurs when device cannot connect to Intersight. It can occur when a power cable is disconnected or input voltage is incorrect.	**1.** Ensure that the power supply is properly inserted and plugged in. **2.** Ensure that the device is supplied with the required input voltage as per the product specifications. **3.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
SwitchInoperable	network.Element	Critical	This alarm typically occurs when the device connector reports that the connectivity state of this switch is down.	**1.** Ensure that the power supply is properly inserted and plugged in. **2.** Ensure that the device is supplied with the required input voltage as per the product specifications. **3.** Ensure that the device is connected to the network. **4.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
SwitchEvacuated	network.Element	Info	This alarm typically occurs when the switch is evacuated.	**1.** Ensure that the Evacuation option is switched off for the Fabric Interconnects. **2.** If the above action does not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
SwitchThermalError	network.Element	Warning	This alarm occurs when the temperature of a Fabric Interconnect exceeds a critical threshold value.	1. Review the product specifications to determine the operating temperature range of the Fabric Interconnect. 2. Power off unused blade servers and rack servers. 3. Verify that the server fans are working properly. 4. Clean the installation site at regular intervals to avoid buildup of dust and debris, which can cause a system to overheat. 5. Set the power profiling, power priority of the server, and the power restore state of the system through server Power Policy. 6. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
EtherTransceiverNotPresent	network.Element	Info	When a switch port is not in an unconfigured state, an SFP is required for its operation. This alarm is raised to indicate that the either SFP is faulty or missing from a configured port.	If you see this fault, insert a supported SFP into the port on the Fabric Interconnect. Refer to the documentation on the Cisco website for a list of supported SFPs.
EtherPortLinkDown	network.Element	Warning	This alarm occurs when a Fabric Interconnect port is in link-down state. This state impacts the traffic destined for the port.	1. Verify that the physical link is properly connected between the Fabric Interconnect and the peer component. 2. Verify that the configuration on the peer entity is properly configured and matches the Fabric Interconnect port configuration. 3. Unconfigure and re-configure the port. 4. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
FcPcLinkDown	network.Element	Warning	This fault occurs when a Fabric Interconnect port channel is in link-down state. This state impacts the traffic destined for the port channel.	1. Check the link connectivity on the upstream Fibre Channel switch. 2. If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.

Name	MO	Severity	Explanation	Recommended Action
FcPortLinkDown	network.Element	Warning	This fault occurs when a Fabric Interconnect port is in link-down state. This state impacts the traffic destined for the port.	**1.** Verify that the physical link is properly connected between the Fabric Interconnect and the peer component. **2.** Verify that the configuration on the peer entity is properly configured and matches the Fabric Interconnect port configuration. **3.** Unconfigure and re-configure the port. **4.** If the above actions do not resolve the issue, create a `show tech-support` file and contact Cisco TAC.
FcTransceiverNotPresent	network.Element	Info	When a switch port is not in an unconfigured state, an SFP is required for its operation. This alarm is raised to indicate that the SFP is missing from a configured port.	If you see this fault, insert a supported SFP into the port on the Fabric Interconnect. Refer to the documentation on the Cisco website for a list of supported SFPs.

CHAPTER 5

General Alarms

General Alarms

General alarms include alerts within Intersight that are generic and not related to Server, Chassis and FEX, or Fabric Interconnect alarms categories.

Following table shows the description of the supported general alarms for Intersight.

Name	MO	Severity	Explanation	Recommended Action
ApiKeyExpiringWarning	iam.ApiKey	Warning	This alarm is raised when there is an API key that is about to expire in the next 30 days.	If permissible, extend the expiration date of the API key. If extension of expiry date is not possible, delete the API key and replace it with a new API key. If the API key is no longer required, disable and delete the API key.
ApiKeyExpiringCritical	iam.ApiKey	Critical	This alarm is raised when there is an API key that is about to expire in the next 7 days.	If permissible, extend the expiration date of the API key. If extension of expiry date is not possible, delete the API key and replace it with a new API key. If the API key is no longer required, disable and delete the API key.
ApiKeyExpired	iam.ApiKey	Critical	This alarm is raised when there is an expired API key.	Take action to rotate the API key. Delete the API key and replace it with a new API key. If the API key is no longer required, delete the API key.
ApiKeyIsNeverExpiring	iam.ApiKey	Info	This alarm is raised when there is an existing API key or a new API key is generated without a specified expiration date.	Keys that never expire pose a security risk. If required, delete the never-expiring key and replace it with a key with an expiration date or set an expiration date using the calendar.
OAuthApplicationExpiringWarning	iam.AppRegistration	Warning	This alarm is raised when there is an OAuth 2.0 Application that is about to expire in the next 30 days.	If permissible, extend the expiration date of the OAuth 2.0 Application. If extension of expiry date is not possible, delete the OAuth 2.0 Application and replace with a new OAuth 2.0 Application. If the OAuth 2.0 Application is no longer required, disable and delete the OAuth 2.0 Application.

Name	MO	Severity	Explanation	Recommended Action
OAuthApplicationExpiringCritical	iam.AppRegistration	Critical	This alarm is raised when there is an OAuth 2.0 Application that is about to expire in the next 7 days.	If permissible, extend the expiration date of the OAuth 2.0 Application. If extension of expiry date is not possible, delete the OAuth 2.0 Application and replace with a new OAuth 2.0 Application. If the OAuth 2.0 Application is no longer required, disable and delete the OAuth 2.0 Application.
OAuthApplicationExpired	iam.AppRegistration	Critical	This alarm is raised when there is an OAuth 2.0 Application that has expired.	Take action to rotate the OAuth 2.0 Application. Delete the OAuth 2.0 Application and replace with a new OAuth 2.0 Application. If the OAuth 2.0 Application is no longer required, disable and delete the OAuth 2.0 Application.
OAuthApplicationIsNeverExpiring	iam.AppRegistration	Info	This alarm is raised when there is an OAuth 2.0 Application that is set to never-expire.	OAuth 2.0 Applications that never expire pose a security risk. If required, delete the never-expiring OAuth 2.0 Application and replace with a new OAuth 2.0 Application with expiration date.
SingleAccountAdminLockoutStatus	iam.Account	Warning	The account is prone to lockout if the configured Account Administrator loses access.	Account is at risk of being locked out if the configured Account Administrator loses access. To mitigate this risk, either configure more than 1 user with the Account Administrator role or configure a User Group with the Account Administrator role assigned to it.