Intersight Alarms Overview

- Alarms in Intersight, on page 1

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	EquipmentSwitchPsu PoweredOff	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.