



Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:

- [Configuring Settings for the Fault Collection Policy, page 1](#)
- [Configuring Settings for the Core File Exporter, page 3](#)
- [Configuring the Syslog, page 4](#)

Configuring Settings for the Fault Collection Policy

Fault Collection Policy

The fault collection policy controls the lifecycle of a fault in a Cisco UCS instance, including when faults are cleared, the flapping interval (the length of time between the fault being raised and the condition being cleared), and the retention interval (the length of time a fault is retained in the system).

A fault in Cisco UCS has the following lifecycle:

- 1 A condition occurs in the system and Cisco UCS Manager raises a fault. This is the active state.
- 2 When the fault is alleviated, it is cleared if the time between the fault being raised and the condition being cleared is greater than the flapping interval, otherwise, the fault remains raised but its status changes to soaking-clear. Flapping occurs when a fault is raised and cleared several times in rapid succession. During the flapping interval the fault retains its severity for the length of time specified in the fault collection policy.
- 3 If the condition reoccurs during the flapping interval, the fault remains raised and its status changes to flapping. If the condition does not reoccur during the flapping interval, the fault is cleared.
- 4 When a fault is cleared, it is deleted if the clear action is set to delete, or if the fault was previously acknowledged, otherwise, it is retained until either the retention interval expires, or if the fault is acknowledged.
- 5 If the condition reoccurs during the retention interval, the fault returns to the active state. If the condition does not reoccur, the fault is deleted.

Configuring the Fault Collection Policy

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** tab.
- Step 2** On the **Admin** tab, expand **All ► Faults, Events, and Audit Log**.
- Step 3** Click **Settings**.
- Step 4** In the **Work** pane, complete the following fields in the **Fault Collection Policy** area:

Name	Description
Flapping Interval field	<p>Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, the system does not allow a fault to change its state until this amount of time has elapsed since the last state change.</p> <p>If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the Clear Action field.</p> <p>Enter an integer between 5 and 3,600. The default is 10.</p>
Clear Action field	<p>This can be:</p> <ul style="list-style-type: none"> • retain—Cisco UCS Manager GUI displays the Length of time to retain cleared faults section. • delete—The system immediately deletes all fault messages as soon as they are marked as cleared.
Length of Time to Retain Cleared Faults Section	
Retention Interval field	<p>This can be:</p> <ul style="list-style-type: none"> • forever—The system leaves all cleared fault messages on the fabric interconnect regardless of how long they have been in the system. • other—Cisco UCS Manager GUI displays the dd:hh:mm:ss field.
dd:hh:mm:ss field	The number of days, hours, minutes, and seconds that should pass before the system deletes a cleared fault message.

- Step 5** Click **Save Changes**.

Configuring Settings for the Core File Exporter

Core File Exporter

Cisco UCS Manager uses the Core File Exporter to export core files as soon as they occur to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core file.

Configuring the Core File Exporter

Procedure

- Step 1** In the **Navigation** pane, click the **Admin** tab.
- Step 2** On the **Admin** tab, expand **All ► Faults, Events, and Audit Log**.
- Step 3** Click **Settings**.
- Step 4** In the **Work** pane, complete the following fields in the **TFTP Core Exporter** area:

Name	Description
Admin State field	This can be: <ul style="list-style-type: none"> • enabled—If an error causes the server to perform a core dump, the system sends the core dump file via FTP to a given location. When this option is selected, Cisco UCS Manager GUI displays the other fields in this area that enable you to specify the FTP export options. • disabled—Core dump files are not automatically exported.
Description field	A user-defined description of the core file.
Port field	The port number to use when exporting the core dump file via TFTP.
Hostname field	The hostname or IP address to connect with via TFTP. Note If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.
Path field	The path to use when storing the core dump file on the remote system.

- Step 5** Click **Save Changes**.

Disabling the Core File Exporter

Procedure

-
- Step 1** In the **Navigation** pane, click the **Admin** tab.
- Step 2** On the **Admin** tab, expand **All ► Faults, Events, and Audit Log**.
- Step 3** Click **Settings**.
- Step 4** In the **Work** pane, click the **Settings** tab.
- Step 5** In the **TFTP Core Exporter** area, click the **disabled** radio button in the **Admin State** field.
- Step 6** Click **Save Changes**.
-

Configuring the Syslog

Procedure

-
- Step 1** In the **Navigation** pane, click the **Admin** tab.
- Step 2** On the **Admin** tab, expand **All ► Faults, Events, and Audit Log**.
- Step 3** Click **Syslog**.
- Step 4** In the **Work** pane, click the **Syslog** tab.
- Step 5** In the **Local Destinations** area, complete the following fields:

Name	Description
Console Section	
Admin State field	This can be: <ul style="list-style-type: none"> • enabled • disabled
Level field	If the Admin State field is enabled , select the lowest message level that you want displayed. The system displays that level and above on the console. <ul style="list-style-type: none"> • emergencies • alerts • critical
Monitor Section	

Name	Description
Admin State field	This can be: <ul style="list-style-type: none"> • enabled • disabled If Admin State is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	If the Admin State field is enabled , select the lowest message level that you want displayed. The system displays that level and above on the monitor. <ul style="list-style-type: none"> • alerts • critical • debugging • emergencies • errors • information • notifications • warnings
File Section	
Admin State field	This can be: <ul style="list-style-type: none"> • enabled • disabled If Admin State is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level and above in a file on the fabric interconnect. <ul style="list-style-type: none"> • alerts • critical • debugging • emergencies • errors • information • notifications

Name	Description
	<ul style="list-style-type: none"> • warnings
Name field	The name of the file in which the messages are logged.
Size field	The maximum size, in bytes, the file can be before Cisco UCS Manager GUI begins to write over the oldest messages with the newest ones.

Step 6 In the **Remote Destinations** area, complete the following fields to configure up to three external logs that can store messages generated by the Cisco UCS components:

Name	Description
Admin State field	<p>This can be:</p> <ul style="list-style-type: none"> • enabled • disabled <p>If Admin State is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.</p>
Level drop-down list	<p>Select the lowest message level that you want the system to store. The system stores that level and above in the remote file.</p> <ul style="list-style-type: none"> • alerts • critical • debugging • emergencies • errors • information • notifications • warnings
Hostname field	<p>The hostname or IP address on which the remote log file resides.</p> <p>Note If you use a hostname rather than an IP address, you must configure a DNS server in Cisco UCS Manager.</p>
Facility drop-down list	<p>This can be:</p> <ul style="list-style-type: none"> • local0 • local1 • local2 • local3

Name	Description
	<ul style="list-style-type: none">• local4• local5• local6• local7

Step 7 Click **Save Changes**.
