Cisco UCS Manager GUI System Monitoring Guide, Release 2.5

First Published: April 07, 2015

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

CONTENTS

Preface

This preface includes the following sections:

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.

Text Type	Indication
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.
{x | y | z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
< >	Nonprinting characters such as passwords are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

For a complete list of all C-Series documentation, see the *Cisco UCS C-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/c-series-doc.

For a complete list of all M-Series documentation, see the *Cisco UCS M-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_M_Series_Servers_Documentation_Roadmap.html

Other Documentation Resources

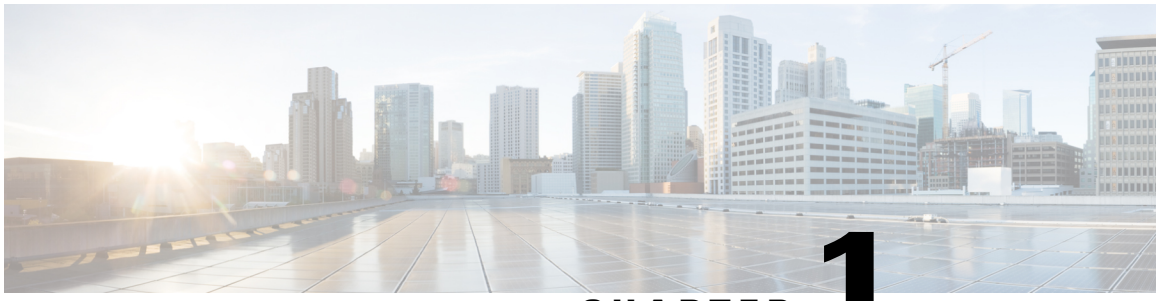
Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to ucs-docfeedback@cisco.com. We appreciate your feedback.

PART I

System Monitoring



CHAPTER 1

Monitoring Traffic

This chapter includes the following sections:

Traffic Monitoring

Traffic monitoring copies traffic from one or more sources and sends the copied traffic to a dedicated destination port for analysis by a network analyzer. This feature is also known as Switched Port Analyzer (SPAN).

Important You can monitor or use SPAN on port channels only for ingress traffic.

Type of Session

When you create a traffic monitoring session, you can choose either an Ethernet or Fibre Channel destination port to receive the traffic. The type of destination port determines the type of session, which in turn determines the types of available traffic sources. For an Ethernet traffic monitoring session, the destination port must be an unconfigured physical port. For a Fibre Channel traffic monitoring session, the destination port must be a Fibre Channel uplink port.

Traffic Sources

An Ethernet traffic monitoring session can monitor any of the following traffic sources:

- Uplink Ethernet port
- Ethernet port channel
- VLAN
- Service profile vNIC
- Service profile vHBA
- FCoE port
- Port channels
- Unified uplink port

A Fibre Channel traffic monitoring session can monitor any of the following traffic sources:

- Uplink Fibre Channel port
- SAN port channel
- VSAN
- Service profile vHBA
- Fibre Channel storage port

Important Fibre Channel, Fibre Channel over Ethernet, vHBA, VSAN, and SAN are not supported in Cisco UCS Release 2.5

Guidelines and Recommendations for Traffic Monitoring

When configuring or activating traffic monitoring, consider the following guidelines:

- You can create and store up to 16 traffic monitoring sessions, but only two can be active at the same time.
- A traffic monitoring session is disabled by default when created. To begin monitoring traffic, you must activate the session.
- A traffic monitoring session must be unique on any fabric interconnect within the Cisco UCS pod. Therefore, you must create each monitoring session with a unique name and unique VLAN source.
- To monitor traffic from a server, add all vNICs from the service profile corresponding to the server.
- You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored using an Ethernet traffic monitoring session, with an Ethernet destination port, the destination traffic will be FCoE.

Important Fibre Channel and Fibre Channel over Ethernet are not supported in Cisco UCS Manager Release 2.5.

- Because a traffic monitoring destination is a single physical port, a traffic monitoring session can monitor only a single fabric. To monitor uninterrupted vNIC traffic across a fabric failover, you must create two sessions—one per fabric—and connect two analyzers. Add the vNIC as the traffic source for both sessions.
- All traffic sources must be located within the same switch as the destination port.
- A port configured as a destination port cannot also be configured as a source port.
- A member port of a port channel cannot be configured individually as a source. If the port channel is configured as a source, all member ports are source ports.
- A Fibre Channel port on a Cisco UCS 6248 fabric interconnect cannot be configured as a source port.
- If you change the port profile of a virtual machine, any associated vNICs being used as source ports are removed from monitoring, and you must reconfigure the monitoring session.
- If a traffic monitoring session was configured on a dynamic vNIC under a release earlier than Cisco UCS Manager Release 2.0, you must reconfigure the traffic monitoring session after upgrading.
- SPAN traffic is rate-limited to 1 Gbps on Cisco UCS 6200 Series fabric interconnects.

Note Traffic monitoring can impose a significant load on your system resources. To minimize the load, select sources that carry as little unwanted traffic as possible and disable traffic monitoring when it is not needed.

Creating an Ethernet Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

Step 3 Right-click ***Fabric_Interconnect_Name*** and choose **Create Traffic Monitoring Session**.

Step 4 In the **Create Traffic Monitoring Session** dialog box, complete the following fields:

Name	Description
Name field	The name of the traffic monitoring session. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Name	Description
Admin State field	Whether traffic will be monitored for the physical port selected in the **Destination** field. This can be one of the following: • **Enabled—**Cisco UCS begins monitoring the port activity as soon as some source components are added to the session. • **Disabled—**Cisco UCS does not monitor the port activity.
Destination drop-down list	Select the physical port whose communication traffic you want to monitor from the navigation tree.
Admin Speed field	The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain.

Step 5 Click **OK**.

What to Do Next

- Add traffic sources to the traffic monitoring session.
- Activate the traffic monitoring session.

Setting the Destination for an Existing Ethernet Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name*** > ***Monitor_Session_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Set Destination**.

Step 5 In the **Set Destination** dialog box, complete the following fields:

Example:

Name	Description
Destination field	The physical port that is being monitored.

Name	Description
Admin Speed field	The data transfer rate of the port channel to be monitored. The available data rates depend on the fabric interconnect installed in the Cisco UCS domain.

Step 6 Click **OK**.

Clearing the Destination for an Existing Ethernet Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name*** > ***Monitor_Session_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Clear Destination**.

Step 5 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Creating a Fibre Channel Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **LAN** tab, expand **SAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

Step 3 Right-click ***Fabric_Interconnect_Name*** and choose **Create Traffic Monitoring Session**.

Step 4 In the **Create Traffic Monitoring Session** dialog box, complete the following fields:

Name	Description
Name field	The name of the traffic monitoring session. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Name	Description
Admin State field	Whether traffic will be monitored for the physical port selected in the **Destination** field. This can be one of the following: • **Enabled—**Cisco UCS begins monitoring the port activity as soon as some source components are added to the session. • **Disabled—**Cisco UCS does not monitor the port activity.
Destination drop-down list	Select the physical port whose communication traffic you want to monitor from the navigation tree.
Admin Speed drop-down list	The data transfer rate of the port channel to be monitored. This can be one of the following: • **1 Gbps** • **2 Gbps** • **4 Gbps** • **8 Gbps** • **Auto—**Cisco UCS determines the data transfer rate.

Step 5 Click **OK**.

What to Do Next

- Add traffic sources to the traffic monitoring session.
- Activate the traffic monitoring session.

Setting the Destination for an Existing Fibre Channel Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name*** > ***Monitor_Session_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Set Destination**.

Step 5 In the **Set Destination** dialog box, complete the following fields:

Name	Description
Destination drop-down list	Select the physical port whose communication traffic you want to monitor from the navigation tree.
Admin Speed drop-down list	The data transfer rate of the port channel to be monitored. This can be one of the following: • **1 Gbps** • **2 Gbps** • **4 Gbps** • **8 Gbps** • **Auto—**Cisco UCS determines the data transfer rate.

Step 6 Click **OK**.

Clearing the Destination for an Existing Fibre Channel Traffic Monitoring Session

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name*** > ***Monitor_Session_Name***.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Actions** area, click **Clear Destination**.

Step 5 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding Traffic Sources to a Monitoring Session

You can choose multiple sources from more than one source type to be monitored by a traffic monitoring session. The available sources depend on the components configured in the Cisco UCS domain.

Note This procedure describes how to add sources for Ethernet traffic monitoring sessions. To add sources for a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Before You Begin

A traffic monitoring session must be created.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to configure.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Sources** area, expand the section for the type of traffic source that you want to add.

Step 6 To see the components that are available for monitoring, click the + button in the right-hand edge of the table to open the **Add Monitoring Session Source** dialog box.

Step 7 Select a source component and click **OK**.
You can repeat the preceding three steps as needed to add multiple sources from multiple source types.

Step 8 Click **Save Changes**.

What to Do Next

Activate the traffic monitoring session. If the session is already activated, traffic will be forwarded to the monitoring destination when you add a source.

Activating a Traffic Monitoring Session

Note This procedure describes how to activate an Ethernet traffic monitoring session. To activate a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Before You Begin

A traffic monitoring session must be created.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to activate.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Properties** area, click the **enabled** radio button for **Admin State**.

Step 6 Click **Save Changes**.

If a traffic monitoring source is configured, traffic begins to flow to the traffic monitoring destination port.

Deleting a Traffic Monitoring Session

Note This procedure describes how to delete an Ethernet traffic monitoring session. To delete a Fibre Channel monitoring session, select the **SAN** tab instead of the **LAN** tab in Step 2.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

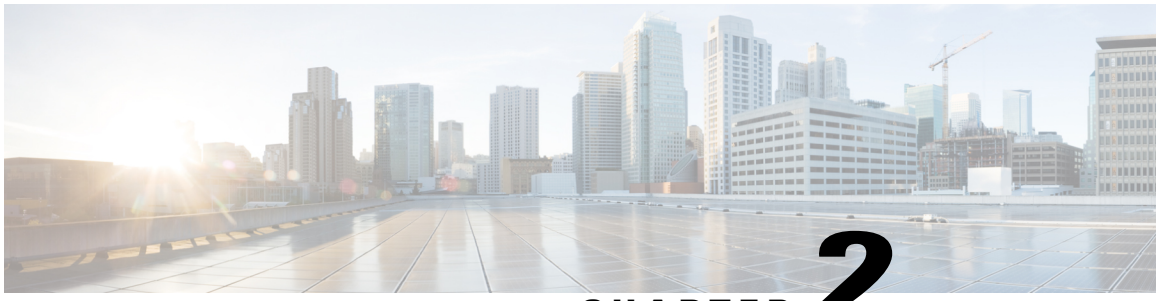
Step 2 On the **LAN** tab, expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

Step 3 Expand ***Fabric_Interconnect_Name*** and click the monitor session that you want to delete.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click the **Delete** icon.

Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.



CHAPTER 2

Monitoring Hardware

This chapter includes the following sections:

Monitoring a Fabric Interconnect

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Fabric Interconnects**.

Step 3 Click the node for the fabric interconnect that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the fabric interconnect:

Option	Description
General tab	Provides an overview of the status of the fabric interconnect, including a summary of any faults, a summary of the fabric interconnect properties, and a physical display of the fabric interconnect and its components.

Option	Description
Physical Ports tab	Displays the status of all ports on the fabric interconnect. This tab includes the following subtabs: • **Uplink Ports** tab • **Server Ports** tab • **Fibre Channel Ports** tab • **Unconfigured Ports** tab
Fans tab	Displays the status of all fan modules in the fabric interconnect.
PSUs tab	Displays the status of all power supply units in the fabric interconnect.
Physical Display tab	Provides a graphical view of the fabric interconnect and all ports and other components. If a component has a fault, the fault icon is displayed next to that component.
Faults tab	Provides details of faults generated by the fabric interconnect.
Events tab	Provides details of events generated by the fabric interconnect.
Statistics tab	Provides statistics about the fabric interconnect and its components. You can view these statistics in tabular or chart format.

Monitoring a Chassis

Tip To monitor an individual component in a chassis, expand the node for that component.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis**.

Step 3 Click the chassis that you want to monitor.

Step 4 Click one of the following tabs to view the status of the chassis:

Option	Description
General tab	Provides an overview of the status of the chassis, including a summary of any faults, a summary of the chassis properties, and a physical display of the chassis and its components.

Option	Description
Servers tab	Displays the status and selected properties of all servers in the chassis.
Service Profiles tab	Displays the status of the service profiles associated with servers in the chassis.
Fans tab	Displays the status of all fan modules in the chassis.
PSUs tab	Displays the status of all power supply units in the chassis.
Hybrid Display tab	Displays detailed information about the connections between the chassis and the fabric interconnects. The display has an icon for the following:
Slots tab	Displays the status of all slots in the chassis.
Installed Firmware tab	Displays the current firmware versions on the following components in the chassis. • Cartridges ◦ Servers ◦ BIOS ◦ CIMC Controller • Board Controller • Chassis Management Controller • Adapter • Storage You can also use this tab to update and activate the firmware on those components.
SEL Logs tab	Displays and provides access to the system event logs for the servers in the chassis.
Power Control Monitor tab	Provides details of the power group, chassis, and servers.
Connectivity Policy tab	Provides details of the chassis ID, fabric ID, and connectivity type for the fabric.
Storage	Provides details of the following storage components in a chassis: • Storage Controller • LUNs • Disks • Faults

Option	Description
Faults tab	Provides details of faults generated by the chassis.
Events tab	Provides details of events generated by the chassis.
Board Controller	Provides details of the Board Controller and the firmware version on it.
Chassis Management Controller	Provides details of the Chassis Management Controller and the firmware version on it.
FSM tab	Provides details about and the status of FSM tasks related to the chassis. You can use this information to diagnose errors with those tasks.
Statistics tab	Provides statistics about the chassis and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Provides temperature statistics for the components of the chassis. You can view these statistics in tabular or chart format.
Power tab	Provides power statistics for the components of the chassis. You can view these statistics in tabular or chart format.

Monitoring a Cartridge

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges**

Step 3 Click the cartridge that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the cartridge:

Option	Description
General tab	Provides an overview of the status of the cartridge, including a summary of any faults, a summary of the cartridge properties, and a physical display of the cartridge and its components.
Faults tab	Displays an overview of the faults generated by the cartridge. You can click any fault to view additional information.

Option	Description
Events tab	Displays an overview of the events generated by the cartridge. You can click any event to view additional information.

Monitoring a Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Click the server that you want to monitor.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the server:

Option	Description
General tab	Provides an overview of the status of the server, including a summary of any faults, a summary of the server properties, and a physical display of the server and its components.

Option	Description
Inventory tab	Provides details about the properties and status of the components of the server on the following subtabs: • **Motherboard—**Information about the motherboard and information about the server BIOS settings. You can also update and activate BIOS firmware from this subtab. • **CIMC—**Information about the CIMC and its firmware, and provides access to the SEL for the server. You can also assign a static or pooled management IP address, and update and activate the CIMC firmware from this subtab. Information about Active vMedia mounts of CDDs and HDDs is also displayed. • **CPUs—**Information about each CPU in the server. • **Memory—**Information about each memory slot in the server and the DIMM in that slot. • **Adapters—**Information about the adapter installed in the chassis. • **HBAs—**Properties of each HBA and the configuration of that HBA in the service profile associated with the server. • **NICs—**Properties of each NIC and the configuration of that NIC in the service profile associated with the server. You can expand each row to view information about the associated VIFs and vNICs. • **iSCSI vNICs—**Properties of each iSCSI vNIC and the configuration of that vNIC in the service profile associated with the server.
Virtual Machines tab	Displays details about any virtual machines hosted on the server.
Installed Firmware tab	Displays the firmware versions on the CIMC, adapters, and BIOS. You can also use this tab to update and activate the firmware on those components.
CIMC Sessions	Displays the CIMC sessions for the server.
SEL Logs tab	Displays the system event log for the server.
VIF Paths tab	Displays the VIF paths for the adapters on the server.
Faults tab	Displays an overview of the faults generated by the server. You can click any fault to view additional information.
Events tab	Displays an overview of the events generated by the server. You can click any event to view additional information.
FSM tab	Provides details about the current FSM task running on the server, including the status of that task. You can use this information to diagnose errors with those tasks.

Option	Description
Statistics tab	Displays statistics about the server and its components. You can view these statistics in tabular or chart format.
Temperatures tab	Displays temperature statistics for the components of the server. You can view these statistics in tabular or chart format.
Power tab	Displays power statistics for the components of the server. You can view these statistics in tabular or chart format.

Monitoring a Shared Adapter

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** ***Number*** > **Shared Adapter**

Step 3 Click **Shared Adapter**.

Step 4 In the **Work** pane, click one of the following tabs to view the status of the shared adapter:

Option	Description
General tab	Provides an overview of the status of the shared adapter, including a summary of any faults, a summary of the module properties, and a physical display of the shared adapter and its components.
Fabric Ports tab	Displays the status and selected properties of all fabric ports in the shared adapter.
Faults tab	Provides details of faults generated by the shared adapter.
Events tab	Provides details of events generated by the shared adapter.
Statistics tab	Provides statistics about the shared adapter and its components. You can view these statistics in tabular or chart format.

Monitoring Management Interfaces

Management Interfaces Monitoring Policy

This policy defines how the mgmt0 Ethernet interface on the fabric interconnect should be monitored. If Cisco UCS detects a management interface failure, a failure report is generated. If the configured number of failure reports is reached, the system assumes that the management interface is unavailable and generates a fault. By default, the management interfaces monitoring policy is enabled.

If the affected management interface belongs to a fabric interconnect which is the managing instance, Cisco UCS confirms that the subordinate fabric interconnect's status is up, that there are no current failure reports logged against it, and then modifies the managing instance for the endpoints.

If the affected fabric interconnect is currently the primary inside of a high availability setup, a failover of the management plane is triggered. The data plane is not affected by this failover.

You can set the following properties related to monitoring the management interface:

- Type of mechanism used to monitor the management interface.
- Interval at which the management interface's status is monitored.
- Maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.

Important In the event of a management interface failure on a fabric interconnect, the managing instance may not change if one of the following occurs:

- A path to the endpoint through the subordinate fabric interconnect does not exist.
- The management interface for the subordinate fabric interconnect has failed.
- The path to the endpoint through the subordinate fabric interconnect has failed.

Configuring the Management Interfaces Monitoring Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All** > **Communication Management**.

Step 3 Click **Management Interfaces**.

Step 4 In the **Work** pane, click the **Management Interfaces Monitoring Policy** tab.

Step 5 Complete the following fields:

Name	Description
Admin Status field	Whether the monitoring policy is enabled or disabled for the management interfaces.

Name	Description
Poll Interval field	The number of seconds Cisco UCS should wait between data recordings. Enter an integer between 90 and 300.
Max Fail Report Count field	The maximum number of monitoring attempts that can fail before Cisco UCS assumes that the management interface is unavailable and generates a fault message. Enter an integer between 2 and 5.
Monitoring Mechanism field	The type of monitoring you want Cisco UCS to use. This can be one of the following: • **Mii Status—**Cisco UCS monitors the availability of the Media Independent Interface (MII). If you select this option, Cisco UCS Manager GUI displays the **Media Independent Interface Monitoring** area. • **Ping Arp Targets—**Cisco UCS pings designated targets using the Address Resolution Protocol (ARP). If you select this option, Cisco UCS Manager GUI displays the **ARP Target Monitoring** area. • **Ping Gateway—**Cisco UCS pings the default gateway address specified for this Cisco UCS domain on the **Management Interfaces** tab. If you select this option, Cisco UCS Manager GUI displays the **Gateway Ping Monitoring** area.

Step 6 If you chose **Mii Status** for the monitoring mechanism, complete the following fields in the **Media Independent Interface Monitoring** area:

Name	Description
Retry Interval field	The number of seconds Cisco UCS should wait before requesting another response from the MII if a previous attempt fails. Enter an integer between 3 and 10.
Max Retry Count field	The number of times Cisco UCS polls the MII until the system assumes the interface is unavailable. Enter an integer between 1 and 3.

Step 7 If you chose **Ping Arp Targets** for the monitoring mechanism, complete the fields on the appropriate tab in the **ARP Target Monitoring** area.
If you are using IPv4 addresses, complete the following fields in the **IPv4** subtab:

Name	Description
Target IP 1 field	The first IPv4 address Cisco UCS pings.

Name	Description
Target IP 2 field	The second IPv4 address Cisco UCS pings.
Target IP 3 field	The third IPv4 address Cisco UCS pings.
Number of ARP Requests field	The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.

If you are using IPv6 addresses, complete the following fields in the **IPv6** subtab:

Name	Description
Target IP 1 field	The first IPv6 address Cisco UCS pings.
Target IP 2 field	The second IPv6 address Cisco UCS pings.
Target IP 3 field	The third IPv6 address Cisco UCS pings.
Number of ARP Requests field	The number of ARP requests Cisco UCS sends to the target IP addresses. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for responses from the ARP targets until the system assumes they are unavailable. Enter an integer between 5 and 15.

Type 0.0.0.0 for an IPv4 address to remove the ARP target or :: for an IPv6 address to remove the N-disc target.

Step 8 If you chose **Ping Gateway** for the monitoring mechanism, complete the following fields in the **Gateway Ping Monitoring** area:

Name	Description
Number of Ping Requests field	The number of times Cisco UCS should ping the gateway. Enter an integer between 1 and 5.
Max Deadline Timeout field	The number of seconds Cisco UCS waits for a response from the gateway until Cisco UCS assumes the address is unavailable. Enter an integer between 5 and 15.

Step 9 Click **Save Changes**.

Local Storage Monitoring

Local storage monitoring in Cisco UCS provides status information on local storage that is physically attached to a chassis. This includes RAID controllers, physical drives and drive groups, virtual drives, and RAID controller batteries (BBU).

Cisco UCS Manager communicates directly with the storage controllers using an out-of-band (OOB) interface, which enables real-time updates. Some of the information that is displayed includes:

- RAID controller status and rebuild rate.
- The drive state, power state, link speed, operability and firmware version of physical drives.
- The drive state, operability, strip size, access policies, drive cache, and health of virtual drives.
- The operability of a BBU, whether it is a supercap or battery.
- Information on RAID health and RAID state, card health, and operability.
- Information on operations that are running on the storage component, such as rebuild, initialization, and relearning.

Note After a CMC reboot or build upgrades, the status, start time, and end times of operations running on the storage component might not be displayed correctly.

- Detailed fault information for all local storage components.

Support for Local Storage Monitoring

Through Cisco UCS Manager, you can monitor local storage components for the Cisco UCSME-142-M4 server:

Prerequisites for Local Storage Monitoring

These prerequisites must be met for local storage monitoring or legacy disk drive monitoring to provide useful status information:

- The drive must be inserted in the chassis.
- The chassis must be powered on.
- The chassis must have completed discovery.
- The results of the BIOS POST complete must be TRUE.

Note This prerequisite is not applicable to the chassis

Viewing the Status of Local Storage Components

Procedure

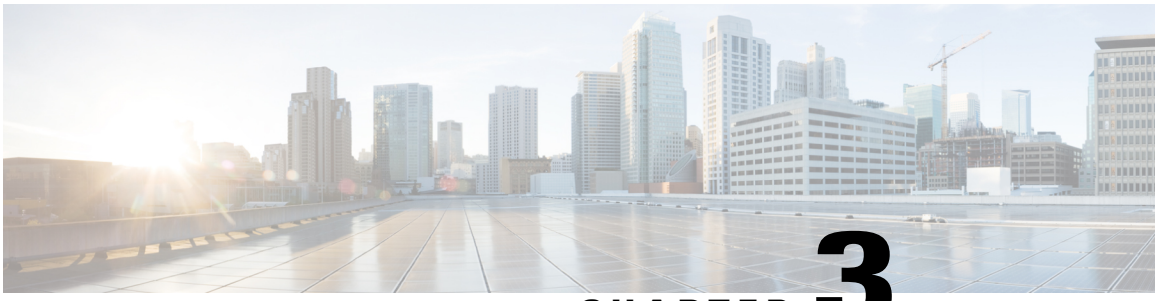
Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number*

Step 3 In the **Work** pane, click the **Storage** tab.

Step 4 Click one of the following subtabs to view the status of your storage:

Option	Description
Controller	Displays the details and status of the storage controller. Click the down arrows to expand the **Local Disk Configuration Policy**, and **Firmware** bars and view additional status information.
LUNs	Displays the status of all the virtual drives in the specified chassis.
Disks	Displays the status of all the disks in the specified chassis.
FSM	Displays the status of the FSM.
Faults	Provides details of faults generated by the chassis.



CHAPTER 3

Configuring Statistics-Related Policies

This chapter includes the following sections:

Configuring Statistics Collection Policies

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are to be collected (collection interval) and how frequently the statistics are to be reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval, which provides Cisco UCS Manager with sufficient data to calculate and report minimum, maximum, and average values.

For NIC statistics, Cisco UCS Manager displays the average, minimum, and maximum of the change since the last collection of statistics. If the values are 0, there has been no change since the last collection.

Statistics can be collected and reported for the following five functional areas of the Cisco UCS system:

- Adapter—statistics related to the adapters
- Chassis—statistics related to the chassis
- Host—this policy is a placeholder for future support
- Port—statistics related to the ports, including server ports, uplink Ethernet ports, and uplink Fibre Channel ports
- Server—statistics related to servers

Note Cisco UCS Manager has one default statistics collection policy for each of the five functional areas. You cannot create additional statistics collection policies and you cannot delete the existing default policies. You can only modify the default policies.

Modifying a Statistics Collection Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 In the **Admin** tab, expand **All** > **Stats Management** > **Stats**.

Step 3 Right-click the policy that you want to modify and select **Modify Collection Policy**.

Step 4 In the **Modify Collection Policy** dialog box, complete the following fields:

Name	Description
Name field	The name of the collection policy. This name is assigned by Cisco UCS and cannot be changed.
Collection Interval field	The length of time the fabric interconnect should wait between data recordings. This can be one of the following: • **30 Seconds** • **1 Minute** • **2 Minutes** • **5 Minutes**

Name	Description
Reporting Interval field	The length of time the fabric interconnect should wait before sending any data collected for the counter to Cisco UCS Manager. This can be one of the following: • **2 Minutes** • **15 Minutes** • **30 Minutes** • **60 Minutes** • **2 Hours** • **4 Hours** • **8 Hours** When this time has elapsed, the fabric interconnect groups all data collected since the last time it sent information to Cisco UCS Manager, and it extracts four pieces of information from that group and sends them to Cisco UCS Manager: • The most recent statistic collected • The average of this group of statistics • The maximum value within this group • The minimum value within this group For example, if the collection interval is set to 1 minute and the reporting interval is 15 minutes, the fabric interconnect collects 15 samples in that 15 minute reporting interval. Instead of sending 15 statistics to Cisco UCS Manager, it sends only the most recent recording along with the average, minimum, and maximum values for the entire group.
States Section	
Current Task field	The task that is executing on behalf of this component. For details, see the associated **FSM** tab. **Note** If there is no current task, this field is not displayed.

Step 5 Click **OK**.

Configuring Statistics Threshold Policies

Statistics Threshold Policy

A statistics threshold policy monitors statistics about certain aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds. For example, you can configure the policy to raise an alarm if the CPU temperature exceeds a certain value, or if a server is overutilized or underutilized.

These threshold policies do not control the hardware or device-level thresholds enforced by endpoints, such as the CIMC. Those thresholds are burned in to the hardware components at manufacture.

Cisco UCS enables you to configure statistics threshold policies for the following components:

- Servers and server components
- Uplink Ethernet ports
- Ethernet server ports, chassis, and fabric interconnects
- Fibre Channel port

Note You cannot create or delete a statistics threshold policy for Ethernet server ports, uplink Ethernet ports, or uplink Fibre Channel ports. You can only configure the existing default policy.

Creating a Server and Server Component Threshold Policy

Tip This procedure documents how to create a server and server component threshold policy on the **Server** tab. You can also create and configure these threshold policies within the appropriate organization in the **Policies** node on the **LAN** tab, **SAN** tab, and under the **Stats Management** node of the **Admin** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.
If the system does not include multitenancy, expand the **root** node.

Step 4 Right-click **Threshold Policies** and choose **Create Threshold Policy**.

Step 5 In the **Define Name and Description** page of the **Create Threshold Policy** wizard, do the following:

a) Complete the following fields:

Name	Description
Name field	The name of the policy. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Description field	A description of the policy. We recommend that you include information about where and when the policy should be used. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Owner field	This can be one of the following: • **Local—**This policy is available only to service profiles and service profile templates in this Cisco UCS domain. • **Pending Global—**Control of this policy is being transferred to Cisco UCS Central. Once the transfer is complete, this policy will be available to all Cisco UCS domains registered with Cisco UCS Central. • **Global—**This policy is managed by Cisco UCS Central. Any changes to this policy must be made through Cisco UCS Central.

b) Click **Next**.

Step 6 In the **Threshold Classes** page of the **Create Threshold Policy** wizard, do the following:

a) Click **Add**.

b) In the **Choose Statistics Class** dialog box, choose the statistics class for which you want to configure a custom threshold from the **Stat Class** drop-down list.

c) Click **Next**.

Step 7 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** fields, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**

- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** fields, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 7.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 8 In the **Threshold Classes** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 6 and 7.
- If you have configured all required threshold classes for the policy, click **Finish**.

Step 9 Click **OK**.

Adding a Threshold Class to an Existing Server and Server Component Threshold Policy

Tip This procedure documents how to add a threshold class to a server and server component threshold policy in the **Server** tab. You can also create and configure these threshold policies within the appropriate organization in the **Policies** node on the **LAN** tab, **SAN** tab, and under the **Stats Management** node of the **Admin** tab.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.
Step 2 On the **Servers** tab, expand **Servers** > **Policies** > *Organization_Name*.
Step 3 Expand the **Threshold Policies** node.
Step 4 Right-click the policy to which you want to add a threshold class and choose **Create Threshold Class**.
Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:

a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.
b) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.
b) From the **Property Type** field, choose the threshold property that you want to define for the class.
c) In the **Normal Value** field, enter the desired value for the property type.
d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Step 8 Click **OK**.

Deleting a Server and Server Component Threshold Policy

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Policies** > *Organization_Name*.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click the policy you want to delete and select **Delete**.

Step 5 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy

Tip You cannot create an uplink Ethernet port threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.

Step 2 On the **LAN** tab, expand **LAN** > **LAN Cloud**.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click **Thr-policy-default** and choose the **Create Threshold Class**.

Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:

a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.

b) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**

- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.
h) Click **Finish Stage**.
i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Adding a Threshold Class to the Ethernet Server Port, Chassis, and Fabric Interconnect Threshold Policy

Tip You cannot create an Ethernet server port, chassis, and fabric interconnect threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **LAN** tab.
Step 2 In the **LAN** tab, expand **LAN** > **Internal LAN**.
Step 3 Expand the **Threshold Policies** node.
Step 4 Right-click **Thr-policy-default** and choose the **Create Threshold Class**.
Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:
a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.

b) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

h) Click **Finish Stage**.

i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.

Adding a Threshold Class to the Fibre Channel Port Threshold Policy

You cannot create a Fibre Channel port threshold policy. You can only modify or delete the default policy.

Procedure

Step 1 In the **Navigation** pane, click the **SAN** tab.

Step 2 On the **SAN** tab, expand **SAN** > **SAN Cloud**.

Step 3 Expand the **Threshold Policies** node.

Step 4 Right-click **Thr-policy-default** and choose the **Create Threshold Class**.

Step 5 In the **Choose Statistics Class** page of the **Create Threshold Class** wizard, do the following:

a) From the **Stat Class** drop-down list, choose the statistics class for which you want to configure a custom threshold.

b) Click **Next**.

Step 6 In the **Threshold Definitions** page, do the following:

a) Click **Add**.
The **Create Threshold Definition** dialog box opens.

b) From the **Property Type** field, choose the threshold property that you want to define for the class.

c) In the **Normal Value** field, enter the desired value for the property type.

d) In the **Alarm Triggers (Above Normal Value)** field, check one or more of the following check boxes:

- **Critical**
- **Major**
- **Minor**
- **Warning**
- **Condition**
- **Info**

e) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

f) In the **Alarm Triggers (Below Normal Value)** field, check one or more of the following check boxes:

- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

g) In the **Up** and **Down** fields, enter the range of values that should trigger the alarm.

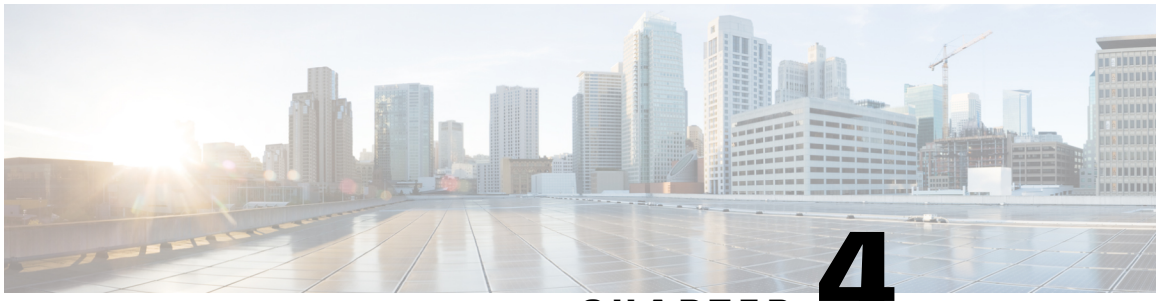
h) Click **Finish Stage**.

i) Do one of the following:

- To define another threshold property for the class, repeat Step 6.
- If you have defined all required properties for the class, click **Finish Stage**.

Step 7 In the **Create Threshold Class** page of the **Create Threshold Policy** wizard, do one the following:

- To configure another threshold class for the policy, repeat Steps 5 and 6.
- If you have configured all required threshold classes for the policy, click **Finish**.



CHAPTER 4

Configuring Call Home

This chapter includes the following sections:

Call Home

Call Home provides an email-based notification for critical system policies. A range of message formats are available for compatibility with pager services or XML-based automated parsing applications. You can use this feature to page a network support engineer, email a Network Operations Center, or use Cisco Smart Call Home services to generate a case with the Technical Assistance Center.

The Call Home feature can deliver alert messages containing information about diagnostics and environmental faults and events.

The Call Home feature can deliver alerts to multiple recipients, referred to as Call Home destination profiles. Each profile includes configurable message formats and content categories. A predefined destination profile is provided for sending alerts to the Cisco TAC, but you also can define your own destination profiles.

When you configure Call Home to send messages, Cisco UCS Manager executes the appropriate CLI **show** command and attaches the command output to the message.

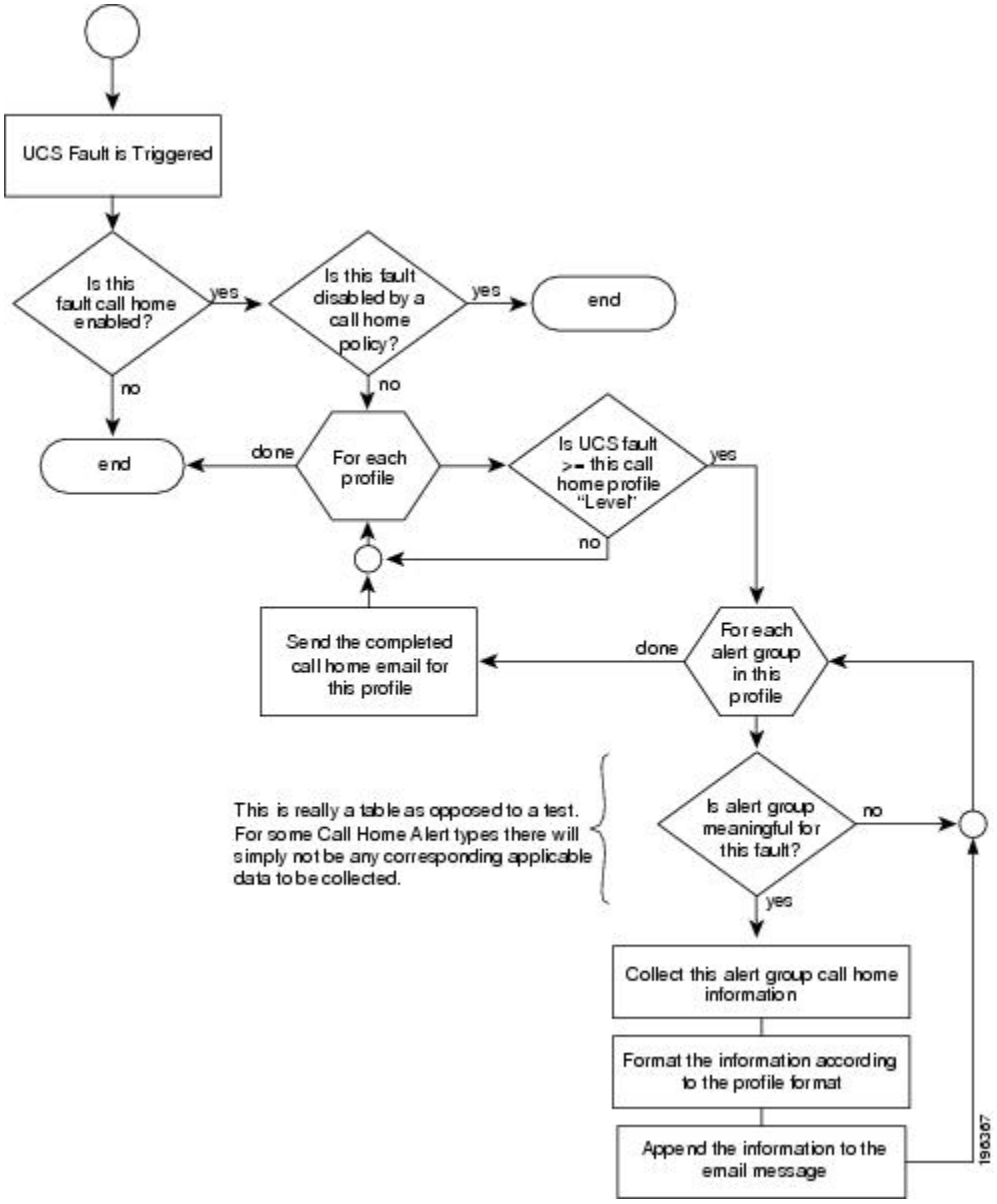
Cisco UCS delivers Call Home messages in the following formats:

- Short text format which provides a one or two line description of the fault that is suitable for pagers or printed reports.
- Full text format which provides fully formatted message with detailed information that is suitable for human reading.
- XML machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). The AML XSD is published on the Cisco.com website. The XML format enables communication with the Cisco Systems Technical Assistance Center.

For information about the faults that can trigger Call Home email alerts, see the *Cisco UCS Faults and Error Messages Reference*.

The following figure shows the flow of events after a Cisco UCS fault is triggered in a system with Call Home configured:

Figure 1: Flow of Events after a Fault is Triggered



Call Home Considerations and Guidelines

How you configure Call Home depends on how you intend to use the feature. The information you need to consider before you configure Call Home includes the following:

Destination Profile

You must configure at least one destination profile. The destination profile or profiles that you use depend upon whether the receiving entity is a pager, email, or automated service such as Cisco Smart Call Home.

If the destination profile uses email message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server when you configure Call Home.

Contact Information

The contact email, phone, and street address information should be configured so that the receiver can determine the origin of messages received from the Cisco UCS domain.

Cisco Smart Call Home sends the registration email to this email address after you send a system inventory to begin the registration process.

If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.

IP Connectivity to Email Server or HTTP Server

The fabric interconnect must have IP connectivity to an email server or the destination HTTP server. In a cluster configuration, both fabric interconnects must have IP connectivity. This connectivity ensures that the current, active fabric interconnect can send Call Home email messages. The source of these email messages is always the IP address of a fabric interconnect. The virtual IP address assigned Cisco UCS Manager in a cluster configuration is never the source of the email.

Smart Call Home

If Cisco Smart Call Home is used, the following are required:

- An active service contract must cover the device being configured
- The customer ID associated with the Smart Call Home configuration in Cisco UCS must be the CCO (Cisco.com) account name associated with a support contract that includes Smart Call Home

Cisco UCS Faults and Call Home Severity Levels

Because Call Home is present across several Cisco product lines, Call Home has developed its own standardized severity levels. The following table describes how the underlying Cisco UCS fault levels map to the Call Home severity levels. You need to understand this mapping when you configure the Level setting for Call Home profiles.

Table 1: Mapping of Faults and Call Home Severity Levels

Call Home Severity	Cisco UCS Fault	Call Home Meaning
(9) Catastrophic	N/A	Network-wide catastrophic failure.
(8) Disaster	N/A	Significant network impact.
(7) Fatal	N/A	System is unusable.

Call Home Severity	Cisco UCS Fault	Call Home Meaning
(6) Critical	Critical	Critical conditions, immediate attention needed.
(5) Major	Major	Major conditions.
(4) Minor	Minor	Minor conditions.
(3) Warning	Warning	Warning conditions.
(2) Notification	Info	Basic notifications and informational messages. Possibly independently insignificant.
(1) Normal	Clear	Normal event, signifying a return to normal state.
(0) debug	N/A	Debugging messages.

Cisco Smart Call Home

Cisco Smart Call Home is a web application which leverages the Call Home feature of Cisco UCS. Smart Call Home offers proactive diagnostics and real-time email alerts of critical system events, which results in higher network availability and increased operational efficiency. Smart Call Home is a secure connected service offered by Cisco Unified Computing Support Service and Cisco Unified Computing Mission Critical Support Service for Cisco UCS.

Note Using Smart Call Home requires the following:

- A CCO ID associated with a corresponding Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service contract for your company.
- Cisco Unified Computing Support Service or Cisco Unified Computing Mission Critical Support Service for the device to be registered.

You can configure and register Cisco UCS Manager to send Smart Call Home email alerts to either the Smart Call Home System or the secure Transport Gateway. Email alerts sent to the secure Transport Gateway are forwarded to the Smart Call Home System using HTTPS.

Note For security reasons, we recommend using the Transport Gateway option. The Transport Gateway can be downloaded from Cisco.

To configure Smart Call Home, you must do the following:

- Enable the Smart Call Home feature.

- Configure the contact information.
- Configure the email information.
- Configure the SMTP server information.
- Configure the default CiscoTAC-1 profile.
- Send a Smart Call Home inventory message to start the registration process.
- Ensure that the CCO ID you plan to use as the Call Home Customer ID for the Cisco UCS domain has the contract numbers from the registration added to its entitlements. You can update the ID in the account properties under Additional Access in the Profile Manager on CCO.

Anonymous Reporting

After you upgrade to the latest release of Cisco UCS Manager, by default, you are prompted with a dialog box to enable anonymous reporting.

To enable anonymous reporting, you need to enter details about the SMTP server and the data file that is stored on the fabric switch. This report is generated every seven days and is compared with the previous version of the same report. When Cisco UCS Manager identifies changes in the report, the report is sent as an e-mail.

Configuring Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Admin** area, complete the following fields to enable Call Home:

Name	Description
State field	This can be one of the following: • **Off—**Call Home is not used for this Cisco UCS domain. • **On—**Cisco UCS generates Call Home alerts based on the Call Home policies and profiles defined in the system. **Note** If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

Name	Description
Switch Priority drop-down list	This can be one of the following: • **Alerts** • **Critical** • **Debugging** • **Emergencies** • **Errors** • **Information** • **Notifications** • **Warnings**
Throttling field	Whether the system limits the number of duplicate messages received for the same event. This can be one of the following: • **On—**If the number of duplicate messages sent exceeds 30 messages within a 2-hour time frame, then the system discards further messages for that alert type. • **Off—**The system sends all duplicate messages, regardless of how many are encountered.

a) In the **State** field, click **on**.

Note If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

b) From the **Switch Priority** drop-down list, select one of the following levels:

- **Alerts**
- **Critical**
- **Debugging**
- **Emergencies**
- **Errors**
- **Information**
- **Notifications**
- **Warnings**

For a large Cisco UCS deployment with several pairs of fabric interconnects, this field enables you to attach significance to messages from one particular Cisco UCS domain, so that message recipients can gauge the priority of the message. This field may not be as useful for a small Cisco UCS deployment, such as a single Cisco UCS domain.

Step 5 In the **Contact Information** area, complete the following fields with the required contact information:

Name	Description
Contact field	The main Call Home contact person. Enter up to 255 ASCII characters.
Phone field	The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code. You can use hyphens but not parentheses.
Email field	The email address for the main contact. Cisco Smart Call Home sends the registration email to this email address. **Note** If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.
Address field	The mailing address for the main contact. Enter up to 255 ASCII characters.

Step 6 In the **Ids** area, complete the following fields with the identification information that Call Home should use:

Tip If you are not configuring Smart Call Home, this step is optional.

Name	Description
Customer Id field	The CCO ID that includes the contract numbers for the support contract in its entitlements. Enter up to 510 ASCII characters.
Contract Id field	The Call Home contract number for the customer. Enter up to 510 ASCII characters.
Site Id field	The unique Call Home identification number for the customer site. Enter up to 510 ASCII characters.

Step 7 In the **Email Addresses** area, complete the following fields with email information for Call Home alert messages:

Name	Description
From field	The email address that should appear in the From field on Call Home alert messages sent by the system.

Name	Description
Reply To field	The return email address that should appear in the From field on Call Home alert messages sent by the system.

Step 8 In the **SMTP Server** area, complete the following fields with information about the SMTP server where Call Home should send email messages:

Name	Description
Host (IP Address or Hostname) field	The IPv4 or IPv6 address, or the hostname of the SMTP server. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Port field	The port number the system should use to talk to the SMTP server. Enter an integer between 1 and 65535. The default is 25.

Step 9 Click **Save Changes**.

Disabling Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Admin** area, click **off** in the **State** field.

Note If this field is set to **off**, Cisco UCS Manager hides the rest of the fields on this tab.

Step 5 Click **Save Changes**.

Enabling Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Admin** area, click **on** in the **State** field.

Note If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

Step 5 Click **Save Changes**.

What to Do Next

Ensure that Call Home is fully configured.

Configuring System Inventory Messages

Configuring System Inventory Messages

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **System Inventory** tab.

Step 4 In the **Properties** area, complete the following fields:

Name	Description
Send Periodically field	If this field is set to **On**, Cisco UCS sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.
Send Interval field	The number of days that should pass between automatic system inventory data collection. Enter an integer between 1 and 30.
Hour of Day to Send field	The hour that the data should be sent using the 24-hour clock format.
Minute of Hour field	The number of minutes after the hour that the data should be sent.

Name	Description
Time Last Sent field	The date and time the information was last sent. **Note** This field is displayed after the first inventory has been sent.
Next Scheduled field	The date and time for the upcoming data collection. **Note** This field is displayed after the first inventory has been sent.

Step 5 Click **Save Changes**.

Sending a System Inventory Message

Use this procedure if you need to manually send a system inventory message outside of the scheduled messages.

Note The system inventory message is sent only to those recipients defined in CiscoTAC-1 profile.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **System Inventory** tab.

Step 4 In the **Actions** area, click **Send System Inventory Now**.
Cisco UCS Manager immediately sends a system inventory message to the recipient configured for Call Home.

Configuring Call Home Profiles

Call Home Profiles

Call Home profiles determine which alerts are sent to designated recipients. You can configure the profiles to send email alerts for events and faults at a desired severity level and for specific alert groups that represent categories of alerts. You can also use these profiles to specify the format of the alert for a specific set of recipients and alert groups.

Alert groups and Call Home profiles enable you to filter the alerts and ensure that a specific profile only receives certain categories of alerts. For example, a data center may have a hardware team that handles issues with fans and power supplies. This hardware team does not care about server POST failures or licensing

issues. To ensure that the hardware team only receives relevant alerts, create a Call Home profile for the hardware team and check only the "environmental" alert group.

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more alert groups when events occur at the level that you specify and provide the recipients with the appropriate amount of information about those alerts.

For example, you may want to configure two profiles for faults with a major severity:

- A profile that sends an alert to the Supervisor alert group in the short text format. Members of this group receive a one- or two-line description of the fault that they can use to track the issue.
- A profile that sends an alert to the CiscoTAC alert group in the XML format. Members of this group receive a detailed message in the machine readable format preferred by the Cisco Systems Technical Assistance Center.

Call Home Alert Groups

An alert group is a predefined subset of Call Home alerts. Alert groups allow you to select the set of Call Home alerts that you want to send to a predefined or custom Call Home profile. Cisco UCS sends Call Home alerts to e-mail destinations in a destination profile only if that Call Home alert belongs to one of the alert groups associated with that destination profile and if the alert has a Call Home message severity at or above the message severity set in the destination profile

Each alert that Cisco UCS generates fits into a category represented by an alert group. The following table describes those alert groups:

Alert Group	Description
Cisco TAC	All critical alerts from the other alert groups destined for Smart Call Home.
Diagnostic	Events generated by diagnostics, such as the POST completion on a server.
Environmental	Events related to power, fan, and environment-sensing elements such as temperature alarms.

Creating a Call Home Profile

By default, you must configure the Cisco TAC-1 profile. However, you can also create additional profiles to send email alerts to one or more specified groups when events occur at the level that you specify.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **Profiles** tab.

Step 4 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create Call Home Profile** dialog box, complete the following information fields:

Name	Description
Name field	A user-defined name for this profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Level field	Cisco UCS faults that are greater than or equal to this level trigger the profile. This can be one of the following: • **Critical** • **Debug** • **Disaster** • **Fatal** • **Major** • **Minor** • **Normal** • **Notification** • **Warning**
Alert Groups field	The group or groups that are alerted based on this Call Home profile. This can be one or more of the following: • **Cisco Tac—**Cisco TAC recipients • **Diagnostic—**POST completion server failure notification recipients • **Environmental—**Recipients of notifications about problems with PSUs, fans, etc.

Step 6 In the **Email Configuration** area, complete the following fields to configure the email alerts:

Name	Description
Format field	This can be one of the following: • **Xml—**A machine readable format that uses Extensible Markup Language (XML) and Adaptive Messaging Language (AML) XML schema definition (XSD). This format enables communication with the Cisco Systems Technical Assistance Center. • **Full Txt—**A fully formatted message with detailed information that is suitable for human reading. • **Short Txt—**A one or two line description of the fault that is suitable for pagers or printed reports.
Max Message Size field	The maximum message size that is sent to the designated Call Home recipients. Enter an integer between 1 and 5000000. The default is 5000000. For full text and XML messages, the maximum recommended size is 5000000. For short text messages, the maximum recommended size is 100000. For the Cisco TAC alert group, the maximum message size must be 5000000.

Step 7 In the **Recipients** area, do the following to add one or more email recipients for the email alerts:

a) On the icon bar to the right of the table, click +.

b) In the **Add Email Recipients** dialog box, enter the email address to which Call Home alerts should be sent in the **Email** field.
After you save this email address, it can be deleted but it cannot be changed.

c) Click **OK**.

Step 8 Click **OK**.

Deleting a Call Home Profile

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **Profiles** tab.

Step 4 Right-click the profile you want to delete and choose **Delete**.

Step 5 Click **Save Changes**.

Configuring Call Home Policies

Call Home Policies

Call Home policies determine whether or not Call Home alerts are sent for a specific type of fault or system event. By default, Call Home is enabled to send alerts for certain types of faults and system events. However, you can configure Cisco UCS not to process certain types.

To disable alerts for a type of fault or events, you must create a Call Home policy for that type, and you must first create a policy for that type and then disable the policy.

Configuring a Call Home Policy

Tip By default, all Call Home policies are enabled to ensure that email alerts are sent for all critical system events.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 On the icon bar to the right of the table, click +.
If the + icon is disabled, click an entry in the table to enable it.

Step 5 In the **Create Call Home Policy** dialog box, complete the following fields:

Name	Description
State field	If this field is **Enabled**, the system uses this policy when an error matching the associated cause is encountered. Otherwise, the system ignores this policy even if a matching error occurs. By default, all policies are enabled.
Cause field	The event that triggers the alert. Each policy defines whether an alert is sent for one type of event.

Step 6 Click **OK**.

Step 7 Repeat Steps 4 and 5 if you want to configure a Call Home policy for a different type of fault or event.

Disabling a Call Home Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the policy that you want to disable and choose **Show Navigator**.
Step 5 In the **State** field, click **Disabled**.
Step 6 Click **OK**.

Enabling a Call Home Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Click the policy that you want to enable and choose **Show Navigator**.
Step 5 In the **State** field, click **Enabled**.
Step 6 Click **OK**.

Deleting a Call Home Policy

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.
Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.
Step 3 In the **Work** pane, click the **Policies** tab.
Step 4 Right-click the policy that you want to disable and choose **Delete**.
Step 5 Click **Save Changes**.

Enabling Anonymous Reporting

Note Anonymous reporting can be enabled even when Call Home is disabled.

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call home**.

Step 3 In the **Work** pane, click the **Anonymous Reporting** tab.

Step 4 In the **Actions** area, click **Anonymous Reporting Data** to view the sample or existing report.

Step 5 In the **Properties** pane, click one of the following radio buttons in the **Anonymous Reporting** field:

- **On—**Enables the server to send anonymous reports.
- **Off—**Disables the server to send anonymous reports.

Step 6 In the **SMTP Server** area, complete the following fields with the information about the SMTP server where anonymous reporting should send email messages:

- **Host (IP Address or Hostname)—**The IPv4 or IPv6 address, or the hostname of the SMTP server.
- **Port—**The port number that the system should use to talk to the SMTP server.
  Enter an integer between 1 and 65535. The default is 25.

Step 7 Click **Save Changes**.

Example: Configuring Call Home for Smart Call Home

Configuring Smart Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **General** tab.

Step 4 In the **Admin** area, do the following to enable Call Home:

a) In the **State** field, click **on**.

Note If this field is set to **On**, Cisco UCS Manager GUI displays the rest of the fields on this tab.

b) From the **Switch Priority** drop-down list, select one of the following urgency levels:

- **Alerts**
- **Critical**
- **Debugging**
- **Emergencies**
- **Errors**
- **Information**
- **Notifications**
- **Warnings**

Step 5 In the **Contact Information** area, complete the following fields with the required contact information:

Name	Description
Contact field	The main Call Home contact person. Enter up to 255 ASCII characters.
Phone field	The telephone number for the main contact. Enter the number in international format, starting with a + (plus sign) and a country code. You can use hyphens but not parentheses.
Email field	The email address for the main contact. Cisco Smart Call Home sends the registration email to this email address. **Note** If an email address includes special characters, such as # (hash), spaces, or & (ampersand), the email server may not be able to deliver email messages to that address. Cisco recommends that you use email addresses which comply with RFC2821 and RFC2822 and include only 7bit ASCII characters.
Address field	The mailing address for the main contact. Enter up to 255 ASCII characters.

Step 6 In the **Ids** area, complete the following fields with the Smart Call Home identification information:

Name	Description
Customer Id field	The CCO ID that includes the contract numbers for the support contract in its entitlements. Enter up to 510 ASCII characters.
Contract Id field	The Call Home contract number for the customer. Enter up to 510 ASCII characters.

Name	Description
Site Id field	The unique Call Home identification number for the customer site. Enter up to 510 ASCII characters.

Step 7 In the **Email Addresses** area, complete the following fields with the email information for Smart Call Home alert messages:

Name	Description
From field	The email address that should appear in the From field on Call Home alert messages sent by the system.
Reply To field	The return email address that should appear in the From field on Call Home alert messages sent by the system.

Step 8 In the **SMTP Server** area, complete the following fields with information about the SMTP server that Call Home should use to send email messages:

Name	Description
Host (IP Address or Hostname) field	The IPv4 or IPv6 address, or the hostname of the SMTP server. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Port field	The port number the system should use to talk to the SMTP server. Enter an integer between 1 and 65535. The default is 25.

Step 9 Click **Save Changes**.

Configuring the Default Cisco TAC-1 Profile

The following are the default settings for the CiscoTAC-1 profile:

- Level is normal
- Only the CiscoTAC alert group is selected
- Format is xml
- Maximum message size is 5000000

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **Profiles** tab.

Step 4 Right-click the Cisco TAC-1 profile and choose **Recipient**.

Step 5 In the **Add Email Recipients** dialog box, do the following:

a) In the **Email** field, enter the email address to which Call Home alerts should be sent. For example, enter callhome@cisco.com.

After you save this email address, it can be deleted but it cannot be changed.

b) Click **OK**.

Configuring System Inventory Messages for Smart Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **System Inventory** tab.

Step 4 In the **Properties** area, complete the following fields to specify how system inventory messages will be sent to Smart Call Home:

Name	Description
Send Periodically field	If this field is set to **On**, Cisco UCS sends the system inventory to the Call Home database. When the information is sent depends on the other fields in this area.
Send Interval field	The number of days that should pass between automatic system inventory data collection. Enter an integer between 1 and 30.
Hour of Day to Send field	The hour that the data should be sent using the 24-hour clock format.
Minute of Hour field	The number of minutes after the hour that the data should be sent.
Time Last Sent field	The date and time the information was last sent. **Note** This field is displayed after the first inventory has been sent.

Name	Description
Next Scheduled field	The date and time for the upcoming data collection. **Note** This field is displayed after the first inventory has been sent.

Step 5 Click **Save Changes**.

Registering Smart Call Home

Procedure

Step 1 In the **Navigation** pane, click the **Admin** tab.

Step 2 On the **Admin** tab, expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **System Inventory** tab.

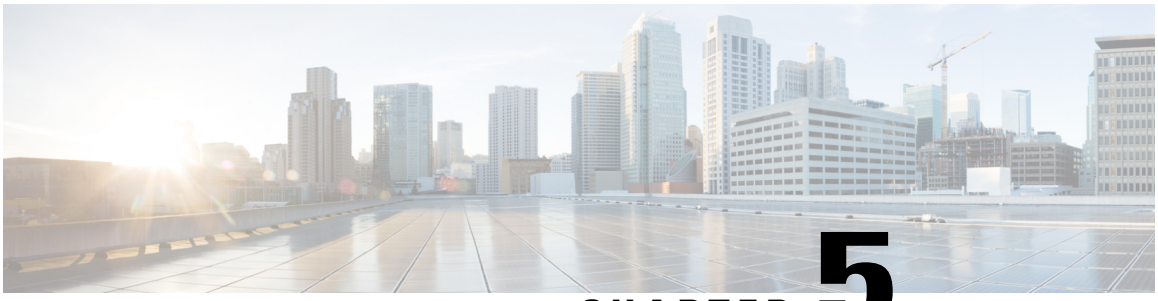
Step 4 In the **Actions** area, click **Send System Inventory Now** to start the registration process.
When Cisco receives the system inventory, a Smart Call Home registration email is sent to the email address that you configured in the **Contact Information** area on the **General** tab.

Step 5 When you receive the registration email from Cisco, do the following to complete registration for Smart Call Home:

a) Click the link in the email.
The link opens the Cisco Smart Call Home portal in your web browser.

b) Log into the Cisco Smart Call Home portal.

c) Follow the steps provided by Cisco Smart Call Home.
After you agree to the terms and conditions, the Cisco Smart Call Home registration for the Cisco UCS domain is complete.



CHAPTER 5

Managing the System Event Log

This chapter includes the following sections:

System Event Log

The system event log (SEL) resides on the CIMC in NVRAM. It records most server-related events, such as over and under voltage, temperature events, fan events, and events from BIOS. The SEL is mainly used for troubleshooting purposes.

The SEL file is approximately 40KB in size, and no further events can be recorded when it is full. It must be cleared before additional events can be recorded.

You can use the SEL policy to backup the SEL to a remote server, and optionally clear the SEL after a backup operation occurs. Backup operations can be triggered based on specific actions, or they can occur at regular intervals. You can also manually backup or clear the SEL.

The backup file is automatically generated. The filename format is sel-*SystemName-ChassisID-ServerID-ServerSerialNumber-Timestamp*; for example, sel-UCS-A-ch01-serv01-QCI12522939-20091121160736.

Viewing the System Event Log for an Individual Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Click the server for which you want to view the system event log.

Step 4 In the **Work** pane, click the **SEL Logs** tab.
Cisco UCS Manager retrieves the system event log for the server and displays the list of events.

Viewing the System Event Log for the Servers in a Chassis

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > *Chassis_Name* .

Step 3 In the **Work** pane, click the **SEL Logs** tab.
Cisco UCS Manager retrieves the system event log for the server and displays the list of events.

Step 4 In the Server table, click the server for which you want to view the system event log.
Cisco UCS Manager retrieves the system event log for the server and displays the list of events.

Configuring the SEL Policy

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, click the **Equipment** node.

Step 3 In the **Work** pane, click the **Policies** tab.

Step 4 Click the **SEL Policy** subtab.

Step 5 (Optional) In the **General** area, type a description of the policy in the **Description** field.
The other fields in this area are read-only.

Step 6 In the **Backup Configuration** area, complete the following fields:

Name	Description
Protocol field	The protocol to use when communicating with the remote server. This can be one of the following: • **FTP** • **TFTP** • **SCP** • **SFTP**
Hostname field	The hostname or IP address of the server on which the backup configuration resides. If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central. **Note** The name of the backup file is generated by Cisco UCS. The name is in the following format: `sel-system-name-chchassis-id-servblade-id-blade-serial-timestamp`
Remote Path field	The absolute path to the file on the remote server, if required. If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.
Backup Interval drop-down list	The time to wait between automatic backups. This can be one of the following: • **Never—**Do not perform any automatic SEL data backups. • **1 Hour** • **2 Hours** • **4 Hours** • **8 Hours** • **24 Hours** • **1 Week** • **1 Month** **Note** If you want the system to create automatic backups, make sure you check the **Timer** check box in the **Action** option box.

Name	Description
Format field	The format to use for the backup file. This can be one of the following: • **Ascii** • **Binary**
Clear on Backup check box	If checked, Cisco UCS clears all system event logs after the backup.
User field	The username the system should use to log in to the remote server. This field does not apply if the protocol is TFTP.
Password field	The password for the remote server username. This field does not apply if the protocol is TFTP.
Action option box	For each box that is checked, then the system creates a SEL backup when that event is encountered: • **Log Full—**The log reaches the maximum size allowed. • **On Change of Association—**The association between a server and its service profile changes. • **On Clear—**The user manually clears a system event log. • **Timer—**The time interval specified in the **Backup Interval** drop-down list is reached.
Reset Configuration button	Click this button to reset the background configuration information.

Step 7 Click **Save Changes**.

Managing the System Event Log for a Server

Copying One or More Entries in the System Event Log

This task assumes that you are viewing the system event log for a server from the **SEL Logs** tab for a server or a chassis.

Procedure

Step 1 After Cisco UCS Manager GUI displays the system event log in the **SEL Logs** tab, use your mouse to highlight the entry or entries that you want to copy from the system event log.

Step 2 Click **Copy** to copy the highlighted text to the clipboard.

Step 3 Paste the highlighted text into a text editor or other document.

Printing the System Event Log

This task assumes that you are viewing the system event log for a server from the **SEL Logs** tab for a server or a chassis.

Procedure

Step 1 After Cisco UCS Manager GUI displays the system event log in the **SEL Logs** tab, click **Print**.

Step 2 In the **Print** dialog box, do the following:

a) (Optional) Modify the default printer or any other fields or options.

b) Click **Print**.

Refreshing the System Event Log

This task assumes that you are viewing the system event log for a server from the **SEL Logs** tab for a server or a chassis.

Procedure

After Cisco UCS Manager GUI displays the system event log in the **SEL Logs** tab, click **Refresh**.
Cisco UCS Manager retrieves the system event log for the server and displays the updated list of events.

Manually Backing Up the System Event Log

This task assumes that you are viewing the system event log for a server from the **SEL Logs** tab for a server or a chassis.

Before You Begin

Configure the system event log policy. The manual backup operation uses the remote destination configured in the system event log policy.

Procedure

After Cisco UCS Manager GUI displays the system event log in the **SEL Logs** tab, click **Backup**. Cisco UCS Manager backs up the system event log to the location specified in the SEL policy.

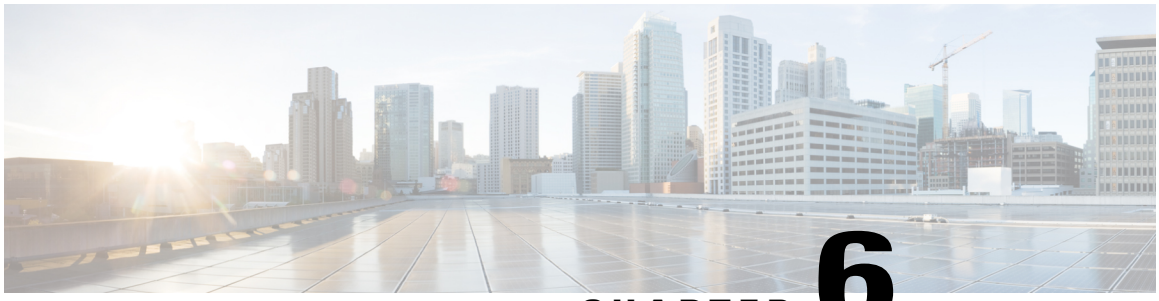
Manually Clearing the System Event Log

This task assumes that you are viewing the system event log for a server from the **SEL Logs** tab for a server or a chassis.

Procedure

After Cisco UCS Manager GUI displays the system event log in the **SEL Logs** tab, click **Clear**.

Note This action triggers an automatic backup if **Clear** is enabled in the SEL policy **Action** option box.



CHAPTER 6

Configuring Settings for Faults, Events, and Logs

This chapter includes the following sections:

Configuring Settings for the Fault Collection Policy

Global Fault Policy

The global fault policy controls the lifecycle of a fault in a Cisco UCS domain, 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 enters a flapping or soaking interval that is designed to prevent flapping. 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 global fault policy.
3. 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.
4. The cleared fault enters the retention interval. This interval ensures that the fault reaches the attention of an administrator even if the condition that caused the fault has been alleviated and the fault has not been deleted prematurely. The retention interval retains the cleared fault for the length of time specified in the global fault policy.
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 Global Fault 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, click the **Global Fault Policy** tab.

Step 5 In the **Global Fault Policy** tab, complete the following fields:

Name	Description
Flapping Interval field	Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, Cisco UCS Manager does not allow a fault to change its state until this amount of time has elapsed since the last state change. 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. Enter an integer between 5 and 3,600. The default is 10.
Initial Severity field	This can be one of the following: • **Info** • **Condition** • **Warning**
Action on Acknowledgment field	Acknowledged actions are always deleted when the log is cleared. This option cannot be changed.
Clear Action field	The action Cisco UCS Manager takes when a fault is cleared. This can be one of the following: • **Retain—**Cisco UCS Manager GUI displays the **Length of time to retain cleared faults** section. • **Delete—**Cisco UCS Manager immediately deletes all fault messages as soon as they are marked as cleared.
Clear Interval field	Whether Cisco UCS Manager automatically clears faults after a certain length of time. This can be one of the following: • **Never—**Cisco UCS Manager does not automatically clear any faults. • **other—**Cisco UCS Manager GUI displays the **dd:hh:mm:ss** field.

Name	Description
dd:hh:mm:ss field	The number of days, hours, minutes, and seconds that should pass before Cisco UCS Manager automatically marks that fault as cleared. What happens then depends on the setting in the **Clear Action** field.
Length of Time to Retain Cleared Faults Section	
Retention Interval field	If the **Clear Action** field is set to **Retain**, this is the length of time Cisco UCS Manager retains a fault once it is marked as cleared. This can be one of the following: • **Forever—**Cisco UCS Manager 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 Cisco UCS Manager deletes a cleared fault message.

Step 6 Click **Save Changes**.

Configuring Fault Suppression

Fault Suppression

Fault suppression allows you to suppress SNMP trap and Call Home notifications during a planned maintenance time. You can create a fault suppression task to prevent notifications from being sent whenever a transient fault is raised or cleared.

Faults remain suppressed until the time duration has expired, or the fault suppression tasks have been manually stopped by the user. After the fault suppression has ended, Cisco UCS Manager will send notifications for any outstanding suppressed faults that have not been cleared.

Fault suppression uses the following:

Fixed Time Intervals or Schedules

You can use the following to specify the maintenance window during which you want to suppress faults.

- Fixed time intervals allow you to create a start time and a duration when fault suppression is active. Fixed time intervals cannot be reused.
- Schedules are used for one time occurrences or recurring time periods and can be saved and reused.

Suppression Policies

These policies define which causes and types of faults you want to suppress. Only one policy can be assigned to a task. The following policies are defined by Cisco UCS Manager:

- **default-chassis-all-maint—**Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs.

  This policy applies only to chassis.

- **default-chassis-phys-maint—**Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis.

  This policy applies only to chassis.

- **default-fex-all-maint—**Suppresses faults for the FEX and all power supplies, fan modules, and IOMs in the FEX.

  This policy applies only to FEXes.

- **default-fex-phys-maint—**Suppresses faults for the FEX and all fan modules and power supplies in the FEX.

  This policy applies only to FEXes.

- **default-server-maint—**Suppresses faults for servers.

  This policy applies to chassis, organizations, and service profiles.

  Note When applied to a chassis, only servers are affected.

- **default-iom-maint—**Suppresses faults for IOMs in a chassis or FEX.

  This policy applies only to chassis, FEXes, and IOMs.

Important FEX and IO Modules are not supported by Cisco UCS M-Series Servers.

Suppression Tasks

You can use these tasks to connect the schedule or fixed time interval and the suppression policy to a component.

Note After you create a suppression task, you can edit the fixed time interval or schedule of the task in both the Cisco UCS Manager GUI and Cisco UCS Manager CLI. However, you can only change between using a fixed time interval and using a schedule in the Cisco UCS Manager CLI.

Viewing Suppressed Faults

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 **Faults**.

Step 4 In the **Work** pane, choose the **suppressed** icon in the **Show:** field.
To view only the suppressed faults, deselect the other icons in the **Show:** field.

Configuring Fault Suppression for a Chassis

Configuring Fault Suppression Tasks for a Chassis

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis**.

Step 3 Click the chassis for which you want to create a fault suppression task.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Start Fault Suppression**.

Tip To configure fault suppression tasks for multiple chassis, use the Ctrl key to select multiple chassis in the **Navigation** pane. Right-click one of the selected chassis and choose **Start Fault Suppression**.

Step 6 In the **Start Fault Suppression** dialog box, complete the following fields:

Name field	The name of the fault suppression task. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Select Fixed Time Interval/Schedule field	When the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Choose this option to specify the start time and duration for the fault suppression task. Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar. Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Choose this option to configure the start time and duration using a pre-defined schedule. Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.
Policy drop-down list	Choose the suppression policy from the drop-down list: • **default-chassis-all-maint—**Suppresses faults for the chassis and all components installed into the chassis, including all servers, power supplies, fan modules, and IOMs. • **default-chassis-phys-maint—**Suppresses faults for the chassis and all fan modules and power supplies installed into the chassis. • **default-server-maint—**Suppresses faults for servers. **Note** When applied to a chassis, only servers are affected. • **default-iom-maint—**Suppresses faults for IOMs in a chassis or FEX. **Important** FEX and IO Modules are not supported by Cisco UCS M-Series Servers.

Step 7 Click **OK**.

Deleting Fault Suppression Tasks for a Chassis

This procedure deletes all fault suppression tasks for a chassis. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for a Chassis, on page 71.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis**.

Step 3 Click the chassis for which you want to delete all fault suppression tasks.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Stop Fault Suppression**.

Tip To delete fault suppression tasks for multiple chassis, use the Ctrl key to select multiple chassis in the **Navigation** pane. Right-click one of the selected chassis and choose **Stop Fault Suppression**.

Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Viewing Fault Suppression Tasks for a Chassis

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis**.

Step 3 Click the chassis for which you want to view fault suppression task properties.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Suppression Task Properties**.

In the **Suppression Tasks** dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

Configuring Fault Suppression for a Shared Adapter

Configuring Fault Suppression Tasks for a Shared Adapter

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Shared Adapter**

Step 3 Click the shared adapter for which you want to create a fault suppression task.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Start Fault Suppression**.

Step 6 In the **Start Fault Suppression** dialog box, complete the following fields:

Name field	The name of the fault suppression task. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Select Fixed Time Interval/Schedule field	When the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Choose this option to specify the start time and duration for the fault suppression task. Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar. Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Choose this option to configure the start time and duration using a pre-defined schedule. Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.
Policy drop-down list	The following suppression policy is selected by default: • **default-iom-maint—**Suppresses faults for IOMs in a chassis or FEX.

Step 7 Click **OK**.

Deleting Fault Suppression Tasks for a Shared Adapter

This procedure deletes all fault suppression tasks for a shared adapter. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for an IOM.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.
Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Shared Adapter**
Step 3 Click the shared adapter for which you want to delete all fault suppression tasks.
Step 4 In the **Work** pane, click the **General** tab.
Step 5 In the **Actions** area, click **Stop Fault Suppression**.
Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Viewing Fault Suppression Tasks for a Shared Adapter

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Shared Adapter**

Step 3 Click the shared adapter for which you want to view fault suppression task properties.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Suppression Task Properties**.
In the **Suppression Tasks** dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

Configuring Fault Suppression for a Server

Configuring Fault Suppression Tasks for a Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Click the server for which you want to create a fault suppression task.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Start Fault Suppression**.

Tip To configure fault suppression tasks for multiple servers, use the Ctrl key to select multiple servers in the **Navigation** pane. Right-click one of the selected servers and choose **Start Fault Suppression**.

Step 6 In the **Start Fault Suppression** dialog box, complete the following fields:

Name field	The name of the fault suppression task. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Select Fixed Time Interval/Schedule field	When the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Choose this option to specify the start time and duration for the fault suppression task. Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar. Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Choose this option to configure the start time and duration using a pre-defined schedule. Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.
Policy drop-down list	The following suppression policy is selected by default: • **default-server-maint—**Suppresses faults for servers.

Step 7 Click **OK**.

Deleting Fault Suppression Tasks for a Server

This procedure deletes all fault suppression tasks for a server. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box.

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Click the server for which you want to delete all fault suppression tasks.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Stop Fault Suppression**.

Tip To delete fault suppression tasks for multiple servers, use the Ctrl key to select multiple servers in the **Navigation** pane. Right-click one of the selected servers and choose **Stop Fault Suppression**.

Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Viewing Fault Suppression Tasks for a Server

Procedure

Step 1 In the **Navigation** pane, click the **Equipment** tab.

Step 2 On the **Equipment** tab, expand **Equipment** > **Chassis** > **Chassis** *Number* > **Cartridges** > **Cartridge** *Number* > **Servers**

Step 3 Click the server for which you want to view fault suppression task properties.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Suppression Task Properties**.
In the **Suppression Tasks** dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

Configuring Fault Suppression for a Service Profile

Configuring Fault Suppression Tasks for a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles**.

Step 3 Click the service profile for which you want to create a fault suppression task.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Start Fault Suppression**.

Tip To configure fault suppression tasks for multiple service profiles, use the Ctrl key to select multiple service profiles in the **Navigation** pane. Right-click one of the selected service profiles and choose **Start Fault Suppression**.

Step 6 In the **Start Fault Suppression** dialog box, complete the following fields:

Name field	The name of the fault suppression task. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Select Fixed Time Interval/Schedule field	When the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Choose this option to specify the start time and duration for the fault suppression task. Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar. Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Choose this option to configure the start time and duration using a pre-defined schedule. Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.
Policy drop-down list	The following suppression policy is selected by default: • **default-server-maint—**Suppresses faults for servers.

Step 7 Click **OK**.

Deleting Fault Suppression Tasks for a Service Profile

This procedure deletes all fault suppression tasks for a service profile. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for a Service Profile, on page 77.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles**.

Step 3 Click the service profile for which you want to delete all fault suppression tasks.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Stop Fault Suppression**.

Tip To delete fault suppression tasks for multiple service profiles, use the Ctrl key to select multiple service profiles in the **Navigation** pane. Right-click one of the selected service profiles and choose **Stop Fault Suppression**.

Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Viewing Fault Suppression Tasks for a Service Profile

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Service Profiles**.

Step 3 Click the service profile for which you want to view fault suppression task properties.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Suppression Task Properties**.
In the **Suppression Tasks** dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

Configuring Fault Suppression for an Organization

Configuring Fault Suppression Tasks for an Organization

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Policies** > ***Organization_Name***.

Step 3 Click the organization for which you want to create a fault suppression task.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Start Fault Suppression**.

Step 6 In the **Start Fault Suppression** dialog box, complete the following fields:

Name field	The name of the fault suppression task. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.

Select Fixed Time Interval/Schedule field	When the fault suppression task will run. This can be one of the following: • **Fixed Time Interval—**Choose this option to specify the start time and duration for the fault suppression task. Specify the day and time the fault suppression task should start in the **Start Time** field. Click the down arrow at the end of this field to select the start time from a pop-up calendar. Specify the length of time this task should run in the **Task Duration** field. To specify that this task should run until it is manually stopped, enter 00:00:00:00 in this field. • **Schedule—**Choose this option to configure the start time and duration using a pre-defined schedule. Choose the schedule from the **Schedule** drop-down list. To create a new schedule, click **Create Schedule**.
Policy drop-down list	The following suppression policy is selected by default: • **default-server-maint—**Suppresses faults for servers.

Step 7 Click **OK**.

Deleting Fault Suppression Tasks for an Organization

This procedure deletes all fault suppression tasks for an organization. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for an Organization, on page 79.

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Policies** > ***Organization_Name***.

Step 3 Click the organization for which you want to delete all fault suppression tasks.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Stop Fault Suppression**.

Step 6 If the Cisco UCS Manager GUI displays a confirmation dialog box, click **Yes**.

Viewing Fault Suppression Tasks for an Organization

Procedure

Step 1 In the **Navigation** pane, click the **Servers** tab.

Step 2 On the **Servers** tab, expand **Servers** > **Policies** > *Organization_Name*.

Step 3 Click the organization for which you want to view fault suppression task properties.

Step 4 In the **Work** pane, click the **General** tab.

Step 5 In the **Actions** area, click **Suppression Task Properties**.
In the **Suppression Tasks** dialog box, you can add new fault suppression tasks, delete existing fault suppression tasks, or modify existing fault suppression tasks.

Configuring Settings for the Core File Exporter

Core File Exporter

Cisco UCS 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, click the **TFTP Core Exporter** tab.

Step 5 On the **TFTP Core Exporter** tab, complete the following fields:

Name	Description
Admin State field	This can be one of the following: • **Enabled—**If an error causes the server to perform a core dump, Cisco UCS 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.

Name	Description
Description field	A user-defined description of the core file. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Port field	The port number to use when exporting the core dump file via TFTP.
Hostname field	The hostname or IPv4 or IPv6 address to connect with via TFTP. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Path field	The path to use when storing the core dump file on the remote system.

Step 6 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	Whether Cisco UCS displays Syslog messages on the console. This can be one of the following: • **Enabled—**Syslog messages are displayed on the console as well as added to the log. • **Disabled—**Syslog messages are added to the log but not displayed on the console.
Level field	If this option is **enabled**, select the lowest message level that you want displayed. Cisco UCS displays that level and above on the console. This can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	
Admin State field	Whether Cisco UCS displays Syslog messages on the monitor. This can be one of the following: • **Enabled—**Syslog messages are displayed on the monitor as well as added to the log. • **Disabled—**Syslog messages are added to the log but not displayed on the monitor. If **Admin State** is enabled, Cisco UCS Manager GUI displays the rest of the fields in this section.

Name	Description
Level drop-down list	If this option is **enabled**, select the lowest message level that you want displayed. The system displays that level and above on the monitor. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
File Section	
Admin State field	Whether Cisco UCS stores messages in a system log file on the fabric interconnect. This can be one of the following: • **Enabled—**Messages are saved in the log file. • **Disabled—**Messages are not saved. 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. Cisco UCS stores that level and above in a file on the fabric interconnect. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**

Name	Description
Name field	The name of the file in which the messages are logged. This name can be up to 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period). The default is messages.
Size field	The maximum size, in bytes, the file can be before Cisco UCS Manager begins to write over the oldest messages with the newest ones. Enter an integer between 4096 and 4194304.

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	This can be one of the following: • **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 the remote file. This can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
Hostname field	The hostname or IP address on which the remote log file resides. **Note** If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.

Name	Description
Facility drop-down list	This can be one of the following: • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

Step 7 In the **Local Sources** area, complete the following fields:

Name	Description
Faults Admin State field	If this field is **Enabled**, Cisco UCS logs all system faults.
Audits Admin State field	If this field is **Enabled**, Cisco UCS logs all audit log events.
Events Admin State field	If this field is **Enabled**, Cisco UCS logs all system events.

Step 8 Click **Save Changes**.

Viewing the Audit Logs

You can view, export, print or refresh the audit logs displayed on this **Audit Logs** page.

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 **Audit Logs**.
Step 4 The **Work** pane displays the audit logs.