Cisco UCS Manager System Monitoring Guide, Release 6.0

First Published: 2025-09-02

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

© 2025 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface xi

Audience xi

Conventions xi

Related Cisco UCS Documentation xiii

Documentation Feedback xiii

CHAPTER 1

New and Changed Information 1

New and Changed Information 1

CHAPTER 2

System Monitoring Overview 3

System Monitoring Overview 3

The Cisco UCS Manager Core and Fault Generation 4

Cisco UCS Manager User Documentation 6

CHAPTER 3

Syslog 9

Syslog 9

Configuring the Syslog Using Cisco UCS Manager GUI 10

CHAPTER 4

System Event Log 15

System Event Log 15

Viewing the System Event Log for an Individual Server 16

Viewing the System Event Log for the Servers in a Chassis 16

Configuring the SEL Policy 16

Copying One or More Entries in the System Event Log 19

Printing the System Event Log 19

Refreshing the System Event Log 19

Manually Backing Up the System Event Log 20
Manually Clearing the System Event Log 20

CHAPTER 5 Core File Exporter 21
Core File Exporter 21
Configuring the Core File Exporter 21
Disabling the Core File Exporter 22

CHAPTER 6 Audit Logs 25
Audit Logs 25
Viewing the Audit Logs 25

CHAPTER 7 Fabric Interconnect Audit Logs 27
Overview 27
Configuring the Fabric Interconnect Audit Logs 27
Viewing and Managing Fabric Interconnect Audit Log Configuration 28
Disabling the Fabric Interconnect Audit Logs 29

CHAPTER 8 Fault Collection and Suppression 31
Configuring Settings for the Fault Collection Policy 31
Global Fault Policy 31
Configuring the Global Fault Policy 32
Configuring Fault Suppression 33
Fault Suppression 33
Viewing Suppressed Faults 34
Configuring Fault Suppression for a Chassis 35
Configuring Fault Suppression Tasks for a Chassis 35
Viewing Fault Suppression Tasks for a Chassis 36
Deleting Fault Suppression Tasks for a Chassis 36
Configuring Fault Suppression for an I/O Module and IFM (IOM for Cisco UCS X-Series Servers) 37
Configuring Fault Suppression Tasks for an IOM and IFM (IOM for Cisco UCS X-Series Servers) 37
Viewing Fault Suppression Tasks for an IOM and IFM (IOM for Cisco UCS X-Series Servers) 38
Deleting Fault Suppression Tasks for an IOM and IFM (IOM for Cisco UCS X-Series Servers) 38

Configuring Fault Suppression for a FEX 39
Configuring Fault Suppression Tasks for a FEX 39
Viewing Fault Suppression Tasks for a FEX 40
Deleting Fault Suppression Tasks for a FEX 40
Configuring Fault Suppression for Servers 41
Configuring Fault Suppression Tasks for a Blade Server 41
Viewing Fault Suppression Tasks for a Blade Server 42
Deleting Fault Suppression Tasks for a Blade Server 42
Configuring Fault Suppression Tasks for a Rack Server 43
Viewing Fault Suppression Tasks for a Rack Server 44
Deleting Fault Suppression Tasks for a Rack Server 45
Configuring Fault Suppression for a Service Profile 45
Configuring Fault Suppression Tasks for a Service Profile 45
Deleting Fault Suppression Tasks for a Service Profile 46
Viewing Fault Suppression Tasks for a Service Profile 47
Configuring Fault Suppression for an Organization 47
Configuring Fault Suppression Tasks for an Organization 47
Deleting Fault Suppression Tasks for an Organization 48
Viewing Fault Suppression Tasks for an Organization 48

CHAPTER 9 **SNMP Configuration** 51
SNMP Overview 51
SNMP Functional Overview 51
SNMP Notifications 52
SNMP Security Levels and Privileges 52
Supported Combinations of SNMP Security Models and Levels 52
SNMPv3 Security Features 53
SNMP Support in Cisco UCS 53
Enabling SNMP and Configuring SNMP Properties 54
Creating an SNMP Trap 55
Deleting an SNMP Trap 56
Creating an SNMPv3 user 56
Deleting an SNMPv3 User 57

CHAPTER 10 **SPDM Security** 59

SPDM Security 59

Creating a SPDM Security Policy 60

Associating the Security Policy with a Server 61

Viewing the Fault Alert Settings 61

CHAPTER 11 **Statistics Collection Policy Configuration** 63

Configuring Statistics Collection Policies 63

Statistics Collection Policy 63

Modifying a Statistics Collection Policy 64

Viewing Statistics Collection Policy Details 66

Configuring Statistics Threshold Policies 66

Statistics Threshold Policy 66

Creating a Server and Server Component Threshold Policy 67

Deleting a Server and Server Component Threshold Policy 69

Adding a Threshold Class to an Existing Server and Server Component Threshold Policy 69

Adding a Threshold Class to the Uplink Ethernet Port Threshold Policy 70

Adding a Threshold Class to the Ethernet Server Port, Chassis, and Fabric Interconnect Threshold Policy 72

Adding a Threshold Class to the Fibre Channel Port Threshold Policy 73

CHAPTER 12 **Call Home and Smart Call Home Configuration** 75

Call Home and Smart Call Home Configuration 75

Call Home in UCS Overview 75

Call Home Considerations and Guidelines 77

Cisco UCS Faults and Call Home Severity Levels 78

Anonymous Reporting 78

Enabling Anonymous Reporting 79

Configuring Call Home 79

Configuring Call Home Profiles 85

Configuring Call Home Policies 89

Cisco Smart Call Home 90

Configuring Smart Call Home 92

Configuring the Default Cisco TAC-1 Profile 95
Configuring System Inventory Messages for Smart Call Home 96
Registering Smart Call Home 97

CHAPTER 13 **Hardware Monitoring** 99
Monitoring a Fabric Interconnect 99
Monitoring a Blade Server 100
Monitoring a Rack-Mount Server 102
Monitoring an IO Module 105
Monitoring PCIe Node 105
Monitoring Crypto Cards 106
Cisco Crypto Card Management for Blade Servers 106
Viewing Crypto Card Properties 107
Monitoring NVMe PCIe SSD Devices 107
NVMe PCIe SSD Storage Device Inventory 107
Viewing NVMe PCIe SSD Storage Inventory 108
Health Monitoring 111
Monitoring CIMC Memory Usage for Blade, and Rack-Mount Servers 111
Monitoring CMC Memory Usage for Input/Output Module and IFM (IOM for Cisco UCS X-Series Servers) 112
Monitoring FEX Statistics 112
Management Interfaces Monitoring Policy 113
Configuring the Management Interfaces Monitoring Policy 114
Local Storage Monitoring 116
Support for Local Storage Monitoring 116
Prerequisites for Local Storage Monitoring 117
Legacy Disk Drive Monitoring 118
Flash Life Wear Level Monitoring 118
Viewing the Status of Local Storage Components 118
RAID 0 Check Consistency Limitation 119
Graphics Card Monitoring 119
Graphics Card Server Support 119
GPU Mezzanine Graphics Module Management for Blade Servers 120
Viewing Graphics Card Properties 121

Managing Transportable Flash Module and Supercapacitor 122
TFM and Supercap Guidelines and Limitations 122
Viewing the RAID Controller Stats 123
Monitoring RAID Battery Status 123
Viewing a RAID Battery Fault 123
TPM Monitoring 124
Viewing TPM Properties 124

CHAPTER 14 **Traffic Monitoring** 125
Traffic Monitoring 125
Guidelines and Recommendations for Traffic Monitoring 127
Choosing Between Traffic Monitoring Sessions 128
Traffic Monitoring for SPAN 128
Creating an Ethernet Traffic Monitoring Session 128
Setting the Destination for an Existing Ethernet Traffic Monitoring Session 129
Clearing the Destination for an Existing Ethernet Traffic Monitoring Session 130
Creating a Fibre Channel Traffic Monitoring Session 130
Setting the Destination for an Existing Fibre Channel Traffic Monitoring Session 132
Clearing the Destination for an Existing Fibre Channel Traffic Monitoring Session 133
ERSPAN Truncation 133
Configuring ERSPAN Truncation 133
Viewing or Modifying an ERSPAN Truncation 134
Adding Traffic Sources to a Monitoring Session 134
Activating a Traffic Monitoring Session 135
Deleting a Traffic Monitoring Session 136

CHAPTER 15 **NetFlow Monitoring** 137
NetFlow Monitoring 137
NetFlow Limitations 138
Enabling NetFlow Monitoring 139
Creating a Flow Record Definition 139
Viewing Flow Record Definitions 140
Defining the Exporter Profile 141
Creating a Flow Collector 141

Creating a Flow Exporter 142
Creating a Flow Monitor 143
Creating a Flow Monitor Session 144
Associating a Flow Monitor Session to a vNIC 145

Preface

- Audience, on page xi
- Conventions, on page xi
- Related Cisco UCS Documentation, on page xiii
- Documentation Feedback, on page xiii

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`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

Text Type	Indication
{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.

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

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

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

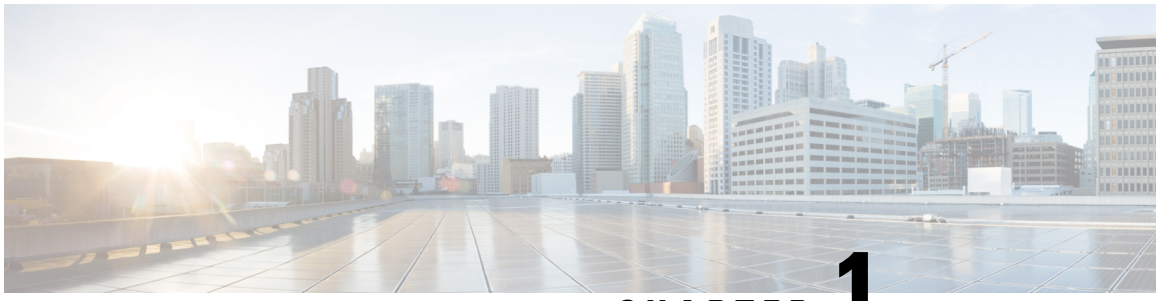
For a complete list of all B-Series documentation, see the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/UCS_roadmap.html

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

For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Documentation Feedback

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



CHAPTER 1

New and Changed Information

- New and Changed Information, on page 1

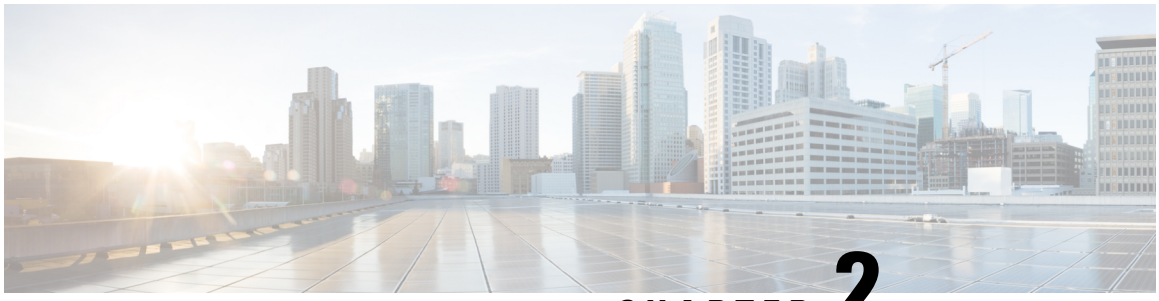
New and Changed Information

The following table provides an overview of the significant changes to this guide for this current release. The table does not provide an exhaustive list of all changes made to this guide or of all new features in this release.

Table 1: New Features and Changed Behavior in Cisco UCS Manager, Release 6.0(1b)

Feature	Description	Where Documented
Audit Log Support for UCS Fabric Interconnects	Cisco UCS Manager introduces support for the Fabric Interconnect Audit Logs feature, employing the Linux Audit Framework (auditd) to record user and system activity on Cisco UCS 6400, 6500, and 6600 Series Fabric Interconnects.	• Overview, on page 27 • Configuring the Fabric Interconnect Audit Logs, on page 27 • Viewing and Managing Fabric Interconnect Audit Log Configuration, on page 28 • Disabling the Fabric Interconnect Audit Logs, on page 29
Support for Cisco UCS 6600 Series Fabric Interconnect	Cisco UCS Manager supports Cisco UCS 6664 Fabric Interconnect	• Configuring the Syslog Using Cisco UCS Manager GUI, on page 10 • NetFlow Monitoring, on page 137 • NetFlow Limitations, on page 138 • Guidelines and Recommendations for Traffic Monitoring, on page 127

Feature	Description	Where Documented
Deprecated support for Cisco UCS 6300 series Fabric Interconnect.	Cisco UCS Manager support for Cisco UCS 6300 Series Fabric Interconnect is deprecated.	-



CHAPTER 2

System Monitoring Overview

- System Monitoring Overview, on page 3
- The Cisco UCS Manager Core and Fault Generation, on page 4
- Cisco UCS Manager User Documentation, on page 6

System Monitoring Overview

This guide describes how to configure and use system monitoring to manage a Cisco UCS Manager environment.

Cisco UCS Manager can detect system faults: critical, major, minor, and warnings. We recommend that:

- You monitor all faults of either critical or major severity status, as immediate action is not required for minor faults and warnings.
- You monitor faults that are not of type Finite State Machine (FSM), as FSM faults will transition over time and resolve.

This guide covers the following information:

- System Log
  - System logs including faults, failures, and alarm thresholds (Syslog)
  - The three types of Syslogs: Fault, Event, and Audit logs
  - The Global Fault Policy and settings that control Syslogs
- System Event Log
  - System hardware events for servers and chassis components and their internal components (System Event Log [SEL] logs)
  - The SEL policy that controls SEL logs
- Simple Network Management Protocol
  - SNMP for monitoring devices from a central network management station and the host and user settings
  - Fault suppression policies for SNMP traps, Call Home notifications, and specific devices

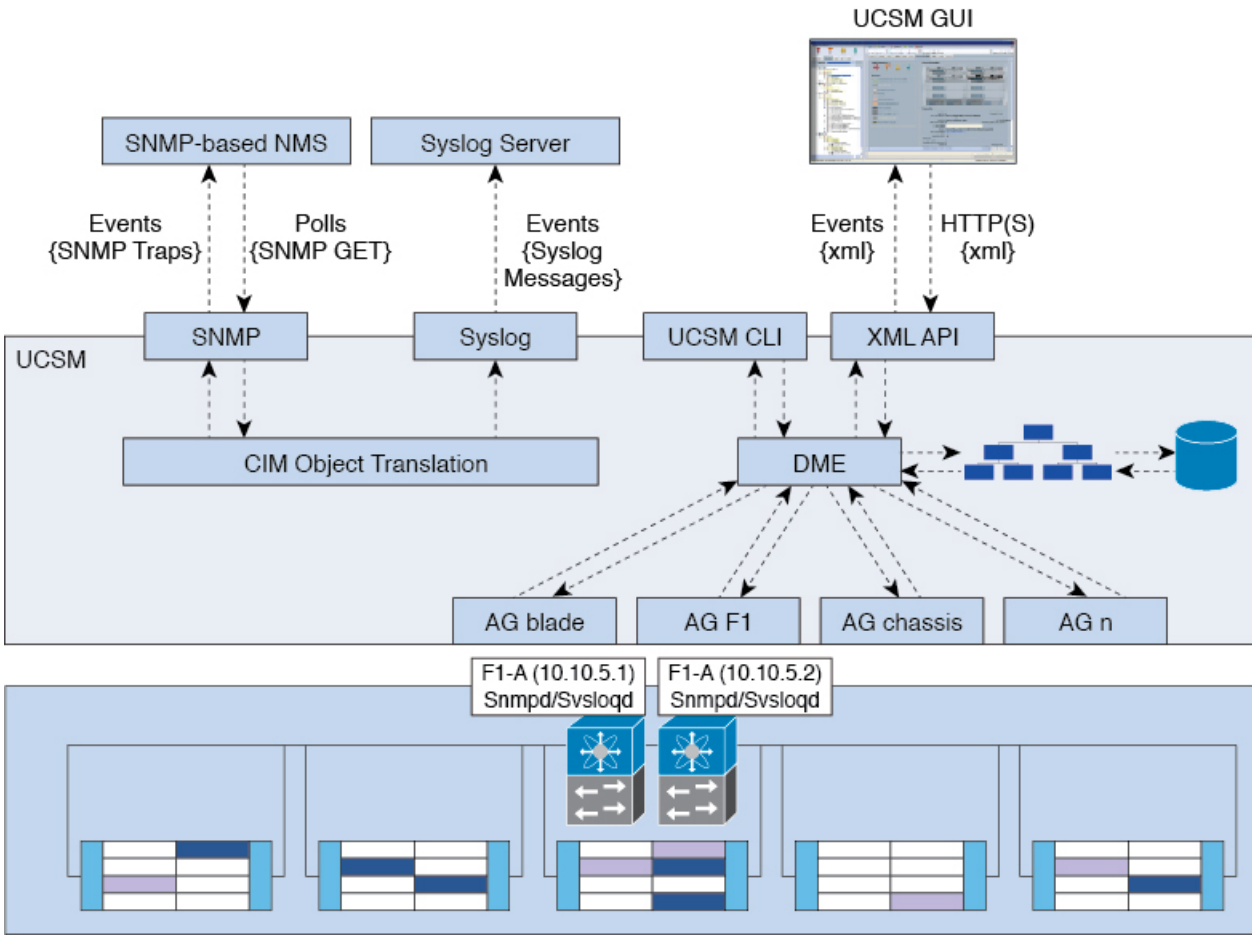
- Core File Exporter and logs, such as Syslog, Audit Log, and the System Event Log
- Statistics Collection and Threshold Policies for adapters, chassis, host, ports, and servers
- Call Home and Smart Call Home Cisco embedded device support
- Hardware monitoring using the Cisco UCS Manager user interface
- Traffic Monitoring sessions for analysis by a network analyzer
- Cisco Netflow Monitor for IP network traffic accounting, usage-based network billing, network planning, security, Denial of Service monitoring capabilities, and network monitoring

The Cisco UCS Manager Core and Fault Generation

The Cisco UCS Manager core is made up of three elements, which are the Data Management Engine, Application Gateway, and user accessible northbound interface. The northbound interface comprises of SNMP, Syslog, XML API, and UCSM CLI.

You can monitor the Cisco UCS Manager servers through XML API, SNMP, and Syslog. Both SNMP and Syslog are interfaces used only used for monitoring as they are read-only, so no configuration changes are allowed from these interfaces. Alternatively, the XML API is a monitoring interface that is read-write, which allows you to monitor Cisco UCS Manager, and change the configuration if needed.

Figure 1: Cisco UCS Manager Core and Monitoring Interfaces



Data Management Engine (DME)

The DME is the center of the Cisco UCS Manager system, which maintains:

- The Cisco UCS XML database which houses the inventory database of all physical elements (blade and rack mount servers, chassis, modules, and fabric interconnects).
- The logical configuration data for profiles, policies, pools, vNIC, and vHBA templates.
- The various networking-related configuration details like VLANs, VSANs, port channels, network uplinks, and server downlinks.

The DME monitors:

- The current health and state of all components of all physical and logical elements in a Cisco UCS domain.
- The transition information of all Finite State Machine (FSM) tasks occurring.

Only the current information of inventory, health, and configuration data of the managed endpoints are stored in the Cisco UCS XML database resulting in near real time. By default the DME does not store a historical log of faults that have occurred on a Cisco UCS domain. As fault conditions are raised on the endpoints, the

DME creates faults in the Cisco UCS XML database. As those faults are mitigated, the DME clears and removes the faults from the Cisco UCS XML database.

Application Gateway (AG)

Application Gateways are software agents that communicate directly with the endpoints to relay the health and state of the endpoints to the DME. AG-managed endpoints include servers, chassis, modules, fabric extenders, fabric interconnects, and NX-OS. The AGs actively monitor the server through the IPMI and SEL logs using the Cisco Integrated Management Controller (CIMC). They provide the DME with the health, state, configuration, and potential fault conditions of a device. The AGs manage configuration changes from the current state to the desired state during FSM transitions when changes are made to the Cisco UCS XML database.

The module AG and chassis AG communicate with the Chassis Management Controller (CMC) to get information about the health, state, configuration, and fault conditions observed by the CMC. The fabric interconnect NX-OS AG communicates directly with NX-OS to get information about the health, state, configuration, statistics, and fault conditions observed by NX-OS on the fabric interconnects. All AGs provide the inventory details to the DME about the endpoints during the various discovery processes. The AGs perform the state changes necessary to configure an endpoint during FSM-triggered transitions, monitor the health and state of the endpoints, and notify the DME of any faults.

Northbound Interfaces

The northbound interfaces include SNMP, Syslog, CLI, and XML API. The XML API present in the Apache webserver layer sends login, logout, query, and configuration requests using HTTP or HTTPS. SNMP and Syslog are both consumers of data from the DME.

SNMP informs and traps are translated directly from the fault information stored in the Cisco UCS XML database. SNMP GET requests are sent through the same object translation engine in reverse, where the DME receives a request from the object translation engine. The data is translated from the XML database to an SNMP response.

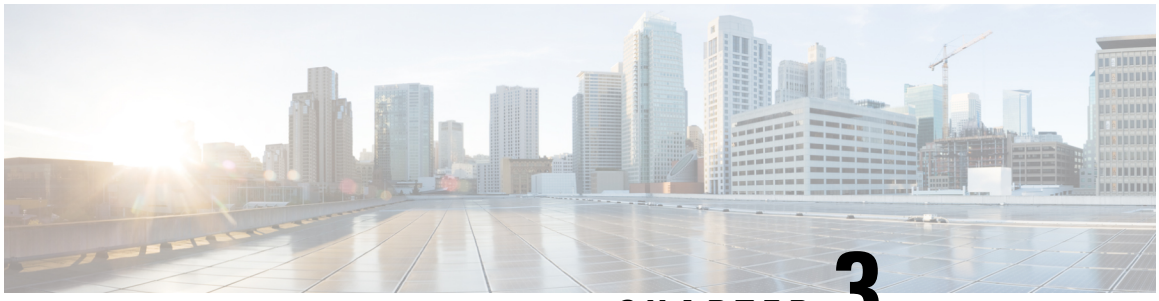
Syslog messages use the same object translation engine as SNMP, where the source of the data (faults, events, audit logs) is translated from XML into a Cisco UCS Manager-formatted Syslog message.

Cisco UCS Manager User Documentation

Cisco UCS Manager offers you a new set of smaller, use-case based documentation described in the following table:

Guide	Description
Cisco UCS Manager Getting Started Guide	Discusses Cisco UCS architecture and Day 0 operations, including Cisco UCS Manager initial configuration and configuration best practices.
Cisco UCS Manager Administration Guide	Discusses password management, role-based access configuration, remote authentication, communication services, CIMC session management, organizations, backup and restore, scheduling options, BIOS tokens, and deferred deployments.

Guide	Description
Cisco UCS Manager Infrastructure Management Guide	Discusses physical and virtual infrastructure components used and managed by Cisco UCS Manager.
Cisco UCS Manager Firmware Management Guide	Discusses downloading and managing firmware, upgrading through Auto Install, upgrading through service profiles, directly upgrading at endpoints using firmware auto sync, managing the capability catalog, deployment scenarios, and troubleshooting.
Cisco UCS Manager Server Management Guide	Discusses the new licenses, registering Cisco UCS domain with Cisco UCS Central, power capping, server boot, server profiles, and server-related policies.
Cisco UCS Manager Storage Management Guide	Discusses all aspects of storage management, such as SAN and VSAN in Cisco UCS Manager.
Cisco UCS Manager Network Management Guide	Discusses all aspects of network management, such as LAN and VLAN connectivity in Cisco UCS Manager.
Cisco UCS Manager System Monitoring Guide	Discusses all aspects of system and health monitoring, including system statistics in Cisco UCS Manager.



CHAPTER 3

Syslog

- Syslog, on page 9
- Configuring the Syslog Using Cisco UCS Manager GUI, on page 10

Syslog

Cisco UCS Manager generates system log, or syslog messages to record the following incidents that take place in the Cisco UCS Manager system:

- Routine system operations
- Failures and errors
- Critical and emergency conditions

There are three kinds of syslog entries: Fault, Event, and Audit.

Each syslog message identifies the Cisco UCS Manager process that generated the message and provides a brief description of the operation or error that occurred. The syslog is useful both in routine troubleshooting, incident handling, and management.

Cisco UCS Manager collects and logs syslog messages internally. You can send them to external syslog servers running a syslog daemon. Logging to a central syslog server helps in aggregation of logs and alerts. Some syslog messages to monitor include, DIMM problems, equipment failures, thermal problems, voltage problems, power problems, high availability (HA) cluster problems, and link failures.

Note The FSM faults, threshold faults, and unresolved policy events are not sent to syslog server. However, SNMP traps are generated for the threshold fault events.

Syslog messages contain an event code and fault code. To monitor syslog messages, you can define syslog message filters. These filters can parse the syslog messages based on the criteria you choose. You can use the following criteria to define a filter:

- By event or fault codes: Define a filter with a parsing rule to include only the specific codes that you intend to monitor. Messages that do not match these criteria are discarded.

- By severity level: Define a filter with a parsing rule to monitor syslog messages with specific severity levels. You can set syslog severity levels individually for OS functions, to facilitate logging and display of messages ranging from brief summaries to detailed information for debugging.

Cisco devices can send their log messages to a Unix-style syslog service. A syslog service simply accepts messages, then stores them in files or prints them according to a simple configuration file. This form of logging is the best available for Cisco devices because it can provide protected long-term storage of logs.

Configuring the Syslog Using Cisco UCS Manager GUI

Procedure

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

Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 Click **Syslog**.

Step 4 In the **Global Settings**, choose to enable/disable **RFC 5424 Compliance**.

- **Enabled**—Syslog messages are displayed as per RFC 5424 format.
- **Disabled**—Syslog messages are displayed in the original format. By default, it is disabled.

Note
This option is applicable only for the following:

- Cisco UCS 6600 Series Fabric Interconnect
- Cisco UCS Fabric Interconnects 9108 100G (Cisco UCS X-Series Direct)
- Cisco UCS 6400 Series Fabric Interconnects
- Cisco UCS 6500 Series Fabric Interconnects

Step 5 In the **Local Destinations** area, complete the following fields:

Name	Description
Console Section	
Admin State field	Indicate 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 are not displayed on the console.

Name	Description
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 level can be one of the following: • **Emergencies** • **Alerts** • **Critical**
Monitor Section	
Admin State field	Indicate whether Cisco UCS displays Syslog messages on the monitor. This state 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 remaining fields in this section.
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 level can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
File Section	
Admin State field	Indicates whether Cisco UCS stores messages in a system log file on the fabric interconnect. This state 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 remaining fields in this section.

Name	Description
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 level can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **Information** • **Debugging**
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 name is **'messages'**.
Size field	The maximum size, in bytes, that 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 remaining fields in this section.

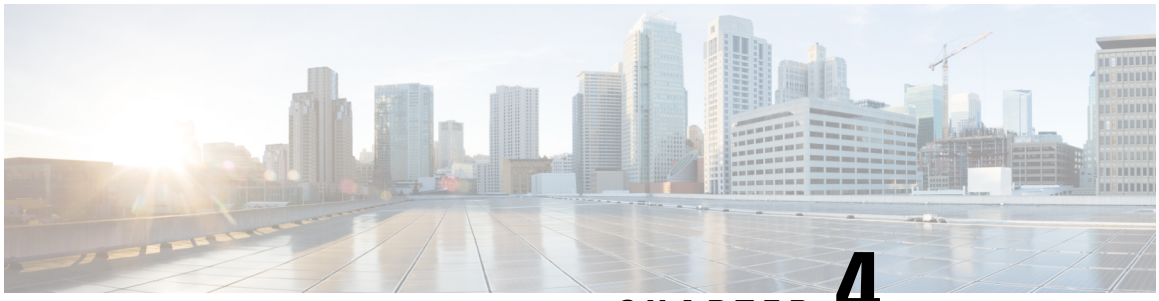
Name	Description
Level drop-down list	Select the lowest message level that you want the system to store. The system stores that level, and above, in the remote file. This level can be one of the following: • **Emergencies** • **Alerts** • **Critical** • **Errors** • **Warnings** • **Notifications** • **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.
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.

Name	Description
Events Admin State field	If this field is **Enabled**, Cisco UCS logs all system events.

Step 8 Click **Save Changes**.



CHAPTER 4

System Event Log

- System Event Log, on page 15
- Viewing the System Event Log for an Individual Server, on page 16
- Viewing the System Event Log for the Servers in a Chassis, on page 16
- Configuring the SEL Policy, on page 16
- Copying One or More Entries in the System Event Log, on page 19
- Printing the System Event Log, on page 19
- Refreshing the System Event Log, on page 19
- Manually Backing Up the System Event Log, on page 20
- Manually Clearing the System Event Log, on page 20

System Event Log

The System Event Log (SEL) resides on the CIMC in NVRAM. The SEL is used for troubleshooting system health. It records most server-related events, such as instances of over or under voltage, temperature events, fan events, and BIOS events. The types of events supported by SEL include BIOS events, memory unit events, processor events, and motherboard events.

The SEL logs are stored in the CIMC NVRAM, through a SEL log policy. It is best practice to periodically download and clear the SEL logs. The SEL file is approximately 40KB in size, and no further events can be recorded once it is full. It must be cleared before additional events can be recorded.

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis 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 **Equipment**.

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 **Equipment**.

Step 2 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** • **USB A**—The USB drive inserted into fabric interconnect A. This option is only available for certain system configurations. • **USB B**—The USB drive inserted into fabric interconnect B. This option is only available for certain system configurations.
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, provided that the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.

Name	Description
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 that you check the **Timer** check box in the **Action** option box.
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 is completed.
User field	The username the system should use to log into 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 check box	For each box that is checked, the system creates an 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**.

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 the 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 the 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 the 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.

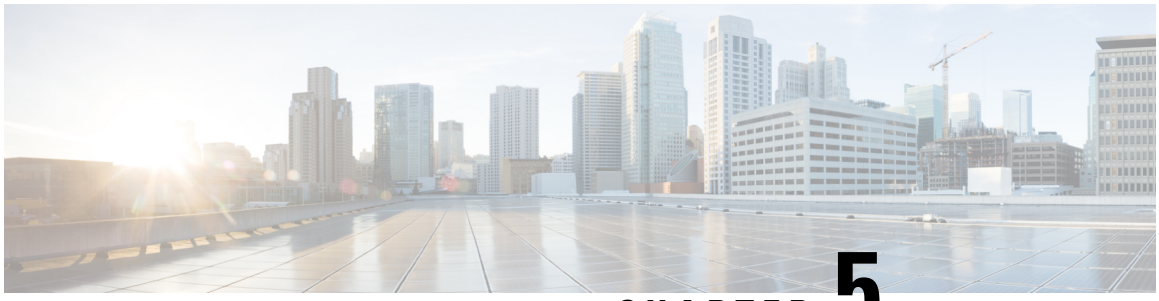
Manually Clearing the System Event Log

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 5

Core File Exporter

- Core File Exporter, on page 21
- Configuring the Core File Exporter, on page 21
- Disabling the Core File Exporter, on page 22

Core File Exporter

Critical failures in the Cisco UCS components, such as a fabric interconnect or an I/O module, can cause the system to create a core dump file. Cisco UCS Manager uses the Core File Exporter to immediately export the core dump files to a specified location on the network through TFTP. This functionality allows you to export the tar file with the contents of the core dump file. The Core File Exporter provides system monitoring and automatic export of core dump files that need to be included in TAC cases.

Configuring the Core File Exporter

Procedure

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

Step 2 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 automatically sends the core dump file via FTP to a given location. When this option is selected, the Cisco UCS Manager GUI displays the other fields that enable you to specify the FTP export options. The Core File Exporter provides system monitoring and automatic export of core files that need to be included in TAC cases. • **Disabled**—Core dump files are not automatically exported.
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.

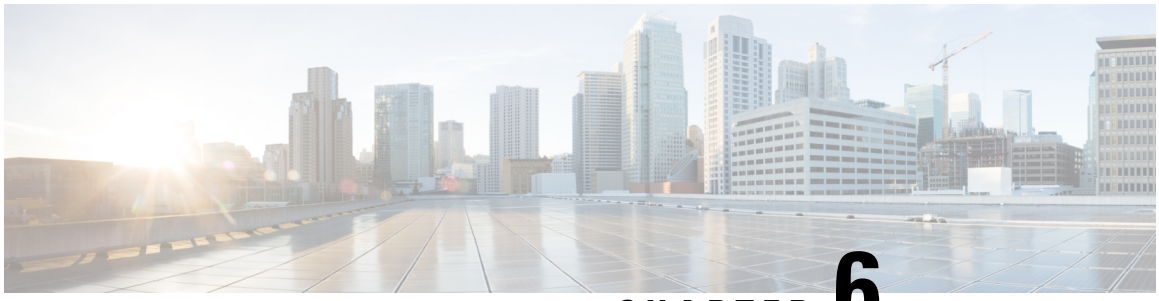
Step 6 Click **Save Changes**.

Disabling the Core File Exporter

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 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**.



CHAPTER 6

Audit Logs

- Audit Logs, on page 25
- Viewing the Audit Logs, on page 25

Audit Logs

Audit Logs record system events that occurred, where they occurred, and which users initiated them.

Viewing the Audit Logs

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

Procedure

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

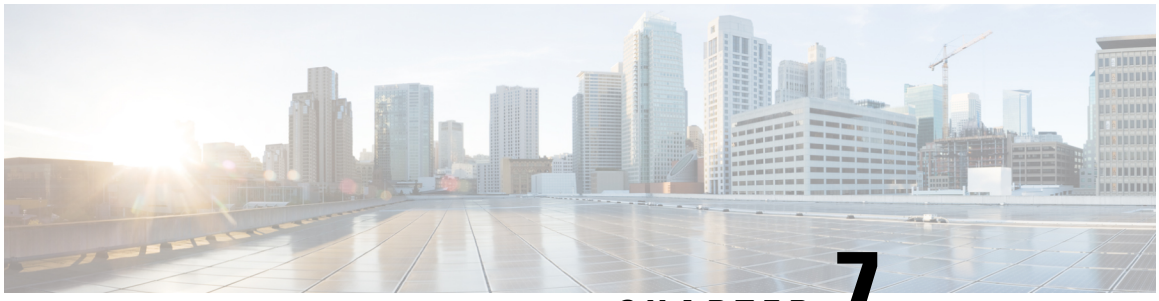
Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 In the work pane, click the **Audit Logs** tab.

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

Name	Description
ID column	The unique identifier associated with the message.
Affected Object column	The component that is affected by this issue. Click the object name to view the properties for this object.
Trig column	The user role associated with the user that triggered the event.
User column	The type of user.
Session ID column	The session ID associated with the session during which the event occurred.
Created at column	The day and time that the fault occurred.

Name	Description
Indication column	This can be one of the following: • **Creation**—A component was added to the system. • **Modification**—An existing component was changed.
Description column	More information about the fault.
Modified Properties column	The system properties that were changed by the event.



CHAPTER 7

Fabric Interconnect Audit Logs

- Overview, on page 27
- Configuring the Fabric Interconnect Audit Logs, on page 27
- Viewing and Managing Fabric Interconnect Audit Log Configuration, on page 28
- Disabling the Fabric Interconnect Audit Logs, on page 29

Overview

Fabric Interconnect Audit Logs utilize the Linux Audit Framework (auditd) to deliver comprehensive monitoring and tracking of user and system activities on Fabric Interconnects. This feature systematically captures and records audit events in log files, enhancing security and compliance by enabling administrators to review and analyze operational activities. Auditd-based audit logging is supported on Cisco UCS 6400, 6500, and 6600 Series Fabric Interconnects.

Note This feature is currently not supported on X-Series Direct (UCSX-S9108-100G) Fabric Interconnects.

Configuring the Fabric Interconnect Audit Logs

You can configure the **Fabric Interconnect Audit Logs** to enable or disable audit logging and set the desired severity level for log entries.

Note Before configuring *Fabric Interconnect Audit Logs*, ensure that *Syslog* is enabled in UCS Manager so logs can be collected and viewed. Also, ensure that the severity level for both *Syslog* and *Fabric Interconnect Audit Logs* is set to **Information** or **Debugging** to view the logs. If you plan to send logs to an external server, configure the remote Syslog server accordingly.

Procedure

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

Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 In the work pane, click the **Fabric Interconnect Audit Logs** tab.

Step 4 **In the Admin State** field, select one of the following options:

- **Enabled**: Activates the audit logging service on the Fabric Interconnects.
- **Disabled**: Deactivates the audit logging service on the Fabric Interconnects. This is the default option.

Step 5 In the **Severity drop-down** list, select the severity level for the audit logs. The available options are:

- Emergencies (most critical events)
- Alerts
- Critical (UCSM Critical)
- Errors (UCSM Major)
- Warnings (UCSM Minor)
- Notifications (UCSM Warning)
- Information
- Debugging

Step 6 Click **Save Changes** to save the configuration.

Viewing and Managing Fabric Interconnect Audit Log Configuration

You can view and manage the configuration settings for **Fabric Interconnect Audit Logs** page.

Procedure

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

Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 In the work pane, click the **Fabric Interconnect Audit Logs** tab.

Step 4 The **Work** pane displays the configuration settings for **Fabric Interconnect Audit Logs**. You can view and modify these settings as needed.

Note

- The actual audit log entries are not displayed on this page; only configuration options for Fabric Interconnect Audit Logs are available.
- If audit log entries are not visible, ensure that Syslog is enabled in UCS Manager. Audit logs are routed through Syslog, and their visibility depends on the configured severity levels. Set the severity level for

both Fabric Interconnect Audit Logs and Syslog to **Information** or **Debugging** to display detailed log entries. Ensure the severity levels match for proper log visibility.

Disabling the Fabric Interconnect Audit Logs

You can unconfigure the **Fabric Interconnect Audit Logs** to disable the logging service and revert any customized settings to their default values.

Procedure

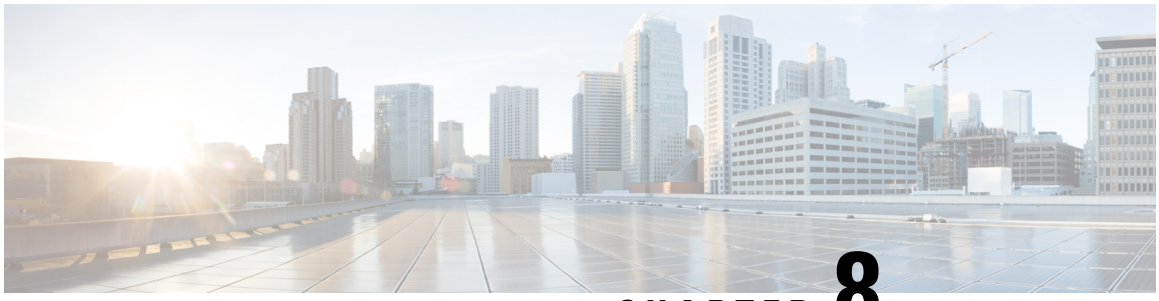
Step 1 In the **Navigation** pane, click **Admin**.

Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 In the work pane, click the **Fabric Interconnect Audit Logs** tab.

Step 4 **In the Admin State** field, select **Disabled** to deactivate the fabric interconnect audit logging service.

Step 5 **Click Save Changes** to confirm the changes and unconfigure the audit logs.



CHAPTER 8

Fault Collection and Suppression

- Configuring Settings for the Fault Collection Policy, on page 31
- Configuring Fault Suppression, on page 33

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 **Admin**.

Step 2 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	Indicate 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.

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 you. After the fault suppression has ended, Cisco UCS Manager will send notifications for any outstanding suppressed faults that have not been cleared.

You can configure fault suppression using the following methods.

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. They 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, 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, 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, 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.

Note Cisco UCS Manager does not suppress SNMP MIB-2 faults generated by NX-OS network operating system designed to support high performance, high reliability server access switches used in the data center. These SNMP MIB-2 faults have no association with this fault suppression policy.

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

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

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 **Admin**.

Step 2 Expand **All** > **Faults, Events, and Audit Log**.

Step 3 Click **Faults**.

Step 4 In the **Work** pane, choose the **Suppressed** icon in the **Severity** area.

To view only the suppressed faults, uncheck the other icons in the **Severity** area.

Configuring Fault Suppression for a Chassis

Configuring Fault Suppression Tasks for a Chassis

Procedure

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

Step 2 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 is saved.
Select Fixed Time Interval/Schedule field	Specify 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, 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.

Step 7 Click **OK**.

Viewing Fault Suppression Tasks for a Chassis

Procedure

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

Step 2 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.

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 36.

Procedure

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

Step 2 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 a confirmation dialog box displays, click **Yes**.

Configuring Fault Suppression for an I/O Module and IFM (IOM for Cisco UCS X-Series Servers)

Configuring Fault Suppression Tasks for an IOM and IFM (IOM for Cisco UCS X-Series Servers)

Beginning with release 4.3(2a), Cisco UCS Manager supports Cisco UCS X9508 server chassis with Cisco UCS X-Series servers. Cisco UCS X-Series servers support Intelligent Fabric Modules (IFM), which function similarly to the Input/Output Module (IOM) in Cisco UCS B-Series servers. This guide uses the term IOM to refer both IOM and IFM.

Procedure

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

Step 2 (Optional) To select IOM modules in a chassis, expand **Equipment** > **Chassis** > *Chassis Number* > **IO Modules**.

Step 3 (Optional) To select IOM modules in a FEX, expand **Equipment** > **FEX** > *FEX Number* > **IO Modules**.

Step 4 Click the IOM for which you want to create a fault suppression task.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Start Fault Suppression**.

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

You can select IOMs in either chassis, FEXes, or both.

Step 7 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 is saved.

Select Fixed Time Interval/Schedule field	Specify 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 8 Click **OK**.

Viewing Fault Suppression Tasks for an IOM and IFM (IOM for Cisco UCS X-Series Servers)

Procedure

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

Step 2 (Optional) To select IOM modules in a chassis, expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 (Optional) To select IOM modules in a FEX, expand **Equipment** > **FEX** > ***FEX Number*** > **IO Modules**.

Step 4 Click the IOM for which you want to view fault suppression task properties.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 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.

Deleting Fault Suppression Tasks for an IOM and IFM (IOM for Cisco UCS X-Series Servers)

This procedure deletes all fault suppression tasks for an IOM. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for an IOM and IFM (IOM for Cisco UCS X-Series Servers), on page 38.

Procedure

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

Step 2 (Optional) To select IOM modules in a chassis, expand **Equipment** > **Chassis** > *Chassis Number* > **IO Modules**.

Step 3 (Optional) To select IOM modules in a FEX, expand **Equipment** > **FEX** > *FEX Number* > **IO Modules**.

Step 4 Click the IOM for which you want to delete all fault suppression tasks.

Step 5 In the **Work** pane, click the **General** tab.

Step 6 In the **Actions** area, click **Stop Fault Suppression**.

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

You can select IOMs in either chassis, FEXes, or both.

Step 7 If a confirmation dialog box displays, click **Yes**.

Configuring Fault Suppression for a FEX

Configuring Fault Suppression Tasks for a FEX

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **FEX**.

Step 3 Click the FEX 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 FEXes, use the **Ctrl** key to select multiple FEXes in the **Navigation** pane. Right-click one of the selected FEXes 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 is saved.

Select Fixed Time Interval/Schedule field	Specify 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-fex-all-maint**—Suppresses faults for the FEX, all power supplies, fan modules, and IOMs in the FEX. • **default-fex-phys-maint**—Suppresses faults for the FEX, all fan modules and power supplies in the FEX. • **default-iom-maint**—Suppresses faults for IOMs in a chassis or FEX.

Step 7 Click **OK**.

Viewing Fault Suppression Tasks for a FEX

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **FEX**.

Step 3 Click the FEX 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.

Deleting Fault Suppression Tasks for a FEX

This procedure deletes all fault suppression tasks for a FEX. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for a FEX, on page 40.

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **FEX**.

Step 3 Click the FEX 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 FEXes, use the **Ctrl** key to select multiple FEXes in the **Navigation** pane. Right-click one of the selected FEXes and choose **Stop Fault Suppression**.

Step 6 If a confirmation dialog box displays, click **Yes**.

Configuring Fault Suppression for Servers

Configuring Fault Suppression Tasks for a Blade Server

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > *Chassis 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 blade servers, use the **Ctrl** key to select multiple blade 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 is saved.

Select Fixed Time Interval/Schedule field	Specify 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**.

Viewing Fault Suppression Tasks for a Blade Server

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis 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.

Deleting Fault Suppression Tasks for a Blade Server

This procedure deletes all fault suppression tasks for a blade server. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for a Blade Server, on page 42.

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis 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 blade servers, use the **Ctrl** key to select multiple blade servers in the **Navigation** pane. Right-click one of the selected servers and choose **Stop Fault Suppression**.

Step 6 If a confirmation dialog box displays, click **Yes**.

Configuring Fault Suppression Tasks for a Rack Server

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **Servers**.

Note
For Cisco UCS C125 M5 Servers, expand **Equipment** > **Rack Mounts** > **Enclosures** > **Rack Enclosure** ***rack_enclosure_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 rack servers, use the **Ctrl** key to select multiple rack 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 is saved.

Select Fixed Time Interval/Schedule field	Specify 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**.

Viewing Fault Suppression Tasks for a Rack Server

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **Servers**.

Note
For Cisco UCS C125 M5 Servers, expand **Equipment** > **Rack Mounts** > **Enclosures** > **Rack Enclosure** ***rack_enclosure_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.

Deleting Fault Suppression Tasks for a Rack Server

This procedure deletes all fault suppression tasks for a rack server. To delete individual tasks, use the **Delete** button on the **Suppression Tasks** dialog box. See Viewing Fault Suppression Tasks for a Rack Server, on page 44.

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **Servers**.

Note
For Cisco UCS C125 M5 Servers, expand **Equipment** > **Rack Mounts** > **Enclosures** > **Rack Enclosure** ***rack_enclosure_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 rack servers, use the **Ctrl** key to select multiple rack servers in the **Navigation** pane. Right-click one of the selected servers and choose **Stop Fault Suppression**.

Step 6 If a confirmation dialog box displays, click **Yes**.

Configuring Fault Suppression for a Service Profile

Configuring Fault Suppression Tasks for a Service Profile

Procedure

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

Step 2 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 is saved.
Select Fixed Time Interval/Schedule field	Specify 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 47.

Procedure

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

Step 2 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 a confirmation dialog box displays, click **Yes**.

Viewing Fault Suppression Tasks for a Service Profile

Procedure

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

Step 2 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 **Servers**.

Step 2 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 is saved.

Select Fixed Time Interval/Schedule field	Specify 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 48.

Procedure

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 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 a confirmation dialog box displays, click **Yes**.

Viewing Fault Suppression Tasks for an Organization

Procedure

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

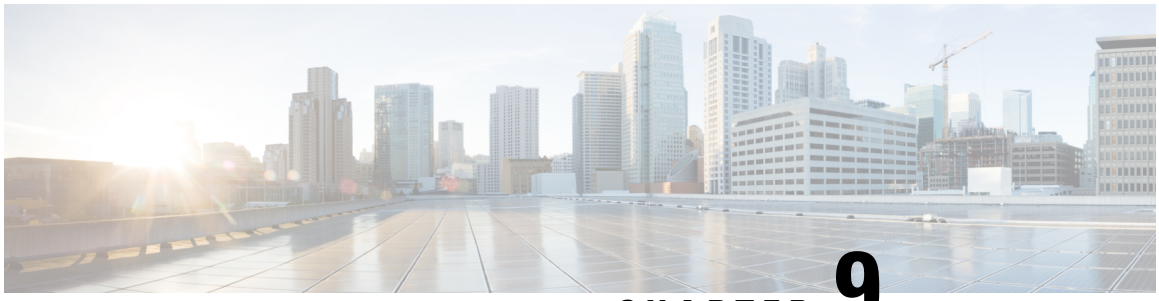
Step 2 Expand **Servers** > **Policies** > ***Organization_Name***.

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.



CHAPTER 9

SNMP Configuration

- SNMP Overview, on page 51
- Enabling SNMP and Configuring SNMP Properties, on page 54
- Creating an SNMP Trap, on page 55
- Deleting an SNMP Trap, on page 56
- Creating an SNMPv3 user, on page 56
- Deleting an SNMPv3 User, on page 57

SNMP Overview

The Simple Network Management Protocol (SNMP) is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language for monitoring and managing devices in a network.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS, the managed device that maintains the data for Cisco UCS, and reports the data as needed to the SNMP manager. Cisco UCS includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Manager.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS release 1.4(1) and higher supports a larger number of MIBs than earlier releases.

Cisco UCS supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMP is defined in the following:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)

- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Cisco UCS Manager generates SNMP notifications as either traps or informs. Traps are less reliable than informs because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Manager cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response Protocol Data Unit (PDU). If the Cisco UCS Manager does not receive the PDU, it can send the inform request again.

SNMP Security Levels and Privileges

SNMPv1, SNMPv2c, and SNMPv3 each represent a different security model. The security model combines with the selected security level to determine the security mechanism applied when the SNMP message is processed.

The security level determines the privileges required to view the message associated with an SNMP trap. The privilege level determines whether the message requires protection from disclosure or whether the message is authenticated. The supported security level depends on which security model is implemented. SNMP security levels support one or more of the following privileges:

- noAuthNoPriv—No authentication or encryption
- authNoPriv—Authentication but no encryption
- authPriv—Authentication and encryption

SNMPv3 provides for both security models and security levels. A security model is an authentication strategy that is set up for a user and the role in which the user resides. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet.

Supported Combinations of SNMP Security Models and Levels

The following table identifies the combinations of security models and levels.

Table 2: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMPv3 Security Features

SNMPv3 provides secure access to devices through a combination of authenticating and encrypting frames over the network. SNMPv3 authorizes only configured users to perform management operations and encrypts SNMP messages. The SNMPv3 User-Based Security Model (USM) refers to SNMP message-level security and offers the following services:

- Message integrity—Ensures that messages are not altered or destroyed in an unauthorized manner, and that data sequences are not altered beyond what can occur non-maliciously.
- Message origin authentication—Ensures that the identity of a message originator is verifiable.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Support in Cisco UCS

Cisco UCS provides the following support for SNMP:

Support for MIBs

Cisco UCS supports read-only access to MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html for B-series servers, and http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/c-series/b_UCS_Standalone_C-Series_MIBRef.html C-series servers.

Authentication Protocols for SNMPv3 Users

Cisco UCS supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)
- HMAC-SHA-96 (SHA)

AES Privacy Protocol for SNMPv3 Users

Cisco UCS uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Manager uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

To deploy such a user, enable **AES-128** encryption.

Enabling SNMP and Configuring SNMP Properties

SNMP messages from a Cisco UCS domain display the fabric interconnect name rather than the system name.

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 Select the **Communication Services** tab.

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

Name	Description
Admin State field	This can be one of the following: • **Enabled** • **Disabled** Enable this service only if your system includes integration with an SNMP server. If **Admin State** is enabled, Cisco UCS Manager GUI displays the remaining fields in this section.

Step 5 Click **Save Changes**.

What to do next

Create SNMP traps and users.

Creating an SNMP Trap

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Traps** area, click **+**.

Step 5 In the **Create SNMP Trap** dialog box, complete the following fields:

Name	Description
Hostname (or IP Address) field	The host name or IP address of the SNMP host to which Cisco UCS Manager should send the trap. You can use an IPv4 address, or an IPv6 address for the SNMP host. The host name can also be a fully qualified domain name of an IPv4 address.
Community/Username field	The SNMP v1 or v2c community name or the SNMP v3 username Cisco UCS Manager includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark), & (ampersand), or an empty space.
Port field	The port on which Cisco UCS Manager communicates with the SNMP host for the trap. Enter an integer between 1 and 65535. The default port is 162.
Version field	The SNMP version and model used for the trap. This can be one of the following: • **V1** • **V2c** • **V3**
Type field	The type of trap to send. If you select **V2c** or **V3** for the version, the type of trap to be sent can be one of the following: • **Traps** • **Informs**

Name	Description
v3 Privilege field	If you select **V3** for the version, the privilege associated with the trap. This can be one of the following: • **Auth**—Authentication but no encryption • **Noauth**—No authentication or encryption • **Priv**—Authentication and encryption

Note
A maximum of 8 hosts can be added for SNMP traps.

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Deleting an SNMP Trap

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Traps** area, click the row in the table that corresponds to the user you want to delete.

Step 5 Click the **Delete** icon to the right of the table.

Step 6 If a confirmation dialog box displays, click **Yes**.

Step 7 Click **Save Changes**.

Creating an SNMPv3 user

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Users** area, click **+**.

Step 5 In the **Create SNMP User** dialog box, complete the following fields:

Name	Description
Name field	The user name assigned to the SNMP user. Enter up to 24 letters or numbers. The user name must begin with a letter and can include the special characters: _ (underscore), . (period), @ (at sign), and - (hyphen). **Note** • User name identical to existing locally authenticated user names is not supported. • User name beginning with a non-letter character is not supported.
Auth Type field	The authorization type. This can be only be **SHA**.
Use AES-128 field	Whether the user uses AES-128 encryption.
Password field	The password for this user.
Confirm Password field	The password again for confirmation purposes. **Note** • The *Password Strength Check* option is supported only for locally authenticated users and is not supported for SNMPv3 users. • For more information on the password guidelines, see the *Guidelines for Cisco UCS Passwords* section in Cisco UCS Manager Administration Management Guide.
Privacy Password field	The privacy password for this user.
Confirm Privacy Password field	The privacy password again for confirmation purposes.

Step 6 Click **OK**.

Step 7 Click **Save Changes**.

Deleting an SNMPv3 User

Procedure

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

Step 2 Expand **All** > **Communication Management** > **Communication Services**.

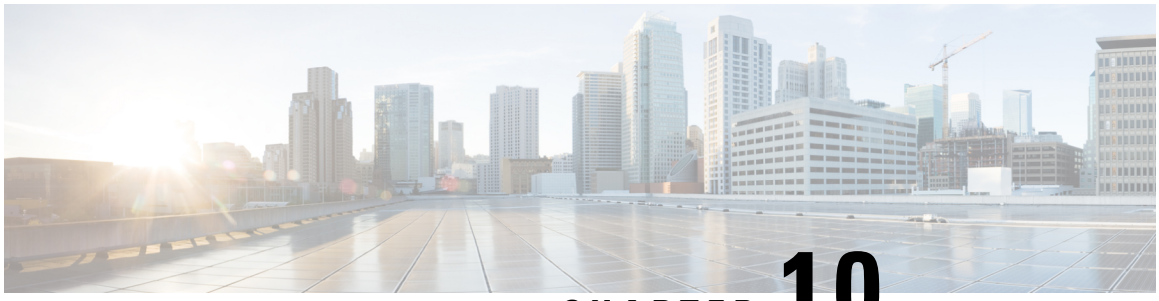
Step 3 Select the **Communication Services** tab.

Step 4 In the **SNMP Users** area, click the row in the table that corresponds to the user you want to delete.

Step 5 Click the **Delete** icon to the right of the table.

Step 6 If a confirmation dialog box displays, click **Yes**.

Step 7 Click **Save Changes**.



CHAPTER 10

SPDM Security

- SPDM Security, on page 59
- Creating a SPDM Security Policy, on page 60
- Associating the Security Policy with a Server, on page 61
- Viewing the Fault Alert Settings, on page 61

SPDM Security

Cisco UCS M6, M7, and M8 servers can contain mutable components that could provide vectors for attack against a device itself or use of a device to attack another device within the system. To defend against these attacks, the Security Protocol and Data Model (SPDM) Specification enables a secure transport implementation that challenges a device to prove its identity and the correctness of its mutable component configuration.

SPDM defines messages, data objects, and sequences for performing message exchanges between devices over a variety of transport and physical media. It orchestrates message exchanges between Baseboard Management Controllers (BMC) and end-point devices over a Management Component Transport Protocol (MCTP). Message exchanges include authentication of hardware identities accessing the BMC. The SPDM enables access to low-level security capabilities and operations by specifying a managed level for device authentication, firmware measurement, and certificate management. Endpoint devices are challenged to provide authentication. and BMC authenticates the endpoints and only allows access for trusted entities.

The UCS Manager optionally allows uploads of external security certificates to BMC. A maximum of 40 SPDM certificates is allowed, including native internal certificates. Once the limit is reached, no more certificates can be uploaded. User uploaded certificates can be deleted but internal/default certificates cannot.

A SPDM security policy allows you to specify one of three Security level settings. Security can be set at one of the three levels listed below:

- Full Security:

  This is the highest MCTP security setting. When you select this setting, a fault is generated when any endpoint authentication failure or firmware measurement failure is detected. A fault will also be generated if any of the endpoints do not support either endpoint authentication or firmware measurements.

- Partial Security (default):

  When you select this setting, a fault is generated when any endpoint authentication failure or firmware measurement failure is detected. There will NOT be a fault generated when the endpoint doesn’t support endpoint authentication or firmware measurements.

- No Security

When you select this setting, there will NOT be a fault generated for any failure (either endpoint measurement or firmware measurement failures).

You can also upload the content of one or more external/device certificates into BMC. Using a SPDM policy allows you to change or delete security certificates or settings as desired. Certificates can be deleted or replaced when no longer needed.

Certificates are listed in all user interfaces on a system.

Creating a SPDM Security Policy

This step creates a SPDM policy.

Note You can upload up to 40 SPDM certificates (including native certificates).

Procedure

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

Step 2 Go to **Policies**. Expand the root node.

Step 3 Right-click **SPDM Certificate Policies** and select **Create SPDM Policy**.

Step 4 Enter a name for this policy and select a **Fault Alert Setting** for the security level: **Disabled**, **Partial**, or **Full**.

Full—If you select this option, then a fault is generated when there is any endpoint authentication failure for both supported and unsupported endpoints.

Partial—If you select this option then a fault is generated when there is any endpoint authentication failure to only supported endpoints. No fault is generated when the endpoint does not support authentication.

Disabled—If you select this option then no fault is generated for endpoint authentication failure for both supported and unsupported endpoints.

The default is **Partial**.

Note
To perform SPDM re-authentication and update the faults, Cisco IMC reboot or host reboot is required when the fault alert value is changed for an associated profile.

Step 5 Click on **Add** in the **Create Policy** window. The **Add SPDM Certificate** window will open.

Step 6 Name the certificate.

UCS Manager supports only **Pem**certificates.

Step 7 Paste the contents of the certificate into the Certificate field.

Step 8 Click **OK** to add the certificate and return to the **Create SPDM Policy** window.

You can add up to 40 certificates.

Step 9 In the **Create SPDM Policy** menu, click **Okay**.

After the SPDM policy is created, it will be listed immediately, along with its Alert setting, when you select **SPDM Certificate Policy** under the Server root Policies.

What to do next

Assign the Certificate to a Service Profile. The Service Profile must be associated with a server for it to take effect.

Associating the Security Policy with a Server

Before you begin

Create the SPDM security policy.

Procedure

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

Step 2 Go to **Service Profiles**. Expand the root node.

Step 3 Select the Service Profile you want to associate with the Policy you created.

a) On the **Policies** tab, scroll down and expand **SPDM Certificate Policy**. In the **SPDM Certificate Policy** dropdown, select the desired policy to associate with this Service Profile.

Step 4 Click **OK**.

The SPDM Policy will now be associated with the service profile.

What to do next

Check the fault alert level to make sure it is set to the desired setting.

Viewing the Fault Alert Settings

You can view the Fault Alert setting associated with a specific chassis.

Before you begin

Create a policy and associate it with a Service Profile.

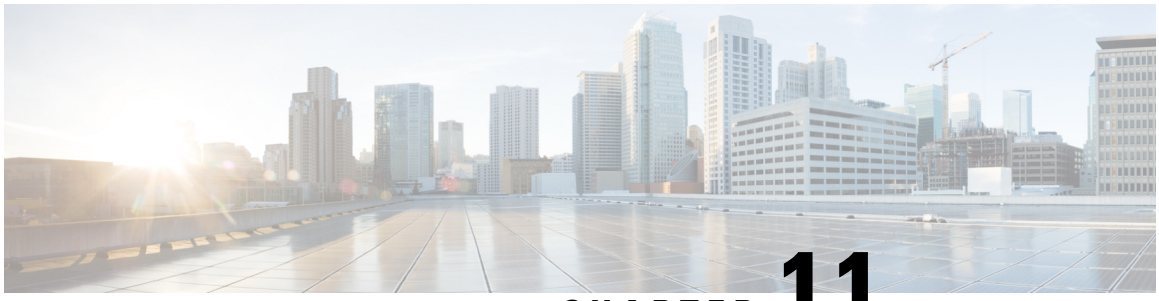
Procedure

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

Step 2 Select a Rack-Mount Server.

Step 3 On the **Inventory** tab, select **CIMC**. .

User uploaded certificates are listed and information for specific certificates can be selected and viewed.



CHAPTER 11

Statistics Collection Policy Configuration

- Configuring Statistics Collection Policies, on page 63
- Configuring Statistics Threshold Policies, on page 66

Configuring Statistics Collection Policies

Statistics Collection Policy

A statistics collection policy defines how frequently statistics are collected (collection interval) and how frequently the statistics are reported (reporting interval). Reporting intervals are longer than collection intervals so that multiple statistical data points can be collected during the reporting interval. This 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.

The values that are displayed for delta counter in Cisco UCS Manager are calculated as the difference between the last two samples in a collection interval. In addition, Cisco UCS Manager displays the average, minimum, and maximum delta values of the samples in the collection interval.

Modifying a Statistics Collection Policy

Procedure

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

Step 2 Expand **All** > **Stats Management** > **Collection Policies**.

Step 3 In the work pane, 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**.

Viewing Statistics Collection Policy Details

Procedure

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

Step 2 Expand **All** > **Stats Management** > **Collection Policies**.

Step 3 In the work pane, click the specific policy for which you want to view details.

Step 4 The work pane will display information about the selected policy across several tabs:

- **General Tab:** This tab displays general information about the selected statistics collection policy.
- **Events Tab:** This tab lists events related to the policy, such as transitions or changes. It provides details like the affected object, event code, ID, cause, creation timestamp, user, and a description of the event.
- **FSM Tab:** This tab provides details about the Finite State Machine (FSM) for the policy. If a task is currently executing on behalf of this component, the **Current Task** field will be displayed, providing insight into the ongoing operations.

  Note
  If there is no current task, this field will not be displayed.

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.

Cisco UCS enables you to configure statistics threshold policies for servers and server components.

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 **Servers**.

Step 2 Expand **Servers** > **Policies**.

Step 3 Expand the node for the organization where you want to create the policy.

If the system does not include multi tenancy, 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 is saved.
Description field	A description of the policy. Cisco recommends including information about where and when to use the policy. 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**.

Deleting a Server and Server Component Threshold Policy

Procedure

Step 1 In the **Navigation** pane, click **Servers**.
Step 2 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 a confirmation dialog box displays, click **Yes**.

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 **Servers**.
Step 2 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**.

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 **LAN**.

Step 2 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 **LAN**.

Step 2 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 **SAN**.
Step 2 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:

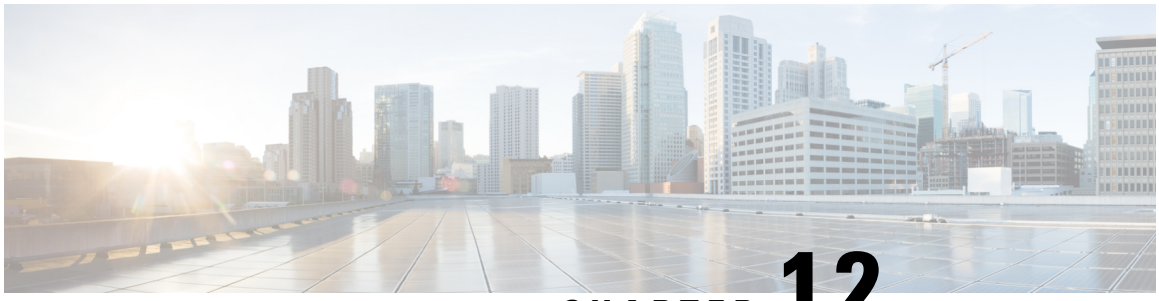
- **Info**
- **Condition**
- **Warning**
- **Minor**
- **Major**
- **Critical**

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 12

Call Home and Smart Call Home Configuration

• Call Home and Smart Call Home Configuration, on page 75

Call Home and Smart Call Home Configuration

Call Home in UCS Overview

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.

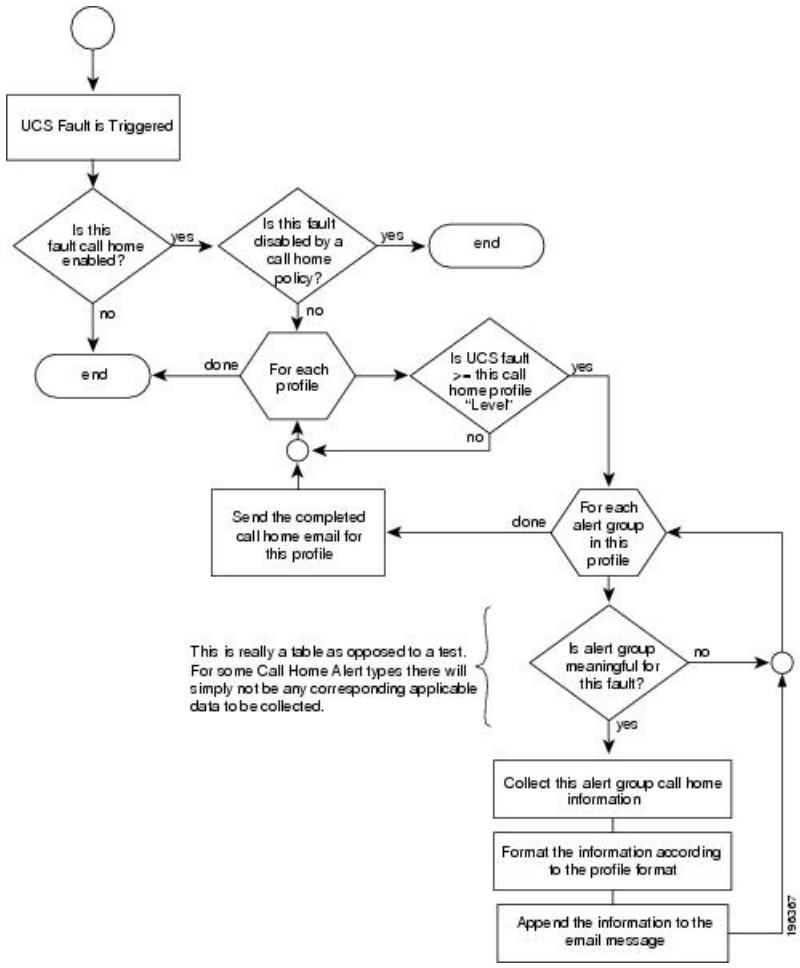
Cisco UCS delivers Call Home messages in the following formats:

- 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 2: Flow of Events after a Fault is Triggered



SMTP Authentication

Beginning with release 4.2(3b), UCS Manager supports secured authentication for the transport email with the SMTP server.

You can toggle **SMTP Authentication** between

- **Off**—SMTP Authentication is not used for this Cisco UCS domain.
- **On**—SMTP Authentication is used for this Cisco UCS domain.

Note SMTP server should be capable of supporting STARTTLS, SSL based SMTP communication.

You should also install the server root CA certificate on the SMTP-Client (switch) for succesfull connection between SSL to SMTP-AUTH server.

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 depends 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 might 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 to Cisco UCS Manager in a cluster configuration is never the source of the email.

Note Ensure that you add each fabric interconnect IP in the SMTP server. Call Home email messages cannot be delivered if the fabric interconnect IPs are not configured in the SMTP server.

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.

SMTP Authentication

Beginning with release 4.2(3b), UCS Manager supports secured authentication for the transport email with the SMTP server.

You can toggle **SMTP Authentication** between

- **Off**—SMTP Authentication is not used for this Cisco UCS domain.

- **On**—SMTP Authentication is used for this Cisco UCS domain.

Note SMTP server should be capable of supporting STARTTLS, SSL based SMTP communication.

You should also install the server root CA certificate on the SMTP-Client (switch) for succesfull connection between SSL to SMTP-AUTH server.

Cisco UCS Faults and Call Home Severity Levels

Because Call Home is present across several Cisco product lines, Call Home has 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 3: 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.
(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.

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.

Enabling Anonymous Reporting

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

Procedure

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

Step 2 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**.

Configuring Call Home

Procedure

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

Step 2 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.
Switch Priority drop-down list	This can be one of the following: • **Alerts** • **Critical** • **Debugging** • **Emergencies** • **Errors** • **Information** • **Notifications** • **Warnings**
Throttling field	Indicates 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 timeframe, 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. **Note** On Cisco UCS 6454, UCS 64108, UCS 6536 Fabric Interconnects, Cisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6664 Fabric Interconnect, ensure to limit the phone number within 17 characters. Cisco UCS Manager system may raise a fault when the phone number limit exceeds 17 characters.
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 might 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 Cisco.com 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.
Reply To field	The return email address that should appear in the **To** 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. If you use **SMTP Authentication** for secure communication, then the standard ports are 465 and 587. You can also configure other ports in your SMTP server.

Name	Description
SMTP Authentication radio button	Beginning with release 4.2(3b), UCS Manager supports secured authentication for the transport email with the SMTP server. This can be one of the following: • **Off**—SMTP Authentication is not used for this Cisco UCS domain. • **On**—SMTP Authentication is used for this Cisco UCS domain. **Note** SMTP server should be capable of supporting STARTTLS, SSL based SMTP communication. You should also install the server root CA certificate on the SMTP-Client (switch) for succesfull connection between SSL to SMTP-AUTH server.
User Name field	Enter an SMTP username. Username can be up to 255 characters, including the following: • Alphabets, lower and upper case • Numbers • _(underscore) • .(period / dot) • -(hyphen)
Password field	Enter a password. Password can be up to 56 characters.

Step 9 Click **Save Changes**.

Disabling Call Home

This step is optional.

When you upgrade a Cisco UCS domain, Cisco UCS Manager restarts the components to complete the upgrade process. This restart causes events that are identical to service disruptions and component failures that trigger Call Home alerts to be sent. If you do not disable Call Home before you begin the upgrade, you can ignore the alerts generated by the upgrade-related component restarts.

Procedure

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

Step 2 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

This step is optional. You only need to enable Call Home if you disabled it before you began the firmware upgrades.

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 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

Procedure

Step 1 In the **Navigation** pane, click **Admin**.
Step 2 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.

Name	Description
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.
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 **Admin**.

Step 2 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. 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 Manager sends Call Home alerts to e-mail destinations in a destination profile only under the following conditions:

- If the Call Home alert belongs to one of the alert groups associated with that destination profile.
- 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 Manager 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. **Note** A Call Home alert is not generated when fans or PSUs are manually removed from the chassis. This is by design.

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 **Admin**.

Step 2 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 is 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.

This email address receives Callhome Alerts/Faults.

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 **Admin**.

Step 2 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.

Note You can configure Cisco UCS Manager not to process the default faults and system events.

To disable alerts for a type of fault or event, you must first create a Call Home 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 **Admin**.

Step 2 Expand **All** > **Communication Management** > **Call Home**.

Step 3 In the **Work** pane, click the **Call Home 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 **Admin**.
Step 2 Expand **All** > **Communication Management** > **Call Home**.
Step 3 In the **Work** pane, click the **Call Home 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 **Admin**.
Step 2 Expand **All** > **Communication Management** > **Call Home**.
Step 3 In the **Work** pane, click the **Call Home 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

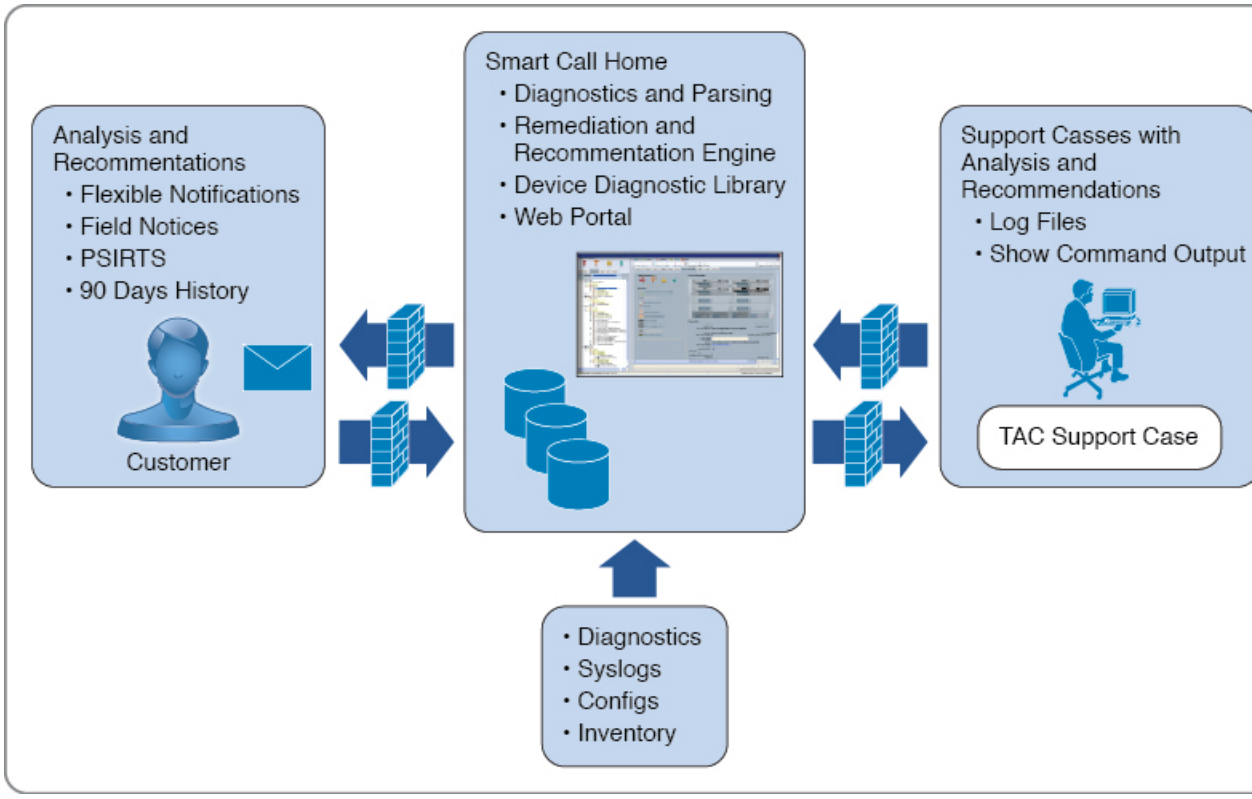
Step 1 In the **Navigation** pane, click **Admin**.
Step 2 Expand **All** > **Communication Management** > **Call Home**.
Step 3 In the **Work** pane, click the **Call Home Policies** tab.
Step 4 Right-click the policy that you want to disable and choose **Delete**.
Step 5 Click **Save Changes**.

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.

Figure 3: Cisco Smart Call Home Features



Note Using Smart Call Home requires the following:

- A Cisco.com 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.
- Beginning with release 4.2(3b), UCS Manager supports secured authentication for the transport email with the SMTP server. You require SMTP server, which is capable of supporting STARTTLS, SSL based SMTP communication.

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.com.

To configure Smart Call Home, 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.

Note In order to apply Callhome sendtestAlert functionality at least one of the email destination should be set for profiles other than CiscoTAC-1.

- Send a Smart Call Home inventory message to start the registration process.
- Ensure that the Cisco.com 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 Cisco.com.

SMTP Authentication

Beginning with release 4.2(3b), UCS Manager supports secured authentication for the transport email with the SMTP server.

You can toggle **SMTP Authentication** between

- **Off**—SMTP Authentication is not used for this Cisco UCS domain.
- **On**—SMTP Authentication is used for this Cisco UCS domain.

Note SMTP server should be capable of supporting STARTTLS, SSL based SMTP communication.

You should also install the server root CA certificate on the SMTP-Client (switch) for succesfull connection between SSL to SMTP-AUTH server.

Configuring Smart Call Home

Procedure

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

Step 2 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 Indicates 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 timeframe, then the system discards further messages for that alert type.
- **Off**—The system sends all duplicate messages, regardless of how many are encountered.

Step 6 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. **Note** On Cisco UCS 6454, UCS 64108, UCS 6536 Fabric Interconnects, Cisco UCS Fabric Interconnects 9108 100G, and Cisco UCS 6664 Fabric Interconnect, ensure to limit the phone number within 17 characters. Cisco UCS Manager system may raise a fault when the phone number limit exceeds 17 characters.
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 might 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.

Name	Description
Address field	The mailing address for the main contact. Enter up to 255 ASCII characters.

Step 7 In the **Ids** area, complete the following fields with the Smart Call Home identification information:

Name	Description
Customer Id field	The Cisco.com 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 8 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 **To** field on Call Home alert messages sent by the system.

Step 9 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. If you use **SMTP Authentication** for secure communication, then the standard ports are 465 and 587. You can also configure other ports in your SMTP server.

Name	Description
SMTP Authentication radio button	Beginning with release 4.2(3b), UCS Manager supports secured authentication for the transport email with the SMTP server. This can be one of the following: • **Off**—SMTP Authentication is not used for this Cisco UCS domain. • **On**—SMTP Authentication is used for this Cisco UCS domain. **Note** SMTP server should be capable of supporting STARTTLS, SSL based SMTP communication. You should also install the server root CA certificate on the SMTP-Client (switch) for succesfull connection between SSL to SMTP-AUTH server.
User Name field	Enter an SMTP username. Username can be up to 255 characters, including the following: • Alphabets, lower and upper case • Numbers • _(underscore) • .(period / dot) • -(hyphen)
Password field	Enter a password. Password can be up to 56 characters.

Step 10 Click **Save Changes**.

Configuring the Default Cisco TAC-1 Profile

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

Note In order to apply Callhome sendtestAlert functionality at least one of the email destination should be set for profiles other than CiscoTAC-1.

- 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 **Admin**.

Step 2 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 **Admin**.

Step 2 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 **Admin**.

Step 2 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:

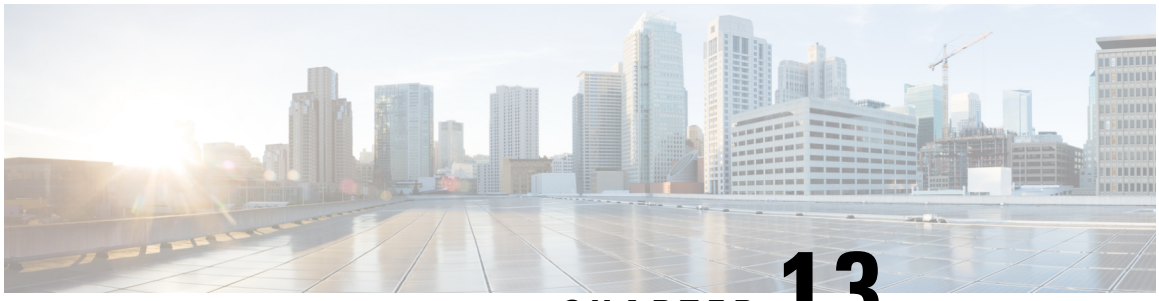
a) Click the link in the email.

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 13

Hardware Monitoring

- Monitoring a Fabric Interconnect, on page 99
- Monitoring a Blade Server, on page 100
- Monitoring a Rack-Mount Server, on page 102
- Monitoring an IO Module, on page 105
- Monitoring PCIe Node, on page 105
- Monitoring Crypto Cards, on page 106
- Monitoring NVMe PCIe SSD Devices, on page 107
- Health Monitoring, on page 111
- Management Interfaces Monitoring Policy, on page 113
- Local Storage Monitoring, on page 116
- Graphics Card Monitoring, on page 119
- Managing Transportable Flash Module and Supercapacitor, on page 122
- TPM Monitoring, on page 124

Monitoring a Fabric Interconnect

Procedure

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

Step 2 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.
Physical Ports tab	Displays the status of all ports on the fabric interconnect. This tab includes the following subtabs: • **Uplink Ports** tab

Option	Description
	• **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.
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.
Faults tab	Provides details of faults generated by the fabric interconnect.
Events tab	Provides details of events generated by the fabric interconnect.
Neighbors tab	Provides details about the LAN, SAN, and LLDP neighbors of the fabric interconnect. **Note** Enable **Info Policy** to view **Neighbors** details.
Statistics tab	Provides statistics about the fabric interconnect and its components. You can view these statistics in tabular or chart format.

Monitoring a Blade Server

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis 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 recover corrupt 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. • **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 each adapter installed in the server. • **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. • **Storage**—Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server. **Tip** If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the **Vendor** field. However, Cisco UCS Manager CLI displays ATA in the **Vendor** field and includes the vendor information, such as the vendor name, in a **Vendor Description** field. This second field does not exist in Cisco UCS Manager GUI.
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 other server components. You can also use this tab to update and activate the firmware on those components.
CIMC Sessions tab	Provides data about the CIMC sessions on 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.

Option	Description
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.
Health tab	Displays details about the health status of the server and its components.
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.

Step 5 In the **Navigation** pane, expand ***Server_ID*** > **Adapters** > ***Adapter_ID*** .

Step 6 In the **Navigation** pane, click on one or more of the following components of the adapter to open the navigator and view the status of the component:

-
- DCE interfaces
- HBAs
- NICs
- iSCSI vNICs

Tip
Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

Monitoring a Rack-Mount Server

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **Servers**.

Note
For Cisco UCS C125 M5 Servers, expand **Equipment** > **Rack Mounts** > **Enclosures** > **Rack Enclosure** ***rack_enclosure_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.
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 recover corrupt 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. • **CPU**—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 each adapter installed in the server. • **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 detailed 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. • **Storage**—Properties of the storage controller, the local disk configuration policy in the service profile associated with the server, and for each hard disk in the server. **Note** If the firmware of C-Series/S-Series servers is upgraded from Cisco UCSM release 2.2(6) to 3.1(2) or later release, the Platform Controller Hub (PCH) storage controller (along with the SSD boot drives) does not appear in UCSM GUI. **Tip** If the server contains one or more SATA devices, such as a hard disk drive or solid state drive, Cisco UCS Manager GUI displays the vendor name for the SATA device in the **Vendor** field. However, Cisco UCS Manager CLI displays ATA in the **Vendor** field and includes the vendor information, such as the vendor name, in a **Vendor Description** field. This second field does not exist in Cisco UCS Manager GUI.

Option	Description
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 other server components. You can also use this tab to update and activate the firmware on those components.
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.
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.

Step 5 In the **Navigation** pane, expand ***Server_ID*** > **Adapters** > ***Adapter_ID*** .

Step 6 In the **Work** pane, right-click one or more of the following components of the adapter to open the navigator and view the status of the component:

- Adapters
- DCE interfaces
- HBAs
- NICs

Tip
Expand the nodes in the table to view the child nodes. For example, if you expand a NIC node, you can view each VIF created on that NIC.

Monitoring an IO Module

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Click the module that you want to monitor.

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

Option	Description
General tab	Provides an overview of the status of the IO module, including a summary of any faults, a summary of the module properties, and a physical display of the module and its components.
Fabric Ports tab	Displays the status and selected properties of all fabric ports in the I/O module.
Backplane Ports tab	Displays the status and selected properties of all backplane ports in the module.
Faults tab	Provides details of faults generated by the module.
Events tab	Provides details of events generated by the module.
FSM tab	Provides details about and the status of FSM tasks related to the module. You can use this information to diagnose errors with those tasks.
Health tab	Provides details about the health status of the module.
Statistics tab	Provides statistics about the module and its components. You can view these statistics in tabular or chart format.

Monitoring PCIe Node

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **PICe Nodes**

Step 3 Select the node that you want to monitor.

Step 4 You can view the following details:

Name	Description
Name column	A navigation tree that allows you to view a particular component and its subcomponents. You can right-click a component to view any actions available for that component.
Slot ID column	Slot ID for the PCIe node in the server.
Model column	Cisco part number of the PCIe node.
Serial Number column	Specifies the serial number of the PCIe node.
Vendor column	The vendor ID of the PCIe node.
Presence column	The presence of the PCIe node, and whether it can be detected in the chassis. This can be one of the following: • Missing—No PCIe node can be detected in the chassis. • Equipped—A PCIe node can be detected in the chassis.

Monitoring Crypto Cards

Cisco Crypto Card Management for Blade Servers

The main function of Cisco Crypto Card is to provide hardware based encryption capability to UCS blade server for certain applications.

Cisco UCS Manager discovers the Crypto Card present in a blade server and displays the model, revision, vendor, serial number on the Equipment > Chassis > *Server_Number* > Inventory > Security subtab. Discovery of the Crypto Card fails if you add the Crypto Card to an unsupported blade server.

Cisco UCS Manager does not support firmware management for the Crypto Card.

Insertion and removal of a Crypto Card triggers deep discovery. Replacing the Crypto Card with another Crypto Card, Adaptor or Fusion I/O, or pass through card triggers deep discovery for commissioned servers. The following are the various Crypto Card replacement scenarios:

- Replacing a Crypto Card with another Crypto Card
- Replacing a Crypto Card with an adaptor
- Replacing a Crypto Card with a Fusion I/O
- Replacing a Crypto Card with a GPU card
- Replacing Crypto Card with a pass through card
- Replacing an adaptor with a Crypto Card
- Replacing a storage Mezzanine with a Crypto Card

- Replacing a GPU card with a Crypto Card

No cleanup is necessary for the downgrade of Cisco UCS Manager to an earlier version. If you upgrade UCS Manager after a downgrade, rediscovery of the card is necessary to inventory the card. For servers that do not support crypto cards, discovery proceeds uninterrupted.

Cisco UCS Manager discovers, associates, disassociates, and decommissions Crypto Cards.

Viewing Crypto Card Properties

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 On the **Work** pane, click the **Inventory** tab, then click the **Security** subtab.

Name	Description
ID field	
Slot ID field	Specifies the Slot ID where the Mezzanine card is placed.
Magma Expander Slot Id field	Specifies the ID number of the PCI slot.
Is Supported field	Specifies whether the card is supported.
Vendor field	Specifies the vendor of the card.
Model field	Specifies the model number of the card.
Serial field	Specifies the serial number of the card.
Firmware Version field	Specifies the Crypto card serial number.

Monitoring NVMe PCIe SSD Devices

NVMe PCIe SSD Storage Device Inventory

Cisco UCS Manager GUI discovers, identifies, and displays the inventory of Non-Volatile Memory Express (NVMe) Peripheral Component Interconnect Express (PCIe) SSD storage devices. You can view the health of the storage devices in the server. NVMe with PCIe SSD storage devices reduce latency, increase Input/Output Operations Per Second (IOPS), and lower power consumption compared to SAS or SATA SSDs.

The optional Intel VMD-enabled NVMe driver and Intel VMD-enabled LED Command line interface tool provide additional functionality by aggregating the NVMe PCIe SSD devices attached to its root port. This

enables Suprise hot-plug and allows optional configuration of LED blinking patterns on PCIe SSD storage attached to Intel VMD enabled domains.

Viewing NVMe PCIe SSD Storage Inventory

Procedure

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

Step 2 Expand **Equipment** > **Rack Mounts** > **Servers** > ***Server Number***.

Step 3 Click the **Inventory** tab.

Step 4 Do one of the following:

a) Click the **Storage** tab.

The list of NVMe PCIe SSD storage devices named **Storage Controller NVME *ID number*** is displayed. You can view the name, size, serial number, operating status, state and other details.

b) Click the NVMe PCIe SSD storage device.

The following inventory details are displayed:

Name	Description
Actions Area	
ID field	The NVMe PCIe SSD storage device configured on the server.
Description field	Brief description of the NVMe PCIe SSD storage device configured on the server.
Model field	The NVMe PCIe SSD storage device model.
Revision field	The NVMe PCIe SSD storage device revision.
Subtype field	The vendor name of the NVMe PCIe SSD storage device.
RAID Support field	Indicated whether the NVMe PCIe SSD storage device is RAID enabled.
OOB Interface Support field	Indicates if the NVMe PCIe SSD storage device supports out-of-band management .
PCIe Address field	The NVMe PCIe SSD storage device on the virtual interface card (VIC).

Name	Description
Number of Local Disks field	The number of disks contained in the NVMe PCIe SSD storage device.
Rebuild Rate field	The time it takes the storage device to rebuild RAID when a disk fails.
SubOemID	The OME ID for the NVMe PCIe SSD storage device on the virtual interface card (VIC).
Supported Strip Sizes field	The strip size supported by the NVMe PCIe SSD storage device.
Sub Device ID field	The sub device ID of the controller
Sub Ventor ID field	The sub vendor ID of the controller
Name field	The name of the controller.
PID field	The NVMe PCIe SSD storage device product ID, also known as product name, model name, product number
Serial field	The storage device serial number.
Vendor field	The vendor that manufactured the NVMe PCIe SSD storage device.
PCI Slot field	The PCI slot of the storage device.
Controller Status field	The current status of the controller as reported by CIMC. This can be one of the following: • Optimal—The controller is functioning properly. • Failed—The controller is not functioning. • Unresponsive—The CIMC is unable to communicate with the controller.
Pinned Cache Status field	The pin cache status of the storage device.

Name	Description
Default Strip Size field	The default strip size the storage device can support.
Device ID field	The ID of the storage device.
Vendor ID field	The ID of the manufacturer.
Security field	The device security applied to the storage device.
Embedded Storage Area	
Presence field	Whether the storage is embedded or not.
Operability field	The operable status of the device.
Block Size field	The memory of the device.
Size (MB) field	The fractional memory of the device in MB.
Connection Protocol field	The connection protocol followed.
Oper Qualified Reason	The operability reason of the device
Number of Blocks field	The number of memory blocks.
Firmware Area	
Boot-loader Version field	Displays the firmware version that is associated with the boot-loader software on the component.
Running Version field	The firmware version used by the component.
Package Version field	The firmware package version in which the firmware was included.
Startup Version field	The version of the firmware that takes effect the next time that the component reboots.

Name	Description
Activate Status field	This can be one of the following: • Ready—Activation succeeded and the component is running the new version. • Activating—The system is activating the new firmware version. • Failed—The firmware activation failed. For more information, double-click the failed component to view its status properties.

Health Monitoring

Monitoring CIMC Memory Usage for Blade, and Rack-Mount Servers

The Cisco Integrated Management Controller (CIMC) reports the following memory usage events for blade, and rack-mount servers:

- When memory falls below 1MB, CIMC has fatal memory usage. Reset is imminent.
- When memory falls below 5 MB, CIMC has extremely high memory usage.
- When memory falls below 10 MB, CIMC has high memory usage.

To view CIMC memory usage events:

Procedure

Do one of the following:

- **For Blade Servers**:
  a. On the **Equipment** tab, expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.
  b. Click ***Server_Number***.
  c. In the **Work** pane, click the **Health** tab.
- **For Rack-Mount Servers**:

a. On the **Equipment** tab, expand **Equipment** > **Rack-Mounts** > **Servers**.

b. Click ***Server_Number***.

c. In the **Work** pane, click the **Health** tab.

If CIMC reports two health events, one with major severity, the other with minor severity, the system raises a major severity fault and displays details under the **Health** tab **Management Services** subtab. Every health event does not translate to a fault. The highest severity health event translates to a fault. Faults appear under ***Server_Number*** > **Faults** tab.

Monitoring CMC Memory Usage for Input/Output Module and IFM (IOM for Cisco UCS X-Series Servers)

The Cisco Chassis Management Controller (CMC) reports memory usage events for IOMs and IFM (IOM for Cisco UCS X-Series Servers) and chassis.

The system raises a fault on the aggregation of reported health status.

To view CMC memory usage events:

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **IO Modules**.

Step 3 Click ***IO Module_Number***.

The **Health** tab **Management Services** subtab appears.

Every event does not translate to a fault. The highest severity events translate to fault. Faults appear under ***IO Module_Number*** > **Faults** tab.

Monitoring FEX Statistics

Cisco UCS Manager reports the following statistics for Cisco Fabric Extenders (FEXs) under the System Stats:

- Load
- Available Memory
- Cached Memory
- Kernel
- Total Memory
- Kernel Memory Free

Cisco 2200 Series and 2300 Series FEX support statistics monitoring.

All FEX stats are added to threshold policy as FexSystemStats where users can define their own thresholds.

Procedure

Step 1 On the **Equipment** tab, expand **Equipment** > **Rack Mounts** > **FEX** > ***FEX Number***.

The **Statistics** tab appears. You can view the statistics in tabular or chart format.

Step 2 Expand the **sys-stats** node to monitor FEX statistics.

Management Interfaces Monitoring Policy

The management interfaces monitoring policy defines how the mgmt0 Ethernet interface on the fabric interconnect is monitored. If Cisco UCS Manager 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.

When the management interface of a fabric interconnect which is currently the managing instance fails, Cisco UCS Manager first confirms if the status of the subordinate fabric interconnect is up. In addition, if there are no current failure reports logged against the fabric interconnect, Cisco UCS Manager modifies the managing instance for the endpoints.

If the affected fabric interconnect is currently the primary in a high availability setup, a failover of the management plane is triggered. This failover does not affect the data plane. You can set the following properties related to monitoring the management interface:

- The type of mechanism used to monitor the management interface.
- The interval at which the status of the management interface is monitored.
- The maximum number of monitoring attempts that can fail before the system assumes that the management is unavailable and generates a fault message.

Important When the management interface fails 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 **Admin**.

Step 2 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	Indicates whether the monitoring policy is enabled or disabled for the management interfaces.
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.

Name	Description
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.
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.

Name	Description
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 blade or rack server. This includes RAID controllers, physical drives and drive groups, virtual drives, RAID controller batteries (Battery Backup Unit), Transportable Flash Modules (TFM), supercapacitors, FlexFlash controllers, and SD cards.

Cisco UCS Manager communicates directly with the LSI MegaRAID controllers and FlexFlash controllers using an out-of-band 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, and information about the TFM.

  LSI storage controllers use a Transportable Flash Module (TFM) powered by a supercapacitor to provide RAID cache protection.
- Information on SD cards and FlexFlash controllers, including 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 CIMC reboot or build upgrades, the status, start time, and end times of operations running on the storage component may not be displayed correctly.

- Detailed fault information for all local storage components.

Note All faults are displayed on the **Faults** tab.

Support for Local Storage Monitoring

The type of monitoring supported depends upon the Cisco UCS server.

Supported Cisco UCS Servers for Local Storage Monitoring

Through Cisco UCS Manager, you can monitor local storage components for the following servers:

- Cisco UCS X410c M7 Compute Node
- Cisco UCS C220 M7 Server
- Cisco UCS C240 M7 Server
- Cisco UCS X210c M7 Compute Node
- Cisco UCS X210c M6 Compute Node
- Cisco UCS B200 M6 Server
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C480 M5 Server

Note Not all servers support all local storage components. For Cisco UCS rack servers, the onboard SATA RAID 0/1 controller integrated on motherboard is not supported.

Supported Cisco UCS Servers for Legacy Disk Drive Monitoring

Only legacy disk drive monitoring is supported through Cisco UCS Manager for the following servers:

- Cisco UCS B200 M1/M2 blade server
- Cisco UCS B250 M1/M2 blade server

Note In order for Cisco UCS Manager to monitor the disk drives, the 1064E storage controller must have a firmware level contained in a Cisco UCS bundle with a package version of 2.0(1) or higher.

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 server drive bay.
- The server must be powered on.
- The server must have completed discovery.
- The results of the BIOS POST complete must be TRUE.

Legacy Disk Drive Monitoring

Note The following information is applicable only for B200 M1/M2 and B250 M1/M2 blade servers.

The legacy disk drive monitoring for Cisco UCS provides Cisco UCS Manager with blade-resident disk drive status for supported blade servers in a Cisco UCS domain. Disk drive monitoring provides a unidirectional fault signal from the LSI firmware to Cisco UCS Manager to provide status information.

The following server and firmware components gather, send, and aggregate information about the disk drive status in a server:

- Physical presence sensor—Determines whether the disk drive is inserted in the server drive bay.
- Physical fault sensor—Determines the operability status reported by the LSI storage controller firmware for the disk drive.
- IPMI disk drive fault and presence sensors—Sends the sensor results to Cisco UCS Manager.
- Disk drive fault LED control and associated IPMI sensors—Controls disk drive fault LED states (on or off) and relays the states to Cisco UCS Manager.

Flash Life Wear Level Monitoring

Flash life wear level monitoring enables you to monitor the life span of solid state drives. You can view both the percentage of the flash life remaining, and the flash life status. Wear level monitoring is supported on the Fusion IO mezzanine card with the following Cisco UCS blade servers:

- Cisco UCS B200 M6 Server
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server

Note Wear level monitoring requires the following:

- Cisco UCS Manager must be at release 2.2(2a) or greater.
- The Fusion IO mezzanine card firmware must be at version 7.1.15 or greater.

Viewing the Status of Local Storage Components

Procedure

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

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Click the server for which you want to view the status of your local storage components.

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

Step 5 Click the **Storage** subtab to view the status of your RAID controllers and any FlexFlash controllers.

Step 6 Click the down arrows to expand the **Local Disk Configuration Policy**, **Actual Disk Configurations**, **Disks**, and **Firmware** bars and view additional status information.

RAID 0 Check Consistency Limitation

The Check Consistency operation is not supported for RAID 0 volumes. You must change the local disk configuration policy to run Check Consistency. For more information, see the *UCS Manager Server Management Guide,* Server Related Policies chapter, Changing a Local Disk Policy topic.

Graphics Card Monitoring

Graphics Card Server Support

With Cisco UCS Manager, you can view the properties for certain graphics cards and controllers. Graphics cards are supported on the following servers:

- Cisco UCS X210c M8 Compute Node
- Cisco UCS X215c M8 Compute Node
- Cisco UCS X410c M7 Compute Node
- Cisco UCS X210c M7 Compute Node
- Cisco UCS X210c M6 Compute Node
- Cisco UCS C240 M8 Server
- Cisco UCS C220 M8 Server
- Cisco UCS C245 M8 Server
- Cisco UCS C225 M8 Server
- Cisco UCS C240 M7 Server
- Cisco UCS C220 M7 Server
- Cisco UCS C240 M6 Server
- Cisco UCS C220 M6 Server
- Cisco UCS C245 M6 Server
- Cisco UCS C225 M6 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C220 M5 Server

- Cisco UCS B200 M6 Server
- Cisco UCS B480 M6 Server
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server

Note Certain NVIDIA Graphics Processing Units (GPU) do not support Error Correcting Code (ECC) and vGPU together. Cisco recommends that you refer to the release notes published by NVIDIA for the respective GPU to know whether it supports ECC and vGPU together.

GPU Mezzanine Graphics Module Management for Blade Servers

Cisco UCS Managerdiscovers the presence of the GPU Graphics Card in a blade server as a field replaceable unit and collects device inventory information, such as model, vendor, serial number, PCI slot and address, and firmware. Cisco UCS Manager displays GPU Card inventory on the Equipment > Chassis > *Server_Number* > Inventory > GPUs subtab.

GPU Card firmware management includes firmware upgrade and downgrade. Upgrade the GPU firmware through existing Cisco UCS Manager service profiles. Do not downgrade GPU firmware with older firmware versions, because cleanup is required.

Place the GPU Card in slot 2 of the blade server. GPU Card discovery fails if you is insert a card in an unsupported blade.

Replacing a GPU card triggers deep discovery for commissioned servers. The following are the various GPU card replacement scenarios that cause deep discovery:

- Replacing a GPU card with another GPU card
- Replacing a GPU card with an adaptor
- Replacing a GPU card with a storage Mezzanine
- Replacing an adaptor with a GPU card
- Replacing a storage Mezzanine with GPU card
- Replacing a GPU card with Crypto card
- Replacing a Crypto card with a GPU card

Cisco UCS Manager discovers, associates, disassociates, and decommissions GPU Graphics Cards. To view GPU Graphics Cards, see Viewing Graphics Card Properties, on page 121.

Note There is a maximum limit on the GPU Graphics Card memory (DIMMS) of 1 TB.

Viewing Graphics Card Properties

Procedure

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

Step 2 Do one of the following:

- Expand **Equipment** > **Chassis** > ***Chassis_Number*** > **Servers** > ***Server_Number***.
- Expand **Equipment** > **Rack-Mounts** > **Servers** > ***Server_Number***.

Step 3 On the **Work** pane, click the **Inventory** tab, then click the **GPU** subtab.

Name	Description
ID field	The unique ID for the graphics card.
PCI Slot field	The PCI slot number where the graphics card is installed.
Expander Slot ID field	The expander slot ID.
PID field	Product Identifier of the graphics card.
Is Supported field	Whether the graphics card is supported. This can be one of the following: • **Yes** • **No**
Vendor field	The name of the manufacturer.
Model field	The model number of the graphics card.
Serial field	The serial number of the component.
Running Version field	The firmware version of the graphics card.
Activate Status	Status of graphics card firmware activation: • **Ready**—Activation succeeded and the component is running the new version. • **Activating**—The system is activating the new firmware version. • **Failed**—The firmware activation failed. For more information, double-click the failed component to view its status properties.
Mode field	The mode of the configured graphics card. This can be one of the following: • **Compute** • **Graphic** • **Any Configuration**

Name	Description
Part Details	
Vendor ID field	The vendor ID of the graphics card.
Sub Vendor ID field	The sub vendor ID of the graphics card.
Device ID field	The device ID of the graphics card.
Sub Device ID field	The sub device ID of the graphics card.

Managing Transportable Flash Module and Supercapacitor

LSI storage controllers use a Transportable Flash Module (TFM) powered by a supercapacitor to provide RAID cache protection. With Cisco UCS Manager, you can monitor these components to determine the status of the battery backup unit (BBU). The BBU operability status can be one of the following:

- **Operable**—The BBU is functioning successfully.
- **Inoperable**—The TFM or BBU is missing, or the BBU has failed and needs to be replaced.
- **Degraded**—The BBU is predicted to fail.

TFM and supercap functionality is supported beginning with Cisco UCS Manager Release 2.1(2).

TFM and Supercap Guidelines and Limitations

Supported Cisco UCS Servers for TFM and Supercap

The following Cisco UCS servers support TFM and supercap:

- Cisco UCS X210c M8 Compute Node
- Cisco UCS X215c M8 Compute Node
- Cisco UCS X410c M7 Compute Node
- Cisco UCS X210c M7 Compute Node
- Cisco UCS X210c M6 Compute Node
- Cisco UCS C240 M8 Server
- Cisco UCS C220 M8 Server
- Cisco UCS C245 M8 Server
- Cisco UCS C225 M8 Server
- Cisco UCS C240 M7 Server
- Cisco UCS C220 M7 Server

- Cisco UCS B200 M6 Server
- Cisco UCS B200 M5 Server
- Cisco UCS B480 M5 Server
- Cisco UCS C220 M5 Server
- Cisco UCS C240 M5 Server
- Cisco UCS C480 M5 Server

Viewing the RAID Controller Stats

The following procedure shows how to see RAID controller stats for a server with PCIe\NVMe Flash Storage

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 In the **Equipment** pane, expand **Chassis** > ***Chassis Number*** > **Servers** > ***Server Number***.
Step 3 In the **Work** pane, click the **Inventory** tab.
Step 4 Click the **Storage** > **Controller** > **General** subtab to view the controller stats.

Monitoring RAID Battery Status

This procedure applies only to Cisco UCS servers that support RAID configuration and TFM. If the BBU has failed or is predicted to fail, you should replace the unit as soon as possible.

Procedure

Step 1 In the **Navigation** pane, click **Equipment**.
Step 2 In the **Equipment** pane, expand **Chassis** > ***Chassis Number*** > **Servers** > ***Server Number***.
Step 3 In the **Work** pane, click the **Inventory** tab.
Step 4 Click the **Storage** subtab to view the **RAID Battery (BBU)** area.

Viewing a RAID Battery Fault

Note This applies only to Cisco UCS servers that support RAID configuration and TFM.

Procedure

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

Step 2 In the **Equipment** pane, expand **Chassis** > ***Chassis Number*** > **Servers** > ***Server Number***.

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

Step 4 Select the battery to see more information on its condition.

TPM Monitoring

Trusted Platform Module (TPM) is included on all Cisco UCS M5 and higher blade and rack-mount servers. Operating systems can use TPM to enable encryption. For example, Microsoft's BitLocker Drive Encryption uses the TPM on Cisco UCS servers to store encryption keys.

Cisco UCS Manager enables monitoring of TPM, including whether TPM is present, enabled, or activated.

Viewing TPM Properties

Procedure

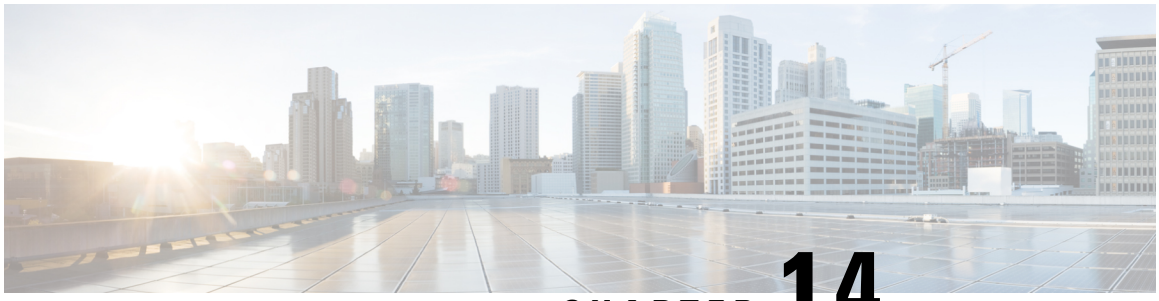
Step 1 In the **Navigation** pane, click **Equipment**.

Step 2 Expand **Equipment** > **Chassis** > ***Chassis Number*** > **Servers**.

Step 3 Choose the server for which you want to view the TPM settings.

Step 4 On the **Work** pane, click the **Inventory** tab.

Step 5 Click the **Motherboard** subtab.



CHAPTER 14

Traffic Monitoring

- Traffic Monitoring, on page 125
- Guidelines and Recommendations for Traffic Monitoring, on page 127
- Choosing Between Traffic Monitoring Sessions, on page 128
- Traffic Monitoring for SPAN, on page 128
- ERSPAN Truncation, on page 133
- Adding Traffic Sources to a Monitoring Session, on page 134
- Activating a Traffic Monitoring Session, on page 135
- Deleting a Traffic Monitoring Session, on page 136

Traffic Monitoring

Traffic monitoring copies traffic from one or more source ports 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).

Types of Traffic Monitoring Sessions

There are two types of monitoring sessions:

- Ethernet
- Fibre channel

The type of destination port determines what kind of monitoring session you need. For an Ethernet traffic monitoring session, the destination port must be an unconfigured physical port.

Traffic Monitoring Across Ethernet

An Ethernet traffic monitoring session can monitor any of the following traffic source and destination ports:

Source Ports	Destination Ports
• Uplink Ethernet port • Ethernet port channel • VLAN • Service profile vNIC • Service profile vHBA • FCoE port • Port channels • Unified uplink port • VSAN	Unconfigured Ethernet Port

Note 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 server port can be a source, only if it is a nonvirtualized rack server adapter-facing port.

- Cisco UCS 6300 Fabric Interconnect supports port-based mirroring.
- Cisco UCS 6300 Fabric Interconnect supports VLAN SPAN only in the Rx or the receive direction.
- Ethernet SPAN is port based on the Cisco UCS 6300 Fabric Interconnect.

Traffic Monitoring Across Fibre Channel

You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored with an Ethernet traffic monitoring session, at an Ethernet destination port, the destination traffic is FCoE.

A Fibre Channel traffic monitoring session can monitor any of the following traffic source and destination ports:

Source Ports	Destination Ports
• FC Port • FC Port Channel • Uplink Fibre Channel port • SAN port channel • VSAN • Service profile vHBA • Fibre Channel storage port	• Fibre Channel uplink port

Guidelines and Recommendations for Traffic Monitoring

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

Traffic Monitoring Sessions

A traffic monitoring session is disabled by default when created. To begin monitoring traffic, first activate the session. A traffic monitoring session must be unique on any fabric interconnect within the Cisco UCS pod. 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.

Maximum Number of Supported Active Traffic Monitoring Sessions Per Fabric-Interconnect

You can create and store up to 16 traffic monitoring sessions, but only four can be active at the same time. The receive and transmit directions each count as one monitoring session, while the bi-direction monitoring session is counted as 2. For example:

- Four active sessions — If each session is configured to monitor traffic in only one direction
- Two active sessions — If each session is configured to monitor traffic bidirectionally.
- Three active sessions — If one session is unidirectional and the second session is bidirectional.

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.

vNIC

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, create two sessions, one per fabric and connect two analyzers. Add the vNIC as the traffic source using the exact same name for both sessions. 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.

vHBA

A vHBA can be a source for either an Ethernet or Fibre Channel monitoring session, but it cannot be a source for both simultaneously. When a VHBA is set as the SPAN source, the SPAN destination only receives VN-Tagged frames. It does not receive direct FC frames.

Choosing Between Traffic Monitoring Sessions

From Cisco UCS Manager 4.3(4a), you can now choose between SPAN or ERSPAN traffic monitoring sessions.

Limitations

Note Existing SPAN limitations apply to ERSPAN too.

The following are the limitations when you choose between SPAN or ERSPAN traffic monitoring sessions:

- Session migration is not supported. You cannot change the session type from SPAN to ERSPAN or vice versa after it is created.
- ERSPAN does not share origin interface or VLAN configuration with Netflow.

  You cannot use the same source VLAN for both Netflow and ERSPAN.

Note IP addresses also cannot be shared with Netflow.

- You cannot enable span capturing control packets on ERSPAN sessions.

Traffic Monitoring for SPAN

Creating an Ethernet Traffic Monitoring Session

Procedure

Step 1 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 is saved.
Admin State field	Indicates 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.
Span Control Packets field	Indicates whether outgoing control packets that are sent from the CPU are monitored. This can be one of the following: • **Enabled**—Cisco UCS monitors outgoing control packets on the port. • **Disabled**—Cisco UCS does not monitor outgoing control packets on the port.
Destination drop-down list	The physical port that is being monitored. Click the link in this field to view the port properties.
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 2 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 **LAN**.

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 drop-down list	The physical port where you want to monitor all the communication from the sources.
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 **LAN**.

Step 2 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 a confirmation dialog box displays, click **Yes**.

Creating a Fibre Channel Traffic Monitoring Session

Procedure

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

Step 2 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 is saved.
Admin State field	Indicates 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.
Span Control Packets field	Indicates whether outgoing control packets that are sent from the CPU are monitored. This can be one of the following: • **Enabled**—Cisco UCS monitors outgoing control packets on the port. • **Disabled**—Cisco UCS does not monitor outgoing control packets on the port.
Destination drop-down list	Select the physical port where you want to monitor all the communication from the sources.
Admin Speed drop-down list	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. This can be one of the following: • **1 Gbps** • **10 Gbps** • **25 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 **SAN**.

Step 2 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 where you want to monitor all the communication from the sources.

Admin Speed drop-down list	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. This can be one of the following:
	• 4G HDFI
	  • **1 Gbps**
	  • **10 Gbps**
	  • **25GB Gbps**
	  • **Auto**
	• 5G
	  • **10 Gbps**
	  • **25 Gbps**
	  • **40 Gbps**
	  • **100 Gbps**

Step 6 Click **OK**.

Clearing the Destination for an Existing Fibre Channel Traffic Monitoring Session

Procedure

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

Step 2 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 a confirmation dialog box displays, click **Yes**.

ERSPAN Truncation

Beginning with Cisco UCS Manager 4.3(4a), you can configure the truncation of source packets for each ERSPAN session based on the size of the maximum transmission unit (MTU). Truncation helps to decrease ERSPAN bandwidth by reducing the size of monitored packets. Any ERSPAN packet that is larger than the configured MTU size is truncated to the given size. For ERSPAN, an additional ERSPAN header is added to the truncated packet from 54 to 166 bytes depending on the ERSPAN header type. For example, if you configure the MTU as 300 bytes, the packets are replicated with an ERSPAN header size from 354 to 466 bytes depending on the ERSPAN header type configuration.

ERSPAN truncation is disabled by default. To use truncation, you must enable it for each ERSPAN session.

Configuring ERSPAN Truncation

You can configure truncation for ERSPAN source sessions only.

Note By default, the ERSPAN session forwards the entire packets (9216 jumbo packets).

This procedure describes how to truncate the MTU size:

Before you begin

Enable packet truncation for an ERSPAN.

Procedure

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

Step 2 Expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

Step 3 In the **Traffic Monitoring Sessions** window, click **Add**.

Step 4 Choose the **ERSPAN Source** radio button to configure the ERSPAN source session.

Step 5 Check the **Enable Packet Truncation** check box to enable packet truncation for an ERSPAN.

Step 6 In the **Maximum Transmission Unit** field, enter the maximum transmission unit.

Note
This field is displayed only when **Enable Packet Truncation** is enabled. The MTU size range is from 64 to 1518 bytes. The maximum allowed size is 1518 bytes.

Step 7 Click **OK**.

Viewing or Modifying an ERSPAN Truncation

Procedure

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

Step 2 Expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

Step 3 Expand **Fabric_Interconnect_Name** and select the ERSPAN traffic monitor session.

Step 4 In the **General** tab, under the **Properties** area, you can view or modify the **Maximum Transmission Unit**.

Step 5 In the **Maximum Transmission Unit** field, modify the maximum transmission unit.

Note
This field is displayed only when **Enable Packet Truncation** is enabled. The MTU size range is from 64 to 1518 bytes. The maximum allowed size is 1518 bytes.

Step 6 Click **Save Changes** to save the configuration change.

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 **LAN**.

Step 2 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 **LAN**.

Step 2 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 **LAN**.

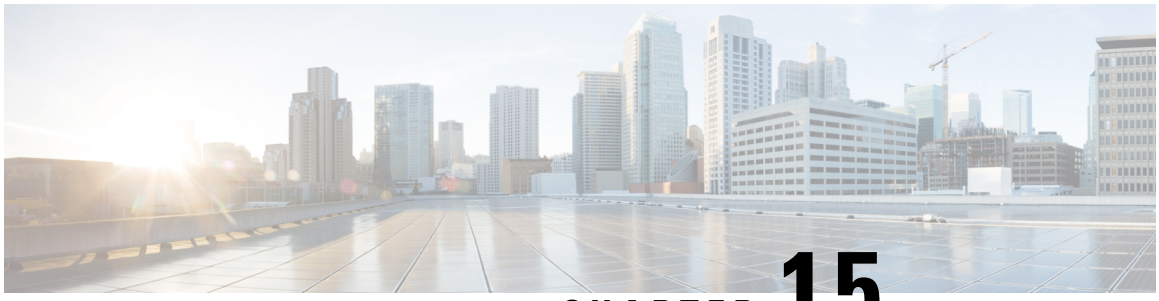
Step 2 Expand **LAN** > **Traffic Monitoring Sessions** > ***Fabric_Interconnect_Name***.

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 a confirmation dialog box displays, click **Yes**.



CHAPTER 15

NetFlow Monitoring

- NetFlow Monitoring, on page 137
- NetFlow Limitations, on page 138
- Enabling NetFlow Monitoring, on page 139
- Creating a Flow Record Definition, on page 139
- Viewing Flow Record Definitions, on page 140
- Defining the Exporter Profile, on page 141
- Creating a Flow Collector, on page 141
- Creating a Flow Exporter, on page 142
- Creating a Flow Monitor, on page 143
- Creating a Flow Monitor Session, on page 144
- Associating a Flow Monitor Session to a vNIC, on page 145

NetFlow Monitoring

NetFlow is a standard network protocol for collecting IP traffic data. NetFlow enables you to define a flow in terms of unidirectional IP packets that share certain characteristics. All packets that match the flow definition are collected and exported to one or more external NetFlow Collectors, where they can be further aggregated, analyzed, and used for application-specific processing.

Cisco UCS Manager uses NetFlow-capable adapters (Cisco UCS Cisco UCS VIC 1300 series, Cisco UCS VIC 1400 series, Cisco UCS VIC 14000 series, and Cisco UCS VIC 15000 series) to communicate with the routers and switches that collect and export flow information.

NetFlow monitoring is supported on Cisco UCS 6400, 6500, 6600, and Cisco UCS X-Series DirectFabric Interconnects.

Network Flows

A flow is a set of unidirectional IP packets that have common properties such as, the source or destination of the traffic, routing information, and protocol used. Flows are collected when they match the definitions in the flow record definition.

Flow Record Definitions

A flow record definition contains information about the properties used to define the flow, which can include both characteristic properties or measured properties. Characteristic properties, also called flow keys, are the

properties that define the flow. Cisco UCS Manager supports IPv4, IPv6, and Layer 2 keys. Measured characteristics, also called flow values or non-keys, measurable values such as the number of bytes contained in all packets of the flow, or the total number of packets.

A flow record definition is a specific combination of flow keys and flow values. The two types of flow record definitions are:

- **System-defined**—Default flow record definitions supplied by Cisco UCS Manager.
- **User-defined**—Flow record definitions that you can create yourself.

Flow Exporters, Flow Exporter Profiles, and Flow Collectors

Flow exporters transfer the flows to the flow connector based on the information in a flow exporter profile. The flow exporter profile contains the networking properties used to export NetFlow packets. The networking properties include a VLAN, the source IP address, and the subnet mask for each fabric interconnect.

Note In the Cisco UCS Manager GUI, the networking properties are defined in an exporter interface that is included in the profile. In the Cisco UCS Manager CLI, the properties are defined in the profile.

Flow collectors receive the flows from the flow exporter. Each flow collector contains an IP address, port, external gateway IP, and VLAN that defines where the flows are sent.

Flow Monitors and Flow Monitor Sessions

A flow monitor consists of a flow definition, one or two flow exporters, and a timeout policy. You can use a flow monitor to specify which flow information you want to gather, and where you want to collect it from. Each flow monitor operates in either the egress or ingress direction.

A flow monitor session contains up to four flow monitors: two flow monitors in the ingress direction and two flow monitors in the egress direction. A flow monitor session can also be associated with a vNIC.

NetFlow Limitations

The following limitations apply to NetFlow monitoring:

- NetFlow monitoring is supported on Cisco UCS VIC 1300, 1400, 14000, and 15000 series adapters. On Cisco UCS VIC 1200 series adapters, NetFlow is not recommended with FCoE traffic.
- For Cisco UCS 6664 Fabric Interconnect, Cisco UCS Fabric Interconnects 9108 100G, Cisco UCS 6500 series, and Cisco UCS 6400 Series Fabric Interconnects:
  - Netflow monitoring includes both host receive and transmit directions. The NetFlow monitoring session applied to the Host Receive Direction Monitor will enable both transmit and receive monitoring, while NetFlow monitoring session applied to the Host Transmit Direction Monitor is a NO-OP.
  - Vethernet interface netflow monitor will always have **NFM_RECORD_L2_SRC_VLAN** enabled.
  - **Active Timeout** and **Inactive Timeout** values in **Flow Timeout Policy** cannot be modified.
- You can have up to 64 flow record definitions, flow exporters, and flow monitors.

- NetFlow is not supported in vNIC template objects.
- PVLANs and local VLANs are not supported for service VLANs.
- All VLANs must be public and must be common to both fabric interconnects.
- VLANs must be defined as an exporter interface before they can be used with a flow collector.
- You cannot use NetFlow with usNIC, Virtual Machine Queue, Virtual Machine Multiple Queues, RoCE, SRIOV, Geneve, or Linux ARFS enabled vNIC.
- Enabling NetFlow Monitoring does not allow you to downgrade Cisco UCS Manager software. To downgrade, disable Netflow Monitoring feature.

Enabling NetFlow Monitoring

You must enable NetFlow monitoring for the feature to work.

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Netflow Monitoring**.
Step 3 Click the **General** tab.
Step 4 In the **Admin State** field, click the **Enabled** radio button to enable NetFlow monitoring.
Step 5 Click **Save Changes** to save the configuration change.

Creating a Flow Record Definition

Procedure

Step 1 In the **Navigation** pane, click **LAN**.
Step 2 Expand **LAN** > **Netflow Monitoring**.
Step 3 Right-click **Flow Record Definitions** and choose **Create Flow Record Definition**.
Step 4 In the **Create Flow Record Definition** dialog box, complete the following fields:

Field	Description
Name	The name of the flow record definition. 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 is saved.

Field	Description
Description	The user-defined description of the flow record definition.
Keys	Choose the radio button for the key that you want to use. This can be one of the following: • **IPv4**—Populates the selection window with IPv4 keys. • **IPv6**—Populates the selection window with IPv6 keys. • **Layer 2 Switched**—Populates the selection window with Layer 2 keys. Check the check boxes for the properties to be included for the flow.
Measured Properties	Check the check box for the nonkey fields to be included for the flow. This can be one or more of the following: • **Counter Bytes Long** • **Counter Packets Long** • **Sys Uptime First** • **Sys Uptime Last**

Step 5 Click **OK**.

Viewing Flow Record Definitions

Procedure

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

Step 2 Expand **LAN** > **Netflow Monitoring**.

Step 3 Choose **Flow Record Definitions** to view the list of all flow definitions.

Step 4 Double-click the name of a flow definition to view the properties for the selected flow definition.

On the **Properties** window, you can modify the keys and non-keys used for the flow.

Defining the Exporter Profile

Procedure

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

Step 2 Expand **LAN** > **Netflow Monitoring** > **Flow Exporters** > **Flow Exporter Profiles**.

Step 3 Click **Flow Exporter Profile default**.

Step 4 In the Properties area, to the side of the Exporter Interface(s) table, click **Add**.

Step 5 In the **Create Exporter Interface** dialog box, complete the following fields:

Name	Description
VLAN	Choose the VLAN that you want to associate with the exporter interface, or click **Create VLANs** to create a new one. PVLAN and local VLANs are not supported. All VLANs must be public and must be common to both fabric interconnects.
Fabric A Source IP	The source IP for the exporter interface on fabric A. **Important** Make sure the IP address you specify is unique within the Cisco UCS domain. IP address conflicts can occur if you specify an IP address that is already being used by Cisco UCS Manager.
Fabric A Subnet Mask	The subnet mask for the exporter interface on fabric A.
Fabric B Source IP	The source IP for the exporter interface on fabric B. **Important** Make sure the IP address you specify is unique within the Cisco UCS domain. IP address conflicts can occur if you specify an IP address that is already being used by Cisco UCS Manager.
Fabric B Subnet Mask	The subnet mask for the exporter interface on fabric B.

Step 6 Click **OK**.

Creating a Flow Collector

Procedure

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

Step 2 Expand **LAN** > **Netflow Monitoring**.

Step 3 In the **Work** pane, click the **Flow Collectors** tab.

Step 4 Click **Add** at the side of the **Flow Collectors** table.

Step 5 In the **Create Flow Collectors** dialog box, complete the following fields:

Name	Description
Name	The name of the flow collector. 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 is saved.
Description	The user-defined description of the flow collector.
Collector IP	The IP address for the flow collector.
Port	The port for the flow collector. Enter a value between 1 and 65535.
Exporter Gateway IP	The external gateway IP for the flow collector.
VLAN	The VLAN associated with the flow collector. VLANs must be defined in the **Create Exporter Interface** dialog box before they can be used with a flow collector.

Step 6 Click **OK**.

Creating a Flow Exporter

Procedure

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

Step 2 Expand **LAN** > **Netflow Monitoring**.

Step 3 Right-click **Flow Exporters** and choose **Create Flow Exporter**.

Step 4 In the **Create Flow Exporter** dialog box, complete the following fields:

Name	Description
Name	The name of the flow exporter. 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 is saved.
Description	The user-defined description of the flow exporter.

Name	Description
DSCP	The differentiated services codepoint (DSCP) value. The range of values is from 0 and 63.
Version	The exporter version. By default, this is version 9.
Exporter Profile	The exporter profile that you want to associate with the flow exporter.
Flow Collector	Choose the flow collector that you want to associate with the flow exporter, or click **Create Flow Exporter** to create a new one.
Template Data Timeout	The timeout period for resending NetFlow template data. Enter a value between 1 and 86400.
Option Exporter Stats Timeout	The timeout period for resending NetFlow flow exporter data. Enter a value between 1 and 86400.
Option Interface Table Timeout	The time period for resending the NetFlow flow exporter interface table. Enter a value between 1 and 86400.

Step 5 Click **OK**.

Creating a Flow Monitor

Procedure

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

Step 2 Expand **LAN** > **Netflow Monitoring**.

Step 3 Right-click **Flow Monitors** and choose **Create Flow Monitor**.

Step 4 In the **Create Flow Monitor** dialog box, complete the following fields:

Name	Description
Name	The name of the flow monitor. 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 is saved.
Description	The user-defined description of the flow monitor.
Flow Definition	Choose the flow definition that you want to use from the list of values, or click **Create Flow Record Definition** to create a new one.

Name	Description
Flow Exporter 1	Choose the flow exporter that you want to use from the list of values, or click **Create Flow Exporter** to create a new one.
Flow Exporter 2	Choose the flow exporter that you want to use from the list of values, or click **Create Flow Exporter** to create a new one.
Timeout Policy	The timeout policy that you want to use from the list of values.

Step 5 Click **OK**.

Creating a Flow Monitor Session

Procedure

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

Step 2 Expand **LAN** > **Netflow Monitoring**.

Step 3 Right-click **Flow Monitor Sessions** and choose **Create Flow Monitor Session**.

Step 4 In the **Create Flow Monitor Session** dialog box, complete the following fields:

Name	Description
Name	The name of the flow monitor 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 is saved.
Description	The user-defined description of the flow monitor session.
Host Receive Direction Monitor 1	Choose the flow monitor that you want to use from the list of values, or click **Create Flow Monitor** to create a new one.
Host Receive Direction Monitor 2	Choose the flow monitor that you want to use from the list of values, or click **Create Flow Monitor** to create a new one.
Host Transmit Direction Monitor 1	Choose the flow monitor that you want to use from the list of values, or click **Create Flow Monitor** to create a new one.
Host Transmit Direction Monitor 2	Choose the flow monitor that you want to use from the list of values, or click **Create Flow Monitor** to create a new one.

Step 5 Click **OK**.

Associating a Flow Monitor Session to a vNIC

Procedure

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

Step 2 Expand **LAN** > **Netflow Monitoring** > **Flow Monitor Sessions**.

Step 3 Click the flow monitor session that you want to associate.

Step 4 Click **Flow Exporter Profile default**.

Step 5 In the **Properties** area, expand **vNICs**.

Step 6 Click **Add** at the side of the table.

Step 7 In the **Add Monitoring Session Source** dialog box, choose the vNIC that you want to associate with the flow monitor session.

Step 8 Click **OK** to close the dialog box.

Step 9 Click **Save** to close the dialog box.