Cisco UCS Central Administration Guide, Release 1.4

First Published: 2015-12-17

Last Modified: 2016-12-12

Last Modified: 2017-04-05

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

CONTENTS

Preface

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

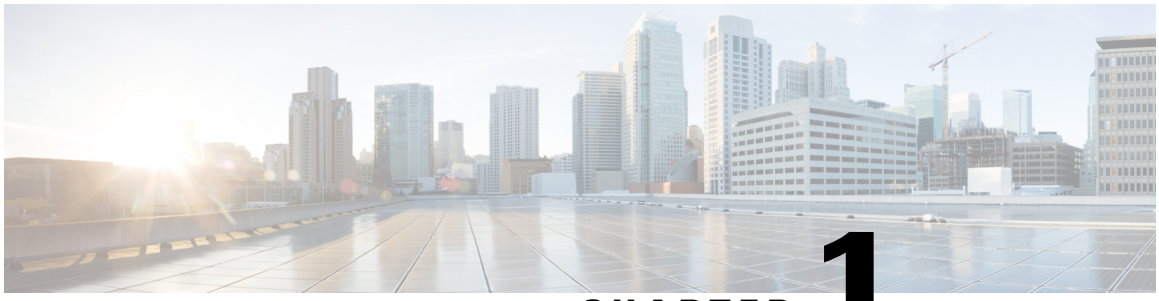
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

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

Documentation Feedback

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



CHAPTER 1

Overview

Overview

This guide contains conceptual and procedural information on the following components that are intrinsic to Cisco UCS Central administrative settings:

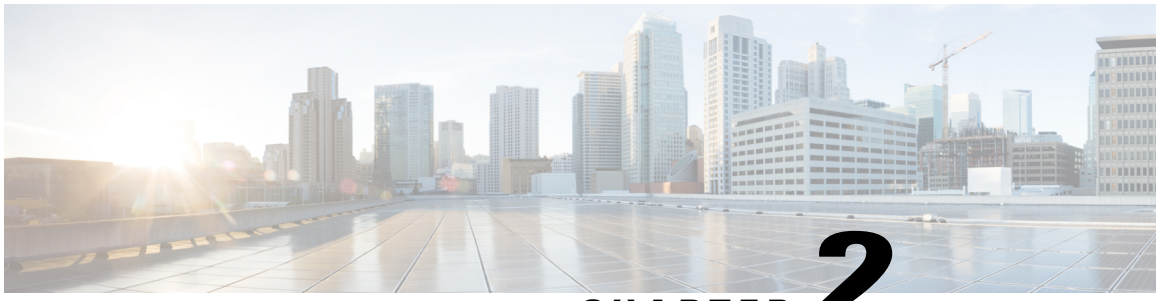
- User Management
- System Management
- Firmware Management
- Backup Management
- Smart Call Home

Cisco UCS Central User Documentation Reference

Beginning with Release 1.4, the Cisco UCS Central user guide has been divided into several use case-based documents. You can use the appropriate guide to understand and configure Cisco UCS Central.

Guide	Description
Cisco UCS Central Getting Started Guide	Provides a brief introduction to the Cisco UCS infrastructure, Cisco UCS Manager, and Cisco UCS Central. Includes an overview of the HTML5 UI, how to register Cisco UCS domains in Cisco UCS Central, and how to activate licenses.
Cisco UCS Central Administration Guide	Provides information on administrative tasks, such as user management, communication, firmware management, backup management, and Smart Call Home.

Guide	Description
Cisco UCS Central Authentication Guide	Provides information on authentication tasks, such as passwords, users and roles, RBAC, TACACS+, RADIUS, LDAP, and SNMP.
Cisco UCS Central Server Management Guide	Provides information on server management, such as equipment policies, physical inventory, service profiles and templates, server pools, server boot, and server policies.
Cisco UCS Central Storage Management Guide	Provides information on storage management, such as ports and port channels, VSAN and vHBA management, storage pools, storage policies, storage profiles, disk groups, and disk group configuration.
Cisco UCS Central Network Management Guide	Provides information on network management, such as ports and port channels, VLAN and vNIC management, network pools, and network policies.



CHAPTER 2

User Management

This chapter includes the following sections:

Managing UCS Central Users

From the **Manage UCS Central Users Administration** dialog box, you can configure users, roles, locales, and password profiles

Step 1 From the System Settings icon, choose **Users**.
This launches the **Manage UCS Central Users Administration** dialog box.

Step 2 Click the icon for the section that you want to configure.

- The **Password Profile** section allows you to perform the same tasks as the **Manage UCS Central Password Profile** dialog box. For more information, see Managing UCS Central Password Profile, on page 4.
- The **Roles** section allows you to perform the same tasks as the **Manage UCS Central Roles** dialog box. For more information, see Managing UCS Central Roles, on page 4.
- The **Locales** section allows you to perform the same tasks as the **Manage UCS Central Locales** dialog box. For more information, see Managing UCS Central Locales, on page 5.
- The **Local Users** section allows you to perform the same tasks as the **Manage UCS Central Local Users** dialog box. For more information, see Managing UCS Central Local Users, on page 5.
- The **Remote Users** section allows you to perform the same tasks as the **Manage UCS Central Remote Users** dialog box. For more information, see Managing UCS Central Remote Users, on page 6.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Managing UCS Central Password Profile

Step 1 In the Task bar, type **Manage UCS Central Password Profile** and press Enter.
This launches the **Manage UCS Central Password Profile** dialog box.

Step 2 In **Password Profile**, choose whether to enable **Password Strength Check**.

Step 3 Select the minimum number of passwords before a previous password can be reused.

Step 4 Choose whether to enable **Password Change During Interval**.

Step 5 Select the **Password Change Interval**.

Step 6 Select the maximum number of passwords during the change interval.
This field is only visible if **Password Change During Interval** is set to **Enabled**.

Step 7 Click **Save**.

Related Topics

Managing UCS Central Roles, on page 4
Managing UCS Central Locales, on page 5
Managing UCS Central Local Users, on page 5
Managing UCS Central Remote Users, on page 6

Managing UCS Central Roles

Step 1 In the Actions bar, type **Manage UCS Central Roles** and press Enter.
This launches the **UCS Central Roles Manage** dialog box.

Step 2 In **Roles**, click + to create a new role, or select an existing role.

Step 3 In the **Network** tab, click + to update and add privileges.

Step 4 Select relevant privileges for the role.

Step 5 Click ✓ to apply the new privileges.

Step 6 Update the **Storage**, **Server**, and **Operations** privileges for the role, in the same manner.

Step 7 Click **Save**.

Related Topics

Managing UCS Central Password Profile, on page 4
Managing UCS Central Locales, on page 5
Managing UCS Central Local Users, on page 5
Managing UCS Central Remote Users, on page 6

Managing UCS Central Locales

Step 1 In the Task bar, type **Manage UCS Central Locales** and press Enter.
This launches the **UCS Central Locales Manage** dialog box.

Step 2 In **Locales**, click + to add a new locale, or select an existing one.

Step 3 Assign **Organizations** and/or **Domain Groups** to the locale.

a) Click + to display the organizations or domain groups.
b) Select the organizations or domain groups.
c) Click ✓ to apply the new privileges.

Step 4 Click **Save**.

Related Topics

Managing UCS Central Password Profile, on page 4
Managing UCS Central Roles, on page 4
Managing UCS Central Local Users, on page 5
Managing UCS Central Remote Users, on page 6

Managing UCS Central Local Users

Step 1 In the Actions bar, type **Manage UCS Central Local Users** and press Enter.
This launches the **UCS Central Local Users Manage** dialog box.

Step 2 In **Local Users**, click + to create a new local user, or select an existing one.

Step 3 In the **Basic** tab, complete the necessary information for the user.

Step 4 In the **Roles** tab, add or remove the roles assigned to the user.

a) Click + to display the roles.
b) Select a role or roles.
c) Click ✓ to apply the new privileges.

Step 5 In the **Locales** tab, add or remove the locales assigned to the user.

a) Click + to display the roles.
b) Select a role or roles.
c) Click ✓ to apply the new privileges.

Step 6 In the **SSH** tab, select the **Authentication Type**.

Step 7 Click **Save**.

Related Topics

Managing UCS Central Password Profile, on page 4
Managing UCS Central Roles, on page 4
Managing UCS Central Locales, on page 5
Managing UCS Central Remote Users, on page 6

Managing UCS Central Remote Users

Step 1 In the Actions bar, type **Manage UCS Central Remote Users** and press Enter.
This launches the **UCS Central Remote Users Manage** dialog box.

Step 2 In **Remote Users**, review the remote LDAP users, roles, and locales.

Note This section is read-only.

Step 3 Click **Cancel** to close the window, or **Save** to save any changes made in other sections.

Related Topics

Managing UCS Central Password Profile, on page 4
Managing UCS Central Roles, on page 4
Managing UCS Central Locales, on page 5
Managing UCS Central Local Users, on page 5

Managing Domain Group Users

Step 1 Click **Domain Group** > **root**.

Step 2 Click **Settings** > **Users**.

Step 3 In **Roles**, select roles to associate them with the domain group. Uncheck roles to disassociate them from the domain group.

Step 4 In the **Network** tab, click + to update and add privileges.

a) Click + to display the organizations.
b) Select relevant privileges for the role.
c) Click ✓ to apply the new privileges.

Step 5 Update the **Storage**, **Server**, and **Operations** privileges for the role, in the same manner.

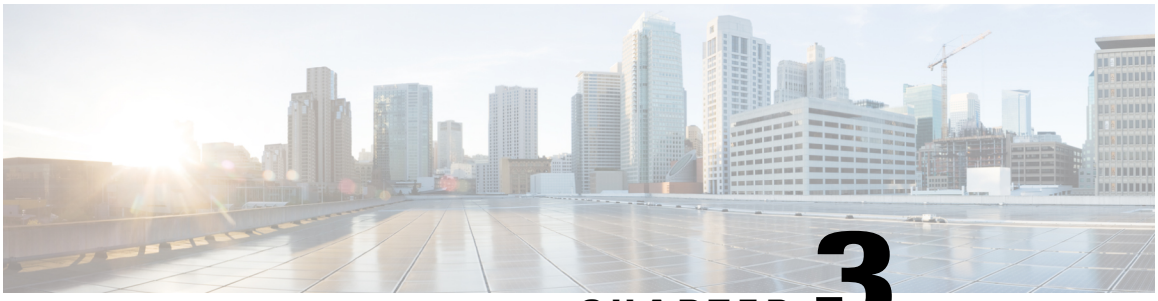
Step 6 In **Locales**, select locales to associate them with the domain group. Uncheck roles to disassociate them from the domain group.

Step 7 Assign **Organizations** to the locale.

a) Click + to display the organizations.

b) Select the organizations or domain groups.
c) Click ✓ to apply the new privileges.

Step 8 Click **Save**.



CHAPTER 3

Firmware Management

Firmware Management

In Cisco UCS Central, you can manage all firmware components for all registered Cisco UCS domains. The status of all firmware updates displays under the **Domains** section:

- **Firmware Ready—**The firmware has been successfully updated.
- **In Progress—**The firmware update is currently in progress.
- **Pending User Ack—**Requires user acknowledgment on the **Alerts** > **Pending Activities** page before it updates the firmware.

Note To manage Cisco UCS domains firmware from Cisco UCS Central, enable the global firmware management option in Cisco UCS Manager. You can enable the global firmware management option when you register Cisco UCS Manager with Cisco UCS Central. You can also turn global management option on or off based on your management requirements.

The Cisco UCS domains are categorized into domain groups in Cisco UCS Central for management purposes. You can manage firmware for each domain group separately, at the domain group level, or for all domain groups from the domain group root. Cisco UCS Central provides the option to manage the following Cisco UCS domain firmware packages:

- **Capability Catalog—**One capability catalog per domain group. All Cisco UCS domains registered to a particular domain group use the capability catalog defined in the domain group.
- **Infrastructure Firmware—**One infrastructure firmware policy per domain group. All Cisco UCS domains registered to a particular domain group use the same Infrastructure firmware version defined in the domain group.

Image Library

The Image Library in Cisco UCS Central displays a list of all firmware images downloaded into the Cisco UCS Central local and remote file systems from Cisco.com.

- The **Packages** tab displays all firmware packages.
- The **Downloads**tab allows you to monitor the status of your downloads.

These firmware images are available for creating firmware policies.

From here you can:

- Delete any downloaded image from the image library by selecting the image and clicking the Delete icon.

Note If the firmware image you are trying to delete is referenced in a scheduled policy, the delete operation fails. You cannot delete this policy from the image library.

- Sync firmware images with images on Cisco.com by clicking the [flash] icon.

Importing Firmware Bundle

Make sure you have downloaded the firmware bundle from Cisco.com and saved it either in your local desktop or in a supported remote file system.

Step 1 On the menu bar, click the **Operations** icon and select **Firmware**.

Step 2 On the Firmware page, click the **Operations** icon and select **Import Firmware Bundle**.
This launches the **Import Firmware Bundle** dialog box.

Step 3 If you have a BIN file containing the firmware bundle in your local system,

a) In **FW Bundle Location** click **Local**.
b) In the **File Name** field, click the file icon to open your local browser.
c) From the file location, select the BIN file and click **Import**.

Step 4 If you have the firmware bundle in a remote file system,

Note Make sure you have the Hostname, User name and Password for the remote file system.

a) In **FW Bundle Location** click **Remote**.
This displays supported file transfer protocols.

b) Select one of the options from where you want to import files, enter the required information in the fields, and click **Import**.
For example, if you want to use the BIN file `ucs-k9-bundle-infra.2.2.3a.A.bin` on the remote server, you would enter the absolute path /home/cisco-ucs-central/firmware/ucs-k9-bundle-infra.2.2.3a.A.bin

What to Do Next

Add the firmware bundle to the appropriate policies and perform the upgrade.

Once the upgrade has been completed, you can delete the firmware bundle from Cisco UCS Central, but you must remove it from all associated policies first.

Enabling Automatic Firmware Update Sync-ups from Cisco.com

You must have a valid Cisco.com username and password to access the updated firmware bundles on Cisco.com.

Step 1 In the Task bar, type **Sync Firmware Updates from Cisco.com** and press Enter.
This launches the **Sync Firmware Updates from Cisco.com** dialog box.

Step 2 Enter your Cisco.com username and password in the appropriate fields.

Step 3 If you want Cisco UCS Central to automatically download new firmware updates:

a) Click **Enable** in the **Sync FW Updates Periodically** field.

b) Select the desired frequency in the **Frequency** field.

Note If you select **On Demand** in this field, Cisco UCS Central does not automatically download new firmware updates. Instead, you must download them manually using the **Sync** button in this dialog box.

Step 4 If you want your system to be able to access Cisco.com via HTTP, select **Enabled** in the **HTTP Proxy To Access Cisco.com** field and enter the HTTP connection information in the appropriate fields.

Note This functionality requires that Cisco UCS Central has network access to Cisco.com. Please enable and apply the proxy server configuration as appropriate.

Step 5 Click **Sync**.

Scheduling Infrastructure Firmware Update for a Cisco UCS Domain Group

You can schedule an infrastructure firmware update for all domains in a domain group.

Step 1 In the Task bar, type **Schedule Infra Firmware Update - Classic** and press Enter.
This launches the **Schedule Infra Firmware Update - Classic** dialog box.

Step 2 Select the domain group in the **Domain Group for UCS Infra Update** drop-down list.
Cisco UCS Central displays the number of domains that will be impacted by the firmware upgrade, and the Cisco UCS Manager version(s) on those domains.

Step 3 Select the firmware version you want to use in the **UCS Infra Update Version** drop-down list.

Step 4 (Optional) Select the catalog version in the **Catalog Version** drop-down list.

Step 5 Select the maintenance window in the **FW Update Maintenance Window** field.

Step 6 Select whether any server reboots require user acknowledgment in the **User Acknowledgement Required To Install** field.

- **Enabled—**A user must manually acknowledge the reboot request before any domain in the selected domain group is rebooted.
- **Disabled—**The domains in the selected domain group will be automatically rebooted as needed during the update.

Step 7 Click **Schedule**.
You can monitor the firmware update on the **Firmware** page. See Firmware Management, on page 9.

Removing an Infrastructure Firmware Schedule for a Cisco UCS Domain Group

Step 1 In the Task bar, type **Remove Infra Firmware Schedule - Classic** and press Enter.
This launches the **Remove Infra Firmware Schedule - Classic** dialog box.

Step 2 Select the domain group in the **Domain Group for UCS Infra Update** drop-down list.
Cisco UCS Central automatically populates the **UCS Infra Update Version**, **Catalog Version**, and **FW Update Maintenance Window** fields.

Step 3 Click **Remove**.

Creating or Editing a Host Firmware Package Policy

Step 1 In the Task bar, type **Create Host Firmware Package Policy** and press Enter.
This launches the **Create Host Firmware Package Policy** dialog box.

Step 2 On the **Basic** tab, click **Organization** and select the location in which you want to create the policy.

Step 3 Enter a **Name** and optional **Description**.
The policy name is case sensitive.

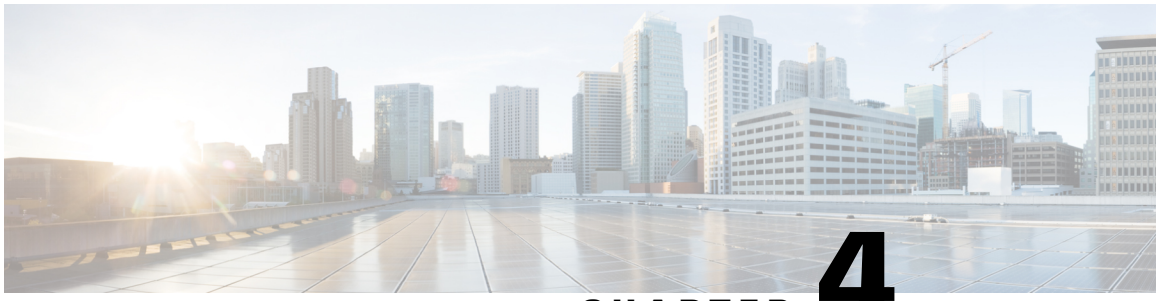
Step 4 Select the **Blade Version**, **Rack Version**, and/or **Modular Version** of the firmware, as required for your environment.

Step 5 In the **Components** tab, click the **Plus** icon to select any components that you would like to exclude from the firmware update.
The included and excluded components are displayed.

Note Excluding components is not supported for registered domains on Cisco UCS Manager release 2.2.6 or earlier.

Step 6 To remove an excluded component, select the check box for the component and click the **Trash** icon.

Step 7 Click **Create**.



CHAPTER 4

System Management

System Policies

You can configure the system policies for all of Cisco UCS Central, or at the domain group level. To configure system policies at the domain group, see Domain Group System Policies, on page 21.

UCS Central system policies include the following:

- **Faults—**Allows you to determine 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).
- **Syslog—**Allows you to determine the type of log files that you want to collect, and where you want to view them or store.
- **Core Dump—**Uses the Core File Exporter to export core files as they occur.

Configuring UCS Central System Policies

From the **Manage UCS Central System Policies** dialog box, you can configure the properties and settings for faults, syslog, and core dump export.

Step 1 From the System Settings icon, choose **System Policies**.
This launches the **Manage UCS Central System Policies** dialog box.

Step 2 Click the icon for the section that you want to configure.

- The **Fault** section allows you to perform the same tasks as the **Manage UCS Central Fault Policy** dialog box. For more information, see Managing a UCS Central Fault Policy, on page 16.
- The **Syslog** section allows you to perform the same tasks as the **Manage UCS Central Syslog** dialog box. For more information, see Managing UCS Central Syslog, on page 17.
- The **Core Dump Export** section allows you to perform the same tasks as the **Manage UCS Central Core Dump Export** dialog box. For more information, see Managing UCS Central Core Dump Export, on page 19.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Related Topics

Managing a UCS Central Fault Policy, on page 16
Managing UCS Central Syslog, on page 17
Managing UCS Central Core Dump Export, on page 19

Managing Equipment Policies

Step 1 Click the **Domain Group Navigation** icon and choose a domain group.

Step 2 Click the **Configuration** icon and choose **System Policies**.

Step 3 In **Equipment**, click **Basic** and complete the following fields:

a) In **Rack Management Action**, select how server management is configured when a new rack server is discovered:

- **Auto Acknowledged**—Cisco UCS automatically configures server management by domain based on the available server connections.
- **User Acknowledged**—Cisco UCS does not automatically configure server management. It waits until acknowledged by the user.

b) In **MAC Address Table Aging Time**, select the length of time an idle MAC address remains in the MAC address table before it is removed:

- **Mode Default—**System uses the default value. For end-host mode, the default is 14,500 seconds. For switching mode, the default is 300 seconds.
- **Never—**Cisco UCS never removes MAC addresses from the table.
- **Other—**Enter a custom value in the dd:hh:mm:ss field.

c) In **VLAN Port Count Optimization**, select whether Cisco UCS can logically group VLANs to optimize the use of ports and reduce the CPU load on the FI.

d) In **Firmware Auto Server Sync State**, select the firmware synchronization policy for recently discovered blade servers or rack servers:

- **User Acknowledged—**Cisco UCS does not synchronize firmware until the administrator acknowledges the upgrade.
- **No Actions—**Cisco UCS does not perform any firmware upgrade on the server.

e) In **Info Action**, select whether the information policy displays the uplink switches that are connected to the Cisco UCS domain.

Step 4 Click **Discovery** and complete the fields to specify how you want the system to behave when you add a new chassis or FEX:

a) In **Chassis/FEX Link Action**, select the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.

b) In **Chassis/FEX Link Grouping Preference**, select whether the links from the system IO controllers, IOMs, or FEXes to the fabric interconnects are grouped in a port channel.

c) In the **Multicast Hardware Hash**, click **Enable** to specify if Cisco UCS can use all of the links from the IOMs or FEXes to the fabric interconnects for multicast traffic.

d) In the **Backplane Speed Preference**, choose the speed that you want to use.

Step 5 Click **Power** and complete the following fields:

a) In **Power Redundancy**, select the power redundancy policy that you want to use:

- **N+1—**The total number of power supplies, plus one additional power supply for redundancy, equally share the power load for the chassis. If any additional power supplies are installed, Cisco UCS sets them to a "turned-off" state.
- **Grid—**Two power sources are turned on, or the chassis requires greater than N+1 redundancy. If one source fails, the surviving power supplies continue to provide power to the chassis.
- **Non-Redundant—**All installed power supplies are turned on and the load is evenly balanced. Only power small configurations (requiring less than 2500W) by a single power supply.

b) In **Power Allocation**, select the power allocation management mode used in the Cisco UCS domain:

- **Policy Driven Chassis Group Cap—**Configures power allocation at the chassis level through power control policies included in the associated service profiles.
- **Manual Blade Level Cap—**Configures power allocation on each individual blade server in all chassis.

c) In **ID Soaking Interval**, specify the number of seconds Cisco UCS Central waits before reassigning a pool entity that Cisco UCS released. Enter an integer between 0 and 86400.

Step 6 Click **Save**.

Managing Rack Discovery Policies

Step 1 Navigate to the root **Domain Group** page.

Step 2 Click the **Settings** icon and select **System Profile**.

Step 3 In **Rack Discovery**, click **Basic**.

Step 4 In **Discovery Policy Action**, select how you want the system to behave when you add a new rack server.

- **User Acknowledged—**Cisco UCS domain waits until the user tells it to search for new servers.
- **Immediate—**Cisco UCS domain attempts to discover new servers automatically.

Step 5 Click **Policies** and select the scrub policy to run on a newly discovered server.
The server must meet the criteria in the selected server pool policy qualification.

Step 6 Click **Save**.

Managing a UCS Central Fault Policy

Step 1 In the Task bar, type **Manage UCS Central Fault Policy** and press Enter.
This launches the **Manage UCS Central Fault Policy** dialog box.

Step 2 In **Fault**, complete the following fields:

Note The **Initial Severity** and **Action on Acknowledgment** fields are read-only, and cannot be modified.

1 Enter a time in seconds in the **Flapping Interval (Seconds)** field.

Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, Cisco UCS Central 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 **Action on Clear** field.

2 In **Soaking Interval**, choose None, or select a custom soaking interval.

3 In **Clear Interval**, select whether Cisco UCS Central should automatically mark faults as cleared based on their age.

If you choose **None**, faults are not automatically cleared. If you choose **Custom Interval**, Cisco UCS automatically clears fault messages after the length of time you specify in the associated interval field.

4 In **Action on Clear**, select the action the system must take when a fault is cleared.

If you choose **Retain Cleared Faults**, then the cleared faults are retained for the length of time specified in the **Retention Interval**. If you choose **Delete Cleared Faults**, then the cleared faults are deleted immediately.

5 If **Action on Clear** is set to **Retain Cleared Faults**, then in **Retention Interval** specify the length of time Cisco UCS retains a fault that is marked as cleared.

If you choose **Forever**, Cisco UCS retains all cleared fault messages regardless of how old they are. If you choose **Custom Interval**, Cisco UCS retains cleared fault messages for the length of time you specify in the associated interval field.

Step 3 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 14
Managing UCS Central Syslog, on page 17
Managing UCS Central Core Dump Export, on page 19

Managing UCS Central Syslog

Step 1 In the Task bar, type **Manage UCS Central Syslog** and press Enter.
This launches the **Manage UCS Central Syslog** dialog box.

Step 2 In **Syslog Sources**, choose **Enabled** for each source for which you want to collect log files.
This can be one of the following:

- **Faults**
- **Audits**
- **Events**

Step 3 In **Local Destination**, specify where the syslog messages can be added and displayed. This can be one of the following:

- **Console—**If enabled, syslog messages are displayed on the console as well as added to the log. Choose the logging level for the messages you would like displayed.
- **Monitor—**If enabled, syslog messages are displayed on the monitor as well as added to the log. Choose the logging level for the messages you would like displayed.
- **Log File—**If enabled, syslog messages are saved in the log file. If disabled, syslog messages are not saved. Choose the logging level, a file name, and the maximum file size.

Select the lowest message level that you want the system to store. The system stores that level and above. The logging levels can be one of the following:

- **Critical (UCSM Critical)**
- **Alert**
- **Emergency**
- **Error (UCSM Major)**
- **Warning (UCSM Minor)**
- **Notification (UCSM Warning)**
- **Information**
- **Debug**

Step 4 In **Remote Destination**, specify whether to store the syslog messages in a primary, secondary, and/or tertiary server. Specify the following information for each remote destination:

- **Logging Level—**Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following:
  - **Critical (UCSM Critical)**
  - **Alert**
  - **Emergency**
  - **Error (UCSM Major)**
  - **Warning (UCSM Minor)**
  - **Notification (UCSM Warning)**
  - **Information**
  - **Debug**
- **Facility—**The facility associated with the remote destination.
- **Host Name/IPAddress—**The hostname or IP address on which the remote log file resides. If you are using a host name rather than a IPv4 or IPv6 address, you must configure the DNS server in Cisco UCS Central.

Step 5 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 14
Managing a UCS Central Fault Policy, on page 16
Managing UCS Central Core Dump Export, on page 19

Managing UCS Central Core Dump Export

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

Step 1 In the Task bar, type **Manage UCS Central Core Dump Export** and press **Enter**.
This launches the **Manage UCS Central Core Dump Export** dialog box.

Step 2 Click **Enable** to export core files.

Step 3 (Optional) Enter a description for the remote server used to store the core file.

Step 4 The **Frequency**, **Maximum No. of Files**, **Remote Copy**, and **Protocol** fields are set by default.

Step 5 (Optional) In **Absolute Remote Path**, enter the path to use when exporting the core file to the remote server.

Step 6 In **Remote Server Host Name/IP Address**, enter a hostname or IP address to connect with via TFTP

Step 7 (Optional) In **TFTP Port**, enter the port number to use when exporting the core file via TFTP. The default port number is 69.

Step 8 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 14
Managing a UCS Central Fault Policy, on page 16
Managing UCS Central Syslog, on page 17

System Profile

The system profile allows you to configure the system information such as the interfaces, date and time, DNS, remote access, trusted points, and certificate information for all of Cisco UCS Central.

To configure the domain group system profile, see Domain Group System Profile, on page 22.

Managing the UCS Central System Profile

Step 1 From the System Settings icon, choose **System Profile**.
This launches the **Manage UCS Central System Profile** dialog box.

Step 2 In the **UCS Central** section, you can view the **UCS Central System Name**, **Mode**, and virtual IPv4 and IPv6 addresses. These values are populated when you first configure Cisco UCS Central. The system name and mode cannot be modified.

Step 3 In **Interfaces**, review or change the following management nodes:

- **Primary Node (IPv4)**
- **Primary Node (IPv6)**

- **Secondary Node (IPv4)**
- **Secondary Node (IPv6)**

Step 4 In **Date & Time**, choose the time zone and add an NTP server.

Step 5 In **DNS**, type the Cisco UCS Central domain name and add a DNS server.

Step 6 In **Remote Access**, choose a Key Ring.

Step 7 In **Trusted Points**, click **Add** to add a new trusted point and certificate chain.

Step 8 In **Certificates**, you can view the existing, or create a new key ring and certificate request.

Step 9 Click **Save**.

Related Topics

Managing the UCS Central NTP Servers, on page 20
Managing the UCS Central Management Node, on page 20
Managing the UCS Central DNS Servers, on page 21

Managing the UCS Central Management Node

Step 1 In the Task bar, type **Manage UCS Central Management Node** and press Enter.
This launches the **Manage UCS Central Management Node** dialog box.

Step 2 In **Management Node**, click the name of the node you would like to configure.

Step 3 Enter values for the **IP Address**, **Subnet Mask**, and **Default Gateway**.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 19
Managing the UCS Central NTP Servers, on page 20
Managing the UCS Central DNS Servers, on page 21

Managing the UCS Central NTP Servers

Step 1 In the Task bar, type **Manage UCS Central NTP Servers** and press Enter.
This launches the **Manage UCS Central NTP Servers** dialog box.

Step 2 In **Time Zone**, select the time zone for the domain.

Step 3 In **NTP Servers**, click **Add** to add a new NTP server, or **Delete** to remove an existing one.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 19
Managing the UCS Central Management Node, on page 20
Managing the UCS Central DNS Servers, on page 21

Managing the UCS Central DNS Servers

Step 1 In the Task bar, type **Manage UCS Central DNS Servers** and press Enter.
This launches the **Manage UCS Central DNS Servers** dialog box.

Step 2 In **UCS Central Domain Name**, type the name of the Cisco UCS Central domain.

Step 3 In **DNS Servers**, click **Add** to add a new DNS server, or **Delete** to remove an existing one.

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 19
Managing the UCS Central NTP Servers, on page 20
Managing the UCS Central Management Node, on page 20

Domain Group System Policies

You can configure the system policies at the domain group level, or for all of Cisco UCS Central. To configure system policies for UCS Central, see System Policies, on page 13.

Domain group system policies include the following:

- **Equipment—**Allows you to set policies for the equipment in your domain group, including discovery and power policies.
- **Rack Discovery—**Allows you to determine what action is taken when a rack-mount server is discovered, and assign a scrub policy.
- **Fault—**Allows you to determine 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).
- **Syslog—**Allows you to determine the type of log files that you want to collect, and where you want to view them or store.

- **Core Dump—**Uses the Core File Exporter to export core files as they occur.
- **Interfaces—**Allows you to set criteria for monitoring your domain group interfaces.
- **System Events—**Allows you to set the criteria for domain group system event logs.

Managing Domain Group System Policies

Note If you are setting the system policies for a sub-domain, you need to enable each policy before you can set it.

Step 1 Navigate to the root **Domain Group** page.

Step 2 Click the **Settings** icon and select **System Profile**.

Step 3 In **Equipment**, complete the necessary fields.
For more information, see Managing Equipment Policies, on page 14.

Step 4 In **Rack Discovery**, complete the necessary fields.
For more information, see Managing Rack Discovery Policies, on page 16.

Step 5 In **Fault**, complete the necessary fields.
For more information, see Managing a UCS Central Fault Policy, on page 16.

Step 6 In **Syslog**, complete the necessary fields.
For more information, see Managing UCS Central Syslog, on page 17.

Step 7 In **Core Dump**, complete the necessary fields.
For more information, see Managing UCS Central Core Dump Export, on page 19.

Step 8 In **Interfaces**, choose whether to enable **Interface Monitoring Policy**.

Step 9 If you select **Enabled**, complete the interface monitoring information as required.

Step 10 In **System Events**, complete the necessary fields to determine how the system event logs will be collected.

Step 11 Click **Save**.

Domain Group System Profile

The domain group system profile allows you to configure the date and time, DNS settings, remote access, and trusted points for each domain group.

To configure the system profile for Cisco UCS Central, see System Profile, on page 19.

Managing the Domain Group System Profile

Step 1 Navigate to the root **Domain Group** page.
Step 2 Click the **Settings** icon and select **System Profile**.
Step 3 In **Date & Time**, choose the time zone and add an NTP server.
Step 4 In **DNS**, type the UCS Central domain name and add a DNS server.
Step 5 In **Remote Access**, type the HTTPS, HTTPS Port, and choose a Key Ring.
Step 6 In **Trusted Points**, click **Add** to create a trusted point and add a certificate chain.
Step 7 Click **Save**.

Maintenance Policy

When you make any change to a service profile that is associated with servers in the registered domains, the change may require a server reboot. The maintenance policy determines how Cisco UCS Central reacts to the reboot request.

You can create a maintenance policy and specify the reboot requirements to make sure the server is not automatically rebooted with any changes to the service profiles. You can specify one of the following options for a maintenance policy:

- **Immediately**: Whenever you make a change to the service profile, apply the changes immediately.
- **User Acknowledgment**: Apply the changes after a user with administrative privileges acknowledges the changes in the system.
- **Schedule**: Apply the changes based on the day and time you specify in the schedule.

When you create the maintenance policy if you specify a schedule, the schedule deploys the changes in the first available maintenance window.

Note A maintenance policy only prevents an immediate server reboot when a configuration change is made to an associated service profile. However, a maintenance policy does not prevent the following actions from taking place right away:

- Deleting an associated service profile from the system
- Disassociating a server profile from a server
- Directly installing a firmware upgrade without using a service policy
- Resetting the server

Creating or Editing a Maintenance Policy

To watch a video on creating a maintenance policy and associating it with a service profile, see Video: Creating a Global Maintenance Policy and Associating the Policy with a Service Profile.

Step 1 In the Task bar, type **Create Maintenance Policy** and press Enter.
This launches the **Create Maintenance Policy** dialog box.

Step 2 Click **Organization** and select the location in which you want to create the policy.

Step 3 Enter the **Name** and optional **Description**.
The name is case sensitive.

Step 4 Select when to apply the changes that require a reboot.
This can be one of the following:

- **User Acknowledgement—**Configuration changes must be acknowledged by the user, and reboots must be confirmed.
- **Schedule—**Configuration changes are applied depending on the schedule you select. To add a new schedule to the list of values, see Creating or Editing a Schedule, on page 24.
- **Save—**Configuration changes are applied immediately on save and cause a reboot.

Step 5 Choose whether to apply the changes on the next reboot, and ignore the selection in the **Apply Changes On** field.

Step 6 Click **Create**.

Creating or Editing a Schedule

Note Simple schedules, whether recurring or a one time occurrence, do not have the option to require user acknowledgment. If you want to require user acknowledgment, you must choose an advanced schedule.

Step 1 In the Task bar, type **Create Schedule** and press Enter.
This launches the **Create Schedule** dialog box.

Step 2 In **Basic**, enter a **Name** and optional **Description**.

Step 3 Choose whether the schedule should be **Recurring**, **One Time**, or **Advanced**.
If **Advanced**, choose whether to require user acknowledgment.

Step 4 In **Schedule**, complete the following:

a) For **Recurring** schedules, select the start date, frequency, time, and other properties.
b) For **One Time** schedules, select the start date, time, and other properties.

c) For **Advanced** schedules, enter a name for the schedule, choose whether to use a one time or recurring schedule, and select values for the other properties.

Step 5 Click **Create**.

Key Rings

Cisco UCS Central allows creation of key rings as a third party certificate for stronger authentication. HTTPS uses components of the Public Key Infrastructure (PKI) to establish secure communications between two devices.

Each PKI device holds a pair of asymmetric Rivest-Shamir-Adleman (RSA) encryption keys, one kept private and one made public, stored in an internal key ring. A message encrypted with either key can be decrypted with the other key. To send an encrypted message, the sender encrypts the message with the receiver's public key, and the receiver decrypts the message using its own private key. A sender can also prove its ownership of a public key by encrypting (also called 'signing') a known message with its own private key. If a receiver can successfully decrypt the message using the public key in question, the sender's possession of the corresponding private key is proven. Encryption keys can vary in length, with typical lengths from 2048 bits to 4096 bits. In general, a longer key is more secure than a shorter key. Cisco UCS Central provides a default key ring with an initial 2048-bit key pair, and allows you to create additional key rings.

Note If you regenerate the default key ring, logging into Cisco UCS Central after the regeneration might take a few minutes.

The default key ring certificate must be manually regenerated if the cluster name changes or the certificate expires.

Note When you create a key ring and certificate request, Cisco UCS Central generates the certificate request with required key usages set. The Key usages on certificate signed from a CA server should include **SSL Client Authentication**, and **SSL Server Authentication** . If you use Microsoft Windows Enterprise Certification Authority Server as Internal CA, you need to use the **Computer** template to generate the certificate, which will have both of these key usages set. If this template is not available in your setup, you need to use appropriate template which has both **SSL Client Authentication**, and **SSL Server Authentication** key usages set.

Creating a Key Ring

Step 1 On the menu bar, click **System Profile**.
Step 2 Click **Certificates** and complete all the fields.
Step 3 Click **OK**.
Step 4 Click **Save**.

Creating a Trusted Point

Cisco UCS Central allows you to create a trusted point containing the certificate of the root certificate authority (CA) and a subordinate CA in a bundled format. The root CA must contain a primary and self-signed certificate.

Step 1 On the menu bar, click **System Profile**.
Step 2 Click**Trusted Points**.
Step 3 In **Trusted Points**, click the + icon and complete all the fields.
Step 4 Click **OK**.
Step 5 Click **Save**.

Fault and Log Monitoring

Cisco UCS Central allows you to view fault logs, audit logs, sessions and other events.

Note If the screen or widget that you are viewing is not current, click the refresh icon to see the latest data.

System Faults

Cisco UCS Central collects and displays all the Cisco UCS Central system faults on the **Fault Logs** page. To view these system fault logs, click the **Alerts** icon and select **System Faults**. The **Faults Logs** page displays information on the type and severity level of the fault, and allow you to monitor and acknowledge the system faults, and filter the faults that are displayed.

The faults table includes the following information for each fault:

- **Code—**The ID associated with the fault

- **Timestamp—**Date and time at which the fault occurred
- **Type—**Origin of the fault
- **Cause—**Cause of the fault
- **Affected Object—**The component that is affected by this fault
- **Fault Details—**The details of the fault.
- **Severity—**The severity of the fault
- **Action—**Any action required by the fault

To manage the information that is collected, see Configuring UCS Central System Policies, on page 14.

UCS Domain Faults

Cisco UCS Central collects and displays faults from registered Cisco UCS domains in the UCS Domain **Faults Log** page. The faults are displayed by type and severity level. You can click on the fault type to expand and view the exact Cisco UCS domains where the faults have occurred. The UCS domain fault logs are categorized and displayed as follows:

- **Fault Level—**The fault level that triggers the profile. This can be one of the following:
  - **Critical—**Critical problems exist with one or more components. These issues should be researched and fixed immediately.
  - **Major—**Serious problems exist with one or more components. These issues should be researched and fixed immediately.
  - **Minor—**Problems exist with one or more components that might adversely affect the system performance. These issues should be researched and fixed as soon as possible before they become major or critical issues.
  - **Warning—**Potential problems exist with one or more components that might adversely affect the system performance if they are allowed to continue. These issues should be researched and fixed as soon as possible before they get worse.
  - **Healthy—**No fault in any of the components in a domain.
  - **Unknown—**No fault in any of the components in a domain.
- **No Of Domains—**The number of domains where the faults have occurred of each severity level.
- **Domain—**The domain where the faults have occurred. Click a type to see the Cisco UCS domains that have one or more faults of that type and the details of the fault.
- **Critical—**The number of critical faults of the selected type in the Cisco UCS domain.
- **Major—**The number of major faults of the selected type in the Cisco UCS domain.
- **Minor—**The number of minor faults of the selected type in the Cisco UCS domain.
- **Warning—**The number of warning faults of the selected type in the Cisco UCS domain.

This table is displayed only when you select a domain from the **UCS Domain Faults** page.

- **Filter—**Allows you to filter the data in the table.
- **ID—** The unique identifier associated with the fault.
- **Timestamp—**The day and time at which the fault occurred.
- **Type—** Information about where the fault originated.
- **Cause—** A brief description of what caused the fault.
- **Affected Object—**The component that is affected by this issue.
- **Fault Details—**More information about the log message.
- **Severity—**Displays an icon denoting the fault severity. The icon key appears below the table.

Event Logs

Cisco UCS Central collects and displays the events that occurred in the system, such as when a user logs in or when the system encounters an error. When such events occur, the system records the event and displays it in the **Event Logs**. To view these event logs, click the **Alerts** icon from the menu bar, and select **Events**. The event logs record information on the following:

- **ID—**Unique identifier associated with the event that caused the fault
- **Timestamp—**Date and time at which the event occurred
- **Trig. By—**Type of user associated with the event
- **Affected Object—**The component that is affected by the event

Audit Logs

You can view a comprehensive list of configuration changes in Cisco UCS Central in the **Audit Logs**. When you perform configuration changes involving creating, editing or deleting tasks in the Cisco UCS Central GUI or the Cisco UCS Central CLI, Cisco UCS Central generates an audit log. In addition to the information related to configuration, the audit logs record information on the following:

- Resources that were accessed.
- Date and time at which the event occurred.
- Unique identifier associated with the log message.
- The user who triggered an action to generate the audit log. This can be an internal session or an external user who made a modification using the Cisco UCS Central GUI or the Cisco UCS Central CLI.
- The source that triggered the action.
- The component that is affected.

Core Dumps

If an error occurs that causes the system to crash, then a core dump file is created. This core dump file includes information of the state of the system before the error occurred, and the time at which the system crashed. To view the core dump files, click the **Alerts** icon on the menu bar and select **Core Dumps**. In the **Core Dumps** log table you can view the following information:

- **Timestamp—**When the core dump file was created.
- **Name—**The full name of the core dump file.
- **Description—**The type of core dump file.

Active Sessions

You can view active sessions for remote and local users in Cisco UCS Central and choose to terminate those sessions from the server. To view the active sessions, click the **Alerts** icon on the menu bar and select **Sessions**. In the **Active Sessions** log table you can view the following information:

- **ID—**The type of terminal from which the user logged in.
- **Timestamp—**Date and time at which the user logged in.
- **User—**The user name.
- **Type—**The type of terminal from which the user logged in.
- **Host—**The IP address from which the user logged in.
- **Status—**Whether the session is currently active.
- **Actions—**Click **Terminate** to end the selected session.

Internal Services

Internal service logs provide information on various providers and the version of the Cisco UCS Central associated with the provider. To view the internal services, click the **Alerts** icon on the menu bar and select **Sessions**.

In the **Services** section of the **Internal Services** page, you can view the following information:

- **Name—**The type of the provider.
- **Last Poll—**Day and time on which Cisco UCS Central last polled the provider.
- **IP Address—**The IP address associated with the provider.
- **Version—**The version of Cisco UCS Central associated with the provider.
- **Status—**The operational state of the provider.

In the **Clean Up** section of the **Internal Services** page, you can view the following information:

- **Domain—**The domain name.

- **Last Poll—**Day and time on which Cisco UCS Central last polled the provider.
- **Lost Visibility—**When Cisco UCS Central lost visibility to the provider.
- **Clean Up—**Click **Clean Up** to remove all references of this Cisco UCS domain from Cisco UCS Central.

Note The domain must be re-registered with Cisco UCS Central before it can be managed again by Cisco UCS Central.

Enabling Tomcat Logging

SUMMARY STEPS

1. UCSC # **scope monitoring**
2. UCSC /monitoring # **scope sysdebug**
3. UCSC /monitoring/sysdebug # **scope mgmt-logging**
4. UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]

DETAILED STEPS

	Command or Action	Purpose
Step 1	UCSC # **scope monitoring**	Enters monitoring mode.
Step 2	UCSC /monitoring # **scope sysdebug**	Enters sysdebug mode.
Step 3	UCSC /monitoring/sysdebug # **scope mgmt-logging**	Enters management logging mode.
Step 4	UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit**	**debug0**	**debug1**	**debug2**	**debug3**	**debug4**	**info**	**major**	**minor**	**warn**]	Sets the logging level.

The following example shows how to set tomcat logging to level debug 4.

```
UCSC # scope monitoring
UCSC /monitoring # scope sysdebug
UCSC /monitoring/sysdebug # scope mgmt-logging
UCSC /monitoring/sysdebug/mgmt-logging # set module tomcat_config debug4
UCSC /monitoring/sysdebug/mgmt-logging #
```

API Communication Reports

Cisco UCS Central, 1.4 enables you to generate reports on active API communication between the GUI and back-end from the Cisco UCS Central GUI. You can collect these communications for use in third party automation. You can start and stop collecting this report at any time during an active communication.

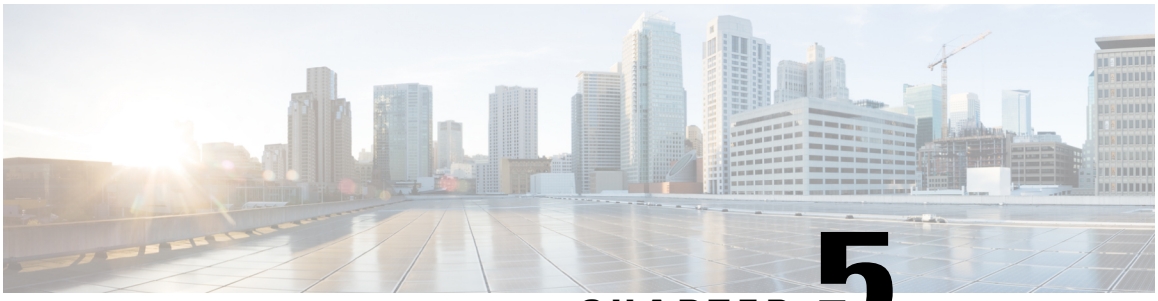
- After you stop logging the session, the report is available for you as text file from the GUI. If you want to use the file at a later time, make sure to save the file in your local desktop.
- If you log out or your sessions expires while recording is in progress, the text file is not generated.

Generating API Communication Reports

Step 1 On the menu bar, click **Operations** icon and select **Start Logging Session**.
Systems starts logging the active API communication between the Cisco UCS Central GUI and the back-end.

Step 2 On the menu bar, click **Operations** icon and select **Stop Logging Session**.
A pop-up dialog box displays the option to Open or Save the API report text file.

Step 3 Select your choice and click **OK** to open or save the file.



CHAPTER 5

Backup Management

Backup and Restore

Cisco UCS Central enables you to backup and restore Cisco UCS Central and the registered UCS domains. You can schedule a backup and restore policy or you can perform an immediate on demand backup of Cisco UCS Central or a selected domain.

From the **Backup & Restore** page, you can schedule a full state backup for Cisco UCS Central and the registered Cisco UCS Domains. For Cisco UCS domains, you can also create the full state backup policy locally.

Scheduled backup policies are disabled by default. If you want to backup Cisco UCS Central or the registered UCS domains, you must enable the backup state for both. The backup process does not interrupt or impact any server or network traffic. You can perform a backup while the domain is up and running. The backup operation saves information from the management plane.

Remotely configured policies are restricted to use the Cisco UCS Central repository for backups which is internally mounted by Cisco UCS Manager.

When you schedule a regular backup, the backup repository can start accumulating data. To manage the backup archives, you can specify the maximum number of backup versions that are saved. Use policy specifications to indicate the number of backups to maintain for each Cisco UCS domain.

Note The maximum number does not impact the number of backup image files you can store on a remote location.

You can view the list of backups for each Cisco UCS domain from the Cisco UCS Central GUI and you can also delete saved or unused backup directories and configurations.

Important

- You must have a user account that includes the admin role to create and run backup and import operations.
- You can delete backups only after a Cisco UCS domain (from which the backup has been taken) has been unregistered.

Backup Image Files

You can save the database or configuration backup files in the following locations:

- **Local File System**: In a local file system.
- **Remote Location**: Remote locations using a protocol such as TFTP, FTP, SCP, or SFTP.

Important You must have Cisco UCS Manager, release 2.2(2x) and above registered with Cisco UCS Central to specify a global backup policy with the option to store the image file in a remote location.

When you schedule the backup, you can also specify the maximum number of backup files you want to save either for system.

Restoring Configuration

You can restore the full state backup for Cisco UCS Central during setup only. For more information, see the appropriate *Cisco UCS Central Installation and Upgrade Guide*.

For Cisco UCS Manager, you can restore the full state backup configuration from the fabric interconnect's console during initial configuration.

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

Backup Locations

The backup location is the destination or folder on the network where you want Cisco UCS Central to export the backup file. You can maintain only one backup operation for each location where you plan to save a backup file.

Potential to Overwrite Backup Files

If you rerun a backup operation without changing the filename, Cisco UCS Central overwrites the existing file on the server. To avoid overwriting existing backup files, change the filename in the backup operation or copy the existing file to another location.

Multiple Types of Backups

You can run and export more than one type of backup to the same location. You need to change the backup type before you rerun the backup operation. We recommend that you change the filename for easier identification of the backup type and to avoid overwriting the existing backup file.

Scheduled Backups

You can create a backup operation in advance and leave the admin state disabled until you are ready to run the backup. Cisco UCS Central does not run the backup operation, save, or export the configuration file until you set the admin state of the backup operation to enabled.

Incremental Backups

You cannot perform incremental backups of Cisco UCS Manager or Cisco UCS Central.

Encryption of Full State Backups

Full state backups are encrypted so that passwords and other sensitive information are not exported as clear text.

Backups from Cisco UCS Manager

Port configurations that include Global VLANs and VSANs are not restored when you do an all-config backup in Cisco UCS Manager. You will need to reconfigure the ports from Cisco UCS Central.

Scheduling a Full State Backup for Cisco UCS Central

To watch a video on scheduling a backup, see Video: Creating Scheduled Backup for UCS Central.

Before You Begin

If you specify a remote location, make sure that location exists. Make sure to have the following information ready for saving backup file in the remote location:

- Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`
- Host name or IP address of the remote server
- Username and password for the remote server

Step 1 In the Task bar, type **Schedule Central Backup** and press Enter.
This launches the **Schedule Central Backup** dialog box.

Step 2 (Optional) In the **Description** field, enter a description for this backup policy.

Step 3 From the **Schedule** drop down, choose a schedule for this backup. This can be one of the following:

- One Time Schedules—The backup occurs at the scheduled date and time only.
- Recurring Schedules—The backup occurs at the scheduled frequency.

Note You must associate this full state backup with a pre-defined schedule. To create a schedule, see Creating or Editing a Schedule, on page 24.

Step 4 In **Maximum No of Backup Files** field, specify the number of backup files you want to keep in the system. After the maximum number of backup files is reached, the oldest backup file is overwritten by the newest backup file.

Step 5 (Optional) If you want to save the backup file in a remote location, in the **Remote Copy** filed, click **Enabled**. Complete the following fields to add the remote location related information.

Name	Description
Transfer Protocol	Choose the transfer protocol. it can be one of the following: • FTP • SFTP • TFTP • SCP
Absolute Remote Path field	The absolute remote path.
Remote Server Host Name/IP Address field	The IP address for the remote server.
User Name field	The user name for the remote server.
Password field	The password for the remote server.

Scheduling a Full State Backup for Cisco UCS Domain

- You can create a full state backup for registered Cisco UCS domains only at the domain group level.
- To watch a video on scheduling a backup, see Video: Creating Scheduled Backup for a UCS Domain.
- To setup a manual backup, provide the Absolute remote path in this format: */path/filename.tgz*
- To setup a scheduled backup, provide the home folder path (/) without the filename. For SFTP, you must create the path and the required subfolders/directories in the SFTP server before you provide the home folder path. Exportation will fail if the folder is not setup in advance. For example, if you want to setup the home folder path of the SFTP server to *C:\sftp*, and if no other folder is present in the hierarchy, and if you provide the Absolute remote path as *C:sftp\abc* the exportation will fail because no such directory would be present in the system.

Before You Begin

If you specify a remote location, make sure that location exists. Make sure to have the following information ready for saving backup file in the remote location:

- Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`
- Host name or IP address of the remote server

- Username and password for the remote server

Step 1 In the **Actions** bar, type **Schedule Domain Backup**.

Step 2 Select a **Domain Group** for which you want to schedule the full state backup.
This selection displays **Schedule** and **No of Backup Files** options.

Step 3 From the **Schedule** drop-down, select a schedule for this backup.

Step 4 In the **Maximum No of Backup Files** field, specify the number of backup files that you want to keep in the system.

Step 5 (Optional) If you want to save the backup file in a remote location, in the **Remote Copy** field, click **Enabled**.
Complete the following fields to add the remote location-related information.

Field Name	Description
Transfer Protocol	Choose the transfer protocol. it can be one of the following: • FTP • SFTP • TFTP • SCP
Absolute Remote Path	The absolute remote path.
Remote Server Host Name/IP Address	The IP address for the remote server.
User Name	The user name for the remote server.
Password	The password for the remote server.

Creating On-Demand Full State Backup

You can create a full state backup for Cisco UCS Central at any time, and save the file in both local and remote locations. However, for registered Cisco UCS domains, you can create a back up on a remote location only.

To watch a video on creating a on-demand backups, see Video: Creating On-Demand Backup for UCS Central or Video: Creating On-Demand Backup for a UCS Domain.

Before You Begin

Make sure you have the following information ready to save the on-demand backup file in a remote location:

- Absolute remote path. For example if the transfer protocol is SCP:
  `scp://user@ipaddress/x/y/backup_filename.tgz`
- Host name or IP address of the remote server

- Username and password for the remote server

Step 1 On the menu bar, click the **Operations** icon and select **Backup & Restore**.

Step 2 Click **UCS Central** or select a domain group.

Step 3 Click the **Backup** icon.
This launches the **Create Backup** dialog box.

Step 4 For a Cisco UCS Central full state backup, choose whether to enable or disable **Remote Copy**.
If you select **Disabled**, a local backup copy will be made, and you can proceed to step 6.

Step 5 Select the **Transfer Protocol**, and entire the required remote location information.

Step 6 Click **Create**.

The full state backup file is created and saved in the specified remote location. To view the backup state for Cisco UCS Domains, click the domain group name.

Note The following error message appears when Cisco UCS Central or Cisco UCS manager on-demand full state backup fails:
End point timed out. Check for IP, password, space or access related issues.
To fix this error, you can resubmit the configuration. On successful re-submission, a backup file is created in the backup repository.

Removing Full State Backup for Cisco UCS Domain

In addition to the procedure described below, full state backup can be disabled/deleted in the following scenarios:

- When you remove root domain group policy, backup/export policy is disabled.
- When you remove sub domain group policy, backup/export policy is deleted.

Step 1 On the menu bar, click the **Operations** icon and select **Backup & Restore**.

Step 2 Click the **Schedule** icon, and select **Remove Domain Backup Schedule**.
This launches the **Remove Domain Backup Schedule** dialog box.

Step 3 Select the **Domain Group** from which you want to remove the backup.

Step 4 Verify the information in the fields that display after the selection to make sure that this is the backup schedule that you want to remove.

Step 5 Click **Remove**.

Removing Full State Backup for Cisco UCS Central

In addition to the procedure described below, full state backup for Cisco UCS Central can be disabled or deleted in the following scenario:

- When you remove a Cisco UCS Central policy, the backup/export policy is disabled.

Step 1 On the menu bar, click the **Operations** icon and select **Backup & Restore**.

Step 2 Click the **Schedule** icon, and select **Remove Central Backup Schedule**.
This launches the **Remove Central Backup Schedule** dialog box.

Step 3 Verify the information in the fields that display to make sure that this is the backup schedule that you want to remove.

Step 4 Click **Remove**.

Viewing Backup files in Cisco UCS Central

Step 1 On the menu bar, choose **Backup & Restore**.

Step 2 Under **Domains**, select the Cisco UCS Central domain to enter the Cisco UCS Central scope.

Step 3 In the right side pane, view the list of all the Cisco UCS Central backup files. For each backup file, you can view the status, last backed up date, schedule, maximum number of files and the location for the remote copy.

Configuration Export and Import

From the Export & Import, you can schedule configuration backup for Cisco UCS Central and the registered Cisco UCS Domains. You can schedule export or import policy or, perform an immediate on demand configuration export of Cisco UCS Central or a selected domain. For a Cisco UCS domain, on demand backups are all stored remotely. If you schedule a backup, it can be stored locally or remotely.

Note In the HTML5 GUI, only the config-all and full-state backups are supported. If you want to use the config-logical or config-system backups, please use the Java-based GUI.

Scheduled backup policies are disabled by default. If you want to backup Cisco UCS Central or the registered Cisco UCS domains, you must enable the backup state for both. Backup process does not interrupt or impact any server or network traffic. You can perform a backup while the domain is up and running. The backup operation saves information from the management plane.

Remotely configured policies are restricted to use the Cisco UCS Central repository for backups which is internally mounted by Cisco UCS Manager.

When you schedule regular backup, the backup repository can start accumulating data. To manage the backup archives, you can specify the maximum number of backup versions that are saved. Use policy specifications to indicate the number of backups to maintain for each Cisco UCS domain.

Note The maximum number does not impact the number of backup image files you can store on a remote location.

You can view the list of backups for each Cisco UCS domain from the Cisco UCS Central GUI (See: Viewing Backup files in Cisco UCS Central, on page 39), and you can also delete saved or unused backup directories and configurations.

Important

- You must have a user account that includes the admin role to create and run backup and import operations.
- You can delete backups only after a Cisco UCS domain (from which the backup has been taken) has been unregistered.

Backup Image Files

You can save the database or configuration backup files in the following locations:

- **Local File System**: In a local file system.
- **Remote Location**: Remote locations using any one of the protocol such as, TFTP, FTP, SCP, or SFTP.

Important You must have Cisco UCS Manager, release 2.2(2x) in registered Cisco UCS domains to specify a global backup policy with the option to store the image file in a remote location. If you do not have Cisco UCS Manager release 2.2(2x) in the Cisco UCS domain, the global backup policy with remote backup will not work.

When you schedule the backup, you can also specify the maximum number of backup files you want to save either for system.

Importing Configuration

You can use the saved configuration from backup repository to import and configure any of the managed Cisco UCS domain. Use TFTP protocol to access the backup configurations.

Scheduling Configuration Export for Cisco UCS Central

To watch a video on using configuration export, see Video: Creating UCS Central Configuration Export.

Before You Begin

If you specify a remote location, make sure that location exists. Make sure to have the following information ready for saving backup file in the remote location:

- Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`
- Host name or IP address of the remote server
- Username and password for the remote server

Step 1 On the menu bar, click the **Operations** icon and select **Export & Import**.

Step 2 On the **Config Export & Import page**, click **UCS Central**.

Step 3 Click the **Schedule** icon and select **Schedule Central Export**.
This launches the **Schedule Central Configuration Export** dialog box.

Step 4 (Optional) In the **Description** field, enter a description for the this backup policy.

Step 5 Click **Schedule** drop down to select a schedule for this backup.

Note You must associate this configuration backup with a pre-defined schedule.

Step 6 In **Maximum No of Backup Files** field, specify the number of backup files you want to keep in the system.

Step 7 (Optional) If you want to save the backup file in a remote location, in the **Remote Copy** field, click **Enabled** and enter the required remote location information.

Scheduling Configuration Export for Cisco UCS Domains

You can create configuration backup for registered Cisco UCS Domains only at the domain group level.

To watch a video on using configuration export, see Video: Creating UCS Domain On-Demand Configuration Export

Before You Begin

If you specify a remote location, make sure that location exists. Make sure to have the following information ready for saving backup file in the remote location:

- Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`
- Host name or IP address of the remote server
- Username and password for the remote server

Step 1 Click **Domain Group** drop down option to select the domain group for which you want to schedule the configuration backup.
This selection displays **Schedule** and **No. of Backup Files** options.

Step 2 Click **Schedule** drop down to select a schedule for this backup.

Note You must associate this configuration backup with a pre defined schedule.

Step 3 In **Maximum No of Backup Files** field, specify the number of backup files you want to keep in the system.

Step 4 (Optional) If you want to save the backup file in a remote location, in the **Remote Copy** filed, click **Enabled**.
Enter required remote location related information in the displayed fields.

Step 5 Click **Schedule**.

Exporting UCS Central Configuration Backup

Before You Begin

If you specify a remote location, make sure that location exists. Make sure to have the following information ready for saving the backup file in the remote location:

- Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`
- Host name or IP address of the remote server
- Username and password for the remote server

Step 1 On the **Config Export & Import** page, click **UCS Central**.

Step 2 Select the backup file that you want to export.

Step 3 Click the **Config Export** icon.

Step 4 If you want to save the backup file in a remote location, in the **Remote Copy** field, click **Enabled**.
If **Disabled** is selected, then the file will be saved locally.

Step 5 For remote locations, choose a **Transfer Protocol**, and enter the required remote location information in the displayed fields.

Step 6 Click **Export**.

Exporting Configuration On-demand Backup for Domains

You can create configuration backup for registered Cisco UCS Domains only at the domain group level.

Before You Begin

An on-demand back up is possible only for a remote location. For a local Cisco UCS domain on-demand backup is not supported. Make sure that you have the following information ready for saving the backup file in the remote location:

- Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`
- Host name or IP address of the remote server

- Username and password for the remote server

Step 1 On the **Config Export & Import** page, select a domain.
Step 2 Select the backup file that you want to export.
Step 3 Click the **Config Export** icon.
Step 4 Choose a **Transfer Protocol**, and enter the required remote location information in the displayed fields.
Step 5 Click **Export**.

Importing Configuration for Cisco UCS Central

You can import a configuration from another Cisco UCS Central, or an xml file you have exported to a local or remote location.

Step 1 On the menu bar, click the **Operations** icon and select **Export & Import**.
Step 2 On the **Config Export & Import page**, click **UCS Central**.
Step 3 Click the **Config Import** icon.
This launches the **Import Central Backup** dialog box.
Step 4 In **Behavior on Configuration Import**, select one of the following options based on your requirements:

Option	Description
Replace	For each object in the imported file, replaces the corresponding object in the current configuration.
Merge	Merges the configuration information in the imported file with the existing configuration information. If there is a conflict, the information in the current configuration is replaced with that in the imported configuration file.

Step 5 In **Config File Location**, select the location from which you want to import all configuration into Cisco UCS Central. If you select-

- **UCS Central**: Select a configuration backup from the **Config File** drop down.
- **Local**: Browse to the file location and select the file.
  Note This backup XML file resides locally.
- **Remote**: Enter the remote server related information and file path.
  Note This backup XML file resides on a remote server.

Step 6 Click **Import**.
The following error message appears when Cisco UCS Central import fails:
End point timed out. Check for IP, password, space or access related issues.
To fix this error, you can resubmit the configuration. On successful re-submission, the import process will begin.

Importing Configuration for Cisco UCS Domain

Note If a Cisco UCS domain is in suspended state, has lost visibility, or lost connectivity, the import configuration feature is disabled.

Before You Begin

Make sure that you have created config-all backup files using backup policies.

Step 1 On the menu bar, click the **Operations** icon and select **Export & Import**.

Step 2 On the **Config Export & Import page**, click the domain where you want to import the backup.

Step 3 Click the **Config Import** icon.
This launches the **Import Domain Config Backup** dialog box.

Step 4 In **Behavior on Configuration Import**, select **Replace** or **Merge** based on your requirements.

Option	Description
Replace	For each object in the imported file, replaces the corresponding object in the current configuration.
Merge	Merges the configuration information in the imported file with the existing configuration information. If there is a conflict, the information in the current configuration is replaced with that in the imported configuration file.

Step 5 In **Import From** drop down, select the domain from which you want to import all configuration into this domain.
The selection here displays the **Config File** drop-down.

Step 6 Click **Config File** drop down to select the configuration file.

Step 7 Click **Import**.

Removing Configuration Export Schedule for Cisco UCS Central

Step 1 On the **Config Export & Import** page, click the **Schedule** icon.

Step 2 Select **Remove Central Export Schedule** icon.

Step 3 View the entries in the schedule.

Note There is only one schedule for Cisco UCS Central.

Step 4 Click **Remove**.

Removing Configuration Export Schedule for Cisco UCS Domain

In addition to the procedure described below, full state backup for Cisco UCS Central can be disabled or deleted in the following scenarios:

- When you remove a sub-domain group policy, the backup/export policy is deleted.
- When you remove either a central or root domain group policy, the backup/export policy is disabled.

Step 1 On the **Config Export & Import** page, click the **Schedule** icon.

Step 2 Select **Remove Domain Export Schedule** icon.

Step 3 Select the domain group where you want to remove the configuration backup.

Step 4 Select the schedule that you want to remove.

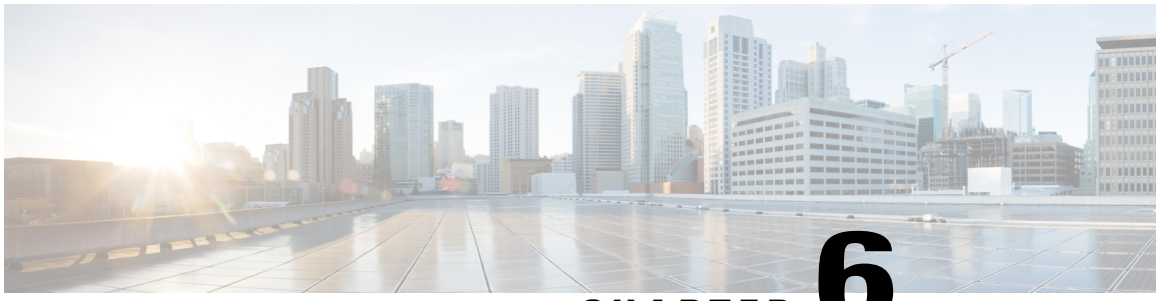
Step 5 Click **Remove**.

Viewing Backup files in Cisco UCS Central

Step 1 On the menu bar, choose **Backup & Restore**.

Step 2 Under **Domains**, select the Cisco UCS Central domain to enter the Cisco UCS Central scope.

Step 3 In the right side pane, view the list of all the Cisco UCS Central backup files. For each backup file, you can view the status, last backed up date, schedule, maximum number of files and the location for the remote copy.



CHAPTER 6

Smart Call Home

Smart Call Home is an automated support capability that helps to minimize downtime by performing proactive diagnostics in Cisco UCS Central. Cisco UCS Central sends system generated real-time alerts to the email address specified in your Call Home settings. You can view details on any detected issues on the Cisco Smart Call Home support page, along with recommendations for possible remediation.

For more information, see the Smart Call Home Web Application chapter of the Smart Call Home User Guide.

Smart Call Home provides alerts for the Cisco UCS Central faults listed in Smart Call Home Faults.

If you want to receive alerts for Cisco UCS Manager faults, see Configuring Call Home for UCS Manager.

Smart Call Home

Smart Call Home is an automated support capability that helps to minimize downtime by performing proactive diagnostics in Cisco UCS Central. Cisco UCS Central sends system generated real-time alerts to the email address specified in your Call Home settings. You can view details on any detected issues on the Cisco Smart Call Home support page, along with recommendations for possible remediation.

For more information, see the Smart Call Home Web Application chapter of the Smart Call Home User Guide.

Smart Call Home provides alerts for the Cisco UCS Central faults listed in Smart Call Home Faults.

If you want to receive alerts for Cisco UCS Manager faults, see Configuring Call Home for UCS Manager.

Configuring Smart Call Home

Before You Begin

You must configure a DNS server before you can configure Smart Call Home.

Step 1 From the System Settings icon, choose **Smart Call Home**.
This launches the UCS Central Smart Call Home dialog box.

Step 2 In the **Basic** tab, click **Enabled**.

Step 3 Enter the required email address of the main contact.
The initial registration and alert notifications are sent to this email address. Only the email address is required to enable Smart Call Home.

Important Make sure that you type the email address correctly. If you enter the incorrect email address, contact Cisco TAC.

Step 4 In **Advanced**, select whether to enable or disable **Throttling** and **Send System Inventory Periodically**.
If Send System Inventory Periodically is enabled, specify the interval in which to send the system inventory to the Call Home database. Alternatively, on the **Basic** tab, you can click the Tools icon and select **Send System Inventory Now** to send it immediately.

Note When you first enable Smart Call Home, the system inventory is sent automatically when you click **Save**.

Step 5 Enter the optional contact information.

Step 6 In **Transport Gateway**, click **Enabled** to use the transport gateway to communicate with the Cisco Smart Call Home portal.
The transport gateway acts as a proxy between Cisco UCS Central and the Smart Call Home servers at Cisco.com.

For HTTP, enter the Transport Gateway URL. If you want to use HTTPS, you also need to enter the Transport Gateway Certificate.

Note Self-signed certificates are only supported. See Transport Gateway Communication over HTTPS for more information on setting up the transport gateway.

Step 7 In **Profiles**, click **Basic** to view the default CiscoTAC-1 profile.

Note The CiscoTAC-1 profile is the only profile supported in Cisco UCS Central release 1.4(1a). This profile cannot be deleted, but you can modify the debug level of the messages that you receive.

Step 8 In **Alerts**, click the plus icon to select the alerts that you want to disable.
No notification is received if disabled events occur.

Step 9 In **Configuration Status**, you can view the current status of your Smart Call Home configuration.

Step 10 Click **Save**.

Smart Call Home Registration

When you first enable Cisco UCS Central Smart Call Home, the system inventory is sent automatically to the Cisco Smart Call Home servers. An automated email message is sent to the email address that you entered with a link to the Smart Call Home portal. You have 3 months (90 days) to confirm the registration.

After you register, if you did not enter a contract ID, a 4 month (120 days) trial period is activated. If you entered a valid contract ID, your registration is complete. Make sure that you enter the contract ID and send the inventory before or after the 120 days trial period to re-activate your registration.

Smart Call Home Faults

The faults described in this section cause the fabric interconnect to raise Smart Call Home alerts. For more information on Cisco UCS Central faults, see the appropriate Cisco UCS Central Faults Reference.

Note In release 1.4(1a), none of the Cisco UCS Central faults raise Service Requests.

Fault Name	Fault Code	Explanation
fltSysdebugCoreCoreFile	F10000005	This fault happens when one of the processes stops responding and a core file is generated.
fltExtpolProviderProviderLostConnectivity	F10000190	This provider is not reachable from the Cisco UCS Central registry. This fault typically occurs if the provider process has stopped responding, or is too busy to respond to a heartbeat message sent by the registry.
fltExtpolControllerControllerLostConnectivity	F10000191	This controller is not reachable from the Cisco UCS Central registry. This fault typically occurs if the controller process has stopped responding, or is too busy to respond to a heartbeat message sent by the registry.
fltExtpolClientClientLostConnectivity	F10000192	This registered UCS Domain is not reachable from the Cisco UCS Central registry. This fault typically occurs if the UCS Domain has lost network access or UCS Domain DME process has stopped responding, or is too busy to respond to a heartbeat message sent by registry.
fltIdentpoolElementDuplicatedAssigned	F10000208	The same ID is assigned to two or more service profiles. This fault occurs when Cisco UCS Central finds one ID is assigned to two or more service profiles probably from local pools.
fltConfigDbConfigStats-DB-Error	F10000536	This fault occurs when the statistics database is configured incorrectly or if the database is down or out of disk space.
fltPkiTPStatus	F10000591	This fault occurs when certificate status of TrustPoint has become invalid.

Fault Name	Fault Code	Explanation
ltPkiKeyRingStatus	F10000592	This fault occurs when the certificate status of Keyring has become invalid.
fltConfigBackupUngrouped-domain	F10000616	Remote scheduled backup failed. This fault typically occurs if the admin supplied the wrong password, host, user name, or path to the remote machine.
fltStorageItemCapacityExceeded	F10000034	This fault occurs when the partition disk usage exceeds 70% but is less than 90%.
fltStorageItemCapacityWarning	F10000035	This fault occurs when the partition disk usage exceeds 90%.
fltSmartlicenseEntitlementEnforcementModeFault	F10000750	Entitlement for a license is not compliant.

Configuring Call Home for UCS Manager

Use the Call Home feature in Cisco UCS Central to view Cisco UCS Manager alerts for your domain groups.

Step 1 From the Domains icon, select the domain group where you want to configure Call Home.
Choose Root to view alerts for all registered domains.

Step 2 From the System Settings icon, select Call Home.

Step 3 In **Basic**, click **Enabled** to enable Call Home.

Step 4 Enter the required contact information.

Step 5 In **Advanced**, select whether to enable or disable **Throttling** and **Send System Inventory Periodically**.
If Send System Inventory Periodically is enabled, specify the interval in which to send the system inventory to the Call Home database. Alternatively, on the **Basic** tab, you can click the Tools icon and select **Send System Inventory Now** to send it immediately.

Note When you first enable Call Home, the system inventory is sent automatically.

Step 6 In **Profiles**, you can add new or remove existing profiles.

a) In **Basic**, enter the description and maximum email size, and select the debug level and email format.
b) In **Alert Groups**, select the type of alerts that you want to receive.
c) In **Alert Recipients**, enter any additional email addresses where you want to send the alerts.

Step 7 In **Alerts**, click the plus icon to select the alerts that you want to disable.
No notification is received if disabled events occur. inventory diagnostic and environmental supported event types

Step 8 Click **Save**.