Cisco UCS Central Administration Guide, Release 2.0

First Published: 2017-05-16

Last Modified: 2018-10-16

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`.
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 Roadmap* available at the following URL: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/overview/guide/ucs_rack_roadmap.html.

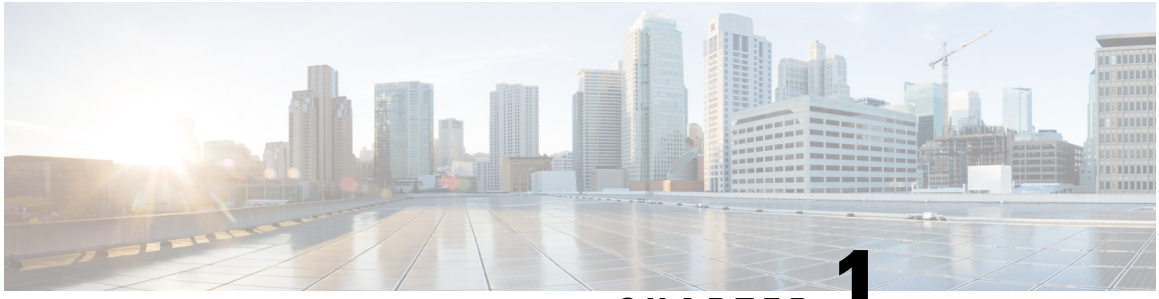
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

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@external.cisco.com. We appreciate your feedback.



CHAPTER 1

Overview

Overview

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

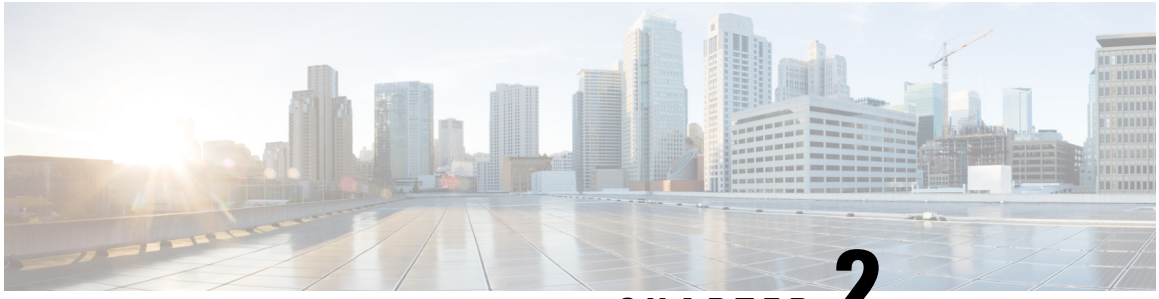
- User Management
- System Management
- Image Library
- Firmware Management
- Backup Management
- Smart Call Home

Cisco UCS Central User Documentation Reference

The Cisco UCS Central following use case-based documents 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.
Cisco UCS Central Operations Guide	Best practices for setting up, configuring, and managing domain groups for small, medium and large deployments.
Cisco UCS Central Troubleshooting Guide	Provides help for common issues in Cisco UCS Central.



CHAPTER 2

User Management

This chapter includes the following sections:

Managing UCS Central Users

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

Procedure

Step 1 Click the **System Configuration** icon and choose **Users**.

This launches the **UCS Central Users Administration Manage** dialog box.

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

- **Password Profile**—Perform the same tasks as the **UCS Central Password Profile Manage** dialog box. For more information, see Managing UCS Central Password Profile, on page 4.
- **Roles**—Perform the same tasks as the **UCS Central Roles Manage** dialog box. For more information, see Managing UCS Central Roles, on page 4.
- **Locales**—Perform the same tasks as the **UCS Central Locales Manage** dialog box. For more information, see Managing UCS Central Locales, on page 5.
- **Local Users**—Perform the same tasks as the **UCS Central Local Users Manage** dialog box. For more information, see Managing UCS Central Local Users, on page 5.
- **Remote Users**—Perform the same tasks as the **UCS Central Remote Users Manage** 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

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Password Profile** and press **Enter**.

This launches the **UCS Central Password Profile Manage** dialog box.

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

Step 3 Select the minimum number of passwords before a user can reuse a previous password.

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

Procedure

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 **Add** to create a new role, or select an existing role.

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

Step 4 Select relevant privileges for the role.

Step 5 Click **Apply** 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

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Locales** and press **Enter**.

This launches the **UCS Central Locales Manage** dialog box.

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

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

a) Click **Add** to display the organizations or domain groups.
b) Select the organizations or domain groups.
c) Click **Apply** 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

Procedure

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 **Add** 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 **Add** to display the roles.
b) Select a role or roles.
c) Click **Apply** to apply the new privileges.

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

a) Click **Add** to display the roles.
b) Select a role or roles.
c) Click **Apply** 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

Procedure

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

Procedure

Step 1 Click the **Domain Group** icon and choose **root**.

Step 2 Click the **Settings** icon and choose **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 **Add** to update and add privileges.

a) Click **Add** to display the organizations.
b) Select relevant privileges for the role.
c) Click **Apply** to apply the new privileges.

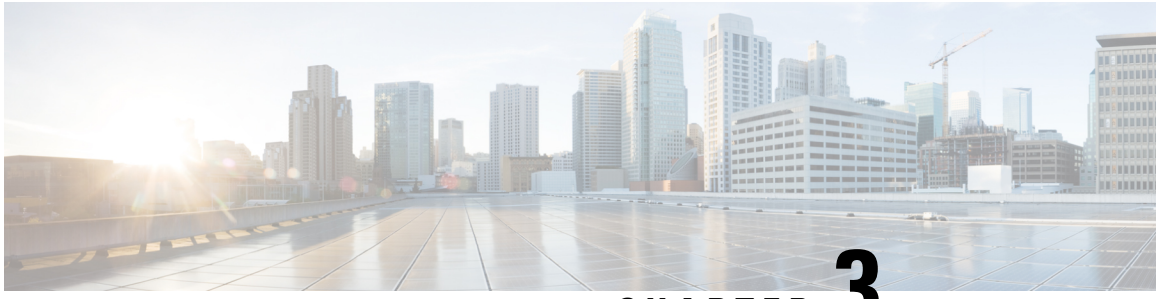
Step 5 Update the **Storage**, **Server**, and **Operations** privileges for the role, in the same manner.

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 **Add** to display the organizations.
b) Select the organizations or domain groups.
c) Click **Apply** to apply the new privileges.

Step 8 Click **Save**.



CHAPTER 3

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 18.

UCS Central system policies include the following:

- **Faults**—Determines when faults are cleared, the flapping interval, and the retention interval.

  Flapping Interval

  Length of time between Cisco UCS Central raising the fault and clearing the condition.

  Retention Interval

  Length of time Cisco UCS Central retains a fault in the system.

- **Syslog**—Determines the type of log files that you want to collect, and where you want to view or store them.

- **Core Dump**—Uses the Core File Exporter to export core files as they occur.

Configuring UCS Central System Policies

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

Procedure

Step 1 Click the **System Configuration** icon and choose **System Policies**.

Step 2 In the **UCS Central System Policies** dialog box, click the icon for the section that you want to configure.

- **Fault**—Perform the same tasks as the **UCS Central Fault Policy Manage** dialog box. For more information, see Managing a UCS Central Fault Policy, on page 12.
- **Syslog**—Perform the same tasks as the **UCS Central Syslog Manage** dialog box. For more information, see Managing UCS Central Syslog, on page 13.
- **Core Dump Export**—Perform the same tasks as the **UCS Central Core Dump Export Manage** dialog box. For more information, see Managing UCS Central Core Dump Export, on page 14.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Related Topics

Managing a UCS Central Fault Policy, on page 12
Managing UCS Central Syslog, on page 13
Managing UCS Central Core Dump Export, on page 14

Managing Equipment Policies

Procedure

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

Procedure

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 **Rack Discovery**, click **Enabled**.

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

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

Step 5 Click **Policies** and select the scrub policy that you want 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

Procedure

Step 1 In the **Actions** bar, type **Manage UCS Central Fault Policy** and press Enter.

Step 2 In the **UCS Central Fault Policy** dialog box, click **Fault** and complete the following fields:

Note The **Initial Severity** and **Action on Acknowledgment** fields are read-only. You cannot modify them.

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

   Flapping occurs when Cisco UCS Central raises and clears a fault several times in rapid succession. To prevent this, Cisco UCS Central does not allow a fault to change its state until the user-defined 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 clears. The behavior 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**, Cisco UCS Central does not automatically clear faults. If you choose **Custom Interval**, Cisco UCS Central automatically clears fault messages after the length of time you specify in the associated interval field.

4. In **Action on Clear**, select the actionCisco UCS Central must take when a fault is cleared.

If you choose **Retain Cleared Faults**, then Cisco UCS Central retains the cleared faults for the length of time specified in the **Retention Interval**. If you choose **Delete Cleared Faults**, then Cisco UCS Central clears the faults immediately.

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

   If you choose **Forever**, Cisco UCS Central retains all cleared fault messages forever. If you choose **Custom Interval**, Cisco UCS Central 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 10
Managing UCS Central Syslog, on page 13
Managing UCS Central Core Dump Export, on page 14

Managing UCS Central Syslog

Procedure

Step 1 In the **Actions** bar, type **Manage UCS Central Syslog** and press Enter.

Step 2 In the **UCS Central Syslog** dialog box, click **Syslog Sources** and choose **Enabled** for each source for which you want to collect log files:

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

Step 3 In **Local Destination**, specify where Cisco UCS Central can add and display the syslog messages:

- **Console**—Displays syslog messages on the console and adds them to the log. Choose the logging level for the messages you want to display.
- **Monitor**—Displays syslog messages on the monitor and adds them to the log. Choose the logging level for the messages you want to display.
- **Log File**—Saves syslog messages to the log file. Choose the logging level, a filename, and the maximum file size.

Logging Level—Select the lowest message level that you want the system to store. The system stores that logging level and above:

- **Alert**
- **Critical (UCSM Critical)**
- **Error (UCSM Major)**
- **Emergency**

- **Warning (UCSM Minor)**
- **Notification (UCSM Warning)**
- **Information**
- **Debug**

Step 4 In **Remote Destination**, specify whether to store the syslog messages in a primary, secondary, 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:
  - **Alert**
  - **Critical (UCSM Critical)**
  - **Error (UCSM Major)**
  - **Emergency**
  - **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 hostname rather than a IPv4 or IPv6 address, configure the DNS server in Cisco UCS Central.

Step 5 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 10
Managing a UCS Central Fault Policy, on page 12
Managing UCS Central Core Dump Export, on page 14

Managing UCS Central Core Dump Export

Cisco UCS uses the Core File Exporter to export core files, through TFTP, to a specified location on the network. This exports the core file in tar format.

Procedure

Step 1 In the **Actions** bar, type **Manage UCS Central Core Dump Export** and press Enter.

Step 2 In the **UCS Central Core Dump Export** dialog box, 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 through TFTP

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

Step 8 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 10
Managing a UCS Central Fault Policy, on page 12
Managing UCS Central Syslog, on page 13

Configuring System Event Logs

Procedure

Step 1 In **Description**, type a description for the System Events.

Step 2 In **SEL Backup**, select if you want to **Enable** or **Disable** the backup.

Step 3 In **SEL Backup Format**, select **ASCII** or **Binary** as the format for the backup file.

Step 4 In **SEL Backup Frequency**, select one of the following options to set the time to wait between automatic backups:

- **Hourly**
- **Every 2 Hours**
- **Every 4 Hours**
- **Every 8 Hours**
- **Daily**
- **Weekly**
- **Monthly**

Step 5 In **Protocol**, select one of the following options as the protocol to communicate with the remote server.

- **FTP**
- **SFTP**
- **TFTP**
- **SCP**

Step 6 In **Absolute Remote Path ***, enter the absolute path to the file on the remote server.

If you use SCP, the absolute path is always required. If you use any other protocol, you may not need to specify a remote path, if the file resides in the default download folder. For details about how your file server is configured, contact your system administrator.

Step 7 In **Remote Server Host Name/IP Address**, type the hostname or IP address of the server where the backup configuration resides. If you use a hostname and not an IP address, you must configure a DNS server.

Step 8 In **User Name**, type the username used to log in to the remote server. This field does not apply if you select TFTP protocol.

Step 9 In **Password**, type the password used to log in to the remote server. This field does not apply if you select TFTP protocol.

Step 10 In **SEL Backup on Log Full**, select the option to create SEL backup when the log reaches the maximum size allowed.

Step 11 In **SEL Backup on Service Profile Association**, select the option to create SEL backup when the association between a server and the service profile changes.

Step 12 In **SEL Backup on Manual Log Clear**, select the option to create SEL backup when you manually clear the system log.

Step 13 In **SEL Backup on Backup Clear Interval**, select the option to create SEL backup when the time interval specified in the **SEL Backup Frequency** drop-down is reached.

Step 14 In **Clear Log on Backup**, select the option to clear all system event logs after the backup.

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 19.

Managing the UCS Central System Profile

Procedure

Step 1 Click the **System Configuration** icon and choose **System Profile**.

Step 2 In the **UCS Central** section, you can view the Cisco UCS Central system name, mode, and virtual IPv4 and IPv6 addresses.

These values are populated when you first configure Cisco UCS Central. You cannot modify the system name and mode.

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 17
Managing the UCS Central Management Node, on page 17
Managing the UCS Central DNS Servers, on page 18

Managing the UCS Central Management Node

Procedure

Step 1 In the Actions bar, type **Manage UCS Central Management Node** and press **`Enter`**.

This launches the **UCS Central Management Node Manage** dialog box.

Step 2 In **Management Node**, click the name of the node that you want 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 16
Managing the UCS Central NTP Servers, on page 17
Managing the UCS Central DNS Servers, on page 18

Managing the UCS Central NTP Servers

Procedure

Step 1 In the Actions bar, type **Manage UCS Central NTP Servers** and press **`Enter`**.

This launches the **UCS Central NTP Servers Manage** 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 16
Managing the UCS Central Management Node, on page 17
Managing the UCS Central DNS Servers, on page 18

Managing the UCS Central DNS Servers

Procedure

Step 1 In the Actions bar, type **Manage UCS Central DNS Servers** and press **Enter**.

This launches the **UCS Central DNS Servers Manage** 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 16
Managing the UCS Central NTP Servers, on page 17
Managing the UCS Central Management Node, on page 17

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 9.

Domain group system policies include the following:

- **Equipment**—Sets policies for the equipment in your domain group, including discovery and power policies.
- **Rack Discovery**—Determines what action is taken when a rack-mount server is discovered, and assign a scrub policy.
- **Faults**—Determines when faults are cleared, the flapping interval, and the retention interval.

  Flapping Interval

  Length of time between Cisco UCS Central raising the fault and clearing the condition.

  Retention Interval

  Length of time Cisco UCS Central retains a fault in the system.
- **Syslog**—Determines 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**—Sets criteria for monitoring your domain group interfaces.
- **System Events**—Sets the criteria for domain group system event logs.

Managing Domain Group System Policies

Note If you are setting the system policies for a subdomain, enable each policy before you can set it.

Procedure

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

Step 2 Click the **Settings** icon.

Step 3 Click **Launch** for System Policies.

Step 4 In **Equipment**, complete the necessary fields.

For more information, see Managing Equipment Policies, on page 10.

Step 5 In **Rack Discovery**, complete the necessary fields.

For more information, see Managing Rack Discovery Policies, on page 12.

Step 6 In **Fault**, complete the necessary fields.

For more information, see Managing a UCS Central Fault Policy, on page 12.

Step 7 In **Syslog**, complete the necessary fields.

For more information, see Managing UCS Central Syslog, on page 13.

Step 8 In **Core Dump**, complete the necessary fields.

For more information, see Managing UCS Central Core Dump Export, on page 14.

Step 9 In **Interfaces**, choose whether to enable **Interface Monitoring Policy**.

Step 10 If you select **Enabled**, complete the interface monitoring information as required.

Step 11 In **System Events**, complete the necessary fields to determine how the system event logs are collected.

For more information, see Configuring System Event Logs, on page 15.

Step 12 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.

Managing the Domain Group System Profile

Procedure

Step 1 Click the **Domain Group Navigation** icon and choose root.

Step 2 Click the **Settings** icon.

Step 3 Click **Launch** for System Policies.

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

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

Step 6 In **Remote Access**, type the HTTPS, HTTPS port, and change the default values for web and shell sessions, if needed.

Note The SSH fields are read-only.

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

Step 8 Click **Save**.

Schedules

Use schedules to determine when certain activities will occur. After you create a schedule in Cisco UCS Central, you can use that schedule in:

- Backup operations
- Configuration export
- Maintenance policies

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.

Creating or Editing a Schedule

Note Simple schedules, whether recurring or single occurrence, do not require user acknowledgment. If you want to require user acknowledgment, choose an advanced schedule.

Procedure

Step 1 In the **Actions** bar, type **Create Schedule** and press Enter.

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

Step 3 Select **Recurring**, **One Time**, or **Advanced** for the schedule.

If **Advanced**, select to enable or disable user acknowledgment.

Step 4 Click **Schedules**.

Step 5 Click **Add** to add a schedule.

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 6 Click **Create**.

Server Maintenance Policy

When you change 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 does not automatically reboot when changes to the service profiles occur. You can specify one of the following options for a maintenance policy:

- **On Save**: When you change a service profile, Cisco UCS Central applies the changes immediately.
- **User Acknowledgment**: Applies the changes after an admin acknowledges the changes.
- **Schedule**: Applies 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 server maintenance policy and associating it with a service profile, see Video: Creating a Global Maintenance Policy and Associating the Policy with a Service Profile.

Procedure

Step 1 In the **Actions** bar, type **Create Maintenance Policy** and press Enter.

Step 2 In the **Maintenance Policy Create** dialog box, choose **Server**.

Step 3 Choose the **Organization** where you want to create the policy, and enter the **Name** and optional **Description**.

The name is case sensitive.

Step 4 For a server maintenance policy, complete the following:

a) Select the Hard Shutdown OS Option :

- If you choose **Enabled**, Cisco UCS Manager waits for the **Hard Shutdown Timer** value specified in Cisco UCS Central before it triggers a shutdown and reboot.

  Note The **Hard Shutdown Timer** specifies time in seconds (150, 300, or 600) that Cisco UCS Manager waits before it triggers a shutdown and reboot. This timer value is specified in the global maintenance policy.

- If you choose **Disabled**, Cisco UCS Manager never performs a server shutdown.

b) Select when to apply the changes that require a reboot:

- **User Acknowledgment**—User must acknowledge configuration changes and confirm reboots.
- **Schedule**—Cisco UCS Central applies configuration changes depending on the schedule that you select. To add a new schedule to the list of values, see Creating or Editing a Schedule, on page 20.
- **On Save**—Cisco UCS Central applies configuration changes immediately on save and causes a reboot.

c) Enable **Apply on Next Reboot**, if you want Cisco UCS Central to apply the changes on the next reboot and ignore the selection in the **Apply Changes On** field.

Step 5 Click **Evaluate** to view the impact of the policy.

Step 6 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. You can decrypt a message encrypted with either key

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 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 for you to create extra key rings.

Note After you regenerate the default key ring, logging in to Cisco UCS Central can take a few minutes.

Manually regenerate the default key ring certificate 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 a certificate signed from a CA server must include **SSL Client Authentication**, and **SSL Server Authentication**. If you use Microsoft Windows Enterprise Certification Authority Server as an internal CA, use the **Computer** template to generate the certificate. It must contain both of the key usages sets. If this template is not available in your setup, use an appropriate template which has both **SSL Client Authentication**, and **SSL Server Authentication** key usages set.

Creating a Key Ring

Procedure

Step 1 Click the **System Configuration** icon and choose **System Profile**.

Step 2 Click **Certificates**.

Step 3 Click **Add** to add a Key Ring.

Step 4 In the Basic tab, leave the Modulus at its default value, or change if necessary.

Step 5 Enter a Trusted Point.

Step 6 Paste in the certificate chain from your generated key ring.

Step 7 Click **Certificate Request**.

Step 8 Fill in the fields with valid information for your organization.

Step 9 Click **Save**.

Note After you create a valid keyring, you must deploy it to Cisco UCS Central. To deploy the keyring, navigate to **System Profile** > **Remote Access** > **Keyring**. Select the keyring you have created based on the instructions above, and click **Save**.

Creating a Trusted Point

Cisco UCS Central allows you to create a trusted point. The trusted point contains the certificate of the root certificate authority (CA) and a subordinate CA in a bundled format.

Note The root CA must contain a primary and self-signed certificate.

Procedure

Step 1 Click the **System Configuration** icon and choose **System Profile**.

Step 2 Click**Trusted Points**.

Step 3 Click **Add** to add a trusted point.

Step 4 Paste in the certificate chain from your generated key ring.

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 **Refresh** to see the latest data.

System Faults

Cisco UCS Central collects and displays all of the Cisco UCS Central system faults on the **Fault Logs** page. To view these system fault logs, click the **System Alerts** icon and choose **System Faults**. The **Faults Logs** page displays information on the type and severity level of the fault. It also allows 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**—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**—Component affected by this fault
- **Fault Details**—Details of the fault.
- **Severity**—Severity of the fault

- **Action**—Action required by the fault

To manage the information collected, see Configuring UCS Central System Policies, on page 10.

Domain Faults

Cisco UCS Central collects and displays faults from registered Cisco UCS domains in the **Domain Faults** page. It also displays Inventory faults. Cisco UCS Central categorizes and displays domain faults as follows:

- **Fault Level**—The fault level that triggers the profile:
  - **Critical**—Critical problems exist with one or more components. Research and fix these issues immediately.
  - **Major**—Serious problems exist with one or more components. Research and fix these issues immediately.
  - **Minor**—Problems exist with one or more components that may adversely affect the system performance. Research and fix these issues as soon as possible before they become major or critical issues.
  - **Warning**—Potential problems exist with one or more components that may adversely affect the system performance if they are allowed to continue. Research and fix these issues as soon as possible before they become major or critical issues.
  - **Cleared**—Condition that caused the fault is resolved, and the fault is cleared.
  - **Info**—Notification or informational message.
  - **Condition**—Informational message about a condition.
- **Filter**—Filter the data in the table.
- **Code**—Unique identifier associated with the fault.
- **Timestamp**—Day and time at which the fault occurred.
- **Type**—Information on where the fault originated.
- **Cause**—Brief description of what caused the fault.
- **Affected Object**—The name and location of the component that this issue affects, and the domain name where it is found.
- **Fault Details**—More information about the log message.
- **Severity**—Displays an icon denoting the fault severity. The icon key displays below the table.
- **Action**—Whether user acknowledgment is required.

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 **System Alerts** icon and choose **Events**. The event logs record the following information:

- **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 affected by the event
- **Event Details**—Details of 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 on 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 **System Alerts** icon and choose **Core Dumps**. In the **Core Dumps** log table you can view the following information:

- **Timestamp**—Creation date.
- **Name**—Full name of the core dump file.
- **Description**—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 **System Alerts** icon and choose **Active Sessions**. In the log table you can view the following information:

- **ID**—Type of terminal from which the user logged in.

- **Timestamp**—Date and time at which the user logged in.
- **User**—User name.
- **Type**—Type of terminal from which the user logged in.
- **Host**—IP address from which the user logged in.
- **Status**—If 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 **System Alerts** icon and choose **Internal Services**.

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

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

In the **Lost Domains** section, you can view the following information:

- **Domain**—Domain name.
- **Last Poll**—Day and time on which Cisco UCS Central last polled the provider.
- **Lost Visibility**—Time when Cisco UCS Central lost visibility to the provider.

Enabling Tomcat Logging

Use a terminal emulator to access the CLI.

Procedure

	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** |	Sets the logging level.

	Command or Action	Purpose
	debug1 | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]	
Step 5	UCSC /monitoring/sysdebug/mgmt-logging # **commit-buffer**	Commits the change.

Example

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 # commit-buffer
```

Prevention of Deleting Critical Objects from Cisco UCS Central

Beginning release 2.0, Cisco UCS Central prevents you from deleting critical objects from the Cisco UCS Central GUI and the command line. When you attempt to delete any of these items from Cisco UCS Central, an error message with the potential impact displays. The table below lists the items and the procedure to follow before you attempt to delete them:

Objects in Cisco UCS Central	Required action before deleting the object from Cisco UCS Central
A service profile associated with a server	Un-associate it from the server
An organization with associated service profiles	Un-associate all service profiles in that organization, and all of its sub-organizations
A service profile template with any associated service profiles bound to it	Either unbind all associated service profiles, or un-associate all of them
A domain group with registered Cisco UCS domains, functional VLANs	• You must not have any registered domains in the domain group, or any of its sub-domain groups • You must not have any VLANs referenced by any associated service profile in it, or any of its sub-domain groups

API Communication Reports

Cisco UCS Central 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 later, 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

Procedure

Step 1 On the menu bar, click the **System Tools** icon and choose **Start Logging Session**.
The system starts logging the active API communication between Cisco UCS Central GUI and the back-end.

Step 2 On the menu bar, click the **System Tools** icon and choose **Stop Logging Session**.
The API report text file saves to your system.

Tech Support Files

When you encounter an issue that requires troubleshooting or a request for assistance to the Cisco Technical Assistance Center (Cisco TAC), collect as much information as possible about Cisco UCS Central or the affected Cisco UCS domain. Cisco UCS Central outputs this information into a tech support file that you can send to Cisco TAC.

You can create a tech support file for all of Cisco UCS Central, or for the following components of a Cisco UCS domain:

- **Entire Domain**—Contains technical support data for the entire Cisco UCS domain.
- **FEX**—Contains technical support data for the given FEX.
- **Domain Management Services**—Contains technical support data for the Cisco UCS Central management services, excluding Fabric Interconnects.
- **Rack Server**—Contains technical support data for the given rack server and adapter.
- **Chassis**—Contains technical support data for the I/O module or the CIMCs on the blade servers in a given chassis only.
- **Server Memory**—Contains server memory technical support data for the given rack-mount servers and blade servers.

Before contacting Cisco TAC, see the following:

1. Generating a Tech Support File, on page 29
2. Downloading a Tech Support File, on page 30

Generating a Tech Support File

You can generate a tech support file for Cisco UCS Central or for a supported component of a Cisco UCS domain.

Procedure

Step 1 Click the **System Tools** icon and choose **Tech Support**.

Step 2 Under **Domains**, select **UCS Central** or the domain for which you want to generate tech support files.

Step 3 Click the **Generate Tech Support** icon.

Step 4 If you selected **UCS Central**, do the following:

a) Choose whether to include system data in the report.

b) Click **Yes** to generate the file.
The list page displays the tech support file collection status while the collection is in progress. When the process completes, it displays the collected time, file name and availability status.

Step 5 If you selected a domain, do the following:

a) Choose the type of data for which you want to generate tech support.

b) Choose whether or not to exclude CLI commands.

c) Click **Generate File**.
The list page displays the tech support file collection status while the collection is in progress. When the process completes, it displays the collected time, file name and availability status.

Downloading a Tech Support File

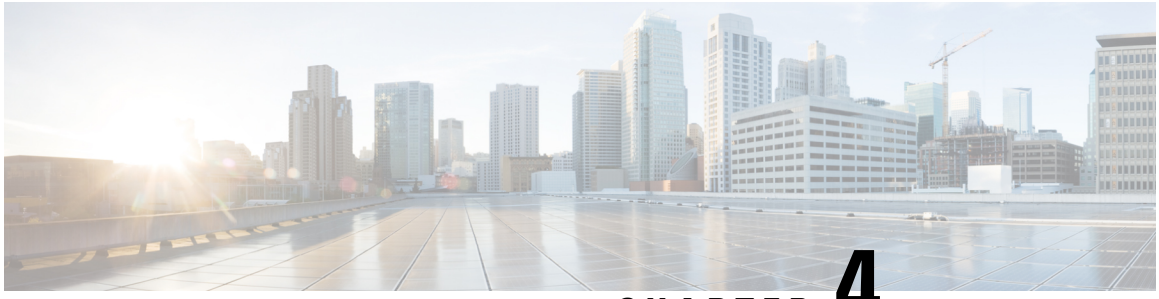
Procedure

Step 1 Click the **System Tools** icon and choose **Tech Support**.

Step 2 Under **Domains**, select **UCS Central** or the domain for which you want to view tech support files.
The right pane displays the list of available tech support files for the selected system.

Step 3 Choose the file that you want to download.

Step 4 Click **Download**.



CHAPTER 4

Image Library

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. Access the Image Library through the **System Tools** icon.

- **Packages**—Displays all firmware packages.
- **Downloads**—Allows you to monitor the status of your downloads.

Use the firmware images when creating firmware policies.

In the Image Library, you can:

- Delete any downloaded image by selecting the image and clicking **Delete**.

  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.

- Schedule Periodic Firmware Image Synchronizations
- Sync firmware images with images on Cisco.com
- Import Firmware Bundles (or Service Packs)

- For more information on downloading images, see Downloading Firmware from Cisco.com , on page 32.

Downloading Firmware from Cisco.com

You can configure Cisco UCS Central to communicate with the Cisco website at specified intervals to fetch the firmware image list. After configuring Cisco credentials for image download, when you refresh, Cisco UCS Central fetches the available image data from Cisco.com and displays the firmware image in the firmware image library. You can download the actual firmware images when creating a policy using the firmware image version or when downloading the image using the **Store Locally** option.

To download the Firmware image from cisco.com, you must:

1. Setup the cisco.com account with user credentials.
2. Accept EULA and K9 through the GUI.
3. Set the frequency of the sync (on-demand, daily, weekly, and bi-weekly).
4. Download the metadata.

Note This process runs in the background and takes approximately 15 minutes to complete. The download time varies based on the number of images.

5. Select an image from the metadata and download the image.

Important Make sure that you create a Cisco.com account to download firmware from Cisco.com to Cisco UCS Central.

Note If you change users in the Cisco.com account, this causes a full synchronization of the Image Library. Download operations are unavailable while it is synchronizing. This can take up to 15 minutes, depending on the size of the library.

Setting Up the Cisco.Com Account

Both the firmware management and hardware compatibility list credentials are managed through your cisco.com account.

Procedure

Step 1 Click the **System Configuration** icon and choose **Cisco.com Account**.

Step 2 Enter your user name and password.

Step 3 If you want your system to access Cisco.com through HTTP, choose **Enabled** in the **HTTP Proxy To Access Cisco.com** field. Enter the HTTP connection information in the appropriate fields.

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

Step 4 Select the Cisco Services that you want to use:

- Firmware Image Downloads—Select if you want to download Infrastructure Firmware updates and Firmware Image downloads from Cisco.com.
- Hardware Compatibility Catalog—Select if you want to synchronize your local list with Cisco.com, and to verify that the hardware you are using is compatible.

Step 5 Click **Save**.

Downloading Infrastructure Firmware Images from Cisco

Procedure

Step 1 Click the **System Tools** icon and choose **Image Library**.

Step 2 Click **Packages** to view the available packages.

Step 3 Select a package, or packages, and click the **Import Selected Image** icon.

Step 4 Click **Downloads**.

You can view information about the status of the download in the table.

Step 5 In the Transfer State column, click **Launch** to view the status dialog.

View detailed information about the download status in this dialog.

Deleting Images from the Firmware Library

The following are the options to delete firmware images from the library:

- **Deleting the firmware image** — You can delete any downloaded image in the firmware library by selecting it and clicking delete.
- **Purging the firmware image metadata** — You can delete the image metadata using the purge option. Even after you delete the firmware image from the library, the metadata will still exist. You can use the metadata information to download the actual firmware image anytime from Cisco.com even after deleting the image. If you want to completely remove the firmware image and associated metadata from the firmware image library, make sure to delete the actual firmware image and purge the metadata from the library.

Important If you have already downloaded the image corresponding to the metadata into the firmware image library, you cannot purge the metadata without deleting the image.

Deleting Image Metadata from the Library of Images

You can only purge metadata through the CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC(ops-mgr) /firmware# **scope download-source cisco**	Accesses the image metadata downloaded from Cisco website.
Step 4	UCSC(ops-mgr) /firmware/download-source# **purge list**	Deletes the firmware images metadata from the library of images.

Example

The following example shows how to delete the image metadata from the library of images:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # scope download-source cisco
UCSC(ops-mgr) /firmware/download-source # purge list
```

Capability Catalog

The Capability Catalog is a set of tunable parameters, strings, and rules. Cisco UCS uses the catalog to update the display and configurability of components such as newly qualified DIMMs and disk drives for servers.

The catalog is divided by hardware components, such as the chassis, CPU, local disk, and I/O module. You can use the catalog to view the list of providers available for that component. There is one provider per hardware component. Each provider is identified by the vendor, model (PID), and revision. For each provider, you can also view details of the equipment manufacturer and the form factor.

For information about which hardware components are dependent upon a particular catalog release, see the component support tables in the Service Notes for the B- Series servers. For information about which components are introduced in a specific release, see the Cisco UCS Release Notes.

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

- Power and thermal constraints
- Slot ranges and numbering
- Adapter capacities

Hardware-Specific Rules

- Firmware compatibility for components such as the BIOS, CIMC, RAID controller, and adapters
- Diagnostics
- Hardware-specific reboot

User Display Strings

- Part numbers, such as the CPN, PID/VID
- Component descriptions
- Physical layout/dimensions
- OEM information

Updates to the Capability Catalog

The Cisco UCS Infrastructure Software Bundle includes Capability Catalog updates. Unless otherwise instructed by Cisco Technical Assistance Center, you only need to activate the Capability Catalog update after you've downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

As soon as you activate a Capability Catalog update, Cisco UCS immediately updates to the new baseline catalog. You do not have to perform any further tasks. Updates to the Capability Catalog do not require you to reboot or reinstall any component in a Cisco UCS domain.

Each Cisco UCS Infrastructure Software Bundle contains a baseline catalog. In rare circumstances, Cisco releases an update to the Capability Catalog between Cisco UCS releases and makes it available on the same site where you download firmware images.

Note The capability catalog version is determined by the version of Cisco UCS that you are using. For example, Cisco UCS 3.x releases work with any 3.x release of the capability catalog, but not with 2.x releases. For information about capability catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Software* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Scheduling Periodic Firmware Image Synchronization

Before you begin

You must have a valid Cisco.com username and password to access the updated firmware bundles on Cisco.com. See Setting Up the Cisco.Com Account

Procedure

Step 1 Click the **System Tools** icon and choose **Image Library**.

Step 2 In the Image Library page, click **Tools** and choose **Schedule Periodic Firmware Image Syncs**.

This launches the **Periodic Firmware Image Sync** dialog box.

Step 3 Select the frequency for infrastructure firmware downloads from www.cisco.com:

- **On Demand**—Downloads the firmware image library list when the user clicks **Schedule**.
- **Daily**—Downloads the firmware image library list once per day.
- **Weekly**—Downloads the firmware image library list once per week.
- **Bi-weekly**—Downloads the firmware image library every other week.

Step 4 Click **Cisco End User License Agreement** and follow the steps to accept the EULA.

Step 5 Click **K9 TM** and follow the steps to accept the agreement.

Step 6 Click **Schedule**.

Note After installing UCS Central, or after upgrading from UCS Central v1.4 to v1.5, and after performing the initial firmware image synchronization, downloading the image catalog from Cisco.com takes 15 minutes.

Importing Firmware Bundle

Before you begin

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

Procedure

Step 1 Click the **System Tools** icon and choose **Image Library**.

Step 2 On the Image Library page, click the **Tools** icon and choose **Import Firmware Bundle**.

This launches the **Firmware Bundle Import** 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 **Open**.
d) In the **Firmware Bundle Import** dialog box, click **Import**.

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

Note Make sure that 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 a transfer protocol.
c) 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 completes, delete the firmware bundle from Cisco UCS Central.

Note Remove the firmware bundle from all associated policies before deleting it.

Creating or Editing a Host Firmware Package Policy

Procedure

Step 1 In the **Actions** bar, type **Create Host Firmware Package Policy** and press Enter.

Step 2 In the **Host Firmware Package Policy** dialog box, click **Basic** and choose the **Organization** where 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** and **Rack Version** of the firmware, as required for your environment.

Step 5 Select the required **Service Pack Version** of the firmware.

A Service pack can be applied only to the base version of a release and it should be compatible with that version. If the service pack is incompatible with the base version, the following error message is displayed:

Package Version of all bundles in the pack must match.

For more information about applicable service packs, see About Service Packs , on page 49. The service pack version rolls back to the default setting when you remove the selection from the drop-down. For more information on downloading images, see Downloading Firmware from Cisco.com in the *Cisco UCS Central Administration Guide*.

Step 6 In the **Components** tab, click **Add** to select any components that want to exclude from the firmware update.

The included and excluded components display.

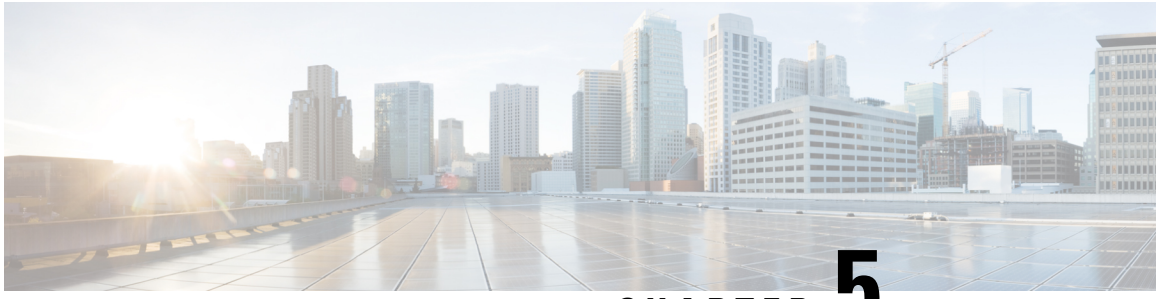
Step 7 To exclude all components, click **Excluded Components**.

Step 8 To remove an excluded component, select it and click **Delete**.

Step 9 Click **Create**.

Note To understand the impact of the policy, click **Evaluate**.

After you create a Host Firmware Package policy and associate it with a service profile template, the Service Pack images take precedence and when it is resolved, the firmware image is applied to the components accordingly.



CHAPTER 5

Firmware Management

Updating Infrastructure Firmware

Previously, users scheduled infrastructure firmware updates per domain group. Cisco UCS Central has changed that feature. Now, you schedule infrastructure firmware updates for specific domains, or domains assigned to a domain group, using maintenance groups and tags.

You can trigger infrastructure firmware updates on one domain, multiple domains, or domains belonging to a domain group, based on the product family. For example, you could update the infrastructure firmware on all of the Cisco UCS Mini systems, and not update any of the blade servers. Another example is that you could update all maintenance groups on the west coast, but none on the east coast. The following is an overview of the initial steps needed.

Procedure

Step 1 Register UCS domains with Cisco UCS Central.

See the *Cisco UCS Central Getting Started Guide* for more information.

Step 2 During registration, subscribe to the infrastructure and catalog firmware policy and make it a global policy.

See the *Cisco UCS Central Getting Started Guide* for more information.

Step 3 Download the appropriate infrastructure firmware image from the Image Library.

See Downloading Infrastructure Firmware Images from Cisco for more information.

Note The update cannot start until the entire image is downloaded.

Step 4 Create values for maintenance group tags. Apply tags to individual domains, or all domains in a domain group, to include them in a maintenance group.

See Creating Maintenance Groups and Including Untagged Domains in the Maintenance Group for more information.

Step 5 Schedule an infrastructure firmware update for a maintenance group tag.

See Scheduling an Infrastructure Firmware Update for more information.

Step 6 If you enabled user acknowledgment, then acknowledge the update in the pending activities section.

See Acknowledging an Infrastructure Firmware Update Policy for more information.

Setting the Firmware Policy to Global

The Infrastructure and Catalog firmware policy is set to local, by default, because it is so disruptive. Edit it and set it to global before scheduling a domain infrastructure firmware update. If the firmware policy is set to local, it does not affect any domain when run.

You can set the policy to global during registration, or from within Cisco UCS Central after registration. The following steps describe how to do it after registration.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Domains**.

Step 2 Select a domain.

Step 3 In the domain page, click the Tools icon and choose **Edit Policy Resolution Control**.

Step 4 In the Infrastructure and Catalog Firmware slot, click **Global**.

Step 5 Click **Save**.

Maintenance Groups

A maintenance group contains a collection of selected domains, or all of the domains assigned to a domain group, for which you want to update the firmware simultaneously. You can upgrade the firmware immediately, or with a schedule. You can require a user to acknowledge the upgrade, or it can start automatically.

A maintenance group tag, or value, allows you to group a collection of domains. You can group domains based on geographic location, job function, hardware, or any other business need. You can also apply a maintenance tag to all of the domains in a domain group.

Important A domain can only have one maintenance group tag assigned to it concurrently.

Catalog Version for Firmware Updates

You can select one catalog per domain infrastructure update scheduled job. Each catalog version only applies to one product family. Therefore, it is a best practice, when updating the catalog, to create a maintenance group which contains only those domains with identical product families. Then, Cisco UCS domains included in that maintenance group are updated with the capability catalog defined for that product family. If you include other product families in that maintenance group, their catalog version is not updated.

Creating Maintenance Groups and Including Untagged Domains in the Maintenance Group

When you initially upgrade to Cisco UCS Central, create maintenance groups and tag domains, or all domains assigned to a domain group, from the Actions bar.

Note You can only tag domains, or a domain group, that are not already tagged with a maintenance group tag.

Procedure

Step 1 In the Actions table, type **Create Maintenance Group Tag** and press **Enter**.

Step 2 Enter a name for the **Maintenance Group Tag Name**.

Step 3 Select how to apply tags to domains:

- **By Domain Group**

  The Maintenance Group tag applies to all domains within the selected domain group. It will not be applicable to any new domains that get added further to the domain group. If you select to include sub-domain groups, the Maintenance Group tag also applies to all of the domains in the sub-domain groups.

- **Manually**

  Manually select domains for inclusion in this Maintenance Group. The domains can belong to a domain group or be ungrouped.

Step 4 Follow the steps for your choice:

If you selected	Do the following
By Domain Group	**1.** Select a domain group in the drop-down list. **2.** Select whether to include all domains from the sub-domain groups. **3.** Click **Create**.

If you selected	Do the following
Manually	**1.** Click **Add** and select domains for inclusion in the Maintenance Group. **2.** Scroll down and click **Select**. **3.** Click **Create**.

Creating Values for Maintenance Group Tags

If you want to create multiple Maintenance Group tags, create them in the Tag type page.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Tag Management**.
Step 2 Click **Tag Types**.
Step 3 Click **Maintenance Group** to select it.
Step 4 Click **Edit**.
Step 5 In the Maintenance Group dialog box, click **Values**.
Step 6 Click **Add** and add a name for the maintenance group.
Step 7 Repeat the previous step to add all of the values that you need for the maintenance groups.
Step 8 Click **Save**.

Tagging a Domain or Domain Group for Inclusion in a Maintenance Group

You can only apply one maintenance group tag to a domain. Currently, Cisco UCS Central does not support applying multiple maintenance group tags to a domain.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Domains**.
Step 2 Select a domain, or filter them based on domain group, to select all domains assigned to a domain group.

Note For individual domains, it does not matter if the domain is in a domain group or if it is ungrouped. That does not affect the domain infrastructure firmware update.

Step 3 Click **Tag**.
Step 4 In the Add Tag dialog box **Type** field, select **Maintenance Group**.
Step 5 In the **Value** field, select a value.
Step 6 Click **Add**.
Step 7 Repeat for all of the domains that you want to include in this maintenance group.

To include all of the domains in the list in your maintenance group, select the domain option in the heading and click **Tag**.

Step 8 If you want to include multiple domain groups in a maintenance group, they must be sub-domains of the parent domain group. Filter based on the domain group and sub-domain group, and then tag all of the domains from that search result.

Scheduling an Infrastructure Firmware Update

In the Infrastructure Firmware update page, you can create new scheduled jobs or modify jobs already created for a future date.

Procedure

Step 1 Click the **System Tools** icon and choose **Firmware Management**.

Step 2 On the Firmware Management page, click the **Tools** icon and choose **Schedule Infrastructure Firmware Update**.

Step 3 In the Infrastructure Firmware Update dialog box, select a tag from the **Maintenance Group** drop-down list.

Step 4 Select the UCS fabric interconnects product family and appropriate firmware versions from the **Infrastructure firmware version** drop-down, to use for the update.

You do not need to update all of the available hardware systems. You can also update different hardware types with different firmware versions.

Step 5 Select the compatible **Service Pack Version** from the drop-down for the fabric interconnects product family.

Service packs are supported from Cisco UCS Manager 3.1(3) and later. If you do not select a service pack, the firmware version is rolled back to the base applicable version for the release. For more information about the supported/applicable service pack versions, see About Service Packs , on page 49.

Note Downgrade of a Cisco UCS domain installed with a Service Pack 3.1(3) or earlier is not supported.

Infrastructure update through a service pack is not supported in the case of an upgrade to Cisco UCS Manager release 3.1(3) from Cisco UCS Manager 3.1(2) or lower versions. In this case, Cisco UCS Manager does not recognize a service pack and the upgrade proceeds considering only the base version.

Step 6 (Optional) Select the catalog version in the **Catalog version** drop-down list for the product family.

Step 7 (Optional) Select the **Force Deploy** option for the product family. When you select **Enable**, Cisco UCS attempts installation even if the previous attempt to install the selected version failed or was interrupted. Upgrade fails when there are upgrade validation failures, and you must resolve the faults and then select the **Force Deploy** option again to continue with the upgrade.

Force Deploy and Fabric Evacuation options are disabled by default. These options are supported only on Cisco UCS Manager, release 3.1(3) and later and do not work on earlier Cisco UCS Manager versions, even if you select the **Enable** option. Select **Configuration Status** from the **Tools** menu drop-down or click the **Domain Status** table to view the status of fabric evacuation.

Step 8 (Optional) Select the **Fabric Evacuation** option for the product family to stop or start traffic on the IO module or the fabric interconnect during AutoInstall.

Step 9 If you want to trigger a firmware update immediately, click **Immediately** in the **Trigger Firmware Update** field.

Step 10 If you want to schedule a firmware update, select the date and time for the update in the **Schedule Infrastructure Firmware update** field.

Step 11 Select whether the update requires user acknowledgment in the **User acknowledgment required to install** field.

- **Enabled**—(Default value) You must manually acknowledge the update request before the domain is updated.

  Note Acknowledgment is per domain, even if the maintenance group includes a domain group.

- **Disabled**—The firmware update runs as scheduled.

Step 12 Click **Schedule**.

You can monitor the firmware update on the **Firmware Management** page. The scheduled firmware updates display in the job list.

Note Deleting a tag in a Maintenance Group interrupts the assigned Firmware Update schedule. If a tag is deleted, the corresponding Infrastructure Update policy on the respective Cisco UCS domain will also get deleted, and the policy ownership will be in the Pending Global state. To trigger an Infrastructure Update again, you must delete the old policy on Cisco UCS Central, and re-create the tag or create a new tag and a policy.

The desktop Firmware Management widget displays all of the jobs scheduled for firmware updates. You can check the status of the firmware updates in the **Configuration Settings** window.

Editing a Scheduled Infrastructure Firmware Update Job

Procedure

Step 1 Click the **System Tools** icon and choose **Firmware Management**.

Step 2 Select the specific job in the job list and click **Edit**.

Step 3 Make the appropriate changes and click **Schedule**.

Note You cannot edit a job that is already in triggered or latest triggered state.

Acknowledging an Infrastructure Firmware Update Policy

If you set an infrastructure firmware update job to require user acknowledgment before starting, Cisco UCS Central does not start the upgrade until this acknowledgment occurs.

Procedure

Step 1 In the Domains Impacted table, when the Firmware Status column changes to Start Pending, click the **Alerts** icon and choose **Pending Activities**.

Step 2 Click **Acknowledge** to start the firmware update for the domain.

Step 3 When the Firmware Status column changes to **Pending User Acknowledgment**, this indicates that Cisco UCS Central requires a user acknowledgment to reboot the fabric interconnects. Repeat steps 1 and 2 to acknowledge the reboot.

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:

- **Maintenance group**—The maintenance group name.
- **Scheduled for**—The details of the scheduled firmware update and the status if it has already been triggered.
- **User Ack**—Status of user acknowledgment. If **User Ack** is **Enabled**, requires user acknowledgment on the **Alerts** > **Pending Activities** page before it updates the firmware.

The following details of the scheduled **Infrastructure Firmware Management** for a **Maintenance Group** are displayed on the right panel:categorized by the , the selected , and the selected **Service Pack Version** are displayed on the right panel.

- **Product family**— The appropriate FI product family
- **Firmware Version**— The selected firmware version
- **Service Pack Version**— The selected service pack version for the product family. You cannot select an incompatible service pack version and schedule an upgrade. For more information about the supported service pack versions for Cisco UCS Manager releases, see About Service Packs , on page 49.
- **Catalog Version**— Details of the catalog versions of a product family.
- **Force Deploy**— The Force Deploy option for the product family. When **Enabled**, Cisco UCS attempts installation even if the previous attempt to install the selected version of the firmware update failed or was interrupted.
- **Evacuation**— Evacuation option for the product family to stop or start traffic on the IO module or the fabric interconnect during AutoInstall.
- **Impacted Domain**— Current Version, Targeted version of the service pack that you are deploying, Firmware Status and the Domain status for the impacted domain.

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.

Preventing an Infrastructure Firmware Update

There are multiple methods for preventing an infrastructure firmware update:

- Canceling an Infrastructure Firmware Update job
- Removing or excluding a domain from a maintenance group
- Deleting a value for a maintenance tag

Removing or Excluding a Domain from a Maintenance Group

If you wish to remove a domain from a maintenance group which affects multiple domains, then delete the maintenance tag assigned to the domain before you start the upgrade. This prevents the policy from impacting the domain. If the domain is untagged after the infrastructure firmware update starts, then the domain is updated.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Domains**.

Step 2 Select a domain.

The assigned tag displays underneath the IP address.

Step 3 Click the **X** in the maintenance tag name label to untag it and remove it from the maintenance group.

A warning displays.

Step 4 Click **Delete**.

Canceling a Firmware Update Job

This cancels the job for all of the included domains.

Procedure

Step 1 Click the **System Tools** icon and choose **Firmware Management**.

Step 2 Select the job in the job list.

Step 3 Click **Delete**.

Deleting a Value for a Maintenance Group

Important Before you delete a value, or tag, for a maintenance group, check that no jobs are associated with it.

- If you delete a maintenance tag **before** the upgrade starts, then the upgrade process deletes after notifying the user.
- If you delete a maintenance tag **after** the upgrade starts, the upgrade continues.
- If you delete a maintenance tag and the job is scheduled for the future, and then you re-create the maintenance tag, the job runs on the domain.
- When you delete a maintenance tag, the job does not delete. It is saved for historical purpose so that you can see what jobs were scheduled and which domains were impacted.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Tag Management**.

Step 2 Click **Tag Types**.

Step 3 Click **Maintenance Group** to select it.

Step 4 Click **Edit**.

Step 5 In the Maintenance Group dialog box, click **Values**.

Step 6 Select the tag and click **Delete**.

Infrastructure Firmware Updates and Disaster Recovery

Cisco UCS Central performs two kinds of backups:

Backup for Cisco UCS Domain—Creates a binary file that includes a snapshot of an entire Cisco UCS Manager domain. The scheduled infrastructure firmware upgrade jobs are not contained in UCS domains. Therefore, restoring a domain does not affect scheduled infrastructure firmware upgrade jobs.

Backup for Cisco UCS Central—Creates a binary file that includes a snapshot of the entire Cisco UCS Central system. You can use the file generated from this backup to restore the system during disaster recovery. Restoring from this backup can affect the job schedule.

Important Due to the impact of upgrading to release 2.0 of Cisco UCS Central, we recommend that you perform all domain group updates before you upgrade. Make sure that you have no update jobs pending user-acknowledgment. All jobs are deleted during the upgrade and must be recreated in release 2.0.

Scenario	Impact
You restore a Cisco UCS Central backup that had jobs scheduled in the **past**.	**No impact:** Updates are not affected. The backup file contains the maintenance tag and registered domains information. It does not contain the previous jobs so nothing is impacted. It does not run jobs scheduled for a previous date.
You restore a Cisco UCS Central backup that had jobs scheduled in the **future**.	**No impact**: The jobs execute as scheduled.
Your Cisco UCS Central system crashes while it is running an infrastructure firmware update.	**Impact**: Jobs do not run once you recover your Cisco UCS Central system. You must reschedule them.
You restore a configuration backup.	**No impact**: Configuration backups do not contain any job information, but they do contain maintenance tag information. If you restore from a configuration backup using the replace option, the restored system does not contain any job information. If you restore using the merge option, and had jobs scheduled for a future date, then any tagged domain, from the backup, are included in the future jobs. (This information displays in the impacted domains list)
You merge a full state backup with a current system.	**Some Impact**: Does not override what you currently have scheduled, but it doesn't restore job descriptions so you must recreate the jobs.
The Cisco UCS Manager domain loses visibility and becomes unregistered before or during an update.	**Impact**: Update does not start again once the domain regains visibility. You must start it manually, (on-demand).
You create a full state backup. You untag a domain. You restore from the backup.	**Impact**: The domain was tagged in the backup, so it is still tagged when you restore that backup. If the job was scheduled for the future, the domain is included. To prevent this, untag the domain again.
Job is running, you want to edit it.	**No impact**: You cannot edit a job while it is in progress. However, you can remove the maintenance tag from a domain, or delete the job, before acknowledging the first pending-acknowledgment request.

Scenario	Impact
An HA failover occurs.	**No impact**: Scheduled jobs occur normally.
Upgrade from a previous release of Cisco UCS Central.	**Impact**: Prior versions performed firmware updates per domain group. The current version performs updates per maintenance group. No domain group or scheduled jobs information is saved or transferred during the upgrade. You must create the maintenance groups and tag domains for inclusion. You must also recreate and reschedule all infrastructure firmware update jobs.

About Lightweight Upgrade

Cisco UCS Central 2.0 introduces a Lightweight upgrade that enhances firmware upgrade and delivers security updates through service packs. Service packs are specific and cumulative to a maintenance release. Cisco UCS Central supports firmware upgrades through service packs for Cisco UCS Manager versions 3.1(3) and later.

- Lightweight upgrade enhances firmware upgrade in the following ways:
  - The firmware version of a component will be updated only if it has been modified.
  - Security updates will be provided through service packs.
  - Within a service pack, updates may only apply to certain components. These components may, at times, be upgraded without an endpoint reboot.
  - Infrastructure and server components updates are delivered through a common service pack bundle. For server components, only the modified firmware images will be part of the service pack bundle.

About Service Packs

Service packs are patches that you can use to apply security updates to Cisco UCS Manager infrastructure and server components. Service packs are specific to a base release. A service pack is provided as a single bundle for infrastructure and server components.

The following guidelines apply to service pack versions:

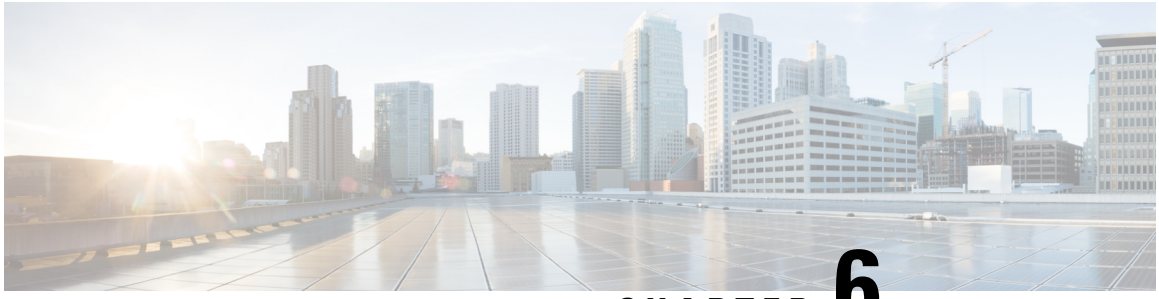
- A service pack can be applied only on its base bundle. You cannot install the service pack independently. For example, service pack 3.1(3)SP2 can be applied only on a 3.1(3) release. It is not compatible with a 3.1(4) or later release.
- Service packs are cumulative. You can use the latest service pack version with any patch version within the same maintenance release. For example, 3.1(3)SP3 will contain all the fixes that went into 3.1(3)SP2 and 3.1(3)SP1. You can apply 3.1(3)SP3 on any 3.1(3) release.
- Service pack version numbering in separate maintenance releases are unrelated. For example, service packs 3.1(3)SP2 and 3.1(4)SP2 are separate and unrelated.

- The same fix can be made available for separate maintenance releases through separate service packs. For example, the same fix can be made available in 3.1(3)SP2 and 3.1(4)SP3.
- You cannot downgrade service packs to versions below the default service pack version for a maintenance release. For example:
  - Base Bundle Version: 3.1(3b)
  - Default Service Pack Version: 3.1(3)SP2(Default)
  - Running Service Pack Version: 3.1(3)SP3
  - Service pack cannot be downgraded below 3.1(3)SP2
- When an upgrade or downgrade of a service pack fails, the default service pack version for that maintenance release becomes the running service pack version.
- You can roll back a service pack that was applied to a base release by removing the service pack selection.

The following table lists the Cisco UCS Manager release versions and the running version deployed in different situations when a service pack is applied:

Update Scenario	Bundle Version	Service Pack Version
Update to a service pack within the same maintenance release	No change is made to the bundle version	Service pack is updated to the specified version
Remove Service Pack	No change is made to the bundle version	Service pack is the default version that comes with the bundle
Update base bundle to another maintenance release	Base bundle changes to the version of the specified maintenance release	Current service pack is removed and is updated to the default version for the base bundle
Update to another maintenance release, and service pack	Base bundle changes to the version of the specified maintenance release	Service pack is updated to the specified version

For more information about selecting the compatible service packs for a firmware upgrade, see *Host Firmware Package Policy*, *Scheduling Firmware Infrasturcture Update*, and *Chassis Firmware Package Policy*.



CHAPTER 6

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. You can also 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 back up Cisco UCS Central or the registered UCS domains, 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.

Cisco UCS Central restricts remotely configured policies to using 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 that you want to save for either 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. Change the backup type before you rerun the backup operation. We recommend that you change the filename for easier identification 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.

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. Reconfigure the ports from Cisco UCS Central.

Backup Types

You can perform one or more of the following types of backups in Cisco UCS Central:

- **Full-state**— You can specify full state backup only during installation. Full state backup is a binary file that includes a snapshot of the entire system. You can use the file generated from this backup to restore the system during disaster recovery. You cannot use this file for an import.

  Note You can only use a full state backup file to restore a system that is running the same version as the system from which the backup file was exported.

- **Config-all**— All configuration back up is an XML file that includes all system and logical configuration settings. You cannot use this file for a system restore during installation.
- **Config-logical**— Logical configuration back up is an XML file that includes all logical configuration settings. These include service profiles, VLANs, VSANs, pools, policies, users, locales, LDAP, NTP, DNS authentication and administration settings. You can use the file generated from this backup to import these configuration settings. You cannot use this file for a full state system restore during installation.
- **Config-system**— System configuration back up is an XML file that includes statistics configuration and scheduler information. You can use the file generated from this backup to import these configuration settings. You cannot use this file for a full state system restore during installation.

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 a backup file in the remote location:

- Absolute remote path. For example, if the transfer protocol is SCP: */home/user01/central*
- Host name or IP address for the remote server
- User name and password for the remote server

Procedure

Step 1 In the **Actions** bar, type **Schedule Central Backup** and press **Enter**.

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

Step 3 From the **Schedule** drop-down, choose a schedule for this backup:

- **One Time Schedules**—Backup occurs at the scheduled date and time only.
- **Recurring Schedules**—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 20.

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** field, click **Enabled**.

Note The remote absolute path is */home/user01/central*.

Complete the following fields to add the remote location related information.

Field Name	Description
Transfer Protocol	Choose the transfer protocol: • 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.

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

Procedure

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.

Field Name	Description
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 backup 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: `/home/test/central/file.tgz`
- Host name or IP address of the remote server
- Username and password for the remote server

Procedure

Step 1 Click the **System Tools** icon and choose **Backup & Restore**.

Step 2 In the UCS Central and Domains list, click **UCS Central** or select a domain group.

Step 3 Click the **Backup** icon.

Step 4 In the **Backup** dialog, choose whether to enable or disable **Remote Copy**.

If you select **Disabled**, a local backup copy is 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**.

Cisco UCS Central creates and saves the full state backup file in the specified remote location. To view the backup state for Cisco UCS domains, click the domain group name.

Note The following error message displays 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, resubmit the configuration. On successful resubmission, Cisco UCS Central creates a backup file in the backup repository.

Removing Full State Backup for Cisco UCS Domain

In addition to the procedure described below, you can disable or delete a full state backup in the following scenarios:

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

Procedure

Step 1 On the menu bar, click the **System Tools** icon and choose **Backup & Restore**.

Step 2 In the Backup and Restore page, click the **Tools** icon and choose **Remove Domain Backup Schedule**.

Step 3 In the **Domain Backup Schedule** dialog box, 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, you can disable or delete a full state backup for Cisco UCS Central in the following scenario:

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

Procedure

Step 1 Click the **System Tools** icon and choose **Backup & Restore**.

Step 2 In the Backup and Restore page, click the **Tools** icon, and choose **Remove Central Backup Schedule**.

Step 3 In the **Central Backup Schedule** dialog box, 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

Procedure

Step 1 Click the **System Tools** icon and choose **Backup & Restore**.

Step 2 In the UCS Central and Domains list, choose UCS Central or a domain.

Step 3 In the right side pane, view the list of backup files. For each backup file, you can view the status, schedule, maximum number of files and the location for the remote copy.

Configuration Export and Import

From the Export & Import, you can schedule configuration backups 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 stored remotely. If you schedule a backup, it can be stored locally or remotely.

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.

Cisco UCS Central restricts remotely configured policies to using 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 57), 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 they unregister from their Cisco UCS domains.

Backup Image Files

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

- **Local**: In a local file system.
- **Remote Location**: Remote locations using any one of the following protocol: 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 does not work.

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

Importing Configuration Files

You can use the saved configuration from a backup repository to import and configure any of the managed Cisco UCS domaina. Use the 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

Procedure

Step 1 On the menu bar, click the **System Tools** icon and choose **Export & Import**.

Step 2 In the UCS Central and Domains list, click **UCS Central**.

Step 3 Click the **Tools** icon and choose **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

Procedure

Step 1 Click the **System Tools** icon and choose **Export and Import**.

Step 2 In the UCS Central and Domains list, click the **Tools** icon and choose **Schedule Domain Export**.

Step 3 Select the domain group for which you want to schedule the configuration backup.

Step 4 Click the **Schedule** drop-down to select a schedule for this backup.

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

Step 5 In the **Maximum No of Backup Files** field, specify the number of backup files to keep in the system.

Step 6 (Optional) If you want to save the backup file in a remote location, in the **Remote Copy** field, click **Enabled**.

Enter the remote location and related information in the displayed fields.

Step 7 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

Procedure

Step 1 Click the **System Tools** icon and choose **Export and Import**.

Step 2 In the UCS Central and Domains list, click **UCS Central**.

Step 3 Select the configuration backup file that you want to export.

Step 4 Click the **Config Export** icon.

Step 5 Required: 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 6 For remote locations, choose a **Transfer Protocol**, and enter the required remote location information in the displayed fields.

Step 7 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

Procedure

Step 1 Click the **System Tools** icon and choose **Export and Import**.

Step 2 In the UCS Central and Domains list, choose a domain.

Step 3 Select the domain backup file that you want to export.

Step 4 Click the **Config Export** icon.

Step 5 Required: 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 6 Required: Choose a **Transfer Protocol**, and enter the required remote location information in the displayed fields.

Step 7 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.

Procedure

Step 1 Click the **System Tools** icon and choose **Export and Import**.

Step 2 In the UCS Central and Domains list, choose UCS Central.

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

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 the configuration into Cisco UCS Central:

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

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.

Procedure

Step 1 Click the **System Tools** icon and choose **Export and Import**.

Step 2 In the UCS Central and Domains list, click the domain where you want to import the backup.

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

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.

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

Step 7 Click **Import**.

Removing Configuration Export Schedule for Cisco UCS Central

Procedure

Step 1 Click the **System Tools** icon and choose **Export and Import**.

Step 2 On the Config Export & Import page, click the **Tools** icon and choose **Remove Central Export Schedule**.

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 subdomain 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.

Procedure

Step 1 Click the **System Tools** icon and choose **Export and Import**.

Step 2 On the Config Export & Import page, click the **Tools** icon and choose **Remove Domain Export Schedule**.

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**.

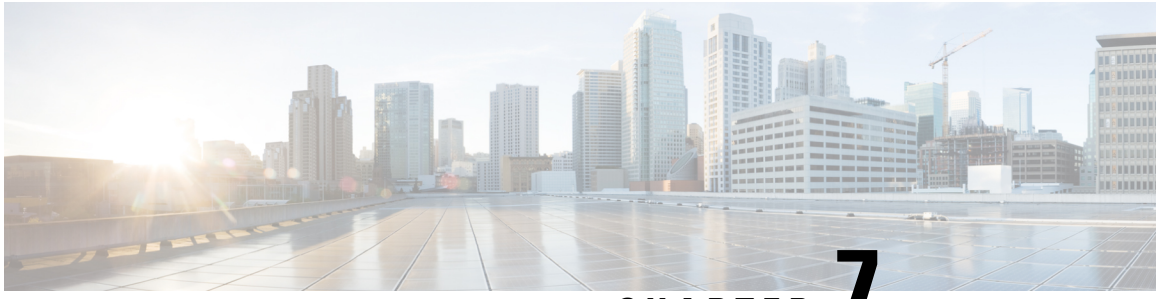
Viewing Backup Files in Cisco UCS Central

Procedure

Step 1 Click the **System Tools** icon and choose **Backup & Restore**.

Step 2 In the UCS Central and Domains list, choose UCS Central or a domain.

Step 3 In the right side pane, view the list of backup files. For each backup file, you can view the status, schedule, maximum number of files and the location for the remote copy.



CHAPTER 7

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.

Procedure

Step 1 Click the **System Configuration** icon and 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 for the main contact.

Cisco UCS Central sends the initial registration and alert notifications 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 Only self-signed certificates are 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. You cannot delete this profile, 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.

You do not receive any notification 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, Cisco UCS Central automatically sends the system inventory to the Cisco Smart Call Home servers. It sends an automated email message 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 activates. If you entered a valid contract ID, your registration is complete. Make sure that you enter the contract ID and send the inventory before 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.

Fault Name	Fault Code	Explanation
fltSysdebugCoreCoreFile	F10000005	Fault occurs when one of the processes stops responding. Cisco UCS Central generates a core file.
fltExtpolProviderProviderLostConnectivity	F10000190	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	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	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	Two or more service profiles possess the same ID. 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	Fault occurs when the statistics database is configured incorrectly or if the database is down or out of disk space.
fltPkiTPStatus	F10000591	Fault occurs when the TrustPoint certificate status has become invalid.
ltPkiKeyRingStatus	F10000592	Fault occurs when the Keyring certificate status 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	Fault occurs when the partition disk usage exceeds 70% but is less than 90%.

Fault Name	Fault Code	Explanation
fltStorageItemCapacityWarning	F10000035	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.

Procedure

Step 1 Click the Domain Group Navigation icon and choose the domain group in which you want to configure Call Home.

Choose Root to view alerts for all registered domains.

Step 2 Click **Settings** and launch 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.

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

If you want to **Send Inventory Now** on a specific UCS Domain you can do it locally on Cisco UCS Manager by making the Monitoring policy Local. The **On Demand Call Home** inventory is not supported at the domain group level.

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

a) **Basic**—Enter the description and maximum email size, and select the debug level and email format.
b) **Alert Groups**—Select the type of alerts that you want to receive.
c) **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.

Step 8 Click **Save**.