Cisco UCS Central Software User Manual for HTML5 GUI, Release 1.3

First Published: April 06, 2015

Last Modified: June 29, 2016

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

CONTENTS

Preface

This preface includes the following sections:

Audience

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

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

Conventions

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

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

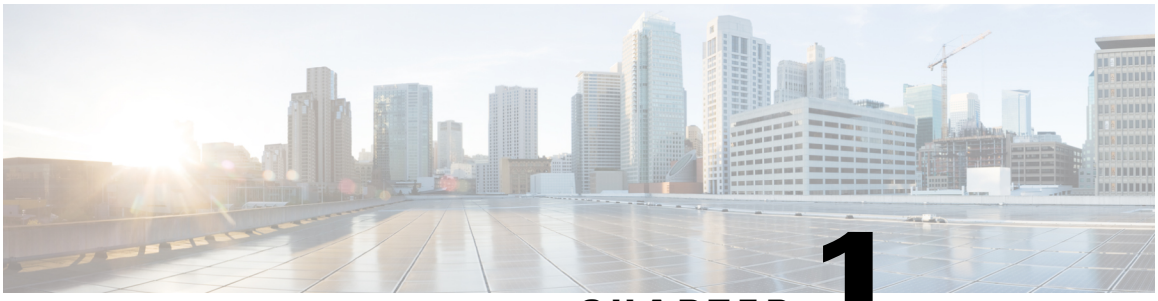
For information on supported firmware versions and supported UCS Manager versions for the rack servers that are integrated with the UCS Manager for management, refer to Release Bundle Contents for Cisco UCS Software.

Other Documentation Resources

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

Documentation Feedback

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



CHAPTER 1

Overview

This chapter includes the following sections:

Introducing Cisco UCS Central

Cisco UCS Central provides scalable management solution for growing Cisco UCS environment. Cisco UCS Central simplifies the management of multiple Cisco UCS domains from a single management point through standardization, global policies and global ID pools. Cisco UCS Central does not replace Cisco UCS Manager, which is the policy driven management for single UCS domain. Instead Cisco UCS Central focuses on managing and monitoring the UCS domains on a global level, across multiple individual Cisco UCS Classic and Mini management domains worldwide.

Cisco UCS Central enables you to manage individual or groups of classic, mini or mixed Cisco UCS domains with the following:

- Centralized Inventory of all Cisco UCS components for a definitive view of the entire infrastructure and simplified integration with current Information Technology Infrastructure Library (ITIL) processes.
- Centralized, policy-based firmware upgrades that can be applied globally or selectively through automated schedules or as business workloads demand
- Global ID pooling to eliminate identifier conflicts
- Global administrative policies that enable both global and local management of the Cisco UCS domains
- An XML API, building on the Cisco UCS Manager XML API for easy integration into higher-level data center management frameworks
- Remote management to manage various end points in registered Cisco UCS domains

Cisco UCS Central does not reduce or change any local management capabilities of Cisco UCS Manager, such as its API. This allows you to continue usingCisco UCS Manager the same way as when you did not have Cisco UCS Central, and also allows all existing third party integrations to continue to operate without change.

Cisco UCS Central Features

The following table provides a list of features with brief description on the management capabilities of Cisco UCS Central:

Feature	Description
Centralized inventory	Cisco UCS Central automatically aggregates a global inventory of all registered Cisco UCS components, organized by domain, with customizable refresh schedules and provides even easier integration with ITIL processes, with direct access to the inventory through an XML interface.
Centralized fault summary	Cisco UCS Central enables you to view the status of all Cisco UCS infrastructure on the global fault summary panel, with a fault summary organized by domain and fault type. Also provides you the ability to view individual Cisco UCS Manager domains for greater fault detail and more rapid problem resolution. Drilling down on a fault launches the UCS Manager in context for a seamlessly integrated experience.
Centralized, policy-based firmware upgrades	You can download firmware updates automatically from the Cisco.com to a firmware library within Cisco UCS Central. Then schedule automated firmware updates, globally or selectively, based on your business requirements. Managing firmware centrally ensures compliance with IT standards and makes reprovisioning of resources a point-and-click operation.
Global ID pools	Cisco UCS Central eliminates identifier conflicts and ensures portability of software licenses. You are able to centralize the sourcing of all IDs, such as universal user IDs (UUIDs), MAC addresses, IP addresses, and worldwide names (WWNs), from global pools and gain real-time ID use summaries. Centralizing server identifier information makes it simple to move a server identifier between Cisco UCS domains anywhere in the world and reboot an existing workload to run on the new server.
Domain groups	Cisco UCS Central simplifies policy management by providing options to create domain groups and subgroups. A domain group is an arbitrary grouping of Cisco UCS domains that can be used to group systems into geographical or organizational groups. Each domain group can have up to five levels of domain sub groups. This provides you the ability to manage policy exceptions when administering large numbers of Cisco UCS domains. Each sub group has a hierarchical relationship with the parent domain group.

Feature	Description
Global administrative policies	Cisco UCS Central helps you to ensure compliance and staff efficiency with global administrative policies. The global policies are defined at the domain group level and can manage anything in the infrastructure, from date and time and user authentication to equipment power and system event log (SEL) policies.
Global service profiles and templates	Global service profiles and templates in Cisco UCS Central enables fast and simplified infrastructure deployment and provides consistency of configurations throughout the enterprise. This feature enables global bare-metal workload mobility very similar to how hypervisor enables virtualized workload mobility.
Backup	Cisco UCS Central provides an automatic backup facility that enables quick and efficient backing up the configuration information of the registered Cisco UCS domains and the UCS Central configuration.
High availability	As with all Cisco UCS solutions, Cisco UCS Central is designed for no single point of failure. High availability for Cisco UCS Central Software allows organizations to run Cisco UCS Central using an active-standby model with a heartbeat that automatically fails over if the active Cisco UCS Central does not respond.
XML API	Cisco UCS Central, just like Cisco UCS Manager, has a high-level industry-standard XML API for interfacing with existing management frameworks and orchestration tools. The XML API for Cisco UCS Central Software is similar to the XML API for Cisco UCS Manager, making integration with high-level managers very fast.
Remote Management	Cisco UCS Central enables you to manage various end points in the registered Cisco UCS domains from one management point. You can manage chassis, servers, fabric interconnects, and fabric extenders from Cisco UCS Central GUI or CLI. You can also access tech support files for registered UCS domains from Cisco UCS Central.

Overview of Cisco UCS Central HTML 5 UI

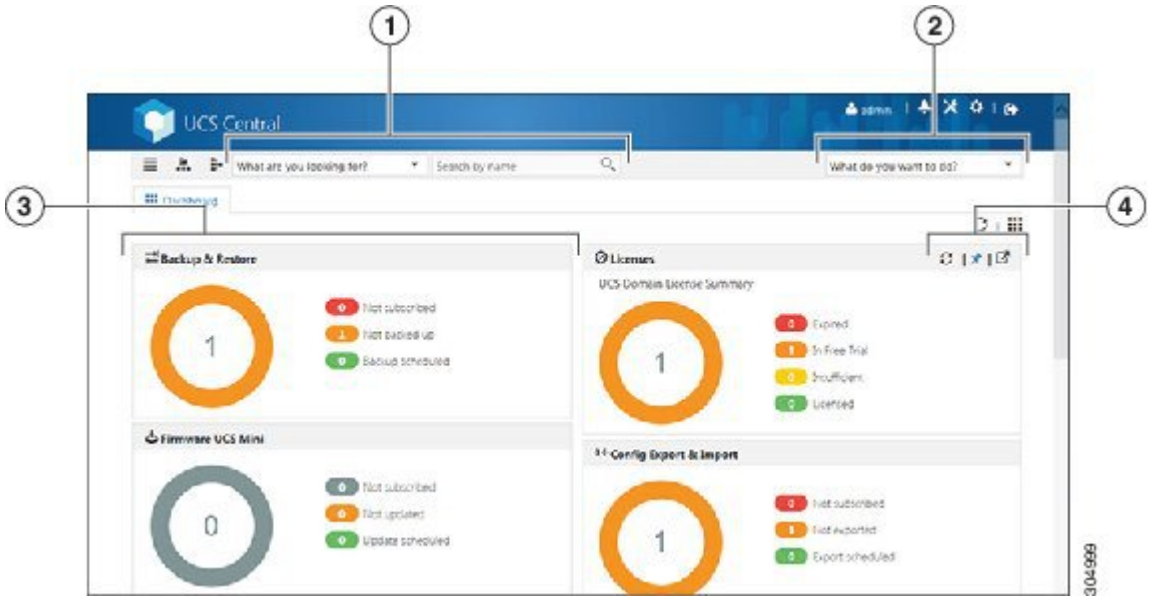
Cisco UCS Central HTML5 based user interface provides flexibility and task based usability for your management purposes.

The dashboard provides a quick overview of components in the system. You can pin the components you use frequently and customize the dashboard to suit your operational requirements. You can click on any object on the dashboard to go to the related page in the system. Click **Play** on this Video to view a brief introduction to the HTML 5 UI.

Using the HTML5 UI

Dashboard

You can pin dashboard widgets and customize the dashboard based on your operational requirements. The following is the basic dashboard structure:

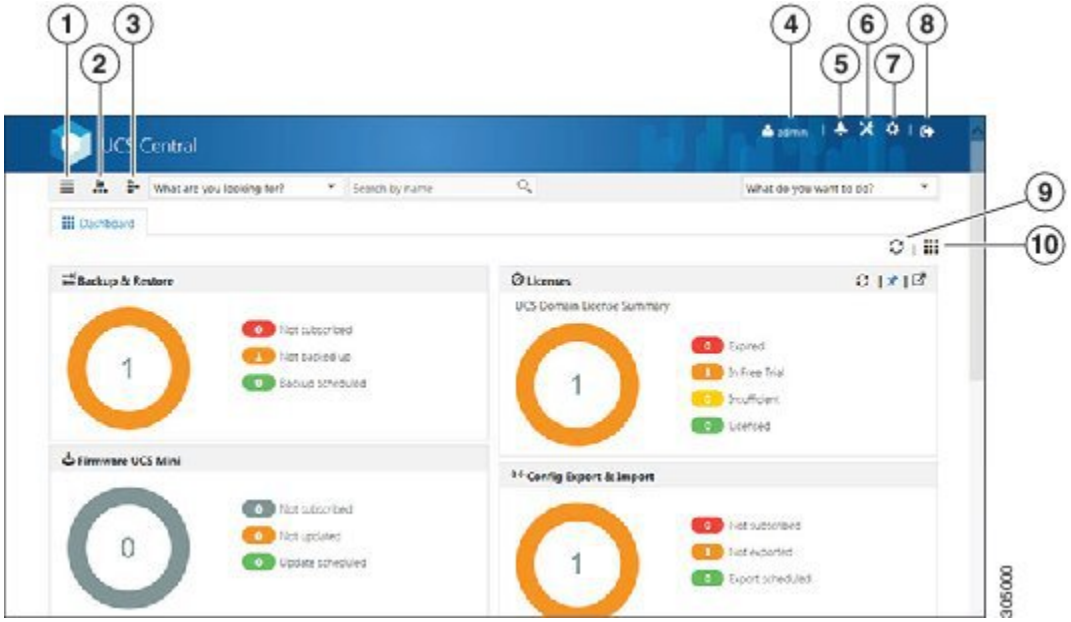


Item	Description
1	Search bar. **What are you looking for?**. You can do the following: • Select the entity type to search for any entity in the system by name. Empty search string returns all entities. • Filter search results by location and status when applicable. • Click on an entity in the search results to open the details in a new page.
2	Actions bar. **What do you want to do?**. You can Create, Schedule, Install, Export and Import from here: • Click drop down to display available actions and select a task or type the task in the field and launch the dialog box and perform the task.
3	Dashboard widget. You can pin any widget on this dashboard. When you mouse over on the widget, other options are enabled on widget's menu bar.

Item	Description
4	From within any widget on the dashboard, when you display additional options, you can do the following: • Refresh the displayed information for this specific widget. • Unpin this widget from the dashboard. • Launch the details page for this operation.

Navigation Icons

The following navigation icons help you navigate around the product to perform management tasks:



Item	Description
1	Search icon. Click to display physical and logical inventory related entities in the system such as, **Domains**, **Fabric Interconnects**, **Servers**, **Chassis**, **FEX**, **vLANs**, **vSANs**, **Service Profiles**, **Templates**, **Pools**, **Policies** and **ID Universe**. Click on any of these entities to launch related page and view details.
2	Organization icon. Click to display org **root** and other sub organizations in the system. You can click on the root or any sub org to launch the details page for a selected org.
3	Domain group icon. Click to display domain group **root** and other domain groups in the system. You can click on a domain group to launch the details page.

Item	Description
4	**User Preferences** icon. Click to launch **User Settings**. From here you can **Change Password**, **Restore Dashboard Defaults**, and **Show First Launch Experience**.
5	Alerts icon. Click to display and navigate to **Pending Activities**, **System Faults**, **Domain Faults**, **Events**, **Audit Logs**, **Core Dumps**, **Sessions** and **Internal Services**.
6	Operations icon. Click to display and navigate to **Firmware**, **Backup & Restore**, **Export & Import**, **Licenses** and **Tech Support**.
7	System Settings icon. Click to display and navigate to **System Profiles**, **System Policies**, **Users**, **Authentication** and **SNMP**.
8	Log out icon. Click to log out from the active UCS Central session.
9	Refresh icon. Click to **Refresh** information in all pinned widgets. Each widget has individual refresh icons to refresh data for individual widgets.
10	Dashboard widgets library icon. Click to view available widgets and click on the widget to pin it to the dashboard.

Behavior and Design Changes in HTML5 UI

Feature Support

The following features that are available in the current UI are not supported in the HTML5 UI at this time:

- Policy Import
- Threshold Policy
- Statistics

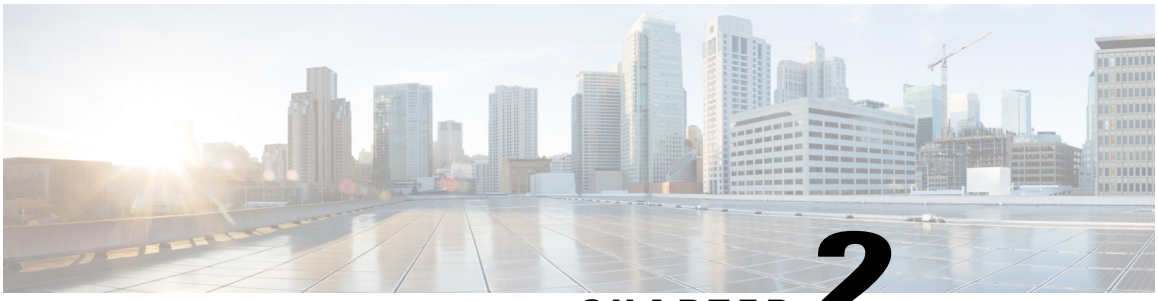
Behavior Changes Based on Design

- You can only create global service profiles using an initial or updating template that uses LAN or SAN connectivity policy. You must create the global service profile template before you can create a service profile.
- The following inline options are not available in a service profile:
  - Manual vNIC
  - iSCSI
  - vHBA
  - Boot Policy

- Static ID

If you have an existing global service profile with any of these options, you cannot edit the global service profile in the HTML5 UI.

- Any changes to the iSCSI boot parameters made in HTML5 UI will not be available in the Flex UI.
- You can use vNIC templates only in a LAN connectivity policy.
- You can use vHBA templates only in a SAN connectivity policy.
- vNIC and vHBA Placement is now referred to as Interface Placement.
- Registration Policy is now referred to as Domain Group Qualification Policy.
- ID Range Qualification Policy is now referred to as ID Range Access Control Policy.
- There are no qualified IP addresses for ID Range Access Control Policy.
- You can create server pool policies when creating a server pool. Select Server Pool Qualification Policies to create these policies. When assigning server pools, additional server pool qualification is not supported in the global service profile.
- The only backup option is config-all backup. Other backup types such as config logical and config system are not supported.
- Local service profile picks up Host Firmware Policy from the Org instead of the Domain Group.
- When Import fails in HTML 5 UI, the message displays the reason for import failure. Make sure to correct errors and resubmit the configuration for import.
- Local service profile inventory is not displayed.
- The maintenance policy and schedules that are currently used by local service porfiles and currently under domain groups will not be available in HTML5 UI.



CHAPTER 2

License Management

This chapter includes the following sections:

Managing Licenses

Domain licenses for each registered Cisco UCS Domains enable you to manage the domains from Cisco UCS Central. You can manage the Cisco UCS domain licenses using both Cisco UCS Central GUI and CLI.

Grace Period

When you start using Cisco UCS Central for the first time, you can register up to five Cisco UCS domains for free, for up to 120 days grace period. If you register any domain after the fifth, you get a 120 grace period for each new registered domain. After the grace period ends, you need an active domain license to manage the domain using Cisco UCS Central. The grace period is measured from the day you register the Cisco UCS domain until the day you obtain and install a license.

The use of grace period for a registered Cisco UCS domain is stored in the system. Unregistering a domain from the system does not reset the grace period. For example, if you register a domain for free and use 40 days of the grace period unregister after 40 days, the system records the 40 days in association with that domain. If you register this Cisco UCS domain again, the grace period for the domain resumes and indicates that 40 days have been used. You must obtain and install a license before the grace period expires. If you did not obtain a license before the grace period expires, the system generates multiple faults as a reminder to procure a license. See Obtaining a License, on page 10

License Types

The following are the two available license types:

- **Initial License**: Initial license includes the initial activation license for Cisco UCS Central and five domain licenses. After installing the initial license, you cannot delete it from the system. You can still delete the download task for the initial license, that does not have any impact on the initial license installation status.
- **Domain License**: If you plan to register more than five domains in Cisco UCS Central, you must purchase domain licenses. After obtaining and downloading the domain licenses, when you register a Cisco UCS domain, you can select the domain and assign a license.

Obtaining a License

You can obtain a license for a Cisco UCS domain using the Cisco License Management Portal.

Note

- This process may change after the release of this document. If one or more of these steps do not apply, contact your Cisco representative for information on how to obtain a license.
- To obtain initial license use the license code **L-UCS-CTR-INI=**.
- To obtain domain licenses use the license code **L-UCS-CTR-LIC=**.

Before You Begin

Obtain the Product Authorization Key (PAK) from the claim certification or other proof of purchase documentation.

Step 1 On the Menu bar, click the **Tools** icon and select **Licenses**.

Step 2 Click**UCS Central GUID** to copy the GUID.
The GUID is unique to each Cisco UCS Central instance for obtaining licenses.

Step 3 Click **Cisco SWIFT** to open the License Administration Portal.

Step 4 Login to the License Administration Portal, and click **Continue to Product License Registration**.

Step 5 On the **Quickstart** page, enter the PAK in the **Enter a Single PAK or Token to fulfill** field and click **Fulfill Single PAK/Token**.

Step 6 On the **Assign SKUs to Devices** page, check the **Quantity Available** checkbox next to the PAK that you entered.

Step 7 Enter the GUID in the **GUID** field, and click **Assign**.

Step 8 Click **Next**.

Step 9 On the **Review** page, enter your email address, select the user ID, and check the **License Agreement** checkbox.

Step 10 Click **Get License**.
Cisco sends you the license zip file by email. The license file is digitally signed to authorize use on only the specified Cisco UCS domain.

Caution After you obtain the license file, you must not tamper with the license code. Any manual edits from your part breaks the tamper proof, and disables the license.

What to Do Next

Unzip the license file and install it.

Installing a License

You can install a license file from a local or remote file system.

Before You Begin

Make sure you have the following:

- Obtained the license from Cisco and saved it to your local system or remote file system.
- Administrative permission for Cisco UCS domain to perform this task.
- If you saved the license file in a remote location, make sure that location exists. Make sure to have the following information ready:
  - Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`
  - Host name or IP address of the remote server
  - Username and password for the remote server

Step 1 On the menu bar, click **Operation** icon, and select **Licenses**.

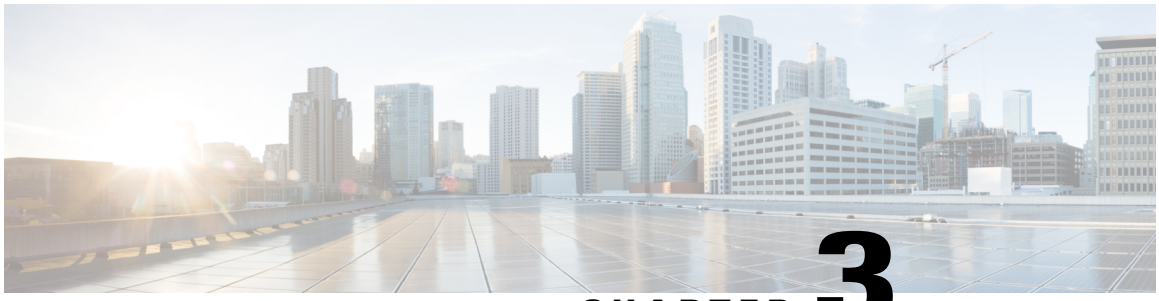
Step 2 In the Licenses menu bar, click Install icon.
This launches the **Install License** dialog box.

Step 3 In **License File Location**, click **Local** or **Remote**.
Select the location depending on where you have saved your license file.

a) If the license file is in the local system, browse to the **File Name** and select the file.
b) If the license file is in remote location, fill in the required information for the remote location.

Step 4 Click **Install**.

If you have selected the right file, the license file is installed in the system. If not, you will see an error message at the end of the dialog box. Make sure to select the right license file.



CHAPTER 3

User Management

This chapter includes the following sections:

Managing UCS Central Users Administration

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

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

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

- The **Password Profile** section allows you to perform the same tasks as the **Manage UCS Central Password Profile** dialog box. For more information, see Managing UCS Central Password Profile, on page 14.
- The **Roles** section allows you to perform the same tasks as the **Manage UCS Central Roles** dialog box. For more information, see Managing UCS Central Roles, on page 14.
- The **Locales** section allows you to perform the same tasks as the **Manage UCS Central Locales** dialog box. For more information, see Managing UCS Central Locales, on page 15.
- The **Local Users** section allows you to perform the same tasks as the **Manage UCS Central Local Users** dialog box. For more information, see Managing UCS Central Local Users, on page 15.
- The **Remote Users** section allows you to perform the same tasks as the **Manage UCS Central Remote Users** dialog box. For more information, see Managing UCS Central Remote Users, on page 16.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Managing UCS Central Password Profile

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

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

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

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

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

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

Step 7 Click **Save**.

Related Topics

Managing UCS Central Roles, on page 14
Managing UCS Central Locales, on page 15
Managing UCS Central Local Users, on page 15
Managing UCS Central Remote Users, on page 16

Managing UCS Central Roles

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

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

Step 3 Update the **Network**, **Storage**, **Server**, and **Operations** privileges for the role.

Step 4 Click **Save**.

Related Topics

Managing UCS Central Password Profile, on page 14
Managing UCS Central Locales, on page 15
Managing UCS Central Local Users, on page 15
Managing UCS Central Remote Users, on page 16

Managing UCS Central Locales

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

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

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

Step 4 Click **Save**.

Related Topics

Managing UCS Central Password Profile, on page 14
Managing UCS Central Roles, on page 14
Managing UCS Central Local Users, on page 15
Managing UCS Central Remote Users, on page 16

Managing UCS Central Local Users

Step 1 In the Task bar, type **Manage UCS Central Local Users** and press Enter.
This launches the **Manage UCS Central Local Users** 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 to be assigned to the user.

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

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

Step 7 Click **Save**.

Related Topics

Managing UCS Central Password Profile, on page 14
Managing UCS Central Roles, on page 14
Managing UCS Central Locales, on page 15
Managing UCS Central Remote Users, on page 16

Managing UCS Central Remote Users

Step 1 In the Task bar, type **Manage UCS Central Remote Users** and press Enter.
This launches the **Manage UCS Central Remote Users** 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 14
Managing UCS Central Roles, on page 14
Managing UCS Central Locales, on page 15
Managing UCS Central Local Users, on page 15

Managing Domain Group Users

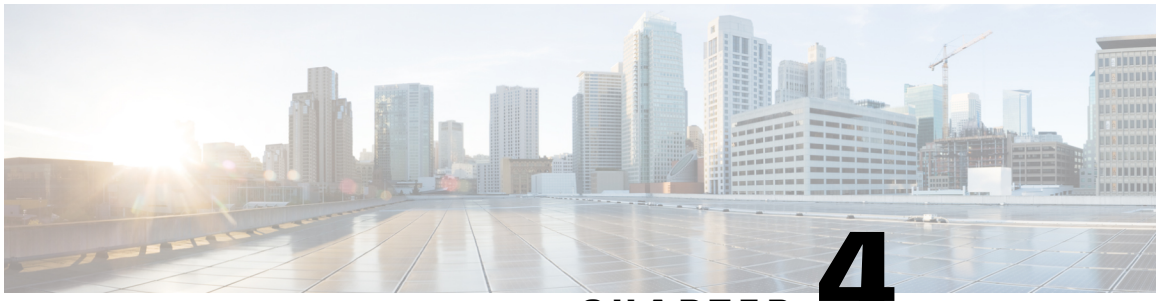
Step 1 Navigate to the root **Domain Group** page.

Step 2 Click the **Settings** icon and select **Users**.

Step 3 In **Roles**, add or delete the roles to be associated with the domain group.

Step 4 In **Locales**, add or delete the locales to be associated with the domain group.

Step 5 Click **Save**.



CHAPTER 4

Authentication

This chapter includes the following sections:

Authentication

From Cisco UCS Central you can configure LDAP, RADIUS, and TACACS+ for a registered UCS domain authentication.

Note Only LDAP can be used for remote authentication.

Guidelines and Recommendations for Remote Authentication Providers

If a system is configured for one of the supported remote authentication services, you must create a provider for that service to ensure that Cisco UCS Central can communicate with it. In addition, you need to be aware of the following guidelines that impact user authorization:

User Accounts in Remote Authentication Services

User accounts can exist locally in Cisco UCS Central or in the remote authentication server. The temporary sessions for users who log in through remote authentication services can be viewed through Cisco UCS Central GUI or Cisco UCS Central CLI.

User Roles in Remote Authentication Services

If you create user accounts in the remote authentication server, you must ensure that the accounts include the roles those users require for working in Cisco UCS Central and that the names of those roles match the names used in Cisco UCS Central. Depending on the role policy, a user may not be allowed to log in or granted only read-only privileges.

Local and Remote User Authentication Support

Cisco UCS Central uses LDAP for remote authentication, but excludes RADIUS and TACACS+ authentication in this release. However, RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains.

User Attributes in Remote Authentication Providers

When a user logs in, Cisco UCS Central does the following:

1. Queries the remote authentication service.
2. Validates the user.
3. If the user is validated, checks for the roles and locales assigned to that user.

The following table contains a comparison of the user attribute requirements for the remote authentication providers supported by Cisco UCS Central.

Table 1: Comparison of User Attributes by Remote Authentication Provider

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	Optional. You can choose to do either of the following: • Do not extend the LDAP schema and configure an existing, unused attribute that meets the requirements. • Extend the LDAP schema and create a custom attribute with a unique name, such as CiscoAVPair.	The Cisco LDAP implementation requires a unicode type attribute. If you choose to create the CiscoAVPair custom attribute, use the following attribute ID: 1.3.6.1.4.1.9.287247.1 A sample OID is provided in the following section.

Sample OID for LDAP User Attribute

The following is a sample OID for a custom CiscoAVPair attribute:

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
```

```
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
lDAPDisplayName: CiscoAVPair
name: CiscoAVPair
objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X
```

LDAP Providers

You can configure remote users, assign roles and locales from Cisco UCS Central the same way as you can create LDAP users from Cisco UCS Manager. You should always create the LDAP provider from Cisco UCS Central Domain Group root.

LDAP Provider Group Maps

You can define up to 28 LDAP provider group maps and nest them up to as many levels as the Active Directory supports for nesting in Cisco UCS Central. When you assign a provider to a nested group, even if the provider is a member of a different LDAP group, they become authenticated member of the parent nested group. During authentication, all the providers within a provider group are tried in order. If all the configured LDAP servers are unavailable or unreachable, Cisco UCS Central automatically falls back to the local authentication method using the local username and password.

LDAP Group Maps

For organizations that already use LDAP groups to restrict access to LDAP databases, group membership information can be used by Cisco UCS domains to assign a role or locale to an LDAP user during login. This eliminates the need to define role or a locale information in the LDAP user object when Cisco UCS Central is deployed.

Cisco UCS Central uses LDAP group rule to determine LDAP groups when assigning user roles and locales to a remote user. When a user logs in, Cisco UCS Central retrieves information about the user's role and locale from the LDAP group map. If the role and locale criteria match the information in the policy, Cisco UCS Central provides access to the user.

Role and locale definitions are configured locally in Cisco UCS Central and do not update automatically based on changes to an LDAP directory. If you delete or rename LDAP groups in the LDAP directory, make sure to update the changes in Cisco UCS Central.

You can configure an LDAP group map to include any of the following combinations of roles and locales:

- Roles only
- Locales only
- Roles and locales

Example: If you want to configure authentication for an LDAP group representing a group of server administrators at a specific location, you can include user roles such as server-profile and server-equipment

to the LDAP group. If you want to restrict access to server administrators at a specific location, you can specify locales with specific site names.

Note Cisco UCS Central includes many out-of-the-box user roles but does not include any locales. So you have to create a custom locale to map an LDAP provider group to a locale.

Nested LDAP Groups

You can search LDAP groups that are nested within another group defined in an LDAP group map. With this capability, you need not create subgroups in a group map in Cisco UCS Central.

Note Nested LDAP search support is supported only for Microsoft Active Directory servers. The supported versions are Microsoft Windows 2003 SP3, Microsoft Windows 2008 R2, and Microsoft Windows 2012.

Note When you create nested LDAP group in MS-AD, if you use special characters in the name, make sure to configure the characters with \\(, \\). Following is an example of creating a nested LDAP group using the Cisco UCS Central CLI:

create ldap-group CN=test1\\(\\),CN=Users,DC=ucsm,DC=qasam-lab,DC=in

Using the LDAP nesting feature, you can add an LDAP group as a member of another group and nest groups to consolidate member accounts and reduce the replication of traffic.

By default, user rights are inherited when an LDAP group is nested within another group. For example, if you make Group_1 a member of Group_2, the users in Group_1 will have the same permissions as the members of Group_2. You can then search users that are members of Group_1 by choosing only Group_2 in the LDAP group map, instead of having to search Group_1 and Group_2 separately.

Managing UCS Central Authentication

Cisco UCS Central uses LDAP for native authentication, but excludes RADIUS and TACACS+ authentication. However, RADIUS, TACACS+ and LDAP remote authentication are supported for Cisco UCS domains, from the Cisco UCS Central Domain Group root.

After creating an authentication domain, you can edit the authentication information as required.

Step 1 On the menu bar, click the **Operations** icon and select **Authentication**.
This launches **Manage Cisco UCS Central Authentication** dialog box.

Step 2 In **LDAP**, complete the appropriate fields for the **Basic**, **Providers**, **Groups**, and **Group Maps** tabs.

Step 3 In **Authentication Domains**, do the following:

Step 4 Click **Native(Default)** and complete the following information:

a) Select the **Default Behavior for Remote Users**.

b) Enter values for the **Web Session Refresh Period(Seconds)** and **Web Session Timeout(Seconds)**.
c) Choose whether **Authentication** should be **Enabled** or **Disabled**.
d) If you selected **Enabled**, choose whether the **Authentication Realm** should be **Local** or **LDAP**.
e) If you selected **LDAP**, select a **Provider Group**.

Step 5 Click **Console(Default)** and complete the following information:

a) Choose whether **Authentication** should be **Enabled** or **Disabled**.
b) If you selected **Enabled**, choose whether the **Authentication Realm** should be **Local** or **LDAP**.
c) If you selected **LDAP**, select a **Provider Group**.

Step 6 Click **Add** to create a new authentication domain.

a) Enter the name of the authentication domain.
This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name once you save it.

For systems using RADIUS as the preferred authentication protocol, the authentication domain name is considered part of the user name and counts toward the 32 character limit for locally created user names. Because Cisco UCS reserves five characters for formatting, you are not allowed to have a combined total of more than 27 characters for the domain name and user name.

b) In **Web Session Refresh Period(Seconds)**, enter the maximum amount of time allowed between refresh requests for a user accessing a Cisco UCS domain included in the selected Cisco UCS Central domain group.
If this time limit is exceeded, Cisco UCS Central considers the web session to be inactive, but it does not terminate the session.

Specify between 60 and 172800. The default is 600 seconds.

c) In **Web Session Timeout(Seconds)**, enter the maximum amount of time that can elapse after the last refresh request before Cisco Cisco UCS Central considers a web session to have ended. If this time limit is exceeded, Cisco UCS Central automatically terminates the web session.
Specify between 60 and 172800. The default is 7200 seconds.

d) Select the **Authentication Realm** applied to users in the domain. This can be one of the following:

- **LDAP—**The user must be defined on the LDAP server specified in Cisco UCS Central.
- **Local—**The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain.

e) If the **Realm** is set to LDAP, you can select an associated provider group from the **Provider Group** drop-down list.

Step 7 Click **Save**.

Managing UCS Central LDAP Configuration

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

Step 2 In **LDAP**, complete the following sections as required:

a) On the **Basic** tab, type values for the **Database Conection Timeout**, **Filter**, **Attribute**, and **Base DN**.
b) On the **Providers** tab, click **Add** to add a provider, and complete the necessary information in the **Basic** and **Group Rules** tabs.
c) On the **Groups** tab, click **Add** to add a provider group, and optionally associate it with a provider.
d) On the **Group Maps** tab, add a **Provider Group Map DN**, and then optionally add **Roles** and **Locales**.

Step 3 In **Authentication Domains**, add a new domain and update the values.

Step 4 Click **Save**.

Managing Domain Group Authentication

Step 1 On the task bar, type **Manage Domain Group Authentication** and press **Enter**.
This launches the **Manage Domain Group Authentication** dialog box.

Step 2 In **LDAP**, complete the following sections as required:
a) On the **Basic** tab, type values for the **Database Conection Timeout**, **Filter**, **Attribute**, and **Base DN**.
b) On the **Providers** tab, click **Add** to add a provider, and complete the necessary information in the **Basic** and **Group Rules** tabs.
c) On the **Groups** tab, click **Add** to add a provider group, and optionally associate it with a provider.
d) On the **Group Maps** tab, add a **Provider Group Map DN**, and then optionally add **Roles** and **Locales**.

Step 3 In **TACACS+**, complete the following sections as required:
a) On the **Basic** tab, type values for the **Database Conection Timeout** and **Retry Count**.
b) On the **Providers** tab, click **Add** to add a provider, and complete the necessary configuration information.
You can use the up and down arrows to change the order of the providers.
c) On the **Groups** tab, click **Add** to add a provider group, and optionally associate it with a provider.

Step 4 In **RADIUS**, complete the following sections as required:
a) On the **Basic** tab, type values for the **Database Conection Timeout** and **Retry Count**.
b) On the **Providers** tab, click **Add** to add a provider, and complete the necessary configuration information.
You can use the up and down arrows to change the order of the providers.
c) On the **Groups** tab, click **Add** to add a provider group, and optionally associate it with a provider.

Step 5

Step 6 In **Authentication Domains**, complete the following sections as required:
a) Click **Add** to create an authentication policy for the selected user-created domain group that overrides the settings inherited from its parent group.
b) Enter the name of the authentication domain.
This name can be between 1 and 16 alphanumeric characters. For systems using RADIUS as their preferred authentication protocol, the authentication domain name is considered part of the user name and counts toward the 32 character limit for locally created user names. Because Cisco UCS inserts 5 characters for formatting, authentication will fail if the combined total of the domain name plus the user name is more than 27 characters.

c) In **Web Session Refresh Period(Seconds)**, enter the maximum amount of time allowed between refresh requests for a user accessing a Cisco UCS domain included in the selected Cisco UCS Central domain group.
If this time limit is exceeded, Cisco UCS Manager considers the web session to be inactive, but it does not terminate the session.

Specify an integer between 60 and 172800. The default is 600 seconds.

d) In **Web Session Timeout(Seconds)**, enter the maximum amount of time that can elapse after the last refresh request before Cisco UCS Manager considers a web session to have ended. If this time limit is exceeded, Cisco UCS Manager automatically terminates the web session.
Specify an integer between 60 and 172800. The default is 7200 seconds.

e) Select the **Authentication Realm** that will be applied to users in the domain.
This can be one of the following:

- **LDAP—**The user must be defined on the LDAP server specified in Cisco UCS Central.
- **Local—**The user account must be defined locally in Cisco UCS Central or the Cisco UCS domain.
- **RADIUS—**The user must be defined on the RADIUS server specified in Cisco UCS Central.
- **TACACS+—**The user must be defined on the TACACS+ server specified in Cisco UCS Central.

Step 7 Click **Save**.

SNMP Policies

Cisco UCS Central supports global SNMP policies enabling or disabling, defining SNMP traps and SNMP users (with regular and privacy passwords, authentication types of md5 or sha, and encryption types DES and AES-128). Registered Cisco UCS domains choosing to define SNMP policies globally within that client's policy resolution control will defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality provides the ability to remotely monitor the Cisco UCS Central. You can also change the Cisco UCS Central host IP, and then restart the SNMP agent on the new IP. SNMP is run on both the active and standby Cisco UCS Central servers and the configuration is persisted on both. Cisco UCS Central offers read-only access to only the operating system managed information base (MIB).Through the Cisco UCS Central CLI you can configure the community strings for SNMP v1, v2c, and create and delete the SNMPv3 users.

SNMP Functional Overview

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within Cisco UCS Central, the managed device, that maintains the data for Cisco UCS Central and reports the data, as needed, to the SNMP manager. Cisco UCS Central includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in Cisco UCS Central.

- A managed information base (MIB)—The collection of managed objects on the SNMP agent. Cisco UCS Central supports only the OS MIBs.

Cisco UCS Central supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. The following RFCs define the SNMP:

- RFC 3410 (http://tools.ietf.org/html/rfc3410)
- RFC 3411 (http://tools.ietf.org/html/rfc3411)
- RFC 3412 (http://tools.ietf.org/html/rfc3412)
- RFC 3413 (http://tools.ietf.org/html/rfc3413)
- RFC 3414 (http://tools.ietf.org/html/rfc3414)
- RFC 3415 (http://tools.ietf.org/html/rfc3415)
- RFC 3416 (http://tools.ietf.org/html/rfc3416)
- RFC 3417 (http://tools.ietf.org/html/rfc3417)
- RFC 3418 (http://tools.ietf.org/html/rfc3418)
- RFC 3584 (http://tools.ietf.org/html/rfc3584)

SNMP Notifications

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

Cisco UCS Central generates SNMP notifications as traps. Traps are less reliable because the SNMP manager does not send any acknowledgment when it receives a trap, and Cisco UCS Central cannot determine if the trap was received.

SNMP Security Features

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

- Message integrity—Ensures that messages have not been altered or destroyed in an unauthorized manner and that data sequences have not been altered to an extent greater than can occur non-maliciously.
- Message origin authentication—Ensures that the claimed identity of the user on whose behalf received data was originated is confirmed.
- Message confidentiality and encryption—Ensures that information is not made available or disclosed to unauthorized individuals, entities, or processes.

SNMP Security Levels and Privileges

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

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

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

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

SNMP Security Models and Levels

The following table describes the combinations of SNMP security models and levels supported in Cisco UCS Central.

Table 2: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v2c	noAuthNoPriv	Community string	No	Uses a community string match for authentication.
v3	noAuthNoPriv	Username	No	Uses a username match for authentication.
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on the Hash-Based Message Authentication Code (HMAC) Message Digest 5 (MD5) algorithm or the HMAC Secure Hash Algorithm (SHA).

Model	Level	Authentication	Encryption	What Happens
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides Data Encryption Standard (DES) 56-bit encryption in addition to authentication based on the Cipher Block Chaining (CBC) DES (DES-56) standard.

SNMP Support in Cisco UCS Central

Support for MIBs

Cisco UCS Central supports read-only access to OS MIBs. No set operations are available for the MIBs. The following MIBs are supported by Cisco UCS Central:

- SNMP MIB-2 System
- HOST-RESOURCES-MIB
    - hrSystem
    - hrStorage
    - hrDevice
    - hrSWRun
    - hrSWRunPerf
- UCD-SNMP-MIB
    - Memory
    - dskTable
    - systemStats
    - fileTable
- SNMP MIB-2 Interfaces
    - ifTable
- IP-MIB
- SNMP-FRAMEWORK-MIB

- snmpEngine

- IF-MIB
- DISMAN-EVENT-MIB
- SNMP MIB-2 snmp

Note Cisco UCS Central does not provide support for IPV6 andCisco UCS Central MIBs.

Related Topics

Enabling SNMP, on page 27
Creating and Editing an SNMP User, on page 28
Creating and Editing an SNMP Trap, on page 27

Enabling SNMP

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

- You can select SNMP by typing **Manage UCS Central SNMP** on the **Task** bar and press **Enter**.

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

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

Step 3 In **Community/User Name**, enter the default SNMP v1 or v2c community name or SNMP v3 username.

Step 4 In **System Contact**, enter the system contact person responsible for the SNMP implementation.
Enter a string of up to 255 characters, such as an email address or a name and telephone number.

Step 5 In **System Location**, enter the location of the host on which the SNMP agent (server) runs.
Enter an alphanumeric string up to 510 characters.

Step 6 Click **Save**.

What to Do Next

Create SNMP traps and users.

Creating and Editing an SNMP Trap

After creating an SNMP trap, you can edit the SNMP trap information as required.

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

This launches **Manage UCS Central SNMP** dialog box.

Step 2 In **Trap Host Name/IP Address**, enter the IP address of the SNMP host to where the trap should be sent.

Step 3 In **SNMP Trap Properties** area, complete the following:

Step 4 In **Community/User Name**, enter the SNMP v1 or v2c community name or the SNMP v3 username that the system includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service.
Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.

Step 5 In **Port**, enter the port on which the system communicates with the SNMP host for the trap.
Enter an integer between 1 and 65535. The default port is 162.

Step 6 Click **V1**, **V2C**, or **V3** to choose the SNMP Version.

Step 7 Click **Trap** to choose the SNMP trap **Type**.

Step 8 To define **V3Privilege**, choose one of the following:

Step 9 Click **Save**.

- **auth—**Authentication but no encryption
- **NoAuth—**No authentication or encryption
- **Priv—**Authentication and encryption

What to Do Next

Create an SNMP user.

Creating and Editing an SNMP User

After creating an SNMP user, you can edit the SNMP user information as required.

Step 1 On the menu bar, click the **Operations** icon and select **SNMP**.
This launches **Manage UCS Central SNMP** dialog box.

Step 2 On the **Manage UCS Central SNMP** page, click **SNMP User**.

Step 3 Click the **Plus** sign to create SNMP user.

Step 4 Enter the username assigned to the SNMP user.
Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).

Step 5 In **SNMP User Properties**, complete the following:

Step 6 In **Authentication Type**, select the authorization type. This can be one of the following:

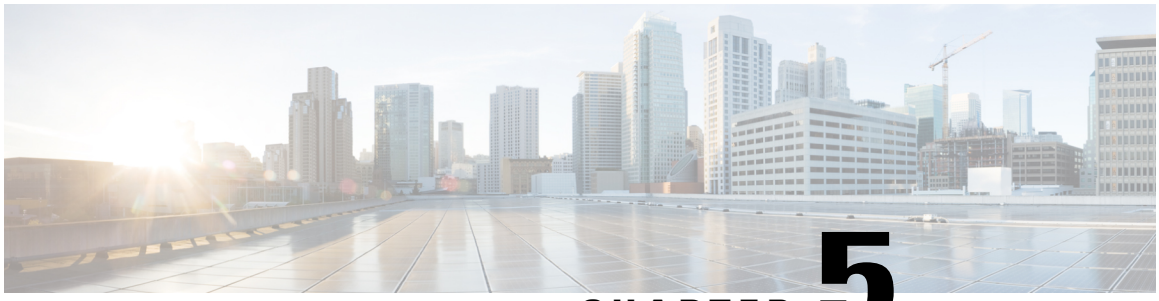
- **MDS**
- **SHA**

Step 7 Enable **AES-128 Encryption**. If enabled, this user uses AES-128 encryption.

Step 8 Enter the password for the user.

Step 9 Enter the privacy password for this user.

Step 10 Click **Save**.



CHAPTER 5

Firmware Management

This chapter includes the following sections:

Firmware Management

Cisco UCS Central enables you to manage all firmware components for all registered Cisco UCS domains and Cisco UCS Mini domains. The status of any firmware updates is displayed under the **Domains** section. This can be one of the following:

- **Firmware Ready—**The firmware has been successfully updated.
- **In Progress—**The firmware update is currently in progress.
- **Pending User Ack—**User acknowledgment is required on the **Pending Activities** page before the firmware is updated. See Viewing and Acknowledging Pending Activities, on page 45.

Note To manage Cisco UCS domains firmware from Cisco UCS Central, you must 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 you 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 will 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 will use the same Infrastructure firmware version defined in the domain group.

Image Library

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

From here you can:

- Use the firmware images to create policies.
- Delete any downloaded image from the image library by selecting the image and clicking the Delete icon.

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

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

Importing Firmware Bundle

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

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

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

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

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

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

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

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

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

What to Do Next

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

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

Enabling Automatic Firmware Update Sync-ups from Cisco.com

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

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

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

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

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

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

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

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

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

Step 5 Click **Sync**.

Scheduling Infrastructure Firmware Update for a Cisco UCS Domain Group

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

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

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

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

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

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

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

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

Step 7 Click **Schedule**.
You can monitor the firmware update on the **Firmware** page. See Firmware Management, on page 31.

Scheduling an Infrastructure Firmware Update for a Cisco UCS Mini Domain Group

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

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

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

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

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

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

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

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

Step 7 Click **Schedule**.
You can monitor the firmware update on the **Firmware** page. See Firmware Management, on page 31.

Removing an Infrastructure Firmware Schedule for a Cisco UCS Domain Group

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

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

Step 3 Click **Remove**.

Removing an Infrastructure Firmware Schedule for a Cisco UCS Mini Domain Group

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

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

Step 3 Click **Remove**.

Creating or Editing a Host Firmware Package Policy

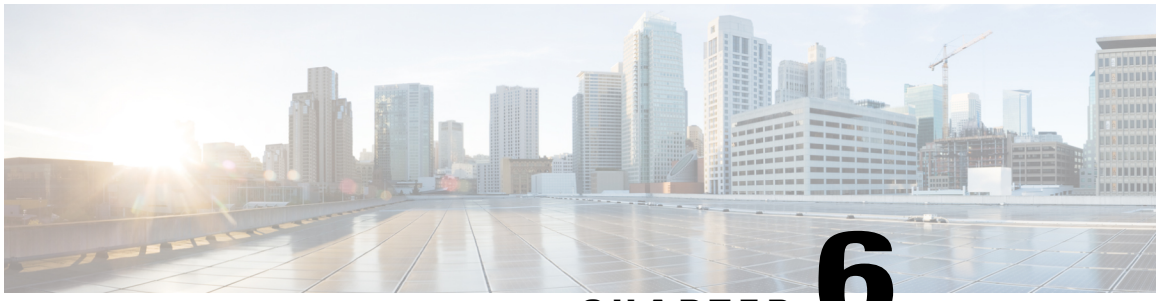
Step 1 In the Task bar, type **Create Host Firmware Package Policy** and press Enter.
This launches the **Create Host Firmware Package Policy** dialog box.

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

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

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

Step 5 Click **Create**.



CHAPTER 6

System Management

This chapter includes the following sections:

Configuring UCS Central System Policies

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

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

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

- The **Fault** section allows you to perform the same tasks as the **Manage UCS Central Fault Policy** dialog box. For more information, see Managing a UCS Central Fault Policy, on page 38.
- The **Syslog** section allows you to perform the same tasks as the **Manage UCS Central Syslog** dialog box. For more information, see Managing UCS Central Syslog, on page 39.
- The **Core Dump Export** section allows you to perform the same tasks as the **Manage UCS Central Core Dump Export** dialog box. For more information, see Managing UCS Central Core Dump Export, on page 40.

Step 3 Complete the fields as required for each section.

Step 4 Click **Save**.

Related Topics

Managing a UCS Central Fault Policy, on page 38
Managing UCS Central Syslog, on page 39
Managing UCS Central Core Dump Export, on page 40

Managing a UCS Central Fault Policy

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

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

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

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

   Flapping occurs when a fault is raised and cleared several times in rapid succession. To prevent this, Cisco UCS Central does not allow a fault to change its state until this amount of time has elapsed since the last state change.

   If the condition reoccurs during the flapping interval, the fault returns to the active state. If the condition does not reoccur during the flapping interval, the fault is cleared. What happens at that point depends on the setting in the **Action on Clear** field.

2. In **Soaking Interval**, choose None, or select a custom soaking interval.
3. In **Clear Interval**, select whether Cisco UCS Central should automatically mark faults as cleared based on their age.

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

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

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

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

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

Step 3 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 37
Managing UCS Central Syslog, on page 39

Managing UCS Central Core Dump Export, on page 40

Managing UCS Central Syslog

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

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

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

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

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

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

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

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

- **Logging Level—**Select the lowest message level that you want the system to store. The system stores that level and above in the remote file. This can be one of the following:
  - **Critical (UCSM Critical)**
  - **Alert**

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

- **Facility—**The facility associated with the remote destination.
- **Host Name/IPAddress—**The hostname or IP address on which the remote log file resides. If you are using a host name rather than a IPv4 or IPv6 address, you must configure the DNS server in Cisco UCS Central.

Step 5 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 37
Managing a UCS Central Fault Policy, on page 38
Managing UCS Central Core Dump Export, on page 40

Managing UCS Central Core Dump Export

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

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

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

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

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

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

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

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

Step 8 Click **Save**.

Related Topics

Configuring UCS Central System Policies, on page 37

Managing a UCS Central Fault Policy, on page 38
Managing UCS Central Syslog, on page 39

Managing the UCS Central System Profile

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

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

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

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

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

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

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

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

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

Step 9 Click **Save**.

Related Topics

Managing the UCS Central NTP Servers, on page 42
Managing the UCS Central Management Node, on page 41
Managing the UCS Central DNS Servers, on page 42

Managing the UCS Central Management Node

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

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

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

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 41
Managing the UCS Central NTP Servers, on page 42
Managing the UCS Central DNS Servers, on page 42

Managing the UCS Central NTP Servers

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

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

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

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 41
Managing the UCS Central Management Node, on page 41
Managing the UCS Central DNS Servers, on page 42

Managing the UCS Central DNS Servers

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

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

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

Step 4 Click **Save**.

Related Topics

Managing the UCS Central System Profile, on page 41
Managing the UCS Central NTP Servers, on page 42
Managing the UCS Central Management Node, on page 41

Managing Domain Group System Policies

Step 1 Navigate to the root **Domain Group** page.
Step 2 Click the **Settings** icon and select **System Profile**.
Step 3 In **Fault**, complete the necessary fields.
For more information, see Managing a UCS Central Fault Policy, on page 38.
Step 4 In **Syslog**, complete the necessary fields.
For more information, see Managing UCS Central Syslog, on page 39.
Step 5 In **Core Dump**, complete the necessary fields.
For more information, see Managing UCS Central Core Dump Export, on page 40.
Step 6 In **Interfaces**, choose whether to enable **Interface Monitoring Policy**.
Step 7 If you select **Enabled**, complete the interface monitoring information as required.
Step 8 In **Equipment**, select the **Power Redundancy**, the **Power Allocation Method**, and enter an **ID Soaking Interval**.
Step 9 In **System Events**, complete the necessary fields to determine how the system event logs will be collected.
Step 10 Click **Save**.

Managing the Domain Group System Profile

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

Tech Support Files

You can generate and tech support files for Cisco UCS Central and registered Cisco UCS Domains. Collecting remote tech support includes the following:

- **Generate Tech Support**: You can generate tech support files for Cisco UCS Central or each registered UCS domains.

- **Download tech support files**: Download the created tech support file to view information.

Note You can download the tech support file only from the Cisco UCS Central GUI.

Generating Tech Support File

Step 1 On the menu bar, click **Operation** icon, and select **Tech Support**.

Step 2 Under **Domains** select **UCS Central** or the domain for which you want to generate tech support files for. This displays any available tech support files and the generate menu option.

Step 3 Click flash icon to **Generate Tech Support** files.

Step 4 In the pop-up confirmation dialog box, click **Yes**.

Step 5 The list page displays tech support file collection status when the collection is in progress. When the process is complete, displays the collected time, file name and availability status.

Downloading a Tech Support File

Step 1 On the menu bar, click **Operation** icon, and select **Tech Support**.

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

Step 3 The right pane displays the list of available tech support files for the selected system.

Step 4 Click to select the file you want to download.

Step 5 Click **Download** icon on the menu bar.

Step 6 In the download dialog box, click **Save** to save the tech support file in your local download folder.

Monitoring System Faults and Logs

Pending Activities

If you configure deferred deployment in a Cisco UCS domains, Cisco UCS Central enables you to view all pending activities. You can view all the activities that are waiting for user acknowledgment and those that have been scheduled.

If a Cisco UCS domain has pending activities, the Cisco UCS Central GUI notifies users with admin privileges when they log in.

Cisco UCS Central displays information about all pending activities, including the following:

- Name of the service profile to be deployed and associated with a server
- Server affected by the deployment
- Disruption caused by the deployment
- Change performed by the deployment
- Whether an activity is acknowledged.

You can also acknowledge the activities.

You cannot specify the maintenance window in which a specific pending activity is applied to the server. The maintenance window depends on the number of pending activities and on the maintenance policy assigned to the service profile. However, any user with admin privileges can manually initiate a pending activity and reboot the server immediately, whether an activity is waiting for an user acknowledgment or for a maintenance window.

To view the pending activities on Cisco UCS Central GUI, click the **Alerts** icon from the menu bar.

Important A pending activity is not displayed in the log, if the activity is caused by a local service profile using a local maintenance policy with a local scheduler. Such pending activities must be acknowledged from Cisco UCS Manager .

Viewing and Acknowledging Pending Activities

Step 1 On the menu bar, click the **Alerts** icon.

Step 2 Select **Pending Activities**.

Step 3 In **Pending Activities**, note the activities that are pending.
You can use the checkboxes in the **Filters** area to narrow down the activities.

Step 4 Click **Acknowledge** to acknowledge a pending activity.

System Faults

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

The faults table includes the following information for each fault:

- **Code—**The ID associated with the fault
- **Timestamp—**Date and time at which the fault occurred

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

To manage the information that is collected, see Configuring UCS Central System Policies, on page 37.

UCS Domain Faults

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

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

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

- **Filter—**Allows you to filter the data in the table.

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

Event Logs

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

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

Audit Logs

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

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

Core Dumps

If an error occurs that causes the system to crash, then a core dump file is created. This core dump file includes information of the state of the system before the error occurred, and the time at which the system crashed. To

view the core dump files, click the **Alerts** icon on the menu bar and select **Core Dumps**. In the **Core Dumps** log table you can view the following information:

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

Active Sessions

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

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

Internal Services

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

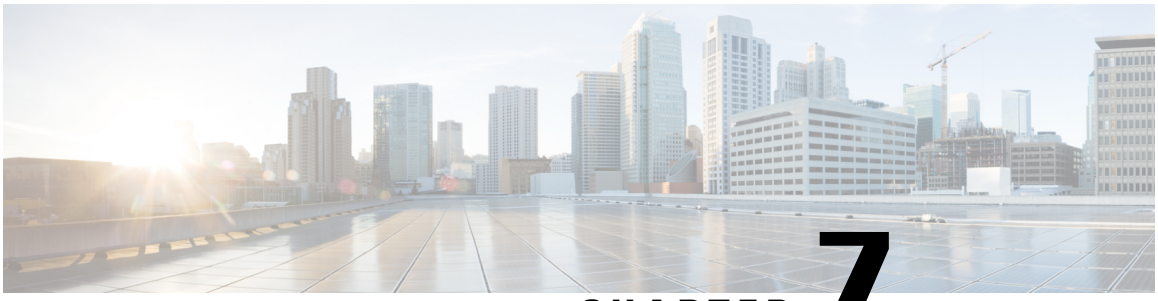
In the **Services** section of the **Internal Services** page, you can view the following information:

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

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

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

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



CHAPTER 7

Domains and Organizations

This chapter includes the following sections:

Domain Groups

Cisco UCS Central creates a hierarchy of Cisco UCS domain groups for managing multiple Cisco UCS domains. You will have the following categories of domain groups in Cisco UCS Central:

- **Domain Group—** A group that contains multiple Cisco UCS domains. You can group similar Cisco UCS domains under one domain group for simpler management.
- **Ungrouped Domains—**When a new Cisco UCS domain is registered in Cisco UCS Central, it is added to the ungrouped domains. You can assign the ungrouped domain to any domain group.

If you have created a domain group policy, and a new registered Cisco UCS domain meets the qualifiers defined in the policy, it will automatically be placed under the domain group specified in the policy. If not, it will be placed in the ungrouped domains category. You can assign this ungrouped domain to a domain group.

Each Cisco UCS domain can only be assigned to one domain group. You can assign or reassign membership of the Cisco UCS domains at any time. When you assign a Cisco UCS domain to a domain group, the Cisco UCS domain will automatically inherit all management policies specified for the domain group.

Before adding a Cisco UCS domain to a domain group, make sure to change the policy resolution controls to local in the Cisco UCS domain. This will avoid accidentally overwriting service profiles and maintenance policies specific to that Cisco UCS domain. Even when you have enabled auto discovery for the Cisco UCS domains, enabling local policy resolution will protect the Cisco UCS domain from accidentally overwriting policies.

Important

- Make sure to create a separate domain groups for all M Series modular server domains. Also make sure the modular server domain groups are not hierarchical.
- You must create separate infrastructure firmware policy for M Series modular domains in Cisco UCS Central. The infrastructure firmware policies must be unique to modular servers. This will prevent any firmware policy resolution with other domain groups.

Creating or Editing a Domain Group

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

Step 2 In **Basic**, click **Domain Group Location** and select the location in which you want to create the domain group.

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

Step 4 In **Qualification**, select the **Qualification Policies** that you want to use to identify the Cisco UCS Manager domains.
All domains that meet the qualification policy are automatically added to the domain group.

Step 5 In **Domains**, select the Cisco UCS Manager domains that you want to add to the domain group.
M Series modular server domains should not be added to a domain group that contains UCS Classic (B Series) domains or UCS Mini domains.

Step 6 Click **Create**.

Adding a Domain to a Domain Group

Step 1 Click the Domain Group icon and select the domain group where you want to add the Cisco UCS Manager domain.

Step 2 Click the **Edit** icon.
The **Edit** dialog box for the domain that you selected displays.

Step 3 Update the description and qualification policies as necessary.

Step 4 Click **Domains** and select the Cisco UCS Manager domains that you want to add to the domain group.

Note M Series modular server domains should not be added to a domain group that contains UCS Classic (B Series) domains or UCS Mini domains.

Step 5 Click **Save**.

Managing Domain Group SNMP

Step 1 In the Task bar, type **Manage Domain Group SNMP** and press Enter.
This launches the **Manage Domain Group SNMP** dialog box.

Step 2 In **Basic**, click **Enabled**, then enter the **Community/User Name**.
Cisco UCS includes the SNMP v1 or v2c community name or the SNMP v3 username when it sends the trap to the SNMP host. This must be the same as the community or username that is configured in **SNMP Traps**.

Step 3 Enter the optional **System Contact** and **System Location**.

Step 4 In **SNMP Traps**, click **Add** and complete the following:

a) Enter the same **Community/User Name** from the **Basic** section.
b) Enter the **Port**, and select values for the SNMP **Version**, the **Type**, and the **V3 Privilege**.

Step 5 In **SNMP Users**, click **Add** and complete the following:

a) Enter the **SNMP User Name**.
b) Select the **Authentication Type** and whether to enable **AES-128 Encryption**.
c) Enter and confirm the values for the password and privacy password.

Step 6 Click **Save**.

Domain Group Qualification Policy

Domain group policy enables you to automatically place new Cisco UCS domains under domain groups. You can create qualifiers based on Owner, Site and IP Address of various Cisco UCS domains based on your management requirements. When you register a new Cisco UCS domain, Cisco UCS Central analyses the domain based on the pre defined qualifiers in the domain group qualification policy and places the domain under a specific domain group for management.

Creating or Editing a Domain Group Qualification Policy

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

Step 2 In **Basic**, click **Organization** and select the location in which you want to create the domain group qualification policy.

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

Step 4 In **Owner**, enter the owner name and regex.
Step 5 In **Site**, enter the site name and regex.
Step 6 In **IP Address**, add the IP address ranges.
Step 7 Click **Create**.

Organizations

Organization

The **Organization** page enables you to view logical entities created under an organization that exists in a registered Cisco UCS domains.

Click one of the following icons to launch the specific page.

- **Service Profiles—**Displays all service profiles in the organization.
- **Service Profile Templates—**Displays all service profile templates in the organization.
- **Pools—**Displays all pools in the organization.
- **Policies—**Displays all policies in the organization.

Updating Organization Descriptions

After an organization is created, you can update the description.

Step 1 From the **Organization** page, click the **Edit** icon.
This launches the **Edit Organization** dialog box.
Step 2 Enter the **Description** for the organization.
Step 3 Click **Save**.

Inventory

Domains Table View

The **Domains Table View** page displays the following information related to the domains registered with Cisco UCS Central:

Domain	Hardware	Configuration	Status
This column displays the following information for a registered domain: • The associated domain name and site • Domain group location • Management IP address • Owner	This column displays the following hardware information for a registered domain: • Fabric interconnect model number and cluster state (HA or Standalone) • Number of chassis and FEX • Number of blade and rack servers • Number of blade servers available for storage • Number of cartridges for Cisco UCS M-Series Modular Servers.	This column displays the following configuration for a registered domain: • Platform family • Firmware version • Firmware status	This column displays the following status for a registered domain: • Overall status • Worst fault level • Trial expiry or status

Domain Group Details

From the **Domain Group** page, you can view information about the entities associated with a domain group. This includes the following:

- **Domains**
- **Fabric Interconnects**
- **Chassis**
- **Servers**
- **FEX**
- **vLANs**
- **vSANs**

If you click the **Settings** icon, you can perform the following tasks:

- Create a system profile or system policy.
- Manage users, authentication, SNMP, and Call Home settings.
- Edit the domain group, and delete any user-created domain group.

Note The domain group root cannot be deleted.

Cisco UCS Domain Main View

The **Cisco UCS Domain** page displays the following information related to a selected Cisco UCS domain:

- **Basic—**Displays information related to the overall status, firmware, resources available, fault summary and management details of the selected Cisco UCS domain.

  Also, you can suspend and acknowledge a UCS Central subscription, and re-evaluate the membership of the domain.

- **FI—**Displays the number of Fabric Interconnects (FI) associated with a domain, overall status, hardware, and firmware details of the FI.

  If you want to view more information on the status of the components in the FI, click on an FI from the list.

- **Chassis—**Displays the number of chassis associated with a domain, overall status, hardware, and configuration details of the chassis. For more information on the status of the components in the chassis, click on a chassis from the list.

- **FEX—**Displays the number of FEX associated with a domain, overall status, hardware, and configuration details of the FEX. For more information on the status of the components in the FEX, click on an FEX from the list.

- **Servers—**Displays the number of servers in a domain and the number of available servers. For more information on overall status, hardware, and configuration details of the server, click **Go to Servers Table**.

On the **Cisco UCS Domain** page, you can do the following:

- Launch Cisco UCS Manager GUI for the selected Cisco UCS domain.
- Suspend UCS Central subscription when the overall status of a domain is OK.
- Activate UCS Central subscription when the overall status of a domain is suspended.
- Re-evaluate membership

Fabric Interconnect

The **Fabric Interconnect** (FI) page displays the following information related to FI associated with the registered Cisco UCS domain:

Fabric Interconnect	Hardware	FW	Status
This column displays the following information for a fabric interconnect: • The associated domain name and FI ID • Domain group location • IP address of the domain	This column displays the following hardware information for a fabric interconnect: • The model number and type of FI • Serial number • The number of fixed and expansion module ports • The number of ethernet and fabric channel ports	This column displays the following firmware details for a fabric interconnect: • Firmware version • Firmware status	This column displays the following status for a fabric interconnect: • Overall status • Worst fault level

Fabric Interconnect Main View

The **Fabric Interconnect Main View** page displays the following information related to the selected Fabric Interconnect (FI) and its components within a registered Cisco UCS domain.

- **Basic—**Displays an overview of the FI within the domain, hardware details, firmware version, number of ports (Ethernet or FC) that are in use and available for use, management IP, and fault summary details.
- **Fixed Mod.—**Displays overall status, firmware, hardware, properties, and fault summary details of the fixed modules installed in the FI .
- **Exp. Mod.—**Displays overall status, firmware, hardware, properties, and fault summary details of the expansion modules installed in the FI.
- **Fans—**Displays overall status, and hardware details of the fan.
- **PSUs—**Displays overall status, fault summary, and hardware details of the PSU.

You can turn on or turn off the locator LED on the chassis by selecting **Toggle Locator LED**.

Servers Table View

The **Servers** page displays the following information related to the servers associated with the registered UCS domain:

Servers	Hardware	Configuration	Status
This column displays the following information for a server: • The associated domain name, chassis ID, and slot ID • Domain group location • Management IP address	This column displays the following hardware information for a server: • Blade server model • The number of cores the CPU has and the total RAM on the motherboard • The serial number • The number of CPUs and the speed	This column displays the following configuration for a server: • Service profile name • Service profile organization location • Firmware version • Firmware status	This column displays the following status for a server: • Overall status • Worst fault level • Power status • Decommissioned server. You can recommission a decommissioned server.

Servers Details Page

The server details page allows you manage and monitor all servers in a Cisco UCS domain.

Note Depending on the server type, the options may vary.

You can view the following information on the selected server and its components:

- **Basic—**Displays associated service profile, fault summary, hardware and firmware details of the selected server.
- **Motherboard—**Displays the overall status and the hardware details of the motherboard.
- **CPUs—**Displays a list of all the CPUs in the server. Click a processor to view overall status and hardware and other details of the selected processor.
- **Memory—**Displays a list of available memory in the selected server. Click a memory to view the current overall status and other details.
- **Adaptors—**Displays details of the adapter in the selected server. Click an adaptor to view overall status, power status and other product details.
- **Storage—**Displays list of the storage in the selected server. Click a disk to view the current overall status, hardware and controller details.

You can also perform the following server-related tasks:

- Launch Cisco UCS Manager or the **KVM Console**.
- Reset, recover, reacknowledge, or decommission a server.
- Toggle the locator LED.

Chassis

The **Chassis** page displays the following information related to the chassis associated with the registered Cisco UCS domain:

Chassis	Hardware	Configuration	Status
This column displays the following information for a chassis: • The associated domain name and chassis ID • Domain group location • Fabric side	This column displays the following hardware information for a chassis: • Model number of the chassis • Serial number of the chassis • Number of blades or modular server. • Number of cartridges	This column displays the following configuration for a Chassis: • Configuration status • Configuration error count	This column displays the following status for a Chassis: • Overall status • Worst fault level • Power status • Thermal status • Decommissioned chassis. You can recommission the chassis by specifying a valid chassis ID.

Chassis Main View

The **Chassis Main View** page allows you to manage and monitor all chassis in a Cisco UCS domain through Cisco UCS Central GUI.

You can view the following information on the selected chassis and its components within a registered Cisco UCS domain:

- **Basic—**Displays the overall status and, overview of all the components within the selected chassis, fault summary, configuration errors and hardware details.
- **IOM Left—**Displays overall status, hardware details and fault summary of the left IOM module.
- **IOM Right—**Displays overall status, hardware details and fault summary details of the right IOM module.
- **Servers—**Displays overall status, hardware, and firmware details of the server associated with this chassis. On selecting a server, the page redirects to the server detail view page of the server in the UCS domain.
- **Fans—**Displays a list of fans in the chassis. Click a fan to view information related to its module, overall status and hardware details.
- **PSUs—** Displays a list of all the PSUs in the chassis. Click a PSU to view information related to its fault summary, overall status, and other property details..

On the **Chassis Main View** page, you can do the following:

- Acknowledge and decommission a chassis.
- Turn on or turn off Locator LED for a chassis.
- Launch Cisco UCS Manager GUI for the selected domain.

Note For Cisco UCS M-Series Modular Servers, you can also view information about the Cartridges, Storage, and LUNs associated with the chassis.

FEX

The **FEX** page displays the following information related to the FEX associated with the registered Cisco UCS domains:

FEX	Hardware	Configuration	Status
This column displays the following information for a FEX: • The associated domain name and FEX ID • Domain group location • Fabric Side	This column displays the following hardware information for a FEX: • Model number • Serial number • Number of ports available	This column displays the following configuration for a FEX: • Configuration status • Configuration error count	This column displays the following status for a FEX: • Overall status • Worst fault level • Power status • Thermal status • Decommissioned FEX. You can recommission the FEX by specifying a valid FEX ID.

FEX Main View

Cisco UCS Central enables you to manage the FEXes in the registered UCS domain from both Cisco UCS Central GUI and CLI.

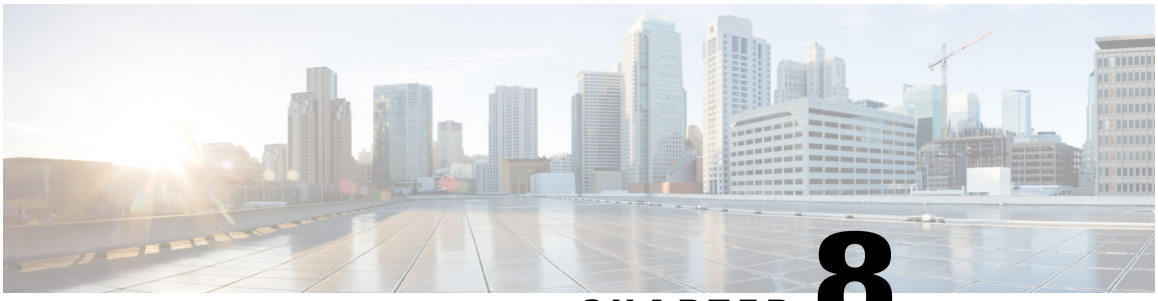
You can view the following information related to the FEX and its components within a registered Cisco UCS domain:

- **Basic—**Displays fault summary, overall status and hardware details of the FEX within UCS domain.
- **IOM—**Displays fault summary, overall status, and properties of the IOM.
- **Servers—**Displays number of rack servers connected to the FEX. Click a server to view more information on overall status, firmware and hardware details of the server.

- **Fans—**Displays a list of fans in the FEX. Click a fan to view more information related to the module number, overall status and hardware details.
- **PSUs—** Displays a list of all the PSUs in the FEX. Click a PSU to view details on fault summary, status, properties, and status of power supply units.

On the **FEX Main View** page, you can do the following:

- Acknowledge, decommission, and recommission a FEX.
- Turn on or turn off Locator LED for FEXes.



CHAPTER 8

Templates

This chapter includes the following sections:

Templates

Displays a complete list of templates in the system. You can use filter to sort by **Template**, **Type**, **Usage Status** or **Tenmplate Org** to view availability and usage.

Service Profile Template Detail View

The Service Profile Template page displays detailed information about a service profile template. From here, you can:

- View audit logs
- Delete, clone, or rename the service profile template
- Create a service profile from this service profile template
- Configure the host interface placement

Creating or Editing a Service Profile Template

If you are editing an existing template, when you make any changes, make sure to click Evaluate to evaluate the impact of the changes you are making to this template.

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

Step 2 In **Basic**, select the **Organization** where you want to create the service profile template.

a) Enter a **Name**, **Description** and a **User Label**.

b) Select the options for **Template Instantiation Mode**, **Desired Power State Check on Association**, and **Compatability Check on Migration Using Server Pool**.

Step 3 Click **Identifiers** to assign identifiers for this service profile.
Click each identifier. On the right, click the drop-down to display available pools and select the one you want for this service profile template.

Step 4 Click **Connectivity** and select the connectivity policies and management vLAN for this template.
Click SAN, LAN and Dynamic connectivity policies and **Management vLAN** to display the details on the right. Then, click the drop-down to display available policies or search for a policy and select the one you want for this service profile template.

Step 5 Click **Servers** and click drop-down on the right. Select or search and assign the servers you want to associate this template with.

Step 6 Click **Storage** and click drop-down on the right. Select or search and assign the storage profile you want to associate this template with.
Storage profiles in Cisco UCS Central release 1.3 are supported only with Cisco UCS M-Series Modular Servers.

Step 7 Click **Policies**.
You can click on all service profile related policies, use the drop-down option on the right, and assign policies to this template.

Creating or Editing a vHBA Template

To edit a specific vHBA template, type vHBA Template in the search bar to find the vHBA template you want to edit.

Note Global vHBAs can be used in local service profiles created in Cisco UCS Manager.

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

Step 2 In **Basic**, select the **Organization** where you want to create the vHBA template.

a) Enter a **Name** and **Description**.

b) Select the options for **Type**, **Fabric ID**, and enter **Max Data Field Size(Bytes).**

Step 3 Click **WWN Address Pool** and select the WWN addresses.
If you do not assign a WWN address pool, the system assigns the default.

Step 4 Click **vSANs** and add the vSANs you want to use for this vHBA template.

Step 5 Click **Policies** .
If the policies are not assigned, click on each of the policies and pin group. On the right, click the drop-down to display related policies and pin group and select the one you want for this vHBA template.

Step 6 Click **Create**.

Creating or Editing a vNIC Template

To edit a specific vNIC template, type vNIC Template in the search bar to find the vNIC template you want to edit.

Note Global vNICs can be used in local service profiles created in Cisco UCS Manager.

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

Step 2 In **Basic**, select the **Organization** where you want to create the vNIC template.

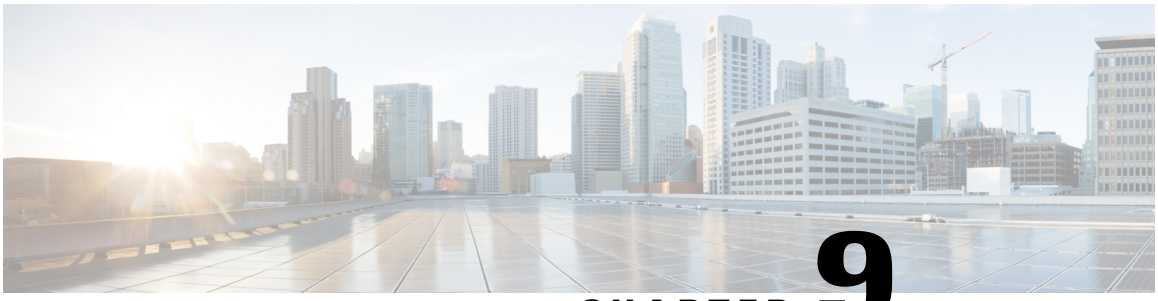
a) Enter a **Name** and **Description**.
b) Select the options for **Type**, **Fabric ID**, **Fabric Failover** and enter **MTU**.

Step 3 Click **MAC Address** and select the MAC address.
If you do not assign a MAC address pool, the system assigns the default.

Step 4 Click **vLANs** and add the vLANs that you want to use for this vNIC template.

Step 5 Click **Policies**.
If the policies are not assigned, click on each of the policies. On the right, click the drop-down to display related policies and select the one you want for this vNIC template.

Step 6 Click **Create**.



CHAPTER 9

Service Profiles

This chapter includes the following sections:

Service Profiles

From the **Service Profiles** page you can view a list of all service profiles in Cisco UCS Central, and filter which service profiles are displayed.

Service Profile Detail View

The Service Profile page displays detailed information about a service profile. From here, you can:

- View logs and configuration status
- Create a service profile template from this service profile
- Delete, clone, or rename the service profile
- Assign or unassign a server
- Configure the host interface placement
- Bind to template
- Shut down server
- Reset server
- Launch KVM and UCS Domain

Creating Service Profile from Template

Step 1 In the Task bar, type **Create Service Profile from Template** and press Enter.
This launches the **Create Service Profile from Template** dialog box.

Step 2 In **Service Profile Template to Instantiate**, click drop-down to select the service profile template from the available list.

Step 3 In **Organization** drop-down, select the org where you want to create this service profile.

Step 4 In **No of Service Profiles**, specify the number of service profiles you want to create using this template.

Step 5 In Service Profile Name Prefix, enter a prefix.

Binding a Service Profile to a Template

Step 1 From the **Service Profile** page, click the **Settings** icon.

Step 2 Click **Bind To Template**.
This launches the **Bind Service Profile** dialog box.

Step 3 In **Service Profile Template to Instantiate**, select the service profile template from the available list.

Step 4 Click **Bind**.

Manually Assigning a Server to a Service Profile

Step 1 From the **Service Profile** page, click the **Settings** icon.

Step 2 Click **Assign Server Manually**.
This launches the **Assign Server Manually** dialog box.

Step 3 Choose whether to enable **Compatibility Check On Migration Using Manual Assignment**.

Step 4 Select the server that you want to assign to the service profile.

Step 5 Click **Assign Server Manually**.

Configuring Interface Placement on a Service Profile or Service Profile Template

Step 1 From the **Service Profile** or **Service Profile Template** page, click the **Settings** icon.

Step 2 Click **Configure Interface Placement**.
This launches the **Configure Host Interface Placement** dialog box.

Step 3 In **Placement**, choose whether to enable **Manual Interface Placement**.
If you select **Disabled**, the system automatically assigns interfaces based on their PCI order.

Step 4 If Enabled, add vHBAs or vNICs.

Step 5 In **Preference**, select the **Virtual Slot Selection Preference** for each virtual slot.

Note This field is only present on service profile templates.

This can be one of the following:

- **all—**All configured vNICs and vHBAs can be assigned. This is the default.
- **assigned-only—**vNICs and vHBAs must be explicitly assigned.
- **exclude-dynamic—**Dynamic vNICs and vHBAs cannot be assigned.
- **exclude-unassigned—**Unassigned vNICs and vHBAs cannot be assigned.
- **exclude-usnic—**usNIC vNICs cannot be assigned.

Step 6 In **PCI Order**, click the up and down arrows to arrange the order.

Note If **Manual Interface Placement** is enabled, the PCI order is read-only.

Step 7 Click **Configure Host Interface Placement**.

Service Profile Faults

Cisco UCS Central collects and displays all the Cisco UCS Central service profile faults on the **Service Profile Fault Logs** page. To view service profile faults, click the **Faults** icon in the **Fault Summary** section of a **Service Profile** details page. The **Faults Logs** page displays information on the type and severity level of the fault, and allow you to monitor and acknowledge the system faults, and filter the faults that are displayed.

The faults table includes the following information for each fault:

- **Code—**The ID associated with the fault
- **Timestamp—**Date and time at which the fault occurred
- **Type—**Origin of the fault
- **Cause—**Cause of the fault
- **Affected Object—**The component that is affected by this fault

- **Fault Details—**The details of the fault.
- **Severity—**The severity of the fault
- **Action—**Any action required by the fault

To manage the information that is collected, see Configuring UCS Central System Policies, on page 37.

Service Profile Server Faults

Cisco UCS Central collects and displays all the server faults associated with a service profile. To view server faults, click the **Faults** icon in the **Server Fault Summary** section of a **Service Profile** details page. The **Faults Logs** page displays information on the type and severity level of the fault, and allow you to monitor and acknowledge the system faults, and filter the faults that are displayed.

The faults table includes the following information for each fault:

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

To manage the information that is collected, see Configuring UCS Central System Policies, on page 37.

Service Profile Event Logs

Displays event logs for the selected service profile. This can include the following:

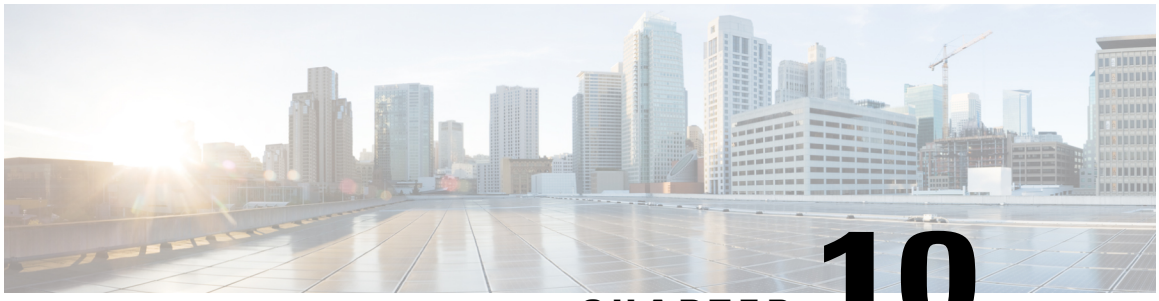
- **ID—**Unique identifier associated with the event that caused the fault
- **Timestamp—**Date and time at which the event occurred
- **Trig. By—**Type of user associated with the event
- **Affected Object—**The component that is affected by the event

Service Profile Audit Logs

Displays the audit logs for the selected service profile. This includes the following:

- Resources that were accessed
- Day 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



CHAPTER 10

Policies

This chapter includes the following sections:

Policies in Cisco UCS Central and Cisco UCS Domains

You can create and manage global policies in Cisco UCS Central and include them in service profiles or service profile templates for one or more Cisco UCS domains. The service profiles and service profile templates that include global policies can be either of the following:

- Local service profiles or service profile templates that are created and managed by Cisco UCS Manager in one Cisco UCS domain. You can only associate local service profiles with servers in that domain. When you include a global policy in a local service profile, Cisco UCS Manager makes a local read-only copy of that policy.
- Global service profiles or service profile templates that are created and managed by Cisco UCS Central. You can associate global service profiles with servers in one or more registered Cisco UCS domains.

You can only make changes to global policies in Cisco UCS Central. Those changes affect all service profiles and service profile templates that include the global policy. All global policies are read-only in Cisco UCS Manager.

You can configure all operational policies under a domain group using IPv6 addresses. These policies are located in the **Operations Management** tab of the Cisco UCS Central GUI.

This feature helps the Cisco UCS Manager to use an IPv6 address while importing these policies from Cisco UCS Central.

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

For each Cisco UCS domain that you register with Cisco UCS Central, you can choose which application will manage certain policies and configuration settings. This policy resolution does not have to be the same for every Cisco UCS domain that you register with the same Cisco UCS Central.

You have the following options for resolving these policies and configuration settings:

- **Local**—The policy or configuration is determined and managed by Cisco UCS Manager.

- **Global—**The policy or configuration is determined and managed by Cisco UCS Central.

The following table contains a list of the policies and configuration settings that you can choose to have managed by either Cisco UCS Manager or Cisco UCS Central:

Name	Description
Infrastructure & Catalog Firmware	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Time Zone Management	Determines whether the date and time is defined locally or comes from Cisco UCS Central.
Communication Services	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Global Fault Policy	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.
User Management	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
DNS Management	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Backup & Export Policies	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Monitoring	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
SEL Policy	Determines whether managed endpoints are defined locally or in Cisco UCS Central.
Power Management	Determines whether the power management is defined locally or in Cisco UCS Central.
Power Supply Unit	Determines whether power supply units are defined locally or in Cisco UCS Central.

Consequences of Policy Resolution Changes

When you register a Cisco UCS domain, you configure policies for local or global resolution. The behavior that occurs when the Cisco UCS domain is registered or when that registration or configuration changes, depends upon several factors, including whether a domain group has been assigned or not.

The following table describes the policy resolution behavior you can expect for each type of policy.

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Call Home	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
SNMP configuration	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
HTTP	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Telnet	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
CIM XML	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Management interfaces monitoring policy	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Power allocation policy	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Power policy (also known as the PSU policy)	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
SEL policy	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Authentication Domains	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
LDAP	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
LDAP provider groups and group maps	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
TACACS, including provider groups	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
RADIUS, including provider groups	N/A Cisco UCS Manager only	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
SSH (Read-only)	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
DNS	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Time zone	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Web Sessions	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Fault	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Core Export	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Syslog	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Global Backup/Export Policy	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Default Authentication	Domain group root	Assigned domain group	Local	Local/Remote	Retains last known policy state	Converted to a local policy
Console Authentication	Domain group root	Assigned domain group	Local	Can be local or remote	Retains last known policy state	Converted to a local policy
Roles	Domain group root	Assigned domain group	Local	Local/Combine (Remote replacing Local)	Deletes remote policies	Converted to a local policy
Locales - Org Locales	Domain group root	Assigned domain group	Local	Local/Combine (Remote replacing Local)	Deletes remote policies	Converted to a local policy
Trust Points	Domain group root	Assigned domain group	Local	Local/Combine (Remote replacing Local)	Deletes remote policies	Converted to a local policy
Firmware Download Policy	Domain group root	N/A	N/A	N/A	N/A	N/A
ID Soaking Policy	Domain group root	N/A	N/A	N/A	N/A	N/A
Locales - Domain Group Locales	Domain group root	N/A	N/A	N/A	N/A	N/A
Infrastructure Firmware Packs	N/A	Assigned domain group	Local	Local/Remote (if Remote exists)	Retains last known policy state	Converted to a local policy
Catalog	N/A	Assigned domain group	Local	Local/Remote (if Remote exists)	Retains last known policy state	Converted to a local policy

Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 78	See Consequences of Service Profile Changes on Policy Resolution, on page 78	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 78	See Consequences of Service Profile Changes on Policy Resolution, on page 78	Deletes remote policies	Converted to a local policy
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 78	See Consequences of Service Profile Changes on Policy Resolution, on page 78	Deletes remote policies	Converted to a local policy

Consequences of Service Profile Changes on Policy Resolution

For certain policies, the policy resolution behavior is also affected by whether or not one or more service profiles that include that policy have been updated.

The following table describes the policy resolution behavior you can expect for those policies.

Policy	Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Domain Group Assigned after Registration with Cisco UCS Central
	Domain Group Unassigned / Domain Group Assigned		
	Service Profile not Modified	Service Profile Modified	
Maintenance Policy **Note** If you are using a global maintenance policy in a local service profile, all pending activities must be acknowledged on the Cisco UCS Central **Pending Activities** page.	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)
Schedule	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)
Host Firmware Packages	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)

Boot Policy

Boot policy overrides the boot order in the BIOS setup menu, and determines the following:

- Selection of the boot device
- Location from which the server boots
- Order in which boot devices are invoked

For example, you can choose to have associated servers boot from a local device, such as a local disk or CD-ROM (VMedia), or you can select a SAN boot or a LAN (PXE) boot.

You can either create a named boot policy that can be associated with one or more service profiles, or create a boot policy for a specific service profile. A boot policy must be included in a service profile, and that service profile must be associated with a server for it to take effect. If you do not include a boot policy in a service profile, the UCS domain applies the default boot policy.

Note Changes to a boot policy will be propagated to all service profiles created with an updating service profile template that includes that boot policy. Reassociation of the service profile with the server to rewrite the boot order information in the BIOS is automatically triggered.

Creating or Editing a Boot Policy

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

Step 2 Choose the organization from the drop-down list, and then enter a unique name and optional description for the policy.

Step 3 (Optional) Click **Enabled** for **Reboot on Boot Order Change** to reboot all servers that use this boot policy after you make changes to the boot order.
For boot policies applied to a server with a non-Cisco VIC adapter, even if Reboot on Boot Order Change is disabled, when SAN devices are added, deleted, or their order is changed, the server always reboots when boot policy changes are saved.

Step 4 (Optional) Click **Enabled** for **Enforce Interface Name** to receive a configuration error if any of the vNICs, vHBAs or iSCSI vNICs in the Boot Order section match the server configuration in the service profile.

Step 5 In **Boot Mode**, click **Legacy** or **Unified Extensible Firmware Interface (UEFI)**.

Step 6 Click the **Boot Order** icon and perform the following:

a) Click the **Add** button to add boot options.
b) Update the required properties for the boot option.
c) Use the up and down arrows to arrange the boot order.

Note If you create a boot policy for iSCSI boot in the HTML5 GUI, you can only update that boot policy in the HTML5 GUI.

Step 7 Click **Save**.

BIOS Policy

The BIOS policy automates the configuration of BIOS settings for a server or group of servers. You can create global BIOS policies available to all servers in the root organization, or you can create BIOS policies in sub-organizations that are only available to that hierarchy.

To use a BIOS policy, do the following:

1. Create the BIOS policy in Cisco UCS Central.
2. Assign the BIOS policy to one or more service profiles.
3. Associate the service profile with a server.

During service profile association, Cisco UCS Central modifies the BIOS settings on the server to match the configuration in the BIOS policy. If you do not create and assign a BIOS policy to a service profile, the server uses the default BIOS settings for that server platform.

Related Topics

Basic BIOS Settings, on page 82
Processor BIOS Settings, on page 84
Intel Directed I/O BIOS Settings, on page 89
RAS Memory BIOS Settings, on page 91
USB BIOS Settings, on page 92
PCI BIOS Settings, on page 94
Boot Options BIOS Settings, on page 100
Server Manager, on page 102
Console , on page 104
Default BIOS Settings, on page 82
Basic BIOS Settings, on page 82
Boot Options BIOS Settings, on page 100
Console , on page 104
Intel Directed I/O BIOS Settings, on page 89
PCI BIOS Settings, on page 95
Processor BIOS Settings, on page 84
RAS Memory BIOS Settings, on page 91
Server Manager, on page 102
USB BIOS Settings, on page 92

Creating or Editing a BIOS Policy

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

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

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

b) (Optional) Complete the other fields as necessary.
For more information, see Basic BIOS Settings, on page 82.

Step 3 In **Processor**, complete the fields as necessary.
For more information, see Processor BIOS Settings, on page 84.

Step 4 In **I/O**, complete the fields as necessary.
For more information, see Intel Directed I/O BIOS Settings, on page 89.

Step 5 In **RAS Memory**, complete the fields as necessary.
For more information, see RAS Memory BIOS Settings, on page 91.

Step 6 In **USB**, complete the fields as necessary.

For more information, see USB BIOS Settings, on page 92.

Step 7 In **PCI**, complete the fields as necessary.
For more information, see PCI BIOS Settings, on page 95.

Step 8 In **Boot Options**, complete the fields as necessary.
For more information, see Boot Options BIOS Settings, on page 100.

Step 9 In **Server Manager**, complete the fields as necessary.
For more information, see Server Manager, on page 102.

Step 10 In **Console**, complete the fields as necessary.
For more information, see Console , on page 104.

Step 11 Click **Create**.

Default BIOS Settings

Cisco UCS Central includes a set of default BIOS settings for each type of server supported by Cisco UCS. The default BIOS settings are available only in the root organization and are global. Only one set of default BIOS settings can exist for each server platform supported by Cisco UCS. You can modify the default BIOS settings, but you cannot create an additional set of default BIOS settings.

Each set of default BIOS settings are designed for a particular type of supported server and are applied to all servers of that specific type which do not have a BIOS policy included in their service profiles.

Unless a Cisco UCS implementation has specific needs that are not met by the server-specific settings, we recommend that you use the default BIOS settings that are designed for each type of server in the Cisco UCS domain.

Cisco UCS Central applies these server platform-specific BIOS settings as follows:

- The service profile associated with a server does not include a BIOS policy.
- The BIOS policy is configured with the platform-default option for a specific setting.

You can modify the default BIOS settings provided by Cisco UCS Central. However, any changes to the default BIOS settings apply to all servers of that particular type or platform. If you want to modify the BIOS settings for only certain servers, we recommend that you use a BIOS policy.

Basic BIOS Settings

The following table lists the main server BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Reboot on BIOS Settings Change	When the server is rebooted after you change one or more BIOS settings. **Enabled—**If you enable this setting, the server is rebooted according to the maintenance policy in the server's service profile. For example, if the maintenance policy requires user acknowledgment, the server is not rebooted and the BIOS changes are not applied until a user acknowledges the pending activity. **Disabled—**If you do not enable this setting, the BIOS changes are not applied until the next time the server is rebooted, whether as a result of another server configuration change or a manual reboot.
Serial Port A	Whether serial port A is enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The serial port is disabled. • **Enabled—**The serial port is enabled.
Quiet Boot	What the BIOS displays during Power On Self-Test (POST). This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The BIOS displays all messages and Option ROM information during boot. • **Enabled—**The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot.
Post Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The BIOS continues to attempt to boot the server. • **Enabled—**The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.

Name	Description
Front Panel Lockout	Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The power and reset buttons on the front panel are active and can be used to affect the server. • **Enabled—**The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI.
Resume AC On Power Loss	How the server behaves when power is restored after an unexpected power loss. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Last State—**The server is powered on and the system attempts to restore its last state. • **Reset—**The server is powered on and automatically reset. • **Stay Off—**The server remains off until manually powered on.

Processor BIOS Settings

The following table lists the processor BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Turbo Boost	Whether the processor uses Intel Turbo Boost Technology, which allows the processor to automatically increase its frequency if it is running below power, temperature, or voltage specifications. This can be one of the following: • **disabled—**The processor does not increase its frequency automatically. • **enabled—**The processor uses Turbo Boost Technology if required. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Enhanced Intel Speedstep	Whether the processor uses Enhanced Intel SpeedStep Technology, which allows the system to dynamically adjust processor voltage and core frequency. This technology can result in decreased average power consumption and decreased average heat production. This can be one of the following: • **disabled—**The processor never dynamically adjusts its voltage or frequency. • **enabled—**The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Hyper Threading	Whether the processor uses Intel Hyper-Threading Technology, which allows multithreaded software applications to execute threads in parallel within each processor. This can be one of the following: • **disabled—**The processor does not permit hyperthreading. • **enabled—**The processor allows for the parallel execution of multiple threads. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure the operating system supports this feature.

Name	Description
Core Multi Processing	Sets the state of logical processor cores per CPU in a package. If you disable this setting, Intel Hyper Threading technology is also disabled. This can be one of the following: • **all—**Enables multiprocessing on all logical processor cores. • **1** through ***n*—**Specifies the number of logical processor cores per CPU that can run on the server. To disable multiprocessing and have only one logical processor core per CPU running on the server, choose 1. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Execute Disabled Bit	Classifies memory areas on the server to specify where the application code can execute. As a result of this classification, the processor disables code execution if a malicious worm attempts to insert code in the buffer. This setting helps to prevent damage, worm propagation, and certain classes of malicious buffer overflow attacks. This can be one of the following: • **disabled—**The processor does not classify memory areas. • **enabled—**The processor classifies memory areas. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Virtualization Technology (VT)	Whether the processor uses Intel Virtualization Technology, which allows a platform to run multiple operating systems and applications in independent partitions. This can be one of the following: • **disabled—**The processor does not permit virtualization. • **enabled—**The processor allows multiple operating systems in independent partitions. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** If you change this option, you must power cycle the server before the setting takes effect.

Name	Description
Direct Cache Access	Allows processors to increase I/O performance by placing data from I/O devices directly into the processor cache. This setting helps to reduce cache misses. This can be one of the following: • **disabled—**Data from I/O devices is not placed directly into the processor cache. • **enabled—**Data from I/O devices is placed directly into the processor cache. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Processor C State	Whether the system can enter a power savings mode during idle periods. This can be one of the following: • **disabled—**The system remains in a high-performance state even when idle. • **enabled—**The system can reduce power to system components such as the DIMMs and CPUs. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
Processor C1E	Allows the processor to transition to its minimum frequency upon entering C1. This setting does not take effect until after you have rebooted the server. This can be one of the following: • **disabled—**The CPU continues to run at its maximum frequency in the C1 state. • **enabled—**The CPU transitions to its minimum frequency. This option saves the maximum amount of power in the C1 state. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Processor C3 Report	Whether the processor sends the C3 report to the operating system. This can be one of the following: • **disabled—**The processor does not send the C3 report. • **acpi-c2—**The processor sends the C3 report using the advanced configuration and power interface (ACPI) C2 format. • **acpi-c3—**The processor sends the C3 report using the ACPI C3 format. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. On the Cisco UCS B440 Server, the BIOS Setup menu uses enabled and disabled for these options. If you specify acpi-c2 or acpi-c2, the server sets the BIOS value for that option to enabled.
Processor C6 Report	Whether the processor sends the C6 report to the operating system. This can be one of the following: • **disabled—**The processor does not send the C6 report. • **enabled—**The processor sends the C6 report. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Processor C7 Report	Whether the processor sends the C7 report to the operating system. This can be one of the following: • **disabled—**The processor does not send the C7 report. • **enabled—**The processor sends the C7 report. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
CPU Performance	Sets the CPU performance profile for the server. This can be one of the following: • **enterprise—**For M3 servers, all prefetchers and data reuse are enabled. For M1 and M2 servers, data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • **high-throughput—**Data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • **hpc—**All prefetchers are enabled and data reuse is disabled. This setting is also known as high-performance computing. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Max Variable MTRR Setting	Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following: • **auto-max—**BIOS uses the default value for the processor. • **8—**BIOS uses the number specified for the variable MTRR. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Intel Directed I/O BIOS Settings

The following table lists the Intel Directed I/O BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
VIrtualization Technology (VT)for Directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). You can select one of the following options: • **disabled—**The processor does not use virtualization technology. • **enabled—**The processor uses virtualization technology. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This option must be enabled if you want to change any of the other Intel Directed I/O BIOS settings.
Interrupt Remap	Whether the processor supports Intel VT-d Interrupt Remapping. You can select one of the following options: • **disabled—**The processor does not support remapping. • **enabled—**The processor uses VT-d Interrupt Remapping as required. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Coherency Support	Whether the processor supports Intel VT-d Coherency. You can select one of the following options: • **disabled—**The processor does not support coherency. • **enabled—**The processor uses VT-d Coherency as required. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Address Translation Services (ATS) Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). You can select one of the following options: • **disabled—**The processor does not support ATS. • **enabled—**The processor uses VT-d ATS as required. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Pass Through DMA Support	Whether the processor supports Intel VT-d Pass-through DMA. You can select one of the following options: • **disabled—**The processor does not support pass-through DMA. • **enabled—**The processor uses VT-d Pass-through DMA as required. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

RAS Memory BIOS Settings

The following table lists the RAS memory BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • **disabled—**The BIOS does not support NUMA. • **enabled—**The BIOS includes the ACPI tables that are required for NUMA-aware operating systems. If you enable this option, the system must disable Inter-Socket Memory interleaving on some platforms. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
LV DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • **power-saving-mode—**The system prioritizes low voltage memory operations over high frequency memory operations. This mode may lower memory frequency in order to keep the voltage low. • **performance-mode—**The system prioritizes high frequency operations over low voltage operations. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
DRAM Refresh Rate	The refresh interval rate for internal memory. This can be one of the following: • **1x** • **2x** • **3x** • **4x** • **auto** • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Memory RAS Config	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • **maximum performance—**System performance is optimized. • **mirroring—**System reliability is optimized by using half the system memory as backup. • **lockstep—**If the DIMM pairs in the server have an identical type, size, and organization and are populated across the SMI channels, you can enable lockstep mode to minimize memory access latency and provide better performance. Lockstep is enabled by default for B440 servers. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

USB BIOS Settings

The following table lists the USB BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Make Device Non Bootable	Whether the server can boot from a USB device. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The server can boot from a USB device. • **Enabled—**The server cannot boot from a USB device.
USB Front Panel Access Lock	USB front panel lock is configured to enable or disable the front panel access to USB ports. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled** • **Enabled**
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • **Auto—**Disables legacy USB support if no USB devices are connected. • **Disabled—**USB devices are only available to EFI applications. • **Enabled—**Legacy USB support is always available. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
USB Idle Power Optimizing Setting	Whether the USB System Idle Power Optimizing setting is used to reduce USB EHCI idle power consumption. Depending upon the value you choose, this setting can have an impact on performance. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **High Performance—**The USB System Idle Power Optimizing setting is disabled, because optimal performance is preferred over power savings. Selecting this option can significantly improve performance. We recommend you select this option unless your site has server power restrictions. • **Lower Idle Power—**The USB System Idle Power Optimizing setting is enabled, because power savings are preferred over optimal performance.

PCI BIOS Settings

The following table lists the PCI BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Max Memory Below 4G	Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Does not maximize memory usage. Choose this option for all operating systems with PAE support. • **Enabled—**Maximizes memory usage below 4GB for an operating system without PAE support.

Name	Description
Memory Mapped IO Above 4Gb Configuration	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**Maps I/O of 64-bit PCI devices to 4GB or greater address space.

PCI BIOS Settings

The following tables list the PCI configuration BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Table 3: Basic Tab

Name	Description
Max Memory Below 4G	Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Does not maximize memory usage. Choose this option for all operating systems with PAE support. • **Enabled—**Maximizes memory usage below 4GB for an operating system without PAE support.

Name	Description
Memory Mapped IO Above 4Gb Configuration	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • **Enabled—**Maps I/O of 64-bit PCI devices to 4GB or greater address space.
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • **Onboard—**Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • **Offboard—**Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • **Onboard VGA Disabled—**Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** Only onboard VGA devices are supported with Cisco UCS B-Series servers.

Name	Description
PCIe OptionROMs	Whether Option ROM is available on all expansion ports. This can be one of the following: • **Disabled—**The expansion slots are not available. • **Enabled—**The expansion slots are available. • **UEFI-Only—**The expansion slots are available for UEFI only. • **Legacy Only—**The expansion slots are available for legacy only. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Mezz OptionRom	Whether all mezzanine PCIe ports are enabled or disabled. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**All LOM ports are enabled. • **Disabled—**All LOM ports are disabled.
PCIe 10G LOM 2 Link	Whether Option ROM is available on the 10G LOM port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Enabled—**The expansion slot is available. • **Disabled—**The expansion slot is not available.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Auto—**The CPU determines the power state. • **Disabled—**ASPM support is disabled in the BIOS. • **Force L0—**Force all links to L0 standby (L0s) state.

Table 4: PCIe Slot Link Speed Tab

Name	Description
Slot *n* Link Speed	This option allows you to restrict the maximum speed of an adapter card installed in PCIe slot ***n***. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **gen1 - 2.5 GT/s—**2.5GT/s (gigatransfers per second) is the maximum speed allowed. • **gen2 - 5 GT/s—**5GT/s is the maximum speed allowed. • **gen3 - 8 GT/s—**8GT/s is the maximum speed allowed. • **Auto—**The maximum speed is set automatically. • **Disabled—**The maximum speed is not restricted.

Table 5: PCIe Slot OptionROM Tab

Name	Description
Slot *n* OptionROM	Whether Option ROM is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.

Name	Description
Slot SAS	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.
Slot HBA	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.
Slot MLOM	Whether Option ROM is available on the PCIe slot connected to the MLOM available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.

Name	Description
Slot N1	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.
Slot N2	Whether is available on the specified port. This can be one of the following: • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **Disabled—**The expansion slot is not available. • **Enabled—**The expansion slot is available. • **UEFI Only—**The expansion slot is available for UEFI only. • **Legacy Only—**The expansion slot is available for legacy only.

Boot Options BIOS Settings

The following table lists the boot options BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Boot Option Retry	Whether the BIOS retries NON-EFI based boot options without waiting for user input. This can be one of the following: • **disabled—**Waits for user input before retrying NON-EFI based boot options. • **enabled—**Continually retries NON-EFI based boot options without waiting for user input. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • **disabled—**The software RAID controller is not available. • **enabled—**The software RAID controller is available. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID	Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following: • **disabled—**The Intel SAS Entry RAID Module is disabled. • **enabled—**The Intel SAS Entry RAID Module is enabled. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.
Intel Entry SAS RAID Module	How the Intel SAS Entry RAID Module is configured. This can be one of the following: • **it-ir-raid—**Configures the RAID module to use Intel IT/IR RAID. • **intel-esrtii—**Configures the RAID module to use Intel Embedded Server RAID Technology II. • **Platform Default—**The BIOS uses the value of this attribute contained in the BIOS defaults for the server type and vendor.

Server Manager

The following tables list the server management BIOS settings that you can configure through a BIOS policy or the default BIOS settings:

Name	Description
Assert NMI on SERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • **disabled—**The BIOS does not generate an NMI or log an error when a SERR occurs. • **enabled—**The BIOS generates an NMI and logs an error when a SERR occurs. You must enable this setting if you want to enable **Assert Nmi on Perr**. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Assert NMI on PERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a processor bus parity error (PERR) occurs. This can be one of the following: • **disabled—**The BIOS does not generate an NMI or log an error when a PERR occurs. • **enabled—**The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert Nmi on Serr** to use this setting. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
OS Boot Watchdog Timer	Whether the BIOS programs the watchdog timer with a predefined timeout value. If the operating system does not complete booting before the timer expires, the CIMC resets the system and an error is logged. This can be one of the following: • **disabled—**The watchdog timer is not used to track how long the server takes to boot. • **enabled—**The watchdog timer tracks how long the server takes to boot. If the server does not boot within the predefined length of time, the CIMC resets the system and logs an error. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. This feature requires either operating system support or Intel Management software.
OS Boot Watchdog Timer Timeout	What timeout value the BIOS uses to configure the watchdog timer. This can be one of the following: • **5-minutes—**The watchdog timer expires 5 minutes after the OS begins to boot. • **10-minutes—**The watchdog timer expires 10 minutes after the OS begins to boot. • **15-minutes—**The watchdog timer expires 15 minutes after the OS begins to boot. • **20-minutes—**The watchdog timer expires 20 minutes after the OS begins to boot. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. This option is only available if you enable the OS Boot Watchdog Timer.

Console

Name	Description
Legacy OS Redirect	Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following: • **disabled—**The serial port enabled for console redirection is hidden from the legacy operating system. • **enabled—** The serial port enabled for console redirection is visible to the legacy operating system. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Console Redirection	Allows a serial port to be used for console redirection during POST and BIOS booting. After the BIOS has booted and the operating system is responsible for the server, console redirection is irrelevant and has no effect. This can be one of the following: • **disabled—**No console redirection occurs during POST. • **serial-port-a—**Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. • **serial-port-b—**Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.

Name	Description
BAUD Rate	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • **9600—**A 9600 BAUD rate is used. • **19200—**A 19200 BAUD rate is used. • **38400—**A 38400 BAUD rate is used. • **57600—**A 57600 BAUD rate is used. • **115200—**A 115200 BAUD rate is used. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.
Terminal Type	What type of character formatting is used for console redirection. This can be one of the following: • **pc-ansi—**The PC-ANSI terminal font is used. • **vt100—**A supported vt100 video terminal and its character set are used. • **vt100-plus—**A supported vt100-plus video terminal and its character set are used. • **vt-utf8—**A video terminal with the UTF-8 character set is used. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Flow Control	Whether a handshake protocol is used for flow control. Request to Send / Clear to Send (RTS/CTS) helps to reduce frame collisions that can be introduced by a hidden terminal problem. This can be one of the following: • **none—**No flow control is used. • **rts-cts—**RTS/CTS is used for flow control. • **Platform Default—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** This setting must match the setting on the remote terminal application.

Ethernet Adapter Policy

Ethernet adapter policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Ethernet adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Note We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

If you are creating an Ethernet adapter policy (instead of using the default Windows adapter policy) for a Windows operating system, you must use the following formulas to calculate values that work with Windows:

Completion Queues = Transmit Queues + Receive Queues
Interrupt Count = (Completion Queues + 2) rounded up to nearest power of 2

For example, if Transmit Queues = 1 and Receive Queues = 8 then:

Completion Queues = 1 + 8 = 9

Interrupt Count = (9 + 2) rounded up to the nearest power of 2 = 16

Creating and Editing an Ethernet Adapter Policy

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

Step 2 In **Basic**, from the **Organization** drop-down list, select the location in which you want to create the ethernet adapter policy.

Step 3 Enter the **Name** and optional **Description**.

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

a) In **Transmit Queues**, enter the number of transmit queue resources to allocate.
b) In **Transmit Queue Ring Size**, enter the number of descriptors in each transmit queue.
c) In **Receive Queues**, enter the number of receive queue resources to allocate.
d) In **Receive Queues Ring Size**, enter the number of descriptors in each receive queue.
e) In **Completion Queues**, enter the number of completion queue resources to allocate. In general, the number of completion queue resources you allocate should be equal to the number of transmit queue resources, plus the number of receive queue resources.
f) In **Interrupts**, enter the number of interrupt resources to allocate. In general, this value should be equal to the number of completion queue resources.

Step 5 In **Settings**, complete the following:

a) Choose whether to enable **Transmit Checksum Offloading**, **Receive Checksum Offloading**, **TCP Segmentation Offloading**, and **Large TCP Receive Offloading**.
b) Select an **Interrupt Mode**.
c) Enter the **Interrupt Timer** value in microseconds.
d) Select the **Interrupt Coalescing Type**.
e) Enter the **Failback Timeout** in seconds.

Step 6 Click **Create**.

IPMI Access Profile

The IPMI access profile policy allows you to determine whether the IPMI commands can be sent directly to the server, using the IP address. For example, you can send commands to retrieve sensor data from the Cisco IMC. This policy defines the IPMI access, including a username and password that can be authenticated locally on the server, and whether the access is read-only or read-write.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating and Editing an IPMI Access Profile

IPMI access profiles require IPMI users. You can create IPMI users at the same time you create the IPMI access profile, or you can add them to an existing IPMI access profile.

To modify the parameters of an IPMI access profile policy, select the policy from the **All policies** page, and click the **Edit** icon.

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

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

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

Step 4 (Optional) In **IPMI Users**, select an IPMI user name, enter a password, and confirm the password.

Step 5 Select whether to allow read only or admin **Serial over LAN Access**.

Step 6 Click **Create**.

What to Do Next

Include the IPMI profile in a service profile or a service profile template.

Serial over LAN Policy

The serial over LAN policy (SOL) configures a serial over LAN connection for all servers associated with service profiles that use the policy. By default, the serial over LAN connection is disabled.

If you implement a serial over LAN policy, we recommend that you also create an IPMI profile.

You must include this policy in a service profile and that service profile must be associated with a server for it to take effect.

Creating and Editing a Serial over LAN Policy

Step 1 In the Task bar, type **Create Serial Over LAN (SOL) Policy** and press Enter.
This launches the **Create Serial Over LAN (SOL) Policy** dialog box.

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

Step 3 Enter the **Name** and optional **Description** for the policy.

Step 4 Select a value for a **Baud Rate**.

Step 5 Click **Enable** to allow the serial over LAN connection.

Step 6 Click **Create**.

Deleting a Serial over LAN Policy

Before You Begin

Step 1 On the **show search tables** bar, click **Policies**.
You can view the polices at an organization or sub-organization level from the **Show Org Navigation** bar by expanding the root node until you reach the applicable organization name. Click **Go to All Policies Table** from the **root organization** page.

This launches the **All Policies** page.

Step 2 Search the policy that you want to delete.
You can search for the policy in one of the following ways:

- Browse through the list of policies.
- Click **Search** icon and enter the policy name.
- Select **Serial Over LAN** from the **Filter** column.

Step 3 In the **Org** column, click the policy.
This launches the selected **SOL policy** page.

Step 4 On the **SOL policy** page, click the **Delete** icon.
A dialog box prompting you to confirm the deletion of the policy appears.

Step 5 Click **Delete**.

What to Do Next

Dynamic vNIC Connection Policy

The dynamic vNIC connection policy determines how the connectivity between VMs and dynamic vNICs is configured. This policy is required for Cisco UCS domains that include servers with VIC adapters on which you have installed VMs and configured dynamic vNICs.

Each dynamic vNIC connection policy includes an Ethernet adapter policy and designates the number of vNICs that can be configured for any server associated with a service profile that includes the policy.

Note Server Migration:

- If you migrate a server that is configured with dynamic vNICs or another migration tool, the dynamic interface used by the vNICs fails and Cisco UCS Central notifies you of that failure.
- When the server comes back up, Cisco UCS Central assigns new dynamic vNICs to the server. If you are monitoring traffic on the dynamic vNIC, you must reconfigure the monitoring source.

Creating or Editing a Dynamic vNIC Connection Policy

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

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

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

Step 4 Enter the number of dynamic vNICS that you want to create.

Step 5 Select the protection mode that you want to use.

Step 6 Select the adapter profile to be associated with this policy.
The profile must already exist to be included in the **Ethernet Adapter** drop-down list.

Step 7 Click **Create**.

Fibre Channel Adapter Policy

Fibre channel adapter policies govern the host-side behavior of the adapter, including how the adapter handles traffic. For example, you can use these policies to change default settings for the following:

- Queues
- Interrupt handling
- Performance enhancement
- RSS hash
- Failover in an cluster configuration with two fabric interconnects

Note For Fibre Channel adapter policies, the values displayed by Cisco UCS Central may not match those displayed by applications such as QLogic SANsurfer. For example, the following values may result in possible mismatch between SANsurfer and Cisco UCS Central:

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. Cisco UCS Central supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In Cisco UCS Central, you configure this value in milliseconds. Therefore, a value of 5500 ms in Cisco UCS Central displays as 5 s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. Cisco UCS Central allows you to set values of any size. Therefore, a value of 900 in Cisco UCS Central displays as 512 in SANsurfer.

Operating System Specific Adapter Policies

By default, Cisco UCS provides a set of Fibre channel adapter policies. These policies include the recommended settings for each supported server operating system. Operating systems are sensitive to the settings in these policies. Storage vendors typically require non-default adapter settings. You can find the details of these required settings on the support list provided by those vendors.

Note We recommend that you use the values in these policies for the applicable operating system. Do not modify any of the values in the default policies unless directed to do so by Cisco Technical Support.

Creating or Editing a Fibre Channel Adapter Policy

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

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

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

Step 4 In **Resources**, complete the fields as necessary.

Step 5 In **Settings**, complete the fields as necessary.

Step 6 Click **Create**.

Host Firmware Package Policy

The host firmware package policy enables you to specify a set of firmware versions that make up the host firmware package (also known as the host firmware pack).

Creating or Editing a Host Firmware Package Policy

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

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

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

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

Step 5 Click **Create**.

Host Interface Placement Policy

The host interface placement policy enables you to determine the user-specified virtual network interface connection (vCon) placement for vNICs and vHBAs.

To create a host interface placement policy, see Creating or Editing a Host Interface Placement Policy, on page 112. Details for existing policies are displayed on the **Host Interface Placement Policy** page.

Creating or Editing a Host Interface Placement Policy

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

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

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

Step 4 Select the **Virtual Slot Mapping Scheme**.
This can be one of the following:

- **Linear Ordered—**The virtual slots are assigned in order.
- **Round Robin—**The virtual slots are assigned sequentially.

Step 5 Select the **Virtual Slot Selection Preference** for each virtual slot.
This can be one of the following:

- **all—**All configured vNICs and vHBAs can be assigned. This is the default.
- **assigned-only—**vNICs and vHBAs must be explicitly assigned.
- **exclude-dynamic—**Dynamic vNICs and vHBAs cannot be assigned.
- **exclude-unassigned—**Unassigned vNICs and vHBAs cannot be assigned.
- **exclude-usnic—**usNIC vNICs cannot be assigned.

Step 6 Click **Create**.

iSCSI Adapter Policy

Creating or Editing an iSCSI Adapter Policy

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

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

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

Step 4 Enter values for the **Connection Timeout**, **LUN Busy Retry Count**, and **DHCP Timeout**.

Step 5 Choose whether to enable **TCP Timestamp**, **HBA Mode**, and **Boot To Target**.

Step 6 Click **Create**.

Creating or Editing an iSCSI Authentication Profile

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

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

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

Step 4 Enter the **User ID**.

Step 5 Type and confirm the password.

Step 6 Click **Create**.

LAN Connectivity Policy

LAN connectivity policies determine the connections and the network communication resources between the server and the LAN on the network. These policies use pools to assign MAC addresses to servers and to identify the vNICs that the servers use to communicate with the network.

Note These policies are included in service profiles and service profile templates, and can be used to configure multiple servers. So, using static IDs in connectivity policies is not recommended.

Creating or Editing a LAN Connectivity Policy

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

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

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

Step 4 In **vNICs**, enter the **vNIC** and enter the appropriate properties values.

Step 5 In **iSCSI vNICs**, enter the **iSCSI vNIC** and enter the appropriate properties values.

Note If you create a LAN Connectivity Policy in the HTML5 GUI, any iSCSI vNIC parameters that you set on the iSCSI vNICS in the policy can only be updated in the HTML5 GUI.

Step 6 Click **Create**.

Local Disk Policy

This policy configures any optional SAS local drives that have been installed on a server through the onboard RAID controller of the local drive. This policy enables you to set a local disk mode for all servers that are associated with a service profile that includes the local disk configuration policy.

The local disk modes include the following:

- **Any Configuration**
- **No Local Storage**
- **No RAID**
- **RAID 1 Mirrored**
- **RAID 10 Mirrored and Striped**
- **RAID 0 Striped**
- **RAID 6 Striped Dual Parity**
- **RAID 60 Striped Dual Parity Striped**
- **RAID 5 Striped Parity**
- **RAID 50 Striped Parity Striped**

Creating or Editing a Local Disk Policy

Step 1 In the Task bar, type **Create Local Disk Policy** and press Enter.

This launches the **Create Local Disk Policy** dialog box.

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

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

Step 4 In **Mode**, select the configuration mode for the local disks.

Step 5 Choose whether to enable or disable **Configuration Protection**, **FlexFlash**, and **FlexFlash RAID Reporting**.

Step 6 Click **Create**.

Maintenance Policy

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

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

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

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

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

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

Creating or Editing a Maintenance Policy

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

This launches the **Create Maintenance Policy** dialog box.

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

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

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

- **User Acknowledgement—**Configuration changes must be acknowledged by the user, and reboots must be confirmed.
- **Schedule—**Configuration changes are applied depending on the schedule you select. To add a new schedule to the list of values, see Creating or Editing a Schedule, on page 116.
- **Save—**Configuration changes are applied immediately on save and cause a reboot.

Step 5 Click **Create**.

Creating or Editing a Schedule

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

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

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

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

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

a) For **Recurring** schedules, select the start date, frequency, time, and other properties.
b) For **One Time** schedules, select the start date, time, and other properties.
c) For **Advanced** schedules, enter a name for the schedule, choose whether to use a one time or recurring schedule, and select values for the other properties.

Step 5 Click **Create**.

Network Control Policy

This policy configures the network control settings for the Cisco UCS domain, including the following:

- Whether the Cisco Discovery Protocol (CDP) is enabled or disabled
- How the virtual interface (VIF) behaves if no uplink port is available in end-host mode
- The action that Cisco UCS Central takes on the remote Ethernet interface, vEthernet interface , or vFibre Channel interface when the associated border port fails
- Whether the server can use different MAC addresses when sending packets to the fabric interconnect
- Whether MAC registration occurs on a per-VNIC basis or for all VLANs

Action on Uplink Fail

By default, the **Action on Uplink Fail** property in the network control policy is configured with a value of link-down. For adapters such as the Cisco UCS M81KR Virtual Interface Card, this default behavior directs Cisco UCS Central to bring the vEthernet or vFibre Channel interface down if the associated border port fails. For Cisco UCS systems using a non-VM-FEX capable converged network adapter that supports both Ethernet and FCoE traffic, such as Cisco UCS CNA M72KR-Q and the Cisco UCS CNA M72KR-E, this default behavior directs Cisco UCS Central to bring the remote Ethernet interface down if the associated border port fails. In this scenario, any vFibre Channel interfaces that are bound to the remote Ethernet interface are brought down as well.

Note if your implementation includes those types of non-VM-FEX capable converged network adapters mentioned in this section and the adapter is expected to handle both Ethernet and FCoE traffic, we recommend that you configure the **Action on Uplink Fail** property with a value of warning. Note that this configuration might result in an Ethernet teaming driver not being able to detect a link failure when the border port goes down.

MAC Registration Mode

MAC addresses are installed only on the native VLAN by default, which maximizes the VLAN port count in most implementations.

Note If a trunking driver is being run on the host and the interface is in promiscuous mode, we recommend that you set the Mac Registration Mode to All VLANs.

Creating or Editing a Network Control Policy

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

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

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

Step 4 Choose whether to enable **Cisco Discovery Protocol (CDP)**.

Step 5 Select values for **Action on Uplink Failure**, **MAC Address Registration**, and **MAC Address Forging**.

Step 6 Click **Create**.

Power Control Policy

You can create a power control policy in Cisco UCS Central and include it in the service profile to enable the system to manage the power allocation control for the blade servers in the registered Cisco UCS domains.

Cisco UCS uses the priority set in the power control policy, along with the blade type and configuration, to calculate the initial power allocation for each blade within a chassis.

During normal operation, the active blades within a chassis can borrow power from idle blades within the same chassis. If all blades are active and reach the power cap, service profiles with higher priority power control policies take precedence over service profiles with lower priority power control policies. Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

For mission-critical application a special priority called no-cap is also available. Setting the priority to no-cap prevents Cisco UCS from leveraging unused power from a particular server. With this setting, the server is allocated the maximum amount of power possible for that type of server.

Creating or Editing a Power Control Policy

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

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

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

Step 4 Choose whether to enable **Power Capping**.

Step 5 If **Enabled**, use the slider to select the **Power Group Priority**.
Priority is ranked on a scale of 1-10, where 1 indicates the highest priority and 10 indicates lowest priority. The default priority is 5.

Step 6 Click **Create**.

Quality of Service Policy

A quality of service (QoS) policy assigns a system class to the outgoing traffic for a vNIC or vHBA. This system class determines the quality of service for that traffic. For certain adapters, you can also specify additional controls on the outgoing traffic, such as burst and rate.

You must include a QoS policy in a vNIC policy or vHBA policy and then include that policy in a service profile to configure the vNIC or vHBA.

Creating or Editing a Quality of Service Policy

Step 1 In the Task bar, type **Create Quality of Service (QOS) Policy** and press Enter.
This launches the **Create Quality of Service (QOS) Policy** dialog box.

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

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

- In the Egress area, choose a Priority, enter the Burst(Bytes) and Rate(Kbps), and choose the Host Control.

Step 4 Select an **Egress Priority**.

Step 5 Choose whether to enable **Host Control Class of Service (CoS)**.

Step 6 Enter an **Egress Burst Size**, and select the egress average traffic rate.

Step 7 Click **Create**.

SAN Connectivity Policy

SAN connectivity policies determine the connections and the network communication resources between the server and the SAN on the network. These policies use pools to assign WWNs, and WWPNs to servers and to identify the vHBAs that the servers use to communicate with the network.

Note These policies are included in service profiles and service profile templates, and can be used to configure multiple servers. So, using static IDs in connectivity policies is not recommended.

Creating or Editing a SAN Connectivity Policy

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

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

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

Step 4 In **Identifiers**, choose the WWNN pool.
For more information, see Creating and Editing a WWN Pool, on page 131.

Step 5 In **vHBAs**, create one or more vHBAs and select the properties.
You can manually create the vHBA or use a vHBA template.

Step 6 Click **Create**.

Scrub Policy

From Cisco UCS Central you can create scrub policy to determine what happens to local data and to the BIOS settings on a server during the discovery process, when the server is reacknowledged, or when the server is disassociated from a service profile.

Note Local disk scrub policies only apply to hard drives that are managed by Cisco UCS Manager and do not apply to other devices such as USB drives.

Depending upon how you configure a scrub policy, the following can occur at those times:

Disk scrub

One of the following occurs to the data on any local drives on disassociation:

- If enabled, destroys all data on any local drives.
- If disabled, preserves all data on any local drives, including local storage configuration.

BIOS Settings Scrub

One of the following occurs to the BIOS settings when a service profile containing the scrub policy is disassociated from a server:

- If enabled, erases all BIOS settings for the server and resets them to the BIOS defaults for that server type and vendor.
- If disabled, preserves the existing BIOS settings on the server.

FlexFlash Scrub

FlexFlash Scrub enables you to pair new or degraded SD cards, resolve FlexFlash metadata configuration failures, and migrate older SD cards with 4 partitions to single partition SD cards. One of the following occurs to the SD card when a service profile containing the scrub policy is disassociated from a server, or when the server is reacknowledged:

- If enabled, the HV partition on the SD card is formatted using the PNUOS formatting utility. If two SD cards are present, the cards are RAID-1 paired, and the HV partitions in both cards are marked as valid. The card in slot 1 is marked as primary, and the card in slot 2 is marked as secondary.
- If disabled, preserves the existing SD card settings.

Note

- Because the FlexFlash scrub erases the HV partition on the SD cards, we recommend that you take a full backup of the SD card(s) using your preferred host operating system utilities before performing the FlexFlash Scrub.
- To resolve metadata config failures in a service profile, you need to disable FlexFlash in the local disk config policy before you run the FlexFlash scrub, then enable FlexFlash after the server is reacknowledged.
- Disable the scrub policy as soon as the pairing is complete or the metadata failures are resolved.

Creating or Editing a Scrub Policy

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

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

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

Step 4 Choose the scrub policies that you want to enable.

Step 5 Click **Create**.

vMedia Policy

A vMedia policy is used to configure the mapping information for remote vMedia devices. Two vMedia devices and mappings for CD and HDD are allowed in a vMedia policy. You can configure one ISO and one IMG at a time. ISO configurations map to a CD drive. IMG configurations map to a HDD device.

Note If you want to map a device to a remote folder, you must create an IMG and map it as a HDD device.

From Cisco UCS Central you can provision vMedia devices ISO images for remote UCS servers. Using Scriptable vMedia, you can programmatically mount IMG and ISO images on a remote server. CIMC mounted vMedia provides communications between other mounted media inside your datacenter with no additional requirements for media connection. Scriptable vMedia allows you to control virtual media devices without using a browser to manually map each Cisco UCS server individually.

Scriptable vMedia supports multiple share types including NFS, CIFS, HTTP, and HTTPS shares. Scriptable vMedia is enabled through BIOS configuration and configured through a Web GUI and CLI interface. You can do the following in the registered Cisco UCS domains using scriptable vMedia:

- Boot from a specific vMedia device
- Copy files from a mounted share to local disk

- Install and update OS drivers

Note Support for Scriptable vMedia is applicable for CIMC mapped devices only. Existing-KVM based vMedia devices are not supported.

Creating or Editing a vMedia Policy

You can create a vMedia policy and associate the policy with a service profile.

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

Step 2 In **Basic**, click **Organization** and select the location in which you want to create this vMedia Policy.

a) Enter a **Name** and optional **Description**.
Policy name is case sensitive.

b) (Optional) Select **Enabled** or **Disabled** for Retry on Mount Failure.
If enabled, the vMedia will continue mounting when a mount failure occurs.

Step 3 (Optional) Click **HDD**, and do the following:

a) Enter the **Mount Name**.
b) Select the **Protocol** and fill in required protocol information.
c) In **Generate File name from Service Profile Name**, click **Enabled** or **Disabled**.
Enabled will automatically use the Service profile name as IMG name. The IMG file with the same name as the service profile must be available at the required path. If you select **Disabled**, fill in remote IMG file name that the policy must use.

Step 4 (Optional) Click **CDD** and do the following:

a) Enter the **Mount Name**.
b) Select the **Protocol** and fill in required protocol information.
c) In **Generate File name from Service Profile Name**, click **Enabled** or **Disabled**.
Enabled will automatically use the Service profile name as ISO name. The ISO file with the same name as the service profile must be available at the required path. If you select **Disabled**, fill in remote ISO file name that the policy must use.

Step 5 Click **Create**.

What to Do Next

Associate the vMedia policy with a service profile.

Call Home Policies

Cisco UCS Central supports global call home policies for notifying all email recipients defined in call home profiles to specific Cisco UCS Manager events. (There is no call home support for Cisco UCS Central in this release.) Profiles define lists of email recipients that receive alert notifications (to a maximum defined message size in full text, short text, or XML format) and alert criteria for triggering notifications.

Alert notifications are sent with predefined content based on alert levels (including major, minor, normal, notification and warning) and selected alert groups identifying events that trigger notification (such as diagnostic, environmental, inventory, license and other predefined events). Individual email recipients may be individually added to existing profiles. Registered Cisco UCS domains choosing to define security policies globally within that client's policy resolution control will defer all call home policies to its registration with Cisco UCS Central.

Configuring Call Home

A call home policy is created from a domain group under the domain group root. Call home policies under the Domain Groups root were already created by the system and ready to configure.

SUMMARY STEPS

1. Navigate to the **Domain Group** page.
2. Click the **Settings** icon and select **Call Home Settings**.
3. In **Basic**, click Enabled to enable the Call Home feature, and complete the necessary information.
4. In **Profiles**, click **Add** to create a new profile, or edit an existing profile.
5. In **Alerts**, click **Add** or **Delete** to manage the events that trigger alerts to be sent.
6. Click **Save**.

DETAILED STEPS

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

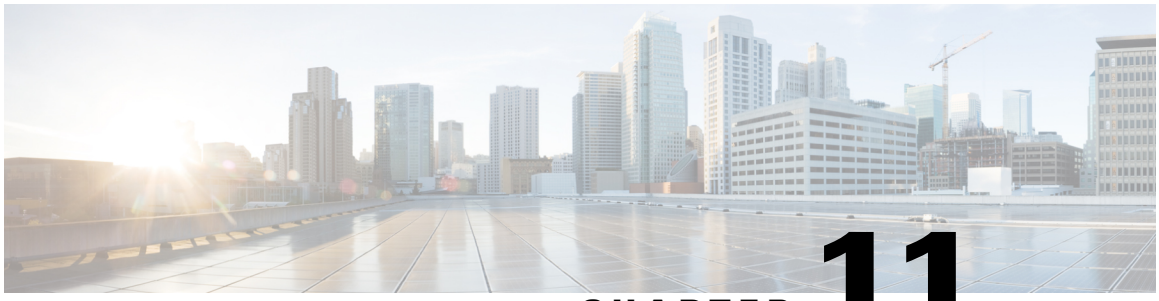
Step 2 Click the **Settings** icon and select **Call Home Settings**.

Step 3 In **Basic**, click Enabled to enable the Call Home feature, and complete the necessary information.

Step 4 In **Profiles**, click **Add** to create a new profile, or edit an existing profile.

Step 5 In **Alerts**, click **Add** or **Delete** to manage the events that trigger alerts to be sent.

Step 6 Click **Save**.



CHAPTER 11

ID Pools

This chapter includes the following sections:

ID Universe

The **ID Universe** displays the pools, collections of identities, or physical or logical resources, that are available in the system. All pools increase the flexibility of service profiles and allow you to centrally manage your system resources. Pools that are defined in Cisco UCS Central are called Global Pools and can be shared between Cisco UCS domains. Global Pools allow centralized ID management across Cisco UCS domains that are registered with Cisco UCS Central. By allocating ID pools from Cisco UCS Central to Cisco UCS Manager, you can track how and where the IDs are used, prevent conflicts, and be notified if a conflict occurs. Pools that are defined locally in Cisco UCS Manager are called Domain Pools.

Note The same ID can exist in different pools, but can be assigned only once. Two blocks in the same pool cannot have the same ID.

You can pool identifying information, such as MAC addresses, to preassign ranges for servers that host specific applications. For example, you can configure all database servers across Cisco UCS domains within the same range of MAC addresses, UUIDs, and WWNs.

From the **ID Universe** page, you can view the total number IDs for each type of pool, and how many of the total are **Available**, **In Use**, or have a **Conflict**. If you click on a **Resource**, you can view detailed information about that ID and where it is used.

IP Pools

IP pools are a collection of IP addresses. You can use IP pools in Cisco UCS Central in one of the following ways:

- For external management of Cisco UCS Managerservers.

- For iSCSI boot initiators.
- For both external management and iSCSI boot initiators in Cisco UCS Manager.

Note The IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

A fault is raised if the same IP address is assigned to two different Cisco UCS domains. If you want to use the same IP address, you can use the **scope** property to specify whether the IP addresses in the block are public or private:

- **public—**The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.
- **private—**The IP addresses in the block can be assigned to multiple Cisco UCS domains.

Cisco UCS Central creates public IP pools by default.

Global IP pools should be used for similar geographic locations. If the IP addressing schemes are different, the same IP pool cannot be used for those sites.

Cisco UCS Central supports creating and deleting IPv4 and IPv6 blocks in IP pools. However, iSCSI boot initiators support only IPv4 blocks.

IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. IQN pools created in Cisco UCS Central can be shared between Cisco UCS domains.

IQN pool members are of the form *prefix***:***suffix***:***number*, where you can specify the prefix, suffix, and a block (range) of numbers.

An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but share the same prefix.

MAC Pools

A MAC pool is a collection of network identities or MAC addresses that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. MAC pools created in Cisco UCS Centralcan be shared between Cisco UCS domains. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Central uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

UUID Suffix Pool

A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable values. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile. Assigning global UUID suffix pools from Cisco UCS Central to service profiles in Cisco UCS Central or Cisco UCS Manager allows them to be shared across Cisco UCS domains.

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS domain. WWN pools created in Cisco UCS Central can be shared between Cisco UCS domain. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA
- Both WW node names and WW port names

Important A WWN pool can include only WWNNs or WWPNs in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks.

WWNN Pools

A World Wide Node Names (WWNN) pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A World Wide Port Name (WWPN) pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

WWxN Pools

A WWxN pool is a WWN pool that contains both WW node names and WW port names. You can specify how many ports per node are created with WWxN pools. The pool size for WWxN pools must be a multiple of *ports-per-node* + 1. For example, if there are 7 ports per node, the pool size must be a multiple of 8. If there are 63 ports per node, the pool size must be a multiple of 64.

All Pools

Display a complete list of ID pools in the system. You can use filter to sort by **Utilization Status**, **Org** or ID **Type** to view availability and usage.

Creating and Editing an IP Pool

After creating an IP pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected IP pool. To select an IP pool, go to **All Pools** page and select the IP pool that you want to edit. The page redirects you to the overall summary page of the selected IP pool.

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

Step 2 In **Basic**, complete the following:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IP pool.
b) Enter the name and description of the pool.

Step 3 Click the respective IP blocks to create a block of IP addresses (IPV4 or IPV6) and complete the following:

a) Click the **Plus** sign to create one or more blocks of IP addresses in the selected pool.
b) In the respective IP block start column, enter the first IPv4 or IPv6 addresses in the block.
c) In the **Size** column, enter the total number of IP addresses in the pool.

Step 4 Click the **Apply** icon.
The page displays additional fields.

Step 5 In **Basic**, complete the following fields:

1. Enter the subnet mask associated with the IPv4 or IPv6 address in the block.
2. Enter the default gateway associated with the IPv4 or IPv6 address in the block.
3. Enter the primary DNS server that this block of IPv4 or IPv6 address should access.
4. Enter the secondary DNS server that this block of IPv4 or IPv6 address should access.
5. Select whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following:

   - **Public—**The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.
   - **Private—**The IP addresses in the block can be assigned to multiple Cisco UCS domains.

Note The scope for an IP address within the block cannot be changed after the block has been saved.

Step 6 In **IPv4** or **IPV6** addresses, you can view a graphical representation of the number of IP addresses in the pool, the number of assigned IP addresses and the number of duplicated IP addresses.

Step 7 In **Access Control**, select a policy to associate with this IP address block from the **ID Range Access Control Policy** drop-down list

Step 8 Click **Create**.

What to Do Next

Creating and Editing an IQN Pool

Note In most cases, the maximum iSCSI Qualified Name (IQN) size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, you must limit the IQN size to 128 characters.

After creating an IQN pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected IQN pool. To select an IQN pool, go to **All Pools** page and select the IQN pool that you want to edit. The page redirects you to the overall summary page of the selected IQN pool.

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

Step 2 In **Basic**, complete the following:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IQN pool.
b) Enter name and description of the IQN pool.
c) Enter the prefix for any IQN blocks created for this pool.

Step 3 In **Suffix Blocks**, complete the following:

a) Click the **Plus** icon to create one or more blocks of IQN suffixes in the selected pool.
b) In the **Suffix Block** column, enter the suffix for this block of IQNs.
c) In the **Start** column, enter the first IQN suffix in the block.
d) In the **Size** column, enter the total number of IQN suffixes in the block.

Step 4 Click the **Apply** icon.

Step 5 Click **Create**.

What to Do Next

Include the IQN suffix pool in a service profile or a service profile template.

Creating and Editing a MAC Pool

After creating a MAC pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected MAC pool. To select a MAC pool, go to **All Pools** page and select the MAC pool that you want to edit. The page redirects you to the overall summary page of the selected MAC pool.

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

Step 2 In **Basic**, complete the following:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access a MAC pool.

b) Enter name and description of the pool.

Step 3 In **MAC Blocks**, complete the following:

a) Click the **Plus** icon to create a block of MAC addresses.

b) In the **MAC Block Start** column, enter the first MAC address in the block.

c) In the **Size** column, enter the number of MAC addresses in the block.

d) Click the **Apply** icon.
Additional fields related to the MAC pools are displayed.

e) In **MAC Addresses**, you can view a graphical representation of the number if MAC addresses in the pool, the number of assigned MAC addresses, duplicate MAC addresses, and MAC summary.

f) In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4 Click **Create**.

What to Do Next

Include the MAC pool in a vNIC template.

Creating and Editing a UUID Suffix Pool

After creating a UUID pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected UUID pool. To select a UUID pool, go to **All Pools** page and select the UUID pool that you want to edit. The page redirects you to the overall summary page of the selected UUID pool.

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

Step 2 In **Basic**, complete the following:

a) From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an UUID pool.

b) Enter name and description of the pool.

c) Enter the sufix for any UUID blocks created for this pool.

Step 3 In **Suffix Blocks**, complete the following:

a) Click the **Create** icon.

b) In the **Suffix Block** column, enter the suffix for this block of UUIDs.

c) In the **Start** column, enter the first UUID suffix in the block.

d) In the **Size** column, enter the total number of UUIDs in the block.

e) Click the **Apply** icon.
Additional fields related to UUID pools are displayed.

f) In **UUIDs**, you can view a graphical representation of the number if UUID addresses in the pool, the number of assigned UUID addresses, duplicate UUID addresses, and UUID summary.
g) In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4 Click **Create**.

What to Do Next

Include the UUID suffix pool in a service profile or service profile template.

Creating and Editing a WWN Pool

After creating a WWN pool you can edit by selecting the **Edit** icon on the overall summary page of the selected WWN pool. To select a WWN pool, go to **All Pools** page and select the WWN pool that you want to edit. The page redirects you to the overall summary page of the selected WWN pool.

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

Step 2 In **Basic**, complete the following:
a) Click **Organization** and select the location in which you want to create the pool.
b) Enter name and description of the WWN pool.
c) In the **World Wide Name (WWN) Used For** area, select one of the following:

- **Port (WWPN)—**The pool is used for both WWNNs and WWPNs.
- **Node (WWNN)—**The pool is used for WWNNs.
- **Both (WWxN)—**The pool is used for WWNNs.

Step 3 In **WWN Blocks**, complete the following:
a) Click the **Create** icon.
b) In the **WWN Block Start** column, enter the first WWN initiator in the block.
c) In the **Size** column, enter the total number of WWN initiators in the pool.
d) Click the **Apply** icon.
Additional fields related to WWN pools are displayed.
e) Click the **WWNs** tab, you can view a graphical representation of the number if WWN addresses in the pool, the number of assigned WWN addresses, and the duplicate MAC addresses and WWN summary.
f) In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4 Click **Create**.
Note You must wait a minimum of 5 seconds before you create another pool.

What to Do Next

- Include the WWPN pool in a vHBA template.
- Include the WWNN pool in a service profile or service profile template.
- Include the WWxN pool in a service profile or service profile template.

Deleting a Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses (from that pool) that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Before You Begin

Step 1 In the navigation bar, click the **Operations** icon and select **Pools**.
This launches the **All Pools** dialog box.

Step 2 In the **Pool name** column, select the pool that you want to delete.
You can search for the pool in one of the following ways:

- Browse through the list of pool.
- Click the **Search** icon and enter the pool name.
- Select a pool type from the **Filter** column.

Step 3 In the **Org** column, click the pool.
This launches the overall summary page of the selected pool.

Step 4 Click the **Delete** icon.
If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory,

local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multitenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

When you select a specific server pool, you can view the individual details for that pool, including the number of servers included in the pool, and the associated qualification policies.

Creating or Editing a Server Pool

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

Step 2 In **Basic**, click **Organization** and select the location in which you want to create the server pool.

Step 3 Enter a **Name** and optional **Description**.

Step 4 In **Qualification**, click **Add** to add new qualification policies, or **Delete** to remove existing ones.
For more information, see Creating or Editing a Server Pool Qualification Policy, on page 134.

Step 5 In **Servers**, add the servers to be included in the pool.

Step 6 Click **Create**.

Server Pool Qualification Policy

Server pool qualification policy qualifies servers based on the server inventory conducted during the discovery process. You can configure these qualifications or individual rules in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration

- Storage configuration and capacity
- Server model or server type
- Owner
- Site
- Address
- Domain group
- Domain name
- Product family

Depending upon the implementation, you might need to configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating or Editing a Server Pool Qualification Policy

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

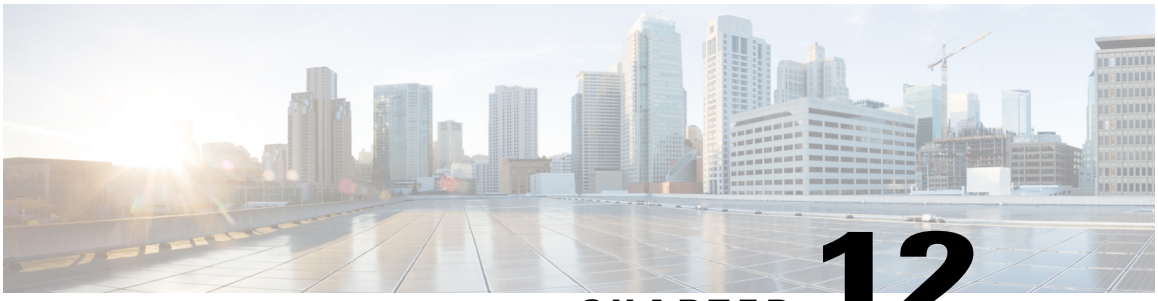
Step 2 In **Basic**, click **Organization** and select the location in which you want to create the server pool qualification policy.

Step 3 Enter a **Name** and optional **Description** and **Server Model/PID**.

Step 4 (Optional) In **Domain**, click the plus sign to add the **Domain Qualifier**.
When you click **Domain Qualifier** the system displays available domain qualification options in tabs on the right pane. Click the appropriate tabs and add the qualification.

Step 5 In **Hardware**, select the appropriate qualification if you enable any of the options such as processor, memory, storage, and adapter.

Step 6 Click **Create**.



CHAPTER 12

Global VLAN and VSAN

This chapter includes the following sections:

Global VLANs

Cisco UCS Central enables you to define global VLANs in LAN cloud at the domain group root or at the domain group level. You can create a single VLAN or multiple VLANs in one operation.

Global VLAN resolution takes place in Cisco UCS Central prior to global service profiles deployment. If a global service profile references a global VLAN, and that VLAN does not exist, the global service profile deployment fails in the Cisco UCS domain due to insufficient resources. All global VLANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Global VLANs are available and can be used in Cisco UCS Manager, even if no global service profile with reference to a global VLAN is deployed in that UCS domain. See Enabling Global VLANs in a Cisco UCS Manager Instance. in the Cisco UCS Central CLI Reference Manual.

Note A global VLAN is not deleted when a global service profile that references it is deleted.

You cannot delete a global VLAN from Cisco UCS Manager. If you want to delete a global VLAN from Cisco UCS Manager, you have to localize the VLAN and then delete it.

VLAN Org Permission

All VLANs configured in Cisco UCS Central are common to the orgs in which they are created. You must assign organization permissions before the Cisco UCS Manager instances that are part of the organizations can consume the resources. When you assign org permission to a VLAN, the VLAN is visible to those organizations, and available to be referenced in service profiles maintained by the Cisco UCS Manager instances that are part of the organization.

VLAN name resolution takes place within the hierarchy of each domain group. If a VLAN with the same name exists in multiple domain groups, the organization permissions are applied to all VLANs with the same name across the domain groups.

You can create, modify or delete VLAN org permission.

Note Make sure to delete the VLAN org permission from the same org you created it in. On Cisco UCS Central GUI you can view the org structure where this VLAN is associated. But at the sub org level on the Cisco UCS Central CLI, you cannot view the VLAN org permission association hierarchy, so if you try to delete the VLAN at the sub org level on the Cisco UCS Central CLI the delete operation will fail.

Creating or Editing a VLAN

You can create a VLAN at the domain group root or at a specific domain group level, and assign specify the orgs that can access the VLAN.

You can edit **VLAN ID**, **Multicast Policy** and access for control for any selected VLANs. After creating a VLAN in a domain group, you can not change the **Domain Group Location** or the **VLAN Name**.

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

Step 2 In **Basic**, click **Domain Group Location** and select the location in which you want to create this VLAN.

Step 3 Enter a **Name** for this VLAN.
VLAN name is case sensitive.

Important Do not use the name **default** when you create a VLAN in Cisco UCS Central. If you want to create a global default VLAN, you may use **globalDefault** for the name.

Step 4 Enter **VLAN ID**.
A VLAN ID can:

- Be between 1 and 3967

  Note If the registered Cisco UCS Domain has UCS Manager version 2.2(4) or above the ID range can be between 1 an 4027.

- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups

Step 5 (Optional) Click **Check VLAN Name Overlap** and **Check VLAN ID Overlap** to identify any overlaps.

Step 6 (Optional) if you want to associate a **Multicast Policy** with this VLAN, enter the multi cast policy name.
Cisco UCS Central identifies the multicast policy and attaches it to the VLAN in the back end.

Step 7 In **Access Control**, click the plus sign to display available orgs.

Step 8 Select the orgs and click the checkmark to apply the selected orgs as **Permitted Orgs** for this VLAN.

Step 9 In **Aliased VLANs**, you can view the existing VLANs to see if a VLAN of the same name already exists.

Step 10 Click **Create**.

Creating or Editing a VLAN Range

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

Step 2 In **Basic**, click **Domain Group Location** and select the location in which you want to create this VLAN.

Step 3 Enter a **Name Prefix** for this VLAN range.

Step 4 Enter **VLAN ID**.
A VLAN ID can:

- Be between 1 and 3967
- Be between 4048 and 4093
- Overlap with other VLAN IDs already defined in other domain groups

Example:
For example, to create six VLANs with IDs 4, 22, 40, 41, 42, and 43, you would enter 4, 22, 40-43.

Step 5 (Optional) Click **Check VLAN Name Overlap** and **Check VLAN ID Overlap** to identify any overlaps.

Step 6 (Optional) if you want to associate a **Multicast Policy** with this VLAN, enter the multi cast policy name.
Cisco UCS Central identifies the multicast policy and attaches it to the VLAN in the back end.

Step 7 In **Access Control**, click the plus sign display available orgs.

Step 8 Select the orgs and click the checkmark to apply the selected orgs as **Permitted Orgs** for this VLAN.

Step 9 In **Aliased VLANs**, you can view the existing VLANs to see if a VLAN of the same name already exists.

Step 10 Click **Create**.

Global VSANs

Cisco UCS Central enables you to define global VSAN in the SAN cloud, at the domain group root, or at a domain group level. The global VSANs created in Cisco UCS Central are specific to the fabric interconnect where you create them. You can assign a VSAN to either Fabric A or Fabric B, or to both Fabric A and B. Global VSANs are not common VSANs in Cisco UCS Central.

Resolution of global VSANs takes place in Cisco UCS Central prior to deployment of global service profiles that reference them to Cisco UCS Manager. If a global service profile references a global VSAN, and that VSAN does not exist, deployment of the global service profile to Cisco UCS Manager will fail due to insufficient resources. All global VSANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Global VSANs are available and can be used in Cisco UCS Manager, even if no global service profile with reference to a global VSAN is deployed in that UCS domain. A global VSAN is not deleted when a global service profile that references it is deleted.

Global VSANs that are referenced by a global service profile available to a Cisco UCS Manager instance remain available unless they are specifically deleted for use from the domain group. Global VSANs can be localized in Cisco UCS Manager, in which case they act as local VSANs. Unless a global VSAN is localized, it cannot be deleted from Cisco UCS Manager.

Creating or Editing a VSAN

You can create a VSAN with IDs from 1 to 4093, except for those in the following reserved ranges:

- If you plan to use FC switch mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3040 to 4078.
- If you plan to use FC end-host mode in a Cisco UCS domain, do not configure VSANs with an ID in the range from 3840 to 4079.

Important FCoE VLANs in the SAN cloud and vLANs in the LAN cloud must have different IDs. Using the same ID for an FCoE vLAN in a VSAN and for a vLAN results in a critical fault and traffic disruption for all vNICs and uplink ports using that VLAN. Ethernet traffic is dropped on any VLAN which has an ID that overlaps with an FCoE vLAN ID.

You can create a VSAN at the domain group root or in a specific domain. You can also assign the VSAN to either fabric A or fabric B, or to both fabric A and B. When you assign the VSAN to both fabrics, both of them must have different VSAN ID and FCoE vLAN ID.

After creating a VSAN, if necessary, you can edit **Fabric Zoning**, **Fabric** assignment, **VSAN ID** and the **FCoE vLAN ID**.

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

Step 2 Click **Domain Group Location** and select the location in which you want to create this VSAN.

Step 3 Enter a **Name**.
VSAN name is case sensitive.

Important Do not use the name **default** when you create a VSAN in Cisco UCS Central. If you want to create a global default VSAN, you may use **globalDefault** for the name.

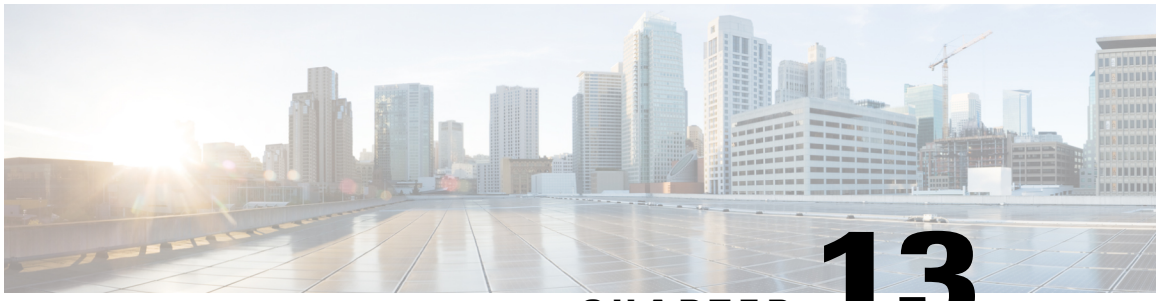
Step 4 (Optional) Select the **Enabled** radio button in the **FC Zoning Settings** panel to enable Fibre Channel zoning.
Fibre Channel zoning can be one of the following:

- disabled—The upstream switch configures and controls the Fibre Channel zoning, or Fibre Channel zoning is not implemented on this VSAN.
- enabled—Cisco UCS Manager will configure and control Fibre Channel zoning when the VSAN is deployed.

Note Fibre Channel zoning is disabled by default.

Step 5 Select the Fabric you want to assign this VSAN.
If you assign the VSAN to both fabrics, enter VSAN ID and FCoE vLAN ID for both fabrics. If not assign the IDs for selected VSAN.

Step 6 Click **Create**.



CHAPTER 13

Storage Profiles

This chapter includes the following sections:

Storage Profiles

With Cisco UCS M-Series modular servers, storage is centralized per chassis, and this centralized storage is shared by all servers in the chassis. Storage profiles allow you to do the following:

- Configure multiple virtual drives and select the physical drives that are used by a virtual drive.
- Configure the storage capacity of a virtual drive.
- Configure the number, type and role of disks in a disk group.
- Associate a storage profile with a service profile.

Creating or Editing a Storage Profile

Note Storage profiles in Cisco UCS Central release 1.3 are supported only with Cisco UCS M-Series Modular Servers.

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

Step 2 In **Basic**, click **Organization** and select the location in which you want to create the storage profile.

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

Step 4 In **Local Luns**, do the following:

a) Click **Add** to add a new local LUN.

b) In the **Basic** tab, enter the size in GB.
c) In the **Disk Group** tab, select the **Disk Group Configuration Policy**.

You can use the up and down arrows to change the order of the local LUNs.

Step 5 Click **Create**.

Disk Group Configuration Policy

Servers in a chassis can use storage that is centralized in that chassis. You can select and configure the disks to be used for storage. A logical collection of these physical disks is called a disk group. Disk groups allow you to organize local disks. The storage controller controls the creation and configuration of disk groups.

A disk group configuration policy defines how a disk group is created and configured. The policy specifies the RAID level to be used for the disk group. It also specifies either a manual or an automatic selection of disks for the disk group, and roles for disks.

Creating or Editing a Disk Group Configuration Policy

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

Step 2 In **Basic**, click **Organization** and select the location in which you want to create the disk group configuration policy.

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

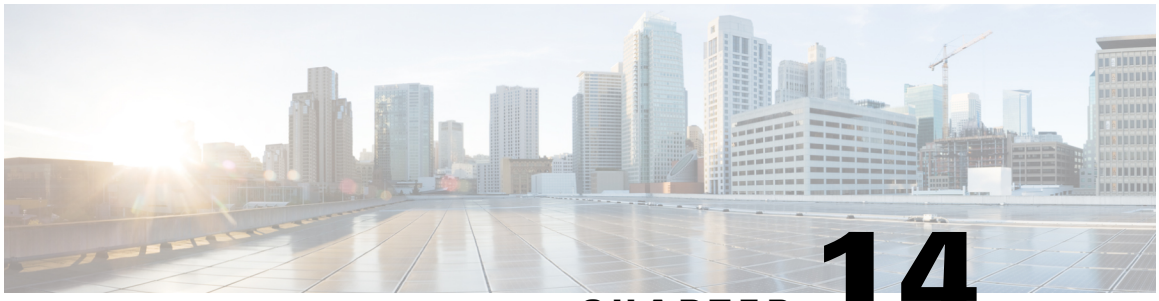
Step 4 Select the **Raid Level**.
This can be one of the following:

- **Platform Default**
- **Simple**
- **RAID**
- **RAID 0 Striped**
- **RAID 1 Mirrored**
- **RAID 5 Striped Parity**
- **RAID 6 Striped Dual Parity**
- **RAID 10 Mirrored & Striped**
- **RAID 50 Striped Parity & Striped**
- **RAID 60 Striped Dual Parity & Striped**

Step 5 In **Disk Group**, select the **Drive Type**, type values for the drive information, and choose whether to use the remaining disks.

Step 6 In **Virtual Drive** icon, complete the fields as necessary.

Step 7 Click **Create**.



CHAPTER 14

Backup and Restore

This chapter includes the following sections:

Backup and Restore

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

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

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

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

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

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

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

Important

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

Backup Image Files

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

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

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

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

Restoring Configuration

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

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

Considerations and Recommendations for Backup Operations

Before you create a backup operation, consider the following:

Backup Locations

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

Potential to Overwrite Backup Files

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

Multiple Types of Backups

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

Scheduled Backups

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

Incremental Backups

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

Encryption of Full State Backups

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

Scheduling a Full State Backup for Cisco UCS Central

Before You Begin

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

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

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

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

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

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

Note You must associate this full state backup with a pre-defined schedule. To create a schedule, see Creating or Editing a Schedule, on page 116.

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

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

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

Scheduling a Full State Backup for Cisco UCS Domain

You can create full state back for registered Cisco UCS Domains only at the domain group level.

Before You Begin

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

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

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

Step 2 From the **Schedule** drop down, choose a schedule for this backup. It can be one of the following:

- Simple – To create an one time occurrence or recurrence.
- Advanced – To create multiple one time occurrences or recurrences.

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

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

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

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

Creating On-Demand Full State Backup

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

Before You Begin

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

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

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

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

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

Step 4 For a Cisco UCS Central full state backup, choose whether to enable or disable **Remote Copy**.

If you select **Disabled**, a local backup copy will be made, and you can proceed to step 6.

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

Step 6 Click **Create**.

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

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

Removing Full State Backup for Cisco UCS Domain

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

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

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

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

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

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

Step 5 Click **Remove**.

Removing Full State Backup for Cisco UCS Central

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

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

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

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

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

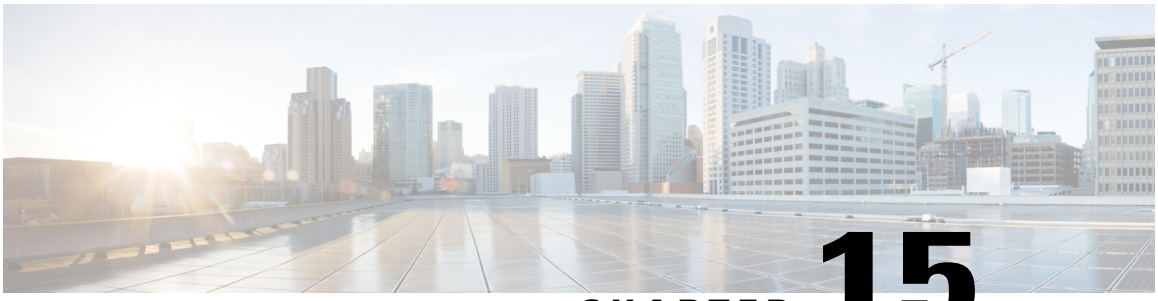
Step 4 Click **Remove**.

Viewing Backup files in Cisco UCS Central

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

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

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



CHAPTER 15

Configuration Export and Import

This chapter includes the following sections:

Configuration Export and Import

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

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

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

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

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

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

You can view the list of backups for each Cisco UCS domain from the Cisco UCS Central GUI (See: Viewing Backup files in Cisco UCS Central, on page 151), and you can also delete saved or unused backup directories and configurations.

Important

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

Backup Image Files

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

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

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

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

Importing Configuration

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

Scheduling Configuration Export for Cisco UCS Central

Before You Begin

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

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

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

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

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

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

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

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

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

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

Scheduling Configuration Export for Cisco UCS Domains

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

Before You Begin

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

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

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

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

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

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

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

Step 5 Click **Schedule**.

Exporting UCS Central Configuration Backup

Before You Begin

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

- Absolute remote path. For example if the transfer protocol is SCP: `scp://user@<ip>/x/y/z`

- Host name or IP address of the remote server
- Username and password for the remote server

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

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

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

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

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

Step 6 Click **Export**.

Exporting Configuration On-demand Backup for Domains

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

Before You Begin

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

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

Step 1 On the **Config Export & Import** page, select a domain.

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

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

Step 4 Choose a **Transfer Protocol**, and enter the required remote location information in the displayed fields.

Step 5 Click **Export**.

Importing Configuration for Cisco UCS Central

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

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

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

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

Step 4 In **Behavior on Configuration Import**, select one of the following options based on your requirements:

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

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

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

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

Importing Configuration for Cisco UCS Domain

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

Before You Begin

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

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

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

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

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

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

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

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

Step 7 Click **Import**.

Removing Configuration Export Schedule for Cisco UCS Central

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

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

Step 3 View the entries in the schedule.

Note There is only one schedule for Cisco UCS Central.

Step 4 Click **Remove**.

Removing Configuration Export Schedule for Cisco UCS Domain

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

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

Step 1 On the **Config Export & Import** page, click the **Schedule** icon.
Step 2 Select **Remove Domain Export Schedule** icon.
Step 3 Select the domain group where you want to remove the configuration backup.
Step 4 Select the schedule that you want to remove.
Step 5 Click **Remove**.

Viewing Backup files in Cisco UCS Central

Step 1 On the menu bar, choose **Backup & Restore**.
Step 2 Under **Domains**, select the Cisco UCS Central domain to enter the Cisco UCS Central scope.
Step 3 In the right side pane, view the list of all the Cisco UCS Central backup files. For each backup file, you can view the status, last backed up date, schedule, maximum number of files and the location for the remote copy.