Cisco UCS Central CLI Reference Manual, Release 1.1

First Published: October 31, 2013

Last Modified: May 06, 2015

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

Text Part Number: OL-30699-01

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.

Other Documentation Resources

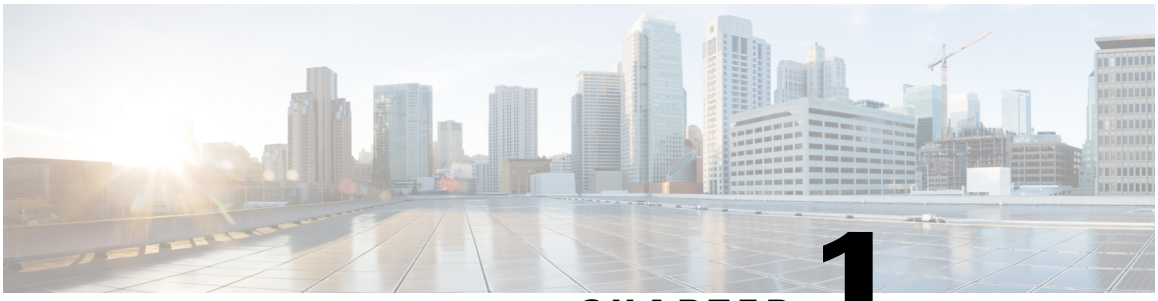
An ISO file containing all B and C-Series documents is available at the following URL: http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821. From this page, click **Unified Computing System (UCS) Documentation Roadmap Bundle**.

The ISO file is updated after every major documentation release.

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

Cisco UCS Central 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 management domains worldwide.

Cisco UCS Central enables you to manage individual or groups of 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
- Bandwidth statistics collection and aggregation with two week or one year retention

- 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.

Feature	Description
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.
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.
Statistics management	Cisco UCS Central enables you to gain a better understanding of how Cisco UCS domains are functioning over time to improve operations to smoothly handle periodic peaks and shifts in workload. You can configure and generate reports from the Cisco UCS Central GUI. To accelerate the collection of statistics, the centralized database schema is open and data can be accessed directly or through the Cisco UCS Central Software GUI, command-line interface (CLI), or XML API.
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.

Feature	Description
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.
Policy/policy component and resources import	Cisco UCS Central provides you the flexibility search for and import a perfect policy/policy component or a resource from one registered UCS domain into CCisco UCS Central. You can then deploy this policy or the resource to other managed domains.

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.

Policies

Cisco UCS Central acts as a global policy server for registered Cisco UCS domains. Configuring global Cisco UCS Central policies for remote Cisco UCS domains involves registering domains and assigning registered domains to domain groups.

In addition, the policy import capability allows a local policy to be globalized inside of Cisco UCS Central. You can then apply these global policies to other registered Cisco UCS domains.

You can define global policies in Cisco UCS Central that are resolved by Cisco UCS Manager in a registered Cisco UCS domain.

Pools

Pools are 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.

Multi-version Management Support

Cisco UCS Central, release 1.1(2a) provides you the ability to manage multiple Cisco UCS domains with different versions of Cisco UCS Manager at the same time. Cisco UCS Central identifies feature capabilities of each Cisco UCS domain at the time of domain registration. This ability enables you to seamlessly integrate multiple versions Cisco UCS Manager with Cisco UCS Central for management and global service profile deployment.

When you upgrade your Cisco UCS Central to a newer release, based on the features you are using, you might not have to upgrade all of your Cisco UCS Manager release versions to make sure the registered UCS domains are compatible with Cisco UCS Central.

When you register a Cisco UCS domain in Cisco UCS Central, along with the inventory information Cisco UCS Central receives the following information from the domain:

- Cisco UCS Manager release version
- List of available supported features in the domain

The available features are sent as a management capability matrix to Cisco UCS Central. Based on this information Cisco UCS Central builds a list of supported features for each registered domain. Based on the feature capabilities in a Cisco UCS domain, Cisco UCS Central decides if certain global management options are possible in the domain. When you perform management tasks, such as deploying a global service profile on a group of domains that include earlier versions of Cisco UCS Manager instances, based on the feature capability matrix, Cisco UCS Central does the following:

- Delivers the task only to the supported domains.
- Displays a version incompatibility message for the domains where the feature is not supported.

Supported Features in Cisco UCS Manager

You can view supported features in a Cisco UCS domain using the Cisco UCS Central CLI. Based on the Cisco UCS Manager versions in the registered Cisco UCS domains, Cisco UCS Central CLI builds list of supported features in the following four categories:

- **Server Feature Mask**: Includes global service profiles, policy mapping and Inband management, advanced boot order
- **Network Feature Mask**: None
- **Storage Feature Mask**: FC Zoning and ISCSI IPv6
- **Environment Feature Mask**: Power group, remote operations, UCS registration, estimate impact on reconnect

Management Exclusion

Multi-version support also provides you the ability to exclude some features from global management. You can log into a registered UCS domain and turn off a specific feature from Cisco UCS Manager CLI. You can disable the following global management capabilities:

- **Global service profile deployment**: If you deploy global service profile on a server pool, and you have disabled global service profile deployment in one of the servers in the pool, Cisco UCS Central excludes the server from the global service profile deployment.
- **In band management**: A service profile with inband management capability will not be deployed on the servers where you have excluded inband management feature.
- **Policy mapping**: This will disable importing policies or policy components from this Cisco UCS domain into Cisco UCS Central.
- **Remote management**: This will restrain controlling physical devices in a Cisco UCS domain from Cisco UCS Central.

You can enable these features any time using the Cisco UCS Manager CLI to restore global management capabilities in the registered Cisco UCS domains at anytime.

Feature Support Matrix

The following table provides a list of features in Cisco UCS Central, and Cisco UCS Manager release versions in which these features are supported:

Important Features such as specifying remote location for backup image files, 3rd party certificate, IPv6 inband management support are built in Cisco UCS Central to be compatible with upcoming Cisco UCS Manager releases.

Cisco UCS Central Features	Supported Cisco UCS Central Versions	Supported Cisco UCS Manager Versions			
		2.1(2a)/2.1(3x)	2.2(1x)	2.2(2x)	3.0(1x)
Multi-version management support and viewing supported Cisco UCS Manager features	1.1(2a)	No	Yes	Yes	Yes
Importing policy/policy component and resources		No	Yes	Yes	Yes
Specifying remote location for backup image files		No	No	Yes	No
3rd party certificate		No	No	Yes	No
IPv6 inband management support		No	No	Yes	No
Estimate Impact on Reconnect	1.2(1a)	No	No	Yes	Yes

Note Searching for policy/policy components or resources is supported in Cisco UCS Manager, releases 2.1(2x) and 2.1(3x). To import policies, you must have Cisco UCS Manager, releases 2.2(1b) or higher

Cisco UCS Central CLI Overview

Managed Objects

Cisco UCS uses a managed object model, where managed objects are abstract representations of physical or logical entities that can be managed. For example, servers, chassis, I/O cards, and processors are physical entities represented as managed objects, and resource pools, user roles, service profiles, and policies are logical entities represented as managed objects.

Managed objects may have one or more associated properties that can be configured.

Command Modes

The CLI is organized into a hierarchy of command modes, with the EXEC mode being the highest-level mode of the hierarchy. Higher-level modes branch into lower-level modes. You use **create**, **enter**, and **scope** commands to move from higher-level modes to modes in the next lower level , and you use the **exit** command to move up one level in the mode hierarchy.

Note Most command modes are associated with managed objects, so you must create an object before you can access the mode associated with that object. You use **create** and **enter** commands to create managed objects for the modes being accessed. The **scope** commands do not create managed objects and can only access modes for which managed objects already exist.

Each mode contains a set of commands that can be entered in that mode. Most of the commands available in each mode pertain to the associated managed object. Depending on your assigned role and locale, you may have access to only a subset of the commands available in a mode; commands to which you do not have access are hidden.

The CLI prompt for each mode shows the full path down the mode hierarchy to the current mode. This helps you to determine where you are in the command mode hierarchy, and it can be an invaluable tool when you need to navigate through the hierarchy.

Object Commands

Four general commands are available for object management:

- **create** *object*
- **delete** *object*
- **enter** *object*
- **scope** *object*

You can use the **scope** command with any managed object, whether a permanent object or a user-instantiated object. The other commands allow you to create and manage user-instantiated objects. For every **create** *object* command, a corresponding **delete** *object* and **enter** *object* command exists.

In the management of user-instantiated objects, the behavior of these commands depends on whether the object exists, as described in the following tables:

Table 1: Command behavior if the object does not exist

Command	Behavior
create *object*	The object is created and its configuration mode, if applicable, is entered.
delete *object*	An error message is generated.

Command	Behavior
enter *object*	The object is created and its configuration mode, if applicable, is entered.
scope *object*	An error message is generated.

Table 2: Command behavior if the object exists

Command	Behavior
create *object*	An error message is generated.
delete *object*	The object is deleted.
enter *object*	The configuration mode, if applicable, of the object is entered.
scope *object*	The configuration mode of the object is entered.

Complete a Command

You can use the Tab key in any mode to complete a command. Partially typing a command name and pressing Tab causes the command to be displayed in full or to the point where another keyword must be chosen or an argument value must be entered.

Command History

The CLI stores all commands used in the current session. You can step through the previously used commands by using the Up Arrow or Down Arrow keys. The Up Arrow key steps to the previous command in the history, and the Down Arrow key steps to the next command in the history. If you get to the end of the history, pressing the Down Arrow key does nothing.

All commands in the history can be entered again by simply stepping through the history to recall the desired command and pressing Enter. The command is entered as if you had manually typed it. You can also recall a command and change it before you press Enter.

Committing, Discarding, and Viewing Pending Commands

When you enter a configuration command in the CLI, the command is not applied until you enter the **commit-buffer** command. Until committed, a configuration command is pending and can be discarded by entering a **discard-buffer** command.

You can accumulate pending changes in multiple command modes and apply them together with a single **commit-buffer** command. You can view the pending commands by entering the **show configuration pending** command in any command mode.

Note Committing multiple commands together is not an atomic operation. If any command fails, the successful commands are applied despite the failure. Failed commands are reported in an error message.

While any commands are pending, an asterisk (*) appears before the command prompt. The asterisk disappears when you enter the **commit-buffer** command.

The following example shows how the prompts change during the command entry process:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create domain-group 12
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Online Help for the CLI

At any time, you can type the ? character to display the options available at the current state of the command syntax.

If you have not typed anything at the prompt, typing ? lists all available commands for the mode you are in. If you have partially typed a command, typing ? lists all available keywords and arguments available at your current position in the command syntax.

Logging into and out of the Cisco UCS Central GUI

Logging into the Cisco UCS Central CLI

Procedure

Step 1 In an SSH or telnet client, connect to the IP address assigned to Cisco UCS Central.

Step 2 At the `login as:` prompt, enter your Cisco UCS Central username and press Enter.

Step 3 At the `Password:` prompt, enter your password and press Enter.

Logging out of the Cisco UCS Central CLI

The Cisco UCS Central CLI clears the buffer of all uncommitted transactions when you exit.

Procedure

Step 1 At the prompt, type exit and press Enter.

Step 2 Continue to type exit and press Enter at each prompt until the window closes.

Viewing Supported Features in a Cisco UCS Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain ID*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show server-feature-mask**	Displays the server feature mask details.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show network-feature-mask**	Displays the network feature mask details.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show storage-feature-mask**	Displays the storage feature mask details.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show envr-feature-mask**	Displays the environment feature mask details.

The following example shows how to view server, network, storage and environment feature masks:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain ID
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show server-feature-mask

Server feature mask:
    Feature mask
    ------------
    Global Sp Feature Mask,Policy Map Feature Mask,In Band Mgmt Feature
Mask

UCSC(resource-mgr) /domain-mgmt/ucs-domain # show network-feature-mask

Network feature mask:
    Feature mask
    ------------
    None
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show storage-feature-mask

Storage feature mask:
    Feature mask
    ------------
    Fc Zoning Feature Mask,Iscsi Ipv6 Feature Mask

UCSC(resource-mgr) /domain-mgmt/ucs-domain # show envr-feature-mask

Environment feature mask:
    Feature mask
    ------------
   Power Group Feature Mask,Remote Operation Feature Mask,Ucs Registration
 Feat
```

```
ure Mask
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Viewing Supported Features for Global Service Profile Deployment

Before deploying a global service profile in a registered UCS domain, you can verify if the domain has the supported feature for this global service profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope org**	Enters the organization root.
Step 3	UCSC(resource-mgr)#/org **scope service profile***Global Service Profile Name*	Enters the service profile.
Step 4	UCSC(resource-mgr) /org/service profile # **show server-feature-mask**	Displays the server feature mask details.
Step 5	UCSC(resource-mgr) /org/service profile #**show network-feature-mask**	Displays the network feature mask details.
Step 6	UCSC(resource-mgr) /org/service profile #**show storage-feature-mask**	Displays the storage feature mask details.
Step 7	UCSC(resource-mgr) /org/service profile # **show envr-feature-mask**	Displays the environment feature mask details.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr)/org# scope service profile service profile name
Server feature mask:
    Feature mask
    ------------
    Global Sp Feature Mask,In Band Mgmt Feature Mask
UCSC(resource-mgr) /org/service-profile # show server-feature-maskненetwork-feature-mask

Network feature mask:
    Feature mask
    ------------
    None
UCSC(resource-mgr) /org/service-profile # show network-feature-mask

storage-feature-mask

Storage feature mask:
    Feature mask
    ------------
    None
UCSC(resource-mgr) /org/service-profile # show storage-feature-mask

envoir-feature-mask

Environment feature mask:
    Feature mask
    ------------
```

```
    Ucs Registration Feature Mask
UCSC(resource-mgr) /org/service-profile #
```

Configuring Identifier Policies

Identifier Policies

Cisco UCS Central supports an identifier policy for the **root** domain group. The identifier policy defines the soak interval, which is the number of seconds Cisco UCS Central waits before reassigning a pool entity that has been released by the Cisco UCS domain to which it was assigned.

Configuring the Identifier Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope identifier-policy**	Enters the identifier policy mode.
Step 4	UCSC(policy-mgr) /domain-group/identifier-policy # **set soak-interval** *soak-time*	Specifies the soak interval for the identifier policy. Specify an integer between 0 and 86400.
Step 5	UCSC(policy-mgr) /domain-group/identifier-policy # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure identifier policy and specify soak interval:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope identifier-policy
UCSC(policy-mgr) /domain-group/identifier-policy # set soak-interval 30
UCSC(policy-mgr) /domain-group/identifier-policy # commit-buffer
UCSC(policy-mgr) /domain-group #
```

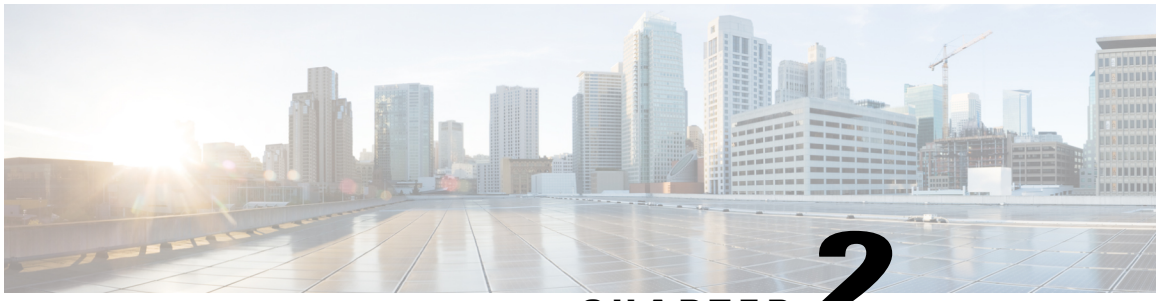
Viewing the Identifier Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope identifier-policy**	Enters the identifier policy mode.
Step 4	UCSC(policy-mgr) /domain-group/identifier-policy # **show**	Displays the identifier policy with soak interval.

The following example shows how to view the identifier policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope identifier-policy
UCSC(policy-mgr) /domain-group/identifier-policy # show
Identifier Policy:
    Soak interval in seconds
    ------------------------
    30
UCSC(policy-mgr) /domain-group #
```



CHAPTER 2

License Management

This chapter includes the following sections:

Managing Licenses in Cisco UCS Central

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.

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.

Note Domain licenses are specific to the installed domain. If you registered a specific domain using one license, you cannot unregister that particular domain and use the license for a different domain.

Downloading and Installing a License

Using the Cisco UCS Central CLI, you can download a license to Cisco UCS Central from a remote file system.

Note If you have the license file saved in your local file system, use Cisco UCS Central GUI to download the license file into Cisco UCS Central.

Before You Begin

To download a license from the local file system to Cisco UCS Central, 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 Central to perform this task.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect service-reg**	Enters service registry mode.
Step 2	UCSC (service-reg) # **scope license**	Enters the licensing configuration mode.
Step 3	UCSC (service-reg) /license # **download license** *protocol:// license file location*	Downloads the license using the specified protocol to connect to the location of the license. You can specify FTP, SFTP, TFTP or SCP as the protocol. For example, in the command **download license scp://user@1.2.3.4/a.lic**, SCP is the protocol specified, and 1.2.3.4 is replaced with the IP address of the server where the license file, a.lic file is saved. If you specify TFTP, then you are not prompted to enter the user name and the password.
Step 4	UCSC (service-reg) /license # **install file** *license file name*	Installs the license.

The following example shows how to download and install a license using the Cisco UCS Central CLI:

```
UCSC # connect service-reg
UCSC (service-reg) # scope license
UCSC (service-reg) /license # download license
scp://UCS-A@1.2.3.4/ws/ucsa-sjc/license_file/newFiles/DOMAIN_REG_2.lic
Password: *****
myPassword(service-reg) /license #
UCS-A(service-reg) /license # install  file DOMAIN_REG_2.lic
```

Deleting a License

You can delete a license that is not associated with a registered UCS domain, from Cisco UCS Central. If you want to delete a license that is associated to a UCS domain, make sure to unregister the domain before deleting the license. When you delete a license, the system automatically adjusts the available license count.

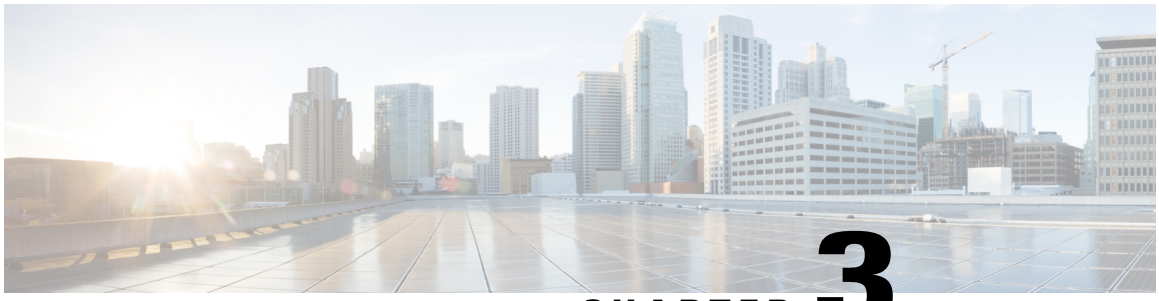
Important Deleting a license from Cisco UCS Central removes only the license file from the system. If you try to download the same license after deleting it from the system, you might encounter a download license error. So when you delete a license, you must delete the associated download task for that license.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect service-reg**	Enters service registry mode.
Step 2	UCSC (service-reg) # **scope license**	Enters licensing configuration mode.
Step 3	UCSC (service-reg) /license # **clear file** *license file name*	Deletes the specified license from the system.
Step 4	UCSC (service-reg) /license # **commit-buffer**	Commits the transaction to the system. **Note** Continue with the following steps to delete the download-task.
Step 5	UCSC (service-reg) /license # **delete download-task** *license file name*	Deletes the download task associated with the specified license file.
Step 6	UCSC (service-reg) /license # **commit-buffer**	Commits the transaction to the system.

The following example shows the process to clear a license file and delete the download task from Cisco UCS Central CLI:

```
UCSC # connect service-reg
UCSC (service-reg) # scope license
UCSC (service-reg) /license # clear file UCSC_123_ini.lic
UCSC (service-reg) /license* # commit-buffer
UCSC (service-reg) /license # delete download-task UCSC_123_ini.lic
UCSC (service-reg) /license* # commit-buffer
```



CHAPTER 3

Managing Administrative Settings

This chapter includes the following sections:

Administrative Settings for Cisco UCS Central

Policies and Authentication

Cisco UCS Central, in this release, supports configuring policies and user authentication natively from the **Administration** tab in the GUI, similar to the tasks defined for UCS domains from the **Operations Management** tab. Most of the features are common across the two tabs, the difference being in the user role and server support.

The **Administration** tab allows you to perform administration tasks in the following areas:

- General Settings
- Users and Authentication

General Settings

You can configure policies from the Cisco UCS Central GUI. These administrative policies are defined at the organization level and can manage anything in the infrastructure, from date and time, SNMP traps, to backup and export policies.

IPv6 Support

Cisco UCS Central supports IPv6 addressing, which is now enabled on the management interface visible to the UCS Manager. However, UCS Central operates on a dual mode where both IPv4 and IPv6 are enabled. This feature helps Cisco UCS Central and Cisco UCS Manager communicate with each other through an IPv6 address, primarily to share pools and policy related information only.

As part of the IPv6 integration, the Cisco UCS Central GUI displays IPv6 addresses of all registered UCS Managers in the Equipments tab. The GUI also displays IPv6 addresses in all the other areas where the device has an IPv6 address.

Cisco UCS Central supports the creation and deletion of IPv4 and IPv6 blocks in the IP pools, and supports IPv6 addressing for the following policies:

- LDAP
- TACAS
- Radius
- NTP
- DNS

You can now register a Cisco UCS Manager using an IPv6 address or an IPv4 address.

You can configure an IPv6 address on the Cisco UCS Central through the GUI or CLI commands. This is also true for all the other areas where IPv6 addresses are used.

You can now create a Global Service Profile (GSP) and a Local Service Profile (LSP) using an Outband management IPv4 address and an Inband IPv4 and/or IPv6 address.

Configuring IPv6 in Standalone Mode

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters System mode.
Step 2	UCSC/System#**network-interface a**	Enters network interface of Node A.
Step 3	UCSC/network-interface#**scope ipv6-config**	Scopes to IPv6 configuration.
Step 4	UCSC/network-interface/ipv6-config#**set net ipv6** *ipv6 address* **ipv6-gw** *IPv6 gateway* **ipv6-prefix** *prefix*	Specifies the IPv6 address, gateway, and prefix.
Step 5	UCSC/network-interface/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to configure IPv6 in standalone mode:

```
UCSC#scope system
UCSC/system#scope network-interface a
UCSC/network-interface# scope ipv6-config
UCSC/ipv6-config# set net ipv6 ipv6 2001:db8:a::11 ipv6-gw  2001:db8:a::1 ipv6-prefix  64
UCSC/ipv6-config# commit-buffer
```

Configuring IPv6 in High Availability Mode

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters System mode.
Step 2	UCSC/System#**scope network-interface a**	Enters Node A of the network interface, which is also the primary virtual machine.
Step 3	UCSC/network-interface#**scope ipv6-config**	Scopes to IPv6 configuration.
Step 4	UCSC/ipv6-config#**set net ipv6** *ipv6 address* **ipv6-gw** *ipv6 gateway***ipv6-prefix** *prefix*	Specifies the IPv6 address, gateway, and prefix.
Step 5	UCSC/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.
Step 6	UCSC/ipv6-config#**top**	Returns to the top most directory.
Step 7	UCSC# **scope system**	Enters System mode.
Step 8	UCSC/System#**scope network-interface b**	Enters Node B of the network interface, which is also the subordinate virtual machine.
Step 9	UCSC/network-interface#**scope ipv6-config**	Scopes to IPv6 configuration.
Step 10	UCSC/ipv6-config#**set net ipv6***ipv6 address* **ipv6-gw***ipv6 gateway***ipv6-prefix***prefix*	Specifies the IPv6 address, gateway, and prefix.
Step 11	UCSC/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.
Step 12	UCSC/ipv6-config#**top**	Returns to the top most directory.
Step 13	UCSC# **scope system**	Enters System mode.
Step 14	UCSC/network-interface#**set virtual ip ipv6***ipv6 address*	Configures a virtual IPv6 address.
Step 15	UCSC/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.
Step 16	UCSC/ipv6-config#**top**	Returns to the top most directory.

The following example shows how to configure IPv6 in the high availability mode:

```
UCSC#scope system
UCSC/system#scope network-interface a
UCSC/network-interface# scope ipv6-config
UCSC/ipv6-config# set net ipv6 2001:db8:a::11 ipv6-gw  2001:db8:a::1 ipv6-prefix  64
UCSC/ipv6-config# commit-buffer
UCSC/ipv6-config# top

UCSC#scope system
UCSC/system#scope network-interface b
UCSC/network-interface# scope ipv6-config
UCSC/ipv6-config# set net ipv6 2001:db8:a::12 ipv6-gw  2001:db8:a::1 ipv6-prefix  64
```

```
UCSC/ipv6-config# commit-buffer
UCSC/ipv6-config# top

UCSC#scope system
UCSC/network-interface# set virtual ip ipv6 2001:db8:a::10
UCSC/ipv6-config# commit-buffer
UCSC/ipv6-config# top
```

Disabling IPv6

You can disable IPv6 on the Cisco UCS Central by setting the IPv6 address (in both the standalone and HA mode) to null.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**scope system**	Enters system mode.
Step 2	UCSC#**scope network-interface a**	Enters Node A of the network interface.
Step 3	UCSC/network-interface#**scope ipv6-config**	Scopes to IPv6 configuration.
Step 4	UCSC/ipv6-config#**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 5	UCSC/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.
Step 6	UCSC/ipv6-config#**top**	Returns to the top most directory.
Step 7	UCSC#**scope system**	Enters system mode.
Step 8	UCSC/system#**set virtual-ip ipv6 ::**	Sets the IPv6 address to null, therefore disabling it.
Step 9	UCSC/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.
Step 10	UCSC/ipv6-config#**top**	Returns to the top most directory.
Step 11	UCSC#**scope system**	Enters system mode.
Step 12	UCSC#**scope network-interface a**	Enters Node A of the network interface.
Step 13	UCSC/network-interface#**scope ipv6-config**	Scopes to IPv6 configuration.
Step 14	UCSC/ipv6-config#**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 15	UCSC/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.
Step 16	UCSC/ipv6-config#**top**	Returns to the top most directory.
Step 17	UCSC#**scope system**	Enters system mode.
Step 18	UCSC#**scope network-interface b**	Enters Node B of the network interface.
Step 19	UCSC/network-interface#**scope ipv6-config**	Scopes to IPv6 configuration.

	Command or Action	Purpose
Step 20	UCSC/ipv6-config#**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 21	UCSC/ipv6-config#**commit-buffer**	Commits the transaction to the system configuration.
Step 22	UCSC/ipv6-config#**top**	Returns to the top most directory.

Setting the IPv6 value to null moves all the affected IPv6 devices to a state of lost visibility.
The following example shows how to disable IPv6 on Cisco UCS Central for the standalone and HA modes:

```
UCSC#scope system
UCSC/system#  scope network-interface a
UCSC/network-interface# scope ipv6-config
UCSC/ipv6-config# set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64
UCSC/ipv6-config# commit-buffer
UCSC/ipv6-config# top


UCSC/# scope system
UCSC/system# set virtual-ip ipv6 ::
UCSC/ipv6-config# commit-buffer
UCSC/ipv6-config# top
UCSC#scope system
UCSC/system#  scope network-interface a
UCSC/network-interface# scope ipv6-config
UCSC/ipv6-config# set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64
UCSC/ipv6-config# commit-buffer
UCSC/ipv6-config# top


UCSC#scope system
UCSC/system#  scope network-interface b
UCSC/network-interface# scope ipv6-config
UCSC/ipv6-config# set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64
UCSC/ipv6-config# commit-buffer
UCSC/ipv6-config# top
```

Configuring an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-name*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope snmp**	Scopes the default SNMP policy's configuration mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/device-profile/snmp # **create snmp-trap** *snmp-trap-ip*	(Optional) If scoping into an organization previously, creates the SNMP trap IP address for that organization (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 6	UCSC(policy-mgr) /org/device-profile/snmp # **scope snmp-trap** *snmp-trap-ip*	(Optional) If scoping into organization previously, scopes the SNMP trap IP address for that organization (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set community** *snmp-trap-community-host-config-string*	Enter the SNMP trap community string to configure the SNMP trap host.
Step 8	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set notificationtype traps**	Enter the notification type for the SNMP trap as SNMP Trap Notifications (traps).
Step 9	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set port** *port-number*	Enter the SNMP trap port number (1-65535).
Step 10	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set v3privilege auth** | **noauth** | **priv**	Enter a V3 Privilege security level for the SNMP trap of authNoPriv Security Level (auth), noAuthNoPriv Security Level (noauth), or authPriv Security Level (priv).
Step 11	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **set version v1** | **v2c** | **v3**	Enter a version for the SNMP trap of SNMP v1, v2c, or v3.
Step 12	UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into an organization, scope the SNMP policy, create the SNMP trap with IP address 0.0.0.0, set the SNMP community host string to snmptrap01, set the SNMP notification type to traps, set the SNMP port to 1, set the v3privilege to priv, set the version to v1, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org# scope device-profile /
UCSC(policy-mgr) /org/device-profile # scope snmp
UCSC(policy-mgr) /org/device-profile/snmp # create snmp-trap 0.0.0.0
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set community snmptrap01
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set port 1
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set v3privilege priv
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # set version v1
UCSC(policy-mgr) /org/device-profile/snmp/snmp-trap* # commit-buffer
```

Configuring an SNMP User

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-name*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/snmp # **create snmp-user** *snmp-user*	Enter a name for the SNMP user.
Step 6	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set aes-128 yes** | **no**	Use AES-128 for the SNMP user (yes or no).
Step 7	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set auth md5** | **sha**	Use MD5 or Sha authorization mode for the SNMP user.
Step 8	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set password** *password*	Enter and confirm a password for the SNMP user.
Step 9	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set priv-password** *private-password*	Enter and confirm a private password for the SNMP user.
Step 10	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into an organization, scope the SNMP policy, scope into the SNMP user named snmpuser01, set aes-128 mode to enabled, set authorization to sha mode, set password to userpassword01, set private password to userpassword02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org# scope device-profile /
UCSC(policy-mgr) /org/device-profile # scope snmp
UCSC(policy-mgr) /org/device-profile/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user # set aes-128 yes
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # set auth sha
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
```

```
Confirm the password: userpassword02
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # commit-buffer
```

Configuring an NTP Server

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-name*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/timezone-ntp-config # **create ntp** server-name	Creates an NTP server instance.
Step 6	UCSC(policy-mgr) /org/device-profile/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into an organization, create an NTP server instance named orgNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org# scope device-profile /
UCSC(policy-mgr) /org/device-profile # scope timezone-ntp-config
UCSC(policy-mgr) /org/device-profile/timezone-ntp-config # create ntp orgNTP01
UCSC(policy-mgr) /org/device-profile/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /org/device-profile/timezone-ntp-config #
```

Configuring a DNS Server

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile # **scope dns-config**	Enter an existing DNS policy's configuration mode from the organization.
Step 5	UCSC(policy-mgr) /org/device-profile/dns-config # **create dns** server-IP-address	Creates a DNS server instance.
Step 6	UCSC(policy-mgr) /org/device-profile/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the organization, create a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr)/org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope dns-config
UCSC(policy-mgr) /org/device-profile # create dns 0.0.0.0
UCSC(policy-mgr) /org/device-profile* # commit-buffer
```

Configuring a Fault Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-name*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **create fault policy**	(Optional) If scoping into a device previously, creates the fault policy for that domain group.
Step 5	UCSC(policy-mgr) /org # **scope fault policy**	(Optional) If scoping into the domain group root previously, scopes the default fault policy's configuration mode from the Domain Group root.
Step 6	UCSC(policy-mgr) /org/device-profile/policy* # **set ackaction delete-on-clear**	Set the fault policy acknowledgment action to delete on clear (delete-on-clear) or reset to initial severity (reset-to-initial-severity).
Step 7	UCSC(policy-mgr) /org/device-profile/policy* # **set clearaction delete** | **retain**	Set the fault policy clear action to delete or retain.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /org/device-profile/policy* # **set clearinterval** *clear-number-of-days* | **retain**	Set the fault policy clear interval to the number of days (0-3600) or retain.
Step 9	UCSC(policy-mgr) /org/device-profile/policy* # **set flapinterval** *flap-number-of-days*	Set the fault policy flap interval to the number of days (0-3600).
Step 10	UCSC(policy-mgr) /org/device-profile/policy* # **set retentioninterval** *retention-number-of-days* | **forever**	Set the fault policy clear interval to the number of days (0-3600) or forever.
Step 11	UCSC(policy-mgr) /org/device-profile/policy* # **set soakingseverity condition** | **info** | **warning**	Set the fault policy soaking severity to condition, info, or warning.
Step 12	UCSC(policy-mgr) /org/device-profile/policy* # **set soakinterval** *soak-number-of-days* | **never**	Set the fault policy soak interval to the number of days (0-3600) or never.
Step 13	UCSC(policy-mgr) /org/device-profile/policy* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the org01, create a global fault debug policy, enter the status settings, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org01
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # create fault policy
UCSC(policy-mgr) /org/device-profile/policy* # set ackaction delete-on-clear
UCSC(policy-mgr) /org/device-profile/policy* # set clearaction delete
UCSC(policy-mgr) /org/device-profile/policy* # set clearinterval 90
UCSC(policy-mgr) /org/device-profile/policy* # set flapinterval 180
UCSC(policy-mgr) /org/device-profile/policy* # set retentioninterval 365
UCSC(policy-mgr) /org/device-profile/policy* # set soakingseverity info
UCSC(policy-mgr) /org/device-profile/policy* # set soakinterval warning
UCSC(policy-mgr) /org/device-profile/policy* # commit-buffer
UCSC(policy-mgr) /org/device-profile/policy #
```

Configuring a TFTP Core Export Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-name*	Enters device profile mode for the specified organization.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile # **scope tftp-core-export-config**	(Optional) Scopes an existing TFTP Core Export Debug policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile # **create tftp-core-export-config**	(Optional) Creates a TFTP Core Export Debug policy if it does not exist, then scopes into the policy.
Step 6	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **enable core-export-target**	Enables the TFTP core export target.
Step 7	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target path** *name-of-path*	Sets the TFTP core export policy target path.
Step 8	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target port** *port-number*	Sets the TFTP core export policy port number (1-65535).
Step 9	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target server-description** *port-number*	Sets the TFTP core export target policy server description. **Note** Do not use spaces in the server description unless the text is quoted (format examples: "Server description text" or Server_description_text).
Step 10	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **set core-export-target server-name** *server-name*	Sets the TFTP core export target policy server name.
Step 11	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into org01, create the TFTP Core Export Policy, configure the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org01
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # create tftp-core-export-config
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # enable core-export-target
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target path
 /target
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target port
 65535
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target
server-description "TFTP core export server 2"
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # set core-export-target
server-name TFTPcoreserver01
UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # commit-buffer
```

Creating a Locally Authenticated User

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create local-user** *local-user-name*	Creates a user account for the specified local user and enters security local user mode.
Step 6	UCSC(policy-mgr) org/device-profile/security/local-user* # **set account-status** {**active** | **inactive**}	Specifies whether the local user account is enabled or disabled. The admin user account is always set to active. It cannot be modified. **Note** If you set the account status to inactive, the configuration is not deleted from the database. The user is prevented from logging into the system using their existing credentials.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set password** *password*	Sets the password for the user account
Step 8	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set firstname** *first-name*	(Optional) Specifies the first name of the user.
Step 9	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set lastname** *last-name*	(Optional) Specifies the last name of the user.
Step 10	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set expiration** *month day-of-month year*	(Optional) Specifies the date that the user account expires. The *month* argument is the first three letters of the month name.
Step 11	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set email** *email-addr*	(Optional) Specifies the user e-mail address.

	Command or Action	Purpose
Step 12	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set phone** *phone-num*	(Optional) Specifies the user phone number.
Step 13	UCSC(policy-mgr) /org/device-profile/security/local-user* # **set sshkey** *ssh-key*	(Optional) Specifies the SSH key used for passwordless access.
Step 14	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

The following example shows how to create the user account named eagle_eye, enable the user account, set the password to eye5687, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org# scope device-profile /
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create local-user eagle_eye
UCSC(policy-mgr) /org/device-profile/security/local-user* # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user* # set password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user* #
```

The following example creates the user account named lincey, enables the user account, sets an OpenSSH key for passwordless access, and commits the transaction.

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org# scope device-profile /
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create local-user lincey
UCSC(policy-mgr) /org/device-profile/security/local-user* # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user* # set sshkey "ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4K
iaQB8X/PDdmtlxQQcawcljk8f4VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpD
 m8HPh2LOgyH7Ei1MI8="
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user* #
```

The following example creates the user account named jforlenz, enables the user account, sets a Secure SSH key for passwordless access, and commits the transaction.

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org# scope device-profile /
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create local-user jforlenz
UCSC(policy-mgr) /org/device-profile/security/local-user* # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user* # set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
>AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
>5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
>IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
> ENDOFBUF
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user* #
```

Creating a Remote User

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope auth-realm**	Enters authentication realm security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/auth-realm # **set remote-user default-role** {**assign-default-role** | **no-login**}	Specifies whether user access to Cisco UCS Central is restricted based on user roles.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the role policy for remote users and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # set remote-user default-role
assign-default-role
UCSC(policy-mgr) /org/device-profile/security/auth-realm* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm #
```

Creating a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create role** *name*	Creates the user role and enters security role mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **add privilege** *privilege-name*	Adds one or more privileges to the role. **Note** You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role, or you can add privileges to the same role using multiple **add** commands.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the service-profile-security-admin role, adds the service profile security and service profile security policy privileges to the role, and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create role ls-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # add privilege service-profile-security

service-profile-security-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
```

Creating a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create locale** *name*	Creates the user role and enters security role mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale * # **create org-ref** *org-ref-name* **orgdn** *orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference, and the *orgdn-name* argument is the distinguished name of the organization being referenced.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create the finance organization for the western locale and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create locale western
UCSC(policy-mgr) /org/device-profile/security/locale* # create org-ref finance-ref orgdn
finance
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
```

Users and Authentication

Cisco UCS Central supports creating local and remote users to access the system. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each of these users must have a unique username and password. For more information, see User Management, on page 451.

Cisco UCS Central uses LDAP for native authentication, but excludes RADIUS and TACACS+ authentication in this release. However, RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains. For more information, see Managing Administrative Settings, on page 19.

Creating an Authentication Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-name*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope auth-realm**	Enters authentication realm mode.
Step 6	UCSC(policy-mgr) / org/device-profile/security/auth-realm # **create auth-domain** *domain-name*	Creates an authentication domain and enters authentication domain mode. The Radius related settings will be applicable only for the Cisco UCS Central under the Domain Group root and child domain groups.
Step 7	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **set refresh-period** *seconds*	(Optional) When a web client connects to Cisco UCS Central, the client needs to send refresh requests to Cisco UCS Central to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Central 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.
Step 8	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **set session-timeout** *seconds*	(Optional) The maximum amount of time that can elapse after the last refresh request before 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 an integer between 60 and 172800. The default is 7200 seconds.

	Command or Action	Purpose
Step 9	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **create default-auth**	(Optional) Creates a default authentication for the specified authentication domain.
Step 10	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set auth-server-group** *auth-serv-group-name*	(Optional) Specifies the provider group for the specified authentication domain.
Step 11	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set realm** {**ldap** | **local** | **radius** | **tacacs**}	Specifies the realm for the specified authentication domain.
Step 12	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an authentication domain called domain1 with a web refresh period of 3600 seconds (1 hour) and a session timeout period of 14400 seconds (4 hours), configure domain1 to use the providers in ldapgroup1, set the realm type to ldap, and commit the transaction.

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope security
UCSC(policy-mgr) /org/security # scope device-profile
UCSC(policy-mgr) /org/security/device-profile # scope auth-realm
UCSC(policy-mgr) /org/security/device-profile/auth-realm # create auth-domain domain1
UCSC(policy-mgr) /org/security/device-profile/auth-realm/auth-domain* # set refresh-period
 3600
UCSC(policy-mgr) /org/security/device-profile/auth-realm/auth-domain* # set session-timeout
 14400
UCSC(policy-mgr) /org/security/device-profile/auth-realm/auth-domain* # create default-auth
UCSC(policy-mgr) /org/security/device-profile/auth-realm/auth-domain/default-auth* # set
auth-server-group ldapgroup1
UCSC(policy-mgr) /org/security/device-profile/auth-realm/auth-domain/default-auth* # set
realm ldap
UCSC(policy-mgr) /org/security/device-profile/auth-realm/auth-domain/default-auth* #
commit-buffer
UCSC(policy-mgr) /org/security/device-profile/auth-realm/auth-domain/default-auth #
```

Creating an LDAP Provider

Before You Begin

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters security LDAP mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create server** *server-name*	Creates an LDAP server instance and enters security LDAP server mode. If SSL is enabled, the server-name , typically an IP address or FQDN, must exactly match a Common Name (CN) in the LDAP server's security certificate. If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set attribute** *attribute*	(Optional) (Optional) An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set basedn** *basedn-name*	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The length of the base DN can be set to a maximum of 255 characters minus the length of CN=username, where username identifies the remote user attempting to access Cisco UCS Manager using LDAP authentication.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set binddn** *binddn-name*	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.
Step 10	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set filter** *filter-value*	The LDAP search is restricted to those user names that match the defined filter.

	Command or Action	Purpose
Step 11	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set password**	To set the password, press **Enter** after typing the **set password** command and enter the key value at the prompt.
Step 12	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set order** *order-num*	The order in which Cisco UCS Central uses this provider to authenticate users.
Step 13	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set port** *port-num*	The port through which Cisco UCS Central communicates with the LDAP database. The standard port number is 389.
Step 14	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set ssl** {**yes** | **no**}	Enables or disables the use of encryption when communicating with the LDAP server. The options are as follows: • **yes —**Encryption is required. If encryption cannot be negotiated, the connection fails. • **no —**Encryption is disabled. Authentication information is sent as clear text.
Step 15	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set timeout** *timeout-num*	
Step 16	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set vendor**	Specifies the vendor for the LDAP group. • **ms-ad —**To specify Microsoft Active Directory, enter ms-ad. • **openldap —**To specify OpenLDAP server, enter openldap.
Step 17	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an LDAP server instance named 10.193.169.246, configure the binddn, password, order, port, and SSL settings, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create server 10.193.169.246
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set password
Enter the password:
Confirm the password:
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set order 2
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set port 389
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set ssl yes
```

```
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # set timeout 30
UCSC(policy-mgr) /org/device-profile/security/ldap/server* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/server #
```

Creating an LDAP Provider Group

Before You Begin

Create one or more LDAP providers.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters security LDAP mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create auth-server-group** *auth-server-group-name*	Creates an LDAP provider group and enters authentication server group security LDAP mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified LDAP provider to the LDAP provider group and enters server reference authentication server group security LDAP mode.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS Central uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is equivalent to giving that server reference the highest priority.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an LDAP provider group called ldapgroup, add two previously configured providers called ldap1 and ldap2 to the provider group, set the order, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create auth-server-group ldapgroup
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # create server-ref
ldap1
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # set order
 1
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # up
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group* # create server-ref
ldap2
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* # set order
 2
UCSC(policy-mgr) /org/device-profile/security/ldap/auth-server-group/server-ref* #
commit-buffer
```

What to Do Next

Configure an authentication domain.

Creating an LDAP Group Map

Before You Begin

- Create an LDAP provider group.
- Configure the distinguished name for the LDAP group in the LDAP server.
- Create user locales in Cisco UCS Central (optional).
- Create user roles in Cisco UCS Central (optional).

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters security LDAP mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create ldap-group** *group-dn*	Creates an LDAP group map for the specified DN.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **create locale** *locale-name*	Maps the LDAP group to the specified locale.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **create role** *role-name*	Maps the LDAP group to the specified role.
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to map the LDAP group mapped to a DN, set the locale to pacific, set the role to admin, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # create ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # create locale pacific
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # create role admin
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group #
```

What to Do Next

Set the LDAP group rule.

Deleting an LDAP Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters security LDAP mode.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete server** *serv-name*	Deletes the specified server.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete the LDAP server called ldap1 and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete server ldap1
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap #
```

Deleting an LDAP Provider Group

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters security LDAP mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete auth-server-group** *auth-server-group-name*	Deletes the LDAP provider group.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an LDAP provider group called ldapgroup and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
```

```
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete auth-server-group ldapgroup
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/ldap #
```

Deleting an LDAP Group Map

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope ldap**	Enters security LDAP mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete ldap-group** *group-dn*	Deletes the LDAP group map for the specified DN.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an LDAP group map and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # delete ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
```

Configuring an HTTPS Certificate

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope https**	Enters the HTTPS service mode.
Step 5	UCSC(policy-mgr) /org/device-profile/https # **set keyring** *keyring-name*	Creates and names the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/https* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to configure an HTTPS Certificate:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope https
UCSC(policy-mgr) /org/device-profile/https # set keyring kr126
UCSC(policy-mgr) /org/device-profile/https* # commit-buffer
```

Creating a Trusted Point

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security #**create trustpoint***trust point name*	Creates a trusted point. Provide a certificate name.
Step 6	UCSC(policy-mgr) /org/device-profile/security/trustpoint* #**set certchain***[certificate chain]*	Specifies certificate information for this trusted point. If you do not specify certificate information in the command, you are prompted to enter a certificate or a list of trustpoints defining a certification path to the

	Command or Action	Purpose
		root certificate authority (CA). On the next line following your input, type ENDOFBUF to finish.

The following example shows how to create a trusted point:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create trustpoint key01
UCSC(policy-mgr) /org/device-profile/security/trustpoint* # set certchain
>-----BEGIN CERTIFICATE-----
>MIIDgzCCAmugAwIBAgIQeXUhz+ZtnrpK4x65oJkQZzANBgkqhkiG9w0BAQUFADBU
>MSIwIAYDVQQDExlibHJxYXVjc2MtV0lOMjAxMi1JUFY2LUNBMB4XDTE0MDIyNjEy
>-----END CERTIFICATE-----
>ENDOFBUF
UCSC(policy-mgr) /org/device-profile/security/trustpoint* # commit-buffer
```

Deleting a Trusted Point

Before You Begin

Ensure that a key ring is not using the trusted point.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security #**delete trustpoint***trustpoint- name*	Deletes the trusted point.
Step 6	UCSC(policy-mgr) /org/device-profile/security#**commit-buffer**	Commits the transaction.

The following example shows how to delete a trusted point:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # delete trustpoint tp1
UCSC(policy-mgr) /org/device-profile/security* #commit-buffer
```

Creating a Key Ring

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **create keyring** *keyring-name*	Creates and names the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/keyring # **set modulus mod2048**	Sets the SSL key length in bits.
Step 7	UCSC(policy-mgr) /org/device-profile/security/keyring* # **set trustpoint** *trustpoint-name*	Sets a trust point within the key ring.
Step 8	UCSC(policy-mgr) /org/device-profile/security/keyring* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a key ring with a key size of 2048 bits:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create keyring kr126
UCSC(policy-mgr) /org/device-profile/security/keyring* # set modulus mod2048
UCSC(policy-mgr) /org/device-profile/security/keyring* # set trustpoint tp1
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

Deleting a Key Ring

Before You Begin

Ensure that the HTTPS service is not using the key ring.

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security #**delete keyring***keyring name*	Deletes the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security#**commit-buffer**	Commits the transaction.

The following example shows how to delete a key ring:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # delete keyring kr126
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

Creating a Certificate Request

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope keyring** *keyring-name*	Enters the configuration mode for the key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/keyring* # **create certreq**	Sets the SSL key length in bits.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set country** *country name*	Specifies the country code of the company.
Step 8	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set dns** *DNS name*	Specifies the Domain Name Server (DNS) address associated with the certificate request.
Step 9	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set e-mail** *E-mail address*	Specifies the e-mail address associated with the certificate request.
Step 10	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set ip** { *certificate request ipv4-address*}	Specifies the IP address of the fabric interconnect.
Step 11	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set locality** *locality name*	Specifies the city or town in which the company requesting the certificate is headquartered.
Step 12	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set org-name** *organization name*	Specifies the organization requesting the certificate.
Step 13	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set org-unit-name** *organizational unit name*	Specifies the organizational unit.
Step 14	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set password** *certificate request password*	Specifies an optional password for the certificate request.
Step 15	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set state** *state, province or country*	Specifies the state or province in which the company requesting the certificate is headquartered.
Step 16	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **set subject-name** *certificate request name*	Specifies the fully qualified domain name of the Fabric Interconnect.
Step 17	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **commit-buffer**	Commits the transaction.

The following example shows how to create a certificate request with an IPv4 address for a key ring, with advanced options:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope keyring
UCSC(policy-mgr) /org/device-profile/security # create certreq
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set ip 192.168.200.123
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set country US
```

```
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set dns bgl-samc-15A
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set email test@gmail.com
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set locality san francisco
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set org-name "xyz"
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set org-unit-name Testing
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set state california
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set subject-name abc01
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* #commit-buffer
```

What to Do Next

- Copy the text of the certificate request, including the BEGIN and END lines, and save it in a file. Send the file with the certificate request to a trust anchor or certificate authority to obtain a certificate for the key ring.
- Create a trusted point and set the certificate chain for the certificate of trust received from the trust anchor.

Regenerating the Default Key Ring

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

Procedure

	Command or Action	Purpose
Step 1	UCSC#**connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org***org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*
Step 3	UCSC(policy-mgr) /org#**scope device-profile***device-id*	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile#**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope keyring default**	Enters key ring security mode for the default key ring.
Step 6	UCSC(policy-mgr) /org/device-profile/security/keyring # **set regenerate yes**	Regenerates the default key ring.
Step 7	UCSC(policy-mgr) /org/device-profile/security/keyring* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to regenerate a default key ring:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # scope keyring default
```

```
UCSC(policy-mgr) /org/device-profile/security/keyring* # set generate yes
UCSC(policy-mgr) /org/device-profile/security/keyring* #commit-buffer
```

Administrative Settings for Cisco UCS Manager

Remote Access Policies

Cisco UCS Central supports global remote access policies defining the interfaces monitoring policy, displaying SSH configuration status, and providing policy settings for HTTP, Telnet, web session limits and CIM XML.

Configuring HTTP

Configuring an HTTP Remote Access Policy

Before You Begin

Before configuring an HTTP remote access policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create http**	(Optional) If scoping into a domain group previously, creates the HTTP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope http**	(Optional) If scoping into the domain group root previously, scopes the default HTTP policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/http # **enable** | **disable** {**http** | **http-redirect**}	Specifies whether the HTTP remote access policy is enabled or disabled in HTTP or HTTP-Redirect mode.
Step 6	UCSC(policy-mgr) /domain-group/http* # **set http port** *port-number*	Specifies the HTTP service port number from the port range 1-65535.
Step 7	UCSC(policy-mgr) /domain-group/http* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root (which has an existing HTTP policy by default), enable the HTTP remote access policy to HTTP redirect mode, set the HTTP service port to 1111, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope http
UCSC(policy-mgr) /domain-group/http # enable http-redirect
UCSC(policy-mgr) /domain-group/http* # set port 1111
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

The following example shows how to scope into the domain group domaingroup01, create the HTTP remote access policy and enable it to HTTP mode, set the HTTP service port to 222, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create http
UCSC(policy-mgr) /domain-group/http* # enable http
UCSC(policy-mgr) /domain-group/http* # set port 222
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

The following example shows how to scope into the domain group root (which has an existing HTTP policy by default), disable the HTTP remote access policy for HTTP redirect mode, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope http
UCSC(policy-mgr) /domain-group/http # disable http-redirect
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

The following example shows how to scope into the domain group domaingroup01, disable the HTTP remote access policy for HTTP mode, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/http # disable http
UCSC(policy-mgr) /domain-group/http* # commit-buffer
UCSC(policy-mgr) /domain-group/http #
```

What to Do Next

Optionally, configure the following remote access policies:

- Telnet
- Web Session Limits
- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting an HTTP Remote Access Policy

An HTTP remote access policy is deleted from a domain group under the domain group root. HTTP remote access policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default HTTP policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete http**	Deletes the HTTP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group/http* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the HTTP policy for that domain group, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/domain-group # delete http
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Configuring Telnet

Configuring a Telnet Remote Access Policy

Before You Begin

Before configuring a Telnet remote access policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create telnetd**	(Optional) If scoping into a domain group previously, creates the Telnet policy for that domain group.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group # **scope telnetd**	(Optional) If scoping into the domain group root previously, scopes the default Telnet policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/telnetd* # **enable** | **disable telnet-server**	Enables or disables Telnet server services.
Step 6	UCSC(policy-mgr) /domain-group/telnetd* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root (which has an existing Telnet policy by default), enable Telnet server services, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope telnetd
UCSC(policy-mgr) /domain-group/telnetd # enable telnet-server
UCSC(policy-mgr) /domain-group/telnetd* # commit-buffer
UCSC(policy-mgr) /domain-group/telnetd #
```

The following example shows how to scope into the domain group domaingroup01, create a Telnet policy, enable Telnet server services, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create telnetd
UCSC(policy-mgr) /domain-group/telnetd* # enable telnet-server
UCSC(policy-mgr) /domain-group/telnetd* # commit-buffer
UCSC(policy-mgr) /domain-group/telnetd #
```

The following example shows how to scope into the domain group root (which has an existing Telnet policy by default), disable Telnet server services, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope telnetd
UCSC(policy-mgr) /domain-group/telnetd # disable telnet-server
UCSC(policy-mgr) /domain-group/telnetd* # commit-buffer
UCSC(policy-mgr) /domain-group/telnetd #
```

The following example shows how to scope into the domain group domaingroup01, disable Telnet server services, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/telnetd # disable telnet-server
UCSC(policy-mgr) /domain-group/telnetd* # commit-buffer
UCSC(policy-mgr) /domain-group/telnetd #
```

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Web Session Limits

- CIM XML
- Interfaces Monitoring Policy
- SSH Configuration

Deleting a Telnet Remote Access Policy

A Telnet remote access policy is deleted from a domain group under the domain group root. Telnet remote access policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default Telnet policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete telnetd**	Deletes the Telnet policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group/http* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the Telnet policy for that domain group, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/domain-group # delete telnetd
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Configuring Web Session Limits

Configuring a Web Session Limits Remote Access Policy

Before You Begin

Before configuring a web session limits remote access policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create web-session-limits**	(Optional) If scoping into a domain group previously, creates the web session limits policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope web-session-limits**	(Optional) If scoping into the domain group root previously, scopes the default web session limits policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/web-session-limits* # **set sessionsperuser** *sessions-per-user*	Sets the sessions per user limit (1-256).
Step 6	UCSC(policy-mgr) /domain-group/web-session-limits* # **set totalsessions** *total-sessions*	Sets the total sessions limit (1-256).
Step 7	UCSC(policy-mgr) /domain-group/web-session-limits* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root (which has an existing web sessions limit policy by default), set the sessions per user limit to 12 sessions, set the total sessions limit to 144 sessions, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope web-session-limits
UCSC(policy-mgr) /domain-group/web-session-limits # set sessionsperuser 12
UCSC(policy-mgr) /domain-group/web-session-limits* # set totalsessions 144
UCSC(policy-mgr) /domain-group/web-session-limits* # commit-buffer
UCSC(policy-mgr) /domain-group/web-session-limits #
```

The following example shows how to scope into the domain group domaingroup01, create a web sessions limit policy, set the sessions per user limit to 12 sessions, set the total sessions limit to 144 sessions, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create web-session-limits
UCSC(policy-mgr) /domain-group/web-session-limits* # set sessionsperuser 12
UCSC(policy-mgr) /domain-group/web-session-limits* # set totalsessions 144
UCSC(policy-mgr) /domain-group/web-session-limits* # commit-buffer
UCSC(policy-mgr) /domain-group/web-session-limits #
```

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- CIM XML
- Interfaces Monitoring Policy

Deleting a Web Session Limits Remote Access Policy

A web session limits remote access policy is deleted from a domain group under the domain group root. Web session limits remote access policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 3	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default web session limits policies cannot be deleted under the domain group root.
Step 4	UCSC(policy-mgr) /domain-group # **delete web-session-limits**	Deletes the web session limits policy for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/http* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete a web sessions limit policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete web-session-limits
UCSC(policy-mgr) /domain-group/web-session-limits* # commit-buffer
UCSC(policy-mgr) /domain-group/web-session-limits #
```

Configuring CIM XML

Configuring a CIM XML Remote Access Policy

Before You Begin

Before configuring a CIM XML remote access policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create cimxml**	(Optional) If scoping into a domain group previously, creates the CIM XML policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope cimxml**	(Optional) If scoping into the domain group root previously, scopes the default CIM XML's policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/cimxml # **enable cimxml**	Enables CIM XML mode.
Step 6	UCSC(policy-mgr) /domain-group/cimxml* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root (which has an existing CIM XML policy by default), enable CIM XML mode, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope cimxml
UCSC(policy-mgr) /domain-group/cimxml # enable cimxml
UCSC(policy-mgr) /domain-group/cimxml* # commit-buffer
UCSC(policy-mgr) /domain-group/cimxml #
```

The following example shows how to scope into the domain group domaingroup01, create a CIM XML policy, enable CIM XML mode, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create cimxml
UCSC(policy-mgr) /domain-group/cimxml* # enable cimxml
UCSC(policy-mgr) /domain-group/cimxml* # commit-buffer
UCSC(policy-mgr) /domain-group/cimxml #
```

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- Interfaces Monitoring Policy

Deleting a CIM XML Remote Access Policy

A CIM XML remote access policy is deleted from a domain group under the domain group root. CIM XML remote access policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default CIM XML policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete cimxml**	Deletes the CIM XML policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group/cimxml* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the CIM XML policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete cimxml
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring Interfaces Monitoring

Configuring an Interfaces Monitoring Remote Access Policy

Before You Begin

Before configuring an interfaces monitoring remote access policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create mgmt-if-mon-policy**	(Optional) If scoping into a domain group previously, creates the management interface monitor policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope mgmt-if-mon-policy**	(Optional) If scoping into the domain group root previously, scopes the default management interface monitors policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/cimxml # **set admin-state enabled** | **disabled**	Enables or disabled the administrator status mode.
Step 6	UCSC(policy-mgr) /domain-group/cimxml # **set arp-deadline** *arp-response-deadline*	Enter the deadline time in minutes to wait for ARP responses (5-15).
Step 7	UCSC(policy-mgr) /domain-group/cimxml # **set arp-requests** *arp-requests*	Enter the number of ARP requests (1-5).
Step 8	UCSC(policy-mgr) /domain-group/cimxml # **set arp-target1** *arp-ip-target-1*	Enter the ARP IP Target1 (in format 0.0.0.0) to remove.
Step 9	UCSC(policy-mgr) /domain-group/cimxml # **set arp-target2** *arp-ip-target-1*	Enter the ARP IP Target2 (in format 0.0.0.0) to remove.
Step 10	UCSC(policy-mgr) /domain-group/cimxml # **set arp-target3** *arp-ip-target-1*	Enter the ARP IP Target3 (in format 0.0.0.0) to remove.
Step 11	UCSC(policy-mgr) /domain-group/cimxml # **set max-fail-reports** *arp-ip-target-1*	Enter the number of failure reports at which the interface is to be marked as down (2-5).
Step 12	UCSC(policy-mgr) /domain-group/cimxml # **set mii-retry-count** *mii-retry-count*	Enter the maximum number of retries when using the Media Independent Interface (MII) status to perform monitoring (1-3).
Step 13	UCSC(policy-mgr) /domain-group/cimxml # **set mii-retry-interval** *mii-retry-interval*	Enter the interval between MII status monitoring retries (3-10).
Step 14	UCSC(policy-mgr) /domain-group/cimxml # **set monitor-mechanism mii-status** | **ping-arp-targets** | **ping-getaway**	Enter the MII monitoring mechanism of MII Status (mii-status), Ping ARP Targets (ping-arp-targets), or Ping Getaway (ping-getaway).

	Command or Action	Purpose
Step 15	UCSC(policy-mgr) /domain-group/cimxml # **set ping-deadline** *ping-deadline*	Enter the deadline time to wait for ping responses (5-15).
Step 16	UCSC(policy-mgr) /domain-group/cimxml # **set ping-requests** *ping-requests*	Enter the number of ping requests (1-5).
Step 17	UCSC(policy-mgr) /domain-group/cimxml # **set poll-interval** *poll-interval*	Enter the polling interval in seconds (90-300).
Step 18	UCSC(policy-mgr) /domain-group/cimxml* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root (which has an existing Management Interfaces Monitoring policy by default), enable Management Interfaces Monitoring mode, enter the status settings, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope mgmt-if-mon-policy
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy # set admin-state enabled
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-deadline 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-requests 1
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target1 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target2 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target3 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set max-fail-reports 2
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-count 1
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-interval 3
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set monitor-mechanism ping-getaway
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-deadline 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-requests 1
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set poll-interval 90
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy #
```

The following example shows how to scope into the domain group domaingroup01, create the Management Interfaces Monitoring policy, enter the status settings, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create mgmt-if-mon-policy
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set admin-state enabled
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-deadline 15
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-requests 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target1 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target2 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set arp-target3 0.0.0.0
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set max-fail-reports 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-count 3
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set mii-retry-interval 10
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set monitor-mechanism ping-getaway
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-deadline 15
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set ping-requests 5
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # set poll-interval 300
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/mgmt-if-mon-policy #
```

What to Do Next

Optionally, configure the following remote access policies:

- HTTP
- Telnet
- Web Session Limits
- CIM XML

Deleting an Interfaces Monitoring Remote Access Policy

An interfaces monitoring remote access policy is deleted from a domain group under the domain group root. Interfaces monitoring remote access policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default Management Interfaces Monitoring policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete mgmt-if-mon-policy**	Deletes the Management Interfaces Monitoring policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the Management Interfaces Monitoring policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # delete mgmt-if-mon-policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Authentication Services

Cisco UCS Central uses LDAP for native authentication, and RADIUS and TACACS+ 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 will be 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 3: 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 Groups

You can define up to 28 LDAP provider groups 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 of the configured servers are unavailable or unreachable, Cisco UCS Central automatically falls back to the local authentication method using the local username and password.

Creating an LDAP Provider

Cisco UCS Central supports a maximum of 16 LDAP providers.

Before You Begin

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with Cisco UCS. This account should be given a non-expiring password.

- In the LDAP server, perform one of the following configurations:
  - Configure LDAP groups. LDAP groups contain user role and locale information.
  - Configure users with the attribute that holds the user role and locale information for Cisco UCS Central. You can choose whether to extend the LDAP schema for this attribute. If you do not want to extend the schema, use an existing LDAP attribute to hold the Cisco UCS user roles and locales. If you prefer to extend the schema, create a custom attribute, such as the CiscoAVPair attribute.

    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

- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

- If you want to use secure communications, create a trusted point containing the certificate of the root certificate authority (CA) of the LDAP server in Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **create server** *server-name*	Creates an LDAP server instance and enters security LDAP server mode. If SSL is enabled, the *server-name* , typically an IP address or FQDN, must exactly match a Common Name (CN) in the LDAP server's security certificate. If you use a hostname rather than an IPv4 or IPv6 address, you must configure a DNS server. If the Cisco UCS domain is not registered with Cisco UCS Central or DNS management is set to **local**, configure a DNS server in Cisco UCS Manager. If the Cisco UCS domain is registered with Cisco UCS Central and DNS management is set to **global**, configure a DNS server in Cisco UCS Central..
Step 6	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set attribute** *attribute*	(Optional) An LDAP attribute that stores the values for the user roles and locales. This property is always a name-value pair. The system queries the user record for the value that matches this attribute name. If you do not want to extend your LDAP schema, you can configure an existing, unused LDAP attribute with the Cisco UCS roles and locales. Alternatively, you can create an attribute named CiscoAVPair in the remote authentication service with the following attribute ID: 1.3.6.1.4.1.9.287247.1 This value is required unless a default attribute has been set on the LDAP **General** tab.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set basedn** *basedn-name*	The specific distinguished name in the LDAP hierarchy where the server should begin a search when a remote user logs in and the system attempts to get the user's DN based on their username. The length of the base DN can be set to a maximum of 255 characters minus the length of CN=username, where username identifies the remote user attempting to access Cisco UCS Manager using LDAP authentication. This value is required unless a default base DN has been set on the LDAP **General** tab.
Step 8	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set binddn** *binddn-name*	The distinguished name (DN) for an LDAP database account that has read and search permissions for all objects under the base DN. The maximum supported string length is 255 ASCII characters.
Step 9	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set filter** *filter-value*	The LDAP search is restricted to those user names that match the defined filter. This value is required unless a default filter has been set on the LDAP **General** tab.
Step 10	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set password**	The password for the LDAP database account specified in the **Bind DN** field. You can enter any standard ASCII characters except for space, § (section sign), ? (question mark), or = (equal sign). To set the password, press **Enter** after typing the **set password** command and enter the key value at the prompt.
Step 11	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set order** *order-num*	The order in which Cisco UCS Central uses this provider to authenticate users.
Step 12	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set port** *port-num*	The port through which Cisco UCS Central communicates with the LDAP database. The standard port number is 389.
Step 13	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set ssl** {**yes** | **no**}	Enables or disables the use of encryption when communicating with the LDAP server. The options are as follows: • **yes —**Encryption is required. If encryption cannot be negotiated, the connection fails. • **no —**Encryption is disabled. Authentication information is sent as clear text. LDAP uses STARTTLS. This allows encrypted communication using port 389.

	Command or Action	Purpose
Step 14	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set timeout** *timeout-num*	The length of time in seconds the system should spend trying to contact the LDAP database before it times out. Enter an integer from 1 to 60 seconds, or enter 0 (zero) to use the global timeout value specified on the LDAP **General** tab. The default is 30 seconds.
Step 15	UCSC(policy-mgr) /domain-group/security/ldap/server* # **set vendor**	Specifies the vendor for the LDAP group. • **ms-ad —**To specify Microsoft Active Directory, enter ms-ad. • **openldap —**To specify OpenLDAP server, enter openldap.
Step 16	UCSC(policy-mgr) /domain-group/security/ldap/server* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an LDAP server instance named 10.193.169.246, configure the binddn, password, order, port, and SSL settings, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # create server 10.193.169.246
UCSC(policy-mgr) /domain-group/security/ldap/server* # set binddn
"cn=Administrator,cn=Users,DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCSC(policy-mgr) /domain-group/security/ldap/server* # set password
Enter the password:
Confirm the password:
UCSC(policy-mgr) /domain-group/security/ldap/server* # set order 2
UCSC(policy-mgr) /domain-group/security/ldap/server* # set port 389
UCSC(policy-mgr) /domain-group/security/ldap/server* # set ssl yes
UCSC(policy-mgr) /domain-group/security/ldap/server* # set timeout 30
UCSC(policy-mgr) /domain-group/security/ldap/server* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap/server #
```

What to Do Next

For implementations involving a single LDAP database, select LDAP as the authentication service.

Note When you specify multiple databases for implementation, if you choose a specific user within the database, the server goes in the order of the specified LDAP databases before authenticating the user.

Configuring Default Settings for LDAP Providers

The properties that you configure in this task are the default settings for all provider connections of this type defined in Cisco UCS Central. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

If you are using Active Directory as your LDAP server, create a user account in the Active Directory server to bind with Cisco UCS. This account should be given a non-expiring password.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **set attribute** *attribute*	Restricts database searches to records that contain the specified attribute.
Step 6	UCSC(policy-mgr) /domain-group/security/ldap* # **set basedn** *distinguished-name*	Restricts database searches to records that contain the specified distinguished name.
Step 7	UCSC(policy-mgr) /domain-group/security/ldap* # **set filter** *filter*	Restricts database searches to records that contain the specified filter.
Step 8	UCSC(policy-mgr) /domain-group/security/ldap* # **set timeout** *seconds*	Sets the time interval the system waits for a response from the LDAP server before noting the server as down.
Step 9	UCSC(policy-mgr) /domain-group/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the LDAP attribute to CiscoAvPair, the base distinguished name to "DC=cisco-ucsm-aaa3,DC=qalab,DC=com", the filter to sAMAccountName=$userid, and the timeout interval to 5 seconds, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # set attribute CiscoAvPair
UCSC(policy-mgr) /domain-group/security/ldap* # set basedn
"DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCSC(policy-mgr) /domain-group/security/ldap* # set filter sAMAccountName=$userid
UCSC(policy-mgr) /domain-group/security/ldap* # set timeout 5
UCSC(policy-mgr) /domain-group/security/ldap* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap #
```

What to Do Next

Create an LDAP provider.

Changing the LDAP Group Rule for an LDAP Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **scope server** *ldap-provider*	Enters security LDAP provider mode.
Step 6	UCSC(policy-mgr) /domain-group/security/ldap/server # **scope ldap-group-rule**	Enters LDAP group rule mode.
Step 7	UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule # **set authorization** {**enable** | **disable**}	Specifies whether Cisco UCS searches LDAP groups when assigning user roles and locales to a remote user. • **disable—**Cisco UCS does not access any LDAP groups. • **enable—**Cisco UCS searches the LDAP provider groups mapped in this Cisco UCS domain. If the remote user is found, Cisco UCS assigns the user roles and locales defined for that LDAP group in the associated LDAP group map. **Note** Role and locale assignment is cumulative. If a user is included in multiple groups, or has a role or locale specified in the LDAP attribute, Cisco UCS assigns that user all the roles and locales mapped to any of those groups or attributes.
Step 8	UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule* # **set member-of-attribute** *attr-name*	The attribute Cisco UCS uses to determine group membership in the LDAP database.

	Command or Action	Purpose
		The supported string length is 63 characters. The default string is memberOf.
Step 9	UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule* # **set traversal** {**non-recursive** | **recursive**}	Specifies whether Cisco UCS takes the settings for a group member's parent group, if necessary. This can be: • **non-recursive—**Cisco UCS only searches those groups that the user belongs to. • **recursive—**Cisco UCS searches all the ancestor groups belonging to the user.
Step 10	UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the LDAP group rule to enable authorization, set the member of attribute to memberOf, set the traversal to non-recursive, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # scope server ldapprovider
UCSC(policy-mgr) /domain-group/security/ldap/server # scope ldap-group-rule
UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule # set authorization
enable
UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule* # set member-of-attribute
 memberOf
UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule* # set traversal
non-recursive
UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap/server/ldap-group-rule #
```

Deleting an LDAP Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **delete server** *serv-name*	Deletes the specified server.
Step 6	UCSC(policy-mgr) /domain-group/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete the LDAP server called ldap1 and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # delete server ldap1
UCSC(policy-mgr) /domain-group/security/ldap* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap #
```

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 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
- Both 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 new capability, you do not always need to 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.

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 you nest an LDAP group 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.

Creating an LDAP Group Map

Before You Begin

- Create an LDAP group in the LDAP server.
- Configure the distinguished name for the LDAP group in the LDAP server.
- Create locales in Cisco UCS Central (optional).
- Create custom roles in Cisco UCS Central (optional).

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **create ldap-group** *group-dn*	Creates an LDAP group map for the specified DN.
Step 6	UCSC(policy-mgr) /domain-group/security/ldap/ldap-group* # **create locale** *locale-name*	Maps the LDAP group to the specified locale.
Step 7	UCSC(policy-mgr) /domain-group/security/ldap/ldap-group* # **create role** *role-name*	Maps the LDAP group to the specified role.
Step 8	UCSC(policy-mgr) /domain-group/security/ldap/ldap-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to map the LDAP group mapped to a DN, set the locale to pacific, set the role to admin, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # create ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /domain-group/security/ldap/ldap-group* # create locale pacific
UCSC(policy-mgr) /domain-group/security/ldap/ldap-group* # create role admin
UCSC(policy-mgr) /domain-group/security/ldap/ldap-group* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap/ldap-group #
```

What to Do Next

Set the LDAP group rule.

Deleting an LDAP Group Map

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **delete ldap-group** *group-dn*	Deletes the LDAP group map for the specified DN.
Step 6	UCSC(policy-mgr) /domain-group/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an LDAP group map and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # delete ldap-group
cn=security,cn=users,dc=lab,dc=com
UCSC(policy-mgr) /domain-group/security/ldap* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap #
```

Configuring RADIUS Providers

Configuring Properties for RADIUS Providers

The properties that you configure in this task are the default settings for all provider connections of this type defined in Cisco UCS Central. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

Note RADIUS native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central under the Domain Group root and domain groups. RADIUS may be used to create global policies for Cisco UCS domains.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope radius**	Enters security RADIUS mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/security/radius # **set retries** *retry-num*	Sets the number of times to retry communicating with the RADIUS server before noting the server as down.
Step 6	UCSC(policy-mgr) /domain-group/security/radius* # **set timeout** *seconds*	Sets the time interval that the system waits for a response from the RADIUS server before noting the server as down.
Step 7	UCSC(policy-mgr) /domain-group/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the RADIUS retries to 4, set the timeout interval to 30 seconds, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope radius
UCSC(policy-mgr) /domain-group/security/radius # set retries 4
UCSC(policy-mgr) /domain-group/security/radius* # set timeout 30
UCSC(policy-mgr) /domain-group/security/radius* # commit-buffer
UCSC(policy-mgr) /domain-group/security/radius #
```

What to Do Next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Central supports a maximum of 16 RADIUS providers. RADIUS native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central under the Domain Group root and domain groups. RADIUS may be used to create global policies for Cisco UCS domains.

Before You Begin

Perform the following configuration in the RADIUS server:

- Configure users with the attribute that holds the user role and locale information for Cisco UCS Central. You can choose whether to extend the RADIUS schema for this attribute. If you do not want to extend the schema, use an existing RADIUS attribute to hold the Cisco UCS user roles and locales. If you prefer to extend the schema, create a custom attribute, such as the cisco-avpair attribute.

  The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001.

  The following syntax example shows how to specify multiples user roles and locales if you choose to create the cisco-avpair attribute: `shell:roles="admin,aaa" shell:locales="L1,abc"`. Use a comma "," as the delimiter to separate multiple values.

- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope radius**	Enters security RADIUS mode.
Step 5	UCSC(policy-mgr) /domain-group/security/radius # **create server** *server-name*	Creates a RADIUS server instance and enters security RADIUS server mode
Step 6	UCSC(policy-mgr) /domain-group/security/radius/server* # **set authport** *authport-num*	(Optional) Specifies the port used to communicate with the RADIUS server.
Step 7	UCSC(policy-mgr) /domain-group/security/radius/server* # **set key**	Sets the RADIUS server key. To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.
Step 8	UCSC(policy-mgr) /domain-group/security/radius/server* # **set order** *order-num*	(Optional) Specifies when in the order this server will be tried.
Step 9	UCSC(policy-mgr) /domain-group/security/radius/server* # **set retries** *retry-num*	(Optional) Sets the number of times to retry communicating with the RADIUS server before noting the server as down.
Step 10	UCSC(policy-mgr) /domain-group/security/radius/server* # **set timeout** *seconds*	(Optional) Sets the time interval that the system waits for a response from the RADIUS server before noting the server as down.
Step 11	UCSC(policy-mgr) /domain-group/security/radius/server* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a server instance named radiusserv7, set the authentication port to 5858, set the key to radiuskey321, set the order to 2, set the retries to 4, set the timeout to 30, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope radius
```

```
UCSC(policy-mgr) /domain-group/security/radius # create server radiusserv7
UCSC(policy-mgr) /domain-group/security/radius/server* # set authport 5858
UCSC(policy-mgr) /domain-group/security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
UCSC(policy-mgr) /domain-group/security/radius/server* # set order 2
UCSC(policy-mgr) /domain-group/security/radius/server* # set retries 4
UCSC(policy-mgr) /domain-group/security/radius/server* # set timeout 30
UCSC(policy-mgr) /domain-group/security/radius/server* # commit-buffer
UCSC(policy-mgr) /domain-group/security/radius/server #
```

What to Do Next

- For implementations involving a single RADIUS database, select RADIUS as the primary authentication service.
- For implementations involving multiple RADIUS databases, configure a RADIUS provider group.

Deleting a RADIUS Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope radius**	Enters security RADIUS mode.
Step 5	UCSC(policy-mgr) /domain-group/security/radius # **delete server** *serv-name*	Deletes the specified server.
Step 6	UCSC(policy-mgr) /domain-group/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete the RADIUS server called radius1 and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope radius
UCSC(policy-mgr) /domain-group/security/radius # delete server radius1
UCSC(policy-mgr) /domain-group/security/radius* # commit-buffer
UCSC(policy-mgr) /domain-group/security/radius #
```

Configuring TACACS+ Providers

Configuring Properties for TACACS+ Providers

The properties that you configure in this task are the default settings for all provider connections of this type defined in Cisco UCS Central. If an individual provider includes a setting for any of these properties, Cisco UCS uses that setting and ignores the default setting.

Note TACACS+ native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central. TACACS+ may be used to create global policies for Cisco UCS domains.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope tacacs**	Enters security TACACS+ mode. The TACACS+ related settings will be applicable only for the Cisco UCS domains under the Domain Group root and child domain groups.
Step 5	UCSC(policy-mgr) /domain-group/security/tacacs # **set key**	Sets the TACACS+ server key. To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.
Step 6	UCSC(policy-mgr) /domain-group/security/tacacs* # **set order** *order-num*	Specifies when in the order this server will be tried.
Step 7	UCSC(policy-mgr) /domain-group/security/tacacs* # **set timeout** *seconds*	Sets the time interval that the system waits for a response from the TACACS+ server before noting the server as down.
Step 8	UCSC(policy-mgr) /domain-group/security/tacacs* # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.
Step 9	UCSC(policy-mgr) /domain-group/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the key to tacacskey321, set the order to 4, set the timeout interval to 45 seconds, set the authentication port to 5859, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope tacacs
UCSC(policy-mgr) /domain-group/security/tacacs # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCSC(policy-mgr) /domain-group/security/tacacs* # set order 4
UCSC(policy-mgr) /domain-group/security/tacacs* # set timeout 45
UCSC(policy-mgr) /domain-group/security/tacacs* # set port 5859
UCSC(policy-mgr) /domain-group/security/tacacs* # commit-buffer
UCSC(policy-mgr) /domain-group/security/tacacs #
```

What to Do Next

Create a TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Central supports a maximum of 16 TACACS+ providers. TACACS+ native authentication is not supported for this release, and cannot be used to create policies in Cisco UCS Central. TACACS+ may be used to create global policies for Cisco UCS domains.

Before You Begin

Perform the following configuration in the TACACS+ server:

- Create the cisco-av-pair attribute. You cannot use an existing TACACS+ attribute.

  The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider.

  The following syntax example shows how to specify multiples user roles and locales when you create the cisco-av-pair attribute: `cisco-av-pair=shell:roles="admin aaa" shell:locales*"L1 abc"`. Using an asterisk (*) in the cisco-av-pair attribute syntax flags the locale as optional, preventing authentication failures for other Cisco devices that use the same authorization profile. Use a space as the delimiter to separate multiple values.

- For a cluster configuration, add the management port IP addresses for both fabric interconnects. This configuration ensures that remote users can continue to log in if the first fabric interconnect fails and the system fails over to the second fabric interconnect. All login requests are sourced from these IP addresses, not the virtual IP address used by Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope tacacs**	Enters security TACACS+ mode.
Step 5	UCSC(policy-mgr) /domain-group/security/tacacs # **create server** *server-name*	Creates an TACACS+ server instance and enters security TACACS+ server mode
Step 6	UCSC(policy-mgr) /domain-group/security/tacacs/server* # **set key**	(Optional) Sets the TACACS+ server key. To set the key value, press **Enter** after typing the **set key** command and enter the key value at the prompt.
Step 7	UCSC(policy-mgr) /domain-group/security/tacacs/server* # **set order** *order-num*	(Optional) Specifies when in the order this server will be tried.
Step 8	UCSC(policy-mgr) /domain-group/security/tacacs/server* # **set timeout** *seconds*	(Optional) Sets the time interval that the system waits for a response from the TACACS+ server before noting the server as down.
Step 9	UCSC(policy-mgr) /domain-group/security/tacacs/server* # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.
Step 10	UCSC(policy-mgr) /domain-group/security/tacacs/server* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a server instance named tacacsserv680, set the key to tacacskey321, set the order to 4, set the authentication port to 5859, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope tacacs
UCSC(policy-mgr) /domain-group/security/tacacs # create server tacacsserv680
UCSC(policy-mgr) /domain-group/security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCSC(policy-mgr) /domain-group/security/tacacs/server* # set order 4
UCSC(policy-mgr) /domain-group/security/tacacs/server* # set timeout 45
UCSC(policy-mgr) /domain-group/security/tacacs/server* # set port 5859
UCSC(policy-mgr) /domain-group/security/tacacs/server* # commit-buffer
UCSC(policy-mgr) /domain-group/security/tacacs/server #
```

What to Do Next

- For implementations involving a single TACACS+ database, select TACACS+ as the primary authentication service.
- For implementations involving multiple TACACS+ databases, configure a TACACS+ provider group.

Deleting a TACACS+ Provider

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope tacacs**	Enters security TACACS+ mode.
Step 5	UCSC(policy-mgr) /domain-group/security/tacacs # **delete server** *serv-name*	Deletes the specified server.
Step 6	UCSC(policy-mgr) /domain-group/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete the TACACS server called tacacs1 and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope tacacs
UCSC(policy-mgr) /domain-group/security/tacacs # delete server TACACS1
UCSC(policy-mgr) /domain-group/security/tacacs* # commit-buffer
UCSC(policy-mgr) /domain-group/security/tacacs #
```

Configuring Multiple Authentication Systems

Multiple Authentication Systems

You can configure Cisco UCS to use multiple authentication systems by configuring the following features:

- Provider groups
- Authentication domains

Once provider groups and authentication domains have been configured in Cisco UCS Central GUI, the following syntax can be used to log in to the system using Cisco UCS Central CLI: **ucs-** *auth-domain*

When multiple authentication domains and native authentication are configured with a remote authentication service, use one of the following syntax examples to log in with SSH or Putty:

From a Linux terminal:

- **ssh ucs-***auth-domain**username*@*Cisco UCS domain-ip-address*

```
ssh ucs-example\\jsmith@192.0.20.11
```

- **ssh -l ucs-***auth-domain**username* {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*}

```
ssh -l ucs-example\\jsmith 192.0.20.11
```

- **ssh** {*Cisco UCS domain-ip-address* | *Cisco UCS domain-host-name*} **-l ucs-***auth-domain**username*

```
ssh 192.0.20.11 -l ucs-example\\jsmith
```

From a Putty client:

- Login as: **ucs-***auth-domain**username*

```
Login as: ucs-example\\jsmith
```

From a SSH client:

- Host Name: *Cisco UCS domain-ip-address*

  User Name: **ucs-***auth-domain**username*

```
Host Name: 192.0.20.11
```

```
User Name: ucs-example\\jsmith
```

Provider Groups

A provider group is a set of providers that will be used by Cisco UCS during the authentication process. Cisco UCS Central allows you to create a maximum of 16 provider groups, with a maximum of eight providers allowed per group.

During authentication, all the providers within a provider group are tried in order. If all of the configured servers are unavailable or unreachable, Cisco UCS Central automatically falls back to the local authentication method using the local username and password.

Creating an LDAP Provider Group

Creating an LDAP provider group allows you to authenticate using multiple LDAP databases.

Note Authenticating with a single LDAP database does not require you to set up an LDAP provider group.

Before You Begin

Create one or more LDAP providers.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **create auth-server-group** *auth-server-group-name*	Creates an LDAP provider group and enters authentication server group security LDAP mode.
Step 6	UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified LDAP provider to the LDAP provider group and enters server reference authentication server group security LDAP mode.
Step 7	UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is equivalent to giving that server reference the highest priority.
Step 8	UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an LDAP provider group called ldapgroup, add two previously configured providers called ldap1 and ldap2 to the provider group, set the order, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # create auth-server-group ldapgroup
UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group* # create server-ref ldap1
UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group/server-ref* # set order 1
UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group/server-ref* # up
UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group* # create server-ref ldap2
UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group/server-ref* # set order 2
UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group/server-ref* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap/auth-server-group/server-ref #
```

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting an LDAP Provider Group

Before You Begin

Remove the provider group from an authentication configuration.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope ldap**	Enters security LDAP mode.
Step 5	UCSC(policy-mgr) /domain-group/security/ldap # **delete auth-server-group** *auth-server-group-name*	Deletes the LDAP provider group.
Step 6	UCSC(policy-mgr) /domain-group/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an LDAP provider group called ldapgroup and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope ldap
UCSC(policy-mgr) /domain-group/security/ldap # delete auth-server-group ldapgroup
UCSC(policy-mgr) /domain-group/security/ldap* # commit-buffer
UCSC(policy-mgr) /domain-group/security/ldap #
```

Creating a RADIUS Provider Group

Creating a RADIUS provider group allows you to authenticate using multiple RADIUS databases.

Note Authenticating with a single RADIUS database does not require you to set up a RADIUS provider group.

Before You Begin

Create one or more RADIUS providers.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope radius**	Enters security RADIUS mode.
Step 5	UCSC(policy-mgr) /domain-group/security/radius # **create auth-server-group** *auth-server-group-name*	Creates a RADIUS provider group and enters authentication server group security RADIUS mode.
Step 6	UCSC(policy-mgr) /domain-group/security/radius/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified RADIUS provider to the RADIUS provider group and enters server reference authentication server group security RADIUS mode.
Step 7	UCSC(policy-mgr) /domain-group/security/radius/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is equivalent to giving that server reference the highest priority.
Step 8	UCSC(policy-mgr) /domain-group/security/radius/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a RADIUS provider group called radiusgroup, add two previously configured providers called radius1 and radius2 to the provider group, set the order, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope radius
UCSC(policy-mgr) /domain-group/security/radius # create auth-server-group radiusgroup
UCSC(policy-mgr) /domain-group/security/radius/auth-server-group* # create server-ref radius1
UCSC(policy-mgr) /domain-group/security/radius/auth-server-group/server-ref* # set order 1
UCSC(policy-mgr) /domain-group/security/radius/auth-server-group/server-ref* # up
UCSC(policy-mgr) /domain-group/security/radius/auth-server-group* # create server-ref radius2
UCSC(policy-mgr) /domain-group/security/radius/auth-server-group/server-ref* # set order 2
UCSC(policy-mgr) /domain-group/security/radius/auth-server-group/server-ref* # commit-buffer
UCSC(policy-mgr) /domain-group/security/radius/auth-server-group/server-ref #
```

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a RADIUS Provider Group

Remove the provider group from an authentication configuration.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope radius**	Enters security RADIUS mode.
Step 5	UCSC(policy-mgr) /domain-group/security/radius # **delete auth-server-group** *auth-server-group-name*	Deletes the RADIUS provider group.
Step 6	UCSC(policy-mgr) /domain-group/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a RADIUS provider group called radiusgroup and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope radius
UCSC(policy-mgr) /domain-group/security/radius # delete auth-server-group radiusgroup
UCSC(policy-mgr) /domain-group/security/radius* # commit-buffer
UCSC(policy-mgr) /domain-group/security/radius #
```

Creating a TACACS+ Provider Group

Creating a TACACS+ provider group allows you to authenticate using multiple TACACS+ databases.

Note Authenticating with a single TACACS+ database does not require you to set up a TACACS+ provider group.

Before You Begin

Create a TACACS+ provider.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope tacacs**	Enters security TACACS+ mode.
Step 5	UCSC(policy-mgr) /domain-group/security/tacacs # **create auth-server-group** *auth-server-group-name*	Creates a TACACS+ provider group and enters authentication server group security TACACS+ mode.
Step 6	UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified TACACS+ provider to the TACACS+ provider group and enters server reference authentication server group security TACACS+ mode.
Step 7	UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group* # **set order** *order-num*	Specifies the order in which Cisco UCS uses this provider to authenticate users. Valid values include no-value and 0-16, with the lowest value indicating the highest priority. Setting the order to no-value is equivalent to giving that server reference the highest priority.
Step 8	UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a TACACS+ provider group called tacacsgroup, add two previously configured providers called tacacs1 and tacacs2 to the provider group, set the order, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope tacacs
UCSC(policy-mgr) /domain-group/security/tacacs # create auth-server-group tacacsgroup
UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group* # create server-ref tacacs1
UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group/server-ref* # set order 1
UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group/server-ref* # up
UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group* # create server-ref tacacs2
UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group/server-ref* # set order 2
```

```
UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group/server-ref* # commit-buffer
UCSC(policy-mgr) /domain-group/security/tacacs/auth-server-group/server-ref #
```

What to Do Next

Configure an authentication domain or select a default authentication service.

Deleting a TACACS+ Provider Group

Remove the provider group from an authentication configuration.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope tacacs**	Enters security TACACS+ mode.
Step 5	UCSC(policy-mgr) /domain-group/security/tacacs # **delete auth-server-group** *auth-server-group-name*	Deletes the TACACS+ provider group.
Step 6	UCSC(policy-mgr) /domain-group/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a TACACS+ provider group called tacacsgroup and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope tacacs
UCSC(policy-mgr) /domain-group/security/tacacs # delete auth-server-group tacacsgroup
UCSC(policy-mgr) /domain-group/security/tacacs* # commit-buffer
UCSC(policy-mgr) /domain-group/security/tacacs #
```

Authentication Domains

Authentication domains are used by Cisco UCS Domain to leverage multiple authentication systems. Each authentication domain is specified and configured during login. If no authentication domain is specified, the default authentication service configuration is used.

You can create up to eight authentication domains. Each authentication domain is associated with a provider group and realm in Cisco UCS Domain. If no provider group is specified, all servers within the realm are used.

Note Effective with this release, authentication domains for LDAP are supported for Cisco UCS Central. However, the authentication domains are supported for managed Cisco UCS domains from the Cisco UCS Central Domain Group root.

Creating an Authentication Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope auth-realm**	Enters authentication realm mode.
Step 5	UCSC(policy-mgr) /domain-group/security/auth-realm # **create auth-domain** *domain-name*	Creates an authentication domain and enters authentication domain mode. The Radius related settings will be applicable only for the Cisco UCS domains under the Domain Group root and child domain groups. **Note** For systems using remote 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 domain name and user name combined character total exceeds 27.
Step 6	UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain* # **set refresh-period** *seconds*	(Optional) When a web client connects to Cisco UCS Central, the client needs to send

	Command or Action	Purpose
		refresh requests to Cisco UCS Central to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Central 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.
Step 7	UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain* # **set session-timeout** *seconds*	(Optional) The maximum amount of time that can elapse after the last refresh request before 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 an integer between 60 and 172800. The default is 7200 seconds.
Step 8	UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain* # **create default-auth**	(Optional) Creates a default authentication for the specified authentication domain.
Step 9	UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain/default-auth* # **set auth-server-group** *auth-serv-group-name*	(Optional) Specifies the provider group for the specified authentication domain.
Step 10	UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain/default-auth* # **set realm** {**ldap** | **local** | **radius** | **tacacs**}	Specifies the realm for the specified authentication domain.
Step 11	UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an authentication domain called domain1 with a web refresh period of 3600 seconds (1 hour) and a session timeout period of 14400 seconds (4 hours), configure domain1 to use the providers in ldapgroup1, set the realm type to ldap, and commit the transaction.

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope auth-realm
UCSC(policy-mgr) /domain-group/security/auth-realm # create auth-domain domain1
UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain* # set refresh-period 3600
UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain* # set session-timeout 14400
UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain* # create default-auth
```

```
UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain/default-auth* # set
auth-server-group ldapgroup1
UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain/default-auth* # set realm
ldap
UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain/default-auth* # commit-buffer
UCSC(policy-mgr) /domain-group/security/auth-realm/auth-domain/default-auth #
```

Selecting a Primary Authentication Service

Selecting the Console Authentication Service

Before You Begin

If the system uses a remote authentication service, create a provider for that authentication service. If the system uses only local authentication through Cisco UCS, you do not need to create a provider first.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope auth-realm**	Enters authentication realm security mode.
Step 5	UCSC(policy-mgr) /domain-group/security/auth-realm # **scope console-auth**	Enters console authorization security mode.
Step 6	UCSC(policy-mgr) /domain-group/security/auth-realm/console-auth # **set realm** *auth-type*	Specifies the console authentication, where the *auth-type* argument is one of the following keywords: • **ldap —**Specifies LDAP authentication • **local —**Specifies local authentication • **none —**Allows local users to log on without specifying a password • **radius —**Specifies RADIUS authentication • **tacacs —**Specifies TACACS+ authentication

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/security/auth-realm/console-auth* # **set auth-server-group** *auth-serv-group-name*	The associated provider group, if any.
Step 8	UCSC(policy-mgr) /domain-group/security/auth-realm/console-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the authentication to LDAP, set the console authentication provider group to provider1, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope auth-realm
UCSC(policy-mgr) /domain-group/security/auth-realm # scope console-auth
UCSC(policy-mgr) /domain-group/security/auth-realm/console-auth # set realm local
UCSC(policy-mgr) /domain-group/security/auth-realm/console-auth* # set auth-server-group
provider1
UCSC(policy-mgr) /domain-group/security/auth-realm/console-auth* # commit-buffer
UCSC(policy-mgr) /domain-group/security/auth-realm/console-auth #
```

Selecting the Default Authentication Service

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope auth-realm**	Enters authentication realm security mode.
Step 5	UCSC(policy-mgr) /domain-group/security/auth-realm # **scope default-auth**	Enters default authorization security mode.
Step 6	UCSC(policy-mgr) /domain-group/security/auth-realm/default-auth # **set realm** *auth-type*	Specifies the default authentication, where *auth-type* is one of the following keywords: • **ldap—**Specifies LDAP authentication • **local—**Specifies local authentication

	Command or Action	Purpose
		• **none**—Allows local users to log on without specifying a password • **radius**—Specifies RADIUS authentication • **tacacs**—Specifies TACACS+ authentication
Step 7	UCSC(policy-mgr) /domain-group/security/auth-realm/default-auth* # **set auth-server-group** *auth-serv-group-name*	(Optional) The associated provider group, if any.
Step 8	UCSC(policy-mgr) /domain-group/security/auth-realm/default-auth* # **set refresh-period** *seconds*	(Optional) When a web client connects to Cisco UCS Central, the client needs to send refresh requests to Cisco UCS Central to keep the web session active. This option specifies the maximum amount of time allowed between refresh requests for a user in this domain. If this time limit is exceeded, Cisco UCS Central considers the web session to be inactive, but it does not terminate the session.
Step 9	UCSC(policy-mgr) /domain-group/security/auth-realm/default-auth* # **set session-timeout** *seconds*	(Optional) The maximum amount of time that can elapse after the last refresh request before 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 an integer between 60 and 172800. The default is 7200 seconds.
Step 10	UCSC(policy-mgr) /domain-group/security/auth-realm/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the default authentication to LDAP, set the default authentication provider group to provider1, set the refresh period to 7200 seconds (2 hours), set the session timeout period to 28800 seconds (8 hours), and commit the transaction.

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope auth-realm
UCSC(policy-mgr) /domain-group/security/auth-realm # scope default-auth
UCSC(policy-mgr) /domain-group/security/default-auth # set realm ldap
UCSC(policy-mgr) /domain-group/security/default-auth* # set auth-server-group provider1
UCSC(policy-mgr) /domain-group/security/default-auth* # set refresh-period 7200
UCSC(policy-mgr) /domain-group/security/default-auth* # set session-timeout 28800
UCSC(policy-mgr) /domain-group/security/default-auth* # commit-buffer
UCSC(policy-mgr) /domain-group/security/default-auth #
```

Role Policy for Remote Users

By default, if user roles are not configured in Cisco UCS Central read-only access is granted to all users logging in to Cisco UCS Central from a remote server using the LDAP protocol (excluding RADIUS and TACACS+ authentication in this release).

Note RADIUS, TACACS+ and LDAP authentication are supported in locally managed Cisco UCS domains.

You can configure the role policy for remote users in the following ways:

- **assign-default-role**

  Does not restrict user access to Cisco UCS Central based on user roles. Read-only access is granted to all users unless other user roles have been defined in Cisco UCS Central.

  This is the default behavior.

- **no-login**

  Restricts user access to Cisco UCS Central based on user roles. If user roles have not been assigned for the remote authentication system, access is denied.

For security reasons, it might be desirable to restrict access to those users matching an established user role in Cisco UCS Central.

Configuring the Role Policy for Remote Users

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope auth-realm**	Enters authentication realm security mode.
Step 5	UCSC(policy-mgr) /domain-group/security/auth-realm # **set remote-user default-role** {**assign-default-role** | **no-login**}	Specifies whether user access to Cisco UCS Central is restricted based on user roles.
Step 6	UCSC(policy-mgr) /domain-group/security/auth-realm* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to set the role policy for remote users and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope auth-realm
UCSC(policy-mgr) /domain-group/security/auth-realm # set remote-user default-role
assign-default-role
UCSC(policy-mgr) /domain-group/security/auth-realm* # commit-buffer
UCSC(policy-mgr) /domain-group/security/auth-realm #
```

Managing DNS Policies

Cisco UCS Central supports global DNS policies defining the DNS server and domain name. Registered Cisco UCS domains choosing to define DNS management globally within that domain's policy resolution control will defer DNS management to its registration with Cisco UCS Central.

Configuring a DNS Policy

Before You Begin

Before configuring a DNS policy in a domain group under the Domain Group root, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope dns-config**	(Optional) If scoping into the domain group root previously, scopes the default DNS policy's configuration mode from the Domain Group root.
Step 4	UCSC(policy-mgr) /domain-group # **create dns-config**	(Optional) If scoping into a domain group previously, creates the DNS policy for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **set domain-name** *server-domain-name*	Defines the DNS domain name.
Step 6	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root (which has an existing DNS policy by default), define the DNS domain name as dnsdomain, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # set domain-name dnsdomain
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to scope into the domain group domaingroup01, create the DNS policy for that domain group, define the DNS domain name as dnsdomain, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create dns-config
UCSC(policy-mgr) /domain-group/domain-group* # set domain-name dnsdomain
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Deleting a DNS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default DNS policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete dns-config**	Deletes the DNS policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the DNS policy for that domain group, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/domain-group # delete dns-config
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Configuring a DNS Server for a DNS Policy

Before You Begin

Configure a DNS policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope dns-config**	Enter an existing DNS policy's configuration mode from the Domain Group root or a domain group scoped into.
Step 4	UCSC(policy-mgr) /domain-group/dns-config # **create dns** server-IP-address	Creates a DNS server instance.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, create a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # create dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to scope into the domain group domaingroup01, create a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # create dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Deleting a DNS Server from a DNS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope dns-config**	Enter an existing DNS policy's configuration mode from the Domain Group root or a domain group scoped into.
Step 4	UCSC(policy-mgr) /domain-group/dns-config # **delete dns** *server-IP-address*	Deletes a DNS server instance.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, delete a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # delete dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to scope into the domain group domaingroup01, delete a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # delete dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Creating a Global Power Allocation Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create cap-policy**	Creates global power allocation policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a global power allocation policy for a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # create cap-policy
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Deleting a Global Power Allocation Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete cap-policy**	Deletes global power allocation policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to delete a global power allocation policy for a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # delete cap-policy
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Configuring a Global Power Allocation Policy for a Chassis Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope cap-policy**	Enters the global power allocation mode.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy # **set cap-policy policy-driven-chassis-group-cap**	Specifies global power allocation policy for chassis group in the domain group.
Step 5	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure a global power allocation policy for a chassis group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope cap-policy
UCSC(policy-mgr) /domain-group/cap-policy # set cap-policy policy-driven-chassis-group-cap

UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Configuring a Global Power Allocation Policy Manually for a Blade Server

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope cap-policy**	Enters the global power allocation mode.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy # **set cap-policy manual-blade-level-cap**	Enables manual blade server level power allocation.
Step 5	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure manual power allocation policy for a blade server:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope cap-policy
UCSC(policy-mgr) /domain-group/cap-policy # set cap-policy manual-blade-level-cap
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Managing Power Policies

Cisco UCS Central supports global equipment policies defining the global power allocation policy (based on policy driven chassis group cap or manual blade level cap methods), power policy (based on grid, n+1 or non-redundant methods). Registered Cisco UCS domains choosing to define power management and power supply units globally within that client's policy resolution control will defer power management and power supply units to its registration with Cisco UCS Central.

Creating an Equipment Power Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create psu-policy**	Creates the power policy from the domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
```

```
UCSC(policy-mgr) /domain-group # create psu-policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an Equipment Power Policy

Procedure

Step 1 UCSC# **connect policy-mgr**
Enters policy manager mode.

Step 2 UCSC(policy-mgr) # **scope domain-group** *domain-group*
Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.

Step 3 UCSC(policy-mgr) /domain-group # **delete psu-policy**
Deletes the power policy from the domain group.

Step 4 UCSC(policy-mgr) /domain-group***** # **commit-buffer**
Commits the transaction to the system.

The following example shows how to delete an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # delete psu-policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring an Equipment Power Policy

Before You Begin

Before configuring a power equipment policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope psu-policy**	Enters the power policy mode.
Step 4	UCSC(policy-mgr) /domain-group # **set** descr *power-policy-description-text*	Specifies the description for the power policy.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group # **set redundancy grid** | **n-plus-1** | **non-redund**	Specifies the redundancy for the power policy for Grid (grid), N-Plus-1 (n-plus-1), or non-redundancy (non-redund).

The following example scopes the domain group dg1 and configures the equipment power policy for that domain group:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group/psu-policy # set descr "Power policy for sector 24"
UCSC(policy-mgr) /domain-group/psu-policy* # set redundancy grid
UCSC(policy-mgr) /domain-group/psu-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/psu-policy #
```

Viewing an Equipment Power Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **show psu-policy**	Enters the power policy mode.

The following example shows how to create an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope psu-policy
UCSC(policy-mgr) /domain-group/psu-policy # show
PSU Policy:
    Domain Group Redundancy Description
    ------------ ---------- -----------
    root/dg1     NPlus1
UCSC(policy-mgr) /domain-group #
```

Managing Time Zones

Cisco UCS Central supports global date and time policies based on international time zones and defined NTP server. Registered Cisco UCS Manager clients choosing to define date and time globally within that client's policy resolution control will defer the configuration for date and time to its registration with Cisco UCS Central.

Configuring a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create domain-group** *domain-group*	(Optional) This step is only necessary to create a new domain group under the Domain Group root (or creates a domain group under the domain group scoped into).
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	(Optional) This step is only necessary after creating a new domain group under the Domain Group root (or creating a domain group under the domain group scoped into). Commits the new domain group to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group # **create timezone-ntp-config**	(Optional) This step is only necessary the first time a date and time policy is configured for the newly created domain group under the Domain Group root that was created in the previous step, then enter the time zone NTP configuration mode. A date and time policy was created by the system for the Domain Group root, and is ready to be configured.
Step 6	UCSC(policy-mgr) /domain-group* # **scope timezone-ntp-config**	(Optional) This step is only necessary if entering an existing date and time policy's time zone NTP configuration mode from the Domain Group root or a domain group scoped into. Skip this step if creating a date and time policy.
Step 7	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **set timezone**	To set the time zone, press **Enter** after typing the set timezone command and enter the key value at the prompt. Configures the NTP server time zone. The attribute options are as follows: • **1 —**Africa • **2 —**Americas • **3 —**Antarctica • **4 —**Arctic Ocean • **5 —**Asia • **6 —**Atlantic Ocean

	Command or Action	Purpose
		• **7 —**Australia • **8 —**Europe • **9 —**India Ocean • **10 —**Pacific Ocean
Step 8	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope the Domain Group root, configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country"), and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to create a new domain group called domaingroup01 under the Domain Group root, commit the transaction, create a date and time policy, configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country"), and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create domain-group domaingroup01
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group # create timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
```

```
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope to domaingroup01 under the Domain Group root, create a date and time policy, configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country"), and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

What to Do Next

Configure an NTP server for a date and time policy.

Deleting a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default date and time policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete timezone-ntp-config**	Deletes the domain group's time zone policy.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope the domain group domaingroup01, delete that domain group's date and time policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete timezone-ntp-config
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

The following example shows how to scope the domain group root, attempt to delete that domain group's date and time policy, commit the transaction and recover from an error message (leaving the buffer in an unrecoverable uncommitted state) by initiating a clean exit and reconnecting to Policy Manager to clear the buffer:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # delete timezone-ntp-config
UCSC(policy-mgr) /domain-group* # commit-buffer
Error: Update failed:
[Timezone and NTP configuration under domain group root cannot be deleted]
UCSC(policy-mgr) /domain-group* # exit
UCSC(policy-mgr)* # exit
UCSC# connect policy-mgr
Cisco UCS Central
UCSC(policy-mgr)#
```

Note In the event you mistakenly scope to the domain group root, and enter the command delete timezone-ntp-config, the buffer will encounter an unrecoverable error, remaining in an uncommitted state and preventing subsequent commit-buffer commands from saving to the buffer. You must immediately exit and reconnect to the Policy Manager to clear the buffer.

Configuring an NTP Server for a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **create ntp** server-name	Creates an NTP server instance.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, create an NTP server instance named domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # create ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope to the domain group domaingroup01 under the domain group root, create an NTP server instance named domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # create ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

What to Do Next

Configure a date and time policy.

Configuring Properties for an NTP Server

The properties of an NTP server consist of its name. Changing those properties, unlike steps in the GUI involving configuring the NTP server's properties, requires deleting that NTP server and recreating it with a new name.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **delete ntp** server-name	Deletes an NTP server instance that requires renaming.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **create ntp** server-name	Creates an NTP server instance to replace the deleted NTP server instance.
Step 6	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, delete an NTP server instance named domaingroupNTP01 with a name that is no longer relevant, create a new NTP server instance named domaingroupNTP02 to replace the deleted NTP server, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # create ntp domaingroupNTP02
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope to the domain group domaingroup01 under the domain group root, delete an NTP server instance named domaingroupNTP01 with a name that is no longer relevant, create a new NTP server instance named domaingroupNTP02 to replace the deleted NTP server, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # create ntp domaingroupNTP02
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

Deleting an NTP Server for a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **delete ntp** server-name	Deletes an NTP server instance.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope the date and time policy in the domain group root, delete the NTP server instance domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope the date and time policy in domaingroup01 under the domain group root, delete the NTP server instance domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

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 4: SNMP Security Models and Levels

Model	Level	Authentication	Encryption	What Happens
v1	noAuthNoPriv	Community string	No	Uses a community string match for authentication.

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

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.

Authentication Protocols for SNMPv3 Users

Cisco UCS Central supports the following authentication protocols for SNMPv3 users:

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

AES Privacy Protocol for SNMPv3 Users

Cisco UCS Central uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826. If AES is disabled but privacy password is set, then DES is used for encryption.

If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Central uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Configuring an SNMP Policy

Before You Begin

Before configuring a SNMP policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create snmp**	(Optional) If scoping into a domain group previously, creates the SNMP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope snmp**	(Optional) If scoping into the domain group root previously, scopes the default SNMP policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **enable** | **disable snmp**	Enable or disable SNMP services for this policy.
Step 6	UCSC(policy-mgr) /domain-group/snmp* # **set community** *snmp-community-name-text*	Enter a name for the SNMP community.
Step 7	UCSC(policy-mgr) /domain-group/snmp* # **set syscontact** *syscontact-name-text*	Enter a name for the SNMP system contact.
Step 8	UCSC(policy-mgr) /domain-group/snmp* # **set syslocation** *syslocation-name-text*	Enter a name for the SNMP system location.
Step 9	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, enable SNMP services, set the SNMP community name to SNMPCommunity01, set the SNMP system contact name to SNMPSysAdmin01, set the SNMP system location to SNMPWestCoast01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the Domain Group domaingroup01, create the SNMP policy, enable SNMP services, set the SNMP community name to SNMPCommunity01, set the SNMP system contact name to SNMPSysAdmin01, set the SNMP system location to SNMPWestCoast01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create snmp
UCSC(policy-mgr) /domain-group/snmp* # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, disable SNMP services, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # disable snmp
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

Configuring an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the default SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **create snmp-trap** *snmp-trap-ip*	(Optional) If scoping into a domain group previously, creates the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 5	UCSC(policy-mgr) /domain-group/snmp # **scope snmp-trap** *snmp-trap-ip*	(Optional) If scoping into the domain group root previously, scopes the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 6	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set community** *snmp-trap-community-host-config-string*	Enter the SNMP trap community string to configure the SNMP trap host.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set notificationtype traps**	Enter the notification type for the SNMP trap as SNMP Trap Notifications (traps).
Step 8	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set port** *port-number*	Enter the SNMP trap port number (1-65535).
Step 9	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set v3privilege auth** | **noauth** | **priv**	Enter a V3 Privilege security level for the SNMP trap of authNoPriv Security Level (auth), noAuthNoPriv Security Level (noauth), or authPriv Security Level (priv).
Step 10	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set version v1** | **v2c** | **v3**	Enter a version for the SNMP trap of SNMP v1, v2c, or v3.
Step 11	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, create the SNMP trap with IP address 0.0.0.0, set the SNMP community host string to snmptrap01, set the SNMP notification type to traps, set the SNMP port to 1, set the v3privilege to priv, set the version to v1, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap01
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege priv
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, scope the SNMP trap IP address 0.0.0.0, set the SNMP community host string to snmptrap02, set the SNMP notification type to traps, set the SNMP port to 65535, set the v3privilege to auth, set the version to v2c, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap02
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 65535
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege auth
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v2c
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

Configuring an SNMP User

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **create snmp-user** *snmp-user*	Enter a name for the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set aes-128 yes** | **no**	Use AES-128 for the SNMP user (yes or no).
Step 6	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set auth md5** | **sha**	Use MD5 or Sha authorization mode for the SNMP user.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set password** *password*	Enter and confirm a password for the SNMP user.
Step 8	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set priv-password** *private-password*	Enter and confirm a private password for the SNMP user.
Step 9	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, scope into the SNMP user named snmpuser01, set aes-128 mode to enabled, set authorization to sha mode, set password to userpassword01, set private password to userpassword02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth sha
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
```

```
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, create the SNMP user named snmpuser01, set aes-128 mode to enabled, set authorization to md5 mode, set password to userpassword01, set private password to userpassword02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example shows how to scope into the Domain Group root, scope the SNMP policy, scope into the SNMP user named snmpuser01, set aes-128 mode to disabled, set authorization to md5 mode, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 no
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

Deleting an SNMP Policy

A SNMP policy is deleted from a domain group under the domain group root. SNMP policies under the domain groups root cannot be deleted.

Deleting an SNMP policy will remove all SNMP trap and SNMP User settings within that policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default Management Interfaces Monitoring policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete snmp**	Deletes the SNMP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the SNMP policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete snmp
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the default SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **delete snmp-trap** *snmp-trap-ip*	Deletes the snmp-trap IP address for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, delete the SNMP trap IP address 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, delete the SNMP trap IP address 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an SNMP User

Procedure

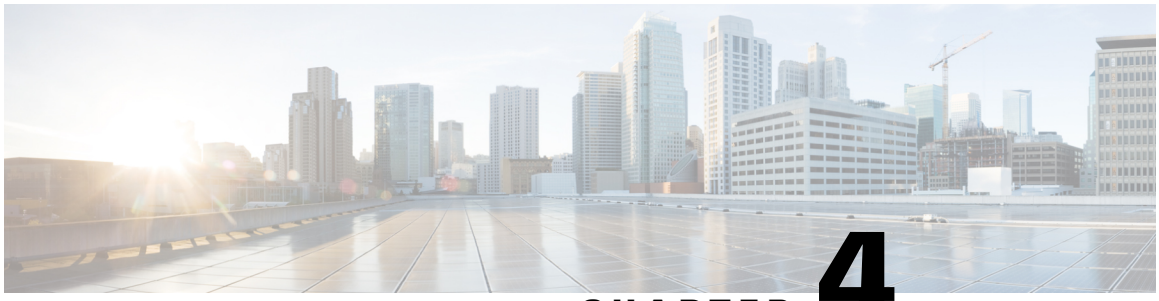
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **delete snmp-user** *snmp-user*	Delete the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, delete the SNMP user named snmpuser01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the Domain Group domaingroup01, scope the SNMP policy, delete the SNMP user named snmpuser02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser02
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```



CHAPTER 4

Domain Management

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.

Creating a Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group**	Enters the domain group root mode.
Step 3	UCSC(policy-mgr) /domain-group # **create domain-group** *12*	Creates the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create domain-group 12
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting a Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group**	Enters the domain group root mode.
Step 3	UCSC(policy-mgr) /domain-group # **delete domain-group** *12*	Deletes the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to delete a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # delete domain-group 12
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Assigning a Domain Group Membership

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.
Step 3	UCSC(resource-mgr) /domain-mgmt # **show ucs-membership** *IP Address*	Displays the membership for the IP address.
Step 4	UCSC(resource-mgr) /domain-mgmt # **scope ucs-membership** *IP Address*	Enters the Cisco UCS domain specified in the IP address.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-membership # **set domain-group** *WORD Domain Group DN*	Specifies the domain group for the IP address.

The following example shows how to assign membership to a Cisco UCS domain:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # show ucs-membership
UCS-Domain Group Membership:
    Mgmt IP          Qualification Type Domain Group DN
    ---------------- ------------------ ---------------
    IP Address     Manual              domaingroup-root
UCSC(resource-mgr) /domain-mgmt # scope ucs-membership IP Address
UCSC(resource-mgr) /domain-mgmt/ucs-membership # set domain-group WORD  Domain Group DN
UCSC(resource-mgr) /domain-mgmt/ucs-membership #
```

Domain Group and Registration Policies

Creating a Domain Group Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **create domain-group** *domain-group-name*	Creates domain group under selected domain group.
Step 4	UCSC(policy-mgr) /org/domain-group # **set qualifier** *qualifier*	(Optional) Specifies domain group to use for qualifying the domain group.
Step 5	UCSC(policy-mgr) /org/domain-group # **commit-buffer**	Commits the transaction to the system configuration.

This following example shows how to create a domain group called dm-gsp1, set the qualifier, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr) /org # create domain group dm-gsp1
UCSC(policy-mgr) /org/domain group* # set qualifier DMGroup1
UCSC(policy-mgr) /org/domain group* # commit-buffer
UCSC(policy-mgr) /org/domain group #
```

Deleting a Domain Group Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete domain-group** *domain-group-name*	Deletes the specified domain group.
Step 4	UCSC(policy-mgr) /org* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a domain group called dm-gsp1, and commits the transaction to the system:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr) /org # delete domain-group dm-gsp1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Creating a Registration Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create registration-policy** *policy-name*	Creates a registration policy.
Step 4	UCSC(policy-mgr) /org/registration-policy # **set descr** *description*	Provides a description for the registration policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation mark will not appear in the description field of any show command output.
Step 5	UCSC(policy-mgr) /org/registration-policy # **create address-qual** *minimum-ip-address maximum-ip-address*	Creates an address qualifier for the registration policy.
Step 6	UCSC(policy-mgr) /org/registration-policy # **create owner-qual**	Creates an owner qualifier for the registration policy.
Step 7	UCSC(policy-mgr) /org/registration-policy # **create site-qual**	Creates a site qualifier for the registration policy.
Step 8	UCSC(policy-mgr) /org/registration-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a registration policy, add an address qualifier, site qualifier, and owner qualifier to the policy, and commit the transaction to the system:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr)/org # create registration-policy RegPol1
UCSC(policy-mgr)/org/registration-policy* # create address-qual 0.0.0.0 1.1.1.1
UCSC(policy-mgr)/org/registration-policy/address-qual* # exit
UCSC(policy-mgr)/org/registration-policy* # create owner-qual TestOwner
UCSC(policy-mgr)/org/registration-policy/owner-qual* # exit
UCSC(policy-mgr)/org/registration-policy* # create site-qual TestSite
UCSC(policy-mgr)/org/registration-policy/site-qual* # commit-buffer
UCSC(policy-mgr)/org/registration-policy/site-qual #
```

ID Range Qualification Policies

ID range qualification policies allow you to create policies and assign them to qualified domain groups and domain IP addresses. The ID range qualification policy is then visible to those domain groups and domain IP addresses. You can also create ID range qualification policies without assigning qualified domain groups or IP addresses. If you do not set qualifiers, the policy is available to all domain groups. ID resolution occurs hierarchically in the organization structure in the same manner as other global policies.

After you create an ID range qualification policy, you can apply it to a block in a new pool or an existing pool.

ID range qualification policies are not automatically pushed from Cisco UCS Central to the Cisco UCS Manager instances in a qualified domain group. If you change a domain group qualifier, a domain group ID, or the IP address of a Cisco UCS Manager domain group in Cisco UCS Central, the reference must be reset in the Cisco UCS Manager local service profile.

Note Global service profiles in Cisco UCS Central do not support ID range qualification policies in this release.

Creating an ID Range Qualification Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create id-range-qual-policy** *policy-name*	Creates an id range qualification policy.
Step 4	UCSC(policy-mgr) /org /id-range-qual-policy # **set descr** *description*	Provides a description for the id range qualification policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation mark will not appear in the description field of any show command output.
Step 5	UCSC(policy-mgr) /org /id-range-qual-policy # **set domaingroup-qual** *qualifier-name domain-group*	Creates the domain group qualifier.
Step 6	UCSC(policy-mgr) /org /id-range-qual-policy/domaingroup-qual # **exit**	Exits domain group qualifier mode.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org /id-range-qual-policy # **set ip-qual** *ip-address*	Creates the IP qualifier.
Step 8	UCSC(policy-mgr) /org /id-range-qual-policy/ip-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an id range qualification policy, set an IP qualifier, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/org # create id-range-qual-policy QualPol1
UCSC(policy-mgr)/org/id-range-qual-policy* # set ip-qual 10.5.5.1
UCSC(policy-mgr)/org/id-range-qual-policy/ip-qual* # commit-buffer
UCSC(policy-mgr)/org/id-range-qual-policy/ip-qual #
```

What to Do Next

Assign the ID range qualification policy to a block.

Deleting an ID Range Qualification Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete id-range-qual-policy** *id-range-qual-policy-name*	Deletes the id range qualification policy.
Step 4	UCSC(policy-mgr) /org* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an ID range qualification policy and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/org# delete id-range-qual-policy QualPolicy1
UCSC(policy-mgr)/org*# commit-buffer
UCSC(policy-mgr)/org#
```

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 a Call Home Policy

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

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create callhome**	If scoping into a domain group previously, creates the Call Home policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group/callhome* # **set contract-id** *contract-id*	Sets the contract ID (numeric and/or text; 0-510 characters).
Step 5	UCSC(policy-mgr) /domain-group/callhome* # **set customer-id** *customer-id*	Sets the customer ID (numeric and/or text; 0-510 characters).
Step 6	UCSC(policy-mgr) /domain-group/callhome* # **set hostname** *smtp-server-address*	Sets the SMTP server address.
Step 7	UCSC(policy-mgr) /domain-group/callhome* # **set phone-contact** *phone-contact*	Sets the phone contact number (e.g., +1-011-408-555-1212).
Step 8	UCSC(policy-mgr) /domain-group/callhome* # **set port** *port*	Sets the port number (1-65535).
Step 9	UCSC(policy-mgr) /domain-group/callhome* # **set site-id** *site-id*	Sets the site ID (numeric and/or text; 0-510 characters).

	Command or Action	Purpose
Step 10	UCSC(policy-mgr) /domain-group/callhome* # **set street-address** *street-address*	Sets the street address (0-255 characters).
Step 11	UCSC(policy-mgr) /domain-group/callhome* # **set switch-priority** *switch-priority*	Sets the switch priority. Parameters available: • alerts • critical • debugging • emergencies • errors • information • notifications • warnings
Step 12	UCSC(policy-mgr) /domain-group/callhome* # **set throttling on** | **off**	Sets throttling to on or off.
Step 13	UCSC(policy-mgr) /domain-group/callhome* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the Call Home policy, configure the Call Home policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create callhome
UCSC(policy-mgr) /domain-group/callhome* # set contract-id contract0995
UCSC(policy-mgr) /domain-group/callhome* # set customer-id customer112
UCSC(policy-mgr) /domain-group/callhome* # set hostname 0.0.0.0
UCSC(policy-mgr) /domain-group/callhome* # set phone-contact +1-011-408-555-1212
UCSC(policy-mgr) /domain-group/callhome* # set port 65535
UCSC(policy-mgr) /domain-group/callhome* # set site-id site15
UCSC(policy-mgr) /domain-group/callhome* # set street-address "75 Main St, Any Town, CA
90000"
UCSC(policy-mgr) /domain-group/callhome* # set switch-priority notifications
UCSC(policy-mgr) /domain-group/callhome* # set throttling on
UCSC(policy-mgr) /domain-group/callhome* # commit-buffer
UCSC(policy-mgr) /domain-group/callhome #
```

What to Do Next

- Configuring a Profile for a Call Home Policy
- Adding Email Recipients to a Call Home Policy
- Configuring a Policy for a Call Home Policy
- Configuring System Inventory for a Call Home Policy

Configuring Email for a Call Home Policy

Before You Begin

- Create a Call Home Policy.
- Before adding email addresses to a profile for a call home policy, this profile must first be created.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope callhome**	Scopes the default Call Home policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/callhome # **set email** *customer-contact-email*	Sets the customer's contact email (using standard email address format)
Step 5	UCSC(policy-mgr) /domain-group/callhome* # **set from-email** *from-email*	Sets the originating or "from" email (using standard email address format)
Step 6	UCSC(policy-mgr) /domain-group/callhome* # **set email** *reply-to-email*	Sets the email to which customer should reply or "reply-to" email (using standard email address format)
Step 7	UCSC(policy-mgr) /domain-group/callhome* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Call Home policy, set the customer's contact email, from email, and reply to email, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope callhome
UCSC(policy-mgr) /domain-group/callhome # set email customer@email.com
UCSC(policy-mgr) /domain-group/callhome # set from-email from@email.com
UCSC(policy-mgr) /domain-group/callhome # set reply-to-email reply-to@email.com
UCSC(policy-mgr) /domain-group/callhome* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting a Call Home Policy

A call home policy is deleted from a domain group under the Domain Group root. Call home policies under the Domain Group root cannot be deleted.

Deleting a call home policy will remove all profiles, policies and system inventory settings within that policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default Call Home policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete callhome**	Deletes the Call Home policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group/callhome* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the Call Home policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete callhome
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring a Profile for a Call Home Policy

Before You Begin

- Create a Call Home Policy.
- Before configuring a profile for a call home policy in a domain group under the Domain Group root, this profile and policy must first be created.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope callhome**	Scopes the default Call Home policy's configuration mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/callhome # **create** | **scope profile** *profile-name*	Creates a Call Home policy profile name and enters profile mode, or scopes an existing Call Home policy's profile mode.
Step 5	UCSC(policy-mgr) /domain-group/callhome/profile* # **set alertgroups** *alert-group*	Sets the profile alert group: • ciscotac • diagnostic • environmental • inventory • license • lifecycle • linecard • supervisor • syslogport • system • test
Step 6	UCSC(policy-mgr) /domain-group/callhome/profile* # **add alertgroups** *alert-group*	(Optional) Adds an additional profile alert group: • ciscotac • diagnostic • environmental • inventory • license • lifecycle • linecard • supervisor • syslogport • system • test **Note** Repeat this step to add additional profile alert groups if required.
Step 7	UCSC(policy-mgr) /domain-group/callhome/profile* # **remove alertgroups** *alert-group*	(Optional) Removes a specific profile alert groups from the buffer:

	Command or Action	Purpose
		• ciscotac • diagnostic • environmental • inventory • license • lifecycle • linecard • supervisor • syslogport • system • test **Note** Repeat this step to remove additional profile alert groups if required.
Step 8	UCSC(policy-mgr) /domain-group/callhome/profile* # **clear alertgroups**	(Optional) Clears all profile alert groups from the buffer.
Step 9	UCSC(policy-mgr) /domain-group/callhome/profile* # **set format** *format*	Sets the format: • fulltxt • shorttxt • xml
Step 10	UCSC(policy-mgr) /domain-group/callhome/profile* # **set level** *level*	Sets the level: • critical • debug • disaster • fatal • major • minor • normal • notification • warning

	Command or Action	Purpose
Step 11	UCSC(policy-mgr) /domain-group/callhome/profile* # **set maxsize** *maximum-size*	Sets the maximum size in megabytes (0-5000000).
Step 12	UCSC(policy-mgr) /domain-group/callhome/profile* # **create** | **delete** | **scope destination** *destination-name* | *destination-email*	Creates, deletes, or scopes the profile destination name or email address.
Step 13	UCSC(policy-mgr) /domain-group/callhome/profile/destination* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Call Home policy, scope the policy profile chprofile01, configure the policy profile, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope callhome
UCSC(policy-mgr) /domain-group/callhome # scope profile chprofile01
UCSC(policy-mgr) /domain-group/callhome/profile # set alertgroups diagnostic
UCSC(policy-mgr) /domain-group/callhome/profile* # add alertgroups lifecycle
UCSC(policy-mgr) /domain-group/callhome/profile* # set level normal
UCSC(policy-mgr) /domain-group/callhome/profile* # set maxsize 5000000
UCSC(policy-mgr) /domain-group/callhome/profile* # create destination destination@cisco.com
UCSC(policy-mgr) /domain-group/callhome/profile/destination* # commit-buffer
UCSC(policy-mgr) /domain-group/callhome/profile/destination #
```

Deleting a Profile for a Call Home Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope callhome**	Scopes the default Call Home policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/callhome # **delete profile** *profile-name*	Deletes a Call Home policy's profile.
Step 5	UCSC(policy-mgr) /domain-group/callhome* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Call Home policy, delete the policy profile chprofile01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope callhome
UCSC(policy-mgr) /domain-group/callhome # delete profile chprofile01
UCSC(policy-mgr) /domain-group/callhome* # commit-buffer
UCSC(policy-mgr) /domain-group/callhome #
```

Configuring a Policy for a Call Home Policy

Before configuring a policy for a call home policy under a domain group, this policy must first be created. Policies for call home policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Call Home Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope callhome**	Scopes the default Call Home policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/callhome # **create** | **scope policy** *policy-name*	Creates a policy for a Call Home policy and enters that policy's mode, or scopes an existing policy for a Call Home policy. Policies for the Call Home policy include: • arp-targets-config-error • association-failed • configuration-failure • connectivity-problem • election-failure • equipment-disabled • equipment-inaccessible • equipment-inoperable • equipment-offline • equipment-problem

	Command or Action	Purpose
		• fru-problem • identity-unestablishable • inventory-failed • license-graceperiod-expired • limit-reached • link-down • management-services-failure • management-services-unresponsive • mgmtif-down • port-failed • power-problem • thermal-problem • version-incompatible • vif-ids-mismatch • voltage-problem
Step 5	UCSC(policy-mgr) /domain-group/callhome/policy* # **enable** | **disable**	Enables or disables the policy for the Call Home policy.
Step 6	UCSC(policy-mgr) /domain-group/callhome/policy* # **set admin-state enabled** | **disabled**	Enables or disables the admin state of the policy for the Call Home policy.
Step 7	UCSC(policy-mgr) /domain-group/callhome/policy* # **exit**	(Optional) Moves up one level to create or scope and configure the next policy for the Call Home policy. Repeating the above three steps until all required policies for the Call Home policy are scoped or created and configured.
Step 8	UCSC(policy-mgr) /domain-group/callhome/profile/destination* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Call Home policy, recursively create policies license-graceperiod-expired and management-services-failure, enable these policies for the Call Home policy, enable the admin-state for each, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope callhome
```

```
UCSC(policy-mgr) /domain-group/callhome # create policy license-graceperiod-expired
UCSC(policy-mgr) /domain-group/callhome/policy* # enable
UCSC(policy-mgr) /domain-group/callhome/policy* # set admin-state enable
UCSC(policy-mgr) /domain-group/callhome/policy* # exit
UCSC(policy-mgr) /domain-group/callhome # create policy management-services-failure
UCSC(policy-mgr) /domain-group/callhome/policy* # enable
UCSC(policy-mgr) /domain-group/callhome/policy* # set admin-state enable
UCSC(policy-mgr) /domain-group/callhome/policy* # commit-buffer
UCSC(policy-mgr) /domain-group/callhome/policy #
```

The following example shows how to scope into the domain group domaingroup01, scope the Call Home policy, recursively scope existing policies connectivity-problem, management-services-unresponsive, and thermal-problem, enable these policies for the Call Home policy, enable the admin-state for each, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope callhome
UCSC(policy-mgr) /domain-group/callhome # scope policy connectivity-problem
UCSC(policy-mgr) /domain-group/callhome/policy # enable
UCSC(policy-mgr) /domain-group/callhome/policy* # set admin-state enable
UCSC(policy-mgr) /domain-group/callhome/policy* # exit
UCSC(policy-mgr) /domain-group/callhome* # scope policy management-services-unresponsive
UCSC(policy-mgr) /domain-group/callhome/policy* # enable
UCSC(policy-mgr) /domain-group/callhome/policy* # set admin-state enable
UCSC(policy-mgr) /domain-group/callhome/policy* # exit
UCSC(policy-mgr) /domain-group/callhome* # scope policy thermal-problem
UCSC(policy-mgr) /domain-group/callhome/policy* # enable
UCSC(policy-mgr) /domain-group/callhome/policy* # set admin-state enable
UCSC(policy-mgr) /domain-group/callhome/policy* # commit-buffer
UCSC(policy-mgr) /domain-group/callhome/policy #
```

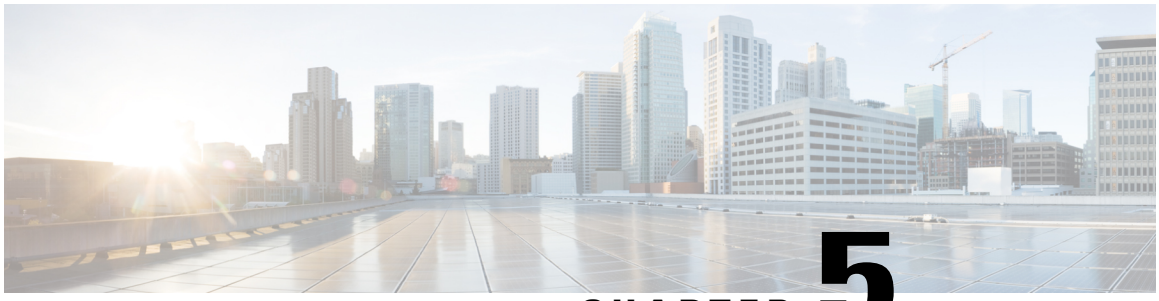
Deleting a Policy for a Call Home Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope callhome**	Scopes the default Call Home policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/callhome # **delete policy** *policy-name*	Deletes a policy for a Call Home policy.
Step 5	UCSC(policy-mgr) /domain-group/callhome* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Call Home policy, delete the policy chpolicy01 from within the Call Home policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope callhome
UCSC(policy-mgr) /domain-group/callhome # delete policy chpolicy01
UCSC(policy-mgr) /domain-group/callhome* # commit-buffer
UCSC(policy-mgr) /domain-group/callhome #
```



CHAPTER 5

Remote Management

This chapter includes the following sections:

Remote Management

Remote management options in Cisco UCS Central enables you to manage the physical devices such as the **Chassis**, **Servers**, **Fabric Interconnect** and **FEX**es in the registered UCS domains from both Cisco UCS Central GUI and CLI.

Important

- If you want to perform any of the remote management operation in the registered UCS domains, make sure the remote operation feature is enabled in the UCS domains.
- When you perform any of these remote operations, Cisco UCS Central initiates a configuration request to the UCS domain. This might take about 30 seconds. Make sure to wait for 30 seconds before you check for the changes based on your remote operation.

Using remote management capability you can do the following:

- **Acknowledge**, **Decommission**, and **Recommission** chassis.
- Perform **Server Maintenance** tasks such as **Decommission**, **Recommission**, **Remove** and **Re-acknowledge** blade and rack-mount servers.
- **Launch KVM Console**, **Boot up**, **Shutdown**, **Reset**, **Recover**, and perform diagnostic interrupt on Fabric Extenders (FEX), blade, and rack-mount servers.
- Turn on/off Locator LED for chassis, blade and rack-mount servers, Fabric Interconnects (FI) and FEXes.
- Create and download **Tech Support Files** from the registered UCS domains.

If the servers are associated to a local or global service profile, you can do the following remote management actions on the associated server from the service profiles:

- **Launch KVM Console**, **Boot up**, **Shutdown**, **Reset**, and **Recover** blade and rack-mount servers for blade and rack servers associated with Global Service Profiles.
- **Launch KVM Console**, **Boot up**, **Shutdown**, **Reset**, and **Recover** blade and rack-mount servers blade and rack servers associated with Local Service Profiles.

Important Make sure you are aware of the guidelines and recommendation to manage the physical devices in the registered Cisco UCS domains. For specific guidelines on physical device operations and server maintenance, see the following sections **Managing the Chassis**, **Managing Blade Servers**, **Managing Rack-Mount Servers** and **Managing I/O Modules** in Cisco UCS Manager GUI and CLI Configuration guides:
http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Recommission a Server

You can recommission a blade server or rack-mount server from the UCS domain.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **recommission** *server 1/2*	Initiates the process to recommission the server from specified domain.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction.

The following example shows recommissioning server 2 in chassis 1 from the UCS domain:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # recommission server 1/2
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Decommissioning a Server

You can decommission a blade server or rack-mount server from the UCS domain.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **decommission** *server 1/2*	Initiates the process to recommission the server from specified domain.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction.

The following example shows decommissioning server 2 in chassis 1 from the UCS domain:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # decommission server 1/2
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Removing a Server

You can remove a blade server or rack-mount server from the UCS domain.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **remove** *server 1/2*	Initiates the process to remove the server from specified domain.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # remove server 1/2
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Resetting a Server CIMC

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope chassis** *chassis number*	Enters the specified chassis.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # **scope server***server number*	Enters the specified server.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # reset-cimc	Rests server CIMC.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # commit-buffer	Commits the transaction.

The following example resets the CIMC for server 2 in chassis 1.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope chassis 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # scope server 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # reset-cimc
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server #
```

Resetting Server CMOS

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope chassis** *chassis number*	Enters the specified chassis.

	Command or Action	Purpose
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # **scope server** *server number*	Enters the specified server.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # **reset-cmos**	Rests CMOS.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # **commit-buffer**	Commits the transaction.

The following example resets the CMOS for server 2 in chassis 1.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope chassis 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # scope server 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # reset-cmos
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server #
```

Resetting a Server IPMI

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope chassis** *chassis number*	Enters the specified chassis.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # **scope server***server number*	Enters the specified server.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # **reset-ipmi**	Rests server IPMI to factory default.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # **commit-buffer**	Commits the transaction.

The following example resets the IPMI to factory default for server 2 in chassis 1.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
```

```
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope chassis 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # scope server 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # reset-ipmi
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server #
```

Resetting a Server KVM

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope chassis** *chassis number*	Enters the specified chassis.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # **scope server** *server number*	Enters the specified server.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # **reset-kvm**	Rests KVM and clears all sessions..
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # **commit-buffer**	Commits the transaction.

The following example resets the KVM and clears all sessions from server 2 in chassis 1.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope chassis 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # scope server 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # reset-kvm
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server #
```

Turning on/off Server Locator LED

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.

	Command or Action	Purpose
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope chassis** *chassis number*	Enters the specified chassis.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # **scope server** *server number*	Enters the specified server.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # **enable I disable locator-led**	Turns on or turns off the locator LED based on your command.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # **commit-buffer**	Commits the transaction.

The following example shows turning the locator LED on and off for server 2 in chassis 1.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope chassis 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # scope server 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # enable locator-led
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # disable locator-led
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server #
```

Acknowledging a Chassis

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **acknowledge** *chassis 7*	Initiated acknowledgment for the specified chassis.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction to the system.

The following example acknowledges chassis 7 and commits transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # acknowledge chassis 7
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Decommissioning a Chassis

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **decommission** *chassis 7*	Initiated recommission for the specified chassis.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction to the system.

The following example initiates decommission for chassis 7 and commits transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # decommision chassis 7
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Recommissioning a Chassis

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **recommission** *chassis 7*	Initiated recommission for the specified chassis.

	Command or Action	Purpose
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction to the system.

The following example initiates the recommission for chassis 7 and commits transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # recommision chassis 7
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Turning on or off the Chassis Locator LED

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope chassis** *chassis number*	Enters the specified chassis.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # **enable I disable locator-led**	Based the enable or disable command you enter, either enables or disables the locator LED.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to turn on or off the locator LED and commits transaction:

```
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope chassis chassis number
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # enable locator-led
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # disable locator-led
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis #
```

Acknowledging a Fabric Extender

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **acknowledge** *fex 7*	Initiated acknowledgment for the specified fabric extender.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction to the system.

The following example acknowledges fabric extender 7 and commits transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # acknowledge fex 7
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Decommissioning a Fabric Extender

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **decommission** *fex 7*	Initiated decommission for the specified fabric extender.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction to the system.

The following example initiates decommission for fabric extender 7 and commits transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
```

```
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # decommision fex 7
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Recommissioning a Fabric Extender

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **recommission** *fex 7*	Initiated recommission for the specified fabric extender.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction to the system.

The following example initiates the recommission for fabric extender 7 and commits transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # recommision fex 7
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Removing a Fabric Extender

You can remove a fabric extender from the UCS domain.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **remove** *fex 1/2*	Initiates the process to remove the fabric extender from specified domain.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction.

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # remove fex 1/2
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Turning on of off Fabric Extender Locator LED

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **scope fex** *fex number*	Enters the specified fabric extender.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fex # **enable I disable locator-led**	Based the enable or disable command you enter, either enables or disables the locator LED.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fex* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to turn on or off the locator LED and commits transaction:

```
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fex fex number
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # enable locator-led
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # disable locator-led
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis #
```

Remote Tech Support for UCS Domains

You can collect tech support files for registered UCS domains from Cisco UCS Central. Collecting remote tech support includes the following:

- **Create tech support files**: You can create tech support files for each registered UCS domains using both Cisco UCS Central GUI and CLI.
- **Download created 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.

Creating a Tech Support File for a UCS Domain

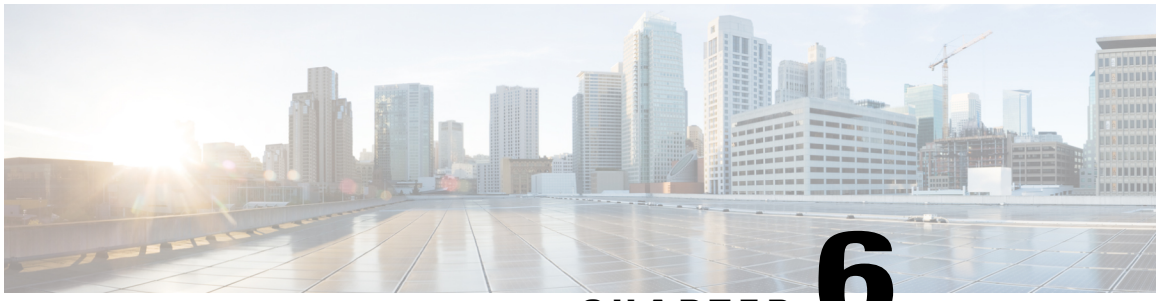
From the registered Cisco UCS domains, you can collect a full set of tech support files for options corresponding to "ucsm" in Cisco UCS Manager.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope domain-mgmt**	Enters domain management.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *domain name*	Enters the specified domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain # **show techsupport ucsm detail**	Initiates creating the tech support file for this domain.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a tech support file for a UCS domain:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain-name
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show techsupport ucsm detail
UCSC(resource-mgr) /domain-mgmt/ucs-domain* # commit-buffer
```



CHAPTER 6

Firmware Management

This chapter includes the following sections:

Downloading Firmware

Firmware Download from Cisco

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

Important Make sure you do the following to download firmware from Cisco into Cisco UCS Central.

- You must enable Cisco UCS Central to access Cisco.com either directly or using a proxy server.
- You must configure valid Cisco user credentials and enable download state in Cisco UCS Central.

Firmware Library of Images

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

The source for images downloaded from Cisco.com is Cisco and for images downloaded from local or remote file system is local. These firmware images are available for creating firmware policies.

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

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

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

Configuring Firmware Image Download from Cisco

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **connect policy-mgr**	Enters policy manager mode from operations manager mode.
Step 3	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 4	UCSC(policy-mgr) /domain-group # **scope download-policy cisco**	Enters the configuration mode.
Step 5	UCSC(policy-mgr) /domain-group/download-policy # **set**	**1** **set admin-state** **2** **set downloadinterval**dayweekon-demand **3** **set http-proxy***server:port* **4** **username***username* **5** **set password***password* **6** **set proxy-password***password* **7** **set proxy-username***username* Enters the configuration details to the system.
Step 6	UCSC(policy-mgr) /domain-group/download-policy/set # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure firmware download to Cisco UCS Central from Cisco:

```
UCSC# (ops-mgr)# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope download-policy cisco
UCSC(policy-mgr) /domain-group/download-policy # set
admin-state  enable
downloadinterval 1 day
http-proxy  Server[:Port]
username          Username
password          Password
proxy-password    HTTP Proxy Password
proxy-username    HTTP Proxy Username
UCSC(policy-mgr) /domain-group/download-policy # commit-buffer
UCSC(policy-mgr) /domain-group/download-policy* #
```

Downloading Firmware Image from Cisco

Procedure

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

The following example shows how to download the actual firmware image from Cisco.com to Cisco UCS Central:

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

Viewing Image Download Status

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.

	Command or Action	Purpose
Step 3	UCSC (ops-mgr)/firmware# **show download-task detail**	Displays the details of the download task.

The following example shows how to view the download task details in Cisco UCS Central:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # show download-task detail
Download task:
File Name: ucs-catalog.2.1.0.475.T.bin
Protocol: Ftp
Server:
Userid: User
Path: /automation/delmar/catalog
Downloaded Image Size (KB): 0
Image Url:
Image Url:
Proxy Userid:
State: Downloaded
Owner: Management
Current Task:
```

Viewing Downloaded Firmware Image Bundles

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC(ops-mgr) /firmware # **show package**	Displays the downloaded firmware image bundles. You can view the Cisco UCS Manager and Cisco UCS Central bundles.

The following example shows how to view the downloaded firmware image bundles in Cisco UCS Central:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # show package
Name                                     Version    Download Status
---------------------------------------- ---------- ---------------
ucs-catalog.2.1.0.489.T.gbin             2.1(0.489)T Downloaded
ucs-k9-bundle-b-series.2.1.0.489.B.gbin  2.1(0.489)B Downloaded
ucs-k9-bundle-infra.2.1.0.489.A.gbin     2.1(0.489)A Downloaded
ucsCENTRAL-bundle.1.0.0.361.bin          1.0(0.361) Downloaded
update.bin                               1.0(0.376) Downloaded
UCSC(ops-mgr) /firmware #
```

Configuring Firmware Image Download from a Remote File System

You can download firmware image from one of the following remote file systems:

- ftp
- scp
- sftp
- tftp

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope firmware**	Enters the firmware management mode.
Step 3	UCSC (ops-mgr)/firmware# **download image**ftpscpsftptftp*image file location*	Enters firmware image download configuration and mode and specifies the remote location for firmware image.
Step 4	UCSC(ops-mgr) /firmware # download image ftp: image file location /**Password:**	Authenticates access to the remote file system.

The following example shows how to configure firmware download to Cisco UCS Central from a remote file system:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope firmware
UCSC(ops-mgr) /firmware # download image ftp:  Enter URL ftp:[//[username@]server][/path]
UCSC(ops-mgr) /firmware # download image ftp://image download path/Password:
UCSC(ops-mgr) /firmware #
```

Deleting Image Metadata from the Library of Images

Procedure

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

	Command or Action	Purpose
Step 4	UCSC(ops-mgr) /firmware/download-source# **purge list**	Deletes the firmware images metadata from the library of images.

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

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

Upgrading Firmware in Cisco UCS Domains

Firmware Upgrades for Cisco UCS Domains

You can deploy infrastructure and server firmware upgrades for registered Cisco UCS domains from Cisco UCS Central.

If desired, you can upgrade the Cisco UCS domains in each domain group with different versions of firmware. Cisco UCS Central also provides you the option to acknowledge the fabric interconnect reboot globally from Cisco UCS Central or individually from each Cisco UCS domain.

Configuring an Infrastructure Firmware Policy Upgrade

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope fw-infra-pack** *name*	Enters the infrastructure firmware policy mode in the domain group.
Step 4	UCSC(policy-mgr) /domain-group/fw-infra-pack # **set** *infrabundleversion*	Specifies the infrastructure policy version for the update.
Step 5	UCSC(policy-mgr) /domain-group/fw-infra-pack # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure an infrastructure firmware policy update for a domain group from Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope fw-infra-pack default
UCSC(policy-mgr) /domain-group/fw-infra-pack # set infrabundleversion 2.1(0.475)T
UCSC(policy-mgr) /domain-group/fw-infra-pack* # commit-buffer
UCSC(policy-mgr) /domain-group/fw-infra-pack #
```

Acknowledging a Pending Activity

This procedure describes the process to acknowledge an fabric interconnect reboot pending activity from Cisco UCS Central CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope domain-group** *Marketing*	Enters the domain group.
Step 3	UCSC(ops-mgr) /domain-group # **scope schedule fi-reboot**	Enters the scheduled task mode.
Step 4	UCSC(ops-mgr) /domain-group/schedule # **show token-request**	Displays the pending activities in the system.
Step 5	UCSC(ops-mgr) /domain-group/schedule # **scope token-request id sys-fw-system-ack**	Finds the pending activity.
Step 6	UCSC(ops-mgr) /domain-group/schedule/token-request # **acknowledge token-request**	Acknowledges the specified pending activity.
Step 7	UCSC(ops-mgr) /domain-group/schedule/token-request* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to acknowledge a pending activity in Cisco UCS Central CLI:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope domain-group Marketing
UCSC(ops-mgr) /domain-group # scope schedule fi-reboot
UCSC(ops-mgr) /domain-group/schedule # show token-request
Token Request:
ID    Name        Client IP       Admin State     Oper State
----- ----------- --------------- --------------- ----------
1033 sys-fw-system-ack 10.193.23.150   Auto Scheduled  Pending Ack
UCSC(ops-mgr) /domain-group/schedule # scope token-request id sys-fw-system-ack
UCSC(ops-mgr) /domain-group/schedule/token-request # acknowledge token-request
UCSC(ops-mgr) /domain-group/schedule/token-request* # commit-buffer
UCSC(ops-mgr) /domain-group/schedule/token-request #
```

Viewing Infrastructure Firmware Packages

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope fw-infra-pack** *name*	Enters the infrastructure firmware policy mode in the domain group.
Step 4	UCSC(policy-mgr) /domain-group/fw-infra-pack #**show**	Displays the infrastructure firmware packages available in the system.

The following example shows how to view the available infrastructure packages using Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope fw-infra-pack default
UCSC(policy-mgr) /domain-group/fw-infra-pack # show
Infra Pack:
Name                  Mode     Infra Bundle Version
--------------------- -------- --------------------
root/default          Staged   2.1(0.480)A
UCSC(policy-mgr) /domain-group/fw-infra-pack #
```

Creating a Host Firmware Package

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create fw-host-pack***policy name*	Creates the specified host firmware pack.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/fw-host-pack* # **set descr** *description*	Specifies the description for the host firmware policy.
Step 5	UCSC(policy-mgr) /domain-group/fw-host-pack* # **set bladebundleversion** *version number*	Specifies the blade server bundle version for the host firmware policy.
Step 6	UCSC(policy-mgr) /domain-group/fw-host-pack* # **set rackbundleversion** *version number*	Specifies the rack server bundle version for the host firmware policy.
Step 7	UCSC(policy-mgr) /domain-group/fw-host-pack* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a host firmware pack in Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create fw-host-pack Policy name
UCSC(policy-mgr) /domain-group/fw-host-pack* # set
bladebundleversion
descr
rackbundleversion
UCSC(policy-mgr) /domain-group/fw-host-pack* # commit-buffer
UCSC(policy-mgr) /domain-group/fw-host-pack* #
```

Viewing Host Firmware Packages

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **show fw-host-pack detail**	Displays a list of host firmware packages.

The following example shows how to display available host firmware packages in Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # show fw-host-pack detail
Compute Host Pack:

Name: root/Default
```

```
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: UCSC

Name: root/default
Mode: Staged
Blade Bundle Version: 2.1(0.474)B
Rack Bundle Version: 2.1(0.474)C
Description: default from UCSC

Name: root/latest
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: latest

Name: root/Marketing/mytest
Mode: Staged
Blade Bundle Version: 2.1(0.469)B
Rack Bundle Version: 2.1(0.469)C
Description: Test
UCSC(policy-mgr) /domain-group #
```

Scheduling Firmware Upgrades

Firmware Upgrade Schedules

To upgrade firmware by domain groups in registered Cisco UCS domains, you can schedule upgrades from Cisco UCS Central in the following ways:

- As a one time occurrence
- As a recurring occurrence that recurs at designated intervals

If you configure the schedules for user acknowledgment, the fabric interconnect will not reboot without explicit acknowledgment.

Creating a One Time Occurrence Schedule

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create schedule onetime**	Creates a one time occurrence schedule.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/schedule* # **set admin-state user-ack**	Specifies user acknowledgment for the specified one time update task.
Step 5	UCSC(policy-mgr) /domain-group/schedule # **create occurrence one-time** *name*	Specifies the time for one time occurrence.
Step 6	UCSC(policy-mgr) /domain-group/schedule/one-time* # **set**	**1** **concur-tasks***Maximum number of concurrent tasks* **2** **date***Start Date* **3** **max-duration***Max Duration (dd:hh:mm:ss)* **4** **min-interval***Minimum Interval Between Tasks Execution* **5** **proc-cap***Maximum Number of Tasks to Execute* Sets other related details for one time occurrence.
Step 7	UCSC(policy-mgr) /domain-group/schedule/one-time* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to schedule a one time occurrence firmware update in Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create schedule onetime
UCSC(policy-mgr) /domain-group/schedule* # set admin-state user-ack
UCSC(policy-mgr) /domain-group/schedule* # commit-buffer
UCSC(policy-mgr) /domain-group/schedule # create occurrence one-time Nov172012
UCSC(policy-mgr) /domain-group/schedule/one-time* # set
concur-tasks  Maximum Number of Concurrent Tasks
date          Start Date
max-duration  Max Duration (dd:hh:mm:ss)
min-interval  Minimum Interval Between Tasks Execution
proc-cap      Maximum Number of Tasks to Execute
UCSC(policy-mgr) /domain-group/schedule/one-time* # set date nov 17 2012 16 00 00
UCSC(policy-mgr) /domain-group/schedule/one-time* # commit-buffer
UCSC(policy-mgr) /domain-group/schedule/one-time* #
```

Viewing One Time Occurrence Schedule

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group/schedule* # **scope schedule one-time**	Enters the schedule mode.
Step 4	UCSC(policy-mgr) /domain-group/schedule/one-time # **show detail**	Displays the one-time schedule.

The following example shows how to display the scheduled one time occurrence in Cisco UCS Central CLI:

```
UCSC#connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope schedule onetime
UCSC(policy-mgr) /domain-group/schedule/one-time # show detail
One-Time Occurrence:
Name: Friday
Start Date: 2012-11-17T16:00:00.000
Max Duration (dd:hh:mm:ss): None
Max Concur Tasks: Unlimited
Max Tasks: Unlimited
Min Interval (dd:hh:mm:ss): None
Executed Tasks: 0
UCSC(policy-mgr) /domain-group/schedule/one-time #
```

Managing Capability Catalog

Capability Catalog

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

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

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

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

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

Hardware-Specific Rules

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

User Display Strings

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

Updates to the Capability Catalog

Capability Catalog updates are included in each Cisco UCS Infrastructure Software Bundle. Unless otherwise instructed by Cisco TAC, you only need to activate the Capability Catalog update after you've downloaded, updated, and activated a Cisco UCS Infrastructure Software Bundle.

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

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

Note The Capability Catalog version is determined by the version of Cisco UCS that you are using. For example, Cisco UCS 2.0 releases work with any 2.0 release of the Capability Catalog, but not with 1.0 releases of the Capability Catalog. For information about Capability Catalog releases supported by specific Cisco UCS releases, see the *Release Notes for Cisco UCS Software* accessible through the *Cisco UCS B-Series Servers Documentation Roadmap* available at the following URL: http://www.cisco.com/go/unifiedcomputing/b-series-doc.

Configuring a Capability Catalog Upgrade

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr)/domain-group# **scope fw-catalog-pack**	Enters the capability catalog packages mode.
Step 4	UCSC(policy-mgr) /domain-group/fw-catalog-pack # **set catalogversion 2.1(0.475)T**	Specifies the capability catalog version for this update.
Step 5	UCSC(policy-mgr) /domain-group/fw-catalog-pack* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure a capability catalog update for a domain group from Cisco UCS Central:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # fw-catalog-pack
UCSC(policy-mgr) /domain-group/fw-catalog-pack # set catalogversion 2.1(0.475)T
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group* #
```

Viewing a Capability Catalog in a Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr)/domain-group# **scope fw-catalog-pack***default*	Enters the capability catalog packages mode.
Step 4	UCSC(policy-mgr) /domain-group/fw-catalog-pack # **show detail**	Specifies the capability catalog version for this update.

The following example shows how to view the capability catalog in a domain group from Cisco UCS Central CLI:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # fw-catalog-pack default
UCSC(policy-mgr) /domain-group/fw-catalog-pack # show detail
Catalog Pack:
Name: root/default
Mode: Staged
Catalog Version: 2.1(0.468)T
Description: default
UCSC(policy-mgr) /domain-group* #
```

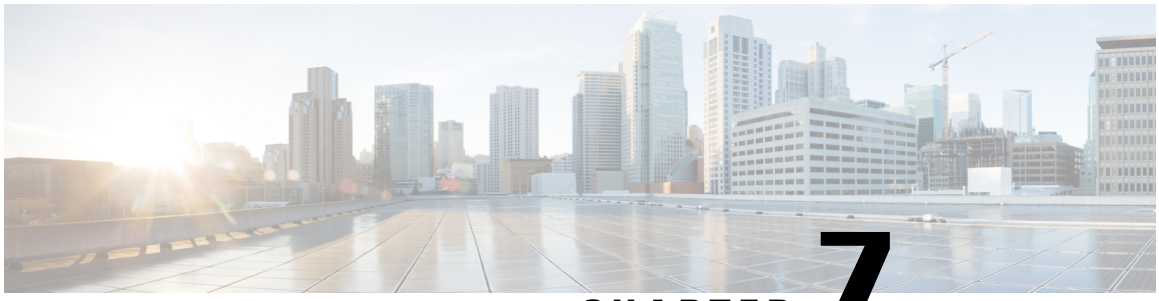
Deleting a Capability Catalog Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete fw-catalog-pack***name*	Deletes the specified catalog policy from the domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to delete a capability catalog policy from a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # delete fw-catalog-pack default
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group* #
```



CHAPTER 7

Monitoring Inventory

This chapter includes the following sections:

Inventory Management

Cisco UCS Central collects the inventory details from all registered Cisco UCS domains. You can view and monitor the components in the registered Cisco UCS domains from the domain management panel.

When a Cisco UCS domain is successfully registered, Cisco UCS Central starts collecting the following details:

- Physical Inventory
- Service profiles and service profile templates
- Fault information

The default data collection interval is 10 minutes. You can customize the interval based on your requirements. If the connection between Cisco UCS domain and Cisco UCS Central fails, whenever the disconnected Cisco UCS domain is detected again, Cisco UCS Central start collecting current data and displays in the domain management panel.

The **General** tab in **Domain Management** panel, displays a list of registered Cisco UCS domains. You can click on the tabs to view details on each component. You can also launch the individual Cisco UCS Manager or the KVM console for a server from this panel.

Physical Inventory

The physical inventory details of the components in Cisco UCS domains are organized under domains. The Cisco UCS domains that do not belong to any domain groups are placed under ungrouped domains. You can view detailed equipment status, and the following physical details of components in the domain management panel:

- Fabric interconnects - switch card modules
- Servers - blades/rack mount servers
- Chassis - io modules
- Fabric extenders

Service Profiles and Templates

You can view a complete list of service profiles and service profile templates available in the registered Cisco UCS domains from the **Servers** tab. The **Service Profile** panel displays a aggregated list of the service profiles. Service profiles with the same name are grouped under the organizations they are assigned to. Instance count next to the service profile name will provide the number of times that particular service profile is used in Cisco UCS domains.

From the **Service Profile Template** panel, you can view the available service profile templates, organization and the number of times each service profile template is used in the Cisco UCS Domain.

Viewing Inventory Details for a UCS Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 4	UCSC(resource-mgr)/domain-mgmt/UCS domain # **show detail**.	Displays a list of all equipments in the specified UCS domain.

The following example shows how to view the details of a registered Cisco UCS Domain from Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show detail
UCS System:
    ID: 1006
    Name: doc-mammoth96
    Total Servers: 6
    Free Servers: 0
    Owner:
    Site:
    Description:
    Fault Status: 1407460783489057
    Current Task:
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Viewing Inventory Details of a Server

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 4	UCS(resource-mgr) /domain-mgmt /ucs-domain # **chassis 1**	Enters the chassis mode
Step 5	UCS(resource-mgr) /domain-mgmt /ucs-domain /chassis # **server 1**	Enters the server mode
Step 6	UCS(resource-mgr) /domain-mgmt /ucs-domain /chassis /server # **show inventory**	Displays inventory details of a server.

The following example shows how to view inventory details of a server within a chassis:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope doamin-mgmt
UCSC(resource-mgr)/doamin-mgmt# scope ucs-domain 1007
UCSC(resource-mgr)/doamin-mgmt/ucs-domain# scope chassis 1
UCSC(resource-mgr)/doamin-mgmt/ucs-domain/chassis# scope server 1
UCSC(resource-mgr)/doamin-mgmt/ucs-domain/chassis/server# show inventory
Server 1/1:
    Name:
    User Defined Description:
    Acknowledged Product Name: Cisco UCS B200 M1
    Acknowledged PID: N20-B6620-1
    Acknowledged VID: V01
    Acknowledged Serial (SN): QCI1415A3Q7
    Acknowledged Memory (MB): 8192
    Acknowledged Effective Memory (MB): 8192
    Acknowledged Cores: 8
    Acknowledged Adapters: 1
UCSC(resource-mgr)/doamin-mgmt/ucs-domain/chassis/server#
```

Viewing Local Service Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org** *org-name*	Enters the organizations mode for the specified organization. To enter the root mode type/ as the*org-name*.
Step 3	UCSC(resource-mgr) /org # scope local-service-profile **local-service-profile_name**	Enters the specified local service profile.
Step 4	UCSC(resource-mgr) /org /local-service-profile # **show instance**	Displays information of the instance in the specified local service profile.

The following example shows how to view local service profile named localSP2:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr)/org# scope local-service-profile localSP2
UCSC(resource-mgr)/org/local-service-profile# show instance
Compute Instance:
    ID      Name         Status        Assoc State   Config State    Physical Ref
    ----- ---------- --------------- ------------   ------------   ------------
    1007   samc02     Config Failure   Unassociated   Failed         localSP2/1007
UCSC(resource-mgr) /org/local-service-profile #
```

Viewing Organization Details

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode type/ as the *org-name*.
Step 3	UCSC(resource-mgr) /org # **show org**	Displays details of an organization.

The following example shows how to view root organization details:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr)/org # show org
Organizations:
```

```
    Name
    ----
    /org1
UCSC(resource-mgr)/org #
```

Viewing Chassis Information

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 4	UCSC(resource-mgr)/domain-mgmt/UCS domain # **show chassis**.	Displays a list of chassis in the specified UCS domain.

The following example shows how to view the chassis information in a registered Cisco UCS Domain from Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show chassis
UCS System chassis:
    Chassis Id Model      Status                  Operability
    ---------- ---------- ----------------------- -----------
             1 N20-C6508  Inoperable              Operable
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Viewing Fabric Interconnects

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 4	UCSC(resource-mgr)/domain-mgmt/UCS domain # **show fabric-interconnect**.	Displays a list of fabric-interconnect in the specified UCS domain.

The following example shows how to view the fabric interconnects in a registered Cisco UCS Domain from Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show fabric-interconnect
ID Operability IP Address      Model      Serial
-- ----------- --------------- ---------- ------
A  Operable    10.193.66.180   UCS-FI-6296UP FOX1512G07K
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Viewing Fabric Extenders

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 4	UCSC(resource-mgr)/domain-mgmt/UCS domain # **show fex**.	Displays a list of fabric extenders in the specified UCS domain.

The following example shows how to view the fabric extenders in a registered Cisco UCS domain from Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show fex
UCS System Fabric-extender:
     Fex Id     Model      Status                     Operability
     ---------- ---------- -------------------------- -----------
             2 N2K-C2232PP-10GE
                           Accessibility Problem    N/A

UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

Viewing Servers

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.

	Command or Action	Purpose
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 4	UCSC(resource-mgr)/domain-mgmt/UCS domain # **show server**.	Displays a list of servers in the specified UCS domain.

The following example shows how to view the rack servers in a registered Cisco UCS Domain from Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show server
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

To view the blade servers, you have to scope into the chassis:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope chassis 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # show server
Blade Server in a UCS Chassis:
    Chassis Id Slot Id Status Cores  Memory (MB)    LS Ref
    ---------- ------- ------ ------ -------------- ------
    1                1 Inoperable
                                  12         131072
    1                2 Ok           8           6144
org-root/req-BIOS-2/inst-100
6
    1                3 Discovery
                                   0              0
    1                5 Ok           8          24576
org-root/req-BIOS-5/inst-100
6
    1                6 Ok           8          12288
org-root/req-BIOS-6/inst-100
6
    1                7 Ok          32          32768
org-root/org-LisasOrg/req-Li
sasOrg_SPClone/inst-1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis #
```

Viewing FSM Operation Status

Procedure

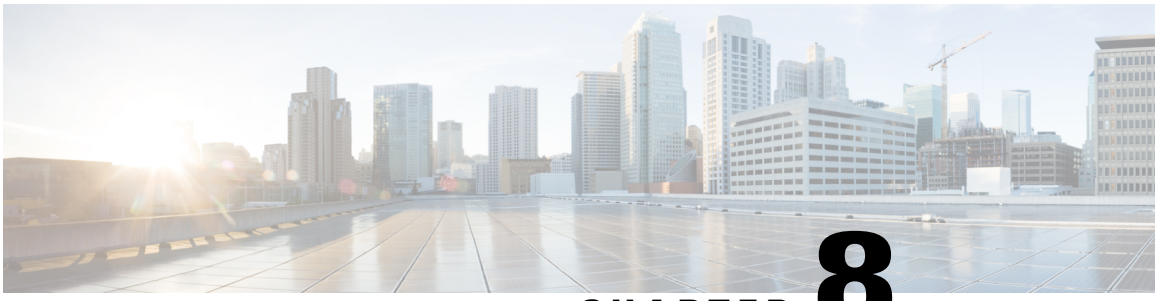
	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-mgmt**	Enters the UCS domains.

	Command or Action	Purpose
Step 3	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 4	UCSC(resource-mgr)/domain-mgmt/UCS domain # **show fsm status**.	Displays the fsm operation status for the specified UCS domain.

The following example shows how to view the FSM operation status in a registered Cisco UCS Domain from Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1006
UCSC(resource-mgr) /domain-mgmt/ucs-domain # show fsm status

ID: 1006
    FSM 1:
        Status: 0
        Previous Status: 0
        Timestamp: Never
        Try: 0
        Progress (%): 100
        Current Task:
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```



CHAPTER 8

Managing Backup and Restore

This chapter includes the following sections:

Backup and Import in Cisco UCS Central

Cisco UCS Central enables you to backup and restore Cisco UCS Central itself and the registered UCS domains. You can schedule backup and restore policy or, you can perform an immediate backup operation. There are two types of scheduled and immediate backup operations:

You can schedule the following backup policies separately for both Cisco UCS Central and Cisco UCS domains:

- **Full state backup policy**: Backs up database.
- **Config all export policy**: Backs up the configuration in XML format.

For a UCS domains, these policies can either be defined locally or defined in Cisco UCS Central

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. 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 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.
- Config-all, config-logical and config-system type backups are only supported in Cisco UCS Central on demand back up.

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.

Restoring Configuration

You can use the saved configuration from backup repository to restore and configure any of the managed Cisco UCS domain. Make sure to use full-state backup for recovery situations. Use TFTP protocol to access the backup configurations. You can use both Cisco UCS Central GUI or CLI to copy the backup file URL and use it to configure a new domain.

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.

Backup Types

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

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

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

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

- **config-system—** System configuration back up is an XML file that includes statistics configuration and scheduler information. You can use the file generated from this backup to import these configuration settings. You cannot use this file for a full state system restore during installation.

Enabling Backup in Cisco UCS Central

By default the backup operation is disabled. You much enable the backup policy for Cisco UCS Central back up and Cisco UCS Domains backup to automatically backup the database or system configuration.

Note This procedure describes the process to enable Cisco UCS Domains backup. You will do the same for Cisco UCS Central from policy-mgr > device-profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters system mode.
Step 3	UCSC(ops-mgr) /system # **scope backup** *hostname*	Enters system backup mode for the specified hostname.
Step 4	UCSC(ops-mgr) /system/backup # **enable**	Enables the backup operation. **Note** For backup operations using FTP, SCP, SFTP, you are prompted for the password. Enter the password before committing the transaction.
Step 5	UCSC(ops-mgr) /system/backup # **commit-buffer**	Commits the transaction.

The following example shows how to enable a backup operation named host35, enter the password for the SCP protocol, and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # scope backup host35
UCSC(ops-mgr) /system/backup # enable
Password:
UCSC(ops-mgr) /system/backup* # commit-buffer
UCSC(ops-mgr) /system/backup #
```

The following example shows how to enable backup for Cisco UCS Central:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope device-profile
UCSC(policy-mgr) /device-profile#  scope backup-policy cfg default
UCSC(policy-mgr) /device-profile/cfg # set admin state enable
UCSC(policy-mgr) /device-profile/cfg* # commit-buffer
UCSC(policy-mgr) /device-profile/cfg#
```

Backing up and Restoring Cisco UCS Central

You can back up Cisco UCS Central database or configuration using scheduled backup policies and on creating on demand backup of the system. The following are two types of scheduled backup policies for Cisco UCS Central from the **Administration** tab:

- **Full-State Backup Policy**: This policy backs up complete Cisco UCS Central database based on the specified schedule. You can store the backup image file either in a local system or on a remote location using protocols such as SCP, SFTP, FTP, and TFTP. The full state backup retains the management interfaces in the complete state.
- **Config-All Export Policy**: The config-all export policy backs up only the system configuration in XML format.

You can also create an on demand backup for Cisco UCS Central at anytime from the **Operations Management** > **Backup and Import** > **UCS Central** > **Create System Backup**.

Creating an On Demand Backup for Cisco UCS Central

Before You Begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters the system mode.
Step 3	UCSC(ops-mgr) /system # **create backup** *URL backup-type* {**disabled** | **enabled**}	Creates a backup operation. Specify the *URL* for the backup file using one of the following syntax: • **ftp:**// *username@hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* **Note** Full-state backup files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect. You can save multiple backup operations, but only one operation for each hostname is saved. If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation

	Command or Action	Purpose
		will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.
Step 4	UCSC(ops-mgr) /system # **commit-buffer**	Commits the transaction.

The following example shows how to create a full-state backup operation for hostname host35 and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system* # create backup scp://user@host35/backups/fullstate.tgz disabled
Password:
UCSC(ops-mgr) /system* # commit-buffer
UCSC(ops-mgr) /system # show fsm status
```

Creating a Config-All Export Policy for Cisco UCS Central

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org**	Enters org mode.
Step 3	UCSC(policy-mgr)/prg # **scope device-profile**	Enters device profile mode.
Step 4	UCSC(policy-mgr) /org/device-profile # **create backup-policy cfg default**	Enters device profile configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/cfg* # **set adminstate** {**disabled** | **enabled**}	(Optional) If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/cfg* # **set descr** *description*	(Optional) Provides a description for the backup policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 7	UCSC(policy-mgr) /org/device-profile/cfg* # **set remote-file**|**nfs-copy**	(Optional) Selects the backup location.
Step 8	UCSC(policy-mgr) /org/device-profile/cfg* # **set protocol**|**ftpsftp**|**scp**|**tftp**	(Optional) Specifies the protocol.
Step 9	UCSC(policy-mgr) /org/device-profile/cfg* # **max-copies**	(Optional) Specifies the maximum number of backups (1 to 30 copies)
Step 10	UCSC(policy-mgr) /org/device-profile/cfg* # **schedule** {**bi-weekly** | **daily** | **weekly**}	(Optional) Specifies the schedule for the backup.
Step 11	UCSC(policy-mgr) /org/device-profile/cfg* # **commit-buffer**	Commits the transaction.

The following example shows how to create a disabled all-configuration backup operation and commit the transaction. The backup schedule is bi-weekly and 25 copies are saved:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group* # create backup-policy cfg default
UCSC(policy-mgr) /org/device-profile/cfg*# set adminstate disabled
UCSC(policy-mgr) /org/device-profile/cfg*# set remote-filenfs-copy
UCSC(policy-mgr) /org/device-profile/cfg*#set protocolftpsftpscptftp
UCSC(policy-mgr) /org/device-profile/cfg*# set max-copies 25
UCSC(policy-mgr) /org/device-profile/cfg*#set schedule bi-weekly
UCSC(policy-mgr) /org/device-profile/cfg*#commit-buffer
UCSC(policy-mgr) /org/device-profile/cfg*#
```

Backing up and Restoring Cisco UCS Domains

You can create global backup policies for registered UCS domains in Cisco UCS Central at the domain group root or at the domain group levels.

When you create a global backup policy, Cisco UCS domains that are part of the domain group inherit the policy creating, update and deletion events. Deleting these policies remotely resets the admin state to disabled in Cisco UCS Manager since these are global policies that cannot be completely deleted. You can schedule a backup and restore operation or you can perform an immediate backup and restore operation.

Important Backing up UCS domains to a remote locations is supported only from Cisco UCS Manager, release 2.2(2x) and above. Trying to backup a UCS domain that is running on any earlier Cisco UCS Manager release versions will not work.

Recommendations

- Make sure to enable **Backup & Export Polices** to **Global** in Cisco UCS Manager.
- You must register a Cisco UCS Domain under a domain group to enable the global backup policy.
- When you have multiple Cisco UCS Manager release versions in your setup, make sure to same release versions of UCS Manager are registered under one domain group.
- You cannot specify multiple backup policies under different domain groups. All of the backup policies must be named default.

Creating a Scheduled Database Backup Policy for Cisco UCS Domains

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group**	Enters domain group mode.
Step 3	UCSC(policy-mgr) /domain-group # **create backup-policy full-state default**	Enters domain group configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/cfg* # **set adminstate** {**disabled** | **enabled**}	(Optional) If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.
Step 5	UCSC(policy-mgr) /domain-group/cfg* # **set descr** *description*	(Optional) Provides a description for the backup policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/cfg* # **set max-copies** *number*	(Optional) Specifies the maximum number of backups (1 to 30 copies)
Step 7	UCSC(policy-mgr) /domain-group/cfg* # **set schedule** {**bi-weekly** | **daily** | **weekly**}	(Optional) Specifies the schedule for the backup.
Step 8	UCSC(policy-mgr) /domain-group/cfg* # **commit-buffer**	Commits the transaction.

The following example shows how to create a disabled full-state backup operation and commit the transaction. The backup schedule is daily and 5 copies are saved:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group* # create backup-policy full-state default
UCSC(policy-mgr) /domain-group/cfg* # set adminstate disabled
UCSC(policy-mgr) /domain-group/cfg* # set max-copies 5
UCSC(policy-mgr) /domain-group/cfg* # set schedule daily
UCSC(policy-mgr) /domain-group/cfg* # commit-buffer
UCSC(policy-mgr) /domain-group/cfg #
```

Deleting a Scheduled All-Configuration and Full-State Backup Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group**	Enters domain group mode.
Step 3	UCSC(policy-mgr) /domain-group # **delete backup-policy cfg** *name*	Deletes the all-configuration backup policy.
Step 4	UCSC(policy-mgr) /domain-group* # **delete backup-policy full-state** *name*	Deletes the all-configuration backup policy.
Step 5	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction.

The following example shows how to delete the all-configuration and the full-state backup operations and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group* # delete backup-policy cfg default
UCSC(policy-mgr) /domain-group/cfg* # delete backup-policy full-state default
UCSC(policy-mgr) /domain-group/cfg* # commit-buffer
UCSC(policy-mgr) /domain-group/cfg #
```

Creating a Backup Operation

Before You Begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters the system mode.
Step 3	UCSC(ops-mgr) /system # **create backup** *URL backup-type* {**disabled** | **enabled**}	Creates a backup operation. Specify the *URL* for the backup file using one of the following syntax: • **ftp:**// *username@hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* The *backup-type* argument can be one of the following values: • **all-configuration —**Backs up the server-, fabric-, and system-related configuration • **logical-configuration —**Backs up the fabric- and service profile-related configuration • **system-configuration —**Backs up the system-related configuration • **full-state —**Backs up the full state for disaster recovery **Note** Full-state backup files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect. You can save multiple backup operations, but only one operation for each hostname is saved. If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.
Step 4	UCSC(ops-mgr) /system # **commit-buffer**	Commits the transaction.

The following example shows how to create a disabled all-configuration backup operation for hostname host35 and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system* # create backup scp://user@host35/backups/all-config9.bak
all-configuration disabled
Password:
UCSC(ops-mgr) /system* # commit-buffer
UCSC(ops-mgr) /system #
```

Deleting a Backup Operation

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters system mode.
Step 3	UCSC(ops-mgr) /system # **delete backup** *hostname*	Deletes the backup operation for the specified hostname.
Step 4	UCSC(ops-mgr) /system # **commit-buffer**	Commits the transaction.

The following example shows how to delete a backup operation for the host35 hostname and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # delete backup host35
UCSC(ops-mgr) /system* # commit-buffer
UCSC(ops-mgr) /system #
```

Deleting an Unused Backup File

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope backup-mgmt**	Enters backup management mode.
Step 3	UCSC(ops-mgr) /backup-mgmt # **delete-backup consumer-catalogue***name* **backup type** {**config-all** | **full-state**} **backup-date** *data/time*	Enters consumer-catalog mode for the specified catalogue.

The following example shows how to delete an unused backup file :

```
UCSC(ops-mgr) /backup-mgmt # delete-backup catalogue 192.168.10.22
backup type config-all backup-date 2012-11-11T07:31:39.00
```

Deleting an Unused Catalogue

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope backup-mgmt**	Enters backup management mode.
Step 3	UCSC(ops-mgr) /backup-mgmt # **delete consumer-catalogue** *hostname*	Specifies the consumer-catalog.
Step 4	UCSC(ops-mgr) /backup-mgmt* # **commit-buffer**	Commits the transaction.

The following example deletes the consumer-catalog host35 :

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope backup-mgmt
UCSC(ops-mgr) /backup-mgmt # delete consumer-catalogue host35
UCSC(ops-mgr) /backup-mgmt* # commit-buffer
```

Modifying a Backup Operation

You can modify a backup operation to save a file of another backup type to that location or to change the filename and avoid overwriting previous backup files.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters the system mode.
Step 3	UCSC(ops-mgr) /system # **scope backup** *hostname*	Enters system backup mode for the specified hostname.
Step 4	UCSC(ops-mgr) /system/backup # **disable**	(Optional) Disables an enabled backup operation so that it does not automatically run when the transaction is committed.
Step 5	UCSC(ops-mgr) /system/backup # **enable**	(Optional) Automatically runs the backup operation as soon as you commit the transaction.

	Command or Action	Purpose
Step 6	UCSC(ops-mgr) /system/backup # **set descr** *description*	(Optional) Provides a description for the backup operation. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 7	UCSC(ops-mgr) /system/backup # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	(Optional) Specifies the protocol to use when communicating with the remote server.
Step 8	UCSC(ops-mgr) /system/backup # **set remote-file** *filename*	(Optional) Specifies the name of the configuration file that is being backed up.
Step 9	UCSC(ops-mgr) /system/backup # **set type** *backup-type*	(Optional) Specifies the type of backup file to be made. The *backup-type* argument can be one of the following values: • **all-configuration —**Backs up the server, fabric, and system related configuration • **logical-configuration —**Backs up the fabric and service profile related configuration • **system-configuration —**Backs up the system related configuration • **full-state —**Backs up the full state for disaster recovery **Note** Full-state backup files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect.
Step 10	UCSC(ops-mgr) /system/backup # **set preserve-pooled-values** {**no** | **yes**}	(Optional) Specifies whether pool-derived identity values, such as vHBA WWPN, vNIC MAC, WWNN, and UUID, will be saved with the backup.
Step 11	UCSC(ops-mgr) /system/backup # **set user** *username*	(Optional) Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 12	UCSC(ops-mgr) /system/backup # **set password**	(Optional) After you press Enter, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.

	Command or Action	Purpose
Step 13	UCSC(ops-mgr) /system/backup # **commit-buffer**	Commits the transaction.

The following example shows how to add a description and change the protocol, username, and password for the host35 backup operation and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # scope backup host35
UCSC(ops-mgr) /system/backup # set descr "This is a backup operation for host35."
UCSC(ops-mgr) /system/backup* # set protocol sftp
UCSC(ops-mgr) /system/backup* # set user UserName32
UCSC(ops-mgr) /system/backup* # set password
Password:
UCSC(ops-mgr) /system/backup* # set preserve-pooled-values no
UCSC(ops-mgr) /system/backup* # commit-buffer
UCSC(ops-mgr) /system #
```

Modifying a Full-State Backup

Use this task to change or restart the backup operation.

Note After modifying the backup operation, enter **enable** inside this scope to restart the operation.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters the system mode.
Step 3	UCSC(ops-mgr) /system # **scope backup** *hostname*	Enters system backup mode for the specified hostname.
Step 4	UCSC(ops-mgr) /system/backup # **set descr** *description*	(Optional) Provides a description for the backup operation. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 5	UCSC(ops-mgr) /system/backup # **set password**	(Optional) After you press Enter, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.

	Command or Action	Purpose
Step 6	UCSC(ops-mgr) /system/backup # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	(Optional) Specifies the protocol to use when communicating with the remote server.
Step 7	UCSC(ops-mgr) /system/backup # **set remote-file** *filename*	(Optional) Specifies the name of the configuration file that is being backed up.
Step 8	UCSC(ops-mgr) /system/backup # **set user** *username*	(Optional) Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 9	UCSC(ops-mgr) /system/backup # **disable**	(Optional) Disables an enabled backup operation so that it does not automatically run when the transaction is committed.
Step 10	UCSC(ops-mgr) /system/backup # **enable**	(Optional) Automatically runs the backup operation as soon as you commit the transaction.
Step 11	UCSC(ops-mgr) /system/backup # **commit-buffer**	Commits the transaction.

The following example shows how to add a description and change the protocol, username, and password for the host35 backup operation and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # scope backup host35
UCSC(ops-mgr) /system/backup # set descr "This is an backup operation for host35."
UCSC(ops-mgr) /system/backup* # set protocol sftp
UCSC(ops-mgr) /system/backup* # set user UserName32
UCSC(ops-mgr) /system/backup* # set password
Password:
UCSC(ops-mgr) /system/backup* # commit-buffer
UCSC(ops-mgr) /system # show detail
```

Modifying a Scheduled All-Configuration Backup Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group**	Enters domain group mode.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope backup-policy cfg default**	Enters backup policy configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/cfg* # **set adminstate** {**disabled** | **enabled**}	(Optional) If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.
Step 5	UCSC(policy-mgr) /domain-group/cfg* # **set descr** *description*	(Optional) Provides a description for the backup policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 6	UCSC(policy-mgr) /domain-group/cfg* # **set max-copies** *number*	(Optional) Specifies the maximum number of backups (1 to 30 copies)
Step 7	UCSC(policy-mgr) /domain-group/cfg* # **set schedule** {**bi-weekly** | **daily** | **weekly**}	(Optional) Specifies the schedule for the backup.
Step 8	UCSC(policy-mgr) /domain-group/cfg* # **commit-buffer**	Commits the transaction.

The following example shows how to modify (change disabled to enabled) an all-configuration backup operation and commit the transaction. The backup schedule is changed to daily and 10 copies are saved:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group* # scope backup-policy cfg default
UCSC(policy-mgr) /domain-group/cfg* # set adminstate enabled
UCSC(policy-mgr) /domain-group/cfg* # set max-copies 10
UCSC(policy-mgr) /domain-group/cfg* # set schedule daily
UCSC(policy-mgr) /domain-group/cfg* # commit-buffer
UCSC(policy-mgr) /domain-group/cfg #
```

Modifying a Scheduled Database Backup Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group**	Enters domain group mode.
Step 3	UCSC(policy-mgr) /domain-group # **scope backup-policy full-state default**	Enters domain group configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/cfg* # **set adminstate** {**disabled** | **enabled**}	(Optional) If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.
Step 5	UCSC(policy-mgr) /domain-group/cfg* # **set descr** *description*	(Optional) Provides a description for the backup policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 6	UCSC(policy-mgr) /domain-group/cfg* # **set max-copies** *number*	(Optional) Specifies the maximum number of backups (1 to 30 copies)
Step 7	UCSC(policy-mgr) /domain-group/cfg* # **set schedule** {**bi-weekly** | **daily** | **weekly**}	(Optional) Specifies the schedule for the backup.
Step 8	UCSC(policy-mgr) /domain-group/cfg* # **commit-buffer**	Commits the transaction.

The following example shows how to modify a disabled full-state backup operation and commit the transaction. The backup schedule is daily and 5 copies are saved:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group* # scope backup-policy full-state default
UCSC(policy-mgr) /domain-group/cfg* # set adminstate enabled
UCSC(policy-mgr) /domain-group/cfg* # set max-copies 5
UCSC(policy-mgr) /domain-group/cfg* # set schedule daily
UCSC(policy-mgr) /domain-group/cfg* # commit-buffer
UCSC(policy-mgr) /domain-group/cfg #
```

Viewing a List of Backups Under a Specific Catalogue

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope backup-mgmt**	Enters backup management mode.
Step 3	UCSC(ops-mgr) /backup-mgmt # **scope consumer-catalogue** *hostname*	Enters consumer-catalog mode for the specified catalogue.
Step 4	UCSC(ops-mgr) /backup-mgmt/consumer-catalogue # **show backup**	Lists the backup operations in a specified cataloge.

The following example shows how to list the backup operations for consumer-catalog host35 :

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope backup-mgmt
UCSC(ops-mgr) /backup-mgmt # scope consumer-catalogue host35
UCSC(ops-mgr) /backup-mgmt/consumer-catalogue  # show backup
Config Backup:
    Type       Gen Number Time
    ---------- ---------- ----
    Config All      1     2012-11-11T07:31:39.000
```

Viewing Internal Backup Archive Operations

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope backup-mgmt**	Enters backup management mode.
Step 3	UCSC(ops-mgr) /backup-mgmt # **show** {**consumer-catalogue** [*detail* | *expand* | *fsm* | *internal name*] | **event** *detail* | **fsm** *FSM task*}	Specifies one of the following to display: • **consumer-catalogue —**The consumer-catalogue including the name, internal name, and owner. • **event —**The event management. • **fsm —**The finite state machine (FSM).

The following example shows how to list the consumer-catalog :

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope backup-mgmt
UCSC(ops-mgr) /backup-mgmt # show consumer-catalogue
Consumer Catalogue:
    Name                 Internal Name        Owner
    -------------------- -------------------- -----
    192.168.10.10        192.168.10.10
    192.168.10.20        192.168.10.20
    192.168.10.25        192.168.10.25
    192.168.10.35        192.168.10.35
    192.168.10.40        192.168.10.40
    ucs-central          ucs-central
```

Import Configuration

You can import any configuration file that was exported from Cisco UCS. The file does not need to have been exported from the same Cisco UCS.

Note You cannot import configuration from a higher release to a lower release.

The import function is available for all configuration, system configuration, and logical configuration files. You can perform an import while the system is up and running. An import operation modifies information on the management plane only. Some modifications caused by an import operation, such as a change to a vNIC assigned to a server, can cause a server reboot or other operations that disrupt traffic.

You cannot schedule an import operation. You can, however, create an import operation in advance and leave the admin state disabled until you are ready to run the import.Cisco UCS will not run the import operation on the configuration file until you set the admin state to enabled.

You can maintain only one import operation for each location where you saved a configuration backup file.

Import Methods

You can use one of the following methods to import and update a system configuration through Cisco UCS:

- **Merge—**The information in the imported configuration file is compared with the existing configuration information. If there are conflicts, the import operation overwrites the information on the Cisco UCS domain with the information in the import configuration file.
- **Replace—**The current configuration information is replaced with the information in the imported configuration file one object at a time.

Creating an Import Operation for Cisco UCS Central

You cannot import a Full State backup file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Before You Begin

Collect the following information that you will need to import a configuration file:

- Backup server IP address and authentication credentials
- Fully qualified name of a backup file

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters the system mode.
Step 3	UCSC(ops-mgr) /system # **create import** *URL* {**merge** | **replace**} {**disabled** | **enabled**}	Creates an import operation for Cisco UCS Central. Specify the URL for the file being imported using one of the following syntax: • **ftp:**// *username***@***hostname* / *path* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* You can save multiple import operations, but only one operation for each hostname is saved. If you use the **merge** keyword, the configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file. If you use the **replace** keyword, the system takes each object in the import configuration file and overwrites the corresponding object in the current configuration. If you use the **enable** keyword, the import operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the import operation will not run until it is enabled. When enabling an import operation, you must specify the hostname you used when creating the import operation.
Step 4	UCSC(ops-mgr) /system/import*# **commit-buffer**	Commits the transaction.

The following example shows how to create a disabled import operation for hostname host35 that replaces the existing configuration and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system* # create import-config scp://user@host35/backups/all-config9.bak
disabled replace
```

```
Password:
UCSC(ops-mgr) /system/import* # commit-buffer
UCSC(ops-mgr) /system/import #
```

Creating an Import Operation to a Cisco UCS Domain

Before You Begin

Collect the following information that you will need to import a configuration file:

- Backup server IP address and authentication credentials
- Fully qualified name of a backup file

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope backup-mgmt**	Enters backup management mode.
Step 3	UCSC(ops-mgr) /backup-mgmt# **create-importer to managed-system** *name* **from consumer-catalogue** *name* **backup-date** *date/time* **import-action** { **merge** | **replace**} **import-action**	
Step 4	UCSC(ops-mgr) /backup-mgmt *# **commit-buffer**	Commits the transaction.

The following example shows how to create an import operation to a Cisco UCS domain and commits the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope backup-mgmt
UCSC(ops-mgr) /backup-mgmt # create-importer to managed-system 10.105.214.103
from consumer-catalogue 10.105.214.103 backup-ate 2012-11-16T16:01:39.000 import-action
merge
UCSC(ops-mgr) /backup-mgmt* # commit-buffer
```

Running an Import Operation

You cannot import a Full State backup file. You can import any of the following configuration files:

- All configuration
- System configuration
- Logical configuration

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters system mode.
Step 2	UCSC /system # **scope import** *hostname*	Enters system backup mode for the specified hostname.
Step 3	UCSC /system/import-config # **enable**	Enables the import operation.
Step 4	UCSC /system/import-config # **commit-buffer**	Commits the transaction.

The following example shows how to enable an import operation for the host35 hostname and commit the transaction:

```
UCSC# scope system
UCSC /system # scope import host35
UCSC /system/import-config # enable
UCSC /system/import-config* # commit-buffer
UCSC /system/import-config #
```

Modifying an Import Operation for Cisco UCS Central

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters system mode.
Step 3	UCSC(ops-mgr) /system # **scope import** *hostname*	Enters system import configuration mode for the specified hostname.
Step 4	UCSC(ops-mgr) /system/import # **disable**	(Optional) Disables an enabled import operation so that it does not automatically run when the transaction is committed.
Step 5	UCSC(ops-mgr) /system/import # **enable**	(Optional) Automatically runs the import operation as soon as you commit the transaction.
Step 6	UCSC(ops-mgr) /system/import # **set action** {**merge** | **replace**}	(Optional) Specifies one of the following action types to use for the import operation: • **Merge —**The configuration information is merged with the existing information. If there are conflicts, the system replaces the information on the current system with the information in the import configuration file.

	Command or Action	Purpose
		• **Replace —**The system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Step 7	UCSC(ops-mgr) /system/import # **set descr** *description*	(Optional) Provides a description for the import operation. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 8	UCSC(ops-mgr) /system/import # **set password**	(Optional) After you press Enter, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used. **Note** Cisco UCS Central does not store this password. Therefore, you do not need to enter this password unless you intend to enable and run the import operation immediately.
Step 9	UCSC(ops-mgr) /system/import # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	(Optional) Specifies the protocol to use when communicating with the remote server.
Step 10	UCSC(ops-mgr) /system/import # **set remote-file-prefix** *filename*	(Optional) Specifies the name and full path of the configuration file that is being imported.
Step 11	UCSC(ops-mgr) /system/import # **set user** *username*	(Optional) Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 12	UCSC(ops-mgr) /system/import # **commit-buffer**	Commits the transaction.

The following example shows how to modify an import operation for Cisco UCS Central to change the description, protocol, and username for the import operation, and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # scope import host35
UCSC(ops-mgr) /system/import # set descr "This is an import operation for ucscentral."
UCSC(ops-mgr) /system/import* # set password
Password:
UCSC(ops-mgr) /system/import* # set protocol ftp
UCSC(ops-mgr) /system/import* # set user admin5
UCSC(ops-mgr) /system/import* # commit-buffer
UCSC(ops-mgr) /system/import #
```

Deleting a Backup, Export, or Import Operation

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters system mode.
Step 3	UCSC(ops-mgr) /system # **delete** {**backup** | **export** | **import**} *hostname*	Deletes the backup, management data export, or management data import operation for the specified hostname.
Step 4	UCSC(ops-mgr) /system # **commit-buffer**	Commits the transaction.

The following example shows how to delete the import operation for the host35 hostname and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # delete import host35
UCSC(ops-mgr) /system* # commit-buffer
UCSC(ops-mgr) /system #
```

Deleting a Cisco UCS Domain Import Operation

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope ucs-domain**	Enters Cisco UCS domain mode.
Step 3	UCSC(ops-mgr) /ucs-domain # **show managed-system**	Enters managed system mode.
Step 4	UCSC(ops-mgr) /ucs-domain/managed-system # **delete importer** *hostname*	Specifies the host to delete.
Step 5	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction.

The following example shows how to delete host35 and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope ucs-domain
UCSC(ops-mgr) /ucs-domain # show managed-system
UCSC(ops-mgr) /ucs-domain/managed-system # delete importer 10.105.214.100
```

```
UCSC(ops-mgr) /ucs-domain/managed-system* # commit-buffer
```

Viewing the Status of an Import Operation to a Cisco UCS Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC(ops-mgr)# **scope ucs-domain**	Enters Cisco UCS domain mode.
Step 3	UCSC(ops-mgr) /ucs-domain # **show managed-system**	Enters managed system mode.
Step 4	UCSC(ops-mgr) /ucs-domain/managed-system # **show importer** [**detail** | **expand** |**fsm** | **hostname**]	Displays the status of the import operation to a Cisco UCS domain.

The following example shows how to display the managed system 1006 import detail:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope ucs-domain
UCSC(ops-mgr) /ucs-domain # show managed-system
Managed System:
    ID         Name      Ip Address      Admin State     Oper State
    ---------- --------- --------------- --------------- ----------
          1006 bgl-samc01
                         192.168.10.25   Managed         Ok
UCSC(ops-mgr) /ucs-domain # scope managed-system 1006
UCSC(ops-mgr) /ucs-domain/managed-system # show importer detail
Importer:
    Hostname: 192.168.10.20
    Remote File: /192.168.10.25/cfg-backups/all-cfg
    Admin State: Disabled
    Action: Merge
    Op Status: All Success
    Status Report:
    Current Task:
```

System Restore

You can use the restore function for disaster recovery.

You can restore a system configuration from any full state backup file that was exported from Cisco UCS. The file does not need to have been exported from Cisco UCS on the system that you are restoring. When restoring using a backup file that was exported from a different system, we strongly recommend that you use a system with the same or similar system configuration and hardware, including fabric interconnects, servers, adapters, and I/O module or FEX connectivity. Mismatched hardware and/or system configuration can lead to the restored system not fully functioning. If there is a mismatch between the I/O module links or servers on the two systems, acknowledge the chassis and/or servers after the restore operation.

The restore function is only available for a full state backup file. You cannot import a full state backup file. You perform a restore through the initial system setup. For more information, see the appropriate *Cisco UCS Central Installation and Upgrade Guide*.

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

Restoring the Configuration for a Fabric Interconnect

Before You Begin

Collect the following information that you will need to restore the system configuration:

- Fabric interconnect management port IPv4 address and subnet mask, or IPv6 address and prefix
- Default gateway IPv4 or IPv6 address
- Backup server IPv4 or IPv6 address and authentication credentials
- Fully qualified name of a Full State backup file

Note You must have access to a Full State configuration file to perform a system restore. You cannot perform a system restore with any other type of configuration or backup file.

Procedure

Step 1 Connect to the console port.

Step 2 If the fabric interconnect is off, power on the fabric interconnect.
You will see the power on self-test message as the fabric interconnect boots.

Step 3 At the installation method prompt, enter **console** .

Step 4 Enter **restore** to restore the configuration from a full-state backup.

Step 5 Enter **y** to confirm that you want to restore from a full-state backup.

Step 6 Enter the IP address for the management port on the fabric interconnect.

Step 7 Enter the subnet mask for the management port on the fabric interconnect.

Step 8 Enter the IP address for the default gateway.

Step 9 Enter one of the following protocols to use when retrieving the backup configuration file:

- **scp**
- **ftp**
- **tftp**
- **sftp**

Step 10 Enter the IP address of the backup server.

Step 11 Enter the full path and filename of the Full State backup file.

Step 12 Enter the username and password to access the backup server.

The fabric interconnect logs in to the backup server, retrieves a copy of the specified full-state backup file, and restores the system configuration. For a cluster configuration, you do not need to restore the secondary fabric interconnect. As soon as the secondary fabric interconnect reboots, Cisco UCS synchronizes the configuration with the primary fabric interconnect.

The following example restores a system configuration from the Backup.bak file, which was retrieved from the 20.10.20.10 backup server using FTP:

```
  Enter the configuration method. (console/gui) ? console

  Enter the setup mode; setup newly or restore from backup. (setup/restore) ? restore

  NOTE:
    To configure Fabric interconnect using a backup file on a remote server,
    you will need to setup management interface.
    The management interface will be re-configured (if necessary),
    based on information stored in the backup file.


  Continue to restore this Fabric interconnect from a backup file (yes/no) ? yes

  Physical Switch Mgmt0 IPv4 address : 192.168.10.10

  Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0

  IPv4 address of the default gateway : 192.168.10.1

  Enter the protocol to get backup file (scp/ftp/tftp/sftp) ?  scp
  Enter the IP address of backup server: 20.10.20.10
  Enter fully qualified backup file name: Backup.bak
  Enter user ID: user
  Enter password:
    Retrieved backup configuration file.
  Configuration file - Ok


Cisco UCS 6100 Series Fabric Interconnect
UCSC login:
```

Creating an Export Operation

Before You Begin

Obtain the backup server IPv4 or IPv6 address and authentication credentials.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters the system mode.
Step 3	UCSC(ops-mgr) /system # **create export** *URL backup-type* {**disabled** | **enabled**}	Creates a backup operation. Specify the *URL* for the backup file using one of the following syntax: • **ftp:**// *username@hostname* / *path*

	Command or Action	Purpose
		• **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* The *backup-type* argument can be one of the following values: • **config-all —**Backs up the server-, fabric-, and system-related configuration • **config-logical —**Backs up the fabric- and service profile-related configuration • **config-system —**Backs up the system-related configuration You can save multiple backup operations, but only one operation for each hostname is saved. If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use the **disable** keyword, the backup operation will not run until it is enabled. When enabling a backup operation, you must specify the hostname you used when creating the backup operation.
Step 4	UCSC(ops-mgr) /system # **commit-buffer**	Commits the transaction.

The following example shows how to create a disabled config-all export operation for hostname host35 and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system* # create export scp://user@host35/backups/all-config9.bak config-all
 disabled
Password:
UCSC(ops-mgr) /system/export* # commit-buffer
UCSC(ops-mgr) /system/export # show fsm status
```

Modifying and Restarting an Export Operation

Use this task to change or restart the export operation.

Note After modifying the export operation, enter **enable** inside this scope to restart the operation.

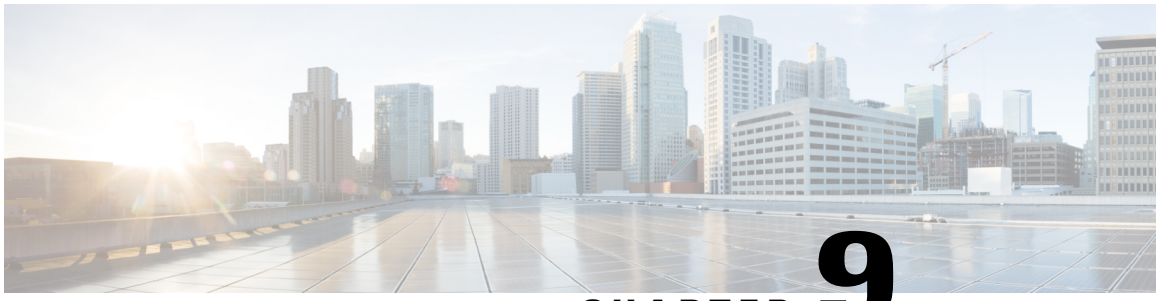
Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Enters operations manager mode.
Step 2	UCSC(ops-mgr)# **scope system**	Enters the system mode.
Step 3	UCSC(ops-mgr) /system # **scope export** *hostname*	Enters system export mode for the specified hostname.
Step 4	UCSC(ops-mgr) /system/export # **disable**	(Optional) Disables an enabled export operation so that it does not automatically run when the transaction is committed.
Step 5	UCSC(ops-mgr) /system/export # **enable**	(Optional) Automatically runs the export operation as soon as you commit the transaction.
Step 6	UCSC(ops-mgr) /system/export # **set descr** *description*	(Optional) Provides a description for the export operation. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any show command output.
Step 7	UCSC(ops-mgr) /system/export # **set password**	(Optional) After you press Enter, you are prompted to enter the password. Specifies the password for the remote server username. This step does not apply if the TFTP protocol is used.
Step 8	UCSC(ops-mgr) /system/export # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	(Optional) Specifies the protocol to use when communicating with the remote server.
Step 9	UCSC(ops-mgr) /system/export # **set remote-file-prefix** *filename*	(Optional) Specifies the name of the configuration file that is being backed up.
Step 10	UCSC(ops-mgr) /system/export # **set type** *export-type*	(Optional) Specifies the type of export file to be made. The *export-type* argument can be one of the following values: • **config-all —**Exports the server-, fabric-, and system-related configuration • **config-logical —**Exports the fabric- and service profile-related configuration • **config-system —**Exports the system-related configuration

	Command or Action	Purpose
		• **full-state —**Exports the full-state file for disaster recovery **Note** Full-state export files cannot be imported using an import operation. They are used only to restore the configuration for a fabric interconnect.
Step 11	UCSC(ops-mgr) /system/export # **set user** *username*	(Optional) Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 12	UCSC(ops-mgr) /system/export # **commit-buffer**	Commits the transaction.

The following example shows how to add a description and change the protocol, username, and password for the host35 export operation and commit the transaction:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # scope export host35
UCSC(ops-mgr) /system/export # set descr "This is an export operation for host35."
UCSC(ops-mgr) /system/export* # set protocol sftp
UCSC(ops-mgr) /system/export* # set user UserName32
UCSC(ops-mgr) /system/export* # set password
Password:
UCSC(ops-mgr) /system/export* # set preserve-pooled-values no
UCSC(ops-mgr) /system/export* # commit-buffer
UCSC(ops-mgr) /system #
```



CHAPTER 9

Working with Policies

This chapter includes the following sections:

Global Policies

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 Conversion Between Global and Local

Under certain circumstances you can convert a global policy to a local policy or a local policy to a global policy in Cisco UCS Manager.

Global service profiles and templates can only refer to global policies. Upon deployment, you cannot convert global policies that are included in global service profiles and templates to local policies. You must first convert the service profile or any policies that use the global policy, such as a LAN or SAN connectivity policy or a vNIC or vHBA template, to local.

When a service profile refers to a global template in Cisco UCS Central and the template includes a global policy, the ownership of the template is with the service profile. The ownership of the global policy remains with Cisco UCS Central, and you cannot make any changes to the policy ownership using Cisco UCS Manager. You can make changes to the policy ownership locally only if the policy is included in a local service profile or template.

Converting a Global Policy to a Local Policy

You can convert a policy from global to local only if the policy is included in a local service profile or service profile template.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **scope maint-policy** *policy-name*	Enters the policy maintenance mode.
Step 3	UCS-A /org/maint-policy # **set policy-owner** *local*	Converts the global policy to local.
Step 4	UCS-A /org/maint-policy* # **commit-buffer**	Commits the transaction to the system configuration.

The policy is now a local policy that can be managed by Cisco UCS Manager.

The following example converts a global policy to local and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope maint-policy GlobalScrubPolicy1
UCS-A /org/maint-policy* # set policy-owner local
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

Converting a Local Policy to a Global Policy

You can change the ownership of the local policies to global only if they are associated with a service profile.

Before You Begin

You must be logged in as an admin or as a user with admin privileges to perform this task.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCS-A /org # **scope maint-policy** *policy-name*	Enters the policy maintenance mode.
Step 3	UCS-A /org/maint-policy # **set policy-owner** *global*	Converts the local policy to global.
Step 4	UCS-A /org/maint-policy* # **commit-buffer**	Commits the transaction to the system configuration.

The policy is now a global policy that can only be managed by Cisco UCS Central and displays as read-only policy in the Cisco UCS Manager.

The following example converts a local policy to global and commits the transaction:

```
UCS-A# scope org /
UCS-A /org # scope maint-policy GlobalScrubPolicy1
UCS-A /org/maint-policy* # set policy-owner global
UCS-A /org/maint-policy* # commit-buffer
UCS-A /org/maint-policy #
```

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.

Name	Description
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

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
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
LDAP	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
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
Global Backup/Export Policy	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
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 214	See Consequences of Service Profile Changes on Policy Resolution, on page 214	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 214	See Consequences of Service Profile Changes on Policy Resolution, on page 214	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 214	See Consequences of Service Profile Changes on Policy Resolution, on page 214	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	Local	Local, but any "default" policies are updated on domain group assignment	Local/Remote (if resolved to "default" post registration)

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	
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)

Configuring Policy Resolution between Cisco UCS Manager and Cisco UCS Central using the Cisco UCS Manager CLI

Before You Begin

You must register the Cisco UCS Domain with Cisco UCS Central before you can configure policy resolution.

Procedure

	Command or Action	Purpose
Step 1	UCS-A# **scope system**	Enters system mode.
Step 2	UCS-A/system # **scope control-ep policy**	Enters control-ep policy mode.
Step 3	UCS-A/system/control-ep # **set backup-policy-ctrl source** {**local** | **global**}	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally or in Cisco UCS Central.
Step 4	UCS-A/system/control-ep # **set communication-policy-ctrl source** {**local** | **global**}	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally or in Cisco UCS Central.
Step 5	UCS-A/system/control-ep # **set datetime-policy-ctrl source** {**local** | **global**}	Determines whether the date and time is defined locally or comes from Cisco UCS Central.
Step 6	UCS-A/system/control-ep # **set dns-policy-ctrl source** {**local** | **global**}	Determines whether DNS servers are defined locally or in Cisco UCS Central.
Step 7	UCS-A/system/control-ep # **set fault-policy-ctrl source** {**local** | **global**}	Determines whether the Global Fault Policy is defined locally or in Cisco UCS Central.

	Command or Action	Purpose
Step 8	UCS-A/system/control-ep # **set infra-pack-ctrl source** {**local** | **global**}	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally or come from Cisco UCS Central.
Step 9	UCS-A/system/control-ep # **set mep-policy-ctrl source** {**local** | **global**}	Determines whether managed endpoints are defined locally or in Cisco UCS Central.
Step 10	UCS-A/system/control-ep # **set monitoring-policy-ctrl source** {**local** | **global**}	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally or in Cisco UCS Central.
Step 11	UCS-A/system/control-ep # **set powermgmt-policy-ctrl source** {**local** | **global**}	Determines whether the power management is defined locally or in Cisco UCS Central.
Step 12	UCS-A/system/control-ep # **set psu-policy-ctrl source** {**local** | **global**}	Determines whether power supply units are defined locally or in Cisco UCS Central.
Step 13	UCS-A/system/control-ep # **set security-policy-ctrl source** {**local** | **global**}	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally or in Cisco UCS Central.
Step 14	UCS-A/system/control-ep # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures policy resolution for a Cisco UCS Domain that is registered with Cisco UCS Central and commits the transaction:

```
UCS-A# scope system
UCS-A /system # scope control-ep policy
UCS-A /system/control-ep* # set backup-policy-ctrl source global
UCS-A /system/control-ep* # set communication-policy-ctrl source local
UCS-A /system/control-ep* # set datetime-policy-ctrl source global
UCS-A /system/control-ep* # set dns-policy-ctrl source global
UCS-A /system/control-ep* # set fault-policy-ctrl source global
UCS-A /system/control-ep* # set infra-pack-ctrl source global
UCS-A /system/control-ep* # set mep-policy-ctrl source global
UCS-A /system/control-ep* # set monitoring-policy-ctrl source global
UCS-A /system/control-ep* # set powermgmt-policy-ctrl source global
UCS-A /system/control-ep* # set psu-policy-ctrl source local
UCS-A /system/control-ep* # set security-policy-ctrl source global
UCS-A /system/control-ep* # commit-buffer
UCS-A /system/control-ep #
```

Policy and Policy Component Import in Cisco UCS Central

Cisco UCS Central enables you to import policies, pools, vLANs, vSANs directly from one registered Cisco UCS domain into Cisco UCS Central. When you have a perfect policy or a policy component in one of your UCS domains, you can import the policy and apply it to multiple domains. This import option enables you to import and apply a policy from one registered UCS domain to multiple UCS domains with a single click.

Using the Cisco UCS Central GUI, you can search for a policy or a component in the registered UCS domains. You can also refine your search using the available filters. From the search results, select the policy or component and import that into Cisco UCS Central.

Note If the search results are more than 1000, the results truncates. Make sure to refine the search using filters.

Depending on the policy or component you are importing, you can import them into either of the following destinations:

- Domain group root or to a specific domain
- Org root or a specific org

Estimate Impact During Import

Cisco UCS Central provides you the option to estimate the impact of most of the management actions you perform using the GUI. Make sure to run estimate impact during an import. Make sure to review the estimate impact results. The results will help you to identify any potential issues such as unintentional server reboot or policy overwrite and take proper precautionary measures before importing the selected policy or component.

Local Policies

The policies you create and manage in Cisco UCS Manager are local to the registered Cisco UCS domain. In Cisco UCS Central you can view the policies available in the registered Cisco UCS Domains as local policies. These policies can only be included in local service profiles or service profile templates that are created and managed within that Cisco UCS domain.

Configuring Threshold Policies

Statistics Threshold Policy

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

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

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

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

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

Server and Server Component Statistics Threshold Policy Configuration

Configuring a Server and Server Component Statistics Threshold Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create stats-threshold-policy** *policy-name*	Creates the specified statistics threshold policy and enters organization statistics threshold policy mode.
Step 4	UCSC(policy-mgr) /org/stats-threshold-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/stats-threshold-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the server and server component statistics threshold policy named ServStatsPolicy, provides a description for the policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create stats-threshold-policy ServStatsPolicy
UCSC(policy-mgr) /org/stats-threshold-policy* # set descr "Server stats threshold policy."
UCSC(policy-mgr) /org/stats-threshold-policy* # commit-buffer
UCSC(policy-mgr) /org/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "Configuring a Server and Server Component Statistics Threshold Policy Class, on page 219."

Configuring a Server and Server Component Statistics Threshold Policy Class

Before You Begin

Configure or identify the server and server component statistics threshold policy that will contain the policy class. For more information, see "Configuring a Server and Server Component Statistics Threshold Policy, on page 218."

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **scope stats-threshold-policy** *policy-name*	Enters organization statistics threshold policy mode.
Step 4	UCSC(policy-mgr) /org/stats-threshold-policy # **create class** *class-name*	Creates the specified statistics threshold policy class and enters organization statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?** command in organization statistics threshold policy mode. **Note** You can configure multiple classes for the statistics threshold policy.
Step 5	UCSC(policy-mgr) /org/stats-threshold-policy /class # **create property** *property-name*	Creates the specified statistics threshold policy class property and enters organization statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the **create property ?** command in organization statistics threshold policy class mode. **Note** You can configure multiple properties for the policy class.
Step 6	UCSC(policy-mgr) /org/stats-threshold-policy/class/property # **set normal-value** *value*	Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set normal-value ?** command in organization statistics threshold policy class property mode.
Step 7	UCSC(policy-mgr) /org/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**}	Creates the specified threshold value for the class property and enters organization statistics threshold policy class property threshold value mode.

	Command or Action	Purpose
	{**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	**Note** You can configure multiple threshold values for the class property.
Step 8	UCSC(policy-mgr) /org/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in organization statistics threshold policy class property threshold value mode. **Note** You can specify both de-escalating and escalating class property threshold values.
Step 9	UCSC(policy-mgr) /org/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the server and server component statistics threshold policy class for CPU statistics, creates a CPU temperature property, specifies that the normal CPU temperature is 48.5° C, creates an above normal warning threshold of 50° C, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope stats-threshold-policy ServStatsPolicy
UCSC(policy-mgr) /org/stats-threshold-policy* # create class cpu-stats
UCSC(policy-mgr) /org/stats-threshold-policy/class* # create property cpu-temp
UCSC(policy-mgr) /org/stats-threshold-policy/class/property* # set normal-value 48.5
UCSC(policy-mgr) /org/stats-threshold-policy/class/property* # create threshold-value
above-normal warning
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* # set escalating
 50.0
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value #
```

Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Configuration

Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr)# **scope eth-server**	Enters Ethernet server mode.
Step 4	UCSC(policy-mgr) /eth-server # **scope stats-threshold-policy default**	Enters Ethernet server statistics threshold policy mode. **Note** You cannot create (or delete) a server port, chassis, and fabric interconnect statistics threshold policy. You can only enter (scope to) the existing default policy.
Step 5	UCSC(policy-mgr) /eth-server/stats-threshold-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 6	UCSC(policy-mgr) /eth-server/stats-threshold-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the default server port, chassis, and fabric interconnect statistics threshold policy, provides a description for the policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr)# scope eth-server
UCSC(policy-mgr) /eth-server* # scope stats-threshold-policy default
UCSC(policy-mgr) /eth-server/stats-threshold-policy* # set descr "Server port, chassis, and
 fabric interconnect stats threshold policy."
UCSC(policy-mgr) /eth-server/stats-threshold-policy* # commit-buffer
UCSC(policy-mgr) /eth-server/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class, on page 221.

Configuring a Server Port, Chassis, and Fabric Interconnect Statistics Threshold Policy Class

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root mode organization, type / as the *org-name*.
Step 3	UCSC(policy-mgr)# **scope eth-server**	Enters Ethernet server mode.
Step 4	UCSC(policy-mgr) /eth-server # **scope stats-threshold-policy default**	Enters Ethernet server statistics threshold policy mode.
Step 5	UCSC(policy-mgr) /eth-server/stats-threshold-policy # **create class** *class-name*	Creates the specified statistics threshold policy class and enters Ethernet server statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?** command in Ethernet server statistics threshold policy mode. **Note** You can configure multiple classes for the statistics threshold policy.
Step 6	UCSC(policy-mgr) /eth-server/stats-threshold-policy /class # **create property** *property-name*	Creates the specified statistics threshold policy class property and enters Ethernet server statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the **create property ?** command in Ethernet server statistics threshold policy class mode. **Note** You can configure multiple properties for the policy class.
Step 7	UCSC(policy-mgr) /eth-server/stats-threshold-policy /class/property # **set normal-value** *value*	Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set normal-value ?** command in Ethernet server statistics threshold policy class property mode.
Step 8	UCSC(policy-mgr) /eth-server/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**} {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	Creates the specified threshold value for the class property and enters Ethernet server statistics threshold policy class property threshold value mode. **Note** You can configure multiple threshold values for the class property.
Step 9	UCSC(policy-mgr) /eth-server/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in Ethernet server statistics threshold policy class property threshold value mode.

	Command or Action	Purpose
		Note You can specify both de-escalating and escalating class property threshold values.
Step 10	UCSC(policy-mgr) /eth-server/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the server port, chassis, and fabric interconnect statistics threshold policy class for chassis statistics, creates an input power (Watts) property, specifies that the normal power is 8kW, creates an above normal warning threshold of 11kW, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr)# scope eth-server
UCSC(policy-mgr) /eth-server* # scope stats-threshold-policy default
UCSC(policy-mgr) /eth-server/stats-threshold-policy* # create class chassis-stats
UCSC(policy-mgr) /eth-server/stats-threshold-policy/class* # create property input-power
UCSC(policy-mgr) /eth-server/stats-threshold-policy/class/property* # set normal-value
8000.0
UCSC(policy-mgr) /eth-server/stats-threshold-policy/class/property* # create threshold-value
 above-normal warning
UCSC(policy-mgr) /eth-server/stats-threshold-policy/class/property/threshold-value* # set
escalating 11000.0
UCSC(policy-mgr) /eth-server/stats-threshold-policy/class/property/threshold-value* #
commit-buffer
UCSC(policy-mgr) /eth-server/stats-threshold-policy/class/property/threshold-value #
```

Fibre Channel Port Statistics Threshold Policy Configuration

Configuring a Fibre Channel Port Statistics Threshold Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter root organization mode, type **/** as the *org-name*.
Step 3	UCSC(policy-mgr)# **scope fc-uplink**	Enters Fibre Channel uplink mode.
Step 4	UCSC(policy-mgr) /fc-uplink # **scope stats-threshold-policy default**	Enters Fibre Channel uplink statistics threshold policy mode. **Note** You cannot create (or delete) an uplink Fibre Channel port statistics threshold policy. You can only enter (scope to) the existing default policy.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 6	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the default uplink Fibre Channel port statistics threshold policy, provides a description for the policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr) # scope fc-uplink
UCSC(policy-mgr) /fc-uplink* # scope stats-threshold-policy default
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy* # set descr "Uplink Fibre Channel stats
 threshold policy."
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy* # commit-buffer
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "Configuring a Fibre Channel Port Statistics Threshold Policy Class, on page 224."

Configuring a Fibre Channel Port Statistics Threshold Policy Class

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr)# **scope fc-uplink**	Enters Fibre Channel uplink mode.
Step 4	UCSC(policy-mgr) /fc-uplink # **scope stats-threshold-policy default**	Enters Fibre Channel uplink statistics threshold policy mode.
Step 5	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy # **create class** *class-name*	Creates the specified statistics threshold policy class and enters Fibre Channel uplink statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?**

	Command or Action	Purpose
		command in Fibre Channel uplink statistics threshold policy mode. **Note** You can configure multiple classes for the statistics threshold policy.
Step 6	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy /class # **create property** *property-name*	Creates the specified statistics threshold policy class property and enters Fibre Channel uplink statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the **create property ?** command in Fibre Channel uplink statistics threshold policy class mode. **Note** You can configure multiple properties for the policy class.
Step 7	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy /class/property # **set normal-value** *value*	Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set normal-value ?** command in Fibre Channel uplink statistics threshold policy class property mode.
Step 8	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**} {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	Creates the specified threshold value for the class property and enters Fibre Channel uplink statistics threshold policy class property threshold value mode. **Note** You can configure multiple threshold values for the class property.
Step 9	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in Fibre Channel uplink statistics threshold policy class property threshold value mode. **Note** You can specify both de-escalating and escalating class property threshold values.
Step 10	UCSC(policy-mgr) /fc-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the uplink Fibre Channel port statistics threshold policy class for Fibre Channel statistics, creates an average bytes received property, specifies that the normal average number of bytes

received for each polling interval is 150MB, creates an above normal warning threshold of 200MB, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr)# scope fc-uplink
UCSC(policy-mgr) /fc-uplink* # scope stats-threshold-policy default
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy* # create class fc-stats
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy/class* # create property bytes-rx-avg
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy/class/property* # set normal-value
150000000
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy/class/property* # create threshold-value
 above-normal warning
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy/class/property/threshold-value* # set
escalating 200000000
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy/class/property/threshold-value* #
commit-buffer
UCSC(policy-mgr) /fc-uplink/stats-threshold-policy/class/property/threshold-value #
```

Uplink Ethernet Port Statistics Threshold Policy Configuration

Configuring an Uplink Ethernet Port Statistics Threshold Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 3	UCSC(policy-mgr) /eth-uplink # **scope stats-threshold-policy default**	Enters Ethernet uplink statistics threshold policy mode. **Note** You cannot create (or delete) an uplink Ethernet port statistics threshold policy. You can only enter (scope to) the existing default policy.
Step 4	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the default uplink Ethernet port threshold policy, provides a description for the policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope eth-uplink
UCSC(policy-mgr) /eth-uplink* # scope stats-threshold-policy default
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy* # set descr "Uplink Ethernet port stats
 threshold policy."
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy* # commit-buffer
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy #
```

What to Do Next

Configure one or more policy classes for the statistics threshold policy. For more information, see "Configuring an Uplink Ethernet Port Statistics Threshold Policy Class, on page 227."

Configuring an Uplink Ethernet Port Statistics Threshold Policy Class

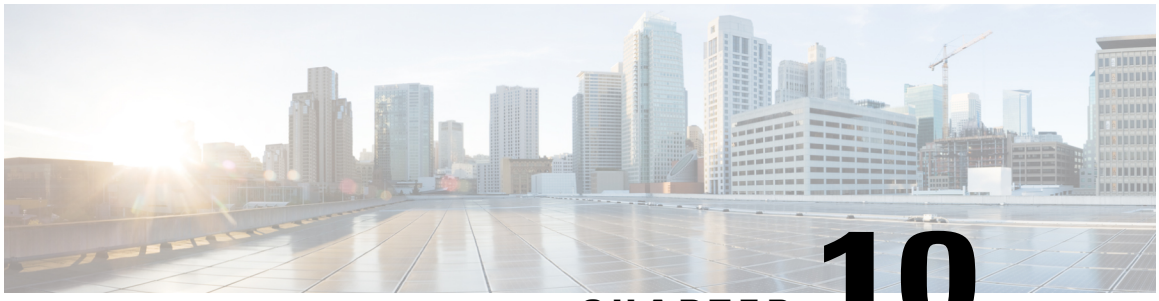
Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope eth-uplink**	Enters Ethernet uplink mode.
Step 3	UCSC(policy-mgr) /eth-uplink # **scope stats-threshold-policy default**	Enters Ethernet uplink statistics threshold policy mode.
Step 4	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy # **create class** *class-name*	Creates the specified statistics threshold policy class and enters Ethernet uplink statistics threshold policy class mode. The *class-name* argument can be any of the class name keywords available for the particular statistics threshold policy being configured. To see a list of the available class name keywords, enter the **create class ?** command in Ethernet uplink statistics threshold policy mode. **Note** You can configure multiple classes for the statistics threshold policy.
Step 5	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy /class # **create property** *property-name*	Creates the specified statistics threshold policy class property and enters Ethernet uplink statistics threshold policy class property mode. The *property-name* argument can be any of the property name keywords available for the particular policy class being configured. To see a list of the available property name keywords, enter the **create property ?** command in Ethernet uplink statistics threshold policy class mode. **Note** You can configure multiple properties for the policy class.
Step 6	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy /class/property # **set normal-value** *value*	Specifies the normal value for the class property. The *value* format can vary depending on the class property being configured. To see the required format, enter the **set**

	Command or Action	Purpose
		normal-value ? command in Ethernet uplink statistics threshold policy class property mode.
Step 7	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy /class/property # **create threshold-value** {**above-normal** | **below-normal**} {**cleared** | **condition** | **critical** | **info** | **major** | **minor** | **warning**}	Creates the specified threshold value for the class property and enters Ethernet uplink statistics threshold policy class property threshold value mode. **Note** You can configure multiple threshold values for the class property.
Step 8	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy /class/property/threshold-value # **set** {**deescalating** | **escalating**} *value*	Specifies the de-escalating or escalating class property threshold value. The *value* format can vary depending on the class property threshold value being configured. To see the required format, enter the **set deescalating ?** or **set escalating ?** command in Ethernet uplink statistics threshold policy class property threshold value mode. **Note** You can specify both de-escalating and escalating class property threshold values.
Step 9	UCSC(policy-mgr) /eth-uplink/stats-threshold-policy /class/property/threshold-value # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the uplink Ethernet port statistics threshold policy class for Ethernet error statistics, creates a cyclic redundancy check (CRC) error count property, specifies that the normal CRC error count for each polling interval is 1000, creates an above normal warning threshold of 1250, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope eth-uplink
UCSC(policy-mgr) /eth-uplink* # scope stats-threshold-policy default
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy* # create class ether-error-stats
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy/class* # create property crc-delta
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy/class/property* # set normal-value 1000
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy/class/property* # create threshold-value
 above-normal warning
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy/class/property/threshold-value* # set
escalating 1250
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy/class/property/threshold-value* #
commit-buffer
UCSC(policy-mgr) /eth-uplink/stats-threshold-policy/class/property/threshold-value #
```



CHAPTER 10

Service Profiles and Templates

This chapter includes the following sections:

Global Service Profiles

Global service profile centralizes the logical configuration deployed in across the data center. This centralization enables the maintenance of all service profiles in the Cisco UCS domains from one central location in Cisco UCS Central. When you use a global service profile, you can do the following across the data center:

- Pick a compute element for the service profile from any of the Cisco UCS domains.
- Migrate the service profile from one element to another.
- Select servers from the available global server pools from any of the Cisco UCS domains.
- Associate global resources such as ID pools and policies.
- Reference to any of the global policies in the Cisco UCS domain.

Creating Global Service Profiles

You can create a global service profile from Cisco UCS Central GUI or Cisco UCS Central CLI or as regular service profiles from Cisco UCS Manager and reference the global polices. When you create the global service profile from Cisco UCS Central, you can create ID pools, vNICs and vHBAs in Cisco UCS Central and reference to the ID.

Configuring Management IP Addresses for Global Service Profiles

Each server in a Cisco UCS domain must have one or more management IP addresses assigned to its Cisco Integrated Management Controller (CIMC) or to the service profile associated with the server. In Cisco UCS Central, the following management IP addresses can be configured to create a service profile:

- Zero or one outband IPv4 address, through which traffic traverses the fabric interconnect through the management port.
- Zero or one inband (IPv4 or IPv6) address, through which traffic traverses the fabric interconnect through the fabric uplink port.

You can configure either a pooled or a static management IP address through the Cisco UCS Central GUI or CLI. However, while creating a global service profile using the global service profile template, you can only configure a pooled management IP address. Static IP address is not supported for this release.

Guidelines and Cautions for Global Service Profile

Make sure to remember the following when you are creating global service profiles:

- When you create a global service profile in Cisco UCS Central, the system validates the following information:
  - Use od ID along with vNICs, vHBAs, iSCSI vNICs etc
  - vLAN and vSAN assignment
  - Association to the compute element based on the availability index
  - Server qualification criteria

    Any incompatibility in these information will be flagged. You can successfully create the global service profile only after resolving these issues.
- After any of the policy reference is resolved in the global service profile, if any of the remote policy is changed, that will result in reconfiguration of the global service profile.
- The VLANs and VSANs in Cisco UCS Central belong to domain groups. Make sure to create the VLANS or VSANs under a domain group. In case of VLAN also assign them to Orgs before a vNIC or vHBA from the global service profile can access the VLAN or VSAN.
- You can modify, disassociate or delete any of the global service profile only from Cisco UCS Central.
- You can rename a global service profile only from Cisco UCS Central. When you rename a service profile, Cisco UCS Central deletes the global service profile with old name and creates a new service profile with the new name in the inventory.
- If a server that is associated to the global service profile is removed from the Cisco UCS domain, when you re-acknowledge the server, it will be unassociated from the service profile.
- You cannot define or access domain specific policies, such as multi-cast policy and flow-control policy from Cisco UCS Central. But, you can reference to these policies from Cisco UCS Central by global service profile resources. When you define the global service profile, you can view the available domain specific policies and refer to them in the service profile by name. When the service profile is deployed, the Cisco UCS domain resolves to the policy and includes it in the service profile for that domain.
- You can localize a global service profile from the deployed Cisco UCS Manager. When you localize, the global service profile is deleted from Cisco UCS Central. But all the global policies still remain global. If you want to localize the global policies, you have to localize each policy separately.

Creating a Global Service Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr)# /org # **create service-profile** *profile-name* **instance**	Creates the specified service profile and enters organization service profile mode. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.
Step 4	UCSC(resource-mgr) /org/service-profile # **set bios-policy** *policy-name*	Associates the specified BIOS policy with the service profile.
Step 5	UCSC(resource-mgr) /org/service-profile # **set boot-policy** *policy-name*	Associates the specified boot policy with the service profile.
Step 6	UCSC(resource-mgr) /org/service-profile # **set descr** *description*	(Optional) Provides a description for the service profile. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 7	UCSC(resource-mgr) /org/service-profile # **set dynamic-vnic-conn-policy** *policy-name*	Associates the specified dynamic vNIC connection policy with the service profile.
Step 8	UCSC(resource-mgr) /org/service-profile # **set extippoolname** *pool-name*	Associates the specified external IP pool with the service profile.
Step 9	UCSC(resource-mgr) /org/service-profile # **set extipstate** *pool-name*	Specifies how the external IP address will be assigned to the service profile. You can set the IP address policy using the following options: • None—The service profile is not assigned an IP address.

	Command or Action	Purpose
		• Pooled—The service profile is assigned an IP address from the IP pool. • Static—The service profile is assigned the configured IP address.
Step 10	UCSC(resource-mgr) /org/service-profile # **set host-fw-policy** *policy-name*	Associates the specified host firmware policy with the service profile.
Step 11	UCSC(resource-mgr) /org/service-profile # **set identity** {**dynamic-uuid** {*uuid* | **derived**} | **dynamic-wwnn** {*wwnn* | **derived**} | **uuid-pool** *pool-name* | **wwnn-pool** *pool-name*}	Specifies how the server acquires a UUID or WWNN. You can do one of the following: • Create a unique UUID in the form *nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn* . • Derive the UUID from the one burned into the hardware at manufacture. • Use a UUID pool. • Create a unique WWNN in the form *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* . • Derive the WWNN from one burned into the hardware at manufacture. • Use a WWNN pool.
Step 12	UCSC(resource-mgr) /org/service-profile # **set ipmi-access-profile** *profile-name*	Associates the specified IPMI access profile with the service profile.
Step 13	UCSC(resource-mgr) /org/service-profile # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*	Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.
Step 14	UCSC(resource-mgr) /org/service-profile # **set lan-connectivity-policy-name** *policy-name*	Associates the specified LAN connectivity policy with the service profile. **Note** You cannot have a LAN connectivity policy and locally created vNICs in the same service profile. When you add a LAN connectivity policy to a service profile, any existing vNIC configuration is erased.
Step 15	UCSC(resource-mgr) /org/service-profile # **set local-disk-policy** *policy-name*	Associates the specified local disk policy with the service profile.
Step 16	UCSC(resource-mgr) /org/service-profile # **set maintpolicyname** *policy-name*	Associates the specified maintenance policy with the service profile.

	Command or Action	Purpose
Step 17	UCSC(resource-mgr) /org/service-profile # **set power-control-policy** *policy-name*	Associates the specified power control policy with the service profile.
Step 18	UCSC(resource-mgr) /org/service-profile # **set san-connectivity-policy-name** *policy-name*	Associates the specified SAN connectivity policy with the service profile. **Note** You cannot have a SAN connectivity policy and locally created vHBAs in the same service profile. When you add a SAN connectivity policy to a service profile, any existing vHBA configuration is erased.
Step 19	UCSC(resource-mgr) /org/service-profile # **set scrub-policy** *policy-name*	Associates the specified scrub policy with the service profile.
Step 20	UCSC(resource-mgr) /org/service-profile # **set sol-policy** *policy-name*	Associates the specified serial over LAN policy with the service profile.
Step 21	UCSC(resource-mgr) /org/service-profile # **set stats-policy** *policy-name*	Associates the specified statistics policy with the service profile.
Step 22	UCSC(resource-mgr) /org/service-profile # **set user-label** *label-name*	Specifies the user label associated with the service profile.
Step 23	UCSC(resource-mgr) /org/service-profile # **set vcon** {**1** | **2** | **3** | **4**} **select** {**all** | **assigned-only** | **exclude-dynamic** | **exclude-unassigned**}	Specifies the selection preference for the specified vCon.
Step 24	UCSC(resource-mgr) /org/service-profile # **set vcon-policy** *policy-name*	Associates the specified vNIC/vHBA placement policy with the service profile. **Note** You can either assign a vNIC/vHBA placement policy to the service profile, or set vCon selection preferences for the service profile, but you do not need to do both.
Step 25	UCSC(resource-mgr) /org/service-profile # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a service profile and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # create service-profile GSP2 instance
UCSC(resource-mgr) /org/service-profile* # set bios-policy biospol1
UCSC(resource-mgr) /org/service-profile* # set boot-policy bootpol32
UCSC(resource-mgr) /org/service-profile* # set  descr "This is a global service profile
example."
UCSC(resource-mgr) /org/service-profile* # set dynamic-vnic-conn-policy mydynvnicconnpolicy
UCSC(resource-mgr) /org/service-profile* # set extippoolname myippool
UCSC(resource-mgr) /org/service-profile* # set extipstate pooled
UCSC(resource-mgr) /org/service-profile* # set host-fw-policy ipmi-user987
UCSC(resource-mgr) /org/service-profile* # set identity dynamic-uuid derived
UCSC(resource-mgr) /org/service-profile* # set ipmi-access-profile ipmiProf16
UCSC(resource-mgr) /org/service-profile* # set local-disk-policy localdiskpol33
```

```
UCSC(resource-mgr) /org/service-profile* # set maintpolicyname maintpol4
UCSC(resource-mgr) /org/service-profile* # set power-control-policy powcontrpol13
UCSC(resource-mgr) /org/service-profile* # set scrub-policy scrubpol55
UCSC(resource-mgr) /org/service-profile* # set sol-policy solpol2
UCSC(resource-mgr) /org/service-profile* # set stats-policy statspol4
UCSC(resource-mgr) /org/service-profile* # set user-label mylabel
UCSC(resource-mgr) /org/service-profile* # set vcon-policy myvconnpolicy
UCSC(resource-mgr) /org/service-profile* # commit-buffer
UCSC(resource-mgr) /org/service-profile #
```

What to Do Next

Deploy the Global Service profile in UCS Domains.

Creating a Global Service Profile Instance from a Service Profile Template

Before You Begin

Verify that there is a service profile template from which to create a service profile instance.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr)# /org # **create service-profile** *profile-name* **instance**	Creates the specified service profile and enters organization service profile mode. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization.
Step 4	UCSC(resource-mgr) /org/service-profile # **set src-templ-name** *profile-name*	Specifies the source service profile template to apply to the service profile instance. All configuration settings from the service profile template will be applied to the service profile instance.
Step 5	UCSC(resource-mgr) /org/service-profile # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a service profile instance, apply the service profile template named ServTemp2, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # create service-profile GSP2 instance
UCSC(resource-mgr) /org/service-profile* # set src-templ-name ServTemp2
```

```
UCSC(resource-mgr) /org/service-profile* # commit-buffer
UCSC(resource-mgr) /org/service-profile #
```

What to Do Next

Associate the service profile to a server, rack server, or server pool.

Configuring a vNIC for a Global Service Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr) /org # **scope service-profile** *profile-name*	Enters organization service profile mode for the specified service profile.
Step 4	UCSC(resource-mgr) /org/service-profile # **create vnic** *vnic-name* [**eth-if** *eth-if-name*] [**fabric** {**a** | **b**}]	Creates a vNIC for the specified service profile and enters organization service profile vNIC mode.
Step 5	UCSC(resource-mgr) /org/service-profile/vnic # **set adapter-policy** *policy-name*	Specifies the adapter policy to use for the vNIC.
Step 6	UCSC(resource-mgr) /org/service-profile/vnic # **set fabric** {**a** | **a-b** | **b** | **b-a**}	Specifies the fabric to use for the vNIC. If you did not specify the fabric when creating the vNIC template in Step 3, you have the option to specify it with this command. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, choose **a-b** (A is the primary) or **b-a** (B is the primary) .

	Command or Action	Purpose
		Note Do not enable fabric failover for the vNIC under the following circumstances: • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • If you plan to associate this vNIC with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so, Cisco UCS Central generates a configuration fault when you associate the service profile with the server.
Step 7	UCSC(resource-mgr) /org/service-profile/vnic # **set identity** {**dynamic-mac** {*mac-addr* | **derived**} | **mac-pool** *mac-pool-name*}	Specifies the identity (MAC address) for the vNIC. You can set the identity using one of the following options: • Create a unique MAC address in the form *nn* **:** *nn* **:** *nn* **:** *nn* **:** *nn* **:** *nn* . • Derive the MAC address from one burned into the hardware at manufacture. • Assign a MAC address from a MAC pool.
Step 8	UCSC(resource-mgr) /org/service-profile/vnic # **set mtu** *size-num*	The maximum transmission unit, or packet size, that this vNIC accepts. Enter an integer between 1500 and 9216. **Note** If the vNIC has an associated QoS policy, the MTU specified here must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets might get dropped during data transmission.
Step 9	UCSC(resource-mgr) /org/service-profile/vnic # **set nw-control-policy** *policy-name*	The network control policy the vNIC should use.
Step 10	UCSC(resource-mgr) /org/service-profile/vnic # **set order** {*order-num* | **unspecified**}	Specifies the relative order for the vNIC.
Step 11	UCSC(resource-mgr) /org/service-profile/vnic # **set pin-group** *group-name*	The LAN pin group the vNIC should use.

	Command or Action	Purpose
Step 12	UCSC(resource-mgr) /org/service-profile/vnic # **set qos-policy** *policy-name*	The quality of service policy the vNIC should use.
Step 13	UCSC(resource-mgr) /org/service-profile/vnic # **set stats-policy** *policy-name*	The statistics collection policy the vNIC should use.
Step 14	UCSC(resource-mgr) /org/service-profile/vnic # **set template-name** *policy-name*	Specifies the dynamic vNIC connectivity policy to use for the vNIC.
Step 15	UCSC(resource-mgr) /org/service-profile/vnic # **set vcon** {**1** | **2** | **3** | **4** | **any**}	Assigns the vNIC to the specified vCon. Use the **any** keyword to have Cisco UCS Central automatically assign the vNIC.
Step 16	UCSC(resource-mgr) /org/service-profile/vnic # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to configure a vNIC for a service profile and commits the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # scope service-profile ServProf2
UCSC(resource-mgr) /org/service-profile* # create vnic vnic3 fabric a
UCSC(resource-mgr) /org/service-profile/vnic* # set adapter-policy AdaptPol2
UCSC(resource-mgr) /org/service-profile/vnic* # set fabric a-b
UCSC(resource-mgr) /org/service-profile/vnic* # set identity mac-pool MacPool3
UCSC(resource-mgr) /org/service-profile/vnic* # set mtu 8900
UCSC(resource-mgr) /org/service-profile/vnic* # set nw-control-policy ncp5
UCSC(resource-mgr) /org/service-profile/vnic* # set order 0
UCSC(resource-mgr) /org/service-profile/vnic* # set pin-group EthPinGroup12
UCSC(resource-mgr) /org/service-profile/vnic* # set qos-policy QosPol5
UCSC(resource-mgr) /org/service-profile/vnic* # set stats-policy StatsPol2
UCSC(resource-mgr) /org/service-profile/vnic* # set template-name VnicConnPol3
UCSC(resource-mgr) /org/service-profile/vnic* # set vcon any
UCSC(resource-mgr) /org/service-profile/vnic* # commit-buffer
UCSC(resource-mgr) /org/service-profile/vnic #
```

Configuring a vHBA for a Global Service Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

	Command or Action	Purpose
Step 3	UCSC(resource-mgr) /org # **scope service-profile** *profile-name*	Enters organization service profile mode for the specified service profile.
Step 4	UCSC(resource-mgr) /org/service-profile # **create vhba** *vhba-name* [**fc-if** *fc-if-name*] [**fabric** {**a** | **b**}]	Creates a vHBA for the specified service profile and enters organization service profile vHBA mode.
Step 5	UCSC(resource-mgr) /org/service-profile/vhba # **set adapter-policy** *policy-name*	Specifies the adapter policy to use for the vHBA.
Step 6	UCSC(resource-mgr) /org/service-profile/vhba # **set fabric** {**a** | **b**}	Specifies the fabric to use for the vHBA. If you did not specify the fabric when creating the vHBA template in Step 4, you have the option to specify it with this command.
Step 7	UCSC(resource-mgr) /org/service-profile/vhba # **set fc-if** *fc-if-name*	Specifies the fibre channel interface to use for the vHBA. If you did not specify the fibre channel interface when creating the vHBA template in Step 4, you have the option to specify it with this command.
Step 8	UCSC(resource-mgr) /org/service-profile/vhba # **set identity** {**dynamic-wwpn** {*wwpn* | **derived**} | **wwpn-pool** *wwn-pool-name*}	Specifies the WWPN for the vHBA. You can set the storage identity using one of the following options: • Create a unique WWPN in the form *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*. You can specify a WWPN in the range 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. If you want the WWPN to be compatible with Cisco MDS Fibre Channel switches, use the WWPN template **20:00:00:25:B5:XX:XX:XX**. • Derive the WWPN from one burned into the hardware at manufacture. • Assign a WWPN from a WWN pool.
Step 9	UCSC(resource-mgr) /org/service-profile/vhba # **set max-field-size** *size-num*	Specifies the maximum size of the Fibre Channel frame payload (in bytes) that the vHBA supports.
Step 10	UCSC(resource-mgr) /org/service-profile/vhba # **set pers-bind** {**disabled** | **enabled**}	Disables or enables persistent binding to Fibre Channel targets.

	Command or Action	Purpose
Step 11	UCSC(resource-mgr) /org/service-profile/vhba # **set pin-group** *group-name*	Specifies the SAN pin group to use for the vHBA.
Step 12	UCSC(resource-mgr) /org/service-profile/vhba # **set qos-policy** *policy-name*	Specifies the QoS policy to use for the vHBA.
Step 13	UCSC(resource-mgr) /org/service-profile/vhba # **set stats-policy** *policy-name*	Specifies the statistics threshold policy to use for the vHBA.
Step 14	UCSC(resource-mgr) /org/service-profile/vhba # **set template-name** *policy-name*	Specifies the vHBA template to use for the vHBA.
Step 15	UCSC(resource-mgr) /org/service-profile/vhba # **set vcon** {**1** | **2** | **3** | **4** | **any**}	Assigns the vHBA to the specified vCon. Use the **any** keyword to have Cisco UCS Central automatically assign the vHBA.
Step 16	UCSC(resource-mgr) /org/service-profile/vhba # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a vHBA for a service profile and commits the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # scope service-profile ServProf2
UCSC(resource-mgr) /org/service-profile* # create vhba vhba3 fabric a
UCSC(resource-mgr) /org/service-profile/vhba* # set adapter-policy AdaptPol2
UCSC(resource-mgr) /org/service-profile/vhba* # set identity wwpn-pool wwpnPool3
UCSC(resource-mgr) /org/service-profile/vhba* # set max-field-size 8900
UCSC(resource-mgr) /org/service-profile/vhba* # set pin-group EthPinGroup12
UCSC(resource-mgr) /org/service-profile/vhba* # set qos-policy QosPol5
UCSC(resource-mgr) /org/service-profile/vhba* # set stats-policy StatsPol2
UCSC(resource-mgr) /org/service-profile/vhba* # set template-name vHBATemp3
UCSC(resource-mgr) /org/service-profile/vhba* # set vcon any
UCSC(resource-mgr) /org/service-profile/vhba* # commit-buffer
UCSC(resource-mgr) /org/service-profile/vhba #
```

Setting up an Inband Pooled Management IP Address

You can set up an inband pooled IPv4 or an IPv6 management address.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters System mode.

	Command or Action	Purpose
Step 2	UCSC/System#**scope org***org-name*	Enters organization mode for the specific organization.
Step 3	UCSC/org#**scope service-profile***service-profile-name*	Enters the service profile mode.
Step 4	UCSC/org/service-profile#**create mgmt-iface***inband*	Creates the inband management interface and enters the interface mode.
Step 5	UCSC/org/service-profile/mgmt-iface#**create mgmt-vlan**	Creates a management VLAN and enters the VLAN configuration mode.
Step 6	UCSC/org/service-profile/mgmt-iface/mgmt-vlan#**create ext-pooled-ip**	Creates an external IP pool and enters the IP pool configuration mode.
Step 7	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip#**set name***ipv4-address-pool-name*	Sets the name of the inband IPv4 pool.
Step 8	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip#**exit**	Exits the IPv4 pool configuration mode.
Step 9	UCSC/org/service-profile/mgmt-iface/mgmt-vlan#**create ext-pooled-ip6**	Creates an external IPv6 pool and enters the IPv6 pool configuration mode.
Step 10	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6#**set name***ipv6-address-pool-name*	Sets the name of the inband IPv6 pool.
Step 11	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6#**commit-buffer**	Commits the transaction in the system configuration.

The following example shows how to configure an pooled inband management IP interface:

```
UCSC#scope system
UCSC/system#scope org org1
UCSC/org# scope service-profile sp2
UCSC/org/service-profile# create mgmt-iface inband1
UCSC/org/service-profile/mgmt-iface#create mgmt-vlan
UCSC/org/service-profile/mgmt-iface/mgmt-vlan# create ext-pooled-ip
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip# set name <ipv4-address-pool-name>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip# exit
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip# create ext-pooled-ip6
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6# set name
<ipv6-address-pool-name>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6# commit-buffer
```

What to Do Next

Associate the inband management IP interface service profile to a server.

Setting up an Inband Static Management IP Address

You can set up an inband static IPv4 or an IPv6 management address.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters System mode.
Step 2	UCSC/System#**scope org***org-name*	Enters organization mode for the specific organization.
Step 3	UCSC/org#**scope service-profile***service-profile-name*	Enters the service profile mode.
Step 4	UCSC/org/service-profile#**create mgmt-iface***inband*	Creates the inband management interface and enters the interface mode.
Step 5	UCSC/org/service-profile/mgmt-iface#**create mgmt-vlan**	Creates a management VLAN and enters the VLAN configuration mode.
Step 6	UCSC/org/service-profile/mgmt-iface/mgmt-vlan#**create ext-static-ip**	Creates an external static IP address and enters the IP pool configuration mode.

	Command or Action	Purpose
Step 7	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip#**set address***ipv4-address*	Sets up the inband static IPv4 address.
Step 8	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip#**set default-gw***gateway-ip*	Sets up the default gateway IP address.
Step 9	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip#**set prefix***prefix*	Sets up the network prefix.
Step 10	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip#**exit**	Exits the IPv4 static configuration mode.
Step 11	UCSC/org/service-profile/mgmt-iface/mgmt-vlan#**create ext-static-ip6**	Creates an external static IPv6 address and enters the IPv6 configuration mode.
Step 12	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip6#**set address***ipv6-address*	Sets the name of the inband IPv6 static address.
Step 13	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip6#**set default-gw***gateway-ipv6*	Sets up the default gateway IPv6 address.
Step 14	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip6#**set prefix***prefix*	Sets up the network prefix.
Step 15	UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip6#**commit-buffer**	Commits the transaction in the system configuration.

The following example shows how to configure an inband static management IP interface:

```
UCSC#scope system
UCSC/system#scope org org1
UCSC/org# scope service-profile sp2
UCSC/org/service-profile# create mgmt-iface inband1
UCSC/org/service-profile/mgmt-iface#create mgmt-vlan
UCSC/org/service-profile/mgmt-iface/mgmt-vlan# create ext-static-ip
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip# set addr <ipv4-address>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip# set default-gw <gateway-ip>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip# set prefix <prefix>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip# exit
UCSC/org/service-profile/mgmt-iface/mgmt-vlan# create ext-static-ip6
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip6# set addr <ipv6-address>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip6# set default-gw <gateway-ipv6>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-static-ip6# set prefix <prefix>
UCSC/org/service-profile/mgmt-iface/mgmt-vlan/ext-pooled-ip6# commit-buffer
```

What to Do Next

Associate the inband management IP interface service profile to a server.

Setting up an Outband Pooled Management IP Address

You can set up an outband pooled management IPv4 address.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters System mode.
Step 2	UCSC/System#**scope org***org-name*	Enters organization mode for the specific organization.
Step 3	UCSC/org#**scope service-profile***service-profile-name*	Enters the service profile mode.
Step 4	UCSC/org/service-profile#**set ext-mgmt-ip-state pooled**	Sets up the external management IP pool.
Step 5	UCSC/org/service-profile#**set ext-mgmt-ip-pool-name***pool-name*	Sets the name of the external management IP pool.
Step 6	UCSC/org/service-profile#**commit-buffer**	Commits the transaction in the system configuration.

The following example shows how to set up an outband pooled management IP address:

```
UCSC#scope system
UCSC/system#scope org org1
UCSC/org# scope service-profile sp1
UCSC/org/service-profile# set ext-mgmt-ip-state pooled
UCSC/org/service-profile#set ext-mgmt-ip-pool-name ipool1
UCSC/org/service-profile# commit-buffer
```

Setting up an Outband Static Management IP Address

You can set up a static outband management IP address.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters System mode.
Step 2	UCSC/System#**scope org***org-name*	Enters organization mode for the specific organization.
Step 3	UCSC/org#**scope service-profile***service-profile-name*	Enters the service profile mode.
Step 4	UCSC/org/service-profile#**set ext-mgmt-ip-state static**	Sets up the state of the external management IP.
Step 5	UCSC/org/service-profile#**create ext-static-ip**	Creates a static external IP.

	Command or Action	Purpose
Step 6	UCSC/org/service-profile/ext-static-ip#**set addr***ip-address*	Sets the IP address.
Step 7	UCSC/org/service-profile/ext-static-ip#**set default-gw***gateway ip-address*	Sets the default gateway IP address.
Step 8	UCSC/org/service-profile/ext-static-ip#**commit-buffer**	Commits the transaction in the system configuration.

The following example shows how to set up an outband static management IP address:

```
UCSC#scope system
UCSC/system#scope org org1
UCSC/org# scope service-profile sp1
UCSC/org/service-profile# set ext-mgmt-ip-state static
UCSC/org/service-profile# create ext-static-ip
UCSC/org/service-profile/ext-static-ip#set addr <ip-address>
UCSC/org/service-profile/ext-static-ip#set default-gw <gateway ip-address>
UCSC/org/service-profile/ext-static-ip# commit-buffer
```

Deleting a Global Service Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr)# /org # **show service-profile**	Displays the existing service profiles and service profile templates.
Step 4	UCSC(resource-mgr)# /org # **delete service-profile** *profile-name*	Deletes the specified service profile.
Step 5	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a service profile and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org # show service-profile
Service Profile:
    Service Profile Name Type              System Id  Server    Assignment Association
    -------------------- ----------------- ---------- --------- ---------- -----------
    GSP_temp             Initial Template                       Unassigned Unassociated
    GSP2                 Instance                               Unassigned Unassociated
    test-upd_temp        Updating Template                      Unassigned Unassociated
    test2                Instance                               Unassigned Unassociated
```

```
UCSC(resource-mgr) /org* # delete service-profile GSP2
UCSC(resource-mgr) /org* # commit-buffer
UCSC(resource-mgr) /org #
```

Global Service Profile Template

Global service profile templates enable to quickly create several service profiles with the same basic parameters, such as the number of vNICs and vHBAs, and with identity information drawn from the same pools. The service profile template in Cisco UCS Central is similar to the service profile templates in Cisco UCS Manager.

Creating a Global Service Profile Template

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr)# /org # **create service-profile** *profile-name* {**initial-template** | **updating-template**}	Creates the specified service profile template and enters organization service profile mode. This name can be between 2 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and this name must be unique across all service profiles and service profile templates within the same organization. You can create service profile templates using the following options: • initial-template—Service profiles created from this template will not update if this template is updated. • updating-template—Service profiles created from this template will automatically update if this template is updated.
Step 4	UCSC(resource-mgr) /org/service-profile # **set bios-policy** *policy-name*	Associates the specified BIOS policy with the service profile template.
Step 5	UCSC(resource-mgr) /org/service-profile # **set boot-policy** *policy-name*	Associates the specified boot policy with the service profile template.

	Command or Action	Purpose
Step 6	UCSC(resource-mgr) /org/service-profile # **set descr** *description*	(Optional) Provides a description for the service profile template. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 7	UCSC(resource-mgr) /org/service-profile # **set dynamic-vnic-conn-policy** *policy-name*	Associates the specified dynamic vNIC connection policy with the service profile template.
Step 8	UCSC(resource-mgr) /org/service-profile # **set extippoolname** *pool-name*	Associates the specified external IP pool with the service profile template.
Step 9	UCSC(resource-mgr) /org/service-profile # **set extipstate** *pool-name*	Specifies how the external IP address will be assigned to the service profile template. You can set the IP address policy using the following options: • None—The service profile is not assigned an IP address. • Pooled—The service profile is assigned an IP address from the IP pool. • Static—The service profile is assigned the configured IP address.
Step 10	UCSC(resource-mgr) /org/service-profile # **set host-fw-policy** *policy-name*	Associates the specified host firmware policy with the service profile template.
Step 11	UCSC(resource-mgr) /org/service-profile # **set identity** {**dynamic-uuid** {*uuid* | **derived**} | **dynamic-wwnn** {*wwnn* | **derived**} | **uuid-pool** *pool-name* | **wwnn-pool** *pool-name*}	Specifies how the server acquires a UUID or WWNN. You can do one of the following: • Create a unique UUID in the form *nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn* . • Derive the UUID from the one burned into the hardware at manufacture. • Use a UUID pool. • Create a unique WWNN in the form *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* . • Derive the WWNN from one burned into the hardware at manufacture. • Use a WWNN pool.

	Command or Action	Purpose
Step 12	UCSC(resource-mgr) /org/service-profile # **set ipmi-access-profile** *profile-name*	Associates the specified IPMI access profile with the service profile template.
Step 13	UCSC(resource-mgr) /org/service-profile # **set iscsi-identity** {**initiator-name** *initiator-name* | **initiator-pool-name** *iqn-pool-name*	Specifies the name of the iSCSI initiator or the name of an IQN pool from which the iSCSI initiator name will be provided. The iSCSI initiator name can be up to 223 characters.
Step 14	UCSC(resource-mgr) /org/service-profile # **set lan-connectivity-policy-name** *policy-name*	Associates the specified LAN connectivity policy with the service profile template. **Note** You cannot have a LAN connectivity policy and locally created vNICs in the same service profile. When you add a LAN connectivity policy to a service profile, any existing vNIC configuration is erased.
Step 15	UCSC(resource-mgr) /org/service-profile # **set local-disk-policy** *policy-name*	Associates the specified local disk policy with the service profile template.
Step 16	UCSC(resource-mgr) /org/service-profile # **set maintpolicyname** *policy-name*	Associates the specified maintenance policy with the service profile template.
Step 17	UCSC(resource-mgr) /org/service-profile # **set power-control-policy** *policy-name*	Associates the specified power control policy with the service profile template.
Step 18	UCSC(resource-mgr) /org/service-profile # **set san-connectivity-policy-name** *policy-name*	Associates the specified SAN connectivity policy with the service profile template. **Note** You cannot have a SAN connectivity policy and locally created vHBAs in the same service profile. When you add a SAN connectivity policy to a service profile, any existing vHBA configuration is erased.
Step 19	UCSC(resource-mgr) /org/service-profile # **set scrub-policy** *policy-name*	Associates the specified scrub policy with the service profile template.
Step 20	UCSC(resource-mgr) /org/service-profile # **set sol-policy** *policy-name*	Associates the specified serial over LAN policy with the service profile template.
Step 21	UCSC(resource-mgr) /org/service-profile # **set stats-policy** *policy-name*	Associates the specified statistics policy with the service profile template.
Step 22	UCSC(resource-mgr) /org/service-profile # **set user-label** *label-name*	Specifies the user label associated with the service profile template.

	Command or Action	Purpose
Step 23	UCSC(resource-mgr) /org/service-profile # **set vcon** {**1** | **2** | **3** | **4**} **select** {**all** | **assigned-only** | **exclude-dynamic** | **exclude-unassigned**}	Specifies the selection preference for the specified vCon.
Step 24	UCSC(resource-mgr) /org/service-profile # **set vcon-policy** *policy-name*	Associates the specified vNIC/vHBA placement policy with the service profile template. **Note** You can either assign a vNIC/vHBA placement policy to the service profile, or set vCon selection preferences for the service profile, but you do not need to do both.
Step 25	UCSC(resource-mgr) /org/service-profile # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a service profile template and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # create service-profile GSP_temp2 initial-template
UCSC(resource-mgr) /org/service-profile* # set bios-policy biospol1
UCSC(resource-mgr) /org/service-profile* # set boot-policy bootpol32
UCSC(resource-mgr) /org/service-profile* # set  descr "This is a global service profile
template example."
UCSC(resource-mgr) /org/service-profile* # set dynamic-vnic-conn-policy mydynvnicconnpolicy
UCSC(resource-mgr) /org/service-profile* # set extippoolname myippool
UCSC(resource-mgr) /org/service-profile* # set extipstate pooled
UCSC(resource-mgr) /org/service-profile* # set host-fw-policy ipmi-user987
UCSC(resource-mgr) /org/service-profile* # set identity dynamic-uuid derived
UCSC(resource-mgr) /org/service-profile* # set ipmi-access-profile ipmiProf16
UCSC(resource-mgr) /org/service-profile* # set local-disk-policy localdiskpol33
UCSC(resource-mgr) /org/service-profile* # set maintpolicyname maintpol4
UCSC(resource-mgr) /org/service-profile* # set power-control-policy powcontrpol13
UCSC(resource-mgr) /org/service-profile* # set scrub-policy scrubpol55
UCSC(resource-mgr) /org/service-profile* # set sol-policy solpol2
UCSC(resource-mgr) /org/service-profile* # set stats-policy statspol4
UCSC(resource-mgr) /org/service-profile* # set user-label mylabel
UCSC(resource-mgr) /org/service-profile* # set vcon-policy myvconnpolicy
UCSC(resource-mgr) /org/service-profile* # commit-buffer
UCSC(resource-mgr) /org/service-profile #
```

Global Service Profile Deployment

When you deploy a global service profile from Cisco UCS Central, the service profile definition is sent to the Cisco UCS domain. Then the Cisco UCS domain identifies the server and deploys the service profile to the server. The service profile definition that is sent to the Cisco UCS domain includes the following information :

- Service profile with reference policy names
- vNICs and vHBAs along with their vLAN bindings
- VCON assignment information for placement of VIFs in to appropriate VCON

- The global VLAN and VSAN definition referred to by a vNIC or vHVA in this service profile

You can deploy the global service profile to any of the compute element in either one of the following two ways:

- Direct assignment: Assign the global service profile to one of the available server in any of the registered Cisco UCS domain. You can also pre-provision a non-existent server.
- Server pool assignment: Assign the global service profile to a server pool. The global service profile will pick one of the available server from the pool for association.
- When the Cisco UCS domain receives the global service profile, the Cisco UCS Domain does the following:
  - Configures the global service profile at the local level
  - Resolves the VLAN and VSAN conditions
  - Reports the configuration and operational states to Cisco UCS Central

Scheduling Service Profile Updates

Deferred Deployment of Service Profiles

Some modifications to a service profile or to an updating service profile template can be disruptive and require a reboot of the server. You can, however, configure deferred deployment to control when those disruptive configuration changes are implemented. For example, you can choose to deploy the service profile changes immediately or have them deployed during a specified maintenance window. You can also choose whether or not a service profile deployment requires explicit user acknowledgement.

Deferred deployment is available for all configuration changes that occur through the association of a service profile with a server. These configuration changes can be prompted by a change to a service profile, to a policy that is included in a service profile, or to an updating service profile template. For example, you can defer the upgrade and activation of firmware through host firmware packages and management firmware packages, such as server BIOS, RAID controller, host HBA, and network adapters. However, you cannot defer the direct deployment of firmware images for components that do not use either of the firmware packages, such as Cisco UCS Central, fabric interconnects, and I/O modules.

Deferred deployment is not available for the following actions which require the reboot of a server:

- Initial association of a service profile with a server
- Final disassociation of a service profile from a server, without associating the service profile with a different server
- Decommissioning a server
- Reacknowledging a server
- Resetting a server

If you want to defer the deployment of service profile changes, you must configure one or more maintenance policies and configure each service profile with a maintenance policy. If you want to define the time period

when the deployment should occur, you also need to create at least one schedule with one or more recurring occurrences or one time occurrences, and include that schedule in a maintenance policy.

Guidelines and Limitations for Deferred Deployment

Cannot Undo All Changes to Service Profiles or Service Profile Templates

If you cancel a pending change, Cisco UCS Central attempts to roll back the change without rebooting the server. However, for complex changes, Cisco UCS Central may have to reboot the server a second time to roll back the change. For example, if you delete a vNIC, Cisco UCS Central reboots the server according to the maintenance policy included in the service profile. You cannot cancel this reboot and change, even if you restore the original vNIC in the service profile. Instead, Cisco UCS Central schedules a second deployment and reboot of the server.

Association of Service Profile Can Exceed Boundaries of Maintenance Window

After Cisco UCS Central begins the association of the service profile, the scheduler and maintenance policy do not have any control over the procedure. If the service profile association does not complete within the allotted maintenance window, the process continues until it is completed. For example, this can occur if the association does not complete in time because of retried stages or other issues.

Cannot Specify Order of Pending Activities

Scheduled deployments run in parallel and independently. You cannot specify the order in which the deployments occur. You also cannot make the deployment of one service profile change dependent upon the completion of another.

Cannot Perform Partial Deployment of Pending Activity

Cisco UCS Central applies all changes made to a service profile in the scheduled maintenance window. You cannot make several changes to a service profile at the same time and then have those changes be spread across several maintenance windows. When Cisco UCS Central deploys the service profile changes, it updates the service profile to match the most recent configuration in the database.

Deferred Deployment Schedules

A schedule contains a set of occurrences. These occurrences can be one time only or can recur at a specified time and day each week. The options defined in the occurrence, such as the duration of the occurrence or the maximum number of tasks to be run, determine whether a service profile change is deployed. For example, if a change cannot be deployed during a given maintenance window because the maximum duration or number of tasks has been reached, that deployment is carried over to the next maintenance window.

Each schedule checks periodically to see whether the Cisco UCS domain has entered one or more maintenance windows. If it has, the schedule executes the deployments that are eligible according to the constraints specified in the maintenance policy

A schedule contains one or more occurrences, which determine the maintenance windows associated with that schedule. An occurrence can be one of the following:

One Time Occurrence

One time occurrences define a single maintenance window. These windows continue until the maximum duration of the window or the maximum number of tasks that can be run in the window has been reached.

Recurring Occurrence

Recurring occurrences define a series of maintenance windows. These windows continue until the maximum number of tasks or the end of the day specified in the occurrence has been reached.

Maintenance Policy

A maintenance policy determines how Cisco UCS Central reacts when a change that requires a server reboot is made to a service profile associated with a server or to an updating service profile bound to one or more service profiles.

The maintenance policy specifies how Cisco UCS Central deploys the service profile changes. The deployment can occur in one of the following ways:

- Immediately
- When acknowledged by a user with admin privileges
- Automatically at the time specified in a schedule

If the maintenance policy is configured to deploy the change during a scheduled maintenance window, the policy must include a valid 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

Pending Activities

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

If a Cisco UCS domain has pending activities, 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

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

Configuring Schedules

Creating a Schedule

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create schedule** *schedule-name*	Creates a schedule and enters schedule mode.
Step 4	UCSC(policy-mgr) /domain-group/schedule # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a schedule and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create schedule MaintSched1
UCSC(policy-mgr) /domain-group/schedule* # commit-buffer
UCSC(policy-mgr) /domain-group/schedule #
```

Creating a One Time Occurrence for a Schedule

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope schedule** *schedule-name*	Enters schedule mode for the specified schedule.
Step 4	UCSC(policy-mgr) /domain-group/schedule # **set admin-state user-ack**	Specifies user acknowledgment is required for the specified schedule.
Step 5	UCSC(policy-mgr) /domain-group/schedule # **create occurrence one-time** *occurrence-name*	Creates a one time occurrence.
Step 6	UCSC(policy-mgr) /domain-group/schedule/one-time # **set concur-tasks** {**unlimited** | *max-num-concur-tasks*}	Sets the maximum number of tasks that can run concurrently during this occurrence. If the maximum number of tasks is reached, the scheduler waits for the amount of time set in the minimum interval property before scheduling new tasks.
Step 7	UCSC(policy-mgr) /domain-group/schedule/one-time # **set date** *month day-of-month year hour minute*	Sets the date and time this occurrence should run.
Step 8	UCSC(policy-mgr) /domain-group/schedule/one-time # **set max-duration** {*none* | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	Sets the maximum length of time that this schedule occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time.
Step 9	UCSC(policy-mgr) /domain-group/schedule/one-time # **set min-interval** {*none* | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	Sets the minimum length of time that the system should wait before starting a new task.
Step 10	UCSC(policy-mgr) /domain-group/schedule/one-time # **set proc-cap** {**unlimited** | *max-num-of-tasks*}	Sets the maximum number of scheduled tasks that can be run during this occurrence.
Step 11	UCSC(policy-mgr) /domain-group/schedule/one-time # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a one time occurrence called onetimemaint for a schedule called maintsched, set the maximum number of concurrent tasks to 5, set the start date to September 1, 2013 at 11:00, and commits the transaction:

```
UCSC# scope system
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope schedule maintsched
UCSC(policy-mgr) /domain-group/schedule # create occurrence one-time onetimemaint
UCSC(policy-mgr) /domain-group/schedule/one-time* # set date sep 1 2013 11 00
UCSC(policy-mgr) /domain-group/schedule/one-time* # set concur-tasks 5
UCSC(policy-mgr) /domain-group/schedule/one-time* # commit-buffer
UCSC(policy-mgr) /domain-group/schedule/one-time #
```

Creating a Recurring Occurrence for a Schedule

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope schedule** *schedule-name*	Enters schedule mode for the specified schedule.
Step 4	UCSC(policy-mgr) /domain-group/schedule # **set admin-state user-ack**	Specifies user acknowledgment is required for the specified schedule.
Step 5	UCSC(policy-mgr) /domain-group/schedule # **create occurrence recurring** *occurrence-name*	Creates a recurring occurrence.
Step 6	UCSC(policy-mgr) /domain-group/schedule/recurring # **set concur-tasks** {**unlimited** | *max-num-concur-tasks*}	Sets the maximum number of tasks that can run concurrently during this occurrence. If the maximum number of tasks is reached, the scheduler waits for the amount of time set in the minimum interval property before scheduling new tasks.
Step 7	UCSC(policy-mgr) /domain-group/schedule/recurring # **set day** {**even-day** | **every-day** | **friday** | **monday** | **never** | **odd-day** | **saturday** | **sunday** | **thursday** | **tuesday** | **wednesday**}	Specifies the day on which Cisco UCS runs an occurrence of this schedule. By default, this property is set to never.
Step 8	UCSC(policy-mgr) /domain-group/schedule/recurring # **set hour** *hour*	Specifies the hour at which this occurrence starts.

	Command or Action	Purpose
		Note Cisco UCS ends all recurring occurrences on the same day in which they start, even if the maximum duration has not been reached. For example, if you specify a start time of 11 p.m. and a maximum duration of 3 hours, Cisco UCS starts the occurrence at 11 p.m. but ends it at 11:59 p.m. after only 59 minutes.
Step 9	UCSC(policy-mgr) /domain-group/schedule/recurring # **set minute** *minute*	Specifies the minute at which this occurrence starts.
Step 10	UCSC(policy-mgr) /domain-group/schedule/recurring # **set max-duration** {*none* | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	Sets the maximum length of time that this schedule occurrence can run. Cisco UCS completes as many scheduled tasks as possible within the specified time.
Step 11	UCSC(policy-mgr) /domain-group/schedule/recurring # **set min-interval** {*none* | *num-of-days num-of-hours num-of-minutes num-of-seconds*}	Sets the minimum length of time that the system should wait before starting a new task.
Step 12	UCSC(policy-mgr) /domain-group/schedule/recurring # **set proc-cap** {**unlimited** | *max-num-of-tasks*}	Sets the maximum number of scheduled tasks that can be run during this occurrence.
Step 13	UCSC(policy-mgr) /domain-group/schedule/recurring # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a recurring occurrence called recurmaint for a schedule called maintsched, set the maximum number of concurrent tasks to 5, sets the day this occurrence will run to even days, sets the time it will start to 11:05, and commits the transaction:

```
UCSC# scope system
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope schedule maintsched
UCSC(policy-mgr) /domain-group/schedule # create occurrence recurring recurmaint
UCSC(policy-mgr) /domain-group/schedule/recurring* # set day even-day
UCSC(policy-mgr) /domain-group/schedule/recurring* # set hour 11
UCSC(policy-mgr) /domain-group/schedule/recurring* # set minute 5
UCSC(policy-mgr) /domain-group/schedule/recurring* # set concur-tasks 5
UCSC(policy-mgr) /domain-group/schedule/recurring* # commit-buffer
UCSC(policy-mgr) /domain-group/schedule/recurring #
```

Configuring Maintenance Policies

Creating a Maintenance Policy

Before You Begin

If you plan to configure this maintenance policy for deferred deployment, create a schedule.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create maint-policy** *policy-name*	Creates the specified maintenance policy and enters maintenance policy mode.
Step 4	UCSC(policy-mgr) /domain-group/maint-policy # **set reboot-policy** {**immediate** | **timer-automatic** | **user-ack**}	When a service profile is associated with a server, the server needs to be rebooted to complete the association. Specifying the reboot-policy command determines when the reboot occurs for all service profiles that include this maintenance policy. Possible values include: • **immediate—**The server reboots as soon as the change is made to the service profile. • **timer-automatic —**You select the schedule that specifies when maintenance operations can be applied to the server using the set scheduler command. Cisco UCS reboots the server and completes the service profile changes at the scheduled time. • **user-ack —**The user must explicitly acknowledge the changes by using the **apply pending-changes** command before changes are applied.
Step 5	UCSC(policy-mgr) /domain-group/maint-policy # **set scheduler** *scheduler-name*	(Optional) If the reboot-policy property is set to timer-automatic, you must select the schedule that specifies when maintenance operations can be applied to the server. Cisco UCS reboots the server and completes the service profile changes at the scheduled time.
Step 6	UCSC(policy-mgr) /domain-group/maint-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a maintenance policy called MaintPol1, set the system to reboot immediately when a service profile is associated with a server, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(Policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group# create maint-policy MaintPol1
UCSC(policy-mgr) /domain-group/maint-policy* # set reboot-policy immediate
UCSC(policy-mgr) /domain-group/maint-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/maint-policy #
```

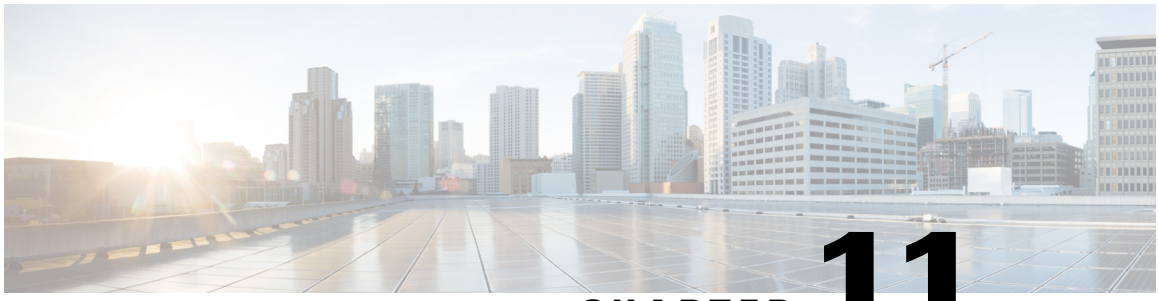
Deleting a Maintenance Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete maint-policy** *policy-name*	Deletes the specified maintenance policy.
Step 4	UCSC(policy-mgr) /org #	Commits the transaction to the system configuration.

The following example shows how to delete a maintenance policy called maintenance and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/org # delete maint-policy maintenance
UCSC(policy-mgr)/org* # commit-buffer
UCSC(policy-mgr)/org #
```



CHAPTER 11

Server Policies

This chapter includes the following sections:

Configuring Server Pools

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.

Creating a Server Pool

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr) /org # **create server-pool** *server-pool-name*	Creates a server pool with the specified name, and enters organization server pool mode.
Step 4	UCSC(resource-mgr) /org/server-pool # **create server** *chassis-num/slot-num*	Creates a server for the server pool. **Note** A server pool can contain more than one server. To create multiple servers for the pool, you must enter multiple create server commands from organization server pool mode.
Step 5	UCSC(resource-mgr) /org/server-pool # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create the server pool named ServPool2, create two servers for the server pool, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org # create server-pool ServPool2
UCSC(resource-mgr) /org/server-pool* # create server 1/1
UCSC(resource-mgr) /org/server-pool* # create server 1/4
UCSC(resource-mgr) /org/server-pool* # commit-buffer
UCSC(resource-mgr) /org/server-pool #
```

Deleting a Server Pool

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(resource-mgr) /org # **delete server-pool** *server-pool-name*	Deletes the specified server pool.

	Command or Action	Purpose
Step 4	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete the server pool named ServPool2 and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org # delete server-pool ServPool2
UCSC(resource-mgr) /org* # commit-buffer
UCSC(resource-mgr) /org #
```

Configuring IP Pools

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 Manager servers.
- 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 addresses, 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 can not be used for those sites.

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

Creating an IP Pool

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create ip-pool** *pool-name*	Creates an IP pool with the specified name, and enters organization IP pool mode.
Step 4	UCSC(policy-mgr) /org/ip-pool # **set descr** *description*	(Optional) Provides a description for the IP pool. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/ip-pool # **create block** *first-ip-addr last-ip-addr gateway-ip-addr subnet-mask*	Creates a block (range) of IP addresses, and enters organization IP pool block mode. You must specify the first and last IP addresses in the address range, the gateway IP address, and subnet mask. **Note** An IP pool can contain more than one IP block. To create multiple blocks, enter multiple **create block** commands from organization IP pool mode.
Step 6	UCSC(policy-mgr) /org/ip-pool/block # **set primdns** *ip-address* **secdns** *ip-address*	Specifies the primary DNS and secondary DNS IP addresses.
Step 7	UCSC(policy-mgr) /org/ip-pool/block #**set scope** {**private** | **public**}	Specifies whether the IP addresses is private or public.
Step 8	UCSC(policy-mgr) /org/ip-pool/block # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to create another pool, wait at least 5 seconds.

The following example shows how to create an IP pool named GPool1, provide a description for the pool, specify a block of IP addresses and a primary and secondary IP address to be used for the pool, set the pool to private, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create ip-pool GPool1
UCSC(policy-mgr) /org/ip-pool* # set descr "This is IP pool GPool1"
UCSC(policy-mgr) /org/ip-pool* # create block 192.168.100.1 192.168.100.200 192.168.100.10
```

```
 255.255.255.0
UCSC(policy-mgr) /org/ip-pool/block* # set primdns 192.168.100.1 secdns 192.168.100.20
UCSC(policy-mgr) /org/ip-pool/block* # set scope private
UCSC(policy-mgr) /org/ip-pool/block* # commit-buffer
UCSC(policy-mgr) /org/ip-pool/block #
```

What to Do Next

Include the IP pool in a service profile and/or template.

Creating an IP Pool with IPv6 Blocks

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) /org # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type/ as the *org-name*
Step 3	UCSC(policy-mgr) /org # **create ip-pool** *global-ip-pool*	Creates a global IP pool with the specified name, and enters the global IP pool mode.
Step 4	UCSC(policy-mgr) /org/ip-pool # **set descr** *description*	(Optional) Provides a description for the IP pool. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/ip-pool # **create ipv6-block** *first-ip-addr last-ip-addr default-gateway ip address prefix*	Creates a block (range) of IP addresses, and enters organization IP pool block mode. You must specify the first and last IP addresses in the address range, the default gateway IP address, and the prefix. **Note** To create multiple blocks, enter multiple **create ipv6-block** commands.
Step 6	UCSC(policy-mgr) /org/ip-pool/ipv6-block # **set primdns** *ip-address* **secdns** *ip-address*	Specifies the primary DNS and secondary DNS IP addresses.
Step 7	UCSC(policy-mgr) /org/ip-pool/ipv6-block #**set qualifier** *word*	Sets the IPv6 block to an existing ID range qualifier name.
Step 8	UCSC(policy-mgr) /org/ip-pool/ipv6-block # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to create another pool, wait at least 5 seconds.

The following example shows how to create an IP pool with and IPv6 block:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org org-name
UCSC(policy-mgr) /org # create ip-pool global-ip-pool
UCSC(policy-mgr) /org/ip-pool* # set descr "This is global-ip-pool gpool1"
UCSC(policy-mgr) /org/ip-pool* # create ipv6-block 2001:db8:111::a1 2001:db8:111::af
2001:db8:111::1 64
UCSC(policy-mgr) /org/ip-pool/ipv6-block* #  set primdns 2001:db8:111::FF secdns
2001:db8:111::FE
UCSC(policy-mgr) /org/ip-pool/ipv6-block* # set qualifier Q1
UCSC(policy-mgr) /org/ip-pool/ipv6-block* # commit-buffer
UCSC(policy-mgr) /org/ip-pool/ipv6-block #
```

Deleting an IP 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.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete ip-pool** *pool-name*	Deletes the specified IP pool.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to delete another pool, wait at least 5 seconds.

The following example shows how to delete the IP pool named GPool1 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete ip-pool GPool1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring IQN Pools

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 sharing the same prefix.

Creating an IQN Pool

Note In most cases, the maximum 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.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create iqn-pool** *pool-name*	Creates an IQN pool with the specified name, and enters organization IQN pool mode. This name can be between 1 and 32 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Step 4	UCSC(policy-mgr) /org/iqn-pool # **set iqn-prefix** *prefix*	Specifies the prefix for the IQN block members. Unless limited by the adapter card, the prefix can contain up to 150 characters.
Step 5	UCSC(policy-mgr) /org/iqn-pool # **set descr** *description*	(Optional) Provides a description for the IQN pool. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), and ' (single quote). **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/iqn-pool # **create block** *suffix from to*	Creates a block (range) of IQNs, and enters organization IQN pool block mode. You must specify the base suffix, the starting suffix number, and the ending suffix number. The resulting IQN pool members are of the form *prefix*:*suffix*:*number*. The suffix can be up to 64 characters. **Note** An IQN pool can contain more than one IQN block. To create multiple blocks, enter multiple **create block** commands from organization IQN pool mode.
Step 7	UCSC(policy-mgr) /org/iqn-pool/block # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to create another pool, wait at least 5 seconds.

The following example shows how to create an IQN pool named GPool1, provide a description for the pool, specify a prefix and a block of suffixes to be used for the pool, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create iqn-pool GPool1
UCSC(policy-mgr) /org/iqn-pool* # set iqn-prefix iqn.alpha.com
UCSC(policy-mgr) /org/iqn-pool* # set descr "This is IQN pool GPool1"
UCSC(policy-mgr) /org/iqn-pool* # create block beta 3 5
UCSC(policy-mgr) /org/iqn-pool/block* # commit-buffer
UCSC(policy-mgr) /org/iqn-pool/block #
```

What to Do Next

Include the IQN suffix pool in a service profile and/or template.

Deleting an IQN 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.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete iqn-pool** *pool-name*	Deletes the specified IQN pool.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to delete another pool, wait at least 5 seconds.

The following example shows how to delete the IQN pool named GPool1 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete iqn-pool GPool1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring UUID Suffix Pools

UUID Suffix Pools

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. 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.

Creating a UUID Suffix Pool

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **create uuid-suffix-pool** *pool-name*	Creates a UUID suffix pool with the specified name, and enters organization UUID suffix pool mode.
Step 4	UCSC(policy-mgr) /org/uuid-suffix-pool # **set descr** *description*	(Optional) Provides a description for the UUID suffix pool. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/uuid-suffix-pool # **create block** *first-uuid last-uuid*	Creates a block (range) of UUID suffixes, and enters organization UUID suffix pool block mode. You must specify the first and last UUID suffixes in the block using the form *nnnn-nnnnnnnnnnnn*, with the UUID suffixes separated by a space. **Note** A UUID suffix pool can contain more than one UUID suffix block. To create multiple UUID suffix blocks, you must enter multiple **create block** commands from organization UUID suffix pool mode.
Step 6	UCSC(policy-mgr) /org/uuid-suffix-pool/block # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to create another pool, wait at least 5 seconds.

The following example shows how to create a UUID suffix pool named GPool1, provide a description for the pool, specify a block of UUID suffixes to be used for the pool, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create uuid-suffix-pool GPool1
UCSC(policy-mgr) /org/uuid-suffix-pool* # set descr "This is UUID suffix pool GPool1"
UCSC(policy-mgr) /org/uuid-suffix-pool* # create block 1000-000000000001 1000-000000000010
UCSC(policy-mgr) /org/uuid-suffix-pool/block* # commit-buffer
UCSC(policy-mgr) /org/uuid-suffix-pool/block #
```

What to Do Next

Include the UUID suffix pool in a service profile and/or template.

Deleting a UUID Suffix 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.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete uuid-suffix-pool** *pool-name*	Deletes the specified UUID suffix pool.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to delete another pool, wait at least 5 seconds.

The following example shows how to delete the UUID suffix pool named GPool1 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete uuid-suffix-pool GPool1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Server-Related Policies

Ethernet and Fibre Channel Adapter Policies

These 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 an apparent 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 5s 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 Ethernet adapter policies and 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.

Important 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.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), 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

Configuring an Ethernet Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create eth-policy** *policy-name*	Creates the specified Ethernet adapter policy and enters organization Ethernet policy mode.
Step 4	UCSC(policy-mgr) /org/eth-policy # **set comp-queue count** *count*	(Optional) Configures the Ethernet completion queue.
Step 5	UCSC(policy-mgr) /org/eth-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 6	UCSC(policy-mgr) /org/eth-policy # **set failover timeout** *timeout-sec*	(Optional) Configures the Ethernet failover.
Step 7	UCSC(policy-mgr) /org/eth-policy # **set interrupt** {**coalescing-time** *sec* | **coalescing-type** {**idle** | **min**} | **count** *count* | **mode** {**intx** | **msi** | **msi-x**}}	(Optional) Configures the Ethernet interrupt.
Step 8	UCSC(policy-mgr) /org/eth-policy # **set offload** {**large-receive** | **tcp-rx-checksum** | **tcp-segment** | **tcp-tx-checksum**} {**disabled** | **enabled**}	(Optional) Configures the Ethernet offload.
Step 9	UCSC(policy-mgr) /org/eth-policy # **set recv-queue** {**count** *count* | **ring-size** *size-num*}	(Optional) Configures the Ethernet receive queue.
Step 10	UCSC(policy-mgr) /org/eth-policy # **set rss receivesidescaling** {**disabled** | **enabled**}	(Optional) Configures the RSS.
Step 11	UCSC(policy-mgr) /org/eth-policy # **set trans-queue** {**count** *count* | **ring-size** *size-num*}	(Optional) Configures the Ethernet transmit queue.
Step 12	UCSC(policy-mgr) /org/eth-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures an Ethernet adapter policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create eth-policy EthPolicy19
UCSC(policy-mgr) /org/eth-policy* # set comp-queue count 16
UCSC(policy-mgr) /org/eth-policy* # set descr "This is an Ethernet adapter policy example."
```

```
UCSC(policy-mgr) /org/eth-policy* # set failover timeout 300
UCSC(policy-mgr) /org/eth-policy* # set interrupt count 64
UCSC(policy-mgr) /org/eth-policy* # set offload large-receive disabled
UCSC(policy-mgr) /org/eth-policy* # set recv-queue count 32
UCSC(policy-mgr) /org/eth-policy* # set rss receivesidescaling enabled
UCSC(policy-mgr) /org/eth-policy* # set trans-queue
UCSC(policy-mgr) /org/eth-policy* # commit-buffer
UCSC(policy-mgr) /org/eth-policy #
```

Deleting an Ethernet Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete eth-policy** *policy-name*	Deletes the specified Ethernet adapter policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an Ethernet adapter policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete eth-policy EthPolicy19
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in an Cisco UCS domain. You can create one or more BIOS policies that include a specific grouping of BIOS settings that match the needs of a server or set of servers, or you can use the default BIOS settings for a specific server platform.

Both the BIOS policy and the default BIOS settings for a server platform enable you to fine tune the BIOS settings for a server managed by Cisco UCS Central.

Depending upon the needs of the data center, you can configure BIOS policies for some service profiles and use the BIOS defaults in other service profiles in the same Cisco UCS domain, or you can use only one of them. You can also use Cisco UCS Central to view the actual BIOS settings on a server and determine whether they are meeting current needs.

Note Cisco UCS Central pushes BIOS configuration changes through a BIOS policy or default BIOS settings to the Cisco Integrated Management Controller (CIMC) buffer. These changes remain in the buffer and do not take effect until the server is rebooted.

We recommend that you verify the support for BIOS settings in the server that you want to configure. Some settings, such as Mirroring Mode for RAS Memory, are not supported by all Cisco UCS servers.

BIOS Policy

The BIOS policy is a policy that 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.

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.

Creating a BIOS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	Configure the BIOS settings	For the CLI commands, descriptions and information about the options for each BIOS setting, see the following topics: • Main BIOS Settings, on page 277 • Processor BIOS Settings, on page 279 • Intel Directed I/O BIOS Settings, on page 291 • RAS Memory BIOS Settings, on page 293 • Serial Port BIOS Settings, on page 295 • USB BIOS Settings, on page 295 • PCI Configuration BIOS Settings, on page 296 • Boot Options BIOS Settings, on page 297 • Server Management BIOS Settings, on page 298
Step 4	UCSC(policy-mgr) /org/bios-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a BIOS policy under the root organization and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/ org #create bios-policy biosPolicy3
UCSC(policy-mgr) /org/bios-policy* # set numa-config numa-optimization enabled
UCSC(policy-mgr) /org/bios-policy* # commit-buffer
UCSC(policy-mgr) /org/bios-policy #
```

Viewing the Actual BIOS Settings for a Server

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope server** *chassis-id* / *server-id*	Enters chassis server mode for the specified server.
Step 4	UCSC(policy-mgr) /org /chassis/server # **scope bios**	Enters BIOS mode for the specified server.
Step 5	UCSC(policy-mgr) /org /chassis/server/bios # **scope bios-settings**	Enters BIOS settings mode for the specified server.
Step 6	UCSC(policy-mgr) /org /chassis/server/bios/bios-settings # **show** *setting*	Displays the BIOS setting. Enter **show ?** to display a list of allowed values for *setting* .

The following example displays a BIOS setting for blade 3 in chassis 1:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/org # scope server 1/3
UCSC(policy-mgr)/org /chassis/server # scope bios
UCSC(policy-mgr)/org /chassis/server/bios # scope  bios-settings
UCSC(policy-mgr)/org /chassis/server/bios/bios-settings # show intel-vt-config

Intel Vt Config:
    Vt
    --
    Enabled

UCSC(policy-mgr)/org /chassis/server/bios/bios-settings #
```

Modifying BIOS Defaults

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope system**	Enters system mode.
Step 4	UCSC(policy-mgr) /org /system # **scope server-defaults**	Enters server defaults mode.
Step 5	UCSC(policy-mgr) /org /system/server-defaults # **show platform**	(Optional) Displays platform descriptions for all servers.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org /system/server-defaults # **scope platform** *platform-description*	Enters server defaults mode for the server specified. For the *platform-description* argument, enter the server description displayed by the **show platform** command using the following format: "*vendor*" *model revision*. **Tip** You must enter the vendor exactly as shown in the **show platform** command, including all punctuation marks.
Step 7	UCSC(policy-mgr) /org /system/server-defaults/platform # **scope bios-settings**	Enters server defaults BIOS settings mode for the server.
Step 8	Reconfigure the BIOS settings.	For the CLI commands, descriptions and information about the options for each BIOS setting, see the following topics: • Main BIOS Settings, on page 277 • Processor BIOS Settings, on page 279 • Intel Directed I/O BIOS Settings, on page 291 • RAS Memory BIOS Settings, on page 293 • Serial Port BIOS Settings, on page 295 • USB BIOS Settings, on page 295 • PCI Configuration BIOS Settings, on page 296 • Boot Options BIOS Settings, on page 297 • Server Management BIOS Settings, on page 298
Step 9	UCSC(policy-mgr) /org /system/server-defaults/platform/bios-settings # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to change the NUMA default BIOS setting for a platform and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr)/org# scope system
UCSC(policy-mgr)/org /system # scope server-defaults
UCSC(policy-mgr)/org /system/server-defaults # show platform

Platform:
    Product Name Vendor     Model      Revision
    ------------ ---------- ---------- --------
    Cisco B200-M1
                 Cisco Systems, Inc.
                            N20-B6620-1
```

```
UCSC(policy-mgr)/org /system/server-defaults # scope platform "Cisco Systems, Inc."
N20-B6620-1 0
UCSC(policy-mgr)/org /system/server-defaults/platform # scope bios-settings
UCSC(policy-mgr)/org /system/server-defaults/platform/bios-settings # set numa-config
numa-optimization disabled
UCSC(policy-mgr)/org /system/server-defaults/platform/bios-settings* # commit-buffer
UCSC(policy-mgr)/org /system/server-defaults/platform/bios-settings #
```

Deleting a BIOS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete bios-policy** *policy-name*	Deletes the specified BIOS policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a BIOS policy under the root organization and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr)/ org #delete bios-policy biosPolicy3
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Main 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. 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. 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.
Quiet Boot	What the BIOS displays during Power On Self-Test (POST). This can be one of the following: • **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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Post Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • **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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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: • **stay-off—**The server remains off until manually powered on. • **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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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: • **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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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. • **—**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. • **—**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. • **—**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.
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. • **—**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.

Name	Description
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. • **—**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. • **—**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.
Hardware Pre-fetcher	Whether the processor allows the Intel hardware prefetcher to fetch streams of data and instruction from memory into the unified second-level cache when necessary. This can be one of the following: • **Disabled—**The hardware prefetcher is not used. • **Enabled—**The processor uses the hardware prefetcher when cache issues are detected. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** must be set to **Custom** in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.

Name	Description
Adjacent Cache Line Pre-fetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • **Disabled—**The processor only fetches the required line. • **Enabled—**The processor fetches both the required line and its paired line. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** must be set to **Custom** in order to specify this value. For any value other than **Custom**, this option is overridden by the setting in the selected CPU performance profile.
DCU Streamer Pre-fetch	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • **Enabled—**The DCU prefetcher analyzes the cache read pattern and prefetches the next line in the cache if it determines that it may be needed. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
DCU IP Pre-fetcher	Whether the processor uses the DCU IP Prefetch mechanism to analyze historical cache access patterns and preload the most relevant lines in the L1 cache. This can be one of the following: • **Disabled—**The processor does not preload any cache data. • **Enabled—**The DCU IP prefetcher preloads the L1 cache with the data it determines to be the most relevant. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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. • **—**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. • **—**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. • **—**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. • **—**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. • **—**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. • **—**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.
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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Local X2 APIC	Allows you to set the type of Application Policy Infrastructure Controller (APIC) architecture. This can be one of the following: • **xapic—**Uses the standard xAPIC architecture. • **x2apic—**Uses the enhanced x2APIC architecture to support 32 bit addressability of processors. • **auto—**Automatically uses the xAPIC architecture that is detected. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Power Technology	Enables you to configure the CPU power management settings for the following options: • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 Power Technology can be one of the following: • **Disabled—**The server does not perform any CPU power management and any settings for the BIOS parameters mentioned above are ignored. • **—**The server determines the best settings for the BIOS parameters mentioned above and ignores the individual settings for these parameters. • **Performance—**The server automatically optimizes the performance for the BIOS parameters mentioned above. • **Custom—**The server uses the individual settings for the BIOS parameters mentioned above. You must select this option if you want to change any of these BIOS parameters. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Energy Performance	Allows you to determine whether system performance or energy efficiency is more important on this server. This can be one of the following: • **performance** • **balanced-performance** • **balanced-energy** • **energy-efficient** • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
Frequency Floor Override	Whether the CPU is allowed to drop below the maximum non-turbo frequency when idle. This can be one of the following: • **Disabled—** The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • **Enabled—** The CPU cannot drop below the maximum non-turbo frequency when idle. This option improves system performance but may increase power consumption. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
P-STATE Coordination	Allows you to define how BIOS communicates the P-state support model to the operating system. There are 3 models as defined by the Advanced Configuration and Power Interface (ACPI) specification. • **HW_ALL—**The processor hardware is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package). • **SW_ALL—**The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a physical package), and must initiate the transition on all of the logical processors. • **SW_ANY—**The OS Power Manager (OSPM) is responsible for coordinating the P-state among logical processors with dependencies (all logical processors in a package), and may initiate the transition on any of the logical processors in the domain. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** must be set to **Custom** or the server ignores the setting for this parameter.

Name	Description
DRAM Clock Throttling	Allows you to tune the system settings between the memory bandwidth and power consumption. This can be one of the following: • **Balanced—** DRAM clock throttling is reduced, providing a balance between performance and power. • **Performance—**DRAM clock throttling is disabled, providing increased memory bandwidth at the cost of additional power. • **—**DRAM clock throttling is increased to improve energy efficiency. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Channel Interleaving	Whether the CPU divides memory blocks and spreads contiguous portions of data across interleaved channels to enable simultaneous read operations. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1-way—**Some channel interleaving is used. • **2-way** • **3-way** • **4-way—**The maximum amount of channel interleaving is used. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Rank Interleaving	Whether the CPU interleaves physical ranks of memory so that one rank can be accessed while another is being refreshed. This can be one of the following: • **Auto—**The CPU determines what interleaving is done. • **1-way—**Some rank interleaving is used. • **2-way** • **4-way** • **8-way—**The maximum amount of rank interleaving is used. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Demand Scrub	Whether the system corrects single bit memory errors encountered when the CPU or I/O makes a demand read. This can be one of the following: • **Disabled—** Single bit memory errors are not corrected. • **Enabled—** Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Patrol Scrub	Whether the system actively searches for, and corrects, single bit memory errors even in unused portions of the memory on the server. This can be one of the following: • **Disabled—**The system checks for memory ECC errors only when the CPU reads or writes a memory address. • **Enabled—**The system periodically reads and writes memory searching for ECC errors. If any errors are found, the system attempts to fix them. This option may correct single bit errors before they become multi-bit errors, but it may adversely affect performance when the patrol scrub is running. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Altitude	This can be one of the following: • **—** • **—** • **—**

Name	Description
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • **Auto—**The CPU determines the physical elevation. • **—**The server is approximately 300 meters above sea level. • **—**The server is approximately 900 meters above sea level. • **—**The server is approximately 1500 meters above sea level. • **—**The server is approximately 3000 meters above sea level. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
Package C State Limit **set PackageCStateLimit**	The amount of power available to the server components when they are idle. This can be one of the following: • —The server may enter any available C state. • —The server provides all server components with full power at all times. This option maintains the highest level of performance and requires the greatest amount of power. • —When the CPU is idle, the system slightly reduces the power consumption. This option requires less power than C0 and allows the server to return quickly to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • —When the CPU is idle, the system reduces the power consumption further than with the C3 option. This option saves more power than C0, C1, or C3, but there may be performance issues until the server returns to full power. • —When the CPU is idle, the system reduces the power consumption further than with the C1 option. This requires less power than C1 or C0, but it takes the server slightly longer to return to high performance mode. • —When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves the maximum amount of power but it also requires the longest time for the server to return to high performance mode. • —When the CPU is idle, the server makes a minimal amount of power available to the components. This option saves more power than C7, but it also requires the longest time for the server to return to high performance mode. • —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
VT for Directed IO	Whether the processor uses Intel Virtualization Technology for Directed I/O (VT-d). This can be one of the following: • **disabled—**The processor does not use virtualization technology. • **enabled—**The processor uses virtualization technology. • **—**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. This can be one of the following: • **disabled—**The processor does not support remapping. • **enabled—**The processor uses VT-d Interrupt Remapping as required. • **—**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. This can be one of the following: • **disabled—**The processor does not support coherency. • **enabled—**The processor uses VT-d Coherency as required. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
ATS Support	Whether the processor supports Intel VT-d Address Translation Services (ATS). This can be one of the following: • **disabled—**The processor does not support ATS. • **enabled—**The processor uses VT-d ATS as required. • **—**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. This can be one of the following: • **disabled—**The processor does not support pass-through DMA. • **enabled—**The processor uses VT-d Pass-through DMA as required. • **—**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
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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Mirroring Mode	Memory mirroring enhances system reliability by keeping two identical data images in memory. This option is only available if you choose the **mirroring** option for **Memory RAS Config**. It can be one of the following: • **inter-socket—**Memory is mirrored between two Integrated Memory Controllers (IMCs) across CPU sockets. • **intra-socket—**One IMC is mirrored with another IMC in the same socket. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Sparing Mode	Sparing optimizes reliability by holding memory in reserve so that it can be used in case other DIMMs fail. This option provides some memory redundancy, but does not provide as much redundancy as mirroring. The available sparing modes depend on the current memory population. This option is only available if you choose **sparing** option for **Memory RAS Config**. It can be one of the following: • **dimm-sparing—**One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • **rank-sparing—**A spare rank of DIMMs is held in reserve. If a rank of DIMMs fails, the contents of the failing rank are transferred to the spare rank. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
DRAM Refresh Rate	This option controls the refresh interval rate for internal memory.

Serial Port BIOS Settings

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

Name	Description
Serial Port A	Whether serial port A is enabled or disabled. This can be one of the following: • **disabled—**The serial port is disabled. • **enabled—**The serial port is enabled. • **—**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: • **disabled—**The server can boot from a USB device. • **enabled—**The server cannot boot from a USB device. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB System 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: • **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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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: • **disabled** • **enabled** • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

PCI Configuration BIOS Settings

The following table lists the PCI configuration 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: • **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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
Memory Mapped IO Above 4Gb Config	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: • **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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Name	Description
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. • **—**The BIOS uses the value for 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. • **—**The BIOS uses the value for 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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

Server Management BIOS Settings

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

General 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**. • **—**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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
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. • **—**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.

Name	Description
OS Boot Watchdog Timer Timeout Policy	What action the system takes if the watchdog timer expires. This can be one of the following: • **power-off—**The server is powered off if the watchdog timer expires during OS boot. • **reset—**The server is reset if the watchdog timer expires during OS boot. • **—**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.
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. • **—**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 Redirection Settings

Name	Description
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. • **—**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.
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. • **—**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
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. • **—**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. • **—**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.
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. • **—**The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.

IPMI Access Profile

This policy allows you to determine whether 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 CIMC. 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.

Configuring an IPMI Access Profile

Before You Begin

Obtain the following:

- Username with appropriate permission that can be authenticated by the operating system of the server
- Password for the username
- Permission associated with the username

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create ipmi-access-profile** *profile-name*	Creates the specified IPMI access profile and enters organization IPMI access profile mode.
Step 4	UCSC(policy-mgr) /org/ipmi-access-profile # **create ipmi-user** *ipmi-user-name*	Creates the specified endpoint user and enters organization IPMI access profile endpoint user mode. **Note** More than one endpoint user can be created within an IPMI access profile, with each endpoint user having its own password and privileges.
Step 5	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **set password**	Sets the password for the endpoint user. After entering the **set password** command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI.
Step 6	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	Specifies whether the endpoint user has administrative or read-only privileges.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates an IPMI access profile named ReadOnly, creates an endpoint user named bob, sets the password and the privileges for bob, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org/ipmi-access-profile* # create ipmi-user bob
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user #
```

What to Do Next

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

Deleting an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete ipmi-access-profile** *profile-name*	Deletes the specified IPMI access profile.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the IPMI access profile named ReadOnly and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Adding an Endpoint User to an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **scope ipmi-access-profile** *profile-name*	Enters organization IPMI access profile mode for the specified IPMI access profile.
Step 4	UCSC(policy-mgr) /org/ipmi-access-profile # **create ipmi-user** *ipmi-user-name*	Creates the specified endpoint user and enters organization IPMI access profile endpoint user mode. **Note** More than one endpoint user can be created within an IPMI access profile, with each endpoint user having its own password and privileges.
Step 5	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **set password**	Sets the password for the endpoint user. After entering the **set password** command, you are prompted to enter and confirm the password. For security purposes, the password that you type does not appear in the CLI.
Step 6	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **set privilege** {**admin** | **readonly**}	Specifies whether the endpoint user has administrative or read-only privileges.
Step 7	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

The following example adds an endpoint user named alice to the IPMI access profile named ReadOnly and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org/ipmi-access-profile* # create ipmi-user alice
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # set privilege readonly
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user* # commit-buffer
UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user #
```

Deleting an Endpoint User from an IPMI Access Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope ipmi-access-profile** *profile-name*	Enters organization IPMI access profile mode for the specified IPMI access profile.
Step 4	UCSC(policy-mgr) /org/ipmi-access-profile # **delete ipmi-user** *epuser-name*	Deletes the specified endpoint user from the IPMI access profile.
Step 5	UCSC(policy-mgr) /org/ipmi-access-profile # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the endpoint user named alice from the IPMI access profile named ReadOnly and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope ipmi-access-profile ReadOnly
UCSC(policy-mgr) /org/ipmi-access-profile # delete ipmi-user alice
UCSC(policy-mgr) /org/ipmi-access-profile* # commit-buffer
UCSC(policy-mgr) /org/ipmi-access-profile #
```

Boot Policy

The Cisco UCS Manager 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 must include this policy 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, Cisco UCS Manager applies the default boot policy.

Note Changes to a boot policy might be propagated to all servers 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 a Boot Policy

Before You Begin

If you are creating a boot policy that boots the server from a SAN LUN and you require reliable SAN boot operations, you must first remove all local disks from servers associated with a service profile that includes the boot policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create boot-policy** *policy-name* [**purpose** {**operational** | **utility**}]	Creates a boot policy with the specified policy name, and enters organization boot policy mode. When you create the boot policy, specify the **operational** option. This ensures that the server boots from the operating system installed on the server. The **utility** options is reserved and should only be used if instructed to do so by a Cisco representative.
Step 4	UCSC(policy-mgr) /org/boot-policy # **set descr** *description*	(Optional) Provides a description for the boot policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks do not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/boot-policy # **set reboot-on-update** {**no** | **yes**}	Specifies whether the servers using this boot policy are automatically rebooted after you make changes to the boot order.
Step 6	UCSC(policy-mgr) /org/boot-policy # **set enforce-vnic-name** {**no** | **yes**}	If you choose **yes**, Cisco UCS Central uses any vNICs or vHBAs defined in the **Boot Order**. If you choose **no**, Cisco UCS Central uses the priority specified in the vNIC or vHBA.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/boot-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a boot policy named boot-policy-LAN, provides a description for the boot policy, specifies that servers using this policy will not be automatically rebooted when the boot order is changed, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create boot-policy boot-policy-LAN purpose operational
UCSC(policy-mgr) /org/boot-policy* # set descr "Boot policy that boots from the LAN."
UCSC(policy-mgr) /org/boot-policy* # set reboot-on-update no
UCSC(policy-mgr) /org/boot-policy* # commit-buffer
UCSC(policy-mgr) /org/boot-policy #
```

What to Do Next

Configure one or more of the following boot options for the boot policy and set their boot order:

- **LAN Boot —**Boots from a centralized provisioning server. It is frequently used to install operating systems on a server from that server.

  If you choose the LAN Boot option, continue to Configuring a LAN Boot for a Boot Policy, on page 309.

- **Storage Boot —** Boots from an operating system image on the SAN. You can specify a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

  We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN, when you move a service profile from one server to another, the new server boots from exactly the same operating system image. Therefore, the new server appears to be exactly the same server to the network.

  If you choose the Storage Boot option, continue to Configuring a SAN Boot for a Boot Policy, on page 310.

- **Virtual Media Boot —**Mimics the insertion of a physical CD into a server. It is typically used to manually install operating systems on a server.

  If you choose the Virtual Media boot option, continue to Configuring a Virtual Media Boot for a Boot Policy, on page 317.

LAN Boot

You can configure a boot policy to boot one or more servers from a centralized provisioning server on the LAN. A LAN (or PXE) boot is frequently used to install operating systems on a server from that LAN server.

You can add more than one type of boot device to a LAN boot policy. For example, you could add a local disk or virtual media boot as a secondary boot device.

Configuring a LAN Boot for a Boot Policy

Before You Begin

Create a boot policy to contain the LAN boot configuration.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **scope boot-policy** *policy-name*	Enters organization boot policy mode for the specified boot policy.
Step 4	UCSC(policy-mgr) /org/boot-policy # **create lan**	Creates a LAN boot for the boot policy and enters organization boot policy LAN mode.
Step 5	UCSC(policy-mgr) /org/boot-policy/lan # **set order** {**1** | **2** | **3** | **4**}	Specifies the boot order for the LAN boot.
Step 6	UCSC(policy-mgr) /org/boot-policy/lan # **create path** {**primary** | **secondary**}	Creates a primary or secondary LAN boot path and enters organization boot policy LAN path mode.
Step 7	UCSC(policy-mgr) /org/boot-policy/lan/path # **set vnic** *vnic-name*	Specifies the vNIC to use for the LAN path to the boot image.
Step 8	UCSC(policy-mgr) /org/boot-policy/lan/path # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the boot policy named lab2-boot-policy, creates a LAN boot for the policy, sets the boot order to 2, creates primary and secondary paths using the vNICs named vNIC1 and vNIC2 , and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope boot-policy lab2-boot-policy
UCSC(policy-mgr) /org/boot-policy* # create lan
UCSC(policy-mgr) /org/boot-policy/lan* # set order 2
UCSC(policy-mgr) /org/boot-policy/lan* # create path primary
UCSC(policy-mgr) /org/boot-policy/lan/path* # set vnic vNIC1
UCSC(policy-mgr) /org/boot-policy/lan/path* # exit
UCSC(policy-mgr) /org/boot-policy/lan* # create path secondary
UCSC(policy-mgr) /org/boot-policy/lan/path* # set vnic vNIC2
UCSC(policy-mgr) /org/boot-policy/lan/path* # commit-buffer
UCSC(policy-mgr) /org/boot-policy/lan/path #
```

What to Do Next

Include the boot policy in a service profile and/or template.

SAN Boot

You can configure a boot policy to boot one or more servers from an operating system image on the SAN. The boot policy can include a primary and a secondary SAN boot. If the primary boot fails, the server attempts to boot from the secondary.

We recommend that you use a SAN boot, because it offers the most service profile mobility within the system. If you boot from the SAN when you move a service profile from one server to another, the new server boots from the exact same operating system image. Therefore, the new server appears to be the exact same server to the network.

To use a SAN boot, ensure that the following is configured:

- The Cisco UCS domain must be able to communicate with the SAN storage device that hosts the operating system image.
- A boot target LUN on the device where the operating system image is located.

Note SAN boot is not supported on Gen-3 Emulex adapters on Cisco UCS blade & rack servers.

Configuring a SAN Boot for a Boot Policy

Note We recommend that the boot order in a boot policy include either a local disk or a SUN LUN, but not both, to avoid the possibility of the server booting from the wrong storage type. If you configure a local disk and a SUN LUN for the boot order storage type and the operating system or logical volume manager (LVM) is configured incorrectly, the server might boot from the local disk rather than the SAN LUN.

For example, on a server with Red Hat Linux installed, where the LVM is configures with default LV names and the boot order is configured with a SUN LUN and a local disk, Linux reports that there are two LVs with the same name and boots from the LV with the lowest SCSI ID, which could be the local disk.

This procedure continues directly from Creating a Boot Policy, on page 307.

Before You Begin

Create a boot policy to contain the SAN boot configuration.

Note If you are creating a boot policy that boots the server from a SAN LUN and you require reliable SAN boot operations, we recommend that you first remove all local disks from servers associated with a service profile that includes the boot policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **scope boot-policy** *policy-name*	Enters organization boot policy mode for the specified boot policy.
Step 4	UCSC(policy-mgr) /org/boot-policy # **create storage**	Creates a SAN boot for the boot policy and enters organization boot policy storage mode.
Step 5	UCSC(policy-mgr) /org/boot-policy/storage # **set order** {**1** | **2** | **3** | **4**}	Sets the boot order for the SAN boot.
Step 6	UCSC(policy-mgr) /org/boot-policy/storage # **create san-image** {**primary** | **secondary**}	Creates a SAN image location, and if the san-image option is specified, enters organization boot policy storage SAN image mode. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.
Step 7	UCSC(policy-mgr) /org/boot-policy/storage/san-image # **set vhba** *vhba-name*	Specifies the vHBA to be used for the SAN boot.
Step 8	UCSC(policy-mgr) /org/boot-policy/storage/san-image # **create path** {**primary** | **secondary**}	Creates a primary or secondary SAN boot path and enters organization boot policy SAN path mode. The use of the terms primary or secondary boot devices does not imply a boot order. The effective order of boot devices within the same device class is determined by PCIe bus scan order.
Step 9	UCSC(policy-mgr) /org/boot-policy/storage/san-image/path # **set** {**lun** *lun-id* | **wwn** *wwn-num*}	Specifies the LUN or WWN to be used for the SAN path to the boot image.
Step 10	UCSC(policy-mgr) /org/boot-policy/storage/san-image/path # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the boot policy named lab1-boot-policy, creates a SAN boot for the policy, sets the boot order to 1, creates a primary SAN image, uses a vHBA named vHBA2, creates primary path using LUN 967295200, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
```

```
UCSC(policy-mgr) /org* # scope boot-policy lab1-boot-policy
UCSC(policy-mgr) /org/boot-policy* # create storage
UCSC(policy-mgr) /org/boot-policy/storage* # set order 1
UCSC(policy-mgr) /org/boot-policy/storage* # create san-image primary
UCSC(policy-mgr) /org/boot-policy/storage* # set vhba vHBA2
UCSC(policy-mgr) /org/boot-policy/storage/san-image* # create path primary
UCSC(policy-mgr) /org/boot-policy/storage/san-image/path* # set lun 967295200
UCSC(policy-mgr) /org/boot-policy/storage/san-image/path* # commit-buffer
UCSC(policy-mgr) /org/boot-policy/storage/san-image/path #
```

What to Do Next

Include the boot policy in a service profile and/or template.

iSCSI Boot

iSCSI boot enables a server to boot its operating system from an iSCSI target machine located remotely over a network.

iSCSI boot is supported on the following Cisco UCS hardware:

- Cisco UCS blade servers that have the Cisco UCS M51KR-B Broadcom BCM57711 network adapter and use the default MAC address provided by Broadcom.
- Cisco UCS M81KR Virtual Interface Card
- Cisco UCS VIC-1240 Virtual Interface Card
- Cisco UCS VIC-1280 Virtual Interface Card
- Cisco UCS rack servers that have the Cisco UCS M61KR-B Broadcom BCM57712 network adapter.
- Cisco UCS P81E Virtual Interface Card
- Cisco UCS VIC1225 Virtual Interface Card

There are prerequisites that must be met before you configure iSCSI boot. For a list of these prerequisites, see iSCSI Boot Guidelines and Prerequisites.

Configuring an iSCSI Boot for a Boot Policy

Before You Begin

You can add up to two iSCSI vNICs per boot policy. One vNIC acts as the primary iSCSI boot source, and the other acts as the secondary iSCSI boot source.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope boot-policy** *policy-name*	Enters organization boot policy mode for the specified boot policy.
Step 4	UCSC(policy-mgr) /org/boot-policy # **create iscsi**	Adds an iSCSI boot to the boot policy and enters iSCSI mode.
Step 5	UCSC(policy-mgr) /org/boot-policy/iscsi # **create path** {**primary** | **secondary**}	Specifies the primary and secondary paths that Cisco UCS Central uses to reach the iSCSI target. With iSCSI boot, you set up two paths. Cisco UCS Central uses the primary path first, and if that fails, then it uses the secondary path.
Step 6	UCSC(policy-mgr) /org/boot-policy/iscsi/path # **set iscsivnicname** *vnic-name*	Specifies the vNIC to use for the iSCSI path to the boot image.
Step 7	UCSC(policy-mgr) /org/boot-policy/iscsi/path # **exit**	Exits iSCSI path mode.
Step 8	UCSC(policy-mgr) /org/boot-policy/iscsi # **set order** *ordernum*	Specifies the order for the iSCSI boot in the boot order.
Step 9	UCSC(policy-mgr) /org/boot-policy/iscsi # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the boot policy named lab2-boot-policy, creates an iSCSI boot for the policy, creates primary and secondary paths using the vNICs named vNIC1 and vNIC2, sets the boot order to 2, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope boot-policy lab2-boot-policy
UCSC(policy-mgr) /org/boot-policy # create iscsi
UCSC(policy-mgr) /org/boot-policy/iscsi* # create path primary
UCSC(policy-mgr) /org/boot-policy/iscsi/path* # set vnic vNIC1
UCSC(policy-mgr) /org/boot-policy/iscsi/path* # exit
UCSC(policy-mgr) /org/boot-policy/iscsi* # set order 2
UCSC(policy-mgr) /org/boot-policy/iscsi* # create path secondary
UCSC(policy-mgr) /org/boot-policy/iscsi/path* # set vnic vNIC2
UCSC(policy-mgr) /org/boot-policy/iscsi/path* # commit-buffer
UCSC(policy-mgr) /org/boot-policy/iscsi/path #
```

What to Do Next

Include the boot policy in a service profile and/or template.

Creating an iSCSI Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create iscsi-policy** *policy-name*	Creates the iSCSI adapter policy.
Step 4	UCSC(policy-mgr) /org/iscsi-policy # **set descr** *description*	(Optional) Provides a description for the iSCSI adapter policy.
Step 5	UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item connection-timeout** *timeout-secs*	The number of seconds until Cisco UCS Central assumes that the initial login has failed and the iSCSI adapter is unavailable. Enter an integer between 0 and 255. If you enter 0, Cisco UCS Central uses the value set in the adapter firmware (default: 15 seconds).
Step 6	UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item dhcp-timeout** *timeout-secs*	The number of seconds to wait before the initiator assumes that the DHCP server in unavailable. Enter an integer between 60 and 300 (default: 60 seconds).
Step 7	UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item lun-busy-retry-count** *num*	The number of times to retry the connection in case of a failure during iSCSI LUN discovery. Enter an integer between 0 and 60. If you enter 0, Cisco UCS Central uses the value set in the adapter firmware (default: 15 seconds).
Step 8	UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item tcp-time-stamp** {**no** | **yes**}	Specifies whether to apply a TCP timestamp. With this setting, transmitted packets are given a time stamp of when the packet was sent so that the packet's round-trip time can be calculated, when needed. This setting applies only to Cisco UCS M51KR-B Broadcom BCM57711 adapters.
Step 9	UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item hbamode** {**no** | **yes**}	Specifies whether to enable HBA mode. This option should only be enabled for servers with the Cisco UCS NIC M51KR-B adapter running the Windows operating system.
Step 10	UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item boottotarget** {**no** | **yes**}	Specifies whether to boot from the iSCSI target.

	Command or Action	Purpose
		This option only applies to servers with the Cisco UCS NIC M51KR-B adapter. It should be disabled until you have installed an operating system on the server.
Step 11	UCSC(policy-mgr) /org/iscsi-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an iSCSI adapter policy called iscsiboot, set the connection timeout, DHCP timeout, and LUN busy retry count, apply a TCP timestamp, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCS-AUCSC(policy-mgr)UCS-A /org # create iscsi-policy iscsiboot
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item connection-timeout 60
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item dhcp-timeout 200
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item lun-busy-retry-count 5
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item tcp-time-stamp yes
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item hbamode yes
UCSC(policy-mgr) /org/iscsi-policy* # set iscsi-protocol-item boottotarget yes
UCSC(policy-mgr) /org/iscsi-policy* # commit-buffer
UCSC(policy-mgr) /org/iscsi-policy #
```

What to Do Next

Include the adapter policy in a service profile and/or template.

Deleting an iSCSI Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete iscsi-policy** *policy-name*	Deletes the iSCSI adapter policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an iSCSI adapter policy named iscsi-adapter-pol and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete iscsi-policy iscsi-adapter-pol
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Creating an iSCSI Authentication Profile

If you use authentication for iSCSI boot, you need to create an authentication profile for both the initiator and target.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create auth-profile** *profile-name*	Creates an authentication profile with the specified name. The name can be up to 16 alphanumeric characters.
Step 4	UCSC(policy-mgr) /org/auth-profile # **set user-id** *id-name*	Creates a log in for authentication.
Step 5	UCSC(policy-mgr) /org/auth-profile # **set password**	Creates a password for authentication.
Step 6	UCSC(policy-mgr) /org/auth-profile # **commit-buffer**	Commits the transaction to the system configuration.
Step 7	UCSC(policy-mgr) /org/auth-profile # **exit**	Exits the current mode.
Step 8	Repeat steps 3 through 7 to create an authentication profile for the target.	
Step 9	UCSC(policy-mgr) /org/auth-profile # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create an authentication profile for an initiator and target and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create auth-profile InitAuth
UCSC(policy-mgr) /org/auth-profile* # set user-id init
UCSC(policy-mgr) /org/auth-profile* # set  password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/auth-profile* # commit-buffer
UCSC(policy-mgr) /org/auth-profile # exit
UCSC(policy-mgr) /org # create auth-profile TargetAuth
UCSC(policy-mgr) /org/auth-profile* # set user-id target
UCSC(policy-mgr) /org/auth-profile* # set  password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /org/auth-profile* # commit-buffer
UCSC(policy-mgr) /org/auth-profile # exit
```

What to Do Next

Create an Ethernet vNIC to be used as the overlay vNIC for the iSCSI device, and then create an iSCSI vNIC.

Deleting an iSCSI Authentication Profile

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete auth-profile** *profile-name*	Deletes the specified iSCSI authentication profile.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an iSCSI authentication profile and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # delete auth-profile InitAuth
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Virtual Media Boot

You can configure a boot policy to boot one or more servers from a virtual media device that is accessible from the server. A virtual media device mimics the insertion of a physical CD/DVD disk (read-only) or floppy disk (read-write) into a server. This type of server boot is typically used to manually install operating systems on a server.

Configuring a Virtual Media Boot for a Boot Policy

Note Virtual Media requires the USB to be enabled. If you modify the BIOS settings that affect the USB functionality, you also affect the Virtual Media. Therefore, we recommend that you leave the following USB BIOS defaults for best performance:

- Make Device Non Bootable—set to **disabled**.
- USB Idle Power Optimizing Setting—set to **high-performance**

Before You Begin

Create a boot policy to contain the virtual media boot configuration.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **scope boot-policy** *policy-name*	Enters organization boot policy mode for the specified boot policy.
Step 4	UCSC(policy-mgr) /org/boot-policy # **create virtual-media** {**read-only** | **read-write**}	Creates a virtual media boot for the boot policy, specifies whether the virtual media is has read-only or read-write privileges, and enters organization boot policy virtual media mode.
Step 5	UCSC(policy-mgr) /org/boot-policy/virtual-media # **set order** {**1** | **2** | **3** | **4**}	Sets the boot order for the virtual-media boot.
Step 6	UCSC(policy-mgr) /org/boot-policy/virtual-media # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the boot policy named lab3-boot-policy, creates a virtual media boot with read-only privileges for the policy, sets the boot order to 3, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope boot-policy lab3-boot-policy
UCSC(policy-mgr) /org/boot-policy* # create virtual-media read-only
UCSC(policy-mgr) /org/boot-policy/virtual-media* # set order 3
UCSC(policy-mgr) /org/boot-policy/virtual-media* # commit-buffer
```

What to Do Next

Include the boot policy in a service profile and/or template.

Deleting a Boot Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete boot-policy** *policy-name*	Deletes the specified boot policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a boot policy and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete boot-policy boot-policy-LAN
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Local Disk Configuration 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:

- **No Local Storage—**For a diskless server or a SAN only configuration. If you select this option, you cannot associate any service profile which uses this policy with a server that has a local disk.
- **RAID 0 Striped—**Data is striped across all disks in the array, providing fast throughput. There is no data redundancy, and all data is lost if any disk fails.
- **RAID 1 Mirrored—**Data is written to two disks, providing complete data redundancy if one disk fails. The maximum array size is equal to the available space on the smaller of the two drives.
- **Any Configuration—**For a server configuration that carries forward the local disk configuration without any changes.
- **No RAID—**For a server configuration that removes the RAID and leaves the disk MBR and payload unaltered.

  If you choose **No RAID** and you apply this policy to a server that already has an operating system with RAID storage configured, the system does not remove the disk contents. Therefore, there may be no visible differences on the server after you apply the **No RAID** mode. This can lead to a mismatch between the RAID configuration in the policy and the actual disk configuration shown in the **Inventory** > **Storage** tab for the server.

  To make sure that any previous RAID configuration information is removed from a disk, apply a scrub policy that removes all disk information after you apply the **No RAID** configuration mode.
- **RAID 5 Striped Parity—**Data is striped across all disks in the array. Part of the capacity of each disk stores parity information that can be used to reconstruct data if a disk fails. RAID 5 provides good data throughput for applications with high read request rates.

- **RAID 6 Striped Dual Parity—**Data is striped across all disks in the array and two parity disks are used to provide protection against the failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.
- **RAID 10 Mirrored and Striped—**RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates.
- **RAID 50 Striped Parity and Striped —**Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance.
- **RAID 60 Striped Dual Parity and Striped —**Data is striped across multiple striped dual parity disk sets to provide high throughput and greater disk failure tolerance.

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

Guidelines for all Local Disk Configuration Policies

Before you create a local disk configuration policy, consider the following guidelines:

No Mixed HDDs and SSDs

Do not include HDDs and SSDs in a single server or RAID configuration.

Do Not Assign a Service Profile with the Default Local Disk Configuration Policy from a B200 M1 or M2 to a B200 M3

Due to the differences in the RAID/JBOD support provided by the storage controllers of B200 M1 and M2 servers and those of the B200 M3 server, you cannot assign or re-assign a service profile that includes the default local disk configuration policy from a B200M1 or M2 server to a B200 M3 server. The default local disk configuration policy includes those with Any Configuration or JBOD configuration.

JBOD Mode Support

Note Only B200 M1, B200 M2, B200 M3, B250 M1, B250 M2 and B22 M3 blade servers support the JBOD mode for local disks.

Guidelines for Local Disk Configuration Policies Configured for RAID

Configure RAID Settings in Local Disk Configuration Policy for Servers with MegaRAID Storage Controllers

If a blade server or integrated rack-mount server has a MegaRAID controller, you must configure RAID settings for the drives in the Local Disk Configuration policy included in the service profile for that server. You can do this either by configuring the local disk configuration policy in the service profile using one of the defined RAID modes for that server, or you can use the **Any Configuration** mode with the LSI Utilities toolset to create the RAID volumes.

If you do not configure your RAID LUNs before installing the OS, disk discovery failures might occur during the installation and you might see error messages such as “No Device Found.”

Server May Not Boot After RAID1 Cluster Migration if Any Configuration Mode Specified in Service Profile

After RAID1 clusters are migrated, you need to associate a service profile with the server. If the local disk configuration policy in the service profile is configured with **Any Configuration** mode rather than **RAID1**, the RAID LUN remains in "inactive" state during and after association. As a result, the server cannot boot.

To avoid this issue, ensure that the service profile you associate with the server contains the identical local disk configuration policy as the original service profile before the migration and does not include the **Any Configuration** mode.

Do Not Use JBOD Mode on Servers with MegaRAID Storage Controllers

Do not configure or use JBOD mode or JBOD operations on any blade server or integrated rack-mount server with a MegaRAID storage controllers. JBOD mode and operations are not intended for nor are they fully functional on these servers.

Maximum of One RAID Volume and One RAID Controller in Integrated Rack-Mount Servers

A rack-mount server that has been integrated with Cisco UCS Manager and is registered with Cisco UCS Central can have a maximum of one RAID volume irrespective of how many hard drives are present on the server.

All the local hard drives in an integrated rack-mount server must be connected to only one RAID Controller. Integration with Cisco UCS Manager does not support the connection of local hard drives to multiple RAID Controllers in a single rack-mount server. We therefore recommend that you request a single RAID Controller configuration when you order rack-mount servers to be integrated with Cisco UCS Manager.

In addition, do not use third party tools to create multiple RAID LUNs on rack-mount servers. Cisco UCS Manager does not support that configuration.

Maximum of One RAID Volume and One RAID Controller in Blade Servers

A blade server can have a maximum of one RAID volume irrespective of how many drives are present in the server. All the local hard drives must be connected to only one RAID controller. For example, a B200 M3 server has an LSI controller and an Intel Patsburg controller, but only the LSI controller can be used as a RAID controller.

In addition, do not use third party tools to create multiple RAID LUNs on blade servers. Cisco UCS Central does not support that configuration.

Number of Disks Selected in Mirrored RAID Should Not Exceed Two

If the number of disks selected in the Mirrored RAID exceed two, RAID 1 is created as a RAID 10 LUN. This issue can occur with the Cisco UCS B440 M1 and B440 M2 servers.

License Required for Certain RAID Configuration Options on Some Servers

Some Cisco UCS servers require a license for certain RAID configuration options. When Cisco UCS Central associates a service profile containing this local disk policy with a server, Cisco UCS Central verifies that the selected RAID option is properly licensed. If there are issues, Cisco UCS Central displays a configuration error during the service profile association.

For RAID license information for a specific Cisco UCS server, see the *Hardware Installation Guide* for that server.

B420 M3 Server Does Not Support All Configuration Modes

The B420 M3 server does not support the following configuration modes in a local disk configuration policy:

- No RAID
- RAID 6 Striped Dual Parity

In addition, the B420 M3 does not support JBOD modes or operations.

Single-Disk RAID 0 Configurations Not Supported on Some Blade Servers

A single-disk RAID 0 configuration is not supported in the following blade servers:

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

Creating a Local Disk Configuration Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create local-disk-config-policy** *policy-name*	Creates a local disk configuration policy and enters local disk configuration policy mode.
Step 4	UCSC(policy-mgr) /org/local-disk-config-policy # **set descr** *description*	(Optional) Provides a description for the local disk configuration policy.
Step 5	UCSC(policy-mgr) /org/local-disk-config-policy # **set mode** {**any-configuration** | **no-local-storage** | **no-raid** | **raid-0-striped** | **raid-1-mirrored** | **raid-5-striped-parity** | **raid-6-striped-dual-parity** | **raid-10-mirrored-and-striped**}	Specifies the mode for the local disk configuration policy.
Step 6	UCSC(policy-mgr) /org/local-disk-config-policy # **set protect** {**yes** | **no**}	Specifies whether the server retains the configuration in the local disk configuration policy even if the server is disassociated from the service profile.

	Command or Action	Purpose
		Caution Protect Configuration becomes non-functional if one or more disks in the server are defective or faulty. When a service profile is disassociated from a server and a new service profile associated, the setting for the Protect Configuration property in the new service profile takes precedence and overwrites the setting in the previous service profile. **Note** If you disassociate the server from a service profile with this option enabled and then associate it with a new service profile that includes a local disk configuration policy with different properties, the server returns a configuration mismatch error and the association fails.
Step 7	UCSC(policy-mgr) /org/local-disk-config-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a local disk configuration policy and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create local-disk-config-policy DiskPolicy7
UCSC(policy-mgr) /org/local-disk-config-policy* # set mode raid-1-mirrored
UCSC(policy-mgr) /org/local-disk-config-policy* # set protect yes
UCSC(policy-mgr) /org/local-disk-config-policy* # commit-buffer
UCSC(policy-mgr) /org/local-disk-config-policy #
```

Viewing a Local Disk Configuration Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **show local-disk-config-policy** *policy-name*	Displays the local disk policy. If you have not configured a local disk policy, the local disk configuration (created by the create local-disk-config command) displays. Displays the local disk definition (set by the create local-disk-config command). If the serial over LAN definition is not set, and if a policy is set (using the set local-disk-config-policy command), then the policy will be displayed.

	Command or Action	Purpose

The following example shows how to display local disk policy information for a local disk configuration policy called DiskPolicy7:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # show local-disk-config-policy DiskPolicy7

Local Disk Config Policy:
Name: DiskPolicy7
Mode: Raid 1 Mirrored
Description:
Protect Configuration: Yes
```

Deleting a Local Disk Configuration Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete local-disk-config-policy** *policy-name*	Deletes the specified local disk configuration policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the local disk configuration policy named DiskPolicy7 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete local-disk-config-policy DiskPolicy7
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Power Control Policy

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.

Note 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 a Power Control Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create power-control-policy** *policy-name*	Creates a power control policy and enters power control policy mode.
Step 4	UCSC(policy-mgr) /org/power-control-policy # **set priority** {*priority-num* | **no-cap**}	Specifies the priority for the power control policy.
Step 5	UCSC(policy-mgr) /org/power-control-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a power control policy and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create power-control-policy PCP-1
UCSC(policy-mgr) /org/power-control-policy* # set priority 1
UCSC(policy-mgr) /org/power-control-policy* # commit-buffer
UCSC(policy-mgr) /org/power-control-policy #
```

Deleting a Power-Control-Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete power-control-policy** *policy-name*	Deletes the specified power control policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a power control policy and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete power-control-policy PCP-1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Scrub Policy

This policy determines 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 sdcards, 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 a Scrub Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create scrub-policy** *policy-name*	Creates a scrub policy with the specified policy name, and enters organization scrub policy mode.
Step 4	UCSC(policy-mgr) /org/scrub-policy # **set descr** *description*	(Optional) Provides a description for the scrub policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/scrub-policy # **set disk-scrub** {**no** | **yes**}	Disables or enables disk scrubbing on servers using this scrub policy as follows: • If enabled, destroys all data on any local drives

	Command or Action	Purpose
		• If disabled, preserves all data on any local drives, including local storage configuration
Step 6	UCSC(policy-mgr) /org/scrub-policy # **set bios-settings-scrub** {**no** | **yes**}	Disables or enables BIOS settings scrubbing on servers using this scrub policy as follows: • 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
Step 7	UCSC(policy-mgr) /org/scrub-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a scrub policy named ScrubPolicy2, enables disk scrubbing on servers using the scrub policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create scrub-policy ScrubPolicy2
UCSC(policy-mgr) /org/scrub-policy* # set descr "Scrub disk but not BIOS."
UCSC(policy-mgr) /org/scrub-policy* # set disk-scrub yes
UCSC(policy-mgr) /org/scrub-policy* # set bios-settings-scrub no
UCSC(policy-mgr) /org/scrub-policy* # commit-buffer
UCSC(policy-mgr) /org/scrub-policy #
```

Deleting a Scrub Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete scrub-policy** *policy-name*	Deletes the specified scrub policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the scrub policy named ScrubPolicy2 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
```

```
UCSC(policy-mgr) /org # delete scrub-policy ScrubPolicy2
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Serial over LAN Policy

This policy sets the configuration for the 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.

Configuring a Serial over LAN Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create sol-policy** *policy-name*	Creates a serial over LAN policy and enters organization serial over LAN policy mode.
Step 4	UCSC(policy-mgr) /org/sol-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/sol-policy # **set speed** {**115200** | **19200** | **38400** | **57600** | **9600**}	Specifies the serial baud rate.
Step 6	UCSC(policy-mgr) /org/sol-policy # {**disable** | **enable**}	Disables or enables the serial over LAN policy. By default, the serial over LAN policy is disabled; you must enable it before it can be applied.
Step 7	UCSC(policy-mgr) /org/sol-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a serial over LAN policy named Sol9600, provides a description for the policy, sets the speed to 9,600 baud, enables the policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create sol-policy Sol9600
UCSC(policy-mgr) /org/sol-policy* # set descr "Sets serial over LAN policy to 9600 baud."
UCSC(policy-mgr) /org/sol-policy* # set speed 9600
UCSC(policy-mgr) /org/sol-policy* # enable
UCSC(policy-mgr) /org/sol-policy* # commit-buffer
UCSC(policy-mgr) /org/sol-policy #
```

Viewing a Serial over LAN Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **show sol-policy** *policy-name*	Displays the serial over LAN definition (set by the create sol-config command). If the serial over LAN definition is not set, and if a policy is set (using the set sol-policy command), then the policy will be displayed.

The following example shows how to display serial over LAN information for a serial over LAN policy called Sol9600:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # show sol-policy Sol9600

SOL Policy:
Full Name: Sol9600
SOL State: Enable
Speed: 9600
Description:
```

Server Pool Policy Qualifications

This policy qualifies servers based on the inventory of a server conducted during the discovery process. The qualifications are individual rules that you configure 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

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 a Server Pool Qualification Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create server-qual** *server-qual-name*	Creates a server pool qualification with the specified name, and enters organization server qualification mode.
Step 4	UCSC(policy-mgr) /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a server pool qualification named ServPoolQual22 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create server-qual ServPoolQual22
UCSC(policy-mgr) /org/server-qual* # commit-buffer
UCSC(policy-mgr) /org/server-qual #
```

Creating a Domain Qualification for a Policy Qualification

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope server-qual** *server-qual-name*	Enters server qualification mode for the specified server pool policy qualification.
Step 4	UCSC(policy-mgr) /org/server-qual # **create domain-qual** *domain-qual-name*	Creates the specified domain qualification and enters domain qualification mode.
Step 5	UCSC(policy-mgr) /org/server-qual/domain-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to add a domain qualification to a server pool policy qualification and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope server-qual ServPoolQual22
UCSC(policy-mgr) /org/server-qual # create domain-qual TestDomain
UCSC(policy-mgr) /org/server-qual/domain-qual* # commit-buffer
UCSC(policy-mgr) /org/server-qual/domain-qual #
```

Creating an Adapter Qualification for a Policy Qualification

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope server-qual** *server-qual-name*	Enters server qualification mode for the specified server pool policy qualification.
Step 4	UCSC(policy-mgr) /org/server-qual # **create adapter**	Creates the specified adapter qualification and enters adapter qualification mode.
Step 5	UCSC(policy-mgr) /org/server-qual/adapter # **create cap-qual** *adapter-type*	Creates an adapter capacity qualification for the specified adapter type and enters organization server qualification

	Command or Action	Purpose
		adapter capacity qualification mode. The *adapter-type* argument can be any of the following values: • **fcoe —**Fibre Channel over Ethernet • **non-virtualized-eth-if —**Non-virtualized Ethernet interface • **non-virtualized-fc-if —**Non-virtualized Fibre Channel interface • **path-encap-consolidated —**Path encapsulation consolidated • **path-encap-virtual —**Path encapsulation virtual • **protected-eth-if —**Protected Ethernet interface • **protected-fc-if —**Protected Fibre Channel interface • **protected-fcoe —**Protected Fibre Channel over Ethernet • **uplink-aggregation —**Uplink Aggregation • **virtualized-eth-if —**Virtualized Ethernet interface • **virtualized-eth-sriov —**Virtualized Ethernet SRIOV • **virtualized-fc-if —**Virtualized Fibre Channel interface • **virtualized-fc-sriov —**Virtualized Fibre Channel SRIOV • **virtualized-scsi-if —**Virtualized SCSI interface
Step 6	UCSC(policy-mgr) /org/server-qual/adapter/cap-qual # **set maximum** {*max-cap* | **unspecified**}	Specifies the maximum capacity for the selected adapter type.
Step 7	UCSC(policy-mgr) /org/server-qual/adapter/cap-qual # **set pid-regex** *regex*	Specifies the regular expression that the PID must match.
Step 8	UCSC(policy-mgr) /org/server-qual/adapter/cap-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to add a domain qualification to a server pool policy qualification and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope server-qual ServPoolQual22
UCSC(policy-mgr) /org/server-qual # create adapter TestAdapter
UCSC(policy-mgr) /org/server-qual/adapter* # create cap-qual non-virtualized-eth-if
```

```
UCSC(policy-mgr) /org/server-qual/adapter/cap-qual* # set maximum unspecified
UCSC(policy-mgr) /org/server-qual/adapter/cap-qual* # commit-buffer
UCSC(policy-mgr) /org/server-qual/adapter/cap-qual #
```

Deleting a Server Pool Policy Qualification

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **delete server-qual** *server-qual-name*	Deletes the specified server pool qualification.
Step 4	UCSC(policy-mgr) /org/server-qual # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the server pool qualification named ServPoolQual22 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # delete server-qual ServPoolQual22
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

vNIC/vHBA Placement Policies

vNIC/vHBA placement policies are used to determine the following:

- How the virtual network interface connections (vCons) are mapped to the physical adapters on a server.
- What types of vNICs or vHBAs can be assigned to each vCon.

Each vNIC/vHBA placement policy contains four vCons that are virtual representations of the physical adapters. When a vNIC/vHBA placement policy is assigned to a service profile, and the service profile is associated with a server, the vCons in the vNIC/vHBA placement policy are assigned to the physical adapters and the vNICs and vHBAs are assigned to those vCons.

For blade or rack servers that contain one adapter, Cisco UCS assigns all vCons to that adapter. For servers that contain four adapters, Cisco UCS assigns vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4.

For blade or rack servers that contain two or three adapters, Cisco UCS assigns the vCons based on the type of server and the selected virtual slot mapping scheme, which can be **Round Robin** or **Linear Ordered**. For details about the available mapping schemes, see vCon to Adapter Placement.

After Cisco UCS assigns the vCons, it assigns the vNICs and vHBAs based on the **Selection Preference** for each vCon. This can be one of the following:

- —All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default.
- —vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA.
- —Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it.
- —Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.

If you do not include a vNIC/vHBA placement policy in the service profile, Cisco UCS Central defaults to the **Round Robin** vCon mapping scheme and the **All** vNIC/vHBA selection preference, distributing the vNICs and vHBAs between the adapters based on the capabilities and relative capacities of each adapter.

Configuring a vNIC/vHBA Placement Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create vcon-policy** *policy-name*	Creates the specified vNIC/vHBA placement profile and enters organization vcon policy mode.
Step 4	UCSC(policy-mgr) /org/vcon-policy # **set descr** *description*	(Optional) Provides a description for the vNIC/vHBA Placement Profile. Enter up to 256 characters. You can use any characters or spaces except ` (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote). **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/vcon-policy # **set mapping-scheme** {**round-robin** | **linear-ordered**}	(Optional) For blade or rack servers that contain one adapter, Cisco UCS Central assign all vCons to that adapter. For servers that contain four adapters, Cisco UCS Central assign vCon1 to Adapter1, vCon2 to Adapter2, vCon3 to Adapter3, and vCon4 to Adapter4. For blade or rack servers that contain two or three adapters, Cisco UCS Central assigns vCons based on the selected virtual slot mapping scheme. This can be one of the following:

	Command or Action	Purpose
		• **Round Robin round-robin—** In a server with two adapter cards, Cisco UCS Central assigns vCon1 and vCon3 to Adapter1, then assigns vCon2 and vCon4 to Adapter2. In a server with three adapter cards, Cisco UCS Central assigns vCon1 to Adapter1, vCon2 and vCon4 to Adapter2, and vCon3 to Adapter3. This is the default scheme. • **Linear Ordered Linear-ordered—** In a server with two adapter cards, Cisco UCS Central assigns vCon1 and vCon2 to Adapter1, then assigns vCon3 and vCon4 to Adapter2. In a server with three adapter cards, Cisco UCS Central assigns vCon1 to Adapter1 and vCon2 to Adapter2, then assigns vCon3 and vCon4 to Adapter3. In N20-B6620 and N20-B6625-2 blade servers, the two adapters are numbered left to right while vCons are numbered right to left. If one of these blade servers has a single adapter, Cisco UCS Central assigns all vCons to that adapter. If the server has two adapters, the vCon assignment depends upon the virtual slot mapping scheme: • **Round Robin round-robin—**Cisco UCS Central assigns vCon2 and vCon4 to Adapter1 and vCon1 and vCon3 to Adapter2. This is the default. • **Linear Ordered linear-ordered—**Cisco UCS Central assigns vCon3 and vCon4 to Adapter1 and vCon1 and vCon2 to Adapter2.
Step 6	UCSC(policy-mgr) /org/vcon-policy # **set vcon** {**1** | **2** | **3** | **4**} **selection** {**all** | **assigned-only** | **exclude-dynamic** | **exclude-unassigned**}	Specifies the selection preference for the specified vCon. The options are: • **All all—**All configured vNICs and vHBAs can be assigned to the vCon, whether they are explicitly assigned to it, unassigned, or dynamic. This is the default. • **Assigned Only assigned-only—**vNICs and vHBAs must be explicitly assigned to the vCon. You can assign them explicitly through the service profile or the properties of the vNIC or vHBA. • **Exclude Dynamic exclude-dynamic —**Dynamic vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for all static vNICs and vHBAs, whether they are unassigned or explicitly assigned to it. • **Exclude Unassigned exclude-unassigned—**Unassigned vNICs and vHBAs cannot be assigned to the vCon. The vCon can be used for dynamic vNICs and vHBAs and for static vNICs and vHBAs that are explicitly assigned to it.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/vcon-policy # **commit-buffer**	Commits the transaction.

The following example creates a vNIC/vHBA placement policy named Adapter1All, sets the vCon mapping scheme to Linear Ordered, specifies that only assigned vNICs and vHBAs can be placed on adapter 1, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create vcon-policy Adapter1
UCSC(policy-mgr) /org/vcon-policy* # set descr "This profile places all vNICs and vHBAs on
 adapter 1."
UCSC(policy-mgr) /org/vcon-policy* # set mapping-scheme linear-ordered
UCSC(policy-mgr) /org/vcon-policy* # set vcon 1 selection assigned-only
UCSC(policy-mgr) /org/vcon-policy* # commit-buffer
UCSC(policy-mgr) /org/vcon-policy* #
UCSC(policy-mgr) /org #
```

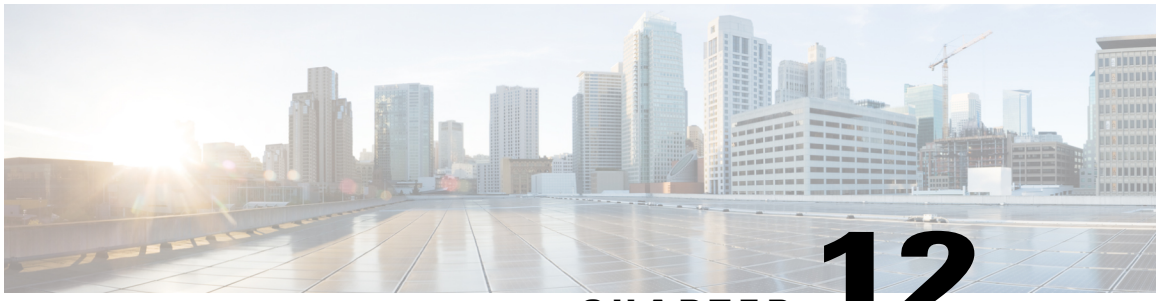
Deleting a vNIC/vHBA Placement Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **delete vcon-policy** *policy-name*	Deletes the specified vNIC/vHBA placement profile.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction.

The following example deletes the vNIC/vHBA placement profile named Adapter1All and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)scope org /
UCSC(policy-mgr) /org # delete vcon-policy Adapter1All
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```



CHAPTER 12

Network Policies

This chapter includes the following sections:

Global VLAN

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 pushed to Cisco UCS along with the global service profiles that reference them. Global VLAN information is visible to Cisco UCS Manager only if a global service profile with reference to a global VLAN is deployed in that UCS domain. When a global VLAN is deployed and becomes available in the UCS domain, locally-defined service profiles and policies can reference the global VLAN.

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 a Single VLAN

This procedure describes how to create a single VLAN in the domain group root or in a specifc domain group.

Important

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-group** *domain-name*	Enters the UCS domain group root.
Step 3	UCSC(resource-mgr) # **scope eth-uplink**	Enters Ethernet uplink command mode.
Step 4	UCSC(resource-mgr) /domain-group/eth-uplink # **create vlan** *vlan-namevlan-id*	Creates a VLAN and assigns a VLAN ID. **Note** The VLAN name is case sensitive.
Step 5	UCSC(resource_mgr)/domain-group/eth-uplink/vlan # **set mcastpolicy** *{default | policy-name}*	(Optional) Assigns a specific multicast policy name. If you do not enter a multicast policy name, the name is resolved from the Cisco UCS Manager domain upon deployment.
Step 6	UCSC(resource-mgr) /domain-group/eth-uplink/vlan# **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a VLAN named Administration in the domain group root, assign it VLAN ID 15, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group /
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink create vlan Administration 15
```

```
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan #
```

The following example shows how to create a VLAN named Administration in domain group 12, assign it VLAN ID 15, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group 12
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink create vlan Administration 15
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan #
```

Creating Multiple VLANs

This procedure describes how to create multiple VLANs.

Important

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) #**scope domain-group** *domain-group*	Enters the UCS domain group root.
Step 3	UCSC(resource-mgr) #**scope eth-uplink**.	Enters Ethernet uplink command mode.
Step 4	UCSC(resource-mgr) /domain-group/eth-uplink #**create vlan** *vlan-name vlan-id*	Creates a VLAN and with the VLAN name and VLAN ID you enter. **Note** The VLAN name is case sensitive.
Step 5	UCSC (resource-mgr) /domain-group/eth-uplink/vlan # **set mcastpolicy** *{default | policy-name}*	(Optional) Assigns a particular multicast policy name. If you do not enter a multicast policy name, the name is resolved from the Cisco UCS Manager upon deployment.
Step 6	UCSC (resource-mgr) /domain-group/eth-uplink/vlan # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create two VLANs in domain group 12, assign multicast policies, and commit the transactions:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group 12
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink create vlan Administration 15
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # set mcastpolicy default
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # create vlan Finance 20
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # set mcastpolicy mpolicy
```

```
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan
```

Deleting a VLAN

This procedure describes how to delete a VLAN from a domain group.

Before You Begin

Consider the following points before deleting global VLANs in Cisco UCS Central:

- Before deleting global VLANs, ensure that any global service profiles that reference them are updated.
- Before deleting the last global VLAN from a domain group, you should remove its organization permissions.
- If you delete a global VLAN, it is also deleted from all registered Cisco UCS Manager instances that are associated with the domain groups in which the VLAN resides.
- Global service profiles that reference a global VLAN that is deleted in Cisco UCS Central will fail due to insufficient resources. Local service profiles that reference a global VLAN that is deleted will be set to virtual network ID 1.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope domain-group** *{/ | domain-name}*	Enters the UCS domain group root or the domain group name you enter.
Step 3	UCSC(resource-mgr) # **scope eth-uplink**	Enters Ethernet uplink command mode.
Step 4	UCSC(resource-mgr) /domain-group/eth-uplink # **delete vlan***vlan-name*	Deletes the VLAN with the name you entered.
Step 5	UCSC(resource-mgr) /domain-group/eth-uplink # **commit-buffer**	Commits the transaction to the system.

The following example shows how to delete the VLAN named Finance from the domain group root and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-group /
UCSC(resource-mgr) /domain-group # scope eth-uplink
UCSC(resource-mgr) /domain-group/eth-uplink delete vlan Finance
UCSC(resource-mgr) /domain-group/eth-uplink/vlan* # commit-buffer
UCSC(resource-mgr) /domain-group/eth-uplink/vlan #
```

Creating VLAN Permissions for an Organization

This procedure describes how to assign a VLAN permission to organizations in Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC# (resource-mgr) **scope org** *{org-name}*	Enters organization management mode for the organization name you enter.
Step 3	UCSC(resource-mgr) /org # **create vlan permit** *vlan-name*	Assigns the specified VLAN permission to the organization, and all of the suborganizations that belong to it. **Note** VLAN name is case sensitive.
Step 4	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system.

The follwing example shows how to assign the VLAN named Administration permission to Sub-Org1, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org Sub-Org1
UCSC(resource-mgr) /org #create vlan-permit Administration
UCSC(resource-mgr) /org* #commit-buffer
UCSC(resource-mgr) /org #
```

Deleting VLAN Permissions from an Organization

This procedure describes how to delete a VLAN Org permission in Cisco UCS Central.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC# (resource-mgr) **scope org** *{org-name}*	Enters organization management mode for the organization name you enter.
Step 3	UCSC(resource-mgr) /org # **delete vlan-permit** *vlan-name*	Deletes permission for the specified VLAN from the organization and all sub organizations that belong to it. **Note** VLAN name is case sensitive.
Step 4	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system.

The follwing example shows how to deleted permission for the VLAN named Administration from Sub-Org1, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org Sub-Org1
UCSC(resouce-mgr) /org #delete vlan-permit Administration
UCSC(resouce-mgr) /org* #commit-buffer
UCSC(resouce-mgr) /org #
```

Configuring MAC Pools

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 Central can 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.

Creating a MAC Pool

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create mac-pool** *pool-name*	Creates a MAC pool with the specified name, and enters organization MAC pool mode.
Step 4	UCSC(policy-mgr) /org/mac-pool # **set descr** *description*	(Optional) Provides a description for the MAC pool. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/mac-pool # **create block** *first-mac-addr last-mac-addr*	Creates a block (range) of MAC addresses, and enters organization MAC pool block mode. You must specify the first and last MAC addresses in the address range using the form *nn*:*nn*:*nn*:*nn*:*nn*:*nn*, with the addresses separated by a space. **Note** A MAC pool can contain more than one MAC address block. To create multiple MAC address blocks, you must enter multiple **create block** commands from organization MAC pool mode.
Step 6	UCSC(policy-mgr) /org/mac-pool/block # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to create another pool, wait at least 5 seconds.

The following example shows how to create a MAC pool named GPool1, provide a description for the pool, specify a block of suffixes to be used for the pool, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create mac-pool GPool1
UCSC(policy-mgr) /org/mac-pool* # set descr "This is MAC pool GPool1"
UCSC(policy-mgr) /org/mac-pool* # create block 00:A0:D7:42:00:01 00:A0:D7:42:01:00
UCSC(policy-mgr) /org/mac-pool/block* # commit-buffer
UCSC(policy-mgr) /org/mac-pool/block #
```

What to Do Next

Include the MAC pool in a vNIC template.

Deleting a MAC 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.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete mac-pool** *pool-name*	Deletes the specified MAC pool.
Step 4	UCSC(policy-mgr) /org/ # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to delete another pool, wait at least 5 seconds.

The following example shows how to delete the MAC pool named GPool1 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete mac-pool GPool1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Network Related Policies

Configuring the Default vNIC Behavior Policy

Default vNIC Behavior Policy

Default vNIC behavior policy allows you to configure how vNICs are created for a service profile. You can choose to create vNICS manually, or you can allow them to be created automatically

You can configure the default vNIC behavior policy to define how vNICs are created. This can be one of the following:

- **None—**Cisco UCS Central does not create default vNICs for a service profile. All vNICs must be explicitly created.
- **HW Inherit—**If a service profile requires vNICs and none have been explicitly defined, Cisco UCS Central creates the required vNICs based on the adapter installed in the server associated with the service profile.

Note If you do not specify a default behavior policy for vNICs, **HW Inherit** is used by default.

Configuring a Default vNIC Behavior Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the root organization mode.
Step 3	UCSC(policy-mgr)/org # **scope vnic-beh-policy**	Enters default vNIC behavior policy mode.
Step 4	UCSC(policy-mgr)/org/vnic-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	Specifies the default vNIC behavior policy. This can be one of the following: • **hw-inherit—**If a service profile requires vNICs and none have been explicitly defined, Cisco UCS Central creates the required vNICs based on the adapter installed in the server associated with the service profile. If you specify **hw-inherit**, you can also specify a vNIC template to create the vNICs. • **none—**Cisco UCS Central does not create default vNICs for a service profile. All vNICs must be explicitly created.
Step 5	UCSC(policy-mgr)/org/vnic-beh-policy # **commit-buffer**	Commits the transaction to the system configuration.

This example shows how to set the default vNIC behavior policy to **hw-inherit**:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr)/org # scope vnic-beh-policy
UCSC(policy-mgr)/org/vnic-beh-policy # set action hw-inherit
UCSC(policy-mgr)/org/vnic-beh-policy* # commit-buffer
UCSC(policy-mgr)/org/vnic-beh-policy #
```

Configuring vNIC Templates

vNIC Template

This policy defines how a vNIC on a server connects to the LAN. This policy is also referred to as a vNIC LAN connectivity policy.

Cisco UCS Central does not automatically create a VM-FEX port profile with the correct settings when you create a vNIC template. If you want to create a VM-FEX port profile, you must configure the target of the vNIC template as a VM.

You need to include this policy in a service profile for it to take effect.

Note If your server has two Emulex or QLogic NICs (Cisco UCS CNA M71KR-E or Cisco UCS CNA M71KR-Q), you must configure vNIC policies for both adapters in your service profile to get a user-defined MAC address for both NICs. If you do not configure policies for both NICs, Windows still detects both of them in the PCI bus. Then because the second eth is not part of your service profile, Windows assigns it a hardware MAC address. If you then move the service profile to a different server, Windows sees additional NICs because one NIC did not have a user-defined MAC address.

Configuring a vNIC Template

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create vnic-templ** *vnic-templ-name* [**eth-if** *vlan-name*] [**fabric** {**a** | **b**}] [**target** [**adapter** | **vm**]]	Creates a vNIC template and enters organization vNIC template mode. The target you choose determines whether or not Cisco UCS Central automatically creates a VM-FEX port profile with the appropriate settings for the vNIC template. This can be one of the following: • **Adapter —**The vNICs apply to all adapters. No VM-FEX port profiles is created if you choose if you this option. • **VM —**The vNICs apply to all virtual machines. A VM-FEX port profiles is created if you choose this option.
Step 4	UCSC(policy-mgr) /org/vnic-templ # **set descr** *description*	(Optional) Provides a description for the vNIC template.
Step 5	UCSC(policy-mgr) /org/vnic-templ # **set fabric** {**a** | **a-b** | **b** | **b-a**}	(Optional) Specifies the fabric to use for the vNIC. If you did not specify the fabric when creating the vNIC template in Step 2, you have the option to specify it with this command. If you want this vNIC to be able to access the second fabric interconnect if the default one is unavailable, choose **a-b** (A is the primary) or **b-a** (B is the primary) .

	Command or Action	Purpose
		Note Do not enable fabric failover for the vNIC under the following circumstances: • If the Cisco UCS domain is running in Ethernet Switch Mode. vNIC fabric failover is not supported in that mode. If all Ethernet uplinks on one fabric interconnect fail, the vNICs do not fail over to the other. • If you plan to associate this vNIC with a server that has an adapter which does not support fabric failover, such as the Cisco UCS 82598KR-CI 10-Gigabit Ethernet Adapter. If you do so,Cisco UCS Central generates a configuration fault when you associate the service profile with the server.
Step 6	UCSC(policy-mgr) /org/vnic-templ # **set mac-pool** *mac-pool-name*	The MAC address pool that vNICs created from this vNIC template should use.
Step 7	UCSC(policy-mgr) /org/vnic-templ # **set mtu** *mtu-value*	The maximum transmission unit, or packet size, that vNICs created from this vNIC template should use. Enter an integer between 1500 and 9216. **Note** If the vNIC template has an associated QoS policy, the MTU specified here must be equal to or less than the MTU specified in the associated QoS system class. If this MTU value exceeds the MTU value in the QoS system class, packets may be dropped during data transmission.
Step 8	UCSC(policy-mgr) /org/vnic-templ # **set nw-control-policy** *policy-name*	The network control policy that vNICs created from this vNIC template should use.
Step 9	UCSC(policy-mgr) /org/vnic-templ # **set pin-group** *group-name*	The LAN pin group that vNICs created from this vNIC template should use.
Step 10	UCSC(policy-mgr) /org/vnic-templ # **set qos-policy** *policy-name*	The quality of service policy that vNICs created from this vNIC template should use.
Step 11	UCSC(policy-mgr) /org/vnic-templ # **set stats-policy** *policy-name*	The statistics collection policy that vNICs created from this vNIC template should use.
Step 12	UCSC(policy-mgr) /org/vnic-templ # **set type** {**initial-template** | **updating-template**}	Specifies the vNIC template update type. If you do not want vNIC instances created from this template to be automatically updated when the template is updated, use the **initial-template** keyword; otherwise, use the **updating-template** keyword to

	Command or Action	Purpose
		ensure that all vNIC instances are updated when the vNIC template is updated.
Step 13	UCSC(policy-mgr) /org/vnic-templ # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a vNIC template and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create vnic template VnicTempFoo
UCSC(policy-mgr) /org/vnic-templ* # set descr "This is a vNIC template example."
UCSC(policy-mgr) /org/vnic-templ* # set fabric a
UCSC(policy-mgr) /org/vnic-templ* # set mac-pool pool137
UCSC(policy-mgr) /org/vnic-templ* # set mtu 8900
UCSC(policy-mgr) /org/vnic-templ* # set nw-control-policy ncp5
UCSC(policy-mgr) /org/vnic-templ* # set pin-group PinGroup54
UCSC(policy-mgr) /org/vnic-templ* # set qos-policy QosPol5
UCSC(policy-mgr) /org/vnic-templ* # set stats-policy ServStatsPolicy
UCSC(policy-mgr) /org/vnic-templ* # set type updating-template
UCSC(policy-mgr) /org/vnic-templ* # commit-buffer
UCSC(policy-mgr) /org/vnic-templ #
```

Deleting a vNIC Template

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete vnic-templ** *vnic-templ-name*	Deletes the specified vNIC template.
Step 4	UCSC(policy-mgr) /org* # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the vNIC template named VnicTemp42 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)UCS-A# scope org /
UCSC(policy-mgr) /org # delete vnic template VnicTemp42
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring LAN Connectivity Policies

LAN and SAN Connectivity Policies

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICs and vHBAs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- admin—Can create LAN and SAN connectivity policies
- ls-server—Can create LAN and SAN connectivity policies
- ls-network—Can create LAN connectivity policies
- ls-storage—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Creating a LAN Connectivity Policy

You can create a LAN connectivity policy for LAN networks.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create lan-connectivity-policy** *policy-name*	Creates the specified LAN connectivity policy, and enters organization network control policy mode. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period) and you cannot change this name after the object has been saved.
Step 4	UCSC(policy-mgr) /org/lan-connectivity-policy # **set descr** *policy-name*	(Optional) Adds a description to the policy. We recommend that you include information about where and how the policy should be used. Enter up to 256 characters. you can use any characters or spaces except ' (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Step 5	UCSC(policy-mgr) /org/lan-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows you how to create a LAN connectivity policy named Local_LAN:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# create lan-connectivity-policy Local_LAN
UCSC(policy-mgr) /org/lan-connectivity-policy # set descr Local on site LAN policy
UCSC(policy-mgr) /org/lan-connectivity-policy # commit buffer
```

Creating a vNIC for a LAN Connectivity Policy

You can create a vNIC for a LAN connectivity policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope lan-connectivity-policy** *policy-name*	Enters organization network control policy mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/lan-connectivity-policy # **enter vnic** *vnic-name*	Creates a vNIC and enters configuration mode for the specified vNIC.
Step 5	UCSC(policy-mgr) /org/lan-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows you how to add a vNIC called vNIC1 to an existing LAN connectivity policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope lan-connectivity-policy Local_LAN
UCSC(policy-mgr) /org/lan-connectivity-policy # enter vnic vNIC1
UCSC(policy-mgr) /org/lan-connectivity-policy # commit buffer
```

Creating an iSCSI vNIC for a LAN Connectivity Policy

You can create an iscsi vNIC for a LAN connectivity policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope lan-connectivity-policy** *policy-name*	Enters organization network control policy mode.
Step 4	UCSC(policy-mgr) /org/lan-connectivity-policy # **enter vnic-iscsi** *iscsi-vnic-name*	Creates an iSCSI vNIC and enters configuration mode for the specified iSCSI vNIC.
Step 5	UCSC(policy-mgr) /org/lan-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows you how to add an iSCSI vNIC called iSCSI_vNIC1 to an existing LAN connectivity policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org# scope lan-connectivity-policy Local_LAN
UCSC(policy-mgr) /org/lan-connectivity-policy # enter vnic-iscsi iSCSI_vNIC1
UCSC(policy-mgr) /org/lan-connectivity-policy # commit buffer
```

Configuring Network Control Policies

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.

Configuring a Network Control Policy

MAC address-based port security for Emulex converged Network Adapters (N20-AE0102) is not supported. When MAC address-based port security is enabled, the fabric interconnect restricts traffic to packets that

contain the MAC address that it first learns. This is either the source MAC address used in the FCoE Initialization Protocol packet, or the MAC address in an ethernet packet, whichever is sent first by the adaptor. This configuration can result in either FCoE or Ethernet packets being dropped.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create nw-ctrl-policy** *policy-name*	Creates the specified network control policy, and enters organization network control policy mode.
Step 4	UCSC(policy-mgr) /org/nw-ctrl-policy # {**disable** | **enable**} **cdp**	Disables or enables Cisco Discovery Protocol (CDP).
Step 5	UCSC(policy-mgr) /org/nw-ctrl-policy # **set uplink-fail-action** {**link-down** | **warning**}	Specifies the action to be taken when no uplink port is available in end-host mode. Use the **link-down** keyword to change the operational state of a vNIC to down when uplink connectivity is lost on the fabric interconnect, and facilitate fabric failover for vNICs. Use the **warning** keyword to maintain server-to-server connectivity even when no uplink port is available, and disable fabric failover when uplink connectivity is lost on the fabric interconnect. The default uplink failure action is link-down.
Step 6	UCSC(policy-mgr) /org/nw-ctrl-policy # **set mac-registration-mode**{**all-host-vlans** | **only-native-vlan**	Whether adapter-registered MAC addresses are added only to the native VLAN associated with the interface or added to all VLANs associated with the interface. This can be one of the following: • **Only Native Vlan—**MAC addresses are only added to the native VLAN. This option is the default, and it maximizes the port+VLAN count. • **All Host Vlan—**MAC addresses are added to all VLANs with which they are associated. Select this option if your VLANs are configured to use trunking but are *not* running in Promiscuous mode.
Step 7	UCSC(policy-mgr) /org/nw-ctrl-policy # **create mac-security**	Enters organization network control policy MAC security mode
Step 8	UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security # **set forged-transmit** {**allow** | **deny**}	Allows or denies the forging of MAC addresses when sending traffic. MAC security is disabled when forged MAC addresses are allowed, and MAC security is enabled when forged MAC addresses are denied. By default,

	Command or Action	Purpose
		forged MAC addresses are allowed (MAC security is disabled).
Step 9	UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates a network control policy named ncp5, enables CDP, sets the uplink fail action to link-down, denies forged MAC addresses (enables MAC security), and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create nw-ctrl-policy ncp5
UCSC(policy-mgr) /org/nw-ctrl-policy* # enable cdp
UCSC(policy-mgr) /org/nw-ctrl-policy* # set uplink-fail-action link-down
UCSC(policy-mgr) /org/nw-ctrl-policy* # create mac-security
UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security* # set forged-transmit deny
UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security* # commit-buffer
UCSC(policy-mgr) /org/nw-ctrl-policy/mac-security #
```

Deleting a Network Control Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the root organization mode.
Step 3	UCSC(policy-mgr) /org # **delete nwctrl-policy** *policy-name*	Deletes the specified network control policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the network control policy named ncp5 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete nwctrl-policy ncp5
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Dynamic vNIC Connections Policies

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.

Ethernet Adapter Policy

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.

Server Migration

Note 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 a Dynamic vNIC Connections Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create dynamic-vnic-conn-policy** *policy-name*	Creates a dynamic vNIC connectivity policy.
Step 4	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **set adapter-policy** *profile-name*	Associates the adapter profile to the policy.
Step 5	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **set dynamic-eth** *value*	(Optional) Displays 54, the default number. You can enter an integer between 0 to 256 for the number of dynamic vNICs this policy affects.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **set protection protected-pref-a**	(Optional) Protects dynamic vNIC connectivity policy. You can choose one of the following: • **Protected Pref A—**Cisco UCS attempts to use fabric A but fails over to fabric B if necessary • **Protected Pref A—** Cisco UCS attempts to use fabric B but fails over to fabric A if necessary • **Protected—**Cisco UCS uses whichever fabric is available
Step 7	UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Following example creates a dynamic vNIC connectivity policy called g-DyVCONPol-1, sets adapter profile g-ethPol-1 to associate with the policy, and commits the transaction.

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr) /org # create dynamic-vnic-conn-policy g-DyVCONPol-1
UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # set adapter-policy g-ethPol-1
UCSC(policy-mgr) /org /dynamic-vnic-conn-policy* # commit-buffer
UCSC(policy-mgr) /org /dynamic-vnic-conn-policy #
```

Deleting a Dynamic vNIC Connection Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **delete dynamic-vnic-conn-policy** *policy-name*	Deletes the specified dynamic vNIC connection policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the dynamic vNIC connection policy named sample-1 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete dynamic-vnic-conn-policy sample-1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Quality of Service Policies

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.

Configuring a QoS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters org mode for the specified organization. To enter the default org mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create qos-policy** *policy-name*	Creates the specified QoS policy, and enters org QoS policy mode.
Step 4	UCSC(policy-mgr) /org/qos-policy # **create egress-policy**	Creates the egress policy (for both vNICs and vHBAs) to be used by the QoS policy, and enters org QoS policy egress policy mode.
Step 5	UCSC(policy-mgr) /org/qos-policy/egress-policy # **set host-cos-control** {**full** | **none**}	(Optional) Specifies whether the host or Cisco UCS Central controls the class of service (CoS) for a vNIC. This setting has no effect on a vHBA. Use the **full** keyword to have the host control the CoS. If the packet has a valid CoS value, the host uses that value. Otherwise, it uses the CoS value associated with the specified class priority. Use the **none** keyword to have Cisco UCS Central use the CoS value associated with the specified priority.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/qos-policy/egress-policy # **set prio** *sys-class-name*	Specifies the system class to be used for the egress policy. The *sys-class-name* argument can be one of the following class keywords: • **FC—**Use this priority for QoS policies that control vHBA traffic only. • **Platinum—**Use this priority for QoS policies that control vNIC traffic only. • **Gold—**Use this priority for QoS policies that control vNIC traffic only. • **Silver—**Use this priority for QoS policies that control vNIC traffic only. • **Bronze—**Use this priority for QoS policies that control vNIC traffic only. • **Best Effort—**Do not use this priority. It is reserved for the Basic Ethernet traffic lane. If you assign this priority to a QoS policy and configure another system class as CoS 0, Cisco UCS Central does not default to this system class. It defaults to the priority with CoS 0 for that traffic.
Step 7	UCSC(policy-mgr) /org/qos-policy/egress-policy # **set rate** {**line-rate** | *kbps*} **burst** *bytes*	Specifies the rate limit for egress traffic by defining the average traffic rate and burst size. The **line-rate** keyword sets the rate limit to the physical line rate. Rate limiting is supported only on vNICs on Cisco VIC 1240 and Cisco VIC 1280. M81KR supports rate limiting on both vNICs and vHBAs.
Step 8	UCSC(policy-mgr) /org/qos-policy/egress-policy # **committ-buffer**	Commits the transaction to the system configuration.

The following example creates a QoS policy for vNIC traffic, assigns the platinum system class and sets the rate limit (traffic rate and burst size) for the egress policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create qos-policy VnicPolicy34
UCSC(policy-mgr) /org/qos-policy* # create egress-policy
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set prio platinum
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
UCSC(policy-mgr) /org/qos-policy/egress-policy* # commit-buffer
UCSC(policy-mgr) /org/qos-policy/egress-policy #
```

The following example creates a QoS policy for vHBA traffic, assigns the fc (Fibre Channel) system class and sets the rate limit (traffic rate and burst size) for the egress policy, and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create qos-policy VhbaPolicy12
UCSC(policy-mgr) /org/qos-policy* # create egress-policy
```

```
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set prio fc
UCSC(policy-mgr) /org/qos-policy/egress-policy* # set rate 5000000 burst 65000
UCSC(policy-mgr) /org/qos-policy/egress-policy* # commit-buffer
UCSC(policy-mgr) /org/qos-policy/egress-policy #
```

What to Do Next

Include the QoS policy in a vNIC or vHBA template.

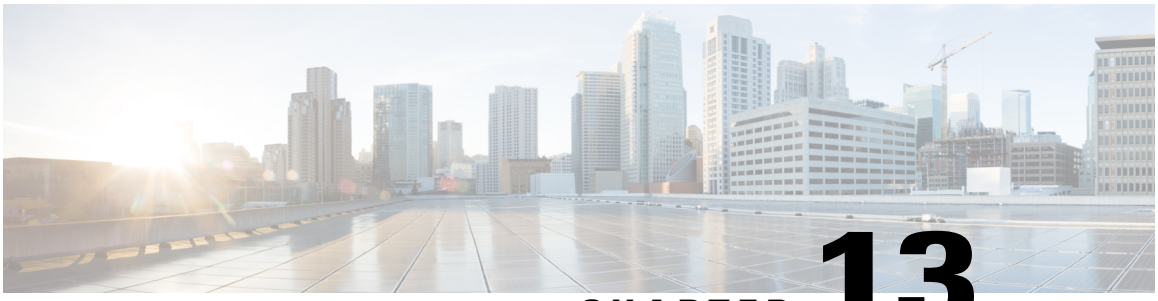
Deleting a QoS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete qos-policy** *policy-name*	Deletes the specified QoS policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following deletes the QoS policy named QosPolicy34 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete qos-policy QosPolicy34
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```



CHAPTER 13

Storage Policies

This chapter includes the following sections:

Creating VSANs

This procedure describes how to create VSANs in a domain group inCisco UCS Central.

Before You Begin

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) #**scope domain-group** *domain-group*	Enters the UCS domain group configuration mode.
Step 3	UCSC(resrouce-mgr) /domain-group #**scope fc-uplink**	Enters fabric configuration command mode.
Step 4	UCSC(resrouce-mgr) /domain-group/fc-uplink #**scope fabric** *{a | b}*.	Enters the configuration mode for the chosen fabric interconnect .
Step 5	UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # **create vsan** *vsan-name vsan-id fcoe-id*	Enters the VSAN configuration command mode, and creates a VSAN with the VSAN name, VSAN ID, and FCoE VLAN ID that you enter.

	Command or Action	Purpose
Step 6	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #**set zoningstate** *{enabled | disabled}* • 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.	Configures Fibre Channel zoning for the VSAN, as follows:
Step 7	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #**commit-buffer**	Commits the transaction to the system.
Step 8	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # **up**	Returns to the the fabric interconnect configuration mode .
Step 9	UCSC(resource-mgr) /domain-group/fc-uplink/fabric # **up**	Returns to the fabric uplink configuration mode.

The following example shows how to create two VSANs each for both fabric interconnect A and B in domain group 12, and commit the transactions:

```
UCSC#connect resource-mgr
UCSC(resource-mgr) #scope domain-group 12
UCSC(resrouce-mgr) /domain-group #scope fc-uplink
UCSC(resrouce-mgr) /domain-group/fc-uplink #scope fabric a
UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # create vsan VSANA 21 21
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # up
UCSC(resource-mgr) /domain-group/fc-uplink/fabric # up
UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # create vsan VSANA2 23 23
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # up
UCSC(resource-mgr) /domain-group/fc-uplink/fabric # up
UCSC(resource-mgr) /domain-group/fc-uplink/up
UCSC(resrouce-mgr) /domain-group/fc-uplink #scope fabric b
UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # create vsan VSANB 22 22
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # up
UCSC(resource-mgr) /domain-group/fc-uplink/fabric # up
UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # create vsan VSANB2 24 24
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # up
UCSC(resource-mgr) /domain-group/fc-uplink/fabric # up
UCSC(resource-mgr) /domain-group/fc-uplink/up
```

The following example shows how to create a VSAN for fabric interconnect A in domain group 12, set the Fibre Channel zoning state, and commit the transaction:

```
UCSC#connect resource-mgr
UCSC(resource-mgr) #scope domain-group 12
UCSC(resrouce-mgr) /domain-group #scope fc-uplink
UCSC(resrouce-mgr) /domain-group/fc-uplink #scope fabric a
UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # create vsan VSANC 25 25
ForDoc(resource-mgr) /domain-group/fc-uplink/fabric/vsan* # set zoningstate enabled
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # up
UCSC(resource-mgr) /domain-group/fc-uplink/fabric # up
```

Modifying VSAN Settings

This procedure describes how to modify VSAN settings for either fabric interconnect A or B in a domain group inCisco UCS Central.

Before You Begin

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) #**scope domain-group** *domain-group*	Enters the UCS domain group configuration mode.
Step 3	UCSC(resource-mgr) /domain-group #**scope fc-uplink**	Enters fabric configuration command mode.
Step 4	UCSC(resource-mgr) /domain-group/fc-uplink #**scope fabric***{a | b}*	Enters configuration mode for the chosen fabric interconnect.
Step 5	UCSC(resource-mgr)#/domain-group/fc-uplink #/fc-uplink/fabric # **scope vsan***vsan-name*	Enters VSAN configuration mode for the chosen VSAN.
Step 6	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # **set id***vsan-id*	Sets the VSAN ID to the value you enter.
Step 7	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* # **set fcoevlan***fcoe-vlan-id*	Sets the FCoE VLAN ID to the value you enter.
Step 8	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #**set zoningstate** *{enabled | disabled}* • disabled—The upstream switch configures and controls the Fibre Channel zoning, or Fibre Channel zoning is not implemented on this VSAN.	Sets the Fibre Channel zoning for the VSAN, as follows:

	Command or Action	Purpose
	• enabled—Cisco UCS Manager will configure and control Fibre Channel zoning when the VSAN is deployed.	
Step 9	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to modify the settings for a VSAN associated with fabric interconnect A in domain group 12:

```
UCSC#connect resource-mgr
UCSC(resource-mgr)# scope domain-group 12
UCSC(resource-mgr)#/domain-group #scope fc-uplink
UCSC(resource-mgr)#/domain-group/fc-uplink #scope fabric a
UCSC(resource-mgr)#/domain-group/fc-uplink #/fc-uplink/fabric # scope vsanVSANC
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # set id2021
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* # set fcoevlan2021
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* # set zoningstatedisabled
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* # commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan #
```

Deleting VSANs

This procedure describes how to delete one or more VSANs from a Cisco UCS Central domain group.

Before You Begin

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) #**scope domain-group** *domain-group*	Enters the UCS domain group configuration mode.
Step 3	UCSC(resource-mgr) /domain-group #**scope fc-uplink**	Enters fabric configuration command mode.
Step 4	UCSC(resource-mgr) /domain-group/fc-uplink #**scope fabric***{a | b}*	Enters configuration mode for the selected fabric interconnect.
Step 5	UCSC(resource-mgr)#/domain-group/fc-uplink #/fc-uplink/fabric # **scope vsan***vsan-name*	Enters VSAN configuration mode for the selected VSAN.
Step 6	UCSC(resource-mgr)#/domain-group/fc-uplink #/fc-uplink/fabric/vsan # **delete vsan**	Deletes the VSAN.

	Command or Action	Purpose
Step 7	UCSC(resource-mgr)#/domain-group/fc-uplink #/fc-uplink/fabric/vsan* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to delete one VSAN from fabric interconnect A and one from fabric interconnect B for domain group 12, and commit the transactions:

```
UCSC#connect resource-mgr
UCSC(resource-mgr) #scope domain-group 12
UCSC(resrouce-mgr) /domain-group #scope fc-uplink
UCSC(resrouce-mgr) /domain-group/fc-uplink #scope fabric a
UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # scope vsan VSANA
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan # up
UCSC(resource-mgr) /domain-group/fc-uplink/fabric # up
UCSC(resource-mgr) /domain-group/fc-uplink/up
UCSC(resrouce-mgr) /domain-group/fc-uplink #scope fabric b
UCSC(resrouce-mgr) /domain-group/fc-uplink/fabric # delete vsan VSANB
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* #commit-buffer
UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan #
```

Configuring Storage Pools

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 domains. 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 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 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.

Creating a WWN Pool

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

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create wwn-pool** *wwn-pool-name* {**node-and-port-wwn-assignment** | **node-wwn-assignment** | **port-wwn-assignment**}	Creates a WWN pool with the specified name and purpose, and enters organization WWN pool mode. This can be one of the following: • **node-and-port-wwn-assignment—**Creates a WWxN pool that includes both world wide node names (WWNNs) and world wide port names (WWPNs). • **node-wwn-assignment—**Creates a WWNN pool that includes only WWNNs. • **port-wwn-assignment—**Creates a WWPN pool that includes only WWPNs.
Step 4	UCSC(policy-mgr) /org/wwn-pool # **set descr** *description*	(Optional) Provides a description for the WWN pool.

	Command or Action	Purpose
		Note If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/wwn-pool # **set descr** *description*	(Optional) Provides a description for the WWN pool. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 6	UCSC(policy-mgr) /org/wwn-pool # **set max-ports-per-node** {**15-ports-per-node** | **3-ports-per-node** | **31-ports-per-node** | **63-ports-per-node** | **7-ports-per-node**}	For WWxN pools, specify the maximum number of ports that can be assigned to each node name in this pool. The default value is **3-ports-per-node**. **Note** The pool size for WWxN pools must be a multiple of *ports-per-node* + 1. For example, if you specify **7-ports-per-node**, the pool size must be a multiple of 8. If you specify **63-ports-per-node**, the pool size must be a multiple of 64.
Step 7	UCSC(policy-mgr) /org/wwn-pool # **create block** *first-wwn last-wwn*	Creates a block (range) of WWNs, and enters organization WWN pool block mode. You must specify the first and last WWN in the block using the form *nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*, with the WWNs separated by a space. **Note** A WWN pool can contain more than one WWN block. To create multiple WWN blocks, you must enter multiple **create block** commands from organization WWN pool mode.
Step 8	UCSC(policy-mgr) /org/wwn-pool/block # **exit**	Exits organization WWN pool block mode.
Step 9	UCSC(policy-mgr) /org/wwn-pool # **create initiator** *wwn wwn*	Creates a single initiator for a WWNN or WWPN pool, and enters organization WWN pool initiator mode. You must specify the initiator using the form *nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*:*nn*. **Note** A WWNN or WWPN pool can contain more than one initiator. To create multiple initiators, you must enter multiple **create initiator** commands from organization WWN pool mode.
Step 10	UCSC(policy-mgr) /org/iqn-pool/block # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to create another pool, wait at least 5 seconds.

The following example shows how to create a WWNN pool named GPool1, provide a description for the pool, specify a block of WWNs and an initiator to be used for the pool, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr) /org # create wwn-pool GPool1 node-wwn-assignment
UCSC(policy-mgr) /org/wwn-pool* # set descr "This is my WWNN pool"
UCSC(policy-mgr) /org/wwn-pool* # create block 20:00:00:25:B5:00:00:00 20:00:00:25:B5:00:00:01
UCSC(policy-mgr) /org/wwn-pool/block* # exit
UCSC(policy-mgr) /org/wwn-pool* # create initiator 23:00:00:05:AD:1E:02:00
UCSC(policy-mgr) /org/wwn-pool/initiator* # commit-buffer
UCSC(policy-mgr) /org/wwn-pool/initiator #
```

The following example shows how to create a WWxN pool named GPool1, provide a description for the pool, specify seven ports per node, specify a block of eight WWNs to be used for the pool, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create wwn-pool GPool1 node-and-port-wwn-assignment
UCSC(policy-mgr) /org/wwn-pool* # set descr "This is my WWxN pool"
UCSC(policy-mgr) /org/wwn-pool* # set max-ports-per-node 7-ports-per-node
UCSC(policy-mgr) /org/wwn-pool* # create block 20:00:00:25:B5:00:00:00 20:00:00:25:B5:00:00:08
UCSC(policy-mgr) /org/wwn-pool/block* # commit-buffer
UCSC(policy-mgr) /org/wwn-pool/block #
```

What to Do Next

- Include the WWPN pool in a vHBA template.
- Include the WWNN pool in a service profile and/or template.
- Include the WWxN pool in a service profile and/or template.

Deleting a WWN 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.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete wwn-pool** *wwn-pool-name*	Deletes the specified WWN pool.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration. **Note** If you plan to delete another pool, wait at least 5 seconds.

The following example shows how to delete the WWNN pool named GPool1 and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr) /org # delete wwn-pool GPool1
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring Storage-Related Policies

vHBA Template

This template is a policy that defines how a vHBA on a server connects to the SAN. It is also referred to as a vHBA SAN connectivity template.

You must include this policy in a service profile for it to take effect.

Configuring a vHBA Template

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create vhba-templ** *vhba-templ-name* [**fabric** {**a** | **b**}] [**fc-if** *vsan-name*]	Creates a vHBA template and enters organization vHBA template mode.
Step 4	UCSC(policy-mgr) /org/vhba-templ # **set descr** *description*	(Optional) Provides a description for the vHBA template.
Step 5	UCSC(policy-mgr) /org/vhba-templ # **set fabric** {**a** | **b**}	(Optional) Specifies the fabric to use for the vHBA. If you did not specify the fabric when creating the vHBA template in Step 2, then you have the option to specify it with this command.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/vhba-templ # **set fc-if** *vsan-name*	(Optional) Specifies the Fibre Channel interface (named VSAN) to use for the vHBA template. If you did not specify the Fibre Channel interface when creating the vHBA template in Step 2, you have the option to specify it with this command.
Step 7	UCSC(policy-mgr) /org/vhba-templ # **set max-field-size** *size-num*	Specifies the maximum size of the Fibre Channel frame payload (in bytes) that the vHBA supports.
Step 8	UCSC(policy-mgr) /org/vhba-templ # **set pin-group** *group-name*	Specifies the pin group to use for the vHBA template.
Step 9	UCSC(policy-mgr) /org/vhba-templ # **set qos-policy** *mac-pool-name*	Specifies the QoS policy to use for the vHBA template.
Step 10	UCSC(policy-mgr) /org/vhba-templ # **set stats-policy** *policy-name*	Specifies the server and server component statistics threshold policy to use for the vHBA template.
Step 11	UCSC(policy-mgr) /org/vhba-templ # **set type** {**initial-template** | **updating-template**}	Specifies the vHBA template update type. If you do not want vHBA instances created from this template to be automatically updated when the template is updated, use the **initial-template** keyword; otherwise, use the **updating-template** keyword to ensure that all vHBA instances are updated when the vHBA template is updated.
Step 12	UCSC(policy-mgr) /org/vhba-templ # **set wwpn-pool** *pool-name*	Specifies the WWPN pool to use for the vHBA template.
Step 13	UCSC(policy-mgr) /org/vhba-templ # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a vHBA template and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create vhba template VhbaTempFoo
UCSC(policy-mgr) /org/vhba-templ* # set descr "This is a vHBA template example."
UCSC(policy-mgr) /org/vhba-templ* # set fabric a
UCSC(policy-mgr) /org/vhba-templ* # set fc-if accounting
UCSC(policy-mgr) /org/vhba-templ* # set max-field-size 2112
UCSC(policy-mgr) /org/vhba-templ* # set pin-group FcPinGroup12
UCSC(policy-mgr) /org/vhba-templ* # set qos-policy policy34foo
UCSC(policy-mgr) /org/vhba-templ* # set stats-policy ServStatsPolicy
UCSC(policy-mgr) /org/vhba-templ* # set type updating-template
UCSC(policy-mgr) /org/vhba-templ* # set wwpn-pool SanPool7
UCSC(policy-mgr) /org/vhba-templ* # commit-buffer
UCSC(policy-mgr) /org/vhba-templ #
```

Deleting a vHBA Template

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **delete vhba-templ** *vhba-templ-name*	Deletes the specified vHBA template.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the vHBA template named VhbaTempFoo and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete vhba template VhbaTempFoo
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Default vHBA Behavior Policy

Default vHBA behavior policy allow you to configure how vHBAs are created for a service profile. You can choose to create vHBAs manually, or you can allow them to be created automatically.

You can configure the default vHBA behavior policy to define how vHBAs are created. This can be one of the following:

- **None—**Cisco UCS Central does not create default vHBAs for a service profile. All vHBAs must be explicitly created.
- **HW Inherit—**If a service profile requires vHBAs and none have been explicitly defined, Cisco UCS Central creates the required vHBAs based on the adapter installed in the server associated with the service profile.

Note If you do not specify a default behavior policy for vHBAs, **none** is used by default.

Configuring a Default vHBA Behavior Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the root organization mode.
Step 3	UCSC(policy-mgr)/org # **scope vhba-beh-policy**	Enters default vHBA behavior policy mode.
Step 4	UCSC(policy-mgr)/org/vhba-beh-policy # **set action** {**hw-inherit** [**template_name** *name*] | **none**}	Specifies the default vHBA behavior policy. This can be one of the following: • **hw-inherit—**If a service profile requires vHBAs and none have been explicitly defined, Cisco UCS Central creates the required vHBAs based on the adapter installed in the server associated with the service profile. If you specify **hw-inherit**, you can also specify a vHBA template to create the vHBAs. • **none—**Cisco UCS Central does not create default vHBAs for a service profile. All vHBAs must be explicitly created.
Step 5	UCSC(policy-mgr)/org/vhba-beh-policy # **commit-buffer**	Commits the transaction to the system configuration.

This example shows how to set the default vHBA behavior policy to **hw-inherit**.

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org /
UCSC(policy-mgr)/org # scope vhba-beh-policy
UCSC(policy-mgr)/org/vhba-beh-policy # set action hw-inherit
UCSC(policy-mgr)/org/vhba-beh-policy* # commit-buffer
UCSC(policy-mgr)/org/vhba-beh-policy #
```

Configuring Fibre Channel Adapter Policies

Ethernet and Fibre Channel Adapter Policies

These 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 an apparent 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 5s 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 Ethernet adapter policies and 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.

Important 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.

However, if you are creating an Ethernet adapter policy for a Windows OS (instead of using the default Windows adapter policy), 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

Configuring a Fibre Channel Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **create fc-policy** *policy-name*	Creates the specified Fibre Channel adapter policy and enters organization Fibre Channel policy mode.
Step 4	UCSC(policy-mgr) /org/fc-policy # **set descr** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /org/fc-policy # **set error-recovery** {**fcp-error-recovery** {**disabled** | **enabled**} | **link-down-timeout** *timeout-msec* | **port-down-io-retry-count** *retry-count* | **port-down-timeout** *timeout-msec*}	(Optional) Configures the Fibre Channel error recovery.
Step 6	UCSC(policy-mgr) /org/fc-policy # **set interrupt mode** {**intx** | **msi** | **msi-x**}}	(Optional) Configures the driver interrupt mode.
Step 7	UCSC(policy-mgr) /org/fc-policy # **set port** {**io-throttle-count** *throttle-count* | **max-luns** *max-num*}	(Optional) Configures the Fibre Channel port.
Step 8	UCSC(policy-mgr) /org/fc-policy # **set port-f-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	(Optional) Configures the Fibre Channel port fabric login (FLOGI).
Step 9	UCSC(policy-mgr) /org/fc-policy # **set port-p-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	(Optional) Configures the Fibre Channel port-to-port login (PLOGI).
Step 10	UCSC(policy-mgr) /org/fc-policy # **set recv-queue** {**count** *count* | **ring-size** *size-num*}	(Optional) Configures the Fibre Channel receive queue.
Step 11	UCSC(policy-mgr) /org/fc-policy # **set scsi-io** {**count** *count* | **ring-size** *size-num*}	(Optional) Configures the Fibre Channel SCSI I/O.

	Command or Action	Purpose
Step 12	UCSC(policy-mgr) /org/fc-policy # **set trans-queue ring-size** *size-num*}	(Optional) Configures the Fibre Channel transmit queue.
Step 13	UCSC(policy-mgr) /org/fc-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures a Fibre Channel adapter policy and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create fc-policy FcPolicy42
UCSC(policy-mgr) /org/fc-policy* # set descr "This is a Fibre Channel adapter policy example."
UCSC(policy-mgr) /org/fc-policy* # set error-recovery error-detect-timeout 2500
UCSC(policy-mgr) /org/fc-policy* # set port max-luns 4
UCSC(policy-mgr) /org/fc-policy* # set port-f-logi retries 250
UCSC(policy-mgr) /org/fc-policy* # set port-p-logi timeout 5000
UCSC(policy-mgr) /org/fc-policy* # set recv-queue count 1
UCSC(policy-mgr) /org/fc-policy* # set scsi-io ring-size 256
UCSC(policy-mgr) /org/fc-policy* # set trans-queue ring-size 256
UCSC(policy-mgr) /org/fc-policy* # commit-buffer
UCSC(policy-mgr) /org/fc-policy #
```

Deleting a Fibre Channel Adapter Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 3	UCSC(policy-mgr) /org # **delete fc-policy** *policy-name*	Deletes the specified Fibre Channel adapter policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the Fibre Channel adapter policy named FcPolicy42 and commits the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete fc-policy FcPolicy42
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Configuring SAN Connectivity Policies

LAN and SAN Connectivity Policies

Connectivity policies determine the connections and the network communication resources between the server and the LAN or SAN on the network. These policies use pools to assign MAC addresses, WWNs, and WWPNs to servers and to identify the vNICs and vHBAs that the servers use to communicate with the network.

Note We do not recommend that you use static IDs in connectivity policies, because these policies are included in service profiles and service profile templates and can be used to configure multiple servers.

Privileges Required for LAN and SAN Connectivity Policies

Connectivity policies enable users without network or storage privileges to create and modify service profiles and service profile templates with network and storage connections. However, users must have the appropriate network and storage privileges to create connectivity policies.

Privileges Required to Create Connectivity Policies

Connectivity policies require the same privileges as other network and storage configurations. For example, you must have at least one of the following privileges to create connectivity policies:

- admin—Can create LAN and SAN connectivity policies
- ls-server—Can create LAN and SAN connectivity policies
- ls-network—Can create LAN connectivity policies
- ls-storage—Can create SAN connectivity policies

Privileges Required to Add Connectivity Policies to Service Profiles

After the connectivity policies have been created, a user with ls-compute privileges can include them in a service profile or service profile template. However, a user with only ls-compute privileges cannot create connectivity policies.

Creating a SAN Connectivity Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enter organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **create san-connectivity-policy** *policy-name*	Creates the specified SAN connectivity policy, and enters organization network control policy mode. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period) and you cannot change this name after the object has been saved.
Step 4	UCSC(policy-mgr) /org/san-connectivity-policy # **set descr** *policy-name*	(Optional) Adds a description to the policy. We recommend that you include information about where and how the policy should be used. Enter up to 256 characters. you can use any characters or spaces except ' (accent mark), \ (backslash), ^ (carat), " (double quote), = (equal sign), > (greater than), < (less than), or ' (single quote).
Step 5	UCSC(policy-mgr) /org/service-profile # **set identity** {**dynamic-uuid** {*uuid* | **derived**} | **dynamic-wwnn** {*wwnn* | **derived**} | **uuid-pool** *pool-name* | **wwnn-pool** *pool-name*}	Specifies how the server acquires a UUID or WWNN. You can do one of the following: • Create a unique UUID in the form *nnnnnnnn-nnnn-nnnn-nnnnnnnnnnnn* • Derive the UUID from the one burned into the hardware at manufacture • Use a UUID pool • Create a unique WWNN in the form *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* **:** *hh* • Derive the WWNN from one burned into the hardware at manufacture • Use a WWNN pool
Step 6	UCSC(policy-mgr) /org/san-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create a SAN connectivity policy named SanConnect242 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # create san-connectivity-policy SanConnect242
UCSC(policy-mgr) /org/san-connectivity-policy* # set descr "SAN connectivity policy"
UCSC(policy-mgr) /org/san-connectivity-policy* # set identity wwnn-pool SanPool7
UCSC(policy-mgr) /org/san-connectivity-policy* # commit-buffer
UCSC(policy-mgr) /org/san-connectivity-policy #
```

What to Do Next

Add one or more vHBAs and/or initiator groups to this SAN connectivity policy.

Creating a vHBA for a SAN Connectivity Policy

If you are continuing from Creating a SAN Connectivity Policy, on page 378, begin this procedure at Step 3

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope san-connectivity-policy** *policy-name*	Enters SAN connectivity policy mode for the specified SAN connectivity policy.
Step 4	UCSC(policy-mgr) /org/san-connectivity-policy # **create vhba** *vhba-name* [**fabric** {**a** | **b**}] [**fc-if** *fc-if-name*]	Creates a vHBA for the specified SAN connectivity policy and enters vHBA mode. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object has been saved.
Step 5	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set adapter-policy** *policy-name*	Specifies the adapter policy to use for the vHBA.
Step 6	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set identity** {**dynamic-wwpn** {*wwpn* | **derived**} | **wwpn-pool** *wwn-pool-name*}	Specifies the WWPN for the vHBA. You can set the storage identity using one of the following options: • Create a unique WWPN in the form *hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*:*hh*. You can specify a WWPN in the range 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. If you want the WWPN to be compatible with Cisco MDS Fibre Channel switches, use the WWPN template **20:00:00:25:B5:XX:XX:XX**. • Derive the WWPN from one burned into the hardware at manufacture. • Assign a WWPN from a WWN pool.
Step 7	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set max-field-size** *size-num*	Specifies the maximum size of the Fibre Channel frame payload (in bytes) that the vHBA supports.

	Command or Action	Purpose
		Enter an integer between 256 and 2112. The default is 2048.
Step 8	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set order** {*order-num* | **unspecified**}	Specifies the PCI scan order for the vHBA.
Step 9	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set pers-bind** {**disabled** | **enabled**}	Disables or enables persistent binding to Fibre Channel targets.
Step 10	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set pin-group** *group-name*	Specifies the SAN pin group to use for the vHBA.
Step 11	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set qos-policy** *policy-name*	Specifies the QoS policy to use for the vHBA.
Step 12	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set stats-policy** *policy-name*	Specifies the statistics threshold policy to use for the vHBA.
Step 13	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set template-name** *policy-name*	Specifies the vHBA template to use for the vHBA. If you choose to use a vHBA template for the vHBA, you must still complete all of the configuration not included in the vHBA template, including Steps 4, 7, and 8.
Step 14	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **set vcon** {**1** | **2** | **3** | **4** | **any**}	Assigns the vHBA to one or all virtual network interface connections.
Step 15	UCSC(policy-mgr) /org/san-connectivity-policy/vhba # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to configure a vHBA for a SAN connectivity policy named SanConnect242 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope san-connectivity-policy SanConnect242
UCSC(policy-mgr) /org/san-connectivity-policy* # create vhba vhba3 fabric a
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set adapter-policy AdaptPol2
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set identity wwpn-pool SanPool7
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set max-field-size 2112
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set order 0
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set pers-bind enabled
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set pin-group FcPinGroup12
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set qos-policy QosPol5
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set stats-policy StatsPol2
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set template-name SanConnPol3
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # set vcon any
UCSC(policy-mgr) /org/san-connectivity-policy/vhba* # commit-buffer
UCSC(policy-mgr) /org/san-connectivity-policy/vhba #
```

What to Do Next

If desired, add another vHBA or an initiator group to the SAN connectivity policy. If not, include the policy in a service profile or service profile template.

Creating an Initiator Group for a SAN Connectivity Policy

If you are continuing from Creating a SAN Connectivity Policy, on page 378, begin this procedure at Step 3.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope san-connectivity-policy** *policy-name*	Enters SAN connectivity policy mode for the specified SAN connectivity policy.
Step 4	UCSC(policy-mgr) /org/san-connectivity-policy # **create initiator-group** *group-name* **fc**	Creates the specified initiator group for Fibre Channel zoning and enters initiator group mode. 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

	Command or Action	Purpose
		cannot change this name after the object has been saved.
Step 5	UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group # **create initiator** *vhba-name*	Creates the specified vHBA initiator in the initiator group. If desired, repeat this step to add a second vHBA initiator to the group.
Step 6	UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group # **set storage-connection-policy** *policy-name*	Associates the specified storage connection policy with the SAN connectivity policy.

	Command or Action	Purpose
		Note This step assumes that you want to associate an existing storage connection policy to associate with the SAN connectivity policy. If you do, continue with Step 10. If you want to create a local storage definition for this policy instead, continue with Step 6.
Step 7	UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group/storage-connection-def # **create storage-target** *wwpn*	Creates a storage target endpoint with the specified WWPN, and enters storage target mode.
Step 8	UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target # **set target-path** {**a** | **b**}	Specifies which fabric interconnect is used for communications with the target endpoint.
Step 9	UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target # **set target-vsan** *vsan*	Specifies which VSAN is used for communications

	Command or Action	Purpose
		with the target endpoint.
Step 10	UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to configure an initiator group named initGroupZone1 with two initiators for a a SAN connectivity policy named SanConnect242, configure a local storage connection policy definition named scPolicyZone1, and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org* # scope san-connectivity-policy SanConnect242
UCSC(policy-mgr) /org/san-connectivity-policy # create initiator-group initGroupZone1 fc
UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group* # set zoning-type sist
UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group* # create initiator vhba1
UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group* # create initiator vhba2
UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group* # create storage-connection-def
 scPolicyZone1
UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group/storage-connection-def* #
create storage-target
20:10:20:30:40:50:60:70
UCSC(policy-mgr)
/org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target* # set
target-path a
UCSC(policy-mgr)
/org/san-connectivity-policy/initiator-group/storage-connection-def/storage-target* # set
target-vsan default
UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group* # commit-buffer
UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group #
```

What to Do Next

If desired, add another initiator group or a vHBA to the SAN connectivity policy. If not, include the policy in a service profile or service profile template.

Deleting a vHBA from a SAN Connectivity Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope san-connectivity-policy** *policy-name*	Enters SAN connectivity policy mode for the specified SAN connectivity policy.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/san-connectivity-policy # **delete vHBA** *vhba-name*	Deletes the specified vHBA from the SAN connectivity policy.
Step 5	UCSC(policy-mgr) /org/san-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete a vHBA named vHBA3 from a SAN connectivity policy named SanConnect242 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope san-connectivity-policy SanConnect242
UCSC(policy-mgr) /org/san-connectivity-policy # delete vHBA vHBA3
UCSC(policy-mgr) /org/san-connectivity-policy* # commit-buffer
UCSC(policy-mgr) /org/san-connectivity-policy #
```

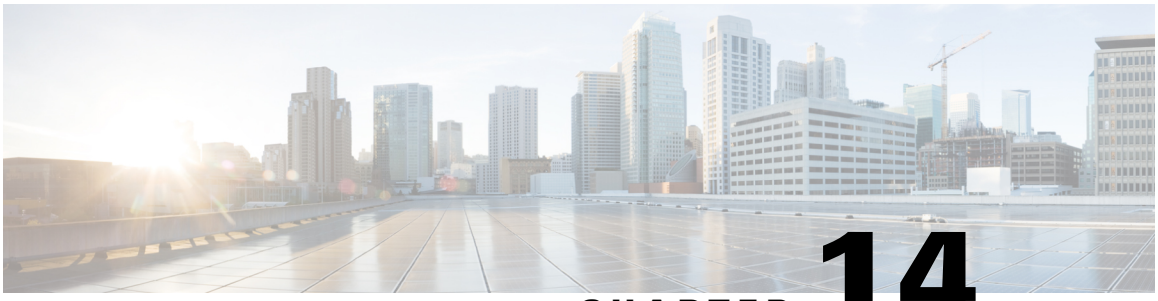
Deleting an Initiator Group from a SAN Connectivity Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, enter, / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **scope san-connectivity-policy** *policy-name*	Enters SAN connectivity policy mode for the specified SAN connectivity policy.
Step 4	UCSC(policy-mgr) /org/san-connectivity-policy # **delete initiator-group** *group-name*	Deletes the specified initiator group from the SAN connectivity policy.
Step 5	UCSC(policy-mgr) /org/san-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to delete an initiator group named initGroup3 from a SAN connectivity policy named SanConnect242 and commit the transaction:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # scope san-connectivity-policy SanConnect242
UCSC(policy-mgr) /org/san-connectivity-policy # delete initiator-group initGroup3
UCSC(policy-mgr) /org/san-connectivity-policy* # commit-buffer
UCSC(policy-mgr) /org/san-connectivity-policy #
```



CHAPTER 14

Statistics Management

This chapter includes the following sections:

Statistics Management

Cisco UCS Central enables you to generate standard and customized reports from the **Statistics** tab. You can generate reports on the following data in the registered Cisco UCS domains:

- Cooling
- Network
- Power
- Temperature

Important You must be logged in as an admin or as a user with statistics privilege to create, modify or delete a report. Other users can only run reports and view available data.

When you generate a report, you can specify the option to view the report either in the format of a table or a chart. Using the display options, you can select top or bottom domains for a specific report type. You can also use overlay to overlay the data for a report type. The following are the two report options:

- **Standard Reports**: Predefined reports on Peak Fan Speed, Receive Traffic(Rx), Transmit Traffic (Tx), Average Power, and Peak Temperature. You can run any of these predefined reports any time to view reports. You can also modify the predefined configurations, but cannot create any new standard report.
- **Custom Reports**: Option to create customized reports from any of the available report options. Based on your requirements, you can create either create individual reports in the **Ungrouped Reports** or create **Report Group**s and then create reports under the groups or sub-groups. You can create, edit or delete the custom report groups at anytime.

Statistics Data Collection in Cisco UCS Central

Cisco UCS Central collects and aggregates statistics data on **Network**, **Temperature**, **Cooling** and **Power** from the registered Cisco UCS domains. During Cisco UCS Central installation, you must specify a default location to store the statistics data. You can store the statistics data in the internal PostgreSQL database called "ucscentral-stats-db" or in an external database such as Oracle 11g, MSSQL, or Postgre SQL. If you have chosen internal storage as the default location during installation, the statistics data is stored only for a maximum of two weeks. If you want to retain the collected data for more than two weeks, it is recommended that you set up an external database, see External Database for Statistics, on page 390.

The collected data is aggregated based on daily, hourly, weekly and real time records and stored in tables. You can run SQL query in this database to retrieve data specific to each of the report components, see Retrieving Data from the External Database, on page 393. Cisco UCS Central database is the default database to store the data.

You can set up statistics collection interval using Cisco UCS Central CLI, to collect information from the registered Cisco UCS domains at a specified interval. When a new Cisco UCS domain is registered in Cisco UCS Central, Cisco UCS Central subscribes the new domain to the statistics collection interval you have specified. If you reconfigure the collection interval, the data is updated in the registered domains. The registered Cisco UCS domains send statistics to Cisco UCS Central based on the specified collection interval.

Statistics collection interval can be one of the following:

- 15 minutes (default)
- 30 minutes
- never—disables statistics collection

Important You can specify the statistics collection interval only in the Cisco UCS Central CLI. You cannot set it from the Cisco UCS Central GUI. You can view the statistics reports only in the Cisco UCS Central GUI and not in the Cisco UCS Central CLI.

Setting the Statistics Collection Interval

The statistics collection policy governs the collection interval for the data from registered UCS domains. Cisco UCS Central subscribes to domain statistics when a new Cisco UCS domain is registered with Cisco UCS Central. This subscription request is also sent when you reconfigure the collection interval. After subscribing to this data, the registered Cisco UCS domains send statistics to Cisco UCS Central based on the specified collection interval.

Before You Begin

You must be logged in as an admin user to perform this task.

Procedure

Step 1 UCSC# **connect stats-mgr**
Enters the statistics manager mode.

Step 2 UCSC (stats-mgr) # **scope collection-policy**
Enters collection policy configuration mode.

Step 3 UCSC (stats-mgr) /collection-policy # **set collection-interval 30min**
Sets the collection interval to 30 minutes. The other options are 15 minutes and never.

Step 4 UCSC (stats-mgr) /collection-policy # **commit-buffer**
Commits the transaction to the system configuration.

Step 5 UCSC (stats-mgr) /collection-policy # **show collection-policy**
Displays the collection policy interval.

The following example sets the statistics collection interval to 15 minutes and commits the transaction:

```
UCSC # connect stats-mgr
UCSC (stats-mgr) # scope collection-policy
UCSC (stats-mgr) /collection-policy # set collection-interval 15min
UCSC (stats-mgr) /collection-policy* # commit-buffer
UCSC (stats-mgr) /collection-policy # show collection-policy
Stats Collection Policy:
    Collection Interval
    -------------------
    15min
UCSC (stats-mgr) /collection-policy #
```

What to Do Next

Leave the system for a few days so statistics are collected and stored. You can then login to Cisco UCS Central GUI and create custom statistic reports for different endpoints.

Setting up an Internal Database for Statistics

Cisco UCS Central collects network statistics data of registered Cisco UCS domains and aggregates it to hourly, daily and weekly data. This statistical data is stored within the Cisco UCS Central environment in a PostgreSQL database called "ucscentral-stats-db". This is the database that is specific to Cisco UCS Central. The statistical data in this Cisco UCS Central database is stored only for a maximum of 2 weeks. Data older than 2 weeks is automatically purged. In addition, when Cisco UCS Central is configured to use the default PostgreSQL database for the statistics data, you can configure a maximum of only 5 Cisco UCS domains for statistics collection. If you want to retain statistics data for a longer period of time, or if you want to register additional Cisco UCS domains for statistics collection, it is recommended that you configure a database external to Cisco UCS Central.

Follow this procedure only when you want to revert from an external database to the default PostgreSQLdatabase.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect stats-mgr**	Enters the statistics manager mode.
Step 2	UCSC (stats-mgr) # **scope db-configuration**	Enters database configuration mode.

	Command or Action	Purpose
Step 3	UCSC (stats-mgr) /db-configuration # **set port** *port-number*	Sets the port. The default port is 5432.
Step 4	UCSC (stats-mgr) /db-configuration # **set database** *db-name*	Sets the database name. For an internal database, the name is ucscentral-stats-db.
Step 5	UCSC (stats-mgr) /db-configuration # **set type** *dbtype*	Sets the database type. In this case, enter postgres.
Step 6	UCSC (stats-mgr) /db-configuration # **set user** *dbusername*	Sets the database user name.
Step 7	UCSC (stats-mgr) /db-configuration # **set pwd** *dbpassword*	Sets the database password. The password for the internal database is always blank, so press Enter.
Step 8	UCSC (stats-mgr) /db-configuration # **commit-buffer**	Commits the transaction to the system configuration.

The following example sets up an internal database for statistics data, commits the transaction and shows details for the database:

```
UCSC# connect stats-mgr
UCSC (stats-mgr)  # scope db-configuration
UCSC (stats-mgr) /db-configuration # set port 5432
UCSC (stats-mgr) /db-configuration # set database ucscentral-stats-db
UCSC (stats-mgr) /db-configuration # set type postgres
UCSC (stats-mgr) /db-configuration # set user postgres
UCSC (stats-mgr) /db-configuration # set pwd
UCSC (stats-mgr) /db-configuration # commit-buffer
UCSC (stats-mgr) /db-configuration # show detail

Database Configuration:
    Type: Postgres
    Hostname: localhost
    Port: 5432
    Database: ucscentral-stats-db
    User: postgres
    Pwd:
```

What to Do Next

Set the statistics collection interval if you want it to be an interval other than the default of 15 minutes.

External Database for Statistics

You can set up an external database to retain the collected data for more than two weeks or to collect statistics data from more than 5 registered Cisco UCS domains. The following are the two supported databases that you can use as external database from Cisco UCS Central:

- Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64-bit Production or higher
- PostgreSQL Server 9.1.8 64-bit or higher

- Microsoft SQL Server 2012 (SP1) - 11.0.3000.0 (X64) or higher
- Microsoft SQL Server 2008 R2 10.50.1600.1 (X64) SP1 or higher

Make sure you have the following information to access and setup either of these databases as your external database:

- Database server host name
- Database name
- Username
- Password
- Port number

Note You must open the firewall ports in the database server so that Cisco UCS Central can access the configured external database.

Setting up an External Database

You can set up the external database either during initial Cisco UCS Central set up or at anytime you have a requirement to set up an external database for statistics collection:

- **Setting up external database with initial setup**: When you are doing the initial set up for Cisco UCS Central, you are prompted to enable statistics collection. If you choose **Yes**, you are prompted to enter information on the external database. If you choose **No**, the collection of statistics data from registered Cisco UCS domains is disabled.
- **Anytime**: You can use the Cisco UCS Central CLI to connect to the external database and set up statistics collection for registered Cisco UCS domains. For information on setting up an Oracle database, see Connecting to an External Oracle Database, on page 395. For information on setting up an PostgreSQL database, see Connecting to an External PostgreSQL Database, on page 396.

The external database stores statistical data on network traffic, temperature, cooling and power from the registered Cisco UCS domains. You can run queries on the external database to retrieve statistics data on network, temperature, cooling and power. For information on running queries on the database, see Retrieving Data from the External Database, on page 393.

Note When you set up an external database to store the statistical data, you must determine the time interval to purge old records from the database. You are responsible for maintaining the external database.

Guidelines for Configuring an External Database

When you configure the database for statistics collection, make sure to restart the Cisco UCS Central services. You must restart the services in the following scenarios:

- After upgrading to the latest version of Cisco UCS Central using the ISO image

Earlier versions of Cisco UCS Central did not have the capability for statistics collection. After the upgrade process is complete, you can use the Cisco UCS Central CLI to set up an external database for statistics data collection.

- You set up an external database for statistics collection after installing Cisco UCS Central. The external database can be either an Oracle database or a PostgreSQL database.
- After switching from an Oracle database to a PostgreSQL database or switching from a PostgreSQL database to an Oracle database.

Backing up and Restoring Cisco UCS Central Statistics Database

The Cisco UCS Central database is not backed up during a full state backup. If you have set up an external database to store statistical data, then you must follow standard database backup and restore procedures. However, prior to restoring an external database, you must stop the Cisco UCS Central service. To stop this service, you must login to the Cisco UCS Central CLI, and run the **pmon stop** command in the **local-mgmt** command mode. After the database is restored, start the Cisco UCS Central service by running the **pmon start** command in the Cisco UCS Central CLI.

Troubleshooting Faults with the External Database

When Cisco UCS Central fails to connect to an external database, a fault is raised. You can view the fault details in the Cisco UCS Central CLI using the **show fault** command or in the Cisco UCS Central GUI, **Fault** panel.. When the problem is resolved ,Cisco UCS Central automatically retries to connect to the external database. If the connection is established, the fault is cleared from the Cisco UCS Central CLI.

Statistics Data in External Database

External database stores the collected statistics data in tables. You can purge old statistics data from the external database using a script. The following table describes the database table names and corresponding data stored in each table:

Table Name	Data Stored in the Table
adaptorHBAVnicStats	HBA Adaptor traffic data.
adaptorNICVnicStats	NIC Adaptor traffic data.
adaptorVnicStats	NIC/HBA Adaptor traffic data.
computeMbPowerStats	Blade Server power data.
computeMbTempStats	Blade Server temperature data.
computeRackUnitMbTempStats	Rack Server temperature data.
equipmentChassisStats	Chassis power data.
equipmentFanStats	Chassis fan speed data.
equipmentNetworkElementFanStats	FI fan speed data.

Table Name	Data Stored in the Table
equipmentPsuStats	Chassis PSU data.
equipmentRackUnitFanStats	Rack server fan speed data.
equipmentRackUnitPsuStats	Rack server PSU data.
etherRxStats	Ethernet traffic receive data
etherTxStats	Ethernet traffic transmit data.
fcStats	FC traffic data.
processorEnvStats	CPU environment data.

Retrieving Data from the External Database

The database collects statistical data on network, temperature, cooling, and power. The data collected from the registered Cisco UCS domains is stored in the database and then aggregated in the following ways:

- Real time records
- Parent to child aggregation

The following table describes the database table and the nature of information stored in this table.

StatType	Stat	Table	MO/TableName	Property
Temperature	Inlet Air Temp	1	computeMbTempStats	fmTempSenIo
	Processor Temp	2	processorEnvStats	Temperature
Power	Blade DC Power	3	computeMbPowerStats	consumedPower
	Chassis AC Power	4	equipmentChassisStats	inputPower
Cooling	FI Fan Speed	5	equipmentNetworkElementFanStats	Speed
	Chassis Fan Speed	6	equipmentFanStats	speed
FI Ethernet Traffic	Transmit	7	etherTxStats	TotalBytes
	Receive	8	etherRxStats	TotalBytes
FI Fibre Channel Traffic	Transmit/Receive	9	fcStats	BytesTx,BytesRx
Server Ethernet Traffic	Transmit/Receive	10	adaptorNICVnicStats	BytesTx,BytesRx
Server FC traffic	Transmit/Receive	11	adaptorHBAVnicStats	BytesTx,BytesRx

StatType	Stat	Table	MO/TableName	Property
Server Eth & FC Traffic	Transmit/Receive	12	adaptorVnicStats	BytesTx,BytesRx
NA	Internal DN mapping table	13	affectedId2Dn	NA

Tip Statistics Database table names can be more than 30 Characters long. In Oracle database, due to a 30 character limitation, the table name may be truncated. Cisco UCS central handles this automatically.

Aggregation on real time records

The statistics collection policy determines the interval for the data from registered Cisco UCS domains. The data received from the registered Cisco UCS domains is stored in the database and aggregated as hourly, daily and weekly records. This aggregation based on real time records is defined by the statistics collection interval. Each of these record types have a specific ID or a unique identifier in the database. The following table lists the identifiers for each record type.

Record Type	ID
Real Time	0
Hourly	1
Daily	2
Weekly	3

If the statistics collection policy is set to 15 minutes, then for every 4 real time records, 1 hourly record is created and stored in the database. The daily and weekly record aggregation is internally defined, and is not determined by the collection interval. Every 24 hours, one daily record is created and stored in the database. Similarly, for every 7 days, one weekly record is created and stored in the database.

Parent to child aggregation

This type of data aggregation is based on the Distinguished Name (DN). A DN is a unique ID for every object that is defined in the database. The total bytes of data is collected and stored in the database tables from the child element to the parent element. For example, in a sample network, a domain has two fabric interconnects. Each fabric interconnect has slots and each of these slots has different ports. The statistics data for these ports is aggregated all the way to the domain level.

Connecting to an External Oracle Database

Before You Begin

- Set up an external Oracle database. The supported version is Oracle Database 11g Enterprise Edition Release 11.2.0.1.0 - 64-bit Production or higher. Note down the database server hostname, the database name, the user name and the password to access the database. You must have privileges to create tables in the database and to add, modify and delete records in those tables.
- You must open the firewall ports in the database server so that Cisco UCS Central can access the external database.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect stats-mgr**	Enters the statistics manager mode.
Step 2	UCSC (stats-mgr) # **scope db-configuration**	Enters database configuration mode.
Step 3	UCSC (stats-mgr) /db-configuration # **set type** *dbtype*	Sets the database type, in this case Oracle.
Step 4	UCSC (stats-mgr) db-configuration # **set hostname** *hostname*	Sets the hostname.
Step 5	UCSC (stats-mgr) /db-configuration # **set port** *port-number*	Sets the port. The default Oracle port is 1521.
Step 6	UCSC (stats-mgr) /db-configuration # **set database** *dbname*	Sets the database name.
Step 7	UCSC (stats-mgr) /db-configuration # **set user** *dbusername*	Sets the database user name.
Step 8	UCSC (stats-mgr) /db-configuration # **set pwd <enter_key>**	Sets the database password.
Step 9	UCSC (stats-mgr) /db-configuration # **commit-buffer**	Commits the transaction to the system configuration.

The following example sets up Cisco UCS Central to use an external Oracle database on the default port and commits the transaction:

```
UCSC # connect stats-mgr
UCSC (stats-mgr) # scope db-configuration
UCSC (stats-mgr) /db-configuration # set type oracle
UCSC (stats-mgr) /db-configuration # set hostname 10.10.10.10
UCSC (stats-mgr) /db-configuration # set port 1521
UCSC (stats-mgr) /db-configuration # set database DB1
UCSC (stats-mgr) /db-configuration # set user User1
UCSC (stats-mgr) /db-configuration # set pwd <enter_key>
Password:
UCSC (stats-mgr) /db-configuration # commit-buffer
```

What to Do Next

You can change the statistics collection interval from the default 15 minutes to 30 minutes. This is optional.

Connecting to an External PostgreSQL Database

Before You Begin

- Set up an external PostgreSQL database. The supported version is PostgreSQL (9.2.3) or higher. Note down the database server hostname, the database name, the user name and the password to access the database. You must have privileges to create tables in the database and to add, modify and delete records in those tables.
- The name of the database should not include the **postgres** phrase.
- You must open the firewall ports in the database server so that Cisco UCS Central can access the external database.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect stats-mgr**	Enters the statistics manager mode.
Step 2	UCSC (stats-mgr) # **scope db-configuration**	Enters database configuration mode.
Step 3	UCSC (stats-mgr) /db-configuration # **set type** *dbtype*	Sets the database type, in this case postgreSQL.
Step 4	UCSC (stats-mgr) /db-configuration # **set hostname** *hostname*	Sets the hostname.
Step 5	UCSC (stats-mgr) /db-configuration # **set port** *port-number*	Sets the port. The default port is 5432.
Step 6	UCSC (stats-mgr) /db-configuration # **set database** *dbname*	Sets the database name.
Step 7	UCSC (stats-mgr) /db-configuration # **set user** *dbusername*	Sets the database user name.
Step 8	UCSC (stats-mgr) /db-configuration # **set pwd <enter_key>**	Sets the database password.
Step 9	UCSC (stats-mgr) /db-configuration # **commit-buffer**	Commits the transaction to the system configuration.

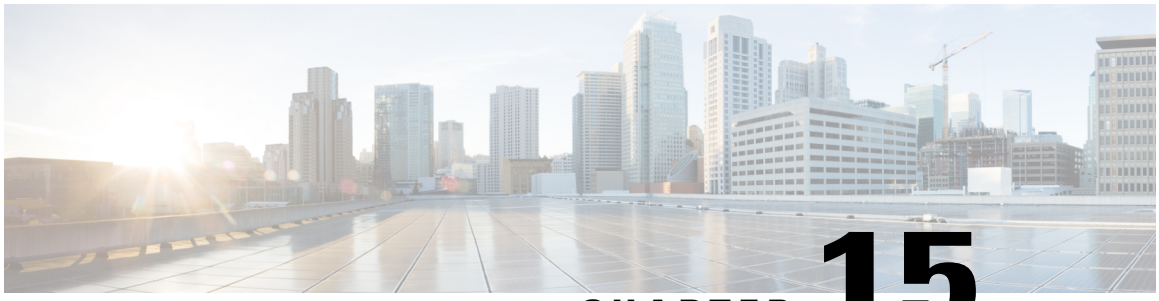
The following example sets up Cisco UCS Central to use an external postgreSQL database on the default port and commits the transaction:

```
UCSC # connect stats-mgr
UCSC (stats-mgr) # scope db-configuration
UCSC (stats-mgr) /db-configuration # set type postgres
UCSC (stats-mgr) /db-configuration # set hostname 10.10.10.10
UCSC (stats-mgr) /db-configuration # set port 5432
```

```
UCSC (stats-mgr) /db-configuration # set database DB1
UCSC (stats-mgr) /db-configuration # set user User1
UCSC (stats-mgr) /db-configuration # set pwd <enter_key>
Password
UCSC (stats-mgr) /db-configuration # commit-buffer
```

What to Do Next

You can change the statistics collection interval from the default 15 minutes to 30 minutes. This is optional.



CHAPTER 15

System Management

This chapter includes the following sections:

Configuring DNS Servers

Managing DNS Policies

Cisco UCS Central supports global DNS policies defining the DNS server and domain name. Registered Cisco UCS domains choosing to define DNS management globally within that domain's policy resolution control will defer DNS management to its registration with Cisco UCS Central.

Configuring a DNS Policy

Before You Begin

Before configuring a DNS policy in a domain group under the Domain Group root, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope dns-config**	(Optional) If scoping into the domain group root previously, scopes the default DNS policy's configuration mode from the Domain Group root.
Step 4	UCSC(policy-mgr) /domain-group # **create dns-config**	(Optional) If scoping into a domain group previously, creates the DNS policy for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **set domain-name** *server-domain-name*	Defines the DNS domain name.
Step 6	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root (which has an existing DNS policy by default), define the DNS domain name as dnsdomain, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # set domain-name dnsdomain
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to scope into the domain group domaingroup01, create the DNS policy for that domain group, define the DNS domain name as dnsdomain, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create dns-config
UCSC(policy-mgr) /domain-group/domain-group* # set domain-name dnsdomain
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Deleting a DNS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default DNS policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete dns-config**	Deletes the DNS policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the DNS policy for that domain group, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group/domain-group # delete dns-config
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Configuring a DNS Server for a DNS Policy

Before You Begin

Configure a DNS policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope dns-config**	Enter an existing DNS policy's configuration mode from the Domain Group root or a domain group scoped into.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/dns-config # **create dns** server-IP-address	Creates a DNS server instance.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, create a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # create dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to scope into the domain group domaingroup01, create a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # create dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Deleting a DNS Server from a DNS Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope dns-config**	Enter an existing DNS policy's configuration mode from the Domain Group root or a domain group scoped into.
Step 4	UCSC(policy-mgr) /domain-group/dns-config # **delete dns** *server-IP-address*	Deletes a DNS server instance.
Step 5	UCSC(policy-mgr) /domain-group/dns-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, delete a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # delete dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

The following example shows how to scope into the domain group domaingroup01, delete a DNS server instance named 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope dns-config
UCSC(policy-mgr) /domain-group/domain-group # delete dns 0.0.0.0
UCSC(policy-mgr) /domain-group/domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group/domain-group #
```

Managing Power Allocation

Creating a Global Power Allocation Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create cap-policy**	Creates global power allocation policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create a global power allocation policy for a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # create cap-policy
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Deleting a Global Power Allocation Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete cap-policy**	Deletes global power allocation policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to delete a global power allocation policy for a domain group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # delete cap-policy
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Configuring a Global Power Allocation Policy for a Chassis Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope cap-policy**	Enters the global power allocation mode.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy # **set cap-policy policy-driven-chassis-group-cap**	Specifies global power allocation policy for chassis group in the domain group.
Step 5	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure a global power allocation policy for a chassis group:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope cap-policy
UCSC(policy-mgr) /domain-group/cap-policy # set cap-policy policy-driven-chassis-group-cap

UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Configuring a Global Power Allocation Policy Manually for a Blade Server

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope cap-policy**	Enters the global power allocation mode.
Step 4	UCSC(policy-mgr) /domain-group/cap-policy # **set cap-policy manual-blade-level-cap**	Enables manual blade server level power allocation.
Step 5	UCSC(policy-mgr) /domain-group/cap-policy* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to configure manual power allocation policy for a blade server:

```
UCSC# connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope cap-policy
UCSC(policy-mgr) /domain-group/cap-policy # set cap-policy manual-blade-level-cap
UCSC(policy-mgr) /domain-group/cap-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/cap-policy #
```

Managing Power Policies

Cisco UCS Central supports global equipment policies defining the global power allocation policy (based on policy driven chassis group cap or manual blade level cap methods), power policy (based on grid, n+1 or non-redundant methods). Registered Cisco UCS domains choosing to define power management and power supply units globally within that client's policy resolution control will defer power management and power supply units to its registration with Cisco UCS Central.

Creating an Equipment Power Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create psu-policy**	Creates the power policy from the domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

The following example shows how to create an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # create psu-policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an Equipment Power Policy

Procedure

Step 1 UCSC# **connect policy-mgr**
Enters policy manager mode.

Step 2 UCSC(policy-mgr) # **scope domain-group** *domain-group*
Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

Step 3 UCSC(policy-mgr) /domain-group # **delete psu-policy**
Deletes the power policy from the domain group.

Step 4 UCSC(policy-mgr) /domain-group* # **commit-buffer**
Commits the transaction to the system.

The following example shows how to delete an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # delete psu-policy
```

```
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring an Equipment Power Policy

Before You Begin

Before configuring a power equipment policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope psu-policy**	Enters the power policy mode.
Step 4	UCSC(policy-mgr) /domain-group # **set** descr *power-policy-description-text*	Specifies the description for the power policy.
Step 5	UCSC(policy-mgr) /domain-group # **set redundancy grid** | **n-plus-1** | **non-redund**	Specifies the redundancy for the power policy for Grid (grid), N-Plus-1 (n-plus-1), or non-redundancy (non-redund).

The following example scopes the domain group dg1 and configures the equipment power policy for that domain group:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group/psu-policy # set descr "Power policy for sector 24"
UCSC(policy-mgr) /domain-group/psu-policy* # set redundancy grid
UCSC(policy-mgr) /domain-group/psu-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/psu-policy #
```

Viewing an Equipment Power Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root.

	Command or Action	Purpose
		To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **show psu-policy**	Enters the power policy mode.

The following example shows how to create an equipment power policy:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group dg1
UCSC(policy-mgr) /domain-group # scope psu-policy
UCSC(policy-mgr) /domain-group/psu-policy # show
PSU Policy:
    Domain Group Redundancy Description
    ------------ ---------- -----------
    root/dg1     NPlus1
UCSC(policy-mgr) /domain-group #
```

Managing Time Zones

Managing Time Zones

Cisco UCS Central supports global date and time policies based on international time zones and defined NTP server. Registered Cisco UCS Manager clients choosing to define date and time globally within that client's policy resolution control will defer the configuration for date and time to its registration with Cisco UCS Central.

Configuring a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create domain-group** *domain-group*	(Optional) This step is only necessary to create a new domain group under the Domain Group root (or creates a domain group under the domain group scoped into).
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	(Optional) This step is only necessary after creating a new domain group under the Domain Group root (or creating a domain group

	Command or Action	Purpose
		under the domain group scoped into). Commits the new domain group to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group # **create timezone-ntp-config**	(Optional) This step is only necessary the first time a date and time policy is configured for the newly created domain group under the Domain Group root that was created in the previous step, then enter the time zone NTP configuration mode. A date and time policy was created by the system for the Domain Group root, and is ready to be configured.
Step 6	UCSC(policy-mgr) /domain-group* # **scope timezone-ntp-config**	(Optional) This step is only necessary if entering an existing date and time policy's time zone NTP configuration mode from the Domain Group root or a domain group scoped into. Skip this step if creating a date and time policy.
Step 7	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **set timezone**	To set the time zone, press **Enter** after typing the set timezone command and enter the key value at the prompt. Configures the NTP server time zone. The attribute options are as follows: • **1 —**Africa • **2 —**Americas • **3 —**Antarctica • **4 —**Arctic Ocean • **5 —**Asia • **6 —**Atlantic Ocean • **7 —**Australia • **8 —**Europe • **9 —**India Ocean • **10 —**Pacific Ocean
Step 8	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope the Domain Group root, configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country"), and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # set timezone
Please identify a location so that time zone rules can be set correctly.
```

```
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to create a new domain group called domaingroup01 under the Domain Group root, commit the transaction, create a date and time policy, configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country"), and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create domain-group domaingroup01
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group # create timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # set timezone
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope to domaingroup01 under the Domain Group root, create a date and time policy, configure the time zone setting to India Ocean ("a continent or ocean") and Maldives ("a country"), and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr) /domain-group # scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # set timezone
Please identify a location so that time zone rules can be set correctly.
```

```
Please select a continent or ocean.
1) Africa            4) Arctic Ocean     7) Australia       10) Pacific Ocean
2) Americas          5) Asia             8) Europe
3) Antarctica        6) Atlantic Ocean   9) Indian Ocean
#? 9
Please select a country.
1) British Indian Ocean Territory       7) Maldives
2) Christmas Island                     8) Mauritius
3) Cocos (Keeling) Islands              9) Mayotte
4) Comoros                             10) Reunion
5) French Southern & Antarctic Lands   11) Seychelles
6) Madagascar
#? 7
The following information has been given:
        Maldives
Therefore timezone 'Indian/Maldives' will be set.
Local time is now:      Thu Oct 25 01:58:03 MVT 2012.
Universal Time is now:  Wed Oct 24 20:58:03 UTC 2012.
Is the above information OK?
1) Yes
2) No
#? 1
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

What to Do Next

Configure an NTP server for a date and time policy.

Deleting a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default date and time policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete timezone-ntp-config**	Deletes the domain group's time zone policy.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope the domain group domaingroup01, delete that domain group's date and time policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete timezone-ntp-config
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

The following example shows how to scope the domain group root, attempt to delete that domain group's date and time policy, commit the transaction and recover from an error message (leaving the buffer in an unrecoverable uncommitted state) by initiating a clean exit and reconnecting to Policy Manager to clear the buffer:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # delete timezone-ntp-config
UCSC(policy-mgr) /domain-group* # commit-buffer
Error: Update failed:
[Timezone and NTP configuration under domain group root cannot be deleted]
UCSC(policy-mgr) /domain-group* # exit
UCSC(policy-mgr)* # exit
UCSC# connect policy-mgr
Cisco UCS Central
UCSC(policy-mgr)#
```

Note In the event you mistakenly scope to the domain group root, and enter the command delete timezone-ntp-config, the buffer will encounter an unrecoverable error, remaining in an uncommitted state and preventing subsequent commit-buffer commands from saving to the buffer. You must immediately exit and reconnect to the Policy Manager to clear the buffer.

Configuring an NTP Server for a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **create ntp** server-name	Creates an NTP server instance.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, create an NTP server instance named domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # create ntp domaingroupNTP01
```

```
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope to the domain group domaingroup01 under the domain group root, create an NTP server instance named domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # create ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

What to Do Next

Configure a date and time policy.

Configuring Properties for an NTP Server

The properties of an NTP server consist of its name. Changing those properties, unlike steps in the GUI involving configuring the NTP server's properties, requires deleting that NTP server and recreating it with a new name.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **delete ntp** server-name	Deletes an NTP server instance that requires renaming.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **create ntp** server-name	Creates an NTP server instance to replace the deleted NTP server instance.
Step 6	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group root, delete an NTP server instance named domaingroupNTP01 with a name that is no longer relevant, create a new NTP server instance named domaingroupNTP02 to replace the deleted NTP server, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
```

```
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # create ntp domaingroupNTP02
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope to the domain group domaingroup01 under the domain group root, delete an NTP server instance named domaingroupNTP01 with a name that is no longer relevant, create a new NTP server instance named domaingroupNTP02 to replace the deleted NTP server, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # create ntp domaingroupNTP02
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

Deleting an NTP Server for a Date and Time Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope timezone-ntp-config**	Enters time zone NTP configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/timezone-ntp-config # **delete ntp** server-name	Deletes an NTP server instance.
Step 5	UCSC(policy-mgr) /domain-group/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope the date and time policy in the domain group root, delete the NTP server instance domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

The following example shows how to scope the date and time policy in domaingroup01 under the domain group root, delete the NTP server instance domaingroupNTP01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope timezone-ntp-config
```

```
UCSC(policy-mgr) /domain-group/timezone-ntp-config # delete ntp domaingroupNTP01
UCSC(policy-mgr) /domain-group/timezone-ntp-config* # commit-buffer
UCSC(policy-mgr) /domain-group/timezone-ntp-config #
```

Configuring SNMP

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 5: SNMP Security Models and Levels

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

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.

Authentication Protocols for SNMPv3 Users

Cisco UCS Central supports the following authentication protocols for SNMPv3 users:

- HMAC-MD5-96 (MD5)

- HMAC-SHA-96 (SHA)

AES Privacy Protocol for SNMPv3 Users

Cisco UCS Central uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826. If AES is disabled but privacy password is set, then DES is used for encryption.

If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS Central uses the privacy password to generate a 128-bit AES key. The AES privacy password can have a minimum of eight characters. If the passphrases are specified in clear text, you can specify a maximum of 64 characters.

Configuring an SNMP Policy

Before You Begin

Before configuring a SNMP policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create snmp**	(Optional) If scoping into a domain group previously, creates the SNMP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope snmp**	(Optional) If scoping into the domain group root previously, scopes the default SNMP policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **enable** | **disable snmp**	Enable or disable SNMP services for this policy.
Step 6	UCSC(policy-mgr) /domain-group/snmp* # **set community** *snmp-community-name-text*	Enter a name for the SNMP community.
Step 7	UCSC(policy-mgr) /domain-group/snmp* # **set syscontact** *syscontact-name-text*	Enter a name for the SNMP system contact.
Step 8	UCSC(policy-mgr) /domain-group/snmp* # **set syslocation** *syslocation-name-text*	Enter a name for the SNMP system location.
Step 9	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, enable SNMP services, set the SNMP community name to SNMPCommunity01, set the SNMP system contact name to SNMPSysAdmin01, set the SNMP system location to SNMPWestCoast01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the Domain Group domaingroup01, create the SNMP policy, enable SNMP services, set the SNMP community name to SNMPCommunity01, set the SNMP system contact name to SNMPSysAdmin01, set the SNMP system location to SNMPWestCoast01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create snmp
UCSC(policy-mgr) /domain-group/snmp* # enable snmp
UCSC(policy-mgr) /domain-group/snmp* # set community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, disable SNMP services, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # disable snmp
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

Configuring an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the default SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **create snmp-trap** *snmp-trap-ip*	(Optional) If scoping into a domain group previously, creates the snmp-trap IP address for that domain group (in

	Command or Action	Purpose
		format 0.0.0.0), and enters SNMP trap configuration mode.
Step 5	UCSC(policy-mgr) /domain-group/snmp # **scope snmp-trap** *snmp-trap-ip*	(Optional) If scoping into the domain group root previously, scopes the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 6	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set community** *snmp-trap-community-host-config-string*	Enter the SNMP trap community string to configure the SNMP trap host.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set notificationtype traps**	Enter the notification type for the SNMP trap as SNMP Trap Notifications (traps).
Step 8	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set port** *port-number*	Enter the SNMP trap port number (1-65535).
Step 9	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set v3privilege auth** | **noauth** | **priv**	Enter a V3 Privilege security level for the SNMP trap of authNoPriv Security Level (auth), noAuthNoPriv Security Level (noauth), or authPriv Security Level (priv).
Step 10	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **set version v1** | **v2c** | **v3**	Enter a version for the SNMP trap of SNMP v1, v2c, or v3.
Step 11	UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, create the SNMP trap with IP address 0.0.0.0, set the SNMP community host string to snmptrap01, set the SNMP notification type to traps, set the SNMP port to 1, set the v3privilege to priv, set the version to v1, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap01
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege priv
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v1
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, scope the SNMP trap IP address 0.0.0.0, set the SNMP community host string to snmptrap02, set the SNMP

notification type to traps, set the SNMP port to 65535, set the v3privilege to auth, set the version to v2c, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set community snmptrap02
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set notificationtype traps
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set port 65535
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set v3privilege auth
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # set version v2c
UCSC(policy-mgr) /domain-group/snmp/snmp-trap* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-trap #
```

Configuring an SNMP User

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **create snmp-user** *snmp-user*	Enter a name for the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set aes-128 yes** | **no**	Use AES-128 for the SNMP user (yes or no).
Step 6	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set auth md5** | **sha**	Use MD5 or Sha authorization mode for the SNMP user.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set password** *password*	Enter and confirm a password for the SNMP user.
Step 8	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set priv-password** *private-password*	Enter and confirm a private password for the SNMP user.
Step 9	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, scope into the SNMP user named snmpuser01, set aes-128 mode to enabled, set authorization to sha mode, set password to userpassword01, set private password to userpassword02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth sha
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, create the SNMP user named snmpuser01, set aes-128 mode to enabled, set authorization to md5 mode, set password to userpassword01, set private password to userpassword02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # create snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set aes-128 yes
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set password userpassword01
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set priv-password userpassword02
Enter a password: userpassword02
Confirm the password: userpassword02
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

The following example shows how to scope into the Domain Group root, scope the SNMP policy, scope into the SNMP user named snmpuser01, set aes-128 mode to disabled, set authorization to md5 mode, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # scope snmp-user snmpuser01
UCSC(policy-mgr) /domain-group/snmp/snmp-user # set aes-128 no
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # set auth md5
UCSC(policy-mgr) /domain-group/snmp/snmp-user* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp/snmp-user #
```

Deleting an SNMP Policy

A SNMP policy is deleted from a domain group under the domain group root. SNMP policies under the domain groups root cannot be deleted.

Deleting an SNMP policy will remove all SNMP trap and SNMP User settings within that policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root itself. System default Management Interfaces Monitoring policies cannot be deleted under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete snmp**	Deletes the SNMP policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the SNMP policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete snmp
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an SNMP Trap

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the default SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **delete snmp-trap** *snmp-trap-ip*	Deletes the snmp-trap IP address for that domain group.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, delete the SNMP trap IP address 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

The following example shows how to scope into the domain group domaingroup01, scope the SNMP policy, delete the SNMP trap IP address 0.0.0.0, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp-trap 0.0.0.0
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting an SNMP User

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope snmp**	Scopes the SNMP policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/snmp # **delete snmp-user** *snmp-user*	Delete the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group root, scope the SNMP policy, delete the SNMP user named snmpuser01, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example shows how to scope into the Domain Group domaingroup01, scope the SNMP policy, delete the SNMP user named snmpuser02, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope snmp
UCSC(policy-mgr) /domain-group/snmp # delete snmp snmpuser02
```

```
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

Managing High Availability

About High Availability in Cisco UCS Central

Cisco UCS Central provides high availability in a cluster setup when you deploy Cisco UCS Central in two virtual nodes. High availability provides stability and redundancy directly to your Cisco UCS Central and indirectly to your Cisco UCS Domains management. The high availability in Cisco UCS Central provides you the following:

- Simplified large scale Cisco UCS deployments with an increased number of servers, chassis, fabric interconnects, and data centers.
- UCS Central VM redundancy in a Hypervisor independent environment.
- A shared storage device to house database and image repositories.
- Built-in failure detection (DME, VM, host, or network failures) and automatic failover to ensure continuous operation.

High Availability Architecture

You will deploy Cisco UCS Central in two VMs on separate hosts to enable high availability. High availability -

- Requires at least one Cisco UCS Manager be registered with Cisco UCS Central for a cluster to support high availability
- Uses the same subnet for individual VMs and VIP addresses
- Allows you to configure a mirrored, multi-path shared storage disk on each VM that is accessible from both hosts
- Uses UCS Manager to store quorum data and determine primary node.
- Exchanges information such as heartbeat and election protocols in the same way as Cisco UCS Manager. This results in a simpler design, more code reusability, and easy to define failover conditions

Cautions and Guidelines for Using High Availability

The following are the guidelines to setup Cisco UCS Central in high availability:

- Make sure both VMs in the cluster should never be on the same server. Otherwise, a single host failure would end up bringing down the cluster.
- Each node in the cluster must have the following:
  - A primary NIC connected to the production network that is used for communicating with Cisco UCS Manager, and for heartbeat communications, with the peer node in the cluster.

- A host bus adapter connected to the Storage Area Network (SAN), that is used to access the storage target.

- **Separate network path for management and storage network**: Make sure the management network used communications between the two Cisco UCS Central nodes are not on the same network as the network that the nodes use to access the shared disk array. The primary heartbeat mechanism relies on exchanging datagrams across the management network. The secondary heartbeat mechanism uses quorum data on Cisco UCS Manager. When you use separate network paths for management and shared disk access, that provides redundant paths between the two nodes making it easier to distinguish node failures from link failures.

Note High availability is supported only in IPv4 addressing without the DHCP. You must configure the node IPs and cluster VIPs statically during the installation. These IP addresses are allocated from the production network over which the UCS Central cluster communicates with UCSMs.

- Both VMs must be configured on IP addresses that belongs to the same subnet.
- Make sure the cluster node infrastructure does not have a single point of failure. You can connect the cluster nodes my multiple, distinct networks. You can also construct the network with redundant switches and routers or similar hardware that removes single points of failure.
- For high availability Cisco UCS Central supports the most commonly used bus types, such as SAS , Fiber Channel (FC), and iSCSI. SCSI compatibility with Persistent Reservations (PRs) is recommended. LUN masking or zoning should be used to isolate the storage volumes accessed by the cluster from other hosts on the network.

Viewing the Cluster State

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show cluster state**	Displays the state of the cluster.

The following example shows how to view the state of a cluster:

```
UCSC# show cluster state

A: UP, PRIMARY
B: UP, SUBORDINATE

HA NOT READY
No device connected to this VM.
```

Viewing the Extended State of a Cluster

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show cluster extended-state** *cluster ID*	Displays the extended state of the cluster.

The following example shows how to view the extended state of a cluster:

```
UCSC# show cluster extended-state 0x2e95deacbd0f11e2-0x8ff35147e84f3de2

Start time: Thu May 16 06:54:22 2013
Last election time: Thu May 16 16:29:28 2013

A: UP, PRIMARY
B: UP, SUBORDINATE

A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP
   heartbeat state PRIMARY_OK

HA READY
Detailed state of the device selected for HA quorum data:
Device 1007, serial: a66b4c20-8692-11df-bd63-1b72ef3ac801, state: active
Device 1010, serial: 00e3e6d0-8693-11df-9e10-0f4428357744, state: active
Device 1012, serial: 1d8922c8-8693-11df-9133-89fa154e3fa1, state: active
```

Viewing a Network Interface

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show network-interface**	Displays the network interface information of a cluster.

The following example shows how to view information about the network interface:

```
UCSC# show network-interface
ID   OOB IP Addr     OOB Gateway     OOB Netmask
    ---- --------------- --------------- -----------
    A    10.106.189.54   10.106.189.1    255.255.255.0
    B    10.106.189.55   10.106.189.1    255.255.255.0
```

Viewing Detailed Information about a Network Interface

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show network-interface detail**	Displays the network interface details about a cluster.

The following example shows how to view the detailed network interface information about a cluster:

```
ucsc# show network-interface detail
VM IP interface:
ID: A
    OOB IP Addr: 10.106.189.54
    OOB Gateway:
    OOB Netmask: 255.255.255.0
    Current Task:

ID: B
    OOB IP Addr: 10.106.189.55
    OOB Gateway:
    OOB Netmask: 255.255.255.0
    Current Task:
```

Viewing Network Interface Information of a Server

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show network-interface** *server* [**a** | **b**]	Displays the network information about a server.

The following example shows how to view the network interface information for a server:

```
UCSC# show network-interfaceserver [ a | b]

ID       OOB IP Addr     OOB Gateway     OOB Netmask
    ---- --------------- --------------- -----------
    A    10.106.189.54   10.106.189.1    255.255.255.0
```

Viewing System Information about a Cluster

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show system**	Displays the system information about a cluster.

The following example shows how to view the system information about a cluster:

```
UCSC# show system
Systems:
    Hostname      Installation Type   System IP Address
     ----------------    ----------------------- ----------------------------
    central-vk2      Cluster                  10.106.189.56
central-lun-A#
```

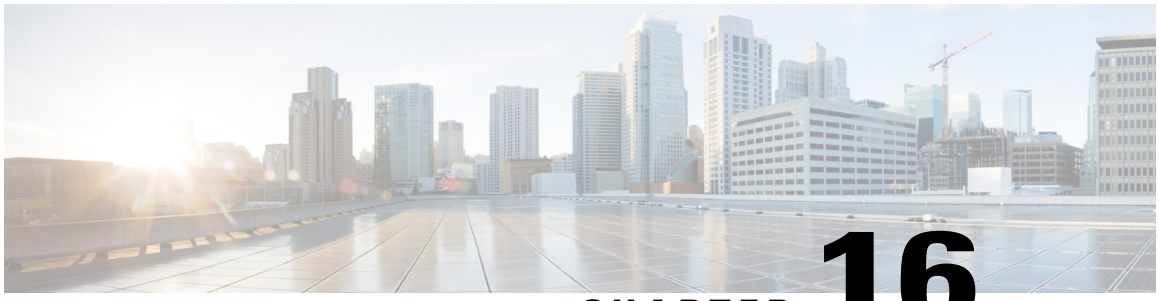
Viewing Detailed System Information about a Cluster

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show system detail**	Displays the system details about the cluster.

The following example shows how to view the system details about a cluster:

```
UCSC# show system detail
System:
    Hostname: central-lun
    Installation Type: Cluster
    System IP Address:
    Current Task:
central-lun-A#
```



CHAPTER 16

Monitoring Logs

This chapter includes the following sections:

System Event Log

System Event Log

Cisco UCS Central supports a global system event log (SEL) policy.

System Event Log

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

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

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

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

Tip For more information about the SEL, including how to view the SEL for each server and configure the SEL policy, see the Cisco UCS Manager configuration guides, which are accessible through the Cisco UCS B-Series Servers Documentation Roadmap.

Configuring the SEL Policy

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope ep-log-policy sel**	Enters organization endpoint log policy mode and scopes the SEL policy.
Step 4	UCSC(policy-mgr) /domain-group/ep-log-policy # **set description** *description*	(Optional) Provides a description for the policy. **Note** If your description includes spaces, special characters, or punctuation, you must begin and end your description with quotation marks. The quotation marks will not appear in the description field of any **show** command output.
Step 5	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup action** [**log-full**] [**on-change-of-association**] [**on-clear**] [**timer**] [**none**]	Specifies an action or actions that will trigger a backup operation.
Step 6	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup clear-on-backup** {**no** | **yes**}	Specifies whether to clear the system event log after a backup operation occurs.
Step 7	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup destination** *URL*	Specifies the protocol, user, password, remote hostname, and remote path for the backup operation. Depending on the protocol used, specify the URL using one of the following syntax: • **ftp://** *username@hostname* **/** *path* • **scp://** *username* **@** *hostname* **/** *path* • **sftp://** *username* **@** *hostname* **/** *path* • **tftp://** *hostname* **:** *port-num* **/** *path*

	Command or Action	Purpose
		Note You can also specify the backup destination by using the **set backup hostname** , **set backup password** , **set backup protocol** , **set backup remote-path** , **set backup user** commands, or by using the **set backup destination** command. Use either method to specify the backup destination.
Step 8	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup format** {*ascii* | *binary*}	Specifies the format for the backup file.
Step 9	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup hostname** {*hostname* | *ip-addr*}	Specifies the hostname or IP address of the remote server.
Step 10	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup interval** {**1-hour** | **2-hours** | **4-hours** | **8-hours** | **24-hours** | **never**}	Specifies the time interval for the automatic backup operation. Specifying the **never** keyword means that automatic backups will not be made.
Step 11	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup password** *password*	Specifies the password for the username. This step does not apply if the TFTP protocol is used.
Step 12	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 13	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup remote-path** *path*	Specifies the path on the remote server where the backup file is to be saved.
Step 14	UCSC(policy-mgr) /domain-group/ep-log-policy # **set backup user** *username*	Specifies the username the system should use to log in to the remote server. This step does not apply if the TFTP protocol is used.
Step 15	UCSC(policy-mgr) /domain-group/ep-log-policy # **commit-buffer**	Commits the transaction.

The following example shows how to configure the SEL policy to back up the system event log (in ascii format) every 24 hours or when the log is full and clear the system event log after a backup operation occurs and commit the transaction

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group #scope ep-log-policy sel
UCSC(policy-mgr) /domain-group/ep-log-policy # set backup destination
scp://user@192.168.1.10/logs
Password:
UCSC(policy-mgr) /domain-group/ep-log-policy* # set backup action log-full
UCSC(policy-mgr) /domain-group/ep-log-policy* #  set backup clear-on-backup yes
UCSC(policy-mgr) /domain-group/ep-log-policy* #  set backup format ascii
UCSC(policy-mgr) /domain-group/ep-log-policy* #  set backup interval 24-hours
```

```
UCSC(policy-mgr) /domain-group/ep-log-policy* #  commit-buffer
UCSC(policy-mgr) /domain-group/ep-log-policy #
```

Configuring Settings for Faults, Events and Logs

Configuring Global Fault Policies

Configuring a Global Fault Debug Policy

Before You Begin

Before configuring a global fault debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create fault policy**	(Optional) If scoping into a domain group previously, creates the fault policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group # **scope fault policy**	(Optional) If scoping into the domain group root previously, scopes the default fault policy's configuration mode from the Domain Group root.
Step 5	UCSC(policy-mgr) /domain-group/policy* # **set ackaction delete-on-clear**	Set the fault policy acknowledgment action to delete on clear (delete-on-clear) or reset to initial severity (reset-to-initial-severity).
Step 6	UCSC(policy-mgr) /domain-group/policy* # **set clearaction delete** | **retain**	Set the fault policy clear action to delete or retain.
Step 7	UCSC(policy-mgr) /domain-group/policy* # **set clearinterval** *clear-number-of-days* | **retain**	Set the fault policy clear interval to the number of days (0-3600) or retain.
Step 8	UCSC(policy-mgr) /domain-group/policy* # **set flapinterval** *flap-number-of-days*	Set the fault policy flap interval to the number of days (0-3600).
Step 9	UCSC(policy-mgr) /domain-group/policy* # **set retentioninterval** *retention-number-of-days* | **forever**	Set the fault policy clear interval to the number of days (0-3600) or forever.

	Command or Action	Purpose
Step 10	UCSC(policy-mgr) /domain-group/policy* # **set soakingseverity condition** | **info** | **warning**	Set the fault policy soaking severity to condition, info, or warning.
Step 11	UCSC(policy-mgr) /domain-group/policy* # **set soakinterval** *soak-number-of-days* | **never**	Set the fault policy soak interval to the number of days (0-3600) or never.
Step 12	UCSC(policy-mgr) /domain-group/policy* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create a global fault debug policy, enter the status settings, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create fault policy
UCSC(policy-mgr) /domain-group/policy* # set ackaction delete-on-clear
UCSC(policy-mgr) /domain-group/policy* # set clearaction delete
UCSC(policy-mgr) /domain-group/policy* # set clearinterval 90
UCSC(policy-mgr) /domain-group/policy* # set flapinterval 180
UCSC(policy-mgr) /domain-group/policy* # set retentioninterval 365
UCSC(policy-mgr) /domain-group/policy* # set soakingseverity info
UCSC(policy-mgr) /domain-group/policy* # set soakinterval warning
UCSC(policy-mgr) /domain-group/policy* # commit-buffer
UCSC(policy-mgr) /domain-group/policy #
```

Deleting a Global Fault Debug Policy

A global fault debug policy is deleted from a domain group under the domain group root. Global fault debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete fault policy**	Deletes the fault policy for that domain group.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the Domain Group domaingroup01, delete the global fault debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group# delete fault policy
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring TFTP Core Export Policies

Core File Exporter

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

Configuring a TFTP Core Export Debug Policy

Before You Begin

Before configuring a TFTP core export debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root were already created by the system and ready to configure.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope tftp-core-export-config**	(Optional) Scopes an existing TFTP Core Export Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group # **create tftp-core-export-config**	(Optional) Creates a TFTP Core Export Debug policy if it does not exist, then scopes into the policy.
Step 5	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **enable core-export-target**	Enables the TFTP core export target.
Step 6	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target path** *name-of-path*	Sets the TFTP core export policy target path.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target port** *port-number*	Sets the TFTP core export policy port number (1-65535).
Step 8	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target server-description** *port-number*	Sets the TFTP core export target policy server description. **Note** Do not use spaces in the server description unless the text is quoted (format examples: "Server description text" or Server_description_text).
Step 9	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **set core-export-target server-name** *server-name*	Sets the TFTP core export target policy server name.
Step 10	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the TFTP Core Export Policy, configure the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create tftp-core-export-config
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # enable core-export-target
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target path /target
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target port 65535
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target
server-description "TFTP core export server 2"
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # set core-export-target server-name
 TFTPcoreserver01
UCSC(policy-mgr) /domain-group/tftp-core-export-config* # commit-buffer
UCSC(policy-mgr) /domain-group/tftp-core-export-config #
```

Deleting a TFTP Core Export Debug Policy

A TFTP core export debug policy is deleted from a domain group under the domain group root. TFTP core export debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **delete tftp-core-export-config**	Deletes the TFTP Core Export Debug policy.
Step 4	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the TFTP core export debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete tftp-core-export-config
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring Syslog Policies

Configuring a Syslog Debug Policy

Before configuring a syslog debug policy under a domain group, this policy must first be created.

Before You Begin

Syslog Debug Policies under the Domain Group root were created by the system.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the Domain Group root.
Step 3	UCSC(policy-mgr) /domain-group # **create syslog**	Creates a Syslog Debug policy if it does not exist, then scopes into the policy.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the Syslog Console Debug Policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/remote-destination #
```

The Syslog Debug Policy is now ready to be configured.

What to Do Next

- Configuring a Syslog Console Debug Policy
- Configuring a Syslog Monitor Debug Policy
- Configuring a Syslog Remote Destination Debug Policy
- Configuring a Syslog Source Debug Policy
- Configuring a Syslog LogFile Debug Policy

Deleting a Syslog Debug Policy

A syslog debug policy is deleted from a domain group under the domain group root. Syslog debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete syslog**	Deletes the Syslog Debug policy.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, delete the Syslog Debug Policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # delete syslog
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring a Syslog Console Debug Policy

Before configuring a syslog console debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope console**	Creates or scopes the Syslog Console Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/console* # **enable**	Enables the Syslog Console Debug policy.
Step 6	UCSC(policy-mgr) /domain-group/syslog/console* # **set level 1** | **2** | **0**	Sets the syslog console to one of the following conditions: Alerts (1), Critical (2), or Emergencies (0).
Step 7	UCSC(policy-mgr) /domain-group/syslog/console* # **exit**	Moves back a level for the next create or scope command.
Step 8	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug policy, scope the Syslog Console Debug policy, configure the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog # scope console
UCSC(policy-mgr) /domain-group/syslog/console # enable
UCSC(policy-mgr) /domain-group/syslog/console* # set level 2
UCSC(policy-mgr) /domain-group/syslog/console* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/console #
```

Disabling a Syslog Console Debug Policy

A syslog console debug policy is disabled from a domain group under the Domain Group root. Syslog console debug policies under the Domain Group root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Scopes an existing Syslog Console Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope console**	Scopes the Syslog Console Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/console* # **disable**	Disables the Syslog Console Debug policy.
Step 6	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope into the Syslog Debug Policy, scope the Syslog Console Debug policy, disable the Syslog Console Debug Policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope console
UCSC(policy-mgr) /domain-group/syslog/console* # disable
UCSC(policy-mgr) /domain-group/syslog/console* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/console #
```

Configuring a Syslog Monitor Debug Policy

Before configuring a syslog monitor debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root.

	Command or Action	Purpose
		To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope monitor**	Creates or scopes the Syslog Monitor Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/monitor* # **enable**	Enables the syslog monitor.
Step 6	UCSC(policy-mgr) /domain-group/syslog/monitor* # **set level 1** | **2** | **3** | **4** | **5** | **6** | **7**	Sets the syslog monitor to one of the following conditions: Alerts (1), Cisco UCS domains Critical (2), Cisco UCS domains Major Error (3), Cisco UCS domains Minor Warnings (4), Cisco UCS domains Warning (5), Information (6), Debugging (7).
Step 7	UCSC(policy-mgr) /domain-group/syslog/monitor* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Monitor Debug Policy, configure the Syslog Monitor Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope monitor
UCSC(policy-mgr) /domain-group/syslog/monitor # enable
UCSC(policy-mgr) /domain-group/syslog/monitor* # set level 3
UCSC(policy-mgr) /domain-group/syslog/monitor* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/monitor #
```

Disabling a Syslog Monitor Debug Policy

A syslog monitor debug policy is disabled from a domain group under the Domain Group root. Syslog monitor debug policies under the Domain Group root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Scopes an existing Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope monitor**	Scopes the syslog Monitor Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/monitor* # **disable**	Disables the syslog monitor.
Step 6	UCSC(policy-mgr) /domain-group/syslog/monitor* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Monitor Debug policy, disable the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope monitor
UCSC(policy-mgr) /domain-group/syslog/monitor* # disable
UCSC(policy-mgr) /domain-group/syslog/monitor* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/monitor #
```

Configuring a Syslog Remote Destination Debug Policy

Before configuring a syslog remote destination debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope remote-destination** | **server-1** | **server-2** | **server-3**	Creates or scopes the Syslog Remote Destination Debug policy to server-1, server-2, or server-3.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **enable**	Enables the syslog remote destination.
Step 6	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **set facility auth** *hostname or level* | **authpriv** *hostname or level* | **cron** *hostname or level* | **daemon** *hostname or level* | **ftp** *hostname or level* | **kernel** *hostname or level* | **local[0-7]** *hostname or level* | **lpr** *hostname or level* | **mail** *hostname or level* | **news** *hostname or level* | **syslog** *hostname or level* | **user** *hostname or level* | **uucp** *hostname or level*	Sets the syslog remote destination facility to the following hostname or level configuration: • Auth • Authpriv • Cron • Daemon • FTP • Kernel • Local0 • Local1 • Local2 • Local3 • Local4 • Local5 • Local6 • Local7 • LPR • Mail • News • Syslog • User • UUCP **Note** • Level is Cisco UCS domains Critical (2), Cisco UCS domains Major Error (3), Cisco UCS domains Minor Warnings (4), Cisco UCS domains Warning (5), Information (6), Debugging (7). • Hostname is 0-255 characters.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Remote Destination Debug policy, configure the Syslog Remote Destination Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope remote-destination server-3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # enable
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility auth 4
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility auth authhost02
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility authpriv 3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility auth authprivhost02

  *** Continue configuring all facility settings as required ***
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/remote-destination #
```

Disabling a Syslog Remote Destination Debug Policy

A syslog remote destination debug policy is disabled in a domain group under the domain group root. Syslog remote destination debug policies under the domain groups root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Scopes an existing Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope remote-destination** | **server-1** | **server-2** | **server-3**	Creates or scopes the Syslog Remote Destination Debug policy to server-1, server-2, or server-3.
Step 5	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **disable**	Disables the syslog remote destination.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog Remote Destination Debug policy, disable the Syslog Remote Destination Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog* # scope remote-destination server-3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # disable
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/remote-destination #
```

Configuring a Syslog Source Debug Policy

Before configuring a syslog source debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope source**	Creates or scopes the Syslog Source Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/source* # **enable**	Enables the syslog source.
Step 6	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Console Debug Policy, scope the Syslog Source Debug policy, configure the Syslog Source Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope source
UCSC(policy-mgr) /domain-group/syslog/source* # enable
UCSC(policy-mgr) /domain-group/syslog/source* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/source #
```

Disabling a Syslog Source Debug Policy

A syslog source debug policy is deleted from a domain group under the domain group root. Syslog source debug policies under the domain groups root cannot be deleted.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group/syslog* # **scope source**	Scopes the Syslog Source Debug policy.
Step 4	UCSC(policy-mgr) /domain-group/syslog/source* # **disable**	Disables the Syslog Source Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/source* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the Syslog Console Debug Policy, scope the Syslog Source Debug policy, disable it, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog* # scope source
UCSC(policy-mgr) /domain-group/syslog/source* # disable
UCSC(policy-mgr) /domain-group/syslog/source* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/source #
```

Configuring a Syslog LogFile Debug Policy

Before configuring a syslog logfile debug policy under a domain group, this policy must first be created. Policies under the Domain Groups root that were already created by the system are ready to configure.

Before You Begin

Create a Syslog Debug Policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **create** | **scope file**	Creates or scopes the Syslog Logfile Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/file* # **enable**	Enables the syslog logfile.
Step 6	UCSC(policy-mgr) /domain-group/syslog/file* # **set level 1** | **2** | **3** | **4** | **5** | **6** | **7**	Sets the syslog file to one of the following conditions: Alerts (1), Cisco UCS domains Critical (2), Cisco UCS domains Major Error (3), Cisco UCS domains Minor Warnings (4), Cisco UCS domains Warning (5), Information (6), Debugging (7).
Step 7	UCSC(policy-mgr) /domain-group/syslog/file* # **set name** *syslog-file-name*	Sets the syslog file name.
Step 8	UCSC(policy-mgr) /domain-group/syslog/file* # **set size** *syslog-file-size*	Sets the syslog file size (4096-4194304 bytes).
Step 9	UCSC(policy-mgr) /domain-group/syslog/file* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, create the Syslog Debug Policy, scope the Syslog LogFile Debug policy, configure the Syslog Logfile Debug policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # create syslog
UCSC(policy-mgr) /domain-group/syslog* # create file
UCSC(policy-mgr) /domain-group/syslog/file* # enable
UCSC(policy-mgr) /domain-group/syslog/file* # set level 4
UCSC(policy-mgr) /domain-group/syslog/file* # set name syslogfilename01
UCSC(policy-mgr) /domain-group/syslog/file* # set size 4194304
UCSC(policy-mgr) /domain-group/syslog/file* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/file #
```

Disabling a Syslog LogFile Debug Policy

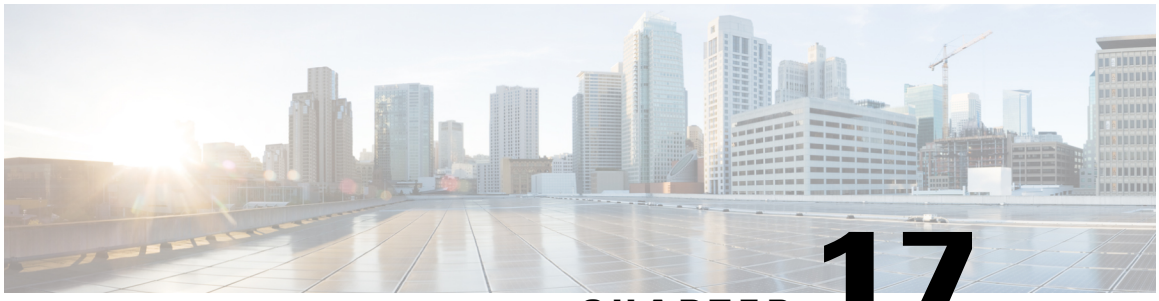
A syslog logfile debug policy is disabled from a domain group under the domain group root. Syslog logfile debug policies under the domain groups root cannot be disabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope syslog**	Creates or scopes a Syslog Debug policy's configuration mode.
Step 4	UCSC(policy-mgr) /domain-group/syslog* # **scope file**	Scopes the Syslog Logfile Debug policy.
Step 5	UCSC(policy-mgr) /domain-group/syslog/file* # **disable**	Disables or enables the syslog logfile.
Step 6	UCSC(policy-mgr) /domain-group/syslog/file* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to scope into the domain group domaingroup01, scope the Syslog Debug Policy, scope the Syslog LogFile Debug policy, disable the policy, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group domaingroup01
UCSC(policy-mgr) /domain-group # scope syslog
UCSC(policy-mgr) /domain-group/syslog* # scope file
UCSC(policy-mgr) /domain-group/syslog/file* # disable
UCSC(policy-mgr) /domain-group/syslog/file* # commit-buffer
UCSC(policy-mgr) /domain-group/syslog/file #
```



CHAPTER 17

User Management

This chapter includes the following sections:

Cisco UCS Central User Accounts

User accounts are used to access the system. Up to 128 user accounts can be configured in each Cisco UCS Central domain. Each user account must have a unique username and password.

A user account can be set with a SSH public key. The public key can be set in either of the two formats: OpenSSH and SECSH.

Admin Account

Cisco UCS Central has an admin account. The admin account is a default user account and cannot be modified or deleted. This account is the system administrator or superuser account and has full privileges. There is no default password assigned to the admin account; you must choose the password during the initial system setup.

The admin account is always active and does not expire. You cannot configure the admin account as inactive.

The local admin user is able to login for fail over, even when authentication is set to remote.

Locally Authenticated User Accounts

A locally authenticated user account is authenticated through the Cisco UCS Central user database, and can be enabled or disabled by anyone with admin or aaa privileges. Once a local user account is disabled, the user cannot log in. Configuration details for disabled local user accounts are not deleted by the database. If you re-enable a disabled local user account, the account becomes active again with the existing configuration, including username and password.

Remotely Authenticated User Accounts

A remotely authenticated user account is any Cisco UCS Central user account that is authenticated through LDAP. Cisco UCS domainssupport LDAP, RADIUS and TACACS+.

If a user maintains a local user account and a remote user account simultaneously, the roles defined in the local user account override those maintained in the remote user account.

Expiration of User Accounts

User accounts can be configured to expire at a predefined time. When the expiration time is reached, the user account is disabled.

By default, user accounts do not expire.

Note After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.

Guidelines for Creating Usernames

The username is also used as the login ID for Cisco UCS Central. When you assign login IDs to Cisco UCS Central user accounts, consider the following guidelines and restrictions:

- The login ID can contain between 1 and 32 characters, including the following:
  - Any alphabetic character
  - Any digit
  - _ (underscore)
  - - (dash)
  - . (dot)
- The login ID must be unique within Cisco UCS Central.
- The login ID must start with an alphabetic character. It cannot start with a number or a special character, such as an underscore.
- The login ID is case-sensitive.
- You cannot create an all-numeric login ID.
- After you create a user account, you cannot change the login ID. You must delete the user account and create a new one.

Reserved Words: Locally Authenticated User Accounts

The following words cannot be used when creating a local user account in Cisco UCS.

- root
- bin

- daemon
- adm
- lp
- sync
- shutdown
- halt
- news
- uucp
- operator
- games
- gopher
- nobody
- nscd
- mailnull
- mail
- rpcuser
- rpc
- mtsuser
- ftpuser
- ftp
- man
- sys
- samdme
- debug

Creating a Locally Authenticated User Account

At a minimum, we recommend that you create the following users:

- Server administrator account
- Network administrator account
- Storage administrator

Before You Begin

Perform the following tasks, if the system includes any of the following:

- Remote authentication services, ensure the users exist in the remote authentication server with the appropriate roles and privileges.
- Multi-tenancy with organizations, create one or more locales. If you do not have any locales, all users are created in root and are assigned roles and privileges in all organizations.
- SSH authentication, obtain the SSH key.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group /**	Enters domain group root mode.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **create local-user** *local-user-name*	Creates a user account for the specified local user and enters security local user mode.
Step 5	UCSC(policy-mgr) /domain-group/security/local-user* # **set account-status** {**active** | **inactive**}	Specifies whether the local user account is enabled or disabled. The admin user account is always set to active. It cannot be modified. **Note** If you set the account status to inactive, the configuration is not deleted from the database. The user is prevented from logging into the system using their existing credentials.
Step 6	UCSC(policy-mgr) /domain-group/security/local-user* # **set password** *password*	Sets the password for the user account
Step 7	UCSC(policy-mgr) /domain-group/security/local-user* # **set firstname** *first-name*	(Optional) Specifies the first name of the user.
Step 8	UCSC(policy-mgr) /domain-group/security/local-user* # **set lastname** *last-name*	(Optional) Specifies the last name of the user.
Step 9	UCSC(policy-mgr) /domain-group/security/local-user* # **set expiration** *month day-of-month year*	(Optional) Specifies the date that the user account expires. The *month* argument is the first three letters of the month name. **Note** After you configure a user account with an expiration date, you cannot reconfigure the account to not expire. You can, however, configure the account with the latest expiration date available.

	Command or Action	Purpose
Step 10	UCSC(policy-mgr) /domain-group/security/local-user* # **set email** *email-addr*	(Optional) Specifies the user e-mail address.
Step 11	UCSC(policy-mgr) /domain-group/security/local-user* # **set phone** *phone-num*	(Optional) Specifies the user phone number.
Step 12	UCSC(policy-mgr) /domain-group/security/local-user* # **set sshkey** *ssh-key*	(Optional) Specifies the SSH key used for passwordless access.
Step 13	UCSC(policy-mgr) /domain-group/security/local-user* # **commit-buffer**	Commits the transaction.

The following example shows how to create the user account named kikipopo, enable the user account, set the password to foo12345, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # create local-user kikipopo
UCSC(policy-mgr) /domain-group/security/local-user* # set account-status active
UCSC(policy-mgr) /domain-group/security/local-user* # set password
Enter a password:
Confirm the password:
UCSC(policy-mgr) /domain-group/security/local-user* # commit-buffer
UCSC(policy-mgr) /domain-group/security/local-user #
```

The following example shows how to create the user account named lincey, enable the user account, set an OpenSSH key for passwordless access, and commit the transaction.

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # create local-user lincey
UCSC(policy-mgr) /domain-group/security/local-user* # set account-status active
UCSC(policy-mgr) /domain-group/security/local-user* #  set sshkey "ssh-rsa AAAAB3NzaC1yc2EAAAA
BIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4
VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8="
UCSC(policy-mgr) /domain-group/security/local-user* # commit-buffer
UCSC(policy-mgr) /domain-group/security/local-user #
```

The following example shows how to create the user account named jforlenz, enable the user account, set a Secure SSH key for passwordless access, and commit the transaction.

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # create local-user jforlenz
UCSC(policy-mgr) /domain-group/security/local-user* # set account-status active
UCSC(policy-mgr) /domain-group/security/local-user* #  set sshkey
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
User's SSH key:
> ---- BEGIN SSH2 PUBLIC KEY ----
> AAAAB3NzaC1yc2EAAAABIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw8
> 5lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4VcOelBxlsGk5luq5ls1ob1VO
> IEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8=
> ---- END SSH2 PUBLIC KEY ----
```

```
> ENDOFBUF
UCSC(policy-mgr) /domain-group/security/local-user* # commit-buffer
UCSC(policy-mgr) /domain-group/security/local-user #
```

Deleting a Locally Authenticated User Account

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **delete local-user** *local-user-name*	Deletes the local-user account.
Step 5	UCSC(policy-mgr) /domain-group/security* # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the foo user account and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # delete local-user foo
UCSC(policy-mgr) /domain-group/security* # commit-buffer
UCSC(policy-mgr) /domain-group/security #
```

Enabling the Password Strength Check for Locally Authenticated Users

You must be a user with admin, aaa, or domain-group-management privileges to enable the password strength check. If the password strength check is enabled, Cisco UCS Central does not permit a user to choose a password that does not meet the guidelines for a strong password.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group /**	Enters domain group root mode.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/security # **scope password-profile**.	Specifies whether the password strength check is enabled or disabled.
Step 5	UCSC(policy-mgr) /domain-group/security/password-profile # **set enforce-strong-password** {**yes** | **no**}	Specifies whether the password strength check is enabled or disabled.

The following example enables the password strength check:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope password-profile
UCSC(policy-mgr) /domain-group/security/password-profile # set enforce-strong-password yes

UCSC(policy-mgr) /domain-group/security/password-profile #
```

Clearing the Password History for a Locally Authenticated User

You must have admin, aaa, or domain-group-management privileges to change the password profile properties.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope local-user** *local-user-name*	Commits the transaction.
Step 5	UCSC(policy-mgr) /domain-group/security/local-user # **scope password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /domain-group/security/password-profile # **set history-count** 0	Setting the **History Count** field to 0 (the default setting) disables the history count and allows users to reuse previously used passwords at any time.
Step 7	UCSC(policy-mgr) /domain-group/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to clear the password history count for the user account named kikipopo, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope local-user kikipopo
UCSC(policy-mgr) /domain-group/security/local-user # scope password-profile
UCSC(policy-mgr) /domain-group/security/password-profile # set history-count 0
UCSC(policy-mgr) /domain-group/security/password-profile* # commit-buffer
UCSC(policy-mgr) /domain-group/security/password-profile #
```

Enabling or Disabling a User Account

You must be a user with admin, aaa, or domain-group-management privileges to enable or disable a local user account.

Before You Begin

Create a local user account.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope local-user**	Enters local-user security mode.
Step 5	UCSC(policy-mgr) /domain-group/security/local-user # **set account-status** {**active** | **inactive**}	Specifies whether the local user account is enabled or disabled. The admin user account is always set to active. It cannot be modified. **Note** If you set the account status to inactive, the configuration is not deleted from the database. The user is prevented from logging into the system using their existing credentials.

The following example shows how to enable a local user account called accounting:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
```

```
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope local-user accounting
UCSC(policy-mgr) /domain-group/security/local-user # set account-status active
```

Web Session Limits for User Accounts

Cisco UCS Central does not support managing a number of concurrent web sessions at this time. We do support 32 concurrent web sessions for Cisco UCS Central users and a total of 256 concurrent sessions for all users.

Monitoring User Sessions

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope system**	Enters system mode.
Step 2	UCSC /system # **scope security**	Enters security mode.
Step 3	UCSC /security # **show user-sessions** {**local** | **remote**} [**detail**]	Displays session information for all users logged in to the system. An asterisk (*) next to the session ID denotes the current login session.

The following example lists all local users logged in to the system. The asterisk indicates which session is the current login session.

```
UCSC# scope system
UCSC /system # scope security
UCSC /security # show user-sessions local
Session Id      User            Host                Login Time
--------------- --------------- ------------------- ----------
pts_25_1_31264* steve           192.168.100.111     2012-05-09T14:06:59.000
ttyS0_1_3532    jeff            console             2012-05-02T15:11:08.000
web_25277_A     faye            192.168.100.112     2012-05-15T22:11:25.000
```

The following example displays detailed information on all local users logged in to the system:

```
UCSC# scope system
UCSC /system # scope security
UCSC /security # show user-sessions local detail
Session Id pts_25_1_31264:
    Fabric Id: A
    Term: pts/25
    User: steve
    Host: 64.101.53.93
    Pid: 31264
    Login Time: 2012-05-09T14:06:59.000

Session Id ttyS0_1_3532:
    Fabric Id: A
    Term: ttyS0
    User: jeff
    Host: console
    Pid: 3532
    Login Time: 2012-05-02T15:11:08.000

Session Id web_25277_A:
```

```
Fabric Id: A
Term: web_25277
User: faye
Host: 192.168.100.112
Pid: 3518
Login Time: 2012-05-15T22:11:25.000
```

Configuring Passwords

Guidelines for Creating Passwords

Each locally authenticated user account requires a password. A user with admin, aaa, or domain-group-management privileges can configure Cisco UCS Central to perform a password strength check on user passwords. If the password strength check is enabled, each user must have a strong password.

Cisco recommends that each user have a strong password. If you enable the password strength check for locally authenticated users, Cisco UCS Central rejects any password that does not meet the following requirements:

- Must contain a minimum of 8 characters and a maximum of 80 characters.
- Must contain at least three of the following:
  - Lower case letters
  - Upper case letters
  - Digits
  - Special characters
- Must not contain a character that is repeated more than 3 times consecutively, such as aaabbb.
- Must not be identical to the username or the reverse of the username.
- Must pass a password dictionary check. For example, the password must not be based on a standard dictionary word.
- Must not contain the following symbols: $ (dollar sign), ? (question mark), and = (equals sign).
- Should not be blank for local user and admin accounts.

Password Profile for Locally Authenticated Users

The password profile contains the password history and password change interval properties for all locally authenticated users of Cisco UCS Central. You cannot specify a different password profile for each locally authenticated user.

Note You must have admin, aaa, or domain-group-management privileges to change the password profile properties. Except for password history, these properties do not apply to users with these administrative privileges.

Password History Count

The password history count allows you to prevent locally authenticated users from reusing the same password over and over again. When this property is configured, Cisco UCS Central stores passwords that were previously used by locally authenticated users up to a maximum of 15 passwords. The passwords are stored in reverse chronological order with the most recent password first to ensure that the only the oldest password can be reused when the history count threshold is reached.

A user must create and use the number of passwords configured in the password history count before being able to reuse one. For example, if you set the password history count to 8, a locally authenticated user cannot reuse the first password until after the ninth password has expired.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously passwords at any time.

If necessary, you can clear the password history count for a locally authenticated user and enable reuse of previous passwords.

Password Change Interval

The password change interval enables you to restrict the number of password changes a locally authenticated user can make within a given number of hours. The following table describes the two configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	This option does not allow passwords for locally authenticated users to be changed within a specified number of hours after a password change. You can specify a no change interval between 1 and 745 hours. By default, the no change interval is 24 hours.	For example, to prevent passwords from being changed within 48 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to disable • No change interval to 48
Password changes allowed within change interval	This option specifies the maximum number of times that passwords for locally authenticated users can be changed within a pre-defined interval. You can specify a change interval between 1 and 745 hours and a maximum number of password changes between 0 and 10. By default, a locally authenticated user is permitted a maximum of 2 password changes within a 48 hour interval.	For example, to allow to be changed a maximum of once within 24 hours after a locally authenticated user changes his or her password, set the following: • Change during interval to enable • Change count to 1 • Change interval to 24

Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin, aaa, or domain-group-management privileges to change the password profile properties. Except for password history, these properties do not apply to users with these administrative privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope password-profile**	Enters password profile security mode.
Step 5	UCSC(policy-mgr) /domain-group/security/password-profile # **set change-during-interval enable**	Restricts the number of password changes a locally authenticated user can make within a given number of hours.
Step 6	UCSC(policy-mgr) /domain-group/security/password-profile* # **set change-count** *pass-change-num*	Specifies the maximum number of times a locally authenticated user can change his or her password during the Change Interval. This value can be anywhere from 0 to 10.
Step 7	UCSC(policy-mgr) /domain-group/security/password-profile* # **set change-interval** *num-of-hours*	Specifies the maximum number of hours over which the number of password changes specified in the **Change Count** field are enforced. This value can be anywhere from 1 to 745 hours. For example, if this field is set to 48 and the**Change Count** field is set to 2, a locally authenticated user can make no more than 2 password changes within a 48 hour period.
Step 8	UCSC(policy-mgr) /domain-group/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to enable the change during interval option, set the change count to 5, set the change interval to 72 hours, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope password-profile
UCSC(policy-mgr) /domain-group/security/password-profile # set change-during-interval enable
UCSC(policy-mgr) /domain-group/security/password-profile* # set change-count 5
UCSC(policy-mgr) /domain-group/security/password-profile* # set change-interval 72
UCSC(policy-mgr) /domain-group/security/password-profile* # commit-buffer
UCSC(policy-mgr) /domain-group/security/password-profile #
```

Configuring a No Change Interval for Passwords

You must have admin, aaa, or domain-group-management privileges to change the password profile properties. Except for password history, these properties do not apply to users with these administrative privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope password-profile**	Enters password profile security mode.
Step 5	UCSC(policy-mgr) /domain-group/security/password-profile # **set change-during-interval disable**	Disables the change during interval feature.
Step 6	UCSC(policy-mgr) /domain-group/security/password-profile* # **set no-change-interval** *min-num-hours*	Specifies the minimum number of hours that a locally authenticated user must wait before changing a newly created password.. This value can be anywhere from 1 to 745 hours. This interval is ignored if the **Change During Interval** property is not set to **Disable**.
Step 7	UCSC(policy-mgr) /domain-group/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to disable the change during interval option, set the no change interval to 72 hours, and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope password-profile
UCSC(policy-mgr) /domain-group/security/password-profile # set change-during-interval disable
UCSC(policy-mgr) /domain-group/security/password-profile* # set no-change-interval 72
UCSC(policy-mgr) /domain-group/security/password-profile* # commit-buffer
UCSC(policy-mgr) /domain-group/security/password-profile #
```

Configuring the Password History Count

You must have admin or aaa privileges to change the password profile properties.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope password-profile**	Enters password profile security mode.
Step 5	UCSC(policy-mgr) /domain-group/security/password-profile # **set history-count** *num-of-passwords*	Specifies the number of unique passwords that a locally authenticated user must create before that user can reuse a previously used password This value can be anywhere from 0 to 15. By default, the **History Count** field is set to 0, which disables the history count and allows users to reuse previously used passwords at any time.
Step 6	UCSC(policy-mgr) /domain-group/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

The following example configures the password history count and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope password-profile
UCSC(policy-mgr) /domain-group/security/password-profile # set history-count 5
UCSC(policy-mgr) /domain-group/security/password-profile* # commit-buffer
UCSC(policy-mgr) /domain-group/security/password-profile #
```

Configuring User Roles

Role-Based Access Control

Role-Based Access Control (RBAC) is a method of restricting or authorizing system access for users based on user roles and locales. A role defines the privileges of a user in the system and the locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, management of individual user privileges is simply a matter of assigning the appropriate roles and locales.

A user is granted write access to desired system resources only if the assigned role grants the access privileges and the assigned locale allows access. For example, a user with the Server Administrator role in the Engineering organization could update server configurations in the Engineering organization but could not update server

configurations in the Finance organization unless the locales assigned to the user include the Finance organization.

User Roles

User roles contain one or more privileges that define the operations that are allowed for a user. One or more roles can be assigned to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role2 has server-related privileges, users with Role1 and Role2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Each domain group in Cisco UCS Central can contain 48 user roles, including the user roles that are inherited from the parent domain group. When user roles are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 roles will be active. Any user roles after the first 48 will be inactive with faults raised.

All roles include read access to all configuration settings in the Cisco UCS domain. Users with read-only roles cannot modify the system state.

Roles can be created, modified to add new or remove existing privileges, or deleted. When a role is modified, the new privileges are applied to all users that have that role. Privilege assignment is not restricted to the privileges defined for the default roles. That is, you can use a custom set of privileges to create a unique role. For example, the default Server Administrator and Storage Administrator roles have a different set of privileges, but a new Server and Storage Administrator role can be created that combines the privileges of both roles.

If a role is deleted after it has been assigned to users, it is also deleted from those user accounts.

User profiles on AAA servers (RADIUS or TACACS+) should be modified to add the roles corresponding to the privileges granted to that user. The attribute is used to store the role information. The AAA servers return this attribute with the request and parse it to get the roles. LDAP servers return the roles in the user profile attributes.

Default User Roles

The system contains the following default user roles:

AAA Administrator

Read-and-write access to users, roles, and AAA configuration. Read access to the rest of the system.

Administrator

Complete read-and-write access to the entire system. The default admin account is assigned this role by default and it cannot be changed.

Facility Manager

Read-and-write access to power management operations through the power-mgmt privilege. Read access to the rest of the system.

Network Administrator

Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the rest of the system.

Operations

Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the rest of the system.

Read-Only

Read-only access to system configuration with no privileges to modify the system state.

Server Compute

Read and write access to most aspects of service profiles. However the user cannot create, modify or delete vNICs or vHBAs.

Server Equipment Administrator

Read-and-write access to physical server related operations. Read access to the rest of the system.

Server Profile Administrator

Read-and-write access to logical server related operations. Read access to the rest of the system.

Server Security Administrator

Read-and-write access to server security related operations. Read access to the rest of the system.

Storage Administrator

Read-and-write access to storage operations. Read access to the rest of the system.

Reserved Words: User Roles

The following words cannot be used when creating custom roles in Cisco UCS.

- network-admin
- network-operator
- vdc-admin
- vdc-operator
- server-admin

Privileges

Privileges give users assigned to user roles access to specific system resources and permission to perform specific tasks. The following table lists each privilege and the user role given that privilege by default.

Table 6: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	Administrator

Privilege	Description	Default Role Assignment
domain-group-management	Domain Group Management	Domain Group Administrator
ext-lan-config	External LAN configuration	Network Administrator
ext-lan-policy	External LAN policy	Network Administrator
ext-lan-qos	External LAN QoS	Network Administrator
ext-lan-security	External LAN security	Network Administrator
ext-san-config	External SAN configuration	Storage Administrator
ext-san-policy	External SAN policy	Storage Administrator
ext-san-qos	External SAN QoS	Storage Administrator
ext-san-security	External SAN security	Storage Administrator
fault	Alarms and alarm policies	Operations
operations	Logs and Smart Call Home	Operations
org-management	Organization management	Operations
pod-config	Pod configuration	Network Administrator
pod-policy	Pod policy	Network Administrator
pod-qos	Pod QoS	Network Administrator
pod-security	Pod security	Network Administrator
power-mgmt	Read-and-write access to power management operations	Facility Manager
read-only	Read-only access Read-only cannot be selected as a privilege; it is assigned to every user role.	Read-Only
server-equipment	Server hardware management	Server Equipment Administrator
server-maintenance	Server maintenance	Server Equipment Administrator
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator

Privilege	Description	Default Role Assignment
service-profile-compute	Service profile compute	Server Compute Administrator
service-profile-config	Service profile configuration	Server Profile Administrator
service-profile-config-policy	Service profile configuration policy	Server Profile Administrator
service-profile-ext-access	Service profile end point access	Server Profile Administrator
service-profile-network	Service profile network	Network Administrator
service-profile-network-policy	Service profile network policy	Network Administrator
service-profile-qos	Service profile QoS	Network Administrator
service-profile-qos-policy	Service profile QoS policy	Network Administrator
service-profile-security	Service profile security	Server Security Administrator
service-profile-security-policy	Service profile security policy	Server Security Administrator
service-profile-server	Service profile server management	Server Profile Administrator
service-profile-server-oper	Service profile consumer	Server Profile Administrator
service-profile-server-policy	Service profile pool policy	Server Security Administrator
service-profile-storage	Service profile storage	Storage Administrator
service-profile-storage-policy	Service profile storage policy	Storage Administrator
stats	Statistics Management	Statistics Administrator

Creating a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **create role** *name*	Creates the user role and enters security role mode.
Step 5	UCSC(policy-mgr) /domain-group/security/role* # **add privilege** *privilege-name*	Adds one or more privileges to the role. **Note** You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role, or you can add privileges to the same role using multiple **add** commands.
Step 6	UCSC(policy-mgr) /domain-group/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the service-profile-security-admin role, adds the service profile security and service profile security policy privileges to the role, and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # create role ls-security-admin
UCSC(policy-mgr) /domain-group/security/role* # add privilege service-profile-security
service-profile-security-policy
UCSC(policy-mgr) /domain-group/security/role* # commit-buffer
UCSC(policy-mgr) /domain-group/security/role #
```

Deleting a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **delete role** *name*	Deletes the user role.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the service-profile-security-admin role and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # delete role service-profile-security-admin
UCSC(policy-mgr) /domain-group/security/role* # commit-buffer
UCSC(policy-mgr) /domain-group/security/role #
```

Adding Privileges to a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope role** *name*	Enters security role mode for the specified role.
Step 5	UCSC(policy-mgr) /domain-group/security/role # **add privilege** *privilege-name*	Adds one or more privileges to the existing privileges of the user role. **Note** You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role, or you can add privileges to the same role using multiple **add privilege** commands.
Step 6	UCSC(policy-mgr) /domain-group/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to add the server security and server policy privileges to the service-profile-security-admin role and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope role
UCSC(policy-mgr) /domain-group/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /domain-group/security/role* # add privilege server-security server-policy
UCSC(policy-mgr) /domain-group/security/role* # commit-buffer
UCSC(policy-mgr) /domain-group/security/role #
```

Replacing Privileges for a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope role** *name*	Enters security role mode for the specified role.
Step 5	UCSC(policy-mgr) /domain-group/security/role # **set privilege** *privilege-name*	Replaces the existing privileges of the user role. **Note** You can specify more than one *privilege-name* on the same command line to replace the existing privilege with multiple privileges. After replacing the privileges, you can add privileges to the same role using the **add privilege** command.
Step 6	UCSC(policy-mgr) /domain-group/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to replace the existing privileges for the service-profile-security-admin role with the server security and server policy privileges and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope role
UCSC(policy-mgr) /domain-group/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /domain-group/security/role* # set privilege server-security server-policy
UCSC(policy-mgr) /domain-group/security/role* # commit-buffer
UCSC(policy-mgr) /domain-group/security/role #
```

Removing Privileges from a User Role

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope role** *name*	Enters security role mode for the specified role.
Step 5	UCSC(policy-mgr) /domain-group/security/role # **remove privilege** *privilege-name*	Removes one or more privileges from the existing user role privileges. **Note** You can specify more than one *privilege-name* on the same command line to remove multiple privileges from the role, or you can remove privileges from the same role using multiple **remove privilege** commands.
Step 6	UCSC(policy-mgr) /domain-group/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

The following example removes the server security and server policy privileges from the service-profile-security-admin role and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope role
UCSC(policy-mgr) /domain-group/security/role # remove privilege server-security server-policy
UCSC(policy-mgr) /domain-group/security/role* # commit-buffer
UCSC(policy-mgr) /domain-group/security/role #
```

Assigning a Role to a User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope local-user** *local-user-name*	Enters security local user mode for the specified local user account.
Step 5	UCSC(policy-mgr) /domain-group/security/local-user # **create role** *role-name*	Assigns the specified role to the user account . **Note** The **create role** command can be entered multiple times to assign more than one role to a user account.
Step 6	UCSC(policy-mgr) /domain-group/security/local-user* # **commit-buffer**	Commits the transaction.

The following example assigns the operations role to the kikipopo local user account and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope local-user kikipopo
UCSC(policy-mgr) /domain-group/security/local-user # create role operations
UCSC(policy-mgr) /domain-group/security/local-user* # commit-buffer
UCSC(policy-mgr) /domain-group/security/local-user #
```

Removing a Role from a User Account

Changes in user roles and privileges do not take effect until the next time the user logs in. If a user is logged in when you assign a new role to or remove an existing role from a user account, the active session continues with the previous roles and privileges.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group

	Command or Action	Purpose
		root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope local-user** *local-user-name*	Enters security local user mode for the specified local user account.
Step 5	UCSC(policy-mgr) /domain-group/security/local-user # **delete role** *role-name*	Removes the specified role from the user account . **Note** The **delete role** command can be entered multiple times to remove more than one role from a user account.
Step 6	UCSC(policy-mgr) /domain-group/security/local-user* # **commit-buffer**	Commits the transaction.

The following example removes the operations role from the kikipopo local user account and commits the transaction:

```
CSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope local-user kikipopo
UCSC(policy-mgr) /domain-group/security/local-user # delete role operations
UCSC(policy-mgr) /domain-group/security/local-user* # commit-buffer
UCSC(policy-mgr) /domain-group/security/local-user #
```

Configuring User Locales

User Locales

A user can be assigned one or more locales. Each locale defines one or more organizations (domains) the user is allowed access, and access would be limited to the organizations specified in the locale. One exception to this rule is a locale without any organizations, which gives unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Each domain group in Cisco UCS Central can contain 48 user locales, including the user locales that are inherited from the parent domain group. When user locales are pushed to Cisco UCS Manager from Cisco UCS Central, only the first 48 locales will be active. Any user locales after the first 48 will be inactive with faults raised.

Users with admin, aaa, or domain-group-management privileges can assign organizations to the locale of other users.

Note You cannot assign a locale to users with the admin privilege.

You can hierarchically manage organizations. A user that is assigned at a top level organization has automatic access to all organizations under it. For example, an Engineering organization can contain a Software Engineering organization and a Hardware Engineering organization. A locale containing only the Software Engineering organization has access to system resources only within that organization; however, a locale that contains the Engineering organization has access to the resources for both the Software Engineering and Hardware Engineering organizations.

Creating a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **create locale** *name*	Creates the user role and enters security role mode.
Step 5	UCSC(policy-mgr) /domain-group/security/locale * # **create org-ref** *org-ref-name* **orgdn** *orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference, and the *orgdn-name* argument is the distinguished name of the organization being referenced.
Step 6	UCSC(policy-mgr) /domain-group/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

The following example shows how to create the finance organization for the western locale and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # create locale western
UCSC(policy-mgr) /domain-group/security/locale* # create org-ref finance-ref orgdn finance
UCSC(policy-mgr) /domain-group/security/locale* # commit-buffer
UCSC(policy-mgr) /domain-group/security/locale #
```

Deleting a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **delete locale** *locale-name*	Deletes the locale.
Step 5	UCSC(policy-mgr) /domain-group/security * # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the western locale and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # delete locale western
UCSC(policy-mgr) /domain-group/security* # commit-buffer
UCSC(policy-mgr) /domain-group/security #
```

Assigning a Locale to a User Account

Note Do not assign locales to users with an admin role.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.

	Command or Action	Purpose
Step 4	UCSC /security # **scope local-user** *local-user-name*	Enters security local user mode for the specified local user account.
Step 5	UCSC(policy-mgr) /domain-group/security/local-user # **create locale** *locale-name*	Assigns the specified locale to the user account. **Note** The **create locale** command can be entered multiple times to assign more than one locale to a user account.
Step 6	UCSC(policy-mgr) /domain-group/security/local-user* # **commit-buffer**	Commits the transaction.

The following example shows how to assign the western locale to the kikipopo local user account and commit the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security/local-user # create locale western
UCSC(policy-mgr) /domain-group/security/local-user* # commit-buffer
UCSC(policy-mgr) /domain-group/security/local-user #
```

Removing a Locale from a User Account

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope local-user** *local-user-name*	Enters security local user mode for the specified local user account.
Step 5	UCSC(policy-mgr) /domain-group/security/local-user # **delete locale** *locale-name*	Removes the specified locale from the user account. **Note** The **delete locale** command can be entered multiple times to remove more than one locale from a user account.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/security/local-user* # **commit-buffer**	Commits the transaction.

The following example removes the western locale from the kikipopo local user account and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security/local-user # delete locale western
UCSC(policy-mgr) /domain-group/security/local-user* # commit-buffer
UCSC(policy-mgr) /domain-group/security/local-user #
```

Assigning an Organization to a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope locale** *locale-name*	Enters security locale mode.
Step 5	UCSC(policy-mgr) /domain-group/security/locale # **create org-ref** *org-ref-name* **orgdn** *orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference, and the *orgdn-name* argument is the distinguished name of the organization being referenced.
Step 6	UCSC(policy-mgr) /domain-group/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the western locale, adds (references) the marketing organization to the locale, names the reference marketing-ref, and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
```

```
UCSC(policy-mgr) /domain-group/security # scope locale western
UCSC(policy-mgr) /domain-group/security/locale # create org-ref marketing-ref orgdn marketing
UCSC(policy-mgr) /domain-group/security/locale* # commit-buffer
UCSC(policy-mgr) /domain-group/security/locale #
```

Deleting an Organization from a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope locale** *locale-name*	Enters security locale mode.
Step 5	UCSC(policy-mgr) /domain-group/security/locale # **delete org-ref** *org-ref-name*	Deletes the organization from the locale.
Step 6	UCSC(policy-mgr) /domain-group/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the finance organization from the western locale and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope locale western
UCSC(policy-mgr) /domain-group/security/locale # delete org-ref finance-ref
UCSC(policy-mgr) /domain-group/security/locale* # commit-buffer
UCSC(policy-mgr) /domain-group/security/locale #
```

Assigning a Domain Group to a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root.

	Command or Action	Purpose
		To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope locale** *locale-name*	Enters security locale mode.
Step 5	UCSC(policy-mgr) /domain-group/security/locale # **create domain-group-ref** *domain-group-ref-name* **domain-group-dn** *domaingroup-root-name*	References (binds) a domain group to the locale. The *domain-group-ref-name* argument (1-16 characters) is the name used to identify the domain group reference, and the *domain-group-dn-name* argument is the distinguished name of the domain group root being referenced.
Step 6	UCSC(policy-mgr) /domain-group/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the western locale, adds (references) the marketing domain group to the locale, names the reference marketdomain01-ref, and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope locale western
UCSC(policy-mgr) /domain-group/security/locale # create domain-group-ref marketdomain01
domain-group-dn marketing
UCSC(policy-mgr) /domain-group/security/locale* # commit-buffer
UCSC(policy-mgr) /domain-group/security/locale #
```

Deleting a Domain Group from a User Locale

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **scope security**	Enters security mode.
Step 4	UCSC(policy-mgr) /domain-group/security # **scope locale** *locale-name*	Enters security locale mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/security/locale # **delete domain-group-ref** *domain-group-ref-name*	Deletes references (unbinds) domain groups referenced to the locale. The *domain-group-ref-name* argument (1-16 characters) is the name used to identify the domain group reference.
Step 6	UCSC(policy-mgr) /domain-group/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the western locale, deletes references (unbinds) the marketing domain group references from the locale marketdomain01, and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope security
UCSC(policy-mgr) /domain-group/security # scope locale western
UCSC(policy-mgr) /domain-group/security/locale # delete domain-group-ref marketdomain01
UCSC(policy-mgr) /domain-group/security/locale* # commit-buffer
UCSC(policy-mgr) /domain-group/security/locale #
```

Configuring User Domain Groups

Creating a User Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **create domain-group** *name*	Creates the domain group.
Step 4	UCSC(policy-mgr) /domain-group * # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the central-audit domain group and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create domain-group central-audit
```

```
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Deleting a User Domain Group

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	UCSC(policy-mgr) /domain-group # **delete domain-group** *name*	Deletes the domain group.
Step 4	UCSC(policy-mgr) /domain-group * # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the central-audit domain group and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # delete domain-group central-audit
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

Configuring User Organizations

User Organizations

A user can create one or more organizations. Each organization defines sub-organizations, faults, events, UUID suffix pools and blocks of UUIDs.

Cisco UCS organizations are hierarchically managed by users. A user that is assigned at the root level organization has automatic access to all organizations and domain groups under it.

Creating a User Organization

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create org** *name*	Creates the organization.
Step 4	UCSC(policy-mgr) /org * # **commit-buffer**	Commits the transaction to the system configuration.

The following example creates the central-audit organization and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create org central-audit
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Deleting a User Organization

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete org** *name*	Deletes the organization.
Step 4	UCSC(policy-mgr) /org * # **commit-buffer**	Commits the transaction to the system configuration.

The following example deletes the central-audit organization and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete org central-audit
```

```
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Creating a User Sub-Organization

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create org** *name*	Creates the sub-organization under the organization scoped.
Step 4	UCSC(policy-mgr) /org * # **commit-buffer**	Commits the transaction to the system configuration.

The following example enters the central-audit organization, creates the north-audit sub-organization and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org central-audit
UCSC(policy-mgr) /org # create org north-audit
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

Deleting a User Sub-Organization

Procedure

Step 1 UCSC# **connect policy-mgr**
Enters policy manager mode.

Step 2 UCSC(policy-mgr) # **scope org** *org-name*
Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.

Step 3 UCSC(policy-mgr) /org # **delete org** *name*
Deletes the sub-organization under the organization scoped.

Step 4 UCSC(policy-mgr) /org * # **commit-buffer**
Commits the transaction to the system configuration.

The following example enters the central-audit organization, deletes the north-audit sub-organization and commits the transaction:

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org central-audit
UCSC(policy-mgr) /domain-group # delete org north-audit
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```