Cisco UCS Central CLI Reference Manual, Release 2.0

First Published: 2017-06-06

Last Modified: 2019-12-20

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

CONTENTS

Preface

Audience

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

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

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in **this font**. Main titles such as window, dialog box, and wizard titles appear in **this font**.
Document titles	Document titles appear in *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	Elements in square brackets are optional.

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

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

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

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

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

Warning IMPORTANT SAFETY INSTRUCTIONS

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

SAVE THESE INSTRUCTIONS

Related Cisco UCS Documentation

Documentation Roadmaps

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

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

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

Other Documentation Resources

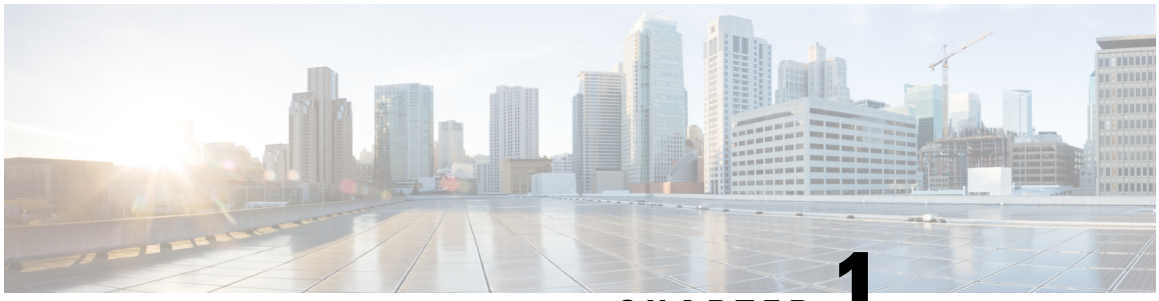
Follow Cisco UCS Docs on Twitter to receive document update notifications.

Documentation Feedback

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

PART I

Getting Started

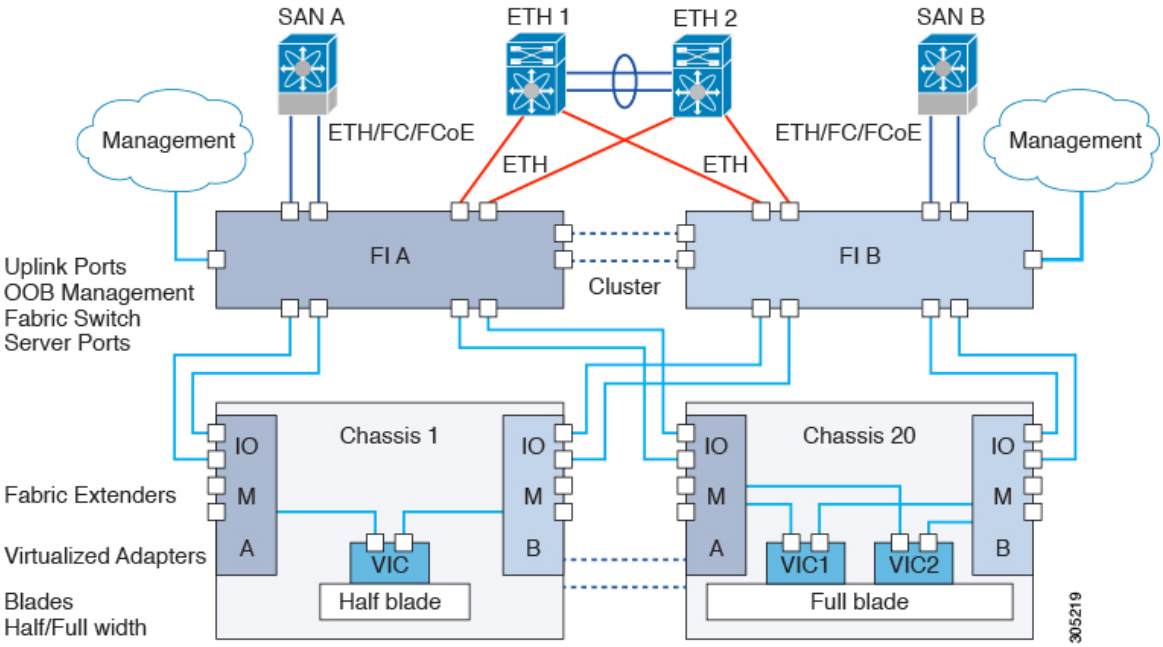


CHAPTER 1

Introduction to Cisco Unified Computing System Infrastructure

Cisco Unified Computing System Overview

Figure 1: Cisco UCS Architecture



Cisco UCS has a unique architecture that integrates compute, data network access, and storage network access into a common set of components under a single-pane-of-glass management interface.

Cisco UCS fuses access layer networking and servers. This high-performance, next-generation server system provides a data center with a high degree of workload agility and scalability. The hardware and software components support Cisco's unified fabric, which runs multiple types of data center traffic over a single converged network adapter.

Architectural Simplification

The simplified architecture of Cisco UCS reduces the number of required devices and centralizes switching resources. By eliminating switching inside a chassis, network access-layer fragmentation is significantly reduced. Cisco UCS implements Cisco unified fabric within racks and groups of racks, supporting Ethernet and Fibre Channel protocols over 10 Gigabit Cisco Data Center Ethernet and Fibre Channel over Ethernet (FCoE) links. This radical simplification reduces the number of switches, cables, adapters, and management points by up to two-thirds. All devices in a Cisco UCS domain remain under a single management domain, which remains highly available through the use of redundant components.

Scalability

A single Cisco UCS domain supports multiple chassis and their servers, all of which are administered through one Cisco UCS Manager. For more detailed information about the scalability, speak to your Cisco representative.

Flexibility

A Cisco UCS domain allows you to quickly align computing resources in the data center with rapidly changing business requirements. This built-in flexibility is determined by whether you choose to fully implement the stateless computing feature. Pools of servers and other system resources can be applied as necessary to respond to workload fluctuations, support new applications, scale existing software and business services, and accommodate both scheduled and unscheduled downtime. Server identity can be abstracted into a mobile service profile that can be moved from server to server with minimal downtime and no need for additional network configuration. With this level of flexibility, you can quickly and easily scale server capacity without having to change the server identity or reconfigure the server, LAN, or SAN. During a maintenance window, you can quickly do the following:

- Deploy new servers to meet unexpected workload demand and rebalance resources and traffic.
- Shut down an application, such as a database management system, on one server and then boot it up again on another server with increased I/O capacity and memory resources.

Optimized for Server Virtualization

Cisco UCS has been optimized to implement VM-FEX technology. This technology provides improved support for server virtualization, including better policy-based configuration and security, conformance with a company's operational model, and accommodation for VMware's VMotion.

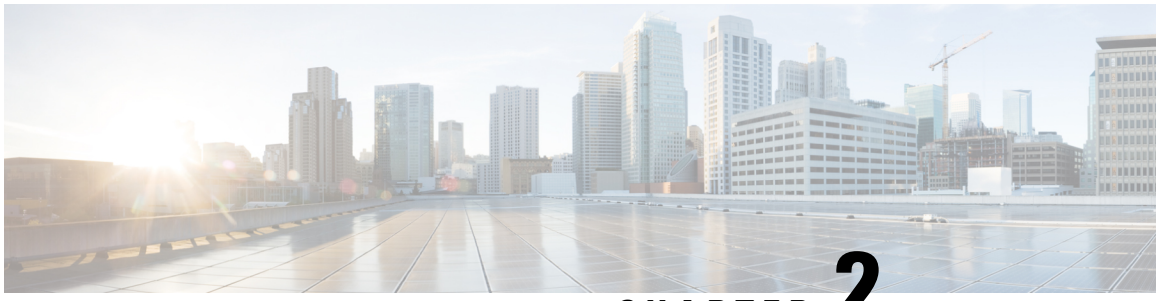
Cisco UCS Manager Overview

Cisco UCS Manager is embedded software that resides on the fabric interconnects, providing complete configuration and management capabilities for all of the components in the Cisco UCS system. This configuration information is replicated between the two fabric interconnects, providing a highly available solution for this critical function. The most common way to access UCS Manager for simple tasks is to use a Web browser to open the Java-based GUI. For command-line or programmatic operations against the system, a command-line interface (CLI) and an XML API are also included with the system.

The Cisco UCS Manager GUI provides role-based access control (RBAC) to allow multiple levels of users granular administrative rights to system objects. Users can be restricted to certain portions of the system based on locale, which corresponds to an optional organizational structure that can be created within the system. Users can also be classified based on their access levels or areas of expertise, such as “Storage Administrator,” “Server Equipment Administrator,” or “Read-Only”. RBAC allows the comprehensive capabilities of the

Cisco UCS Manager GUI to be properly shared across multiple individuals or teams within your organization in a flexible, secure manner.

Cisco UCS Manager provides unified, embedded management of all software and hardware components. Every instance of Cisco UCS Manager and all of the components managed by it form a domain. For organizations that deploy multiple Cisco UCS domains, Cisco UCS Central software providesa centralized user interface that allows you to manage multiple, globallydistributed Cisco UCS domains with thousands of servers. Cisco UCS Central integrates with Cisco UCS Manager and utilizes it to provide globalconfiguration capabilities for pools, policies, and firmware.



CHAPTER 2

Introduction to Cisco UCS Central

Introducing Cisco UCS Central

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

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

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

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

Cisco UCS Central Features

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

Note For a full list of new features, see the Release Notes for Cisco UCS Central.

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

Feature	Description
Global service profiles and templates	Global service profiles and templates in Cisco UCS Central enables fast and simplified infrastructure deployment and provides consistency of configurations throughout the enterprise. This feature enables global bare-metal workload mobility very similar to how hypervisor enables virtualized workload mobility.
Backup	Cisco UCS Central provides an automatic backup facility that enables quick and efficient backing up the configuration information of the registered Cisco UCS domains and the UCS Central configuration.
XML API	Cisco UCS Central, just like Cisco UCS Manager, has a high-level industry-standard XML API for interfacing with existing management frameworks and orchestration tools. The XML API for Cisco UCS Central Software is similar to the XML API for Cisco UCS Manager, making integration with high-level managers very fast.
Remote Management	Cisco UCS Central enables you to manage various end points in the registered Cisco UCS domains from one management point. You can manage chassis, servers, fabric interconnects, and fabric extenders from Cisco UCS Central GUI or CLI. You can also access tech support files for registered UCS domains from Cisco UCS Central.

Overview of Cisco UCS Central 2.0 Features

Cisco UCS Central 2.0 supports new features listed in the sections in this topic. Some of these features are built in Cisco UCS Central to be compatible with Cisco UCS Manager release 3.1(3) and later. For more information about the appropriate supported Cisco UCS Manager releases, see the feature support matrix in the Cisco UCS Central Release Notes.

Feature	Function
Support for IOE Controller	Supports a second RAID Controller in the IO Expander on Cisco UCS S3260 Storage Server (UCS-C3K-M4RAID).
Support for HBA Controller	Supports Dual HBA Controllers on Cisco UCS S3260 Storage Server (UCS-S3260-DHBA).
BIOS Asset Tag	Service profiles now display an Asset Tag to uniquely identify servers.
Globalization of Service Profiles	Allows you to globalize Local Service Profiles from Cisco UCS Manager intoCisco UCS Central to deploy and use Cisco UCS Central in a legacy software environment.

Feature	Function
Integrated Server Diagnostics	Enables you to verify the health of hardware components on your servers and provides various tests to stress and exercise the hardware subsystems, such as memory and CPU, on the servers.
Lightweight Upgrades/ Hot Patching	Delivers Cisco UCS Manager firmware security updates for infrastructure and server components through service pack bundles.
Set KVM IP on Physical servers	Allows you to configure KVM IP s on physical servers for Inband and Outband management.
SED Management, KMIP Support	Introduces security policies for Self-Encrypting Drives (SEDs) for management of data encryption. The security keys required to encrypt the media encryption key can be configured locally, or remotely using the KMIP server.
Smart SSD	Supports monitoring SSD health and provides statistics about various SSD properties, and a threshold limit for each property.
User-defined FC Zoning	Allows you to create an FC Zone profile to group all zoning needs for a VM to represent a single data replication solution between storage arrays.
Fabric Evacuation in Firmware Auto Install	Supports automatic configuration of Fabric Evacuation during an FI upgrade and reboot during AutoInstall, and ensures that the appropriate failover settings are configured for the firmware upgrade.
Launch HTML5 KVM Client	Launches the HTML5 based KVM client directly from the Cisco UCS Central GUI.
New Policies	The following new policies are introduced in Cisco UCS Central 2.0: • Multicast Policy with IGMP Snooping • Power Sync Policy • Statistics Threshold Policy • Graphics Card Policy • QoS System Class • Hardware Change Discovery Policy • Port Auto-Discovery Policy • KMIP Certification Policy

Feature	Function
Server Reboot Log	Displays a server reboot log with the last five reasons for the reset, along with the time and source of power transition.
Cisco UCS Manager DirectView tabs	Launches DirectView of Cisco UCS Manager Server Statistics tabs from 2.0 to view details of CIMC Sessions, System Event Logs, VIF paths, Statistics, Temperatures, Power, and Installed Firmware.
UI enhancements	Introduces the following UI enhancements: • Spotlight search bar to enable a comprehensive search for objects by their names. Top 10 results and suggested entries are displayed. • Restore Tabs to save open tabs and enable direct access to the same session when you log back in to Cisco UCS Central. • Favorites widget on the widgets menu bar to save your most used components, tabs, and dialogs for creating or editing policies. • Clone Policies icon to enable deep cloning a policy with a new name, parent organization or domain group, and description if applicable, in order to help you make minor edits without having to create a new policy.

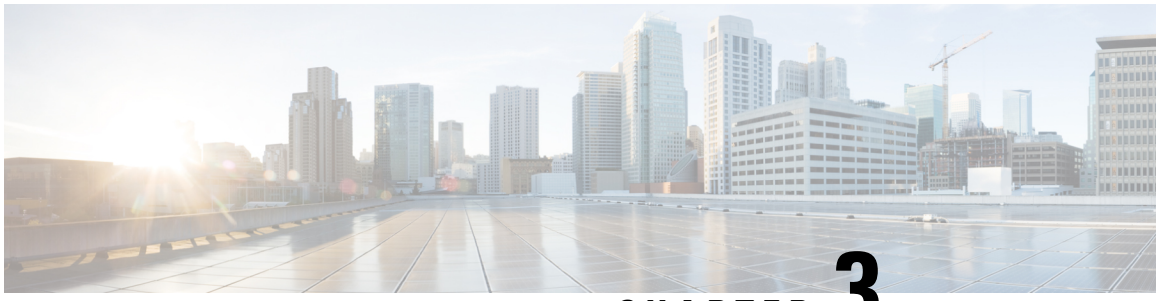
Cisco UCS Central CLI Release 2.0 Features

The following table provides a list of features with a brief description on the command-line (CLI) capabilities of Cisco UCS Central:

Note For a full list of new features, see the Release Notes for Cisco UCS Central.

Feature	Description
Set KVM IP on Physical servers	Allows you to configure KVM IP s on physical servers for Inband and Outband management.
SED Management, KMIP Support	Introduces security policies for Self-Encrypting Drives (SEDs) for management of data encryption. The security keys required to encrypt the media encryption key can be configured locally, or remotely using the KMIP server.
Smart SSD	Supports monitoring SSD health and provides statistics about various SSD properties, and a threshold limit for each property.

Feature	Description
User-defined FC Zoning	Allows you to create an FC Zone profile to group all zoning needs for a VM to represent a single data replication solution between storage arrays.
Fabric Evacuation in Firmware Auto Install	Supports automatic configuration of Fabric Evacuation during an FI upgrade and reboot during AutoInstall, and ensures that the appropriate failover settings are configured for the firmware upgrade.
New Policies	The following new policies are introduced in Cisco UCS Central 2.0: • Multicast Policy with IGMP Snooping • Power Sync Policy • Statistics Threshold Policy • Graphics Card Policy • QoS System Class • Hardware Change Discovery Policy • Port Auto-Discovery Policy • KMIP Certification Policy



CHAPTER 3

Working with Cisco UCS Manager

Cisco UCS Domains and Cisco UCS Central

Cisco UCS Central provides centralized management capabilities to multiple Cisco UCS domains across one or more data centers. Cisco UCS Central works with Cisco UCS Manager to provide a scalable management solution for a growing Cisco UCS environment.

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 using Cisco UCS Manager the same way you did before Cisco UCS Central. This also allows all existing third party integrations to continue to operate without change.

Registering Cisco UCS Domains

You can use a Fully Qualified Domain Name (FQDN) or IP address to register Cisco UCS domains in Cisco UCS Central.

To manage Cisco UCS Manager through Cisco UCS Central, you must register the Cisco UCS domains in Cisco UCS Central. You can register a Cisco UCS domain as a part of a domain group or as an ungrouped domain. When you have a domain group, all registered domains in the domain group can share common policies and other configurations.

Note During the initial registration process with Cisco UCS Central, all of the active Cisco UCS Manager GUI sessions are terminated.

Before registering a domain in Cisco UCS Central, do the following:

- Configure an NTP server and the correct time zone in both Cisco UCS Manager and Cisco UCS Central to ensure that they are in sync. If the time and date in the Cisco UCS domain and Cisco UCS Central are out of sync, the registration might fail.
- Obtain the hostname or IP address of Cisco UCS Central. You cannot use the same hostname for both Cisco UCS Central and Cisco UCS Manager. For standalone mode, use individual VM IP address.

- Obtain the shared secret that you configured when you deployed Cisco UCS Central.

Note

- Cisco recommends that you always register Cisco UCS domains using Cisco UCS Central's Fully Qualified Domain Name (FQDN). If domains are registered with FQDN, any change in the Cisco UCS Central IP address is transparent to the domain.
- If Cisco UCS Central is deployed on RHEL 7.2 KVM, the first time you register a Cisco UCS domain, you must regenerate the certificate using the **set regenerate yes** command.
- If the registered Cisco UCS domains have a latency of greater than 300ms for a round trip from Cisco UCS Central, there might be some performance implications for the Cisco UCS domains.
- When you unregister a Cisco UCS domain from Cisco UCS Central the global service profiles become local service profiles in Cisco UCS Manager.

  For more information about Changing Cisco UCS Central's IP address, see Changing Cisco UCS Central IP Address.

Warning You must upgrade to Cisco UCS Manager Release 2.1(2) or greater before registering with Cisco UCS Central. If you try to register earlier versions of Cisco UCS Manager, the registration will fail.

Registering a Cisco UCS Domain with the CLI

You can register a Cisco UCS Manager domain to any Cisco UCS Central system. However you can only register the Cisco UCS Manager domain to one Cisco UCS Central system at a time.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope system**	Enters into the system.
Step 3	UCSC(resource-mgr) /system # **create policy-control-ep** *UCSM domain IP address* admin	Creates a policy control for the UCSM domain. **Note** You must be logged in as an admin to register a domain.
Step 4	UCSC(resource-mgr) /system # Domain Admin Password: *password*	Specifies the password.
Step 5	UCSC(resource-mgr) /system/policy-control-ep # **set srcaddrfmt ipv4** { *hostname* | *ipv4* | *ipv6* }	Sets the address format for the domain.
Step 6	UCSC(resource-mgr) /system/policy-control-ep # **commit-buffer**	Commits the transaction to the system and registers the Cisco UCS Manager domain to Cisco UCS Central.

	Command or Action	Purpose
Step 7	UCSC(resource-mgr) /system/policy-control-ep # **show detail**	Displays the status of the Cisco UCS Manager domain.

Example

The following example shows how to register a Cisco UCS Manager domain with Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope system
UCSC(resource-mgr) /system # create policy-control-ep 10.193.01.01 admin
UCSC(resource-mgr) /system #  Domain Admin Password:
UCSC(resource-mgr) /system/policy-control-ep* #
UCSC(resource-mgr) /system/policy-control-ep # set srcaddrfmt ipv4
UCSC(resource-mgr) /system/policy-control-ep # commit-buffer
UCSC(resource-mgr) /system/policy-control-ep # show detail
hostname or ip address: 10.193.190.130
Registration Status: Registered
Cleanup Mode: Localize Global
Current Task:
```

Unregistering a Cisco UCS Domain with the CLI

Caution If you want to unregister any registered Cisco UCS domain in a production system, contact Cisco Technical Support.

When you unregister a Cisco UCS domain from Cisco UCS Central:

- You can no longer manage the service profiles, policies and other configuration for the Cisco UCS Domain from Cisco UCS Central
- All global service profiles and policies become local and continue to operate as local entities. When you re-register the domain, the service profiles and polices still remain local.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope system**	Enters into the system.
Step 3	UCSC(resource-mgr) /system # **scope policy-control-ep** *UCSM domain IP address*	Creates a policy control for the UCSM domain.
Step 4	UCSC(resource-mgr) /system/policy-control-ep # **set actionevent unregister**	Prepares to unregister the domain.

	Command or Action	Purpose
Step 5	UCSC(resource-mgr) /system/policy-control-ep # **commit-buffer**	Commits the transaction to the system and unregisters the Cisco UCS Manager domain from Cisco UCS Central.

Example

The following example shows how to unregister a Cisco UCS Manager domain with Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope system
UCSC(resource-mgr) /system # scope policy-control-ep 10.193.01.01 admin
UCSC(resource-mgr) /system/policy-control-ep # set actionevent unregister
UCSC(resource-mgr) /system/policy-control-ep # commit-buffer
UCSC(resource-mgr) /system/policy-control-ep # show detail
hostname or ip address: 10.193.190.130
Registration Status: Failed
Cleanup Mode: Localize Global
Current Task:
```

Domains and Domain Groups

When you register a Cisco UCS Manager instance in Cisco UCS Central, that instance becomes an ungrouped domain in Cisco UCS Central. You must assign this domain to a domain group to start managing this domain using global policies in Cisco UCS Central.

Cisco UCS Central creates a hierarchy of Cisco UCS domain groups for managing multiple Cisco UCS domains.

- **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 is automatically be placed under the domain group specified in the policy. If not, it is placed in the ungrouped domains category until the domain group is assigned to a domain group.

You can only assign each Cisco UCS domain 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 automatically inherits 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 avoids 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 protects 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.

Example

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.

Example

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 information for the registered domains.
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** *Domain Group Name*	Specifies the domain group for the IP address.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-membership # **commit-buffer**	Commits the transaction to the system.

Example

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
    ---------------- ------------------ ---------------
    10.193.01.01     Manual             domaingroup-root
UCSC(resource-mgr) /domain-mgmt # scope ucs-membership 10.193.01.01
UCSC(resource-mgr) /domain-mgmt/ucs-membership # set domain-group DG-test
UCSC(resource-mgr) /domain-mgmt/ucs-membership #
```

Domain Group Qualification Policy

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

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

Example

This following example shows how to create a qualifier:

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

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.

Example

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.

Example

The following example shows how to create a registration policy:

```
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 #
```

Policies in Cisco UCS Central and Cisco UCS Domains

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

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

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

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

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

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

Policy Resolution Control

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:

Note The policy resolution options in Cisco UCS Central are not supported on all versions of Cisco UCS Manager. If your Cisco UCS Manager version is earlier than the earliest supported release, the policy resolution screen may display the value as global even if it is not applicable.

In a case where you choose certain policies to be resolved locally using the Policy Resolution Control feature in Cisco UCS Central, or when a Cisco UCS Domain is unregistered from Cisco UCS Central, the global settings/unnamed policies (such as QoS Settings, Discovery policies) stay as previously configured. You must manually change the policy details to the desired state.

Caution Unregistering a Cisco UCS Domain has serious implications. You must not unregister the Cisco UCS Domain unless you choose to permanently not manage it from Cisco UCS Central.

Name	Earliest Supported Release	Description
Infrastructure & Catalog Firmware	2.1(2)	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally in Cisco UCS Manager or come from Cisco UCS Central.
Time Zone Management	2.1(2)	Determines whether the time zone and NTP server settings are defined locally in Cisco UCS Manager or comes from Cisco UCS Central.
Communication Services	2.1(2)	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Global Fault Policy	2.1(2)	Determines whether the Global Fault Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
User Management	2.1(2)	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally in Cisco UCS Manager or in Cisco UCS Central.
DNS Management	2.1(2)	Determines whether DNS servers are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Backup & Export Policies	2.1(2)	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally in Cisco UCS Manager or in Cisco UCS Central.

Name	Earliest Supported Release	Description
Monitoring	2.1(2)	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
SEL Policy	2.1(2)	Determines whether the SEL Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Allocation Policy	2.1(2)	Determines whether the Power Allocation Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Policy	2.1(2)	Determines whether the Power Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Equipment Policy	2.2(7)	Determines whether the Equipment Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Port Configuration	2.2(7)	Determines whether port configuration is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Quality of Service (QoS) Configuration	2.2(7)	Determines whether QoS configuration is defined locally in Cisco UCS Manager or in Cisco UCS Central.

Policies

To assign a policy or a Management IP pool/policy to a domain profile, click on the policy and then click on the drop-down list to select the policy you want to assign to a profile. You can assign the following policies to a domain:

- **QoS System Class** - Defines a configurable set of system classes that you can include in a QoS Policy.
- **Port Auto-Discovery Policy**- Determines whether Server Port Auto-Discovery enabled or disabled in Cisco UCS Central.
- **Hardware Change Discovery Policy**- Determines if a hardware replacement deep discovery is triggered automatically, or after user acknowledgement from Cisco UCS Central.
- **KMIP Certification Policy** - KMIP Certification Policy enables using Self-Encrypting Drives (SEDs) through key management servers. This policy aims to generate a certificate that will be used by CIMC to communicate with KMIP server to get the key. You can configure this policy to a domain if it is created in a global scope.

Management IP

You can assign the following pools/policies from the **Management IP** pool:

- **Inband Policy** - Policy to configure the Inband IP address on a server directly, or through an Inband policy.
- **Outband Pool** - Sets the Management IP Pool created for Outband network management.

Note The **Management IP** tab in the **Domain Configuration Settings** window is enabled only when the registered Cisco UCS Domain is Cisco UCS Manager 3.1(3) and later. For all earlier Cisco UCS Manager releases, the Management IP tab is hidden.

Consequences of Policy Resolution Changes

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

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

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

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
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
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

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
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
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

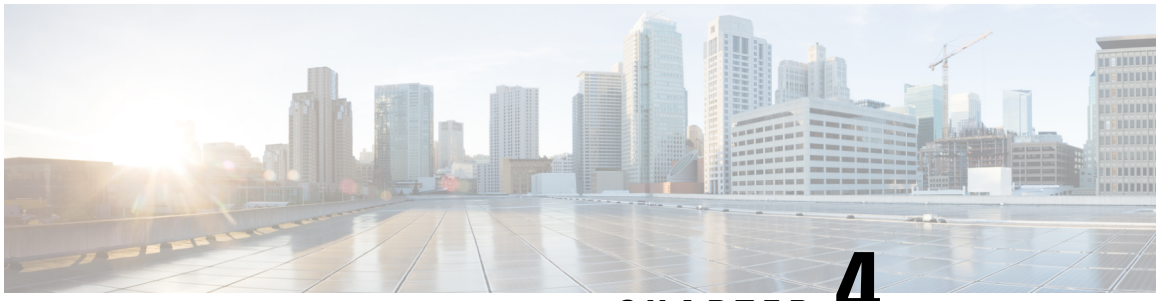
Policies and Configuration	Policy Source		Behavior in Cisco UCS Manager on Registration with Cisco UCS Central		Behavior in Cisco UCS Manager when Registration Changed	
	Cisco UCS Central	Cisco UCS Manager	Domain Group Unassigned	Domain Group Assigned	Unassigned from Domain Group	Deregistered from Cisco UCS Central
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
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 25	See Consequences of Service Profile Changes on Policy Resolution, on page 25	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 25	See Consequences of Service Profile Changes on Policy Resolution, on page 25	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 25	See Consequences of Service Profile Changes on Policy Resolution, on page 25	Deletes remote policies	Converted to a local policy

Consequences of Service Profile Changes on Policy Resolution

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

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

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



CHAPTER 4

Tags

Tags and Tag Types

Cisco UCS Central uses tags to allow users to group objects outside of the Organization or Domain Group structures. You can use the following types of tags:

- System-defined tags—Tags that are defined by Cisco UCS Central. This includes the Maintenance Group tag, the Operating System for HCR tag, and the Adapter Driver for HCR tag.
- User-defined tags—Tags that are created by users but have specific values.
- Basic tags—Free text tags that can allow any value.

From the **Tag Management** page in the GUI, you can view all Tag Types that have been created in Cisco UCS Central. However, you can view only the Tags that are associated with an object and are in active use at any given time.

Creating Tag Types

You can add tags to policies, logical resources such as service profiles and ID pools, and physical inventory components such as domains or servers.

Note Only users with the Tag permission can create tag types.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope fabric**	Scopes into the fabric interconnect.
Step 3	UCSC(policy-mgr) /fabric # **scope tag-mgmt**	Scopes into tag management.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /fabric/tag-mgmt # **create tag-type** *tag-type-name*	Creates the tag type.
Step 5	(Optional) UCSC(policy-mgr) /fabric/tag-mgmt/tag-type/tag-item # **set** {*color* | *descr* | *restricted* {yes|no}}	Sets the following for the tag type: • Color—Sets the color for the tag display. **Note** You must enter color in hex code. • Description—Allows user to enter a description. • Restriction—Yes | No • No—Does not restrict the tag. Allows you to enter any text to the tag. • Yes—Restricts the tag to a predefined list. You can create a list of values, or add additional values to an existing list of values. When you assign the tag, you choose one of the values from the list.
Step 6	UCSC(policy-mgr) /fabric/tag-mgmt/tag-type/tag-item # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create a tag and set options for it:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope fabric
UCSC(policy-mgr) /fabric # scope tag-mgmt
UCSC(policy-mgr) /fabric/tag-mgmt # create tag-type USA
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # set color 722607
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # set descr 'USA updates'
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # set restricted no
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type/tag-item # commit-buffer
```

Creating Tag Values

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope fabric**	Scopes into the fabric interconnect.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /fabric # **scope tag-mgmt**	Scopes into tag management.
Step 4	UCSC(policy-mgr) /fabric/tag-mgmt # **scope tag-type** *tag-type*	Scopes into a specific tag type.
Step 5	UCSC(policy-mgr) /fabric/tag-mgmt/tag-type/tag-item # **create tag-item** *tag-name*	Creates a new tag value.
Step 6	UCSC(policy-mgr) /fabric/tag-mgmt/tag-type/tag-item # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create tag values:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope fabric
UCSC(policy-mgr) /fabric # scope tag-mgmt
UCSC(policy-mgr) /fabric/tag-mgmt # show tag-type
Tag Type:
    Name                       Color      System Defined Multiple Restricted
    -------------------------- ---------- -------------- -------- ----------
    Adapter Driver for HCR     049fd9     Yes            Yes      Yes
    Basic                      5bc0de     Yes            Yes      No
    Geographic                 5bc0de     No             Yes      No
    Maintenance Group          049fd9     Yes            No       Yes
    Operating System for HCR   049fd9     Yes            No       Yes
UCSC(policy-mgr) /fabric/tag-mgmt # scope tag-type 'Maintenance Group'
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # create tag-item FW_Update
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type/tag-item # commit-buffer
```

Viewing Tags

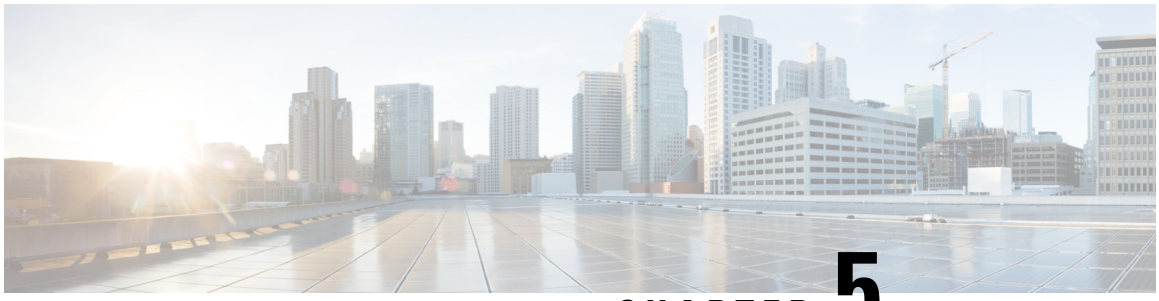
Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope fabric**	Scopes into the fabric interconnect.
Step 3	UCSC(policy-mgr) /fabric # **scope tag-mgmt**	Scopes into tag management.
Step 4	UCSC(policy-mgr) /fabric/tag-mgmt # **show tag-type**	Displays all tag types.
Step 5	UCSC(policy-mgr) /fabric/tag-mgmt # **scope tag-type** '*tag-type*'	Scopes into a specific tag type.
Step 6	UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # **show tag-item**	Displays the values for the selected tag.

Example

The following example shows how to view maintenance group tags:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope fabric
UCSC(policy-mgr) /fabric # scope tag-mgmt
UCSC(policy-mgr) /fabric/tag-mgmt # show tag-type
Tag Type:
    Name                        Color      System Defined Multiple Restricted
    --------------------------- ---------- -------------- -------- ----------
    Adapter Driver for HCR      049fd9     Yes            Yes      Yes
    Basic                       5bc0de     Yes            Yes      No
    Geographic                  5bc0de     No             Yes      No
    Maintenance Group           049fd9     Yes            No       Yes
    Operating System for HCR    049fd9     Yes            No       Yes
UCSC(policy-mgr) /fabric/tag-mgmt # scope tag-type 'Maintenance Group'
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # show tag-item
Tag Item:
    Value
    -----
    tag1
    tag2
    tag3
    tag4
```



CHAPTER 5

License Management

Overview

Cisco Smart licensing is simple, flexible and a smart way of procuring, deploying and managing licenses in your environment. For more information on smart licensing, see http://www.cisco.com/web/ordering/smart-software-licensing/index.html

You can have smart licensing and traditional licensing in your system at the same time. But only one type of licensing can be active. The following table describes the differences between traditional and smart licensing:

Traditional Licensing	Smart Licensing
Licenses are associated with registered domains.	Dynamic licensing. Licenses are associated with products and transferable within the virtual account.
You must obtain a license and manually download and install it on each device in Cisco UCS Central.	No license installation is necessary. The device initiates an HTTPS call home session and requests the licenses that it is configured to use.
Licenses are associated with specific domains.	License pools are account-specific. Any device in your company can use them.
Licenses are not easily transferable from one device to another.	Licenses can be transferred between product instances without any software installation. You can transfer unused licenses from one virtual account to another.

Smart Licensing

Smart licenses are server based licenses. You will purchase, deploy and track licenses for servers instead of domains. Instead of registering individual products with license files or PAKs, Smart Licensing provides the option to create a pool of licenses that can be used across your company's portfolio.

Smart licensing uses Virtual Accounts, Product Instances and Registration Tokens to procure, deploy and manage licenses in your environment.

Virtual Accounts

Virtual accounts are collections of licenses and product instances. You can create virtual accounts in Cisco Smart Software Manager to organize the licenses for your company into logical entities. You can use virtual accounts to organize licenses by business unit, product type, IT group, or whatever makes sense for your organization. For example, if you segregate your company into different geographic regions, you can create a virtual account for each region to hold the licenses and product instances for that region.

All new licenses and product instances are placed in a virtual account. You choose the virtual account when you register a product instance. You can transfer existing licenses or product instances from one virtual account to another.

For more information on creating virtual accounts in Cisco Smart Software Manager, see http://www.cisco.com/web/ordering/smart-software-manager/docs/smart-software-manager-user-guide.pdf.

Product Instances

A Cisco UCS Central product instance has a unique device identifier (UDI) that is registered using a product instance registration token. You can register several instances of a product with a single registration token. Each product instance can have one or more licenses that reside in the same virtual account.

Registration Tokens

Registration tokens are stored in the Product Instance Registration Token Table that is associated with your smart account. After you enable Smart Licensing in Cisco UCS Central, you can generate a new token in a virtual account on the Smart Software Licensing portal to register in Cisco UCS Central.

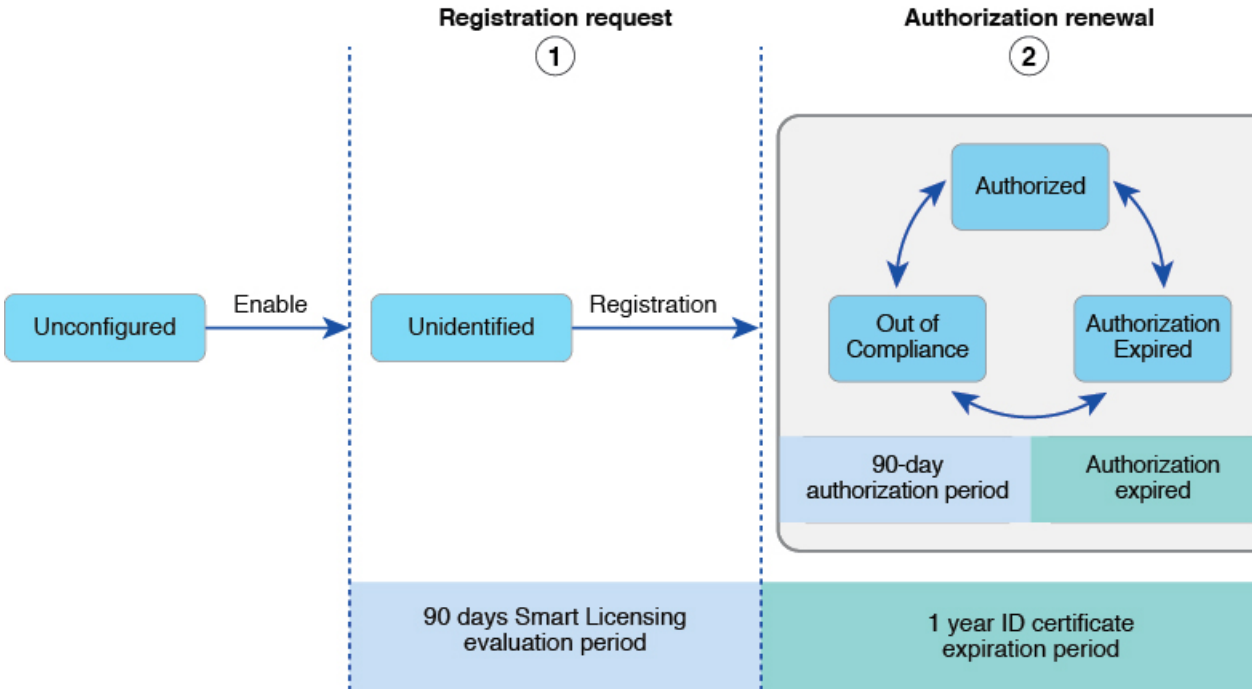
For more information on creating virtual accounts in Cisco Smart Software Manager, see http://www.cisco.com/web/ordering/smart-software-manager/docs/smart-software-manager-user-guide.pdf.

Obtaining Licenses

To obtain licenses using smart licensing, you will have to do the following:

- Generate tokens in Cisco Smart Software Manager virtual accounts.
- Register licenses for product instances in Cisco UCS Central.

The following illustrations explains the smart licensing process:



1	**Registration request**	The Smart Licensing 90-evaluation period starts when the product instance begins using the licensing feature. It not renewable. When the evaluation period expires, the agent sends a notification to the platform.
2	**Authorization renewal**	Authorization requests can result in an **Authorized** or **Out of Compliance (OOC)** response, or in an error due to a communication failure. Authorization periods are renewed every 30 days as long as authorization requests return **Authorized** or **Out of Compliance (OOC)** responses. When the authorization period expires, the agent continues to retry renewal with authorization requests. If successful, a new authorization period starts. If ID cert renewal (authorization renewal) fails, the product instance moves to an Unidentified state and begins consuming the evaluation period.

Enabling Smart Licensing

Before you begin

You must enable Smart Call Home before you can enable Smart Licensing. See Configuring Smart Call Home Using the CLI for more information.

Procedure

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

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)# **scope org**	Enters into the organization.
Step 3	UCSC (policy-mgr) /org # **scope device-profile**	Enters device profile mode.
Step 4	UCSC (policy-mgr) # **scope smart-license**	Enters Smart License mode.
Step 5	UCSC (policy-mgr) /smart-license # **set smart-license** *enable*	Enables Smart Licensing.
Step 6	UCSC (policy-mgr) /smart-license* # **commit-buffer**	Commits the transaction to the system configuration.

Step 7	UCSC (policy-mgr) /smart-license # **show smart-license**	Shows the smart license status. For example:
		`Smart License Status`
		`====================`
		`Smart License: Enable`

Example

This example shows how to enable Smart Licensing.

```
UCSC # connect policy-manager
UCSC(policy-mgr) # scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope smart-license
UCSC(policy-mgr) /org/device-profile/smart-license # set smart-license enable
UCSC(policy-mgr) /org/device-profile/smart-license* # commit-buffer
UCSC(policy-mgr) /org/device-profile/smart-license # show smart-license
```

Disabling Smart Licensing

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters resource manager mode.
Step 2	UCSC (policy-mgr)# **scope org**	Enters into the organization.
Step 3	UCSC (policy-mgr) /org/device-profile # **scope device-profile**	Enters device profile mode.
Step 4	UCSC (policy-mgr) /org/device-profile # **scope smart-license**	Enters Smart License mode.
Step 5	UCSC (policy-mgr) /org/device-profile/smart-license # **set smart-license** *disable*	Disables Smart Licensing.
Step 6	UCSC (policy-mgr) /org/device-profile/smart-license* # **commit-buffer**	Commits the transaction to the system configuration.

	Command or Action	Purpose

Step 7	UCSC (policy-mgr) /org/device-profile/smart-license #**show smart-license**	Shows the smart license status. For example:
		`Smart License Status`
		`==========`
		`Smart License: Disable`

Example

This example shows how to disable Smart Licensing.

```
UCSC # connect policy-manager
UCSC(policy-mgr)# scope org
UCSC(policy-mgr)/org # scope device-profile
UCSC(policy-mgr)/org/device-profile # scope smart-license
UCSC(policy-mgr)/org/device-profile/smart-license # set smart-license disable
UCSC(policy-mgr)/org/device-profile/smart-license* # commit-buffer
UCSC(policy-mgr)/org/device-profile/smart-license # show smart-license
```

Registering an ID Token

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope smart-license**	Enters smart license mode.
Step 3	UCSC (resource-mgr) /smart-license # **register-idtoken** *ID token*	Registers an ID token.
Step 4	UCSC (resource-mgr) /smart-license* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to register an ID token:

```
UCSC # connect resource-mgr
UCSC(resource-mgr)# scope smart-license
UCSC(resource-mgr) /smart-license # register-idtoken
UCSC(resource-mgr) /smart-license* # commit-buffer
```

Refreshing the License Server State

The system automatically updates the Authorization state from the License Server daily. When the Authorization state is Eval, you have the option of manually receiving the Authorization state from the Smart License server. With the following commands, you can check the time remaining in the Eval period.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope smart-license**	Enters smart license mode.
Step 3	UCSC (resource-mgr) /smart-license # **refresh-state**	Refreshes the count of Smart License Server entitlements.
Step 4	UCSC (resource-mgr) /smart-license* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to refresh the license server state:

```
UCSC # connect resource-mgr
UCSC(resource-mgr)# scope smart-license
UCSC(resource-mgr)/smart-license # refresh-state
UCSC(resource-mgr)/smart-license* # commit-buffer
UCSC(resource-mgr)/smart-license #
```

Renewing an Entitlement (Authorization)

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope smart-license**	Enters smart license mode.
Step 3	UCSC (resource-mgr) /smart-license # **renew-entitlement**	Renews entitlement (authorization)
Step 4	UCSC (resource-mgr) /smart-license* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to renew an entitlement:

```
UCSC # connect resource-mgr
UCSC(resource-mgr)# scope smart-license
UCSC(resource-mgr)/smart-license # renew-entitlement
UCSC(resource-mgr)/smart-license* # commit-buffer
UCSC(resource-mgr)/smart-license #
```

Renewing an ID Certificate (Registration)

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope smart-license**	Enters smart license mode.
Step 3	UCSC (resource-mgr) /smart-license # **renew-id-certificate**	Renews an ID certificate (registration).
Step 4	UCSC (resource-mgr) /smart-license* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to renew an ID certificate:

```
UCSC # connect resource-mgr
UCSC(resource-mgr) # scope smart-license
UCSC(resource-mgr)/smart-license # renew-id-certificate
UCSC(resource-mgr)/smart-license* # commit-buffer
UCSC(resource-mgr)/smart-license* #
```

Deregistering Smart Licensing

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope smart-license**	Enters smart license mode.
Step 3	UCSC (resource-mgr) /smart-license # **deregister**	Deregisters Smart Licensing.
Step 4	UCSC (resource-mgr) /smart-license* # **commit-buffer**	Commits the transaction to the system configuration.

Step 5	UCSC (resource-mgr) /smart-license #**show license status**	Shows the smart license registration status. For example:
		`UCSC(resource-mgr) /smart license # show license status`
		`Smart Licensing Status`
		`==========`
		`Smart License: Enable`
		`Registration`
		`==========`
		`Registration Status: Not Registered <<<<`

Example

This example shows how to deregister smart-licensing:

```
UCSC # connect resource-mgr
UCSC(resource-mgr)# scope smart-license
UCSC(resource-mgr)/smart-license # deregister
UCSC(resource-mgr)/smart-license* # commit-buffer
UCSC(resource-mgr)/smart-license #
```

Traditional Licensing

Traditional PAK-based licensing uses domain-based licenses instead of the product-based license that Smart Licensing offers. You can manage domain licenses through the Cisco UCS Central GUI or CLI.

You have a 120 day grace period to evaluate Cisco UCS Central at no cost. The grace period is measured from the day you register your first Cisco UCS domain and is stored in the system. Unregistering a domain from the system does not reset the grace period. For example, if you register a domain, use 40 days of the grace period, and then 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 you have used 40 days.

You must obtain and install a valid domain license before the grace period expires. If you do not the system generates multiple faults as a reminder to procure a license.

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 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 the service registry mode.
Step 2	UCSC (service-reg) # **scope license**	Enters the licensing configuration mode.

	Command or Action	Purpose
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.

Example

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
```

Uninstalling a License

After a license file is cleared, the license count is automatically adjusted.

Before you begin

You can remove or clear a license file that is not in use.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect service-reg**	Enters service registration mode.
Step 2	UCSC (service-reg) # **scope license**	Enters licensing configuration mode.
Step 3	UCSC (service-reg) /license # **clear file** *license file name*	Uninstalls the specified license.

Example

This example shows how to clear a license.

```
UCSC # connect service-reg
UCSC (service-reg) # scope license
UCSC (service-reg) /license # clear file DOMAIN_REG_2.lic
UCSC (service-reg) /license* # commit-buffer
UCSC (service-reg) /license #
```

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.

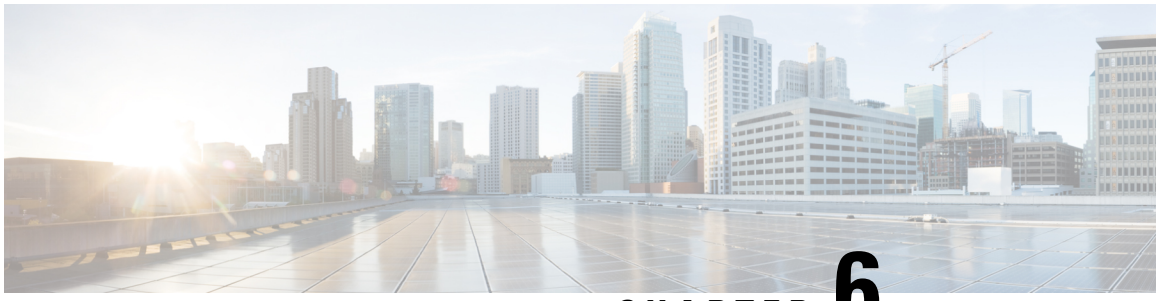
Procedure

	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.

Example

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 6

Domain Management

Cisco UCS Domains and Cisco UCS Central

Cisco UCS Central provides centralized management capabilities to multiple Cisco UCS domains across one or more data centers. Cisco UCS Central works with Cisco UCS Manager to provide a scalable management solution for a growing Cisco UCS environment.

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 using Cisco UCS Manager the same way you did before Cisco UCS Central. This also allows all existing third party integrations to continue to operate without change.

Registering Cisco UCS Domains

You can use a Fully Qualified Domain Name (FQDN) or IP address to register Cisco UCS domains in Cisco UCS Central.

To manage Cisco UCS Manager through Cisco UCS Central, you must register the Cisco UCS domains in Cisco UCS Central. You can register a Cisco UCS domain as a part of a domain group or as an ungrouped domain. When you have a domain group, all registered domains in the domain group can share common policies and other configurations.

Note During the initial registration process with Cisco UCS Central, all of the active Cisco UCS Manager GUI sessions are terminated.

Before registering a domain in Cisco UCS Central, do the following:

- Configure an NTP server and the correct time zone in both Cisco UCS Manager and Cisco UCS Central to ensure that they are in sync. If the time and date in the Cisco UCS domain and Cisco UCS Central are out of sync, the registration might fail.
- Obtain the hostname or IP address of Cisco UCS Central. You cannot use the same hostname for both Cisco UCS Central and Cisco UCS Manager. For standalone mode, use individual VM IP address.

- Obtain the shared secret that you configured when you deployed Cisco UCS Central.

Note

- Cisco recommends that you always register Cisco UCS domains using Cisco UCS Central's Fully Qualified Domain Name (FQDN). If domains are registered with FQDN, any change in the Cisco UCS Central IP address is transparent to the domain.
- If Cisco UCS Central is deployed on RHEL 7.2 KVM, the first time you register a Cisco UCS domain, you must regenerate the certificate using the **set regenerate yes** command.
- If the registered Cisco UCS domains have a latency of greater than 300ms for a round trip from Cisco UCS Central, there might be some performance implications for the Cisco UCS domains.
- When you unregister a Cisco UCS domain from Cisco UCS Central the global service profiles become local service profiles in Cisco UCS Manager.

  For more information about Changing Cisco UCS Central's IP address, see Changing Cisco UCS Central IP Address.

Warning You must upgrade to Cisco UCS Manager Release 2.1(2) or greater before registering with Cisco UCS Central. If you try to register earlier versions of Cisco UCS Manager, the registration will fail.

Registering a Cisco UCS Domain with the CLI

You can register a Cisco UCS Manager domain to any Cisco UCS Central system. However you can only register the Cisco UCS Manager domain to one Cisco UCS Central system at a time.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope system**	Enters into the system.
Step 3	UCSC(resource-mgr) /system # **create policy-control-ep** *UCSM domain IP address* admin	Creates a policy control for the UCSM domain. **Note** You must be logged in as an admin to register a domain.
Step 4	UCSC(resource-mgr) /system # Domain Admin Password: *password*	Specifies the password.
Step 5	UCSC(resource-mgr) /system/policy-control-ep # **set srcaddrfmt ipv4** { *hostname* | *ipv4* | *ipv6* }	Sets the address format for the domain.
Step 6	UCSC(resource-mgr) /system/policy-control-ep # **commit-buffer**	Commits the transaction to the system and registers the Cisco UCS Manager domain to Cisco UCS Central.

	Command or Action	Purpose
Step 7	UCSC(resource-mgr) /system/policy-control-ep # **show detail**	Displays the status of the Cisco UCS Manager domain.

Example

The following example shows how to register a Cisco UCS Manager domain with Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope system
UCSC(resource-mgr) /system # create policy-control-ep 10.193.01.01 admin
UCSC(resource-mgr) /system #  Domain Admin Password:
UCSC(resource-mgr) /system/policy-control-ep* #
UCSC(resource-mgr) /system/policy-control-ep # set srcaddrfmt ipv4
UCSC(resource-mgr) /system/policy-control-ep # commit-buffer
UCSC(resource-mgr) /system/policy-control-ep # show detail
hostname or ip address: 10.193.190.130
Registration Status: Registered
Cleanup Mode: Localize Global
Current Task:
```

Unregistering a Cisco UCS Domain with the CLI

Caution If you want to unregister any registered Cisco UCS domain in a production system, contact Cisco Technical Support.

When you unregister a Cisco UCS domain from Cisco UCS Central:

- You can no longer manage the service profiles, policies and other configuration for the Cisco UCS Domain from Cisco UCS Central
- All global service profiles and policies become local and continue to operate as local entities. When you re-register the domain, the service profiles and polices still remain local.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope system**	Enters into the system.
Step 3	UCSC(resource-mgr) /system # **scope policy-control-ep** *UCSM domain IP address*	Creates a policy control for the UCSM domain.
Step 4	UCSC(resource-mgr) /system/policy-control-ep # **set actionevent unregister**	Prepares to unregister the domain.

	Command or Action	Purpose
Step 5	UCSC(resource-mgr) /system/policy-control-ep # **commit-buffer**	Commits the transaction to the system and unregisters the Cisco UCS Manager domain from Cisco UCS Central.

Example

The following example shows how to unregister a Cisco UCS Manager domain with Cisco UCS Central:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope system
UCSC(resource-mgr) /system # scope policy-control-ep 10.193.01.01 admin
UCSC(resource-mgr) /system/policy-control-ep # set actionevent unregister
UCSC(resource-mgr) /system/policy-control-ep # commit-buffer
UCSC(resource-mgr) /system/policy-control-ep # show detail
hostname or ip address: 10.193.190.130
Registration Status: Failed
Cleanup Mode: Localize Global
Current Task:
```

Domains and Domain Groups

When you register a Cisco UCS Manager instance in Cisco UCS Central, that instance becomes an ungrouped domain in Cisco UCS Central. You must assign this domain to a domain group to start managing this domain using global policies in Cisco UCS Central.

Cisco UCS Central creates a hierarchy of Cisco UCS domain groups for managing multiple Cisco UCS domains.

- **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 is automatically be placed under the domain group specified in the policy. If not, it is placed in the ungrouped domains category until the domain group is assigned to a domain group.

You can only assign each Cisco UCS domain 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 automatically inherits 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 avoids 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 protects 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.

Example

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.

Example

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 information for the registered domains.
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** *Domain Group Name*	Specifies the domain group for the IP address.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-membership # **commit-buffer**	Commits the transaction to the system.

Example

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
    ---------------- ------------------ ---------------
    10.193.01.01     Manual             domaingroup-root
UCSC(resource-mgr) /domain-mgmt # scope ucs-membership 10.193.01.01
UCSC(resource-mgr) /domain-mgmt/ucs-membership # set domain-group DG-test
UCSC(resource-mgr) /domain-mgmt/ucs-membership #
```

Domain Group Qualification Policy

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

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

Example

This following example shows how to create a qualifier:

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

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.

Example

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.

Example

The following example shows how to create a registration policy:

```
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 #
```

Policies in Cisco UCS Central and Cisco UCS Domains

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

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

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

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

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

Policy Resolution between Cisco UCS Manager and Cisco UCS Central

Policy Resolution Control

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:

Note The policy resolution options in Cisco UCS Central are not supported on all versions of Cisco UCS Manager. If your Cisco UCS Manager version is earlier than the earliest supported release, the policy resolution screen may display the value as global even if it is not applicable.

In a case where you choose certain policies to be resolved locally using the Policy Resolution Control feature in Cisco UCS Central, or when a Cisco UCS Domain is unregistered from Cisco UCS Central, the global settings/unnamed policies (such as QoS Settings, Discovery policies) stay as previously configured. You must manually change the policy details to the desired state.

Caution Unregistering a Cisco UCS Domain has serious implications. You must not unregister the Cisco UCS Domain unless you choose to permanently not manage it from Cisco UCS Central.

Name	Earliest Supported Release	Description
Infrastructure & Catalog Firmware	2.1(2)	Determines whether the Capability Catalog and infrastructure firmware policy are defined locally in Cisco UCS Manager or come from Cisco UCS Central.
Time Zone Management	2.1(2)	Determines whether the time zone and NTP server settings are defined locally in Cisco UCS Manager or comes from Cisco UCS Central.
Communication Services	2.1(2)	Determines whether HTTP, CIM XML, Telnet, SNMP, web session limits, and Management Interfaces Monitoring Policy settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Global Fault Policy	2.1(2)	Determines whether the Global Fault Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
User Management	2.1(2)	Determines whether authentication and native domains, LDAP, RADIUS, TACACS+, trusted points, locales, and user roles are defined locally in Cisco UCS Manager or in Cisco UCS Central.
DNS Management	2.1(2)	Determines whether DNS servers are defined locally in Cisco UCS Manager or in Cisco UCS Central.
Backup & Export Policies	2.1(2)	Determines whether the Full State Backup Policy and All Configuration Export Policy are defined locally in Cisco UCS Manager or in Cisco UCS Central.

Name	Earliest Supported Release	Description
Monitoring	2.1(2)	Determines whether Call Home, Syslog, and TFTP Core Exporter settings are defined locally in Cisco UCS Manager or in Cisco UCS Central.
SEL Policy	2.1(2)	Determines whether the SEL Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Allocation Policy	2.1(2)	Determines whether the Power Allocation Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Power Policy	2.1(2)	Determines whether the Power Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Equipment Policy	2.2(7)	Determines whether the Equipment Policy is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Port Configuration	2.2(7)	Determines whether port configuration is defined locally in Cisco UCS Manager or in Cisco UCS Central.
Quality of Service (QoS) Configuration	2.2(7)	Determines whether QoS configuration is defined locally in Cisco UCS Manager or in Cisco UCS Central.

Policies

To assign a policy or a Management IP pool/policy to a domain profile, click on the policy and then click on the drop-down list to select the policy you want to assign to a profile. You can assign the following policies to a domain:

- **QoS System Class** - Defines a configurable set of system classes that you can include in a QoS Policy.
- **Port Auto-Discovery Policy**- Determines whether Server Port Auto-Discovery enabled or disabled in Cisco UCS Central.
- **Hardware Change Discovery Policy**- Determines if a hardware replacement deep discovery is triggered automatically, or after user acknowledgement from Cisco UCS Central.
- **KMIP Certification Policy** - KMIP Certification Policy enables using Self-Encrypting Drives (SEDs) through key management servers. This policy aims to generate a certificate that will be used by CIMC to communicate with KMIP server to get the key. You can configure this policy to a domain if it is created in a global scope.

Management IP

You can assign the following pools/policies from the **Management IP** pool:

- **Inband Policy** - Policy to configure the Inband IP address on a server directly, or through an Inband policy.
- **Outband Pool** - Sets the Management IP Pool created for Outband network management.

Note The **Management IP** tab in the **Domain Configuration Settings** window is enabled only when the registered Cisco UCS Domain is Cisco UCS Manager 3.1(3) and later. For all earlier Cisco UCS Manager releases, the Management IP tab is hidden.

Consequences of Policy Resolution Changes

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

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

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

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
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
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

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
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
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

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
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
Maintenance Policy Schedule Host Firmware Packs	N/A	Assigned domain group	See Consequences of Service Profile Changes on Policy Resolution, on page 25	See Consequences of Service Profile Changes on Policy Resolution, on page 25	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 25	See Consequences of Service Profile Changes on Policy Resolution, on page 25	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 25	See Consequences of Service Profile Changes on Policy Resolution, on page 25	Deletes remote policies	Converted to a local policy

Consequences of Service Profile Changes on Policy Resolution

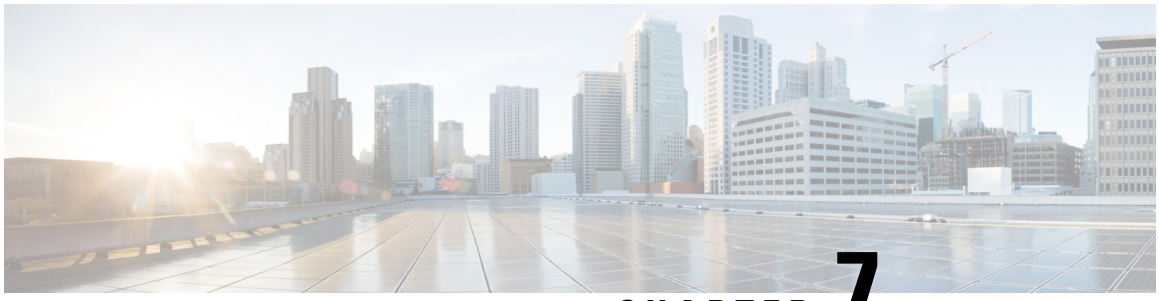
For certain policies, the policy resolution behavior is also affected by whether or not one or more service profiles that include that policy have been updated.

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

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

PART II

Administration



CHAPTER 7

User Management

This chapter includes the following sections:

Cisco UCS Central User Accounts

Access the system with user accounts. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each user account must have a unique username and password.

You can setup a user account with an SSH public key, in either of the two formats: OpenSSH or SECSH.

Admin Account

The Cisco UCS Central admin account is the default user account. You cannot modify or delete it. 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 can 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. Anyone with admin or aaa privileges can enable or disable it. Once you disable a local user account, the user cannot log in.

Note Cisco UCS Central does not delete configuration details for disabled local user accounts from 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 domains support 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

You can configure user accounts to expire at a predefined time. When the user account reaches the expiration time, the account disables.

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 to expire with the farthest 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

You cannot use the following words 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, Cisco recommends 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—Ensures that the users exist in the remote authentication server with the appropriate roles and privileges.
- Multitenancy with organizations—Creates 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—Obtains the SSH key.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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, Cisco UCS Central does not delete the configuration from the database. It prevents the user 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	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set firstname** *first-name*	Specifies the first name of the user.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set lastname** *last-name*	Specifies the last name of the user.

	Command or Action	Purpose
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set expiration** *month day-of-month year*	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. However, you can configure the account to use the latest expiration date available.
Step 11	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set email** *email-addr*	Specifies the user e-mail address.
Step 12	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set phone** phone-num	Specifies the user phone number.
Step 13	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set sshkey** *ssh-key*	Specifies the SSH key used for passwordless access.
Step 14	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Creates the user account named kikipopo
- Enables the user account
- Sets the password to foo12345
- 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 kikipopo
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
- 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
AAAAB3NzaC1yc2EAAAA
BIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4
VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8="
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 hpotter
- Enables the user account,
- Sets a Secure SSH key for passwordless access
- 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 hpotter
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 #
```

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 org /**	Enters the organization root.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Deletes the local-user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the foo user account
- 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 # delete local-user foo
UCSC(policy-mgr) /org/device-profile/security* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security #
```

Enabling the Password Strength Check for Locally Authenticated Users

You must have privileges to enable the password strength check. If enabled, 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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 password-profile**.	Specifies whether the password strength check is enabled or disabled.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set enforce-strong-password** {**yes** | **no**}	Specifies whether the password strength check is enabled or disabled.
Step 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Enables the password strength check
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set enforce-strong-password
 yes
UCSC(policy-mgr) /org/device-profile/security/password-profile # commit-buffer
```

Clearing the Password History for a Locally Authenticated User

You must have admin, aaa, or org/device-profile-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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Commits the transaction.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **scope password-profile**	Enters password profile security mode.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/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 8	UCSC(policy-mgr) /org/device-profile/security/password-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Clears the password history count for the user account named kikipopo
- 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 # scope local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set history-count 0
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Enabling or Disabling a User Account

You must have 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 org**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user**	Enters local-user security mode.

	Command or Action	Purpose
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.

Example

The following example:

- Enables a local user account called accounting
- 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 # scope local-user accounting
UCSC(policy-mgr) /org/device-profile/security/local-user # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user # commit-buffer
```

Web Session Limits for User Accounts

Cisco UCS Manager uses web session limits to restrict the number of web sessions (both GUI and XML) that a given user account is permitted to access at any one time.

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.

Example

The following example lists all of the 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. Cisco recommends that each user have a strong 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 you enabled the password strength check, each user must use a strong password.

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. Meaning, 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 the password change interval properties for all locally authenticated users of . You cannot specify a different password profile for locally authenticated users.

Password History Count

The password history count prevents locally authenticated users from reusing the same password. When you configure the password history count, stores up to a maximum of 15 previously used passwords. The password history count stores the passwords in reverse chronological order with the most recent password first. This ensures that the user can only reuse the oldest password when the history count reaches its threshold.

A user can create and use the number of passwords configured in the password history count before reusing a password. For example, if you set the password history count to 8, a user cannot reuse the first password until the ninth password expires.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously used passwords at any time.

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 restricts the number of password changes that a locally authenticated user can make within a specific number of hours. The following table describes the two interval configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	Does not allow changing passwords for locally authenticated user 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.	To prevent the user from changing passwords within 48 hours after a password change: • Set **Change during interval** to disable • Set **No change interval** to 48
Password changes allowed within change interval	Specifies the maximum number of times that a locally authenticated user password change can occur 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 two password changes within a 48-hour interval.	To allow a password change for a maximum of one time within 24 hours after a password change: • Set **Change during interval** to enable • Set **Change count** to 1 • Set **Change interval** to 24

Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin, aaa, or org/device-profile-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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/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 7	UCSC(policy-mgr) /org/device-profile/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.

	Command or Action	Purpose
		This value can be anywhere from 0 to 10.
Step 8	UCSC(policy-mgr) /org/device-profile/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 9	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enables the change during interval property
- Sets the change count to 5
- Sets the change interval to 72 hours
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set change-during-interval
 enable
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set change-count 5
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set change-interval 72
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Configuring a No Change Interval for Passwords

You must have admin, aaa, or org/device-profile-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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set change-during-interval disable**	Disables the change during interval feature.
Step 7	UCSC(policy-mgr) /org/device-profile/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 set to **Disable**.
Step 8	UCSC(policy-mgr) /org/device-profile/security/password-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Disables the change during interval property
- Sets the no change interval to 72 hours
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set change-during-interval
 disable
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set no-change-interval
72
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/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 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Configures the password history count
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set history-count 5
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Configuring User Roles

Role-Based Access Control Overview

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 a locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, you can manage individual user privileges by assigning the appropriate roles and locales.

A user is granted write access to the required 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 can update server configurations in the Engineering organization. They cannot, however, 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. You can assign one or more roles to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role 2 has server-related privileges, users with Role1 and Role 2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Any user roles configured after the first 48 are accepted, but they are 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.

You can create, modify or remove existing privileges, and delete roles. When you modify a role, the new privileges apply to all users with that role. Privilege assignment is not restricted to the privileges defined for the default roles. Meaning, 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. However, you can create a Server and Storage Administrator role that combines the privileges of both roles.

Note If you delete a role after it was assigned to users, it is also deleted from those user accounts.

Modify the user profiles on AAA servers (RADIUS or TACACS+) to add the roles corresponding to the privileges granted to that user. The attribute stores the role information. The AAA servers return this attribute with the request and parse it to obtain 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 remaining system.

Administrator

Complete read-and-write access to the entire system. Assigns this role to the default administrator account by default. You cannot change it.

Facility Manager

Read-and-write access to power management operations through the power management privilege. Read access to the remaining system.

Network Administrator

Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the remaining system.

Operations

Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the remaining 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 remaining system.

Server Profile Administrator

Read-and-write access to logical server-related operations. Read access to the remaining system.

Server Security Administrator

Read-and-write access to server security-related operations. Read access to the remaining system.

Storage Administrator

Read-and-write access to storage operations. Read access to the remaining system.

Reserved Words: User Roles

You cannot use the following words 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.

Tip Detailed information about these privileges and the tasks that they enable users to perform is available in *Privileges in Cisco UCS* available at the following URL: http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html.

Table 1: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	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

Privilege	Description	Default Role Assignment
server-policy	Server policy	Server Equipment Administrator
server-security	Server security	Server Security Administrator
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 endpoint 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

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 /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 role security mode.

	Command or Action	Purpose
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. You can also 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.

Example

The following example:

- Creates the service-profile-security-admin role
- Adds the service profile security to the role
- Adds the service profile security policy privileges to the role
- 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 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
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 # **delete role** *name*	Deletes the user role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the service-profile-security-admin role
- 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 # delete role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/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. You can also add privileges to the same role using multiple **add privilege** commands.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Adds the server security to the service-profile-security-admin role
- Adds the server policy privileges to the service-profile-security-admin role
- 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 # scope role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # add privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **set privilege** *privilege-name*	Replaces the existing privileges of the user role.

	Command or Action	Purpose
		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 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Replaces the existing privileges for the service-profile-security-admin role with server security
- Replaces the existing privileges for the service-profile-security-admin role with server policy privileges
- 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 # scope role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # set privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 # **scope role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/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. You can also remove privileges from the same role using multiple **remove privilege** commands.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Removes the server security from the service-profile-security-admin role
- Removes the server policy privileges from the service-profile-security-admin role
- 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 # scope role
UCSC(policy-mgr) /org/device-profile/security/role # remove privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **create role** *role-name*	Assigns the specified role to the user account. **Note** You can enter the **create role** command multiple times to assign more than one role to a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Assigns the operations role to the kikipopo local user account
- 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 # scope local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # create role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **delete role** *role-name*	Removes the specified role from the user account. **Note** You can enter the **delete role** command multiple times to remove more than one role from a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Removes the operations role from the kikipopo local user account
- Commits the transaction

```
CSC # 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 local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # delete role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```

Configuring User Locales

User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. Access is usually limited to the organizations specified in the locale. An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised.

Users with admin or aaa privileges can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization, a user assigned to that locale can only assign the Engineering organization to other users.

Note You cannot assign a locale to users with one or more of the following privileges:

- aaa
- admin
- fault
- operations

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations below 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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 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** org-root/org-*orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference. The *orgdn-name* argument is the distinguished name of the organization referenced.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates the finance organization for the western locale
- 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 locale western
UCSC(policy-mgr) /org/device-profile/security/locale* # create org-ref finance-ref orgdn
org-root/org-finance
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 locale** *locale-name*	Deletes the locale.
Step 6	UCSC(policy-mgr) /org/device-profile/security # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the western locale
- 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 # delete locale western
```

```
UCSC(policy-mgr) /org/device-profile/security* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC /security # **scope local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **create locale** *locale-name*	Assigns the specified locale to the user account. **Note** You can enter the **create locale** command multiple times to assign more than one locale to a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user # **commit-buffer**	Commits the transaction.

Example

The following example:

- Assigns the western locale to the kikipopo local user account
- 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/local-user # create locale western
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **delete locale** *locale-name*	Removes the specified locale from the user account. **Note** You can enter the **delete locale** command multiple times to remove more than one locale from a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Removes the western locale from the kikipopo local user account
- 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/ # scope local-user
UCSC(policy-mgr) /org/device-profile/security/local-user # delete locale western
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 locale** *locale-name*	Enters locale security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **create org-ref** *org-ref-name* **orgdn org-root/org-**_orgdn-name_	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference. The *orgdn-name* argument is the distinguished name of the organization referenced.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Adds (references) the marketing organization to the locale
- Names the reference marketing-ref
- 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 # scope locale western
UCSC(policy-mgr) /org/device-profile/security/locale # create org-ref marketing-ref orgdn
org-root/org-marketing
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 locale** *locale-name*	Enters security locale mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **delete org-ref** *org-ref-name*	Deletes the organization from the locale.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the finance organization from the western locale
- 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 # scope locale western
UCSC(policy-mgr) /org/device-profile/security/locale # delete org-ref finance-ref
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) #**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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) /domain-group/security # **scope locale** *locale-name*	Enters security locale mode.
Step 6	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. The *domain-group-dn-name* argument is the distinguished name of the domain group root referenced.
Step 7	UCSC(policy-mgr) /domain-group/security/locale # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Adds (references) the marketing domain group to the locale
- Names the reference marketdomain01-ref
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
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 domaingroup-root/domaingroup-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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 locale** *locale-name*	Enters security locale mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **delete domain-group-ref** *domain-group-ref-name*	Deletes references (unbinds) domain groups referenced to the locale. The *domaingroup-ref* argument (1-16 characters) is the name used to identify the domain group reference.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Deletes references (unbinds) the marketing domain group references from the locale marketdomain01
- 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 # scope locale western
UCSC(policy-mgr) /org/device-profile/security/locale # delete domain-group-ref marketdomain01
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 sub-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.

Example

The following example:

- Creates the central-audit domain group
- 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 sub-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 domain-group** *name*	Deletes the domain group.
Step 4	UCSC(policy-mgr) /domain-group * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the central-audit domain group
- 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.

Example

The following example:

- Creates the central-audit organization
- 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.

Example

The following example:

- Deletes the central-audit organization
- 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.

Example

The following example:

- Enters the central-audit organization
- Creates the north-audit sub-organization
- 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

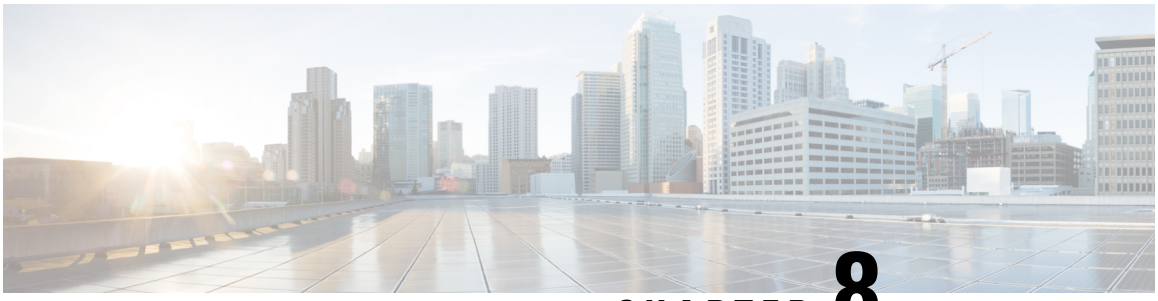
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete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

Example

The following example:

- Enters the central-audit organization
- Deletes the north-audit sub-organization
- 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 #
```



CHAPTER 8

System Management

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 sub-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.

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

Example

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 sub-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.

Example

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 sub-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).

Example

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 sub-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 # **show psu-policy**	Enters the power policy mode.

Example

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 #
```

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 sub-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.

Example

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 sub-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.

Example

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 sub-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.

Example

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 sub-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.

Example

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 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 sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **scope dns-config**	If scoping into the domain group root previously, scopes the default DNS policy's configuration mode from the Domain Group root.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **create dns-config**	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.

Example

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
- 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.

Example

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 sub-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 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.

Example

The following example shows how to:

- Scope into the domain group root
- Create a DNS server instance named 0.0.0.0
- 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
- 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 sub-domain group under the domain

	Command or Action	Purpose
		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.

Example

The following example shows how to:

- Scope into the domain group root
- Delete the DNS server instance named 0.0.0.0
- 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 the DNS server instance named 0.0.0.0
- 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 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 sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create domain-group** *domain-group*	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	(Optional) UCSC(policy-mgr) /domain-group* # **commit-buffer**	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	(Optional) UCSC(policy-mgr) /domain-group # **create timezone-ntp-config**	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	(Optional) UCSC(policy-mgr) /domain-group* # **scope timezone-ntp-config**	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

	Command or Action	Purpose
		• **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.

Example

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")
- 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 in 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")
- 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 into domaingroup01 in 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")
- 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.

Example

The following example shows how to:

- Scope the domain group domaingroup01

- Delete that domain group's date and time policy
- 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
- Recover from an error message (leaving the buffer in an unrecoverable uncommitted state) by initiating a clean exit and reconnecting to the 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 sub-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.

	Command or Action	Purpose
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.

Example

The following example shows how to:

- Scope into the domain group root
- Create an NTP server instance named domaingroupNTP01
- 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 into the domain group domaingroup01 under the domain group root
- Create an NTP server instance named domaingroupNTP01
- 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 sub-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.

Example

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
- 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 #
```

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.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-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.

Example

The following example shows how to delete the NTP server instance domaingroupNTP01:

```
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 delete the NTP server instance domaingroupNTP01:

```
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 #
```

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

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 sub-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

	Command or Action	Purpose
		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	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **enable on-next-boot**	Choose whether to apply the changes on the next reboot, and ignore the selection in the **reboot-policy**.
Step 6	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **disable on-next-boot**	Disables the **on-next-boot** option.
Step 7	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **set scheduler** *scheduler-name*	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 8	(Optional) UCSC(policy-mgr) /domain-group/maint-policy # **set scheduler** *scheduler-name*	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 9	UCSC(policy-mgr) /domain-group/maint-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Scope into the Domain group root
- Create a maintenance policy called MaintPol1
- Set the system to reboot immediately when a service profile is associated with a server
- 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.

Example

The following example shows how to delete a maintenance policy called maintenance:

```
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 #
```

System Event Log

Cisco UCS Central supports a global system event log (SEL) policy.

The system event log (SEL) 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.

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 sub-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	(Optional) UCSC(policy-mgr) /domain-group/ep-log-policy # **set description** *description*	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,

	Command or Action	Purpose
		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* **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.

Example

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
- Clear the system event log after a backup operation occurs
- 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 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 sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create tftp-core-export-config**	Creates a TFTP Core Export Debug policy if it does not exist, then scopes into the policy.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope tftp-core-export-config**	Scopes an existing TFTP Core Export Debug policy's configuration mode.
Step 5	UCSC(policy-mgr) /domain-group/tftp-core-export-config* # **enable core-export-target**	Enables the TFTP core export target.

	Command or Action	Purpose
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.
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.

Example

The following example shows how to:

- Scope into the domain group domaingroup01
- Create the TFTP Core Export Policy
- Configure the policy
- 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 #
```

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. The Core File Exporter provides system monitoring and automatic export of core files to be included in TAC cases.

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 sub-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 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.

Example

The following example shows how to delete the TFTP core export debug policy:

```
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 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.

Example

The following example shows how to create the Syslog Console debug policy:

```
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 sub-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 syslog**	Deletes the Syslog Debug policy.
Step 4	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete the Syslog debug policy:

```
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 sub-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.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

Example

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
- 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

Disable a syslog console debug policy from a sub-domain group. You cannot disable syslog console debug policies under the Domain Group root.

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 sub-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.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/syslog/console* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable the Syslog Console debug policy:

```
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 sub-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 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).

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /domain-group/syslog/monitor* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to configure the Syslog Monitor debug policy:

```
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

Disable a syslog monitor debug policy from a domain group under the Domain Group root. You cannot disable a syslog monitor debug policies under the Domain Group root.

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 sub-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 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.

Example

The following example shows how to disable the policy:

```
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 sub-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.
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

	Command or Action	Purpose
		• 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.
Step 7	UCSC(policy-mgr) /domain-group/syslog/remote-destination* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to configure the Syslog Remote Destination Debug policy:

```
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 hostname 02
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility authpriv 3
UCSC(policy-mgr) /domain-group/syslog/remote-destination* # set facility authpriv hostname
 02
  *** 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 sub-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.

Example

The following example shows how to disable the Syslog Remote Destination debug policy:

```
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* # 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 sub-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.

Example

The following example shows how to configure the Syslog Source Debug policy:

```
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

Delete a syslog source debug policy from a sub-domain group of domain group root. You cannot delete syslog source debug policies under the domain groups root.

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 sub-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.

	Command or Action	Purpose
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.

Example

The following example shows how to disable the Syslog Source Debug policy

```
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.
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-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),

	Command or Action	Purpose
		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.

Example

The following example shows how to configure the Syslog Logfile debug policy:

```
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* # 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

Disable a syslog logfile debug policy from a domain group under the domain group root. You cannot diable syslog logfile debug policies under the domain groups root.

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 sub-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.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/syslog/file* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to disable the Syslog LogFile debug policy:

```
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 #
```

Enabling Tomcat Logging

Use a terminal emulator to access the CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **scope monitoring**	Enters monitoring mode.
Step 2	UCSC /monitoring # **scope sysdebug**	Enters sysdebug mode.
Step 3	UCSC /monitoring/sysdebug # **scope mgmt-logging**	Enters management logging mode.
Step 4	UCSC /monitoring/sysdebug/mgmt-logging # **set module tomcat_config** [**crit** | **debug0** | **debug1** | **debug2** | **debug3** | **debug4** | **info** | **major** | **minor** | **warn**]	Sets the logging level.
Step 5	UCSC /monitoring/sysdebug/mgmt-logging # **commit-buffer**	Commits the change.

Example

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

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

Managing High Availability

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 Cisco UCS Central cluster communicates with Cisco UCS Manager.

- Both VMs must be configured on IP addresses that belongs to the same subnet.
- For NFS, you should configure an NTP server on the NFS server to ensure that the time of both VMs is always synced to Cisco UCS Central.
- 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.

Example

The following example shows how to view the state of a cluster where A is the primary and B the subordinate:

```
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**	Displays the extended state of the cluster.

Example

The following example shows how to view the extended state of a cluster, where A is the primary and B the subordinate:

```
UCSC# show cluster extended-state
Cluster Id: 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
```

Changing the Cluster Lead

Use this command to designate a cluster leader.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect local-mgmt**	Enters local management mode.
Step 2	UCSC(local-mgmt)# **cluster lead** {**a** | **b**}	Change the cluster lead to the specified fabric interconnect. **Note** When the cluster lead changes, the VIP connection will be disconnected. You should log in again to the VIP address, and ensure that it now references the -B node.

Example

The following example shows how to view the primary, change the cluster lead to fabric interconnect B, and verify the result:

```
UCSC-A# show cluster state
Cluster Id: 0x1efd4e4ea47511e5-0x94961118a1af3b76

A: UP, PRIMARY
B: UP, SUBORDINATE

HA NOT READY
No device connected to this VM

UCSC-A# connect local-mgmt
UCSC-A(local-mgmt)# cluster lead b
Cluster Id:0x1efd4e4ea47511e5-0x94961118a1af3b76
UCSC-A(local-mgmt)#
```

After the VIP disconnects, log back in to verify the primary is now fabric interconnect B.

```
UCSC-B# show cluster state
Cluster Id: 0x1efd4e4ea47511e5-0x94961118a1af3b76

B: UP, PRIMARY
A: UP, SUBORDINATE

HA NOT READY
No device connected to this VM

UCSC-B#
```

Force a FI to be Primary

This command forces the secondary FI to be primary. This can be used when the primary FI has failed or remains in Election in Progress state.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect local-mgmt**	Enters local management mode.
Step 2	UCSC(local-mgmt)# **cluster force primary**	Forces the current FI to be the primary.

Example

The following example shows how to use the cluster force primary command:

```
UCSC-A# connect local-mgmt
UCSC-A(local-mgmt)# cluster force primary
Cluster Id:0x1efd4e4ea47511e5-0x94961118a1af3b76

UCSC-A(local-mgmt)#
```

Viewing a Network Interface

Procedure

	Command or Action	Purpose
Step 1	UCSC # **show network-interface**	Displays the network interface information of a cluster.

Example

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.

Example

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.

Example

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.

Example

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

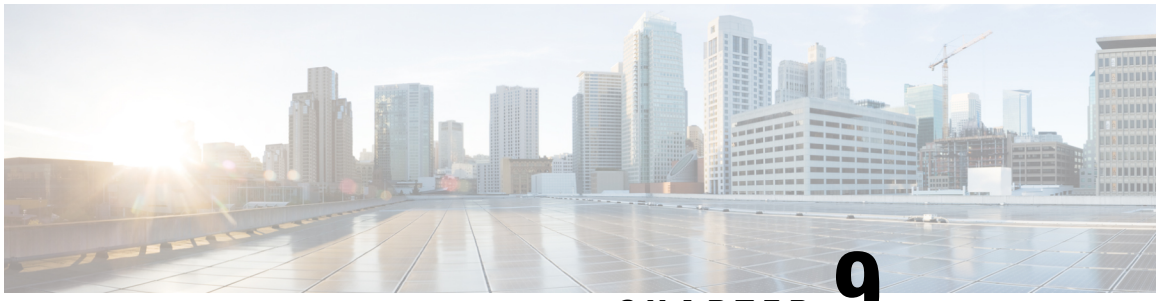
Procedure

	Command or Action	Purpose
Step 1	UCSC # **show system detail**	Displays the system details about the cluster.

Example

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 9

Image Library

Image Library

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

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

Use the firmware images when creating firmware policies.

In the Image Library, you can:

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

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

- Schedule Periodic Firmware Image Synchronizations

- Sync firmware images with images on Cisco.com
- Import Firmware Bundles (or Service Packs)
- For more information on downloading images, see Downloading Firmware from Cisco.com , on page 146.

Downloading Firmware from Cisco.com

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

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

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

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

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

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

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

Setting Up the Cisco.Com Account

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

Important You must accept the EULA and K9 agreements when creating a Cisco.com account. However, EULA and K9 are not supported through the CLI. You must go to the GUI and accept them.

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 sub-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 connection-policy cisco**	Enters the connection policy mode for cisco.com.
Step 4	UCSC(policy-mgr) /domain-group/connection-policy # **set username** *username*	Enters the username for your cisco.com account
Step 5	UCSC(policy-mgr) /domain-group/connection-policy # **set password**	Enters the password for your cisco.com account. Password:
Step 6	Enter your cisco.com password.	
Step 7	(Optional) UCSC(policy-mgr) /domain-group/connection-policy # **set http-proxy** *IP address of proxy server| proxy URL*	Enables your system to access Cisco.com through an HTTP proxy server. **Note** This functionality requires that Cisco UCS Central has network access to Cisco.com.
Step 8	(Optional) UCSC(policy-mgr) /domain-group/connection-policy # **set proxy-username** *proxy username*	Enters your username for the HTTP proxy server.
Step 9	(Optional) UCSC(policy-mgr) /domain-group/connection-policy # **set proxy-password**	Enters your password for the HTTP proxy server. Password:
Step 10	(Optional) Enter your proxy server password.	
Step 11	UCSC(policy-mgr) /domain-group/fw-autosync-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a cisco.com account:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group BayArea
UCSC(policy-mgr) /domain-group # scope connection-policy cisco
UCSC(policy-mgr) /domain-group/connection-policy # set username mdixon
UCSC(policy-mgr) /domain-group/connection-policy # set password
Password: password
UCSC(policy-mgr) /domain-group/connection-policy* # set http-proxy 10.193.200.100
UCSC(policy-mgr) /domain-group/connection-policy* # set proxy-username mdixon
UCSC(policy-mgr) /domain-group/connection-policy* # set proxy-password
HTTP Proxy Password: proxy password
UCSC(policy-mgr) /domain-group/connection-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/connection-policy #
```

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 sub-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**	**a.** **set admin-state** enabled | disabled **Note** Admin state is mandatory. **b.** **set downloadinterval** day | week | on-demand **Note** Download interval is mandatory. **c.** **set eula-status** *yes* | *no* **Note** EULA status is mandatory. **d.** **set http-proxy** *server:port* **e.** **username** *username* **Note** Username is mandatory. **f.** **set password** *password* **Note** Password is mandatory.

	Command or Action	Purpose
		g. **set proxy-password** *password* **h.** **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.

Example

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

```
UCSC# connect operation-mgr
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.

Example

The following example shows how to download a 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
```

Deleting Images from the Firmware Library

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

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

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

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

Example

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. **Note** The classic UCS Infra bundle is not provided as an option for auto-install.

Example

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 #
```

Downloading a Firmware Image

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** ftp | scp | sftp | tftp | *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.

Example

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

You can only purge metadata through the CLI.

Procedure

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

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

Example

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

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

Periodic Firmware Synchronization

You can use the firmware auto-sync policy to determine whether firmware versions on recently discovered servers must be upgraded or not. With this policy, you can upgrade the firmware versions of recently discovered unassociated servers to match the firmware version defined in the default host firmware pack. In addition, you can determine if the firmware upgrade process should run immediately after the server is discovered or run at a later time.

Important The firmware automatic synchronization is dependent on the default host firmware pack. If you delete the default host firmware pack, it triggers a major fault. If you have configured a default host firmware pack, but not specified or configured a blade or rack server firmware in it, then it triggers a minor fault. Irrespective of the severity of the fault raised, you must resolve these faults prior to setting the **Firmware Auto Sync Server policy**.

Following are the values for the **Firmware Auto Sync Server policy**:

- **No Action**—No firmware upgrade is initiated on the server.

  This value is selected by default.

- **User Acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the upgrade in the **Pending Activities** dialog box.

The firmware for a server is automatically triggered when the following conditions occur:

- The firmware version on a server, or the endpoint on a server, differs from the firmware version configured in the default host firmware pack.
- The value for the firmware auto-sync policy has been modified.

Setting the Firmware Auto-Sync Policy

Use this policy to determine when and how you must update the firmware version of a recently discovered, unassociated server so that it matches with the firmware version of the default host firmware pack.

If the firmware version of a specific endpoint of a server differs from the version in the default host firmware pack, the FSM state displays the update status for that specific endpoint only. The firmware version of the server is not updated.

Before you begin

- You must create a default host firmware pack before setting this policy.
- You must log in as an administrator to complete this task.

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 sub-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-autosync-policy**	Enters the firmware auto synchronization policy mode.
Step 4	UCSC(policy-mgr) /domain-group/fw-autosync-policy # **set auto-sync** {**no-actions** | **user-acknowledge**}	Choose one of the following values: • **user-acknowledge**—Firmware on the server is not synchronized until the administrator acknowledges the discovered server in the server command mode. • **no-actions**—No firmware upgrade is initiated on the server.
Step 5	UCSC(policy-mgr) /domain-group/fw-autosync-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to set the firmware autosync policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope fw-autosync-policy
UCSC(policy-mgr) /domain-group/fw-autosync-policy # set auto-sync user-acknowledge
UCSC(policy-mgr) /domain-group/fw-autosync-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/fw-autosync-policy #
```

What to do next

If you set the value to User Acknowledge, then you must acknowledge the pending activity for the server for the firmware synchronization to occur.

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 org** *org-name*	Enters the organizations mode for the specified organization. To enter the root mode type/ as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create fw-host-pack***policy name*	Creates the specified host firmware pack.
Step 4	UCSC(policy-mgr) /org/fw-host-pack # **set descr** *description*	Specifies the description for the host firmware policy.
Step 5	UCSC(policy-mgr) /org/fw-host-pack # **set bladebundleversion** *version number*	Specifies the blade server bundle version for the host firmware policy.
Step 6	UCSC(policy-mgr) /org/fw-host-pack # **set rackbundleversion** *version number*	Specifies the rack server bundle version for the host firmware policy.
Step 7	UCSC(policy-mgr) /org/fw-host-pack #**create exclude-server-component** {**adapter** | **board-controller** | **cimc** | **flexflash-controller** | **graphics-card** | **host-hba** | **host-hba-optionrom** | **host-nic** | **host-nic-optionrom** | **local-disk** | **psu** | **raid-controller** | **sas-expander** | **server-bios**}	Creates an excluded component and enters exclude server component mode. **Note** You must repeat the **exclude-server-component** command for each component that you want to exclude from the host firmware package.
Step 8	UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component #**exit**	Returns to host firmware pack mode.
Step 9	UCSC(policy-mgr) /org/fw-host-pack # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to:

- Create a host firmware pack called FWPack1
- Add a blade server bundle version

- Exclude the psu and server-bios

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create fw-host-pack FWPack1
UCSC(policy-mgr) /org/fw-host-pack* # create exclude-server-component psu
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component* # exit
UCSC(policy-mgr) /org/fw-host-pack* # create exclude-server-component server-bios
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component* # commit-buffer
UCSC(policy-mgr) /org/fw-host-pack/exclude-server-component #
```

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 org**	Enters into the organization.
Step 3	UCSC(policy-mgr) /org # **show fw-host-pack detail**	Displays a list of host firmware packages.

Example

The following example shows how to display available host infrastructure firmware packages:

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

Acknowledging a Pending Activity

This procedure describes the process to acknowledge the start of a host firmware update from the Cisco UCS Central CLI.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters into the organization.
Step 3	UCSC(resource-mgr) /org # **show ucs-service-profile**	Displays the existing service profiles.
Step 4	UCSC(resource-mgr) /org # **scope ucs-service-profile***service-profile-name*	Enters the UCS service profile.
Step 5	UCSC(resource-mgr) /org/ucs-service-profile # **show instance**	Displays the instances in the service profile.
Step 6	UCSC(resource-mgr) /org/ucs-service-profile # **scope instance***instance-ID*	Scopes into the instance.
Step 7	UCSC(resource-mgr) /org/ucs-service-profile/instance # **show pending-changes**	Displays all pending activities for that service profile.
Step 8	UCSC(resource-mgr) /org/ucs-service-profile/instance # **apply pending-changes immediate**	Acknowledges all of pending activities.
Step 9	UCSC(resource-mgr) /org/ucs-service-profile/instance * # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to acknowledge a pending activity:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org
UCSC(resource-mgr) /org # show ucs-service-profile
Service Profiles deployed on UCS domain:
    Name                 Status               Ref Count Instantiation State
    -------------------- -------------------- --------- -------------------
    SP-1                 Ok                           1 Instantiated
```

```
    SPCSCuz56952         Ok                            1 Instantiated

UCSC(resource-mgr) /org # scope ucs-service-profile SP-1
UCSC(resource-mgr) /org/ucs-service-profile # show instance
Compute Instance:
    ID    Name             Status          Assoc State  Config State Physical Ref
    ----- ---------------- --------------- ------------ ------------ ------------
     1008 Dhana            Ok              Associated   Applied      SP-1/1008

UCSC(resource-mgr) /org/ucs-service-profile/ # scope instance 1008
UCSC(resource-mgr) /org/ucs-service-profile/instance # show pending-changes
Pending Changes:
    State                    Pending Changes       Pending Disruptions
    ------------------------ --------------------- -------------------
    Untriggered              0                     0

UCSC(resource-mgr) /org/ucs-service-profile/instance # apply pending-changes immediate
UCSC(resource-mgr) /org/ucs-service-profile/instance* # commit-buffer
```

Capability Catalog

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

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

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

Contents of the Capability Catalog

The contents of the Capability Catalog include the following:

Implementation-Specific Tunable Parameters

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

Hardware-Specific Rules

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

User Display Strings

- Part numbers, such as the CPN, PID/VID

- Component descriptions
- Physical layout/dimensions
- OEM information

Updates to the Capability Catalog

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

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

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

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

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 org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*.	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr)/org # **scope fw-catalog-pack-config** <*config-name*>	Enters the capability catalog packages mode.
Step 5	UCSC(policy-mgr) /org/fw-catalog-pack # **set catalogversion** <*catalogversion*>	Specifies the capability catalog version for this update.
Step 6	UCSC(policy-mgr) /org/fw-catalog-pack* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure a capability catalog update:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)* # scope org
UCSC policy-mgr) /org* # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile/ # scope fw-catalog-pack-config job50
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # set catalogversion 1.5
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config #
```

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 org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*.	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr)/org/domain-infra-profile # **scope fw-catalog-pack-config** *default*	Enters the capability catalog packages mode.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack # **show detail**	Specifies the capability catalog version for this update.

Example

The following example shows how to view the capability catalog:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)* # scope org
UCSC policy-mgr) /org* # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope fw-catalog-pack-config default
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # show detail
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config * #
```

Deleting a Capability Catalog Policy

Procedure

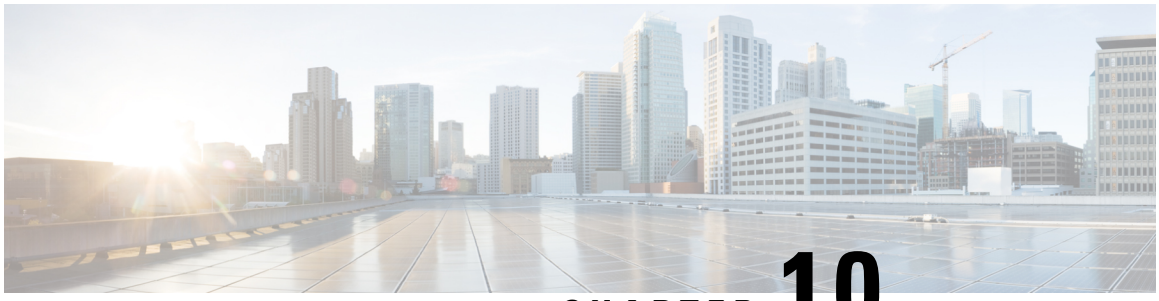
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) #**scope org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*.	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr) /domain-group # **delete fw-catalog-pack-config***name*	Deletes the specified catalog policy from the domain group.
Step 5	UCSC(policy-mgr) /domain-group* # **commit-buffer**	Commits the transaction to the system.

Example

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

```
UCSC# connect policy-mgr
UCSC(policy-mgr)* # scope org
UCSC policy-mgr) /org* # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope fw-catalog-pack-config config1
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # delete
fw-catalog-pack-config config1
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* #
```



CHAPTER 10

Firmware Management

Maintenance Groups

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

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

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

Creating a Domain Infrastructure Profile and Assigning a Tag

After you create tags, you can apply them to domains. Apply tags to domains through the GUI.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **create domain-infra-profile** *job-name*	Creates the infrastructure firmware policy mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/domain-infra-profile #**set tag-name** *tag-name*	Creates a tag.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile #**commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create a domain infrastructure profile and a maintenance group tag

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create domain-infra-profile batch1
UCSC(policy-mgr) /org/domain-infra-profile* # set tag-name Tag1
UCSC(policy-mgr) /org/domain-infra-profile* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile #
```

Viewing Tags

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope fabric**	Scopes into the fabric interconnect.
Step 3	UCSC(policy-mgr) /fabric # **scope tag-mgmt**	Scopes into tag management.
Step 4	UCSC(policy-mgr) /fabric/tag-mgmt # **show tag-type**	Displays all tag types.
Step 5	UCSC(policy-mgr) /fabric/tag-mgmt # **scope tag-type** '*tag-type*'	Scopes into a specific tag type.
Step 6	UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # **show tag-item**	Displays the values for the selected tag.

Example

The following example shows how to view maintenance group tags:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope fabric
UCSC(policy-mgr) /fabric # scope tag-mgmt
UCSC(policy-mgr) /fabric/tag-mgmt # show tag-type
Tag Type:
    Name                      Color      System Defined Multiple Restricted
    ------------------------- ---------- -------------- -------- ----------
    Adapter Driver for HCR    049fd9     Yes            Yes      Yes
```

```
    Basic                     5bc0de     Yes            Yes      No
    Geographic                5bc0de     No             Yes      No
    Maintenance Group         049fd9     Yes            No       Yes
    Operating System for HCR  049fd9     Yes            No       Yes
UCSC(policy-mgr) /fabric/tag-mgmt # scope tag-type 'Maintenance Group'
UCSC(policy-mgr) /fabric/tag-mgmt/tag-type # show tag-item
Tag Item:
    Value
    -----
    tag1
    tag2
    tag3
    tag4
```

Catalog Version for Firmware Updates

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

Setting the Catalog Version

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*	Enters the infrastructure firmware policy mode.
Step 4	UCSC(policy-mgr) /org/domain-infra-profile # **create fw-catalog-pack-config default**	Creates the firmware upgrade package.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # **set catalogversion** *catalogversion*	Specifies the infrastructure policy version for the update.
Step 6	(Optional) UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config # **set descr** *description*	Specifies a description for this infrastructure firmware pack.
Step 7	UCSC(policy-mgr) /org/domain-infra-profile/fw-infra-pack-config* #**commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to set the catalog version to v3.1(1e)T:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope domain-infra-profile batch1
UCSC(policy-mgr) /org/domain-infra-profile # create fw-catalog-pack-config default
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* # set catalogversion
3.1(1e)T
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* # set descr sanjose
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/fw-catalog-pack-config #
```

Setting Policy Control to Global

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

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope system**	Enters system mode.
Step 3	UCSC(resource-mgr) /system # **show policy-control-ep**	Displays local domains registered to this Cisco UCS Central system.
Step 4	UCSC(resource-mgr) /system # scope policy-control-ep *IP address of registered domain*	Enters the policy resolution control for the registered domain.
Step 5	UCSC(resource-mgr) /system/policy-control-ep # **set infra-pack-ctrl source** *local* | *global*	Sets the Infrastructure and Catalog firmware policy resolution control to local or global.
Step 6	UCSC(resource-mgr) /system/policy-control-ep * #**commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to set the catalog version to v3.1(1e)T:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope system
UCSC(resource-mgr) /system # show policy-control-ep

policy controlep:
    hostname or ip address
    ----------------------
```

```
    10.193.200.100

UCSC(resource-mgr) /system # scope policy-control-ep 10.193.200.100
UCSC(resource-mgr) /system/policy-control-ep # set infra-pack-ctrl source global
UCSC(resource-mgr) /system/policy-control-ep*# commit-buffer
UCSC(resource-mgr) /system/policy-control-ep #
```

Scheduling Infrastructure Firmware Updates for Cisco UCS Domains

You can manage all firmware upgrades for Cisco UCS domains from Cisco UCS Cental.

When you create the infrastructure firmware policy in Cisco UCS Central CLI, the system automatically creates a schedule for the policy. You can edit the automatic scheduled for **fw-infra** and **fi-reboot** to change the date and time.

Before you begin

You must create a domain infrastructure profile and a tag before you can schedule an update. See Creating a Domain Infrastructure Profile and Assigning a Tag for more information.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr) /org/domain-infra-profile* # **scope product-family** *ucs-classic* | *ucs-mini* | *ucs-classic-3gen*	Enters the specified product family mode in the maintenance group.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/product-family # **create fw-infra-pack-config** *job name*	Initiates the process to create infrastructure firmware policy.
Step 6	UCSC(policy-mgr) /org/domain-infra-profile/product-family/fw-infra-pack-config # **set** *infrabundleversion*	Specifies the infrastructure policy version for the update.
Step 7	(Optional) UCSC(policy-mgr) /org/domain-infra-profile/product-family/fw-infra-pack-config # **set** *description*	Specifies a description for this infrastructure firmware pack.
Step 8	UCSC(policy-mgr) /org/domain-infra-profile/product-family/fw-infra-pack-config* #**commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to schedule an infrastructure firmware update for a Cisco UCS Mini:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope domain-infra-profile batch1
UCSC(policy-mgr) /org/domain-infra-profile # scope product-family ucs-mini
UCSC(policy-mgr) /org/domain-infra-profile/product-family # create fw-infra-pack-config
default
UCSC(policy-mgr) /org/domain-infra-profile/product-family/fw-infra-pack-config* # set
infrabundleversion 3.1(1e)T
UCSC(policy-mgr) /org/domain-infra-profile/product-family/fw-infra-pack-config* # set descr
 sanjose
UCSC(policy-mgr) /org/domain-infra-profile/product-family/fw-infra-pack-config* #
commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/product-family/fw-infra-pack-config #
```

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 org**	Enters into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*	Enters the infrastructure firmware policy job that you created previously.
Step 4	UCSC(policy-mgr) /org/domain-infra-profile* # **scope product-family** *ucs-classic* | *ucs-mini* | *ucs-classic-3gen*	Enters the specified product family mode in the maintenance group.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/product-family # **scope fw-infra-pack-config**	Enters the infrastructure firmware package mode.
Step 6	UCSC(policy-mgr) /org/domain-group/product-family/fw-infra-pack-config #**show**	Displays the infrastructure firmware packages available in the system.

Example

The following example shows how to view the available infrastructure packages:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope product-family ucs-classic
UCSC(policy-mgr) /org/domain-infra-profile/product-family # scope fw-infra-pack-config
```

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

Firmware Upgrade Schedules

When upgrading the firmware, 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 does 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 org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*	Enters the infrastructure firmware policy mode.
Step 4	UCSC(policy-mgr) /org/domain-infra-profile # **scope schedule***job-name*	Enters the infrastructure firmware scheduling mode.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/schedule/ # **scope occurrence***one-time* | *recurring*	Enters the scheduling occurrence mode.
Step 6	UCSC(policy-mgr) /org/domain-infra-profile/schedule/ # **scope occurrence one-time infra-fw**	Enters the scheduling mode for a one-time occurrence.
Step 7	UCSC(policy-mgr) /org/domain-infra-profile/schedule/one-time # **set date apr 7 2016 18 00 00**	Specifies the date and time for the one time occurrence.
Step 8	UCSC(policy-mgr) /org/domain-infra-profile/schedule/one-time* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to schedule a one time occurrence firmware update:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope schedule infra-fw
UCSC(policy-mgr) /org/domain-infra-profile/schedule # scope occurrence
one-time   recurring
UCSC(policy-mgr) /org/domain-infra-profile/schedule # scope occurrence one-time infra-fw
UCSC(policy-mgr) /org/domain-infra-profile/schedule/one-time # set date apr 7 2016 18 00
00
UCSC(policy-mgr) /org/domain-infra-profile/schedule/one-time* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/schedule/one-time #
```

Viewing 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 org**	Scopes into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*	Enters the infrastructure firmware policy mode.
Step 4	UCSC(policy-mgr) /org/domain-infra-profile # **scope schedule** *schedule-name*	Enters the infrastructure firmware scheduling mode.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/schedule # **show detail**	Displays the one-time schedule.

Example

The following example shows how to display the scheduled one time occurrence:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope schedule one-time
UCSC(policy-mgr) /org/domain-infra-profile/schedule # 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 #
```

Enabling User-Acknowledgment

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters into the organization.
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*	Enters the infrastructure firmware policy mode.
Step 4	UCSC(policy-mgr) /org/domain-infra-profile # **create | scope schedule***schedule-name*	Enters the scheduling mode.
Step 5	UCSC(policy-mgr) /org/domain-infra-profile/schedule # **set admin-state user-ack**	Sets state to user-acknowledgment required before initiating upgrade, and before a fabric interconnect reboots.
Step 6	UCSC(policy-mgr) /org/domain-infra-profile/schedule* # **commit-buffer**	Commits the transaction to the system.

Example

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 org
UCSC(policy-mgr) /org # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope schedule infra-fw
UCSC(policy-mgr) /org/domain-infra-profile/schedule # set admin-state user-ack
UCSC(policy-mgr) /org/domain-infra-profile/schedule/one-time* # commit-buffer
UCSC(policy-mgr) /org/domain-infra-profile/schedule/one-time* #
```

Acknowledging a Pending Activity

This procedure describes the process to acknowledge the start of an infrastructure firmware update from the Cisco UCS Central CLI.

Procedure

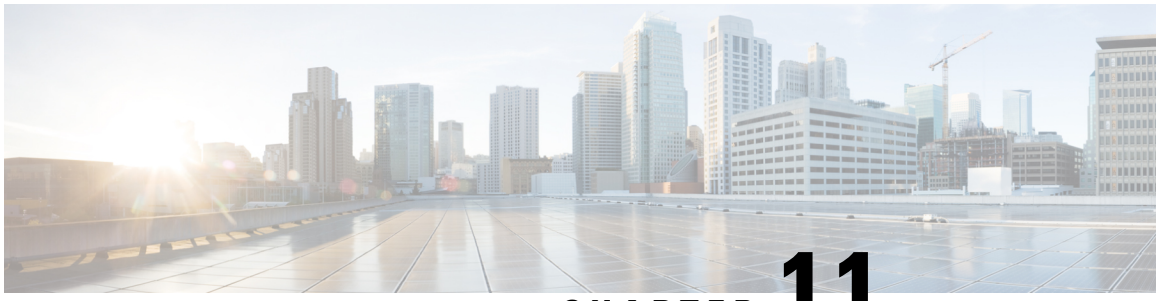
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters into the organization.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope domain-infra-profile** *job-name*	Enters the infrastructure firmware policy mode.
Step 4	UCSC(policy-mgr) /org/domain-infra-profile # **scope schedule***schedule-name*	Enters the scheduling mode.
Step 5	UCSC(ops-mgr) /org/domain-infra-profile/schedule # **show token-request**	Displays the pending tokens in the system.
Step 6	UCSC(ops-mgr) /org/domain-infra-profile/schedule # **scope token-request***domain-ID* | *token-name*	Finds the pending activity.
Step 7	UCSC(ops-mgr) /org/domain-infra-profile/schedule/token-request # **acknowledge token-request**	Acknowledges the specified pending activity.
Step 8	UCSC(ops-mgr) /org/domain-infra-profile/schedule/token-request * # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to acknowledge a pending activity:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope domain-infra-profile job1
UCSC(policy-mgr) /org/domain-infra-profile # scope schedule infra-fw
UCSC(ops-mgr) /org/domain-infra-profile/schedule # show token-request
Keyword for user-ack:
    Domain ID Token Request Name Client IP  Admin State     Oper State
    --------- ------------------ ---------- --------------- ----------
         1008 sys-fw-system-fw-infra  10.193.189.6
                                             Auto Scheduled  Pending Ack
UCSC(ops-mgr) /org/domain-infra-profile/schedule # scope token-request 1008
sys-fw-system-fw-infra
UCSC(ops-mgr) /org/domain-infra-profile/schedule/token-request # acknowledge token-request

UCSC(ops-mgr) /org/domain-infra-profile/schedule/token-request* # commit-buffer
```



CHAPTER 11

Backup Management

Backup and Import in Cisco UCS Central

Cisco UCS Central enables you to backup and restore Cisco UCS Central and the registered UCS domains. You can schedule a backup and restore policy or, you can perform an immediate 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 backups, 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 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.
- Cisco UCS Central supports Config and Full State Backup On Demand and through the backup policy for both Cisco UCS Central and Cisco UCS Domains managed by the particular UCS Central instance.

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 for either system.

Restoring Configuration

You can use the saved configuration from the backup repository to restore and configure any of the managed Cisco UCS domains. 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 to which you want Cisco UCS Central to export the backup file. You can maintain only one backup operation for each location where you plan to save a backup file.

Potential to Overwrite Backup Files

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

Multiple Types of Backups

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

Scheduled Backups

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

Incremental Backups

You cannot perform incremental backups.

Encryption of Full State Backups

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

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 to automatically backup the database or system configuration.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Connects to operation manager mode.
Step 2	UCSC(policy-mgr) # **scope org**	Enters into the organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile # **scope backup-policy** {*cfg* | *full-state*} *hostname*	Enters system backup mode for the specified hostname.
Step 5	UCSC(policy-mgr) /org/device-profile/cfg # **set adminstate** {*enable* | *disable*}	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 6	UCSC(policy-mgr) /org/device-profile/cfg # **commit-buffer**	Commits the transaction.

Example

The following example shows how to enable backup for Cisco UCS Central:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org #scope device-profile
UCSC(policy-mgr) /org/device-profile #  scope backup-policy cfg default
UCSC(policy-mgr) /org/device-profile/cfg # set adminstate enable
UCSC(policy-mgr) /org/device-profile/cfg* # commit-buffer
UCSC(policy-mgr) /org/device-profile/cfg #
```

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*

	Command or Action	Purpose
		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 does 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.

Example

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	(Optional) UCSC(policy-mgr) /org/device-profile/cfg* # **set adminstate** {**disable** | **enable**}	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

	Command or Action	Purpose
		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 6	(Optional) UCSC(policy-mgr) /org/device-profile/cfg* # **set descr** *description*	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	(Optional) UCSC(policy-mgr) /org/device-profile/cfg* # **set remote-file**	Selects the backup location.
Step 8	(Optional) UCSC(policy-mgr) /org/device-profile/cfg* # **set protocol**|**ftpsftp**|**scp**|**tftp**	Specifies the protocol.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/cfg* # **set max-copies**	Specifies the maximum number of backups (1 to 30 copies)
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/cfg* # **set schedule** {**bi-weekly** | **daily** | **weekly**}	Specifies the schedule for the backup.
Step 11	UCSC(policy-mgr) /org/device-profile/cfg* # **commit-buffer**	Commits the transaction.

Example

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 org
UCSC(policy-mgr) /org* # 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 set **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	(Optional) UCSC(policy-mgr) /domain-group/full-state * # **set adminstate** {**disabled** | **enabled**}	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 5	(Optional) UCSC(policy-mgr) /domain-group/full-state * # **set descr** *description*	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	(Optional) UCSC(policy-mgr) /domain-group/full-state * # **set max-copies** *number*	Specifies the maximum number of backups (1 to 30 copies)
Step 7	(Optional) UCSC(policy-mgr) /domain-group/full-state * # **set schedule** {**bi-weekly** | **daily** | **weekly**}	Specifies the schedule for the backup.
Step 8	UCSC(policy-mgr) /domain-group/full-state * # **commit-buffer**	Commits the transaction.

Example

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/full-state * # set adminstate disabled
UCSC(policy-mgr) /domain-group/full-state * # set max-copies 5
UCSC(policy-mgr) /domain-group/full-state * # set schedule daily
UCSC(policy-mgr) /domain-group/full-state * # commit-buffer
UCSC(policy-mgr) /domain-group/full-state #
```

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.
Step 3	UCSC(policy-mgr) /domain-group # **scope backup-policy cfg default**	Enters backup policy configuration mode.
Step 4	(Optional) UCSC(policy-mgr) /domain-group/cfg* # **set adminstate** {**disabled** | **enabled**}	If you use the **enable** keyword, the backup operation automatically runs as soon as you enter the **commit-buffer** command. If you use

	Command or Action	Purpose
		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	(Optional) UCSC(policy-mgr) /domain-group/cfg* # **set descr** *description*	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	(Optional) UCSC(policy-mgr) /domain-group/cfg* # **set max-copies** *number*	Specifies the maximum number of backups (1 to 30 copies)
Step 7	(Optional) UCSC(policy-mgr) /domain-group/cfg* # **set schedule** {**bi-weekly** | **daily** | **weekly**}	Specifies the schedule for the backup.
Step 8	UCSC(policy-mgr) /domain-group/cfg* # **commit-buffer**	Commits the transaction.

Example

The following example shows how to modify an all-configuration backup operation. The backup schedule is set 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.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /domain-group # **scope backup-policy full-state default**	Enters domain group configuration mode.
Step 4	(Optional) UCSC(policy-mgr) /domain-group/full-state* # **set adminstate** {**disabled** | **enabled**}	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	(Optional) UCSC(policy-mgr) /domain-group/full-state* # **set descr** *description*	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	(Optional) UCSC(policy-mgr) /domain-group/full-state* # **set max-copies** *number*	Specifies the maximum number of backups (1 to 30 copies)
Step 7	(Optional) UCSC(policy-mgr) /domain-group/full-state* # **set schedule** {**bi-weekly** | **daily** | **weekly**}	Specifies the schedule for the backup.
Step 8	UCSC(policy-mgr) /domain-group/full-state* # **commit-buffer**	Commits the transaction.

Example

The following example shows how to modify a disabled full-state backup operation. 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/full-state* # set adminstate enabled
UCSC(policy-mgr) /domain-group/full-state* # set max-copies 5
UCSC(policy-mgr) /domain-group/full-state* # set schedule daily
UCSC(policy-mgr) /domain-group/full-state* # commit-buffer
UCSC(policy-mgr) /domain-group/full-state #
```

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.

Example

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* # delete backup-policy full-state default
UCSC(policy-mgr) /domain-group* # commit-buffer
UCSC(policy-mgr) /domain-group #
```

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* {**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*

	Command or Action	Purpose
		• **tftp:**// *hostname* **:** *port-num* / *path* 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/backup # **commit-buffer**	Commits the transaction.

Example

The following example shows how to create a disabled backup operation for host35:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system* # create backup scp://user@10.0.0.1/backups disabled
Password:
UCSC(ops-mgr) /system* # commit-buffer
UCSC(ops-mgr) /system #
```

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	(Optional) UCSC(ops-mgr) /system/backup-mgmt # **disable**	Disables an enabled backup operation so that it does not automatically run when the transaction is committed.
Step 5	(Optional) UCSC(ops-mgr) /system/backup-mgmt # **enable**	Automatically runs the backup operation as soon as you commit the transaction.

	Command or Action	Purpose
Step 6	(Optional) UCSC(ops-mgr) /system/backup-mgmt # **set descr** *description*	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	(Optional) UCSC(ops-mgr) /system/backup-mgmt # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 8	(Optional) UCSC(ops-mgr) /system/backup-mgmt # **set remote-file** *filename*	Specifies the name of the configuration file that is being backed up.
Step 9	(Optional) UCSC(ops-mgr) /system/backup-mgmt # **set 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 10	(Optional) UCSC(ops-mgr) /system/backup-mgmt # **set password**	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 11	UCSC(ops-mgr) /system/backup-mgmt # **commit-buffer**	Commits the transaction.

Example

The following example shows how to:

- Add a description
- Change the protocol
- Change the username
- Change the password

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # scope backup host35
UCSC(ops-mgr) /system/backup-mgmt # set descr "This is a backup operation for host35."
UCSC(ops-mgr) /system/backup-mgmt* # set protocol sftp
UCSC(ops-mgr) /system/backup-mgmt* # set user UserName32
UCSC(ops-mgr) /system/backup-mgmt* # set password
Password:
```

```
UCSC(ops-mgr) /system/backup-mgmt* # 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.

Example

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 #
```

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** *URL*	Enters system backup mode for the specified hostname.

	Command or Action	Purpose
Step 4	(Optional) UCSC(ops-mgr) /system/backup # **set descr** *description*	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	(Optional) UCSC(ops-mgr) /system/backup # **set password**	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 6	(Optional) UCSC(ops-mgr) /system/backup # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 7	(Optional) UCSC(ops-mgr) /system/backup # **set remote-file** *filename*	Specifies the name of the configuration file that is being backed up.
Step 8	(Optional) UCSC(ops-mgr) /system/backup # **set 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 9	(Optional) UCSC(ops-mgr) /system/backup # **disable**	Disables an enabled backup operation so that it does not automatically run when the transaction is committed.
Step 10	(Optional) UCSC(ops-mgr) /system/backup # **enable**	Automatically runs the backup operation as soon as you commit the transaction.
Step 11	UCSC(ops-mgr) /system/backup # **commit-buffer**	Commits the transaction.

Example

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
```

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.

Example

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.

Example

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
```

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.

Example

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).

Example

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 Central. The file does not need to have been exported from the same Cisco UCS Central.

Note You cannot import a 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 Central 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 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.

	Command or Action	Purpose
Step 4	UCSC(ops-mgr) /system/import* # **commit-buffer**	Commits the transaction.

Example

The following example shows how to create a disabled import operation that replaces the existing configuration:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system* # create import scp://user@10.0.0.1/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 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**	Creates an import operation to a Cisco UCS domain.
Step 4	UCSC(ops-mgr) /backup-mgmt *# **commit-buffer**	Commits the transaction.

Example

The following example shows how to create an import operation to a Cisco UCS domain:

```
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
```

Enabling an Import Operation to Run

If you set your import operation to disabled when you created it, you must enable it so it can run.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect operation-mgr**	Connects to operation manager mode.
Step 2	UCSC# **scope system**	Enters system mode.
Step 3	UCSC /system # **scope import** {*hostname* | *host IP address*}	Enters system backup mode for the specified hostname.
Step 4	UCSC /system/import # **enable**	Enables the import operation.
Step 5	UCSC /system/import # **commit-buffer**	Commits the transaction.

Example

The following example shows how to enable an import operation:

```
UCSC# scope system
UCSC /system # scope import 10.0.0.1
UCSC /system/import # enable
UCSC /system/import*# commit-buffer
UCSC /system/import #
```

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	(Optional) UCSC(ops-mgr) /system/import # **disable**	Disables an enabled import operation so that it does not automatically run when the transaction is committed.
Step 5	(Optional) UCSC(ops-mgr) /system/import # **enable**	Automatically runs the import operation as soon as you commit the transaction.

	Command or Action	Purpose
Step 6	(Optional) UCSC(ops-mgr) /system/import # **set action** {**merge** | **replace**}	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. • **Replace** —The system takes each object in the import configuration file and overwrites the corresponding object in the current configuration.
Step 7	(Optional) UCSC(ops-mgr) /system/import # **set descr** *description*	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	(Optional) UCSC(ops-mgr) /system/import # **set password**	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	(Optional) UCSC(ops-mgr) /system/import # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 10	(Optional) UCSC(ops-mgr) /system/import # **set remote-file-prefix** *filename*	Specifies the name and full path of the configuration file that is being imported.
Step 11	(Optional) UCSC(ops-mgr) /system/import # **set 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 12	UCSC(ops-mgr) /system/import # **commit-buffer**	Commits the transaction.

Example

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:

```
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 UCS Central."
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.

Example

The following example shows how to delete the import operation:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # delete import 10.0.0.1
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.

	Command or Action	Purpose
Step 3	UCSC(ops-mgr) /ucs-domain # **scope managed-system**	Enters managed system mode.
Step 4	UCSC(ops-mgr) /ucs-domain/managed-system* # **delete importer** {*hostname* | *host IP address*}	Specifies the host to delete.
Step 5	UCSC(ops-mgr) /ucs-domain/managed-system* # **commit-buffer**	Commits the transaction.

Example

The following example shows how to delete a domain import operation:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope ucs-domain
UCSC(ops-mgr) /ucs-domain # scope 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.

Example

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:
```

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* • **scp:**// *username@hostname* / *path* • **sftp:**// *username@hostname* / *path* • **tftp:**// *hostname* **:** *port-num* / *path* • **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

	Command or Action	Purpose
		hostname you used when creating the backup operation.
Step 4	UCSC(ops-mgr) /system/export* # **commit-buffer**	Commits the transaction.

Example

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	(Optional) UCSC(ops-mgr) /system/export # **disable**	Disables an enabled export operation so that it does not automatically run when the transaction is committed.
Step 5	(Optional) UCSC(ops-mgr) /system/export # **enable**	Automatically runs the export operation as soon as you commit the transaction.

	Command or Action	Purpose
Step 6	(Optional) UCSC(ops-mgr) /system/export # **set descr** *description*	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	(Optional) UCSC(ops-mgr) /system/export # **set password**	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	(Optional) UCSC(ops-mgr) /system/export # **set protocol** {**ftp** | **scp** | **sftp** | **tftp**}	Specifies the protocol to use when communicating with the remote server.
Step 9	(Optional) UCSC(ops-mgr) /system/export # **set remote-file-prefix** *filename*	Specifies the name of the configuration file that is being backed up.
Step 10	(Optional) UCSC(ops-mgr) /system/export # **set type** *export-type*	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 • **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	(Optional) UCSC(ops-mgr) /system/export # **set 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 12	UCSC(ops-mgr) /system/export # **commit-buffer**	Commits the transaction.

Example

The following example shows how to add a description and change the protocol, username, and password:

```
UCSC# connect operation-mgr
UCSC(ops-mgr)# scope system
UCSC(ops-mgr) /system # scope export 10.0.0.1
UCSC(ops-mgr) /system/export # set descr "This is an export operation for 10.0.0.1"
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 #
```

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 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 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 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 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.

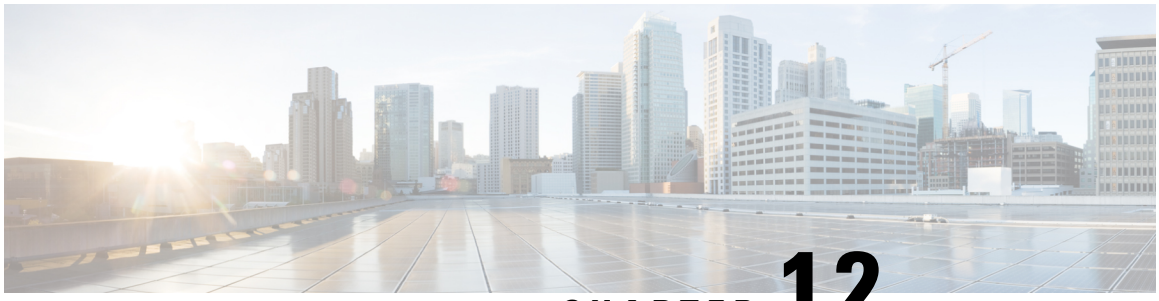
Procedure

	Command or Action	Purpose
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.

Example

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:
```



CHAPTER 12

Smart Call Home

Smart Call Home

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

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

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

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

Configuring Smart Call Home Using the CLI

Use this procedure to configure and enable Smart Call Home.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC (policy-mgr) # **scope org**	Enters organization mode.
Step 3	UCSC (policy-mgr) /org # **scope device-profile**	Enters device profile mode.
Step 4	UCSC (policy-mgr) /org/device-profile # **scope smart-callhome**	Enters Smart Call Home mode.
Step 5	UCSC (policy-mgr) /org/device-profile/smart-callhome # **enable**	Enables Smart Call Home.

Example

This example shows how to enable and configure Smart Call Home.

```
UCSC # connect policy-manager
UCSC (policy-mgr) # scope org
UCSC (policy-mgr) /org # scope device-profile
UCSC (policy-mgr) /org/device-profile # scope smart-callhome
UCSC(policy-mgr) /org/device-profile/smart-callhome # set contract-id
UCSC(policy-mgr) /org/device-profile/smart-callhome/ # set customer-id
UCSC(policy-mgr) /org/device-profile/smart-callhome/* # set email
UCSC(policy-mgr) /org/device-profile/smart-callhome/* # set phone-contact
UCSC(policy-mgr) /org/device-profile/smart-callhome/* # set site-id
UCSC(policy-mgr) /org/device-profile/smart-callhome/* # set street-address
UCSC(policy-mgr) /org/device-profile/smart-callhome/* # set throttling
UCSC(policy-mgr) /org/device-profile/smart-callhome/* # enable
```

Configuring an HTTP Proxy Using the CLI

Use this procedure to configure an HTTP proxy for Smart Call Home.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization root mode.
Step 3	UCSC(policy-mgr)# /org **scope device-profile**	Enters device-profile mode.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope smart-callhome**	Enters the default Smart Call Home policy configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/smart-callhome # **scope proxy**	Scopes the Transport Gateway.
Step 6	UCSC(policy-mgr) /org/device-profile/smart-callhome/proxy # **set** {*port* | *url*}	Sets the proxy parameters.
Step 7	UCSC(policy-mgr) /org/device-profile/smart-callhome/proxy # **commit-buffer**	

Example

This example shows how to configure an HTTP proxy for Smart Call Home.

```
UCSC # connect policy-manager
UCSC(policy-mgr) # scope org
UCSC(policy-mgr) /org # scope device-profile
```

```
UCSC(policy-mgr) /org/device-profile # scope smart-callhome
UCSC(policy-mgr) /org/device-profile/smart-callhome/ # scope proxy
UCSC(policy-mgr) /org/device-profile/smart-callhome/proxy # set port 80
UCSC(policy-mgr) /org/device-profile/smart-callhome/proxy # set url 10.0.0.1
UCSC(policy-mgr) /org/device-profile/smart-callhome/proxy # commit-buffer
```

Configuring System Inventory for Smart Call Home Using the CLI

Use this procedure to configure inventory options for Smart Call Home.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC (policy-mgr) # **scope org**	Enters organization mode.
Step 3	UCSC (policy-mgr) /org # **scope device-profile**	Enters device profile mode.
Step 4	UCSC (policy-mgr) /org/device-profile # **scope smart-callhome**	Enters Smart Call Home mode.
Step 5	UCSC (policy-mgr) /org/device-profile/smart-callhome # **scope inventory**	Enters inventory mode.
Step 6	UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # **set interval-days** *interval-days*	Sets the system inventory interval days (1-30).
Step 7	UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # **set send-periodically** {*on* | *off*}	Sets the frequency for sending inventory.
Step 8	UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # **set timeofday-hour** *timeofday-hour*	Sets the inventory hour of the day to send (1-23).
Step 9	UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # **set timeofday-minute** *timeofday-minute*	Sets the inventory minute of the hour to send (0-59).
Step 10	UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to scope and configure inventory options:

```
UCSC # connect policy-manager
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
```

```
UCSC(policy-mgr) /org/device-profile # scope smart-callhome
UCSC(policy-mgr) /org/device-profile/smart-callhome # scope inventory
UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory # set interval-days 30
UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # set send-periodically on
UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # set timeofday-hour 23
UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # set timeofday-minute 59
UCSC(policy-mgr) /org/device-profile/smart-callhome/inventory* # commit-buffer
```

Configuring the Transport Gateway Using the CLI

Use this procedure to configure the transport gateway to communicate with the Cisco Smart Call Home portal. The transport gateway acts as a proxy between Cisco UCS Central and the Smart Call Home servers at Cisco.com.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization root mode.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device-profile mode.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope smart-callhome**	Scopes the default Call Home policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/smart-callhome # **scope transport-gateway**	Scopes the Transport Gateway.
Step 6	UCSC(policy-mgr) /org/device-profile/smart-callhome/transport-gateway # **set url** *URL of transport gateway*	Sets the HTTP address for the transport gateway URL.
Step 7	UCSC(policy-mgr) /org/device-profile/smart-callhome/transport-gateway # **set certificate** *transport gateway certificate*	Sets the gateway certificate if you are using a secure (HTTPS) URL for access.
Step 8	UCSC(policy-mgr) /org/device-profile/smart-callhome/transport-gateway # **set enabled** {*yes* | *no*}	Enables the transport gateway.

Example

The following example shows how to enable and configure the transport gateway:

```
UCSC # connect policy-manager
UCSC(policy-mgr) # scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope smart-callhome
UCSC(policy-mgr) /org/device-profile/smart-callhome # score transport-gateway
UCSC(policy-mgr) /org/device-profile/smart-callhome/transport-gateway # set URL 10.0.0.1
UCSC(policy-mgr) /org/device-profile/smart-callhome/transport-gateway # set certificate
Transport Gateway Certificate:
```

```
UCSC(policy-mgr) /org/device-profile/smart-callhome/transport-gateway # set enabled yes
UCSC(policy-mgr) /org/device-profile/smart-callhome/transport-gateway # commit-buffer
```

Viewing the Destination Profile Using the CLI

Follow these steps to view the CiscoTAC-1 default destination profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization root mode.
Step 3	UCSC(policy-mgr)# /org**scope device-profile**	Enters organization root mode.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope smart-callhome**	Scopes the default Smart Call Home policy configuration mode.

Step 5	UCSC (policy-mgr) /org/device-profile/smart-callhome # **show profile detail**	`Destination Profile:`
		`  Name: CiscoTAC-1`
		`  Descr: Built-in TAC smartprofile`
		`  Level: Normal`
		`  Alert Groups:`
		`All,Inventory,Diagnostic,Environmental`
		`  Max Size: 5000000`
		`  Format: Xml`

Configuring Smart Call Home Alerts Using the CLI

Use this procedure to set Smart Call Home alerts.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org**	Enters organization root mode.
Step 3	UCSC(policy-mgr)# /org**scope device-profile**	Enters device-profile mode.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope smart-callhome**	Scopes the default Call Home policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/smart-callhome # **create alerts** {*capacity-exceeded* | *client-lost-connectivity* | *controller-lost-connectivity* | *core-file-generated* | *db-connect-read-write-error* | *duplicated-assigned* | *invalid-keyring-certificate* | *invalid-trustpoint-cert-chain* |	Creates an alert.

	Command or Action	Purpose
	not-in-compliance | *provider-lost-connectivity* | *remote-failed*}	
Step 6	UCSC(policy-mgr) /org/device-profile/callhome/profile* # **set admin-state** {*enable* | *disable*}	Sets the admin-state.
Step 7	UCSC(policy-mgr) /org/device-profile/callhome/profile/destination* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create and enable an alert:

```
UCSC # connect policy-manager
UCSC(policy-mgr) # scope org
UCSC(policy-mgr) /org # scope device-profile
UCSC(policy-mgr) /org/device-profile # scope smart-callhome
UCSC(policy-mgr) /org/device-profile/callhome # create alerts client-lost-connectivity
UCSC(policy-mgr) /org/device-profile/callhome/profile/alerts* # set admin-state disabled
UCSC(policy-mgr) /org/device-profile/callhome/profile/alerts* # commit-buffer
```

Smart Call Home Registration

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

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

Smart Call Home Faults

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

Fault Name	Fault Code	Explanation
fltSysdebugCoreCoreFile	F10000005	Fault occurs when one of the processes stops responding. Cisco UCS Central generates a core file.
fltExtpolProviderProviderLostConnectivity	F10000190	Provider is not reachable from the Cisco UCS Central registry. This fault typically occurs if the provider process has stopped responding, or is too busy to respond to a heartbeat message sent by the registry.

Fault Name	Fault Code	Explanation
fltExtpolControllerControllerLostConnectivity	F10000191	Controller is not reachable from the Cisco UCS Central registry. This fault typically occurs if the controller process has stopped responding, or is too busy to respond to a heartbeat message sent by the registry.
fltExtpolClientClientLostConnectivity	F10000192	Registered UCS domain is not reachable from the Cisco UCS Central registry. This fault typically occurs if the UCS domain has lost network access or UCS domain DME process has stopped responding, or is too busy to respond to a heartbeat message sent by registry.
fltIdentpoolElementDuplicatedAssigned	F10000208	Two or more service profiles possess the same ID. This fault occurs when Cisco UCS Central finds one ID is assigned to two or more service profiles probably from local pools.
fltConfigDbConfigStats-DB-Error	F10000536	Fault occurs when the statistics database is configured incorrectly or if the database is down or out of disk space.
fltPkiTPStatus	F10000591	Fault occurs when the TrustPoint certificate status has become invalid.
ltPkiKeyRingStatus	F10000592	Fault occurs when the Keyring certificate status has become invalid.
fltConfigBackupUngrouped-domain	F10000616	Remote scheduled backup failed. This fault typically occurs if the admin supplied the wrong password, host, user name, or path to the remote machine.
fltStorageItemCapacityExceeded	F10000034	Fault occurs when the partition disk usage exceeds 70% but is less than 90%.
fltStorageItemCapacityWarning	F10000035	Fault occurs when the partition disk usage exceeds 90%.
fltSmartlicenseEntitlementEnforcementModeFault	F10000750	Entitlement for a license is not compliant.

Smart Call Home Policies

Use the Smart Call Home policies in Cisco UCS Central to view Cisco UCS Manager alerts for your domain groups. The global Smart Call Home policies notify all email recipients, defined in Smart Call Home profiles, to specific Cisco UCS Manager events. 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 sub-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 | scope} callhome**	Create a new policy or scope into an existing one.
Step 4	UCSC(policy-mgr) /domain-group/callhome* # **set contact** *contact name*	Sets the contact name.
Step 5	UCSC(policy-mgr) /domain-group/callhome* # **set contract-id** *contract-id*	Sets the contract ID (numeric and/or text; 0-510 characters).
Step 6	UCSC(policy-mgr) /domain-group/callhome* # **set customer-id** *customer-id*	Sets the customer ID (numeric and/or text; 0-510 characters).
Step 7	UCSC(policy-mgr) /domain-group/callhome # **set email** *customer-contact-email*	Sets the customer's contact email (using standard email address format).
Step 8	UCSC(policy-mgr) /domain-group/callhome* # **set from-email** *from-email*	Sets the originating or "from" email (using standard email address format).
Step 9	UCSC(policy-mgr) /domain-group/callhome* # **set hostname** *smtp-server-address*	Sets the SMTP server address.
Step 10	UCSC(policy-mgr) /domain-group/callhome* # **set phone-contact** *phone-contact*	Sets the phone contact number (e.g., +1-011-408-555-1212).
Step 11	UCSC(policy-mgr) /domain-group/callhome* # **set port** *port*	Sets the port number (1-65535).
Step 12	UCSC(policy-mgr) /domain-group/callhome* # **set reply-to email** *reply-to-email*	Sets the email to which the customer should reply or "reply-to" email (using standard email address format).
Step 13	UCSC(policy-mgr) /domain-group/callhome* # **set site-id** *site-id*	Sets the site ID (numeric and/or text; 0-510 characters).
Step 14	UCSC(policy-mgr) /domain-group/callhome* # **set street-address** *street-address*	Sets the street address (0-255 characters).
Step 15	UCSC(policy-mgr) /domain-group/callhome* # **set switch-priority** {*alerts* | *critical* |	Sets the switch priority parameters.

	Command or Action	Purpose
	debugging | *emergencies errors* | *information* | *notifications* | *warnings*}	
Step 16	UCSC(policy-mgr) /domain-group/callhome* # **set throttling on** | **off**	Sets throttling to on or off.
Step 17	UCSC(policy-mgr) /domain-group/callhome* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create and configure the Call Home policy:

```
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

Deleting a Call Home Policy

You can delete a Call Home policy from a sub-domain group. You cannot delete a Call Home policies in the Domain Group root.

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.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a sub-domain group in the domain group root. **Note** Do not enter the domain group root. You cannot delete system default Call Home policies in 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* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete the Call Home policy:

```
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.

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 sub-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**} **profile** *profile-name*	Creates a Call Home policy profile name and enters profile mode, or it scopes into an existing Call Home policy.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /domain-group/callhome/profile* # **set alertgroups** {*ciscotac* | *diagnostic* | *environmental* | *inventory* | *license lifecycle* | *linecard* | *supervisor* | *syslogport* | *system* | *test*}|	Sets the profile alert group.
Step 6	(Optional) UCSC(policy-mgr) /domain-group/callhome/profile* # **add alertgroups** {*ciscotac* | *diagnostic* | *environmental* | *inventory* | *license lifecycle* | *linecard* | *supervisor* | *syslogport* | *system* | *test*}	Adds an additional profile alert group: **Note** Repeat this step to add additional profile alert groups if required.
Step 7	(Optional) UCSC(policy-mgr) /domain-group/callhome/profile* # **remove alertgroups** {*ciscotac* | *diagnostic* | *environmental* | *inventory* | *license lifecycle* | *linecard* | *supervisor* | *syslogport* | *system* | *test*}	Removes a specific profile alert groups from the buffer: **Note** Repeat this step to remove additional profile alert groups if required.
Step 8	(Optional) UCSC(policy-mgr) /domain-group/callhome/profile* # **clear alertgroups**	Clears all profile alert groups from the buffer.
Step 9	UCSC(policy-mgr) /domain-group/callhome/profile* # **set format** {*fulltxt* | *shorttxt* | *xml*	Sets the format.
Step 10	UCSC(policy-mgr) /domain-group/callhome/profile* # **set level** {*critical* | *debug* | *disaster* | *fatal* | *major minor* | *normal* | *notification* | *warning*}	Sets the level.
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.

Example

The following example shows how to configure a policy profile:

```
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 sub-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.

Example

The following example shows how to delete the policy profile chprofile01:

```
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 sub-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, 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 • 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

	Command or Action	Purpose
		• 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	(Optional) UCSC(policy-mgr) /domain-group/callhome/policy* # **exit**	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.

Example

The following example shows how to:

- Recursively create policies license-graceperiod-expired
- Recursively create policies management-services-failure
- Enable these policies for the Call Home policy
- Enable the admin-state for each
- 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 #
```

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 sub-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.

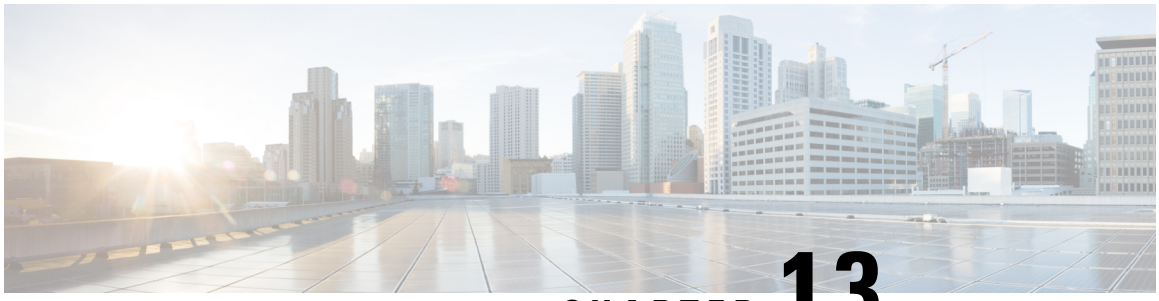
Example

The following example shows how to delete the policy chpolicy01 from within the Call Home policy:

```
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 #
```

PART III

Authentication



CHAPTER 13

Users and Roles

Cisco UCS Central User Accounts

Access the system with user accounts. You can configure up to 128 user accounts in each Cisco UCS Central domain. Each user account must have a unique username and password.

You can setup a user account with an SSH public key, in either of the two formats: OpenSSH or SECSH.

Admin Account

The Cisco UCS Central admin account is the default user account. You cannot modify or delete it. 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 can 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. Anyone with admin or aaa privileges can enable or disable it. Once you disable a local user account, the user cannot log in.

Note Cisco UCS Central does not delete configuration details for disabled local user accounts from 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 domains support 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

You can configure user accounts to expire at a predefined time. When the user account reaches the expiration time, the account disables.

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 to expire with the farthest 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

You cannot use the following words 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, Cisco recommends 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—Ensures that the users exist in the remote authentication server with the appropriate roles and privileges.
- Multitenancy with organizations—Creates 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—Obtains the SSH key.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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, Cisco UCS Central does not delete the configuration from the database. It prevents the user 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	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set firstname** *first-name*	Specifies the first name of the user.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set lastname** *last-name*	Specifies the last name of the user.

	Command or Action	Purpose
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set expiration** *month day-of-month year*	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. However, you can configure the account to use the latest expiration date available.
Step 11	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set email** *email-addr*	Specifies the user e-mail address.
Step 12	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set phone** phone-num	Specifies the user phone number.
Step 13	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set sshkey** *ssh-key*	Specifies the SSH key used for passwordless access.
Step 14	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Creates the user account named kikipopo
- Enables the user account
- Sets the password to foo12345
- 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 kikipopo
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
- 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
AAAAB3NzaC1yc2EAAAA
BIwAAAIEAuo9VQ2CmWBI9/S1f30klCWjnV3lgdXMzO0WUl5iPw85lkdQqap+NFuNmHcb4KiaQB8X/PDdmtlxQQcawclj+k8f4
VcOelBxlsGk5luq5ls1ob1VOIEwcKEL/h5lrdbNlI8y3SS9I/gGiBZ9ARlop9LDpDm8HPh2LOgyH7Ei1MI8="
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 hpotter
- Enables the user account,
- Sets a Secure SSH key for passwordless access
- 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 hpotter
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 #
```

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 org /**	Enters the organization root.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Deletes the local-user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the foo user account
- 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 # delete local-user foo
UCSC(policy-mgr) /org/device-profile/security* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security #
```

Enabling the Password Strength Check for Locally Authenticated Users

You must have privileges to enable the password strength check. If enabled, 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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 password-profile**.	Specifies whether the password strength check is enabled or disabled.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set enforce-strong-password** {**yes** | **no**}	Specifies whether the password strength check is enabled or disabled.
Step 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Enables the password strength check
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set enforce-strong-password
 yes
UCSC(policy-mgr) /org/device-profile/security/password-profile # commit-buffer
```

Clearing the Password History for a Locally Authenticated User

You must have admin, aaa, or org/device-profile-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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Commits the transaction.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **scope password-profile**	Enters password profile security mode.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/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 8	UCSC(policy-mgr) /org/device-profile/security/password-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Clears the password history count for the user account named kikipopo
- 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 # scope local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set history-count 0
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Enabling or Disabling a User Account

You must have 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 org**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user**	Enters local-user security mode.

	Command or Action	Purpose
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.

Example

The following example:

- Enables a local user account called accounting
- 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 # scope local-user accounting
UCSC(policy-mgr) /org/device-profile/security/local-user # set account-status active
UCSC(policy-mgr) /org/device-profile/security/local-user # commit-buffer
```

Web Session Limits for User Accounts

Cisco UCS Manager uses web session limits to restrict the number of web sessions (both GUI and XML) that a given user account is permitted to access at any one time.

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.

Example

The following example lists all of the 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
```

Guidelines for Creating Passwords

Each locally authenticated user account requires a password. Cisco recommends that each user have a strong 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 you enabled the password strength check, each user must use a strong password.

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. Meaning, 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 the password change interval properties for all locally authenticated users of . You cannot specify a different password profile for locally authenticated users.

Password History Count

The password history count prevents locally authenticated users from reusing the same password. When you configure the password history count, stores up to a maximum of 15 previously used passwords. The password history count stores the passwords in reverse chronological order with the most recent password first. This ensures that the user can only reuse the oldest password when the history count reaches its threshold.

A user can create and use the number of passwords configured in the password history count before reusing a password. For example, if you set the password history count to 8, a user cannot reuse the first password until the ninth password expires.

By default, the password history is set to 0. This value disables the history count and allows users to reuse previously used passwords at any time.

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 restricts the number of password changes that a locally authenticated user can make within a specific number of hours. The following table describes the two interval configuration options for the password change interval.

Interval Configuration	Description	Example
No password change allowed	Does not allow changing passwords for locally authenticated user 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.	To prevent the user from changing passwords within 48 hours after a password change: • Set **Change during interval** to disable • Set **No change interval** to 48

Interval Configuration	Description	Example
Password changes allowed within change interval	Specifies the maximum number of times that a locally authenticated user password change can occur 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 two password changes within a 48-hour interval.	To allow a password change for a maximum of one time within 24 hours after a password change: • Set **Change during interval** to enable • Set **Change count** to 1 • Set **Change interval** to 24

Configuring the Maximum Number of Password Changes for a Change Interval

You must have admin, aaa, or org/device-profile-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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/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 7	UCSC(policy-mgr) /org/device-profile/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 8	UCSC(policy-mgr) /org/device-profile/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.

	Command or Action	Purpose
		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 9	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enables the change during interval property
- Sets the change count to 5
- Sets the change interval to 72 hours
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set change-during-interval
 enable
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set change-count 5
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set change-interval 72
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Configuring a No Change Interval for Passwords

You must have admin, aaa, or org/device-profile-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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/password-profile # **set change-during-interval disable**	Disables the change during interval feature.
Step 7	UCSC(policy-mgr) /org/device-profile/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 set to **Disable**.
Step 8	UCSC(policy-mgr) /org/device-profile/security/password-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Disables the change during interval property
- Sets the no change interval to 72 hours
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set change-during-interval
 disable
UCSC(policy-mgr) /org/device-profile/security/password-profile* # set no-change-interval
72
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 password-profile**	Enters password profile security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/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 7	UCSC(policy-mgr) /org/device-profile/security/password-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Configures the password history count
- 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 # scope password-profile
UCSC(policy-mgr) /org/device-profile/security/password-profile # set history-count 5
UCSC(policy-mgr) /org/device-profile/security/password-profile* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/password-profile #
```

Configuring User Locales

User Locales

You can assign a user to one or more locales. Each locale defines one or more organizations (domains) to which a user can access. Access is usually limited to the organizations specified in the locale. An exception is a locale without any organizations. It provides unrestricted access to system resources in all organizations.

A Cisco UCS domain can contain up to 48 user locales. Any user locales configured after the first 48 are accepted, but are inactive with faults raised.

Users with admin or aaa privileges can assign organizations to the locale of other users. The assignment of organizations is restricted to only those in the locale of the user assigning the organizations. For example, if a locale contains only the Engineering organization, a user assigned to that locale can only assign the Engineering organization to other users.

Note You cannot assign a locale to users with one or more of the following privileges:

- aaa
- admin
- fault
- operations

You can hierarchically manage organizations. A user who is assigned to a top-level organization has automatic access to all organizations below 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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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** org-root/org-*orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference. The *orgdn-name* argument is the distinguished name of the organization referenced.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates the finance organization for the western locale
- 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 locale western
UCSC(policy-mgr) /org/device-profile/security/locale* # create org-ref finance-ref orgdn
org-root/org-finance
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 locale** *locale-name*	Deletes the locale.
Step 6	UCSC(policy-mgr) /org/device-profile/security # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the western locale
- 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 # delete locale western
UCSC(policy-mgr) /org/device-profile/security* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC /security # **scope local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **create locale** *locale-name*	Assigns the specified locale to the user account. **Note** You can enter the **create locale** command multiple times to assign more than one locale to a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user # **commit-buffer**	Commits the transaction.

Example

The following example:

- Assigns the western locale to the kikipopo local user account
- 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/local-user # create locale western
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **delete locale** *locale-name*	Removes the specified locale from the user account. **Note** You can enter the **delete locale** command multiple times to remove more than one locale from a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Removes the western locale from the kikipopo local user account

- 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/ # scope local-user
UCSC(policy-mgr) /org/device-profile/security/local-user # delete locale western
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 locale** *locale-name*	Enters locale security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **create org-ref** *org-ref-name* **orgdn org-root/org-***orgdn-name*	References (binds) an organization to the locale. The *org-ref-name* argument is the name used to identify the organization reference. The *orgdn-name* argument is the distinguished name of the organization referenced.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Adds (references) the marketing organization to the locale
- Names the reference marketing-ref
- 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 # scope locale western
UCSC(policy-mgr) /org/device-profile/security/locale # create org-ref marketing-ref orgdn
org-root/org-marketing
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 locale** *locale-name*	Enters security locale mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **delete org-ref** *org-ref-name*	Deletes the organization from the locale.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the finance organization from the western locale
- 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 # scope locale western
UCSC(policy-mgr) /org/device-profile/security/locale # delete org-ref finance-ref
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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) /domain-group/security # **scope locale** *locale-name*	Enters security locale mode.
Step 6	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. The *domain-group-dn-name* argument is the distinguished name of the domain group root referenced.
Step 7	UCSC(policy-mgr) /domain-group/security/locale # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Adds (references) the marketing domain group to the locale
- Names the reference marketdomain01-ref
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # scope device-profile
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 domaingroup-root/domaingroup-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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 locale** *locale-name*	Enters security locale mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/locale # **delete domain-group-ref** *domain-group-ref-name*	Deletes references (unbinds) domain groups referenced to the locale. The *domaingroup-ref* argument (1-16 characters) is the name used to identify the domain group reference.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Enters the western locale
- Deletes references (unbinds) the marketing domain group references from the locale marketdomain01
- 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 # scope locale western
UCSC(policy-mgr) /org/device-profile/security/locale # delete domain-group-ref marketdomain01
UCSC(policy-mgr) /org/device-profile/security/locale* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 sub-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.

Example

The following example:

- Creates the central-audit domain group
- 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 sub-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 domain-group** *name*	Deletes the domain group.
Step 4	UCSC(policy-mgr) /domain-group * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the central-audit domain group
- 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.

Example

The following example:

- Creates the central-audit organization
- 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.

Example

The following example:

- Deletes the central-audit organization
- 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.

Example

The following example:

- Enters the central-audit organization
- Creates the north-audit sub-organization
- 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

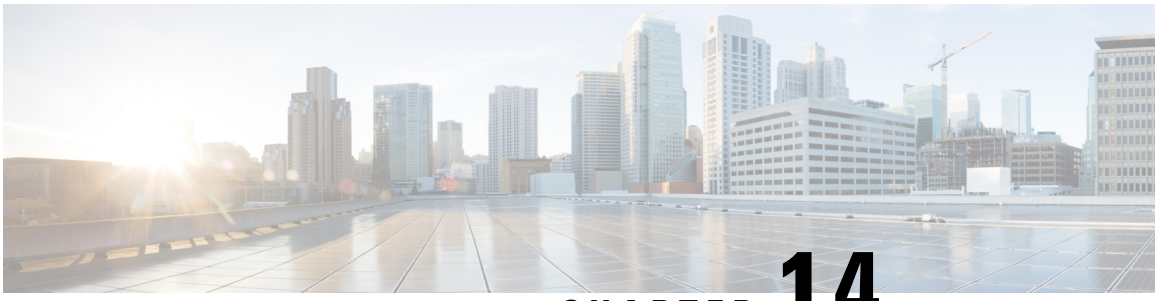
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **delete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

Example

The following example:

- Enters the central-audit organization
- Deletes the north-audit sub-organization
- 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 #
```



CHAPTER 14

Role-Based Access Controls

Configuring User Roles

Role-Based Access Control Overview

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 a locale defines the organizations (domains) that a user is allowed access. Because users are not directly assigned privileges, you can manage individual user privileges by assigning the appropriate roles and locales.

A user is granted write access to the required 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 can update server configurations in the Engineering organization. They cannot, however, 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. You can assign one or more roles to each user. Users with multiple roles have the combined privileges of all assigned roles. For example, if Role1 has storage-related privileges, and Role 2 has server-related privileges, users with Role1 and Role 2 have both storage-related and server-related privileges.

A Cisco UCS domain can contain up to 48 user roles, including the default user roles. Any user roles configured after the first 48 are accepted, but they are 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.

You can create, modify or remove existing privileges, and delete roles. When you modify a role, the new privileges apply to all users with that role. Privilege assignment is not restricted to the privileges defined for the default roles. Meaning, 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. However, you can create a Server and Storage Administrator role that combines the privileges of both roles.

Note If you delete a role after it was assigned to users, it is also deleted from those user accounts.

Modify the user profiles on AAA servers (RADIUS or TACACS+) to add the roles corresponding to the privileges granted to that user. The attribute stores the role information. The AAA servers return this attribute with the request and parse it to obtain 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 remaining system.

Administrator

Complete read-and-write access to the entire system. Assigns this role to the default administrator account by default. You cannot change it.

Facility Manager

Read-and-write access to power management operations through the power management privilege. Read access to the remaining system.

Network Administrator

Read-and-write access to fabric interconnect infrastructure and network security operations. Read access to the remaining system.

Operations

Read-and-write access to systems logs, including the syslog servers, and faults. Read access to the remaining 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 remaining system.

Server Profile Administrator

Read-and-write access to logical server-related operations. Read access to the remaining system.

Server Security Administrator

Read-and-write access to server security-related operations. Read access to the remaining system.

Storage Administrator

Read-and-write access to storage operations. Read access to the remaining system.

Reserved Words: User Roles

You cannot use the following words 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.

Tip Detailed information about these privileges and the tasks that they enable users to perform is available in *Privileges in Cisco UCS* available at the following URL: http://www.cisco.com/en/US/products/ps10281/prod_technical_reference_list.html.

Table 2: System Defined Roles

Role	Privileges	Role to Configure in LDAP/RADIUS/TACACS Server
AAA Administrator	aaa	aaa
Administrator	admin	admin
KVM Administrator	kvm	kvm
Network	pod-qos,pod-config,pod-policy,ext-lan-qos,pod-security,	network
Operations	fault, operations	fault, operations
Read-Only	read-only	read-only
Server-Compute Administrator		server-compute
Server-Equipment Administrator	server-policy,server-equipment,server-maintenance	server-equipment
Server Profile Administrator		server-profile
Server Security Administrator		server-security
Statistics Administrator	stats	stats-management
Storage Administrator		storage

Table 3: User Privileges

Privilege	Description	Default Role Assignment
aaa	System security and AAA	AAA Administrator
admin	System administration	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
kvm	Launch KVM	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 endpoint 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

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 /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 role security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **add privilege** *privilege-name*	Adds one or more privileges to the role.

	Command or Action	Purpose
		Note You can specify more than one *privilege-name* on the same command line to add multiple privileges to the role. You can also 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.

Example

The following example:

- Creates the service-profile-security-admin role
- Adds the service profile security to the role
- Adds the service profile security policy privileges to the role
- 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 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
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 role** *name*	Deletes the user role.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the service-profile-security-admin role
- 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 # delete role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/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. You can also add privileges to the same role using multiple **add privilege** commands.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Adds the server security to the service-profile-security-admin role
- Adds the server policy privileges to the service-profile-security-admin role
- 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 # scope role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # add privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/security/role # **set privilege** *privilege-name*	Replaces the existing privileges of the user role.

	Command or Action	Purpose
		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 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Replaces the existing privileges for the service-profile-security-admin role with server security
- Replaces the existing privileges for the service-profile-security-admin role with server policy privileges
- 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 # scope role
UCSC(policy-mgr) /org/device-profile/security/role # scope role service-profile-security-admin
UCSC(policy-mgr) /org/device-profile/security/role* # set privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 # **scope role** *name*	Enters role security mode for the specified role.
Step 6	UCSC(policy-mgr) /org/device-profile/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. You can also remove privileges from the same role using multiple **remove privilege** commands.
Step 7	UCSC(policy-mgr) /org/device-profile/security/role* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Removes the server security from the service-profile-security-admin role
- Removes the server policy privileges from the service-profile-security-admin role
- 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 # scope role
UCSC(policy-mgr) /org/device-profile/security/role # remove privilege server-security
server-policy
UCSC(policy-mgr) /org/device-profile/security/role* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **create role** *role-name*	Assigns the specified role to the user account. **Note** You can enter the **create role** command multiple times to assign more than one role to a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Assigns the operations role to the kikipopo local user account
- 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 # scope local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # create role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org /**	Enters the organization root.

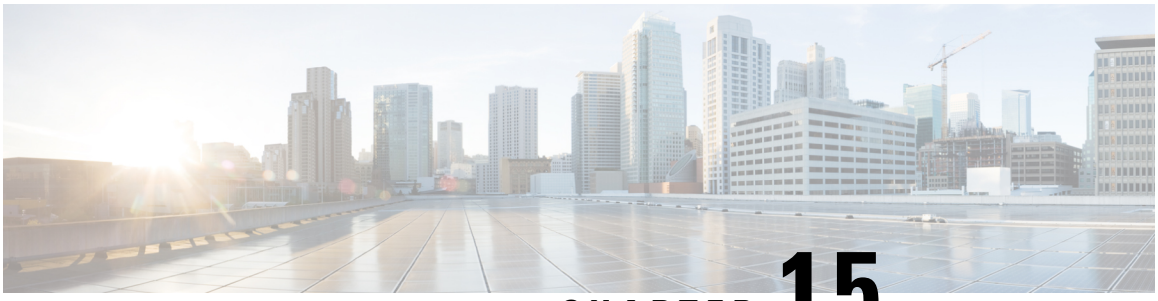
	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile # **scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope local-user** *local-user-name*	Enters local user security mode for the specified local user account.
Step 6	UCSC(policy-mgr) /org/device-profile/security/local-user # **delete role** *role-name*	Removes the specified role from the user account. **Note** You can enter the **delete role** command multiple times to remove more than one role from a user account.
Step 7	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Removes the operations role from the kikipopo local user account
- Commits the transaction

```
CSC # 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 local-user kikipopo
UCSC(policy-mgr) /org/device-profile/security/local-user # delete role operations
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user #
```



CHAPTER 15

Authentication Services

General Settings

You can configure and define policies in Cisco UCS Central at the organization level. Manage them in the infrastructure.

IPv6 Support

Cisco UCS Central supports IPv6 addressing. Cisco UCS Central operates on a dual mode where it enables both IPv4 and IPv6. 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.

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 domain 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 Cisco UCS Central uses IPv6 addresses.

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 # **scope 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.

Example

The following example:

- Configures IPv6 in standalone mode
- Commits the transaction.

```
UCSC #scope system
UCSC /system #scope network-interface a
UCSC /network-interface # scope ipv6-config
UCSC /network-interface/ipv6-config # set net ipv6 ipv6 2001:db8:a::11 ipv6-gw  2001:db8:a::1
 ipv6-prefix  64
UCSC /network-interface/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 /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.
Step 6	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.

	Command or Action	Purpose
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/ipv6-config #**scope ipv6-config**	Scopes to IPv6 configuration.
Step 10	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 11	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 12	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.
Step 13	UCSC # **scope system**	Enters system mode.
Step 14	UCSC /system # **set virtual ip ipv6***ipv6 address*	Configures a virtual IPv6 address.
Step 15	UCSC /system # **commit-buffer**	Commits the transaction to the system configuration.
Step 16	UCSC /system # **top**	Returns to the top most directory.

Example

The following example:

- Configures IPv6 in high availability mode
- Commits the transaction

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

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

UCSC # scope system
UCSC /system # set virtual-ip ipv6 2001:db8:a::10
UCSC /system # commit-buffer
UCSC /system # 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 /system #**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 /network-interface/ipv6-config #**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 5	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 6	UCSC /network-interface/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 /system # **commit-buffer**	Commits the transaction to the system configuration.
Step 10	UCSC /system # **top**	Returns to the top most directory.
Step 11	UCSC # **scope system**	Enters system mode.
Step 12	UCSC /system # **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 /network-interface/ipv6-config #**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 15	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 16	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.
Step 17	UCSC # **scope system**	Enters system mode.
Step 18	UCSC /system # **scope network-interface b**	Enters node B of the network interface.
Step 19	UCSC /network-interface #**scope ipv6-config**	Scopes to IPv6 configuration.
Step 20	UCSC /network-interface/ipv6-config #**set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64**	Sets the IPv6 address to null, therefore disabling it.
Step 21	UCSC /network-interface/ipv6-config #**commit-buffer**	Commits the transaction to the system configuration.
Step 22	UCSC /network-interface/ipv6-config #**top**	Returns to the top most directory.

Setting the IPv6 value to null moves all of the affected IPv6 devices to a state of lost visibility.

Example

The following example:

- Disables IPv6 on Cisco UCS Central for the standalone and HA modes
- Commits the transaction

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

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

```
UCSC # scope system
UCSC /system #  scope network-interface b
UCSC /network-interface # scope ipv6-config
UCSC /network-interface/ipv6-config # set net ipv6 ipv6 :: ipv6-gw :: ipv6-prefix 64
UCSC /network-interface/ipv6-config # commit-buffer
UCSC /network-interface/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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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	(Optional) UCSC(policy-mgr) /org/device-profile/snmp # **create snmp-trap** *snmp-trap-ip*	If scoping into an organization previously created, it creates the SNMP trap IP address for that organization (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 6	(Optional) UCSC(policy-mgr) /org/device-profile/snmp # **scope snmp-trap** *snmp-trap-ip*	If scoping into organization previously created, it 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.

Example

The following example:

- Scopes into an organization
- Scopes the SNMP policy
- Creates the SNMP trap with IP address 0.0.0.0
- Sets the SNMP community host string to snmptrap01
- Sets the SNMP notification type to traps
- Sets the SNMP port to 1
- Sets the v3privilege to priv

- Sets the version to v1
- 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 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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**	Enter and confirm a password for the SNMP user.
Step 9	UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # **set priv-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.

Example

The following example:

- Scopes into an organization
- Scopes the SNMP policy
- Scopes into the SNMP user named snmpuser01
- Sets aes-128 mode to enabled
- Sets authorization to sha mode
- Sets password to userpassword01
- Sets private password to userpassword02
- 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 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
Enter a password: userpassword01
Confirm the password: userpassword01
UCSC(policy-mgr) /org/device-profile/snmp/snmp-user* # set priv-password
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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/device-profile/timezone-ntp-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into an organization
- Creates an NTP server instance named orgNTP01
- 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 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
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.

Example

The following example:

- Scopes into the organization
- Creates a DNS server instance named 0.0.0.0
- Commis\ts 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	(Optional) UCSC(policy-mgr) /org # **scope fault policy**	If scoping into the domain group root previously created, scopes the default fault policy's configuration mode from the domain group root.
Step 5	UCSC(policy-mgr) /org/device-profile/policy* # **set ackaction delete-on-clear**	Sets 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) /org/device-profile/policy* # **set clearaction delete** | **retain**	Sets the fault policy clear action to delete or retain.
Step 7	UCSC(policy-mgr) /org/device-profile/policy* # **set clearinterval** *days* | *hours* | *minutes* | *seconds* | **retain**	Sets the fault policy clear interval to the number of days, hours, minutes, and seconds or retain.
Step 8	UCSC(policy-mgr) /org/device-profile/policy* # **set flapinterval** *flap-number-of-days*	Sets the fault policy flap interval to the number of days.
Step 9	UCSC(policy-mgr) /org/device-profile/policy* # **set retentioninterval** *days* | *hours* | *minutes* | *seconds* | **forever**	Sets the fault policy clear interval to the number of days, hours, minutes, and seconds or forever.
Step 10	UCSC(policy-mgr) /org/device-profile/policy* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Creates a global fault debug policy
- Enters the status settings
- 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 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 15 30 60 90
UCSC(policy-mgr) /org/device-profile/policy* # set flapinterval 180
UCSC(policy-mgr) /org/device-profile/policy* # set retentioninterval 180 54 52 63
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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	(Optional) UCSC(policy-mgr) /org/device-profile # **scope tftp-core-export-config**	Scopes an existing TFTP core export debug policy's configuration mode.
Step 5	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **enable core-export-target**	Enables the TFTP core export target.
Step 6	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 7	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 8	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* #	Sets the TFTP core export target policy server description.

	Command or Action	Purpose
	set core-export-target server-description *port-number*	**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) /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 10	UCSC(policy-mgr) /org/device-profile/tftp-core-export-config* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Scopes the TFTP Core Export Policy
- Configures the policy
- 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 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**	Enters organization mode for the specified organization.

	Command or Action	Purpose
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 to enable or disable the local user account. The admin user account is always set to active. You cannot modify it. **Note** If you set the account status to inactive, Cisco UCS Central does not delete the configuration from the database. Cisco UCS Central prevents the user 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	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set firstname** *first-name*	Specifies the first name of the user.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set lastname** *last-name*	Specifies the last name of the user.
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set expiration** *month day-of-month year*	Specifies the date that the user account expires. The *month* argument is the first three letters of the month name.
Step 11	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set email** *email-addr*	Specifies the user e-mail address.
Step 12	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set phone** *phone-num*	Specifies the user phone number.
Step 13	(Optional) UCSC(policy-mgr) /org/device-profile/security/local-user* # **set sshkey** *ssh-key*	Specifies the SSH key used for passwordless access.
Step 14	UCSC(policy-mgr) /org/device-profile/security/local-user* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Scopes into the organization
- Creates the user account named eagle_eye
- Enables the user account
- Sets the password to eye5687
- 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 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: eye5687
Confirm the password: eye5687
UCSC(policy-mgr) /org/device-profile/security/local-user* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/local-user* #
```

The following example:

- Scopes into the organization
- Creates the user account named lincey
- Enables the user account
- Sets an openSSH key for passwordless access
- 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:

- Scopes into the organization
- Creates the user account named jforlenz
- Enables the user account
- Sets an secure SSH key for passwordless access
- 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 Login Policy

Procedure

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

Example

The following example:

- Sets the role policy for remote users
- 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 # 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Creates the service-profile security-admin role
- Adds the service profile security to the role
- Adds service profile security policy privileges to the role
- Commits the transaction

```
UCSC # connect policy-mgr
UCSC(policy-mgr) /org# scope device-profile
UCSC(policy-mgr) /org/device-profile # scope security
UCSC(policy-mgr) /org/device-profile/security # create role security-admin
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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 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 referenced.
Step 7	UCSC(policy-mgr) /org/device-profile/security/locale * # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates the finance organization for the western locale
- 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 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 user must have a unique username and password.

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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 are applicable only for the Cisco UCS Central in the domain group root and sub-domain groups.
Step 7	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **create default-auth**	Creates a default authentication for the specified authentication domain.
Step 8	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set auth-server-group** *auth-serv-group-name*	Specifies the provider group for the specified authentication domain.
Step 9	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 10	UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Creates an authentication domain called domain1
- Sets the web refresh period to 3600 seconds (1 hour)
- Sets the session timeout period to14400 seconds (4 hours)
- Configures domain1 to use the providers in ldapgroup1

- Sets the realm type to ldap
- 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 # scope auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # create auth-domain domain1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # create default-auth
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
auth-server-group ldapgroup1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
realm ldap
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth #
```

Creating an LDAP Provider

Create and configure LDAP remote users, and assign roles and locales from Cisco UCS Central, in the same manner as Cisco UCS Manager. Always create the LDAP provider from the Cisco UCS Central domain group root.

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. Give this account 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 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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create server** *server-name*	• Creates an LDAP server instance • Enters LDAP security server mode **Note** • If SSL is enabled, the server-name must 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	(Optional) UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set attribute** *attribute*	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.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set basedn** *basedn-name*	The name in the LDAP hierarchy, where the server begins a search, when a remote user logs in. After log in, the system attempts to obtain the user's DN based on their username. You can set the length of the base DN to a maximum of 255 characters minus the length of CN=username. Where username identifies the remote user attempting to access Cisco UCS Central 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*	Restricts the LDAP search to those user names that match the defined filter.
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 encryption when communicating with the LDAP server. The options are as follows: • **yes** —Encryption required. If Cisco UCS Central cannot negotiate encryption, the connection fails. • **no** —Encryption disabled. Authentication information sent as clear text.
Step 15	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set timeout** *timeout-num*	If the LDAP provider does not receive an LDAP response within the specified period, it aborts the read attempt.
Step 16	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set vendor**	Specifies the vendor for the LDAP group. • **ms-ad** —Specifies Microsoft Active Directory.

	Command or Action	Purpose
		• **openldap** —Specifies OpenLDAP server.
Step 17	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Creates an LDAP server instance named 10.193.169.246
- Configures the binddn
- Configures the password
- Configures the order
- Configures the port
- Configures the SSL settings
- 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 # 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security 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.
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.

Example

The following example:

- Creates an LDAP provider group called ldapgroup
- Adds two previously configured providers called ldap1 and ldap2 to the provider group
- Sets the order
- 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 # 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security 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.
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.

	Command or Action	Purpose
Step 9	UCSC(policy-mgr) /org/device-profile/security/ldap/ldap-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Maps the LDAP group mapped to a DN
- Sets the locale to pacific
- Sets the role to admin
- 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 # 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security 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.

Example

The following example:

- Deletes the LDAP server called ldap1
- 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 # 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) /org/device-profile/security/ldap #
```

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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **delete auth-server-group** *auth-server-group-name*	Deletes the LDAP provider group.

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

Example

The following example:

- Deletes an LDAP provider group called ldapgroup
- 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 # 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security 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.

Example

The following example:

- Deletes an LDAP group map
- 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 # 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
```

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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 root certificate authority (CA). On the next line following your input, type ENDOFBUF to finish.

Example

The following example:

- Creates a trusted point
- 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 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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.

Example

The following example:

- Deletes a trusted point
- 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 # 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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.

Example

The following example:

- Creates a key ring with a key size of 2048 bits
- 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 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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.

Example

The following example:

- Scopes into the organization
- Deletes a key ring
- 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 # 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 # **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.
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 Cisco UCS Manager.
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 short name of Cisco UCS Manager. For example, this field could contain short alternatives to the FQDN.
Step 17	UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # **commit-buffer**	Commits the transaction.

Example

The following example:

- Creates a certificate request with an IPv4 address for a key ring
- Sets advanced options
- 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 # 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 abc123.example.com
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* # set e-mail 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 abc123
UCSC(policy-mgr) /org/device-profile/security/keyring/certreq* #commit-buffer
```

Configuring an HTTPS Certificate

Procedure

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

Example

The following example:

- Configures an HTTPS certificate
- 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 https
UCSC(policy-mgr) /org/device-profile/https # set keyring kr126
UCSC(policy-mgr) /org/device-profile/https* # commit-buffer
```

Regenerating the Default Key Ring

You must manually regenerate the default key ring certificate 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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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.

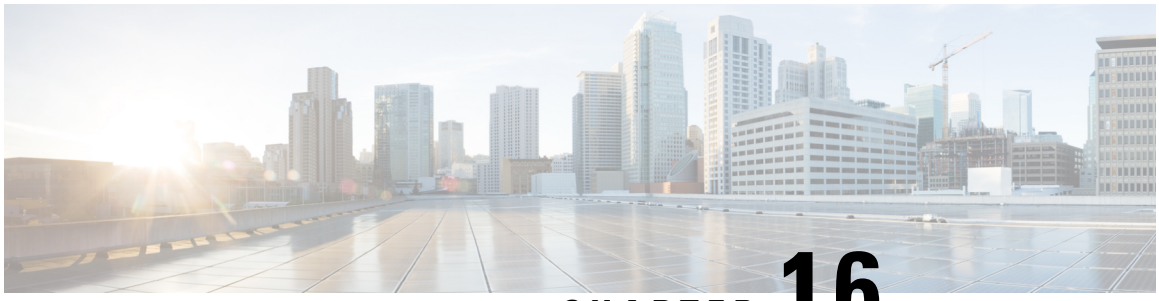
Example

The following example:

- Regenerates a default key ring
- 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 # scope keyring default
```

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



CHAPTER 16

Remote Authentication

Authentication Services

Cisco UCS Central supports the following methods for authenticating user logins:

- Local user authentication for user accounts that exist locally in Cisco UCS Central
- Remote user authentication for registered UCS domains with one of the following protocols:
  - LDAP
  - RADIUS
  - TACACS+

Guidelines and Recommendations for Remote Authentication Providers

If you configure a system 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, 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. You can view the temporary sessions for users who log in through remote authentication services 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, ensure that:

- Accounts include the roles those users require for working in Cisco UCS Central.
- Names of those roles match the names used in Cisco UCS Central.

Depending on the role policy, a user may not have permission to log in, or they may only have read-only privileges.

Local and Remote User Authentication Support

Cisco UCS Central uses LDAP, RADIUS and TACACS+ for remote authentication.

User Attributes in Remote Authentication Providers

When a user logs in, Cisco UCS Central:

1. Queries the remote authentication service.
2. Validates the user.
3. Checks for the roles and locales assigned to that user, (if user passed validation).

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

Table 4: Comparison of User Attributes by Remote Authentication Provider

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
LDAP	Optional	Do one 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 The following section contains a sample OID (object identifier).
RADIUS	Optional	Do one of the following: • Do not extend the RADIUS schema and use an existing unused attribute that meets the requirements. • Extend the RADIUS schema and create a custom attribute with a unique name, such as cisco-avpair.	The vendor ID for the Cisco RADIUS implementation is 009 and the vendor ID for the attribute is 001. The following syntax example specifies 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.

Authentication Provider	Custom Attribute	Schema Extension	Attribute ID Requirements
TACACS+	Required	You must extend the schema and create a custom attribute with the name cisco-av-pair.	The cisco-av-pair name is the string that provides the attribute ID for the TACACS+ provider. The following syntax example specifies 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.

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
```

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 you have configured provider groups and authentication domains in Cisco UCS Central, you can use the following syntax to log in to the system using Cisco UCS Central CLI: **ucs-** *auth-domain*

When you configure multiple authentication domains and native authentication 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 Cisco UCS uses 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 of 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.

Before you begin

Create one or more LDAP providers.

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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create auth-server-group** *auth-server-group-name*	Creates an LDAP provider group. 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. 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 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.

Example

The following example:

- Creates an LDAP provider group called ldapgroup
- Adds two previously configured providers called ldap1 and ldap2 to the provider group
- Sets the order
- 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 # 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
UCSC(policy-mgr) /org/device-profile/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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security 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.

Example

The following example:

- Deletes an LDAP provider group called ldapgroup
- 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 # 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 #
```

Creating a RADIUS Provider Group

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

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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 radius**	Enters RADIUS security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/radius # **create auth-server-group** *auth-server-group-name*	Creates a RADIUS provider group. Enters authentication server group security RADIUS mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # **create server-ref** *radius-provider-name*	Adds the specified RADIUS provider to the RADIUS provider group. Enters server reference authentication server group security RADIUS mode.
Step 8	UCSC(policy-mgr) /org/device-profile/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 9	UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates a RADIUS provider group called radiusgroup
- Adds two previously configured providers called radius1 and radius2 to the provider group
- Sets the order
- 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 # scope radius
UCSC(policy-mgr) /org/device-profile/security/radius # create auth-server-group radiusgroup
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # create server-ref
 radius1
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* # set
order 1
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* # up
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group* # create server-ref
 radius2
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* # set
order 2
UCSC(policy-mgr) /org/device-profile/security/radius/auth-server-group/server-ref* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 radius**	Enters RADIUS security mode.

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

Example

The following example:

- Deletes a RADIUS provider group called radiusgroup
- 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 # scope radius
UCSC(policy-mgr) /org/device-profile/security/radius # delete auth-server-group radiusgroup
UCSC(policy-mgr) /org/device-profile/security/radius* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/radius #
```

Creating a TACACS+ Provider Group

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

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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 tacacs**	Enters TACACS+ security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/tacacs # **create auth-server-group** *auth-server-group-name*	Creates a TACACS+ provider group and enters authentication server group security TACACS+ mode.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # **create server-ref** *ldap-provider-name*	Adds the specified TACACS+ provider to the TACACS+ provider group. Enters server reference authentication server group security TACACS+ mode.
Step 8	UCSC(policy-mgr) /org/device-profile/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 9	UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates a TACACS+ provider group called tacacsgroup
- Adds two previously configured providers called tacacs1 and tacacs2 to the provider group
- Sets the order
- 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 # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # create auth-server-group tacacsgroup
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # create server-ref
 tacacs1
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* # set
order 1
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* # up
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group* # create server-ref
 tacacs2
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* # set
order 2
UCSC(policy-mgr) /org/device-profile/security/tacacs/auth-server-group/server-ref* #
commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 tacacs**	Enters TACACS+ security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/tacacs # **delete auth-server-group** *auth-server-group-name*	Deletes the TACACS+ provider group.
Step 7	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes a TACACS+ provider group called tacacsgroup
- 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 # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # delete auth-server-group tacacsgroup
UCSC(policy-mgr) /org/device-profile/security/tacacs* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs #
```

Authentication Domains

Cisco UCS Central uses authentication domains to leverage multiple authentication systems. You specify and configure each authentication domain during login. If you do not specify an authentication domain, Cisco UCS Central uses the default authentication service configuration.

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.

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**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 are applicable only for the sub-domains in the domain group root and sub-domain groups. **Note** For systems using the remote authentication protocol, the authentication domain name is considered part of the username and counts toward the 32-character limit for locally created usernames. Because Cisco UCS inserts 5 characters for formatting, authentication fails if the domain name and username combined characters total exceeds 27.
Step 7	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **set refresh-period** *seconds*	When a web client connects to Cisco UCS Central, the client must 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 the client exceeds the time limit, Cisco UCS Central considers the web session inactive, but it does not terminate the session. Specify an integer between 60 and 172800. The default is 600 seconds.
Step 8	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **set session-timeout** *seconds*	The maximum amount of time that can elapse after the last refresh request before Cisco UCS Central considers a web session to have ended.

	Command or Action	Purpose
		If the client exceeds the time limit, Cisco UCS Central automatically terminates the web session. Specify an integer between 60 and 172800. The default is 7200 seconds.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # **create default-auth**	Creates a default authentication for the specified authentication domain.
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # **set auth-server-group** *auth-serv-group-name*	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.

Example

The following example:

- Creates an authentication domain called domain1
- Creates a web refresh period of 3600 seconds (1 hour)
- Creates a session timeout period of 14400 seconds (4 hours)
- Configures domain1 to use the providers in ldapgroup1
- Sets the realm type to ldap
- 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 # scope auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # create auth-domain domain1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # set refresh-period
 3600
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # set session-timeout
 14400
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain* # create default-auth
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
auth-server-group ldapgroup1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* # set
realm ldap
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth* #
```

```
commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm/auth-domain/default-auth #
```

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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 # **scope console-auth**	Enters console authorization security mode.
Step 7	UCSC(policy-mgr) /org/device-profile/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
Step 8	UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # **set auth-server-group** *auth-serv-group-name*	The associated provider group, if any.

	Command or Action	Purpose
Step 9	UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the authentication to LDAP
- Sets the console authentication provider group to provider1
- 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 # scope auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # scope console-auth
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth # set realm local
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # set auth-server-group
 provider1
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/auth-realm/console-auth #
```

Selecting a Primary Authentication Service

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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 # **scope default-auth**	Enters default authorization security mode.

	Command or Action	Purpose
Step 7	UCSC(policy-mgr) /org/device-profile/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 • **none**—Allows local users to log on without specifying a password • **radius**—Specifies RADIUS authentication • **tacacs**—Specifies TACACS+ authentication
Step 8	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **set auth-server-group** *auth-serv-group-name*	The associated provider group, if any.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **set refresh-period** *seconds*	When a web client connects to Cisco UCS Central, the client must 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 the client exceeds the time limit, Cisco UCS Central considers the web session inactive, but it does not terminate the session.
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **set session-timeout** *seconds*	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 the client exceeds the time limit, Cisco UCS Central automatically terminates the web session. Specify an integer between 60 and 172800. The default is 7200 seconds.
Step 11	UCSC(policy-mgr) /org/device-profile/security/auth-realm/default-auth* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the default authentication to LDAP
- Sets the default authentication provider group to provider1

- Sets the refresh period to 7200 seconds (2 hours)
- Sets the session timeout period to 28800 seconds (8 hours)
- 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 # scope auth-realm
UCSC(policy-mgr) /org/device-profile/security/auth-realm # scope default-auth
UCSC(policy-mgr) /org/device-profile/security/default-auth # set realm ldap
UCSC(policy-mgr) /org/device-profile/security/default-auth* # set auth-server-group provider1
UCSC(policy-mgr) /org/device-profile/security/default-auth* # set refresh-period 7200
UCSC(policy-mgr) /org/device-profile/security/default-auth* # set session-timeout 28800
UCSC(policy-mgr) /org/device-profile/security/default-auth* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/default-auth #
```

Role Policy for Remote Users

By default, if you do not configure user roles in Cisco UCS Central, then it grants read-only access to all users logging in from a remote server.

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. Cisco UCS Central grants read-only access to all users unless you defined other user roles in Cisco UCS Central.

  This is the default behavior.

- **no-login**

  Restricts user access to Cisco UCS Central based on user roles. If you did not assign user roles for the remote authentication system, access is denied.

For security reasons, you can 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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 # **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 if 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.

Example

The following example:

- Sets the role policy for remote users
- 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 # 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 #
```

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

Create this policy before configuring an HTTP remote access policy in a domain group. Policies in the domain group root were previously created by the system and are ready to configure.

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 sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create http**	If scoping into a domain group previously created, creates the HTTP policy for that domain group.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope http**	If scoping into the domain group root previously created, 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.

Example

The following example:

- Scopes into the domain group root (which has an existing HTTP policy by default)
- Enables the HTTP remote access policy to HTTP redirect mode
- Sets the HTTP service port to 1111
- Commits 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:

- Scopes into the domain group domaingroup01
- Creates the HTTP remote access policy and enable it to HTTP mode
- Sets the HTTP service port to 222
- Commits 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:

- Scopes into the domain group root (which has an existing HTTP policy by default)
- Disables the HTTP remote access policy for HTTP redirect mode
- Commits 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:

- Scopes into the domain group domaingroup01
- Disables the HTTP remote access policy for HTTP mode
- Commits 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

You can delete an HTTP remote access policy from a sub-domain group under the domain group root. You cannot delete HTTP remote access policies in the domain groups root.

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. You cannot delete system default HTTP policies 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.

Example

The following example:

- Scopes into the domain group domaingroup01
- Deletes the HTTP policy for that domain group
- Commits 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 Web Session Limits

Configuring a Web Session Limits Remote Access Policy

Before you begin

Create this policy before configuring a web session limits remote access policy under a domain group. Policies under the domain groups root were already created by the system and 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 sub-domain group under the domain

	Command or Action	Purpose
		group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create web-session-limits**	If scoping into a domain group previously created, creates the web session limits policy for that domain group.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope web-session-limits**	If scoping into the domain group root previously created, 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.

Example

The following example:

- Scopes into the domain group root (which has an existing web sessions limit policy by default)
- Sets the sessions per user limit to 12 sessions
- Sets the total sessions limit to 144 sessions
- Commits 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:

- Scopes into the domain group domaingroup01
- Creates a web sessions limit policy
- Sets the sessions per user limit to 12 sessions
- Sets the total sessions limit to 144 sessions
- Commits 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

You can delete a web session limits remote access policy from a sub-domain group in the domain group root. You cannot delete web session limits remote access policies under the domain groups root.

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 in the domain group root. **Note** Do not enter the domain group root. You cannot delete system default web session limits policies 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.

Example

The following example:

- Scopes into the domain group domaingroup01
- Deletes a web sessions limit policy

- Commits 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

Create the policy before configuring a CIM XML remote access policy in a sub-domain group. Policies under the domain group root were already created by the system and 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 sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create cimxml**	If scoping into a domain group previously created, it creates the CIM XML policy for that domain group.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope cimxml**	If scoping into the domain group root previously created, it 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.

Example

The following example:

- Scopes into the domain group root (which has an existing CIM XML policy by default)
- Enables CIM XML mode
- Commits 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:

- Scopes into the domain group domaingroup01
- Creates a CIM XML policy
- Enables CIM XML mode
- Commits 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

You can delete a CIM XML remote access policy from a sub-domain group in the domain group root. You cannot delete CIM XML remote access policies in the domain group root.

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. You cannot delete system default CIM XML policies under the domain group root.
Step 3	UCSC(policy-mgr) /domain-group # **delete cimxml**	Deletes the CIM XML policy for that domain group.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/cimxml* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group domaingroup01
- Deletes the CIM XML policy
- Commits 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

Create the monitoring remote access policy before configuring it in a domain group. Policies in the domain group root were already created by the system and 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 sub-domain group under the domain group root. To enter the domain group root mode, type **/** as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create mgmt-if-mon-policy**	If scoping into a domain group previously created, creates the management interface monitor policy for that domain group.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope mgmt-if-mon-policy**	If scoping into the domain group root previously created, scopes the default management interface monitors policy's configuration mode from the Domain Group root.

	Command or Action	Purpose
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 (Address Resolution Protocol) 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 considered 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).
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.

Example

The following example:

- Scopes into the domain group root (which has an existing Management Interfaces Monitoring policy by default)

- Enables Management Interfaces Monitoring mode
- Enters the status settings
- Commits 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:

- Scopes into the domain group domaingroup01
- Creates the Management Interfaces Monitoring policy
- Enters the status settings
- Commits 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

You can delete an interfaces monitoring remote access policy from a sub-domain group in the domain group root. You cannot delete interfaces monitoring remote access policies under the domain group root.

Procedure

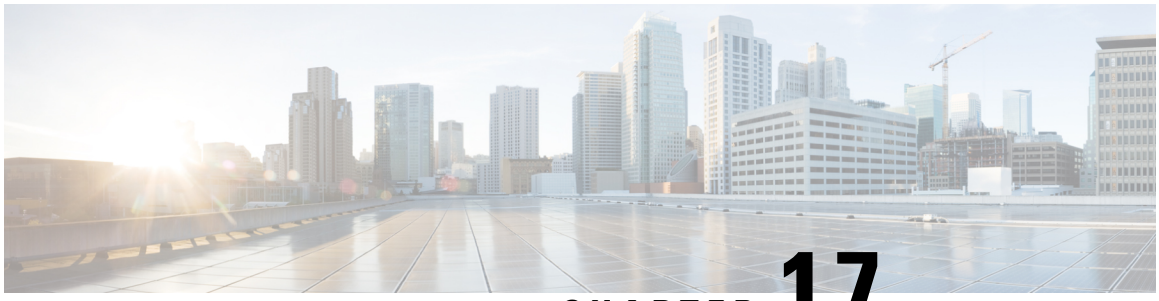
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)# **scope domain-group** *domain-group*	Enters a domain group under the domain group root. **Note** Do not enter the domain group root. You cannot delete system default Management Interfaces Monitoring policies in 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.

Example

The following example:

- Scopes into the domain group domaingroup01
- Deletes the Management Interfaces Monitoring policy
- Commits 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 #
```



CHAPTER 17

LDAP Authentication

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

Create and configure LDAP remote users, and assign roles and locales from Cisco UCS Central, in the same manner as Cisco UCS Manager. Always create the LDAP provider from the Cisco UCS Central domain group root.

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. Give this account 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 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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org#**scope device-profile**	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 LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **create server** *server-name*	• Creates an LDAP server instance • Enters LDAP security server mode

	Command or Action	Purpose
		Note • If SSL is enabled, the server-name must 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	(Optional) UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set attribute** *attribute*	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 name in the LDAP hierarchy, where the server begins a search, when a remote user logs in. After log in, the system attempts to obtain the user's DN based on their username. You can set the length of the base DN to a maximum of 255 characters minus the length of CN=username. Where username identifies the remote user attempting to access Cisco UCS Central 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*	Restricts the LDAP search 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 encryption when communicating with the LDAP server. The options are as follows: • **yes** —Encryption required. If Cisco UCS Central cannot negotiate encryption, the connection fails. • **no** —Encryption disabled. Authentication information sent as clear text.
Step 15	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set timeout** *timeout-num*	If the LDAP provider does not receive an LDAP response within the specified period, it aborts the read attempt.
Step 16	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **set vendor**	Specifies the vendor for the LDAP group. • **ms-ad** —Specifies Microsoft Active Directory. • **openldap** —Specifies OpenLDAP server.
Step 17	UCSC(policy-mgr) /org/device-profile/security/ldap/server* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the organization
- Creates an LDAP server instance named 10.193.169.246
- Configures the binddn
- Configures the password
- Configures the order
- Configures the port

- Configures the SSL settings
- 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 # 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 #
```

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. Give this account 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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org # **scope device-profile**	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 LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **set attribute** *attribute*	Restricts database searches to records that contain the specified attribute.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap* # **set basedn** *distinguished-name*	Restricts database searches to records that contain the specified distinguished name.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap* # **set filter** *filter*	Restricts database searches to records that contain the specified filter.
Step 9	UCSC(policy-mgr) /org/device-profile/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 10	UCSC(policy-mgr) /org/device-profile/security/ldap* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the LDAP attribute to CiscoAvPair
- Sets the base distinguished name to "DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
- Sets the filter to sAMAccountName=$userid
- Sets the timeout interval to 5 seconds
- 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 # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # set attribute CiscoAvPair
UCSC(policy-mgr) /org/device-profile/security/ldap* # set basedn
"DC=cisco-ucsm-aaa3,DC=qalab,DC=com"
UCSC(policy-mgr) /org/device-profile/security/ldap* # set filter sAMAccountName=$userid
UCSC(policy-mgr) /org/device-profile/security/ldap* # set timeout 5
UCSC(policy-mgr) /org/device-profile/security/ldap* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 LDAP security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/ldap # **scope server** *ldap-provider*	Enters security LDAP provider mode.
Step 7	UCSC(policy-mgr) /org/device-profile/security/ldap/server # **scope ldap-group-rule**	Enters LDAP group rule mode.
Step 8	UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule # **set authorization** {**enable** | **disable**}	Specifies if 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 it finds the remote user, 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 9	UCSC(policy-mgr) /org/device-profile/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. The supported string length is 63 characters. The default string is **`memberOf`**.
Step 10	UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # **set traversal** {**non-recursive** | **recursive**}	Specifies if Cisco UCS inherits the settings for a group member's parent group:

	Command or Action	Purpose
		• **non-recursive**—Cisco UCS only searches those groups to which the user belongs. • **recursive**—Cisco UCS searches all of the ancestor groups belonging to the user.
Step 11	UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the LDAP group rule to enable authorization
- Sets the member of attribute to memberOf
- Sets the traversal to non-recursive
- 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 # scope ldap
UCSC(policy-mgr) /org/device-profile/security/ldap # scope server ldapprovider
UCSC(policy-mgr) /org/device-profile/security/ldap/server # scope ldap-group-rule
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule # set authorization
 enable
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # set
member-of-attribute memberOf
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # set traversal
 non-recursive
UCSC(policy-mgr) /org/device-profile/security/ldap/server/ldap-group-rule* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.

	Command or Action	Purpose
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 LDAP security mode.
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.

Example

The following example:

- Deletes the LDAP server called ldap1
- 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 # 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) /org/device-profile/security/ldap #
```

LDAP Group Maps

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

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.

The number of LDAP group maps you can define depends upon the version of Cisco UCS Manager.

You can nest LDAP group maps up to as many levels as the Windows 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 an authenticated member of the parent nested group. During authentication, Cisco UCS Central tries all of the providers within a provider group in order. If Cisco UCS Central cannot reach all of the configured servers, it automatically falls back to the local authentication method using the local username and password.

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

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

- Roles only
- Locales only
- Roles and locales

For 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. You must create a custom locale to map an LDAP provider group to a locale.

Nested LDAP Groups

You can nest LDAP groups as members of other groups to consolidate accounts and reduce replication.

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

You can search nested groups that are defined in LDAP group maps. Nesting groups eliminates the need to create subgroups.

Note Searching nested LDAP groups is supported for Microsoft Active Directory servers only. The supported versions are Microsoft Windows 2003 SP3, Microsoft Windows 2008 R2, and Microsoft Windows 2012.

If you include special characters in nested group names, make sure to escape them using the syntax shown in the following example.

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

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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 LDAP security 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.
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.

Example

The following example:

- Maps the LDAP group mapped to a DN
- Sets the locale to pacific
- Sets the role to admin
- 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 # 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 Group Map

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 LDAP security 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.

Example

The following example:

- Deletes an LDAP group map
- 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 # 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
UCSC(policy-mgr) /org/device-profile/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.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 radius**	Enters RADIUS security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/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 7	UCSC(policy-mgr) /org/device-profile/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 8	UCSC(policy-mgr) /org/device-profile/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the RADIUS retries to 4
- Sets the timeout interval to 30 seconds
- 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 # scope radius
```

```
UCSC(policy-mgr) /org/device-profile/security/radius # set retries 4
UCSC(policy-mgr) /org/device-profile/security/radius* # set timeout 30
UCSC(policy-mgr) /org/device-profile/security/radius* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/radius #
```

What to do next

Create a RADIUS provider.

Creating a RADIUS Provider

Cisco UCS Central supports a maximum of 16 RADIUS providers.

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 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 specifies 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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 radius**	Enters RADIUS security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/radius # **create server** *server-name*	Creates a RADIUS server instance and enters security RADIUS server mode.

	Command or Action	Purpose
Step 7	(Optional) UCSC(policy-mgr) /org/device-profile/security/radius/server* # **set authport** *authport-num*	Specifies the port used to communicate with the RADIUS server.
Step 8	UCSC(policy-mgr) /org/device-profile/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 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/radius/server* # **set order** *order-num*	Specifies when in the order this server is tried.
Step 10	(Optional) UCSC(policy-mgr) /org/device-profile/security/radius/server* # **set retries** *retry-num*	Sets the number of times to retry communicating with the RADIUS server before noting the server as down.
Step 11	(Optional) UCSC(policy-mgr) /org/device-profile/security/radius/server* # **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 12	UCSC(policy-mgr) /org/device-profile/security/radius/server* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates a server instance named radiusserv7
- Sets the authentication port to 5858
- Sets the key to radiuskey321
- Sets the order to 2
- Sets the retries to 4
- Sets the timeout to 30
- 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 # scope radius
UCSC(policy-mgr) /org/device-profile/security/radius # create server radiusserv7
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set authport 5858
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set key
Enter the key: radiuskey321
Confirm the key: radiuskey321
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set order 2
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set retries 4
```

```
UCSC(policy-mgr) /org/device-profile/security/radius/server* # set timeout 30
UCSC(policy-mgr) /org/device-profile/security/radius/server* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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 security policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 radius**	Enters RADIUS security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/radius # **delete server** *serv-name*	Deletes the specified server.
Step 7	UCSC(policy-mgr) /org/device-profile/security/radius* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the RADIUS server called radius1
- 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 # scope radius
UCSC(policy-mgr) /org/device-profile/security/radius # delete server radius1
```

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

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr)#**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 tacacs**	Enters TACACS+ security mode. The TACACS+ related settings are applicable only for the Cisco UCS domains under the domain group root and sub-domain groups.
Step 6	UCSC(policy-mgr) /org/device-profile/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 7	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **set order** *order-num*	Specifies when in the order this server will be tried.
Step 8	UCSC(policy-mgr) /org/device-profile/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 9	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.
Step 10	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Sets the key to tacacskey321
- Sets the order to 4
- Sets the timeout interval to 45 seconds
- Sets the authentication port to 5859
- 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 # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCSC(policy-mgr) /org/device-profile/security/tacacs* # set order 4
UCSC(policy-mgr) /org/device-profile/security/tacacs* # set timeout 45
UCSC(policy-mgr) /org/device-profile/security/tacacs* # set port 5859
UCSC(policy-mgr) /org/device-profile/security/tacacs* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs #
```

What to do next

Create a TACACS+ provider.

Creating a TACACS+ Provider

Cisco UCS Central supports a maximum of 16 TACACS+ providers.

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 specifies 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 org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	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 tacacs**	Enters TACACS+ security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/tacacs # **create server** *server-name*	Creates an TACACS+ server instance and enters security TACACS+ server mode
Step 7	(Optional) UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **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 8	(Optional) UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **set order** *order-num*	Specifies when in the order this server is tried.
Step 9	(Optional) UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **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 10	UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **set port** *port-num*	Specifies the port used to communicate with the TACACS+ server.
Step 11	UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Creates a server instance named tacacsserv680
- Sets the key to tacacskey321
- Sets the order to 4

- Sets the authentication port to 5859
- 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 # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # create server tacacsserv680
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set key
Enter the key: tacacskey321
Confirm the key: tacacskey321
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set order 4
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set timeout 45
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # set port 5859
UCSC(policy-mgr) /org/device-profile/security/tacacs/server* # commit-buffer
UCSC(policy-mgr) /org/device-profile/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

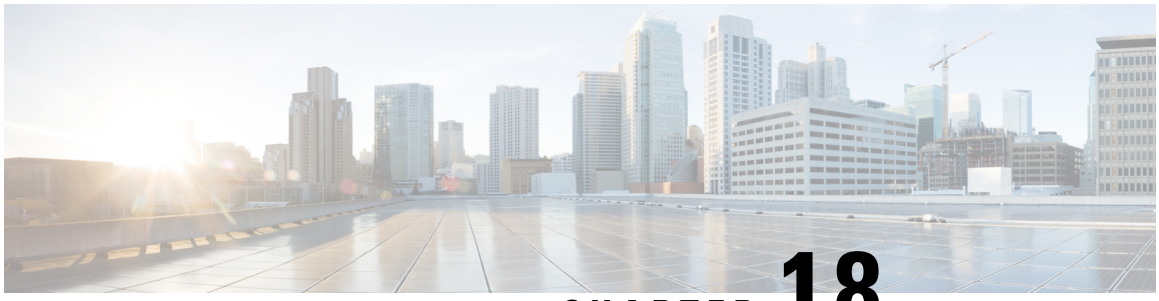
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) #**scope org**	Enters organization mode for the specified organization.
Step 3	UCSC(policy-mgr) /org #**scope device-profile**	Enters device profile mode for the specified organization.
Step 4	UCSC(policy-mgr) /org/device-profile #**scope security**	Enters security mode.
Step 5	UCSC(policy-mgr) /org/device-profile/security # **scope tacacs**	Enters TACACS+ security mode.
Step 6	UCSC(policy-mgr) /org/device-profile/security/tacacs # **delete server** *serv-name*	Deletes the specified server.
Step 7	UCSC(policy-mgr) /org/device-profile/security/tacacs* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Deletes the TACACS server called tacacs1
- 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 # scope tacacs
UCSC(policy-mgr) /org/device-profile/security/tacacs # delete server TACACS1
UCSC(policy-mgr) /org/device-profile/security/tacacs* # commit-buffer
UCSC(policy-mgr) /org/device-profile/security/tacacs #
```



CHAPTER 18

SNMP Authentication

SNMP Policies

Cisco UCS Central supports:

- Global SNMP policies
- Defining SNMP traps and informs
- Defining SNMP users

You can define them 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 defer all SNMP policies to its registration with Cisco UCS Central.

The SNMP Agent functionality remotely monitors 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. The configuration persists 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:

SNMP Manager

System used to control and monitor the activities of network devices using SNMP.

SNMP Agent

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.

Managed Information Base (MIB)

Collection of managed objects in the SNMP agent. Cisco UCS Central supports only the OS MIBs.

For information about the specific MIBs available for Cisco UCS and where you can obtain them, see the MIB Reference for Cisco UCS Manager for B-series servers, and MIB Reference for Cisco UCS Standalone C-Series Servers C-series servers.

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 the SNMP manager send the requests. 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 than Informs because the SNMP manager does not send any acknowledgment when it receives a trap. Therefore, Cisco UCS Central cannot determine if it received the trap.

An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If Cisco UCS Central does not receive the PDU, it can send the inform request again.

SNMP Security Features

SNMPv3 provides secure access to devices through 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 nothing has altered or destroyed any messages in an unauthorized manner. Also ensures that nothing has altered data sequences to an extent greater than can occur non-maliciously.

Message Origin Authentication

Confirms the claimed identity of the user who received the data.

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. A security model is an authentication strategy that is set up for a user and the role in which the user resides. The security model combines with the selected security level to determine the security mechanism applied when Cisco UCS Central processes the SNMP message.

The security level determines the privileges required to view the message associated with an SNMP trap. The security level determines whether Cisco UCS Central must protect the message from disclosure, or authenticate it. The supported security level depends upon which security model is implemented. A combination of a security model and a security level determines which security mechanism is employed when handling an SNMP packet. 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.

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.

Model	Level	Authentication	Encryption	What Happens
v3	authNoPriv	HMAC-MD5 or HMAC-SHA	No	Provides authentication based on: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA)
v3	authPriv	HMAC-MD5 or HMAC-SHA	DES	Provides authentication based on: • Hash-based Message Authentication code (HMAC) • Message Digest 5 (MD5) algorithm • HMAC Secure Hash algorithm (SHA) • Provides Data Encryption Standard (DES) 56-bit encryption. • Provides 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 and Cisco 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 uses Advanced Encryption Standard (AES) as one of the privacy protocols for SNMPv3 message encryption and conforms with RFC 3826.

The privacy password, or priv option, offers a choice of DES or 128-bit AES encryption for SNMP security encryption. If you enable AES-128 configuration and include a privacy password for an SNMPv3 user, Cisco UCS 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

You can configure policies in the domain group root. You can also create new policies.

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 sub-domain group under the domain group root. To enter the domain group root mode, type / as the *domain-group*.
Step 3	(Optional) UCSC(policy-mgr) /domain-group # **create snmp**	If scoped into a domain group previously created, it creates the SNMP policy for that domain group.
Step 4	(Optional) UCSC(policy-mgr) /domain-group # **scope snmp**	If scoping into the domain group root previously created, it scopes the default SNMP policy's configuration mode from the domain group root.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **enable** | **disable snmp**	Enables or disable SNMP services for this policy.
Step 6	UCSC(policy-mgr) /domain-group/snmp* # **set snmp community** *snmp-community-name-text*	Enters a name for the SNMP community.
Step 7	UCSC(policy-mgr) /domain-group/snmp* # **set snmp syscontact** *syscontact-name-text*	Enters a name for the SNMP system contact.
Step 8	UCSC(policy-mgr) /domain-group/snmp* # **set snmp syslocation** *syslocation-name-text*	Enters a name for the SNMP system location.
Step 9	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Enables SNMP services
- Sets the SNMP community name to SNMPCommunity01
- Sets the SNMP system contact name to SNMPSysAdmin01
- Sets the SNMP system location to SNMPWestCoast01
- Commits 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 snmp community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
```

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

The following example:

- Scopes into the domain group domaingroup01
- Creates the SNMP policy
- Enables SNMP services
- Sets the SNMP community name to SNMPCommunity01
- Sets the SNMP system contact name to SNMPSysAdmin01
- Sets the SNMP system location to SNMPWestCoast01
- Commits 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 snmp community SNMPCommunity01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syscontact SNMPSysAdmin01
UCSC(policy-mgr) /domain-group/snmp* # set snmp syslocation SNMPWestCoast01
UCSC(policy-mgr) /domain-group/snmp* # commit-buffer
UCSC(policy-mgr) /domain-group/snmp #
```

The following example:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Disables SNMP services
- Commits 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 sub-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 snmp**	Scopes the default SNMP policy's configuration mode.
Step 4	(Optional) UCSC(policy-mgr) /domain-group/snmp # **create snmp-trap** *snmp-trap-ip*	If scoped into a domain group previously created, it creates the snmp-trap IP address for that domain group (in format 0.0.0.0), and enters SNMP trap configuration mode.
Step 5	(Optional) UCSC(policy-mgr) /domain-group/snmp # **scope snmp-trap** *snmp-trap-ip*	If scoped into the domain group root, it 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.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Creates the SNMP trap with IP address 0.0.0.0
- Sets the SNMP community host string to snmptrap01
- Sets the SNMP notification type to traps
- Sets the SNMP port to 1

- Sets the v3privilege to priv
- Sets the version to v1
- Commits 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:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Scopes the SNMP trap with IP address 0.0.0.0
- Sets the SNMP community host string to snmptrap02
- Sets the SNMP notification type to traps
- Sets the SNMP port to 65535
- Sets the v3privilege to auth
- Sets the version to v2c
- Commits 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.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-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*	Enters a name for the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set aes-128 yes** | **no**	Uses AES-128 for the SNMP user (yes or no).
Step 6	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set auth md5** | **sha**	Uses MD5 or SHA authorization mode for the SNMP user.
Step 7	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set password** *password*	Enters and confirm a password for the SNMP user.
Step 8	UCSC(policy-mgr) /domain-group/snmp/snmp-user* # **set priv-password** *private-password*	Enters 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.

Example

The following example:

- Scopes into the domain group root
- Scopes into the SNMP user named snmpuser01
- Sets aes-128 mode to enabled,
- Sets authorization to sha mode
- Sets password to userpassword01,
- Sets private password to userpassword02
- Commits 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:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Creates into the SNMP user named snmpuser01
- Sets aes-128 mode to enabled,
- Sets authorization to MD5 mode
- Sets password to userpassword01,
- Sets private password to userpassword02
- Commits 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:

- Scopes into the domain group root
- Scopes the SNMP policy
- Scopes into the SNMP user named snmpuser01
- Sets aes-128 mode to disnabled
- Sets authorization to MD5 mode
- Commits 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

You can delete an SNMP policy from a sub-domain group of the domain group root. You cannot delete SNMP policies that reside in the domain group root.

Deleting an SNMP policy removes 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 sub-domain group under the domain group root. **Note** Do not enter the domain group root. You cannot delete system default management interfaces monitoring policies in 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.

Example

The following example:

- Scopes into the domain group domaingroup01
- Deletes the SNMP policy
- Commits 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 sub-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.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Deletes the SNMP trap IP address 0.0.0.0
- Commits 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:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Deletes the SNMP trap IP address 0.0.0.0
- Commits 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 sub-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*	Deletes the SNMP user.
Step 5	UCSC(policy-mgr) /domain-group/snmp* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example:

- Scopes into the domain group root
- Scopes the SNMP policy
- Deletes the SNMP user named snmpuser01
- Commits 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 #
```

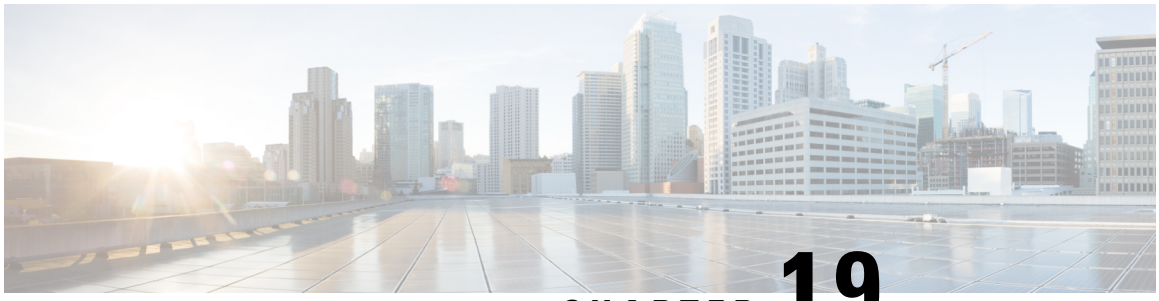
The followings example:

- Scopes into the domain group domaingroup01
- Scopes the SNMP policy
- Deletes the SNMP user named snmpuser02
- Commits 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 #
```

PART IV

Server Management



CHAPTER 19

Cisco UCS Servers

Server Management

With global policies, global server pools and firmware management in Cisco UCS Central, you can manage general and complex server deployments for the following servers in your registered UCS domains:

- Cisco UCS B-Series Blade Servers
- Cisco UCS C-Series Rack-Mount Servers
- Cisco UCS Mini

Equipment Policies

Equipment policies allow you to tune your servers and other equipment to suit your requirements. Equipment policies can only be set at the domain group level, and apply to all servers in that domain group.

Note Equipment policies are not included in service profiles.

Configuring the Chassis/FEX Discovery 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 sub-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 chassis-disc-policy**	Enters organization chassis/FEX discovery policy mode.
Step 4	UCSC(policy-mgr) /domain-group/chassis-disc-policy # **set action** {**1-link** | **2-link** | **4-link** | **8-link** | **platform-max**}	Specifies the minimum threshold for the number of links between the chassis or FEX and the fabric interconnect.
Step 5	UCSC(policy-mgr) /domain-group/chassis-disc-policy # **set link-aggregation-pref** {**none** | **port-channel**}	Specifies whether the links from the IOMs or FEXes to the fabric interconnects are grouped in a port channel. **Note** The link grouping preference only takes effect if both sides of the links between an IOM or FEX and the fabric interconnect support fabric port channels. If one side of the links does not support fabric port channels, this preference is ignored and the links are not grouped in a port channel.
Step 6	UCSC(policy-mgr) /domain-group/chassis-disc-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Configure the chassis discovery policy to discovery chassis with four links to a fabric interconnect
- Set the link grouping preference to port channel

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope chassis-disc-policy
UCSC(policy-mgr) /domain-group/chassis-disc-policy # set action 4-link
UCSC(policy-mgr) /domain-group/chassis-disc-policy* # set link-aggregation-pref port-channel
UCSC(policy-mgr) /domain-group/chassis-disc-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/chassis-disc-policy #
```

Configuring the Rack Server Discovery 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 sub-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 rackserver-disc-policy**	Enters rack server discovery policy mode.
Step 4	UCSC(policy-mgr) /domain-group/rackserver-disc-policy # **set action** {**immediate** | **user-acknowledged**}	Specifies the way the system reacts when you add a new rack server.
Step 5	UCSC(policy-mgr) /domain-group/rackserver-disc-policy # **set scrub-policy** *policy-name*	Specifies the scrub policy that should run on a newly discovered rack server.
Step 6	UCSC(policy-mgr) /domain-group/rackserver-disc-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Set the rack server discovery policy to immediately discover new rack servers
- Specify the scrub policy ScrubPol1

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # scope rackserver-disc-policy
UCSC(policy-mgr) /domain-group/rackserver-disc-policy # set action immediate
UCSC(policy-mgr) /domain-group/rackserver-disc-policy # set scrub-policy ScrubPol1
UCSC(policy-mgr) /domain-group/rackserver-disc-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/rackserver-disc-policy #
```

Configuring the Rack Management Connection 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 sub-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 server-management-connectivity-policy**	Enters server management connectivity policy mode.
Step 4	UCSC(policy-mgr) /domain-group/server-management-connectivity-policy # **set action** {**auto-acknowledged** | **user-acknowledged**}	Select whether servers are automatically configured based on the available server connections.
Step 5	UCSC(policy-mgr) /domain-group/server-management-connectivity-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to configure the rack management connection policy to wait for user acknowledgment.

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope scope server-management-connectivity-policy
UCSC(policy-mgr) /domain-group/server-management-connectivity-policy # set action
user-acknowledged
UCSC(policy-mgr) /domain-group/server-management-connectivity-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/server-management-connectivity-policy #
```

Configure MAC Address Table Aging 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 sub-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 lan-cloud**	Enters LAN cloud mode.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /domain-group/lan-cloud # **set mac-aging** {*time* | **mode-default** | **never**}	Specify the length of time an idle MAC address remains in the MAC address table before it is removed. This can be one of the following: • *time*—Enter the number of days, hours, minutes, and seconds in the following format: dd hh mm ss. • mode-default—The system uses the default value. For end-host mode, the default is 14,500 seconds. For switching mode, the default is 300 seconds. • never—MAC addresses are never removed from the table.
Step 5	UCSC(policy-mgr) /domain-group/lan-cloud # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to set the MAC table aging to never.

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope lan-cloud
UCSC(policy-mgr) /domain-group/lan-cloud # set mac-aging never
UCSC(policy-mgr) /domain-group/lan-cloud* # commit-buffer
UCSC(policy-mgr) /domain-group/lan-cloud #
```

Setting VLAN Port Count Optimization

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 sub-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 lan-cloud**	Enters LAN cloud mode.
Step 4	UCSC(policy-mgr) /domain-group/lan-cloud # **set vlan-compression** {**enabled** | **disabled**}	Select whether VLAN port count optimization is enabled or disabled.
Step 5	UCSC(policy-mgr) /domain-group/lan-cloud # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to enable VLAN port count optimization.

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope lan-cloud
UCSC(policy-mgr) /domain-group/lan-cloud # set vlan-compression enabled
UCSC(policy-mgr) /domain-group/lan-cloud* # commit-buffer
UCSC(policy-mgr) /domain-group/lan-cloud #
```

Configuring an Information 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 sub-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 info-policy**	Enters information policy mode.
Step 4	UCSC(policy-mgr) /domain-group/info-policy # **set state** {**enabled** | **disabled**}	Select whether the information policy will display the uplink switches that are connected to the Cisco UCS domain.
Step 5	UCSC(policy-mgr) /domain-group/info-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to configure the information policy to display the uplink switches.

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope info-policy
UCSC(policy-mgr) /domain-group/info-policy # set state enabled
UCSC(policy-mgr) /domain-group/info-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/info-policy #
```

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 the power control 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	Required: UCSC(policy-mgr) /org/power-control-policy # **set priority** {*priority-num* | **no-cap**}	Specifies the priority for the power control policy.
Step 5	Required: UCSC(policy-mgr) /org/power-control-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

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.
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	Required: UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

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 #
```

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

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.

Example

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.

Example

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.

	Command or Action	Purpose
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.

Example

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.

Example

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.

Example

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.

Example

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.

Example

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.

Example

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

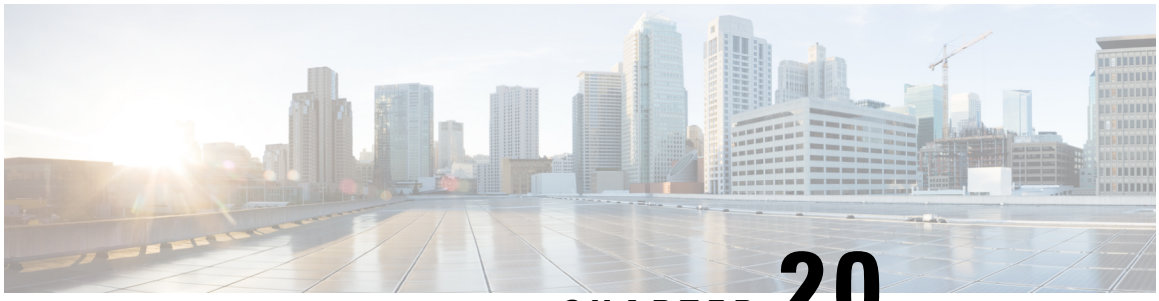
Procedure

	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.
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.

Example

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 20

Service Profiles and Templates

Global Service Profiles

Global service profiles centralize the logical configuration deployed 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	(Optional) UCSC(resource-mgr) /org/service-profile # **set descr** *description*	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.

Example

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

	Command or Action	Purpose
		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.

Example

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

	Command or Action	Purpose
		unavailable, choose **a-b** (A is the primary) or **b-a** (B is the primary) . **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.

	Command or Action	Purpose
		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.
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.

Example

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*.
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,

	Command or Action	Purpose
		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.
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.

Example

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.
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.

Example

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.
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.

Example

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.

Example

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.
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.

Example

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.

Example

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.
Step 6	(Optional) UCSC(resource-mgr) /org/service-profile # **set descr** *description*	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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
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.
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.

	Command or Action	Purpose
		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.

Example

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

UUID Synchronization Behavior

For Cisco UCS M3 and greater server models, the UUID that is configured in Cisco UCS Manager is not synchronized with the UUID that is seen by the operating systems running on those servers. UUID synchronization flips the prefix of the UUID in Cisco UCS Manager to match the UUID on the server operating system. By default, the UUIDs are unsynchronized.

Note Changing the UUID synchronization behavior may cause the server to reboot.

The following guidelines apply to UUID synchronization:

- UUID synchronization is supported only for global service profiles.
- UUID synchronization is supported only on the following Cisco UCS Manager releases:
  - Cisco UCS Manager release 2.2(7) and above
  - Cisco UCS Manager release 3.1(2) and above
- UUID synchronization is not applicable on Cisco UCS M1 and M2 server models.
- If UUID synchronization is enabled, you must disable UUID synchronization before downgrading or upgrading to a Cisco UCS Manager version that does not support UUID synchronization.
- When changing the service profile to which a server is associated:
  - Cisco UCS M1 and M2 server models are automatically synchronized at association.
  - If synchronization is enabled, Cisco UCS M3 and greater server models are automatically synchronized at association
  - If synchronization is not enabled, Cisco UCS M3 and greater server models are not synchronized at association.

Configuring UUID Synchronization Behavior

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 # **set uuid-behavior write-mode** [**sync** | **unsync**]	Enables or disables UUID synchronization.
Step 5	UCSC(resource-mgr) /org/service-profile # **commit-buffer**	Sets the UUID synchronization.

Example

The following example shows how to enable UUID synchronization for service profile ServProf2 and commit 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* # set uuid-behavior write-mode sync
Warning: When committed, this command will require a server reboot if a custom UUID is
configured in the service profile
UCSC(resource-mgr) /org/service-profile* # commit-buffer
UCSC(resource-mgr) /org/service-profile #
```

Changing the Service Profile Association

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 # **associate server** {*rack-server-id* |	Associates the service profile with the specified server. Choose one of the following:

	Command or Action	Purpose
	chassis-id/*blade-server-id* | *chassis-id*/*cartridge-id*/*server-id*}	• **rack-server-id**—For C-Series Rack servers, enter the rack server ID. • **chassis-id/blade-server-id**—For B-Series Blade servers, enter the chassis ID and the blade server ID. • **chassis-id/cartridge-id/server-id**—For M-Series Modular servers, enter the chassis ID, cartridge ID, and the server ID for the cartridge.
Step 5	UCSC(resource-mgr) /org/service-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to change the service profile association to a C-Series Rack server and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # scope service-profile GSP1
UCSC(resource-mgr) /org/service-profile # associate server 3
UCSC(resource-mgr) /org/service-profile* # commit-buffer
UCSC(resource-mgr) /org/service-profile #
```

The following example shows how to change the service profile association to a B-Series Blade server and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # scope service-profile GSP2
UCSC(resource-mgr) /org/service-profile # associate server 1/1
UCSC(resource-mgr) /org/service-profile* # commit-buffer
UCSC(resource-mgr) /org/service-profile #
```

The following example shows how to change the service profile association to an M-Series Modular server and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # scope service-profile GSP3
UCSC(resource-mgr) /org/service-profile # associate server 1/4/2
UCSC(resource-mgr) /org/service-profile* # commit-buffer
UCSC(resource-mgr) /org/service-profile #
```

Scheduling Service Profile Updates

Service Profile Deferred Deployments

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 acknowledgment.

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 , 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
- Re-acknowledging 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 Deployments

Service Profile Association Changes and Maintenance Policy Options

When changing service profile association, the following maintenance policy options can affect how the changes are applied:

- If the **On Next Boot** and **User Ack** options are enabled in a maintenance policy, the service profile association change displays a warning that an acknowledgement is required. However, association will happen immediately.
- If the **On Next Boot** and **User Ack** options are not enabled in a maintenance policy, the service profile association change displays a warning that an acknowledgement is required, and will remain pending until acknowledged.

Cannot Undo All Changes to Service Profiles or Service Profile Templates

If you cancel a pending change, attempts to roll back the change without rebooting the server. However, for complex changes, may have to reboot the server a second time to roll back the change. For example, if you delete a vNIC, 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, schedules a second deployment and reboot of the server.

Association of Service Profile Can Exceed Boundaries of Maintenance Window

After 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

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 deploys the service profile changes, it updates the service profile to match the most recent configuration in the database.

Schedules for Deferred Deployments

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 was reached, that deployment is carried over to the next maintenance window.

Each schedule checks periodically to see whether the Cisco UCS domain entered one or more maintenance windows. If so, 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 is 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 was reached.

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 sub-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.

Example

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 sub-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.

	Command or Action	Purpose
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.

Example

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.

	Command or Action	Purpose
Step 2	UCSC(policy-mgr) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-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. **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.

	Command or Action	Purpose
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.

Example

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 #
```

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 acknowledgment 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.

You can view the following information related to pending activities:

- 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

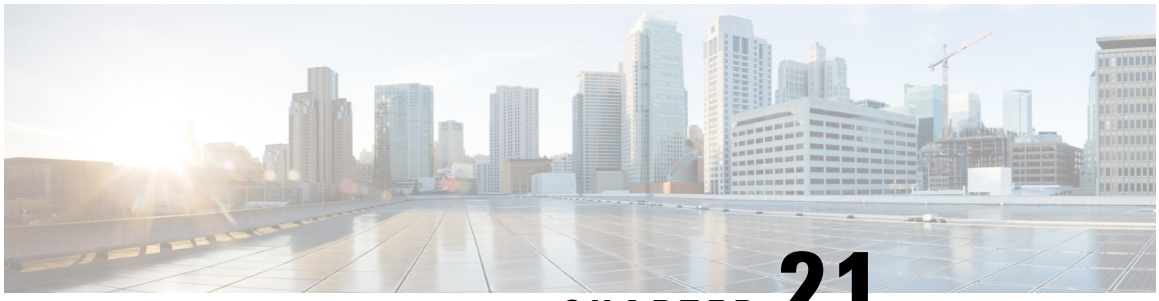
Note You cannot specify the maintenance window in which a specific pending activity is applied to the server. The maintenance window depends upon how many activities are pending and which maintenance policy is assigned to the service profile. However, any user with admin privileges can manually initiate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

From Cisco UCS Central GUI you can view the pending activities from the following two locations:

- From **Servers** on the menu bar, click **Servers** > **Pending Activities**. Pending activities are displayed in two tabs, such as **User Acknowledged Activities** and **Scheduled Activities**.
- The Cisco UCS Central GUI displays a fault summary panel above the menu bar with the following information in dynamic display. You can click one of the following three options to launch associated page on Cisco UCS Central GUI.
  - **UCS Central Fault Summary**
  - **UCS Domains Fault Summary**
  - **Pending Activities**

When the display is on **Pending Activities**, click on the panel to go to **Servers** > **Pending Activities** and view details.

Important Top level summary panel does not display pending activities caused by local service profile using a local maintenance policy with local scheduler. These pending activities must be acknowledged from Cisco UCS Manager..



CHAPTER 21

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.

When you select a specific server pool, you can view the individual details for that pool, including the number of servers included in the pool, and the associated qualification policies.

Creating 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*.

	Command or Action	Purpose
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** {*[1-255 Rack ID | n/n (<chassis-id>/<blade-id>) | n/n/n <chassis-id>/<cartridge-id>/<server-unit-id>*] **ucs-domain** *hostname*}	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.

Example

The following example shows how to create the server pool named ServPool2 which includes two servers:

```
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 ucs-domain 1008
UCSC(resource-mgr) /org/server-pool* # create server 1/4/6 ucs-domain 1008
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.
Step 4	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete the server pool named ServPool2:

```
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 #
```

Server Pool Qualification Policy

The server pool qualification policy qualifies servers based on the server inventory conducted during the discovery process. You can configure these qualifications or individual rules in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it. You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration
- Storage configuration and capacity
- Server model or server type
- Owner
- Site
- Address
- Domain group
- Domain name
- Product family

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*.

	Command or Action	Purpose
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.

Example

The following example shows how to create a server pool qualification named ServPoolQual22:

```
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.

Example

The following example shows how to add a domain qualification to a server pool policy qualification:

```
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 adapter capacity qualification mode. The *adapter-type* argument can be any of the following values: • **fcoe**—Fibre Channel over Ethernet (FCoE) • **non-virtualized-eth-if**—Ethernet • **non-virtualized-fc-if**—Fiber Channel (FC) • **path-encap-consolidated**—Consolidated Path Encapsulation • **path-encap-virtual**—Virtual Path Encapsulation • **protected-eth-if**—Protected Ethernet • **protected-fc-if**—Protected Fibre Channel (FC) • **protected-fcoe**—Protected Fibre Channel over Ethernet (FCoE) • **uplink-aggregation**—Uplink Aggregation • **virtualized-eth-if**—Virtual Ethernet • **virtualized-eth-sriov**—Virtual Ethernet SRIOV • **virtualized-fc-if**—Virtual Fibre Channel (FC) • **virtualized-fc-sriov**—Virtual FC SRIOV

	Command or Action	Purpose
		• **virtualized-scsi-if**—Virtual iSCSI
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.

Example

The following example shows how to add a domain qualification to a server pool policy qualification:

```
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.

Example

The following example deletes the server pool qualification named ServPoolQual22:

```
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 #
```

IP Pools

IP pools are a collection of IP IPv4 or IPv6 addresses. You can use IP pools in Cisco UCS Central in one of the following ways:

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

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

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

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

Cisco UCS Central creates public IP pools by default.

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

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

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.

	Command or Action	Purpose
Step 4	(Optional) UCSC(policy-mgr) /org/ip-pool # **set descr** *description*	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 primary-dns** *ip-address* **secondary-dns** *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.

Example

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 primary-dns 192.168.100.1 secondary-dns
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 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	(Optional) UCSC(policy-mgr) /org/ip-pool # **set descr** *description*	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.

Example

The following example shows how to create an IP pool with an 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, does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. 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.

Example

The following example shows how to delete the IP pool named GPool1:

```
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 #
```

IQN Pools

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

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

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

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	(Optional) UCSC(policy-mgr) /org/iqn-pool # **set descr** *description*	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

	Command or Action	Purpose
		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.
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.

Example

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 for the pool
- 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 template.

Deleting an IQN Pool

If you delete a pool, does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. 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 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.

Example

The following example shows how to delete the IQN pool named GPool1:

```
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 #
```

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 values. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile. Assigning global UUID suffix pools from Cisco UCS Central to service profiles in Cisco UCS Central or Cisco UCS Manager allows them to be shared across Cisco UCS domains.

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*.
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	(Optional) UCSC(policy-mgr) /org/uuid-suffix-pool # **set descr** *description*	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.

Example

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 for the pool

```
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, does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. 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.

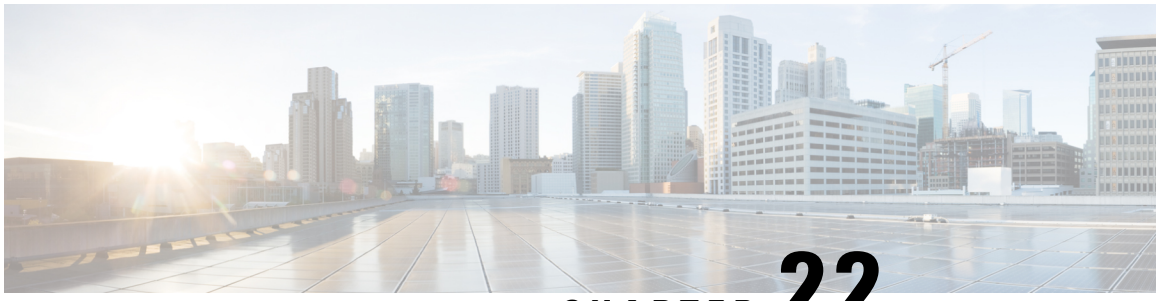
Procedure

	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.

Example

The following example shows how to delete the UUID suffix pool named GPool1:

```
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 #
```



CHAPTER 22

Server Boot

This chapter includes the following sections:

Boot Policy

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

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

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

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

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

Boot Order

Cisco UCS Central enables you to use standard or enhanced boot order for the global boot policies you create in Cisco UCS Central.

- Standard boot order is supported for all Cisco UCS servers, and allows a limited selection of boot order choices. You can add a local device, such as a local disk, CD-ROM, or floppy, or you can add SAN, LAN, or iSCSI boot.
- Enhanced boot order allows you greater control over the boot devices that you select for your boot policy. Enhanced boot order is supported for all Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers at release 2.2(1b) or greater.

The following boot order devices are supported for standard boot order, but can be used with both:

- **Local LUN/Local Disk**—Enables standard boot from a local hard disk. Do not enter a primary or secondary LUN name. Those are reserved for enhanced boot order only.
- **CD/DVD ROM Boot**—Enables standard boot from local CD/DVD ROM drive.
- **Floppy**—Enables standard boot from local floppy drive.
- **LAN Boot**—Enables standard boot from a specified vNIC.
- **SAN Boot**—Enables standard boot from a specified vHBA.
- **iSCSI Boot**—Enables standard boot from a specified iSCSI vNIC.

The following boot order devices are supported only for enhanced boot order:

- **Local LUN/Local Disk**—Enables boot from local hard disk, or local LUN.
- **Local CD/DVD**—Enables boot from local CD/DVD drive.
- **Local Floppy**—Enables boot from local floppy drive.
- **SD Card**—Enables boot from SD Card.
- **Internal USB**—Enables boot from Internal USB.
- **External USB**—Enables boot from External USB.
- **Embedded Local Disk**—Enables booting from the embedded local disk on the Cisco UCS C240 M4SX and C240 M4L servers.

Note You can add either the embedded local disk or the embedded local LUN to the boot order. Adding both is not supported.

- **Embedded Local LUN**—Enables boot from the embedded local LUN on the Cisco UCS C240 M4SX and C240 M4L servers.

  Note You can add either the embedded local disk or the embedded local LUN to the boot order. Adding both is not supported.

- **Local JBOD**—Enables boot from a local disk.
- **KVM Mapped CD/DVD**—Enables boot from KVM mapped ISO images.
- **KVM Mapped Floppy**—Enables boot from KVM mapped image files.
- **CIMC Mapped HDD**—Enables boot from CIMC mapped vMedia drives.
- **CIMC MAPPED CD/DVD**—Enables boot from CIMC mapped vMedia CDs and DVDs.
- **LAN Boot**—Enables you to select a specific vNIC from which to boot.
- **SAN Boot**—Enables you to select a specific vHBA from which to boot.
- **iSCSI Boot**—Enables you to select a specific iSCSI vNIC from which to boot.
- **Remote Virtual Drive**—Enables boot from a remote virtual drive.

Note

- If a boot policy with enhanced boot order is applied to Cisco UCS M1 and M2 blade and rack servers, or to Cisco UCS M3 blade and rack servers with a release prior to Release 2.2(1b) installed, the association fails with configuration errors.
- You must enable USB for Virtual Media. If you modify the BIOS settings, that in turn affects the Virtual media. The following USB BIOS default settings are recommended for best performance:
  - **Make Device Non Bootable**—set to disabled
  - **USB Idle Power Optimizing Setting**—set to high-performance

UEFI Boot Mode

Unified Extensible Firmware Interface (UEFI) is a specification that defines a software interface between an operating system and platform firmware. Cisco UCS uses UEFI to replace the BIOS firmware interfaces. This allows the BIOS to run in UEFI mode while still providing legacy support.

You can choose either legacy or UEFI boot mode when you create a boot policy. Legacy boot mode is supported for all Cisco UCS servers. UEFI boot mode is supported on Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and M4 Rack Servers, and allows you to enable UEFI secure boot mode.

The following limitations apply to the UEFI boot mode:

- UEFI boot mode is not supported on Cisco UCS B-Series M1 and M2 Blade Servers and Cisco UCS C-Series M1 and M2 Rack Servers.

- UEFI boot mode is not supported with the following combinations:
  - Gen-3 Emulex & QLogic adapters on Cisco UCS blade & rack servers integrated with Cisco UCS domain.
  - PXE boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS domain.
  - iSCSI boot for all adapters on Cisco UCS rack servers integrated with Cisco UCS domain.
- You cannot mix UEFI and legacy boot mode on the same server.
- Make sure an UEFI-aware operating system is installed in the device. The server will boot correctly in UEFI mode only if the boot devices configured in the boot policy have UEFI-aware OS installed. If a compatible OS is not present, the boot device is not displayed on the **Boot Policies** page.
- In some corner cases, the UEFI boot may not succeed because the UEFI boot manager entry was not saved correctly in the BIOS NVRAM. You can use the UEFI shell to enter the UEFI boot manager entry manually. This situation could occur in the following situations:
  - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and the blade is manually powered on using the **Server** page or the front panel.
  - If a blade server with UEFI boot mode enabled is disassociated from the service profile, and a direct VIC firmware upgrade is attempted.
  - If a blade or rack server with UEFI boot mode enabled is booted off SAN LUN, and the service profile is migrated.

UEFI Secure Boot

Cisco UCS Central supports UEFI secure boot on Cisco UCS B-Series M3 and M4 Blade Servers and Cisco UCS C-Series M3 and Rack Servers. When UEFI secure boot is enabled, all executables, such as boot loaders and adapter drivers, are authenticated by the BIOS before they can be loaded. To be authenticated, the images must be signed by either the Cisco Certificate Authority (CA) or a Microsoft CA.

The following limitations apply to UEFI secure boot:

- UEFI boot mode must be enabled in the boot policy.
- The Cisco UCS Manager software and the BIOS firmware must be at Release 2.2 or greater.
- User-generated encryption keys are not supported.
- UEFI secure boot can only be controlled by Cisco UCS Manager or Cisco UCS Central.
- If you want to downgrade to an earlier version of Cisco UCS Manager, and you have a blade server in secure boot mode, you must disassociate and reassociate the blade server before downgrading. Otherwise, the blade will not be discovered successfully.

Cautions and Guidelines for Downgrading a Boot Policy

You cannot downgrade to an earlier version of Cisco UCS Manager if:

- An associated server has a boot policy with UEFI boot mode enabled.

- An associated server has a boot policy with UEFI secure boot enabled.
- An associated server has a boot policy with enhanced boot order. For example, if an associated server has a boot policy which contains any of the following:
  - SD card
  - Internal USB
  - External USB
- An associated server has a boot policy that includes both SAN and local LUN.

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. Only use it if instructed to do so by a Cisco representative.
Step 4	(Optional) UCSC(policy-mgr) /org/boot-policy # **set descr** *description*	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.

	Command or Action	Purpose
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 boot-mode** {**legacy** | **uefi**}	Specifies whether the servers using this boot policy are using UEFI or legacy boot mode.
Step 7	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.
Step 8	UCSC(policy-mgr) /org/boot-policy # **commit-buffer**	Commits the transaction to the system configuration.
Step 9	UCSC(policy-mgr) /org/boot-policy # **create boot-security**	Enters boot security mode for the specified boot policy.
Step 10	UCSC(policy-mgr) /org/boot-policy/boot-security # **set secure-boot** {**no** | **yes**}	Specifies whether secure boot is enabled for the boot policy.
Step 11	UCSC(policy-mgr) /org/boot-policy/boot-security # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following shows how to:

- Create a boot policy named boot-policy-LAN
- Provide a description for the boot policy
- Specify that servers using this policy will not automatically reboot when the boot order is changed

```
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* # set boot-mode uefi
UCSC(policy-mgr) /org/boot-policy* # commit-buffer
UCSC(policy-mgr) /org/boot-policy* # create boot-security
UCSC(policy-mgr) /org/boot-policy* # set secure-boot yes
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, on page 432:

- **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 437.

- **SAN 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 SAN Boot option, continue to Configuring a SAN Boot for a Boot Policy, on page 439.

- **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 449.

- **Local Disk Boot**—Boots from local storage.

  If you choose the Local Disk Boot option, continue to Configuring a Local Disk Boot for a Boot Policy, on page 447.

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.

	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 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.

Example

The following example shows how to:

- Enter the boot policy named lab2-boot-policy
- Create a LAN boot for the policy
- Set the boot order to 2
- Create primary and secondary paths using the vNICs named vNIC1 and vNIC2

```
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.

Cisco recommends using 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 same operating system image. Therefore, the new server appears as the 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 (Logical Unit Number) 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 and 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 SAN 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 SAN 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 SAN 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 435.

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 san**	Creates a SAN boot for the boot policy and enters organization boot policy san mode.
Step 5	UCSC(policy-mgr) /org/boot-policy/san # **set order** *order_num*	Sets the boot order for the SAN boot. Enter a number between 1 and 16.
Step 6	UCSC(policy-mgr) /org/boot-policy/san # **create san-image** {**primary** | **secondary**}	Creates a SAN image location, and if the san-image option is specified, enters organization boot policy 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/san/san-image # **set vhba** *vhba-name*	Specifies the vHBA to be used for the SAN boot.
Step 8	UCSC(policy-mgr) /org/boot-policy/san/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/san/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/san/san-image/path # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Enter the boot policy named lab1-boot-policy
- Create a SAN boot for the policy
- Set the boot order to 1
- Create a primary SAN image
- Use a vHBA named vHBA2
- Create a primary path using LUN 967295200

```
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 san
UCSC(policy-mgr) /org/boot-policy/san* # set order 1
UCSC(policy-mgr) /org/boot-policy/san* # create san-image primary
UCSC(policy-mgr) /org/boot-policy/san* # set vhba vHBA2
UCSC(policy-mgr) /org/boot-policy/san/san-image* # create path primary
UCSC(policy-mgr) /org/boot-policy/san/san-image/path* # set lun 967295200
UCSC(policy-mgr) /org/boot-policy/san/san-image/path* # commit-buffer
UCSC(policy-mgr) /org/boot-policy/san/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 VIC 1225 Virtual Interface Cardon Cisco UCS rack servers

There are prerequisites that must be met before you configure iSCSI boot. For a list of these prerequisites, see Configuring an iSCSI Boot for a Boot Policy.

For a high-level procedure for implementing iSCSI boot, see the UCS Manager GUI Configuration Guide.

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* .
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.

Example

The following example shows how to:

- Enter the boot policy named lab2-boot-policy
- Create an iSCSI boot for the policy
- Create primary and secondary paths using the vNICs named vNIC1 and vNIC2
- Set the boot order to 2

```
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.

Known Issues iSCSI Boot Configuration

1. You can configure iSCSI initiator parameters using the **LAN Connectivity Policy** on the Cisco UCS Central GUI, but not through the Cisco UCS Central CLI. To configure them from the CLI, you must apply the IQN Pool, Authentication profile, and other properties related to the iSCSI through a service profile. Similarly, you can create the boot parameters only through a service profile using the Cisco UCS Central CLI. When you configure iSCSI targets under a service profile, or a service profile template using the Cisco UCS Central CLI, only the iSCSI name is displayed in the Cisco UCS Central GUI under the iSCSI Boot Policy, and the iSCSI Boot appears under the **Decide Later** mode instead of the **Static** mode. To resolve these issues, you must create a LUN object under a static target, create an IP interface and pooled IP parameters under the iSCSI Boot vNIC.
   - To configure an iSCSI Boot for a Boot Policy, see Configuring an iSCSI Boot for a Boot Policy, on page 442.
   - To create an iSCSI vNIC in a service profile, see Creating an iSCSI vNIC in a Service Profile, on page 443.
   - To create a LUN object under a static- target, and to create an IP interface and pooled IP parameters, see Creating an iSCSI Static Target, on page 444.
2. When an iSCSI vNIC (for an iSCSI boot) is created in the **LAN Connectivity Policy** from the Cisco UCS Central CLI and the policy is applied to a global service profile and associated to a server, the association fails and the Cisco UCS Central GUI displays the following error message:

   No VLAN/IP configured or static and target cannot be mixed.

   This error message disappears when you navigate to the **LAN Connectivity Policy** and click the **iSCSI vNICs** tab and click the other sub-tabs and then click **Save**. Since configuring the iSCSI initiator parameters is not supported for the **LAN Connectivity Policy** in the Cisco UCS Central CLI, this workaround does not resolve the issue and the error message recurs. For more information on configuring iSCSI initiator parameters from the service profile, see item **1.** above.

Creating an iSCSI vNIC in a Service Profile

You can create an iSCSI vNIC in a service profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource manager**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) /org # **scope service-profile** *profile-name*	Enters service profile organization mode for the service profile.
Step 3	UCSC (resource-mgr) /org/service-profile # **create vnic-iscsi** *iscsi-vnic-name* .	Specifies the iSCSI vNIC name.
Step 4	UCSC (resource-mgr) /org/service-profile/vnic-iscsi* # **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 5	UCSC (resource-mgr) /org/service-profile/vnic-iscsi* # **set overlay-vnic-name** *overlay-vnic-name*	Specifies the Ethernet vNIC that is used by the iSCSI device as the overlay vNIC. For more information, see Configuring a vNIC for a Global Service Profile, on page 391.
Step 6	UCSC (resource-mgr) /org/service-profile/vnic-iscsi* # **create eth-if**	Creates an Ethernet interface for a VLAN assigned to the iSCSI vNIC.
Step 7	UCSC (resource-mgr) /org/service-profile/vnic-iscsi/eth-if* # **set vlanname** *vlan-name*.	Specifies the VLAN name. The default VLAN is default.
Step 8	UCSC (resource-mgr) /org/service-profile/vnic-iscsi/eth-if* # **commit buffer** .	Commits the transaction to the system configuration.

Example

The following example shows how to create an iSCSI vNIC in a service profile:

```
UCSC (resource-mgr)# scope org /
UCSC (resource-mgr) /org # scope service-profile SPTest
UCSC (resource-mgr) /org/service-profile # create vnic-iscsi iSCSI0
UCSC (resource-mgr) /org/service-profile/vnic-iscsi* # set iscsi-identity initiator-pool-name
 myIQNPool
UCSC (resource-mgr) /org/service-profile/vnic-iscsi* # set overlay-vnic-name eth0
UCSC (resource-mgr)/org/service-profile/vnic-iscsi* # create eth-if
UCSC (resource-mgr) /org/service-profile/vnic-iscsi/eth-if* # set vlanname gVlan309
UCSC (resource-mgr)/org/service-profile/vnic-iscsi/eth-if* # commit buffer#
```

Creating an iSCSI Static Target

Before you begin

You must have created an iSCSI vNIC.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) /org # **scope service profile** *name*	Enters service profile organization mode for the service profile to which you want to add an iSCSI target.
Step 3	UCSC(resource-mgr)/ org /service profile # **scope iscsi-boot**	Enters the mode for configuring iSCSI boot parameter.
Step 4	UCSC(resource-mgr) /org / service-profile/iscsi-boot # **create vnic-iscsi** *iscsi name*	Creates an iSCSI vNIC.
Step 5	UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi* # **create static-target-if** {**1** | **2**}	Creates a static target for the iSCSI vNIC and assigns a priority level to it. Valid priority levels are 1 or 2.
Step 6	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi/ static-target-if* # **create lun**	Creates the LUN that corresponds to the location interface.
Step 7	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi/ static-target-if/ lun*# **set id** *lun number*	Specifies the target LUN id. Valid values are from 0 to 65535.
Step 8	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi/ static-target-if/lun* #**up**	Moves to the previous configuration mode.
Step 9	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi/ static-target-if* #**set ip address***n.n.n.n*	The IPv4 address assigned to the iSCSI target.
Step 10	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi/ static-target-if # **set name***name*	
Step 11	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi/ static-target-if* #**up**	Moves to the previous configuration mode.
Step 12	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi* #**create ip-if**	Creates an IP interface.
Step 13	UCSC(resource-mgr) /org / service-profile/iscsi-boot/ vnic-iscsi/ ip-if *# **create pooled-ip-params**	Specifies that the iSCSI initiator boot using one of the IP addresses from the previously created iSCSI initiator IP pool.
Step 14	UCSC(resource-mgr) /org/ service-profile/ iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* # **set identity-pool***name*	Specifies a name for the identity-pool.

	Command or Action	Purpose
Step 15	UCSC(resource-mgr) /org/ service-profile/ iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* # **commit buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a LUN under a static target, and create IP interface and pooled IP parameters under an iSCSI Boot vNIC.

```
UCSC(resource-mgr) /org/service-profile # sc iscsi-boot
UCSC(resource-mgr) /org/service-profile/iscsi-boot # create vnic-iscsi iscsi0
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi* # create static-target-if 1
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # create
lun
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # set
id 10
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if/lun* # up
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # set
ipaddress 4.4.4.4
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if # set name
abcd
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/static-target-if* # up
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi* # create ip-if
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/ip-if* # create pooled-ip-params

UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* # set
 identity-pool ipPool
UCSC(resource-mgr) /org/service-profile/iscsi-boot/vnic-iscsi/ip-if/pooled-ip-params* #
commit buffer
```

Local Disk Boot

If a server has a local drive, you can configure a boot policy to boot the server from the top-level local disk device or from any of the following second-level devices:

- **local-any**—Enables boot from any local device. This is the top-level local disk device. Use for Cisco UCS M1 and M2 blade and rack servers using standard boot order.
- **local-lun**—Enables boot from local disk or local LUN.
- **local-jbod**—Enables boot from a bootable JBOD.
- **sd-card**—Enables boot from SD card.
- **usb-intern**—Enables boot for internal USB.
- **usb-extern**—Enables boot from external USB.
- **embedded-local-lun**—Enables boot from the embedded local LUN on the Cisco UCS 240 M4 server.
- **embedded-local-disk**—Enables boot from the embedded local disk on the Cisco UCS C240 M4SX and the M4L servers.

Note For Cisco UCS blade and rack servers using enhanced boot order, you can select both top-level and second-level boot devices. For Cisco UCS blade and rack servers using standard boot order, you can only select a top-level device using **local-any**.

Configuring a Local Disk Boot for a Boot Policy

This procedure continues directly from Creating a Boot Policy, on page 435.

Before you begin

Create a boot policy to contain the local disk 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 storage**	Creates a storage boot for the boot policy and enters boot policy storage mode. **Note** If you delete all of the boot order items under **storage**, the storage group is also deleted. You will need to recreate the storage group before you can add a new local boot disk.
Step 5	UCSC(policy-mgr) /org/boot-policy/storage # **set order** *order_num*	Sets the boot order for the local disk boot. Enter a number between 1 and 16. **Note** If you create more than one local disk boot, set the order on the local disk boot level.
Step 6	UCSC(policy-mgr) /org/boot-policy/storage # **create local**	Creates a local disk location and enters organization boot policy local storage mode.
Step 7	UCSC(policy-mgr) /org/boot-policy/storage/local # **create** {**embedded-local-jbod** | **embedded-local-lun**	Specifies the type of local storage. For more information, see Local Disk Boot, on page 446.

	Command or Action	Purpose
	| **local-any** | **local-jbod** | **local-lun** | **sd-card** | **usb-extern** | **usb-intern**}	**Note** You can add either the embedded local disk or the embedded local LUN to the boot order. Adding both is not supported.
Step 8	UCSC(policy-mgr) /org/boot-policy/storage/local # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Enter the boot policy named lab1-boot-policy
- Create a local jbod and sd card boots for the policy
- Set the boot orders for each

```
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* # create local
UCSC(policy-mgr) /org/boot-policy/storage/local* # create local-jbod
UCSC(policy-mgr) /org/boot-policy/storage/local/local-jbod* # set order 1
UCSC(policy-mgr) /org/boot-policy/storage/local/local-jbod* # up
UCSC(policy-mgr) /org/boot-policy/storage/local* # create sd-card
UCSC(policy-mgr) /org/boot-policy/storage/local/sd-card* # set order 2
UCSC(policy-mgr) /org/boot-policy/storage/local/sd-card* # commit-buffer
UCSC(policy-mgr) /org/boot-policy/storage/local/sd-card #
```

What to do next

Include the boot policy in a service profile and/or template.

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.

Example

The following example shows how to:

- Enter the boot policy named lab3-boot-policy
- Create a virtual media boot with read-only privileges for the policy
- Set the boot order to 3

```
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.
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.

Example

The following example shows how to delete a boot policy:

```
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 #
```

Displaying Server Reboot log

A server reboot log is displayed for all Blade and Rack servers. This log displays the last 5 reasons for the server reset with the timestamp, and the source of the last power transition with the number of times a reason was the source of power transition.

Note The server reboot reasons log is supported only on Cisco UCS Manager release 3.1(3) and later. For Blade servers, the firmware versions should match that of Cisco UCS Manager 3.1(2) or later. For Rack servers and Cisco S3260 series servers, the firmware version must match that of Cisco UCS Manager release 3.1(3) or later.

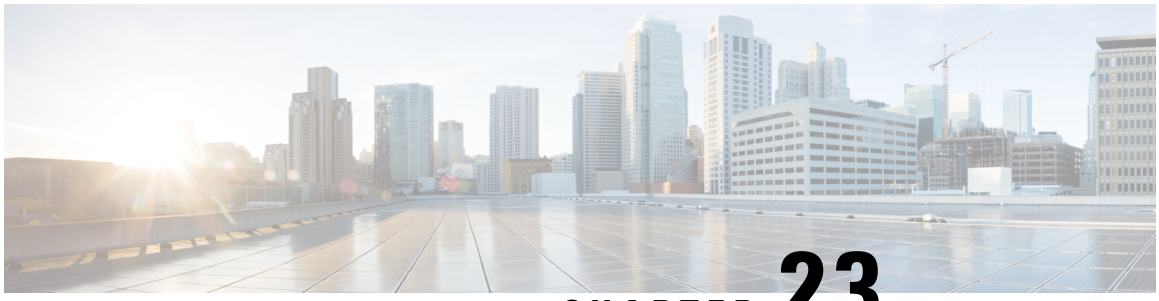
Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 2	UCSC(resource-mgr) /domain-mgmt # **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 3	UCSC (resource-mgr) /domain-mgmt /ucs-domain # **scope chassis** *name*	Enters into the specific chassis.
Step 4	UCSC(resource-mgr)/domain-mgmt/ucs-domain# **scope server***name*	Enters into the specific server
Step 5	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server# **show power-transition-log**	Displays the power transition log for the server.

Example

This example shows the log for the last five reasons for a server reset:

```
UCSC(resource-mgr)/domain-mgmt# ucs-domain
UCSC(resource-mgr)/domain-mgmt/ucs-domain# scope chassis
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis # scope server 1/7
UCSC(resource-mgr) /domain-mgmt/ucs-domain/chassis/server # show power-transition-log

Last 5 server reboots (Newest first):

Pwr Change Source          Last pwr transition timestamp
-------------------------      -----------------------------
Ucsm Associate                 2016-10-28T18:51:00.807
Ucsm Server Discover           2016-10-28T18:40:14.124

UCSC(resource-mgr)/domain-mgmt# ucs-domain/chassis/server # exit
UCSC(resource-mgr)/domain-mgmt# ucs-domain # scope server 1/2
UCSC(resource-mgr)/domain-mgmt# ucs-domain/chassis/server # show power-transition-log

Last 5 server reboots (Newest first):

Pwr Change Source          Last pwr transition timestamp
-------------------------      -----------------------------
Ucsm Turnup                  2016-10-31T18:09:16.298
None                         2016-10-31T18:08:53.263
Ucsm Turnup                  2016-10-27T22:28:53.825
None                         2016-10-27T22:28:31.641
Host Pwr Transition          2016-10-27T21:56:40.020
```



CHAPTER 23

Server Policies

Server Policies

Server policies allow you to apply changes globally to your Cisco UCS servers.

Note You must include policies in a service profile and associate them with a server before Cisco UCS Central can apply them.

BIOS Policy

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

To use a BIOS policy:

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.

Server BIOS Settings

Cisco UCS provides two methods for making global modifications to the BIOS settings on servers in a 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. Alternatively, 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 on 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.

Creating a BIOS Policy

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 # **create bios-policy** *BIOS policy name*

Creates the BIOS policy and enters BIOS policy mode.

Step 4 UCSC(policy-mgr) /org/bios-policy # **set** *BIOS settings*

Configure the BIOS settings. For descriptions and information about the options for each CLI BIOS setting, see the following topics:

- Basic BIOS Settings
- Processor BIOS Settings
- I/O BIOS Settings
- RAS Memory BIOS Settings
- USB BIOS Settings
- PCI BIOS Settings
- Boot Options BIOS Settings
- Server Manager BIOS Settings
- Console BIOS Settings

Step 5 UCSC(policy-mgr) /org/bios-policy # **commit-buffer**

Commits the transaction to the system configuration.

Example

The following example shows how to create a BIOS policy under the root organization, and set the NUMA configuration:

```
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 #
```

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.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to delete a BIOS policy in the root organization:

```
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 #
```

Default BIOS Settings

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

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

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

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

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

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

Basic BIOS Settings

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

Name	Description
Organization	Select an organization.
Name	Enter a name between 1 and 16 alphanumeric characters.

Name	Description
Description	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).
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.
Serial Port A	Whether serial port A is enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The serial port is disabled. • —The serial port is enabled.
Quiet Boot	What the BIOS displays during Power On Self-Test (POST). This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS displays all messages and Option ROM information during boot. • —The BIOS displays the logo screen, but does not display any messages or Option ROM information during boot.
Post Error Pause	What happens when the server encounters a critical error during POST. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS continues to attempt to boot the server. • —The BIOS pauses the attempt to boot the server and opens the Error Manager when a critical error occurs during POST.

Name	Description
Front Panel Lockout	Whether the power and reset buttons on the front panel are ignored by the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The power and reset buttons on the front panel are active and can be used to affect the server. • —The power and reset buttons are locked out. The server can only be reset or powered on or off from the CIMC GUI.
Consistent Device Naming (CDN)	Whether Consistent Device Naming (CDN) is enabled. CDN allows Ethernet interfaces to be named in a consistent manner, making Ethernet interface names more uniform, easy to identify, and persistent when adapter or other configuration changes are made. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —CDN is disabled for this BIOS policy. • —CDN is enabled for this BIOS policy.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server is powered on and the system attempts to restore its last state. • —The server is powered on and automatically reset. • —The server remains off until manually powered on.
QuickPath Interconnect (QPI) Link Frequency	The Intel QuickPath Interconnect (QPI) link frequency, in megatransfers per second (MT/s). This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **6400** • **7200** • **8000** • **9600** • —The CPU determines the QPI link frequency.

Name	Description
QuickPath Interconnect (QPI) Snoop Mode	This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The snoop is always spawned by the home agent (centralized ring stop) for the memory controller. This mode has a higher local latency than early snoop, but it provides extra resources for a larger number of outstanding transactions. • —This mode is available only for processors that have 10 or more cores. It is the best mode for highly NUMA optimized workloads. • —The distributed cache ring stops can send a snoop probe or a request to another caching agent directly. This mode has lower latency and it is best for workloads that have shared data sets across threads and can benefit from a cache-to-cache transfer, or for workloads that are not NUMA optimized.
Trusted Platform Module (TPM)	Whether TPM is used to securely store artifacts that are used to authenticate the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —TPM is used for authentication. • —TPM is not used for authentication.
Intel Trusted Execution Technology (TXT)	Whether TXT is used for data protection. TXT can be enabled only after TPM, Intel Virtualization technology (VT) and Intel Virtualization Technology for Directed I/O (VTDio) are enabled. If you only enable TXT, it implicitly enables TPM, VT, and VTDio also. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —TXT is used for extra security. • —TXT is not used for extra security.

Processor BIOS Settings

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

Table 6: Basic Tab

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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not classify memory areas. • —The processor classifies memory areas. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Data from I/O devices is not placed directly into the processor cache. • —Data from I/O devices is placed directly into the processor cache.
Local X2 Application Policy Infrastructure Controller (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. • —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
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: • —The CPU can drop below the maximum non-turbo frequency when idle. This option decreases power consumption but may reduce system performance. • — 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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **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 CPU determines the level.
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: • —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: • —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
Altitude	The approximate number of meters above sea level at which the physical server is installed. This can be one of the following: • —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.
CPU Hardware Power Management	Manages the CPU power functions. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not classify memory areas. • —The processor classifies memory areas.
Energy Performance Tuning	This item selects whether the BIOS or Operating System can turn on the energy performance bias tuning. The options are BIOS and OS. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not use energy performance management. • —The processor uses energy performance management.
Workload Configuration	The BIOS uses values that are default for the server type and vendor. Balanced is selected for workload optimization. This is the recommended setting. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The workload configuration optimazations are disabled. • —The workload configuration optimazations are enabled.

Table 7: Prefetchers Tab

Name	Description
Hardware Prefetcher	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. • —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.
Adjacent Cache Line Prefetcher	Whether the processor fetches cache lines in even/odd pairs instead of fetching just the required line. This can be one of the following: • —The processor only fetches the required line. • —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.
Data Cache Unit (DCU) Streamer Prefetcher	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: • —The processor does not try to anticipate cache read requirements and only fetches explicitly requested lines. • —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.

Name	Description
Data Cache Unit (DCU) IP Prefetcher	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: • —The processor does not preload any cache data. • —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.

Table 8: Technology Tab

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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not increase its frequency automatically. • —The processor uses Turbo Boost Technology if required.
Enhanced Intel Speed Step	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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor never dynamically adjusts its voltage or frequency. • —The processor utilizes Enhanced Intel SpeedStep Technology and enables all supported processor sleep states to further conserve power. We recommend that you contact your operating system vendor to make sure your operating system supports this feature.

Name	Description
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not permit hyperthreading. • —The processor allows for the parallel execution of multiple threads. 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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **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. 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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not permit virtualization. • —The processor allows multiple operating systems in independent partitions. **Note** If you change this option, you must power cycle the server before the setting takes effect.

Table 9: Power Tab

Name	Description
Power Management	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: • —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. • —The server automatically optimizes the performance for the BIOS parameters mentioned above. • —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: • • • • • —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
Processor C State	Whether the system can enter a power savings mode during idle periods. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The system remains in a high-performance state even when idle. • —The system can reduce power to system components such as the DIMMs and CPUs. 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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU continues to run at its maximum frequency in the C1 state. • —The CPU transitions to its minimum frequency. This option saves the maximum amount of power in the C1 state.
CPU Performance	Sets the CPU performance profile for the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —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. • —Data reuse and the DCU IP prefetcher are enabled, and all other prefetchers are disabled. • —All prefetchers are enabled and data reuse is disabled. This setting is also known as high-performance computing. • **Custom**

Name	Description
Package C State Limit	The amount of power available to the server components when they are idle. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU determines the available power. • —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 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 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 server may enter any available C state.

Table 10: Errors and Reporting Tab

Name	Description
Processor C3 Report	Whether the processor sends the C3 report to the operating system. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not send the C3 report. • —The processor sends the C3 report. • —The processor sends the C3 report using the advanced configuration and power interface (ACPI) C2 format. • —The processor sends the C3 report using the ACPI C3 format. On the Cisco UCS B440 Server, the BIOS Setup menu uses enabled and disabled for these options. If you specify acpi-c2 or acpi-c3, 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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not send the C6 report. • —The processor sends the C6 report.
Processor C7 Report	Whether the processor sends the C7 report to the operating system. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The processor does not send the C7 report. • —The processor sends the C7 report. • —The processor sends the C7 report. • —The processor sends the C7s report. **Note** The selections vary depending on the server and operating system.

Name	Description
Processor CMCI	The BIOS uses values that are default for the server type and vendor. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • — Corrected Machine Check Interrupt is not generated. • — Corrected Machine Check Interrupt is generated.
Max Variable MTRR Setting	Allows you to select the number of mean time to repair (MTRR) variables. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —BIOS uses the default value for the processor. • **8**—BIOS uses the number specified for the variable MTRR.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • — Single bit memory errors are corrected in memory and the corrected data is set in response to the demand read. • — Single bit memory errors are not corrected.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **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 system checks for memory ECC errors only when the CPU reads or writes a memory address.

Name	Description
CPU Hardware Power Management	Enables processor Hardware Power Management (HWPM). This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —HWPM is disabled. • —HWPM native mode is enabled. • —HWPM Out-Of-Box mode is enabled.

I/O BIOS Settings

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

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

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

RAS Memory BIOS Settings

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

Name	Description
NUMA	Whether the BIOS supports NUMA. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —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 does not support NUMA.

Name	Description
LV DDR Mode	Whether the system prioritizes low voltage or high frequency memory operations. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —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. • —The system prioritizes high frequency operations over low voltage operations. • —The CPU determines the priority.
DRAM Refresh Rate	The refresh interval rate for internal memory. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **1x** • **2x** • **3x** • **4x** •
Memory RAS Configuration Mode	How the memory reliability, availability, and serviceability (RAS) is configured for the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —System performance is optimized. • —System reliability is optimized by using half the system memory as backup. • —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. • —Enables sparing mode.

Name	Description
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 the sparing option for the Memory RAS Config parameter. It can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —One DIMM is held in reserve. If a DIMM fails, the contents of a failing DIMM are transferred to the spare DIMM. • —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.
DDR3 Voltage Selection	The voltage to be used by the dual-voltage RAM. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • •

USB BIOS Settings

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

Basic Tab

Name	Description
Make Device Non Bootable	Whether the server can boot from a USB device. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server can boot from a USB device. • —The server cannot boot from a USB device.

Name	Description
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • •
Legacy USB Support	Whether the system supports legacy USB devices. This can be one of the following: • —Disables legacy USB support if no USB devices are connected. • —USB devices are only available to EFI applications. • —Legacy USB support is always available. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
USB Idle Power Optimizing Setting	Whether the USB System Idle Power Optimizing setting is used to reduce USB EHCI idle power consumption. Depending upon the value you choose, this setting can have an impact on performance. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —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. • —The USB System Idle Power Optimizing setting is enabled, because power savings are preferred over optimal performance.
Port 60h/64h Emulation Support	Whether the system supports 60h/64h emulation for complete USB keyboard legacy support. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —60h/64 emulation is not supported. • —60h/64 emulation is supported. You should select this option if you are using a non-USB aware operating system on the server.

Name	Description
xHCI Mode Support	How onboard USB 3.0 ports behave. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Onboard USB 3.0 ports function as USB 2.0 ports. • —Onboard USB 3.0 ports function as USB 3.0 ports.

Device Management Tab

Name	Description
Front Panel USB Ports	Whether the front panel USB devices are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the front panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • —Enables the front panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
Rear Panel USB Ports	Whether the rear panel USB devices are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the rear panel USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • —Enables the rear panel USB ports. Devices connected to these ports are detected by the BIOS and operating system.
Internal USB Ports	Whether the internal USB devices are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the internal USB ports. Devices connected to these ports are not detected by the BIOS and operating system. • —Enables the internal USB ports. Devices connected to these ports are detected by the BIOS and operating system.

Name	Description
KVM I/O	Whether the KVM ports are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the KVM keyboard and/or mouse devices. Keyboard and/or mouse will not work in the KVM window. • —Enables the KVM keyboard and/or mouse devices.
SD Card Drives	Whether the SD card drives are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the SD card drives. The SD card drives are not detected by the BIOS and operating system. • —Enables the SD card drives.
vMedia Devices	Whether the virtual media devices are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Disables the vMedia devices. • —Enables the vMedia devices.
All USB Devices	Whether all physical and virtual USB devices are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —All USB devices are disabled. • —All USB devices are enabled.

PCI BIOS Settings

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

Table 11: Basic Tab

Name	Description
Max Memory Below 4G	Whether the BIOS maximizes memory usage below 4GB for an operating system without PAE support, depending on the system configuration. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Does not maximize memory usage. Choose this option for all operating systems with PAE support. • —Maximizes memory usage below 4GB for an operating system without PAE support.
Memory Mapped IO Above 4Gb Configuration	Whether to enable or disable memory mapped I/O of 64-bit PCI devices to 4GB or greater address space. Legacy option ROMs are not able to access addresses above 4GB. PCI devices that are 64-bit compliant but use a legacy option ROM may not function correctly with this setting enabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Does not map I/O of 64-bit PCI devices to 4GB or greater address space. • —Maps I/O of 64-bit PCI devices to 4GB or greater address space.

Name	Description
VGA Priority	Allows you to set the priority for VGA graphics devices if multiple VGA devices are found in the system. This can be one of the following: • —Priority is given to the onboard VGA device. BIOS post screen and OS boot are driven through the onboard VGA port. • —Priority is given to the PCIE Graphics adapter. BIOS post screen and OS boot are driven through the external graphics adapter port. • —Priority is given to the PCIE Graphics adapter, and the onboard VGA device is disabled. **Note** The vKVM does not function when the onboard VGA is disabled. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. **Note** Only onboard VGA devices are supported with Cisco UCS B-Series servers.
PCIe OptionROMs	Whether Option ROM is available on all expansion ports. This can be one of the following: • —The expansion slots are not available. • —The expansion slots are available. • —The expansion slots are available for UEFI only. • —The expansion slots are available for legacy only. • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor.
PCIe Mezz OptionRom	Whether all mezzanine PCIe ports are enabled or disabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —All LOM ports are enabled. • —All LOM ports are disabled.

Name	Description
PCIe 10G LOM 2 Link	Whether Option ROM is available on the 10G LOM port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is available. • —The expansion slot is not available.
ASPM Support	Allows you to set the level of ASPM (Active Power State Management) support in the BIOS. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The CPU determines the power state. • —ASPM support is disabled in the BIOS. • —Force all links to L0 standby (L0s) state.

Table 12: PCIe Slot Link Speed Tab

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

Table 13: PCIe Slot OptionROM Tab

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

Name	Description
Slot MLOM	Whether Option ROM is available on the PCIe slot connected to the MLOM available on the specified port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot N1	Whether is available on the specified port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
Slot N2	Whether is available on the specified port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • —The expansion slot is available for UEFI only. • —The expansion slot is available for legacy only.
PCI ROM CLPset pci-rom-clp-support pci-rom-clp-config	The following options are available for PCI ROM CLP. • — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. .

Name	Description
SIOC1 Option ROMset sloc1-option rom-config sloc1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
SB Mezz1 Option ROMset sbmezz1 -optionrom-config sbmezz1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IOE Slot1 Option ROMset ioeslot1-option-config ioeslot1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IOE Mezz1 Option ROMset ioemezz1-optionrom-config ioemezz1-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.

Name	Description
IOE Slot2 Option ROMset ioeslot2-optionrom-config ioeslot2-optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IO ENVMe1 Option ROMset ioenvme1-optionrom-config ioenvme1 -optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. . • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
IO ENVMe2 Option ROMset ioenvme2-optionrom-config ioenvme2 -optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.
SBNVMe1 Option ROMset ioenvme1-optionrom-config ioenvme1 -optionrom	• — The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The expansion slot is not available. • —The expansion slot is available. • **Legacy-only**—The expansion slot is available for legacy only. • **UEFI-only**—The expansion slot is available for UEFI only.

Graphics Configuration BIOS Settings

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

Name	Description
Integrated Graphics	Enables integrated graphics. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Integrated graphic is enabled. • —Integrated graphics is disabled.
Integrated Graphics Aperture Size	Allows you to set the size of mapped memory for the integrated graphics controller. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • • • • • •
Onboard Graphics	Enables onboard graphics (KVM). This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Onboard graphics is enabled. • —Onboard graphics is disabled.

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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Waits for user input before retrying NON-EFI based boot options. • —Continually retries NON-EFI based boot options without waiting for user input.

Name	Description
Onboard SCU Storage Support	Whether the onboard software RAID controller is available to the server. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The software RAID controller is not available. • —The software RAID controller is available.
Intel Entry SAS RAID	Whether the Intel SAS Entry RAID Module is enabled. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The Intel SAS Entry RAID Module is disabled. • —The Intel SAS Entry RAID Module is enabled.
Intel Entry SAS RAID Module	How the Intel SAS Entry RAID Module is configured. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —Configures the RAID module to use Intel IT/IR RAID. • —Configures the RAID module to use Intel Embedded Server RAID Technology II.

Server Manager BIOS Settings

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

Name	Description
Assert NMI on SERR	Whether the BIOS generates a non-maskable interrupt (NMI) and logs an error when a system error (SERR) occurs. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS does not generate an NMI or log an error when a SERR occurs. • —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**.

Name	Description
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The BIOS does not generate an NMI or log an error when a PERR occurs. • —The BIOS generates an NMI and logs an error when a PERR occurs. You must enable **Assert Nmi on Serr** to use this setting.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The watchdog timer is not used to track how long the server takes to boot. • —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. This feature requires either operating system support or Intel Management software.
FRB-2 Timer	Whether the FRB-2 timer is used to recover the system if it hangs during POST. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The FRB-2 timer is not used. • —The FRB-2 timer is started during POST and used to recover the system if necessary.
Out of Band Management	This is used for the Windows Special Administration Control (SAC). • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The option to use the Windows Special Administration Control (SAC) is disabled. • —The option to use the Windows Special Administration Control (SAC) is enabled.

Name	Description
OS Boot Watchdog Timer Timeout	What action the system takes if the watchdog timer expires. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The server is powered off if the watchdog timer expires during OS boot. • —The server is powered off if the watchdog timer expires during OS boot. 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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The watchdog timer expires 5 minutes after the OS begins to boot. • —The watchdog timer expires 10 minutes after the OS begins to boot. • —The watchdog timer expires 15 minutes after the OS begins to boot. • —The watchdog timer expires 20 minutes after the OS begins to boot. This option is only available if you enable the OS Boot Watchdog Timer.
Redirection After BIOS POST	• —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The option to redirect is disabled. • —The option to redirect is disabled.

Console BIOS Settings

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

Name	Description
Legacy OS Redirect	Whether redirection from a legacy operating system, such as DOS, is enabled on the serial port. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —The serial port enabled for console redirection is hidden from the legacy operating system. • — The serial port enabled for console redirection is visible to the legacy operating system.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • —No console redirection occurs during POST. • —Enables serial port A for console redirection during POST. This option is valid for blade servers and rack-mount servers. • —Enables serial port B for console redirection and allows it to perform server management tasks. This option is only valid for rack-mount servers. • —Console redirection occurs during POST. • —Enables console redirection of BIOS POST messages to server COM port 0. **Note** If you enable this option, you also disable the display of the Quiet Boot logo screen during POST.

Name	Description
BAUD Rate	What BAUD rate is used for the serial port transmission speed. If you disable Console Redirection, this option is not available. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **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. **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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **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. **Note** This setting must match the setting on the remote terminal application.
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: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **None**—No flow control is used. • —RTS/CTS is used for flow control. **Note** This setting must match the setting on the remote terminal application.

Name	Description
Putty KeyPad	Allows you to change the action of the PuTTY function keys and the top row of the numeric keypad. This can be one of the following: • —The BIOS uses the value for this attribute contained in the BIOS defaults for the server type and vendor. • **ESCN**—The default mode. The function keys match the general behavior of Digital terminals. The function keys generate sequences such as **ESC [11~** and **ESC [12~**. • **LINUX**—Mimics the Linux virtual console. Function keys F6 to F12 behave like the default mode, but F1 to F5 generate **ESC [[A** through **ESC [[E**. • **SCO**—The function keys F1 to F12 generate **ESC [M** through **ESC [X**. The function and shift keys generate **ESC [Y** through **ESC [j**. The control and function keys generate **ESC [k** through **ESC [v**. The shift, control and function keys generate **ESC [w** through **ESC [{**. • **vt100**—The function keys generate **ESC OP** through **ESC O[.** • **VT400**—The function keys behave like the default mode. The top row of the numeric keypad generates **ESC OP** through **ESC OS**. • **XTERMR6**—Function keys F5 to F12 behave like the default mode. Function keys F1 to F4 generate **ESC OP** through ESC OS, which are the sequences produced by the top row of the keypad on Digital terminals.

IPMI Access Profile

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

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

Configuring an IPMI Access Profile

Before you begin

Obtain the following:

- Username that the operating system of the server can authenticate

- Password for the username
- Permissions 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.
Step 7	UCSC(policy-mgr) /org/ipmi-access-profile/ipmi-user # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create an IPMI access profile named ReadOnly
- Create an endpoint user named bob
- Set the password and the privileges for bob

```
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.

Example

The following example deletes the IPMI access profile named ReadOnly:

```
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* .

	Command or Action	Purpose
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.

Example

The following example adds an endpoint user named alice to the IPMI access profile named ReadOnly:

```
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.

	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 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.

Example

The following example deletes the endpoint user named alice from the IPMI access profile named ReadOnly:

```
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 #
```

Serial over LAN Policy

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

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

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

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.

	Command or Action	Purpose
Step 4	(Optional) UCSC(policy-mgr) /org/sol-policy # **set descr** *description*	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.

Example

The following example shows how to:

- Create a serial over LAN policy named Sol9600
- Provide a description for the policy
- Set the speed to 9,600 baud
- Enable the policy

```
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.

	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 # **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.

Example

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:
```

iSCSI Adapter Policy

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	(Optional) UCSC(policy-mgr) /org/iscsi-policy # **set descr** "*description*"	Provides a description for the iSCSI adapter policy.
Step 5	Required: 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.

	Command or Action	Purpose
		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	Required: 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	Required: 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	Required: 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	Required: 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	Required: UCSC(policy-mgr) /org/iscsi-policy # **set iscsi-protocol-item boottotarget** {**no** | **yes**}	Specifies whether to boot from the iSCSI target. 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	Required: UCSC(policy-mgr) /org/iscsi-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create an iSCSI adapter policy called iscsiboot
- Set the connection timeout
- DHCP timeout

- LUN busy retry count
- Apply a TCP timestamp

```
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.

Example

The following example shows how to delete an iSCSI adapter policy named iscsi-adapter-pol:

```
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	Required: UCSC(policy-mgr) /org/auth-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create an authentication profile for an initiator and a target:

```
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 for use as the overlay vNIC for the iSCSI device. 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	Required: UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

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 #
```

Local Disk Policy

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

The local disk modes include the following:

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

- **RAID 5 Striped Parity**
- **RAID 50 Striped Parity Striped**

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

The B200 M3 server supports JBOD mode for local disks.

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 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. 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 associates a service profile containing this local disk policy with a server, verifies that the selected RAID option is properly licensed. If there are issues, 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	(Optional) UCSC(policy-mgr) /org/local-disk-config-policy # **set descr** *description*	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-50-striped-parity-and-striped** | **raid-6-striped-dual-parity** | **raid-60-striped-parity-and-striped** | **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**}	Set configuration protection to yes in order to prevent a service profile using this local disk policy from being associated to a server with a different physical disk configuration. If the service profile includes a local disk policy with configuration protection enabled, and there is an attempt to associate that service profile to a server that includes disks with a different local disk configuration, the association immediately fails and produces a configuration mismatch error.

	Command or Action	Purpose
		Caution We recommend that you enable configuration protection to preserve any data that may exist on local disks. If disabled, any existing volume that does not match the local disk configuration policy will be deleted.
Step 7	UCSC(policy-mgr) /org/local-disk-config-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example configures a local disk configuration policy:

```
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.

Example

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.

Example

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 #
```

Scrub Policy

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

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

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

Disk scrub

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

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

BIOS Settings Scrub

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

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

FlexFlash Scrub

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

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

Note

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

Creating 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	(Optional) UCSC(policy-mgr) /org/scrub-policy # **set descr** *description*	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 • 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.

Example

The following example creates and enables a scrub policy named ScrubPolicy2 on servers using the scrub policy:

```
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.

Example

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 #
```

vMedia Policy

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

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

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

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

- Boot from a specific vMedia device
- Copy files from a mounted share to local disk
- Install and update OS drivers

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

Creating a vMedia 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 vmedia-policy** *policy-name*	Creates the specified vMedia policy and enters organization vMedia policy mode.
Step 4	UCSC(policy-mgr) /org/vmedia-policy # **set retry-on-mount-fail** {**yes** | **no**}	Select whether the vMedia will continue mounting when a mount failure occurs.
Step 5	UCSC(policy-mgr) /org/vmedia-policy # **create vmedia-mapping** *name*	Creates a vMedia policy sub-directory with the specified mapping name.
Step 6	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set device-type** {**cdd** | **hdd**}	Specifies the remote vMedia image type that you wish to mount.
Step 7	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set image-file-name** *filename*	Specifies the image file name.

	Command or Action	Purpose
Step 8	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set image-path** *path*	Specifies the image path.
Step 9	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set image-variable-name** {**none** | **service-profile-name**}	Specifies the name to be used for the image. This can be one of the following: • **none**—Enter the name manually. • **service-profile-name**—Automatically uses the name of the service profile that the policy is associated with. **Note** The service profile must be available at the required path, and you cannot change the name of the service profile.
Step 10	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set mount-protocol** {**cifs** | **http** | **https** | **nfs**}	Specifies the remote vMedia protocol.
Step 11	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set auth-option** {**default** | **none** | **ntlm** | **ntlmi** | **ntlmssp** | **ntlmsspi** | **ntlmv2** | **ntlmv2i**}	Specifies the remote authentication options.
Step 12	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set password** *password*	Specifies the password.
Step 13	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set remote-ip** *ip-address*	Specifies the remote IP address.
Step 14	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **set user-id** *name*	Specifies the user ID for mounting the vMedia device.
Step 15	UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create a vMedia policy named vMediaPol2
- Create a mapping directory called MapDir
- Specify the device type and other criteria

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create vmedia-policy vmediaPol2
UCSC(policy-mgr) /org/vmedia-policy* # create vmedia-mapping MapDir
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set device-type hdd
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set image-file-name win2011.iso
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set image-path /home/vMedia
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set password MyPass
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set remote-ip 10.0.0.0
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # set user-id VMediaAdmin
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping* # commit-buffer
UCSC(policy-mgr) /org/vmedia-policy/vmedia-mapping #
```

Creating or Editing Power Sync 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-sync-policy***name*	Creates power-sync policy for the specified organization.
Step 4	UCSC(policy-mgr) /org/power-sync policy* # **commit-buffer**	Commits the transaction to the system.
Step 5	UCSC(policy-mgr) /org/power-sync policy # **set**	
Step 6	UCSC(policy-mgr) /org/power-sync policy* # **set syncoption**	Displays the power sync policy options. They can be one of the following : • always-sync - During shallow association, this option will always sync desired power state to the physical server even if the physical server power state is on and the desired power state is off. • default-sync - During shallow association, this option will sync desired power state to the physical server if the physical server power state is off and the desired power state is on. • initial-only-sync - This option only syncs power to the server during deep association, the first time we associate the service profile to a new server. During shallow association, this option does not

	Command or Action	Purpose
		sync power. When the user resets or cycles physical server power and this option is enabled, we will not set the desired power state for the service profile.
Step 7	UCSC(resource-mgr) # **scope org**	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 8	UCSC(resource-mgr) /org # **scope service-profile** *profile-name*	Enters service profile organization mode for the service profile.
Step 9	UCSC(resource-mgr) /org/ service-profile # **set power-sync-policy** *name*	

Example

The following example shows how to create a power-sync policy and assign it to a service profile:

```
 UCSC(policy-mgr)# scope org
 UCSC(policy-mgr) /org # create power-sync-policy PowerSync
 UCSC(policy-mgr) /org/power-sync-policy* # set syncoption initial-only-sync
 UCSC(policy-mgr) /org/power-sync-policy* # commit-buffer
 UCSC(policy-mgr) /org/power-sync-policy # end
 UCSC(policy-mgr)# exit

UCSC(resource-mgr)# scope org
UCSC(policy-mgr)(resource-mgr) /org # scope service-profile AAA
UCSC(policy-mgr)(resource-mgr) /org/service-profile # set power-sync-policy PowerSync
UCSC(policy-mgr)(resource-mgr) /org/service-profile* # commit-buffer
```

Creating a Statistics Threshold Policy

Cisco UCS Central lets you create a statistics threshold policy that monitors statistics about certain aspects of the system and generates an event if the threshold is crossed.

Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr) # **connect policy-mgr**	Enters the policy-manager mode.
Step 2	UCSC(policy-mgr)/org # **create stats-threshold-policy** *policy-name*	Creates statistics threshold policy and assigns a name to the policy.
Step 3	UCSC(policy-mgr)/org/stats-threshold-policy* # **create class nvme-stats**	Creates a class for the policy.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr)/org/stats-threshold-policy # **create property temperature**	Creates a property (temperature) for the policy.
Step 5	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **set normal value** *number-value*	Sets a normal value.
Step 6	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **create threshold d-value above-normal warning**	Creates above normal warning range.
Step 7	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **set escalating** *number-value*	Sets the escalating value of the property.
Step 8	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **set deescalating** *number-value*	Sets the deescalating value of the property
Step 9	UCSC(policy-mgr)/org/stats-threshold-policy/class/property* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how Cisco UCS Central creates a statistical threshold policy called test:

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

UCSC(policy-mgr) /org # create stats-threshold-policy test
UCSC(policy-mgr) /org/stats-threshold-policy* # create class nvme-stats
UCSC(policy-mgr) /org/stats-threshold-policy/class* #create property  temperature
UCSC(policy-mgr) /org/stats-threshold-policy/class/property* # set normal-value    100
UCSC(policy-mgr) /org/stats-threshold-policy/class/property* # create threshol d-value
above-normal warning
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* # set escalating
 104
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* #  set
deescalating 101
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value* # commit-buffer
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value # show
configuration
enter threshold-value above-normal warning
     set deescalating 101.000000
     set escalating 104.000000
exit
UCSC(policy-mgr) /org/stats-threshold-policy/class/property/threshold-value # exit
UCSC(policy-mgr) /org/stats-threshold-policy/class/property # exit
UCSC(policy-mgr) /org/stats-threshold-policy/class # exit
UCSC(policy-mgr) /org/stats-threshold-policy # show configuration
enter stats-threshold-policy test
     enter class nvme-stats
         enter property temperature
             enter threshold-value above-normal warning
                 set deescalating 101.000000
                 set escalating 104.000000
             exit
             set normal-value 100.000000
         exit
     exit
```

```
     set descr ""
exit
UCSC(policy-mgr) /org/stats-threshold-policy #
```

Monitoring Threshold Statistics

Cisco UCS Central lets you monitor statistics about aspects of the system and generates an event if the threshold is crossed. You can set both minimum and maximum thresholds which are enforced by endpoints, such as the CIMC.

Note The thresholds are burned into the hardware components at manufacture.

Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr) # **scope system**	Enters into the system.
Step 2	UCSC(resource-mgr) /system # **show stats**	

Example

The following example shows how Cisco UCS Central displays threshold statistics:

```
UCSC(resource-mgr) /system # scope server
UCS-A /chassis/server # show stats

Mb Power Stats:
    Time Collected: 2010-04-20T08:45:31.209
    Monitored Object: sys/chassis-2/blade-4/board
    Suspect: No
    Consumed Power (W): 116.653679
    Input Voltage (V): 12.051000
    Input Current (A): 9.680000
    Thresholded: Input Voltage Min

Mb Temp Stats:
    Time Collected: 2010-04-20T08:45:31.209
    Monitored Object: sys/chassis-2/blade-4/board
    Suspect: No
    Fm Temp Sen Io (C): 19.000000
    Fm Temp Sen Rear (C): 18.000000
    Fm Temp Sen Rear L (C):: N/A
    Fm Temp Sen Rear R (C): N/A
    Thresholded: 0

UCS-A /chassis/server #
```

Creating or Editing a Hardware Change Discovery Policy

You can create a **Hardware Change Discovery** policy in a domain group in Cisco UCS Central and assigned it a 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 sub-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 server-hwchange-disc-policy** *name*	Creates a Hardware Change Discovery policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy *# **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy # **show detail**	Displays details of the Hardware Change Discovery policy .
Step 6	(Optional) UCSC(policy-mgr) /domain-group# **scope server-hwchange-disc-policy** *name*	Enters the specific Hardware Change Discovery Policy.
Step 7	(Optional) UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy *# **show detail**	Displays details of the Hardware Change Discovery policy .
Step 8	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy # **set action user-acknowledged**	Sets the status of the Hardware Change Discovery policy to user acknowledged. This option would trigger a deep-discovery of hardware change after you acknowledge the server and clear the fault.
Step 9	UCSC(policy-mgr) /domain-group/ server-hwchange-disc-policy *# **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a Hardware Change Discovery policy, show details of the policy, and how to set (edit) the policy.

```
UCSC(policy-mgr)connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create server-hwchange-disc-policy hwdp1
UCSC(policy-mgr) /domain-group/server-hwchange-disc-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/server-hwchange-disc-policy # show detail

Server Hardware Change Discovery Policy:
```

```
Name: hwdp1
Description:
Action: User Acknowledged

UCSC(policy-mgr) /domain-group/server-hwchange-disc-policy # exit
UCSC(policy-mgr) /domain-group # show server-hwchange-disc-policy
Server Hardware Change Discovery Policy:
Name Description Action
---------- ----------- ------
hcd-2 User Acknowledged
hd-test1 User Acknowledged
HW_CDP_DG2 User Ack on DG2
User Acknowledged
HwCDP-AutoAck
Auto Acknowledged
HWCDP-Demo1
User Acknowledged
HwCDP-UserAck
Auto Acknowledged
hwdp1 User Acknowledged
Editing a Policy

UCSC(policy-mgr)(policy-mgr) /domain-group/server-hwchange-disc-policy # set action
auto-acknowledged
UCSC(policy-mgr)(policy-mgr) /domain-group/server-hwchange-disc-policy* # commit-buffer
UCSC(policy-mgr)(policy-mgr) /domain-group/server-hwchange-disc-policy # show detail

Server Hardware Change Discovery Policy:
Name: hwdp1
Description:
Action: Auto Acknowledged
```

Deleting a Hardware Change Discovery Policy

Before you begin

You must have created a Hardware Change Discovery policy and assigned it to a domain.

Note If you delete this policy from Cisco UCS Central, the domain profile retains the policy name and automatically associates it with the policy when you create it later with the same name. When you delete a Hardware Change Discovery Policy from Cisco UCS Central, it becomes locally editable on Cisco UCS Manager.

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 sub-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 server-hw-change-disc-policy***name*	Deletes the Hardware Change Discovery policy in the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group *# **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group # **show server-hwchange-disc-policy**	Displays the existing Hardware Change Discovery policies in the system.

Example

This example displays the status of the existing Hardware Change Discovery policies in the system. The policy hwd2 is deleted and does not appear in the list of policies.

```
UCSC(policy-mgr)connect policy-mgr
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr)/domain-group # delete server-hwchange-disc-policy hwd2
UCSC(policy-mgr)/domain-group* # commit-buffer
UCSC(policy-mgr)/domain-group # show server-hwchange-disc-policy
Server Hardware Change Discovery Policy:
Name Description    Action
 ---   --------       ------
hwd-1 from Central User Acknowledged

test1            User Acknowledged
```

Assigning a Hardware Change Discovery Policy to a Domain

You can assign a **Hardware Change Discovery** policy in a domain group to a domain profile.

Before you begin

You must have created a **Hardware Change Discovery** policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile # **set hwchange-disc-policy-name** *name*	Assigns the Hardware Change Discovery policy to the domain profile .

	Command or Action	Purpose
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .
Step 7	(Optional) UCSC(resource-mgr) /fabric/domain/ domain-profile # **show detail**	Displays details of the domain profile and the Hardware Change Discovery Policy name assigned to this domain .

Example

This example shows how to assign a Hardware Discovery Policy hwd1 to a domain profile.

```
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr)/fabric # scope domain 1009
UCSC(resource-mgr)/fabric/domain # scope domain-profile default
UCSC(resource-mgr)/fabric/domain/domain-profile # set
descr hw-change-disc-policy-name inband-policy-name kmip-certificate-policy-name
outband-management-pool
port-disc-policy-name qos-class-policy-name
UCSC(resource-mgr)/fabric/domain/domain-profile # set hw-change-disc-policy-name hwdp1
UCSC(resource-mgr)/fabric/domain/domain-profile* # commit-buffer
UCSC(resource-mgr)/fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: hwdp1
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
```

Unassigning a Hardware Change Discovery Policy

You can un-assign a **Hardware Change Discovery** policy from a domain profile.

Before you begin

You must have assigned a Hardware Change Discovery policy to a domain profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.

	Command or Action	Purpose
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile # **set hw-change-disc-policy ''**	Un-assigns the Hardware Change Discovery policy from the domain profile. The empty string value indicates that no policy is associated with the domain. This prevents the policy from getting pushed down to Cisco UCS Manager.
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .

Example

This example shows how to un-assign a Hardware Change Discovery Policy from a domain profile.

```
UCSC(resource-mgr) /fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: hwdp1 <<< Before unassigned
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
UCSC(resource-mgr) /fabric/domain/domain-profile # set hw-change-disc-policy-name ''
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
UCSC(resource-mgr) /fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: << After Unassigned
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
```

Creating a Port Auto-Discovery Policy

You can create a Port Auto-Discovery Policy and assign it to a domain through the domain profile.

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 sub-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 port-disc-policy** *name*	Creates a Port Auto-Discovery policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ port-disc-policy *# **set server-auto-disc enabled**	Sets the Port Auto-Discovery policy to automatically enabled status.
Step 5	UCSC(policy-mgr) /domain-group/ port-disc-policy* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to create a Port Auto-Discovery Policy and set enable port auto discovery.

```
----------------------------------------------------------------------------------------------
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr)/domain-group # create port-disc-policy-p1
UCSC(policy-mgr)/domain-group/create port-disc-policy* # set server-auto-disc enabled
UCSC(policy-mgr)/domain-group/inband-policy* # commit-buffer
```

Assigning Port Auto-Discovery Policy to a Domain Profile

You can assign a **Port Auto-Discovery** policy in a domain group to a domain profile.

Before you begin

You must have created a port Auto-Discovery policy.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile *# **set port-policy***name*	Assigns the Port Auto-Discovery policy to the domain profile .

	Command or Action	Purpose
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .

Example

This example shows how to assign a Port Auto-Discovery Policy p1 to a domain profile.

```
UCSC # scope resource-mgr
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr)/fabric# scope domain 1009
UCSC(resource-mgr)/fabric/domain# scope domain-profile default
UCSC(resource-mgr) /fabric/domain/domain-profile # set port-policy p1
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
```

Unassigning a Port Auto-Discovery Policy from a Domain

Before you begin

You must have assigned a port Auto-Discovery policy to a domain profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC (resource-mgr) /fabric # **scope domain** *domain ID*	Enters a the specific domain.
Step 4	UCSC (resource-mgr) /fabric/domain # **scope domain-profile default**	Enters a the specific domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile *# **set port-policy″ ″**	Un-assigns the Port Auto-Discovery policy from the domain profile. The empty string value indicates that no policy is associated with the domain profile and it will not be pushed down to Cisco UCS Manager.
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile *# **commit-buffer**	Commits the transaction to the system configuration .

Example

This example shows how to un-assign a Port Auto-Discovery Policy from a domain profile.

```
UCSC # scope resource-mgr
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr)/fabric# scope domain 1009
UCSC(resource-mgr)/fabric/domain# scope domain-profile default
UCSC(resource-mgr) /fabric/domain/domain-profile # set port-policy " "
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
```

Creating a Graphics Card Policy

You can create a Graphics Card Policy to configure an NVIDIA GPU card and assign it to a service profile. This policy facilitates Cisco UCS Manager's support to NVIDIA GPU cards for blade servers. The GPU cards are integrated with the ability to upgrade device firmware through service profiles. Follow this procedure to create or edit or delete a graphics card 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 graphics-card-policy** *name*	Creates graphics card policy for the specified organization.
Step 4	UCSC(policy-mgr) /org/graphics-card-policy* # **commit-buffer**	Commits the pending transaction.

Example

```
UCSC# connect policy-mgr
UCSC(policy-mgr) # scope org
UCSC(policy-mgr) /org # create graphics-card-policy GPUName
UCSC(policy-mgr) /org/graphics-card-policy* # set
descr             graphicscardmode
```

Deleting a Graphics Card Policy

Before you begin

You must have created a Graphics card policy and assigned it to a service 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 graphics-card-policy***name*	Deletes the graphics-card-policy for the specified organization.
Step 4	UCSC* # **commit-buffer**	Commits any pending transactions.

Deleting a Graphics Card Policy

```
UCSC(policy-mgr)/org # delete graphics-card-policy GPU1
UCSC(policy-mgr)* # commit buffer
```

Associating a Service Profile to GPU card

Before you begin

You must have created a Graphics Card policy and assigned it to a 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 service profile organization mode for the service profile.
Step 4	UCSC(resource-mgr) /org /service-profile # **set graphics-card-policy** *mode*	Specifies the GPU mode. It can be graphics, compute or any configuration.
Step 5	UCSC(resource-mgr) /org /service-profile* # **commit-buffer**	Commits the transaction to the system.

Example

This example shows how to associate a service profile to a GPU policy with no mode set.

```
UCSC # connect resource-mgr
```

```
UCSC (resource-mgr)# scope org
UCSC(resource-mgr) /org # scope service-profile GSP_1
UCSC(resource-mgr) /org/service-profile # set graphicscard-policy GPUNone
UCSC(resource-mgr) /org/service-profile* # commit-buffer
```

Inband Policy

Cisco UCS Central lets you configure the Inband IP address on a server directly, or through an **Inband Policy**. This feature is supported on Cisco UCS Manager release 3.1 (3) and later. After you create an Inband policy, you can assign it to a domain group from the **Domain Configuration Settings**. The **Inband Policy** displays details about the corresponding **VLAN Group**, the **Default Management VLAN**, and the **Management IP pool** associated with the policy.

Creating or Editing an Inband Policy

You can create an inband policy and assign it to a domain through the domain profile. You can manually configure the KVM inband IP on the domain servers or through the Inband policy. When you manually change the server's inband configuration, the domain's inband policy remains unchanged.

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 sub-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 inband-policy** *name*	Creates an Inband policy for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ inband-policy *# **set net-group name** *name*	Assigns the netgroup to the inband-policy.
Step 5	UCSC(policy-mgr) /domain-group/ inband-policy *# **set default-ip-pool name**	Assigns the Management IP Pool to the Inband policy.
Step 6	UCSC(policy-mgr) /domain-group/ inband-policy *# **set default-net-name** *name*	Assigns the network (VLAN) to the Inband policy.
Step 7	UCSC(policy-mgr) /domain-group/ inband-policy *# **set default-net-group-name**	Assigns the netgroup to the Inband policy.
Step 8	UCSC(policy-mgr) /domain-group/ inband-policy* # **commit-buffer**	

Example

This example shows how to create an Inband Policy.

```
-----------------------------------------------------------------------------------------------
UCSC(policy-mgr)/domain-group # create inband-policy inband-123
UCSC(policy-mgr)/domain-group/inband-policy* # set net-group-name netgroup-123
UCSC(policy-mgr)/domain-group/inband-policy* # set default-net-name vlan-123
UCSC(policy-mgr)/domain-group/inband-policy* # set default-ip-pool ip-pool-123
UCSC(policy-mgr)/domain-group/inband-policy* # commit-buffer
UCSC(policy-mgr)/domain-group/inband-policy # show detail

Inband Policy:
Name: inband-123
Net Group Name: netgroup-123
Default Network: vlan-123
Default IP Pool: ip-pool-123
Name: inband-pol-1
Net Group Name:
Default Network:
Default IP Pool: pool-abc
UCSC(policy-mgr) /domain-group/inband-policy # exit
UCSC(policy-mgr) /domain-group # show inband-policy

Inband Policy:
Name Net Group Name Default Network Default IP Pool
---------- -------------- --------------- ---------------
inband-123 netgroup-123 vlan-123 ip-pool-123
```

Creating a Management IP Pool

You can create a Management IP Pool comprising IPv4 and IPv6 blocks and assign them to an Inband policy or use it as an Outband Pool.

Note IPv6 is not supported for Outband KVM management.

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 sub-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 ip-pool** *pool-name*	Creates an IPv4 pool for the specified domain group.
Step 4	UCSC(policy-mgr) /domain-group/ ip-pool* # **commit-buffer**	Commits the transaction to the system configuration.
Step 5	UCSC(policy-mgr) /domain-group/ ip-pool# **create block** *IP from IP to Default Gateway Subnet Mask*	Creates an IPv4 pool block.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /domain-group/ ip-pool/block* # **commit-buffer**	Commits the transaction to the system configuration.
Step 7	UCSC(policy-mgr) /domain-group/ ip-pool/block # **show detail**	Displays details of the IPv4 block.
Step 8	UCSC(policy-mgr) /domain-group/ ip-pool/block # **exit**	Exits the IP pool block.
Step 9	UCSC(policy-mgr) /domain-group/ ip-pool # **create IPv6-block** *IP from IP to prefix block qualifier*	Creates an IPv6 block.
Step 10	UCSC(policy-mgr) /domain-group/ ip-pool/ ipv6-block* # **commit-buffer**	Commits the transaction to the system configuration.
Step 11	UCSC(policy-mgr) /domain-group/ ip-pool/ ipv6-block* # **show detail**	Displays the block of IPv6 addresses.

Example

This example shows how to create an IP Pool and add block addresses.

```
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create ip-pool test
UCSC(policy-mgr) /domain-group/ip-pool* # commit buffer
UCSC(policy-mgr) /domain-group/ip-pool # create block 1.2.3.4 1.2.3.8 1.2.3.254 255.255.255.0

UCSC(policy-mgr) /domain-group/ip-pool/block* # commit buffer
UCSC(policy-mgr) /domain-group/ip-pool/block # show detail
Block of IP Addresses:
    From: 1.2.3.4
    To: 1.2.3.8
    Default Gateway: 1.2.3.254
    Subnet Mask: 255.255.255.0
    Primary DNS: 0.0.0.0
    Secondary DNS: 0.0.0.0
    Scope: Public
    Config Scope: Public
    Block Qualifier:
USCS(policy-mgr) /domain-group/ip-pool/block # exit
UCSC(policy-mgr) /domain-group/ip-pool*# create ipv6-block
UCSC(policy-mgr) /domain-group/ip-pool*# create ipv6-block 2001:0000::808:808
2001:0000::808:880 2001:0000::808:801 64
UCSC(policy-mgr) /domain-group/ip-pool/ipv6-block* # commit buffer
UCSC(policy-mgr) /domain-group/ip-pool/ipv6-block # show detail
Block of IPv6 Addresses:
From To Prefix Block Qualifier
----------------------- ------------------------ ------ ---------------
2001:0000::808:808 2001:0000::808:880 64
```

Assigning KVM Outband to a UCS Domain

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	
Step 2	UCSC(resource-mgr) # **scope fabric**	Enters the fabric.
Step 3	UCSC(resource-mgr) /fabric# **scope domain** *ID*	Enters the specific domain .
Step 4	UCSC(resource-mgr) /fabric/domain # **scope domain-profile default**	Sets the default domain profile.
Step 5	UCSC(resource-mgr) /fabric/domain/domain-profile # **set outband-management-pool** *name*	Assigns the Outband Management pool to the domain.
Step 6	UCSC(resource-mgr) /fabric/domain/domain-profile* # **commit-buffer**	Commits the transaction to the system configuration.

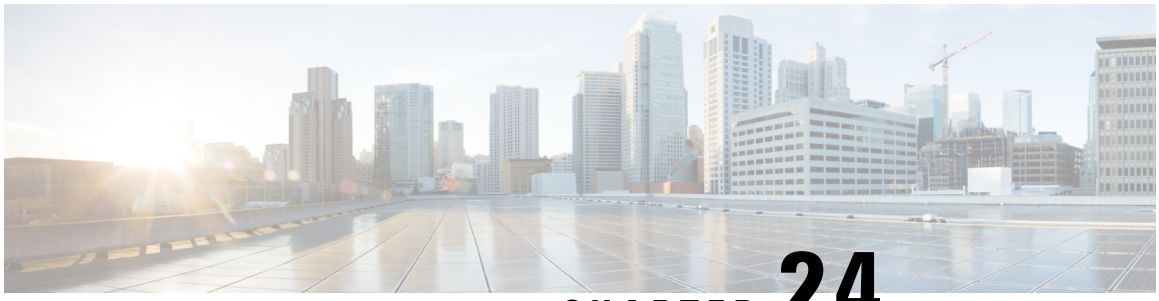
Example

This example shows how to assign a 'pool-abc' to domain 1009 as a KVM Outband and show detail:

```
--------------------------------------
UCSC# connect resouce-mgr
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr) /fabric # scope domain 1009
UCSC(resource-mgr) /fabric # scope domain-profile default
UCSC(resource-mgr) /fabric/domain/domain-profile # set outband-management-pool pool-abc
UCSC(resource-mgr) /fabric/domain/domain-profile* # commit-buffer
UCSC(resource-mgr) /fabric/domain/domain-profile # show detail

Domain Profile:
Name: default
Port Disc Policy Name:
HW Change Disc Policy Name: HwCDP-UserAck
Inband Policy Name:
KMIP Certificate Policy Name:
Outband Management Pool: pool-abc <<<<
Qos Class Policy Name:
Descr: Autogenerated domain profile for domain id 1009
Current Task:
```

PART V

Storage Management



CHAPTER 24

Ports and Port Channels

Server and Uplink Ports

Each fabric interconnect can include the following port types:

Server Ports

Server ports handle data traffic between the fabric interconnect and the adapter cards on the servers.

Uplink Ethernet Ports

Uplink Ethernet ports handle Ethernet traffic between the fabric interconnect and the next layer of the network. All network-bound Ethernet traffic is pinned to one of these ports.

By default, Ethernet ports are unconfigured. However, you can configure them to function in the following ways:

- Uplink
- FCoE
- Appliance

You can configure uplink Ethernet ports on either the fixed module or an expansion module.

Uplink Fibre Channel Ports

Uplink Fibre Channel ports handle FCoE traffic between the fabric interconnect and the next layer of the storage area network. All network-bound FCoE traffic is pinned to one of these ports.

By default, Fibre Channel ports are uplink. However, you can configure them to function as Fibre Channel storage ports. This is useful in cases where Cisco UCS requires a connection to a Direct-Attached Storage (DAS) device.

You can only configure uplink Fibre Channel ports on an expansion module. The fixed module does not include uplink Fibre Channel ports.

Unified Ports

Unified ports can be configured to carry either Ethernet or Fibre Channel traffic. These ports are not reserved. A Cisco UCS domain cannot use these ports until you configure them.

All ports on the following fabric interconnects are unified:

- Cisco UCS 6248 UP Fabric Interconnect
- Cisco UCS 6296 UP Fabric Interconnect
- Cisco UCS 6324 Fabric Interconnect
- Cisco UCS 6332-16UP Fabric Interconnect

Note When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. If the port is connected to another device, this may cause traffic disruption. You can disable the port after configuring it.

Unified Storage Ports

Unified storage is configuring the same physical port as an Ethernet storage interface and FCoE storage interface. You can configure any appliance port or FCoE storage port as a unified storage port on either a fixed module or an expansion module. To configure a unified storage port, the fabric interconnect must be in Fibre Channel switching mode.

In a unified storage port, you can enable/disable individual FCoE storage or appliance interfaces.

- In an unified storage port, if you do not specify a non default VLAN for the appliance port the fcoe-storage-native-vlan will be assigned as the native VLAN on the unified storage port. If the appliance port has a non default native VLAN specified as native VLAN, this will be assigned as the native VLAN for unified storage port.
- When you enable or disable the appliance interface, the corresponding physical port is enabled/disabled. So when you disable the appliance interface in a unified storage, even if the FCoE storage is enabled, it goes down with the physical port.
- When you enable or disable FCoE storage interface, the corresponding VFC is enabled or disabled. So when the FCoE storage interface is disabled in a unified storage port, the appliance interface will continue to function normally.

Unified Uplink Ports

When you configure an Ethernet uplink and an FCoE uplink on the same physical Ethernet port, it is called the unified uplink port. You can individually enable or disable either FCoE or Ethernet interfaces independently.

- Enabling or disabling the FCoE uplink results in corresponding VFC being enabled or disabled.
- Enabling or disabling an Ethernet uplink results in corresponding physical port being enabled or disabled.

If you disable an Ethernet uplink, it disables the underlying physical port in an unified uplink. So, even if the FCoE uplink is enabled, the FCoE uplink also goes down. But if you disable an FCoE uplink, only the VFC goes down. If the Ethernet uplink is enabled, it can still function properly in the unified uplink port.

Ports on the Cisco UCS 6300 Series Fabric Interconnects

The Cisco UCS 6300 Series Fabric Interconnect includes the Cisco UCS 6324 Fabric Interconnect for UCS Mini (Cisco UCS Manager Release 3.0), and the Cisco UCS 6332 and 6332-16UP Fabric Interconnects (Cisco UCS Manager Release 3.1).

The following table summarizes the port usage for the Cisco UCS 6300 Series Fabric Interconnects:

Fabric Interconnect Name:	Cisco UCS 6324 (Cisco UCS Mini)	Cisco UCS 6332	Cisco UCS 6332-16UP
Description:	Fabric Interconnect with 4 unified ports and 1 scalability port	32–Port Fabric Interconnect	40–Port Fabric Interconnect
Number of fixed 40 GB Interfaces:	—	6 (ports 17-32)	6 (ports 35-40)
Number of 1GB/10GB Interfaces (depending on the SFP module installed)	All	Ports 5–26 using breakout cable	Ports 17–34 using breakout cable
Unified Ports (8 Gb/s, FC, FCoE)	4	None	Ports 1–16

Note Cisco UCS 6300 Series Fabric Interconnects support breakout capability for ports. For more information on how the 40G ports can be converted into four 10G ports, see Scalability and Breakout Ports, on page 547.

Port Modes

The port mode determines whether a unified port on the fabric interconnect is configured to carry Ethernet or Fibre Channel traffic. The fabric interconnect does not automatically discover the port mode. You configure the port mode in Cisco UCS Central.

Changing the port mode deletes the existing port configuration and replaces it by a new logical port. Any objects associated with that port configuration, such as VLANs and VSANS, are removed. There is no restriction on the number of times you can change the port mode for a unified port.

Effect of Port Mode Changes on Data Traffic

Port mode changes can cause an interruption to the data traffic for the Cisco UCS domain. The length of the interruption and the traffic that is affected depend upon the configuration of the Cisco UCS domain and the module on which you made the port mode changes.

Tip To minimize the traffic disruption during system changes, form a Fibre Channel uplink port-channel across the fixed and expansion modules.

Impact of Port Mode Changes on an Expansion Module

After you make port mode changes on an expansion module, the module reboots. All traffic through ports on the expansion module is interrupted for approximately one minute while the module reboots.

Impact of Port Mode Changes on the Fixed Module in a Cluster Configuration

A cluster configuration has two fabric interconnects. After you make port changes to the fixed module, the fabric interconnect reboots. The impact on the data traffic depends upon whether or not you have configured the server vNICs to failover to the other fabric interconnect when one fails.

If you change the port modes on the expansion module of one fabric interconnect and then wait for that to reboot before changing the port modes on the second fabric interconnect, the following occurs:

- With server vNIC failover, traffic fails over to the other fabric interconnect and no interruption occurs.
- Without server vNIC failover, all data traffic through the fabric interconnect on which you changed the port modes is interrupted for approximately eight minutes while the fabric interconnect reboots.

If you change the port modes on the fixed modules of both fabric interconnects simultaneously, all data traffic through the fabric interconnects are interrupted for approximately eight minutes while the fabric interconnects reboot.

Impact of Port Mode Changes on the Fixed Module in a Standalone Configuration

A standalone configuration has only one fabric interconnect. After you make port changes to the fixed module, the fabric interconnect reboots. All data traffic through the fabric interconnect is interrupted for approximately eight minutes while the fabric interconnect reboots.

Port Roles

The port role defines the type of traffic carried over a unified port connection.

All of the port roles listed are configurable on both the fixed and expansion module, including server ports, which are configurable on the 6200 and later series fabric interconnect expansion modules.

By default, unified ports changed to Ethernet port mode are set to the uplink Ethernet port role. Unified ports changed to Fibre Channel (FC) port mode are set to the FC uplink port role. You cannot unconfigure FC ports.

Changing the port role does not require a reboot.

When you set the port mode to Ethernet, you can configure the following port roles:

- Server ports
- Ethernet uplink ports
- FCoE storage ports
- FCoE uplink ports
- Appliance ports

When you set the port mode to FC, you can configure the following port roles:

- FC uplink ports
- FC storage ports

Guidelines for Configuring Unified Ports

Consider the following guidelines and restrictions when configuring unified ports:

Hardware and Software Requirements

Unified ports are not supported on 6100 series fabric interconnects.

Port Mode Placement

Because the Cisco UCS Central GUI interface uses a slider to configure the port mode for unified ports on a fixed or expansion module, it automatically enforces the following restrictions which limits how port modes can be assigned to unified ports. When using the Cisco UCS Central CLI interface, these restrictions are enforced when you commit the transaction to the system configuration. If the port mode configuration violates any of the following restrictions, the Cisco UCS Central CLI displays an error:

- Ethernet ports must be grouped together in a block. For each module (fixed or expansion), the Ethernet port block must start with the first port and end with an even numbered port.
- Fibre Channel ports must be grouped together in a block. For each module (fixed or expansion), the first port in the Fibre Channel port block must follow the last Ethernet port and extend to include the rest of the ports in the module. For configurations that include only Fibre Channel ports, the Fibre Channel block must start with the first port on the fixed or expansion module.
- Alternating Ethernet and Fibre Channel ports is not supported on a single module.

Example of a valid configuration— Might include unified ports 1–16 on the fixed module configured in Ethernet port mode and ports 17–32 in Fibre Channel port mode. On the expansion module you could configure ports 1–4 in Ethernet port mode and then configure ports 5–16 in Fibre Channel mode. The rule about alternating Ethernet and Fibre Channel port types is not violated because this port arrangement complies with the rules on each individual module.

Example of an invalid configuration— Might include a block of Fibre Channel ports starting with port 16. Because each block of ports has to start with an odd-numbered port, you would have to start the block with port 17.

Note The total number of uplink Ethernet ports and uplink Ethernet port channel members that can be configured on each fabric interconnect is limited to 31. This limitation includes uplink Ethernet ports and uplink Ethernet port channel members configured on the expansion module.

The 40GB ports on the 6300 series fabric interconnects do not support expansion module configuration.

Cautions and Guidelines for Configuring Unified Uplink Ports and Unified Storage Ports

The following are cautions and guidelines to follow while working with unified uplink ports and unified storage ports:

- You must configure a non default native VLAN on FCoE and unified uplink ports. This VLAN is not used for any traffic. Cisco UCS Central will reuse an existing fcoe-storage-native-vlan for this purpose. This fcoe-storage-native-vlan will be used as a native VLAN on FCoE and unified uplinks.
- In an unified uplink port, if you do not specify a non default VLAN for the Ethernet uplink port the fcoe-storage-native-vlan will be assigned as the native VLAN on the unified uplink port. If the Ethernet port has a non default native VLAN specified as native VLAN, this will be assigned as the native VLAN for unified uplink port.
- When you create or delete a member port under an Ethernet port channel, Cisco UCS Central automatically creates or deletes the member port under FCoE port channel. The same happens when you create or delete a member port in FCoE port channel.
- When you configure an Ethernet port as a standalone port, such as server port, Ethernet uplink, FCoE uplink or FCoE storage and make it as a member port for an Ethernet or FCOE port channel, Cisco UCS Central automatically makes this port as a member of both Ethernet and FCoE port channels.
- When you remove the membership for a member port from being a member of server uplink, Ethernet uplink, FCoE uplink or FCoE storage, Cisco UCS Central deletes the corresponding members ports from Ethernet port channel and FCoE port channel and creates a new standalone port.
- For unified uplink ports and unified storage ports, when you create two interfaces, only one license is checked out. As long as either interface is enabled, the license remains checked out. The license will be released only if both the interfaces are disabled for a unified uplink port or a unified storage port.
- Cisco UCS 6100 series fabric interconnect switch can only support 1VF or 1VF-PO facing same downstream NPV switch.

Configuring Ports

Note Ports configured for Cisco UCS Manager releases prior to 3.1 were supported in Cisco UCS Central release 1.3, but are not supported in later releases of Cisco UCS Central. Any additional configuration of those ports must be done in Cisco UCS Manager.

Before you begin

- You must be running Cisco UCS Manager release 3.1 or above.
- All Cisco UCS Manager domains must be included in a Cisco UCS Central domain group.
- Port Configuration must be set to Global on the Policy Resolution Control page in Cisco UCS Manager.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click **Ports**.

Step 4 Choose the port that you want to configure.

Step 5 On the Ports page, click the **Tools** icon on the far right and select **Configure Port**.

The **Configure Port** page for the selected port displays.

Step 6 Select the **Role** for the port.

For Ethernet ports, this can be one of the following:

- Appliance
- FCoE Storage
- FCoE Uplink
- Server
- Uplink

For FC ports, this can be one of the following:

- FC Uplink
- FC Storage

Step 7 Complete the fields as required for your selection.

Step 8 Click **Save**.

Configuring an Appliance Port

Appliance ports are used to connect fabric interconnects to directly attached NFS storage.

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured. To enable or disable the port, enter the interface mode and use **enable** or **disable** command.

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# **scope eth-storage**	Enters the Ethernet storage mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric # **create interface** *slot-id port-id*	Creates the appliance port and enters interface mode.
Step 7	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface # **set user-label** *user-label-name*	Sets the user label for this port.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure the appliance port and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-storage
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric # create interface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface* # set user-label
EthStorage1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface #
```

Configuring an Ethernet Uplink Port

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured. To enable or disable the port, enter the interface mode and use **enable** or **disable** command.

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# **scope eth-uplink**	Enters the Ethernet uplink mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric # **create interface** *slot-id port-id*	Creates the ethernet uplink port and enters interface mode.
Step 7	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface # **set** {**eth-link-profile** *eth-link-profile-name* | **flow-control-policy** *policy-name* | **speed** {**1** | **10** | **40**} | **user-label** *user-label-name*}	Enables you to specify options for this uplink port. You can specify all of the following options at the same time or do any one of them as required: • **eth-link-profile**—Sets the Ethernet link profile name. • **flow-control-policy**—Sets the flow control policy. • **speed**—Sets the desired speed. If you do not specify the speed, the default speed will be 10 gbps. • **user-label**—Sets the user label.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure the Ethernet uplink port and commit the transaction:

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

```
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric # create interface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface* # set eth-link-profile
 ELP_1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface* # set
flow-control-policy FCP_1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface #
```

Configuring an Ethernet Server Port

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured. To enable or disable the port, enter the interface mode and use **enable** or **disable** command.

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# **scope eth-server**	Enters the Ethernet server mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric # **create interface** *slot-id port-id*	Creates the server port and enters interface mode.
Step 7	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/interface # **set user-label** *user-label-name*	Sets the user label for this port.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/interface # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure the server port and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-server
```

```
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric # create interface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/interface* # set user-lable
EthServer1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/interface* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/interface #
```

Configuring an FCoE Storage Port

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured. To enable or disable the port, enter the interface mode and use **enable** or **disable** command.

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# **scope fc-storage**	Enters the FCoE storage mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # **create interface fcoe** *slot-id port-id*	Creates the FCoE storage port and enters FCoE mode.
Step 7	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe # **set user-label** *user-label-name* | **vsan-member** *vsan_name*}	Enables you to specify options for this FCoE storage port. You can specify all of the following options at the same time or do any one of them as required: • **user-label**—Sets the user label. • **vsan-member**—Sets the VSAN member name.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure the FCoE storage port and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-storage
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # create interface fcoe 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe* # set fillpattern idle
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe* # set vsan-member VSAN1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe #
```

Configuring an FCoE Uplink Port

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured. To enable or disable the port, enter the interface mode and use **enable** or **disable** command.

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# **scope fc-uplink**	Enters the FC uplink mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create fcoeinterface** *slot-id port-id*	Creates the FCoE uplink port and enters interface mode.
Step 7	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface # **set** {**eth-link-profile** *eth-link-profile-name* | **user-label** *user-label-name*}	Enables you to specify options for this FCoE uplink port. You can specify all of the following options at the same time or do any one of them as required: • **eth-link-profile**—Sets the Ethernet link profile name. • **user-label**—Sets the user label.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure the FCoE uplink port and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create fcoeinterface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface* # set
eth-link-profile ELP_1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface #
```

Configuring an FC Storage Port

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured. To enable or disable the port, enter the interface mode and use **enable** or **disable** command.

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# **scope fc-storage**	Enters the FC storage mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # **create interface fc** *slot-id port-id*	Creates the fc storage port and enters FC mode.
Step 7	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc # **set** {**fillpattern** {**arbff** | **idle**} | **user-label** *user-label-name* | **vsan-member** *vsan_name*}	Enables you to specify options for this FC storage port. You can specify all of the following options at the same time or do any one of them as required: • **fillpattern**—Sets the fill pattern. • **user-label**—Sets the user label. • **vsan-member**—Sets the VSAN member name.

	Command or Action	Purpose
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure the FC storage port and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-storage
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # create interface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc* # set fillpattern idle
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc* # set vsan-member VSAN1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc #
```

Configuring an FC Uplink Port

When you configure a port on a fabric interconnect, the administrative state is automatically set to enabled. You can disable the port after it is configured. To enable or disable the port, enter the interface mode and use **enable** or **disable** command.

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# **scope fc-uplink**	Enters the FC uplink mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create interface** *slot-id port-id*	Creates the ethernet uplink port and enters interface mode.
Step 7	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface # **set** {**fillpattern** {**arbff** | **idle**} | **user-label** *user-label-name* | **vsan-member** *vsan_name*}	Enables you to specify options for this FC uplink port. You can specify all of the following options at the same time or do any one of them as required: • **fillpattern**—Sets the fill pattern.

	Command or Action	Purpose
		• **user-label**—Sets the user label. • **vsan-member**—Sets the VSAN member name.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure the FC uplink port and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create interface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface* # set fillpattern
idle
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface* # set vsan-member
VSAN1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface #
```

Scalability and Breakout Ports

The Cisco UCS 6300 Series Fabric Interconnects contain scalability ports that can be broken out into groups of 4 10-Gigabit Ethernet ports. The configuration requires a Small Form-Factor Pluggable adapter (SPF) that has one 40GB QSFP+ on one end to connect to the Fabric Interconnect, and four 10 GB ports to connect to different end points supporting 10 GB connectivity.

- The Cisco UCS 6324 Fabric Interconnect contains one scalability port that can be used as a licensed server port for supported Cisco UCS rack servers, an appliance port, or a FCoE storage port.
- The Cisco UCS 6332 and Cisco UCS 6332-16 UP fabric interconnects contain multiple 40-Gigabet Ethernet ports that can be broken out into 10-Gigabit Ethernet ports.

Caution Configuring breakout ports requires rebooting the Fabric Interconnect. Any existing configuration on a port is erased. It is recommended to break out all required ports in a single transaction.

Once you configure a breakout port, you can configure each 10 GB sub-port as server, uplink, FCoE uplink, FCoE storage or appliance port as required.

The following table summarizes the constraints for breakout functionality for the Cisco UCS 6332 and 6332-16UP fabric interconnects:

Fabric Interconnect	Breakout Configurable Ports	Normal Ports with no Breakout Support
UCS-FI-6332	1-12,15-26	13-14,27-32 **Note** • Auto-negotiate behavior is not supported on ports 27–32. • A maximum of four ports are allowed as breakout ports if using QoS jumbo frames.
UCS-FI-6332-16UP	17-34	1-16,35-40 **Note** • Auto-negotiate behavior is not supported on ports 35-40. • A maximum of four ports are allowed as breakout ports if using QoS jumbo frames.

Creating a Port Channel

Procedure

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 In the Fabric Interconnect page, click the **Tools** icon and choose **Create Port Channel**.

Step 4 In **Basic**, select the type of port channel that you want to create.

This can be one of the following:

Step 5 Complete the fields as required for your selection.

Step 6 Click **Save**.

Configuring an Appliance Port Channel

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# **scope eth-storage**	Enters the Ethernet storage mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric # **create port-channel** *port-channel-ID*	Creates the appliance port channel and enters port channel mode.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/port-channel # **create member-port** *slot-id port-id*	Creates the appliance port and enters interface mode.
Step 8	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/port-channel/member-port # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure an appliance port channel with two members and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-storage
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric # create port-channel 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/port-channel* # create
member-port 1 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/port-channel/member-port* #
exit
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/port-channel* # create
member-port 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/port-channel/member-port* #
commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/port-channel/member-port #
```

Configuring an FC Uplink Port Channel

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# **scope fc-uplink**	Enters the FC uplink mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create port-channel** *port-channel-ID*	Creates the ethernet uplink port and enters interface mode.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel # **create member-port** *slot-id port-id*	Creates the member port for this port channel, and enters FC uplink member port mode.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel/member-port # **set fillpattern** {**arbff** | **idle**}	Sets the fill pattern.
Step 9	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel/member-port # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure an FC uplink port channel with two members and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create port-channel 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel* # create member-port
 1 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel/member-port* #
exit
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel* # create member-port
 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel/member-port* #
commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel/member-port #
```

Configuring an FCoE Uplink Port Channel

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# **scope fc-uplink**	Enters the FC uplink mode.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {**a** | **b**}	Enters the fabric interconnect mode.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create fcoe-port-channel** *port-channel-ID*	Creates the FCoE uplink port channel and enters FCoE port channel mode.
Step 7	Required: UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel # **create fcoe-member-port** *slot-id port-id*	Creates the member port for this port channel, and enters FCoE uplink member port mode.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **eth-link-profile**	Sets the Ethernet link profile name.
Step 9	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel/fcoe-member-port # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to configure an FCoE uplink port channel with two members and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create fcoe-port-channel 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel* # create
fcoe-member-port 1 1
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel/fcoe-member-port* # exit
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel* # create
fcoe-member-port 1 2
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel/fcoe-member-port* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel/fcoe-member-port
 #
```

Pin Groups

LAN Pin Groups

Cisco UCS uses LAN pin groups to pin Ethernet traffic from a vNIC on a server to an uplink Ethernet port or port channel on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

To configure pinning for a server, you must include the LAN pin group in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server. All traffic from the vNIC travels through the I/O module to the specified uplink Ethernet port.

Note If you do not assign a pin group to a server interface through a vNIC policy, Cisco UCS Central chooses an uplink Ethernet port or port channel for traffic from that server interface dynamically. This choice is not permanent. A different uplink Ethernet port or port channel may be used for traffic from that server interface after an interface flap or a server reboot.

If an uplink is part of a LAN pin group, the uplink is not necessarily reserved for only that LAN pin group. Other vNIC's policies that do not specify a LAN pin group can use the uplink as a dynamic uplink.

SAN Pin Groups

Cisco UCS uses SAN pin groups to pin Fibre Channel traffic from a vHBA on a server to an uplink Fibre Channel port on the fabric interconnect. You can use this pinning to manage the distribution of traffic from the servers.

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups will be ignored.

To configure pinning for a server, you must include the SAN pin group in a vHBA policy. The vHBA policy is then included in the service profile assigned to that server. All traffic from the vHBA will travel through the I/O module to the specified uplink Fibre Channel port.

You can assign the same pin group to multiple vHBA policies. As a result, you do not need to manually pin the traffic for each vHBA.

Important Changing the target interface for an existing SAN pin group disrupts traffic for all vHBAs which use that pin group. The fabric interconnect performs a log in and log out for the Fibre Channel protocols to re-pin the traffic.

Configuring a LAN Pin Group

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 # **scope eth-uplink**	Enters Ethernet uplink mode.
Step 5	UCSC(resource-mgr) /domain-mgmt /ucs-domain/eth-uplink # **create pin-group** *pin_group_name*	Creates an Ethernet (LAN) pin group with the specified name, and enters Ethernet uplink pin group mode.
Step 6	UCSC(resource-mgr) /domain-mgmt /ucs-domain/eth-uplink/pin-group # **set target** {**a** | **b**} {**port** *slot-num*/*port-num* | **port-channel** *port-channel-ID*}	Sets the Ethernet pin target to the specified fabric and port, or fabric and port channel.
Step 7	UCSC(resource-mgr) /domain-mgmt /ucs-domain/eth-uplink/pin-group # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a LAN pin group named ethpingroup12, set the pin group target to slot 1, port 2, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1009
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink # create pin-group ethpingroup12
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/pin-group* # set target a port 1/2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/pin-group* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/pin-group #
```

Configuring a SAN Pin Group

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.

	Command or Action	Purpose
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 # **scope fc-uplink**	Enters Fibre Channel uplink mode.
Step 5	UCSC(resource-mgr) /domain-mgmt /ucs-domain/fc-uplink # **create pin-group** *pin_group_name*	Creates a Fibre Channel (SAN) pin group with the specified name, and enters Fibre Channel uplink pin group mode.
Step 6	UCSC(resource-mgr) /domain-mgmt /ucs-domain/fc-uplink/pin-group # **set target** {**a** | **b**} {**port** *slot-num*/*port-num* | **port-channel** *port-channel-ID*}	Sets the Fibre Channel pin target to the specified fabric and port, or fabric and port-channel.
Step 7	UCSC(resource-mgr) /domain-mgmt /ucs-domain/fc-uplink/pin-group # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a SAN pin group named fcpingroup12, set the pin group target to slot 2, port 1, and commit the transaction:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1009
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # create pin-group fcpingroup12
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/pin-group* # set target a port 2/1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/pin-group* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/pin-group #
```

Fibre Channel Switching Mode

The Fibre Channel switching mode determines how the fabric interconnect behaves as a switching device between the servers and storage devices. The fabric interconnect operates in either of the following Fibre Channel switching modes:

End-Host Mode

End-host mode allows the fabric interconnect to act as an end host to the connected fibre channel networks, representing all servers (hosts) connected to it through virtual host bus adapters (vHBAs). This behavior is achieved by pinning (either dynamically pinned or hard pinned) vHBAs to Fibre Channel uplink ports, which makes the Fibre Channel ports appear as server ports (N-ports) to the rest of the fabric. When in end-host mode, the fabric interconnect avoids loops by denying uplink ports from receiving traffic from one another.

End-host mode is synonymous with N Port Virtualization (NPV) mode. This mode is the default Fibre Channel Switching mode.

Note When you enable end-host mode, if a vHBA is hard pinned to an uplink Fibre Channel port and this uplink port goes down, the system cannot repin the vHBA, and the vHBA remains down.

Switch Mode

Switch mode is the traditional Fibre Channel switching mode. Switch mode allows the fabric interconnect to connect directly to a storage device. Enabling Fibre Channel switch mode is useful in Pod models where there is no SAN (for example, a single Cisco UCS domain that is connected directly to storage), or where a SAN exists (with an upstream MDS).

Switch mode is not the default Fibre Channel switching mode.

Note In Fibre Channel switch mode, SAN pin groups are irrelevant. Any existing SAN pin groups are ignored.

Configuring Fibre Channel Switching Mode

You can configure your fabric interconnect to use either FC End-Host Mode or FC Switch Mode. By default, the FI is set to end-host mode.

Note When you change the Fibre Channel switching mode, Cisco UCS Central logs you out and restarts the fabric interconnect. For a cluster configuration, Cisco UCS Central restarts both fabric interconnects sequentially. The second fabric interconnect can take several minutes to complete the change in Fibre Channel switching mode and become system ready.

Procedure

Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 On the fabric interconnect page, click the **Tools** icon and select the **FC switching mode**.

If you are using end-host mode, **Set FC Switching Mode** displays. If you are using FC switching mode, **Set FC End-Host Mode** displays.

Step 4 Click **Yes** on the warning page to change the configuration and restart the FI.

Viewing Port Configuration Status

Procedure

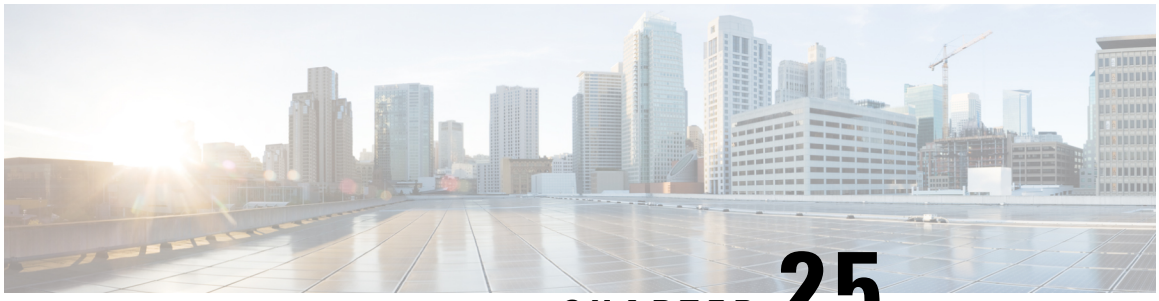
Step 1 Click the **Browse Tables** icon and choose **Fabric Interconnects**.

Step 2 Click on a Fabric Interconnect to open it for editing.

Step 3 Click the Tools icon on the far right and select **Configuration Status**.

The Configuration Status page for the selected port displays.

Step 4 Click **Close** to close the window.



CHAPTER 25

Global VSAN

Global VSAN

Cisco UCS Central enables you to define global VSAN in the SAN cloud, at the domain group root, or at a domain group level. The global VSANs created in Cisco UCS Central are specific to the fabric interconnect where you create them. You can assign a VSAN to either Fabric A or Fabric B, or to both Fabric A and B. Global VSANs are not common VSANs in Cisco UCS Central.

Resolution of global VSANs takes place in Cisco UCS Central prior to deployment of global service profiles that reference them to Cisco UCS Manager. If a global service profile references a global VSAN, and that VSAN does not exist, deployment of the global service profile to Cisco UCS Manager will fail due to insufficient resources. All global VSANs created in Cisco UCS Central must be resolved before deploying that global service profile.

Note Beginning with Cisco UCS Manager Release 1.3, you can push global VSANs to Cisco UCS Manager without deploying a service profile. For more information, see .

VSANs deployed with a global service profile are visible to Cisco UCS Manager only if a global service profile is deployed that references the VSANs. Once a VSAN deployed with a global service profile becomes available in Cisco UCS Manager, locally-defined service profiles and policies can reference it. A global VSAN is not deleted when a global service profile that references it is deleted.

Global VSANs that are referenced by a global service profile available to a Cisco UCS Manager instance remain available unless they are specifically deleted for use from the domain group. Global VSANs can be localized in Cisco UCS Manager, in which case they act as local VSANs. Unless a global VSAN is localized, it cannot be deleted from Cisco UCS Manager.

Creating VSANs

This procedure describes how to create VSANs in a domain group 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 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 the configuration mode for the chosen fabric interconnect .
Step 5	UCSC(resource-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.
Step 6	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan #**commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create two VSANs each for both fabric interconnect A and B 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/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(resource-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(resource-mgr) /domain-group/fc-uplink #scope fabric b
UCSC(resource-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(resource-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
```

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. • enabled—Cisco UCS Manager will configure and control Fibre Channel zoning when the VSAN is deployed.	Sets the Fibre Channel zoning for the VSAN, as follows:
Step 9	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan* # **commit-buffer**	Commits the transaction to the system.

Example

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 #
```

Enabling Global VSANs in a Cisco UCS Manager Instance

The **publish vsan** command allows you to use global VSANs that were created in Cisco UCS Central in a Cisco UCS Manager instance without deploying a service profile.

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 domain management configuration mode.
Step 3	UCSC(resource-mgr) /domain-mgmt #**scope ucs-domain** *domain-ID*	Enters the UCS domain configuration mode for the specified domain ID. **Note** If you do not know the UCS domain ID, use the **show ucs-domain** command.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain #**publish vsan** *vsan_name [a \ b]*.	Pushes the selected global VSAN to the Cisco UCS Manager instance in the specified fabric interconnect.

Example

The following example shows how to enable global VSAN globVSAN for fabric interconnect A in the local domain 1008:

```
UCSC# connect resource-mgr
UCSC(resource-mgr) # scope domain-mgmt
UCSC(resrouce-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resrouce-mgr) /domain-mgmt/ucs-domain # publish vsan globVSAN a

Publish Vsan is a standalone operation. You may lose any uncommitted changes in this CLI
session.
Do you want to continue? (yes/no): yes
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

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-name*	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.
Step 7	UCSC(resource-mgr)#/domain-group/fc-uplink #/fc-uplink/fabric/vsan* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to delete one VSAN from fabric interconnect A and one from fabric interconnect B for domain group 12:

```
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 #
```

Fibre Channel Zoning

Fibre Channel (FC) zoning allows you to partition the Fibre Channel fabric into one or more zones. Each zone defines the set of FC initiators and FC targets that can communicate with each other in a VSAN.

The access and data traffic control provided by zoning does the following:

- Enhances SAN network security
- Helps prevent data loss or corruption
- Reduces performance issues

Cisco UCS Central FC zoning combines direct attach storage with local zoning. Fibre Channel or FCoE storage is directly connected to the fabric interconnects, and zoning is performed in Cisco UCS Central, using Cisco UCS local zoning.

Configuring FC Zoning on a VSAN

This procedure describes how to create Fibre Channel zoning on an existing VSAN.

Procedure

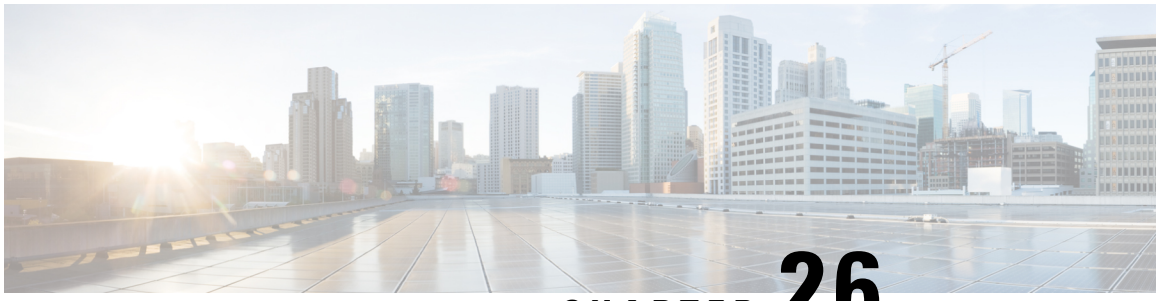
	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) #**scope domain-group** *domain-group*	Enters the UCS domain group configuration mode.
Step 3	UCSC(resource-mgr) /domain-group #**scope fc-uplink**	Enters fabric configuration command mode.
Step 4	UCSC(resource-mgr) /domain-group/fc-uplink #**scope fabric** *{a | b}*.	Enters the configuration mode for the chosen fabric interconnect .
Step 5	UCSC(resource-mgr) /domain-group/fc-uplink/fabric # **enter vsan** *vsan-name vsan-id fcoe-id*	Enters the VSAN configuration command mode for the specified VSAN.
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:

	Command or Action	Purpose
Step 7	UCSC(resource-mgr) /domain-group/fc-uplink/fabric/vsan #**commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to set the Fibre Channel zoning state on VSAN VSAN1A on 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/fabric # enter vsan VSAN1A 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 #
```



CHAPTER 26

vHBA Management

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	(Optional) UCSC(policy-mgr) /org/vhba-templ # **set descr** *description*	Provides a description for the vHBA template.
Step 5	(Optional) UCSC(policy-mgr) /org/vhba-templ # **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 2, then you have the option to specify it with this command.
Step 6	(Optional) UCSC(policy-mgr) /org/vhba-templ # **set fc-if** *vsan-name*	Specifies the Fibre Channel interface (named VSAN) to use for the vHBA template. If you did not specify the Fibre Channel interface

	Command or Action	Purpose
		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.

Example

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.

Example

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**— 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, 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.

Example

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 #
```

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 Placements.

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:

Note You can specify the PCI order for the vHBA; however, the desired order works within a class of devices, such as vNICs or vHBAs and not across them. Within an adapter, vNICs are always placed ahead of the vHBAs.

- —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.
- —Cisco usNICs cannot be assigned to the vCon. The vCon can be used for all other configured vNICs and vHBAs, whether they are explicitly assigned to it, unassigned, or dynamic.

Note An SRIOV usNIC that is explicitly assigned to a vCon set to will remain assigned to that vCon.

If you do not include a vNIC/vHBA placement policy in the service profile, 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.

	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 vcon-policy** *policy-name*	Creates the specified vNIC/vHBA placement profile and enters organization vcon policy mode.
Step 4	(Optional) UCSC(policy-mgr) /org/vcon-policy # **set descr** *description*	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	(Optional) UCSC(policy-mgr) /org/vcon-policy # **set mapping-scheme** {**round-robin** | **linear-ordered**}	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: • **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

	Command or Action	Purpose
		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

	Command or Action	Purpose
		and vHBAs that are explicitly assigned to it.
Step 7	UCSC(policy-mgr) /org/vcon-policy # **commit-buffer**	Commits the transaction.

Example

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

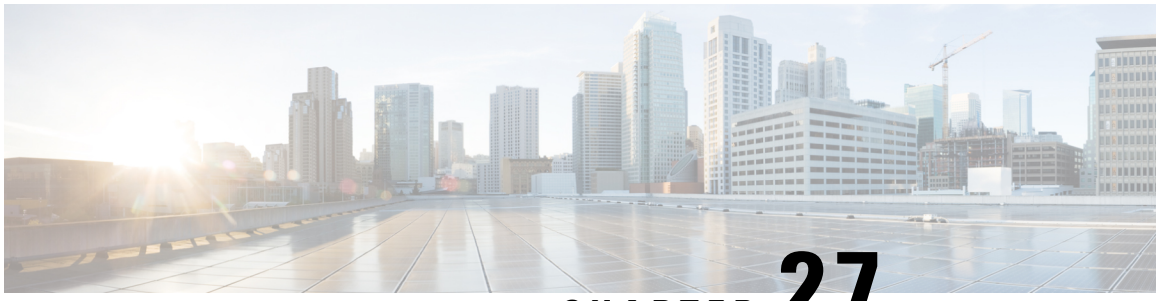
Procedure

	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.

Example

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 27

Storage Pools

This chapter includes the following sections:

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:00:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF:FF. All other WWN ranges are reserved. When fibre channel traffic is sent through the Cisco UCS infrastructure, the source WWPN is converted to a MAC address. You cannot use WWPN pool which can translate to a source multicast MAC address. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, Cisco recommends using 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:00:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:00:FF:FF:FF:FF:FF. All other WWN ranges are reserved. When fibre channel traffic is sent through the Cisco UCS infrastructure, the source WWPN is converted to a MAC address. You cannot use WWPN pool which can translate to a source multicast MAC address. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, Cisco recommends using 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	(Optional) UCSC(policy-mgr) /org/wwn-pool # **set descr** *description*	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	(Optional) UCSC(policy-mgr) /org/wwn-pool # **set descr** *description*	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/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.

Example

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/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 template.
- Include the WWxN pool in a service profile and template.

Deleting a WWN Pool

If you delete a pool, does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. 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

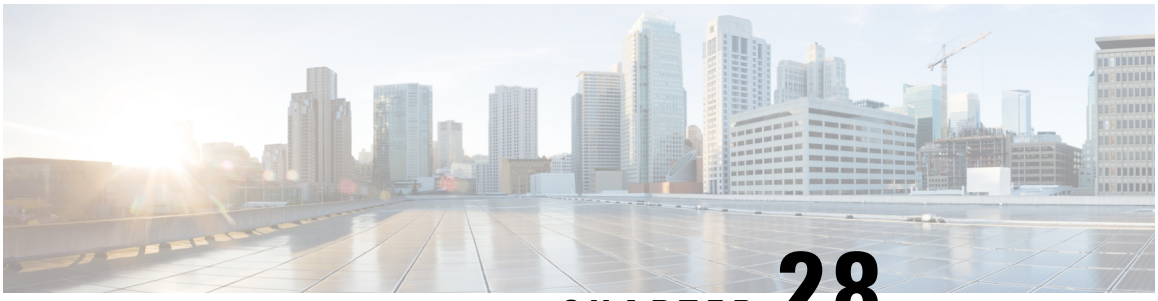
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.

	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 wwn-pool** *wwn-pool-name*	Deletes the specified WWN 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.

Example

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 #
```



CHAPTER 28

Storage Policies

This chapter includes the following sections:

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 a cluster configuration with two fabric interconnects

Note For Fibre Channel adapter policies, the values displayed by 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 :

- Max LUNs Per Target—SANsurfer has a maximum of 256 LUNs and does not display more than that number. supports a higher maximum number of LUNs.
- Link Down Timeout—In SANsurfer, you configure the timeout threshold for link down in seconds. In , you configure this value in milliseconds. Therefore, a value of 5500 ms in displays as 5s in SANsurfer.
- Max Data Field Size—SANsurfer has allowed values of 512, 1024, and 2048. allows you to set values of any size. Therefore, a value of 900 in displays as 512 in SANsurfer.
- LUN Queue Depth—The LUN queue depth setting is available for Windows system FC adapter policies. Queue depth is the number of commands that the HBA can send and receive in a single transmission per LUN. Windows Storport driver sets this to a default value of 20 for physical miniports and to 250 for virtual miniports. This setting adjusts the initial queue depth for all LUNs on the adapter. Valid range for this value is 1 to 254. The default LUN queue depth is 20.
- IO TimeOut Retry—When the target device is not responding to an IO request within the specified timeout, the FC adapter will abort the pending command then resend the same IO after the timer expires. The FC adapter valid range for this value is 0 to 59000 milliseconds. The default IO retry timeout is 5 seconds.

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	(Optional) UCSC(policy-mgr) /org/fc-policy # **set descr** *description*	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	(Optional) 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*}	Configures the Fibre Channel error recovery.
Step 6	(Optional) UCSC(policy-mgr) /org/fc-policy # **set interrupt mode** {**intx** | **msi** | **msi-x**}}	Configures the driver interrupt mode.
Step 7	(Optional) UCSC(policy-mgr) /org/fc-policy # **set port** {**io-throttle-count** *throttle-count* | **max-luns** *max-num*}	Configures the Fibre Channel port.
Step 8	(Optional) UCSC(policy-mgr) /org/fc-policy # **set port-f-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	Configures the Fibre Channel port fabric login (FLOGI).
Step 9	(Optional) UCSC(policy-mgr) /org/fc-policy # **set port-p-logi** {**retries** *retry-count* | **timeout** *timeout-msec*}	Configures the Fibre Channel port-to-port login (PLOGI).
Step 10	(Optional) UCSC(policy-mgr) /org/fc-policy # **set recv-queue** {**count** *count* | **ring-size** *size-num*}	Configures the Fibre Channel receive queue.

	Command or Action	Purpose
Step 11	(Optional) UCSC(policy-mgr) /org/fc-policy # **set scsi-io** {**count** *count* | **ring-size** *size-num*}	Configures the Fibre Channel SCSI I/O.
Step 12	(Optional) UCSC(policy-mgr) /org/fc-policy # **set trans-queue ring-size** *size-num*}	Configures the Fibre Channel transmit queue.
Step 13	UCSC(policy-mgr) /org/fc-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

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.

Example

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 #
```

About the 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.

	Command or Action	Purpose
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*.
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	(Optional) UCSC(policy-mgr) /org/san-connectivity-policy # **set descr** *policy-name*	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.

Example

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 583, 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

	Command or Action	Purpose
		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. 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.

Example

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 583, 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 cannot change this name after the object has been saved.

	Command or Action	Purpose
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. **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 with the target endpoint.
Step 10	UCSC(policy-mgr) /org/san-connectivity-policy/initiator-group # **commit-buffer**	Commits the transaction to the system configuration.

Example

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.
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.

Example

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.

Example

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 #
```

Storage Connection Policy

The storage connection policy contains a collection of target storage ports on storage array that you use to configure fibre channel zoning.

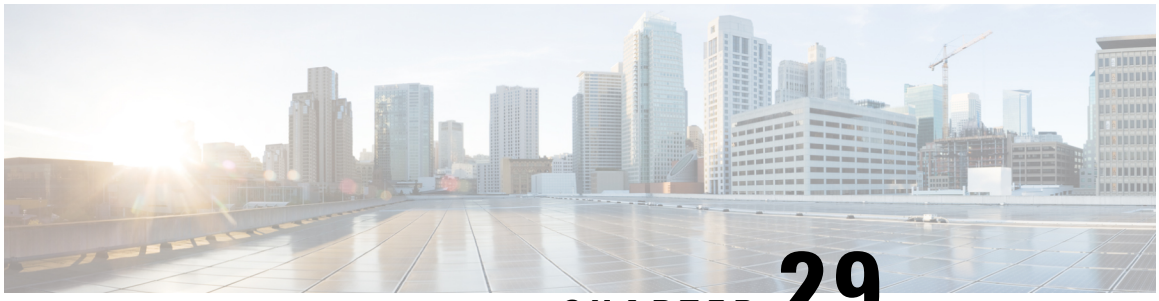
From Cisco UCS Central you can create a storage connection policy in an organization.

Creating a Storage Connection 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 storage-connection-policy** *profile-name*	Creates the specified storage connection policy and enters organization storage connection policy mode.
Step 4	UCSC(policy-mgr) /org/storage-connection-policy # **set zoning type** {**none** | **simt** | **sist**}	Select the zoning type. This can be one of the following: • None—FC zoning is not configured. • Single Initiator Multiple Targets—The system automatically creates one zone for each vHBA. We recommend that you configure this type of zoning if you expect the number of zones to reach or exceed the maximum supported. • Single Initiator Single Target—The system automatically creates one zone for each vHBA and storage port pair. Each zone has two members. We recommend that you configure this type of zoning unless you expect the number of zones to exceed the maximum supported. This is the default.
Step 5	UCSC(policy-mgr) /org/storage-connection-policy # **create storage-target** *WWPN_ID*	Creates a target on the selected WWPN.
Step 6	UCSC(policy-mgr) /org/storage-connection-policy/storage-target # **set target-path** {**a** | **b**}	Sets the target fabric interconnect. By default, fabric interconnect A is used for communications with the target endpoint.
Step 7	UCSC(policy-mgr) /org/storage-connection-policy/storage-target # **set target-vsan** *VSAN_name*	Select the VSAN associated with the FI Port and the target endpoint.
Step 8	UCSC(policy-mgr) /org/storage-connection-policy # **commit-buffer**	Commits the transaction to the system configuration.



CHAPTER 29

SED Management

Security Policies for Self Encrypting Drives

Self-Encrypting Drives (SEDs) have special hardware that encrypts incoming data and decrypts outgoing data in real-time. The data on the disk is always encrypted in the disk and stored in the encrypted form. The encrypted data is always decrypted on the way out of the disk. A media encryption key controls this encryption and decryption. This key is never stored in the processor or memory. Cisco UCS Manager supports SEDs on Cisco UCS C-Series and S-Series servers.

SEDs are locked using a security key. The security key, which is also known as Key-Encryption Key or an authentication passphrase, is used to encrypt the media encryption key. If the disk is not locked, no key is required to fetch the data.

Cisco UCS Central enables you to configure security keys locally or remotely. When you configure the key locally, you must remember the key. In case you forget the key, it cannot be retrieved and the data is lost. You can configure the key remotely by using a key management server (also known as KMIP server). This method addresses the issues related to safe-keeping and retrieval of the keys in the local management.

The encryption and decryption for SEDs is done through the hardware. Thus, it does not affect the overall system performance. SEDs reduce the disk retirement and redeployment costs through instantaneous cryptographic erasure. Cryptographic erasure will render all data on the SED unreadable when the encryption key is destroyed.

Security Guidelines and Limitations for SED Management

The following security guidelines and limitations apply to SED management from Cisco UCS Central:

- Storage operations get applied only when the server is powered on, and they do not trigger a server reboot.
- A global service profile (GSP) with a security policy gets pushed to Cisco UCS Manager releases prior to 3.1(3), and the security policies related operations are cleaned up and an unsecured LUN is created.
- A Cisco UCS Manager downgrade fails if a storage controller with **Drive Security Enable** is present in the domain.
- A GSP association fails with a `config-failure` status/message if it is associated with an unsupported server, or a supported server with unsupported firmware.
- A GSP association fails with a `config-failure` status/message if LUN security is set to **Enabled** in the Disk Configuration Policy but if the Security policy is not created in the storage profile.
- A GSP association fails if the Security policy is deleted from the storage profile after the Storage Controller is set to **Drive Security Enable**.

Security Flags for Controller and Disk

Security flags indicate the current security status of the storage controller and disks.

The storage controller and disks have the following security flags:

- **Security Capable**—Indicates that the controller, LUN, or disk is capable of supporting SED management.
- **Security Enable**—Indicates that the security key is programmed on the controller, disk, or LUN, and security is enabled on the device. This flag is set when you configure a security policy and associate it to a server, making the controller and disk secure. This flag is not set on a Cisco HyperFlex device.
- **Secured**—Indicates that the security key is programmed on the disk, and security is enabled on the Cisco HyperFlex device.

The following security flags are exclusive to storage disks:

- **Locked**—Indicates that the disk key does not match the key on the controller. This happens when you move disks across servers that are programmed with different keys. The data on a locked disk is inaccessible and the operating system cannot use the disk. To use this disk, you must either unlock the disk or secure erase the foreign configuration.
- **Foreign Secured**—Indicates that a secure disk is in foreign configuration. This happens when you unlock a locked disk with the right key, but the disk is in a foreign configuration state and the data on it is encrypted. To use this disk, you can either import or clear the foreign configuration.

Security Related Operations

You can create security policies for Self-Encrypting Drives (SEDs) through a Storage Profile in Cisco UCS Central. In addition to creating security policies, you can perform additional operations on the supported servers. The following table lists the remote operations and their descriptions:

Component	Remote Action	Action
Controller	Unlock Disk	Unlocks ForeignSecured and Locked Disks encrypted using a Local Policy.
	Modify Remote Key	Modifies the Key in the KMIP Server and fetches the new Key for Encryption.
	Disable Security	Disables Security on the Controller when no Secured Disks are present on Controller.
	Unlock for Remote	Unlocks ForeignSecured and Locked Disks encrypted using a Remote Policy.
Virtual Disk	Secure Virtual Drive	Secures LUNs comprised only of SEDs when the Controller is Security Enabled.
Physical Disk	Enable Encryption	Used to Secure JBOD Self-Encrypting Drive(SED) when Controller is Security Enabled.
	Secure Erase	Erases disk cryptographically to make it Unsecured and Reusable.
	Secure Erase Foreign Configuration	Erases ForeignSecured and Locked disks cryptographically to make them Unsecured and Unconfigured Good

For more information about SED Management and security policies, see *Cisco UCS Manager Storage Management Guide*.

Enabling Security on a Disk

You can configure the drive security settings for the Self Encrypting Disks using the Storage profile settings.

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 storage-profile** *profile-name*	Creates the specified storage profile and enters organization storage profile mode.
Step 4	UCSC(policy-mgr) /org/storage-profile* # **create security**	Creates a security policy for the specified storage profile and enters the security policy mode.

	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **create drive-security**	Creates a drive security policy for the specified storage profile security and enters the drive security policy mode.
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security* # **create local**	Creates a local security policy for the specified storage profile and enters the local policy mode.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **set security-key***security-key*	Sets the specified security key for the local policy. The security key must have 32 characters.
Step 8	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **commit buffer**	Commits the transaction to the system configuration.

Creating a Local Security 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 storage-profile** *profile-name*	Creates the specified storage profile and enters organization storage profile mode.
Step 4	UCSC(policy-mgr) /org/storage-profile* # **create security**	Creates a security policy for the specified storage profile and enters the security policy mode.
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **create drive-security**	Creates a drive security policy for the specified storage profile security and enters the drive security policy mode.
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security* # **create local**	Creates a local security policy for the specified storage profile and enters the local policy mode.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **set security-key***security-key*	Sets the specified security key for the local policy. The security key must have 32 characters.
Step 8		

	Command or Action	Purpose
Step 9	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local* # **commit buffer**	Commits the transaction to the system configuration.

Example

```
UCSC # connect policy mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr)# create storage-profile stp-demo

UCSC(policy-mgr)/org/storage-profile* # create security
UCSC(policy-mgr)/org/storage-profile/security* # create drive-security
UCSC(policy-mgr)/org/storage-profile/security/drive-security* # create local
UCSC(policy-mgr)/org/storage-profile/security/drive-security/local* # set security-key
thereare32charactersinthisseckey
UCSC(policy-mgr)/org/storage-profile/security/drive-security/local* # commit-buffer
```

Modifying the Security Policy from Local to Remote

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 storage-profile** *profile-name*	Enters the specified storage profile configuration mode for the specified storage profile.
Step 4	UCSC(policy-mgr) /org/storage-profile # **scope security**	Enters the security policy mode for the specified storage profile.
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **scope drive-security**	Enters the drive security policy mode for the specified storage profile security.
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security # **create remote**	Creates and enters the remote policy mode.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set deployed-security-key***existing-security-key*	Specifies the existing key deployed on the server.
Step 8	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set primary-server***primary-server-name*	Sets the primary server hostname or IP address.

	Command or Action	Purpose
Step 9	(Optional) UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set secondary-server***secondary-server-name*	(Optional) Sets the secondary server hostname or IP address.
Step 10	(Optional) UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set port***kmip-server-port-number*	Sets the port number of the KMIP server. KMIP server port numbers can range from 1024 to 65535.
Step 11	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set server-certificate**	Sets the KMIP certificate to the remote security policy.
Step 12	(Optional) UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **set timeout** *timeout*	Sets the number of seconds in which communication between the storage and the KMIP server times out. Timeout can range from 5 seconds to 20 seconds.
Step 13	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **commit-buffer**	Commits the transaction to the system configuration.
Step 14	UCSC(policy-mgr) /org/storage-profile/security/drive-security/remote*# **exit**	Enters the drive security policy mode.

Modifying the Security Key of a Local Security 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 storage-profile** *profile-name*	Enters the specified storage profile configuration mode for the specified storage profile.
Step 4	UCSC(policy-mgr) /org/storage-profile # **scope security**	Enters the security policy mode for the specified storage profile.
Step 5	UCSC(policy-mgr) /org/storage-profile/security* # **scope drive-security**	Enters the drive security policy mode for the specified storage profile security.

	Command or Action	Purpose
Step 6	UCSC(policy-mgr) /org/storage-profile/security/drive-security # **scope local**	Enters the local policy mode for the the specified storage profile.
Step 7	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local*# **set deployed-security-key***existing-security-key*	Specifies the existing key deployed on the server to configure a new key.
Step 8	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local*# **set security-key***new-security-key*	Sets the new security key for the local policy.
Step 9	UCSC(policy-mgr) /org/storage-profile/security/drive-security/local*# **commit-buffer**	Commits the transaction to the system configuration.

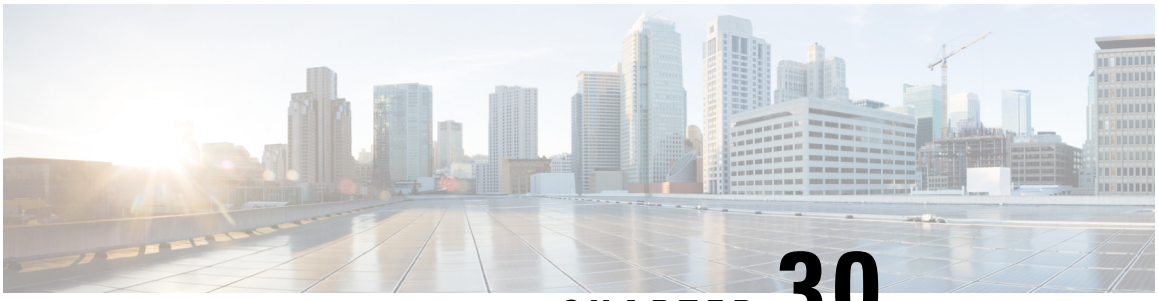
Remote Operations

This section describes the options for configuring security related operations on the controller, local disk, or virtual disk. For more information on the permitted operations, see Security Related Operations, on page 594.

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr)/domain-mgmt# **scope ucs-domain** *name*	Enters the specified UCS domain.
Step 3	UCSC(resource-mgr)/domain-mgmt/ucs-domain# **scope chassis** *name*	Enters the specific chassis.
Step 4	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis# **scope server** *name*	Enters the specific server.
Step 5	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server# **scope raid-controller** *raid-controller-id*	Enters the RAID controller mode.
Step 6	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server# **set admin-state** name	Set an admin state for the RAID controller. See Security Related Operations, on page 594 for a list of the permitted security operations.
Step 7	(Controller) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/ raid-controller # **set admin-state** unlock-disk*name*	Unlock Disk for a Local Security Policy requires a Key as a parameter. The Key must be 32 characters long.
Step 8	UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/ raid-controller # **commit buffer**	Commits the transaction to the system configuration.

	Command or Action	Purpose
Step 9	(Controller) (Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller # **set admin-state** unlock-disk	Unlock Disk for a Remote Security Policy does not require a Key as a parameter.
Step 10	(Local-Disk)(Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller/local-disk # **set admin-state** enable-security	Set security for the local disk.
Step 11	(Local-Disk)(Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller/local-disk # **set admin-state** clear *name* • secure-drive - Equivalent to Secure Erase in the Cisco UCS Central GUI. • secure-foreign-config-drive - Equivalent to Secure Erase Foreign Configuration in the Cisco UCS Central GUI.	These choices are available for a local disk:
Step 12	(Virtual-Disk)(Optional) UCSC(resource-mgr)/domain-mgmt/ucs-domain/chassis/server/raid-controller/virtual-drive # **set admin-state** secure-drive-group	



CHAPTER 30

Chassis Profiles and Templates

About Cisco UCS Storage Servers

A Cisco UCS storage server is a dense storage rack server with dual server nodes, optimized for large datasets used in environments such as big data, cloud, object storage, and content deliver.

A Cisco UCS storage server is designed to operate in a standalone environment and as part of the Cisco Unified Computing System with Cisco UCS Manager integration. The following features are available:

- System IO Controllers (SIOC).
- Support of up to two server modules
- Capability to operate in a standalone mode.
- Chassis level functionality in the standalone mode—Shared components such as storage adapters, fans and power supply units are configured at the chassis level.
- Data Center Ethernet connectivity to a server host through a shared dual virtual interface card (VIC).
- Individual hard disk drives (HDD) can be assigned to either server in the dedicated or shared mode.

  In addition, one of the server slots in the Cisco UCS storage server can be utilized by a storage expansion module for an additional four 3.5" drivers. The server modules can also accommodate two solid state drives (SDD) for internal storage dedicated to that module. The chassis supports Serial Attached SCSI (SAS) expanders that can be configured to assign the 3.5" drives to individual server modules.

  For more information, see the Cisco UCS S3260 Storage Server Installation and Service Guide.

Chassis Profiles

A chassis profile defines the storage, firmware and maintenance characteristics of a chassis. When a chassis profile is associated to a chassis, Cisco UCS Central automatically configures the chassis to match the configuration in the chassis profile.

A chassis profile includes four types of information:

- **Chassis definitions**—Defines the specific chassis to which the profile is assigned.
- **Maintenance policy**—Includes the maintenance policy to be applied to the profile.
- **Firmware specification**—Defines the chassis firmware package that can be applied to a chassis through this profile.
- **Disk zoning policy**—Includes the zoning policy to be applied to the storage disks.

Guidelines and Recommendations for Chassis Profiles

In addition to any guidelines or recommendations that are specific to the policies included in chassis profiles and chassis profile templates, such as the disk zoning policy, adherence to the following guidelines that impact the ability to associate a chassis profile with a chassis are recommended:

- Each chassis can be associated with only one chassis profile. Similarly, each chassis profile can be associated with only one chassis at a time.
- Chassis profiles are currently supported.
- C bundles earlier than Cisco UCS Manager Release 3.1(2) are not supported on the Cisco UCS S3260 Storage Server.

Creating a Chassis Profile

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **create chassis-profile** *profile-name* **instance**	Creates the specified chassis profile instance and enters organization chassis profile mode. Enter a unique *profile-name* to identify this chassis profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you

	Command or Action	Purpose
		cannot change this name after the object is saved.
Step 3	(Optional) UCSC(resource-mgr) /org/chassis-profile* # **set descr** *description*	Provides a description for the chassis 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 4	(Optional) UCSC(resource-mgr) /org/chassis-profile* # **set chassis-fw-policy-name** *chassis-firmware-policy-name*	Associates the specified chassis firmware policy with the chassis profile.
Step 5	(Optional) UCSC(resource-mgr) /org/chassis-profile* # **set chassis-profile-maint-policy** *policy-name*	Associates the specified chassis maintenance policy with the chassis profile.
Step 6	(Optional) UCSC(resource-mgr) /org/chassis-profile* # **set user-label** *label-name*	Specifies the user label associated with the chassis profile.
Step 7	(Optional) UCSC(resource-mgr) /org/chassis-profile* # **set src-templ-name** *source-chassis-profile-template-name*	Binds the specified chassis profile template with the chassis profile.
Step 8	(Optional) UCSC(resource-mgr) /org/chassis-profile* # **set disk-zoning-policy** *disk-zoning-policy-name*	Associates the specified disk zoning policy with the chassis profile.
Step 9	UCSC(resource-mgr) /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a chassis profile instance and commit the transaction:

```
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # create chassis-profile- ChassisProfile1 instance
UCSC(resource-mgr) /org/chassis-profile* # set  descr "This is a chassis profile example."
UCSC(resource-mgr) /org/chassis-profile* # set chassis-profile-maint-policy chassismaintpol4
UCSC(resource-mgr) /org/chassis-profile* # set user-label mycplabel
UCSC(resource-mgr) /org/chassis-profile* # set chassis-fw-policy-name cfp1
UCSC(resource-mgr) /org/chassis-profile* # set src-templ-name chassispt1
UCSC(resource-mgr) /org/chassis-profile* # set disk-zoning-policy dzp1
UCSC(resource-mgr) /org/chassis-profile* # commit-buffer
UCSC(resource-mgr) /org/chassis-profile #
```

What to do next

Associate the chassis profile with a S3260 chassis.

Renaming a Chassis Profile

When you rename a chassis profile, the following occurs:

- Event logs and audit logs that reference the previous name for the chassis profile are retained under that name.
- A new audit record is created to log the rename operation.
- All records of faults against the chassis profile under its previous name are transferred to the new chassis profile name.

Note You cannot rename a chassis profile with pending changes.

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **scope chassis-profile** *profile-name*	Enters organization chassis profile mode for the specified chassis profile.
Step 3	UCSC(resource-mgr) /org/chassis-profile # **rename-to** *new-profile-name*	Renames the specified chassis profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved. When you enter this command, you are warned that this is a standalone operation and that you may lose all uncommitted changes in this CLI session. Type **yes** to confirm that you want to continue.

Example

This example shows how to change the name of a chassis profile from CP5 to CP10 and commits the transaction:

```
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org # scope chassis-profile CP5
```

```
UCSC(resource-mgr) /org/chassis-profile # rename-to CP10
Rename is a standalone operation. You may lose any uncommitted changes in this CLI session.
Do you want to continue? (yes/no): yes
The managed object in the current mode no longer exists. Changing to mode: /org
UCSC(resource-mgr) /org #
```

Deleting a Chassis Profile

This procedure explains how to delete a chassis profile.

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **delete chassis-profile** *profile-name*	Deletes the specified chassis profile.
Step 3	UCSC(resource-mgr) /org* # **commit-buffer**	Commits the transaction to the system configuration.

Example

This example shows how to delete a chassis profile ChasInst90 and commit the transaction:

```
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org delete chassis-profile ChasInst90
UCSC(resource-mgr) /org* # commit-buffer
UCSC(resource-mgr) /org #
```

Associating a Chassis Profile with a Chassis

Follow this procedure if you did not associate the chassis profile with a chassis when you created it, or to change the chassis with which a chassis profile is associated.

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **scope chassis-profile** *profile-name*	Enters organization chassis profile mode for the specified chassis profile.

	Command or Action	Purpose
Step 3	UCSC(resource-mgr) /org/chassis-profile # **associate chassis** *chassis-id* ucs-domain domain-number [restrictmigration]	Associates the chassis profile with a single chassis. Adding the optional **restrictmigration** keyword prevents the chassis profile from being migrated to another chassis.
Step 4	UCSC(resource-mgr) /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example associates the chassis profile named ChassisProf1 with chassis 1, and commits the transaction:

```
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # scope chassis-profile ChassisProf1
UCSC(resource-mgr) /org/chassis-profile # associate chassis 1 ucs-domain 1003
UCSC(resource-mgr) /org/chassis-profile* # commit-buffer
UCSC(resource-mgr) /org/chassis-profile #
```

Disassociating a Chassis Profile from a Chassis

This procedure covers disassociating a chassis profile from a chassis.

Note When a chassis is disassociated from a chassis profile, effects of disk zoning policy will be still be persistent in the chassis.

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **scope chassis-profile** *profile-name*	Enters organization chassis profile mode for the specified chassis profile.
Step 3	UCSC(resource-mgr) /org/chassis-profile # **disassociate**	Disassociates the chassis profile from the chassis.
Step 4	UCSC(resource-mgr) /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example disassociates the chassis profile named ChassisProf1 from the chassis to which it was associated and commits the transaction:

```
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # scope chassis-profile ChassisProf1
UCSC(resource-mgr) /org/chassis-profile # disassociate
UCSC(resource-mgr) /org/chassis-profile* # commit-buffer
UCSC(resource-mgr) /org/chassis-profile #
```

Creating a Chassis Profile Template

Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr)# **scope org** *org-name*	Enters the organization mode for the specified organization. To enter the root organization mode, enter / as the *org-name*.
Step 2	UCSC(resource-mgr) /org # **create chassis-profile** *profile-name* {**initial-template** | **updating-template**}	Creates the specified chassis profile template and enters organization chassis profile mode. Enter a unique *profile-name* to identify this chassis profile template. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved. Chassis profile template types are: • **initial-template**—Instances will not automatically update if this template is updated. • **updating-template**—Instances will automatically update if this template is updated.
Step 3	(Optional) UCSC(resource-mgr) /org/chassis-profile* # **set descr** *description*	Provides a description for the chassis profile template.

	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 4	UCSC(resource-mgr) /org/chassis-profile* # **set chassis-fw-policy-name** *chassis-firmware-policy-name*	Associates the specified chassis firmware policy with the chassis profile template.
Step 5	UCSC(resource-mgr) /org/chassis-profile* # **set chassis-profile-maint-policy** *policy-name*	Associates the specified chassis maintenance policy with the chassis profile template.
Step 6	UCSC(resource-mgr) /org/chassis-profile* # **set user-label** *label-name*	Specifies the user label associated with the chassis profile template.
Step 7	UCSC(resource-mgr) /org/chassis-profile* # **set src-templ-name** *source-chassis-profile-template-name*	Binds the specified chassis profile template with the chassis profile.
Step 8	UCSC(resource-mgr) /org/chassis-profile* # **set disk-zoning-policy** *disk-zoning-policy-name*	Associates the specified disk zoning policy with the chassis profile template.
Step 9	UCSC(resource-mgr) /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a chassis profile template and commit the transaction:

```
UCSC(resource-mgr)# scope org /
UCSC(resource-mgr) /org* # create chassis-profile ChassisProTemp1 updating-template
UCSC(resource-mgr) /org/chassis-profile* # set  descr "This is a chassis profile template
example."
UCSC(resource-mgr) /org/chassis-profile* # set chassis-profile-maint-policy chassismaintpol2
UCSC(resource-mgr) /org/chassis-profile* # set user-label mycptlabel
UCSC(resource-mgr) /org/chassis-profile* # set chassis-fw-policy-name cptf1
UCSC(resource-mgr) /org/chassis-profile* # set src-templ-name chassispt1
UCSC(resource-mgr) /org/chassis-profile* # set disk-zoning-policy dzp1
UCSC(resource-mgr) /org/chassis-profile* # commit-buffer
UCSC(resource-mgr) /org/chassis-profile #
```

What to do next

Create a chassis profile instance from the chassis profile template.

Creating a Chassis Profile Instance from a Chassis Profile Template

Before you begin

Verify that there is a chassis profile template from which to create a chassis profile instance.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name* .
Step 2	UCSC /org # **create chassis-profile** *profile-name* **instance**	Creates the specified chassis profile instance and enters organization chassis profile mode. Enter a unique *profile-name* to identify this chassis profile. This name can be between 1 and 16 alphanumeric characters. You cannot use spaces or any special characters other than - (hyphen), _ (underscore), : (colon), and . (period), and you cannot change this name after the object is saved.
Step 3	UCSC /org/chassis-profile* # **set src-templ-name** *profile-name*	Specifies the source chassis profile template to apply to the chassis profile instance. All configuration settings from the chassis profile template will be applied to the chassis profile instance.
Step 4	UCSC /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a chassis profile instance named ChassisProf02, applies the chassis profile template named ChassisProfTemp2, and commits the transaction:

```
UCSC# scope org /
UCSC /org* # create chassis-profile ChassisProf02 instance
UCSC /org/chassis-profile* # set src-templ-name ChassisProfTemp2
UCSC /org/chassis-profile* # commit-buffer
UCSC /org/chassis-profile #
```

What to do next

Associate the chassis profile to a chassis.

Binding a Chassis Profile to a Chassis Profile Template

You can bind a chassis profile to a chassis profile template. When you bind the chassis profile to a template, Cisco UCS Central configures the chassis profile with the values defined in the chassis profile template. If the existing chassis profile configuration does not match the template, Cisco UCS Central reconfigures the chassis profile. You can only change the configuration of a bound chassis profile through the associated template.

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **scope chassis-profile** *profile-name*	Enters organization chassis profile mode for the specified chassis profile.
Step 3	UCSC(resource-mgr) /org/chassis-profile # **set src-templ-name** *chassis-profile-template-name*	Binds the chassis profile to the specified chassis profile template.
Step 4	UCSC(resource-mgr) /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example binds the chassis profile named ChassisProf1 to ChassisProfileTemplate1 and commits the transaction:

```
UCSC(resource-mgr)# scope org
UCSC(resource-mgr) /org # scope chassis-profile ChassisProf1
UCSC(resource-mgr) /org/chassis-profile # set src-templ-name ChassisProfileTemplate1
UCSC(resource-mgr) /org/chassis-profile* # commit-buffer
UCSC(resource-mgr) /org/chassis-profile #
```

Unbinding a Chassis Profile from a Chassis Profile Template

To unbind a chassis profile from a chassis profile template, bind the chassis profile to an empty value (quotes without space).

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **scope chassis-profile** *profile-name*	Enters organization chassis profile mode for the specified chassis profile.
Step 3	UCSC(resource-mgr) /org/chassis-profile # **set src-templ-name ""**	Unbinds the chassis profile from the chassis profile template.
Step 4	UCSC(resource-mgr) /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example unbinds the chassis profile named ChassisProf1 and commits the transaction:

```
UCSC(resource-mgr)# scope org
UCSC(resource-mgr) /org # scope chassis-profile ChassisProf1
UCSC(resource-mgr) /org/chassis-profile # set src-templ-name ""
UCSC(resource-mgr) /org/chassis-profile* # commit-buffer
UCSC(resource-mgr) /org/chassis-profile #
```

Assigning a Policy to a Chassis Profile

Cisco UCS Central lets you assign a policy to a chassis profile.

Procedure

	Command or Action	Purpose
Step 1	UCSC(resource-mgr) # **scope org**	Enters the organization root.
Step 2	UCSC(resource-mgr) /system # **create chassis-profile** *chassis-profile-name*	Creates a chassis profile using a unique name.
Step 3	UCSC(resource-mgr) /org/chassis-profile* # **commit buffer**	Commits the transaction to the system configuration.
Step 4	UCSC(resource-mgr) /org/chassis-profile* # **set chassis-fw-policy** *policy-name*	Sets the policy name to the chassis.
Step 5	UCSC(resource-mgr) /org/chassis-profile* # **commit buffer**	Commits the transaction to the system.
Step 6	UCSC(resource-mgr) /org/chassis-profile* # **show detail**	Displays the details of the assigning process.

Example

The following example shows how Cisco UCS Central assigns a policy to a chassis profile:

```
UCSC(resource-mgr)# scope org
UCSC(resource-mgr) /org # create chassis-profile CP3
UCSC(resource-mgr) /org/chassis-profile* # com
UCSC(resource-mgr) /org/chassis-profile # set
  chassis-fw-policy-name        Chassis Firmware Policy
  chassis-profile-maint-policy  Maintenance Policy
  compute-conn-policy           Compute Conn Policy
  descr                         Description
  disk-zoning-policy            Disk Zoning Policy
  src-templ-name                Source Template
  user-label                    User Label

UCSC(resource-mgr) /org/chassis-profile # set cha
chassis-fw-policy-name        chassis-profile-maint-policy
UCSC(resource-mgr) /org/chassis-profile # set chassis-fw-policy-name A1
UCSC(resource-mgr) /org/chassis-profile* # com
UCSC(resource-mgr) /org/chassis-profile # show detail

Chassis Profile:
    Chassis Profile Name: CP3
    Type: Instance
    Chassis Dn:
    Chassis Config Issues: N/A
    Storage Config Issues: N/A
    User Label:
    Description:
    Assign State: Unassigned
    Assoc State: Unassociated
    Chassis Firmware Policy: A1
    Oper Chassis Fw Policy Name: org-root/fw-chassis-pack-global-default
    Disk Zoning Policy: global-default
    Oper Disk Zoning Policy: org-root/disk-zoning-policy-global-default
    Resolve Remote: Yes
    Source Template:
    Oper Src Templ Name:
    Maintenance Policy: global-default
    Oper Maint Policy Name: org-root/chassis-profile-maint-global-default
    Compute Conn Policy: global-default
    Equipment Oper Compute Conn Policy: org-root/compute-conn-policy-global-default
    Current Task: Throttle
wait(FSM-STAGE:sam:dme:EquipmentChassisProfileConfigure:ThrottleWait)
```

Creating a Chassis Profile Maintenance Policy

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(policy-mgr) /org # **create chassis-profile-maint-policy** *policy-name*	Creates the specified maintenance policy and enters maintenance policy mode.
Step 3	UCSC(policy-mgr) /org/chassis-profile-maint-policy* # **set reboot-policy user-ack**	When a policy is associated with a chassis, the chassis needs to be re-acknowledged to complete the association. The user must explicitly acknowledge the changes by using the **apply pending-changes** command before changes are applied.
Step 4	(Optional) UCSC(policy-mgr) /org/chassis-profile-maint-policy* # **set descr** *description*	A description of the policy. Cisco recommends including information about where and when to use the policy.
Step 5	UCSC(policy-mgr) /org/maint-policy #* **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example creates a maintenance policy called maintenance, and commits the transaction:

```
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # create chassis-profile-maint-policy maintenance
UCSC(policy-mgr) /org/chassis-profile-maint-policy* # set reboot-policy user-ack
UCSC(policy-mgr) /org/chassis-profile-maint-policy* # commit-buffer
UCSC(policy-mgr) /org/maint-policy #
```

Configuring the Maintenance Policy for a Chassis Profile/Chassis Profile Template

Procedure

	Command or Action	Purpose
Step 1	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 2	UCSC(resource-mgr) /org # **scope chassis-profile** *profile-name*|*template-name*	Enters organization chassis profile/chassis profile template mode for the specified chassis profile//chassis profile template.
Step 3	UCSC(resource-mgr) /org/chassis-profile # **set chassis-profile-maint-policy** *maintenance-policy-name*	Associates the specified maintenance policy with the chassis profile//chassis profile template. Use an existing maintenance policy name or enter a new policy.

	Command or Action	Purpose
Step 4	UCSC(resource-mgr) /org/chassis-profile* # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to associate a maintenance policy with a chassis profile and commit the transaction:

```
UCSC(resource-mgr)# scope org
UCSC(resource-mgr) /org # scope chassis-profile ChassisProfile1
UCSC(resource-mgr) /org/chassis-profile # set chassis-profile-maint-policy default
UCSC(resource-mgr) /org/chassis-profile* # commit-buffer
UCSC(resource-mgr) /org/chassis-profile #
```

Disk Zoning Policies

Disk zoning policies allow you to manage the disk on your chassis servers when associated in a chassis profile. After a disk zoning policy has been created, you can view the disk zoning policy page to review what is included in the policy.

Depending on the storage controller, the disk types that are supported for your disk zoning policy may vary:

Storage Controller	Supported Disk Types
UCSC-C3X60-R1GB	Supports unassigned, dedicated, and chassis spare disks.
UCS-C3K-M4RAID	Supports unassigned, dedicated, and chassis spare disks on the UCSC-C3K-M4SRB server only.
UCS-C3X60-HBA	Supports shared disks for data storage operations only. LUNs cannot be created on the shared disks.

Creating a Disk Zoning Policy

Procedure

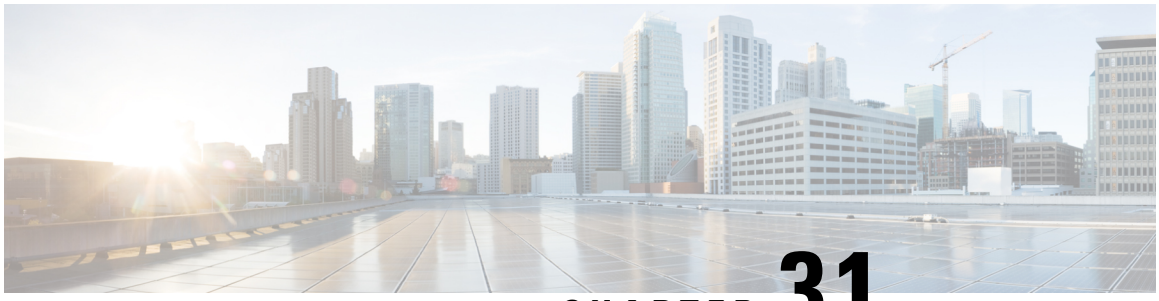
	Command or Action	Purpose
Step 1	UCSC# **connect policy-mgr**	Enters policy manager mode.
Step 2	UCSC(policy-mgr) # **scope org** *org-name*	Enters organization mode for the specified organization. To enter the root organization mode, type / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create disk-zoning-policy***diskzoning policy-name*	Creates a disk zoning policy name with the specified disk zoning policy name.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org/disk-zoning-policy* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create the dzp1 disk zoning policy:

```
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create disk-zoning-policy dzp1
UCSC(policy-mgr) /org/disk-zoning-policy*# commit-buffer
UCSC(policy-mgr) /org/disk-zoning-policy#
```



CHAPTER 31

Storage Profiles

This chapter includes the following sections:

Storage Profiles

To allow flexibility in defining the number of storage disks, roles and usage of these disks, and other storage parameters, you can create and use storage profiles. A storage profile encapsulates the storage requirements for one or more service profiles. LUNs configured in a storage profile can be used as boot LUNs or data LUNs, and can be dedicated to a specific server. You can also specify a local LUN as a boot device.

Note Storage profiles on Cisco UCS rack and blade servers are supported on Cisco UCS Manager release 2.2.7 and above, and Cisco UCS Manager release 3.1.1 and above.

Because Cisco UCS M-series Modular Servers have been deprecated, storage profiles with boot orders created in Cisco UCS Central release 1.4 are not supported in Cisco UCS Central release 1.5 and later.

Storage profiles allow you to do the following:

- Configure multiple virtual drives and select the physical drives that are used by a virtual drive.
- Configure the storage capacity of a virtual drive.
- Configure the number, type and role of disks in a disk group.
- Associate a storage profile with a service profile.

Note LUN resizing is not supported.

Virtual Drives

A disk group can be partitioned into virtual drives. Each virtual drive appears as an individual physical device to the Operating System.

All virtual drives in a disk group must be managed by using a single disk group policy.

Configuration States

Indicates the configuration states of a virtual drive. Virtual drives can have the following configuration states:

- Applying—Creation of the virtual drive is in progress.
- Applied—Creation of the virtual drive is complete, or virtual disk policy changes are configured and applied successfully.
- Failed to apply—Creation, deletion, or renaming of a virtual drive has failed due to errors in the underlying storage subsystem.
- Orphaned—The service profile that contained this virtual drive is deleted or the service profile is no longer associated with a storage profile.
- Not in use—The service profile that contained this virtual drive is in the disassociated state.

Deployment States

Indicates the actions that you are performing on virtual drives. Virtual drives can have the following deployment states:

- No action—No pending work items for the virtual drive.
- Creating—Creation of the virtual drive is in progress.
- Deleting—Deletion of the virtual drive is in progress.
- Modifying—Modification of the virtual drive is in progress.
- Apply-Failed—Creation or modification of the virtual drive has failed.

Operability States

Indicates the operating condition of a virtual drive. Virtual drives can have the following operability states:

- Optimal—The virtual drive operating condition is good. All configured drives are online.
- Degraded—The virtual drive operating condition is not optimal. One of the configured drives has failed or is offline.
- Cache-degraded—The virtual drive has been created with a write cache policy of Write Back Good BBU mode, but the BBU has failed, or there is no BBU.

Note This state does not occur if you select Always Write Back mode.

- Partially degraded—The operating condition in a RAID 6 virtual drive is not optimal. One of the configured drives has failed or is offline. RAID 6 can tolerate up to two drive failures.

- Offline—The virtual drive is not available to the RAID controller. This is essentially a failed state.
- Unknown—The state of the virtual drive is not known.

Presence States

Indicates the presence of virtual drive components. Virtual drives have the following presence states:

- Equipped—The virtual drive is available.
- Mismatched—A virtual drive deployed state is different from its configured state.
- Missing—Virtual drive is missing.

Virtual Drive Naming

When you use Cisco UCS Central to create a virtual drive, Cisco UCS Central assigns a unique ID that can be used to reliably identify the virtual drive for further operations. Cisco UCS Central also provides the flexibility to provide a name to the virtual drive at the time of service profile association. Any virtual drive without a service profile or a server reference is marked as an orphan virtual drive.

In addition to a unique ID, a name is assigned to the drive. Names can be assigned in two ways:

- When configuring a virtual drive, you can explicitly assign a name that can be referenced in storage profiles.
- If you have not preprovisioned a name for the virtual drive, Cisco UCS Central generates a unique name for the virtual drive.

You can rename virtual drives that are not referenced by any service profile or server.

RAID Levels

The RAID level of a disk group describes how the data is organized on the disk group for the purpose of ensuring availability, redundancy of data, and I/O performance.

The following are features provided by RAID:

- Striping—Segmenting data across multiple physical devices. This improves performance by increasing throughput due to simultaneous device access.
- Mirroring—Writing the same data to multiple devices to accomplish data redundancy.
- Parity—Storing of redundant data on an additional device for the purpose of error correction in the event of device failure. Parity does not provide full redundancy, but it allows for error recovery in some scenarios.
- Spanning—Allows multiple drives to function like a larger one. For example, four 20 GB drives can be combined to appear as a single 80 GB drive.

The supported RAID levels include the following:

- 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. A minimum of one disk is required for RAID 0.

- 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. A minimum of two disks are required for RAID 1.
- 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 5 distributes parity data blocks among the disks that are part of a RAID-5 group and requires a minimum of three disks.
- RAID 6 Striped Dual Parity—Data is striped across all disks in the array and two sets of parity data are used to provide protection against failure of up to two physical disks. In each row of data blocks, two sets of parity data are stored.

  Other than addition of a second parity block, RAID 6 is identical to RAID 5 . A minimum of four disks are required for RAID 6.
- RAID 10 Mirrored and Striped—RAID 10 uses mirrored pairs of disks to provide complete data redundancy and high throughput rates through block-level striping. RAID 10 is mirroring without parity and block-level striping. A minimum of four disks are required for RAID 10.
- RAID 50 Striped Parity and Striped—Data is striped across multiple striped parity disk sets to provide high throughput and multiple disk failure tolerance. A minimum of six disks are required for RAID 50.
- 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. A minimum of eight disks are required for RAID 60.

Supported LUN Modifications

Some modifications that are made to the LUN configuration when LUNs are already deployed on an associated server are supported.

The following are the types of modifications that can be performed:

- Creation of a new virtual drive.
- Deletion of an existing virtual drive, which is in the orphaned state.
- Non-disruptive changes to an existing virtual drive. These changes can be made on an existing virtual drive without loss of data, and without performance degradation:
  - Policy changes. For example, changing the write cache policy.
  - Modification of boot parameters

The removal of a LUN will cause a warning to be displayed. Ensure that you take action to avoid loss of data.

Unsupported LUN Modifications

Some modifications to existing LUNs are not possible without destroying the original virtual drive and creating a new one. All data is lost in these types of modification, and these modifications are not supported.

Disruptive modifications to an existing virtual drive are not supported. The following are unsupported disruptive changes:

- Any supported RAID level change that can be handled through reconstruction. For example, RAID0 to RAID1.
- Increasing the size of a virtual drive through reconstruction.
- Addition and removal of disks through reconstruction.

Destructive modifications are also not supported. The following are unsupported destructive modifications:

- RAID-level changes that do not support reconstruction. For example, RAID5 to RAID1.
- Shrinking the size of a virtual drive.
- RAID-level changes that support reconstruction, but where there are other virtual drives present on the same drive group.
- Disk removal when there is not enough space left on the disk group to accommodate the virtual drive.
- Explicit change in the set of disks used by the virtual drive.

LUN Dereferencing

A LUN is dereferenced when it is no longer used by any service profile. This can occur as part of the following scenarios:

- The LUN is no longer referenced from the storage profile
- The storage profile is no longer referenced from the service profile
- The server is disassociated from the service profile
- The server is decommissioned

When the LUN is no longer referenced, but the server is still associated, re-association occurs. When the service profile that contained the LUN is disassociated, the LUN state is changed to Not in Use. When the service profile that contained the LUN is deleted, the LUN state is changed to Orphaned. When decommissioning the server, the state of all the LUNs associated with the server is changed to Not in use or Orphaned. However, no action is taken to delete the actual LUNs.

Note When LUNs are orphaned, the LUNs stay in the shared storage and the content is preserved. You can reclaim the orphan LUN to retrieve the data and attach the LUN to a new service profile.

Creating a Storage Profile

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 storage-profile** *profile-name*	Creates the specified storage profile and enters organization storage profile mode.
Step 4	UCSC(policy-mgr) /org/storage-profile # **create local-lun** *name*	Creates a local LUN with the specified name, and enters local LUN mode.
Step 5	UCSC(policy-mgr) /org/storage-profile/local-lun # **set auto-deploy**	Enables automatic deployment for the local LUN. Use the **set no-auto-deploy** command to disable.
Step 6	UCSC(policy-mgr) /org/storage-profile/local-lun # **set disk-policy-name** *policy-name*	Specifies the disk group configuration policy that you want to use.
Step 7	UCSC(policy-mgr) /org/storage-profile/local-lun # **set order** {*order_number* | **not-applicable**}	For Cisco UCS M-Series servers, you can select an order for your local LUNs. LUN order is not supported for Cisco UCSB-Series and C-Series servers.
Step 8	UCSC(policy-mgr) /org/storage-profile/local-lun # **exit**	Set the size in GB or select unspecified to expand the LUN to use the entire available disk group. For each service profile, only one LUN can use this option.
Step 9	UCSC(policy-mgr) /org/storage-profile/local-lun # **exit**	Returns to organization storage profile mode.
Step 10	UCSC(policy-mgr) /org/storage-profile # **create controller-def** *name*	Creates the specified controller definition and enters controller def mode.
Step 11	UCSC(policy-mgr) /org/storage-profile/controller-def # **enter controller-mode-config**	Enters controller configuration mode.
Step 12	UCSC(policy-mgr) /org/storage-profile/controller-def/controller-mode-config # **set protect-config** {**yes** | **no**}	Choose whether to enable configuration protection in order to prevent a service profile using this local disk policy from being associated to a server with a different physical disk configuration. If the service profile includes a local disk policy with configuration protection enabled, and there is an attempt to associate that service profile to a server that includes disks with a different local disk configuration, the association will immediately fail with a configuration mismatch error.

	Command or Action	Purpose
Step 13	UCSC(policy-mgr) /org/storage-profile/controller-def/controller-mode-config # **set raid-mode** {**any-configuration** | **no-local-storage** | **no-raid** | **raid-0-striped** | **raid-1-mirrored** | **raid-5-striped-parity** | **raid-50-striped-parity-and-striped** | **raid-6-striped-dual-parity** | **raid-60-striped-dual-parity-and-striped** | **raid-10-mirrored-and-striped**}	Set the raid level.
Step 14	UCSC(policy-mgr) /org/storage-profile/controller-def/controller-mode-config # **commit-buffer**	Commits the transaction to the system configuration.

Creating an FC Zone Profile

FC Zone Profile is a logical representation of all zoning needs for a VM, to represent a single data replication solution between a few storage arrays. An FC Zone Profile contains a collection of all endpoint WWPNs along with their VSAN and FC Zoning enabled. You can create an FC Zone Profile after meeting the following prerequisites:

- FC Zone Active option must be enabled.
- The fabric interconnects on Cisco UCS Manager must have FC switching mode turned on.
- VSANs must have FC Zoning enabled.

Procedure

	Command or Action	Purpose
Step 1	UCSC# **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope fabric**	Enters fabric interconnect configuration mode.
Step 3	UCSC(resource-mgr) /fabric # **scope domain** *unique-domain-number*	Enters the domain mode.
Step 4	UCSC(resource-mgr) /fabric/domain # **scope fabric-ep**	Enters the fabric-ep mode.
Step 5	UCSC(resource-mgr) /fabric/domain/fabric-ep # **scope fc-storage**	Enters the fc-storage mode.
Step 6	UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage # **create fc-zone-profile** *fc-zone-profile-name*	Creates an fc-zone-profile with a unique name.
Step 7	UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-strorage/fc-zone profile* # **create fc-user-zone** *fc-user-zone-name*	Creates an fc-user-zone with a unique name.

	Command or Action	Purpose
Step 8	UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-user-profile/fc-user-zone* # **create member** *member-zone-port-number*	Creates a zone member using a specific World Wide Port Number (WWPN) for the zone set.
Step 9	UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-user-profile/fc-user-zone/member* # **exit**	Exits the fc-user-zone.
Step 10	UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-user-profile/fc-user-zone/member* # **create member** *member-zone-port-number*	Creates a second zone member using a specific World Wide Port Number (WWPN) for the zone set.
Step 11	UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-user-profile/fc-user-zone/member* # **exit**	Exits the member zone.
Step 12	UCSC(resource-mgr) /fabric-ep/fc-storage/fc-zone-user-profile/fc-user-zone* # **set fc-zone-path** *fc-zone-path-variable*	Sets the member zone.
Step 13	UCSC(resource-mgr) /fabric-ep/fc-storage/fc-zone-user-profile/fc-user-zone* # **set fc-zone-vsan** *fc-zone-vsan-variable*	Sets the target VSAN.
Step 14	UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-user-profile/fc-user-zone/member* # **exit**	Exits the member zone.

FC Zone Profile

The following example shows how Cisco UCS Central creates a FC Zone Profile:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope fabric
UCSC(resource-mgr) /fabric # show domain

UCS Domain:
    Id         Ip              Name
    ---------- --------------- ----
          1008 10.193.190.120
          1009 10.193.23.230
UCSC(resource-mgr) /fabric # scope domain 1009
UCSC(resource-mgr) /fabric/domain # scope fabric-ep
UCSC(resource-mgr) /fabric/domain/fabric-ep # scope fc-storage
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage # create fc-zone-profile newzp
UC213(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile* # create fc-user-zone

  WORD  Name (Min size 2, Max size 16)
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile* # create fc-user-zone
 zoneA

UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* #
create member 20:00:00:25:B5:10:23:03
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone/member*
 # exit
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* #
create member 20:00:00:25:B4:11:23:03
```

```
UC213(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone/member*
 # exit
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* # set
  fc-zone-path  FC Zone Path
  fc-zone-vsan  FC Zone Vsan

UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* # set
 fc
fc-zone-path  fc-zone-vsan
UC213(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* # set
 fc-zone-path
  a  Fabric A
  b  Fabric B

UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* # set
 fc-zone-path A
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* # set
 fc-zone-vsan VSAN300
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile/fc-user-zone* # exit
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile* # show configuration
+enter fc-zone-profile newzp
+    disable
+    enter fc-user-zone zoneA
+        enter member 20:00:00:25:B4:11:23:03
+        exit
+        enter member 20:00:00:25:B5:10:23:03
+        exit
+        set fc-zone-path a
+        set fc-zone-vsan VSAN300
+    exit
+    set descr ""
+exit
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile* # enable
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile* # show configuration
+enter fc-zone-profile newzp
+    enable
+    enter fc-user-zone zoneA
+        enter member 20:00:00:25:B4:11:23:03
+        exit
+        enter member 20:00:00:25:B5:10:23:03
+        exit
+        set fc-zone-path a
+        set fc-zone-vsan VSAN300
+    exit
+    set descr ""
+exit
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage/fc-zone-profile* # commit-buffer
UCSC(resource-mgr) /fabric/domain/fabric-ep/fc-storage # show fc-zone-profile expand detail


    Name: 1009/newzp
    Descr:
    Admin State: Enabled
    Oper State: Ok
    Current Task:

    FC User Zone:
        Name: zoneA
        Zone Name:
        FC Zone Vsan: VSAN300
        FC Zone Path: A
        Zone ID: 0
        Config State: Not Applied
```

```
Oper State: Active

Zone Member:
    Member wwpn address: 20:00:00:25:B4:11:23:03

    Member wwpn address: 20:00:00:25:B5:10:23:03

Target VSAN:
    Name: VSAN300

        Fibre Channel Interface:
            Name: VSAN300
            Fabric ID: A
            Operational VSAN: domaingroup-root/fabric/san/A/net-VSAN300
```

Disk Groups and Disk Group Configuration Policies

Servers in a chassis can use storage that is centralized in that chassis. You can select and configure the disks to be used for storage. A logical collection of these physical disks is called a disk group. Disk groups allow you to organize local disks. The storage controller controls the creation and configuration of disk groups.

A disk group configuration policy defines how a disk group is created and configured. The policy specifies the RAID level to be used for the disk group. It also specifies either a manual or an automatic selection of disks for the disk group, and roles for disks. You can use a disk group policy to manage multiple disk groups. However, a single disk group can be managed only by one disk group policy.

Creating a Disk Group 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 disk-group-config-policy** *policy-name*	Creates the specified disk group configuration policy and enters disk group configuration policy mode.
Step 4	UCSC(policy-mgr) /org/disk-group-config-policy # **set raid-level** {**raid-0-striped** | **raid-1-mirrored** | **raid-10-mirrored-and-striped** | **raid-5-striped-parity** | **raid-50-striped-parity-and-striped** | **raid-6-striped-dual-parity** | **raid-60-striped-dual-parity-and-striped**}	Specifies the RAID level for the disk group configuration policy.

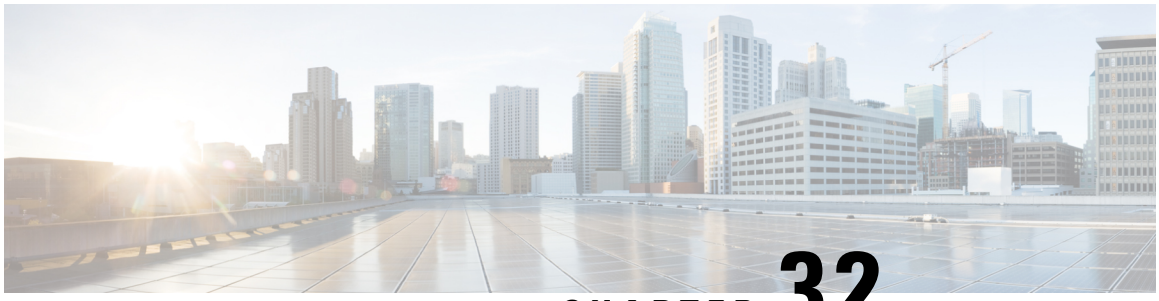
	Command or Action	Purpose
Step 5	UCSC(policy-mgr) /org/disk-group-config-policy # **create disk-group-qual**	Creates a disk group qualification policy and enters disk group qualification mode.
Step 6	UCSC(policy-mgr) /org/disk-group-config-policy/disk-group-qual # **set drive-type** {**hdd** | **ssd** | **unspecified**}	Specifies the drive type for the disk group. **Note** If you specify unspecified as the type of drive, the first available drive is selected. After this drive is selected, subsequent drives will be of a compatible type. For example, if the first was SSD, all subsequent drives would be SSD.
Step 7	UCSC(policy-mgr) /org/disk-group-config-policy/disk-group-qual # **set drive-size** {*drive_size* | **unspecified**}	Specifies the minimum drive size for the disk group. Only disks that match this criteria will be available for selection. The range for minimum drive size is from 0 to10240 GB. If you set the minimum drive size as unspecified, drives of all sizes will be available for selection.
Step 8	UCSC(policy-mgr) /org/disk-group-config-policy/disk-group-qual # **set num-ded-hot-spares** {*number_of_spares* | **unspecified**}	Specifies the number of dedicated hot spares for the disk group. The range for dedicated hot spares is from 0 to 24 hot spares. If you set the number of dedicated hot spares as unspecified, the hot spares will be selected according to the disk selection process.
Step 9	UCSC(policy-mgr) /org/disk-group-config-policy/disk-group-qual # **set num-drives** {*number_of_drives* | **unspecified**}	Specifies the number of drives for the disk group. The range for drives is from 0 to 24 drives for Cisco UCS C240, C220, C24, and C22 servers. For all other servers, the limit is 16 drives per server. If you set the number of drives as unspecified, the number of drives will be selected according to the disk selection process.
Step 10	UCSC(policy-mgr) /org/disk-group-config-policy/disk-group-qual # **exit**	Returns to disk group configuration policy mode.
Step 11	UCSC(policy-mgr) /org/disk-group-config-policy # **create local-disk-config-ref** *slot_number*	Creates a local disk configuration reference for the specified slot and enters local disk configuration reference mode.

	Command or Action	Purpose
Step 12	UCSC(policy-mgr) /org/disk-group-config-policy/local-disk-config-ref # **set role** {**dedicated-hot-spare** | **global-hot-spare** | **normal**}	Specifies the role of the local disk in the disk group.
Step 13	UCSC(policy-mgr) /org/disk-group-config-policy/local-disk-config-ref # **set span-id** {*span-id* | **unspecified**}	Specifies the ID of the span group to which the disk belongs. Disks belonging to a single span group can be treated as a single disk with a larger size. The values range from 0 to 8. You can also set the span ID as unspecified when spanning information is not required.
Step 14	UCSC(policy-mgr) /org/disk-group-config-policy/local-disk-config-ref # **exit**	Returns to disk group configuration policy mode.
Step 15	UCSC(policy-mgr) /org/disk-group-config-policy # **create virtual-drive-def**	Creates a virtual drive definition and enters the virtual drive definition mode.
Step 16	(Optional) UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def* # **set security** *value*	You can enable disk security by setting the value to Yes or No.
Step 17	UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def # **set access-policy** {**blocked** | **platform-default** | **read-only** | **read-write**}	Specifies the access policy.
Step 18	UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def # **set drive-cache** {**disable** | **enable** | **no-change** | **platform-default**}	Specifies the state of the drive cache.
Step 19	UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def # **set io-policy** {**cached** | **direct** | **platform-default**}	Specifies the I/O policy.
Step 20	UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def # **set read-policy** {**normal** | **platform-default** | **read-ahead**}	Specifies the read policy.
Step 21	UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def # **set stripe-size** {**1042kb** | **128kb** | **16kb** | **256kb** | **32kb** | **512kb** | **64kb** | **8kb** | **platform-default**}	Specifies the strip size.
Step 22	UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def # **set write-cache-policy** {**always-write-back**	Specifies the write-cache-policy.

	Command or Action	Purpose
	| **platform-default** | **write-back-good-bbu** | **write-through**}	
Step 23	UCSC(policy-mgr) /org/disk-group-config-policy/virtual-drive-def # **commit-buffer**	Commits the transaction to the system configuration.

PART VI

Network Management



CHAPTER 32

Global VLANs

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. A global VLAN is not deleted when a global service profile that references it is deleted.

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.

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.

Example

The following example shows how to create a VLAN named Administration in the domain group root and ssign it VLAN ID 15:

```
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 and assign it VLAN ID 15:

```
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.

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.

Example

The following example shows how to create two VLANs in domain group 12 and assign multicast policies:

```
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
```

Enabling Global VLANs in a Cisco UCS Manager Instance

The **publish vlan** command allows you to use global VLANs that were created in Cisco UCS Central in a Cisco UCS Manager instance without deploying a service profile.

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 domain management configuration mode.
Step 3	UCSC(resource-mgr) /domain-mgmt #**scope ucs-domain** *domain-ID*	Enters the UCS domain configuration mode for the specified domain ID. **Note** If you do not know the UCS domain ID, use the **show ucs-domain** command.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain #**publish vlan** *vlan_name* .	Pushes the selected global VLAN to the Cisco UCS Manager instance.

Example

The following example shows how to enable global VLAN globVLAN in the local domain 1008:

```
UCSC# connect resource-mgr
UCSC(resource-mgr) # scope domain-mgmt
UCSC(resrouce-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resrouce-mgr) /domain-mgmt/ucs-domain # publish vlan globVLAN

Publish Vlan is a standalone operation. You may lose any uncommitted changes in this CLI
session.
Do you want to continue? (yes/no): yes
UCSC(resource-mgr) /domain-mgmt/ucs-domain #
```

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.

Example

The following example shows how to delete the VLAN named Finance from the domain group root:

```
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.

	Command or Action	Purpose
Step 4	UCSC(resource-mgr) /org # **commit-buffer**	Commits the transaction to the system.

Example

The follwing example shows how to assign the VLAN named Administration permission to Sub-Org1:

```
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.

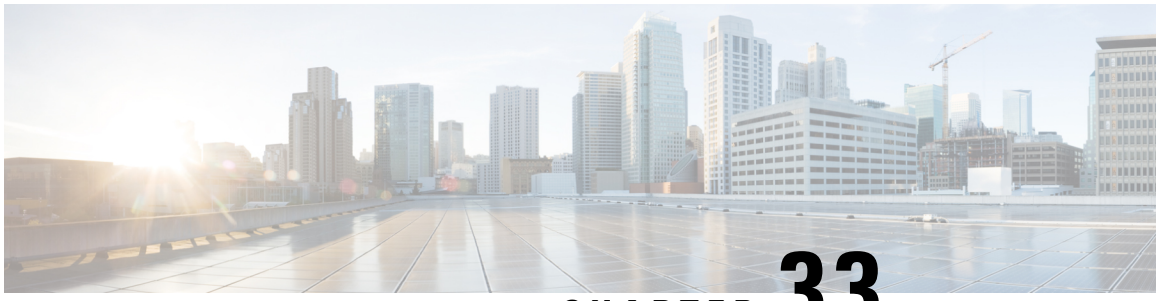
Procedure

	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.

Example

The follwing example shows how to delete permission for the VLAN named Administration from Sub-Org1:

```
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 #
```



CHAPTER 33

vNICs

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 create them automatically.

You can configure the default vNIC behavior policy to define how vNICs are created. This can be one of the following:

- **None**— 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, 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

	Command or Action	Purpose
		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.

Example

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 #
```

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.

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 cdn-source** {**user-defined** | **vnic-name**}	Specifies the source for the consistent device naming.
Step 5	UCSC(policy-mgr) /org/vnic-templ # **set cdn-name** *cnd_name*	If you selected user-defined CDN name, enter the CDN name that you want to use.
Step 6	(Optional) UCSC(policy-mgr) /org/vnic-templ # **set descr** *description*	Provides a description for the vNIC template.
Step 7	(Optional) UCSC(policy-mgr) /org/vnic-templ # **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 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 8	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 9	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 10	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 11	UCSC(policy-mgr) /org/vnic-templ # **set pin-group** *group-name*	The LAN pin group that vNICs created from this vNIC template should use.

	Command or Action	Purpose
Step 12	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 13	UCSC(policy-mgr) /org/vnic-templ # **set redundancy-peer-template-name**	Creates a name for the peer template.
Step 14	UCSC(policy-mgr) /org/vnic-templ # **set redundancy-type** {*no-redundancy* | *primary-template* | *secondary-template*	Select a redundancy type: • No-redundancy—No redundancy pair association • Primary-template—Primary template drives changes in the redundancy template • Secondary-template—Secondary template inherits common properties from template
Step 15	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 16	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 ensure that all vNIC instances are updated when the vNIC template is updated.
Step 17	UCSC(policy-mgr) /org/vnic-templ # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example configures a vNIC template:

```
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 cdn-name eth0
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

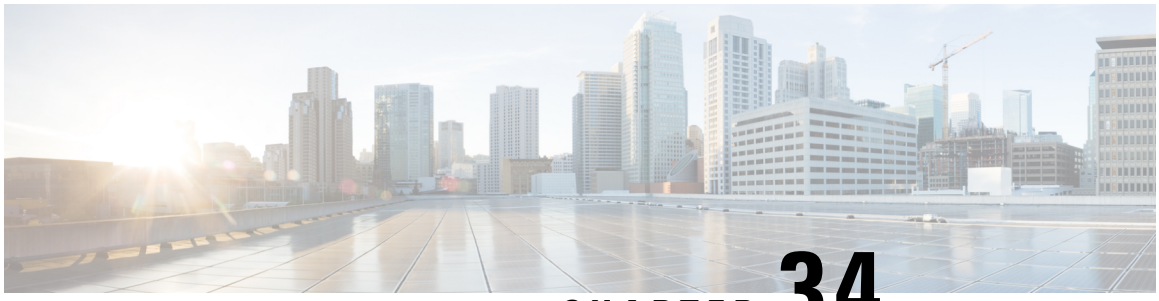
Procedure

	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.

Example

The following example deletes the vNIC template named VnicTemp42:

```
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 #
```



CHAPTER 34

Network 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 multitenancy, 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.

	Command or Action	Purpose
Step 4	(Optional) UCSC(policy-mgr) /org/mac-pool # **set descr** *description*	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.
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.

Example

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

```
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, does not reallocate any addresses from that pool that were assigned to vNICs or vHBAs. 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.

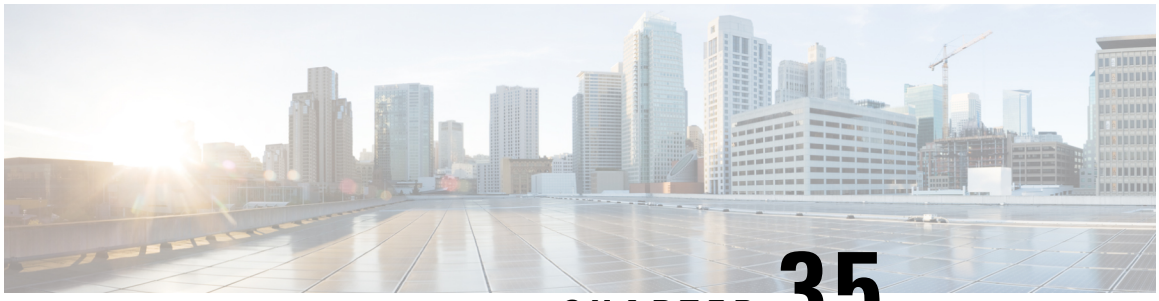
Procedure

	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 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.

Example

The following example shows how to delete the MAC pool named GPool1:

```
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 #
```



CHAPTER 35

Network 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

	Command or Action	Purpose
		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, 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.

Example

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)

```
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** *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 nw-ctrl-policy** *policy-name*	Deletes the specified network control policy.
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example deletes the network control policy named ncp5:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org /
UCSC(policy-mgr) /org # delete nw-ctrl-policy ncp5
UCSC(policy-mgr) /org* # commit-buffer
UCSC(policy-mgr) /org #
```

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 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 :

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

	Command or Action	Purpose
Step 4	(Optional) UCSC(policy-mgr) /org/eth-policy # **set arfs accelaratedrfs** {**enabled** | **disabled**}	Select whether to enable Accelerated Receive Flow Steering (ARFS).
Step 5	(Optional) UCSC(policy-mgr) /org/eth-policy # **set comp-queue count** *count*	Configures the Ethernet completion queue.
Step 6	(Optional) UCSC(policy-mgr) /org/eth-policy # **set descr** *description*	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 7	(Optional) UCSC(policy-mgr) /org/eth-policy # **set failback timeout** *timeout-sec*	Configures the Ethernet failover.
Step 8	(Optional) UCSC(policy-mgr) /org/eth-policy # **set interrupt** {**coalescing-time** *sec* | **coalescing-type** {**idle** | **min**} | **count** *count* | **mode** {**intx** | **msi** | **msi-x**}}	Configures the Ethernet interrupt.
Step 9	(Optional) UCSC(policy-mgr) /org/eth-policy # **set nvgre adminstate** {**enabled** | **disabled**}	Select whether to enable NVGRE.
Step 10	(Optional) UCSC(policy-mgr) /org/eth-policy # **set offload** {**large-receive** | **tcp-rx-checksum** | **tcp-segment** | **tcp-tx-checksum**} {**disabled** | **enabled**}	Configures the Ethernet offload.
Step 11	(Optional) UCSC(policy-mgr) /org/eth-policy # **set recv-queue** {**count** *count* | **ring-size** *size-num*}	Configures the Ethernet receive queue.
Step 12	(Optional) UCSC(policy-mgr) /org/eth-policy # **set roce adminstate** {**enabled** | **disabled**}	Select whether to enable RoCE.
Step 13	(Optional) UCSC(policy-mgr) /org/eth-policy # **set roce memoryregions** *memory_regions_number*	Specify the RoCE memory regions. This can be between 1 and 524288.
Step 14	(Optional) UCSC(policy-mgr) /org/eth-policy # **set roce queuepairs** *queue_pairs_number*	Specify the RoCE queue pairs. This can be between 1 and 8192.
Step 15	(Optional) UCSC(policy-mgr) /org/eth-policy # **set roce resourcegroups** *resource_groups_number*	Specify the RoCE queue pairs. This can be between 1 and 128.
Step 16	(Optional) UCSC(policy-mgr) /org/eth-policy # **set rss receivesidescaling** {**disabled** | **enabled**}	Configures the RSS.

	Command or Action	Purpose
Step 17	(Optional) UCSC(policy-mgr) /org/eth-policy # **set trans-queue** {**count** *count* | **ring-size** *size-num*}	Configures the Ethernet transmit queue.
Step 18	(Optional) UCSC(policy-mgr) /org/eth-policy # **set vxlan adminstate** {**enabled** | **disabled**}	Select whether to enable VXLAN.
Step 19	UCSC(policy-mgr) /org/eth-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example configures an Ethernet adapter policy:

```
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.

Example

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 #
```

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, the dynamic interface used by the vNICs fails and notifies you of that failure.

When the server comes back up, 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.

	Command or Action	Purpose
		You can enter an integer between 0 to 256 for the number of dynamic vNICs this policy affects.
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.

Example

The following example creates a dynamic vNIC connectivity policy called g-DyVCONPol-1 and sets adapter profile g-ethPol-1 to associate with the policy.

```
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.

	Command or Action	Purpose
Step 4	UCSC(policy-mgr) /org # **commit-buffer**	Commits the transaction to the system configuration.

Example

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 a usNIC 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 # **create usnic-conn-policy** *policy-name*	Creates a usNIC connection policy and enters organization usNIC mode.
Step 4	UCSC(policy-mgr) /org/usnic-conn-policy # **set adapter-profile** *profile-name*	Specifies the adapter profile that you want to use for the usNIC. We recommend that you choose the usNIC adapter profile, which is created by default.
Step 5	UCSC(policy-mgr) /org/usnic-conn-policy # **set usnic-count** *number-of-usNICs*	Specifies the number of Cisco usNICs that you want to create.
Step 6	UCSC(policy-mgr) /org/usnic-conn-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a usNIC connection policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create usnic-conn-policy usnic-pol1
UCSC(policy-mgr) /org/usnic-conn-policy* # set descr "This is a usNIC connection policy
```

```
example."
UCSC(policy-mgr) /org/usnic-conn-policy* # set adapter-profile usnic
UCSC(policy-mgr) /org/usnic-conn-policy* # set usnic-count 58
UCSC(policy-mgr) /org/usnic-conn-policy* # commit-buffer
UCSC(policy-mgr) /org/usnic-conn-policy #
```

About the 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	(Optional) UCSC(policy-mgr) /org/lan-connectivity-policy # **set descr** *policy-name*	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.

Example

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.

	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 lan-connectivity-policy** *policy-name*	Enters organization network control policy mode.
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.

Example

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.

Example

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
```

UniDirectional Link Detection (UDLD)

UniDirectional Link Detection (UDLD) is a Layer 2 protocol that enables devices connected through fiber-optic or twisted-pair Ethernet cables to monitor the physical configuration of the cables and detect when a unidirectional link exists. All connected devices must support UDLD for the protocol to successfully identify and disable unidirectional links. When UDLD detects a unidirectional link, it marks the link as unidirectional. Unidirectional links can cause a variety of problems, including spanning-tree topology loops.

UDLD works with the Layer 1 mechanisms to determine the physical status of a link. At Layer 1, autonegotiation takes care of physical signaling and fault detection. UDLD performs tasks that autonegotiation cannot perform, such as detecting the identities of neighbors and shutting down misconnected interfaces. When you enable both autonegotiation and UDLD, the Layer 1 and Layer 2 detections work together to prevent physical and logical unidirectional connections and the malfunctioning of other protocols.

A unidirectional link occurs whenever traffic sent by a local device is received by its neighbor but traffic from the neighbor is not received by the local device.

Modes of Operation

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD can detect unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD can also detect unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and to misconnected interfaces on fiber-optic links.

In normal mode, UDLD detects a unidirectional link when fiber strands in a fiber-optic interface are misconnected and the Layer 1 mechanisms do not detect this misconnection. If the interfaces are connected correctly but the traffic is one way, UDLD does not detect the unidirectional link because the Layer 1 mechanism, which is supposed to detect this condition, does not do so. In case, the logical link is considered undetermined, and UDLD does not disable the interface. When UDLD is in normal mode, if one of the fiber strands in a pair is disconnected and autonegotiation is active, the link does not stay up because the Layer 1 mechanisms did not detect a physical problem with the link. In this case, UDLD does not take any action, and the logical link is considered undetermined.

UDLD aggressive mode is disabled by default. Configure UDLD aggressive mode only on point-to-point links between network devices that support UDLD aggressive mode. With UDLD aggressive mode enabled, when a port on a bidirectional link that has a UDLD neighbor relationship established stops receiving UDLD packets, UDLD tries to reestablish the connection with the neighbor and administratively shuts down the affected port. UDLD in aggressive mode can also detect a unidirectional link on a point-to-point link on which no failure between the two devices is allowed. It can also detect a unidirectional link when one of the following problems exists:

- On fiber-optic or twisted-pair links, one of the interfaces cannot send or receive traffic.
- On fiber-optic or twisted-pair links, one of the interfaces is down while the other is up.
- One of the fiber strands in the cable is disconnected.

Methods to Detect Unidirectional Links

UDLD operates by using two mechanisms:

- Neighbor database maintenance

  UDLD learns about other UDLD-capable neighbors by periodically sending a hello packet (also called an advertisement or probe) on every active interface to keep each device informed about its neighbors. When the switch receives a hello message, it caches the information until the age time (hold time or time-to-live) expires. If the switch receives a new hello message before an older cache entry ages, the switch replaces the older entry with the new one.

  UDLD clears all existing cache entries for the interfaces affected by the configuration change whenever an interface is disabled and UDLD is running, whenever UDLD is disabled on an interface, or whenever the switch is reset. UDLD sends at least one message to inform the neighbors to flush the part of their caches affected by the status change. The message is intended to keep the caches synchronized.

- Event-driven detection and echoing

  UDLD relies on echoing as its detection mechanism. Whenever a UDLD device learns about a new neighbor or receives a resynchronization request from an out-of-sync neighbor, it restarts the detection window on its side of the connection and sends echo messages in reply. Because this behavior is the same on all UDLD neighbors, the sender of the echoes expects to receive an echo in reply.

  If the detection window ends and no valid reply message is received, the link might shut down, depending on the UDLD mode. When UDLD is in normal mode, the link might be considered undetermined and might not be shut down. When UDLD is in aggressive mode, the link is considered unidirectional, and the interface is shut down.

If UDLD in normal mode is in the advertisement or in the detection phase and all the neighbor cache entries are aged out, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbors.

If you enable aggressive mode when all the neighbors of a port have aged out either in the advertisement or in the detection phase, UDLD restarts the link-up sequence to resynchronize with any potentially out-of-sync neighbor. UDLD shuts down the port if, after the fast train of messages, the link state is still undetermined.

UDLD Configuration Guidelines

The following guidelines and recommendations apply when you configure UDLD:

- A UDLD-capable interface also cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch.
- When configuring the mode (normal or aggressive), make sure that the same mode is configured on both sides of the link.
- UDLD should be enabled only on interfaces that are connected to UDLD capable devices. The following interface types are supported:
  - Ethernet uplink

- FCoE uplink
- Ethernet uplink port channel member
- FCoE uplink port channel member

Configuring a UDLD Link 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 sub-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 udld-link-policy** *policy-name*	Creates a UDLD link policy and enters domain group UDLD link policy mode.
Step 4	UCSC(policy-mgr) /domain-group/udld-link-policy # **set mode** {**aggressive** | **normal**}	Specifies the mode for the UDLD link policy.
Step 5	UCSC(policy-mgr) /domain-group/udld-link-policy # **set admin-state** {**disabled** | **enabled**}	Enables or disables UDLD on the interface.
Step 6	UCSC(policy-mgr) /domain-group/udld-link-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create a UDLD link policy called UDLDPol1
- Set the mode to aggressive
- Enable UDLD on the interface

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create udld-link-policy UDLDPol1
UCSC(policy-mgr) /domain-group/udld-link-policy* # set mode aggressive
UCSC(policy-mgr) /domain-group/udld-link-policy* # set admin-state enabled
UCSC(policy-mgr) /domain-group/udld-link-policy* # commit-buffer
UCSC(policy-mgr) /domain-group/udld-link-policy #
```

Configuring a Link Profile

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 sub-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 eth-link-profile** *profile-name*	Creates a link profile and enters domain group link profile mode.
Step 4	UCSC(policy-mgr) /domain-group/eth-link-profile # **set udld-link-policy** *udld-link-policy-name*	Assigns the specified UDLD link policy to the link profile.
Step 5	UCSC(policy-mgr) /domain-group/eth-link-profile # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a link profile called LinkProfile1, assign the default UDLD link policy, and commit the transaction.

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # create eth-link-profile LinkProfile1
UCSC(policy-mgr) /domain-group/eth-link-profile* # set udld-link-policy default
UCSC(policy-mgr) /domain-group/eth-link-profile* # commit-buffer
UCSC(policy-mgr) /domain-group/eth-link-profile #
```

Flow Control Policy

Flow control policies determine whether the uplink Ethernet ports in a Cisco UCS domain send and receive IEEE 802.3x pause frames when the receive buffer for a port fills. These pause frames request that the transmitting port stop sending data for a few milliseconds until the buffer clears.

For flow control to work between a LAN port and an uplink Ethernet port, you must enable the corresponding receive and send flow control parameters for both ports. For Cisco UCS, the flow control policies configure these parameters.

When you enable the send function, the uplink Ethernet port sends a pause request to the network port if the incoming packet rate becomes too high. The pause remains in effect for a few milliseconds before traffic is reset to normal levels. If you enable the receive function, the uplink Ethernet port honors all pause requests from the network port. All traffic is halted on that uplink port until the network port cancels the pause request.

Because you assign the flow control policy to the port, changes to the policy have an immediate effect on how the port reacts to a pause frame or a full receive buffer.

Configuring a Flow Control Policy

Note If you have selected global port configuration for **Policy Resolution Control** in Cisco UCS Manager, then any local flow control policies will be overwritten by global flow control policies in the same domain group that have the same 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 sub-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 flow-control**	Enters domain group flow control mode.
Step 4	UCSC(policy-mgr) /domain-group/flow-control # **create policy** *flow-control-policy-name*	Creates the specified flow control policy.
Step 5	UCSC(policy-mgr) /domain-group/flow-control/policy # **set prio** {**auto** | **on**}	Specifies whether PPP is enabled or negotiated between Cisco UCS and the network.
Step 6	UCSC(policy-mgr) /domain-group/flow-control/policy # **set receive** {**off** | **on**}	Specifies whether pause requests from the network are honored or ignored.
Step 7	UCSC(policy-mgr) /domain-group/flow-control/policy # **set send** {**off** | **on**}	Specifies whether traffic flows normally regardless of the packet load, or if Cisco UCS sends pause requests if the incoming packet rate becomes too high.
Step 8	UCSC(policy-mgr) /domain-group/flow-control/policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to configure a flow control policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope domain-group /
UCSC(policy-mgr) /domain-group # scope flow-control
UCSC(policy-mgr) /domain-group/flow-control # create policy FlowCon1
```

```
UCSC(policy-mgr) /domain-group/flow-control/policy* # set prio auto
UCSC(policy-mgr) /domain-group/flow-control/policy* # set receive on
UCSC(policy-mgr) /domain-group/flow-control/policy* # set send on
UCSC(policy-mgr) /domain-group/flow-control/policy* # commit-buffer
UCSC(policy-mgr) /domain-group/flow-control #
```

Creating, Editing, or Viewing Multicast 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) # **scope domain-group** *domain-group*	Enters domain group root mode and (optionally) enters a sub-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 # **create multicast-policy***name*	Creates multicast policy for the specified organization.
Step 5	UCSC(policy-mgr) /domain-group /multicast-policy * # **set**	
Step 6	UCSC(policy-mgr) /domain-group /multicast-policy # **show detail**	Commits the transaction to the system.

Example

The following example shows how to create a multicast policy and assign it to a service profile:

```
UCSC(policy-mgr)# scope domain-group
UCSC(policy-mgr) /domain-group # create multicast-policy Multi
UCSC(policy-mgr) /domain-group/multicast-policy* # set
  querier-ip-addr       Querier IP Addr
  querier-ip-addr-peer  Querier IP Addr Peer
  querier-state         Querier State
  snooping-state        Snooping State

UCSC(policy-mgr) /domain-group/multicast-policy # show detail
Multicast Policy:
    Name: Multi
    Snooping State: Enabled
    Querier State: Disabled
    Querier IP Addr: 0.0.0.0
    Querier IP Addr Peer: 0.0.0.0
```

Deleting a Multicast Policy

Before you begin

You must have created a Multicast Policy and assigned it to a service 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) /domain-group # **delete multicast-policy***name*	Deletes the multicast policy for the specified organization.
Step 4	UCSC* # **commit-buffer**	Commits any pending transactions.

Deleting a Multicast Policy

```
UCSC(policy-mgr)/domain-group # delete multicast-policy Multi
UCSC(policy-mgr)/domain-group* # commit buffer
```

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 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 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.
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**—(Fibre Channel) 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.

	Command or Action	Purpose
		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 # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to:

- Create a QoS policy for vNIC traffic
- Assign the platinum system class
- Set the rate limit (traffic rate and burst size) for the egress policy

```
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 shows how to:

- Create a QoS policy for vHBA traffic
- Assign the FC (Fibre Channel) system class
- Set the rate limit (traffic rate and burst size) for the egress policy

```
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.

Example

The following deletes the QoS policy named QosPolicy34:

```
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 #
```

VMQ Connection Policy

VMQ provides improved network performance to the entire management operating system. From Cisco UCS Central you can create a VMQ connection policy for a vNIC on a service profile. To configure the VMQ vNIC on a service profile for a server, at least one adapter in the server must support VMQ. Make sure the servers have at least one the following adapters installed:

- UCS-VIC-M82-8P
- UCSB-MLOM-40G-01
- UCSC-PCIE-CSC-02

You must have one of the following Operating systems to use VMQ:

- Windows 2012
- Windows 2012R2

When you select the vNIC connection policy for a service profile, make sure to select one of the three options such as Dynamic, usNIC or VMQ connection policy for the vNIC. You can apply only any one of the vNIC connection policies on a service profile at any one time.

When you have selected VMQ policy on the vNIC for a service profile, you must also have the following settings in the service profile:

- Select SRIOV in the BIOS policy.
- Select Windows in the Adapter policy.

Configuring a VMQ vNIC connection policy involves the following:

- Creating a VMQ connection policy
- Creating a static vNIC in a service profile
- Applying the VMQ connection policy to the vNIC

Configuring a VMQ Connection Policy

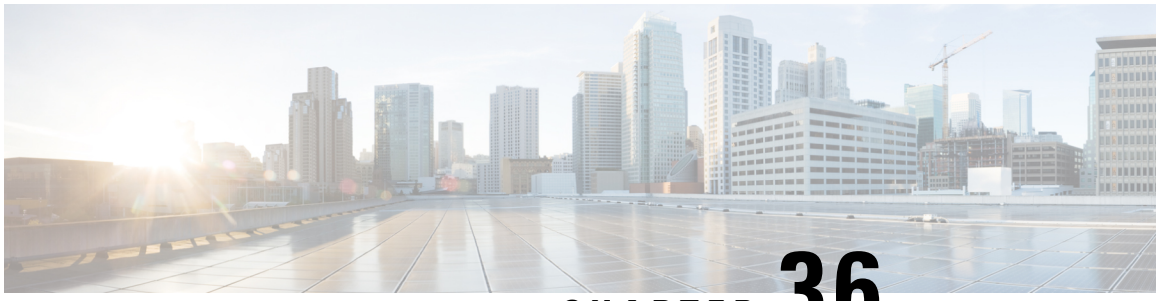
Procedure

	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, enter / as the *org-name*.
Step 3	UCSC(policy-mgr) /org # **create vmq-conn-policy** *policy-name*	Creates a VMQ connection policy and enters organization VMQ connection policy mode.
Step 4	UCSC(policy-mgr) /org/vmq-conn-policy # **set queue-count** *queue-count*	Specifies the queue count for the VMQ connection policy.
Step 5	UCSC(policy-mgr) /org/vmq-conn-policy # **set interrupt-count** *interrupt-count*	Specifies the interrupt count for the VMQ connection policy.
Step 6	UCSC(policy-mgr) /org/vmq-conn-policy # **commit-buffer**	Commits the transaction to the system configuration.

Example

The following example shows how to create a VMQ connection policy:

```
UCSC# connect policy-mgr
UCSC(policy-mgr)# scope org
UCSC(policy-mgr) /org # create vmq-conn-policy vmq-pol1
UCSC(policy-mgr) /org/vmq-conn-policy* # set descr "This is a VMQ connection policy example."
UCSC(policy-mgr) /org/vmq-conn-policy* # set queue-count 10
UCSC(policy-mgr) /org/vmq-conn-policy* # set interrupt-count 10
UCSC(policy-mgr) /org/vmq-conn-policy* # commit-buffer
UCSC(policy-mgr) /org/vmq-conn-policy #
```



CHAPTER 36

Traffic Monitoring

Traffic Monitoring

Traffic monitoring copies traffic, from one or more source ports, and sends it to a dedicated destination port for analysis by a network analyzer. This feature is also known as Switched Port Analyzer (SPAN).

Important For FC port channels on Cisco UCS 6200 Fabric Interconnects, you can monitor only egress traffic.

For FC port channels on Cisco UCS 6300 Fabric Interconnects, you can monitor only ingress traffic.

Traffic Monitoring Session Types

When you create a traffic monitoring session, you can choose either an Ethernet or Fibre Channel destination port to receive the traffic. The type of destination port determines the type of session, which in turn determines the types of available traffic sources. For an Ethernet traffic monitoring session, the destination port must be an unconfigured physical port. For a Fibre Channel traffic monitoring session, the destination port must be a Fibre Channel uplink port.

Note For Cisco UCS 6300 Fabric Interconnects, the destination port must also be an unconfigured physical Ethernet port. For Cisco UCS 6332 and Cisco UCS 6332-16UP Fabric Interconnects, you cannot choose Fibre Channel destination ports, but can use unconfigured ethernet ports as a destination for FC traffic monitoring sessions.

Traffic Monitoring Across Ethernet

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

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

Traffic Monitoring for UCS 6300 Interconnects

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

Traffic Monitoring for UCS 6200 Interconnects

- Cisco UCS 6200 and 6324 supports monitoring traffic in the transmit (tx) direction for up to two sources per Fabric Interconnect.
- Cisco UCS 6200 SPAN traffic is rate-limited by the SPAN destination port speed. This can be either 1 Gbps or 10 Gbps.

Traffic Monitoring Across Fibre Channel

You can monitor Fibre Channel traffic using either a Fibre Channel traffic analyzer or an Ethernet traffic analyzer. When Fibre Channel traffic is monitored with an Ethernet traffic monitoring session, the destination traffic is FCoE. The Cisco UCS 6300 Fabric Interconnect supports FC SPAN only on the ingress side. You cannot configure a Fibre Channel port on a Cisco Cisco UCS 6248 Fabric Interconnect as a source port.

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

Source Ports	Destination Ports
• FC Port • FC Port Channel • Uplink Fibre Channel port • SAN port channel • VSAN • Service profile vHBA • Fibre Channel storage port	• Fibre Channel uplink port • Ethernet Port (only for Cisco UCS 6300 Fabric Interconnects)

Guidelines and Recommendations for Traffic Monitoring

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

Traffic Monitoring Sessions

A traffic monitoring session is disabled by default when created. To begin monitoring traffic, you must activate the session.

- Create a unique traffic monitoring session on any fabric interconnect within the Cisco UCS pod.
- Create each monitoring session with a unique name and unique source.
- Add all vNICs from the service profile of a server to monitor traffic from a server.
- Locate all traffic sources within the same switch as the destination port.
- Do not add the same source in multiple traffic monitoring sessions.
- Do not configure a port as a destination port and a source port.
- Do not configure a member port, of a port channel, individually as a source. If you configure the port channel as a source, all member ports are source ports.

Maximum Supported Active Traffic Monitoring Sessions

You can only monitor up to four traffic directions for each Cisco UCS 6300 Fabric Interconnect. You can create and store up to 16 traffic monitoring sessions, but only four can be active at the same time for each Fabric Interconnect. The receive and transmit directions each count separately as one active session, while the bidirectional is counted as two active sessions. For example:

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

Note Traffic monitoring can impose a significant load on your system resources. To minimize the load, select sources that carry as little unwanted traffic as possible and disable traffic monitoring when it is not needed.

vNIC

Because a traffic monitoring destination is a single physical port, a traffic monitoring session can monitor only a single fabric. To monitor uninterrupted vNIC traffic across a fabric failover, create two sessions, one per fabric, and connect two analyzers. Add the vNIC as the traffic source using the exact same name for both sessions. If you change the port profile of a virtual machine, you must reconfigure the monitoring session. All associated vNICs used as source ports are removed from monitoring.

vHBA

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

SPAN Ports Support Matrix

Note For Cisco UCS 6200 and 6324 FIs, you can only set the source mode to transmit for two sources per Cisco UCS domain.

Ethernet Span Port Sources

Source Ethernet SPAN ports are supported in the following configurations:

Source Type	Source Mode		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
Ethernet Uplink	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
Ethernet Port-Channel	Receive	Receive	Receive, Transmit, Both
FCoE Uplink	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
FCoE Port-Channel	Receive	Receive	Receive, Transmit, Both
Appliance Port	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
FCoE Storage	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
Unified Ports	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both

Source Type	Source Mode		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
VLAN	Receive	Receive	Receive
Static vNIC	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both
vHBA	Receive, Transmit, Both	Receive, Transmit, Both	Receive, Transmit, Both

Ethernet Span Port Destinations

Destination Ethernet SPAN ports are supported in the following configurations:

Session Type	Admin Speed		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
Ethernet SPAN Ports	Ethernet Unconfigured at 1 Gbps, 10 Gbps	Ethernet Unconfigured at 1 Gbps, 10 Gbps	Ethernet Unconfigured at 1Gbps, 10 Gbps, 40 Gbps

FC Span Port Sources

Source FC SPAN ports are supported in the following configurations:

Source Type	Source Mode		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
FC Uplink	Transmit	Not Supported	Receive
FC Port-Channel	Transmit	Not Supported	Receive
FC Storage	Transmit	Not Supported	Receive
VSAN	Not Supported	Not Supported	Receive
vHBA	Receive, Transmit, Both	Not Supported	Receive, Transmit, Both

FC Span Port Destinations

Destination FC SPAN ports are supported in the following configurations:

Session Type	Admin Speed		
	on Cisco UCS 6200 FI	on Cisco UCS 6324 FI	on Cisco UCS 6332 FI
FC SPAN Ports	FC Uplink at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, Auto	Not Supported	FC Unconfigured at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, 16 Gbps, Auto
FC SPAN Ports	FC Monitor at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, Auto	Not Supported	FC Monitor at 1 Gbps, 2 Gbps, 4 Gbps, 8 Gbps, 16 Gbps, Auto

Setting Policy Control to Global

Before creating a traffic monitoring session in Cisco UCS Central, ensure that the port configuration is set to global on the Policy Resolution Control page.

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC (resource-mgr) # **scope system**	Enters system mode.
Step 3	UCSC(resource-mgr) /system # **show policy-control-ep**	Displays local domains registered to this system.
Step 4	UCSC(resource-mgr) /system # **scope policy-control-ep** *IP address of registered domain*	Enters the policy resolution control for the registered domain.
Step 5	UCSC(resource-mgr) /system/policy-control-ep # **set port-config-ctrl source** {*local* | *global*}	Sets the port configuration policy resolution control to local or global.
Step 6	UCSC(resource-mgr) /system/policy-control-ep* # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to set the port configuration to global:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope system
UCSC(resource-mgr) /system # show policy-control-ep

policy controlep:
    hostname or ip address
    ----------------------
    10.193.200.100

UCSC(resource-mgr) /system # scope policy-control-ep 10.193.200.100
UCSC(resource-mgr) /system/policy-control-ep # set port-config-ctrl source global
UCSC(resource-mgr) /system/policy-control-ep*# commit-buffer
UCSC(resource-mgr) /system/policy-control-ep #
```

Creating a Traffic Monitoring Session for an Ethernet Port

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope eth-traffic-mon**	Enters into ethernet traffic monitoring mode.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric # **create eth-mon-session** *session-name*	Creates the Ethernet Traffic monitoring session
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session * # **enable**	Enables the admin state for the session.
Step 8	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session # **create dest-aggr-interface** *slot ID port ID*	Aggregates the slot ID and port ID into one logical port to increase the uplink bandwidth and availability. • Slot ID—The slot ID of the interface. It must be a value between 1-5. • Port ID—The port ID of the interface. It must be a value between 1-40.
Step 9	UCSC(resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface* # **create br-dest-interface** *slot-ID*	Creates the breakout aggregrate port.
Step 10	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface* # **up**	Returns to the destination aggregate interface.
Step 11	UCSC(resource-mgr) /domain-mgmt/ucs-domain/	Commits the transaction.

	Command or Action	Purpose
	eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface/br-dest-interface* # **commit-buffer**	
Step 12	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface/br-dest-interface* # **up**	Returns to the Ethernet Traffic monitoring session.
Step 13	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session # **create dest-interface** *slot ID port ID*	Creates the destination port.
Step 14	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session/dest-interface* # **set speed**	Sets the data transfer rate of the port channel to be monitored. This can be: • 1gbps—1 Gbps • 10gbps—10 Gbps • 20gbps—20 Gbps • 40gbps—40 Gbps
Step 15	UCSC(resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session/dest-interface * # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create a traffic monitoring session named traffic1:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-traffic-mon
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric # create eth-mon-session
 traffic1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session* # enable
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session* # create
 dest-aggr-interface 2 33
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface* # create
 br-dest-interface 2
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface/br-dest-interface*
 # commit-buffer
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface/br-dest-interface*
 # up
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session # create
 dest-interface 4 22
UCSC(resource-mgr)
```

```
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-interface* # set speed
 10gbps
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-interface* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric #
```

Setting the Destination Interface and Destination Aggregate Interface for Ethernet Ports

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope eth-traffic-mon**	Enters into ethernet traffic monitoring mode.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric # **scope eth-mon-session** *session-name*	Creates the Ethernet Traffic monitoring session.
Step 7	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session # **create dest-aggr-interface** *slot ID port ID*	Aggregates the slot ID and port ID into one logical port to increase the uplink bandwidth and availability. • Slot ID—The slot ID of the interface. It must be a value between 1-5. • Port ID—The port ID of the interface. It must be a value between 1-40.
Step 8	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface* # **up**	Returns to the Ethernet Traffic monitoring session.
Step 9	UCSC (resource-mgr) /domain-mgmt/ucs-domain/	Creates the destination port.

	Command or Action	Purpose
	eth-traffic-mon/fabric/eth-mon-session # **create dest-interface** *slot ID port ID*	
Step 10	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/eth-mon-session/dest-interface* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to create a destination interface and a destination aggregate interface:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-traffic-mon
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric # scope eth-mon-session
traffic1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session # create
 dest-aggr-interface 2 33
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-aggr-interface* # up
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session # create
 dest-interface 3 23
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-interface*# show
dest-interface detail
Destination Interface:
    Slot ID: 3
    Port ID: 23
    Speed: 10 Gbps
    Admin State:
    Operational State:
    State Reason
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-interface*# commit-buffer
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/dest-interface #
```

Creating a Traffic Monitoring Session for a Fibre Channel Port

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 mode.

	Command or Action	Purpose
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-traffic-mon**	Enters into Fibre Channel traffic monitoring mode.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric # **create fc-mon-session** *session-name*	Creates the Fibre Channel Traffic monitoring session
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session * # **enable**	Enables the admin state for the session.
Step 8	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session # **create dest-aggr-interface** *slot ID port ID*	Aggregates the slot ID and port ID into one logical port to increase the uplink bandwidth and availability. • Slot ID—The slot ID of the interface. It must be a value between 1-5. • Port ID—The port ID of the interface. It must be a value between 1-40.
Step 9	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session/dest-aggr-interface* # **up**	Returns to the Fibre Channel traffic monitoring session.
Step 10	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session # **create dest-interface** *slot ID port ID*	Creates the destination port.
Step 11	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session/dest-interface* **set speed**	Sets the data transfer rate of the port channel to be monitored. This can be: • 16gbps—16 Gbps • 1gbps—1 Gbps • 2gbps—2 Gbps • 4gbps—4 Gbps • 8gbps—8 Gbps • auto—Cisco UCS determines the data transfer rate.

	Command or Action	Purpose
Step 12	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session/dest-interface* # **up**	Returns to the Fibre Channel traffic monitoring session.
Step 13	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session # **create dest-eth-interface** *slot ID port ID*	Creates an ethernet port as the destination port.
Step 14	UCSC(resource-mgr) /domain-mgmt/ucs-domain/ fc-traffic-mon/fabric/fc-mon-session/dest-eth-interface * # **commit-buffer**	Commits the transaction to the system.

Example

The following example shows how to create a traffic monitoring session:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-traffic-mon
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric # create fc-mon-session
traffic1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session* # enable
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session* # create
dest-aggr-interface 2 33
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/dest-aggr-interface* # up
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session # create
dest-interface 4 22
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/dest-interface* # up
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session* # create
dest-eth-interface 1 11
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/dest-eth-interface* #
commit-buffer
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/dest-eth-interface #
```

Adding Appliance Port as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC(resource-mgr) /domain-mgmt/ucs-domain/ # **scope eth-storage**	Scopes into Ethernet storage.
Step 5	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage # **scope fabric** {*a* | *b*}	Scopes into the Fabric Interconnect.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric # **create interface** {*interface # port #*}	Scopes into the interface.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface* # **create mon-src** *monitoring-source-name*	Creates a monitoring source.
Step 8	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface/mon-src* # **set direction** {*receive* | *transmit* | *both*}	Sets the direction for the port.
Step 9	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an appliance port as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain/ # scope eth-storage
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/ # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric # create interface 1 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface* # create mon-src
gf1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface/mon-src* # set
direction both
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-storage/fabric/interface* # commit-buffer
```

Adding an Ethernet Uplink as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope eth-uplink**	Enters into the ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-uplink # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric # **scope interface** {*interface # port #*}	Enters into the interface.
Step 7	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface # **create mon-src** *monitoring source name*	Creates a monitoring source.
Step 8	(Optional) UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface/mon-src* # **set direction** {*receive* | *transmit* | *both*}	Sets the direction for the port.
Step 9	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface/mon-src **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an ethernet uplink as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric # scope interface 2 33
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface # create mon-src
my_monsrc1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface/mon-src* # set
direction both
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface/mon-src* #
commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/interface/mon-src* #
```

Adding Ethernet Port Channel as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope eth-uplink**	Enters into the ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-uplink # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric # **create port-channel** *port ID*	Creates a port channel and scopes into it.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/port-channel* # **create mon-src** *monitoring-source-name*	Creates a monitoring source and scopes into it.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/port-channel* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an ethernet port channel as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric # create port-channel 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/port-channel # create mon-src
 my_monsrc1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/port-channel* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-uplink/fabric/port-channel* #
```

Adding Ethernet Server Port as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ # **scope eth-server**	Scopes into Ethernet storage.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-server # **scope fabric** {*a* | *b*}	Scopes into the Fabric Interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric # **create aggr-interface** {*interface # port #*}	Scopes into the aggregate interface.
Step 7	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/aggr-interface* # **create br-interface** *interface #*	Creates a breakout interface.
Step 8	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/aggr-interface/br-interface* # **up**	Scopes back into the aggregate server interface.
Step 9	UCSC (resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/aggr-interface* # **up**	Scopes back into the fabric.
Step 10	(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric* # **create interface** {*interface # port #*}	Creates and interface.
Step 11	UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/aggr-interface* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an ethernet server port as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain/ # scope eth-server
```

```
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/ # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric # create aggr-interface 1 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/aggr-interface* # create
br-interface 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/aggr-interface/br-interface*
# up
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric/aggr-interface* # up
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric* # create interface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-server/fabric* # commit-buffer
```

Adding an FC Uplink Port as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-uplink**	Enters into the ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create interface** {*slot-ID* | *por-ID*}	Creates the interface with a slot and port ID.
Step 7	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface* # **create mon-src** *monitoring-source name*	Creates a monitoring source.
Step 8	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/interface* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an Fibre Channel uplink port as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create interface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fc* # create mon-src gf1
```

```
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fc* # commit-buffer
```

Adding an FC Port Channel as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-uplink**	Enters into the ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create port-channel** *port number*	Creates a port channel and scopes into it.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel* # **create mon-src** *monitoring-source-name*	Creates a monitoring source and scopes into it.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an FC port channel as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create port-channel 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel # create mon-src
my_monsrc1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/port-channel* #
```

Adding an FC Storage Port as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-storage**	Enters into the ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-storage # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # **create interface fc** *slot IDport ID*	Creates an interface and scopes into it.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc* # **create mon-src** *monitoring-source-name*	Creates a monitoring source and scopes into it.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc/mon-src* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an FC storage port as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-storage
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # create interface fc 1 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc # create mon-src my_monsrc1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/interface* #
```

Adding an FCoE Uplink Port as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-uplink**	Enters into the ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create fcoeinterface** {*slot ID port ID*}	Creates a port channel and scopes into it.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface* # **create mon-src** *monitoring-source-name*	Creates a monitoring source and scopes into it.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an FCoE uplink port as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create fcoeinterface 1 2
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface # create mon-src
 my_monsrc1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoeinterface* #
```

Adding an FCoE Port Channel as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-uplink**	Enters into the Ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # **scope fabric** {*a* | *b*}	Enters into the Fabric Interconnect.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # **create fcoe-port-channel** *port number*	Creates a port channel and scopes into it.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel* # **create mon-src** *monitoring-source-name*	Creates a monitoring source and scopes into it.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an FCoE port channel as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-uplink
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric # create fcoe-port-channel 1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel # create
mon-src my_monsrc1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-uplink/fabric/fcoe-port-channel* #
```

Adding an FCoE Storage Port as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-storage**	Enters into the ethernet uplink.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-storage # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # **create interface fcoe** *slot IDport ID*	Creates an interface and scopes into it.
Step 7	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe* # **create mon-src** *monitoring-source-name*	Creates a monitoring source and scopes into it.
Step 8	UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fcoe/mon-src* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to add an FCoE storage port as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-storage
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric # create interface fc 1 22
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc # create mon-src my_monsrc1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc/mon-src* # commit-buffer
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-storage/fabric/fc/mon-src* #
```

Adding a vLAN as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope eth-traffic-mon**	Enters into ethernet traffic monitoring mode.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon # **scope fabric** {*a* | *b*}	Enters into the fabric interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric # **scope eth-mon-session** *session-name*	Creates the ethernet traffic monitoring session.
Step 7	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/ eth-mon-session* # **show vnic**	Displays all vNICs associated with this fabric.
Step 8	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/ eth-mon-session* # **scope vnic** *vnic-name*	Enters into the vNICs.
Step 9	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/ eth-mon-session/vnic # **create vlan-member** *vlan-member name*	Creates a vLAN member.
Step 10	UCSC (resource-mgr) /domain-mgmt/ucs-domain/ eth-traffic-mon/fabric/ eth-mon-session/vnic/vlan-member* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to configure a vlan as a monitoring source:

```
UCSC# connect resource-mgr
```

```
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope eth-traffic-mon
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric # scope eth-mon-session
traffic1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session* # scope
 vnic my_vnic1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/vnic #
create vlan-member my_vlan1
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/vnic/vlan-member* #
commit-buffer
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/eth-traffic-mon/fabric/eth-mon-session/vnic/vlan-member* #
```

Adding a vSAN as a Monitoring Source

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 mode.
Step 3	UCSC (resource-mgr) /domain-mgmt # **scope ucs-domain** *ucs-domain ID*	Enter into the specific UCS domain.
Step 4	UCSC (resource-mgr) /domain-mgmt/ucs-domain # **scope fc-traffic-mon**	Enters into Fibre Channel traffic monitoring mode.
Step 5	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon # **scope fabric** {*a*| *b*}	Enters into the fabric interconnect.
Step 6	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric # **scope fc-mon-session** *session-name*	Creates the Fibre Channel traffic monitoring session.
Step 7	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session* # **show monvsan**	Displays the monitoring vSANs.
Step 8	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session* # **scope monvsan** *monvsan-name*	Enters into the vSAN.
Step 9	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/monvsan # **create vsan-member** *vSAN-member name*	Creates a new vSAN member.

	Command or Action	Purpose
Step 10	UCSC (resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/monvsan/vsan-member* # **commit-buffer**	Commits the transaction to the buffer.

Example

The following example shows how to configure a vSAN as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr)# scope domain-mgmt
UCSC(resource-mgr) /domain-mgmt # scope ucs-domain 1008
UCSC(resource-mgr) /domain-mgmt/ucs-domain # scope fc-traffic-mon
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon # scope fabric a
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric # scope fc-mon-session
session1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session* # scope
monvsan monvsan1
UCSC(resource-mgr) /domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/monvsan #
create vsan-member my_vsan1
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/monvsan/vsan-member*#
commit-buffer
UCSC(resource-mgr)
/domain-mgmt/ucs-domain/fc-traffic-mon/fabric/fc-mon-session/monvsan/vsan-member #
```

Adding a vHBA as a Monitoring Source

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters into organization mode.
Step 3	UCSC(resource-mgr) /org # **scope service-profile** *service-profile-name*	Enters into the service profile.
Step 4	UCSC(resource-mgr) /org/service-profile* # **scope vhba** *vhba-name*	Enters into the vHBA.
Step 5	UCSC(resource-mgr) /org/service-profile/vhba* # **create mon-src** *monitoring-source-name*	Adds the vhba as a traffic monitoring source.
Step 6	UCSC(resource-mgr) /org/service-profile/vhba/mon-src* # **commit-buffer**	Commits transaction to the buffer.

Example

The following example shows how to add a vHBA as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr) # scope org
UCSC(resource-mgr) /org # scope service-profile sp1
UCSC(resource-mgr) /org/service-profile* # scope vhba test-vhba
UCSC(resource-mgr) /org/service-profile/vhba* # create mon-src gf1
UCSC(resource-mgr) /org/service-profile/vhba/mon-src* # commit-buffer
```

Adding a vNIC as a Monitoring Source

Procedure

	Command or Action	Purpose
Step 1	UCSC # **connect resource-mgr**	Enters resource manager mode.
Step 2	UCSC(resource-mgr) # **scope org**	Enters into organization mode.
Step 3	UCSC(resource-mgr) /org # **scope service-profile** *service-profile-name*	Enters into the service profile.
Step 4	UCSC(resource-mgr) /org/service-profile* # **scope vnic** *vnic-name*	Enters into the vNIC.
Step 5	UCSC(resource-mgr) /org/service-profile/vnic* # **create mon-src** *monitoring-source-name*	Adds the vNIC as a traffic monitoring source.
Step 6	UCSC(resource-mgr) /org/service-profile/vnic/mon-src* # **commit-buffer**	Commits transaction to the buffer.

Example

The following example shows how to add a vNIC as a monitoring source:

```
UCSC# connect resource-mgr
UCSC(resource-mgr) # scope org
UCSC(resource-mgr) /org # scope service-profile sp1
UCSC(resource-mgr) /org/service-profile* # scope vnic test-vnic
UCSC(resource-mgr) /org/service-profile/vnic* # create mon-src gf1
UCSC(resource-mgr) /org/service-profile/vnic/mon-src* # commit-buffer
```